Cisco Prime Infrastructure Classic View
ワイヤレス デバイス コンフィギュレーション ガイド

ソフトウェアリリース 1.4
2013 年 7 月

Text Part Number: OL-27653-04-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに

ここでは、『*Cisco Prime InfrastructureClassic View ワイヤレス デバイス コンフィギュレーション ガイド リリース 1.4*』の対象読者、目的、および表記法について説明し、関連資料を示し、必要に応じて他のマニュアルの取得方法およびテクニカル サポートの利用方法を説明します。ここでは、次の項について説明します。

対象読者

このマニュアルでは、Cisco Prime Infrastructure（Prime Infrastructure）Classic View について説明します。このガイドは、Prime Infrastructure を使用して Cisco Unified Network Solution を管理するネットワーキング専門家を対象としています。このガイドを使用するには、有線 LAN および無線 LAN に関連する概念および用語を十分に理解している必要があります。

目的

このガイドには、Prime Infrastructure を使用して Cisco Unified Network Solution を管理するときに必要な情報が記載されています。

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

- コマンドおよびキーワードは、**太字**で示しています。
- 変数は*イタリック体*で示しています。
- 文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
- [Option] > [Option]：一連のメニュー オプションを選択するときに使用します。

- 画面に表示される例およびコマンドラインは、screen フォントで示します。
- 入力する必要がある情報を例示する場合は、**太字の screen** フォントで示します。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

Prime Infrastructure および関連製品の詳細については、次の URL を参照してください。

http://www.cisco.com/cisco/web/psa/default.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

Cisco Prime Infrastructure の概要

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

Cisco Unified Network Solution

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

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

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

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

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

Prime Infrastructure について

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

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

Cisco Prime Infrastructure ユーザ インターフェイスには次のサポートされているブラウザの 1 つが必要です。

- Google Chrome 25.0、26.0、または 27.0。
- Microsoft Internet Explorer 8.0 または 9.0（Chrome プラグインを使用）。ネイティブ Internet Explorer はサポートされません。
- Mozilla ESR 17.x、17 以降。

ブラウザを実行するクライアントには、最小で 1 GB のメモリと 2 GHz のプロセッサが必要です。クライアント デバイスでは、CPU やメモリを大量に使用するアプリケーションを実行しないでください。

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

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

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

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

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

Cisco Unified Network コンポーネント

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

Cisco Prime Prime Infrastructure

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

WLAN コントローラ

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

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

サポート対象の Wireless LAN コントローラ ハードウェア モデルおよびソフトウェア バージョンの詳細については、次の URL にある『*Release Notes for Cisco Prime Infrastructure, Release 1.4*』を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.4/release/notes/cpi_rn_14.html

仮想 LAN コントローラ

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

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

仮想 LAN コントローラでサポートされていない機能

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

（注）　FlexConnect モードで屋外 AP がサポートされます。

アクセス ポイント

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

サポート対象のアクセス ポイントの詳細については、次の URL にある『*Release Notes for Cisco Prime Infrastructure, Release 1.4*』を参照してください：

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.4/release/notes/cpi_rn_14.html

組み込みアクセス ポイント

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

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

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

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

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

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

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

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

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

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

AP801 は、FlexConnect モードで使用できます。FlexConnect の詳細は、「FlexConnect の設定」（P.12-757）を参照してください。

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

アクセス ポイント通信プロトコル

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

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

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

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

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

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

ここでは、次の内容について説明します。

- 「CAPWAP 使用のガイドラインと制限」（P.1-6）
- 「Cisco Wireless LAN Controller AutoDiscovery」（P.1-6）
- 「コントローラ ディスカバリのプロセス」（P.1-7）

CAPWAP 使用のガイドラインと制限

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

Cisco Wireless LAN Controller AutoDiscovery

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

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

- オペレータは、IP アドレスによって単独のコントローラを検索できます。

- 指定した IP アドレス範囲内のネットワーク上にあるコントローラを検出します。
- コントローラ情報を Cisco Prime Infrastructure データベースに自動的に入力します。

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

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

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

コントローラ ディスカバリのプロセス

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

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

- Layer 3 CAPWAP または LWAPP ディスカバリ：アクセス ポイントとは異なるサブネット上で行われ、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IP アドレスと UDP パケットが使用されます。
- Over-The-Air Provisioning（OTAP）：この機能は Cisco 4400 シリーズ コントローラでサポートされています。この機能がコントローラ上で有効にされると（コントローラの [General] ページ）、関連付けられたアクセス ポイントすべてはワイヤレス CAPWAP または LWAPP ネイバー メッセージを送信し、新しいアクセス ポイントはこれらのメッセージからコントローラの IP アドレスを受信します。この機能はデフォルトでは無効です。すべてのアクセス ポイントをインストールする際は、無効のままにしておいてください。
- ローカルに保存されているコントローラの IP アドレス ディスカバリ：アクセス ポイントがすでにコントローラにアソシエートされている場合、プライマリ、セカンダリおよびターシャリ コントローラの IP アドレスはアクセス ポイントの不揮発性メモリに保存されます。今後の展開用にアクセス ポイントにコントローラの IP アドレスを保存するこのプロセスは、「*アクセス ポイントのプライミング*」と呼ばれます。
- DHCP サーバの検出：この機能では、DHCP オプション 43 を使用してアクセス ポイントにコントローラの IP アドレスを割り当てます。Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。
- DNS の検出：アクセス ポイントでは、ドメイン ネーム サーバ（DNS）を介してコントローラを検出できます。アクセス ポイントでこれを実行するには、CISCO-CAPWAP-CONTROLLER.*localdomain* または CISCO-LWAPP-CONTROLLER.*localdomain* への応答としてコントローラの IP アドレスを返すよう、DNS を設定する必要があります。ここで、*localdomain* はアクセス ポイント ドメイン名です。アクセス ポイントは、DHCP サーバから IP アドレスと DNS の情報を受信すると、DNS に接続し

て CISCO-CAPWAP-CONTROLLER.*localdomain* または CISCO-LWAPP-CONTROLLER.*localdomain* を解決します。DNS からコントローラの IP アドレスのリストを受信すると、アクセス ポイントはコントローラに discovery request を送信します。

Prime Infrastructure サービス

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

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

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

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

Cisco Context Aware Service ソリューション

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

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

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

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

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

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

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

Cisco Identity Service Engine ソリューション

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

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

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

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

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

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

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

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

Cisco Adaptive Wireless Intrusion Prevention Service

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

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

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

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

- wIPS ソフトウェア実行中のモビリティ サービス エンジン（MSE）：すべてのコントローラとそれらの各 wIPS モニタ モード アクセス ポイントからのアラーム集約の中央ポイント。アラーム情報とフォレンジック ファイルはアーカイブ目的でモビリティ サービス エンジンに保存されます。

- wIPS モニタ モード アクセス ポイント：攻撃検出とフォレンジック（パケット キャプチャ）機能を備えた固定チャネル スキャンを提供します。
- ローカル モード アクセス ポイント：タイムスライス型不正スキャンに加え、ワイヤレス サービスをクライアントに提供します。
- ワイヤレス LAN コントローラ : wIPS モニタ モード アクセス ポイントから受信した攻撃情報をモビリティ サービス エンジンに転送し、設定パラメータをアクセス ポイントに配布します。
- Prime Infrastructure：モビリティ サービス エンジン上での wIPS サービス設定、コントローラへの wIPS 設定内容のプッシュ、wIPS モニタ モードのアクセス ポイント設定を行う、一元化された管理プラットフォームを管理者に提供します。Prime Infrastructure は、wIPS アラーム、フォレンジック、報告の表示や、攻撃百科事典へのアクセスにも使用されます。

はじめに

この章では、システム要件、および Cisco Prime Infrastructure の設定と開始について説明します。Prime Infrastructure は、有線ネットワークとワイヤレス ネットワークを設定、管理、およびモニタするために使用されるアプリケーションです。この章の内容は、次のとおりです。

Prime Infrastructure の配信モード

Prime Infrastructure は、さまざまなパフォーマンス特性を持つ物理アプライアンスにプリインストールされます。Prime Infrastructure ソフトウェアは、専用の Prime Infrastructure アプライアンスまたは VMware サーバで実行されます。Prime Infrastructure ソフトウェア イメージはこの専用プラットフォーム上での他のパッケージまたはアプリケーションのインストールはサポートしていません。Prime Infrastructure が本来備えている拡張性によって、アプライアンスを展開に追加して、パフォーマンスと復元力を向上させることができます。

Prime Infrastructure は物理アプライアンスと仮想アプライアンスの 2 種類のモードで提供されます。ここでは、次の内容について説明します。

物理アプライアンス

物理アプライアンスは、16 GB のメモリ、および RAID レベル 5 構成で稼働する 4 台のハード ドライブを備えたデュアル Intel 2.40 GHz Xeon E5620 クアッド コア プロセッサです。物理アプライアンスは、最新の 64 ビット Red Hat Linux オペレーティング システムを実行します。

物理アプライアンスでは、最大 15000 台の Cisco Aironet Lightweight アクセス ポイント、5000 台のスタンドアロン型アクセス ポイント、5000 台のスイッチ、および 1200 台の Cisco ワイヤレス LAN コントローラがサポートされます。

（注）　Prime Infrastructure で予期したとおりの結果を得るには、ハード ディスク、電源、および内蔵冷却ファンのための復元力が組み込まれた、高いパフォーマンスの物理アプライアンスが必要です。

仮想アプライアンス

Prime Infrastructure は、下位レベルの展開のサポートに役立つように仮想アプライアンスとしても提供されます。

Prime Infrastructure 仮想アプライアンス ソフトウェアは、Open Virtualization Archive（OVA）ファイルとして配布されます。さまざまなリソースとデバイス数がサポートされる Prime Infrastructure の配布には、3 つの推奨レベルがあります。

ここでは、次の内容について説明します。

- 「超大規模な展開のための仮想アプライアンス」（P.2-12）
- 「大規模な展開のための仮想アプライアンス」（P.2-13）
- 「中規模な展開のための仮想アプライアンス」（P.2-13）
- 「小規模な展開のための仮想アプライアンス」（P.2-13）

（注）　OVA ファイルは vSphere Client から直接展開できます。展開を実行する前にアーカイブを抽出する必要はありません。

Prime Infrastructure 仮想アプライアンスは、VMware 環境でサポートされる OVF を展開するための方法のいずれかを使用してインストールできます。開始する前に、Prime Infrastructure 仮想アプライアンスの配布アーカイブが、vSphere Client を実行しているコンピュータからアクセス可能な場所にあることを確認します。

（注）　VMware 環境の設定の詳細については、VMware vSphere 4.0 のマニュアルを参照してください。

超大規模な展開のための仮想アプライアンス

この展開は、Prime Assurance を購入し、Prime Infrastructure と同じサーバで実行することを選択した場合に推奨されます。

- 最大 15000 台の Cisco Aironet Lightweight アクセス ポイント、5000 台のスタンドアロン型アクセス ポイント、5000 台のスイッチ、および 1200 台の Cisco ワイヤレス LAN コントローラがサポートされます。

- 16 vCPU。
- 16 GB のメモリ。
- ハード ドライブには、最小 1.2 TB の空きディスク領域が必要です。

（注） 上記の空きディスク領域は最小要件ですが、実行するバックアップの数に応じて、各システムで異なることがあります。

大規模な展開のための仮想アプライアンス

- 最大 15000 台の Cisco Aironet Lightweight アクセス ポイント、5000 台のスタンドアロン型アクセス ポイント、5000 台のスイッチ、および 1200 台の Cisco ワイヤレス LAN コントローラがサポートされます。
- 16 vCPU。
- 16 GB のメモリ。
- ハード ドライブでは、最小 400 GB の空きディスク領域が必要です。

（注） 上記の空きディスク領域は最小要件ですが、実行するバックアップの数に応じて、各システムで異なることがあります。

中規模な展開のための仮想アプライアンス

- 最大 7500 台の Cisco Aironet Lightweight アクセス ポイント、2500 台のスタンドアロン型アクセス ポイント、2500 台のスイッチ、および 600 台の Cisco ワイヤレス LAN コントローラがサポートされます。
- 4 vCPU。
- 12 GB のメモリ。
- ハード ドライブでは、最小 300 GB の空きディスク領域が必要です。

小規模な展開のための仮想アプライアンス

- 最大 3000 台の Cisco Aironet Lightweight アクセス ポイント、1000 台のスタンドアロン型アクセス ポイント、1000 台のスイッチ、および 240 台の Cisco ワイヤレス LAN コントローラがサポートされます。
- 4 vCPU。
- 8 GB のメモリ。
- ハード ドライブでは、最小 200 GB の空きディスク領域が必要です。

（注） すべてのサーバ レベルで、示されている Intel vCPU と同等の AMD vCPU もサポートされます。

（注）　上記の空きディスク領域は最小要件ですが、ディスク領域はいくつかの変数（バックアップなど）の影響を受けます。

（注）　Cisco UCS Server を使用して Prime Infrastructure の仮想アプライアンスを展開する場合は、UCS C シリーズまたは B シリーズを使用できます。選択するサーバが、「仮想アプライアンス」（P.2-12）の展開で指定されているプロセッサ、メモリ、およびハード ディスクの要件と一致することを確認してください。

クライアントの要件

Cisco Prime Infrastructure ユーザ インターフェイスには次のサポートされているブラウザの 1 つが必要です。

- Google Chrome 25.0、26.0、または 27.0。
- Microsoft Internet Explorer 8.0 または 9.0（Chrome プラグインを使用）。ネイティブ Internet Explorer はサポートされません。
- Mozilla ESR 17.x、17 以降。

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

ブラウザを実行するクライアントには、最小で 1 GB のメモリと 2 GHz のプロセッサが必要です。クライアント デバイスでは、CPU やメモリを大量に使用するアプリケーションを実行しないでください。

（注）　推奨される最小画面解像度は 1280 x 800 ピクセルです。

前提条件

Prime Infrastructure をインストールする前に、次の項目が完了したことを確認します。

- Prime Infrastructure に必要なハードウェアおよびソフトウェアの要件を満たしていること。
- サポートされるコントローラ、Cisco IOS ソフトウェア リリースの互換性マトリクスを確認します。

物理アプライアンスへの Prime Infrastructure のインストール

物理アプライアンスに Prime Infrastructure をインストールするには、次の手順を実行します。

ステップ 1　提供される Prime Infrastructure ソフトウェア イメージ DVD を挿入します。システムがブートし、次のコンソールが表示されます。

```
ISOLINUX 3.11 2005-09-02  Copyright (C) 1994-2005 H.Peter Anvin

           Welcome to Cisco Prime Prime Infrastructure

To boot from hard disk, press <Enter>.

Available boot options:

[1] Prime Infrastructure Installation (Keyboard/Monitor)
  [2] Prime Infrastructure Installation (Serial Console)
  [3] Recover administrator password.(Keyboard/Monitor)
  [4] Recover administrator password.(Serial Console)
  <Enter> Boot existing OS from Hard Disk.

Enter boot option and press <return>.

boot:
```

ステップ 2　Prime Infrastructure ソフトウェア イメージをインストールするには、オプション 1 を選択します。システムがリブートし、[configure appliance] 画面が表示されます。

ステップ 3　ログイン プロンプトで、**setup** コマンドを入力します。

```
localhost.localdomain login: setup
```

ステップ 4　「Prime Infrastructure の設定」（P.2-19）で説明されているように、初期設定パラメータを入力し、再度システムをリブートします。DVD を取り出し、手順に従って Prime Infrastructure サーバを起動します。

Prime Infrastructure 仮想アプライアンスの展開

この項では、[Deploy OVF] ウィザードまたはコマンド ラインを使用して vSphere Client から Prime Infrastructure 仮想アプライアンスを展開する方法について説明します。（VMware vSphere Client は vCenter Server を管理および設定するための Windows アプリケーションです）。

VMware vSphere Client からの Prime Infrastructure 仮想アプライアンスの展開

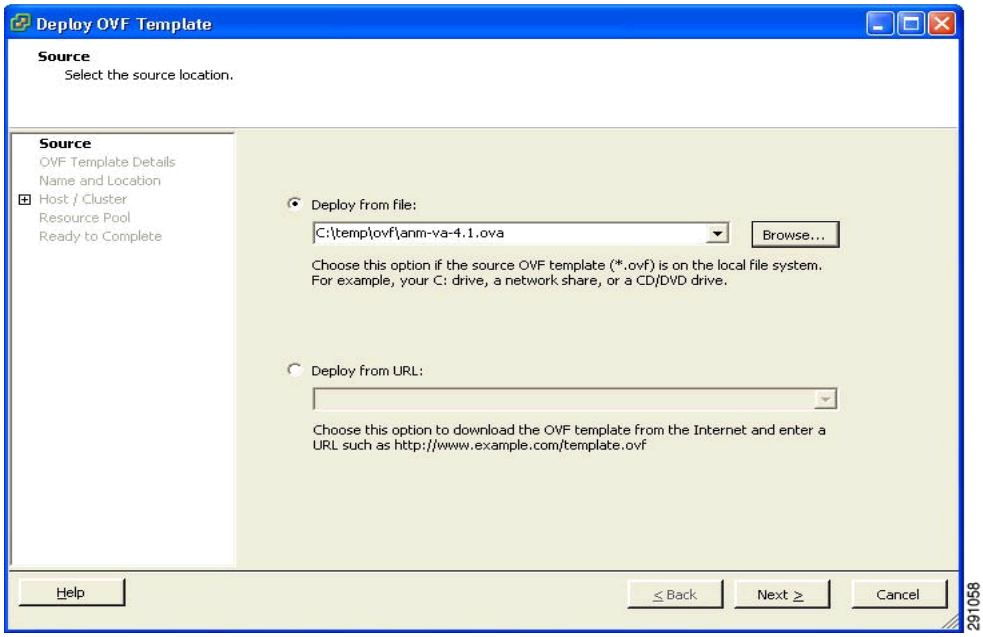
Prime Infrastructure 仮想イメージは OVA ファイルとしてパッケージされています。OVA は、項目の集合を単一のアーカイブにしたものです。vSphere Client では、この項で説明されているように、[Deploy OVF] ウィザードを使用して仮想マシンを作成し、Prime Infrastructure 仮想アプライアンス アプリケーションを実行できます。

（注）　次の手順には、Prime Infrastructure 仮想アプライアンスの展開方法に関する一般的なガイドラインが記載されていますが、実行する必要がある正確な手順は、ご使用の VMware 環境と設定の特性によって異なる可能性があります。

Prime Infrastructure 仮想アプライアンスを展開するには、次の手順を実行します。

ステップ 1　VMware vSphere Client のメイン メニューで、[File] > [Deploy OVF Template] を選択します。[Deploy OVF Template Source] ウィンドウが表示されます（図 2-1 を参照）。

図 2-1　[Deploy OVF Template] ウィンドウ

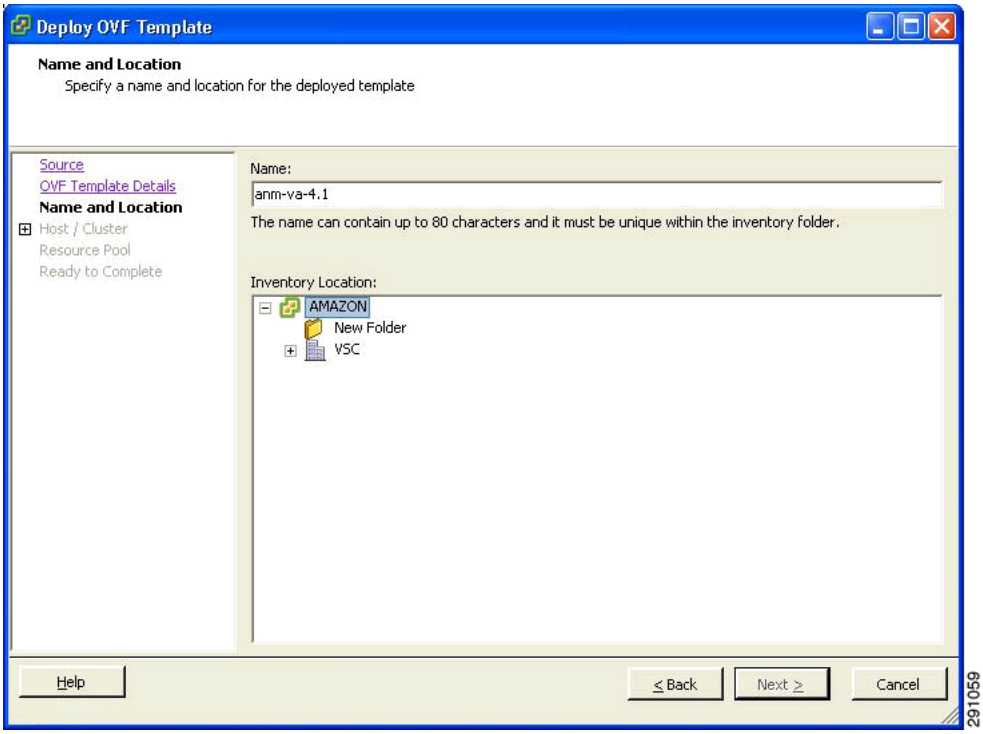


ステップ 2　[Deploy from file] を選択して、Prime Infrastructure 仮想アプライアンスの配布が含まれている OVA ファイルを選択します。

ステップ 3　[Next] をクリックします。[OVF Template Details] ウィンドウが表示されます。VMware ESX/ESXi が OVA 属性を読み取ります。詳細には、インストールする製品、OVA ファイルのサイズ（ダウンロード サイズ）、および仮想マシンに使用できる必要があるディスク領域の量（ディスクのサイズ）が含まれます。

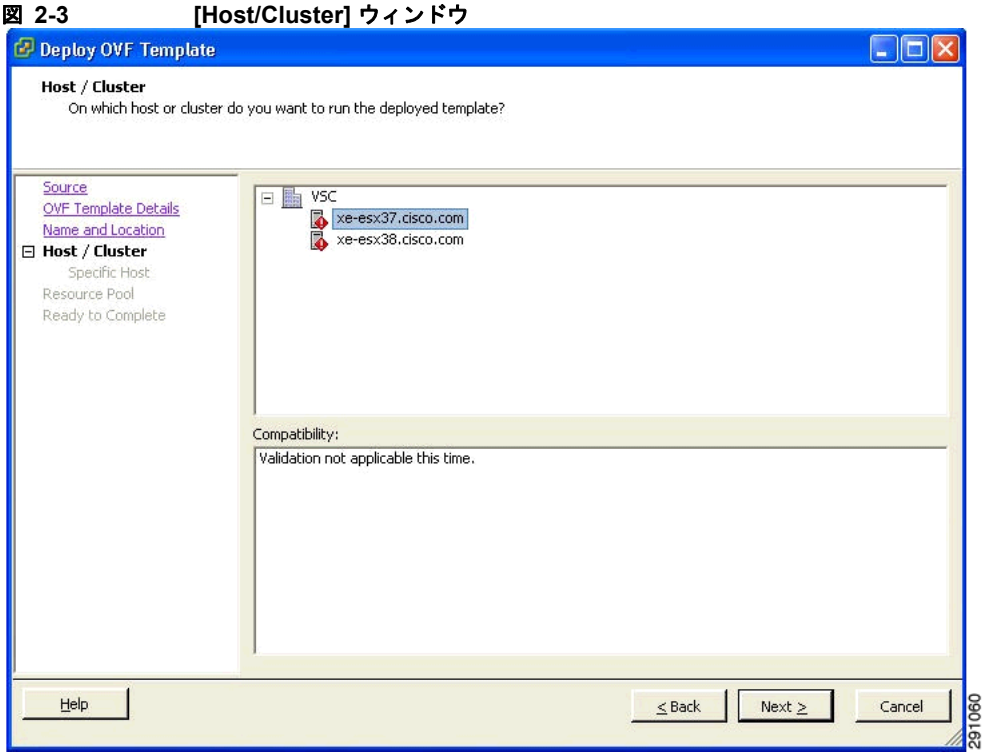
ステップ 4　OVF テンプレートの詳細を確認して、[Next] をクリックします。[Name and Location] ウィンドウが表示されます（図 2-2 を参照）。

図 2-2　[Name and Location] ウィンドウ



ステップ 5　[Name] テキスト ボックスで展開対象の VM のデフォルトの名前を維持するか、新しい名前を指定して、[Next] をクリックします。この名前値は、VMware インフラストラクチャで新しい仮想マシンを特定するために使用されます。この特定の VM をご使用の環境で区別する任意の名前を指定する必要があります。[Host / Cluster] ウィンドウが表示されます（図 2-3 を参照）。

図 2-3　[Host/Cluster] ウィンドウ



ステップ 6　Prime Infrastructure VM を展開する宛先ホストまたは HA クラスタを選択して、[Next] をクリックします。[Resource Pool] ウィンドウが表示されます。

ステップ 7　宛先ホスト環境に複数のリソース プールがある場合は、展開に使用するリソース プールを選択して、[Next] をクリックします。[Ready to Complete] ウィンドウが表示されます。

ステップ 8　展開のために表示される設定を確認して、必要に応じて [Back] をクリックして示される設定を変更します。

ステップ 9　[Finish] をクリックして、展開を完了します。インストールが完了するとメッセージで通知され、インベントリで Prime Infrastructure 仮想アプライアンスを確認できます。

ステップ 10　[Deployment Completed Successfully] ダイアログボックスを閉じるには、[Close] をクリックします。

Prime Infrastructure 仮想アプライアンスの基本設定

新規仮想マシンへの Prime Infrastructure 仮想アプライアンスの展開（インストール）が完了しました。仮想マシンのノードが、VMware vSphere Client ウィンドウのリソース ツリーに表示されるようになります。OVF テンプレートを展開すると、Prime Infrastructure 仮想アプライアンス アプリケーションと関連するリソースがすでにインストールされた新規仮想マシンが vCenter に作成されます。展開後に、Prime Infrastructure 仮想アプライアンスの基本設定を行う必要があります。Prime Infrastructure の設定を開始するには、次の手順を実行します。

ステップ 1　vSphere Client のリソース ツリーで、Prime Infrastructure **仮想アプライアンス** ノードをクリックします。仮想マシン ノードが、Prime Infrastructure 仮想アプライアンスを展開したホスト、クラスタ、またはリソース プールの下の [Hosts and Clusters] ツリーに表示されます。

ステップ 2　[Getting Started] タブで、[Basic Tasks] の下にある [Power on the virtual machine] リンクをクリックします。[vSphere Client] ペインの下部にある [Recent Tasks] ペインは、仮想マシンの電源オンに関連するタスクのステータスを示しています。仮想マシンを正常に起動した後で、タスクのステータス列に [Completed] と表示されます。

ステップ 3　キーボード入力でコンソール プロンプトをアクティブにするには、コンソール ペイン内で [Console] タブをクリックします。

次に、「Prime Infrastructure の設定」（P.2-19）の説明に従って仮想アプライアンスを設定する必要があります。

Prime Infrastructure の設定

ここでは、Prime Infrastructure 仮想アプライアンスの初期設定を行う方法について説明します。

（注）　これらの手順は、Prime Infrastructure 仮想アプライアンスの最初のインストール時に一度のみ実行する必要があります。

Prime Infrastructure 仮想アプライアンス システムの基本ネットワークとログイン設定を行うには、次の手順を実行します。手順が完了すると、Prime Infrastructure 仮想アプライアンスがネットワーク経由でアクセス可能になります。

（注）　再インストールのため、物理アプライアンスに Prime Infrastructure のイメージ DVD を入れると、同じコンソール プロンプトが表示されます。物理アプライアンスの Prime Infrastructure を再インストールするには、次の手順を使用します。

ステップ 1　ログイン プロンプトで、**setup** コマンドを入力します。

```
localhost.localdomain login: setup
```

Prime Infrastructure の設定スクリプトを起動します。スクリプトによって、Prime Infrastructure 仮想アプライアンスの初期設定手順が示されます。最初の一連の手順では、ネットワーク設定を行います。

ステップ 2　プロンプトが表示されたら、次の設定を入力します。

a.　仮想アプライアンスのホスト名。

b.　仮想アプライアンスの IP アドレス。

c.　入力した IP アドレスの IP デフォルト サブネット マスク。

d.　仮想マシンを作成するネットワーク環境のデフォルト ゲートウェイの IP アドレス。

e.　宛先環境のデフォルトの DNS ドメイン。

f.　ネットワーク内のプライマリ IP ネームサーバの IP アドレスまたはホスト名。

g.　必要に応じて、[Add/Edit another nameserver] プロンプトで、**y**（はい）と入力してネームサーバを追加します。それ以外の場合は、Enter キーを押して、続行します。

h.　NTP サーバの場所（または Enter を押して、デフォルトを受け入れます）。[Add/Edit secondary NTP server] プロンプトで、**y**（はい）を入力して、別の NTP サーバを追加できます。それ以外の場合は、**n**（いいえ）を入力して続行します。

ステップ 3　仮想マシン上で実行されている Prime Infrastructure システムにアクセスする際に使用するユーザ アカウントのユーザ名を入力します。デフォルトのユーザ名は admin ですが、ここで入力することで別のユーザ名に変更できます。

ステップ 4　Prime Infrastructure のパスワードを入力します。パスワードは 8 文字以上でなければならず、小文字と大文字の両方と、少なくとも 1 つの数字を使用する必要があります。ユーザ名を含めることはできません。パスワードの入力後に、スクリプトによって、設定したネットワーク設定が検査されます。たとえば、設定したデフォルト ゲートウェイへの到達を試行します。

ネットワーク設定の検査後に、スクリプトは Prime Infrastructure インストール プロセスを開始します。このプロセスは数分かかることがあり、その間画面フィードバックは表示されません。終了したら、次のバナーが画面に表示されます。

```
=== Initial Setup for Application: Prime Infrastructure ===
```

このバナーが表示されたら、設定がデータベース スクリプトで開始され、サーバが再起動されます。

（注）　物理アプライアンスをインストールする場合は、DVD トレイから ISO DVD を取り出します。

ステップ 5　admin としてログインして、admin のパスワードを入力します。

ステップ 6　**exit** コマンドを使用してコンソールを終了します。

Prime Infrastructure サーバの起動

ここでは、物理アプライアンスまたは仮想アプライアンスのいずれかで Prime Infrastructure を起動する手順について説明します。

（注）　Prime Infrastructure のステータスの確認はいつでもできます。指定するには、「Prime Infrastructure のステータスの確認」（P.4-118）の手順に従ってください。

物理アプライアンスまたは仮想アプライアンスへのインストール時に Prime Infrastructure を起動するには、次の手順を実行します。

ステップ 1　administrator としてシステムにログインします。

ステップ 2　コマンドライン インターフェイスを使用して、次のコマンドを入力します。

```
ncs start
```

Prime Infrastructure ユーザ インターフェイスへのログイン

Web ブラウザを介して Prime Infrastructure ユーザ インターフェイスにログインするには、次の手順を実行します。

ステップ 1　Prime Infrastructure をインストールして起動したコンピュータ以外のコンピュータでブラウザを起動します。

（注）　Firefox を使用して初めて Prime Infrastructure にログインしてアクセスすると、Firefox Web ブラウザには、このサイトが信頼できないことを示す警告が表示されます。Firefox にこの警告が表示される場合は、プロンプトに従って、セキュリティ例外を追加し、自己署名された証明書を Prime Infrastructure サーバからダウンロードします。この手順の完了後に、Firefox は、現在と将来の両方のログイン試行すべてで Prime Infrastructure サーバを信頼できるサイトとして受け入れるようになります。

ステップ 2　ブラウザのアドレス行に、https://ncs-ip-address と入力します。ここで、ncs-ip-address は、Prime Infrastructure をインストールして起動したサーバの IP アドレスです。Prime Infrastructure ユーザ インターフェイスが [Login] ページが表示されます。

ステップ 3　ユーザ名を入力します。デフォルトのユーザ名は root です。

ステップ 4　設定中に作成した root のパスワードを入力します。

（注）　ライセンスの問題が発生した場合は、アラート ボックスにメッセージが表示されます。評価ライセンスがある場合は、ライセンスの有効期限までの日数が表示されます。また、期限切れになったライセンスに対するアラートも表示されます。これらの問題に対処するには、直接ライセンス ページに移動するオプションがあります。

ステップ 5　[Login] をクリックして、Prime Infrastructure にログインします。Prime Infrastructure ユーザ インターフェイスは、これでアクティブになり、使用可能になります。Prime Infrastructure ホーム ページが表示されます。Prime Infrastructure ホーム ページでは、表示する情報を選択できます。ダッシュボードというユーザ定義のタブで情報を整理できます。デフォルトの画面にはデフォルトのダッシュボードと、それに事前に選択されたダッシュレットがそれぞれ表示されますが、これらは自由に配置できます。このホーム ページに表示する内容は、ネットワークに重要なモニタリング ダッシュレットを選択しておくことによって、事前に定義しておくことができます。たとえば、メッシュ ダッシュボードをカスタマイズできるように、メッシュ ネットワークには別のモニタリング ダッシュレットを選択できます。

（注）　データベースまたは Apache Web サーバが起動しない場合は、Linux で launchout.txt ファイルを確認してください。「failed to start database」または「failed to start the Apache web server」といった一般的なメッセージが表示されます。

（注）　アップグレードが行われると、以前のバージョンで以前のユーザが配置したユーザ定義のタブは保持されます。そのため、最新のダッシュレットが表示されないことがあります。追加された新しいダッシュレットについては、[Edit dashboard] リンクを参照してください。

ホーム ページには、カバレッジ エリア、最新の検出済み不正アクセス ポイント、アクセス ポイントの動作データ、報告されたカバレッジ ホール、時系列で示されたクライアントの分散状況など、Cisco Unified Network Solution の概要が表示されます。

デフォルトでは、Prime Infrastructure ホーム ページには、[General]、[Client]、[Security]、[Mesh]、[CleanAir]、および [ContextAware] ダッシュボードの 6 個のダッシュボードが表示されます。

（注）　Prime Infrastructure を初めて使用するときには、[Network Summary] ページに Controllers、Coverage Areas、Most Recent Rogue APs、Top 5 APs、および Most Recent Coverage Holes データベースが空であることが表示されます。また、どのクライアント デバイスもシステムに接続されていないことが表示されます。1 つ以上のコントローラで Prime Infrastructure データベースを設定した後に、更新された情報が Prime Infrastructure ホーム ページに表示されます。

Prime Infrastructure ユーザ インターフェイスを終了するには、ブラウザ ページを閉じるか、ページの右上隅にある [Log Out] をクリックします。Prime Infrastructure ユーザ インターフェイス セッションを終了しても、サーバ上の Prime Infrastructure はシャットダウンされません。

Prime Infrastructure セッション中にシステム管理者が Prime Infrastructure サーバを停止すると、セッションが終了し、Web ブラウザに「The page cannot be displayed.」というメッセージが表示されます。サーバが再起動される際に、セッションは Prime Infrastructure に再アソシエートされません。Prime Infrastructure セッションを再起動する必要があります。

Prime Infrastructure ソフトウェア ライセンスの適用

ここでは、Prime Infrastructure へのライセンスの適用方法について説明します。開始する前に、Cisco License Center からライセンスをすでに取得していて、Prime Infrastructure からネットワークでアクセス可能な場所に格納していることを確認してください。新しい Prime Infrastructure ライセンス ファイルを追加するには、次の手順を実行します。

ステップ 1　[Administrator] メニューで、[License Center] > [Files] > [Prime Infrastructure Files] ページを選択して、[Add] をクリックします。

ステップ 2　[Add a License File] ダイアログボックスで、該当するライセンス ファイルを入力するか、ブラウズして選択します。

ステップ 3　[License File] テキスト ボックスに表示されたら、[Upload] をクリックします。

新しいライセンスを追加するには、「ライセンスの管理」（P.15-924）を参照してください。

Prime Infrastructure ホーム ページについて

Prime Infrastructure ホーム ページ

- 管理者は、HTTPS Web ブラウザ ページを使用して、Cisco Unified Network Solution カバレッジ エリア レイアウトの作成と設定、システムの動作パラメータの設定、リアルタイムの Cisco Unified Network Solution 操作のモニタ、およびトラブルシューティング タスクの実行を行うことができます。
- また、ユーザ アカウントの作成、変更、および削除、パスワードの変更、権限の割り当て、および定期的なメンテナンス タスクのスケジュールを行うことができます。管理者は、ユーザ名とパスワードを新規作成して、これらを定義済みのアクセス権グループに割り当てます。
- 管理者は、必要なすべてのネットワーク管理タスクを 1 つのページから実行できます。Prime Infrastructure ホーム ページは、リアルタイム モニタリングを表示し、データのトラブルシューティングを行うランディング ページです。ページの上部にあるナビゲーション タブとメニューでは、その他すべての管理機能にポイントアンドクリック式でアクセスできます。

Prime Infrastructure ユーザ インターフェイスには、さまざまなデバイスとサービスを管理できる統合されたネットワーク管理コンソールがあります。これには、有線デバイスとクライアントおよびワイヤレス デバイスとクライアントが含まれます。サービスには、モニタリング、トラブルシューティング、およびレポート作成だけでなく、認証、許可、プロファイラ、ロケーション、およびモビリティ サービスがあります。これらすべてのデバイスとサービスは、Prime Infrastructure ホーム ページという単一のコンソールから管理できます。

ここでは、Prime Infrastructure ユーザ インターフェイス ページについて説明します。内容は次のとおりです。

ダッシュボード

Prime Infrastructure ダッシュボードは、ネットワークのヘルスとセキュリティの概要が視覚的に表示されるダッシュレットとグラフで構成されます。ダッシュボード要素は、複雑な情報を簡易なフォーマットで視覚的に伝えます。この表示により、データをすばやく分析して、必要に応じて詳細情報にドリルダウンできます。ダッシュレットは、円グラフ、スパークライン、棒グラフ、およびメトリック メーターを含むさまざまな要素を使用して、データを表示します。

ダッシュボードの基本的な目的は、Prime Infrastructure の最も重要な部分を一目でわかるようにすることです。ダッシュボードの迅速なスキャンによって、注意が必要な項目があるかどうかを把握できます。ダッシュボードには通常、ステータスとアラート、モニタリングとレポート情報が示されます。ダッシュボードには、いくつかのダッシュレットが含まれています。これは、テキスト、フォーム要素、表、グラフ、タブ、およびネストされたコンテンツ モジュールなどのさまざまなウィジェットを表示する UI コンテナです。

ダッシュボードには、クライアントの分散など、ネットワークのステータスと使用状況を反映した現在のステータスが表示されます。ダッシュボードには、クライアント数など、ある期間にわたってデータを収集する時系列の使用状況とステータスを反映したトレンドも表示されます。

（注）　Prime Infrastructure ダッシュボードにダッシュレットを表示するには、Adobe Flash Player がインストールされている必要があります。

ここでは、6 個の Prime Infrastructure ダッシュボードについて説明します。ここでは、次の内容について説明します。

- 「[Context Aware] ダッシュボード」（P.2-36）
- 「ドメインのインシデント ダッシュボード」（P.2-37）
- 「ネットワーク ダッシュボード」（P.2-37）

ネットワーク管理のニーズに応じて、事前定義されたダッシュレットのセットをカスタマイズできます。ユーザ定義のダッシュボードで情報を整理できます。デフォルト ビューには、デフォルトのダッシュボードとそれぞれに事前選択されたダッシュレットがあります。

（注）

- ダッシュレット見出しの横にあるラベル [Edited] は、ダッシュレットがカスタマイズされていることを示します。デフォルト設定にリセットすると、[Edited] ラベルはクリアされます。編集した情報を表示するには、マウス カーソルをラベルの上に移動します。
- アップグレードが行われると、前のバージョンのダッシュレットの配置が維持されます。このため、新規リリースで追加されたダッシュレットまたは機能は表示されません。新規ダッシュレットを見つけるには、[Manage Dashboards] リンクをクリックします。
- ダッシュレットをズームすると、水平方向と垂直方向のスクロールバーが表示されます。スクロールバーのないダッシュレットを表示するには、ズーム レベルをリセットしてゼロに戻すか、ズームなしにします。

[General] ダッシュボード

表 2-1 に、[General] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-1　[General] ダッシュボード

ダッシュレット	説明
Inventory Detail Status	次の項目が表示されます。 • [Controllers] : Prime Infrastructure で管理対象となっているコントローラの数を一覧表示します。到達可能なコントローラと到達不可能なコントローラをグラフで示します。 • [Switches] : Prime Infrastructure で管理対象となっているスイッチの数を一覧表示します。到達可能なスイッチと到達不可能なスイッチをグラフで示します。 • [Radios] : Prime Infrastructure で管理対象となっている無線の数を一覧表示します。停止中（重大）、マイナー（比較的重大でない）、および良好状態の無線の数をグラフで示します。このダッシュレットでは、最も重大な無線アラーム ステータスのみが反映されます。つまり、無線にマイナー アラームと重大アラームがある場合は、無線ステータスには重大と表示されます。 • [Autonomous APs] : Prime Infrastructure で管理対象となっている Autonomous AP の数を一覧表示します。到達可能な Autonomous AP と到達不可能な Autonomous AP をグラフで示します。 • [MSEs] : Prime Infrastructure で管理対象となっている MSE の数を一覧表示します。到達可能なサーバと到達不可能なサーバをグラフで示します。サーバを手動で Prime Infrastructure に追加する際に問題が発生しなかったことを確認するには、インストール ログを調べてください。（MSE のトレースをオンにしておく必要があります）。 • [Third Party Controllers] : Prime Infrastructure で管理対象となっているサードパーティのコントローラの数を一覧表示します。到達可能なサードパーティのコントローラと到達不可能なサードパーティのコントローラをグラフで示します。 • [Third Party Access Points] : Prime Infrastructure で管理対象となっているサードパーティのアクセス ポイントの数を一覧表示します。到達可能なアクセス ポイントと到達不可能なアクセス ポイントをグラフで示します。 **（注）** グラフの対応するセクションをクリックすると、インベントリの項目リスト ビューが表示されます。
Device Uptime	デバイスのアップ時間に基づいてデバイスを表示します。

表 2-1　[General] ダッシュボード （続き）

ダッシュレット	説明
Coverage Area	カバレッジ エリアごとにアクセス ポイント、無線、およびクライアントの詳細を表示します。
Top 5 Devices by Memory Utilization	メモリ使用率に基づいて上位 5 台のデバイスを表示します。
Recent Coverage Holes	カバレッジ アラームのうち、最新 5 つを表示します。
Client Count By IP Address Type	次のタイプの IP アドレスに基づいてクライアント総数を表示します。 • IPv4 Address • IPv6 Address • Dual Stack (IPv4/IPv6) Address • Unknown
Client Traffic By Address Type	IP アドレス タイプに基づいてクライアント トラフィックを表示します。 （注）　有線クライアントのトラフィック情報は使用不可であるため、これには有線クライアントのトラフィックは含まれません。
IP Address Type Distribution	クライアントの分散を IP アドレス タイプ別に表示します。

表 2-1　[General] ダッシュボード （続き）

ダッシュレット	説明
Network Device Summary	Prime Infrastructure によって管理されるデバイスすべてのステータスを表示します。このダッシュレットには、次が含まれます。 • [Total Managed Device Count]：Prime Infrastructure で管理しているすべてのデバイスを画像化したグラフまたは表を表示します。この分布はルータ、コントローラ、スイッチ、およびハブなどのデバイス ファミリに基づいています。 （注）　自律 AP とアクセス ポイントはこの円グラフまたはカウントには含まれていません。 • [AP Availability]：Prime Infrastructure によって検出されたアクセス ポイントを画像化したグラフまたは表を表示します。さらに、サードパーティ コントローラまたは Autonomous アクセス ポイントを追加した場合は検出されたアクセス ポイントを表示します。アクセス ポイントが管理上起動して場合のみアップと見なされます。 • [Total Unreachable Device Count]：Prime Infrastructure で管理されていないすべてのデバイスを画像化したグラフまたは表を表示します。この分布はルータ、コントローラ、スイッチ、およびハブなどのデバイス ファミリに基づいています。 （注）　自律 AP とアクセス ポイントはこの円グラフまたはカウントには含まれていません。「Unknown」状態のデバイスは表示されません。
Most Recent AP Alarms	アクセス ポイント アラームのうち、最新 5 つを表示します。すべてのアラームを表示する [Alarms] ページを開くには、カッコ内の番号をクリックします。
Recent Alarms	デフォルトで、アラームのうち最新 5 つを表示します。[Alarms] ページを開くには、カッコ内の番号をクリックします。
AP Uptime	アクセス ポイントがアクティブで送受信できる状態になっている時間を表示します。
CAPWAP Uptime	CAPWAP 接続がアクティブになっていた時間が表示されます。
AP Join Taken Time	アクセス ポイント名と、アクセス ポイントの加入に要した時間（日、分、および秒単位）を表示します。
GET VPN Network Status	GETVPN ネットワークのステータスを提供します。
Top 5 Devices By CPU Utilization	CPU 使用率に基づいて上位 5 台のデバイスを表示します。

表 2-1　[General] ダッシュボード （続き）

ダッシュレット	説明
License Summary By Device Type	デバイス タイプに基づいてライセンスの概要を表示します。
License Summary By License Type	ライセンス タイプに基づいてライセンスの概要を表示します。

（注）　[Life Cycle] ビューの [General] ダッシュボードに表示されるグラフのルック アンド フィールは [Classic] ビューのものとは異なります。

[Client] ダッシュボード

表 2-2 に、[Client] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-2　[Client] ダッシュボード

ダッシュレット	説明
Client Troubleshooting	クライアントの MAC アドレスを入力してから、[Troubleshoot] をクリックすることで、クライアントをトラブルシューティングできます。
Client Distribution	プロトコル、EAP タイプ、および認証別のクライアントの分散と、現在のクライアント総数を表示します。 • 802.3 は有線クライアントを表します • 802.11 はワイヤレス クライアントを表します （注）　グラフの対応するセクションをクリックすると、クライアントのユーザの項目リスト ビューが表示されます。
Client Alarms and Events Summary	クライアント アラームとイベントの要約を表示します。
Client Traffic	特定の期間におけるアップストリームとダウンストリームの両方のクライアント トラフィックのトレンドを表示します。
Client Traffic by IP Address Type	次のタイプの IP アドレスのクライアント トラフィックを表示します。 • IPv4 Upstream • IPv4 Downstream • IPv6 Upstream • IPv6 Downstream • Dual Stack (IPv4/IPv6) Upstream • Dual Stack (IPv4/IPv6) Downstream
Wired Client Speed Distribution	有線クライアントの速度と、速度ごとのクライアント数を表示します。

表 2-2　[Client] ダッシュボード （続き）

ダッシュレット	説明
Top 5 SSIDs by Client Count	上位 5 つの SSID クライアント数を表示します。
Top 5 Switches by Client Count	クライアントの数が最も多い 5 つのスイッチ、およびスイッチに関連付けられたクライアントの数を表示します。
Client Posture Status	クライアント ポスチャ ステータスと、次の各ステータス カテゴリのクライアント数を表示します。 • Compliant • Non-compliant • Unknown • Pending • Not Applicable • Error
IP Address Type Distribution	次のタイプの IP アドレスのクライアント数を表示します。 • IPv4 Upstream • IPv4 Downstream • IPv6 Upstream • IPv6 Downstream • Dual Stack (IPv4/IPv6) Upstream • Dual Stack (IPv4/IPv6) Downstream
Client Count By Association/Authentication	選択した期間内の、Prime Infrastructure 内のクライアント総数を関連と認証別に表示します。 • [Associated client] : すべてのクライアントが、認証されているかどうかに関係なく接続されています。 • [Authenticated client] : すべてのクライアントが、RADIUS または TACACS サーバ経由で接続されています。 **（注）** クライアント数には、自律クライアントが含まれます。 **（注）** 開いたポートに接続されている有線クライアントは認証済みとしてカウントされますが、オープン ポリシーのため認証は実際には起こりません。これは OPEN WLAN に接続されたワイヤレス クライアントにも適用されます。2 つのエリアがオーバーラップする場合、色はダッシュレットで混ざります。

表 2-2　[Client] ダッシュボード （続き）

ダッシュレット	説明
Client Count by Wireless/Wired	選択した期間内の、Prime Infrastructure 内のクライアント総数を有線とワイヤレス別に表示します。 （注）　クライアント数には、自律クライアントが含まれます。
Client Protocol Distribution	現在のクライアント数分散をプロトコル別表示します。
Client EAP Type Distribution	EAP タイプに基づいた数を表示します。
Guest Users Count	指定した期間にわたるゲスト クライアント数を表示します。
Client Authentication Type Distribution	認証タイプごとにクライアント数を表示します。
Top APs By Client Count	上位の AP をクライアント数別に表示します。
Most Recent Client Alarms	最新のクライアント アラームを表示します。
Recent 5 Guest User Accounts	作成または変更された最新のゲスト ユーザ アカウントを表示します。
Latest 5 logged in Guest Users	ログインする最新のゲスト ユーザを表示します。
Clients Detected by Context-Aware Service	過去 15 分間以内に Context Aware Service によって検出されたクライアント数を表示します。
Client Count By IP Address Type	各種 IP アドレス タイプ別にクライアント数のトレンドを時系列で表示します。タイプには、IPv4、IPv6、Dual-Stack、および Unknown が含まれます。
IPv6 Assignment Distribution	IPv6 アドレスがどのように割り当てられるかに基づき、すべてのクライアントの分布を表示します。タイプには Unknown、DHCPv6、Self-Assigned、SLACC、または Static などがあります。
User Auth Failure Count	ユーザ認証の失敗数の傾向を時系列で表示します。
Client CCX Distribution	異なる CCX バージョン間のクライアントの分布が表示されます。
Top N Client Count	クライアントの数に基づいて、上位 N 個の要素を表示します。要素には、SSID、AP、コントローラ、エンドポイント タイプ、ベンダー、スイッチ、アンカー コントローラが含まれます。これは異なる個別の Top N グラフを置き換える汎用 Top N グラフです。
Client Mobility Status Distribution	ローカルと固定されたクライアント間のクライアントの分布を表示します。
Client 11u Distribution	11u クライアントと non-11u クライアントを示した円グラフが表示されます。
11u Client Count	11u クライアント数の時系列のトレンドを示すグラフが表示されます。

表 2-2　[Client] ダッシュボード （続き）

ダッシュレット	説明
11u Client Traffic	11u クライアント トラフィックの時系列のトレンドを示すグラフが表示されます。
PMIP Clients Distribution	PMIP クライアントと非 PMIP クライアントを示した円グラフが表示されます。
PMIP Client Count	PMIP クライアント数の時系列のトレンドを示すグラフが表示されます。

（注）　クライアントのダッシュボードでは、「Floor Area」または「Outdoor Area」でのクライアント数には屋内および屋外の両方の領域のクライアントが含まれます。たとえば、ダッシュレットのオプションで [Floor Area] > [Above Campus] > [All buildings] > [All Floor] を選択した場合、Prime Infrastructure ではマップに割り当てられていないクライアントも含めて屋内または屋外のすべてのクライアントがリストされます。

[Security] ダッシュボード

表 2-3 に、[Security] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-3　[Security] ダッシュボード

ダッシュレット	説明
Security Index	Prime Infrastructure 管理対象ネットワークのセキュリティを示します。セキュリティ インデックスは、さまざまなセキュリティ設定にプライオリティを割り当てることで計算され、視覚的に表示されます。
Malicious Rogue APs	悪意のある不正アクセス ポイントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Unclassified Rogue APs	未分類の不正アクセス ポイントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Friendly Rogue APs	危険性のない不正アクセス ポイントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Adhoc Rogues	アドホックの不正を、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
CleanAir Security	Cleanair セキュリティ イベントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Attacks Detected	wIPS とシグニチャ攻撃を、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Cisco Wired IPS Events	有線 IPS イベントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。

表 2-3　[Security] ダッシュボード （続き）

ダッシュレット	説明
AP Threats/Attacks	アクセス ポイントに対する脅威または攻撃を、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
MFP Attacks	MFP 攻撃を、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Client Security Events	クライアント セキュリティ イベントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Recent Malicious Rogue AP Alarms	最近の悪意のある不正 AP アラームを表示します。
Most Recent Security Alarms	セキュリティ アラームのうち、最新 5 件分を表示します。[Alarms] ページを開くには、カッコ内の番号をクリックします。
Client CCX Distribution	異なる CCX バージョン間のクライアントの分布を示す円グラフが表示されます。
Top N Client Count	クライアントの数に基づいて、上位 N 個の要素を示す棒グラフを表示します。要素には、SSID、AP、コントローラ、エンドポイント タイプ、ベンダー、スイッチ、アンカー コントローラが含まれます。これは異なる個別の Top N グラフを置き換える汎用 Top N グラフです。
Client Mobility Status Distribution	ローカル（非アンカー）とアンカー間でのクライアント分布を示す円グラフを表示します。
Client 11u Distribution	11u クライアントと non-11u クライアントを示した円グラフが表示されます。
11u Client Count	11u クライアント数の時系列のトレンドを示すグラフが表示されます。
11u Client Traffic	11u クライアント トラフィックの時系列のトレンドを示すグラフが表示されます。
PMIP Clients Distribution	PMIP クライアントと非 PMIP クライアントを示した円グラフが表示されます。
PMIP Client Count	PMIP クライアント数の時系列のトレンドを示すグラフが表示されます。
Client Count By IP Address Type	各種 IP アドレス タイプ別にクライアント数のトレンドを時系列で示すチャートを表示します。タイプには、IPv4、IPv6、Dual-Stack、および unknown が含まれます。
IPv6 Assignment Distribution	IPv6 アドレスがどのように割り当てられるかに基づき、すべてのクライアントの分布を示す円グラフを表示します。タイプには Unknown、DHCPv6、Self-Assigned、SLACC、または Static などがあります。
User Auth Failure Count	ユーザ認証の失敗数の傾向を時系列で示すチャートを表示します。

（注）　通知として設定される不正アラームは、[Security] ダッシュボードには表示できません。

[Mesh] ダッシュボード

表 2-4 に、[Mesh] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-4　[Mesh] ダッシュボード

ダッシュレット	説明
Most Recent Mesh Alarms	メッシュ アラームのうち、最新 5 つを表示します。[Alarms] ページを表示するには、カッコ内の番号をクリックします。
Mesh Worst SNR Links	最低 Signal to Noise Ratio（SNR; 信号対雑音比）のリンクを表示します。データには、Parent AP Name、Child AP Name、および Link SNR が記載されます。
Mesh Worst Node Hop Count	最低ノード ホップ カウントを表示します。データには、AP Name、Hop Count、および Parent AP Name が記載されます。
Mesh Worst Packet Error Rate	最低のパケット エラー率を表示します。データには、Parent AP Name、Child AP Name、および Packet Error Rate が記載されます。
Mesh AP By Hop Count	ホップ カウントに基づいて AP を表示します。
Mesh AP Queue based on QOS	QoS に基づいて AP を表示します。
Mesh Top Over Subscribed AP	オーバーサブスクライブ型 AP を表示します。
Mesh Parent Changing AP	親の変更に基づいて最低のメッシュ AP を表示します。

[CleanAir] ダッシュボード

表 2-5 に、[Mesh] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-5　[CleanAir] ダッシュボード

ダッシュレット	説明
802.11a/n Avg Air Quality	一定期間のネットワーク全体の平均の電波品質を表す線グラフを示します。802.11 a/n 帯域での平均の電波品質を表示します。データには、時間と平均の電波品質が含まれます。
802.11b/g/n Avg Air Quality	一定期間のネットワーク全体の平均の電波品質を表す線グラフを示します。802.11 b/g/n 帯域での平均の電波品質を表示します。データには、時間と平均の電波品質が含まれます。
802.11a/n Min Air Quality	一定期間のネットワーク全体の最小の電波品質を表す線グラフを示します。802.11 a/n 帯域での最小の電波品質を表示します。データには、時間と最小の電波品質が含まれます。

表 2-5　[CleanAir] ダッシュボード （続き）

ダッシュレット	説明
802.11b/g/n Min Air Quality	一定期間のネットワーク全体の最小の電波品質を表す線グラフを示します。802.11 b/g/n 帯域での最小の電波品質を表示します。データには、時間と最小の電波品質が含まれます。
Worst 802.11a/n Interferers	802.11 a/n 帯域の最低のセキュリティ レベルとともにアクティブな干渉のリストを示します。グラフには、現在アクティブな最低の干渉のうち上位 10 個が表示されます。データには、[InterfererID]、[Type]、[Status]、[Severity]、[Affected Channels]、[Duty Cycle(%)]、[Discovered]、[Last Updated]、および [Floor] が含まれます。
Worst 802.11b/g/n Interferers	802.11 b/g/n 帯域の最低のセキュリティ レベルとともにアクティブな干渉のリストを示します。グラフには、現在アクティブな最低の干渉のうち上位 10 個が表示されます。データには、[InterfererID]、[Type]、[Status]、[Severity]、[Affected Channels]、[Duty Cycle(%)]、[Discovered]、[Last Updated]、および [Floor] が含まれます。
802.11a/n Interferer Count	選択した期間内の、すべてのチャネルでの干渉の総数を表す線グラフを表示します。802.11 a/n 帯域で干渉しているデバイスの数を表示します。データには、時間と干渉数が含まれます。 **（注）** 電波品質は、CleanAir 対応のアクセス ポイントがある、ネットワーク内のすべてのコントローラについて計算されます。レポートには、ネットワーク全体で集約された電波品質データが含まれます。
802.11b/g/n Interferer Count	選択した期間内の、すべてのチャネルでの干渉の総数を表す線グラフを表示します。802.11 b/g/n 帯域で干渉しているデバイスの数を表示します。データには、時間と干渉数が含まれます。 **（注）** 最低の干渉と干渉数のグラフの情報は、モビリティ サービス エンジン（MSE）から収集されます。MSE が使用不可の場合は、このグラフに結果は表示されません。

表 2-5　[CleanAir] ダッシュボード （続き）

ダッシュレット	説明
Recent-Security risk Interferers	各帯域のシビリティ レベルが最も深刻であるアクティブな干渉のリストを示します。ワイヤレス ネットワークでの最近のセキュリティ リスク干渉を表示します。データには、[Type]、[Severity]、[Affected Channels]、[Last Detected]、[Detected AP] が含まれます。 **（注）** このグラフには、セキュリティ アラームが有効になっている干渉に関する情報が含まれています。 このダッシュレットに示されるデータは異なる形式でも表示できます。
Recent CAS Notifications for Interferers	干渉に関する最近の CAS の通知についての情報を提供します。

[Context Aware] ダッシュボード

表 2-6 に、[Context Aware] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-6　[Context Aware] ダッシュボード

ダッシュボード	説明
MSE Historical Element Count	指定の期間のタグ、クライアント、不正 AP、不正クライアント、干渉、有線クライアント、およびゲスト クライアントの数の履歴トレンドを表示します。 **（注）** MSE 履歴数情報は、時間ベースのグラフで表示されます。時間ベースのグラフでは、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。詳細については、6-71 ページの「時間ベースのグラフ」の項を参照してください。
Rogue Elements detected by CAS	不正 AP と不正クライアントのインデックスをパーセンテージで表示します。また、1 時間、24 時間、および 24 時間を超える期間以内に各 MSE によって検出された不正 AP と不正クライアントの数も表示します。 不正 AP のインデックスは、Prime Infrastructure 上のすべての MSE で不正 AP として検出されたアクティブな追跡済み要素の合計に対するパーセンテージとして定義されます。 不正クライアントのインデックスは、Prime Infrastructure 上のすべての MSE で不正クライアントとして検出されたアクティブな追跡済み要素の合計に対するパーセンテージとして定義されます。
Location Assisted Client Troubleshooting	ロケーション アシスタンスとともにこのオプションを使用して、クライアントをトラブルシューティングできます。トラブルシューティングの基準として MAC アドレス、ユーザ名、または IP アドレスのいずれかを指定できます。 **（注）** ユーザ名、IP アドレス、および部分的な MAC アドレスベースのトラブルシューティングは、バージョン 7.0.200.0 以降を使用する MSE のみでサポートされます。 ロケーション アシストされるクライアントのトラブルシューティングの詳細については、「[Context Aware] ダッシュボード」（P.2-36）を参照してください。

表 2-6　[Context Aware] ダッシュボード （続き）

ダッシュボード	説明
MSE Tracking Counts	各要素タイプの追跡数と非追跡数を表します。要素タイプには、タグ、不正 AP、不正クライアント、干渉、有線クライアント、ワイヤレス クライアント、およびゲスト クライアントが含まれます。
Top 5 MSEs	ライセンス使用率のパーセンテージに基づいて上位 5 つの MSE を一覧表示します。また、MSE ごとに各要素タイプの数を表示します。 （注）　Prime Infrastructure ライセンスをインストールしていても、MSE を Prime Infrastructure に追加していない場合、[Context-Aware] ダッシュボードは空です。ただし、MSE を追加するためのリンクとともにメッセージが表示されます。 詳細なレポートを取得するには、ダッシュレットで数リンクをクリックします。 グラフとグリッド ビューを切り替えるには、ダッシュレット内のアイコンを使用します。 グリッドまたはグラフを全画面で表示するには、[Enlarge Chart] アイコンを使用します。

ドメインのインシデント ダッシュボード

表 2-7 に、[Domain Incident] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-7　ドメインのインシデント ダッシュボード

ダッシュボード	説明
デバイスの到達可能性ステータス	デバイスが到達可能かどうかを表示します。

ネットワーク ダッシュボード

表 2-8 に、[Network] ダッシュボードの工場出荷時のデフォルト ダッシュレットを示します。

表 2-8　ネットワーク ダッシュボード

ダッシュボード	説明
Top N CPU Utilization	CPU 使用率に基づいて上位 N 台のデバイスを表示します。
Top N Memory Utilization	メモリ使用率に基づいて上位 N 台のデバイスを表示します。

インタラクティブ グラフ

ここでは、次の内容について説明します。

インタラクティブ グラフの概要

インタラクティブ グラフ機能は、Adobe Flex テクノロジーに基づいています。このテクノロジーでは、Flash を使用してグラフをブラウザ上に表示し、ユーザによる操作を可能にします。

最低限の要件には、次のものがあります。

- Windows：Flash Player バージョン 9.0.115.0。
- Linux：Flash Player バージョン 9.0.115.0。

（注）　Flash Player がインストールされていない場合や、バージョンが古い場合には、エラー ページにその旨が表示されます。[Get Latest Flash Player] リンクをクリックして Adobe の Web サイトにアクセスします。このサイトから、最新版の Flash Player をダウンロードできます。Flash Player をダウンロードする必要があるのは一度だけです。ダウンロード後は必ずブラウザを再起動します。

Prime Infrastructure インタラクティブ グラフには、折れ線グラフ、面積グラフ、円グラフ、積み重ね表示棒グラフが含まれています。

インタラクティブ グラフの機能

インタラクティブ グラフには次の機能が含まれています。

- 次の 2 種類のグラフがあります。
  - <CrossRef> 時間ベースのグラフ
  - 時間ベースでないグラフ
- 自動更新のサポート：グラフは、事前に定義した間隔で自動的に更新されます。
- 次の 2 つのグラフ ビューがあります。
  - グラフ（チャート）ビュー（デフォルト）
  - テーブル（グリッド）ビュー

（注）　2 つのグラフ ビューの間で切り替えるには、グラフ ページの左下にある 2 つのトグル ボタンを使用します。ボタンの種類を表示するには、マウス カーソルを該当するボタンに合わせることで、ツール チップに [View in Chart] または [View in Grid] が表示されます。データをグラフに表示するには、[View in Chart] をクリックします。データを表に表示するには、[View in Grid] をクリックします。

- [Enlarged View]：グラフの右下にあるボタンをクリックすると、グラフが別のページに拡大表示されます。新しいページには、表示されるグラフの種類を変更するための、[Chart View] ボタンと [Grid View] ボタンがあります。

時間ベースのグラフ

時間ベースのグラフでは、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。タイム フレーム オプションには次のものがあります。

- [6h]：現在の時刻から最近の 6 時間分のデータを表します。データは、現在のデータベース テーブルから収集されます。
- [1d]：現在の時刻から最近の 1 日（24 時間）分のデータを表します。データは、現在のデータベース テーブルから収集されます。
- [1w]：現在の時刻から最近の 1 週間（7 日間）分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [2w]：現在の時刻から最近の 2 週間分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [4w]：現在の時刻から最近の 4 週間分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [3m]：現在の時刻から最近の 3 ヵ月間分のデータを表します。データは、日単位で集積したテーブルから収集されます。
- [6m]：現在の時刻から最近の 6 ヵ月間分のデータを表します。データは、週単位で集積したテーブルから収集されます。
- [1y]：現在の時刻から最近の 1 年間（12 ヵ月間）分のデータを表します。データは、週単位で集積したテーブルから収集されます。
- [Custom]：ユーザが選択した期間。開始日と終了日の日付と時刻を設定できます。現在のデータを使用するのか、または時間単位、日単位、週単位で集積したデータ元を使用するのかは、選択した開始日によって変わります。

（注） 集積したテーブルのデータ管理設定は、「管理設定」（P.15-851）の [Administration] メニューにあります。デフォルト設定の値は、日単位で集積したデータの場合は 31 日、週単位で集積したデータの場合は 10 週間です。

アイコン

ダッシュレットと [General]、[Client]、[Security]、[Mesh]、[CleanAir]、および [Context Aware] ダッシュボード内のアイコンには、表 2-9 に示されている次の機能があります。

表 2-9　アイコン表示

アイコン	説明
	[Dashlet Options] アイコンによって、変数と検索オプションを使用して、データをカスタマイズおよびフィルタリングできます。たとえば、SSID、フロア領域、コントローラ、特定の Autonomous AP などのクライアント数のトレンドを検索できます。
	[Refresh Dashlet] アイコンによって、現在のネットワーク ステータスを反映するように、ダッシュボードを自動的に更新できます。
	[Detach Dashlet] アイコンを使用すると、ダッシュレットを切り離すことができます。
	[Maximize Dashlet] アイコンを使用すると、完全なビューで表示されるようにダッシュレットを最大化できます。
	[collapse Dashlet] アイコンを使用すると、ダッシュレットが表示されないようにダッシュレットを最小化できます。
	[View in Chart] アイコンを使用すると、表形式ではなくグラフでダッシュレットを表示できます。
	[View in Grid] アイコンを使用すると、グラフ形式ではなく表でダッシュレットを表示できます。

メニュー バー

Prime Infrastructure で使用される主なナビゲーション方式は、Prime Infrastructure ページの上部にあるメニューです。管理者は、このメニューからさまざまなタスクをモニタおよび実行できます。このメニューは、簡単にアクセスできるポップアップ メニューであり、基本メニューに関連付けられたサブメニューにすばやくアクセスできます。関連するメニューにアクセスするには、任意のメニュー タイトルの上にマウス カーソルを移動します。メニュー タイトルをクリックすると、機能ページに直接移動します。次の図は、主要な Prime Infrastructure メニューの例です（図 2-4 を参照）。

図 2-4　Prime Infrastructure の主要なグローバル メニュー

ここでは、メニューについて説明します。取り上げる事項は次のとおりです。

- 「[Monitor] メニュー」（P.2-41）
- 「[Configure] メニュー」（P.2-41）

- 「[Services] メニュー」（P.2-42）
- 「[Reports] メニュー」（P.2-42）
- 「[Administration] メニュー」（P.2-42）

5 つのメニュー タイトルのいずれかにマウス カーソルを移動すると、ドロップダウン メニューが表示されます。

[Monitor] メニュー

[Monitor] メニューでは、ネットワーク デバイスの最上位レベルの説明が表示されます。ネットワーク、マップ、Google Earth マップ、ネットワーク デバイス（コントローラ、スイッチ、アクセス ポイント、クライアント、タグ、チョークポイント、Wi-Fi TDOA 受信機）、RRM、アラーム、およびイベントをモニタできます。

[Monitor] メニューからは次のサブメニュー オプションを使用できます。

- コントローラのモニタリング
- スイッチのモニタリング
- アクセス ポイントのモニタリング
- RFID タグのモニタリング
- チョークポイントのモニタリング
- 干渉のモニタリング
- WiFi TDOA レシーバのモニタリング
- 無線リソース管理（RRM）のモニタリング
- クライアントとユーザのモニタリング
- アラームのモニタリング
- イベントのモニタリング
- マップのモニタリング
- Google Earth マップのモニタリング

[Configure] メニュー

[Configure] メニューでは、ネットワークでテンプレート、コントローラ、アクセス ポイント、スイッチ、チョークポイント、Wi-Fi TDOA 受信機、設定グループ、オート プロビジョニング、スケジュール設定タスク、プロファイル、ACS ビュー サーバ、および TFTP サーバを設定できます。

[Configure] ドロップダウン メニューからは次のサブメニュー オプションを使用できます。

- コントローラの設定
- スイッチの設定
- 不明デバイスの設定
- アクセス ポイントの設定
- チョークポイントの設定
- Spectrum Expert の設定
- Wi-Fi TDOA 受信機の設定
- スケジュール設定タスクの設定

- ロギング オプションの設定
- wIPS プロファイルの設定
- Controller Template Launch Pad へのアクセス
- Lightweight アクセス ポイント テンプレートの設定
- Autonomous アクセス ポイント テンプレートの設定
- スイッチ位置設定テンプレートの設定
- Autonomous AP 移行テンプレートの設定
- コントローラ設定グループの設定
- ACS View Server の設定
- TFTP、FTP、SFTP サーバの設定

[Services] メニュー

[Services] メニューでは、モビリティ サービス エンジンとアイデンティティ サービス エンジンを含むモビリティ サービスを管理できます。

[Services] ドロップダウン メニューからは次のサブメニュー オプションを使用できます。

- 現在のモビリティ サービスの表示
- サービスの同期化
- 同期履歴の表示
- モビリティ サービスの通知概要の表示
- Identity Services

[Reports] メニュー

[Reports] メニューには、次のサブメニュー オプションがあります。

- レポート ラウンチ パッド
- スケジュールされた実行結果の管理
- 保存されたレポート テンプレートの管理

[Administration] メニュー

[Administration] メニューを使用すると、バックアップの作成、デバイス ステータスの確認、ネットワークの監査、MSE の同期などのタスクをスケジュールできます。さまざまなロギング モジュールを有効にして、再起動の要件を指定できる [Logging] も含まれています。パスワードの変更、グループの設定、アプリケーション セキュリティの設定などのユーザ管理では、[AAA] を選択します。[Administration] メニューから、ライセンス情報にアクセスして、ユーザ設定を行い、ハイ アベイラビリティ（Prime Infrastructure が実行されているセカンダリ バックアップ デバイス）を設定することもできます。

[Administration] ドロップダウン メニューからは次のサブメニュー オプションを使用できます。

- バックグラウンド タスクの実行
- 仮想ドメインの設定
- 管理設定

- ライセンスの管理
- アプライアンス詳細の表示
- AAA の設定
- ロギング オプションの設定
- ハイ アベイラビリティの設定
- ライセンスの管理

グローバル ツールバー

グローバル ツールバーは Prime Infrastructure ページの下部で常に使用可能であり、ツール、Prime Infrastructure オンライン ヘルプ システム、アラーム通知のサマリーへ即時にアクセスできます。使用可能なオンライン ヘルプにアクセスするには、[Help] アイコンの上にマウス カーソルを移動します（図 2-5 を参照）。

[Alarms Browser] の上にマウス カーソルを移動すると、要約された [Alarms] ページが、最近のシステム アラームのリストと、特定の特性を持つアラームをフィルタリングする機能とともに表示されます。個々のアラームに関する詳細情報にドリルダウンすることもできます。アラームの詳細については、「アラーム サマリー」（P.2-44）を参照してください。

図 2-5　　グローバル ツールバー

ここでは、次の内容について説明します。

- 「Tools」（P.2-43）
- 「Help」（P.2-43）

Tools

[Tools] メニューからは、Prime Infrastructure の [Voice Audit]、[Configuration Audit]、および [Migration Analysis] 機能にアクセスできます。

[Tools] ドロップダウン メニューからは次のサブメニュー オプションを使用できます。

- Voice Audit
- Location Accuracy Tools
- Config Audit
- Migration Analysis
- TAC Case Attachment

Help

[Help] メニューでは、オンライン ヘルプと学習モジュールへのアクセス、フィードバックの送信、および現在のバージョンの Prime Infrastructure の確認を行うことができます。[Help] アイコンは、Prime Infrastructure ページのグローバル ツールバーの左下隅にあります。[Help] からは、Prime Infrastructure の包括的なオンライン ヘルプにすばやくアクセスできます。

[Help] ドロップダウン メニューからは次のサブメニュー オプションを使用できます。

- [Online Help]：オンライン ヘルプを表示できます。オンライン ヘルプはコンテキスト ヘルプであり、現在開いている Prime Infrastructure ウィンドウのマニュアルを開きます。
- [Learning Modules]：特定の Prime Infrastructure 機能の短いビデオ クリップにアクセスできます。Cisco Prime Infrastructure の機能の詳細については、Cisco.com にアクセスして、Prime Infrastructure 設定ワークフロー、モニタリング、およびトラブルシューティングなどに関するマルチメディア プレゼンテーションをご覧ください。将来のリリースでは、学習を強化するために、他の概要および技術プレゼンテーションが追加されます。
- [MSE Installation Guide]：MSE インストール セクションへのリンクがあります。
- [Submit Feedback]：Prime Infrastructure に関するフィードバックを入力できるページにアクセスできます。
- [Help Us Improve Cisco Products]：お客様とお客様の組織が Cisco ワイヤレス製品を使用する方法に関するデータを自動収集するための許可を付与できます。このデータは、製品のパフォーマンスと可用性を向上させるために有益です。データは自動的に収集され、暗号化された形式で Cisco に送信されます。データには、お客様の組織に関する情報が含まれていることがあります。そのようなデータが、Cisco の外部で共有されたり使用されたりすることはありません。

（注）　自動化されたフィードバックを有効にするには、[Administration] > [Settings] > [Mail Server Configuration] を選択して、メール サーバを設定する必要があります。

- [About Cisco Prime Infrastructure]：実行している Prime Infrastructure のバージョンを確認できます。バージョン、ホスト名、機能、AP 制限値、およびタイプが表示されます。

Prime Infrastructure のバージョンを確認するには、[About Cisco Prime Infrastructure] を選択します。次の情報が表示されます。

- 製品名
- バージョン番号
- ホスト名
- 機能
- AP 制限値
- ライセンス タイプ
- 著作権宣言文

アラーム サマリー

Prime Infrastructure は、コントローラからアラーム メッセージを受信すると、Prime Infrastructure ページの下部にアラーム インジケータを表示します（図 2-6 を参照）。アラームは、注意が必要な要素の現在の障害またはステートを示し、通常、1 つ以上のイベントにより生成されます。アラームをクリアすることはできますが、イベントは残ります。アラーム ダッシュボードには、重大（赤）、やや重大（オレンジ）、比較的重大でない（黄）の各アラームが、左から右の順に表示されます。

（注）　[Administration] > [Settings] > [Alarms] ページには [Hide Acknowledged Alarms] チェックボックスがあります。承認したアラームを Prime Infrastructure およびアラーム リスト ページに表示する場合は、このチェックボックスをオフにする必要があります。デフォルトでは、承認済みアラームは表示されません。

図 2-6　Prime Infrastructure のアラーム サマリー

（注）　アラーム数は 15 秒ごとに更新されます。

360 度ビューの使用

360 度ビューは、デバイスのステータス、インターフェイスのステータス、および関連付けられたデバイス情報など、詳細なデバイス情報を提供します。デバイスの IP アドレスが表示されているほぼすべての画面で、360 度ビューを表示できます。

デバイスの 360 度ビューを起動するには、デバイスの IP アドレスの上にカーソルを置き、表示されるアイコンをクリックします。

（注）　360 度ビューに表示される機能は、デバイス タイプによって異なります。

表 2-10　360 度機能

360 度ビューの機能	説明
Device status	デバイスが到達可能かどうか、管理されているかどうか、および Prime Infrastructure データベースと同期されているかどうかを示します。
[Tool] アイコン	Alarm Browser の起動、デバイスへの ping 送信、デバイスでの traceroute の実行を行えます。
[Modules] タブ	デバイス モジュールと、それらの名前、タイプ、状態、およびポートがリストされます。
[Alarms] タブ	アラーム ステータス、タイム スタンプ、およびカテゴリなど、デバイスのアラームがリストされます。
[Interfaces] タブ	デバイス インターフェイスと、各インターフェイスの上位 3 つのアプリケーションがリストされます。
Neighbors	デバイスのインデックス、ポート、デュプレックス ステータス、およびシステム名など、デバイスのネイバーがリストされます。

フィルタ

フィルタ機能を使用して、Prime Infrastructure インターフェイスで特定の情報を表示できます。データが表形式で表示されるときは常に [Filter] アイコンが表示されます。次のタイプのフィルタを使用できます。

- 「クイック フィルタ」（P.2-46）
- 「拡張フィルタ」（P.2-46）

クイック フィルタ

このフィルタを使用すると、フィルタを特定のテーブル列に適用することで、テーブル内のデータを絞り込むことができます。さまざまな演算子を適用するには、[Advanced Filter] オプションを使用します。

クイック フィルタを起動するには、[Filter] ドロップダウン メニューから [Quick Filter] を選択します。

クイック フィルタをクリアするには、[Filter] ボタンをクリックします。

拡張フィルタ

このフィルタを使用すると、Does not contain、Does not equal、Ends with、Is empty など、複数の演算子を使用してフィルタを適用することによって、表内のデータを絞り込むことができます。たとえば、ドロップダウン メニューからフィルタ パターン（テーブル列名ごと）と演算子を選択できます。さらに、Prime Infrastructure データベースで使用可能なデータに基づいて、フィルタ基準を入力する必要があります。

拡張フィルタを起動するには、[Filter] ドロップダウン メニューから [Advance Filter] を選択します。

図 2-7　　拡張フィルタ

拡張フィルタで使用するフィルタ基準を保存するには、次の手順に従います（図 2-7 を参照）。

1. 拡張フィルタ基準を入力して、[Go] をクリックします。

   フィルタ基準に基づいて、データがフィルタリングされます。

2. [Save] アイコンをクリックします。

   [Save Preset Filter] ウィンドウが表示されます。

3. 現在のフィルタの名前を入力し、[Save] をクリックします。

コマンド ボタン

Prime Infrastructure ユーザ インターフェイスでは、ページ全体で多数のコマンド ボタンが使用されます。最も一般的なコマンド ボタンは次のとおりです。

- [Apply]：選択した情報を適用します
- [Delete]：選択した情報を削除します
- [Cancel]：現在のページで入力した新しい情報をキャンセルして、前のページに戻ります
- [Save]：現在の設定を保存します
- [Audit]：このアクセス ポイントの現在のステータスを検出します
- [Place AP]：Prime Infrastructure データベース デバイスの設定間の相違にフラグを立てることによって、選択したエンティティの設定を監査します

メイン データ ページ

メイン データ ページは、必要なパラメータ情報によって決定されます。データ ページのアクティブ領域には、次のものが含まれます。

- データを入力できるテキスト ボックス
- いくつかのオプションのうちの 1 つを選択できるドロップダウン リスト
- 表示されたリストから 1 つ以上の項目を選択できるチェックボックス
- パラメータをオンまたはオフにできるオプション ボタン
- Prime Infrastructure ユーザ インターフェイスの別のページへ移動できるハイパーリンク

入力テキスト ボックスは、白い背景の黒のテキストです。データを入力または選択しても、コントローラには送信されませんが、[Go] をクリックするまでテキスト ボックスに保存されます。

管理要素

次に、現在の Prime Infrastructure ユーザに関する情報を示します。

- [User] : 現在の Prime Infrastructure ユーザのユーザ名を示します。ユーザのパスワードを変更するには、[User] リンクをクリックします。詳細については、「パスワードの変更」（P.15-889）を参照してください。
- [Virtual Domain] : この Prime Infrastructure ユーザの現在の仮想ドメインを示します。詳細については、「仮想ドメインの設定」（P.15-842）を参照してください。

（注） ドメイン名を切り替えるには、仮想ドメイン名の右側にある青い反転された三角形アイコンをクリックして、[switch to another Virtual Domain] ページを開きます。[new virtual domain] オプション ボタンを選択して、[Save] をクリックします。それに従って権限が変更されます。

アイコン	説明
	Prime Infrastructure オンライン ヘルプにアクセスする場合にクリックします。 **（注）** オンライン ヘルプは、現在の Prime Infrastructure バージョンに適した情報を提供します。
	現在の Prime Infrastructure バージョンでデータを更新する場合にクリックします。
	現在の Prime Infrastructure の印刷に適したバージョンにアクセスする場合にクリックします。 **（注）** [Print] をクリックして現在の Prime Infrastructure バージョンを印刷するか、[Exit Print View] をクリックして前のページに戻ります。
	ダッシュボードを編集するか、Prime Infrastructure で新しいダッシュボードを追加する場合にクリックします。

Prime Infrastructure ホーム ページのカスタマイズ

Prime Infrastructure ホーム ページ ダッシュレットには、カスタマイズできる、デフォルトの事前定義されたダッシュレットのリストが含まれています。Prime Infrastructure ホーム ページでは、次のカスタマイズが可能です。

- ダッシュレットのドラッグ アンド ドロップ
- ダッシュボードの追加または削除
- ダッシュボードの並べ替え
- ダッシュレットとダッシュボードの名前変更
- レイアウトのカスタマイズ

（注） ダッシュレットを追加または削除するには、定義済みリストから選択します。

（適切なアイコンをクリックすることで）グリッドまたはグラフ形式で表示できる時間ベースまたは非時間ベースのインタラクティブ グラフでホーム ページをカスタマイズできます。これらのグラフは、所属タスクのデフォルトのポーリング サイクルに基づいて、事前設定された時間内に自動的に更新されます。または、[Refresh dashlet] アイコンをクリックして、最新のステータスを取得することもできます。[Enlarge Chart] アイコンをクリックして、グラフを別個のページで拡大できます。

ここでは、次の内容について説明します。

- 「Prime Infrastructure ホーム ページの編集」（P.2-48）
- 「ダッシュレットの追加」（P.2-49）
- 「新しいダッシュボードの追加」（P.2-51）
- 「フィルタの追加」（P.2-52）

Prime Infrastructure ホーム ページの編集

Prime Infrastructure ホーム ページ ダッシュレットをカスタマイズするには、次の手順を実行します。

ステップ 1　Prime Infrastructure ホーム ページで、  をクリックします。ドロップダウン メニューが表示されます。

ステップ 2　使用可能なダッシュレットのリストを表示するには、[Add Dashlet] をクリックします。右側の列で [Add] をクリックして、必要なダッシュレットを追加します。ダッシュレットが、適切なダッシュボードに追加されます。

ステップ 3　[Apply] をクリックします。

ダッシュレットの追加

表 2-11 に、Prime Infrastructure ホーム ページで追加できるデフォルトのダッシュレット オプションを示します。

表 2-11　デフォルトのダッシュレット

ダッシュレット	説明
AP Join Taken Time	アクセス ポイント名と、アクセス ポイントの加入に要した時間（日、分、および秒単位）を表示します。
AP Threats/Attacks	さまざまなタイプのアクセス ポイントの脅威と攻撃を表示し、発生した各タイプの数を示します。
AP Uptime	各アクセス ポイント名と、それぞれに関連付けられた時間を表示します。
Ad hoc Rogues	アドホックの不正を、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Cisco Wired IPS Events	有線 IPS イベントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Client	クライアント アソシエーションの失敗、クライアント認証の失敗、クライアント WEP キー復号化エラー、クライアント WPA MIC エラー、およびクライアント除外とともに最近のクライアント アラームを 5 つ表示します。
Client Authentication Type	認証タイプごとにクライアント数を表示します。
Client Count	特定の期間内の、関連付けられた認証済みのクライアント数のトレンドを表示します。
Client Distribution	クライアントの分散方法をプロトコル、EAP タイプ、および認証タイプ別に表示します。
Client EAP Type Distribution	EAP タイプに基づいた数を表示します。
Client Protocol Distribution	現在のクライアント数分散をプロトコル別表示します。
Client Security Events	除外されたクライアント イベント、WEP 復号化エラー、WPA MIC エラー、回避クライアント、および IPsec エラーを含む、過去 24 時間以内のクライアント セキュリティ イベントを表示します。
Client Traffic	特定の期間内のクライアント トラフィックのトレンドを表示します。Context-Aware
Client Troubleshooting	クライアントの MAC アドレスを入力して、ネットワーク内のクライアントを診断するための情報を取得できます。
Clients Detected by Context-Aware Service	過去 15 分間以内に Context Aware Service によって検出されたクライアント数を表示します。
Controller CPU Utilization (%)	平均、最大、および最小の CPU 使用量を表示します。

表 2-11　デフォルトのダッシュレット （続き）

ダッシュレット	説明
Controller Memory Utilization	コントローラの平均、最大、および最小メモリ使用量をパーセンテージで表示します。
Coverage Areas	カバレッジ エリアのリストと、各カバレッジ エリアに関する詳細を表示します。
Friendly Rogue APs	危険性のない不正アクセス ポイントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。
Guest Users Count	指定した期間にわたるゲスト クライアント数を表示します。
Inventory Detail Status	次のデバイス タイプのステータスを要約したグラフを表示します。 - コントローラ - スイッチ - Autonomous AP - 無線 - MSE - サードパーティのコントローラ - サードパーティのアクセス ポイント
Inventory Status	クライアント コントローラの総数と、到達不能コントローラの数を表示します。
LWAPP Uptime	アクセス ポイント名と、アップ時間を日、分、および秒単位で表示します。
Latest 5 Logged in Guest Users	ログインする最新のゲスト ユーザを表示します。
Mesh AP by Hop Count	ホップ カウントに基づいて AP を表示します。
Mesh AP Queue Based on QoS	QoS に基づいて AP を表示します。
Mesh Parent Changing AP	親の変更に基づいて最低のメッシュ AP を表示します。
Mesh Top Over Subscribed AP	オーバーサブスクライブ型 AP を表示します。
Mesh Worst Node Hop Count2-28	ルート AP からの最低の AP ノード ホップ カウントを表示します。
Mesh Worst Packet Error Rate	リンクのパケット エラー率に基づいて最低のメッシュ AP リンクを表示します。
Mesh Worst SNR Link	リンクの SNR 値に基づいて最低のメッシュ AP リンクを表示します。
Most Recent AP Alarms	アクセス ポイント アラームのうち、最新 5 つを表示します。すべてのアラームを表示する [Alarms] ページを開くには、カッコ内の番号をクリックします。
Most Recent Client Alarms	最新のクライアント アラームを表示します。
Most Recent Mesh Alarms	最新のメッシュ アラームを表示します

表 2-11　デフォルトのダッシュレット （続き）

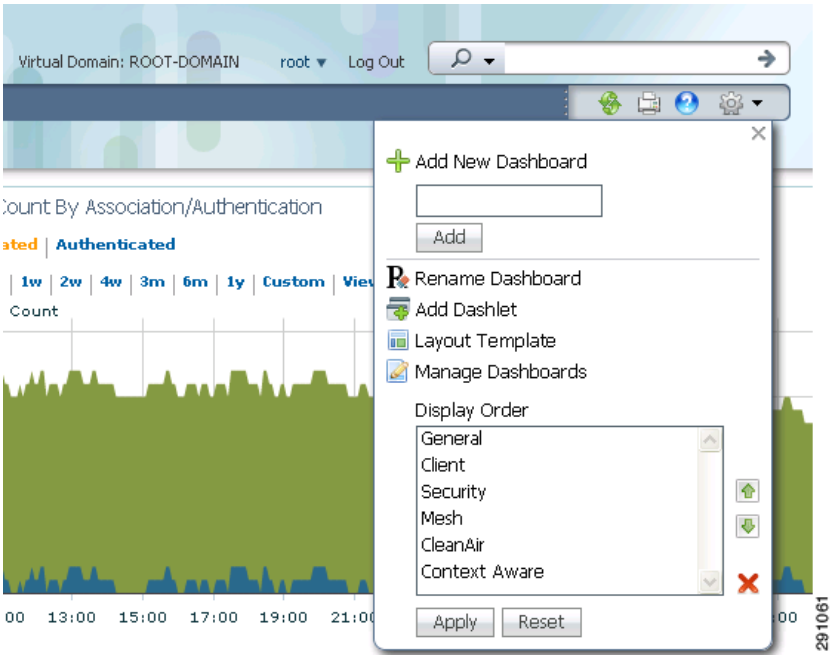
ダッシュレット	説明
Most Recent Security Alarms	セキュリティ アラームのうち、最新 5 件分を表示します。[Alarms] ページを開くには、カッコ内の番号をクリックします。
Recent 5 Guest User Accounts	作成または変更された最新のゲスト ユーザ アカウントを表示します。
Recent Alarms	デフォルトで、アラームのうち最新 5 つを表示します。[Alarms] ページを開くには、カッコ内の番号をクリックします。
Recent Coverage Holes	アクセス ポイントによってリストされた最近のカバレッジ ホール アラームを表示します。
Recent Malicious Rogue AP Alarms	最近の悪意のある不正 AP アラームを表示します。
Recent Rogue Alarms	不正アラームのうち、最新 5 つを表示します。アラームを表示する [Alarms] ページを開くには、カッコ内の番号をクリックします。
Security Index	ワイヤレス ネットワークのセキュリティ インデックス スコアを表示します。セキュリティ インデックスは、「設定の同期」バックグラウンド タスクの一部として計算されます。
Top APs by Client Count	上位の AP をクライアント数別に表示します。
Unclassified Rogue APs	未分類の不正アクセス ポイントを、過去 1 時間、過去 24 時間、および合計のアクティブ数で表示します。

新しいダッシュボードの追加

新しいダッシュボードを作成するには、次の手順を実行します。

ステップ 1　Prime Infrastructure ホーム ページで、⚙▾をクリックします。ドロップダウン メニューが表示されます（図 2-8 を参照）。

図 2-8　　ダッシュボードの編集



ステップ 2　新しく作成するダッシュボードの名前を入力し、[Add] をクリックします。追加したダッシュボード名が [Display Order] リストに表示されます。

（注）　保存しなくて済む操作は、[Add] だけです。[X]、[Move Up]、または [Move Down] をクリックした場合は、[Apply] をクリックして変更内容を適用する必要があります。

ステップ 3　新しいダッシュボードにダッシュレットを追加できます。詳細については、「ダッシュレットの追加」（P.2-49）を参照してください。

（注）　図 2-8 に示されている復元された出荷時の初期状態に戻すには、[Reset] をクリックして、出荷時の初期状態にリセットします。

フィルタの追加

[General]、[CleanAir]、および [Client] ダッシュボード ページでフィルタを追加するには、次の手順を実行します。

ステップ 1　Prime Infrastructure ホーム ページで、⚙ をクリックします。ドロップダウン メニューが表示されます。

ステップ 2　使用可能なフィルタのリストを表示するには、[Add/Remove Filter(s)] をクリックします。[Add] をクリックして必要なフィルタを追加します。フィルタが、適切なダッシュボードに追加されます。

Prime Infrastructure ではダッシュレットをフィルタするために次の 3 つのフィルタリング オプションを提供します。

- タイム フレーム フィルタ
- サイト フィルタ
- クライアント フィルタ

タイム フレーム フィルタの使用

[General]、[CleanAir]、および [Client] ダッシュボードで使用可能なダッシュレットを、タイム フレームに基づいてフィルタフィルタできます。

タイム フレーム オプションには次のものがあります。

- [Past 1 Hour]：現在の時刻から最近の 1 時間分のデータを表します。データは、現在のデータベース テーブルから収集されます。
- [Past 6 Hours]：現在の時刻から最近の 6 時間分のデータを表します。データは、現在のデータベース テーブルから収集されます。
- [Past 24 Hours]：現在の時刻から最近の 24 時間分のデータを表します。データは、現在のデータベース テーブルから収集されます。
- [Past 1 Week]：現在の時刻から最近の 1 週間（7 日間）分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [Past 2 Week]：現在の時刻から最近の 2 週間分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [Past 4 week]：現在の時刻から最近の 4 週間分のデータを表します。データは、時間単位で集積したテーブルから収集されます。
- [Past 3 Months]：現在の時刻から最近の 3 ヵ月間分のデータを表します。データは、日単位で集積したテーブルから収集されます。
- [Past 6 Months]：現在の時刻から最近の 6 ヵ月間分のデータを表します。データは、週単位で集積したテーブルから収集されます。
- [Past 1 Year]：現在の時刻から最近の 1 年間（12 ヵ月間）分のデータを表します。データは、週単位で集積したテーブルから収集されます。

サイト フィルタの使用

[Client] ダッシュボードで使用可能なダッシュレットを、サイトの詳細に基づいてフィルタできます。

クライアント フィルタの使用

[Client] ダッシュボードで使用可能なダッシュレットを、クライアントの詳細に基づいてフィルタするには、次の手順を実行します。

ステップ 1　 をクリックして、クライアントの詳細を入力します。

ステップ 2　次のいずれかを実行します。

- [Select from Client List] ボタンをクリックして、[Client] リストからクライアントを選択します。

  または

- 次の属性の少なくとも 1 つを入力します。
  - ユーザ名
  - IP アドレス
  - MAC アドレス

– サイト

ステップ 3　[OK] をクリックします。

ステップ 4　[Go] をクリックします。

検索機能の使用方法

拡張された Prime Infrastructure 検索機能（図 2-9 を参照）により、Advanced Search オプションと Saved Search に簡単にアクセスできます。Prime Infrastructure 内の任意のページから検索オプションにアクセスして、デバイスまたは SSID（Service Set IDentifier）を簡単に検索できます。

図 2-9　Prime Infrastructure 検索機能

Prime Infrastructure を使用して、次の検索が可能です。

- 「Quick Search」（P.2-54）
- 「Advanced Search」（P.2-55）
- 「Saved Search」（P.2-67）

Quick Search

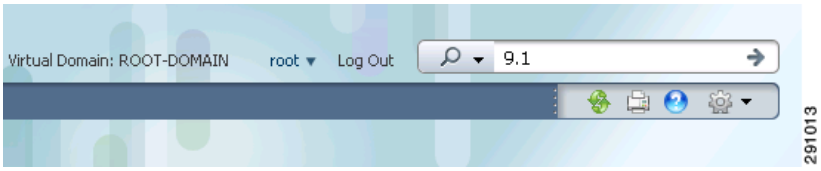
Quick Search では、クライアント、アラーム、アクセス ポイント、コントローラ、マップ、タグ、または不正クライアントの部分的または完全な IP アドレス、MAC アドレス、名前、または SSID を入力できます（図 2-9 を参照）。

（注）　クライアントを検索する場合は、ユーザ名を入力することもできます。

デバイスをすばやく検索するには、次の手順を実行します。

ステップ 1　[Search] テキスト ボックスにデバイスの完全または部分的な IP アドレス、デバイス名、SSID、または MAC アドレスを入力します（図 2-10 を参照）。

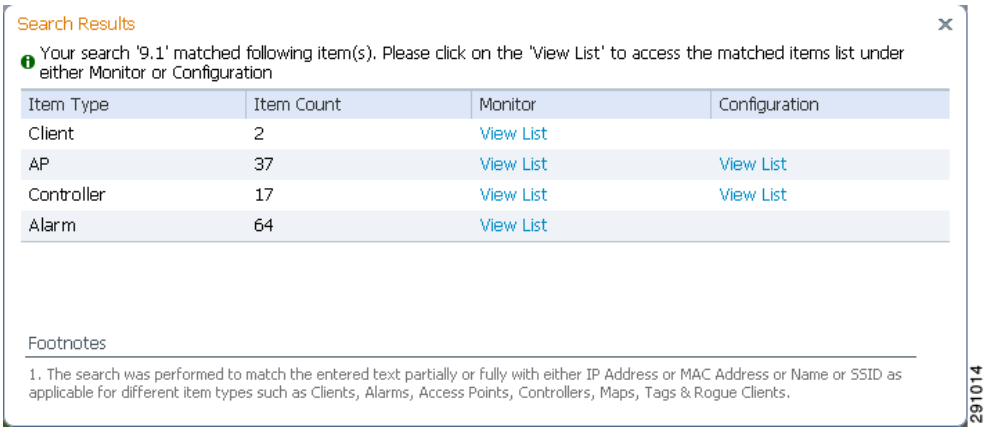
図 2-10　部分的な IP アドレスを使用した Quick Search



ステップ 2　Quick Search パラメータと一致するすべてのデバイスを表示するには、[Search] をクリックします。

検索結果には、一致する項目タイプ、検索パラメータと一致する項目の数、および一致する結果のリストへのリンクが表示されます（図 2-11 を参照）。[Monitor] または [Configuration] ページで一致するデバイスを表示するには、[View List] をクリックします。

図 2-11　Quick Search 結果の Advanced Search



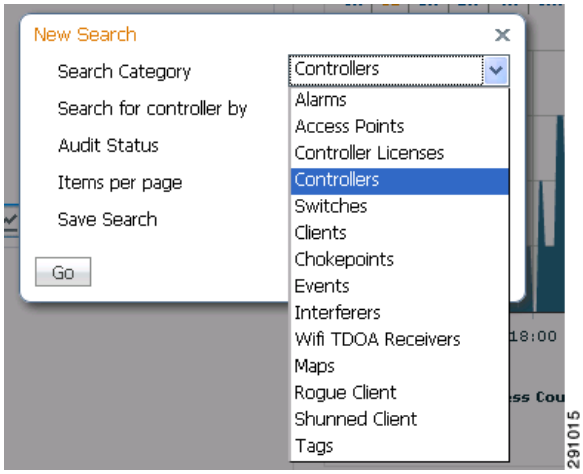
Advanced Search

Prime Infrastructure 内のデバイスに対してさらに絞り込んだ検索を行うには、次の手順を実行します。

ステップ 1　Prime Infrastructure の右上隅にある [Advanced Search] をクリックします（図 2-9 を参照）。

ステップ 2　[New Search] ダイアログで、[Search Category] ドロップダウン リストからカテゴリを選択します（図 2-12 を参照）。

図 2-12　[Search Category] ドロップダウン リスト



（注）　詳細については、次の各カテゴリをクリックします。

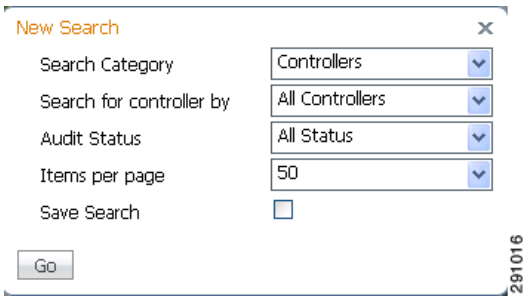
検索カテゴリには、次のものが含まれています。

- アラーム
- アクセス ポイント
- コントローラ ライセンス
- コントローラ
- スイッチ
- クライアント
- チョークポイント
- イベント
- 干渉
- Wi-Fi TDOA 受信機
- マップ
- 不正クライアント
- 回避クライアント
- タグ

ステップ 3　検索に適したすべてのフィルタまたはパラメータを選択します（図 2-13 を参照）。

（注）　検索パラメータは、選択したカテゴリによって変わります。リリース 6.0 には、事前定義の検索フィルタとして [Associated Clients]、[Authenticated Clients]、[Excluded Clients]、[Probing Clients]、[All Clients]、[New Clients detected in last 24 hours]、[unauthenticated clients]、[2.4 GHz clients]、および [5 GHz clients] が追加されています。

図 2-13　[New Search] フィールド



ステップ 4　結果ページに表示する項目の数を選択します。

ステップ 5　この検索を保存するには、[Save Search] チェックボックスを選択して、テキスト ボックスに検索の名前を入力します。

ステップ 6　すべてのフィルタとパラメータを設定したら、[Go] をクリックします。

アラームの検索

アラームの Advanced Search の実行時に、次のパラメータを設定できます（表 2-12 を参照）。

表 2-12　[Search Alarms] フィールド

フィールド	オプション
Severity	[All Severities] 、[Critical]、[Major]、[Minor]、[Warning]、または [Clear] を選択します。
Alarm Category	[All Types]、[Access Points]、[Controller]、[Switches]、[Coverage Hole]、[Config Audit]、[Mobility Service]、[Context-Aware Notifications]、[Interference]、[Mesh Links]、[Rogue AP]、[Adhoc Rogue]、[Security]、[Prime Infrastructure]、または [Performance] を選択します。
Condition	ドロップダウン リストを使用し、条件を選択します。また、このドロップダウン リストに入力して、条件を入力することもできます。 **（注）** アラーム カテゴリを選択した場合は、このドロップダウン リストには、そのカテゴリで使用可能な条件が含まれています。
Time Period	[Any Time] から [Last 7 days] までの時間増分を選択します。デフォルトは [Any Time] です。

表 2-12　[Search Alarms] フィールド （続き）

フィールド	オプション
Acknowledged State	承認済みステートまたは未承認ステートのアラームを検索するには、このチェックボックスを選択します。このチェックボックスを選択しない場合、承認済みステートは検索基準の考慮に入れられません。
Assigned State	割り当て済みステートまたは未割り当てステートのアラームを検索するか、所有者名によってアラームを検索するには、このチェックボックスを選択します。このチェックボックスを選択しない場合は、割り当て済みステートは検索基準に含まれません。 （注）　[Assigned State] > [Owner Name] を選択する場合は、使用可能なテキスト ボックスに所有者名を入力します。

（注）　アラームの検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

アクセス ポイントの検索

アクセス ポイントの Advanced Search の実行時に、次のパラメータを設定できます（表 2-13 を参照）。

表 2-13　[Search Access Points] フィールド

フィールド	オプション
Search By	[All APs]、[Base Radio MAC]、[Ethernet MAC]、[AP Name]、[IP Address]、[Controller Name]、[Controller IP]、[All Unassociated APs]、[Floor Area]、[Outdoor Area]、[Unassigned APs]、または [Alarms] を選択します。 （注）　検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。たとえば、[Floor Area] を選択した場合は、キャンパスとビルディングも特定する必要があります。または、[Alarms] を選択した場合は、アラームのシビリティに基づいてアクセス ポイントを検索できます。
AP Type	[All Types]、[LWAPP]、または [Autonomous] を選択します。

表 2-13　[Search Access Points] フィールド （続き）

フィールド	オプション
AP Mode	[All Modes]、[Local]、[Monitor]、[**FlexConnect**]、[Rogue Detector]、[Sniffer]、[Bridge]、または [SE-Connect] を選択します。
Radio Type	[All Radios]、[802.11a]、または [802.11b/g] を選択します。
802.11n Support	802.11n がサポートされるアクセス ポイントを検索するには、このチェックボックスを選択します。
OfficeExtend AP Enabled	OfficeExtend アクセス ポイントを検索するには、このチェックボックスを選択します。
CleanAir Support	CleanAir をサポートするアクセス ポイントを検索するには、このチェックボックスを選択します。
CleanAir Enabled	CleanAir がサポートされ、有効になっているアクセス ポイントを検索するには、このチェックボックスを選択します。
Items per page	検索結果ページに表示するレコードの数を設定します。

（注）　アクセス ポイントの検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

コントローラ ライセンスの検索

コントローラ ライセンスの Advanced Search の実行時に、次のパラメータを設定できます（表 2-14 を参照）。

表 2-14　[Search Controller Licenses] フィールド

フィールド	オプション
Controller Name	ライセンス検索に関連付けられたコントローラ名を入力します。
Feature Name	ライセンス ティアに応じて、[All]、[Plus]、または [Base] を選択します。
Type	[All]、[Demo]、[Extension]、[Grace Period]、または [Permanent] を選択します。
% Used or Greater	このドロップダウン リストからライセンスの使用パーセンテージを選択します。0 ～ 100 の範囲のパーセント値を使用します。
Items per page	検索結果ページに表示するレコードの数を設定します。

ライセンスと License Center の詳細については、「ライセンスの管理」（P.15-924）を参照してください。

コントローラの検索

コントローラの Advanced Search の実行時に、次のパラメータを設定できます（表 2-15 を参照）。

表 2-15　[Search Controllers] フィールド

フィールド	オプション
Search for controller by	[All Controllers]、[IP Address]、または [Controller Name] を選択します。 **（注）** 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。
Enter Controller IP Address	このテキスト ボックスは、[Search for controller by] ドロップダウン リストから [IP Address] を選択した場合のみ表示されます。
Enter Controller Name	このテキスト ボックスは、[Search for controller by] ドロップダウン リストから [Controller Name] を選択した場合のみ表示されます。
Audit Status	ドロップダウン リストから、次のいずれかのオプションを選択します。 • **All Status** • [Mismatch]：最新の監査で、Prime Infrastructure とコントローラ間の設定の相違が検出された。 • [Identical]：最新の監査で、設定の相違は検出されなかった。 • [Not Available]：監査ステータスは使用できない。
Items per page	検索結果ページに表示するレコードの数を設定します。

（注） コントローラの検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

スイッチの検索

スイッチの Advanced Search の実行時に、次のパラメータを設定できます（表 2-16 を参照）。

表 2-16　[Search Switches] フィールド

フィールド	オプション
Search for Switches by	[All Switches]、[IP Address]、または [Switch Name] を選択します。ワイルドカード（*）を使用できます。たとえば、[IP Address] を選択して、**172*** を入力した場合、Prime Infrastructure は、IP アドレス 172 で始まるすべてのスイッチを返します。
Items per page	検索結果ページに表示するレコードの数を設定します。

クライアントの検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

クライアントの検索

クライアントの Advanced Search の実行時に、次のパラメータを設定できます（表 2-17 を参照）。

表 2-17　[Search Clients] フィールド

フィールド	オプション
Media Type	[All]、[Wireless Clients]、または [Wired Clients] を選択します。
Wireless Type	[Media Type] リストから [Wireless Clients] を選択した場合は、[All]、[Lightweight]、または [Autonomous Clients] を選択します。
Search By	[All Clients]、[All Excluded Clients]、[All Wired Clients]、[All Logged in Guests]、[IP Address]、[User Name]、[MAC Address]、[Asset Name]、[Asset Category]、[Asset Group]、[AP Name]、[Controller Name]、[Controller IP]、[MSE IP]、[Floor Area]、[Outdoor Area]、[Switch Name]、または [Switch Type] を選択します。 **（注）** 検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。たとえば、[IP address] を選択した場合は、この検索の特定の IP アドレスを入力する必要があります。
Clients Detected By	[Prime Infrastructure] または [MSEs] を選択します。 [Clients detected by Prime Infrastructure]：Prime Infrastructure データベースに格納されたクライアント。 [Clients detected by MSE]：コントローラと直接通信する MSE で Context Aware Service によって検索されるクライアント。

表 2-17　[Search Clients] フィールド （続き）

フィールド	オプション
Client States	[All States]、[Idle]、[Authenticated]、[Associated]、[Probing]、または [Excluded] を選択します。
Posture Status	デバイスがクリーンであるかどうかを確認するには、[All]、[Unknown]、[Passed] 、[Failed] を選択します。
Restrict By Radio Band	特定の無線帯域を示すには、このチェックボックスを選択します。ドロップダウン リストから [5 GHz] または [2.4 GHz] を選択します。
Restrict By Protocol	特定のプロトコルを示すには、このチェックボックスを選択します。ドロップダウン リストから [802.11a]、[802.11b]、[802.11g]、[802.11n]、[802.11ac]、または [Mobile] を選択します。
SSID	このチェックボックスを選択して、ドロップダウン リストから適切な SSID を選択します。
Profile	選択したプロファイルに関連するすべてのクライアントを一覧表示するには、このチェックボックスを選択します。 **（注）** チェックボックスの選択後に、ドロップダウン リストから適切なプロファイルを選択します。
CCX Compatible	Cisco Client Extensions との互換性があるクライアントを検索するには、このチェックボックスを選択します。 **（注）** チェックボックスの選択後に、ドロップダウン リストから、適切なバージョンとして [All Versions] または [Not Supported] を選択します。
E2E Compatible	エンドツーエンドの互換性のあるクライアントを検索するには、このチェックボックスを選択します。 **（注）** チェックボックスの選択後に、ドロップダウン リストから、適切なバージョンとして [All Versions] または [Not Supported] を選択します。
NAC State	特定のネットワーク アドミッション コントロール（NAC）ステートによって識別されたクライアントを検索するには、このチェックボックスを選択します。 **（注）** チェックボックスの選択後に、ドロップダウン リストから [Quarantine]、[Access]、[Invalid]、および [Not Applicable] のうち適切なステートを選択します。

表 2-17　[Search Clients] フィールド （続き）

フィールド	オプション
Include Disassociated	ネットワークに存在しないが、Prime Infrastructure が履歴レコードを保持しているクライアントを含めるには、このチェックボックスを選択します。
Items per page	検索結果ページに表示するレコードの数を設定します。

（注）　クライアントの検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

チョークポイントの検索

チョークポイントの Advanced Search の実行時に、次のパラメータを設定できます（表 2-18 を参照）。

表 2-18　[Search Chokepoint] フィールド

フィールド	オプション
Search By	[MAC Address] または [Chokepoint Name] を選択します。 （注）　検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。たとえば、[MAC address] を選択した場合は、この検索の特定の MAC アドレスを入力する必要があります。

イベントの検索

イベントの Advanced Search の実行時に、次のパラメータを設定できます（表 2-19 を参照）。

表 2-19　[Search Events] フィールド

フィールド	オプション
Severity	[All Severities]、[Critical]、[Major]、[Minor]、[Warning]、[Clear]、または [Info. Color coded] を選択します。
Event Category	[All Types]、[Access Points]、[Controller]、[Security]、[Coverage Hole]、[Rogue AP]、[Adhoc Rogue]、[Interference]、[Mesh Links]、[Client]、[Mobility Service]、[Location Notifications]、[Pre Coverage Hole]、または [Prime Infrastructure] を選択します。

表 2-19　[Search Events] フィールド （続き）

フィールド	オプション
Condition	ドロップダウン リストを使用し、条件を選択します。また、このドロップダウン リストに入力して、条件を入力することもできます。 （注）　イベント カテゴリを選択した場合は、このドロップダウン リストには、そのカテゴリで使用可能な条件が含まれています。
Search All Events	検索結果ページに表示するレコードの数を設定します。

イベントの詳細については、「不正アラーム イベントのモニタリング」（P.5-109）を参照してください。

干渉の検索

アクセス ポイントによって検出される干渉の Advanced Search の実行時に、次のパラメータを設定できます（表 2-20 を参照）。

表 2-20　[Search SE-Detected Interferers] フィールド

フィールド	オプション
Search By	[All Interferers]、[Interferer ID]、[Interferer Category]、[Interferer Type]、[Affected Channel]、[Affected AP]、[Severity]、[Power]、または [Duty Cycle] を選択します。 （注）　検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。
Detected By	[All Spectrum Experts] を選択するか、ドロップダウン リストから特定の Spectrum Expert を選択します。
Detected within the last	干渉検出の時間範囲を選択します。時間範囲は、5 分～ 24 時間または [All History] です。
Interferer Status	このドロップダウン リストから [All]、[Active]、または [Inactive] を選択します。
Restrict by Radio Bands/Channels	無線帯域またはチャネルによる検索を設定します。
Items per page	検索結果ページに表示するレコードの数を設定します。

SE-detected 干渉の検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

AP-Detected 干渉の検索

アクセス ポイントによって検出される干渉の Advanced Search の実行時に、次のパラメータを設定できます（表 2-21 を参照）。

表 2-21　[Search AP-Detected Interferers] フィールド

フィールド	オプション
Search By	[All Interferers]、[Interferer ID]、[Interferer Type]、[Affected Channel]、[Severity]、[Duty Cycle]、または [Location] を選択します。 （注）　検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。
Detected within the last	干渉検出の時間範囲を選択します。時間範囲は、5 分～ 24 時間または [All History] です。
Active Interferers Only	検索にアクティブな干渉のみを含めるには、このチェックボックスを選択します。

（注）　AP-detected 干渉の検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

Wi-Fi TDOA 受信機の検索

Wi-Fi TDOA 受信機の Advanced Search の実行時に、次のパラメータを設定できます（表 2-22 を参照）。

表 2-22　[Search Wi-Fi TDOA Receivers] フィールド

フィールド	オプション
Search By	[MAC Address] または [Wi-Fi TDOA Receivers Name] を選択します。 （注）　検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。

マップの検索

マップの Advanced Search の実行時に、次のパラメータを設定できます（表 2-23 を参照）。

表 2-23　[Search Map] フィールド

フィールド	オプション
Search for	[All Maps]、[Campuses]、[Buildings]、[Floor Areas]、または [Outdoor Areas] を選択します。
Map Name	マップ名で検索します。テキスト ボックスにマップ名を入力します。
Items per page	検索結果ページに表示するレコードの数を設定します。

（注）　マップの検索結果ページに表示する情報を決定できます。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

マップの詳細については、「マップについて」（P.6-153）を参照してください。

不正クライアントの検索

不正クライアントの Advanced Search の実行時に、次のパラメータを設定できます（表 2-24 を参照）。

表 2-24　[Search Rogue Client] フィールド

フィールド	オプション
Search for clients by	[All Rogue Clients]、[MAC Address]、[Controller]、[MSE]、[Floor Area]、または [Outdoor Area] を選択します。
Search In	[MSEs] または [Prime Infrastructure Controllers] を選択します。
Status	チェックボックスを選択して、ドロップダウン リストから [Alert]、[Contained]、または [Threat] を選択して、検索基準にステータスを含めます。

不正クライアントの詳細については、「不正アクセス ポイント、アドホック イベント、およびクライアント」（P.3-77）を参照してください。

回避クライアントの検索

（注）　有線ネットワーク上の Cisco IPS センサーが不審なクライアントまたは脅威的なクライアントを検出した場合は、そのクライアントを回避するようにコントローラに警告します。

回避クライアントの Advanced Search の実行時に、次のパラメータを設定できます（表 2-25 を参照）。

表 2-25　[Search Shunned Client] フィールド

フィールド	オプション
Search By	[All Shunned Clients]、[Controller]、または [IP Address] を選択します。 （注）　検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。

タグの検索

タグの Advanced Search の実行時に、次のパラメータを設定できます（表 2-26 を参照）。

表 2-26　[Search Tags] フィールド

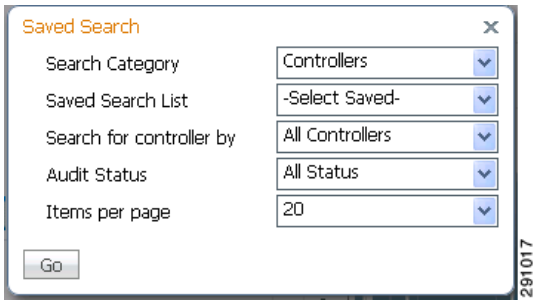
フィールド	オプション
Search for tags by	[All Tags]、[Asset Name]、[Asset Category]、[Asset Group]、[MAC Address]、[Controller]、[MSE]、[Floor Area]、または [Outdoor Area] を選択します。 （注）　検索パラメータは、選択したカテゴリによって変わることがあります。適用可能な場合は、[Search By] カテゴリの特定に役立つよう、追加のパラメータまたはフィルタ情報を入力します。
Search In	[MSEs] または [Prime Infrastructure Controllers] を選択します。
Last detected within	時間増分を 5 分～ 24 時間の間で選択します。デフォルト値は、15 分です。
Tag Vendor	このチェックボックスを選択して、[Aeroscout]、[G2]、[PanGo]、または [WhereNet] を選択します。
Telemetry Tags only	適宜にタグを検索するには、[Telemetry Tags only] チェックボックスを選択します。
Items per page	検索結果ページに表示するレコードの数を設定します。

Saved Search

Saved Search 機能を使用して、以前に保存した検索にアクセスして、実行できます（図 2-14 を参照）。

（注）　検索を保存する場合は、検索に固有の名前を割り当てる必要があります。Saved Search は、現在のパーティションのみに適用されます。

図 2-14　[Saved Search] ページ



Saved Search にアクセスして実行するには、次の手順を実行します。

ステップ 1　[Saved Search] をクリックします。

ステップ 2　[Search Category] ドロップダウン リストからカテゴリを選択します。

ステップ 3　[Saved Search List] ドロップダウン リストから保存した検索を選択します。

ステップ 4　必要に応じて、保存した検索の現在のパラメータを変更します。

ステップ 5　[Go] をクリックします。

検索結果の表示（[Edit View]）の設定

[Edit View] ページでは、[Search Results] ページに表示する列を選択できます。

列名は、次のいずれかのリストに表示されます。

- [Hide Information]：表に表示されない列を一覧表示します。[Hide] ボタンはこのリストを指します。
- [View Information]：表に表示する列を一覧表示します。[Show] ボタンはこのリストを指します。

表に列を表示するには、[Hide Information] リストでその列をクリックして、[Show] をクリックします。表から列を削除するには、[View Information] リストでその列をクリックして、[Hide] をクリックします。Shift キーまたは Ctrl キーを押したまま、複数の列を選択できます。

[View Information] リストで列の位置を変更するには、その列をクリックして、[Up] または [Down] をクリックします。リスト内での列の位置が高いほど、表では左側に表示されます。

コマンド ボタン

[Edit View] ページには、次のコマンド ボタンが表示されます。

- [Reset]：表をデフォルトの表示に設定します。
- [Show]：強調表示した列を [Hide Information] リストから [View Information] リストに移動します。
- [Hide]：強調表示した列を [View Information] リストから [Hide Information] リストに移動します。
- [Up]：強調表示した列をリストの上の方（表ではさらに左側）に移動します。
- [Down]：強調表示した列をリストの下の方（表ではさらに右側）に移動します。
- [Submit]：表列への変更を保存して、前のページに戻ります。
- [Cancel]：表列への変更を取り消して、前のページに戻ります。

セキュリティ ソリューションの設定

この章では、無線 LAN のセキュリティ ソリューションについて説明します。ここで説明する内容は、次のとおりです。

Cisco Unified Wireless Network Solution セキュリティ

Cisco Unified Wireless Network Solution は、潜在的に複雑化する可能性のあるレイヤ 1、レイヤ 2、およびレイヤ 3 の 802.11 アクセス ポイントのセキュリティ コンポーネントを 1 つのシンプルなポリシー マネージャにまとめたもので、システム全体のセキュリティ ポリシーを無線 LAN ごとにカスタマイズできます。これにより、シンプルで統一された体系的なセキュリティ管理が実現します。

企業での無線 LAN 展開の最も大きな課題の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy（WEP）です。低価格なアクセス ポイントの登場も新たな問題で、企業ネットワークに接続して中間者攻撃および DoS 攻撃に利用される可能性があります。また、次々に追加されるセキュリティ ソリューションの複雑さから、多くの IT マネージャが無線 LAN セキュリティの最新技術を採用することをためらっています。

ここでは、次の内容について説明します。

レイヤ 1 ソリューション

Cisco Unified Wireless Network Solution オペレーティング システムのセキュリティ ソリューションによって、すべてのクライアントはアクセスの試行回数を、オペレータが設定した回数までに制限されます。クライアントがその制限回数内にアクセスできなかった場合、そのクライアントは、オペレータが設定したタイマーが切れるまで自動的に除外（アクセスをブロック）されます。そのオペレーティング システムは、無線 LAN ごとに SSID ブロードキャストを無効にすることもできます。

レイヤ 2 ソリューション

上位レベルのセキュリティと暗号化が必要な場合、ネットワーク管理者は、Extensible Protocol（EAP; 拡張認証プロトコル）を使用する 802.1X 動的キーや Wi-Fi Protected Access（WPA）動的キーなど業界標準のセキュリティ ソリューションも実装できます。Cisco Unified Wireless Network Solution の WPA 実装には、Advanced Encryption Standard（AES）動的キー、Temporal Key Integrity Protocol + Message Integrity Code Checksum（TKIP + Michael）動的キー、または WEP 静的キーが含まれます。無効化も使用され、オペレータが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 2 アクセスがブロックされます。

どの無線セキュリティ ソリューションを採用した場合も、コントローラとアクセス ポイントとの間のすべてのレイヤ 2 有線通信は、Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）トンネルを使用してデータを渡すことにより保護されます。

レイヤ 3 ソリューション

WEP の問題の解決をさらに進めるには、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）などの業界標準のレイヤ 3 セキュリティ ソリューションを使用します。

Cisco Unified Wireless Network Solution では、ローカルおよび RADIUS メディア アクセス コントロール（MAC）フィルタリングがサポートされています。このフィルタリングは、802.11 アクセス カードの MAC アドレス一覧情報が把握できている小規模のクライアント グループに適しています。Cisco Unified Wireless Network Solution は、ローカルおよび RADIUS ユーザ/パスワード認証もサポートします。この認証は、小規模から中規模のクライアント グループに適しています。

シングル ポイントでの設定ポリシー マネージャのソリューション

Cisco Unified Wireless Network Solution に Cisco Prime Infrastructure を装備した場合、システム全体のセキュリティ ポリシーを無線 LAN ごとに設定できます。スモール オフィス、ホームオフィス（SOHO）のアクセス ポイントでは、アクセス ポイントごとにセキュリティ ポリシーを個別に設定する必要があります。また、複数のアクセス ポイントにわたってセキュリティ ポリシーを設定するには、サードパーティのアプライアンスを使用する必要があります。Cisco Unified Wireless Network Solution セキュリティ ポリシーは Prime Infrastructure からシステム全体に適用できるため、エラーを除去することができ、全体的な作業量が大幅に減少します。

不正アクセス ポイントのソリューション

この項では、不正アクセス ポイントに対するセキュリティ ソリューションについて説明します。内容は次のとおりです。

不正アクセス ポイントの問題

不正アクセス ポイントは、正規のクライアントをハイジャックし、プレーン テキスト、他の DoS 攻撃、または中間者攻撃を使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正アクセス ポイントを使用して、パスワードやユーザ名などの機密情報を取得できるのです。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。このフレームはアクセス ポイントを模倣し、特定の無線 LAN クライアント アダプタに伝送して、他のすべてのアダプタには待機するように指示します。その結果、正規のクライアントは、無線 LAN リソースに接続できなくなります。したがって、無線 LAN サービス プロバイダーは、空間からの不正アクセス ポイントの締め出しに強い関心を持っています。

オペレーティング システムのセキュリティ ソリューションでは、「不正アクセス ポイントのタギングと封じ込め」（P.3-71）の説明にあるように、無線リソース管理（RRM）機能を使用して、すべての近隣アクセス ポイントを継続的にモニタし、不正アクセス ポイントを自動的に検出し、位置を特定します。

不正アクセス ポイントのタギングと封じ込め

Prime Infrastructure を使用して Cisco Unified Wireless Network Solution をモニタしている場合、不正アクセス ポイントが検出されるとフラグが生成され、既知の不正アクセス ポイントの MAC アドレスが表示されます。オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示できます。その後、それらを Known または Acknowledged 不正アクセス ポイントとしてマークする（追加の処置はなし）、それらを Alert 不正アクセス ポイントとしてマークする（監視し、アクティブになったときに通知）、それらを Contained 不正アクセス ポイントとしてマークする（1 ～ 4 台のアクセス ポイントから、不正アクセス ポイントのクライアントが不正アクセス ポイントとアソシエートするたびにそれらのクライアントに認証解除とアソシエート解除のメッセージを送信することによって封じ込め処理を行う）のいずれかを実行します。

不正アクセス ポイントに対するネットワークの保護

MAC フィルタ リストに定義されていないアクセス ポイントからのアクセス ポイント攻撃を禁止し、すべての不正アクセス ポイントからネットワークを保護することができます。

MAC フィルタリングを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　MAC フィルタを設定したいコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Security] > [AAA] > [MAC Filtering] の順に選択します。[MAC Filtering] ページが表示されます。

RADIUS 互換モード、MAC デリミタ、MAC アドレス、プロファイル名、インターフェイス、および説明が表示されます。

ステップ 4　複数のデバイスにわたって同じ設定を行うには、[Select a command] ドロップダウン リストから [Add MAC Filter] を選択し、[Go] をクリックします。テンプレートがあり、それを適用できます。テンプレートを作成する必要がある場合は、URL をクリックすると、テンプレート作成ページにリダイレクトされます。

（注）　MAC フィルタ リスト内で指定されていなくてもコントローラに接続できるのは、メッシュ アクセス ポイントだけです。

ステップ 5　プロファイル名、インターフェイス、説明などを変更するには、[MAC Address] 列の特定の MAC アドレスをクリックします。

セキュリティ ダッシュボードの説明

無許可の不正アクセス ポイントは安価で入手しやすいことから、そうしたアクセス ポイントを従業員が既存の LAN に接続し、IT 部門の承諾を得ずにアドホック無線ネットワークを構築する場合があります。これらの不正アクセス ポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、無線ユーザはセキュリティで保護されていないアクセス ポイントの場所を頻繁に公表するため、企業のセキュリティが侵害される危険性も増大します。

Cisco Unified Wireless Network Solution では、担当者がスキャナを持って不正アクセス ポイントを手動で検出するのではなく、管理対象のアクセス ポイントにより MAC アドレスと IP アドレス情報をもとに不正アクセス ポイントを検出して、その情報を自動的に収集し、システム オペレータがその不正アクセス ポイントの位置の特定、タグ付け、および封じ込めができるようになります。また、1 ～ 4 台のアクセス ポイントから、不正アクセス ポイントのクライアントに認証解除とアソシエート解除のメッセージを送信することで不正アクセス ポイントを防ぐこともできます。

ネットワークの既存イベントおよびセキュリティ状態の概要については、Prime Infrastructure ホームページで [Security] ダッシュボードをクリックします。

ここでは、[Security] ダッシュボードのダッシュレットについて説明します。内容は次のとおりです。

- 「セキュリティ インデックス」（P.3-73）
- 「Malicious Rogue Access Points」（P.3-73）
- 「Adhoc Rogues」（P.3-74）
- 「CleanAir Security」（P.3-75）
- 「未分類の不正アクセス ポイント」（P.3-75）
- 「危険性のない不正アクセス ポイント」（P.3-75）
- 「アクセス ポイントの脅威または攻撃」（P.3-76）
- 「MFP Attacks」（P.3-77）
- 「Attacks Detected」（P.3-77）

[Security] ダッシュボードで表示する情報の順序はカスタマイズできます。ダッシュレットを移動して順序を変更できます。ダッシュレットに表示される情報をカスタマイズするには、[Edit Dashlet] アイコンを使用します。[Edit Dashlet] のアイコンを使用すると、ダッシュレットのタイトルの変更、リフレッシュの有効化、リフレッシュ間隔の設定ができます。

セキュリティ インデックス

[Security Index] ダッシュレットには Prime Infrastructure が管理するネットワーク全体のセキュリティ課題などの情報が表示されます。この情報は、日単位のバックグラウンド タスクの一部として計算されます。さまざまなセキュリティ設定に重みを割り当てることによって計算され、視覚的に表示されます。合算された重みの範囲は 0 ～ 100 です。0 は最も安全でないことを示し、100 は最も安全であることを示します。重みは、Prime Infrastructure 内で保持されている、セキュリティ設定と紐付くコントローラおよび Location Server/Mobility Service Engine の中で、最もスコアの低いものから導き出されます。Prime Infrastructure 管理ネットワークのセキュリティ インデックスは、最低スコアのコントローラと最低スコアの Location Service/Mobility Service Engine を加算した値と同等です。

セキュリティ サーモメータの色の範囲は、次のように表示されます。

- 80 以上：緑色
- 60 以上 80 未満：黄色
- 60 未満：赤色

（注） ゲスト WLAN は、スコアリング対象の WLAN から除外されます。Web 認証または Web パススルーが有効な WLAN は、ゲスト WLAN として識別されます。

最新リリースにおけるセキュリティ インデックスは、必要とされるセキュリティ設定に対する基準となります。たとえば、以前のバージョンのコードに AES 暗号化がない場合、AES 暗号化のセキュリティ設定に関連する数値分インデックスが減少します。同様に、新しい設定が行われると、重みが変わります。

（注） Prime Infrastructure で Refresh from Controller コマンドが実行されない場合、Prime Infrastructure に保存されている設定は、コントローラの設定を反映した最新の情報でないことがあります。設定の同期タスクでセキュリティ インデックスの計算を実行することで、すべてのコントローラから最新の設定データを取得できます。セキュリティ インデックスを有効にする手順については、「設定の同期の実行」（P.15-806）を参照してください。

Malicious Rogue Access Points

このダッシュレットには、[Malicious]（悪意あり）として分類された不正アクセス ポイントに関する情報が表示されます。表 3-1 では、危険性のない不正アクセス ポイントのパラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

（注） 悪意のあるアクセス ポイントとは、システム内で検出される悪意のある信頼できないアクセス ポイントまたは未知のアクセス ポイントです。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。

表 3-1　悪意のある不正アクセス ポイントの詳細

フィールド	説明
Alert	アラート状態にある不正なアクセス ポイントの数を示します。 （注）　ネイバー リスト、またはユーザが定義する危険性のない AP リストに登録がないアクセス ポイントは、[Alert] 状態に分類されます。
Contained	封じ込められた不正アクセス ポイントの数を示します。
Threat	脅威を与える / 危険性の高い不正アクセス ポイントの数を示します。
Contained Pending	封じ込められた不正アクセス ポイントの保留の数を示します。 （注）　[Contained Pending] は、リソースを利用できないため、封じ込め処理が遅延していることを示しています。

Adhoc Rogues

[Adhoc Rogues] ダッシュレットには、過去 1 時間および過去 24 時間に発生した不正の件数と、アクティブな不正の合計数が表示されます。表 3-2 では、危険性のない不正アクセス ポイントのパラメータについて説明します。この任意の列にある数字をクリックすると、詳細情報を含むページが表示されます。

（注）　コントローラが最初にスキャンを実行したタイミングでは、不正アドホック アクセス ポイントの状態は [Alert] と表示され、オペレーティング システムの ID を確認中の場合は [Pending] と表示されます。

表 3-2　Ad hoc Rogues

フィールド	説明
Alert	アラート状態にある不正アドホック アクセス ポイントの数を示します。 （注）　ネイバー リスト、またはユーザが定義する危険性のない AP リストに登録がないアクセス ポイントは、[Alert] 状態に分類されます。
Contained	封じ込められた不正アクセス ポイントの数を示します。
Threat	脅威を与える / 危険性の高い不正アクセス ポイントの数を示します。
Contained Pending	封じ込められた不正アクセス ポイントの保留の数を示します。 （注）　[Contained Pending] は、リソースを利用できないため、封じ込め処理が遅延していることを示しています。

CleanAir Security

このダッシュレットは、CleanAir セキュリティに関する情報を提供し、またワイヤレス ネットワークにおける過去 1 時間および過去 24 時間内のセキュリティ リスク デバイスの数と、アクティブなセキュリティ リスク デバイスの合計数に関する情報を提供します。

次の情報が表示されます。

- Severity
- Failure Source
- Owner
- Date/Time
- Message
- Acknowledged

セキュリティ リスク干渉に関する詳細については、「CleanAir セキュリティ アラームのモニタリング」（P.5-138）を参照してください。

未分類の不正アクセス ポイント

表 3-3 で、未分類の不正アクセス ポイント パラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

（注） 未分類の不正アクセス ポイントとは、[Malicious]（危険性あり）または [Friendly]（危険性なし）のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。

表 3-3　未分類の不正アクセス ポイント

フィールド	説明
Alert	アラート状態にある未分類のアクセス ポイントの数。コントローラで最初にスキャンすると、不正なアクセス ポイント無線が [Alert] と表示され、またオペレーティング システムの ID を確認中の場合は、[Pending] と表示されます。
Contained	封じ込められた未分類の不正アクセス ポイントの数。
Contained Pending	封じ込められた未分類の不正アクセス ポイントの保留の数。

危険性のない不正アクセス ポイント

このダッシュレットには、[Friendly]（危険性なし）として分類された不正アクセス ポイントに関する情報が表示されます。表 3-4 では、危険性のない不正アクセス ポイントのパラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

（注）　危険性のない不正アクセス ポイントとは、既知のアクセス ポイント、認知済みアクセス ポイント、または信頼されたアクセス ポイントです。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。

表 3-4　危険性のない不正なアクセス ポイントの詳細

フィールド	説明
Alert	アラート状態にある不正なアクセス ポイントの数を示します。 （注）　ネイバー リスト、またはユーザが定義する危険性のない AP リストに登録がないアクセス ポイントは、[Alert] 状態に分類されます。
Internal	内部アクセス ポイント数を示します。 （注）　[Internal] とは、検出されたアクセス ポイントがネットワーク内にあり、手動で [Friendly - Internal] に設定されたことを示します。
External	外部アクセス ポイント数を示します。 （注）　[External] とは、検出されたアクセス ポイントがネットワーク外にあり、手動で [Friendly - External] に設定されたことを示します。

アクセス ポイントの脅威または攻撃

表 3-5 では、アクセス ポイントの脅威または攻撃のパラメータについて説明します。これらの各パラメータについて、過去 1 時間および過去 24 時間に検出したアクセス ポイントに対する脅威または攻撃の回数と、現在まで合計が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

表 3-5　AP Threats/Attacks

フィールド	説明
Fake AP Attacks	疑似攻撃数。
AP Missing	不明なアクセス ポイントの検出数。
AP Impersonation	アクセス ポイントのなりすまし数。
AP Invalid SSID	無効なアクセス ポイント SSID 数。
AP Invalid Preamble	無効なアクセス ポイント プリアンブル数。
AP Invalid Encryption	無効なアクセス ポイント暗号化数。
AP Invalid Radio Policy	無効なアクセス ポイント無線ポリシー数。
Denial of Service (NAV related)	DoS（NAV 関連）要求数。
AP Detected Duplicate IP	IP アドレス重複を検出したアクセス ポイント数。

MFP Attacks

インフラストラクチャおよびクライアント MFP 攻撃に対して、過去 1 時間、過去 24 時間の発生件数、および現在までの合計件数が表示されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

Attacks Detected

過去 1 時間および過去 24 時間の wIPS サービス拒否攻撃、wIPS セキュリティ ペネトレーション攻撃、およびカスタム シグニチャ攻撃の数、およびアクティブなこれらの各攻撃の合計数に関する値が提供されます。いずれかの分類期間にある下線付きの数字をクリックすると、詳細情報のページが表示されます。

Recent Rogue AP Alarms

不正アクセス ポイント アラームのうち、最新 5 件分を表示します。[Alarms] ページを表示するには、カッコ内の番号をクリックします。アラームの詳細を表示するには、[MAC Address] の下の項目をクリックします。

Recent Adhoc Rogue Alarm

アドホックの不正アラームのうち、最新 5 件分を表示します。[Alarms] ページを表示するには、カッコ内の番号をクリックします。アドホックの詳細を表示するには、[MAC Address] の下の項目をクリックします。

Most Recent Security Alarms

セキュリティ アラームのうち、最新 5 件分を表示します。[Alarms] ページを表示するには、カッコ内の番号をクリックします。

不正アクセス ポイント、アドホック イベント、およびクライアント

この項では、不正なデバイスに対するセキュリティ ソリューションについて説明します。不正なデバイスとは、ネットワーク内で管理対象のアクセス ポイントによって検出される、未知（管理対象外）のアクセス ポイントまたはクライアントのことです。

コントローラは、すべての近隣のアクセス ポイントを継続的にモニタし、不正なアクセス ポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラで不正なアクセス ポイントが検出されると、不正ロケーション検出プロトコル（RLDP）を使用して、不正なアクセス ポイントがネットワークに接続されているかどうかが判定されます。

（注）　Prime Infrastructure は、コントローラのすべての不正アクセス ポイント データを集約します。

管理者は、すべてのアクセス ポイント上、もしくはモニタ モード（受信専用）アクセス ポイント上でのみ、RLDP を使用するようコントローラを設定することが可能です。この後者のオプションでは、輻輳している RF 空間での不正なアクセス ポイントを簡単に自動検出できるようになります。そして、不要な干渉を生じさせたり、通常のデータ アクセス ポイント機能に影響を与えたりすることなく、モニ

タリングを行えるようになります。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ モード アクセス ポイントとローカル（データ）通信用アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 処理用アクセス ポイントとして、モニタ モード アクセス ポイントを選択します。ネットワーク上に不正があると RLDP で判断された場合は、検出された不正を手動で封じ込め処理を行うことも、自動的に封じ込め処理を行うこともできます。

ここでは、次の内容について説明します。

- 「不正なアクセス ポイントの分類」（P.3-78）
- 「不正アクセス ポイントの分類タイプ」（P.3-79）
- 「アドホックの不正」（P.3-81）

不正なアクセス ポイントの分類

不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行われます。コントローラに対し、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類して表示させる各種ルールを作成できます。

（注）　Prime Infrastructure は、コントローラのすべての不正アクセス ポイント データを集約します。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセス ポイントは分類し直されます。ルールを変更するたびに、Alert 状態にあるすべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にそのルールが適用されます。

（注）　ルール ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

（注）　5500 シリーズ コントローラは最大で 2000 個の不正（認知済みの不正情報含め）に対応します。4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチは最大で 625 個の不正に対応します。2100 シリーズ コントローラおよびサービス統合型ルータのコントローラ ネットワーク モジュールは最大で 125 個の不正に対応します。各コントローラは、不正アクセス ポイントの封じ込めを無線チャンネルごとに 3 台（モニタ モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly として分類します。
2. 未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正状態の分類ルール適用処理を開始します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。

4. コントローラは、優先度の一番高いルールを適用します。不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントに対して手動で封じ込め処理を行うことができますが（不正を自動的に封じ込めるよう RLDP が設定されていない限り）、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセス ポイントを手動で封じ込め処理を行うことができるようになります。
8. 必要に応じて、各アクセス ポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

前述のように、コントローラでは、ユーザ定義のルールに基づいて未知（管理対象外）のアクセス ポイントの分類タイプと不正の状態が自動的に変更されます。もしくは、未知（管理対象外）のアクセス ポイントを本来とは異なる分類タイプと不正の状態に手動で変更することができます。表 3-6 に、未知（管理対象外）のアクセス ポイントに設定できる分類タイプや不正の状態の推移の組み合わせを示します。

表 3-6　設定可能な分類タイプ/不正の状態の推移

推移前	推移後
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが封じ込められないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に変更する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

不正アクセス ポイントの分類タイプ

不正アクセス ポイントの分類タイプには次のものがあります。

- Malicious：システム内で検出されているが、悪意のある、信頼できない、または未知（管理対象外）のアクセス ポイント。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。詳細については、「Malicious Rogue Access Points」（P.3-73）を参照してください。
- Friendly：既知、認知済み、または信頼されたアクセス ポイント。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。詳細については、「危険性のない不正アクセス ポイント」（P.3-80）を参照してください。危険性のないアクセス ポイントのルールを設定するときの詳細については、「危険性のないアクセス ポイント テンプレートの設定」（P.11-683）を参照してください。
- Unclassified：Malicious または Friendly のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。詳細については、「未分類の不正アクセス ポイント」（P.3-81）を参照してください。

悪意のある不正アクセス ポイント

悪意のある不正アクセス ポイントとは、システム内で検出される悪意のある信頼できないアクセス ポイントまたは未知（管理対象外）のアクセス ポイントです。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間、過去 24 時間の各状態の悪意のある不正アクセス ポイントの数と、アクティブな悪意のある不正アクセス ポイントの総数が表示されます。

悪意のある不正アクセス ポイントの状態には次のものがあります。

- Alert：該当アクセス ポイントがネイバー リストまたはユーザ設定の [Friendly AP] リストにないことを示します。
- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。
- Contained Pending：リソースを利用できないため、封じ込め処理が遅延することを示します。
- Removed：この未知（管理対象外）のアクセス ポイントは以前検出されたものの、現在は見つかりません。

悪意のある不正アクセス ポイントに関する詳細な情報を表示するには、いずれかの期間のカテゴリにある下線付きの数値をクリックします。詳細については、「不正アクセス ポイントのモニタリング」（P.5-87）を参照してください。

危険性のない不正アクセス ポイント

危険性のない不正アクセス ポイントとは、既知のアクセス ポイント、認知済みアクセス ポイント、または信頼されたアクセス ポイントです。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の危険性のない不正アクセス ポイントの数と、アクティブな危険性のない不正アクセス ポイントの総数が表示されます。

危険性のない不正アクセス ポイントの状態には次のものがあります。

- Internal：未知（管理対象外）のアクセス ポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。
- External：未知（管理対象外）のアクセス ポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近所のコーヒーショップ設置されているアクセス ポイントなどです。
- Alert：未知（管理対象外）のアクセス ポイントはネイバー リストにもユーザ設定の [Friendly AP] リストにもありません。

危険性のない不正アクセス ポイントの詳細を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。詳細については、「不正アクセス ポイントのモニタリング」（P.5-87）を参照してください。

未分類の不正アクセス ポイント

未分類の不正アクセス ポイントとは、[Malicious]（危険性あり）または [Friendly]（危険性なし）のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の未分類の不正アクセス ポイントの数と、アクティブな未分類の不正アクセス ポイントの総数が表示されます。

未分類の不正アクセス ポイントの状態には次のものがあります。

- Pending：最初の検出で、未知（管理対象外）のアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセス ポイントでは、未知（管理対象外）のアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。
- Alert：未知（管理対象外）のアクセス ポイントはネイバー リストにもユーザ設定の [Friendly AP] リストにもありません。
- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Contained Pending：未知（管理対象外）のアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

詳細情報を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。「不正アクセス ポイントのモニタリング」（P.5-87）を参照してください。

アドホックの不正

アドホック ネットワークで動作しているモバイル クライアントの MAC アドレスが許可された MAC アドレスのリストにない場合は、アドホックの不正であると識別されます。

不正アクセス ポイントのロケーション、タギング、および封じ込め

Prime Infrastructure を使用して Cisco Unified Wireless Network Solution をモニタしている場合、不正アクセス ポイントが検出されるとフラグが生成され、既知の不正アクセス ポイントの MAC アドレスが表示されます。オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示できます。その後、それらを Known または Acknowledged 不正アクセス ポイントとしてマークする（追加の処置はなし）、それらを Alert 不正アクセス ポイントとしてマークする

（監視し、アクティブになったときに通知）、それらを Contained 不正アクセス ポイントとしてマークする（1 ～ 4 台のアクセス ポイントから、不正アクセス ポイントのクライアントが不正アクセス ポイントとアソシエートするたびにそれらのクライアントに認証解除とアソシエート解除のメッセージを送信することによって封じ込め処理を行う）のいずれかを実行します。

この組み込み型の検出、タギング、モニタリング、および封じ込めの機能を使用すると、システム管理者は、次に挙げる適切な処理を実行できます。

- 不正アクセス ポイントを特定します。
- 新しい不正アクセス ポイントの通知を受け取ります（通路をスキャンして歩く必要なし）。
- 未知（管理対象外）の不正アクセス ポイントが削除または認知されるまでモニタします。
- 最も近い場所の許可済みアクセス ポイントを特定して、高速かつ効果的に誘導スキャンを行えるようにします。
- 1 ～ 4 台のアクセス ポイントから、不正アクセス ポイントのクライアントに認証解除とアソシエーション解除のメッセージを送信して、不正アクセス ポイントを封じ込めます。この封じ込め処理は、MAC アドレスを使って個々の不正アクセス ポイントに対して行うことも、企業サブネットに接続されているすべての不正アクセス ポイントに対して要求することもできます。
- 不正アクセス ポイントにタグを付けます。
  - 不正アクセス ポイントが LAN の外部にあり、LAN または無線 LAN のセキュリティを脅かさない場合は認知します。
  - 不正アクセス ポイントが LAN または無線 LAN のセキュリティを脅かさない場合は容認します。
  - 不正アクセス ポイントが排除または認知されるまで、未知（管理対象外）のアクセス ポイントとしてタグ付けします。
  - 不正アクセス ポイントを封じ込め処理済みとしてタグ付けし、1 ～ 4 台のアクセス ポイントから、すべての不正アクセス ポイント クライアントに認証解除およびアソシエーション解除のメッセージを転送することにより、クライアントが不正アクセス ポイントにアソシエートしないようにします。この機能は、同じ不正アクセス ポイント上のすべてのアクティブなチャネルに適用されます。

ここでは、次の内容について説明します。

- 「ネットワーク上のアクセス ポイントの検出」（P.3-82）
- 「コントローラ別不正アクセス ポイントの表示」（P.3-83）

ネットワーク上のアクセス ポイントの検出

不正アクセス ポイントを検出している Cisco Lightweight アクセス ポイントに関する情報を表示するには、アクセス ポイントの検出機能を使用します。

[Rogue AP Alarms] 詳細ページにアクセスするには、次の手順を実行します。

ステップ 1　[Rogue AP Alarms] ページを表示するには、次のいずれかを実行します。

- 不正 AP の検索を実行します。この検索機能の詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。このページには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- ダッシュレットにある [Malicious AP] を示す数字のリンクをクリックします。

ステップ 2　[Rogue AP Alarms] ページで、該当する不正アクセス ポイントの [Rogue MAC Address] をクリックします。[Rogue AP Alarms] 詳細ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[View AP Detecting AP on Network] を選択します。

ステップ 4　[Go] をクリックします。

いずれかのリスト項目をクリックすると、その項目に関するデータが表示されます。

- AP Name
- Radio
- Detecting AP Location
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [WEP]：有効または無効。
- [WPA]：有効または無効。
- [Pre-Amble]：Long（長型）または Short（短型）。
- [RSSI]：受信信号強度インジケータ（dBm）。
- [SNR]：信号対雑音比。
- [Containment Type]：このアクセス ポイントによる封じ込め処理のタイプ。
- [Containment Channels]：このアクセス ポイントが現在封じ込め処理を実行しているチャネル。

コントローラ別不正アクセス ポイントの表示

アクセス ポイント検出機能を使用すると、コントローラ別に不正アクセス ポイントに関する情報を表示できます。

[Rogue AP Alarms] 詳細ページにアクセスするには、次の手順を実行します。

ステップ 1　[Rogue AP Alarms] ページを表示するには、次のいずれかを実行します。

- 不正 AP の検索を実行します。この検索機能の詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。このページには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- ダッシュレットにある [Malicious AP] を示す数字のリンクをクリックします。

ステップ 2　[Rogue AP Alarms] ページで、該当する不正アクセス ポイントの [Rogue MAC Address] をクリックします。[Rogue AP Alarms] 詳細ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[View AP Details by Controller] を選択します。

ステップ 4　[Go] をクリックします。

いずれかのリスト項目をクリックすると、その項目に関するデータが表示されます。

- Controller IP Address
- Detecting AP Name
- Radio

- Detecting AP Location
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [RSSI]：受信信号強度インジケータ（dBm）。
- [Classification]：不正 AP の分類を示します。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。追加情報については、「不正アクセス ポイントの分類タイプ」（P.3-79）を参照してください。
- [On Network]：このネットワークに属しているかどうかで、「Yes」または「No」です。
- [Containment Level]：不正アクセス ポイントの封じ込め処理レベル、または Unassigned（封じ込めなし）を示します。
- Last Updated Time

アラームの処理

Prime Infrastructure を使用し、アクセス ポイントおよびモビリティ サービス エンジン上で、アラームとイベントを表示、割り当て、クリアできます。

アラームの電子メール通知を受信する方法の詳細についても説明します。ここでは、次の内容について説明します。

- 「アラームの割り当てと割り当て解除」（P.3-84）
- 「アラームの削除とクリア」（P.3-85）
- 「アラームの認知」（P.3-85）

アラームの割り当てと割り当て解除

自分にアラームを割り当てたり割り当て解除したりするには、次の手順を実行します。

ステップ 1　アクセス ポイント アラームについて高度な検索を実行します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。

ステップ 2　対応するチェックボックスをオンにすることで、自分に割り当てるアラームを選択します。

（注）　自分に割り当てられているアラームを割り当て解除するには、該当アラームの隣にあるボックスをオフにします。他の人に割り当てられているアラームの割り当ては解除できません。

ステップ 3　[Select a command] ドロップダウン リストから、[Assign to Me]（または [Unassign]）を選択し、[Go] をクリックします。

[Assign to Me] を選択した場合、自分のユーザ名が [Owner] 欄に表示されます。[Unassign] を選択した場合、ユーザ名の欄は空白になります。

アラームの削除とクリア

モビリティ サービス エンジンからアラームを削除またはクリアするには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] ページで、対応するチェックボックスをオンにして、削除またはクリアするアラームを選択します。

（注）　アラームを削除すると、アラームは Prime Infrastructure によってデータベースから削除されます。アラームをクリアすると、アラームは Prime Infrastructure データベースには残りますが、[Clear] 状態になります。アラームは、その原因となった状況が存在しなくなったときにクリアします。

ステップ 2　[Select a command] ドロップダウン リストから、[Delete] または [Clear] を選択し、[Go] をクリックします。

（注）　古いアラームとクリアされたアラームのクリーンアップを設定するには、[Administration] > [Settings] > [Alarms] の順に選択します。

アラームの認知

状況によっては、特定のアラームを [Alarms] リストから削除した方がよい場合があります。たとえば、802.11g インターフェイス上で特定のアクセス ポイントから干渉アラームを継続的に受信している場合は、ページまたはその他のアラーム リストで、そのアクセス ポイントがアクティブなアラームとしてカウントされないように設定しておくと便利です。そのためには、[Alarms] リストで 802.11g インターフェイスのアラームを探し、チェックボックスをオンにして、[Select a command] ドロップダウン リストから [Acknowledge] を選択します。

これで、そのアクセス ポイントが同じインターフェイスで新しい違反を検出しても、Prime Infrastructure によって新しいアラームが生成されず、ページにも新しいアラームが表示されません。ただし、802.11a など別のインターフェイス上では干渉違反が検出され、新しいアラームが生成されます。

一度認知したすべてのアラームは、ページ上にも、アラーム リスト ページにも表示されません。さらに、アラームを認知済みとしてマークした場合は、電子メールも生成されません。デフォルトでは、認知済みアラームは検索対象となりません。このデフォルトを変更するには、[Administration] > [Settings] > [Alarms] ページを選択し、[Hide Acknowledged Alarms] 設定を無効にします。

（注）　アラームを認知すると、この機能を無効にしない限り、問題が再度発生しても別のアラームが生成されない旨の注意を促すために、警告が表示されます。この警告メッセージを無効にするには、[Administration] > [User Preferences] ページを使用します。

また、以前の認知済みアラームをすべて検索して、過去 7 日間に認知されたアラームを表示することもできます。Prime Infrastructure は、7 日以上経過した解除済みアラートを自動的に削除するため、検索結果として表示されるのは最近 7 日間のアクティビティのみです。既存のアラームが削除されるまで、Prime Infrastructure がすでにアラームを生成している管理対象エンティティに対して新しいアラームを生成できません。

不正アラーム イベントのモニタリング

[Events] ページでは、不正アラーム イベントに関する情報を参照できます。Prime Infrastructure では、不正アクセス ポイントが検出されるか、不正アクセス ポイントが手動で変更（状態の変更など）された場合に、イベントが生成されます。[Rogue AP Events] リスト ページには、すべての不正アクセス ポイント イベントが表示されます。

[Rogue AP Events] リスト ページにアクセスするには、次の手順を実行します。

ステップ 1　次のいずれかを実行します。

- Prime Infrastructure の Advanced Search 機能を使用して不正アクセス ポイント イベントを検索します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- [Rogue AP Alarms] 詳細ページで [Select a command] ドロップダウン リストから [Event History] を選択します。

ステップ 2　[Rogue AP Events] リスト ページには、次のイベント情報が表示されます。

- [Severity]：アラームの重大度を示します。
- [Rogue MAC Address]：[Rogue AP Event Details] ページを表示するには、不正な MAC アドレスをクリックします。詳細については、「不正 AP イベントの詳細の表示」（P.3-86）を参照してください。
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [Classification Type]：Malicious、Friendly、Unclassified。詳細については、「不正アクセス ポイントの分類タイプ」（P.3-79）を参照してください。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Date/Time]：イベントが生成された日時。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。追加情報については、「不正アクセス ポイントの分類タイプ」（P.3-79）を参照してください。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。

不正 AP イベントの詳細の表示

不正アクセス ポイント イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Rogue AP Events] リスト ページで、[Rogue MAC Address] リンクをクリックします。

ステップ 2　[Rogue AP Events Details] ページに、次の情報が表示されます。

- Rogue MAC Address
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [On Network]：不正が検出された方法を示します。

  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Classification Type]：Malicious、Friendly、Unclassified。詳細については、「不正アクセス ポイントの分類タイプ」（P.3-79）を参照してください。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。追加情報については、「不正アクセス ポイントの分類タイプ」（P.3-79）を参照してください。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [Containment Level]：不正アクセス ポイントの封じ込めレベル、または Unassigned（未割り当て）。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Created]：イベントが生成された日時。
- [Generated By]：イベントの生成方法（コントローラなど）。
- デバイスの IP アドレス
- [Severity]：アラームの重大度を示します。
- [Message]：現在のイベントの詳細を示します。

アドホック不正イベントのモニタリング

[Events] ページでは、アドホック不正イベントに関する情報を参照できます。アドホック不正が検出されるか、アドホック不正を手動で変更した場合（その状態を変更するなど）、Prime Infrastructure によりイベントが生成されます。[Adhoc Rogue Events] リスト ページには、すべてのアドホック不正イベントが表示されます。

[Rogue AP Events] リスト ページにアクセスするには、次の手順を実行します。

ステップ 1　次のいずれかを実行します。

- Prime Infrastructure の Advanced Search 機能を使用してアドホック不正イベントを検索します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- [Adhoc Rogue Alarms] 詳細ページで [Select a command] ドロップダウン リストから [Event History] を選択します。

ステップ 2　[Rogue AP Events] リスト ページには、次のイベント情報が表示されます。

- [Severity]：アラームの重大度を示します。
- [Rogue MAC Address]：[Rogue AP Event Details] ページを表示するには、不正な MAC アドレスをクリックします。詳細については、「アドホック不正 AP イベントの詳細の表示」（P.3-88）を参照してください。
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。

  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Date/Time]：イベントが生成された日時。
- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。

アドホック不正 AP イベントの詳細の表示

不正アクセス ポイント イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Rogue AP Events] リスト ページで、[Rogue MAC Address] リンクをクリックします。

ステップ 2　[Rogue AP Events Details] ページに、次の情報が表示されます。

- Rogue MAC Address
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [Containment Level]：不正アクセス ポイントの封じ込めレベル、または Unassigned（未割り当て）。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Created]：イベントが生成された日時。
- [Generated By]：イベントの生成方法（コントローラなど）。
- デバイスの IP アドレス
- [Severity]：アラームの重大度を示します。
- [Message]：現在のイベントの詳細を示します。

セキュリティの概要

Prime Infrastructure は、IT 管理者が一元化された場所から企業の無線ネットワークを設計、制御、保護、モニタできる、基礎になります。

Prime Infrastructure には、Cisco ワイヤレス ネットワーク インフラで、ワイヤレス セキュリティの設定とポリシーを管理および適用するための、次のツールが用意されています。

- ユーザ認証、暗号化、アクセス制御などのネットワーク セキュリティ ポリシーの作成と施行。
- ワイヤレス インフラストラクチャのセキュリティ設定。
- 不正 AP の検出、位置検知、封じ込め。
- ワイヤレス侵入防御システム（wIPS）。
- ワイヤレス IPS のシグニチャの修正と管理。
- 管理フレーム保護（MFP）。
- 無許可または悪意のあるワイヤレス ユーザ アクティビティのモニタリングと緩和措置のための Cisco 有線ネットワーク IPS とのコラボレーション。
- 包括的なセキュリティ イベント管理およびレポート機能。

セキュリティ脆弱性アセスメント

Cisco Unified Wireless Network バージョン 5.1 では、自動化されたセキュリティ脆弱性アセスメントを使用でき、企業の全体的なワイヤレス セキュリティ ポスチャを解析しやすくなるだけでなく、WLAN オペレータは、業界のベスト プラクティスを基準として、自社のセキュリティ サービス設定をリアルタイムで評価できます。自動化されたセキュリティ脆弱性アセスメントにより以下が提供されます。

- ワイヤレス ネットワーク全体の予防的な脆弱性モニタリング。
- データ損失、ネットワークへの侵入、または悪意のある攻撃を招くおそれのあるセキュリティの脆弱性に関する包括的な情報。
- ワイヤレス セキュリティ ポスチャの弱点の分析と是正に必要な時間と専門知識の削減。

自動化されたワイヤレス脆弱性アセスメントでは、ワイヤレス ネットワーク全体のセキュリティ ポスチャを脆弱性について監査します。これらの脆弱性は、次のような結果につながる可能性があります。

- 無許可の管理アクセス、または管理プロトコルを使用したネットワークの侵害またはネットワークへの悪影響。
- 無許可のネットワーク アクセス、データ漏えい、中間者攻撃、またはリプレイ アタック。
- サービス拒否（DoS）攻撃など、ネットワーク プロトコルとサービスの操作を介した、ネットワークへの侵害またはネットワークへの悪影響。

Prime Infrastructure では、ネットワーク全体が自動的にスキャンされ、その設定が、シスコが推奨するワイヤレス セキュリティ設定および業界のベスト プラクティスのワイヤレス セキュリティ設定と自動的に比較されます。Prime Infrastructure の自動化されたワイヤレス セキュリティ アセスメント機能では、Wireless LAN Controller、アクセス ポイント、およびネットワーク管理インターフェイスをスキャンして、設定、暗号化、ユーザ認証、インフラストラクチャ認証ネットワーク管理、およびアクセス制御における脆弱性を確認します。

ワイヤレス ネットワーク セキュリティのステータスは、ワイヤレス ネットワーク管理者がセキュリティ イベントをダッシュボードで簡単に参照できるよう、グラフィカルに表示されます。Prime Infrastructure では、Prime Infrastructure セキュリティ ダッシュボードに、セキュリティ インデックス

を介して脆弱性評価の結果が表示されます。セキュリティ インデックスでは、単一の合成セキュリティ スコアと、優先度を付けた脆弱性のサマリーによって、ネットワーク セキュリティ ポスチャを要約しています。詳細については、「セキュリティ インデックス」（P.3-90）を参照してください。

セキュリティ サマリーに含まれているイベントについて詳細を調査する必要がある場合、管理者は、Security Index Detailed レポートにドリルダウンできます。Security Index Detailed レポートには、ネットワークをまたがる脆弱性の綿密な解析が含まれています。最適なセキュリティ設定の内容と、脆弱性を是正するために推奨される変更点も含まれています。管理者の行うすべての変更は、セキュリティ インデックス スコアを更新して反映されます。詳細については、「Security Index Detailed レポート」（P.3-91）を参照してください。

セキュリティ インデックス

セキュリティ インデックスは Prime Infrastructure 管理ネットワークのセキュリティの目安になります。セキュリティ インデックスは、さまざまなセキュリティ設定に重みを割り当てることで計算され、視覚的に表示されます。統合される重みの範囲は 0 ～ 100 です。0 は最も安全でないことを示し、100 は最も安全であることを示します。

重みは、Prime Infrastructure 内で保持されている、セキュリティ設定と紐付くコントローラおよび Location Server/Mobility Service Engine の中で、最もスコアの低いものから導き出されます。たとえば、Prime Infrastructure 管理ネットワークのセキュリティ インデックスは、最低スコアのコントローラと最低スコアの Location Service/Mobility Service Engine を加算した値と同等です。

セキュリティ インデックスには、次の配色が適用されます。

- 80 以上：緑色
- 60 以上 80 未満：黄色
- 60 未満：赤色

（注）　ゲスト WLAN は、スコアリング対象の WLAN から除外されます。Web 認証または Web パススルーが有効な WLAN は、ゲスト WLAN として識別されます。

最新リリースにおけるセキュリティ インデックスは、必要とされるセキュリティ設定に対する基準となります。たとえば、以前のバージョンのコードに AES 暗号化がない場合、AES 暗号化のセキュリティ設定に関連する数値分インデックスが減少します。同様に、新しい設定が行われると、重みが変わります。

Prime Infrastructure で Refresh from Controller コマンドが実行されない場合、Prime Infrastructure に保存されている設定は、コントローラの設定を反映した最新の情報でないことがあります。設定の同期タスクでセキュリティ インデックスの計算を実行し、すべてのコントローラから最新の設定データを取得できます。

主なセキュリティ問題

[Top Security Issues] セクションには、セキュリティ上の問題の上位 5 件が表示されます。[View All] と [Devices] のリンクは、関連する列を並べ替え、すべてのコントローラで発生したセキュリティ上の問題に関するレポートを表示します。Security Index Detailed レポートを開くには、[View All] をクリックします。Security Index Controller レポートを表示するには [Devices] をクリックします。

- 「Security Index Detailed レポート」（P.3-91）
- 「Security Index Controller レポート」（P.3-91）

- 「潜在的なセキュリティ問題」（P.3-92）

Security Index Detailed レポート

Security Index Detailed レポートには、すべてのコントローラ、ロケーション サーバ、およびモビリティ サービス エンジンをまたがって見つかった、すべてのセキュリティ上の問題が表示されます。デバイスから取得された特定のセキュリティ設定で検出された問題について、詳細に説明されています。特定の問題が認知された場合（アラームと同様）、設定の同期タスクが次回実行されるとき、この問題は無視されます（セキュリティ インデックスの計算が有効である場合）。

認知済みの問題があり、設定の同期タスクの次回実行時にこの問題が無視される一部のケースでは、最終的なセキュリティ インデックス スコアは変更されません。この事象には、次のような原因が考えられます。

- 認知済みの問題は、セキュリティ インデックス スコアに直接影響していないコントローラ（たとえば、最低スコア以外のコントローラ）に関連しています。
- 認知済みの問題は、セキュリティ インデックス スコアに直接影響していない WLAN に関連しています。最低スコアのコントローラの最低スコアの WLAN のみが、セキュリティ インデックス スコアに影響します。

コントローラ上で SSH と Telnet が有効化されており、このいずれも問題としてフラグ付けされている場合は、Telnet の問題の方が SSH の問題よりも優先されます。スコアが最も低いコントローラで SSH が認知されていても、セキュリティ インデックスに変化はありません。

すべてのセキュリティ上の問題（認知済みと未認知の両方）を表示するには、[Select a command] ドロップダウン リストから、[Show All] を選択します。未認知のセキュリティ上の問題のみを表示するには、[Show Unacknowledged] を選択します。これは、[Security Summary] ページから [View All] を選択した場合のデフォルト表示です。認知済みのセキュリティ上の問題のみを表示するには、[Show Acknowledged] を選択します。

（注） ユーザによるセキュリティ上の問題の認知または未認知のために、ユーザは「Ack and Unack Security Index Issues」権限を有効にしておく必要があります。

Security Index Controller レポート

このページには、セキュリティ違反のレポートが各コントローラの概要として表示されます。行ごとに、コントローラに発生したセキュリティ問題の数が表示され、すべてのセキュリティ問題へのリンクが表示されます。

[Security Issues Count] 列の数値をクリックすると、Security Index Detailed レポートが表示されます。

潜在的なセキュリティ問題

表 3-7および表 3-8 では、潜在的なセキュリティ問題について説明してあります。

表 3-7　潜在的なセキュリティ問題

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上の WLAN SSID の認証方式が脆弱です。	WLAN 認証方式としては弱いため、WLAN パケットが傍受される場合にオンラインで使用できるツールを使用して突破することができます。	最も安全な認証方式および WPA+WPA2 の方式を使用します。
コントローラ上の WLAN SSID に脆弱な認証方式（CKIP）が設定されています。	WLAN の認証方式としては弱くなります。	最も安全な認証方式および WPA+WPA2 の方式を使用します。
コントローラ上の WLAN SSID にユーザ認証が設定されていません。	認証方式を設定していないため、WLAN にセキュリティ上のリスクがあります。	WPA+WPA2 などの強い認証方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（キー置換を含む CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH を含む CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH とキー置換を含む CKIP WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH を含む CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（キー置換を含む CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上の WLAN SSID に脆弱な暗号化方式（MMH とキー置換を含む CKIP WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 40 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 128 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（TKIP）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に暗号化が設定されていません。	暗号化方式を設定していないため、WLAN に明確なセキュリティ上のリスクがあります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID に脆弱な暗号化方式（WEP 104 ビット）が設定されています。	WLAN の暗号化方式としては弱くなります。	WPA+WPA2 と AES などの強い認証および暗号化方式を設定します。
コントローラ上の WLAN SSID にキー管理方式が設定されていません（WPA+WPA2 のみ該当）。	キー管理方式によって、キーのセキュリティが強化されます。キー管理方式を使用していない場合、WLAN は危険です。	CCKM などのキー管理方式を最低 1 つ設定します。
コントローラ上の WLAN SSID の MFP Client Protection に「Optional」が設定されています。	WLAN について MFP Client Protection がオプションに設定されると、認証済みクライアントがスプーフされたフレームから保護されない場合があります。	MFP Client Protection に「Required」を設定して、不正アクセス ポイントに接続しているクライアントから保護します。
コントローラ上の WLAN SSID の MFP Client Protection に「Disabled」が設定されています。	WLAN について MFP Client Protection が無効に設定されると、認証済みクライアントがスプーフされたフレームから保護されない場合があります。	MFP Client Protection に「Required」を設定して、不正アクセス ポイントに接続しているクライアントから保護します。
コントローラ上で WLAN SSID インターフェイスに「management」が設定されています。	SAFE から推奨されるように、ユーザ トラフィックは管理トラフィックと別にする必要があります。	コントローラ上で WLAN インターフェイスに「management」を設定することはできません。
WLAN について 1 を設定したインターフェイスは、VLAN です。	SAFE から推奨されるように、ユーザ トラフィックは VLAN トラフィックと別にする必要があります。	WLAN では、管理でなく、VLAN を含んでもいないインターフェイスに 1 を設定する必要があります。
コントローラ上の WLAN SSID で「Client Exclusion」が無効です。	Client Exclusion ポリシーが無効である場合、攻撃者は WLAN ネットワークへのアクセスを継続して試行できます。	「Client Exclusion」を有効にして、悪意のある WLAN クライアントの動作から保護します。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上の WLAN SSID で「Broadcast SSID」が有効です。		「Broadcast SSID」を無効にして、ワイヤレス ネットワークを保護します。
コントローラ上の WLAN SSID で「MAC Filtering」が無効です。		「MAC Filtering」を有効にして、ワイヤレス ネットワークを保護します。
コントローラ上で [Protection Type] に「AP Authentication」が設定されています。	[AP Authentication] が設定されている場合、アクセス ポイントは、隣接するアクセス ポイントのビーコン/プローブ応答フレームをチェックして RF グループの情報要素（IE）と一致する認証された IE が含まれているかどうかを確認します。これによってある程度のセキュリティは確保されますが、一部の管理フレームは対象外であり、不正アクセス ポイントによる変更を受けてしまいます。	コントローラ上の [Protection Type] に「Management Frame Protection (MFP)」を設定します。
コントローラで [Protection Type] に「None」が設定されています。	802.11 管理メッセージのセキュリティがアクセス ポイントとクライアント間で受け渡されません。	コントローラ上の [Protection Type] に「Management Frame Protection (MFP)」を設定します。
無線の種類は、DCA チャネルでのみ不正を検出するように設定されています。	国またはすべてのチャネルのサブセットのみで不正検出を実行することは、国またはすべてのチャネルで実行することに比べて安全性が低くなります。	国チャネルまたはすべてのチャネルで不正を検出するように、無線の種類 802.11a/n および 802.11b/g/n を設定します。
無線の種類は、国チャネルと DCA チャネルのいずれの不正も検出するように設定されていません。	国チャネルと DCA チャネルのいずれでも不正検出を設定していない場合は、国またはすべてのチャネルで実施する場合に比べて安全性が低くなります。	国チャネルまたはすべてのチャネルで不正を検出するように、無線の種類 802.11a/n および 802.11b/g/n を設定します。
コントローラ上で、アドホック ネットワークを検出およびレポートする不正ポリシーが無効になっています。	アドホック ネットワークの検出およびレポートが無効である場合、アドホックの不正アクセス ポイントが検出されません。	アドホック ネットワークを検出およびレポートする不正ポリシーを有効にします。
コントローラ上で「すべての標準シグニチャおよびカスタム シグニチャのチェック」が無効になっています。	すべての標準シグニチャおよびカスタム シグニチャのチェックを無効にすると、受信 802.11 パケットのさまざまなタイプの攻撃が検出されないことがあります。	一部の標準シグニチャのみが無効な場合には、無効なシグニチャに関連する攻撃が検出されないことがあります。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
一部の標準シグニチャがコントローラ上で無効です。	一部の標準シグニチャのみが無効な場合には、受信 802.11 パケットのさまざまなタイプの攻撃が検出されないことがあります。	コントローラですべての標準シグニチャを有効にします。
コントローラ上で「過剰な 802.11 のアソシエーションの失敗」によるクライアントの除外ポリシーが無効になっています。	アソシエーションの試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	コントローラ上で「過剰な 802.11 のアソシエーションの失敗」によるクライアントの除外ポリシーを有効にします。
コントローラ上で「過剰な 802.11 認証の失敗」によるクライアントの除外ポリシーが無効になっています。	認証の試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	コントローラ上で「過剰な 802.11 認証の失敗」によるクライアントの除外ポリシーを有効にします。
コントローラ上で「過剰な 802.1X 認証の失敗」によるクライアントの除外ポリシーが無効になっています。	802.1X 認証の試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	インフラストラクチャに対する DoS 攻撃を回避するには、過剰な 802.1X 認証の失敗によるクライアントの除外ポリシーを有効にする必要があります。
コントローラ上で「過剰な 802.11 Web 認証の失敗」によるクライアントの除外ポリシーが無効になっています。	802.11 Web の Web 認証の試みが過剰に失敗すると、システム リソースを消費して、インフラストラクチャに対する DoS 攻撃になることがあります。	コントローラ上で「過剰な 802.11 Web 認証の失敗」によるクライアントの除外ポリシーを有効にします。
コントローラ上で、「IP の盗難または IP の再使用」クライアント除外ポリシーが無効になっています。	IP の盗難または再使用のクライアントの除外ポリシーが無効である場合、別のクライアントになりすました攻撃者が禁止されなくなります。	コントローラ上で、「IP の盗難または IP の再使用」クライアント除外ポリシーを有効にします。
コントローラ上に CIDS センサーが設定されていません。	有効な IDS センサーが設定されていない場合、IP レベルの攻撃は通常は検出されません。	コントローラに 1 つ以上の CIDS センサーを設定します。
コントローラは、SNMP v1/v2 のデフォルト コミュニティ ストリングを使用して設定されています。	デフォルト コミュニティの SNMP V1 または V2 が設定されている場合、デフォルト コミュニティはよく知られているため、攻撃を受けやすくなります。	Auth タイプおよび Privacy タイプの SNMPv3 を使用します。
コントローラは、SNMP v1/v2 のデフォルトでないコミュニティ ストリングを使用して設定されています。	デフォルト コミュニティでない SNMP V1 または V2 はデフォルト コミュニティに比べてやや安全ですが、SNMP V3 に比べると安全ではありません。	Auth タイプおよび Privacy タイプの SNMPv3 を使用します。
コントローラ上で、SNMPv3 はデフォルト ユーザを使用して設定されています。	デフォルト ユーザを使用すると、SNMP V3 接続の安全性が低下します。	Auth タイプおよび Privacy タイプの SNMPv3 にデフォルト以外のユーザ名を使用します。

表 3-7　潜在的なセキュリティ問題 （続き）

コントローラのセキュリティ問題	問題となる理由	ソリューション
コントローラ上で SNMPv3 は Auth タイプも Privacy タイプも使用しないで設定されています。	Auth タイプまたは Privacy タイプの SNMP V3 が None に設定されている場合、SNMP V3 接続の安全性が低下します。	Auth タイプおよび Privacy タイプの SNMPv3 を使用して、ワイヤレス ネットワークを保護します。
コントローラ上で HTTP（Web モードは有効、セキュア Web モードは無効）が有効になっています。	HTTP は HTTPS に比べて安全性が低くなります。	コントローラ上で HTTPS（Web モードとセキュア Web モードの両方）を有効にします。
Telnet はコントローラ上で有効になっています。	Telnet が有効な場合、コントローラはハッキングされるリスクがあります。	コントローラ上の Telnet を無効にします。
コントローラ上で SSH は無効になっており、タイムアウト値はゼロに設定されています。	SSH が有効でタイムアウトが 0 に設定されている場合、コントローラはハッキングされるリスクがあります。	コントローラ上でゼロ以外のタイムアウト値を設定して SSH を有効にします。
Telnet は AP 上で有効になっています。	Telnet が有効な場合、アクセス ポイントはハッキングされるリスクがあります。	すべてのアクセス ポイントで Telnet を無効にします。
SSH は AP 上で有効になっています。		すべてのアクセス ポイントで SSH を無効にします。
AP の少なくとも 1 つが、デフォルト ユーザ名またはパスワードで設定されています。	デフォルトのパスワードが設定されている場合、アクセス ポイントはネットワーク外部からの接続により影響を受けやすくなります。	コントローラにアソシエートされているすべてのアクセス ポイントに、デフォルト以外のユーザ名および強度が高いパスワードを設定します。

表 3-8　潜在的なセキュリティ問題

ロケーション サーバ/モビリティ サーバ エンジンのセキュリティ問題	問題となる理由	ソリューション
HTTP がロケーション サーバ上で有効です。	HTTP は HTTPS に比べて安全性が低くなります。	ロケーション サーバ上で HTTPS を有効にします。
ロケーション サーバのユーザにデフォルトのパスワードが設定されています。	デフォルトのパスワードが設定されている場合、ロケーション サーバ/モビリティ サーバ エンジンはネットワーク外部からの接続により影響を受けやすくなります。	ロケーション サーバのユーザに強度が高いパスワードを設定します。
HTTP がモビリティ サービス エンジン上で有効です。	HTTP は HTTPS に比べて安全性が低くなります。	モビリティ サービス エンジン上で HTTPS を有効にします。

表 3-8　潜在的なセキュリティ問題 （続き）

ロケーション サーバ/モビリティ サーバ エンジンのセキュリティ問題	問題となる理由	ソリューション
モビリティ サービス エンジンのユーザにデフォルトのパスワードが設定されています。	デフォルトのパスワードが設定されている場合、ロケーション サーバ/モビリティ サーバ エンジンはネットワーク外部からの接続により影響を受けやすくなります。	モビリティ サービス エンジン上のユーザに、強度が高いパスワードを設定します。
wIPS サービスがモビリティ サービス エンジン上で有効ではありません。	ネットワークは、高度なセキュリティ上の脅威に対して脆弱です。	wIPS サービスを展開して、高度なセキュリティ上の脅威からネットワークを保護します。

スイッチ ポート トレース

現在、Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、ネイバー リストにないフレームから検出された BSSID アドレスが記載されています。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方法を使用した場合、Prime Infrastructure では、そのまま、コントローラから受信した情報を収集します。一方、ソフトウェア リリース 5.1 では、有線の不正アクセス ポイントのスイッチ ポートに関するスイッチ ポート トレーシングを組み込むことができます。この機能拡張により、検出された不正なアクセス ポイントに対応し、今後発生する攻撃を回避できます。トレース情報は不正アクセス ポイントの Prime Infrastructure ログだけで使用でき、不正クライアントのログには使用できません。

（注）　不正アクセス ポイントに接続した不正クライアントの情報を使用して、ネットワークで不正アクセス ポイントに接続したスイッチ ポートを追跡します。

（注）　危険性のない不正アクセス ポイントまたは削除された不正アクセス ポイントにトレーシングを設定しようとすると、警告メッセージが表示されます。

（注）　スイッチ ポート トレーシングで、SNMP v3 を使用してスイッチ ポートを正常にトレースするには、すべての OID を SNMP v3 のビューに含める必要があり、SNMP v3 グループ内の VLAN ごとに VLAN の内容を作成する必要があります。

スイッチ ポート トレーシングの確立

スイッチ ポート トレーシングを確立するには、次の手順に従ってください。

ステップ 1　Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。

ステップ 2　[Rogue APs and Adhoc Rogues] ダッシュレットで、不正要素の過去 1 時間以内、過去 24 時間以内、および合計のアクティブ数な指定する数値 URL をクリックします。[Alarms] ウィンドウが開きます。

ステップ 3　チェックボックスをオンにして、スイッチ ポートのトラッキングを設定している不正を選択します。

ステップ 4　[Troubleshoot] ドロップダウン リストから、[Traceroute] を選択します。[Traceroute] ウィンドウが開き、Prime Infrastructure がスイッチ ポートのトレースを実行します。

検索可能な MAC アドレスを 1 つ以上使用できる場合、Prime Infrastructure では CDP を使用して、検出中のアクセス ポイントから最大 2 ホップ離れて接続されているすべてのスイッチを検出します。各 CDP が検出したスイッチの MIB は、対象の MAC アドレスのいずれかが含まれているかどうかを確認するために検証されます。いずれかの MAC アドレスが見つかった場合、該当するポート番号が返され、不正アクセス ポイントのスイッチ ポートとして報告されます。

統合されたセキュリティ ソリューション

Cisco Unified Wireless Network Solution では、次の統合されたセキュリティ ソリューションも用意されています。

- Cisco Unified Wireless Network Solution オペレーティング システムのセキュリティは、堅牢な 802.1X AAA（認証、許可、アカウンティング）エンジンを中心に構築されており、オペレータは、Cisco Unified Wireless Network Solution 全体にわたってさまざまなセキュリティ ポリシーを迅速に設定および適用できます。
- コントローラおよびアクセス ポイントには、システム全体の認証および許可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステム セキュリティが実現されています。
- オペレーティング システムのセキュリティ ポリシーは個別の無線 LAN に割り当てられ、アクセス ポイントは設定されたすべての無線 LAN（最大 16）に同時にブロードキャストします。このポリシーにより、干渉の増加やシステム スループットの低下が発生する可能性のある、アクセス ポイントの追加が不要になる場合があります。
- オペレーティング システムのセキュリティは、RRM 機能を使用して、干渉およびセキュリティ侵犯がないか継続的に空間をモニタし、それらを検出したときはオペレータに通知します。
- オペレーティング システムのセキュリティは、業界標準の AAA サーバで動作し、システム統合が単純で簡単です。
- Cisco Intrusion Detection System（IDS; 侵入検知システム）/Intrusion Protection System（IPS; 侵入防御システム）は、特定のクライアントに影響を及ぼす攻撃を検出すると、コントローラにそれらのクライアントの無線ネットワークへのアクセスをブロックするように指示します。
- オペレーティング システムのセキュリティ ソリューションは、通常、高い処理能力を必要とする、包括的なレイヤ 2 およびレイヤ 3 の暗号化アルゴリズムを実現します。コントローラに VPN/ 拡張セキュリティ モジュールを装備することで、高度なセキュリティ設定に必要なハードウェアとしての機能も実現でき、暗号化を別のサーバで行う必要はありません。

Prime Infrastructure を使用した Cisco Unified Wireless Network Solution のレイヤ 3 モードからレイヤ 2 モードへの変換

Prime Infrastructure ユーザ インターフェイスを使用して Cisco Unified Wireless Network Solution をレイヤ 3 モードからレイヤ 2 LWAPP 転送モードに変換する手順は以下のとおりです。

（注） Cisco ベースの Lightweight アクセス ポイントでは、レイヤ 2 LWAPP モードはサポートされません。このようなアクセス ポイントは、レイヤ 3 でしか実行できません。

（注） この手順を実行すると、コントローラが再度ブートしてアクセス ポイントがコントローラと再アソシエートするまで、アクセス ポイントはオフラインになります。

ステップ 1　コントローラとアクセス ポイントはすべて同じサブネット上に配置するようにします。

（注） 変換を実行する前に、コントローラおよびアソシエートしているアクセス ポイントをレイヤ 2 モードで動作するように設定する必要があります。

ステップ 2　Prime Infrastructure ユーザ インターフェイスにログインします。LWAPP 転送モードをレイヤ 3 からレイヤ 2 に変換する手順は、次のとおりです。

a. [Configure] > [Controllers] の順に選択し、[All Controllers] ページに移動します。

b. 目的のコントローラの IP アドレスをクリックして、[IP Address] > [Controller Properties] ページを表示します。

c. 左側のサイドバーのメニューから、[System] > [General] の順にクリックして、[IP Address] > [General] ページを表示します。

d. LWAPP 転送モードを [Layer2] に変更し、[Save] をクリックします。

e. Prime Infrastructure で次のメッセージが表示された場合、[OK] をクリックします。

```
Please reboot the system for the LWAPP Mode change to take effect.
```

ステップ 3　Cisco Unified Wireless Network Solution を再起動する手順は以下のとおりです。

a. [IP Address] > [Controller Properties] ページに戻ります。

b. [System] > [Commands] の順にクリックして、[IP Address] > [Controller Commands] ページを表示します。

c. [Administrative Commands] で、[Save Config To Flash] を選択し [Go] をクリックして、変更した設定をコントローラに保存します。

d. [OK] をクリックして作業を続行します。

e. [Administrative Commands] で、[Reboot] を選択し [Go] をクリックして、コントローラをリブートします。

f. [OK] をクリックし、設定を保存してリブートすることを確認します。

ステップ 4　コントローラが再度ブートした後で LWAPP 転送モードがレイヤ 2 になっていることを確認する手順は、次のとおりです。

a. [Monitor] > [Controllers] の順にクリックし、[Controllers] > [Search Results] ページに移動します。

b. 目的のコントローラの IP アドレスをクリックして、[Controllers] > [IP Address] > [Summary] ページを表示します。

c. [General] で、現在の LWAPP 転送モードが [Layer2] になっていることを確認します。

これで、レイヤ 3 からレイヤ 2 への LWAPP 転送モードの変換が完了しました。オペレーティング システムのソフトウェアによって、同じサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

Prime Infrastructure のファイアウォールの設定

Prime Infrastructure サーバと Prime Infrastructure ユーザ インターフェイスがファイアウォールの同じ側にない場合、ファイアウォール上の次のポートが双方向のトラフィックに対してオープンになっていない限り、これらは通信できません。

- 80（初期 HTTP 用）
- 69（TFTP）
- 162（トラップ）
- 443（HTTPS）
- 1522（プライマリとセカンダリの Prime Infrastructure 間で HA を設定する場合）

これらのポートをオープンにして、Prime Infrastructure サーバと Prime Infrastructure ユーザ インターフェイスとの間の通信を許可するようにファイアウォールを設定します。

アクセス ポイント許可

アクセス ポイントが許可に使用する証明書の種類とともに、許可済みアクセス ポイントの一覧を表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　[IP Address] 列で URL の 1 つをクリックします。

ステップ 3　左側のサイドバーのメニューから [Security] > [AP/MSE Authorization] の順に選択します。

ステップ 4　ページの [AP Policies] 部分に、アクセス ポイントの許可が有効かどうかが示されます。また、自己署名証明書（SSC AP）の承認が有効かどうかも示されます。通常は、アクセス ポイントは AAA または証明書によって許可されます。（SSC は 4400 シリーズ コントローラおよび 2100 シリーズ コントローラのみに使用）。

これらの値を変更するには、[Select a command] ドロップダウン リストから [Edit AP Policies] を選択し、[Go] をクリックします。

ステップ 5　[AP Authorization List] 部分にアクセス ポイントの無線 MAC アドレス、証明書の種類、およびキー ハッシュが表示されます。別の許可エントリを追加するには、[Select a command] ドロップダウン リストから [Add AP/MSE Auth Entry] を選択し、[Go] をクリックします。

ステップ 6　ドロップダウン リストからこのコントローラに適用するテンプレートを選択して [Apply] をクリックします。アクセス ポイント許可の新しいテンプレートを作成するには、[click here] をクリックして、テンプレート作成ページにリダイレクトされるようにします。新しいテンプレートの作成手順については、「アクセス ポイント許可または MSE 許可テンプレートの設定」（P.11-664）を参照してください。

管理フレーム保護（MFP）

Management Frame Protection（MFP; 管理フレーム保護）では、アクセス ポイントとクライアント間で送受信される 802.11 管理メッセージを保護および暗号化することにより、セキュリティが確保されます。MFP は、インフラストラクチャとクライアント サポートの両方を実現します。

- インフラストラクチャ MFP：敵対者を発見することにより、管理フレームを保護します。敵対者は、DoS 攻撃を引き起こし、アソシエーションおよびプローブ パケットでネットワークを氾濫させ、不正アクセス ポイントをさしはさみ、QoS および無線測定フレームを攻撃してネットワーク パフォーマンスに影響を与えます。インフラストラクチャ MFP はまた、フィッシング インシデントの効果的かつ迅速な検出/報告手段を提供します。

  特に、インフラストラクチャ MFP では、アクセス ポイントによって送信される管理フレームに Message Integrity Check Information Element（MIC IE）を追加することにより、802.11 セッション管理機能を保護します。Message Integrity Check Information Element（MIC IE）はネットワーク内のその他のアクセス ポイントにより検証されます。インフラストラクチャ MFP はパッシブです。侵入を検知し報告しますが、それを止めることはできません。

- クライアント MFP：認証されたクライアントをスプーフィング フレームから保護し、無線 LAN に対する多くの一般化した攻撃が効力を発揮することのないようにします。認証解除攻撃などのほとんどの攻撃では、有効なクライアントとの競合により簡単にパフォーマンスを悪化させます。

  特に、アクセス ポイントとクライアントの両方が、スプーフされたクラス 3 管理フレーム（つまり、認証済みでアソシエートが完了しているアクセス ポイントとクライアント間で受け渡される管理フレーム）をドロップして予防措置を講じることができるように、クライアント MFP ではアクセス ポイントと Cisco Compatible Extension クライアント間で送信される管理フレームを暗号化します。クライアント MFP は、IEEE 802.11i によって定義されたセキュリティ メカニズムを利用し、アソシエーション解除、認証解除、および QoS（WMM）アクションといったタイプのクラス 3 ユニキャスト管理フレームを保護します。クライアント MFP はアクティブです。最も一般的な DoS 攻撃から、クライアントとアクセス ポイントとのセッションを保護できます。ここでは、セッションのデータ フレームで使用されるのと同じ暗号化方式を使用することにより、クラス 3 管理フレームが保護されます。アクセス ポイントまたはクライアントにより受信されたフレームの暗号化解除に失敗すると、そのフレームはドロップされ、イベントがコントローラに報告されます。

  クライアント MFP を使用するには、クライアントは Cisco Compatible Extensions（バージョン 5）MFP をサポートしている必要があり、TKIP または AES-CCMP のいずれかを使用する WPA2 をネゴシエートする必要があります。EAP または PSK は、PMK を取得するために使用できます。アクセス ポイント間、またはレイヤ 2 とレイヤ 3 の高速ローミングでセッション キーを配信するために、CCKM およびコントローラ モビリティ管理が使用されます。

  ブロードキャスト フレームに対する攻撃を防ぐために、Cisco Compatible Extensions（バージョン 5）をサポートしているアクセス ポイントは、ブロードキャスト クラス 3 管理フレーム（アソシエーション解除、認証解除、またはアクションなど）を送信しません。Compatible Extensions クライアント（バージョン 5）とアクセス ポイントは、ブロードキャスト クラス 3 管理フレームを破棄します。

  クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足します。これは、インフラストラクチャ MFP が、無効なクラス 1 管理フレームとクラス 2 管理フレームだけでなく、クライアント MFP 対応ではないクライアントに送信される無効なユニキャスト フレームを検出して報告し続けるためです。インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

インフラストラクチャ MFP は次の 3 つの主要なコンポーネントで構成されます。

- 管理フレーム保護：アクセス ポイントは、送信される各管理フレームに MIC IE を追加することによってフレームを保護します。フレームのコピー、変更、再送が試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。

- 管理フレーム検証：インフラストラクチャ MFP でアクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。これにより、MC IE が存在し（発信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身が一致していることを確認できます。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの正当な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。タイムスタンプが適切に機能するには、すべてのコントローラでネットワーク タイム プロトコル（NTP）が同期されている必要があります。
- イベント報告：アクセス ポイントは異常を検出するとコントローラに通知し、コントローラは受信した異常イベントを集約して、SNMP トラップ経由でネットワーク管理システムに結果を報告します。

（注）　クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP は、デフォルトで有効化されており、システム全体で無効化できます。以前のソフトウェア リリースからアップグレードする場合、アクセス ポイント認証が有効になっているときは、これら 2 つの機能は相互に排他的であるため、インフラストラクチャ MFP はシステム全体で無効になります。インフラストラクチャ MFP がシステム全体で有効にされている場合、選択した WLAN に対してシグニチャ生成（送信フレームへの MIC の追加）を無効にし、選択したアクセス ポイントに対して検証を無効にできます。

WLAN テンプレートで MFP を設定します。「WLAN テンプレートの設定」（P.11-620）を参照してください。

MFP の使用に関するガイドライン

MFP を使用する際のガイドラインは次のとおりです。

- MFP 機能では、AP 1500 シリーズのメッシュ アクセス ポイントを除く、Cisco Aironet Lightweight アクセス ポイントでの使用がサポートされています。
- Lightweight アクセス ポイントは、ローカル モードとモニタ モードでインフラストラクチャ MFP をサポートし、アクセス ポイントがコントローラに接続されているときには REAP モードと FlexConnect モードをサポートします。クライアント MFP は、ローカル モード、FlexConnect モード、およびブリッジ モードでサポートされます。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する Cisco Compatible Extensions（バージョン 5）クライアントでだけ使用がサポートされています。
- Cisco Compatible Extensions（バージョン 5）以外のクライアントは、クライアント MFP が無効もしくはオプション設定の場合のみ、WLAN にアソシエートできます。

侵入検知システム（IDS）の設定

Cisco Intrusion Detection System（IDS; 侵入検知システム）/Intrusion Prevention System（IPS; 侵入防御システム）は、特定のクライアントに影響を及ぼす攻撃を検出すると、このクライアントのワイヤレス ネットワークへのアクセスをブロックするようにコントローラに指示します。このシステムにより、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーションの不正使用などの脅威を検出し、分類し、阻止するための重要なネットワーク保護を実現できます。IDS で攻撃の検出に使用できる方法は 2 つあります。

- IDS センサー（レイヤ 3 用）
- IDS シグニチャ（レイヤ 2 用）

IDS センサーの表示

センサーが攻撃を識別した場合は、攻撃しているクライアントを回避するようにコントローラに警告します。新しい IDS センサーを追加した場合は、回避したクライアントのレポートをセンサーがコントローラに送信できるように、コントローラをその IDS センサーに登録します。また、コントローラは定期的にセンサーをポーリングします。

IDS センサーを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[Security] > [IDS Sensor Lists] の順に選択します。[IDS Sensor] ページが表示されます。このページでは、このコントローラに設定されているすべての IDS センサーが一覧表示されます。

IDS シグニチャの設定

コントローラ上で、*IDS シグニチャ*、または受信する 802.11 パケットにおけるさまざまなタイプの攻撃を識別するのに使用されるビット パターンのマッチング ルールを設定することができます。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が取られます。

シスコでは、標準シグニチャとカスタムなシグニチャのページで示すように、コントローラで 17 個の標準シグニチャをサポートします。このページを開くには、[Configure] > [Controllers] を選択し、コントローラの IP アドレスを選択して、左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Standard Signatures] を選択します。

これらのシグニチャは 6 つの主要なグループに分かれます。最初の 4 つのグループには管理フレーム用シグニチャが含まれ、最後の 2 つのグループにはデータ フレーム用シグニチャが含まれます。

- ブロードキャスト解除フレーム シグニチャ：ブロードキャスト認証解除フレーム攻撃において、ハッカーは別のクライアントのブロードキャスト MAC 宛先アドレスに対して 802.11 認証解除フレームを送信します。この攻撃により、宛先クライアントは接続アクセス ポイントから強制的にアソシエーション解除させられ、ネットワークの接続断が発生します。この処理が繰り返されると、クライアントでサービス利用ができない状態が発生します。ブロードキャスト認証解除フレーム シグニチャ（優先順位 1）を使用してそのような攻撃を検出する場合、アクセス ポイントでは、シグニチャの特性と一致するクライアント送信ブロードキャスト認証解除フレームがリッスンされます。アクセス ポイントは、そのような攻撃を検出すると、コントローラに警告を送ります。システムの設定に応じて、危険性のあるデバイスが封じ込められて、そのデバイスの信号が許可されたクライアントに干渉しないようにされるか、コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されるか、または、その両方が実行されます。
- NULL プローブ応答シグニチャ：NULL プローブ応答攻撃において、ハッカーはワイヤレス クライアント アダプタに NULL プローブ応答を送信します。結果として、クライアント アダプタがロックされます。NULL プローブ応答シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントはワイヤレス クライアントを特定し、コントローラに警告を送ります。NULL プローブ応答シグニチャには次のものがあります。
  - NULL probe resp 1（優先順位 2）
  - NULL probe resp 2（優先順位 3）

- 管理フレーム フラッドシグニチャ：管理フレーム フラッド攻撃において、ハッカーはアクセス ポイントに大量の 802.11 管理フレームを送り付けます。その結果、アクセス ポイントにアソシエートしている、もしくはアソシエートを試みているすべての端末に対して、サービス利用ができない状態が発生します。この攻撃は、アソシエーション要求、認証要求、再アソシエーション要求、プローブ要求、アソシエーション解除要求、認証解除要求、予約管理サブタイプなど、さまざまなタイプの管理フレームを使用して実行されます。

  管理フレーム フラッド シグニチャによってこれらの攻撃を検出すると、アクセス ポイントは、シグニチャの全体的な特性と合致する管理フレームを特定します。これらのフレームの検出頻度が、シグニチャで設定されたしきい値より大きくなると、これらのフレームを受信するアクセス ポイントによって警告が送信されます。コントローラではトラップが生成され、Prime Infrastructure に転送されます。

  管理フレーム フラッド シグニチャには次のものがあります。

  - Assoc flood（優先順位 4）
  - Auth flood（優先順位 5）
  - Reassoc flood（優先順位 6）
  - Broadcast probe flood（優先順位 7）
  - Disassoc flood（優先順位 8）
  - Deauth flood（優先順位 9）
  - Reserved mgmt 7（優先順位 10）
  - Reserved mgmt F（優先順位 11）

  予約管理フレーム シグニチャ（Reserved mgmt）7 および F は、将来使用するために予約されています。

- EAPOL フラッド シグニチャ：EAPOL フラッド攻撃において、ハッカーは 802.1X 認証要求を含む EAPOL フレームを大量に発生させます。結果として、802.1X 認証サーバはすべての要求に応答できなくなり、有効なクライアントに正常な認証応答を送信できなくなります。そして、その影響を受けるすべてのクライアントにおいてサービス利用ができない状況が発生します。EAPOL フラッド シグニチャ（優先順位 12）を使用してそのような攻撃が検出されると、アクセス ポイントは EAPOL パケットの最大許容数を超えるまで待機します。次に、コントローラに警告を送り、適切な緩和措置を実行します。

- NetStumbler シグニチャ：NetStumbler は、無線 LAN スキャン ユーティリティです。これによって、アクセス ポイントのブロードキャスト関連情報（動作チャネル、RSSI 情報、アダプタ製造業者名、SSID、WEP ステータス、GPS が接続された NetStumbler を実行するデバイスの経度と緯度など）が報告されます。NetStumbler は、アクセス ポイントに対する認証とアソシエーションに成功すると、次の文字列のデータ フレーム（表 3-9 にリストした NetStumbler のバージョンによって異なる）を送信します。

表 3-9　NetStumbler バージョン

バージョン	文字列
3.2.0	「Flurble gronk bloopit, bnip Frundletrune」
3.2.3	「All your 802.11b are belong to us」
3.3.0	ホワイト スペースを送信

NetStumbler シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定してコントローラに警告を送ります。NetStumbler シグニチャには次のものがあります。

- NetStumbler 3.2.0（優先順位 13）
- NetStumbler 3.2.3（優先順位 14）
- NetStumbler 3.3.0（優先順位 15）
- NetStumbler generic（優先順位 16）

- Wellenreiter シグニチャ：Wellenreiter は、無線 LAN スキャンおよびディスカバリ ユーティリティです。これを使用すると、アクセス ポイントおよびクライアントに関する情報が漏洩してしまう可能性があります。Wellenreiter シグニチャ（優先順位 17）を使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定し、コントローラに警告を送ります。

この項では、シグニチャを設定する手順について説明します。この項で取り上げるトピックは次のとおりです。

- 「IDS シグニチャのアップロード」（P.3-105）
- 「IDS シグニチャのダウンロード」（P.3-106）
- 「IDS シグニチャの有効化または無効化」（P.3-107）

IDS シグニチャのアップロード

コントローラから IDS シグニチャをアップロードする手順は、次のとおりです。

ステップ 1　シスコからシグニチャ ファイルを入手します（以降、*標準シグニチャ ファイル*）。「IDS シグニチャのダウンロード」（P.3-106）に従い、独自のシグニチャ ファイル（*カスタム シグニチャ ファイル*）を作成することもできます。

ステップ 2　シグニチャ ダウンロード用の TFTP サーバを設定します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。ただし、管理ポートがダウンしている間、TFTP サーバを別のネットワークに配置する場合は、サービス ポートのあるサブネットにゲートウェイがあれば、スタティック ルートを追加します（config route add *IP address of TFTP server*）。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 3　[Configure] > [Controllers] の順に選択します。

ステップ 4　IP アドレスをクリックしてコントローラを選択します。

ステップ 5　左側のサイドバーのメニューから [Security] を選択し、[Standard Signatures] または [Custom Signatures] を選択します。

ステップ 6　[Select a Command] ドロップダウン リストから、[Upload Signature Files from Controller] を選択します。

ステップ 7　転送に使用している TFTP サーバ名を指定します。

ステップ 8　新規の TFTP サーバを利用する場合は、[Server IP Address] フィールドで TFTP IP アドレスを入力します。

ステップ 9　[File Type] ドロップダウン リストから [Signature Files] を選択します。

ステップ 10　このシグニチャ ファイルは、TFTP サーバによる使用に対して設定されたルート ディレクトリにアップロードされます。[Upload to File] フィールドで別のディレクトリに変更できます（このフィールドは、[Server Name] がデフォルト サーバの場合のみ表示）。コントローラはベース ネームとしてこのローカル ファイル名を使用し、標準シグニチャ ファイルの拡張子として *_std.sig* を、カスタム シグニチャ ファイルの拡張子として *_custom.sig* を追加します。

ステップ 11　[OK] をクリックします。

IDS シグニチャのダウンロード

標準のシグニチャ ファイルがすでにコントローラ上にあり、カスタマイズされたシグニチャをコントローラにダウンロードする場合は、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Download IDS Signatures] を選択し、[Go] をクリックします。

ステップ 5　シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 6　[File is Located On] フィールドから [local machine] を選択します。ファイル名および、サーバのルート ディレクトリに対する相対的なパスがわかる場合は、TFTP サーバを選択することもできます。

ステップ 7　[Maximum Retries] フィールドに、コントローラがシグニチャ ファイルのダウンロードを試みる最大回数を入力します。

ステップ 8　[Timeout] フィールドに、シグニチャ ファイルのダウンロードを試行する際、コントローラがタイムアウトになるまでの最大時間を秒単位で入力します。

ステップ 9　ファイルは /localdisk/tftp ディレクトリにアップロードされます。そのディレクトリでのローカル ファイル名を指定し、[Browse] ボタンを使用してそのファイル名に移動します。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

ステップ 10　何らかの理由で転送がタイムアウトした場合には、[File Is Located On] フィールドの [TFTP] サーバ オプションを選択すると、[Server File Name] が読み込まれ、再試行されます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、[download web] ページには、自動的にファイル名が入力されます。

ステップ 11　[OK] をクリックします。

IDS シグニチャの有効化または無効化

IDS シグニチャを有効または無効にする手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから [Security] を選択し、[Standard Signatures] または [Custom Signatures] を選択します。

ステップ 4　個々のシグニチャを有効または無効にするには、有効または無効にしたい攻撃の種類の [Name] 列をクリックします。

[Standard Signature Parameters] ページには、現在コントローラ上にあるシスコ提供のシグニチャの一覧が表示されます。[Custom Signatures] ページには、現在コントローラ上に存在する、カスタマー提供のシグニチャのリストが表示されます。シグニチャ ページまたは詳細シグニチャ ページに次の情報が表示されます。

- [Precedence]：コントローラがシグニチャ チェックを行う順序、または優先順位。
- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータフレームの種類。
- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。なにも処置をとらない場合は *None*、検出を報告する場合は *Report* となります。
- [Frequency]：シグニチャの検出頻度、もしくは攻撃が検出される前に、各アクセス ポイント レベルでの検出において識別されるべき、[Interval] 設定間隔におけるシグニチャに合致するパケット数。設定可能な値の範囲は、[Interval] 設定間隔あたり 1 ～ 32,000 パケットです。デフォルト値は [Interval] 設定間隔あたり 50 パケットです。
- [Quiet Time]：各アクセス ポイント レベルで攻撃が検出されなくなってから、アラームを停止するまでの時間の長さ（秒単位）。この設定は、次項の [MAC Information] の設定が [all] もしくは [both] の場合にだけ表示されます。設定可能な値の範囲は 60 ～ 32,000 秒で、デフォルト値は 300 秒です。
- [MAC Information]：アクセス ポイント レベルの検出においてシグニチャをネットワークごとまたは MAC アドレスごと、または両方で追跡するどうか。
- [MAC Frequency]：シグニチャ MAC の検出頻度、もしくは攻撃が検出される前にコントローラ レベルの検出において識別する必要のある、[Interval] 設定間隔ごとのシグニチャと一致するパケット数です。有効な範囲は [Interval] 設定間隔あたり 1 ～ 32,000 パケットです。デフォルト値は [Interval] 設定間隔あたり 30 パケットです。
- [Interval]：シグニチャの検出頻度がしきい値に達したかどうかをチェックする間隔（秒単位）を入力します。設定可能な値の範囲は 1 ～ 3600 秒で、デフォルト値は 1 秒です。
- [Enable]：セキュリティ攻撃の検出でこのシグニチャを有効にする場合に選択し、このシグニチャを無効にする場合に選択解除します。
- [Signature Patterns]：セキュリティ攻撃の検出に使用されるパターン。

ステップ 5　[Enabled yes or no] ドロップダウン リストで、[yes] を選択します。カスタマイズされたシグニチャをダウンロードしているため、_custom.sgi という名前の付いたファイルを有効にし、同じ名前で異なる拡張子を持つ標準シグニチャを無効にする必要があります。（たとえば、ブロードキャスト プローブの大量送信をカスタマイズしている場合に、ブロードキャスト プローブの大量送信を標準シグニチャでは無効にしたいがカスタム シグニチャでは有効にしたい場合がある）。

ステップ 6　現在コントローラ上にある標準シグニチャとカスタム シグニチャをすべて有効にするは、[Select a command] ドロップダウン リストから [Edit Signature Parameters] を選択し、[Go] を選択します。[Edit Signature Parameters] ページが表示されます。

ステップ 7　[Check for All Standard and Custom Signatures] フィールド、[Enable] チェックボックスをオンにします。これにより、ステップ 5 で個々に選択して有効にしたシグニチャすべてを有効にします。このチェックボックスをオフのままにすると、前にステップ 5 で有効にしていても、すべてのファイルは無効になります。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。

ステップ 8　[Save] をクリックします。

Web ログインの有効化

Web 認証により、ゲストはブラウザを起動すると自動的に Web 認証ページにリダイレクトされます。ゲストは、この Web ポータルから WLAN にアクセスできます。この認証メカニズムを使用している無線 LAN 管理者は、ゲスト ユーザによるアクセスに対して、暗号化通信と非暗号化通信のどちらを設定するかを選択できます。ゲスト ユーザは、SSL で暗号化される有効なユーザ名とパスワードを使用して無線ネットワークにログインできます。Web 認証アカウントはローカルに作成するか、RADIUS サーバで管理できます。Cisco Wireless LAN Controller は Web 認証クライアントをサポートするように設定できます。コントローラで提供される Web 認証ページを置き換えるテンプレートを作成するには、「Web 認証テンプレートの設定」（P.11-667）を参照してください。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　[IP Address] 列で IP アドレス URL をクリックして、Web 認証を有効にするコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [Web Auth Configuration] の順に選択します。

ステップ 4　ドロップダウン リストから適切な Web 認証のタイプを選択します。選択肢は、デフォルトの内部、カスタマイズ Web 認証、または外部です。

- デフォルトの内部を選択した場合でも、ページ タイトル、メッセージ、リダイレクト URL、およびロゴを表示するかどうかを変更できます。ステップ 5 に進みます。
- カスタマイズされた Web 認証を選択する場合は、「カスタマイズされた Web 認証のダウンロード」（P.3-109）に進んでください。
- 外部を選択する場合は、認証に成功した後でリダイレクトする URL を入力する必要があります。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 5　会社のロゴを表示させたい場合は、[Logo Display] チェックボックスをオンにします。

ステップ 6　Web 認証ページに表示するタイトルを入力します。

ステップ 7　Web 認証ページに表示するメッセージを入力します。

ステップ 8　[Customer Redirect URL] フィールドに、認証に成功した後でユーザがリダイレクトされる URL を指定します。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 9　[Save] をクリックします。

カスタマイズされた Web 認証のダウンロード

カスタマイズされた Web 認証ページをコントローラにダウンロードできます。カスタマイズ Web ページは、ユーザ Web アクセス用のユーザ名とパスワードを設定するために作成されます。

カスタマイズ Web 認証をダウンロードする際は、次のガイドラインに従う必要があります。

- ユーザ名を指定する。
- パスワードを指定する。
- リダイレクト URL は、元の URL から引用した後、非表示の入力項目として保持する。
- 操作 URL は、元の URL から引用および設定する。
- 戻りステータス コードをデコードするスクリプトを含める。
- メイン ページで使用されるすべてのパスは相対パスとする。

前の項のステップ 4 において、カスタマイズされた Web 認証オプションを選択した場合は、ダウンロードの前に、次の手順を実行します。

ステップ 1　プレビュー画像をクリックして、サーバからサンプルの login.html バンドル ファイルをダウンロードします。login.html ファイルの例については、図 3-1 を参照してください。ダウンロードしたバンドルは .TAR ファイルとなります。

図 3-1　　Login.html

ステップ 2　Login.html を開いて編集し、これを .tar または .zip ファイルとして保存します。

（注）　任意のテキスト エディタまたは HTML エディタで [Submit] ボタンのテキストを「Accept terms and conditions and Submit」（条件を承諾して送信）などに変更できます。

ステップ 3　ダウンロードに Trivial File Transfer Protocol（TFTP）サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。

- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 4　リンク「After editing the HTML you might click **here** to redirect to the Download Web Auth Page」の [here] をクリックして、.tar ファイルまたは .zip ファイルをコントローラにダウンロードします。[Download Customized Web Auth Bundle to Controller] ページが表示されます。

（注）　バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。

ステップ 5　[File is Located On] フィールドから [local machine] を選択します。ファイル名および、サーバのルート ディレクトリに対する相対的なパスがわかる場合は、TFTP サーバを選択することもできます。

（注）　ローカル マシンのダウンロードには、.zip または .tar のファイル オプションがありますが、Prime Infrastructure では自動的に .zip を .tar に変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイルだけを指定します。

ステップ 6　[Timeout] フィールドに、ファイルをダウンロードする際、コントローラがタイムアウトするまでの最大時間を秒単位で入力します。

ステップ 7　[Prime Infrastructure Server Files In field] は Prime Infrastructure サーバ ファイルのある場所を指定します。そのディレクトリでのローカル ファイル名を指定し、[Browse] ボタンを使用してそのファイル名に移動します。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

ステップ 8　何らかの理由で転送がタイムアウトした場合には、[File Is Located On] フィールドの TFTP サーバ オプションを選択すると、[Server File Name] が読み込まれます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、[download web] ページには、自動的にファイル名が入力されます。

ステップ 9　[OK] をクリックします。

何らかの理由で転送がタイムアウトした場合には、[File Is Located On] フィールドの TFTP サーバ オプションを選択すると、[Server File Name] が読み込まれます。

ステップ 10　ダウンロードが完了すると、新しいページに接続され、認証できます。

ゲスト WLAN への接続

ゲスト セントラル WLAN に接続して Web 認証プロセスを実行する手順は、次のとおりです。ゲスト ユーザ アカウントの詳細については、「ゲスト ユーザ アカウントの作成」（P.7-252）を参照してください。

ステップ 1　オープン認証の設定で接続されている場合は、ブラウザで仮想インターフェイスの IP アドレスにアクセスします（/209.165.200.225/login.html など）。

ステップ 2　Prime Infrastructure ユーザ インターフェイスに [Login] ページが表示されたら、ユーザ名とパスワードを入力します。

（注）　入力する文字はすべて、大文字と小文字が区別されます。

Lobby Ambassador は、ゲスト ユーザを追加する場合以外は、テンプレートにアクセスできません。

証明書署名要求（CSR）の生成

Prime Infrastructure を使用してサードパーティ証明書の証明書署名要求（CSR）を生成するには、付録 C「Cisco Prime Infrastructure でのサードパーティ証明書の証明書署名要求（CSR）の生成」を参照してください。

メンテナンス操作の実行

システム ソフトウェアの更新や証明書のダウンロードなど、システム レベルでさまざまな項目に使用可能なアクションを実行できます。

この章では、Cisco Prime Infrastructure で実行するシステム レベル タスクについて説明します。ここで説明する内容は、次のとおりです。

メンテナンス操作についての情報

システム レベル タスクは、Prime Infrastructure データベース全体に適用される操作に関連したタスクを集めたものです。システム タスクには、Prime Infrastructure データベースの復元も含まれます。詳細については、「Prime Infrastructure データベースの復元方法」（P.4-121）を参照してください。

システム タスクの実行

ここでは、Prime Infrastructure を使用してシステムレベルのタスクを実行する方法について説明します。ここでは、次の内容について説明します。

Prime Infrastructure データベースへのコントローラの追加

Prime Infrastructure データベースにコントローラを追加するには、次の手順に従います。

（注）　セキュリティを向上させるために、コントローラを専用のサービス ポートで管理することを推奨します。ただし、サービス ポートがないコントローラを管理する場合（2000 シリーズ コントローラなど）、またはサービス ポートが無効になっている場合は、コントローラ管理インターフェイスを通してコントローラを管理する必要があります。

ステップ 1　Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Configure] > [Controllers] の順に選択して、[All Controllers] ページを表示します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Controller] を選択し、[Go] をクリックします。

ステップ 4　[Add Controller] ページで、コントローラの IP アドレス、ネットワーク マスク、および必要な SNMP 設定を入力します。

ステップ 5　[OK] をクリックします。コントローラに接続している間、Prime Infrastructure により「Please Wait」というメッセージが表示され、現在のコントローラ設定が Prime Infrastructure データベースに追加されます。次に [Add Controller] ページに戻ります。

ステップ 6　Prime Infrastructure によって、入力した IP アドレスでコントローラが発見されなかった場合は、[Discovery Status] ダイアログに次のメッセージが表示されます。

```
No response from device, check SNMP.
```

次の設定を確認して、問題に対処します。

- コントローラのサービス ポートの IP アドレスが正しく設定されていない可能性があります。コントローラのサービス ポートの設定を確認してください。
- Prime Infrastructure がコントローラに接続できなかった可能性があります。Prime Infrastructure サーバからコントローラに ping できることを確認してください。
- コントローラの SNMP の設定が Prime Infrastructure で入力された SNMP の設定と一致していない可能性があります。コントローラの SNMP の設定が Prime Infrastructure で入力された SNMP の設定と一致していることを確認してください。

ステップ 7　必要に応じてさらにコントローラを追加します。

Prime Infrastructure を使用したシステム ソフトウェアの更新

Prime Infrastructure を使用してコントローラ（およびアクセス ポイント）ソフトウェアを更新するには、次の手順に従います。

ステップ 1　ping *ip-address* コマンドを入力して、Prime Infrastructure サーバがコントローラと通信できるかどうか確認します。外部 TFTP サーバを使用している場合は、ping *ip-address* コマンドを入力して、Prime Infrastructure サーバが TFTP サーバと通信できるかどうか確認します。

（注）　コントローラの Distribution System（DS;ディストリビューション システム）ネットワーク ポートを経由してダウンロードする場合、DS ポートはルーティング可能なので TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。

ステップ 2　[Configure] > [Controllers] の順に選択し、[All Controllers] ページに移動します。

ステップ 3　コントローラのチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Download Software (TFTP or FTP)] を選択して、[Go] をクリックします。Prime Infrastructure で [Download Software to Controller] ページが表示されます。

ステップ 4　組み込みの Prime Infrastructure TFTP サーバを使用する場合は、[Server Name] ドロップダウン リスト ボックスから [Default Server] を選択します。外部 TFTP サーバを使用する場合、[Server Name] ドロップダウン リスト ボックスから [New] を選択し、外部 TFTP サーバの IP アドレスを追加します。

ステップ 5　ファイル パスとサーバ ファイル名を、それぞれのテキストボックスに入力します（たとえば、2000 シリーズ コントローラの場合は AS_2000_*release*.aes）。このファイルは、TFTP サーバによる使用に対して設定されたルート ディレクトリにアップロードされます。別のディレクトリに変更できます。

（注）　コントローラ機種ごとに正しいソフトウェア ファイルを用意する必要があります。

ステップ 6　[Download] をクリックします。Prime Infrastructure によってソフトウェアがコントローラにダウンロードされ、コントローラによってコードがフラッシュ メモリに書き込まれます。Prime Infrastructure がこの機能を実行しているときには、[Status] フィールドに進捗が表示されます。

ベンダー デバイス証明書のダウンロード

各無線デバイス（コントローラ、アクセス ポイント、およびクライアント）は、独自のデバイス証明書を備えています。たとえば、コントローラには、シスコによりインストールされたデバイスの証明書が付属しています。この証明書は、ローカル EAP 認証時に無線クライアントを認証するために、（PAC を使用していない場合）EAP-TLS と EAP-FAST により使用されます。ただし、ご自身のベンダー固有のデバイス証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。

ベンダー固有のデバイス証明書をコントローラにダウンロードするには、次の手順に従います。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　証明書は 2 種類の方法でダウンロードできます。

a.　選択するコントローラのチェックボックスをオンにします。

b.　[Select a Command] ドロップダウン リストから [Download Vendor Device Certificate] を選択し、[Go] をクリックします。

または

a.　[IP Address] 列で必要なコントローラの URL をクリックします。

b.　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

c.　[Upload/Download Command] セクションで、[TFTP] または [FTP] を選択します。

d.　[Upload/Download Commands] ドロップダウン リストから [Download Vendor Device Certificate] を選択し、[Go] をクリックします。

ステップ 3　[Certificate Password] テキスト ボックスに、証明書の保護に使用されたパスワードを入力します。

ステップ 4　ダウンロードする証明書が TFTP サーバ上にあるか、ローカル マシン上にあるかを指定します。証明書が TFTP サーバ上にある場合は、[Server File Name] フィールドにその名前を指定する必要があります。証明書がローカル マシン上にある場合は、[Choose File] ボタンをクリックして、[Local File Name] フィールドにファイル パスを指定します。

ステップ 5　[Server Name] フィールドに TFTP サーバ名を入力します。デフォルトは、Prime Infrastructure サーバを TFTP サーバとして動作させるためのものです。

ステップ 6　サーバの IP アドレスを入力します。

ステップ 7　[Maximum Retries] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 8　[Timeout] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 9　[Local File Name] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 10　[OK] をクリックします。

ベンダー CA 証明書のダウンロード

コントローラとアクセス ポイントには、デバイスの証明書の署名と確認に使用される認証局（CA）の証明書があります。コントローラには、シスコによりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時にワイヤレス クライアントを認証するために、（PAC を使用していない場合）EAP-TLS と EAP-FAST により使用される場合があります。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。ベンダー CA 証明書をコントローラにダウンロードするには、次の手順に従います。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　証明書は 2 種類の方法でダウンロードできます。

a.　選択するコントローラのチェックボックスをオンにします。

b.　[Select a Command] ドロップダウン リストから [Download Vendor CA Certificate] を選択し、[Go] をクリックします。

または

a.　[IP Address] 列で必要なコントローラの URL をクリックします。

b.　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

c.　[Upload/Download Commands] ドロップダウン リストから [Download Vendor CA Certificate] を選択し、[Go] をクリックします。

ステップ 3　ダウンロードする証明書が TFTP サーバ上にあるか、ローカル マシン上にあるかを指定します。証明書が TFTP サーバ上にある場合は、ステップ 9 の [Server File Name] フィールドにその名前を指定する必要があります。証明書がローカル マシン上にある場合は、[Browse] ボタンをクリックして、ステップ 8 の [Local File Name] フィールドにファイル パスを指定します。

ステップ 4　[Server Name] フィールドに TFTP サーバ名を入力します。デフォルトは、Prime Infrastructure サーバを TFTP サーバとして動作させるためのものです。

ステップ 5　サーバの IP アドレスを入力します。

ステップ 6　[Maximum Retries] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 7　[Timeout] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 8　[Local File Name] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 9　[OK] をクリックします。

Prime Infrastructure を使用したロング プリアンブルの有効化（SpectraLink 社の NetLink 電話用）

無線プリアンブル（ヘッダーとも呼ばれる）は、パケットの先頭部分にあるデータのセクションです。これには、パケットを送受信する際に無線デバイスが必要とする情報が格納されています。ショート プリアンブルの方がスループット パフォーマンスが向上するため、デフォルトではこちらが有効になっています。ただし、SpectraLink 社の NetLink 電話などの一部の無線デバイスは、ロング プリアンブルを必要とします。

無線 LAN 上にある SpectraLink 社 NetLink 電話の動作を最適化するために、Prime Infrastructure を使用してロング プリアンブルを有効化するには、次の手順に従います。

ステップ 1　Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Configure] > [Controllers] の順に選択し、[All Controllers] ページに移動します。

ステップ 3　目的のコントローラの IP アドレスをクリックします。

ステップ 4　左側のサイドバーのメニューから、[802.11b/g/n] >[Parameters] の順に選択します。

ステップ 5　[*IP Address* > 802.11b/g/n Parameters] ページでショート プリアンブルが有効になっている場合は、次のステップに進みます。ショート プリアンブルが無効になっている場合（つまりロング プリアンブルが有効な場合）、コントローラはすでに SpectraLink 社の NetLink 電話に対して最適化されているため、以降の手順を実行する必要はありません。

ステップ 6　[Short Preamble] チェックボックスをオフにすることによってロング プリアンブルを使用可能にします。

ステップ 7　[Save] をクリックして、コントローラの設定をアップデートします。

ステップ 8　コントローラの設定を保存するには、左側のサイドバーのメニューから [System] > [Commands] の順に選択し、[Administrative Commands] ドロップダウン リストから [Save Config To Flash] を選択してから、[Go] をクリックします。

ステップ 9　コントローラをリブートするには、[Administrative Commands] ドロップダウン リストから [Reboot] を選択して、[Go] をクリックします。

ステップ 10　次のメッセージが表示された場合、[OK] をクリックします。

```
Please save configuration by clicking "Save Config to flash". Do you want to continue
rebooting anyways?
```

コントローラがリブートします。これにはしばらく時間がかかる場合があります。その間に Prime Infrastructure はコントローラから切断されます。

（注）　コマンドライン インターフェイス セッションでコントローラのリブート プロセスを表示できます。

RF キャリブレーション モデルの作成

ビルディングの 1 フロアまたは複数フロア全体におけるクライアントおよび不正アクセス ポイントの位置の正確さを Prime Infrastructure Location で向上させる場合は、物理的に収集された RF 測定値を使用して位置アルゴリズムを微調整する RF キャリブレーション モデルを作成することができます。較正されたフロアと同じ物理レイアウトのフロアがビルディング内に複数ある場合、同じ RF キャリブレーション モデルを他のフロアに使用することで、他のフロアを較正する時間を短縮できます。

キャリブレーション モデルは、別々のフロア領域に適用できる測定済みの RF 信号特性を使用して RF オーバーレイとして使用されます。これによって Cisco Unified Wireless Network Solution インストール チームは複数フロア領域の 1 フロアをレイアウトし、RF キャリブレーション ツールを使用して新しいキャリブレーション モデルとしてそのフロアの RF 特性を測定して保存し、そのキャリブレーション モデルを同一の物理レイアウトを備えるすべての他のフロアに適用できます。

Prime Infrastructure 操作の実行

ここでは、次の内容について説明します。

Prime Infrastructure のステータスの確認

ここでは、Prime Infrastructure のステータスをチェックする方法を説明します。Prime Infrastructure のステータスをチェックするには、次の手順に従います。次の手順に従って、いつでもステータスをチェックできます。

ステップ 1　admin としてシステムにログインします。

ステップ 2　CARS コマンドライン インターフェイスを使用して、**ncs status** コマンドを入力します。

Prime Infrastructure のステータスを示すメッセージがコマンドライン インターフェイスに表示されます。

Prime Infrastructure の停止

ここでは、Prime Infrastructure を停止方法について説明します。Prime Infrastructure はいつでも停止できます。Prime Infrastructure を停止するには、次の手順に従います。

（注）　Prime Infrastructure を停止するときにユーザがログインしている場合、Prime Infrastructure セッションは機能停止します。

ステップ 1　admin としてシステムにログインします。

（注）　現在インストールされている Prime Infrastructure のバージョンを確認するには、**show application version ncs** と入力します。

ステップ 2　CARS コマンドライン インターフェイスを使用して、**ncs stop** コマンドを入力します。

Prime Infrastructure を停止していることを示すメッセージがコマンドライン インターフェイスに表示されます。

Prime Infrastructure データベースのバックアップ

ここでは、Prime Infrastructure データベースのバックアップ方法について説明します。Prime Infrastructure ユーザ インターフェイスで定期バックアップをスケジューリングすること、または手動でバックアップを始動することができます。Prime Infrastructure ユーザ インターフェイスとコマンドライン インターフェイスのどちらを使用した場合でも、次のファイルがバックアップされます。

- Oracle データベース
- マップ
- レポート ファイル
- レポートの生成に使用される精度ファイル
- USERMGT ファイル

デバイス設定はバック アップ ファイルのデバイスから取得されます。

（注）　バックアップが別のデバイスに復元される場合、マシン固有の設定（FTP 有効/無効、FTP ポート、FTP ルート ディレクトリ、TFTP 有効/無効、TFTP ポート、TFTP ルート ディレクトリ、HTTP 転送有効/無効、HTTP ポート、HTTPS ポート、レポート リポジトリ ディレクトリ、すべてのハイ アベイラビリティ設定など）はバックアップと復元機能に含められません。

ここでは、次の内容について説明します。

- 「自動バックアップのスケジュール」（P.4-120）
- 「手動バックアップの実行」（P.4-120）

自動バックアップのスケジュール

Prime Infrastructure データベースの自動バックアップをスケジューリングするには、次の手順に従います。

ステップ 1　Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Administration] > [Background Tasks] の順に選択して、[Scheduled Tasks] ページを表示します。

ステップ 3　[NCS Server Backup] タスクをクリックします。

ステップ 4　[Enabled] チェックボックスをオンにします。

ステップ 5　[Backup Repository] フィールドで、既存のバックアップ リポジトリを選択するか、[Create] をクリックして新規リポジトリを作成します。

ステップ 6　リモートの場所にバックアップする場合、[FTP Repository] チェックボックスをオンにします。リモート マシンの FTP ロケーション、ユーザ名、およびパスワードを入力する必要があります。

ステップ 7　[Interval (Days)] テキスト ボックスに、バックアップの間隔を日数で入力します。たとえば、1 = 毎日のバックアップ、2 = 1 日おきのバックアップ、7 = 毎週のバックアップなどを入力します。

範囲：1 ～ 360

デフォルト：7

ステップ 8　[Time of Day] テキスト ボックスに、バックアップの開始時間を入力します。次の形式で入力してください。*hh*:*mm* AM/PM（例：03:00 AM）

（注）　大きなデータベースのバックアップは、Prime Infrastructure サーバのパフォーマンスに影響を与えます。そのため、Prime Infrastructure サーバがアイドル状態にある時間帯（深夜など）にバックアップの実行をスケジューリングすることを推奨します。

ステップ 9　[Submit] をクリックして設定値を保存します。バックアップ ファイルは .zip ファイルとして *ftp-install-dir*/ftp-server/admin/NCSBackup ディレクトリに保存されます。.zip ファイルの形式は次のとおりです。*dd-mmm-yy_hh-mm-ss*.zip。
（例：11-Nov-05_10-30-00.zip）。

手動バックアップの実行

Prime Infrastructure データベースをバック アップするには、次の手順に従います。

（注）　システムが実行されている場合は、ユーザ インターフェイスを使用してバックアップを実行することを推奨します。これを行うには、[Administration] > [Background Tasks] の順に選択し、[NCS Server Backup] タスクを選択し、[Execute Now] を選択します。

ステップ 1　admin としてシステムにログインします。

ステップ 2　コマンドライン インターフェイスを使用してバックアップを実行できます。

ステップ 3　次のコマンドを入力して、アプリケーション データをリポジトリ（ローカルまたはリモート）にバックアップします。

```
backup testbackup repository backup_repo application NCS
```

Prime Infrastructure データベースの復元方法

ここでは、Prime Infrastructure データベースの復元方法について説明します。ここでは、次の内容について説明します。

Prime Infrastructure データベースをハイ アベイラビリティ環境に復元する場合、「ハイ アベイラビリティ環境での Prime Infrastructure データベース復元」（P.4-121）を参照してください。バックアップ ファイルから Prime Infrastructure データベースを復元するには、次の手順を実行します。

ステップ 1　ローカル リポジトリのバックアップをすべて表示するには、次のコマンドを入力します。

```
show repository backup_repo
```

（注）　可能であれば、データベースを安定化するために、すべての Prime Infrastructure ユーザ インターフェイスを終了します。

ステップ 2　**ncs stop** コマンドを使用して、プラットフォームを手動でシャットダウンします。

ステップ 3　次のコマンドを入力して、アプリケーションのバックアップを復元します。

restore *backup gpg file* **repository** *repository name* **application NCS**

ステップ 4　Prime Infrastructure が実行されていて、シャットダウンする必要があることを示すメッセージが表示された場合は、[Yes] をクリックします。

Prime Infrastructure データベースの復元中を示すメッセージがコマンドライン インターフェイスに表示されます。

ハイ アベイラビリティ環境での Prime Infrastructure データベース復元

セカンダリ Prime Infrastructure サーバをプライマリ Prime Infrastructure サーバのハイ アベイラビリティ サポートとして使用するかどうかの決定を促すプロンプトが、インストール中に表示されました。ハイ アベイラビリティ環境を選択し、[Administration] > [High Availability] ページから有効化している場合、ステータスが [HA enabled] と表示されます。データベース復元前に、ステータスを [HA not configured] に変更しておく必要があります。

注意　システムが [HA enabled] モードの間は、システムをアップグレードしないでください。ステータスが [HA enabled] に設定された状態でデータベース復元を試行すると、予想外の結果が生じるおそれがあります。

[HA enabled] から [HA not configured] にステータスを変更するには、次の手順を実行します。

- [Administration] > [High Availability] を選択します。
- [HA Configuration] ページで [Remove] をクリックします。

プライマリ サーバは [HA Not Configured] モードに変更され、バックアップからデータを安全に復元できるようになりました。

データが正常に復元され、システムが動作状態になった後、プライマリ システムとセカンダリ システム間の HA を再設定します。

WCS から Prime Infrastructure へのアップグレード

WCS リリースから Prime Infrastructure 1.2 への直接アップグレードはサポートされていません。最初に NCS 1.1 リリースにアップグレードしてから、Prime Infrastructure 1.2 にアップグレードする必要があります。

Prime Infrastructure は、NCS Release 1.0.2.29、1.1.0.58、および 1.1.1.24 のデータ移行もサポートしています。NCS リリースを Prime Infrastructure 1.2 に移行する前に、以下を実行する必要があります。

- 既存のシステムに「ディスク領域管理」パッチをインストールします。
- アップグレードする前にバックアップを実行する必要があります。
- アップグレードするとき、Telnet/SSH 端末タイムアウトを避けるために、コンソール接続を使用します。
- アップグレードを実行する前にハイ アベイラビリティを削除します。

アプリケーションのアップグレードに関する詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/quickstart/guide/cpi_qsg.html#wp56675

ハイ アベイラビリティ環境で Prime Infrastructure にアップグレードする場合、「ハイ アベイラビリティ環境での Prime Infrastructure のアップグレード」（P.4-122）を参照してください。

ハイ アベイラビリティ環境での Prime Infrastructure のアップグレード

プライマリとセカンダリの Prime Infrastructure がある場合、スムーズなアップグレードのため、次の手順に従います。

ステップ 1　最初に、次の手順で HA 設定を削除しておく必要があります。

a. プライマリ Prime Infrastructure サーバにログインします。

b. [Administration] > [High Availability] の順に選択し、左側のサイドバーのメニューから [HA Configuration] を選択します。

c. [Remove] をクリックして HA 設定を削除します。

（注）　削除完了まで数分かかる場合があります。

ステップ 2　先にセカンダリ Prime Infrastructure 設定を次の手順でアップグレードしておく必要があります。

a. セカンダリ Prime Infrastructure をシャットダウンします。詳細については、「Prime Infrastructure の停止」（P.4-119）を参照してください。

（注）　グレースフル シャットダウンのための **ncs stop** を使用できます。

b. セカンダリ Prime Infrastructure のアップグレードを実行します。

c. セカンダリ Prime Infrastructure を起動します。

ステップ 3　プライマリ Prime Infrastructure をアップグレードします。

a. プライマリ Prime Infrastructure をシャット ダウンします。詳細については、「Prime Infrastructure の停止」（P.4-119）を参照してください。

b. プライマリ Prime Infrastructure のアップグレードを実行します。

c. プライマリ Prime Infrastructure を起動します。

ステップ 4　プライマリ Prime Infrastructure で HA を再度有効にします。

a. プライマリ Prime Infrastructure サーバにログインします。

b. [Administration] > [High Availability] と選択し、左側のサイドバーのメニューから [HA Configuration] を選択します。

c. HA 設定の内容を入力し、[Save] をクリックしてハイ アベイラビリティを有効にします。

ネットワークのアップグレード

ネットワークのアップグレードには、データベース同士が同期化を保てるよう、推奨手順に従ってください。たとえば、Prime Infrastructure は現在のバージョンのままでアップグレードせずに、ネットワークのコントローラ部分を新しいリリースにアップグレードすることはできません。サポートされているアップグレード順序は、Prime Infrastructure、コントローラ、その他増設デバイスの順です。

データベースの再初期化

同期に関する問題、またはある種の破損により、データベースをリセットする必要がある場合は、**ncs db reinitdb** と入力してデータベースを再初期化します。

Prime Infrastructure パスワードの回復

Prime Infrastructure アプリケーションのルート ユーザまたは FTP のユーザ パスワードは変更可能です。パスワードを回復して Prime Infrastructure に再びアクセスできるようにするには、次の手順に従います。

（注） Linux を使用している場合、コマンドを実行するには admin ユーザとしてログインする必要があります。

ステップ 1　admin ユーザとして Prime Infrastructure コマンドライン インターフェイスにログインします。

ステップ 2　次のコマンドを入力します。

ncs password root password *password*

ここで、*password* は root ユーザのログイン パスワードです。80 文字までのパスワードを入力できます。

コマンド使用例：

```
ncs-appliance/admin# ncs password root password <newpassword>
CompilerOracle: exclude org/snmp4j/Snmp.send
Loading USER - root
Validating new password..
Resetting password ..
Resetting password COMPLETED.
EXECUTION STATUS : Success
ncs-appliance/admin#
```

これで、新しい root パスワードで Prime Infrastructure の Web インターフェイスにログインできるようになりました。

ディスクのクリーンアップの実行

Prime Infrastructure のディスク領域が不足していると、アラームがシステムで発生します。また、次のエラーがポップアップ ダイアログボックスに表示されます。

```
The system is running low on diskspace, please refer to online help to perform
disk cleanup.
```

この問題を解決するには、次の CLI コマンドを使用します。

ncs cleanup

このコマンドを使用すると、ディスク領域を解放し、再利用できます。

詳細については、「ディスクのクリーンアップの実行」（P.A-10）を参照してください。

CHAPTER 5

デバイスのモニタリング

モニタリングについて

この章では、Cisco Prime Infrastructure を使用して Cisco WLAN ソリューションのデバイス設定をモニタする方法について説明します。この章の内容は、次のとおりです。

コントローラのモニタリング

コントローラ リストのページにアクセスするには、[Monitor] > [Controllers] を選択します。コントローラの詳細を表示するには、その IP アドレスをクリックします。

ここでは、次の内容について説明します。

- 「コントローラのセキュリティのモニタリング」（P.5-14）
- 「コントローラ モビリティのモニタリング」（P.5-21）
- 「コントローラの 802.11a/n のモニタリング」（P.5-23）
- 「コントローラの 802.11b/g/n のモニタリング」（P.5-27）
- 「コントローラの IPv6 のモニタリング」（P.5-30）
- 「mDNS サービス プロバイダー情報のモニタリング」（P.5-31）

コントローラのリストの表示

[Monitor] > [Controllers] を選択するか、コントローラ検索を実行して、コントローラ リスト ページにアクセスします。

（注）　高度な検索の実行の詳細については、「Advanced Search」（P.2-55）を参照してください。

このページのデータ エリアには、次の列を含む表が表示されます。

表 5-1　　コントローラ リストの詳細

フィールド	説明
IP Address	コントローラ管理インターフェイスのローカル ネットワーク IP アドレス。リスト中の IP アドレスをクリックすると、コントローラの詳細が表示されます。
Controller Name	コントローラの名前。
Location	地理的位置（キャンパスやビルディングなど）。
Mobility Group Name	コントローラ モビリティ グループまたは WPS グループの名前。
Reachability Status	到達可能または到達不能。タイトルをクリックすると、昇順および降順に並べ替えられます。

タイトルをクリックすると、昇順および降順に並べ替えられます。テーブルで列の追加、削除、または並べ替えを行うには、[Edit View] リンクをクリックして、[Edit View] ページに移動します。

コントローラ リスト表示の設定

[Edit View] ページでは、[Controllers] テーブルの列を追加、削除、または並べ替えができます。

[Controllers] テーブルで使用可能な列を編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Controllers] の順に選択します。

ステップ 2　[Edit View] リンクをクリックします。

ステップ 3　コントローラ テーブルに列を追加するには、左側のリストで、追加する列見出しをクリックして強調表示します。[Show] をクリックして、見出しを右側のリストに移動します。右側のリストにあるすべての項目が [Controllers] テーブルに表示されます。

ステップ 4　[Controllers] テーブルから列を削除するには、右側のリストで、リストの見出しをクリックして強調表示します。[Hide] をクリックして、見出しを左側のリストに移動します。左側のリストにある項目は [Controllers] テーブルに表示されません。

ステップ 5　ボタンを使用して、テーブル内での情報の並び順を指定します。目的のリストの見出しを強調表示し、[Up] または [Down] をクリックして、現在のリスト内で上下に移動します。

ステップ 6　デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7　[Submit] をクリックして、変更内容を確定します。

システム パラメータのモニタリング

この項では、コントローラのシステム パラメータのモニタリングについて詳しく説明します。内容は次のとおりです。

Monitoring System Summary

このページには、コントローラのパラメータの要約が、コントローラのステータスを示すグラフィックとともに表示されます。コントローラの前面のグラフィックは、前面パネルのポートを示しています（ポートの情報を表示するには、ポートをクリックし、[Monitor Controllers] > [*IPaddr*] > [Ports] > [General] の順に選択します）。コントローラに関するアラーム、イベント、アクセス ポイントの詳細へのリンクが表示されます。

このページには次のようにしてアクセスできます。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックします。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックします。
- [Configure] > [Access Points] の順に選択し、[AP Name] でリスト項目を選択し、[Registered Controller] をクリックします。

ページ タイトルの [Controllers] をクリックし、すべてのコントローラ リストを表示します。「コントローラのリストの表示」（P.5-2）を参照してください。

表 5-2 に、[Monitoring System Summary] ページのフィールドの一覧を示します。

表 5-2　[Monitoring System Summary] ページのフィールド

フィールド	説明
General	
IP Address	コントローラ管理インターフェイスのローカル ネットワーク IP アドレス。
Name	ユーザ定義のコントローラ名。
Device Type	コントローラの種類。
UP Time	最後のリブートからの経過時間（日数、時間、および分単位）。
System Time	コントローラによって使用された時間。
Internal Temperature	コントローラの温度。

表 5-2　[Monitoring System Summary] ページのフィールド （続き）

フィールド	説明
Location	コントローラのユーザ定義された物理的な位置。
Contact	コントローラの担当者または所有者。
Total Client Count	現在コントローラにアソシエートされているクライアントの総数。
Current CAPWAP Transport Mode	Control And Provisioning of Wireless Access Points（CAPWAP）プロトコルのトランスポート モード。コントローラとアクセス ポイント間の通信です。[Layer 2] または [Layer 3] を選択します。
Power Supply One	電源が使用でき動作しているかどうか。これは 4400 シリーズ コントローラ専用です。
Power Supply Two	電源が使用でき動作しているかどうか。これは 4400 シリーズ コントローラ専用です。
Inventory	
Software Version	現在コントローラで実行されているコードのオペレーティング システムの release.version.dot.maintenance 番号。
Emergency Image Version	コントローラのイメージ バージョン。
Description	インベントリ項目の説明
Model No	Vital Product Data で定義されたマシン モデル。
Serial No	このコントローラの一意のシリアル番号。
Burned-in MAC Address	このコントローラのバーンドイン MAC アドレス。
Number of APs Supported	コントローラでサポートされているアクセス ポイントの最大数。
Gig Ethernet/Fiber Card	オプションの 1000BASE-T/1000BASE-SX GigE カードの有無を示します。
Crypto Card One	IPsec セキュリティを有効にして拡張処理能力を提供する、拡張セキュリティ モジュールの有無を示します。 **（注）** デフォルトでは、拡張セキュリティ モジュールはコントローラに装着されていません。 Cisco Wireless LAN Controller に装着できる Crypto カードの最大数。 – Cisco 2000 シリーズ : なし – Cisco 4100 シリーズ : 1 – Cisco 4400 シリーズ : 2
Crypto Card Two	2 番めの拡張セキュリティ モジュールの有無を示します。
GIGE Port(s) Status	Up または Down。ポートのステータスを確認するにはクリックします。
Unique Device Identifier (UDI)	
Name	製品の種類。コントローラの場合は Chassis、アクセス ポイントの場合は Cisco AP。
Description	アクセス ポイントの数など、コントローラの説明。
Product ID	注文可能な製品 ID

表 5-2　[Monitoring System Summary] ページのフィールド （続き）

フィールド	説明
Version ID	製品 ID のバージョン
Serial No	一意の製品シリアル番号
Utilization	
CPU Utilization	指定した期間の最大、平均、および最小 CPU 使用率のグラフが表示されます。
Memory Utilization	指定した期間の最大、平均、および最小メモリ使用率のグラフが表示されます。

スパニングツリー プロトコルのモニタリング

スパニングツリー プロトコル（STP）はリンク管理プロトコルの 1 つです。Cisco WLAN ソリューションでは、メディア アクセス コントロール ブリッジ用に IEEE 802.1D 標準が実装されています。

スパニングツリー アルゴリズムは、ステーション間の複数のアクティブ パスによって作成される、ネットワーク内の無用なループを避けるとともに、冗長性を備えています。STP では、任意の 2 台のネットワーク デバイス間で同時に 1 つのアクティブなパスのみが存在できますが（これによりループが防止されます）、初期リンクが障害になった場合のバックアップとして冗長リンクが確立されます。

このページには次のようにしてアクセスできます。

- [Monitor] > [Controllers] の順に選択し、IP アドレスを選択し、左側のサイドバー メニューで [System] > [Spanning Tree Protocol] の順に選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [System] > [Spanning Tree Protocol] の順に選択します。

（注）　スパニングツリー プロトコルをサポートしていないコントローラは、WISM、2500、5500、7500、および SMWLC です。

表 5-3 に、[Spanning Tree Protocol] ページのフィールドの一覧を示します。

表 5-3　[Spanning Tree Protocol] ページのフィールド

フィールド	説明
General	
Spanning Tree Specification	実行しているスパニングツリー プロトコルのバージョン。IEEE 802.1D の実装は「IEEE 802.1D」を返します。現在のバージョンと互換性がない、将来のバージョンの IEEE スパニングツリー プロトコルがリリースされた場合に、新しい値が定義されます。
Spanning Tree Algorithm	このコントローラがスパニングツリー プロトコルに参加するかどうかを指定します。ドロップダウン リストで対応する行を選択することで有効または無効にできます。工場出荷時のデフォルトは無効です。

表 5-3　[Spanning Tree Protocol] ページのフィールド （続き）

フィールド	説明
Priority	ブリッジ ID の書き込み可能な部分の値、つまり、ブリッジ ID の最初の 2 つのオクテット（8 オクテット長）です。ブリッジ ID の残りの（後半の）6 オクテットは、ブリッジの MAC アドレスの値によって設定されます。この値には 0 ～ 65535 の数値を指定できます。工場出荷時のデフォルトは 32768 です。
STP Statistics	
Topology Change Count	管理エンティティが最後にリセット、または初期化されてから、このブリッジによって検知されたトポロジに対する変更の総数。
Time Since Topology Changed	ブリッジによりトポロジの変更が検知されてから経過した時間（単位は日、時、分、秒）。
Designated Root	このノードで実行されているスパニングツリー プロトコルによって決定される、スパニングツリーのルートのブリッジ ID。この値は、このノードを起点とするコンフィギュレーション BPDU のすべての Root Identifier パラメータとして使用されます。
Root Cost	このブリッジからルートへのパスのコスト。
Root Port	このブリッジからルート ブリッジへの最も低いコスト パスを提供するポートのポート番号。
Maximum Age (seconds)	このブリッジがルートとして機能する場合、すべてのブリッジが MaxAge に使用する値。 **（注）** 802.1D-1990 によって、このパラメータの範囲は STP ブリッジのハロー タイムの値に関連することが規定されています。このタイマーの粒度は、802.1D- 1990 によって 1 秒に規定されています。有効な値は 6 ～ 40 秒です。工場出荷時のデフォルトは 20 です。
Hello Time (seconds)	このブリッジがルートとして機能する場合、すべてのブリッジが HelloTime に使用する値です。このタイマーの粒度は、802.1D-1990 によって 1 秒に規定されています。有効な値は 1 ～ 10 秒です。工場出荷時のデフォルトは 2 です。
Forward Delay (seconds)	このブリッジがルートとして機能する場合、すべてのブリッジが ForwardDelay に使用する値です。802.1D-1990 によって、このパラメータの範囲は STP ブリッジの最大経過時間の値に関連することが規定されています。このタイマーの粒度は、802.1D- 1990 によって 1 秒に指定されています。整数秒でない値を設定しようとした場合、エージェントによって badValue エラーが返されることがあります。有効な値は 4 ～ 30 秒です。工場出荷時のデフォルトは 15 です。
Hold Time seconds	特定の LAN ポートを通じたコンフィギュレーション BPDU の送信の間の最小経過時間。Hold Time 期間内に、多くても 1 個のコンフィギュレーション BPDU を送信します。

CLI セッションのモニタリング

コントローラの [CLI Sessions] ページには、次の方法でアクセスできます。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューで [System] > [CLI Sessions] の順に選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [System] > [CLI Sessions] の順に選択します。

表 5-4 に、[CLI Sessions] ページのフィールドの一覧を示します。

表 5-4　[CLI Sessions] ページのフィールド

フィールド	説明
Session Index	セッション ID。
Username	ログイン ユーザ名。
Connection Type	Telnet またはシリアル セッション。
Connection From	クライアント コンピュータ システムの IP アドレス。
Session Time	経過したアクティブ セッション時間。
Idle Time	経過した非アクティブ セッション時間。

DHCP 統計情報のモニタリング

Prime Infrastructure では、バージョン 5.0.6.0 以降のコントローラについて DHCP サーバ統計情報が提供されます。この統計情報には、送受信されたパケットに関する情報、DHCP サーバ応答情報、最新要求のタイムスタンプの情報が含まれます。

このページにアクセスするには、[Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューで [System] > [DHCP Statistics] の順に選択します。

表 5-5 に、[DHCP Statistics] ページのフィールドの一覧を示します。

表 5-5　[DHCP Statistics] ページのフィールド

フィールド	説明
Server IP	サーバの IP アドレスが示されます。
Is Proxy	このサーバがプロキシかどうかが示されます。
Discover Packets Sent	使用可能なサーバの場所を特定するために送信されたパケット数の合計が示されます。
Request Packets Sent	サーバのクライアントの要求パラメータから送信されたパケット数、またはアドレスの正当性を確認するために送信されたパケット数の合計が示されます。
Decline Packets	ネットワーク アドレスがすでに使用中であることを示すパケットの数が示されます。
Inform Packets	クライアントにはすでに外部でネットワーク アドレスが設定されており、そのクライアントから DHCP サーバへのローカル設定パラメータ要求の数を示します。
Release Packets	ネットワーク アドレスをリリースし、残りのリースをキャンセルするパケット数が示されます。
Reply Packets	応答パケット数が示されます。

表 5-5　[DHCP Statistics] ページのフィールド （続き）

フィールド	説明
Offer Packets	検出パケットに応答し、設定パラメータを提示するパケットの数が示されます。
Ack Packets	正常に送信されたことを知らせるパケットの数が示されます。
Nak Packets	送信でエラーが発生したことを知らせるパケット数が示されます。
Tx Failures	発生した転送エラーの数が示されます。
Last Response Received	最後に受け取った応答のタイムスタンプ。
Last Request Sent	最後に送信した要求のタイムスタンプ。

WLAN のモニタリング

[Monitor] > [Controllers] の順に選択し、コントローラの IP アドレスをクリックし、左側のサイドバーメニューから [WLANs] を選択します。このページでは、このコントローラで設定した Wireless Local Access Network（WLAN）の要約が表示されます。

表 5-6 に [WLAN Details] ページのフィールドの一覧を示します。

表 5-6　[WLAN] ページのフィールド

フィールド	説明
WLAN ID	WLAN の識別番号。
Profile Name	最初に WLAN を作成するときに指定したユーザ定義プロファイル名。プロファイル名は WLAN 名です。
SSID	ユーザ定義の SSID 名。
Security Policies	WLAN で有効になっているセキュリティ ポリシー。
No of Mobility Anchors	モビリティ アンカーは、WLAN のアンカー コントローラとして指定されるモビリティ グループのサブセットです。
Admin Status	WLAN のステータスは有効または無効のいずれかです。
No.of Clients	この WLAN に現在アソシエートされているクライアントの数。

ポートのモニタリング

この項では、コントローラのポート パラメータのモニタリングについて詳しく説明します。内容は次のとおりです。

- 「一般的なポートのモニタリング」（P.5-9）
- 「CDP インターフェイス ネイバーのモニタリング」（P.5-13）

一般的なポートのモニタリング

[Ports] > [General] ページでは、選択したコントローラの物理ポートに関する情報が提供されます。ポート番号をクリックすると、そのポートの詳細が表示されます。詳細については、「ポートの詳細」（P.5-10）を参照してください。

表 5-7 に [General] ページのフィールドの一覧を示します。

表 5-7　[General] ページのフィールド

フィールド	説明
Port	ポートの詳細を表示するには、ポート番号をクリックします。詳細については、「ポートの詳細」（P.5-10）を参照してください。
Physical Mode	すべてのポートの物理モードが表示されます。次の選択肢があります。 – 100 Mbps Full Duplex – 100 Mbps Half Duplex – 10 Mbps Full Duplex – 10 Mbps Half Duplex
Admin Status	ポートの状態が Enable または Disable で表示されます。
STP State	ポートの STP の状態が Forwarding または Disabled で表示されます。
Physical Status	実際のポートの物理インターフェイスが、次のいずれかで表示されます。 – Auto Negotiate – Half Duplex 10 Mbps – Full Duplex 10 Mbps – Half Duplex 100 Mbps – Full Duplex 100 Mbps – Full Duplex 1 Gbps
Link Status	赤（ダウン/障害）、黄（アラーム）、緑（アップ/正常）。

[Monitor] > [Ports] > [General] ページを表示するには、次のいずれかの手順を実行します。

- [Configure] > [Controllers] の順に選択し、該当する IP アドレスをクリックします。左側のサイドバー メニューから、[Ports] で [General] を選択します。
- [Monitor] > [Controllers] の順に選択し、該当するものをクリックし、ポートをクリックしてこのページにアクセスします。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、ポートをクリックしてこのページにアクセスします。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、ポートをクリックしてこのページにアクセスします。

ポートの詳細

（注）　[Alarms] をクリックして [Monitor Alarms] ページを表示します。詳細については、「アラームのモニタリング」（P.5-127）を参照してください。
[Events] をクリックして [Monitor Events] ページを開きます。詳細については、「イベントのモニタリング」（P.5-143）を参照してください。

表 5-8 に、[Port Detail] ページのフィールドの一覧を示します。

表 5-8　[Port Details] ページのフィールド

フィールド	説明
Interface	
Operational Status	コントローラの動作ステータスが表示されます。UP または DOWN のいずれかになります。
Unknown Protocol Packets	このサーバからこのポート上で受信した不明なタイプのパケットの数。
Traffic (Received and Transmitted)	
Total Bytes	受信したパケットの総数。
Packets	長さが示されたオクテット範囲（フレーミング ビットは除くが、FCS オクテットは含む）の受信パケットの総数（不良パケットを含む）。 範囲には次のものがあります。 – 64 Octets – 65-127 Octets – 128-255 Octets – 256-511 Octets – 512-1023 Octets – 1024-1518 Octets
Packets (Received and Transmitted)	
Total	受信または送信されたパケットの総数。
Unicast Packets	上位レイヤのプロトコルに配信または送信されたサブネットワーク ユニキャスト パケットの数。
Broadcast Packets	ブロードキャスト アドレス宛の受信または送信されたパケットの総数。
Packets Discarded	[Packets Discarded (Received/Transmitted)]：エラーが検出されなかったにもかかわらず、上位レイヤ プロトコルに配信されないようにするため、廃棄することが選択された受信または送信パケットの数。パケットを廃棄する理由の 1 つは、バッファ スペースを解放することです。
Errors in Packets	受信パケットのうちエラーがあるパケットの総数。
Received packets with MAC errors	

表 5-8　[Port Details] ページのフィールド （続き）

フィールド	説明
Jabbers	1518 オクテットより長く（フレーミング ビットは除くが、FCS オクテットは含む）、オクテット数が整数でフレーム チェック シーケンス（FCS）が不正であるか（FCS エラー）、オクテット数が整数でなく FCS が不正な（アライメント エラー）、受信パケット数の合計。 （注）　ジャバーのこの定義は、IEEE-802.3 のセクション 8.2.1.5（10Base-5）およびセクション 10.3.1.4（10Base-2）の定義と異なります。これらのドキュメントでは、ジャバーが、パケットが 20 ms を超える状況と定義されています。ジャバーを検出するための許可される範囲は、20 ～ 150 ms です。
Fragments/Undersize	長さが 64 オクテット（フレーミング ビットは除外するが、FCS オクテットは含む）未満の受信済みパケットの総数。
Alignment Errors	長さが 64 ～ 1518 オクテット（フレーミング ビットは除くが、FCS オクテットは含む）であるが、オクテット数が整数でなくフレーム チェック シーケンス（FCS）が不正な受信パケットの総数。
FCS Errors	長さが 64 ～ 1518 オクテット（フレーミング ビットは除くが、FCS オクテットは含む）であるが、オクテット数が整数でありフレーム チェック シーケンス（FCS）が不正な受信パケットの総数。
Transmit discards	
Single Collision Frames	送信が 1 つのコリジョンだけによって妨げられた特定のインターフェイスで正常に送信されたフレームの数。
Multiple Collision Frames	送信が 2 つ以上のコリジョンによって妨げられた特定のインターフェイスで正常に送信されたフレームの数。
Deferred Transmissions	遅延送信によって特定のインターフェイスでの送信に失敗したフレームの数。
Late Collisions	レイト コリジョンが生じたことによって、特定のインターフェイス上で送信が失敗したフレームのカウントです。
Excessive Collisions	過度のコリジョンが生じたことによって、特定のインターフェイス上で送信が失敗したフレームの数。
Ether Stats	

表 5-8　[Port Details] ページのフィールド （続き）

フィールド	説明
CRC Align Errors	チェックサム（FCS）アラインメント エラーがある着信パケットの数。これは、長さが整数オクテットでなく、FCS チェックに合格しない、特定のインターフェイスで受信したフレームの数を表します。複数のエラー条件がある受信フレームは、IEEE 802.3 のレイヤ管理の規則によれば、LLC に提示されたエラー ステータスのみに従ってカウントされます。
Undersize Packets	長さが 64 オクテット（フレーミング ビットは除外するが、FCS オクテットは含む）未満の受信済みパケットの総数。
Oversize Packets	許可される最大フレーム サイズを超えたフレームの総数。このカウンタの最大インクリメント速度は、10 Mbps で 1 秒あたり 815 回です。
Ether Stats Collisions	コリジョン エラーがあるパケットの数。
SQE Test Errors	送信中の信号品質エラー テスト エラー（つまりハートビート）。これは、トランシーバの重要なコリジョン検出電子部品をテストし、コンピュータのイーサネット インターフェイスに、コリジョン検出回路と信号パスが正常に動作していることを知らせます。エラーは、特定のインターフェイスについて、SQE TEST ERROR メッセージが PLS サブレイヤによって生成された回数を示します。SQE TEST ERROR メッセージは、ANSI/IEEE 802.3-1985 のセクション 7.2.2.2.4 で定義され、このメッセージの生成は同じ文書のセクション 7.2.4.6 で定義されています。
Internal MAC Receive Errors	内部 MAC サブレイヤの受信エラーのために特定のインターフェイスでの受信が失敗したフレームの数。フレームは、FrameTooLong プロパティ、AlignmentErrors プロパティ、または FCSErrors プロパティの対応するインスタンスによってカウントされない場合にのみ、このオブジェクトのインスタンスによってカウントされます。このオブジェクトのインスタンスによって表されるカウントの厳密な意味は、実装固有です。特に、このオブジェクトのインスタンスは、特定のインターフェイス上の、他のオブジェクトではカウントされない受信エラーのカウントを表す場合があります。

表 5-8　[Port Details] ページのフィールド （続き）

フィールド	説明
Internal MAC Transmit Errors	内部 MAC サブレイヤの送信エラーのために特定のインターフェイスで送信が失敗したフレームの数。フレームは、LateCollisions プロパティ、ExcessiveCollisions プロパティ、または CarrierSenseErrors プロパティの対応するインスタンスによってカウントされない場合にのみ、このオブジェクトのインスタンスによってカウントされます。このオブジェクトのインスタンスによって表されるカウントの厳密な意味は、実装固有です。特に、このオブジェクトのインスタンスは、特定のインターフェイス上の、他のオブジェクトではカウントされない送信エラーのカウントを表す場合があります。
Carrier Sense Errors	キャリア センスはキャリアの存在を検出します。特定のインターフェイスでフレームを送信しようとしたときに、キャリア センス状態が失われたか、一度もアサートされなかった回数です。
Too Long Frames	特定のインターフェイスで受信され、最大許可フレーム サイズを超えたフレームのカウント。このオブジェクトのインスタンスによって表されるカウントは、FrameTooLong ステータスが MAC レイヤから LLC（または他の MAC ユーザ）に返された場合にインクリメントされます。複数のエラー条件がある受信フレームは、IEEE 802.3 のレイヤ管理の規則によれば、LLC に提示されたエラー ステータスのみに従ってカウントされます。

CDP インターフェイス ネイバーのモニタリング

[Monitor CDP Interface Neighbors] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[CDP Interface Neighbors] を選択します（[Port] 見出しの下）。

ステップ 4　表 5-9 に、[CDP Interface Neighbors] ページのフィールドの一覧を示します。

表 5-9　[CDP Interface Neighbors] ページのフィールド

フィールド	説明
Local Interface	ローカル ポート情報。
Neighbor Name	各 CDP ネイバーの名前。
Neighbor Address	各 CDP ネイバーの IP アドレス。
Neighbor Port	CDP パケットを送信するために各 CDP ネイバーが使用するポート。
Capability	各 CDP ネイバーの機能。
Platform	各 CDP ネイバー デバイスのハードウェア プラットフォーム。
Duplex	全二重なのか半二重なのかを示します。
Software Version	CDP ネイバーで実行されているソフトウェア。

コントローラのセキュリティのモニタリング

この項では、コントローラのセキュリティのモニタリングについて詳しく説明します。内容は次のとおりです。

- 「RADIUS 認証のモニタリング」（P.5-14）
- 「RADIUS アカウンティングのモニタリング」（P.5-16）
- 「管理フレーム保護のモニタリング」（P.5-18）
- 「不正 AP ルールのモニタリング」（P.5-19）
- 「ゲスト ユーザのモニタリング」（P.5-20）

RADIUS 認証のモニタリング

[RADIUS Authentication] ページには RADIUS 認証サーバの情報が表示され、RADIUS 認証サーバを追加または削除できます。

このページにアクセスするには、次のいずれかの手順を実行します。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューで [Security] > [Radius Authentication] の順に選択します。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Security] > [Radius Authentication] の順に選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Security] > [Radius Authentication] の順に選択します。

表 5-10 に、[RADIUS Authentication] ページのフィールドの一覧を示します。

表 5-10　[RADIUS Authentictaion] ページのフィールド

フィールド	説明
RADIUS Authentication Servers	
Server Index	RADIUS サーバのプライオリティ番号にアクセスします。最大 4 台のサーバを設定でき、サーバのコントローラによるポーリングはインデックス 1 で始まり、次にインデックス 2 というようになります。インデックス番号は、RADIUS サーバをコントローラに追加した順番で決まります。
IP Address	RADIUS サーバの IP アドレス。
ping	アイコンをクリックすると、コントローラから RADIUS サーバに ping が実行され、リンクが確認されます。
Port	インターフェイス プロトコルのコントローラのポート番号。
Admin Status	サーバが有効であるか無効であるかを示します。
Authentication Server Statistics	
Msg Round Trip Time	この RADIUS 認証サーバからの、最新の Access-Reply/Access-Challenge と、それに一致した Access-Request の間の間隔（ミリ秒単位）。
First Requests	このサーバに送信された RADIUS Access-Request パケットの数。再送信は含みません。
Retry Requests	この RADIUS 認証サーバに再送信された RADIUS Authentication-Request パケットの数。
Accept Responses	このサーバから受信した RADIUS Access-Accept パケットの数（有効または無効）。
Reject Responses	このサーバから受信した RADIUS Access-Reject パケットの数（有効または無効）。
Challenge Responses	このサーバから受信した RADIUS Access-Challenge パケットの数（有効または無効）。
Malformed Msgs	このサーバから受信した不正な形式の RADIUS Access-Response パケットの数。不正な形式のパケットには、長さが不正なパケットが含まれます。オーセンティケータまたはシグニチャ属性の不正や不明なタイプは、不正な形式のアクセス応答に含まれません。
Pending Requests	このサーバ宛の、まだタイムアウトしていないか、応答を受信していない RADIUS Access-Request パケットの数。この変数は、Access-Request を送信したときに増加し、Access-Accept、Access-Reject、または Access-Challenge の受信か、タイムアウトまたは再送信により減少します。

表 5-10　[RADIUS Authentictaion] ページのフィールド （続き）

フィールド	説明
Bad Authentication Msgs	不正なオーセンティケータまたはシグニチャ属性が含まれた、このサーバから受信した RADIUS Access-Response パケットの数。
Timeouts Requests	このサーバに対する認証タイムアウトの数。タイムアウト後、クライアントは同じサーバに再試行するか、異なるサーバに送信するか、あきらめる可能性があります。同じサーバへの再試行は、再送信およびタイムアウトとしてカウントされます。異なるサーバへの送信は、要求およびタイムアウトとしてカウントされます。
Unknown Type Msgs	このサーバから認証ポート上で受信した不明なタイプの RADIUS パケットの数。
Other Drops	このサーバから認証ポート上で受信し、他の何らかの理由でドロップされた RADIUS パケットの数。

RADIUS アカウンティングのモニタリング

このページには次のいずれかの方法でアクセスできます。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューで [Security] > [Radius Accounting] の順に選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Security] > [Radius Accounting] の順に選択します。
- [Monitor] > [Maps] の順に選択し、[Name] 欄で項目を選択し、アクセス ポイント アイコン、[Controller] の順にクリックし、左側のサイドバー メニューで [Security] > [Radius Accounting] の順に選択します。
- [Configure] > [Access Points] の順に選択し、[AP Name] でリスト項目を選択し、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Security] > [Radius Accounting] の順に選択します。

表 5-11 に、[RADIUS Accounting] ページのフィールドの一覧を示します。

表 5-11　[RADIUS Accounting] ページのフィールド

フィールド	説明
RADIUS Accounting Server	
Server Index	RADIUS サーバのプライオリティ番号にアクセスします。最大 4 台のサーバを設定でき、サーバのコントローラによるポーリングはインデックス 1 で始まり、次にインデックス 2 というようになります。インデックス番号は、RADIUS サーバをコントローラに追加した順番で決まります。
IP Address	RADIUS サーバの IP アドレス。
ping	アイコンをクリックすると、コントローラから RADIUS サーバに ping が実行され、リンクが確認されます。

表 5-11　[RADIUS Accounting] ページのフィールド （続き）

フィールド	説明
Port	RADIUS サーバのポート。
Admin Status	サーバが有効であるか無効であるかを示します。
Accounting Statistics	
Msg Round Trip Time	この RADIUS アカウンティングサーバからの、最新の Accounting-Response とそれに一致した Accounting-Request の間の時間（ミリ秒単位）。
First Requests	送信した RADIUS Accounting-Request パケットの数。再送信は含みません。
Retry Requests	この RADIUS アカウンティング サーバに再送信された RADIUS Accounting-Request パケットの数。再送信には、Identifier と Acct-Delay が更新された再試行と、それらが同じ再試行が含まれます。
Accounting Responses	このサーバからアカウンティング ポートで受信した RADIUS パケットの数。
Malformed Msgs	このサーバから受信した不正な形式の RADIUS Accounting-Response パケットの数。不正な形式のパケットには、長さが不正なパケットが含まれます。オーセンティケータの不正や不明なタイプは、不正な形式のアカウンティング応答に含まれません。
Bad Authentication Msgs	このサーバから受信した、無効なオーセンティケータが含まれる RADIUS Accounting-Response パケットの数。
Pending Requests	このサーバに送信した、まだタイムアウトしていないか、応答を受信していない RADIUS Accounting-Request パケットの数。この変数は、Accounting-Request を送信したときに増加し、Accounting-Response の受信か、タイムアウトまたは再送信により減少します。
Timeouts Requests	このサーバに対するアカウンティング タイムアウトの数。タイムアウト後、クライアントは同じサーバに再試行するか、異なるサーバに送信するか、あきらめる可能性があります。同じサーバへの再試行は、再送信およびタイムアウトとしてカウントされます。異なるサーバへの送信は、Accounting-Request およびタイムアウトとしてカウントされます。
Unknown Type Msgs	このサーバからアカウンティング ポート上で受信した不明なタイプの RADIUS パケットの数。
Other Drops	このサーバからアカウンティング ポート上で受信し、他の何らかの理由でドロップされた RADIUS パケットの数。

管理フレーム保護のモニタリング

このページには、管理フレーム保護（MFP）の要約情報が表示されます。MFP は、802.11 管理フレームの認証機能を備えています。管理フレームを保護することにより敵対者を検知できるようになり、DoS 攻撃や、プローブのフラッディング、不正 AP の設置を検知でき、QoS および無線測定フレームへの攻撃を防止しネットワーク パフォーマンスへの影響を抑えます。

コントローラの 1 つ以上の WLAN で MFP が有効になっている場合、コントローラは各登録済みアクセス ポイントに、それらの WLAN についてアクセス ポイントが使用する各 BSSID の一意のキーを送信します。MFP が有効になっている WLAN 経由でアクセス ポイントによって送信された管理フレームは、フレーム保護情報要素（IE）で署名されます。フレームを変更しようとするとメッセージが無効になり、MFP フレームを検出するように設定されている受信側アクセス ポイントが WLAN コントローラに不一致を報告します。

このページにアクセスするには、次のいずれかの手順を実行します。

- [Monitor] > [Controllers] の順に選択します。[Controllers] > [Search Results] ページから、該当する IP アドレスをクリックし、左側のサイドバー メニューで [Security] > [Management Frame Protection] の順に選択します。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Security] > [Management Frame Protection] の順に選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Security] > [Management Frame Protection] の順に選択します。

表 5-12 に [MFP] ページのフィールドの一覧を示します。

表 5-12　[MFP] ページのフィールド

フィールド	説明
General	
Management Frame Protection	コントローラでインフラストラクチャ MFP がグローバルに有効になっているかどうかを示します。
Controller Time Source Valid	[Controller Time Source Valid] フィールドは、コントローラの時刻が（時刻を手動で入力することにより）ローカルで設定されているか、外部ソース（NTP サーバなど）を通して設定されているかを示します。時刻が外部ソースにより設定されている場合、このフィールドの値は「True」です。時刻がローカルで設定されている場合、このフィールドの値は「False」です。時刻ソースは、モビリティ グループ内の複数のコントローラのアクセス ポイント間の管理フレーム上のタイムスタンプの検証に使用されます。
WLAN Details	
WLAN ID	WLAN ID。1 ～ 17。
WLAN Name	最初に WLAN を作成するときに指定したユーザ定義プロファイル名。SSID 名とプロファイル名の両方がユーザ定義です。WLAN 名はプロファイル名と同じです。

表 5-12　[MFP] ページのフィールド （続き）

フィールド	説明
MFP Protection	管理フレーム保護は、有効または無効のいずれかです。
Status	WLAN のステータスは有効または無効のいずれかです。
AP Details	
AP Name	オペレータが定義したアクセス ポイント名。
MFP Validation	管理フレーム保護は、有効または無効のいずれかです。
Radio	802.11a または 802.11b/g。
Operation Status	動作ステータス（UP または DOWN）が表示されます。
Protection	Full（全フレーム）。
Validation	Full（全フレーム）。

不正 AP ルールのモニタリング

不正 AP ルールは、認証タイプ、一致する設定された SSID、クライアント カウント、および RSSI 値などの条件に基づいて、不正なアクセス ポイントを自動的に分類します。Prime Infrastructure では、不正アクセス ポイントの分類ルールをコントローラおよびそれぞれのアクセス ポイントに適用します。

これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントを無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

不正 AP ルールは、誤アラームを減らすためにも役立ちます。

（注）　不正クラスには以下の種類があります。
Malicious Rogue：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
Friendly Rogue：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
Unclassified Rogue：検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

[Monitor] > [Controllers] の順に選択します。[Controllers] > [Search Results] ページから、該当する IP アドレスをクリックし、左側のサイドバー メニューで [Security] > [Rogue AP Rules] の順に選択します。

[Rogue AP Rules] ページには、現在このコントローラに適用されている、すべての不正アクセス ポイント ルールの一覧が表示されます。

不正アクセス ポイント ルールの次の情報が表示されます。

- [Rogue AP Rule name]：リンクをクリックすると不正 AP ルールの詳細が表示されます。
- [Rule Type]：Malicious または Friendly。
  - [Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。

  - [Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
- [Priority]：この不正 AP ルールのプライオリティ レベルを示します。

（注）　不正 AP ルールの詳細については、「不正 AP ルール テンプレートの設定」（P.11-680）を参照してください。

Rogue AP Rules

表 5-13 に、[Rogue AP Rules] ページのフィールドの一覧を示します。

表 5-13　[Rogue AP Rule] ページのフィールド

フィールド	説明
Rule Name	ルールの名前。
Rule Type	Malicious または Friendly – [Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。 – [Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
Match Type	match any または match all 条件。
Enabled Rule Conditions	有効なすべてのルール条件を示します。次のものが含まれます。 – Open Authentication – Match Managed AP SSID – Match User Configured SSID – Minimum RSSI – Time Duration – Minimum Number Rogue Clients

（注）　不正 AP ルールの詳細については、「不正 AP ルール テンプレートの設定」（P.11-680）を参照してください。

ゲスト ユーザのモニタリング

[Monitor] > [Controllers] の順に選択します。[Controllers] > [Search Results] ページから、該当する IP アドレスをクリックし、左側のサイドバー メニューで [Security] > [Guest Users] の順に選択します。

Prime Infrastructure では、[Guest Users] ページと Prime Infrastructure のホーム ページでゲスト ユーザをモニタできます。

[Guest Users] ページには、ゲスト アクセスの配置とネットワーク使用状況の要約が表示されます。

現在ネットワークに関連付けられているゲスト ユーザの次の情報が表示されます。表 5-14 に、[Guest Users] ページのフィールドの一覧を示します。

表 5-14　[Guest Users] ページのフィールド

フィールド	説明
Guest User Name	ゲスト ユーザのログイン名を示します。
Profile	ゲスト ユーザが結びつけられているプロファイルを示します。
Lifetime	ゲスト ユーザ アカウントがアクティブな時間の長さを示します。時間の長さは、日、時間、分単位で表示されるか、Never Expires と表示されます。
Start Time	ゲスト ユーザ アカウントがアクティブ化された時刻を示します。
Remaining Lifetime	ゲスト ユーザ アカウントの残り時間を示します。
Role	指定されたユーザ ロールを示します。
First Logged in at	ユーザが最初にログインした日付と時刻を示します。
Number of logins	このゲスト ユーザの合計ログイン回数を示します。
Description	識別を目的とする、ゲスト ユーザ アカウントのユーザ定義の説明です。

コントローラ モビリティのモニタリング

モビリティ統計情報のモニタリング

[Mobility Stats] ページには、モビリティ グループ イベントの統計情報が表示されます。

このページにアクセスするには、次のいずれかの手順を実行します。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューで [Mobility] > [Mobility Stats] の順に選択します。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Mobility] > [Mobility Stats] の順に選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [Mobility] > [Mobility Stats] の順に選択します。

表 5-15 に、[Mobility Stats] ページのフィールドの一覧を示します。

表 5-15　[Mobility Stats] ページのフィールド

フィールド	説明
Global Mobility Statistics	
Rx Errors	短すぎるパケットや不正な形式などの、一般的なプロトコル パケット受信エラー。
Tx Errors	パケット送信失敗など、一般的なプロトコル パケット送信エラー。
Responses Retransmitted	モビリティ プロトコルは UDP を使用し、応答が受信されない場合には、複数回にわたって要求が再送信されます。ネットワークの遅延または処理の遅延のため、応答側が最初に要求に応答した後に、1 回以上の再試行要求を受信する場合があります。このフィールドは、応答が再送信された回数です。
Handoff Requests Received	ハンドオフ要求が受信、無視または応答された合計回数。
Handoff End Requests	ハンドオフ終了要求が受信された合計回数。これらの要求は、クライアント セッションの終了について相手に通知するために、アンカー コントローラまたは外部コントローラによって送信されます。
State Transitions Disallowed	PEM（ポリシー施行モジュール）がクライアントのステート遷移を拒否しました。通常、その結果としてハンドオフが中断されます。
Resource Unavailable	バッファなどの必要なリソースが使用できませんでした。その結果としてハンドオフが中断されます。
Mobility Responder Statistics	
Handoff Requests Ignored	無視されたハンドオフ要求またはクライアント通知の数。コントローラには、単にそのクライアントに関する知識がありません。
Ping Pong Handoff Requests Dropped	ハンドオフ期間が短すぎた（3 秒）ために拒否されたハンドオフ要求の数。
Handoff Requests Dropped	クライアントについての認識が不完全であるか、パケットの問題が原因でドロップされたハンドオフ要求の数。
Handoff Requests Denied	積極的に拒否されたハンドオフ要求の数。
Client Handoff as Local	ローカル ロール中に送信されたハンドオフ応答の数。
Client Handoff as Foreign	外部ロール中に送信されたハンドオフ応答の数。
Anchor Requests Received	受信したアンカー要求の数。
Anchor Requests Denied	拒否されたアンカー要求の数。
Anchor Requests Granted	許可されたアンカー要求の数。

表 5-15　[Mobility Stats] ページのフィールド（続き）

フィールド	説明
Anchor Transferred	クライアントが外部コントローラから現在のアンカーと同じサブネット上のコントローラに移動したために、転送されたアンカーの数。
Mobility Initiator Statistics	
Handoff Requests Sent	コントローラにアソシエートされ、モビリティ グループに通知されたクライアントの数。
Handoff Replies Received	送信された要求に応答して受信された、ハンドオフ応答の数。
Handoff as Local Received	クライアント セッション全体が転送されたハンドオフの数。
Handoff as Foreign Received	クライアント セッションが別の場所でアンカーされたハンドオフの数。
Handoff Denies Received	拒否されたハンドオフの数。
Anchor Request Sent	スリーパーティ（外部から外部）ハンドオフ用に送信されたアンカー要求の数。ハンドオフが別の外部コントローラから受信され、新しいコントローラがクライアントを移動させるようアンカーに要求しています。
Anchor Deny Received	現在のアンカーによって拒否されたアンカー要求の数。
Anchor Grant Received	現在のアンカーによって許可されたアンカー要求の数。
Anchor Transfer Received	現在のアンカーによって受信されたアンカー転送の数。

コントローラの 802.11a/n のモニタリング

この項では、802.11a/n パラメータのモニタリングについて詳しく説明します。内容は次のとおりです。

- 「802.11a/n パラメータのモニタリング」（P.5-23）
- 「802.11a/n RRM グループのモニタリング」（P.5-25）

802.11a/n パラメータのモニタリング

[802.11a/n Parameters] ページにアクセスするには、次のいずれかの方法を使用します。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューの [802.11a/n] セクションから [Parameters] を選択します。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11a/n] セクションから [Parameters] を選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11a/n] セクションから [Parameters] を選択します。

表 5-16 に、[802.11a/n Parameters] ページのフィールドの一覧を示します。

表 5-16　[802.11 a/n Parameters] ページのフィールド

フィールド	説明
MAC Operation Parameters	
RTS Threshold	これを下回った場合に RTS/CTS ハンドシェイクが実行されない、MPDU 内のオクテット数を示します。 **（注）** RTS/CTS ハンドシェイクは、すべてのフレーム交換シーケンスの開始時に、MPDU がデータまたは管理タイプで、MPDU の Address1 フィールドに個別のアドレスがあり、MPDU の長さがこのしきい値よりも長い場合に実行されます。この属性を最大 MSDU サイズよりも大きくすると、この STA によって送信されるデータまたは管理タイプ フレームの RTS/CTS ハンドシェイクが無効になります。この属性にゼロを設定すると、転送されるすべてのデータまたは管理タイプ フレームで RTS/CTS ハンドシェイクが有効になります。
Short Retry Limit	障害状態が通知される前に実行される、フレームの最大送信回数（dot11RTSThreshold 以下）。デフォルト値は 7 です。
Long Retry Limit	障害状態が通知される前に実行されるフレームの最大送信回数（dot11RTSThreshold より上）。デフォルト値は 4 です。
Max Tx MSDU Lifetime	MSDU の初回送信後、MSDU の以降の送信の試みを停止するまでの、TU 単位の経過時間。デフォルト値は 512 です。
Max Rx Lifetime	フラグメント化された MMPDU または MSDU の初回受信後、MMPDU または MSDU の以降の再構成の試みを停止するまでの、TU 単位の経過時間。デフォルト値は 512 です。
Physical Channel Fields	
TI Threshold	ビジー メディアを検出するために使用するしきい値（頻度）。CCA は、このしきい値を超える RSSI を検出するとビジー メディアを報告します。
Channel Agility Enabled	物理チャネル敏捷性機能が実装されているかどうか。
Station Configuration Fields	
Medium Occupancy Limit	ポイント コーディネータが、1 つ以上の DCF のインスタンスがメディアにアクセスするのに十分な時間制御を放棄せずに、ワイヤレス メディアの使用を制御する可能性がある最大時間を、TU 単位で示します。デフォルト値は 100 で、最大値は 1000 です。

表 5-16　[802.11 a/n Parameters] ページのフィールド （続き）

フィールド	説明
CFP Period	CFP の開始の間の DTIM 間隔の数。これは、MLME-START.request プリミティブによって変更されます。
CFP Max Duration	PCF によって生成される可能性がある、CFP の最大期間（TU 単位）。これは、MLME-START.request プリミティブによって変更されます。
CF Pollable	この属性が実装されている場合、クライアントは SIFS 時間内にデータ フレームで CF-Poll に応答できることを示します。STA が SIFS 時間内にデータ フレームで CF-Poll に応答できない場合、この属性は実装されません。
CF Poll Request	CFP がクライアントによって要求されるかどうかを示します。
DTIM Period	DTIM Count フィールドが 0 の TIM 要素を含むビーコン フレームの送信の間に経過する、ビーコン間隔の数。この値は、ビーコン フレームの DTIM Period フィールドで送信されます。

802.11a/n RRM グループのモニタリング

[RRM Grouping] ページにアクセスするには、次のいずれかの手順を実行します。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューの [802.11a/n] セクションから [Grouping] または [WPS Grouping] を選択します。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11a/n] セクションから [RRM Grouping] または [WPS Grouping] を選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11a/n] セクションから [RRM Grouping] または [WPS Grouping] を選択します。

表 5-17 に、[802.11a/n RRM Grouping] ページのフィールドの一覧を示します。

表 5-17　[802.11 a/n RRM Grouping] ページのフィールド

フィールド	説明
802.11a Grouping Control	
Grouping Mode	動的グループ化のモードは、オンとオフの 2 つです。グループ化がオフの場合、動的グループ化は実行されません。各コントローラは、アクセス ポイントの自身のパラメータのみを最適化します。グループ化をオンにすると、コントローラはグループを形成し、リーダーを選択してより適切な動的パラメータの最適化を実行します。

表 5-17　[802.11 a/n RRM Grouping] ページのフィールド（続き）

フィールド	説明
Grouping Role	次の 5 つのグループ化ロールがあります。 – [None]：このグループ化ロールは、[RF Group Mode] が [Off] に設定されている場合に表示されます。 – [Auto-Leader]：このグループ化ロールは、[RF Group Mode] が [Automatic] に設定され、自動グループ化アルゴリズムによってコントローラがリーダーとして選択されている場合に表示されます。 – [Auto-Member]：このグループ化ロールは、[RF Group Mode] が [Automatic] に設定され、自動グループ化アルゴリズムによってコントローラがメンバーとして選択されている場合に表示されます。 – [Static-Leader]：このグループ化ロールは、[RF Group Mode] が [Leader] に設定されている場合に表示されます。 – [Static-member]：このグループ化ロールは、[RF Group Mode] が [Automatic] に設定され、リーダーからの参加要求の結果、コントローラがリーダーに参加している場合に表示されます。
Group Leader IP Address	これはグループ リーダーの IP アドレスです。
Group Leader MAC Address	これは、このコントローラが属しているグループのグループ リーダーの MAC アドレスです。
Is 802.11a Group Leader	このコントローラがグループ リーダーの場合は [Yes]、コントローラがグループ リーダーでない場合は [No]。
Last Update Time (secs)	最後にグループを更新してからの経過時間（秒単位）。これは、このコントローラがグループ リーダーである場合のみ有効です。
Group Update Interval (secs)	グループ化がオンになっている場合、この間隔（秒単位）は、グループ化アルゴリズムがグループ リーダーによって実行される期間を表します。グループ化アルゴリズムは、グループの内容が変更され、自動グループ化が有効であるときも実行されます。動的グループ化は、システム管理者からの要求時に開始できます。デフォルト値は 3600 秒です。
Group Members	
Group Member Name	グループ メンバーの名前。
Group Member IP Address	グループ メンバーの IP アドレス。
Member Join Reason	メンバーの現在の状態。

コントローラの 802.11b/g/n のモニタリング

この項では、802.11b/g/n パラメータのモニタリングについて詳しく説明します。内容は次のとおりです。

802.11b/g/n パラメータのモニタリング

[802.11b/g/n Parameters] ページにアクセスするには、次のいずれかの方法を使用します。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューの [802.11b/g/n] セクションから [Parameters] を選択します。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11b/g/n] セクションから [Parameters] を選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11b/g/n] セクションから [Parameters] を選択します。

表 5-18 に、[802.11b/g Parameters] ページのフィールドの一覧を示します。

表 5-18　[802.11 b/g/n Parameters] ページのフィールド

フィールド	説明
MAC Operation Parameters	
RTS Threshold	これを下回った場合に RTS/CTS ハンドシェイクが実行されない、MPDU 内のオクテット数を示します。 **（注）** RTS/CTS ハンドシェイクは、すべてのフレーム交換シーケンスの開始時に、MPDU がデータまたは管理タイプで、MPDU の Address1 フィールドに個別のアドレスがあり、MPDU の長さがこのしきい値よりも長い場合に実行されます。この属性を最大 MSDU サイズよりも大きくすると、この STA によって送信されるデータまたは管理タイプ フレームの RTS/CTS ハンドシェイクが無効になります。この属性にゼロを設定すると、転送されるすべてのデータまたは管理タイプ フレームで RTS/CTS ハンドシェイクが有効になります。
Short Retry Limit	障害状態が通知される前に実行される、フレームの最大送信回数（dot11RTSThreshold 以下）。デフォルト値は 7 です。
Long Retry Limit	障害状態が通知される前に実行されるフレームの最大送信回数（dot11RTSThreshold より上）。デフォルト値は 4 です。

表 5-18　[802.11 b/g/n Parameters] ページのフィールド （続き）

フィールド	説明
Max Tx MSDU Lifetime	MSDU の初回送信後、MSDU の以降の送信の試みを停止するまでの、TU 単位の経過時間。デフォルト値は 512 です。
Max Rx Lifetime	フラグメント化された MMPDU または MSDU の初回受信後、MMPDU または MSDU の以降の再構成の試みを停止するまでの、TU 単位の経過時間。デフォルト値は 512 です。
Physical Channel Fields	
TI Threshold	ビジー メディアを検出するために使用するしきい値（頻度）。CCA は、このしきい値を超える RSSI を検出するとビジー メディアを報告します。
Channel Agility Enabled	物理チャネル敏捷性機能が実装されているかどうか。
Station Configuration Fields	
Medium Occupancy Limit	ポイント コーディネータが、1 つ以上の DCF のインスタンスがメディアにアクセスするのに十分な時間制御を放棄せずに、ワイヤレス メディアの使用を制御する可能性がある最大時間を、TU 単位で示します。デフォルト値は 100 で、最大値は 1000 です。
CFP Period	CFP の開始の間の DTIM 間隔の数。これは、MLME-START.request プリミティブによって変更されます。
CFP Max Duration	PCF によって生成される可能性がある、CFP の最大期間（TU 単位）。これは、MLME-START.request プリミティブによって変更されます。
CF Pollable	この属性が実装されている場合、クライアントは SIFS 時間内にデータ フレームで CF-Poll に応答できることを示します。STA が SIFS 時間内にデータ フレームで CF-Poll に応答できない場合、この属性は実装されません。
CF Poll Request	CFP がクライアントによって要求されるかどうかを示します。
DTIM Period	DTIM Count フィールドが 0 の TIM 要素を含むビーコン フレームの送信の間に経過する、ビーコン間隔の数。この値は、ビーコン フレームの DTIM Period フィールドで送信されます。

802.11b/g/n RRM グループのモニタリング

[802.11b/g/n RRM Grouping] ページにアクセスするには、次のいずれかの方法を使用します。

- [Monitor] > [Controllers] の順に選択し、該当する IP アドレスをクリックし、左側のサイドバー メニューの [802.11b/g/n] セクションから [RRM Grouping] または [WPS Grouping] を選択します。

- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11b/g/n] セクションから [RRM Grouping] または [WPS Grouping] を選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューの [802.11b/g/n] セクションから [RRM Grouping] または [WPS Grouping] を選択します。

表 5-19 に、[802.11b/g/n RRM Grouping] ページのフィールドの一覧を示します。

表 5-19　[802.11 b/g/n RRM Grouping] ページのフィールド

フィールド	説明
802.11 b/g/n Grouping Control	
Grouping Mode	動的グループ化のモードは、オンとオフの 2 つです。グループ化がオフの場合、動的グループ化は実行されません。各コントローラは、アクセス ポイントの自身のパラメータのみを最適化します。グループ化をオンにすると、コントローラはグループを形成し、リーダーを選択してより適切な動的パラメータの最適化を実行します。
Grouping Role	次の 5 つのグループ化ロールがあります。 – [None]：このグループ化ロールは、[RF Group Mode] が [Off] に設定されている場合に表示されます。 – [Auto-Leader]：このグループ化ロールは、[RF Group Mode] が [Automatic] に設定され、自動グループ化アルゴリズムによってコントローラがリーダーとして選択されている場合に表示されます。 – [Auto-Member]：このグループ化ロールは、[RF Group Mode] が [Automatic] に設定され、自動グループ化アルゴリズムによってコントローラがメンバーとして選択されている場合に表示されます。 – [Static-Leader]：このグループ化ロールは、[RF Group Mode] が [Leader] に設定されている場合に表示されます。 – [Static-member]：このグループ化ロールは、[RF Group Mode] が [Automatic] に設定され、リーダーからの参加要求の結果、コントローラがリーダーに参加している場合に表示されます。
Group Leader IP Address	これはグループ リーダーの IP アドレスです。
Group Leader MAC Address	これは、このコントローラが属しているグループのグループ リーダーの MAC アドレスです。
Is 802.11a Group Leader	このコントローラがグループ リーダーの場合は [Yes]、コントローラがグループ リーダーでない場合は [No]。

表 5-19　[802.11 b/g/n RRM Grouping] ページのフィールド （続き）

フィールド	説明
Last Update Time (secs)	最後にグループを更新してからの経過時間（秒単位）。これは、このコントローラがグループ リーダーである場合のみ有効です。
Group Update Interval (secs)	グループ化がオンになっている場合、この間隔（秒単位）は、グループ化アルゴリズムがグループ リーダーによって実行される期間を表します。グループ化アルゴリズムは、グループの内容が変更され、自動グループ化が有効であるときも実行されます。動的グループ化は、システム管理者からの要求時に開始できます。デフォルト値は 3600 秒です。
Group Members	
Group Member Name	グループ メンバーの名前。
Group Member IP Address	グループ メンバーの IP アドレス。
Member Join Reason	メンバーの現在の状態。

コントローラの IPv6 のモニタリング

ネイバー バインド カウンタ統計情報のモニタリング

[Neighbor Bind Counter Statistics] ページにアクセスするには、次のいずれかの方法を使用します。

- [Monitor] > [Controllers] の順に選択し、IP アドレスを選択し、左側のサイドバー メニューで [IPv6] > [Neighbor Bind Counters] の順に選択します。
- [Monitor] > [Access Points] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [IPv6] > [Neighbor Bind Counters] の順に選択します。
- [Monitor] > [Clients] の順に選択し、[AP Name] でリスト項目をクリックし、[Registered Controller] をクリックした後、左側のサイドバー メニューで [IPv6] > [Neighbor Bind Counters] の順に選択します。

表 5-20 に、[Neighbor Bind Counter Stats] ページのフィールドの一覧を示します。

表 5-20　[Neighbor Bind Counter Stats] ページのフィールド

フィールド	説明
Neighbor Bind Counters	IPv6 アドレス、リンク、MTU などを生成および取得するために、ホストまたはクライアントとルータの間で交換されたメッセージ数の統計情報を提供します。
Received Messages	NDP および DHCPv6 の、アドバタイズメントや送信要求などの、受信したメッセージの数。
Bridged Messages	NDP および DHCPv6 の、アドバタイズメントや送信要求などの、ブリッジングしたメッセージの数。

表 5-20　[Neighbor Bind Counter Stats] ページのフィールド （続き）

フィールド	説明
Total Snooping Dropped Messages	NDP および DHCPv6 の、アドバタイズメントや送信要求などの、ブリッジングしたメッセージの数と、ドロップの理由。
Neighbor Discovery Suppress Drop Counter	ドロップされたネイバー探索メッセージの総数。
Total Suppress Dropped Messages	ネイバー探索メッセージのドロップ理由。

（注）　[Total Snooping/Suppress Drop Messages] 欄の値にマウス カーソルを合わせると、対応するメッセージがドロップされた理由が表示されます。

mDNS サービス プロバイダー情報のモニタリング

このページでは、mDNS サービスおよびサービス プロバイダー情報のリストを表示できます。

[mDNS Service Provider Information] ページにアクセスするには、[Monitor] > [Controllers] を選択し、IP アドレスを選択後、左側のサイド バー メニューから [mDNS] > [Service Provider Information] を選択します。

表 5-21 に [Service Provider Information] ページのフィールドの一覧を示します。

表 5-21　[Service Provider Information] ページのフィールド

フィールド	説明
Service Name	mDNS サービスの名前。
MAC Address	サービス プロバイダーの MAC アドレス。
Service Provider Name	サービス プロバイダーの名前。最大 100 のサービス プロバイダーをコントローラに関連付けることができます。
VLAN ID	サービス プロバイダーの VLAN ID。
Type	サービスを使用できるインターフェイスが表示されます。たとえば、有線、無線、優先ゲスト。
TTL (seconds)	サービス プロバイダーによって提供されるサービスの有効性を決定する存続可能時間（TTL）値（秒）。TTL が期限切れになると、サービス プロバイダーはコントローラから削除されます。
Time Left (seconds)	サービス プロバイダーがコントローラから削除されるまでの残り時間（秒）。

スイッチのモニタリング

スイッチに関する詳細情報を表示するには、[Monitor] > [Switches] を選択します。この項では、スイッチのモニタリングについて詳しく説明します。内容は次のとおりです。

- 「スイッチの検索」（P.5-32）
- 「スイッチの表示」（P.5-32）
- 「スイッチ システム パラメータのモニタリング」（P.5-33）
- 「スイッチ インターフェイスのモニタリング」（P.5-39）
- 「スイッチ クライアントのモニタリング」（P.5-41）

スイッチの検索

Prime Infrastructure 検索機能を使用して、特定のスイッチを検索するか、カスタム検索を作成して保存します。

スイッチの高度な検索の実行時に、次のフィールドを設定できます（表 5-22 を参照）。

表 5-22　[Search Switches] のフィールド

フィールド	オプション
Search for Switches by	[All Switches]、[IP Address]、または [Switch Name] を選択します。ワイルドカード（*）を使用できます。たとえば、[IP Address] を選択して、172* を入力した場合、Prime Infrastructure は、IP アドレス 172 で始まるすべてのスイッチを返します。
Items per page	ページあたりに返すスイッチの数を選択します。

追加情報については、次のいずれかのトピックを参照してください。

- 「検索機能の使用方法」（P.2-54）
- 「Quick Search」（P.2-54）
- 「Advanced Search」（P.2-55）
- 「Saved Search」（P.2-67）

スイッチの表示

スイッチの一覧を表示するには、[Monitor] > [Switches] の順に選択します。このページから、表 5-23 に示すデフォルト情報を含め、スイッチの要約を参照できます。

表 5-23　スイッチの表示

フィールド	説明
IP Address	スイッチに割り当てられている IP アドレス。リスト項目をクリックするとアクセス ポイントの詳細が表示されます。
Device Name	スイッチ名。
Device Type	スイッチのタイプ。
Reachability Status	スイッチが到達可能な場合は [OK] が表示され、スイッチが到達不能な場合は [Unreachable] が表示されます。
Endpoint Count	スイッチ上のエンドポイントの数。

スイッチ リスト ページの設定

[Edit View] ページでは、[Switches] テーブルの列を追加、削除、または並べ替えができます。

テーブルの列を編集する手順は、次のとおりです。

ステップ 1　[Monitor] > [Switches] の順に選択します。

ステップ 2　[Edit View] リンクをクリックします。

ステップ 3　テーブルに新しい列を追加するには、左側の列で、追加する列見出しをクリックして強調表示します。[Show] をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。

ステップ 4　テーブルから列を削除するには、右側の列で、削除する列見出しをクリックして強調表示します。[Hide] をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。

ステップ 5　[Up] ボタンと [Down] ボタンを使用して、表内での情報の並び順を指定します。目的の列見出しを選択し、[Up] または [Down] をクリックして、現在のリスト内での位置を変更します。

ステップ 6　デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7　[Submit] をクリックして、変更内容を確定します。

スイッチ システム パラメータのモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。この項では、各スイッチ詳細ページについて詳しく説明します。内容は次のとおりです。

スイッチの要約情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。表 5-24 に、表示される要約情報を示します。

表 5-24　スイッチの要約情報の表示

General	
IP Address	スイッチの IP アドレス。
Device Name	スイッチ名。
Device Type	スイッチの種類。
Up Time	最後にリブートしてからの時間。
System Time	スイッチ上の時刻。
Reachability Status	有効な値は次のとおりです。 • Reachable • Unreachable
Location	スイッチの場所。
Contact	スイッチの担当者名。
Cisco Identity Capable	スイッチがアイデンティティ対応かどうかを示します。
Location Capable	スイッチがロケーション情報を保存できるかどうかを示します。
CPU Utilization	指定した期間の最大、平均、および最小 CPU 使用率のグラフが表示されます。
Unique Device Identifier (UDI)	
Name	製品の種類。
Description	UDI の説明。
Product ID	注文可能な製品 ID
Version ID	製品 ID のバージョン
Serial Number	一意の製品シリアル番号
Inventory	
Software Version	現在スイッチで動作しているソフトウェアのバージョン。
Model No.	スイッチのモデル番号。
Port Summary	
Number of Ports Up	スイッチでアップ状態のポートの数。
Number of Ports Down	スイッチでダウン状態のポートの数。
Memory Utilization	指定した期間の最大、平均、および最小メモリ使用率のグラフが表示されます。

関連項目

- 「スイッチ インターフェイスのモニタリング」（P.5-39）

スイッチのメモリ情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Memory] を選択します。表 5-25 に、表示されるメモリ情報を示します。

表 5-25　スイッチのメモリ情報の表示

メモリ プール	
Type	メモリのタイプ。
Name	メモリ プールに割り当てられた名前。
Used (MB)	使用中のメモリ量（MB 単位）。
Free (MB)	使用可能なメモリ量（MB 単位）。

スイッチの環境情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Environment] を選択します。表 5-26 に、表示される環境情報を示します。

表 5-26　スイッチの環境情報の表示

電源モジュール	
Model Name	電源のモデル名。
Description	電源の説明。
Operational Status	関連付けられている電源のステータス。 • 緑：電源は動作可能です。 • 赤：電源は動作不能です。
Manufacturer Name	電源のメーカー名。
Free	空き電源スロット。
Vendor Equipment Type	ベンダー製機器タイプの説明。
ファン	
Name	ファンの名前。
Description	ファンの説明。
Operational Status	ファンのステータス。 • 緑：ファンは動作可能です。 • 赤：ファンは動作不能です。
Vendor Equipment Type	ベンダー製機器タイプの説明。
Serial Number	ファンのシリアル番号。

スイッチ モジュール情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Modules] を選択します。表 5-27 に、表示されるモジュール情報を示します。

表 5-27　スイッチ モジュール情報の表示

モジュール	
Product Name	モジュールの名前。

表 5-27　スイッチ モジュール情報の表示 （続き）

Physical Location	モジュールが格納されている場所。
Number of Ports	モジュールがサポートするポートの数。
Operational State	モジュールの動作ステータス。
Equipment Type	機器の種類。
Inline Power Capable	モジュールにインライン パワー機能があるかどうかを示します。

スイッチの VLAN 情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [VLANs] を選択します。表 5-28 に、表示される VLAN 情報を示します。

表 5-28　スイッチの VLAN 情報の表示

VLAN	
VLAN ID	VLAN の ID。
VLAN Name	VLAN の名前。
VLAN Type	VLAN の種類。

スイッチの VTP 情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [VTP] を選択します。表 5-29 に、表示される VTP 情報を示します。

表 5-29　スイッチの VTP 情報の表示

VTP	
VTP Domain Name	VTP ドメインの名前。
VTP Version	使用している VTP のバージョン。
VTP Mode	VTP モード。 • Client • Server • [Transparent] : VTP メッセージを生成またはリッスンしませんが、メッセージを転送します。 • [Off] : VTP メッセージを生成、リッスン、転送しません。
Pruning Enabled	VTP プルーニングが有効かどうかを示します。

スイッチの物理ポート情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Physical Ports] を選択します。表 5-30 に、表示される物理ポート情報を示します。

表 5-30　スイッチの物理ポート情報の表示

物理ポート	
Port Name	物理ポートの名前。
Port Description	物理ポートの説明。
Residing Module	物理ポートがあるモジュール。
Vendor Equipment Type	ベンダー製機器タイプの説明。

スイッチのセンサー情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Sensors] を選択します。表 5-31 に、表示されるセンサー情報を示します。

表 5-31　スイッチのセンサー情報の表示

センサー	
Sensor Name	センサーの名前。
Sensor Description	センサーの説明
Type	センサーの種類。
Vendor Sensor Type	ベンダー製センサーの種類の説明。
Equipment Name	機器の名前。
Precision	範囲が 1 ～ 9 の場合、精度は、センサー値の固定小数点数値の小数点以下の桁数です。範囲が -8 ～ -1 の場合、センサーの精度は、センサー値の固定小数点数値の正確な桁数です。
Status	センサーの動作ステータス。

スイッチのスパニングツリー情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Spanning Tree] を選択します。表 5-32 に、表示されるスパニングツリー情報を示します。

表 5-32　スイッチのスパニングツリー情報の表示

スパニングツリー	
STP Instance ID	STP の ID。STP インスタンス ID をクリックすると、「スパニングツリーの詳細の表示」（P.5-38）に示すスパニングツリーの詳細が表示されます。
VLAN ID	VLAN の ID。
Root Path Cost	パスのルート コスト。
Designated Root	転送ポート。
Bridge Priority	ブリッジのプライオリティ。
Root Bridge Priority	ルート ブリッジのプライオリティ番号。
Max Age (sec)	最大経過時間の STP タイマー値（秒単位）。
Hello Interval (sec)	STP タイマー値（秒単位）。

スパニングツリーの詳細の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Spanning Tree] を選択し、STP インスタンス ID をクリックすると、表 5-33 に示すスパニングツリーの詳細が表示されます。

表 5-33　スパニングツリーの詳細の表示

スパニングツリー	
STP Port	STP ポートの名前。
Port Role	ポートのロール。
Port Priority	ポートのプライオリティ番号。
Path Cost	パスのコスト。
Port State	ポートの状態。
Port Type	ポートの種類。

スイッチのスタック情報の表示

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックして、スイッチに関する詳細を表示します。[System] メニューから [Stacks] を選択します。表 5-34 に、表示されるスパニングツリー情報を示します。

表 5-34　スイッチのスタック情報の表示

スタック	
MAC Address	スタックの MAC アドレス。
Role	スタックの役割。 • [Master]：スタック マスター • [Member]：スタックのアクティブ メンバー • [Not Member]：非アクティブ スタック メンバー
Switch Priority	スイッチのプライオリティ番号。
State	スタックの現在の状態。
Software Version	スイッチで動作しているソフトウェア イメージ。

スイッチの NMSP およびロケーション情報の表示

左側のサイドバー メニュー [System] を使用し、スイッチの NMSP およびロケーション情報を表示できます。

スイッチの NMSP およびロケーション情報を表示するには、[Monitor] > [Switches] の順に選択し、[IP Address] 欄の IP アドレスをクリックします。[System] > [NMSP and Location] の順に選択します。

[NMSP and Location] ページが表示されます。

[NMSP Status] グループ ボックスに NMSP ステータスが表示され、[Location] グループ ボックスにロケーション情報が表示されます。

NMSP とロケーションの詳細については、「スイッチ NMSP およびロケーションの設定」を参照してください。

スイッチ インターフェイスのモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックします。[System] メニューから [Interfaces] を選択し、この項で説明する次のいずれかのインターフェイスを選択します。ここでは、次の内容について説明します。

- 「スイッチのイーサネット インターフェイスのモニタリング」（P.5-39）
- 「スイッチの IP インターフェイスのモニタリング」（P.5-40）
- 「スイッチの VLAN インターフェイスのモニタリング」（P.5-40）
- 「スイッチの EtherChannel インターフェイスのモニタリング」（P.5-40）

スイッチのイーサネット インターフェイスのモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックします。[System] メニューから、[Interfaces] > [Ethernet Interfaces] の順に選択します。表 5-35 に、表示されるイーサネット インターフェイス情報を示します。

表 5-35　スイッチのイーサネット インターフェイスの表示

Name	イーサネット インターフェイスの名前。イーサネット インターフェイス名をクリックすると、「スイッチのイーサネットインターフェイスの詳細のモニタリング」（P.5-39）に示す詳細が表示されます。
MAC Address	イーサネット インターフェイスの MAC アドレス。
Speed (Mbps)	イーサネット インターフェイスの現在の帯域幅の推測値（bps 単位）。
Operational Status	イーサネット インターフェイスの現在の動作状態。
MTU	インターフェイスで送受信できる最大のパケット サイズ。
Desired VLAN Mode	VLAN モード。
Access VLAN	ポートが設定されている VLAN。

スイッチのイーサネットインターフェイスの詳細のモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックします。[System] メニューから、[Interfaces] > [Ethernet Interfaces] の順に選択し、[Name] 欄のイーサネット インターフェイス名をクリックします。表 5-36 に、表示されるイーサネット インターフェイスの詳細情報を示します。

表 5-36　スイッチのイーサネット インターフェイスの詳細の表示

Ethernet Interfaces	
Name	イーサネット インターフェイスの名前。
Admin Status	インターフェイスの管理ステータス。
Duplex Mode	インターフェイスで設定されているデュプレックス モード。
VLAN Switch Port	
Operational VLAN Mode	VLAN スイッチ ポートの動作モードを示します（アクセス ポートまたはトランク ポート）。
Desired VLAN Mode	VLAN モード（truck、access、dynamic、または desirable）。
Access VLAN	ポートが設定されている VLAN。

表 5-36　スイッチのイーサネット インターフェイスの詳細の表示

Operational Truck Encapsulation	トランクのカプセル化（*802.1Q* または *none*）。
VLAN Trunk	
Native VLAN	トランク スイッチ ポートのタグなし VLAN。
Prune Eligible	トランク ポート上の VLAN をプルーニングできるかどうかを示します。
Allows VLANs	トランク ポート上の許可される VLAN のリスト。
Desired Trunking Encapsulation	トランク カプセル化
Trunking Encapsulation Negotiation	インターフェイスがネイバー インターフェイスとネゴシエーションを行い、近接インターフェイスの設定および機能に応じて、ISL トランク（優先）または 802.1Q トランクになるよう指定します。

スイッチの IP インターフェイスのモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックします。[System] メニューから、[Interfaces] > [IP Interfaces] の順に選択します。表 5-37 に、表示される IP インターフェイス情報を示します。

表 5-37　スイッチの IP インターフェイスの表示

Interface	インターフェイスの名前。
IP Address	インターフェイスの IP アドレス。
Address Type	アドレス タイプ（IPv4 または IPv6）。

スイッチの VLAN インターフェイスのモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックします。[System] メニューから、[Interfaces] > [VLAN Interfaces] の順に選択します。表 5-38 に、表示される VLAN インターフェイス情報を示します。

表 5-38　スイッチの VLAN インターフェイスの表示

Port Name	VLAN ポートの名前。
VLAN ID	VLAN ポートの ID。
Operational Status	VLAN インターフェイスの現在の動作状態。
Admin Status	VLAN インターフェイスの現在の管理状態。
Port Type	VLAN ポートの種類。
Maximum Speed (Mbps)	VLAN インターフェイスのサポートされる最大速度。
MTU	VLAN インターフェイスで送受信できる最大のパケット サイズ。

スイッチの EtherChannel インターフェイスのモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックします。[System] メニューから、[Interfaces] > [EtherChannel Interfaces] の順に選択します。表 5-39 に、表示される EtherChannel インターフェイス情報を示します。

表 5-39　スイッチの EtherChannel インターフェイスの表示

Name	EtherChannel インターフェイスの名前。
Channel Group ID	EtherChannel の数値 ID。
Control Method	EtherChannel を管理するためのプロトコル（LACP または TAgP）。
Actor Admin Key	チャネル ID。
Number of (LAG) Members	設定されているポート数。

スイッチ クライアントのモニタリング

[Monitor] > [Switches] の順に選択して、[IP Address] 欄で IP アドレスをクリックします。[System] メニューから [Clients] を選択します。表 5-39 に、表示される EtherChannel インターフェイス情報を示します。

表 5-40　現在関連付けられているクライアントの表示

IP Address	クライアントの IP アドレス。
MAC Address	クライアントの MAC アドレス。
User Name	クライアントのユーザ名。
Vendor Name	クライアントのベンダー名。
Map Location	クライアントの場所。
VLAN	クライアントが設定されている VLAN。
Interface	クライアントが設定されているインターフェイス。
Association Time	クライアント アソシエーションのタイムスタンプ。
Authorization Profile Name	格納されている許可プロファイル名。

アクセス ポイントのモニタリング

この項では、コントローラ アクセス ポイントの詳細へのアクセスについて説明します。それぞれのアクセス ポイントの詳細にアクセスするには、メインの日付領域を使用します。

このページにアクセスするには、[Monitor] > [Access Points] の順に選択します。この項では、アクセス ポイントのモニタリングについて詳しく説明します。内容は次のとおりです。

- 「アクセス ポイントの検索」（P.5-42）
- 「アクセス ポイントのリストの表示」（P.5-42）
- 「アクセス ポイントのレポートの生成」（P.5-46）
- 「アクセス ポイントの詳細のモニタリング」（P.5-56）
- 「アクセス ポイントの無線の詳細のモニタリング」（P.5-68）
- 「メッシュ アクセス ポイントのモニタリング」（P.5-78）
- 「コントローラとアクセス ポイント上の一意のデバイス ID の取得」（P.5-84）
- 「カバレッジ ホールのモニタリング」（P.5-85）
- 「不正アクセス ポイントのモニタリング」（P.5-87）
- 「アドホック不正のモニタリング」（P.5-103）

- 「Advanced Search を使用した不正クライアントの検索」（P.5-107）
- 「不正アクセス ポイントの場所、タギング、および封じ込めのモニタリング」（P.5-107）

アクセス ポイントの検索

Prime Infrastructure 検索機能を使用して、特定のアクセス ポイントを検索するか、カスタム検索を作成して保存します。追加情報については、次のいずれかのトピックを参照してください。

- 「検索機能の使用方法」（P.2-54）
- 「Quick Search」（P.2-54）
- 「Advanced Search」（P.2-55）
- 「Saved Search」（P.2-67）

アクセス ポイントのリストの表示

[Monitor] > [Access Points] の順に選択するか、アクセス ポイントの検索を行ってこのページにアクセスします。

このページでは、表 5-41 に示すデフォルト情報を含む、アクセス ポイントの要約が表示されます。

表 5-41　アクセス ポイントの検索結果

フィールド	説明
AP Name Ethernet MAC	アクセス ポイントに割り当てられている名前。リスト項目をクリックするとアクセス ポイントの詳細が表示されます。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。
IP Address	アクセス ポイントのローカル IP アドレス。
Radio	不正アクセス ポイントのプロトコルは、802.11a、802.11b、または 802.11g です。リスト項目をクリックするとアクセス ポイントの無線の詳細が表示されます。詳細については、「アクセス ポイントの無線の詳細のモニタリング」（P.5-68）を参照してください。
Map Location	リスト項目をクリックすると、リストで示された場所に移動します。
Controller	リスト項目をクリックすると、コントローラに関するグラフィックと情報が表示されます。詳細については、「Monitoring System Summary」（P.5-3）を参照してください。
Client Count	現在コントローラにアソシエートされているクライアントの総数が表示されます。
Admin Status	アクセス ポイントの管理状態が、有効または無効で表示されます。
AP Mode	アクセス ポイントの動作モードが表示されます。

表 5-41　アクセス ポイントの検索結果 （続き）

フィールド	説明
Oper Status	Cisco WLAN ソリューション デバイスの動作ステータス（Up または Down）が表示されます。[Admin Status] が disabled の場合、動作ステータスはダウンとラベル付けされ、アラームはありません。
Alarm Status	アラームのカラー コードは、次のとおりです。 – 透明：アラームなし – 赤：重大なアラーム – オレンジ：やや重大なアラーム – 黄：比較的重大でないアラーム （注）　このステータスは無線アラームのステータスのみを示し、動作ステータスの管理ステータスは表示しません。

アクセス ポイント リスト表示の設定

テーブルで列の追加、削除、または並べ替えを行うには、[Edit View] リンクをクリックして、[Edit View] ページに移動します。表 5-42 に、検索結果で使用できるオプションのアクセス ポイント パラメータの一覧を示します。

表 5-42　[Edit View] の検索結果

フィールド	説明
AP Type	アクセス ポイントの種類を示します（Unified または Autonomous）。
Antenna Azim.Angle	アンテナの水平方向の角度を示します。
Antenna Diversity	アンテナ ダイバーシティがイネーブルであるかディセーブルであるかを示します。アンテナ ダイバーシティは、適切なアンテナを選択するためにアクセス ポイントが 2 つの統合アンテナ ポートから無線信号をサンプリングすることをいいます。
Antenna Elev.Angle	アンテナの垂直方向の角度を示します。
Antenna Gain	無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 X 0.5 = 2dBi のゲインであることを意味します。
Antenna Mode	低展開、全方向性、または不適切など、アンテナ モードを示します。
Antenna Name	アンテナの名前または種類を示します。

表 5-42　[Edit View] の検索結果 （続き）

フィールド	説明
Audit Status	次の監査ステータスのいずれかを示します。 – [Mismatch]：最新の監査で、Prime Infrastructure とコントローラ間の設定の相違が検出された。 – [Identical]：最新の監査で、設定の相違は検出されなかった。 – [Not Available]：監査ステータスは使用できない。
Base Radio MAC	ベース無線の MAC アドレスを示します。
Bridge Group Name	必要に応じて、アクセス ポイントが属するブリッジ グループの名前を示します。
CDP Neighbors	全方向に接続したシスコ デバイスを示します。
Channel Control	チャネル コントロールが自動かカスタムかを示します。
Channel Number	Cisco 無線がブロードキャストしているチャネルを示します。
Channel Width	この無線のチャネル帯域を示します。[Channel Width] フィールドは、11n AP のみでサポートされます。他の AP では「N/A」と表示されます。
Controller Port	コントローラ ポートの数を示します。
Google Earth Location	Google Earth の場所が割り当てられているかどうかと、場所を示します。
Location	アクセス ポイントの物理的な場所を示します。
Node Hops	アクセス ポイント間のホップ数を示します。
OfficeExtend AP	OfficeExtend アクセスが有効かどうかを示します。無効の場合、アクセス ポイントはリモートで配置されており、セキュリティ リスクが高まります。
PoE Status	アクセス ポイントの Power over Ethernet ステータスを示します。可能な値は次のとおりです。 – [Low]：イーサネットから供給されるアクセス ポイントの電力が低い。 – [Lower than 15.4 volts]：イーサネットから供給されるアクセス ポイントの電力が 15.4 V 未満。 – [Lower than 16.8 volts]：イーサネットから供給されるアクセス ポイントの電力が 16.8 V 未満。 – [Normal]：アクセス ポイントの操作に十分な電力が供給されている。 – [Not Applicable]：電源がイーサネットではない。

表 5-42　[Edit View] の検索結果 （続き）

フィールド	説明
Primary Controller	このアクセス ポイントのプライマリ コントローラの名前を示します。
Radio MAC	無線の MAC アドレスを示します。
Reg.Domain Supported	規制区域がサポートされているかどうかを示します。
Serial Number	アクセス ポイントのシリアル番号を示します。
Slot	スロット番号を示します。
Tx Power Control	送信電力コントロールが自動かカスタムかを示します。
Tx Power Level	送信電力レベルを示します。
Up Time	アクセス ポイントが送受信できる状態になっている時間（日、時間、分、秒）を示します。
WLAN Override Names	WLAN のオーバーライド プロファイル名を示します。
WLAN Override	WLAN のオーバーライドがイネーブルかディセーブルかを示します。

アクセス ポイント リストの表示の設定

[Edit View] ページでは、[Access Points] テーブルの列を追加、削除、または並べ替えができます。

アラーム テーブルの列を編集する手順は、次のとおりです。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　[Edit View] リンクをクリックします。

ステップ 3　アクセス ポイント表に新しい列を追加するには、左側の領域で、列見出しをクリックして選択します。[Show] をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。

ステップ 4　アクセス ポイント表から列を削除するには、右側の領域で、削除する列見出しをクリックして選択します。[Hide] をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。

ステップ 5　[Up] ボタンと [Down] ボタンを使用して、表内での情報の並び順を指定します。目的の列見出しを選択し、[Up] または [Down] をクリックして、現在のリスト内での位置を変更します。

ステップ 6　デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7　[Submit] をクリックして、変更内容を確定します。

（注）　[Edit View] で追加できるアクセス ポイント フィールドについては、「アクセス ポイントのリストの表示」（P.5-42）を参照してください。

アクセス ポイントのレポートの生成

（注）　[Access Points] リスト（[Monitor] > [Access Points]）で作成するレポートはカスタマイズできません。

アクセス ポイントのレポートを生成するには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　レポートを実行するアクセス ポイントをクリックして選択します。

ステップ 3　[Select a report] ドロップダウン リストから該当するレポートを選択します。

ステップ 4　[Go] をクリックします。

表 5-43 に使用可能なレポートの一覧を示します。

表 5-43　アクセス ポイント レポート

レポート	説明	参照先
Load	ロード情報が含まれるレポートを生成します。	詳細については、「トラフィック負荷のモニタリング」（P.5-48）を参照してください。
Dynamic Power Control	動的電力制御情報が含まれるレポートを生成します。	詳細については、「動的電力制御のモニタリング」（P.5-49）を参照してください。
Noise	ノイズ情報が含まれるレポートを生成します。	詳細については、「アクセス ポイントのノイズのモニタリング」（P.5-50）を参照してください。
Interference	干渉情報が含まれるレポートを生成します。	詳細については、「アクセス ポイントの干渉のモニタリング」（P.5-50）を参照してください。
Coverage (RSSI)	カバレッジ（RSSI）情報が含まれるレポートを生成します。	詳細については、「アクセス ポイントのカバレッジ（RSSI）のモニタリング」（P.5-51）を参照してください。
Coverage (SNR)	カバレッジ（SNR）情報が含まれるレポートを生成します。	詳細については、「アクセス ポイントのカバレッジ（SNR）のモニタリング」（P.5-51）を参照してください。
Up/Down Statistics	最後のリブートからの経過時間（日数、時間、および分単位）。アップタイム情報が含まれるレポートを生成します。	詳細については、「アクセス ポイント アップ/ダウン統計情報のモニタリング」（P.5-51）を参照してください。
Voice Statistics	音声トラフィックによる無線使用率を示す、選択したアクセス ポイントのレポートを生成します。	詳細については、「アクセス ポイントの音声統計情報のモニタリング」（P.5-52）を参照してください。
Voice TSM Table	選択したアクセス ポイントと無線のレポートを生成します。クライアントごとに、その音声トラフィック ストリームの QoS ステータス、PLR、および遅延が表示されます。	詳細については、「アクセス ポイント音声 TSM テーブルのモニタリング」（P.5-52）を参照してください。

表 5-43　アクセス ポイント レポート （続き）

レポート	説明	参照先
Voice TSM Reports	TSM テーブルのグラフィカル表現。ただし、複数のクライアントからのメトリックがグラフ上で平均されています。	詳細については、「アクセス ポイントの音声 TSM レポートのモニタリング」（P.5-54）を参照してください。
802.11 Counters	MAC レイヤでのアクセス ポイントのカウンタが表示されます。エラー フレーム、フラグメント数、RTS/CTS フレーム数、再試行フレームなどの統計情報は、フィルタリング基準に基づいて生成され、MAC 層のパフォーマンス（および問題）を解釈するために役立ちます。	詳細については、「アクセス ポイントの 802.11 カウンタのモニタリング」（P.5-54）を参照してください。
AP Profile Status	アクセス ポイントの負荷、ノイズ、干渉、およびカバレッジ プロファイル ステータスが表示されます。	詳細については、「アクセス ポイントの AP プロファイル ステータスのモニタリング」（P.5-55）を参照してください。
Air Quality vs.Time	設定された期間の間のワイヤレス ネットワークの電波品質の指標が表示されます。	詳細については、「電波品質のモニタリング」（P.5-56）を参照してください。
Traffic Stream Metrics	指定したクライアントの現在および過去の Quality of Service（QoS）を無線レベルで判断する場合に役立ちます。また、パケット損失率、平均キューイング遅延、遅延パケットの配布、ローミング遅延などのアップリンクおよびダウンリンク統計情報も表示されます。	詳細については、「アクセス ポイントのトラフィック ストリーム メトリックのモニタリング」（P.5-55）を参照してください。
Tx Power and Channel	レポートを生成するときに使用したフィルタリング条件に基づいて、デバイスのチャネル計画の割り当てと送信電力レベルの傾向が表示されます。予期しない動作やネットワークのパフォーマンスの問題を識別するために役立つことがあります。	詳細については、「アクセス ポイント送信電力とチャネルのモニタリング」（P.5-55）を参照してください。
VoIP Calls Graph	ネットワーク上の VoIP コール（無線ごと）の数と期間の詳細を時間とともに表示するなど、音声の観点からワイヤレス ネットワークの使用状況を分析するために役立ちます。このレポートから有益なデータを収集するには、WLAN で VoIP スヌーピングが有効になっている必要があります。このレポートでは、グラフで情報が表示されます。	詳細については、「VoIP コールのモニタリング」（P.5-56）を参照してください。
VoIP Calls Table	VoIP Calls Graph レポートと同じ情報が表形式で表示されます。	詳細については、「VoIP コールのモニタリング」（P.5-56）を参照してください。

表 5-43　アクセス ポイント レポート （続き）

レポート	説明	参照先
Voice Statistics	ネットワーク上の音声クライアント、ボイス コール、ローミング コール、および拒否されたコール（無線ごと）によって使用される帯域幅のパーセンテージなどの詳細を表示することで、音声の観点からワイヤレス ネットワークの使用状況を分析するために役立ちます。このレポートから有用なデータを収集するためには、コール アドミッション制御（CAC）が音声クライアントでサポートされていることを確認してください。	詳細については、「音声統計情報のモニタリング」（P.5-56）を参照してください。
Worst Air Quality APs	干渉の問題がネットワークに影響を与えている箇所を「一目で」理解できるように、概要的なわかりやすいメトリックが提供されます。電波品質（AQ）はチャネル、フロア、およびシステム レベルで報告され、AQ が望ましいしきい値を下回った場合に自動的に通知されるように AQ アラートがサポートされています。	詳細については、「電波品質のモニタリング」（P.5-56）を参照してください。

トラフィック負荷のモニタリング

トラフィック負荷は、トラフィックの送受信のために使用される合計帯域幅です。これにより、WLAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越してネットワーク拡張の計画を立てることができます。

アクセス ポイント負荷レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Load] を選択します。

ステップ 4　[Go] をクリックします。選択したアクセス ポイントの Load レポートが表示されます。

表 5-44 に、このページに表示されるフィールドの一覧を示します。

表 5-44　トラフィックの負荷

フィールド	説明
AP Name	アクセス ポイント名をクリックすると、アクセス ポイントの詳細が表示されます。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。
Radio	不正アクセス ポイントのプロトコルは、802.11a、802.11b、または 802.11g です。このアクセス ポイントのオンデマンド統計情報を表示するには、無線をクリックします。詳細については、「アクセス ポイントの無線の詳細のモニタリング」（P.5-68）を参照してください。

表 5-44　トラフィックの負荷 （続き）

フィールド	説明
Attached Client Count	接続されているクライアントの数（実際の値としきい値）。
Channel Utilization	0 ～ 100 % の 802.11a の RF 利用率のしきい値（実際の値としきい値）。
Receive Utilization	0 ～ 100 % の 802.11a または 802.11b/g RF の RF 受信使用率のしきい値。
Transmit Utilization	0 ～ 100 % の 802.11a または 802.11b/g RF の RF 送信使用率のしきい値。
Status	クライアント接続のステータス。

動的電力制御のモニタリング

アクセス ポイント負荷レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Dynamic Power Control] を選択します。

ステップ 4　[Go] をクリックします。選択したアクセス ポイントの Dynamic Power Control レポートが表示されます。

表 5-45 に、このページに表示されるアクセス ポイントの動的制御のフィールドの一覧を示します。

表 5-45　[Dynamic Power Control] ページのフィールド

フィールド	説明
AP Name	アクセス ポイントに割り当てられた名前。アクセス ポイントのフィールドにアクセスするには、リスト中のアクセス ポイント名をクリックします。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。
Radio	不正なアクセス ポイントのプロトコルは、802.11a または 802.11b/g のいずれかです。リスト中の Cisco 無線 をクリックするとそのフィールドにアクセスできます。詳細については、「アクセス ポイントの無線の詳細のモニタリング」（P.5-68）を参照してください。

表 5-45　[Dynamic Power Control] ページのフィールド （続き）

フィールド	説明
Current Power Level	送信電力テーブルから取得した動作送信電力レベルが表示されます。アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。 （注）　電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。
Power Assignment Mode	動的送信電力割り当てには次の 3 つのモードがあります。 – [Automatic]：送信電力は、この動作を許可するすべての Cisco 1000 シリーズ Lightweight アクセス ポイントで定期的に更新されます。 – [On Demand]：送信電力は、[Assign Now] ボタンを選択したときに更新されます。 – [Fixed]：動的な送信電力の割り当ては行われず、値はグローバル デフォルトに設定されます。デフォルトは Automatic です。 – 推奨される電力レベルです。

アクセス ポイントのノイズのモニタリング

アクセス ポイントの Noise レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

（注）　複数のアクセス ポイントが選択されている場合、無線タイプが同じである必要があります。

ステップ 3　[Generate a report selected APs] ドロップダウン リストから、[Noise] を選択します。

ステップ 4　[Go] をクリックします。選択したアクセス ポイントの Noise レポートが表示されます。

このページには、各チャネルのノイズ（dBm 単位の RSSI）の棒グラフが表示されます。

アクセス ポイントの干渉のモニタリング

アクセス ポイントの Interference レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

（注）　複数のアクセス ポイントが選択されている場合、無線タイプが同じである必要があります。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Interference] を選択します。

ステップ 4　[Go] をクリックします。選択したアクセス ポイントの Interference レポートが表示されます。

このページには、各チャネルの干渉（dBm 単位の RSSI）の棒グラフが表示されます。

- 高い干渉は -40 ～ 0 dBm です。
- 限界の干渉は -100 ～ -40 dBm です。
- 低い干渉は -110 ～ -100 dBm です。

アクセス ポイントのカバレッジ（RSSI）のモニタリング

アクセス ポイントの Coverage (RSSI) レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Coverage (RSSI)] を選択します。

ステップ 4　[Go] をクリックします。選択したアクセス ポイントの Coverage (RSSI) レポートが表示されます。

このページには、クライアント数対 dBm 単位の RSSI を示す、受信信号強度ごとのクライアント分布の棒グラフが表示されます。

アクセス ポイントのカバレッジ（SNR）のモニタリング

アクセス ポイントの Coverage (SNR) レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Coverage (SNR)] を選択します。

ステップ 4　[Go] をクリックします。選択したアクセス ポイントの Coverage (SNR) レポートが表示されます。

このページには、クライアント数対 SNR を示す、信号対雑音比ごとのクライアント分布の棒グラフが表示されます。

アクセス ポイント アップ/ダウン統計情報のモニタリング

アクセス ポイントの Up/Down Statistics レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Up/Down Statistics] を選択します。[Go] をクリックします。選択したアクセス ポイントの Up/Down Statistics レポートが表示されます。

（注）　アップ タイムは最後のリブートからの経過時間（日数、時間、および分単位）です。

このページには、時間に対するアクセス ポイントのアップ タイムの折れ線グラフが表示されます。

複数のアクセス ポイントを選択すると、次のメッセージが表示されます。

Please select only one AP for the Up Time Report.

アクセス ポイントの音声統計情報のモニタリング

音声トラフィックによる無線使用率を示す、選択したアクセス ポイントのレポートを生成します。レポートには現在のコールの数が含まれています。

（注）　Voice Statistics レポートは、CAC/WMM クライアントのみに適用されます。

アクセス ポイントの Voice Statistics レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Voice Statistics] を選択します。[Go] をクリックします。選択したアクセス ポイントの Voice Statistics レポートが表示されます。

このページには、次のアクセス ポイントの音声統計情報が表示されます。

- [AP Name] : [AP Name] で項目を選択します。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。
- [Radio] : [Radio] で項目を選択します。詳細については、「アクセス ポイントの無線の詳細のモニタリング」（P.5-68）を参照してください。
- [Calls in Progress] : 進行中のコールの数。
- [Roaming Calls in Progress] : 進行中のローミング コールの数。
- [Bandwidth in Use] : 使用中の帯域幅のパーセンテージ。

アクセス ポイント音声 TSM テーブルのモニタリング

選択したアクセス ポイントと無線のレポートを生成します。クライアントごとに、その音声トラフィック ストリームの QoS ステータス、PLR、および遅延が表示されます。

アクセス ポイントの Voice TSM Table レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Voice TSM Table] を選択します。

ステップ 4　[Go] をクリックします。選択したアクセス ポイントの Voice Traffic Stream Metrics Table レポートが表示されます。

表 5-46 に [Voice Traffic Stream Metrics Table] ページのフィールドの一覧を示します。

表 5-46　[Voice Traffic Stream Metrics Table] ページのフィールド

フィールド	説明
Time	アクセス ポイントから統計情報が収集された時刻。
Client MAC	クライアントの MAC アドレス。これには、過去 90 秒の間隔中に評価されたクライアントのリストが表示されます。クライアントとしては、VoIP 電話、ラップトップ、PDA などがあり、測定値を収集しているアクセス ポイントに接続されたすべてのクライアントを示します。
QoS	WLAN に影響を与える可能性のある QoS 値（パケット遅延、パケット ジッタ、パケット損失、ローミング時間）がモニタされます。アクセス ポイントおよびクライアントでメトリックを測定し、アクセス ポイントで計測結果を収集してこれらをコントローラに送信します。アクセス ポイントでは、90 秒ごとにコントローラのトラフィック ストリーム メトリック情報を更新し、一度に 10 分間分のデータが格納されます。
% PLR (Downlink)	90 秒の間隔中にダウンリンク（アクセス ポイントからクライアントへ向かう方向）で失われたパケットの割合。
% PLR (Uplink)	90 秒の間隔中にアップリンク（クライアントからアクセス ポイントへ向かう方向）で失われたパケットの割合。
Avg Queuing Delay (ms) (Downlink)	ダウンリンクの平均キューイング遅延（ミリ秒単位）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
Avg Queuing Delay (ms) (Uplink)	アップリンクの平均キューイング遅延（ミリ秒単位）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
% Packets > 40 ms Queuing Delay	40 ms を超えるキューイング遅延パケットのパーセンテージ。
% Packets > 20 ms Queuing Delay	20 ms を超えるキューイング遅延パケットのパーセンテージ。
Roaming Delay	ローミング遅延（ミリ秒単位）。クライアントによって測定されるローミング遅延は、古いアクセス ポイントから最後のパケットを受信した時点から、ローミングが正常に行われた後で新しいアクセス ポイントから最初のパケットを受信した時点まで測定されます。

アクセス ポイントの音声 TSM レポートのモニタリング

このレポートは、Voice Traffic Stream Metrics Table をグラフィカル表示したものです。ただし、複数のクライアントからのメトリックがグラフ上で平均されています。

アクセス ポイントの Voice Traffic Stream Metrics Table レポートにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスをオンにします。

ステップ 3　[Generate a report for selected APs] ドロップダウン リストから、[Voice TSM Reports] を選択します。

[Go] をクリックします。選択したアクセス ポイントの Voice Traffic Stream Metrics Table レポートが表示されます。

このページには、次のダウンリンクおよびアップリンク メトリック情報の折れ線グラフが、時刻および日付とともに表示されます（表 5-47 を参照）。

表 5-47　[Voice Traffic Stream Metrics Table Reports] ページのフィールド

フィールド	説明
Average Queuing Delay (ms)	平均キューイング遅延（ミリ秒単位）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
% Packet with less than 10 ms delay	遅延が 10 ミリ秒未満のパケットのパーセンテージ。
% Packet with more than 10 < 20 ms delay	遅延が 10 ミリ秒よりも大きく 20 ミリ秒未満のパケットのパーセンテージ。
% Packet with more than 20 < 40 ms delay	遅延が 20 ミリ秒よりも大きく 40 ミリ秒未満のパケットのパーセンテージ。
% Packet with more than 40 ms delay	遅延が 40 ミリ秒よりも大きいパケットのパーセンテージ。
Packet Loss Ratio	失われたパケットの割合。
Total Packet Count	パケットの総数。
Roaming Count	この 90 秒間のメトリック ページでローミング ネゴシエーションのために交換されたパケットの数。
Roaming Delay	ローミング遅延（ミリ秒単位）。

アクセス ポイントの 802.11 カウンタのモニタリング

MAC レイヤでのアクセス ポイントのカウンタが表示されます。エラー フレーム、フラグメント数、RTS/CTS フレーム数、再試行フレームなどの統計情報は、フィルタリング基準に基づいて生成され、MAC 層のパフォーマンス（および問題）を解釈するために役立ちます。

802.11 Counters レポートの詳細については、「レポートの設定および管理」（P.14-774）を参照してください。

アクセス ポイントの AP プロファイル ステータスのモニタリング

アクセス ポイントの負荷、ノイズ、干渉、およびカバレッジ プロファイル ステータスが表示されます。

AP Profile Status レポートの詳細については、「レポートの設定および管理」（P.14-774）を参照してください。

アクセス ポイントの無線使用率のモニタリング

Radio Utilization レポートの詳細については、「レポートの設定および管理」（P.14-774）を参照してください。

アクセス ポイントのトラフィック ストリーム メトリックのモニタリング

指定したクライアントの現在および過去の Quality of Service（QoS）を無線レベルで判断する場合に役立ちます。また、パケット損失率、平均キューイング遅延、遅延パケットの配布、ローミング遅延などのアップリンクおよびダウンリンク統計情報も表示されます。

Traffic Stream Metrics レポートの詳細については、「レポートの設定および管理」（P.14-774）を参照してください。

アクセス ポイント送信電力とチャネルのモニタリング

Tx Power and Channel レポートの詳細については、「レポートの設定および管理」（P.14-774）を参照してください。

Current Tx Power Level 設定は、最大伝導送信電力を制御します。最大使用可能送信電力は、設定されたチャネル、個々の国の規制、およびアクセス ポイントの機能に応じて異なります。アクセス ポイントの機能を確認するには、『*Product Guide*』または www.cisco.com にある各モデルのデータ シートを参照してください。

Current Tx Power Level 設定 1 は、アクセス ポイントの最大伝導電力設定を表します。以降の電力レベル（たとえば、2、3、4 など）は、直前の電力レベルからの約 50 %（または 3dBm）の送信電力の低下を表します。

（注） 実際の電力低下は、アクセス ポイントのモデルによって若干異なります。

設定されたアンテナのゲイン、設定されたチャネル、および設定された電力レベルに基づき、特定の国の規制を超えないように、アクセス ポイントでの実際の送信電力が低減されることがあります。

（注） 割り当て方式に Global と Custom のいずれを選択したかにかかわらず、アクセス ポイントでの実際の伝導送信電力は、国固有の規制を超えないように確認されます。

コマンド ボタン

- [Save]：現在の設定を保存します。
- [Audit]：このアクセス ポイントの現在のステータスを検出します。

VoIP コールのモニタリング

VoIP コール レポートは、ネットワーク上の VoIP コール（無線ごと）の数と期間の詳細を時間とともに表示するなど、音声の観点からワイヤレス ネットワークの使用状況を分析するために役立ちます。このレポートから有益なデータを収集するには、WLAN で VoIP スヌーピングが有効になっている必要があります。このレポートでは、グラフで情報が表示されます。

レポート ラウンチ パッドの [VoIP Calls Graph] をクリックして [VoIP Calls Graph Reports] ページを開きます。このページから、現在保存されているレポート テンプレートを有効、無効、削除、または実行できます。詳細については、「レポートの設定および管理」（P.14-774）を参照してください。

音声統計情報のモニタリング

Voice Statistics レポートは、ネットワーク上の音声クライアント、ボイス コール、ローミング コール、および拒否されたコール（無線ごと）によって使用された帯域幅のパーセンテージなどの詳細を表示することで、音声の観点からワイヤレス ネットワークの使用状況を分析するために役立ちます。このレポートから有用なデータを収集するためには、コール アドミッション制御（CAC）が音声クライアントでサポートされていることを確認してください。詳細については、「レポートの設定および管理」（P.14-774）を参照してください。

電波品質のモニタリング

干渉の問題がネットワークに影響を与えている箇所を「一目で」理解できるように、Prime Infrastructure では、詳細な情報が、電波品質（AQ）と呼ばれる、概要的なわかりやすいメトリックにまとめられています。AQ はチャネル、フロア、およびシステム レベルで報告され、AQ が望ましいしきい値を下回った場合に自動的に通知されるように AQ アラートがサポートされています。詳細については、「CleanAir 電波品質イベントのモニタリング」（P.5-148）を参照してください。

アクセス ポイントの詳細のモニタリング

[Access Points Details] ページでは、1 つのアクセス ポイントのアクセス ポイント情報を参照できます。

このページにアクセスするには、[Monitor] > [Access Points] を選択し、[AP Name] 欄で項目をクリックします。アクセス ポイントの種類に応じて、次のタブが表示されます。この項では、各 [Access Points Details] ページのタブについて詳しく説明します。内容は次のとおりです。

- 「[General] タブ」（P.5-57）
- 「[Interfaces] タブ」（P.5-63）
- 「[Mesh Statistics] タブ」（P.5-79）
- 「[Mesh Links] タブ」（P.5-83）
- 「[CDP Neighbors] タブ」（P.5-65）
- 「[Current Associated Clients] タブ」（P.5-66）
- 「[SSID] タブ」（P.5-67）
- 「[Clients Over Time] タブ」（P.5-67）

[General] タブ

（注）　[General] タブのフィールドは、Lightweight アクセス ポイントと Autonomous アクセス ポイントで異なります。

ここでは、次の内容について説明します。

- 「[General]：Lightweight アクセス ポイント」（P.5-57）
- 「[General]：Autonomous」（P.5-61）

[General]：Lightweight アクセス ポイント

表 5-48 に、[General (for Lightweight Access Points)] タブのフィールドの一覧を示します。

表 5-48　[General (for Lightweight Access Points)] タブのフィールド

フィールド	説明
General	
AP Name	オペレータが定義したアクセス ポイント名。
AP IP address、Ethernet MAC address、および Base Radio MAC address	IP アドレス、イーサネット MAC アドレス、および無線 MAC アドレス。
Country Code	サポートされる国コード。1 台のコントローラで最大 20 の国をサポートできます。 （注）　運用する国向けに設計されていない場合、アクセス ポイントは正しく動作しない可能性があります。製品ごとにサポートされる国コードの完全なリストについては、次の URL を参照してください。 http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html.
Link Latency Settings	コントローラでリンク遅延を設定して、アクセス ポイントおよびコントローラの間のリンクを計測できます。詳細については、「アクセス ポイントのリンク遅延の設定」（P.9-514）を参照してください。 – [Current Link Latency (in msec)]：アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間のハートビート パケットの現在のラウンドトリップ時間（ミリ秒）。 – [Minimum Link Latency (in msec)]：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間のハートビート パケットの最短ラウンドトリップ時間（ミリ秒）。 – [Maximum Link Latency (in msec)]：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間のハートビート パケットの最長ラウンドトリップ時間（ミリ秒）。
LWAPP/CAPWAP Uptime	LWAPP/CAPWAP 接続がアクティブになっていた時間が表示されます。

表 5-48　[General (for Lightweight Access Points)] タブのフィールド （続き）

フィールド	説明
LWAPP/CAPWAP Join Taken Time	LWAPP/CAPWAP 接続が参加していた時間が表示されます。
Admin Status	アクセス ポイントの管理状態が、有効または無効で表示されます。
AP Mode	
Local	デフォルト モード。設定したチャネルをスキャンしてノイズと不正を探す間、データ クライアントにサービスが提供されます。アクセス ポイントは 50 ミリ秒間、チャネルの不正をリッスンします。Auto RF 設定の下で指定された期間の間、各チャネルを巡回します。 （注）　Local または FlexConnect アクセス ポイントで Cisco Adaptive wIPS 機能を設定するには、[Local] または [FlexConnect] を選択し、[Enhanced wIPS Engine Enabled] チェックボックスをオンにします。
Monitor	無線受信専用モード。アクセス ポイントは、設定されたすべてのチャネルを 12 秒ごとにスキャンします。このように設定されたアクセス ポイントでは、認証解除のパケットだけが無線で送信されます。モニタ モード アクセス ポイントは、不正アクセス ポイントにクライアントとして接続できます。 （注）　アクセス ポイントで Cisco Adaptive wIPS 機能を設定するには、[Monitor] を選択します。[Enhanced wIPS Engine Enabled] チェックボックスをオンにして、[Monitor Mode Optimization] ドロップダウン リストから [wIPS] を選択します。アクセス ポイントで wIPS モードを有効にする前に、アクセス ポイントの無線を無効にする必要があります。アクセス ポイントの無線を無効にしないと、エラー メッセージが表示されます。 （注）　アクセス ポイントで wIPS を有効にした後、無線を再度有効にします。
Rogue Detector	アクセス ポイントの無線がオフに切り替わり、アクセス ポイントは有線トラフィックだけをリッスンします。このモードで動作するコントローラは、不正アクセス ポイントをモニタします。コントローラはすべての不正アクセス ポイントとクライアントの MAC アドレスのリストを不正検出器に送信して、不正検出器がこの情報を WLC に転送します。MAC アドレスの一覧が、WLC アクセス ポイントがネットワーク上で取得した内容と比較されます。MAC アドレスが一致する場合は、どの不正アクセス ポイントが有線ネットワークに接続されるかを判別できます。
Sniffer	アクセス ポイントは特定チャネル上のすべてのパケットを取得して、AiroPeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。この機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合のみ有効にできます。

表 5-48　[General (for Lightweight Access Points)] タブのフィールド （続き）

フィールド	説明
FlexConnect	FlexConnect アクセス ポイントは、コントローラへの接続を失ったとき、クライアント データ トラフィックをローカルにスイッチングし、クライアント認証をローカルで実行できます。 （注）　OfficeExtend アクセス ポイントを設定するには、[FlexConnect] を選択する必要があります。AP モードが FlexConnect の場合、FlexConnect の設定オプションが表示されます。これには、OfficeExtend AP を有効にするオプションと、Least Latency Controller Join を有効にするオプションが含まれます。
Bridge	これは、Autonomous アクセス ポイントが無線クライアントのように機能して、Lightweight アクセス ポイントに接続する特殊なモードです。AP モードが [Bridge] に設定され、アクセス ポイントがブリッジ対応である場合、ブリッジとその有線クライアントは、Prime Infrastructure にクライアントとしてリストされます。
Spectrum Expert	このモードでは、CleanAir 対応のアクセス ポイントを、すべてのモニタ対象チャネル上の干渉源検出のために広範囲に使用できます。IDS スキャンや Wi-Fi などのその他の機能はすべて一時停止されます。
Enhanced wIPS Engine	[Enabled] または [Disabled] のいずれかが設定され、Cisco Adaptive wIPS 機能を使用したセキュリティ攻撃のモニタが可能となります。
Operational Status	[Registered] または [Not Registered] のいずれかとなり、コントローラで決定されます。
Registered Controller	アクセス ポイントが登録されているコントローラ。登録済みのコントローラの詳細を表示します。詳細については、「Monitoring System Summary」（P.5-3）を参照してください。
Primary Controller	このアクセス ポイントのプライマリ コントローラの名前。
Port Number	アクセス ポイントのプライマリ コントローラの SNMP 名。アクセス ポイントは、すべてのネットワーク操作について、ハードウェア リセットが発生した場合、このコントローラに最初にアソシエートしようとします。
AP Uptime	アクセス ポイントがアクティブで送受信できる状態になっている時間を表示します。
Map Location	アクセス ポイントのカスタマー定義の場所名。クリックするとマップ上で実際の場所が表示されます。詳細は、[Monitor] > [Access Points] > [*name*] > [Map Location] の順に選択してください。
Google Earth Location	Google Earth の場所が割り当てられているかどうかを示します。
Location	アクセス ポイントが配置されている物理的な場所（または Unassigned）。
Statistics Timer	このカウンタは、アクセス ポイントがその DOT11 統計情報をコントローラに送信する時間を秒単位で設定します。

表 5-48　[General (for Lightweight Access Points)] タブのフィールド （続き）

フィールド	説明
PoE Status	アクセス ポイントの Power over Ethernet ステータス。可能な値は次のとおりです。 – [Low] : イーサネットから供給されるアクセス ポイントの電力が低い。 – [Lower than 15.4 volts] : イーサネットから供給されるアクセス ポイントの電力が 15.4 V 未満。 – [Lower than 16.8 volts] : イーサネットから供給されるアクセス ポイントの電力が 16.8 V 未満。 – [Normal] : アクセス ポイントの操作に十分な電力が供給されている。 – [Not Applicable] : 電源がイーサネットではない。
Rogue Detection	不正検出が有効になっているかどうかを示します。 （注）　家庭環境に導入されるアクセス ポイントは、多数の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出は自動的に無効にされます。OfficeExtend アクセス ポイントの詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。
OfficeExtend AP	アクセス ポイントが OfficeExtend アクセス ポイントとして有効になっているかどうかを示します。デフォルトは [Enabled] です。
Encryption	暗号化が有効になっているかどうかを示します。 （注）　暗号化機能を有効または無効にすると、アクセス ポイントがリブートし、クライアントの接続が失われます。 （注）　DTLS データ暗号化は、セキュリティを維持するため、OfficeExtend アクセス ポイントで自動的に有効になります。暗号化は、Plus ライセンスが設定された 5500 シリーズ コントローラにアクセス ポイントが接続されている場合のみ使用できます。
Least Latency Join	アクセス ポイントは、プライオリティ順序検索（プライマリ、セカンダリ、ターシャリ コントローラ）から、遅延測定値が最善（最短遅延）のコントローラの検索に切り替えます。遅延が最短のコントローラが、最善のパフォーマンスを提供します。
Telnet Access	Telnet アクセスが有効になっているかどうかを示します。
SSH Access	SSH が有効になっているかどうかを示します。 （注）　OfficeExtend アクセス ポイントは、デフォルトのパスワードがアクセス ポイントで使用されている場合に外部アクセスを許可する可能性がある WAN に直接接続されていることがあります。このため、Telnet と SSH アクセスは、OfficeExtend アクセス ポイントでは自動的に無効になります。
Versions	
Software Version	現在コントローラで実行されているコードのオペレーティング システムの release.version.dot.maintenance 番号。
Boot Version	オペレーティング システム ブートローダのバージョン番号。
Inventory Information	

表 5-48　[General (for Lightweight Access Points)] タブのフィールド （続き）

フィールド	説明
AP Type	アクセス ポイントの種類
AP Model	アクセス ポイントのモデル番号。
Cisco IOS Version	Cisco IOS Release の詳細。
AP Certificate Type	Self Signed または Manufacture Installed のいずれか。
FlexConnect Mode Supported	FlexConnect モードがサポートされているかどうかを示します。
[wIPS Profile]（該当する場合）	
Profile Name	ユーザ定義プロファイル名をクリックすると、wIPS プロファイルの詳細が表示されます。
Profile Version	
Unique Device Identifier (UDI)	
Name	アクセス ポイントの Cisco AP の名前。
Description	アクセス ポイントの説明。
Product ID	注文可能な製品 ID
Version ID	製品 ID のバージョン
Serial Number	一意の製品シリアル番号
Run Ping Test Link	クリックするとアクセス ポイントに ping が実行されます。結果はポップアップ ダイアログボックスに表示されます。
Alarms Link	クリックすると、このアクセス ポイントに関連付けられたアラームが表示されます。
Events Link	クリックすると、このアクセス ポイントに関連付けられたイベントが表示されます。
Cable Modem Stats	AP1552C AP のケーブル モデムの稼働状態をモニタするには、このリンクをクリックします。詳細については、「ケーブル モデムの統計情報」（P.5-63）を参照してください。

[General] : Autonomous

（注）　自律クライアントについては、Prime Infrastructure はクライアント数のみを収集します。[Monitor] ページとレポートのクライアント数には、自律クライアントが含まれています。クライアント検索、クライアント トラフィック グラフ、その他のクライアント レポート（Unique Clients、Busiest Clients、Client Association など）には、Autonomous アクセス ポイントからのクライアントは含まれ*ていません*。

表 5-49 に、[General (for Autonomous Access Points)] タブのフィールドの一覧を示します。

表 5-49　[General (for Autonomous Access Points)] タブのフィールド

フィールド	説明
AP Name	オペレータが定義したアクセス ポイント名。
AP IP address and Ethernet MAC address	アクセス ポイントの IP アドレス、イーサネット MAC アドレス。

表 5-49　[General (for Autonomous Access Points)] タブのフィールド （続き）

フィールド	説明
AP UpTime	アクセス ポイントが送受信できる状態になっている時間（日、時間、分、秒）を示します。
Map Location	アクセス ポイントのカスタマー定義の場所名。クリックするとマップ上で実際の場所が表示されます。詳細については、「マップのモニタリング」（P.6-153）を参照してください。
WGB Mode	アクセス ポイントがワーク グループ ブリッジ モードかどうかを示します。
SNMP Info	
SysObjectId	システム オブジェクト ID。
SysDescription	システム デバイスの種類とファームウェアの現在のバージョン。
SysLocation	デバイスが設置されている建物の名前や部屋など、デバイスの物理的な場所。
SysContact	デバイスを担当するシステム管理者の名前。
Versions	
Software Version	現在コントローラで実行されているコードのオペレーティング システムの release.version.dot.maintenance 番号。
CPU Utilization	指定した期間の最大、平均、および最小 CPU 使用率が表示されます。
Memory Utilization	指定した期間の最大、平均、および最小メモリ使用率が表示されます。
Inventory Information	
AP Type	autonomous または lightweight。
AP Model	アクセス ポイントのモデル番号。
AP Serial Number	このアクセス ポイントの一意のシリアル番号。
FlexConnect Mode Supported	FlexConnect モードがサポートされているかどうか。
Unique Device Identifier (UDI)	
Name	アクセス ポイントの Cisco AP の名前。
Description	アクセス ポイントの説明。
Product ID	注文可能な製品 ID
Version ID	製品 ID のバージョン
Serial Number	一意の製品シリアル番号

（注）　メモリと CPU 使用率のグラフが表示されます。

（注）　[Alarms] をクリックすると、このアクセス ポイントに関連付けられたアラームが表示されます。[Events] をクリックすると、このアクセス ポイントに関連付けられたイベントが表示されます。

ケーブル モデムの統計情報

[General] タブで、[Cable Modem Stats] リンクをクリックします。以下の 2 個のタブが表示されます。

- [Statistics]：このタブには次のプロパティが表示されます。
  - ケーブル モデムの MAC アドレス
  - ケーブル モデムのシリアル番号
  - メッシュ AP MAC アドレス
  - ケーブル モデムの状態
  - ダウン ストリーム受信周波数（Hz）
  - アップ ストリームに送信周波数（Hz）
  - ダウン ストリーム受信電力信号レベル（dBmV）
  - アップ ストリーム送信電力信号レベル（dBmV）
  - アップ ストリーム搬送波対雑音比（dB）
- [Event Logs]：このタブは、ケーブル モデムによって生成されたイベントを表示します。

[Interfaces] タブ

表 5-50 に、[Interfaces] タブのフィールドの一覧を示します。

表 5-50　[Interfaces] タブのフィールド

フィールド	説明
Interface	
Admin Status	イーサネット インターフェイスが有効になっているかどうかを示します。
Operational Status	イーサネット インターフェイスが動作可能かどうかを示します。
Rx Unicast Packets	受信したユニキャスト パケットの数を示します。
Tx Unicast Packets	送信したユニキャスト パケットの数を示します。
Rx Non-Unicast Packets	受信した非ユニキャスト パケットの数を示します。
Tx Non-Unicast Packets	送信した非ユニキャスト パケットの数を示します。
Radio Interface	
Protocol	802.11a/n または 802.11b/g/n。
Admin Status	アクセス ポイントが有効であるか無効であるかを示します。
CleanAir Capable	アクセス ポイントが CleanAir を使用できるかどうかを示します。
CleanAir Status	CleanAir のステータスを示します。
Channel Number	Cisco 無線がブロードキャストしているチャネルを示します。
Extension Channel	Cisco 無線がブロードキャストしているセカンダリ チャネルを示します。

表 5-50　[Interfaces] タブのフィールド （続き）

フィールド	説明
Power Level	アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。
Channel Width	この無線インターフェイスのチャネル帯域幅を示します。チャネル帯域幅の設定の詳細については、「802.11a/n RRM 動的チャネル割り当ての設定」（P.9-422）を参照してください。 最小（デフォルト）設定は 20 MHz です。最大設定は、この無線でサポートされている最大チャネル幅です。
Antenna Name	アンテナの種類を示します。

インターフェイス名をクリックするとそのプロパティが表示されます（表 5-51 を参照）。

表 5-51　インターフェイスのプロパティ

フィールド	説明
AP Name	アクセス ポイントの名前。
Link speed	インターフェイスの速度を Mbps 単位で示します。
RX Bytes	インターフェイス上で受信したエラーのないパケットの総バイト数を示します。
RX Unicast Packets	インターフェイス上で受信したユニキャスト パケットの総数を示します。
RX Non-Unicast Packets	インターフェイス上で受信した非ユニキャストまたはマルチキャスト パケットの総数を示します。
Input CRC	インターフェイス上で受信したパケット内の CRC エラーの総数を示します。
Input Errors	インターフェイスでの受信中に発生した、パケットのすべてのエラーの合計を示します。
Input Overrun	入力レートがレシーバのデータ処理能力を超えたために、レシーバ ハードウェアが受信データをハードウェア バッファに送信できなかった回数を示します。
Input Resource	インターフェイス上で受信したパケット内のリソース エラーの総数を示します。
Runts	メディアの最小パケット サイズよりも小さいために廃棄されたパケット数を示します。
Throttle	インターフェイスが、送信中のパケットが多すぎるため、配信速度を落とすように、送信 NIC にアドバイスを送信した合計回数を示します。
Output Collision	イーサネット コリジョンにより再送信したパケットの総数を示します。
Output Resource	インターフェイス上で送信したパケットのリソース エラーの総数を示します。
Output Errors	最終的にインターフェイスからのパケットの送信ができなかった原因となるエラーの合計数を示します。
Operational Status	AP 上の物理イーサネット インターフェイスの動作状態を示します。

表 5-51　インターフェイスのプロパティ （続き）

フィールド	説明
Duplex	インターフェイスのデュプレックス モードを示します。
TX Bytes	インターフェイス上で送信したエラーのないパケットの総バイト数を示します。
TX Unicast Packets	インターフェイス上で送信したユニキャスト パケットの総数を示します。
TX Non-Unicast Packets	インターフェイス上で送信した非ユニキャストまたはマルチキャスト パケットの総数を示します。
Input Aborts	インターフェイス上で受信中に中断されたパケットの総数を示します。
Input Frames	インターフェイス上で受信した、CRC エラーがあり、オクテット数が整数でないパケットの総数を示します。
Input Drops	インターフェイス上での受信中に、キューが一杯だったためにドロップされたパケットの総数を示します。
Unknown Protocol	不明なプロトコルが原因でインターフェイス上で廃棄されたパケットの総数を示します。
Giants	メディアの最大パケット サイズを超過したために廃棄されたパケット数を示します。
Interface Resets	インターフェイスが完全にリセットされた回数を示します。
Output No Buffer	バッファ領域がなかったために廃棄されたパケットの総数を示します。
Output Underrun	ルータの処理能力を超えた速度でトランスミッタが動作した回数を示します。
Output Total Drops	インターフェイスからの送信中に、キューが一杯だったためにドロップされたパケットの総数を示します。

[CDP Neighbors] タブ

表 5-52 に、[CDP Neighbors] タブのフィールドの一覧を示します。

（注）　このタブは、CDP が有効になっている場合のみ表示されます。

表 5-52　[CDP Neighbors] タブのフィールド

フィールド	説明
AP Name	アクセス ポイントに割り当てられている名前。
AP IP Address	アクセス ポイントの IP アドレス。
Port No	アクセス ポイントに接続されているか割り当てられているポート番号。
Local Interface	ローカル インターフェイスを示します。
Neighbor Name	隣接するシスコ デバイスの名前。
Neighbor Address	隣接するシスコ デバイスのネットワーク アドレス。
Neighbor Port	隣接するシスコ デバイスのポート。

表 5-52　[CDP Neighbors] タブのフィールド （続き）

フィールド	説明
Duplex	全二重なのか半二重なのかを示します。
Interface Speed	インターフェイスが動作している速度。

[Current Associated Clients] タブ

表 5-53 に、[Current Associated Clients] タブのフィールドの一覧を示します。

（注）　このタブは、AP（CAPWAP または Autonomous AP）に関連付けられているクライアントがある場合にのみ表示されます。

表 5-53　[Current Associated Clients] タブのフィールド

フィールド	説明
Username	ユーザ名をクリックすると、このクライアントの [Monitor Client Details] ページが表示されます。詳細については、「クライアントとユーザのモニタリング」（P.10-567）を参照してください。
IP Address	関連付けられているクライアントの IP アドレス。
Client MAC Address	クライアントの MAC アドレスをクリックすると、このクライアントの [Monitor Client Details] ページが表示されます。詳細については、「クライアントとユーザのモニタリング」（P.10-567）を参照してください。
Association Time	アソシエーションの日時。
UpTime	アソシエーションの継続時間。
SSID	ユーザ定義の SSID 名。
SNR (dB)	関連付けられているクライアントの、信号対雑音比（dB 単位）。
RSSI	受信信号強度インジケータ（dBm）。
Bytes Tx	イーサネット インターフェイスをいずれかの方向に通過したデータの合計量を示します。
Bytes Rx	イーサネット インターフェイスでいずれかの方向で受信したデータの合計量を示します
アクセス ポイントがコントローラに関連付けられていない場合、コントローラ自身ではなく、データベースを使用してデータが取得されます。アクセス ポイントが関連付けられていない場合、次のフィールドが表示されます。	
User Name	クライアントのユーザ名。
IP Address	ローカル IP アドレス。
Client MAC Address	クライアントの MAC アドレス
Association Time	クライアント アソシエーションのタイムスタンプ。
Session Length	セッションの時間の長さ。
SSID	ユーザ定義の SSID 名。

表 5-53　[Current Associated Clients] タブのフィールド （続き）

フィールド	説明
Protocol	
Avg.Session Throughput	
Traffic (MB) as before	

（注）　[Current Associated Clients] テーブルの列を追加、削除、順序変更するには、[Edit View] リンクをクリックします。[Edit View] を使用した新しいフィールドの追加については、「アクセス ポイント リストの表示の設定」（P.5-45）を参照してください。

[SSID] タブ

表 5-54 に、[SSID] タブのフィールドの一覧を示します。

（注）　このタブは、アクセス ポイントが Autonomous AP であり、AP で SSID が設定されている場合のみ表示されます。

表 5-54　[SSID] タブ

フィールド	説明
SSID	アクセス ポイントの無線によってブロードキャストされているサービス セット ID。
SSID Vlan	アクセス ポイント上の SSID は、特定の VLAN ID または名前を認識するために設定されます。
SSID Vlan Name	アクセス ポイント上の SSID は、特定の VLAN ID または名前を認識するために設定されます。
MB SSID Broadcast	SSID ブロードキャストを無効にすると、ワイヤレス クライアントがすでに SSID を知っているか、AP の関連付けられたクライアントからのトラフィックをモニタまたは「スニフィング」しない限り、アクセス ポイントが基本的に認識不能になります。
MB SSID Time Period	この指定された期間中に SSID 内の内部通信が動作し続けます。

[Clients Over Time] タブ

このタブには、次のグラフが表示されます。

- [Client Count on AP]：アクセス ポイントに現在関連付けられているクライアントの総数が、時間とともに表示されます。
- [Client Traffic on AP]：AP に接続されているクライアントによって生成されたトラフィックが、時間とともに表示されます。

（注）　上記のグラフに表示される情報は、時間ベースのグラフに表示されます。時間ベースのグラフでは、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。詳細については、6-71 ページの「時間ベースのグラフ」の項を参照してください。

アクセス ポイントの無線の詳細のモニタリング

このページにアクセスするには、[Monitor] > [Access Points] の順に選択し、[Radio] 欄で項目をクリックします。

このページにアクセスするには、[Monitor] > [Maps] の順に選択し、[Name] 欄で項目をクリックし、アクセス ポイント アイコンをクリックします。

このページにアクセスするには、[Monitor] > [Access Points] の順に選択し、[AP Name] 欄の項目をクリックし、[AP Interfaces] タブで [802.11a] または [802.11b] または [802.11ac] をクリックします。このページでは、1 つの 802.11a または 802.11b/g Cisco 無線 のアクセス ポイント情報を参照できます。

デフォルトでは [On Demand Statistics] が表示されます。異なるビューを選択するには、[View] ドロップダウン リストを使用します。

- [On Demand Statistics] を表示するには、[On Demand Statistics] を選択し、[Go] をクリックします。詳細については、「オンデマンド統計情報のモニタリング」（P.5-68）を参照してください。
- [Operational Parameters] を表示するには、[Operational Parameters] を選択し、[Go] をクリックします。詳細については、「動作パラメータのモニタリング」（P.5-72）を参照してください。
- [802.11 MAC Counters] を表示するには、[802.11 MAC Counters] を選択し、[Go] をクリックします。詳細については、「802.11 MAC カウンタのモニタリング」（P.5-75）を参照してください。
- [View Alarms] を表示するには、[View Alarms] を選択し、[Go] をクリックします。詳細については、「アラーム表示のモニタリング」（P.5-77）を参照してください。
- [View Events] を表示するには、[View Events] を選択し、[Go] をクリックします。詳細については、「イベント表示のモニタリング」（P.5-77）を参照してください。

オンデマンド統計情報のモニタリング

アクセス ポイントのオンデマンド統計情報を表示するには、[Monitor] > [Access Points] ページで該当するアクセス ポイントの [Radio] をクリックします。[Radio Details] ページに、デフォルトでオンデマンド統計情報が表示されます。無線の詳細については、「アクセス ポイントの無線の詳細のモニタリング」（P.5-68）を参照してください。

（注）　また、[Radio Details] ページにあるドロップダウン リストから [On Demand Statistics] を選択することもできます。

このページでは、次のアクセス ポイントの 802.11a、802.11b、802.11ac の無線統計情報が、1 台のアクセス ポイントについて表示されます。

General

- [AP Name]：アクセス ポイントの詳細を表示する場合にクリックします。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。

- AP MAC Address
- Radio
- [CleanAir Capable]：アクセス ポイントが CleanAir 対応かどうかを示します。
- [AP in SE-Connect Mode]：[Yes] または [No] です。アクセス ポイントが SE-Connect モードで接続されているかどうかを示します。
- [CleanAir Enabled]：アクセス ポイントで CleanAir が有効になっているかどうかを示します。
- [CleanAir Sensor Status]：CleanAir センサーの動作ステータス（[Up] または [Down]）を示します。
- [Admin Status]：有効または無効。
- [Operational Status]：Cisco Radio の動作ステータス（[Up] または [Down]）を表示します。
- [Controller]：コントローラ システムの詳細を表示する場合にクリックします。詳細については、「Monitoring System Summary」（P.5-3）を参照してください。
- [Channel]：Cisco 無線がブロードキャストしているチャネル。
- [Extension Channel]：Cisco Radio がブロードキャストしているセカンダリ チャネルを示します。
- [Channel Width]：この無線インターフェイスのチャネル帯域幅を示します。チャネル帯域幅の設定の詳細については、「802.11a/n RRM 動的チャネル割り当ての設定」（P.9-422）を参照してください。
- [Power Level]：アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。

  電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。
- [Port]：（1 ～ 24）アクセス ポイントが接続されているポート。
- [Map Location]：アクセス ポイントの場所を示すフロア マップを表示する場合にクリックします。

Management Frame Protection

- [Protection Capability]：すべてのフレーム
- [Validation Capability]：すべてのフレーム
- [MFP Version Supported]：サポートされ設定されている管理フレーム保護バージョン。

Profile Information

- [Noise Profile]：ノイズ プロファイルの状態が Success と Failure の間で変化したときに通知が送信されます。
- [Interference Profile]：干渉プロファイルの状態が Success と Failure の間で変化したときに通知が送信されます。
- [Load Profile]：ロード プロファイルの状態が Success と Failure の間で変化したときに通知が送信されます。
- [Coverage Profile]：カバレッジ プロファイルの状態が Success と Failure の間で変化したときに通知が送信されます。

（注）　関連付けられているアラームを表示するには、[Success] または [Failure] をクリックします。

Noise by Channel (dBm)

チャネルとノイズを示すグラフ。

Interference by Channel (dBm%)

チャネルごとの干渉のパーセンテージを示すグラフ。

（注）　チャネル使用率は、受信電力（RX）+ 送信電力（TX）+ 干渉の組み合わせです。
Interference : 干渉する 802.11 の送信に占められているメディアのパーセンテージに関するアクセス ポイント レポート（これは、外部 AP に加えて非ネイバーからの重複する信号による場合があります）。

（注）　モニタ間隔の下の [channel scan duration] フィールドを使用して、チャネル リスト（[RRM] ページから設定します）が完全にスキャンされます。たとえば、2.4 GHz の 11 チャネルすべてをスキャンし、デフォルトの期間（180 秒）を使用する場合、スキャンする各チャネルの間隔が約 180/11 = 16.36 秒になります。

Load Statistics

- [RX Utilization] : 0 ～ 100 % の 802.11a または 802.11b/g RF の RF 受信使用率のしきい値。
- [TX Utilization] : 0 ～ 100 % の 802.11a または 802.11b/g RF の RF 送信使用率のしきい値。
- [Channel Utilization] : 0 ～ 100 % の 802.11a の RF 使用率のしきい値（実際およびしきい値のサブカラム）。
- [Attached Client Count] : 接続されているクライアントの総数。

[General] タブ

ここでは、[General] タブに表示される情報について説明します。内容は次のとおりです。

- 「% Client Count by RSSI」（P.5-70）
- 「% Client Count by SNR」（P.5-70）
- 「Channel Utilization (% Busy)」（P.5-70）
- 「Noise by Channel(dBm)」（P.5-71）
- 「Rx Neighbors」（P.5-71）
- 「Channel Utilization Statistics」（P.5-71）

% Client Count by RSSI

% および受信信号強度インジケータが表示されたグラフ。

% Client Count by SNR

% および信号対雑音比が表示されたグラフ。

Channel Utilization (% Busy)

チャネル番号が X 軸に表示され、チャネル使用率が Y 軸に表示されたグラフ。

Noise by Channel(dBm)

チャネルが X 軸に表示され、電力が dBm 単位で Y 軸に表示されたグラフ。

Rx Neighbors

- Radio MAC Address
- [AP Name]：クリックするとアクセス ポイントの詳細が表示されます。
- [Map]：クリックするとマップが表示されます。
- Mobility Group-Leader IP Address
- Neighbor Channel
- Channel Bandwidth
- RSSI (dBm)

Channel Utilization Statistics

- Time
- [Picc]：共通チャネル AP およびクライアントからの受信フレームによって消費された時間のパーセンテージ。
- [Pib]：正しく復調できないチャネル上の干渉によって消費された時間のパーセンテージ。

（注）　Picc と Pib の値は、チャネルの干渉によってアクセス ポイントがビジーである時間のパーセンテージを示す適切な指標です。

Client Count Over last 24 Hrs

このグラフには、AP 無線固有のクライアント数（過去 24 時間）が表示されます。

[CleanAir] タブ

ここでは、[CleanAir] タブに表示される情報について説明します。内容は次のとおりです。

- 「Air Quality」（P.5-71）
- 「Interference Power」（P.5-71）
- 「Non-WiFi Channel Utilization」（P.5-72）
- 「Active Interferers」（P.5-72）
- 「[View] ドロップダウン リスト」（P.5-72）

Air Quality

このグラフには、ワイヤレス ネットワークの電波品質の指標が表示されます。値 100 は、電波品質が最良であることを示し、値 1 は干渉が最大であることを示します。

Interference Power

このグラフには、チャネル番号に対して干渉するデバイスの干渉電力が表示されます。

Non-WiFi Channel Utilization

このグラフには、ワイヤレス ネットワークの非 Wi-Fi チャネル使用率が表示されます。

Active Interferers

このセクションには、ワイヤレス ネットワークに対するアクティブな干渉源の詳細が表示されます。次の詳細を使用できます。

- [Interferer Name]：干渉デバイスの名前。
- [Affected Channels]：干渉デバイスが影響を与えているチャネル。
- [Detected Time]：干渉源が検出された時刻。
- [Severity]：干渉デバイスの重大度インデックス。
- [Duty Cycle(%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- [RSSI(dBm)]：干渉しているデバイスの受信信号強度。

[View] ドロップダウン リスト

- このアクセス ポイントの無線の [On Demand Statistics] を表示するには、[On Demand Statistics] を選択し、[Go] をクリックします。詳細については、「オンデマンド統計情報のモニタリング」（P.5-68）を参照してください。
- このアクセス ポイントの無線の [Operational Parameters] を表示するには、[Operational Parameters] を選択し、[Go] をクリックします。詳細については、「動作パラメータのモニタリング」（P.5-72）を参照してください。
- このアクセス ポイントの無線の [802.11 MAC Counters] を表示するには、[802.11 MAC Counters] を選択し、[Go] をクリックします。詳細については、「802.11 MAC カウンタのモニタリング」（P.5-75）を参照してください。
- このアクセス ポイントの無線のアラームを表示するには、[View Alarms] を選択し、[Go] をクリックします。詳細については、「アラーム表示のモニタリング」（P.5-77）を参照してください。
- このアクセス ポイントの無線のイベントを表示するには、[View Events] を選択し、[Go] をクリックします。詳細については、「イベント表示のモニタリング」（P.5-77）を参照してください。

動作パラメータのモニタリング

アクセス ポイントの無線の動作パラメータを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択し、該当するアクセス ポイントの無線をクリックします。

ステップ 2　[View] ドロップダウン リストから、[Operational Parameters] を選択します。

ステップ 3　[Go] をクリックします。

このページでは、1 つの 802.11a または 802.11b のシスコの無線の設定情報を参照できます。

General

- [AP Name]：アクセス ポイントの詳細を表示する場合にクリックします。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。

- AP MAC Address
- Radio
- [Admin Status]：有効または無効。
- [Operational Status]：Cisco Radio の動作ステータス（[Up] または [Down]）を表示します。
- [Controller]：コントローラ システムの詳細を表示する場合にクリックします。詳細については、「Monitoring System Summary」（P.5-3）を参照してください。
- [Channel]：Cisco 無線がブロードキャストしているチャネル。
- [Extension Channel]：Cisco Radio がブロードキャストしているセカンダリ チャネルを示します。
- [Channel Width]：この無線インターフェイスのチャネル帯域幅を示します。チャネル帯域幅の設定の詳細については、「802.11a/n RRM 動的チャネル割り当ての設定」（P.9-422）を参照してください。
- [Power Level]：アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。

  電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。
- [Port]：（1 ～ 24）アクセス ポイントが接続されているポート。
- [Map Location]：アクセス ポイントの場所を示すフロア マップを表示する場合にクリックします。

Station Configuration Parameters

- [Configuration Type]：Automatic または Custom です。
- [Number of WLANs]：デフォルトでは 1 です。
- [Medium Occupancy Limit]：ポイント コーディネータが、1 つ以上の DCF のインスタンスがメディアにアクセスするのに十分な時間制御を放棄せずに、ワイヤレス メディアの使用を制御する可能性がある最大時間を、TU 単位で示します。デフォルト値は 100 で、最大値は 1000 です。
- [CFP Period]：CFP の開始の間の DTIM 間隔の数。
- [CFP Max.Duration]：PCF によって生成される可能性がある、CFP の最大期間（TU 単位）。
- [BSSID]：アクセス ポイントの MAC アドレス。
- [Beacon Period]：アクセス ポイントによる SSID のブロードキャスト レート。100 ～ 600 ミリ秒。
- [DTIM Period]：DTIM Count フィールドが 0 の TIM 要素を含むビーコン フレームの送信の間に経過する、ビーコン間隔の数。この値は、ビーコン フレームの DTIM Period フィールドで送信されます。
- [Country String]：ステーションが動作している国を示します。この文字列の先頭の 2 オクテットは、2 文字の国コードです。

Physical Channel Parameters

- [Current Channel]：現在の動作周波数チャネル。
- [Configuration]：ローカル カスタマイズまたはグローバル制御。
- [Current CCA Mode]：動作中の CCA 方式。有効な値は、次のとおりです。
  - エネルギー検出のみ（edonly）= 01。
  - キャリア センスのみ（csonly）= 02。
  - キャリア センスとエネルギー検出（edandcs）= 04。

  - キャリア センスとタイマー（cswithtimer）= 08。
  - 高速キャリア センスとエネルギー検出（hrcsanded）=16。
- [ED/TI Threshold]：ビジー メディアを検出するために使用されているエネルギー検出としきい値（周波数）。CCA は、このしきい値を超える RSSI を検出するとビジー メディアを報告します。

Physical Antenna Parameters

- [Antenna Type]：Internal または External。
- [Diversity]：内部アンテナか、コネクタ A またはコネクタ B によって有効になります。（有効または無効）。

RF Recommendation Parameters

- [Channel]：802.11a Low Band、Medium Band、および High Band、802.11b/g。
- [Tx Power Level]：Radio Resource Management（RRM）が無効な場合は 0、Radio Resource Management（RRM）が有効な場合は 1 ～ 5。
- [RTS/CTS Threshold]：Radio Resource Management（RRM）が無効な場合は 0、Radio Resource Management（RRM）が有効な場合は 1 ～ 5。
- [Fragmentation Threshold]：Radio Resource Management（RRM）が無効な場合は 0。

MAC Operation Parameters

- [Configuration Type]：Automatic または Custom です。
- [RTS Threshold]：この属性は、これを下回った場合に RTS/CTS ハンドシェイクが実行されない、MPDU 内のオクテット数を示します。

  RTS/CTS ハンドシェイクは、すべてのフレーム交換シーケンスの開始時に、MPDU がデータまたは管理タイプで、MPDU の Address1 フィールドに個別のアドレスがあり、MPDU の長さがこのしきい値よりも長い場合に実行されます。この属性を最大 MSDU サイズよりも大きくすると、この STA によって送信される Data または Management タイプ フレームの RTS/CTS ハンドシェイクが無効になります。この属性に 0 を設定すると、この STA によって送信される Data または Management タイプのすべてのフレームで RTS/CTS ハンドシェイクが有効になります。この属性のデフォルト値は 2347 です。
- [Short Retry Limit]：長さが dot11RTSThreshold 以下のフレームの、障害状態と見なす前に行う最大送信試行回数。この属性のデフォルト値は 7 です。
- [Long Retry Limit]：長さが dot11RTSThreshold を超えるフレームの、障害状態と見なす前に行う最大送信試行回数。この属性のデフォルト値は 4 です。
- [Fragmentation Threshold]：PHY に配信される可能性がある MPDU の現在の最大サイズ（オクテット単位）。MAC ヘッダーとトレーラーを追加した後で、MSDU のサイズがこの属性値を超えている場合、フラグメントに分割されます。得られたフレームの Address1 フィールドに個別のアドレスがあり、フレームの長さがこのしきい値よりも長い場合、MSDU または MMPDU はフラグメント化されます。この属性のデフォルト値は、2346 または接続されている PHY の aMPDUMaxLength の小さい方になり、2346 と接続されている PHY の aMPDUMaxLength よりも小さい方よりも大きくなることはありません。この属性の値は、256 よりも小さくなることはありません。
- [Max Tx MSDU Lifetime]：MSDU の初回送信後、MSDU の以降の送信の試みを停止するまでの、TU 単位の経過時間。この属性のデフォルト値は 512 です。

- [Max Rx Lifetime] : MaxReceiveLifetime は、フラグメント化された MMPDU または MSDU の初回受信後、MMPDU または MSDU の以降の再構成の試みを停止するまでの、TU 単位の経過時間です。デフォルト値は 512 です。

Tx Power

- [# Supported Power Levels] : オペレータの設定に応じた、5 個以下の電力レベル。
- [Tx Power Level x] : アクセス ポイント送信電力レベル : 1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。

（注）　電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。

- [Tx Power Configuration] : グローバルに制御されるか、このアクセス ポイントに対してカスタマイズされるか（Custom または Global）。
- [Current Tx Power Level] : 送信電力テーブルから取得した動作送信電力レベルが表示されます。

802.11 MAC カウンタのモニタリング

アクセス ポイントの無線の動作パラメータを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択し、該当するアクセス ポイントの無線をクリックします。
ステップ 2　[View] ドロップダウン リストから、[802.11 MAC Counters] を選択します。
ステップ 3　[Go] をクリックします。

このページでは、1 つの 802.11a または 802.11b Cisco 無線 の 802.11 MAC カウンタ情報を参照できます。

General

- [AP Name] : アクセス ポイントの詳細を表示する場合にクリックします。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。
- AP MAC Address
- Radio
- [Admin Status] : 有効または無効。
- [Operational Status] : Cisco Radio の動作ステータス（[Up] または [Down]）を表示します。
- [Controller] : コントローラ システムの詳細を表示する場合にクリックします。詳細については、「Monitoring System Summary」（P.5-3）を参照してください。
- [Channel] : Cisco 無線がブロードキャストしているチャネル。
- [Extension Channel] : Cisco Radio がブロードキャストしているセカンダリ チャネルを示します。
- [Channel Width] : この無線インターフェイスのチャネル帯域幅を示します。チャネル帯域幅の設定の詳細については、「802.11a/n RRM 動的チャネル割り当ての設定」（P.9-422）を参照してください。

（注）　最小（デフォルト）設定は 20 MHz です。最大設定は、この無線でサポートされている最大チャネル幅です。

- [Power Level]：アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。

  電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。
- [Port]：（1 ～ 24）アクセス ポイントが接続されているポート。
- [Map Location]：アクセス ポイントの場所を示すフロア マップを表示する場合にクリックします。

RF Counters

- [Tx Fragment Count]：このカウンタは、種類が Data または Management の MPDU を正常に受信するたびに増加します。
- [Multicast Tx Frame Count]：このカウンタは、正常に送信した MSDU の宛先 MAC アドレス中でマルチキャスト ビットが設定されている場合に減少します。ESS で STA として動作している場合、これらのフレームはアクセス ポイントに送信されます。これは、関連付けられたすべての MPDU に対する確認応答を受信したことを示します。
- [Tx Failed Count]：このカウンタは、1 回以上の再送信の後で MSDU が正常に送信された場合に増分されます。
- [Retry Count]：このカウンタは、1 回以上の再送信の後で MSDU が正常に送信された場合に増分されます。
- [Multiple Retry Count]：このカウンタは、複数回の再送信の後で MSDU が正常に送信された場合に増分されます。
- [Frame Duplicate Count]：このカウンタは、Sequence Control フィールドで重複が示されているフレームを受信した場合に増分されます。
- [RTS Success Count]：このカウンタは、RTS への応答として CTS を受信したときに増分されます。
- [RTS Failure Count]：このカウンタは、RTS への応答として CTS を受信しなかったときに増分されます。
- [ACK Failure Count]：このカウンタは、期待したときに ACK を受信しなかった場合に増分されます。
- [Rx Fragment Count]：長さが 64 オクテット（フレーミング ビットは除外するが、FCS オクテットは含む）未満の受信済みパケットの総数。
- [Multicast Rx Framed Count]：このカウンタは、宛先 MAC アドレスにマルチキャスト ビットが設定された MSDU を受信したときに増加します。
- [FCS Error Count]：このカウンタは、受信した MPDU で FCS エラーが検出されたときに増分されます。
- [Tx Frame Count]：このカウンタは、MSDU を正常に送信するたびに増分されます。
- [WEP Undecryptable Count]：このカウンタは、Frame Control フィールドの WEP サブフィールドに 1 が設定され、AT MAC アドレスにマッピングされたキーの WEP On の値が、フレームを暗号化すべきでなかったことを示しているか、受信 STA がプライバシー オプションを実装していないためにフレームが廃棄されることを示している場合に増分されます。

アラーム表示のモニタリング

[Monitor Access Points] ページから [View Alarms] ページにアクセスするには、次の手順を実行します。

（注）　AP が関連付け解除されている場合、[Monitor] > [Access Points] ページで、無線ステータスが重大なステータスになっています。1 つのアラームのみがあり、AP が関連付け解除されています。これは、無線アラームが AP 関連付け解除アラームに関連付けられているためです。

（注）　コントローラがダウンした場合、コントローラ インベントリ ダッシュレットでコントローラのステータスが重大として表示されます。しかし、無線インベントリ ダッシュレットでは、最後の既知のステータスのままになります。[Monitor] > [Access Point] ページで、AP アラームのステータスが「Unknown」と表示されます。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントの [Radio Type] 欄で [Radio Type] を選択します。

ステップ 3　[View] ドロップダウン リストから、[View Alarms] を選択します。

ステップ 4　[Go] をクリックします。

アラーム表示の詳細については、「アラームのモニタリング」（P.5-127）を参照してください。

イベント表示のモニタリング

[Monitor Access Points] ページから [View Events] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントの [Radio Type] 欄で [Radio Type] を選択します。

ステップ 3　[View] ドロップダウン リストから、[View Events] を選択します。

ステップ 4　[Go] をクリックします。

イベント表示の詳細については、「イベントのモニタリング」（P.5-143）を参照してください。

サードパーティのアクセス ポイントのモニタリング

Prime Infrastructure では特定のサードパーティのアクセス ポイントのモニタリングをサポートします。

サードパーティ アクセス ポイントについて、次のパラメータがモニタリングされます。

- Current configuration of SSID
- Mode
- Current Channel
- Tx-Power
- RTS Threshold
- Retry Limit
- Preamble
- Beacon Interval
- Power management
- Load balance
- Rates
- DTIM Period
- LMS address
- Encryption
- Status
- Ageout
- MTU
- Location
- Hide SSID
- Deny Broadcast
- BG mode
- Radio Chipset
- Regulatory Domain
- Country Code
- Tx Rates

サードパーティ アクセス ポイントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Third Party Access Points] の順に選択します。

ステップ 2　[Third Party Access Point] ページで、アクセス ポイントの名前をクリックします。情報は、[General] タブに表示されます。

メッシュ アクセス ポイントのモニタリング

Mesh Health では、特に記載されている場合を除き、メッシュ アクセス ポイントとして設定されている場合、Cisco Aironet 1500 および 1520 シリーズの屋外アクセス ポイントと、Cisco Aironet 1130 および 1240 シリーズの屋内アクセス ポイントの全体的な状況をモニタします。この環境情報の追跡は、屋外に配置されたアクセス ポイントの場合、特に重要です。次のようなファクタがモニタされます。

- [Temperature] : アクセス ポイントの内部温度を華氏および摂氏で表示します（Cisco Aironet 1510 および 1520 屋外アクセス ポイントのみ）。
- [Heater Status] : ヒータのステータスをオン / オフで表示します（Cisco Aironet 1510 および 1520 屋外アクセス ポイントのみ）。
- [AP Up time] : アクセス ポイントがアクティブで送受信できる状態になっている時間を表示します。
- [LWAPP Join Taken Time] : LWAPP 接続の確立に要した時間を表示します（Cisco Aironet 1505 アクセス ポイントを除く）。
- [LWAPP Up Time] : LWAPP 接続アクティブとなっている時間を表示します（Cisco Aironet 1505 アクセス ポイントを除く）。

Mesh Health 情報は、メッシュ アクセス ポイントの [General Properties] ページに表示されます。

（注）　wIPS モードは、Cisco Aironet 1500 シリーズのメッシュ アクセス ポイントではサポートされません。

特定のメッシュ アクセス ポイントの Mesh Health の詳細を表示する手順は、次のとおりです。

ステップ 1　[Monitor] > [Access Points] の順に選択します。アクセス ポイントに属する無線の一覧が表示されます。

（注）　[Monitor] > [Access Points] の順に選択すると、無線のステータス（アクセス ポイントのステータスではありません）が表示されます。表示されるステータスは、トラップとワイヤレス ステータス ポーリングにより頻繁に更新され、実際の無線ステータスを反映するには数分かかります。アクセス ポイント全体のステータスは、マップ上のアクセス ポイントを参照することで見つかります。

（注）　[New Search] ボタンを使用しても、メッシュ アクセス ポイントの概要を表示できます。[New Search] オプションを使用すると、表示されるアクセス ポイントの基準をさらに定義できます。検索の基準は、AP Type、AP Mode、Radio Type、および 802.11n Support です。

ステップ 2　[AP Name] リンクをクリックして、メッシュ アクセス ポイントの詳細を表示します。そのメッシュ アクセス ポイントの [General] タブが表示されます。

（注）　Prime Infrastructure マップ ページからでも、メッシュ アクセス ポイントの [General] タブにアクセスすることができます。ページを表示するには、メッシュ アクセス ポイント ラベルをダブルクリックします。タブ付きのページが表示され、選択したアクセス ポイントの [General] タブが表示されます。

テーブルで列の追加、削除、または並べ替えを行うには、[Monitor] > [Access Points] ページの [Edit View] リンクをクリックします。

[Mesh Statistics] タブ

子メッシュ アクセス ポイントの認証の際、または子メッシュ アクセス ポイントの親メッシュ アクセス ポイントへのアソシエートの際に、メッシュの統計が報告されます。

子メッシュ アクセス ポイントがコントローラからのアソシエートを解除すると、セキュリティのエントリは削除され、表示されなくなります。

メッシュ アクセス ポイントに対して、次のメッシュ セキュリティの統計が表示されます。

- ブリッジング
- キュー
- セキュリティ

特定のメッシュ アクセス ポイントのメッシュ統計情報を表示する手順は、次のとおりです。

ステップ 1　[Monitor] > [Access Points] の順に選択します。アクセス ポイントに属する無線の一覧が表示されます。

（注）　[Monitor] > [Access Points] の順に選択すると、無線のステータス（アクセス ポイントのステータスではありません）が表示されます。表示されるステータスは、トラップとワイヤレス ステータス ポーリングにより頻繁に更新され、実際の無線ステータスを反映するには数分かかります。アクセス ポイント全体のステータスは、マップ上のアクセス ポイントを参照することで見つかります。

（注）　[New Search] ボタンを使用しても、アクセス ポイントの概要を表示できます。[New Search] オプションを使用すると、表示されるアクセス ポイントの基準をさらに定義できます。検索基準には、[AP Name]、[IP address]、[MAC address]、[Controller IP or Name]、[Radio type]、および [Outdoor area] が含まれます。

ステップ 2　目的のメッシュ アクセス ポイントの [AP Name] リンクをクリックします。

タブ付きのページが表示され、選択したアクセス ポイントの [General Properties] ページが表示されます。

ステップ 3　[Mesh Statistics] タブをクリックします。3 つのタブが付いた、[Mesh Statistics] ページが表示されます。

（注）　[Mesh Statistics] タブとその下位のタブ（[Bridging]、[Queue]、[Security]）は、メッシュ アクセス ポイントに対してだけ表示されます。[Mesh Link Alarms] および [Mesh Link Events] リンクは、3 つのタブ付きパネルのそれぞれからアクセスできます。関連するアラームとイベントを表示するには、これらのリンクをクリックします。

（注）　Prime Infrastructure マップからでも、メッシュ アクセス ポイントの [Mesh Securities] ページにアクセスすることができます。ページを表示するには、メッシュ アクセス ポイント ラベルをダブルクリックします。

表 5-55、表 5-56、および表 5-57 では、それぞれブリッジ、キュー、およびセキュリティの統計の概要とそれらの定義について説明しています。

表 5-55　ブリッジ メッシュ統計

フィールド	説明
Role	メッシュ アクセス ポイントの役割。オプションは、メッシュ アクセス ポイント（MAP）とルート アクセス ポイント（RAP）です。
Bridge Group Name	MAP または RAP がメンバーとなっているブリッジ グループの名前。ブリッジ グループ名の中でメンバーシップを割り当てることを推奨します。割り当てられていない場合、デフォルトでは、MAP はデフォルトのブリッジ グループ名に割り当てられます。
Backhaul Interface	メッシュ アクセス ポイントの無線バックホール。
Routing State	親の選択の状態。表示される値は、Seek、Scan、および Maint です。Maint は、親の選択が完了すると表示されます。

表 5-55　ブリッジ メッシュ統計 （続き）

フィールド	説明
Malformed Neighbor Packets	ネイバーから受信した不正な形式のパケットの数。不正な形式のパケットの例には、不正な形式のショート DNS パケットや不正な形式の DNS 応答といったトラフィックの悪意のあるフラッドがあります。
Poor Neighbor SNR	信号対雑音比がバックホール リンクで 12 dB 未満になった回数。
Excluded Packets	除外したネイバー メッシュ アクセス ポイントから受信したパケットの数。
Insufficient Memory	メモリ不足になった状態の数。
RX Neighbor Requests	ネイバー メッシュ アクセス ポイントから受信したブロードキャストおよびユニキャストの要求数。
RX Neighbor Responses	ネイバー メッシュ アクセス ポイントから受信した応答数。
TX Neighbor Requests	ネイバー メッシュ アクセス ポイントに送信したブロードキャストおよびユニキャストの要求数。
TX Neighbor Responses	ネイバーのメッシュ アクセス ポイントに送信された応答の数
Parent Changes	メッシュ アクセス ポイント（子）が別の親に移動した回数。
Neighbor Timeouts	ネイバー タイムアウト回数。
Node Hops	MAP と RAP 間のホップ カウント。値のリンクをクリックすると、レポート内容の詳細やノードのホップ値が更新される頻度を設定したり、レポートをグラフィカルに表示したりすることができるダイアログ ボックスが表示されます。

表 5-56　キュー メッシュ統計

フィールド	説明
Silver Queue	定義された統計期間中に Silver（ベスト エフォート）キューで待機していたパケットの平均および最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。
Gold Queue	定義された統計期間中に Gold（ビデオ）キューで待機していたパケットの平均および最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。
Platinum Queue	定義された統計期間中に Platinum（音声）キューで待機していたパケットの平均および最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。

表 5-56　キュー メッシュ統計 （続き）

フィールド	説明
Bronze Queue	定義された統計期間中に Bronze（バックグラウンド）キューで待機していたパケットの平均および最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。
Management Queue	定義された統計期間中に管理キューで待機していたパケットの平均および最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。

表 5-57　セキュリティ メッシュ統計

フィールド	説明
Packets Transmitted	選択したメッシュ アクセス ポイントがセキュリティ ネゴシエーションの際に送信したパケットの合計数。
Packets Received	選択したメッシュ アクセス ポイントがセキュリティ ネゴシエーションの際に受信したパケットの合計数。
Association Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生するアソシエーション要求のエラーの合計数。
Association Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生するアソシエーション要求のタイムアウトの合計数。
Association Request Success	選択したメッシュ アクセス ポイントとその親の間で発生する正常なアソシエーション要求の合計数。
Authentication Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生する認証要求のエラーの合計数。
Authentication Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生する認証要求のタイムアウトの合計数。
Authentication Request Success	選択したメッシュ アクセス ポイントとその親メッシュ ノードの間で発生する正常な認証要求の合計数。
Reassociation Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生する再アソシエーション要求のエラーの合計数。
Reassociation Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生する再アソシエーション要求のタイムアウトの合計数。
Reassociation Request Success	選択したメッシュ アクセス ポイントとその親の間で発生する正常な再アソシエーション要求の合計数。
Reauthentication Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生する再認証要求のエラーの合計数。

表 5-57　セキュリティ メッシュ統計 （続き）

フィールド	説明
Reauthentication Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生した再認証要求のタイムアウトの合計数。
Reauthentication Request Success	選択したメッシュ アクセス ポイントとその親の間で発生した正常な再認証要求の合計数。
Invalid Association Request	親メッシュ アクセス ポイントが選択した子メッシュ アクセス ポイントから受信する無効のアソシエーション要求の合計数。この状態は、選択した子が有効なネイバーであっても、アソシエーションが許可された状態にない場合に発生することがあります。
Unknown Association Requests	親メッシュ アクセス ポイントが子から受信する不明のアソシエーション要求の合計数。不明なアソシエーション要求は、子が不明なネイバー メッシュ アクセス ポイントの場合によくみられます。
Invalid Reassociation Request	親メッシュ アクセス ポイントが子から受信する無効の再アソシエーション要求の合計数。この状態は、子が有効なネイバーであっても、再アソシエーションに適した状態にない場合に発生することがあります。
Unknown Reassociation Request	親メッシュ アクセス ポイントが子から受信する不明の再アソシエーション要求の合計数。これは、子メッシュ アクセス ポイントが不明ネイバーの場合に発生することがあります。
Invalid Reauthentication Request	選択したメッシュ アクセス ポイントとその親の間で発生した無効な再認証要求の合計数。この状態は、選択したメッシュ アクセス ポイントが有効なネイバーであっても、再認証が許可された状態にない場合に発生することがあります。

[Mesh Links] タブ

表 5-58 に、[Mesh Links] タブのフィールドの一覧を示します。

（注）　このタブは、メッシュ アクセス ポイントの場合にのみ表示されます。関連するアラームとイベントを表示するには、[Mesh Link Alarms] リンクおよび [Mesh Link Events] リンクをクリックします。

表 5-58　[Mesh Links] タブのフィールド

フィールド	説明
Type	アクセス ポイントの種類。
AP Name	アクセス ポイントに割り当てられた名前。
AP MAC Address	アクセス ポイントの MAC アドレス。

表 5-58　[Mesh Links] タブのフィールド （続き）

フィールド	説明
PER	リンク テストで送信された合計パケットから測定されたパケット エラー率。
Link Detail	クリックすると、メッシュ リンク アラーム、メッシュ リンク イベント、およびリンク メトリックの詳細が表示されます。
Link Test	AP とネイバー AP 間のエアー リンク品質を測定するテスト。
Channel	メッシュ アクセス ポイントのチャネル番号。
Link SNR (dB)	AP とネイバー AP 間で測定されたエアー リンク SNR。
SNR Down	AP からネイバー AP へのエアー リンクで測定された信号雑音比。
SNR Up	ネイバー AP から AP へのエアー リンクで測定された信号雑音比。

（注）　[Mesh Links] テーブルの列を追加、削除、または順序変更するには、[Edit View] リンクをクリックします。[Edit View] を使用した新しいフィールドの追加については、「アクセス ポイント リストの表示の設定」（P.5-45）を参照してください。

コントローラとアクセス ポイント上の一意のデバイス ID の取得

一意のデバイス ID（UDI）規格は、すべてのシスコ製ハードウェア製品ファミリにわたって、一意に製品を識別するので、ビジネスおよびネットワーク操作を通じてシスコ製品を識別および追跡し、資産運用システムを自動化できます。この規格は、すべての電子的、物理的、および標準のビジネス コミュニケーションにわたって一貫性があります。UDI は、次の 5 つのデータ要素で構成されています。

- 注文可能な製品 ID（PID）
- 製品 ID のバージョン（VID）
- シリアル番号（SN）
- エンティティ名
- 製品の説明

UDI は工場でコントローラと Lightweight アクセス ポイントの Electrically Erasable Programmable Read-Only Memory（EEPROM; 電気的消去再書き込み可能 ROM）に焼き付けられ、GUI を通して取得できます。

コントローラとアクセス ポイントの UDI を取得するには、次の手順を実行します。

ステップ 1　[Monitor] > [Controllers/Access Points] の順に選択します。[Controllers/Access Points] ページが表示されます。

ステップ 2　UDI 情報を取得するコントローラまたはアクセス ポイントの IP アドレスをクリックします。コントローラまたはアクセス ポイントの UDI のデータ要素が表示されます。これらの要素については、表 5-59 で説明しています。

表 5-59　Cisco Wireless LAN Controller にインストールできる Crypto カードの最大数

コントローラの種類	Crypto カードの最大数
Cisco 2000 シリーズ	なし
Cisco 4100 シリーズ	1
Cisco 4400 シリーズ	2

カバレッジ ホールのモニタリング

カバレッジ ホールとは、クライアントが無線ネットワークから信号を受信できない領域のことです。Cisco Unified Network Solution の無線リソース管理（RRM）によって、これらのカバレッジ ホール領域が特定され Prime Infrastructure に報告されます。IT マネージャはユーザからの要求に基づいてカバレッジ ホールに対応します。

Prime Infrastructure は、コントローラにより、確かに検出されたカバレッジ ホールについて通知されます。Prime Infrastructure は、これらのカバレッジ ホールについてユーザに警告します。カバレッジ ホールの検出の詳細については、次の場所にあるシスコ コンテキスト認識サービスのマニュアルを参照してください。
http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/CAS/configuration/guide/msecg_ch7_CAS.html

（注）　カバレッジ ホールはアラームとして表示されます。プレカバレッジ ホールはイベントとして表示されます。

プレカバレッジ ホールのモニタリング

プレカバレッジ ホール イベントを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Events] の順に選択して、現在のすべてのイベントを表示します。

ステップ 2　プレカバレッジ ホール イベントのみを表示するには [Advanced Search] リンクをクリックします。

ステップ 3　[New Search] ページで、[Search Category] ドロップダウンを [Events] に変更します。

ステップ 4　[Event Category] ドロップダウン リストで、[Pre Coverage Hole] を選択し、[Go] をクリックします。

[Pre-Coverage Hole Events] ページには、表 5-60 で説明する情報が表示されます。

表 5-60　[Pre-Coverage Hole] のフィールド

フィールド	説明
Severity	プレカバレッジ ホールのイベントは、常に通知（Info）と見なされます。
Client MAC Address	プレカバレッジ ホールの影響を受けるクライアントの MAC アドレス。

表 5-60　[Pre-Coverage Hole] のフィールド （続き）

フィールド	説明
AP MAC Address	該当するアクセス ポイントの MAC アドレス。
AP Name	該当するアクセス ポイントの名前。
Radio Type	該当するアクセス ポイントの無線の種類（802.11b/g または 802.11a）。
Power Level	アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50% の電力、3 = 25% の電力、4 = 6.25 ～ 12.5% の電力、5 = 0.195 ～ 6.25% の電力。
Client Type	クライアントの種類は次のいずれかになります。 laptop(0) pc(1) pda(2) dot11mobilephone(3) dualmodephone(4) wgb(5) scanner(6) tabletpc(7) printer(8) projector(9) videoconfsystem(10) camera(11) gamingsystem(12) dot11deskphone(13) cashregister(14) radiotag(15) rfidsensor(16) server(17)
WLAN Coverage Hole Status	現在のカバレッジ ホールの状態が有効か無効かを特定します。
WLAN	この WLAN の名前。
Date/Time	イベントが発生した日時。タイトルをクリックすると、昇順および降順に並べ替えられます。

ステップ 5　[Client MAC Address] を選択して、プレカバレッジ ホール イベントの詳細を表示します。

- [General]：次の情報が表示されます。
  - Client MAC Address
  - AP MAC Address
  - AP Name
  - Radio Type

  - Power Level
  - Client Type
  - Category
  - Created
  - Generated By
  - Device AP Address
  - Severity
- [Neighbor AP's] : 近隣アクセス ポイントの MAC アドレス、その RSSI 値、およびその無線の種類が示されます。
- [Message] : プレカバレッジ ホールを報告したデバイス、およびプレカバレッジ ホールが検出されたコントローラが説明されます。
- [Help] : 該当する場合は、イベント処理に関する追加情報が表示されます。

不正アクセス ポイントのモニタリング

この項では、不正なデバイスに対するセキュリティ ソリューションについて説明します。不正なデバイスとは、ネットワーク内で管理対象のアクセス ポイントによって検出される、未知（管理対象外）のアクセス ポイントまたはクライアントのことです。

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や中間者攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連の Clear To Send（CTS; クリア ツー センド）フレームを送信できるようになります。アクセス ポイントになりすましてこの CTS フレームが送信され、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。したがって、無線 LAN サービス プロバイダーは、境域からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、許可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正なアクセス ポイントは、企業のファイアウォールの背後にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯につながるおそれがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセス ポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

不正なデバイスの検出

コントローラは、すべての近隣のアクセス ポイントを継続的にモニタし、不正なアクセス ポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラで不正なアクセス ポイントが検出されると、不正ロケーション検出プロトコル（RLDP）を使用して、不正なアクセス ポイントがネットワークに接続されているかどうかが判定されます。

（注）　Prime Infrastructure は、コントローラのすべての不正アクセス ポイント データを集約します。

管理者は、すべてのアクセス ポイント上、もしくはモニタ モード（受信専用）アクセス ポイント上でのみ、RLDP を使用するようコントローラを設定することが可能です。この後者のオプションでは、輻輳している RF 空間での不正なアクセス ポイントを簡単に自動検出できるようになります。そして、不要な干渉を生じさせたり、通常のデータ アクセス ポイント機能に影響を与えたりすることなく、モニタリングを行えるようになります。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ モード アクセス ポイントとローカル（データ）通信用アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 処理用アクセス ポイントとして、モニタ モード アクセス ポイントを選択します。ネットワーク上に不正があると RLDP で判断された場合は、検出された不正を手動で封じ込め処理を行うことも、自動的に封じ込め処理を行うこともできます。RLDP を有効化する方法は、「不正ポリシーの設定」（P.9-402）を参照してください。

（注）　不正アクセス ポイントのパーティションは、検出中のいずれかのアクセス ポイント（最新または最も強い RSSI 値を持つアクセス ポイント）と関連付けられます。検出中のアクセス ポイント情報がある場合、Prime Infrastructure は検出中のコントローラを使用します。不正アクセス ポイントが異なるパーティションに存在する 2 つのコントローラによって検出された場合、不正アクセス ポイントのパーティションは随時変更される場合があります。

ここでは、次の内容について説明します。

- 「不正 AP アラーム詳細の表示」（P.5-96）
- 「不正 AP アラームのモニタリング」（P.5-92）
- 「不正 AP アラーム詳細の表示」（P.5-96）
- 「不正クライアントの詳細の表示」（P.5-100）
- 「不正 AP 履歴の詳細の表示」（P.5-101）
- 「不正 AP イベント履歴の詳細の表示」（P.5-102）
- 「アドホック不正のアラームのモニタリング」（P.5-103）

不正なアクセス ポイントの分類

不正なアクセス ポイントの分類および報告は、不正の状態と、不正なアクセス ポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行われます。コントローラに対し、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類して表示させる各種ルールを作成できます。

（注）　Prime Infrastructure は、コントローラのすべての不正アクセス ポイント データを集約します。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセス ポイントは分類し直されます。ルールを変更するたびに、Alert 状態にあるすべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にそのルールが適用されます。

（注）　ルール ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

（注）　5500 シリーズ コントローラは最大で 2000 個の不正（認知済みの不正情報含め）に対応します。4400 シリーズ コントローラ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチは最大で 625 個の不正に対応します。2100 シリーズ コントローラおよびサービス統合型ルータのコントローラ ネットワーク モジュールは最大で 125 個の不正に対応します。各コントローラは、不正アクセス ポイントの封じ込めを無線チャンネルごとに 3 台（モニタ モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly として分類します。
2. 未知（管理対象外）のアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正状態の分類ルール適用処理を開始します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。
4. コントローラは、優先度の一番高いルールを適用します。不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントに対して手動で封じ込め処理を行うことができますが（不正を自動的に封じ込めるよう RLDP が設定されていない限り）、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセス ポイントを手動で封じ込め処理を行うことができるようになります。
8. 必要に応じて、各アクセス ポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

前述のように、コントローラでは、ユーザ定義のルールに基づいて未知（管理対象外）のアクセス ポイントの分類タイプと不正の状態が自動的に変更されます。もしくは、未知（管理対象外）のアクセス ポイントを本来とは異なる分類タイプと不正の状態に手動で変更することができます。表 5-61 に、未知（管理対象外）のアクセス ポイントに設定できる分類タイプや不正の状態の推移の組み合わせを示します。

表 5-61　設定可能な分類タイプ/不正の状態の推移

推移前	推移後
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）

表 5-61　設定可能な分類タイプ/不正の状態の推移 （続き）

推移前	推移後
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが封じ込められないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に変更する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

不正アクセス ポイントの分類には次のものがあります。

- Malicious：システム内で検出されているが、悪意のある、信頼できない、または未知（管理対象外）のアクセス ポイント。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。詳細については、「悪意のある不正アクセス ポイント」（P.5-90）を参照してください。
- Friendly：既知、認知済み、または信頼されたアクセス ポイント。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。詳細については、「危険性のない不正アクセス ポイント」（P.5-91）を参照してください。危険性のないアクセス ポイントのルールを設定するときの詳細については、「危険性のないアクセス ポイント テンプレートの設定」（P.11-683）を参照してください。
- Unclassified：Malicious または Friendly のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。詳細を参照してください。詳細については、「未分類の不正アクセス ポイント」（P.5-91）を参照してください。

悪意のある不正アクセス ポイント

悪意のある不正アクセス ポイントとは、システム内で検出される悪意のある信頼できないアクセス ポイントまたは未知（管理対象外）のアクセス ポイントです。また、これらの分類には、ユーザが定義した Malicious ルールに合致したアクセス ポイント、または危険性のないアクセス ポイント分類から手動で移動したアクセス ポイントも含まれます。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間、過去 24 時間の各状態の悪意のある不正アクセス ポイントの数と、アクティブな悪意のある不正アクセス ポイントの総数が表示されます。

悪意のある不正アクセス ポイントの状態には次のものがあります。

- Alert：該当アクセス ポイントがネイバー リストまたはユーザ設定の [Friendly AP] リストにないことを示します。
- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。
- Contained Pending：リソースを利用できないため、封じ込め処理が遅延することを示します。
- Removed：この未知（管理対象外）のアクセス ポイントは以前検出されたものの、現在は見つかりません。

悪意のある不正アクセス ポイントに関する詳細な情報を表示するには、いずれかの期間のカテゴリにある下線付きの数値をクリックします。詳細については、「不正アクセス ポイントのモニタリング」（P.5-87）を参照してください。

危険性のない不正アクセス ポイント

危険性のない不正アクセス ポイントとは、既知のアクセス ポイント、認知済みアクセス ポイント、または信頼されたアクセス ポイントです。また、ユーザ定義の Friendly ルールと一致するアクセス ポイントを指します。危険性のない不正アクセス ポイントに対して封じ込め処理は実行できません。

（注）　Prime Infrastructure ユーザのみが不正アクセス ポイントの MAC アドレスを [Friendly AP] リストに追加できます。Prime Infrastructure では、[Friendly AP] の MAC アドレスはコントローラに適用されません。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の危険性のない不正アクセス ポイントの数と、アクティブな危険性のない不正アクセス ポイントの総数が表示されます。

危険性のない不正アクセス ポイントの状態には次のものがあります。

- Internal：未知（管理対象外）のアクセス ポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。
- External：未知（管理対象外）のアクセス ポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近所のコーヒー ショップ設置されているアクセス ポイントなどです。
- Alert：未知（管理対象外）のアクセス ポイントはネイバー リストにもユーザ設定の [Friendly AP] リストにもありません。

危険性のない不正アクセス ポイントの詳細を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。詳細については、「不正アクセス ポイントのモニタリング」（P.5-87）を参照してください。

[Friendly AP] リストから不正アクセス ポイントを削除するには、Prime Infrastructure とコントローラの両方で不正アクセス ポイントが [Friendly AP] リストから削除されることを確認します。不正アクセス ポイントを、[Friendly AP Internal] または [Friendly AP External] から [Unclassified] または [Malicious Alert] に変更します。

未分類の不正アクセス ポイント

未分類の不正アクセス ポイントとは、[Malicious]（危険性あり）または [Friendly]（危険性なし）のいずれにも分類されない不正アクセス ポイントです。これらのアクセス ポイントは封じ込め処理を行うことができ、また、危険性のない不正なアクセス ポイント リストへ手動で変更することもできます。

Prime Infrastructure ホーム ページの [Security] ダッシュボードには、過去 1 時間および過去 24 時間の各状態の未分類の不正アクセス ポイントの数と、アクティブな未分類の不正アクセス ポイントの総数が表示されます。

未分類の不正アクセス ポイントの状態には次のものがあります。

- Pending：最初の検出で、未知（管理対象外）のアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセス ポイントでは、未知（管理対象外）のアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。
- Alert：未知（管理対象外）のアクセス ポイントはネイバー リストにもユーザ設定の [Friendly AP] リストにもありません。

- Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。
- Contained Pending：未知（管理対象外）のアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

詳細情報を参照するには、いずれかの分類期間にある下線付きの数字をクリックします。「不正アクセス ポイントのモニタリング」（P.5-87）を参照してください。

不正 AP アラームのモニタリング

不正アクセス ポイント無線は、1 つ以上の Cisco 1000 シリーズ Lightweight アクセス ポイントによって検出された無許可のアクセス ポイントです。[Rogue AP Alarms] ページを表示する手順は、次のとおりです。

- 不正 AP を検索します。この検索機能の詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- Prime Infrastructure ホーム ページで、[Security] ダッシュボードをクリックします。このページには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- [Alarm Summary] の [Malicious AP number] リンクをクリックします。

（注）　アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。スクロール矢印を使用して、その他のアラームを表示します。

（注）　不正アクセス ポイントのパーティションは、検出中のいずれかのアクセス ポイント（最新または最も強い RSSI 値を持つアクセス ポイント）と関連付けられます。検出中のアクセス ポイント情報がある場合、Prime Infrastructure は検出中のコントローラを使用します。不正アクセス ポイントが異なるパーティションに存在する 2 つのコントローラによって検出された場合、不正アクセス ポイントのパーティションは随時変更される場合があります。

[Rogue AP Alarms] ページのフィールドは次のとおりです。

（注）　Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、[Radio Types] など）が不正の存続期間中に変更される可能性があります。

- [Severity]：次のアイコンを含む、アラームの重大度を示します。

表 5-62　アラーム重大度インジケータ アイコン

アイコン	意味
	Critical
	Major
	Minor

表 5-62　アラーム重大度インジケータ アイコン （続き）

アイコン	意味
	Warning
	Info
	Unknown （注）　コントローラがダウンした場合、コントローラ インベントリ ダッシュレットでコントローラのステータスが重大として表示されます。しかし、無線インベントリ ダッシュレットでは、最後の既知のステータスのままになります。[Monitor] > [AP] ページで、AP アラームのステータスが「Unknown」と表示されます。
	Clear：不正がどのアクセス ポイントでも検出されなくなった場合に表示されます。 （注）　不正は、複数のアクセス ポイントによって検出されることがあります。1 つのアクセス ポイントが不正を検出しなくなっても、他のアクセス ポイントが検出する場合は、クリアは送信されません。 （注）　不正の重大度が Clear になると、アラームは 30 日後に Prime Infrastructure から削除されます。

Severity Configuration 機能を使用して、次の不正アクセス ポイント アラーム タイプの重大度を決定できます。

- Rogue detected
- Rogue detected contained
- Rogue detected on network

詳細については、「アラームのシビリティの設定」（P.15-872）を参照してください。

- [Rogue MAC Address]：不正アクセス ポイントの MAC アドレスを示します。「不正 AP アラーム詳細の表示」（P.5-96）を参照してください。
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [Classification Type]：Pending、Malicious、Friendly、または Unclassified。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Strongest AP RSSI]：不正の存続期間全体でこの不正アクセス ポイントの最も強い AP RSSI を表示します。不正の存続期間で最も強い AP RSSI は、不正アクセス ポイントとユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。
- [No.of Rogue Clients]：この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。

（注）　この数は、Prime Infrastructure データベースから取得され、2 時間ごとに更新されます。[Monitor] > [Alarms] > [Alarm Details] ページには、リアルタイムの数が表示されます。この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。

- [Owner]：このアラームに割り当てられている個人の名前または（ブランク）。
- [Last Seen Time]：不正アクセス ポイントが最後に認識された日時を示します。

- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。追加情報については、「不正なアクセス ポイントの分類」（P.5-88）を参照してください。
  - 悪意のある不正アクセス ポイントの状態には、Alert、Contained、Threat、Contained Pending、および Removed があります。詳細については、「悪意のある不正アクセス ポイント」（P.5-90）を参照してください。
  - 危険性のない不正アクセス ポイントの状態には、Internal、External、および Alert があります。詳細については、「危険性のない不正アクセス ポイント」（P.5-91）を参照してください。
  - 未分類の不正アクセス ポイントの状態には、Pending、Alert、Contained、および Contained Pending があります。詳細については、「未分類の不正アクセス ポイント」（P.5-91）を参照してください。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID を示します。SSID がブロードキャストされていない場合は空欄になります。
- [Map Location]：この不正アクセス ポイントのマップの場所を示します。
- [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。

  [Alarm Summary] ページに表示されないように、アラームを承認できます。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。詳細については、「アラームの認知」（P.5-136）を参照してください。

（注） アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

注意 不正なデバイスを封じ込めることを選択すると、「There may be legal issues following this containment.Are you sure you want to continue?」という警告メッセージが表示されます。工業、科学、医療用（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に解放されているので、ライセンスなしで使用できます。したがって、別のネットワーク上のデバイスを封じ込めると、法的責任を負う場合があります。

[Select a command] メニュー

対応するチェックボックスを選択して 1 つ以上のアラームを選択するか、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。アラームがどのアクセス ポイントでも検出されなくなったことを示します。

（注） 重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。

- [Acknowledge Alarm]：アラームを認識した後は、[Alarm Summary] ページで表示されないようにできます。詳細については、「アラームの認知」（P.5-136）を参照してください。

（注）　アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge Alarm]：すでに認知しているアラームを未認知にします。
- [Email Notification]：[All Alarms] > [Email Notification] ページに移動し、電子メール通知を表示および設定します。詳細については、「RFID タグのモニタリング」（P.5-113）を参照してください。
- [Severity Configuration]：新しく生成されるアラームの重大度を変更できます。詳細については、「アラームのシビリティの設定」（P.15-872）を参照してください。
- [Detecting APs]：不正アクセス ポイントを現在検出している Cisco 1000 シリーズ Lightweight アクセス ポイントを表示します。詳細については、「アクセス ポイントの検出」（P.5-108）を参照してください。
- [Map (High Resolution)]：ここをクリックすると、不正アクセス ポイントの位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アクセス ポイントにアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アクセス ポイントが表示されます。詳細については、「不正クライアントの詳細の表示」（P.5-100）を参照してください。Prime Infrastructure 検索機能を使用してこの情報にアクセスすることもできます。詳細については、「検索機能の使用方法」（P.2-54）または「Advanced Search」（P.2-55）を参照してください。
- [Set State to 'Unclassified - Alert']：不正アクセス ポイントを最小脅威レベルと見なしてモニタリングを継続し、封じ込め機能を解除します。未分類の不正アクセス ポイントの詳細については、「未分類の不正アクセス ポイント」（P.5-91）を参照してください。
- [Set State to 'Malicious - Alert']：不正アクセス ポイントに「Malicious」タグを設定します。悪意のある不正アクセス ポイントの詳細については、「悪意のある不正アクセス ポイント」（P.5-90）を参照してください。
- [Set State to 'Friendly - Internal']：不正アクセス ポイントに「内部」タグを設定し、[Known Rogue APs] リストに追加します。さらに、封じ込め機能を解除します。危険性のない不正の詳細については、「危険性のない不正アクセス ポイント」（P.5-91）を参照してください。
- [Set State to 'Friendly - External']：不正アクセス ポイントに「外部」タグを設定し、[Known Rogue APs] リストに追加します。さらに、封じ込め機能を解除します。危険性のない不正の詳細については、「危険性のない不正アクセス ポイント」（P.5-91）を参照してください。
- [1 AP Containment]：不正アクセス ポイントを 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アクセス ポイントを 2 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アクセス ポイントを 3 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アクセス ポイントを 4 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

（注）　不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。

注意　不正アクセス ポイントの封じ込めは法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。　処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

不正 AP アラーム詳細の表示

不正アクセス ポイント無線は、Cisco 1000 シリーズ Lightweight アクセス ポイントによって検出された無許可のアクセス ポイントです。[Rogue AP Alarms] リスト ページで、各不正アクセス ポイントに関するアラーム イベントの詳細を参照できます。

不正アクセス ポイントの無線のアラーム イベントを表示するには、不正アクセス ポイント アラームの [Monitor] > [Alarms] ページで、該当するアラームの不正 MAC アドレスをクリックします。

[Alarm Details] ページのすべてのフィールド（[No. of Rogue Clients] を除く）は、ポーリングによってデータが設定され、2 時間ごとに更新されます。不正クライアントの数はリアルタイムの数であり、不正アクセス ポイント アラームの [Alarm Details] ページにアクセスするたびに更新されます。

コントローラ（バージョン 7.4 または 7.5）がカスタムの不正 AP アラームを送信すると、Prime Infrastructure は未分類の不正アラームとしてこれを表示します。これは、Prime Infrastructure がカスタムの不正 AP アラームをサポートしていないためです。

（注）　Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI]、[No. of Rogue Clients]、[Channel]、[SSID]、[Radio Types] など）が不正の存続期間中に変更される可能性があります。

[Alarm Details] ページには、次の情報が表示されます。

- General
  - [Rogue MAC Address]：不正アクセス ポイントの MAC アドレス。
  - [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。

    （注）　[Airlink] の不正アクセス ポイント アラームが表示される場合、ベンダーは Airlink ではなく Alpha と表示されます。

  - [Rogue Type]：AP などの不正の種類が示されます。
  - [On Network]：不正が検出された方法を示します。

    [Controller]：コントローラが不正を検出しました（Yes または No）。

    [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
  - [Owner]：オーナーを示します（または空白）。
  - [Acknowledged]：担当ユーザがこのアラームを認知しているかどうかを示します。

[Alarm Summary] ページに表示されないように、アラームを承認できます。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。詳細については、「アラームの認知」（P.5-136）を参照してください。

- [Classification Type]：Malicious、Friendly、Unclassified。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：不正アクセス ポイントのチャネル。
- [Containment Level]：不正アクセス ポイントの封じ込め処理レベル、または Unassigned（封じ込めなし）を示します。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Strongest AP RSSI]：不正の存続期間全体でこの不正アクセス ポイントの最も強い AP RSSI を表示します。不正の存続期間で最も強い AP RSSI は、不正アクセス ポイントとユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。
- [No.of Rogue Clients]：この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。

（注）　不正クライアントの数は、[Monitor] > [Alarm] > [Alarm Details] ページの唯一のリアルタイム フィールドです。これは、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。
[Alarm Details] ページのその他すべてのフィールドは、ポーリングによってデータが設定され、2 時間ごとに更新されます。

- [First Seen Time]：不正アクセス ポイントが最初に検出された日時を示します。この情報は、コントローラから入力されます。
- [Last Seen Time]：不正アクセス ポイントが最後に検出された日時を示します。この情報は、コントローラから入力されます。
- [Modified]：アラーム イベントが修正された日時。
- [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。

  [NMS (Network Management System - Prime Infrastructure)]：ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。

  [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。
- [Severity]：次のアイコンを含む、アラームの重大度。

アイコン	意味
	Critical
	Major

アイコン	意味
	Minor
	Warning
	Info
	Clear：不正がどのアクセス ポイントでも検出されなくなった場合に表示されます。 **（注）** 不正は、複数のアクセス ポイントによって検出されることがあります。1 つのアクセス ポイントが不正を検出しなくなっても、他のアクセス ポイントが検出する場合は、クリアは送信されません。 **（注）** 不正の重大度が Clear になると、アラームは 30 日後に Prime Infrastructure から削除されます。

Severity Configuration 機能を使用して、不正アクセス ポイントの重大度を決定できます。詳細については、「アラームのシビリティの設定」（P.15-872）を参照してください。

- [Previous Severity]：アラームの以前の重大度（Critical、Major、Minor、または Clear）。
- [Event Details]：イベントの詳細を表示するには、[Event History] リンクをクリックします。
- [Rogue AP History]：不正アラームの詳細を表示するには、[Rogue AP History] リンクをクリックします。
- [Switch Port Trace Status]：スイッチ ポート トレース ステータスを示します。スイッチ ポート トレース ステータスには、[Traced, but not found]、[Traced and found]、[Not traced]、[Failed] があります。詳細については、「スイッチ ポート トレーシングの設定」（P.15-878）を参照してください。

- [Switch Port Tracing Details]：最新のスイッチ ポート トレースの詳細が表示されます。追加のトレースの詳細を表示するには、[Click here for more details] リンクをクリックします。詳細については、「スイッチ ポート トレーシングの設定」（P.15-878）を参照してください。
- [Rogue Clients]：このアクセス ポイントの不正クライアントの一覧が表示されます。これには、クライアントの MAC アドレス、クライアントが認識された最後の日時、現在のクライアントのステータスが含まれます。詳細については、「不正クライアントの詳細の表示」（P.5-100）を参照してください。

（注） 不正クライアントの数は、[Monitor] > [Alarm] > [Alarm Details] ページの唯一のリアルタイム フィールドです。これは、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。
[Alarm Details] ページのその他すべてのフィールドは、ポーリングによってデータが設定され、2 時間ごとに更新されます。

- [Message]：この不正アクセス ポイントに関する最新のメッセージが表示されます。メッセージが送信されるのは、不正アクセス ポイントが最初に検出された場合、トラップが送信された場合、状態が変化した場合です。
- [Annotations]：この不正アクセス ポイントに関する現在の注釈が表示されます。新しい注釈を追加するには、[New Annotation] をクリックします。注釈を入力し、[Post] をクリックして注釈を保存および表示するか、[Cancel] をクリックして、注釈を保存せずにページを閉じます。

- [Location Notifications]：クライアントに対して記録された場所の通知の数が表示されます。リンクをクリックすると、通知が表示されます。
- [Location]：場所情報が表示されます（利用可能な場合）。

（注）　スイッチ ポート トレースは、重大度、状態などの不正の属性を更新しません。不正の属性はスイッチ ポート トレースで更新されないため、スイッチ ポート トレースを使用して、不正が「ネットワーク上にある」と検出された場合、アラームは生成されません。

[Select a command] メニュー

[Rogue AP Alarm Details] ページにある [Select a command] ドロップダウン リストには、次のオプションがあります。ドロップダウン リストからオプションを選択し、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。
- [Acknowledge Alarm]：アラームを認識した後は、[Alarm Summary] ページで表示されないようにできます。詳細については、「アラームの認知」（P.5-136）を参照してください。

（注）　アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [Trace Switch Port]：クリックすると、この不正アクセス ポイントのスイッチ ポート トレースが実行されます。詳細については、「スイッチ ポート トレーシングの設定」（P.15-878）を参照してください。
- [Event History]：クリックすると、この不正アクセス ポイントのイベントの一覧が表示されます。詳細については、「不正アラーム イベントのモニタリング」（P.5-109）を参照してください。
- [Refresh from Network]：クリックすると、ネットワークから不正 AP が同期されます。
- [View Detecting AP on Network]：現在不正アクセス ポイントを検出している Cisco 1000 シリーズ Lightweight アクセス ポイントが表示されます。詳細については、「アクセス ポイントの検出」（P.5-108）を参照してください。

（注）　[Detecting AP Name]、[Radio]、[SSID] の情報は、コントローラに情報がないために空白となる場合があります。AP の詳細を表示するには、不正 AP タスクが完了した後でページを更新します。

- [View Details by Controller]：コントローラによって報告された不正 AP の分類の種類と状態が表示されます。
- [Map (High Resolution)]：ここをクリックすると、不正アクセス ポイントの位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アクセス ポイントにアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アクセス ポイントが表示されます。詳細については、「不正クライアントの詳細の表示」（P.5-100）を参照

してください。Prime Infrastructure 検索機能を使用してこの情報にアクセスすることもできます。詳細については、「検索機能の使用方法」（P.2-54）または「Advanced Search」（P.2-55）を参照してください。

- [Set State to 'Unclassified - Alert']：不正アクセス ポイントを最小脅威レベルと見なしてモニタリングを継続し、封じ込め機能を解除します。未分類の不正アクセス ポイントの詳細については、「未分類の不正アクセス ポイント」（P.5-91）を参照してください。
- [Set State to 'Malicious - Alert']：不正アクセス ポイントに「Malicious」タグを設定します。悪意のある不正アクセス ポイントの詳細については、「悪意のある不正アクセス ポイント」（P.5-90）を参照してください。
- [Set State to 'Friendly - Internal']：不正アクセス ポイントに「内部」タグを設定し、[Known Rogue APs] リストに追加します。さらに、封じ込め機能を解除します。危険性のない不正の詳細については、「危険性のない不正アクセス ポイント」（P.5-91）を参照してください。
- [Set State to 'Friendly - External']：不正アクセス ポイントに「外部」タグを設定し、[Known Rogue APs] リストに追加します。さらに、封じ込め機能を解除します。危険性のない不正の詳細については、「危険性のない不正アクセス ポイント」（P.5-91）を参照してください。
- [1 AP Containment]：不正アクセス ポイントを 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アクセス ポイントを 2 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アクセス ポイントを 3 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アクセス ポイントを 4 つの Cisco 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

（注） 不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。

不正クライアントの詳細の表示

不正クライアントは、次のいくつかの方法で表示できます。

- Prime Infrastructure 検索機能を使用して不正クライアントを検索します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- 該当する不正アクセス ポイントの [Alarm Details] ページから、特定の不正アクセス ポイントの不正クライアントのリストを表示します。該当する不正クライアントの不正 MAC アドレスをクリックし、[Rogue Client details] ページを表示します。
- 不正アクセス ポイントの [Alarms Details] ページで、[Select a command] ドロップダウン リストから [Rogue Clients] を選択します。

[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、そのコントローラ、および関連付けられている不正アクセス ポイントが表示されます。

（注） 不正クライアントのステータスには、Contained（コントローラにより、攻撃しているデバイスの信号が許可されたクライアントに干渉しないように封じ込められています）、Alert（コントローラは即時アラートをシステム管理者に転送し、さらなる処置を求めます）、および Threat（不正は既知の脅威です）があります。

不正クライアントのクライアント MAC アドレスをクリックすると、[Rogue Client details] ページが表示されます。[Rogue Client details] ページには、次の情報が表示されます。

- [General]：情報には、クライアントの MAC アドレス、このクライアントを検出したアクセス ポイントの数、クライアントと最初に通信した日時と最後に通信した日時、不正アクセス ポイントの MAC アドレス、クライアントの現在のステータスが含まれます。
- [Location Notifications]：この不正クライアントの通知の数を示します（absence、containment、distance、および all が含まれます）。通知の数をクリックすると、該当する [Monitor] > [Alarms] ページが表示されます。
- [APs that detected the rogue client]：この不正クライアントを検出したすべてのアクセス ポイントの、ベース無線の MAC アドレス、アクセス ポイント名、チャネル番号、無線の種類、RSSI、SNR、および不正クライアントと最後に通信した日時が表示されます。
- [Location]：場所情報が表示されます（利用可能な場合）。

（注）　不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。

Select a command

[Rogue Client details] ページの [Select a command] ドロップダウン リストには、次のオプションが含まれています。

- [Set State to 'Unknown - Alert']：不正クライアントを最小脅威レベルと見なしてモニタリングを継続し、封じ込め機能を解除します。
- [1 AP Containment]：不正クライアントを 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正クライアントを 2 つのアクセス ポイントで封じ込めます。
- [3 AP Containment]：不正クライアントを 3 つのアクセス ポイントで封じ込めます。
- [4 AP Containment]：不正クライアントを 4 つのアクセス ポイントで封じ込めます。（最大封じ込めレベル）。
- [Map (High Resolution)]：ここをクリックすると、不正クライアントの位置を示す高解像度マップが表示されます。
- [Location History]：クリックすると、RF フィンガープリントに基づいて、不正クライアントの位置の履歴が表示されます。

不正 AP 履歴の詳細の表示

不正 AP アラームの履歴を表示するには、[Rogue AP Alarm] ページで [Rogue AP History] リンクをクリックします。

[Rogue AP History] ページには、次の情報が表示されます。

- [Severity]：アラームの重大度。
- [Rogue MAC Address]：不正アクセス ポイントの MAC アドレス。
- [Classification Type]：Malicious、Friendly、Unclassified。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Strongest AP RSSI]：不正の存続期間全体でこの不正アクセス ポイントの最も強い AP RSSI を表示します。不正の存続期間で最も強い AP RSSI は、不正アクセス ポイントとユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。

- [No.of Rogue Clients]：この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。

（注）　不正クライアントの数は、[Monitor] > [Alarm] > [Alarm Details] ページの唯一のリアルタイム フィールドです。これは、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。[Alarm Details] ページのその他すべてのフィールドは、ポーリングによってデータが設定され、2 時間ごとに更新されます。

- [First Seen Time]：不正アクセス ポイントが最初に検出された日時を示します。この情報は、コントローラから入力されます。
- [Last Seen Time]：不正アクセス ポイントが最後に検出された日時を示します。この情報は、コントローラから入力されます。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Category]：このアラームのカテゴリ（Security、Prime Infrastructure など）を示します。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Channel Number]：アドホック不正のチャネルを示します。
- [Containment Level]：アドホック不正の封じ込めレベル、または Unassigned を示します。
- [Switch Port Trace Status]：スイッチ ポート トレース ステータスを示します。スイッチ ポート トレース ステータスには、[Traced, but not found]、[Traced and found]、[Not traced]、[Failed] があります。

不正 MAC アドレスをクリックすると、特定の不正 AP 履歴の詳細ページが表示されます。不正 AP 履歴の詳細ページには、上記の詳細と、実際のアラーム メッセージが表示されます。

不正 AP イベント履歴の詳細の表示

不正 AP のイベントの詳細を表示するには、[Rogue AP Alarm] ページで [Event History] リンクをクリックします。

[Rogue AP Event History] ページには、次の情報が表示されます。

- [Severity]：アラームの重大度。
- [Rogue MAC Address]：不正アクセス ポイントの MAC アドレス。
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [Classification Type]：Malicious、Friendly、Unclassified。
- [On Network]：不正検出が発生したかどうかを示します。コントローラが不正を検出しました（Yes または No）。
- [Date/Time]：イベントが生成された日時。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。

- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。

アドホック不正のモニタリング

アドホック ネットワークで動作しているモバイル クライアントの MAC アドレスが許可された MAC アドレスのリストにない場合は、アドホックの不正であると識別されます。ここでは、次の内容について説明します。

- 「アドホック不正のアラームのモニタリング」（P.5-103）
- 「アドホック不正アラームの詳細の表示」（P.5-105）

アドホック不正のアラームのモニタリング

[Adhoc Rogue Alarms] ページには、アドホック不正のアラーム イベントが表示されます。[Adhoc Rogue Alarms] ページにアクセスするには、次のいずれかの手順を実行します。

- アドホック不正のアラームの検索を実行します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- Prime Infrastructure ホーム ページで、[Security] ダッシュボードをクリックします。このページには、過去 1 時間と過去 24 時間に検出されたアドホック不正がすべて表示されます。アドホック不正の番号をクリックすると、アドホック不正のアラームが表示されます。

アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

[Adhoc Rogue Alarms] ページには次のフィールドがあります。

（注）　Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI、[No.of Rogue Clients]、[Channel]、[SSID]、[Radio Types] など）が不正の存続期間中に変更される可能性があります。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。

  Severity Configuration 機能を使用して、次のアドホック不正アラーム タイプの重大度を決定できます。

  - Adhoc Rogue auto contained
  - Adhoc Rogue detected
  - Adhoc Rogue detected on network
  - Adhoc Rogue detected on network

  詳細については、「アラームのシビリティの設定」（P.15-872）を参照してください。
- [Rogue MAC Address]：不正の MAC アドレスを示します。詳細については、「アドホック不正アラームの詳細の表示」（P.5-105）を参照してください。
- [Vendor]：アドホック不正のベンダー名または Unknown を示します。

- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Strongest AP RSSI]：不正の存続期間全体でこの不正の最も強い AP RSSI を表示します。不正の存続期間で最も強い AP RSSI は、不正とユーザのビルディングまたは場所間に存在した最も近い距離を示します。RSSI が大きいほど、場所は近くなります。

  [No.of Rogue Clients]：この不正アクセス ポイントに関連付けられた不正クライアントの数を示します。

  （注）　不正クライアントの数は、[Monitor] > [Alarm] > [Alarm Details] ページの唯一のリアルタイム フィールドです。これは、この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。
  [Alarm Details] ページのその他すべてのフィールドは、ポーリングによってデータが設定され、2 時間ごとに更新されます。

- [Owner]：オーナーを示します（または空白）。
- [Last Seen Time]：アラームが最後に表示された日時を示します。
- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [SSID]：不正なアドホック無線によってブロードキャストされているサービス セット ID。ブロードキャストがない場合は空白になります。
- [Map Location]：このアドホック不正のマップの場所を示します。
- [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。

  [Alarm Summary] ページに表示されないように、アラームを承認できます。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。詳細については、「アラームの認知」（P.5-136）を参照してください。

[Select a command] メニュー

対応するチェックボックスを選択して 1 つ以上のアラームを選択するか、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。詳細については、「アラームの認知」（P.5-136）を参照してください。

  （注）　アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [Email Notification]：[All Alarms] > [Email Notification] ページに移動し、電子メール通知を表示および設定します。詳細については、「RFID タグのモニタリング」（P.5-113）を参照してください。
- [Detecting APs]：不正アドホックを現在検出しているアクセス ポイントを表示します。詳細については、「アクセス ポイントの検出」（P.108）を参照してください。

- [Map (High Resolution)]：ここをクリックすると、アドホック不正の位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、このアドホック不正に関連する不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、およびアドホック不正が表示されます。
- [Set State to 'Alert']：アドホック不正を最小脅威レベルと見なし、不正アクセス ポイントのモニタリングを継続し、封じ込め機能を解除します。
- [Set State to 'Internal']：アドホック不正に「内部」タグを設定し、[Known Rogue APs] リストに追加します。さらに、封じ込め機能を解除します。
- [Set State to 'External']：アドホック不正に「外部」タグを設定し、[Known Rogue APs] リストに追加します。さらに、封じ込め機能を解除します。
- [1 AP Containment]：アドホック不正を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：アドホック不正を 2 つのアクセス ポイントで封じ込めます。
- [3 AP Containment]：アドホック不正を 3 つのアクセス ポイントで封じ込めます。
- [4 AP Containment]：アドホック不正を 4 つのアクセス ポイントで封じ込めます。（最大封じ込めレベル）。

注意　アドホック不正の封じ込め処理は法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

アドホック不正アラームの詳細の表示

[Adhoc Rogue Alarms] ページから、各アドホック不正に関するアラーム イベント情報を参照できます。

アドホック不正無線のアラーム イベントを表示するには、[Adhoc Rogue Alarms] ページで該当する不正 MAC アドレスをクリックします。

このページには、不正アクセス ポイント無線のアラーム イベントが表示されます。不正アクセス ポイント無線は、Cisco 1000 シリーズ Lightweight アクセス ポイントによって検出された無許可のアクセス ポイントです。

（注）　Prime Infrastructure によるポーリング時に、一部のデータが変更または更新されることがあります。このため、表示される不正データの一部（[Strongest AP RSSI、[No.of Rogue Clients]、[Channel]、[SSID]、[Radio Types] など）が不正の存続期間中に変更される可能性があります。

- General
  - [Rogue MAC Address]：アドホック不正の MAC アドレス。
  - [Vendor]：アドホック不正のベンダー名、または Unknown。
  - [On Network]：不正が検出された方法を示します。

    [Controller]：コントローラが不正を検出しました（Yes または No）。

[Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。

- [Owner]：オーナー（または空白）。
- [Acknowledged]：担当ユーザがこのアラームを認知しているかどうかを示します。

  [Alarm Summary] ページに表示されないように、アラームを承認できます。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。詳細については、「アラームの認知」（P.5-136）を参照してください。
- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [SSID]：アドホック不正無線によってブロードキャストされている SSID。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：アドホック不正のチャネルを示します。
- [Containment Level]：アドホック不正の封じ込めレベル、または Unassigned を示します。
- [Radio Type]：このアドホック不正に適用されるすべての無線タイプをリストします。
- [Strongest AP RSSI]：この Prime Infrastructure の最も強い受信信号強度インジケータを示します（すべてのコントローラと、すべての検出時間にわたる、すべての検出アクセス ポイントが含まれます）。
- [No.of Rogue Clients]：このアドホックに関連する不正クライアントの数を示します。

  （注） この数は、Prime Infrastructure データベースから取得されます。2 時間ごとに更新されます。[Monitor] > [Alarms] > [Alarm Details] ページには、リアルタイムの数が表示されます。この不正アクセス ポイントの [Alarm Details] ページを開くたびに更新されます。
- [Created]：アラーム イベントが作成された日時。
- [Modified]：アラーム イベントが修正された日時。
- [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。

  [NMS (Network Management System - Prime Infrastructure)]：ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。

  [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。
- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Previous Severity]：アラームの以前の重大度（Critical、Major、Minor、または Clear）。色分けして表示されます。

- [Annotations]：このボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。
- [Message]：アラームに関する説明が表示されます。
- [Help]：アラームに関する最新情報が表示されます。
- [Event History]：クリックすると、[Monitor] > [Events] ページが開きます。詳細については、「イベントのモニタリング」（P.5-143）を参照してください。

- [Annotations]：このアラームの現在の注釈が表示されます。

Advanced Search を使用した不正クライアントの検索

無線 LAN 上のアクセス ポイントの電源が入りコントローラにアソシエートされると、Prime Infrastructure はただちに不正アクセス ポイントのリスニングを開始します。コントローラによって不正アクセス ポイントが検出されると、ただちに Prime Infrastructure に通知され、Prime Infrastructure によって不正アクセス ポイントのアラームが作成されます。

Advanced Search を使用して不正アクセス ポイントのアラームを見つけるには、次の手順を実行します。

ステップ 1　Prime Infrastructure のメイン ページの右上で、[Advanced Search] をクリックします。

ステップ 2　[Search Category] ドロップダウン リストから [Rogue Client] を選択します。

ステップ 3　（任意）必要に応じて他の検索条件を使用して検索をさらにフィルタできます。

ステップ 4　[Search] をクリックします。不正クライアントの一覧が表示されます。

ステップ 5　クライアントの MAC アドレスをクリックして不正クライアントを選択します。[Rogue Client] の詳細ページが表示されます。

ステップ 6　アラームを変更するには、[Select a command] ドロップダウン リストから次のコマンドのいずれかを選択し、[Go] をクリックします。

- [Set State to 'Unknown-Alert']：アドホックの不正を最小脅威レベルと見なしてモニタリングを継続し、封じ込め機能を解除します。
- [1 AP Containment] ～ [4 AP Containment]：不正な機器にアソシエートされたクライアント デバイスに認証解除とアソシエート解除のメッセージを送信している、不正な機器の近辺にあるアクセス ポイント数（1 ～ 4）を示します。
- [Map (High Resolution)]：計算された不正アクセス ポイントの現在位置を [Maps] > [Building Name] > [Floor Name] ページに表示します。
- [Location History]：RF フィンガープリントに基づいて、不正クライアントの位置の履歴が表示されます。

（注）　位置の履歴が表示されるためには、クライアントが MSE によって検出される必要があります。

不正アクセス ポイントの場所、タギング、および封じ込めのモニタリング

Prime Infrastructure を使用して Cisco Unified Network Solution をモニタしている場合、不正アクセス ポイント トラップとしてフラグが生成され、既知の不正アクセス ポイントが MAC アドレスで表示されます。オペレータは、それぞれの不正アクセス ポイントに最も近いアクセス ポイントの場所を示すマップを表示できます。その後、それらを Known または Acknowledged 不正アクセス ポイントとしてマークする（追加の処置はなし）、それらを Alert 不正アクセス ポイントとしてマークする（監視し、アクティブになったときに通知）、それらを Contained 不正アクセス ポイントとしてマークする（1 ～ 4 台のアクセス ポイントから、不正アクセス ポイントのクライアントが不正アクセス ポイントとアソシエートするたびにそれらのクライアントに認証解除とアソシエート解除のメッセージを送信することによって封じ込め処理を行う）のいずれかを実行します。

この組み込み型の検出、タギング、モニタリング、および封じ込めの機能を使用すると、システム管理者は、次に挙げる適切な処理を実行できます。

- 不正アクセス ポイントを特定します。
- 新しい不正アクセス ポイントの通知を受け取ります（通路をスキャンして歩く必要なし）。
- 不明な不正アクセス ポイントが削除または認識されるまでモニタします。
- 最も近い場所の許可済みアクセス ポイントを特定して、高速かつ効果的に誘導スキャンを行えるようにします。
- 1 ～ 4 台のアクセス ポイントから、不正アクセス ポイントのクライアントに認証解除とアソシエーション解除のメッセージを送信して、不正アクセス ポイントを封じ込めます。この封じ込め処理は、MAC アドレスを使って個々の不正アクセス ポイントに対して行うことも、企業サブネットに接続されているすべての不正アクセス ポイントに対して要求することもできます。
- 不正アクセス ポイントにタグを付けます。
  - 不正アクセス ポイントが LAN の外部にあり、LAN または無線 LAN のセキュリティを脅かさない場合は承諾します。
  - 不正アクセス ポイントが LAN または無線 LAN のセキュリティを脅かさない場合は容認します。
  - 不正アクセス ポイントが削除または認識されるまで、未知（管理対象外）のアクセス ポイントとしてタグ付けします。
- 不正アクセス ポイントを封じ込め処理済みとしてタグ付けし、1 ～ 4 台のアクセス ポイントから、すべての不正アクセス ポイント クライアントに認証解除およびアソシエーション解除のメッセージを転送することにより、クライアントが不正アクセス ポイントにアソシエートしないようにします。この機能は、同じ不正アクセス ポイント上のすべてのアクティブなチャネルに適用されます。

アクセス ポイントの検出

不正アクセス ポイントを検出している Cisco Lightweight アクセス ポイントに関する情報を表示するには、アクセス ポイントの検出機能を使用します。

[Rogue AP Alarms] 詳細ページにアクセスするには、次の手順を実行します。

ステップ 1　[Rogue AP Alarms] ページを表示するには、次のいずれかを実行します。

- 不正 AP の検索を実行します。この検索機能の詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。このダッシュボードには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- [Alarm Summary] ボックスの [Malicious AP] の件数のリンクをクリックします。

ステップ 2　[Rogue AP Alarms] ページで、該当する不正アクセス ポイントの [Rogue MAC Address] をクリックします。[Rogue AP Alarms] 詳細ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから [Detecting APs] を選択します。

ステップ 4　[Go] をクリックします。

いずれかのリスト項目をクリックすると、その項目に関するデータが表示されます。

- AP Name

- Radio
- Map Location
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [WEP]：有効または無効。
- [WPA]：有効または無効。
- [Pre-Amble]：Long（長型）または Short（短型）。
- [RSSI]：受信信号強度インジケータ（dBm）。
- [SNR]：信号対雑音比。
- [Containment Type]：このアクセス ポイントによる封じ込め処理のタイプ。
- [Containment Channels]：このアクセス ポイントが現在封じ込め処理を実行しているチャネル。

不正アラーム イベントのモニタリング

[Events] ページでは、不正アラーム イベントに関する情報を参照できます。Prime Infrastructure では、不正アクセス ポイントが検出されるか、不正アクセス ポイントが手動で変更（状態の変更など）された場合に、イベントが生成されます。[Rogue AP Events] リスト ページには、すべての不正アクセス ポイント イベントが表示されます。

[Rogue AP Events] リスト ページにアクセスするには、次の手順を実行します。

ステップ 1　次のいずれかを実行します。

- Prime Infrastructure の Advanced Search 機能を使用して不正アクセス ポイント イベントを検索します。詳細については、「Advanced Search」（P.2-55）を参照してください。
- [Rogue AP Alarms] 詳細ページで、[Select a command] ドロップダウン リストから [Event History] をクリックします。詳細については、「不正 AP アラーム詳細の表示」（P.5-96）を参照してください。

ステップ 2　[Rogue AP Events] リスト ページには、次のイベント情報が表示されます。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Rogue MAC Address]：[Rogue AP Event Details] ページを表示するには、不正な MAC アドレスをクリックします。詳細については、「不正 AP イベントの詳細の表示」（P.5-110）を参照してください。
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [Classification Type]：Malicious、Friendly、Unclassified。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。

- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Date/Time]：イベントが生成された日時。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。

不正 AP イベントの詳細の表示

不正アクセス ポイント イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Rogue AP Events] リスト ページで、[Rogue MAC Address] リンクをクリックします。

ステップ 2　[Rogue AP Events Details] ページに、次の情報が表示されます。

- Rogue MAC address
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Classification Type]：Malicious、Friendly、Unclassified。
- [State]：アラームの状態を示します。可能な状態は、不正アクセス ポイントの分類タイプによって異なります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [Containment Level]：不正アクセス ポイントの封じ込めレベル、または Unassigned（未割り当て）。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Created]：イベントが生成された日時。
- [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。
  - [NMS (Network Management System - Prime Infrastructure)]：ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。
  - [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。
- デバイスの IP アドレス
- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Message]：現在のイベントの詳細を示します。

アドホック不正イベントのモニタリング

[Events] ページでは、アドホック不正イベントに関する情報を参照できます。アドホック不正が検出されるか、アドホック不正を手動で変更した場合（その状態を変更するなど）、Prime Infrastructure によりイベントが生成されます。[Adhoc Rogue Events] リスト ページには、すべてのアドホック不正イベントが表示されます。

[Rogue AP Events] リスト ページにアクセスするには、次の手順を実行します。

ステップ 1　次のいずれかを実行します。

- Prime Infrastructure の Advanced Search 機能を使用してアドホック不正イベントを検索します。詳細については、「Advanced Search」（P.2-55）を参照してください。
- [Adhoc Rogue Alarms] 詳細ページで、[Select a command] ドロップダウン リストから [Event History] をクリックします。詳細については、「アドホック不正アラームの詳細の表示」（P.5-105）を参照してください。

ステップ 2　[Rogue AP Events] リスト ページには、次のイベント情報が表示されます。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Rogue MAC Address]：[Rogue AP Event Details] ページを表示するには、不正な MAC アドレスをクリックします。詳細については、「アドホック不正イベントの詳細の表示」（P.5-111）を参照してください。
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Date/Time]：イベントが生成された日時。
- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。

アドホック不正イベントの詳細の表示

不正アクセス ポイント イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Rogue AP Events] リスト ページで、[Rogue MAC Address] リンクをクリックします。

ステップ 2　[Rogue AP Events Details] ページに、次の情報が表示されます。

- Rogue MAC Address
- [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。

  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Channel Number]：不正アクセス ポイントがブロードキャストしているチャネル。
- [Containment Level]：不正アクセス ポイントの封じ込めレベル、または Unassigned（未割り当て）。
- [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Created]：イベントが生成された日時。
- [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。
  - [NMS (Network Management System - Prime Infrastructure)]：ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。
  - [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。
- デバイスの IP アドレス
- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Message]：現在のイベントの詳細を示します。

未接続アクセス ポイントのトラブルシューティング

Lightweight アクセス ポイントは、初回起動時に、無線 LAN コントローラを検出し、接続しようとします。アクセス ポイントは、ワイヤレス コントローラに接続した後、必要に応じてそのソフトウェア イメージを更新し、デバイスとネットワークの構成の詳細をすべて受信します。アクセス ポイントが正常にワイヤレス コントローラを接続した後、そのアクセス ポイントは Prime Infrastructure で検出および管理できます。アクセス ポイントが正常にワイヤレス コントローラを接続するまで、そのアクセス ポイントは Prime Infrastructure で管理できないため、クライアント アクセスを可能にする適切な設定は組み込まれません。

Prime Infrastructure は、アクセス ポイントがコントローラに接続できない理由を診断し、対処方法を一覧表示するツールを提供しています。

[Unjoined AP] ページには、ワイヤレス コントローラに接続していないアクセス ポイントが一覧表示されます。このページには、未接続アクセス ポイントについて収集されたすべての情報が含まれます。この情報には、名前、MAC アドレス、IP アドレス、コントローラの名前と IP アドレス、アクセス ポイントの接続先のスイッチとポート、および接続が失敗した理由（判明している場合）が含まれます。

未接続アクセス ポイントのトラブルシューティングを行うには、次の手順を実行します。

ステップ 1　[Monitor] > [Unjoined APs] の順に選択します。[Unjoined APs] ページが表示され、ワイヤレス コントローラに接続できなかったアクセス ポイントの一覧が表示されます。

ステップ 2　診断するアクセス ポイントを選択し、[Troubleshoot] をクリックします。アクセス ポイントに対して分析が実行され、アクセス ポイントがワイヤレス コントローラに接続できなかった理由が特定されます。分析の実行後、[Unjoined APs] ページに結果が表示されます。

ステップ 3　アクセス ポイントが複数のワイヤレス コントローラに接続しようとし、失敗した場合、それらのコントローラが左ペインに一覧表示されます。コントローラを選択します。

ステップ 4　中央のペインで、問題を確認できます。このペインには、エラー メッセージとコントローラのログ情報も一覧表示されます。

ステップ 5　右側のペインに、問題を解決するための推奨事項が表示されます。推奨処置を実行します。

ステップ 6　さらに問題を診断する必要がある場合、[Unjoined AP] ページから RTTS を実行できます。これにより、アクセス ポイントが同時に接続しようとしたすべてのワイヤレス コントローラからのデバッグ メッセージが表示されます。

RTTS を実行するには、テーブルの右側にある RTTS のアイコン（  ）をクリックします。デバッグ メッセージがテーブルに表示されます。次に、メッセージを検証して、アクセス ポイントがコントローラに接続できない原因を特定できるかどうか判別できます。

RFID タグのモニタリング

[Monitor] > [RFID Tags] ページでは、タグの詳細の確認に加えて、タグ ステータスと Prime Infrastructure マップ上のロケーションをモニタできます。

（注）　このページは、Prime Infrastructure の Location バージョンのみで使用できます。

このセクションには、ロケーション アプライアンスにより検出されるタグについての情報が表示されます。

このセクションにアクセスするには、[Monitor] > [RFID Tags] の順に選択します。デフォルトでは、タグの概要ページが表示されます。

ここでは、次の内容について説明します。

- 「タグの概要」（P.5-113）
- 「タグの検索」（P.5-114）
- 「RFID タグの検索結果の表示」（P.5-114）
- 「タグ リストの表示」（P.5-115）

タグの概要

このページにアクセスするには、[Monitor] > [RFID Tags] の順に選択します。

このページには、MSE によって検出されたタグの数に関する情報が表示されます。メイン データ領域には次のフィールドが表示されます。

- [Device Name]：MSE デバイスの名前。
- [Total Tags]：タグの詳細を表示するには数値をクリックします。数値をクリックすると、MSE によって検出されたタグの一覧が表示されます。MAC アドレスをクリックすると、その MAC アドレスに関係するタグの詳細が表示されます。

タグの検索

特定のタグまたはすべてのタグを探すには、Prime Infrastructure の Advanced Search 機能を使用します。

Prime Infrastructure でタグを検索するには、次の手順を実行します。

ステップ 1　[Advanced Search] をクリックします。

ステップ 2　[Search Category] ドロップダウン リストから [Tags] を選択します。

ステップ 3　次のものを含む該当するタグ検索フィールドを識別します。

- [Search By] : [All Tags]、[Asset Name]、[Asset Category]、[Asset Group]、[MAC Address]、[Controller]、[MSE]、[Floor Area]、または [Outdoor Area] を選択します。

（注）　[Search] フィールドは、選択したカテゴリによって変わる可能性があります。該当する場合は、[Search By] カテゴリの識別に役立つように、追加のフィールドまたはフィルタ情報を入力します。

- [Search In] : MSE または Prime Infrastructure コントローラを選択します。
- [Last detected within] : 増分する時間を 5 分から 24 時間の間で選択します。デフォルト値は、15 分です。
- [Tag Vendor] : このチェックボックスを選択して、[Aeroscout]、[G2]、[PanGo]、または [WhereNet] を選択します。
- [Telemetry Tags only] : テレメトリ タグを検索するには、[Telemetry Tags only] チェックボックスをオンにします。

ステップ 4　[Go] をクリックします。

RFID タグの検索結果の表示

Prime Infrastructure ページの右上にある Prime Infrastructure Advanced Search 機能を使用して、アセット タイプ（名前、カテゴリ、およびグループ）、MAC アドレス、システム（コントローラまたはロケーション アプライアンス）、および領域（フロア領域および屋外領域）を条件としてタグを検索します。

（注）　[Search] フィールドは、選択したカテゴリによって変わる可能性があります。該当する場合は、[Search By] カテゴリの識別に役立つように、追加のフィールドまたはフィルタ情報を入力します。

Advanced Search の各フィールドを使用して、さらに検索を微調整し、将来使用するために検索条件を保存できます。保存した検索条件は、ナビゲーション バーにある [Saved Searches] から取得できます。

詳細については、「Advanced Search」（P.2-55）および「Saved Search」（P.2-67）を参照してください。

検索結果ページでタグの場所の MAC アドレスをクリックすると、タグの次の詳細が表示されます。

- タグ ベンダー

（注）　このオプションは、タグの検索条件が [Asset Name]、[Asset Category]、[Asset Group]、または [MAC Address] の場合は表示されません。

- タグが関連付けられているコントローラ
- テレメトリ データ（CCX v1 準拠のタグのみ）
  - 表示されるテレメトリ データはベンダー固有ですが、GPS の場所、バッテリー拡張情報、圧力、温度、湿度、動作、ステータス、および緊急コードなど、いくつかの内容が共通して報告されます。

（注）　テレメトリ データ オプションは、[Search for tags by] オプションで [MSE]（ロケーション サーバで選択）、[Floor Area]、または [Outdoor Area] が選択されている場合にのみ表示されます。

（注）　テレメトリをサポートしているベンダー タグのみが表示されます。

- 資産情報（名前、カテゴリ、グループ）
- 統計情報（受信したバイトとパケット）
- 場所（フロア、最終場所、MSE、マップ）
- 場所の通知（不在、封じ込め、距離、すべて）

（注）　表示されるテレメトリ データはベンダー固有ですが、GPS の場所、バッテリー拡張情報、圧力、温度、湿度、動作、ステータス、および緊急コードなど、いくつかの内容が共通して報告されます。

- 緊急データ（CCX v1 準拠のタグのみ）

タグ リストの表示

[Total Tags number] リンクをクリックすると、該当するデバイス名のタグ リストが表示されます。タグ リストには次の情報が含まれています。

- MAC Address
- Asset Name
- Asset Group
- Asset Category
- Vendor Name
- Mobility Services Engine
- Controller
- Battery Status
- Map Location

チョークポイントのモニタリング

チョークポイントは、チョークポイントのベンダーによって推奨されるとおりに設置および設定されます。チョークポイントの設置が完了し、動作するようになった後は、チョークポイントを Prime Infrastructure に追加して、フロア マップに配置できます。同期を実行中に、これらがロケーション サーバにプッシュされます。

[Monitor] > [Chokepoints] の順に選択します。見つかったチョークポイントの一覧が表示されたページが開きます。特定のチョークポイントの [Map Location] 欄からリンクをクリックすると、そのチョークポイントの位置を示すマップが表示されます。

次のフィールドが表示されます。

- [MAC Address]：チョークポイントの MAC アドレス。
- [Chokepoint Name]：ユーザが定義したチョークポイント名。
- [Entry/Exit Chokepoint]：チョークポイントが Entry/Exit チョークポイントかどうかを示します。
- [Range]：チョークポイントの範囲（フィート単位）。
- [Static IP]：チョークポイントのスタティック IP アドレス。
- [Map Location]：チョークポイントの位置を示すマップへのリンク。

チョークポイントの検索

高度な検索では、チョークポイントを検索できます。

Prime Infrastructure でチョークポイントの高度な検索を行うには、次の手順を実行します。

ステップ 1　Prime Infrastructure の右上隅にある [Advanced Search] をクリックします。

ステップ 2　[New Search] ページで、[Search Category] ドロップダウン リストから [Chokepoint] を選択します。

ステップ 3　[Search for Chokepoint by] ドロップダウン リストから、検索する方法（MAC アドレスによる検索またはチョークポイント名による検索）を選択します。

ステップ 4　選択した検索方法に応じて、MAC アドレスまたはチョークポイント名を入力します。

ステップ 5　[Search] をクリックします。

干渉のモニタリング

[Monitor] > [Interferer] ページでは、CleanAir 対応アクセス ポイントにより検出された干渉デバイスをモニタできます。

この項では、CleanAir 対応アクセス ポイントにより検出される干渉について説明します。デフォルトでは、AP で検出された干渉のモニタリングページが表示されます。

ここでは、次の内容について説明します。

- 「AP で検出された干渉のモニタリング」（P.5-117）
- 「AP で検出した干渉源の詳細のモニタリング」（P.5-118）
- 「AP で検出した干渉源の詳細のロケーション履歴のモニタリング」（P.5-119）

- 「検索結果表示の設定」（P.5-119）

AP で検出された干渉のモニタリング

ワイヤレス ネットワーク上の CleanAir 対応アクセス ポイントにより検出されたすべての干渉デバイスを表示するには、[Monitor] > [Interferers] の順に選択します。このページには干渉デバイスの概要が表示されます。表示される概要には、次のデフォルト情報が含まれています。

- [Interferer ID]：干渉の固有識別子。これは、疑似乱数によって生成される ID です。この ID は、MAC アドレスに似ていますが、Bluetooth ヘッドセットで使用されるような実アドレスではありません。
- [Type]：干渉源のカテゴリを示します。デバイスのタイプの詳細を参照するには、ここをクリックします。ポップアップ ウィンドウに詳細が表示されます。次のカテゴリがあります。
  - [Bluetooth link]：Bluetooth リンク（802.11b/g/n のみ）
  - [Microwave Oven]：電子レンジ（802.11b/g/n のみ）
  - [802.11 FH]：802.11 周波数ホッピング デバイス（802.11b/g/n のみ）
  - [Bluetooth Discovery]：Bluetooth 検出（802.11b/g/n のみ）
  - [TDD Transmitter]：時分割複信（TDD）トランスミッタ
  - [Jammer]：電波妨害デバイス
  - [Continuous Transmitter]：連続トランスミッタ
  - [DECT-like Phone]：Digital Enhanced Cordless Communication（DECT）対応電話
  - [Video Camera]：ビデオ カメラ
  - [802.15.4]：802.15.4 デバイス（802.11b/g/n のみ）
  - [WiFi Inverted]：スペクトル反転 Wi-Fi 信号を使用するデバイス
  - [WiFi Invalid Channel]：非標準の Wi-Fi チャネルを使用するデバイス
  - [SuperAG]：802.11 SuperAG デバイス
  - [Canopy]：Motorola Canopy デバイス
  - [Radar]：レーダー デバイス（802.11a/n のみ）
  - [XBox]：Microsoft Xbox（802.11b/g/n のみ）
  - [WiMAX Mobile]：WiMAX モバイル デバイス（802.11a/n のみ）
  - [WiMAX Fixed]：WiMAX 固定デバイス（802.11a/n のみ）
  - [WiFi AOCI]：AOCI を使用する WiFi デバイス
  - Unclassified
- [Status]：干渉デバイスのステータスを示します。
  - [Active]：CleanAir 対応アクセス ポイントにより現在干渉源が検出されていることを示します。
  - [Inactive]：干渉源が CleanAir 対応アクセス ポイントで検出されなくなったか、Prime Infrastructure で到達不能になったことを示します。
- [Severity]：干渉デバイスの重大度ランクを示します。
- [Affected Band]：このデバイスが干渉している帯域を表示します。
- [Affected Channels]：影響を受けるチャネルを表示します。

- [Duty Cycle (%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- [Discovered]：検出された時刻を表示します。
- [Last Updated]：干渉源が最後に検出された時刻。
- [Floor]：干渉デバイスが存在していたロケーション。

AP で検出した干渉源の詳細のモニタリング

[Monitor] > [Interferers] > [*Interferer ID*] の順に選択し、このページを表示します。このページでは、アクセス ポイントにより検出された干渉デバイスの詳細情報が表示されます。このページには、干渉デバイスに関する次の詳細情報が表示されます。

- [Interferer Properties]
  - [Type]：AP により検出された干渉デバイスのタイプが表示されます。
- [Status]：干渉デバイスのステータス。干渉デバイスのステータスを示します。
  - [Active]：CleanAir 対応アクセス ポイントにより現在干渉源が検出されていることを示します。
  - [Inactive]：干渉源が CleanAir 対応アクセス ポイントで検出されなくなったか、Prime Infrastructure で到達不能になったことを示します。
  - [Severity]：干渉デバイスの重大度ランクを示します。
  - [Duty Cycle (%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
  - [Affected Band]：このデバイスが干渉している帯域を表示します。
  - [Affected Channels]：影響を受けるチャネルを表示します。
  - [Discovered]：検出された時刻を表示します。
  - [Last Updated]：干渉源が最後に検出された時刻。
- Location
  - [Floor]：この干渉デバイスが検出されたロケーション。
  - [Last Located At]：干渉デバイスが最後に検出された時刻。
  - [On MSE]：この干渉デバイスが検出されたモビリティ サーバ エンジン。
- Clustering Information
  - [Clustered By]：アクセス ポイントからの干渉情報を収集したコントローラまたは MSE の IP アドレスが表示されます。
  - [Detecting APs]：干渉デバイスを検出したアクセス ポイントの詳細情報を表示します。詳細情報には、[Access Point Name (Mac)]、[Severity]、および [Duty Cycle(%)] などが含まれます。
- [Details]：干渉タイプに関する短い説明を表示します。

Select a command

[Select a command] ドロップダウン リストでは、アクセス ポイントにより検出された干渉デバイスのロケーション履歴が表示されます。「AP で検出した干渉源の詳細のロケーション履歴のモニタリング」（P.5-119）を参照してください。

AP で検出した干渉源の詳細のロケーション履歴のモニタリング

このページを表示するには、[Monitor] > [Interferers] > [*Interference Device ID*] の順に選択し、[Select a command] ドロップダウン リストから [Location History] を選択し、[Go] をクリックします。

- [Interferer Information]：干渉デバイスに関する基本情報を表示します。
  - [Data Collected At]：データが収集された時点のタイムスタンプ。
  - [Type]：干渉デバイスのタイプ。
  - [Severity]：干渉デバイスの重大度インデックス。
  - [Duty Cycle]：干渉デバイスのデューティ サイクル（パーセンテージ）。
  - [Affected Channels]：影響を受けるチャネルのカンマ区切りリスト。
- [Interferer Location History]：干渉デバイスのロケーション履歴を表示します。
  - Time Stamp
  - Floor
- Clustering Information
  - Clustered By
- Detecting APs
  - [AP Name]：干渉デバイスを検出したアクセス ポイント。
  - [Severity]：干渉デバイスの重大度インデックス。
  - [Duty Cycle(%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- Location
  - [Location Calculated At]：この情報が生成された時点のタイムスタンプを表示します。
  - [Floor]：干渉デバイスのロケーション情報を表示します。
  - 干渉デバイスのロケーションがマップにグラフィカルに表示されます。イメージを拡大表示するには [Enlarge] リンクをクリックします。

検索結果表示の設定

[Edit View] ページでは、[AP Detected Interferers Summary] ページの列を追加、削除、並び替えできます。

[AP Detected Interferers] ページの列を編集するには、次の手順に従います。

ステップ 1　[Monitor] > [Interferers] の順に選択します。[AP Detected Interferers] ページが表示されます。このページには、CleanAir 対応アクセス ポイントにより検出された干渉源の詳細が表示されます。

ステップ 2　[Edit View] リンクをクリックします。

ステップ 3　アクセス ポイント表に新しい列を追加するには、左側の領域で、列見出しをクリックして選択します。[Show] をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。

ステップ 4　アクセス ポイント表から列を削除するには、右側の領域で、削除する列見出しをクリックして選択します。[Hide] をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。

ステップ 5　[Up] ボタンと [Down] ボタンを使用して、表内での情報の並び順を指定します。目的の列見出しを選択し、[Up] または [Down] をクリックして、現在のリスト内での位置を変更します。

ステップ 6　デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7　[Submit] をクリックして、変更内容を確定します。

Spectrum Expert のモニタ

Spectrum Expert クライアントは、リモート干渉センサーとして機能し、動的な干渉データを Prime Infrastructure に送信します。この機能により、Prime Infrastructure はネットワーク内の Spectrum Expert から詳細な干渉データと電波品質データを収集、保管、およびモニタできます。

[Monitor Spectrum Experts] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Spectrum Experts] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、Spectrum Expert の概要ページと干渉源の概要ページにアクセスできます。

Spectrum Expert の概要

[Spectrum Experts] > [Summary] ページはデフォルトのページであり、システムに追加された Spectrum Expert の表が表示されます。この表には、次の Spectrum Expert の情報が記載されています。

- [Hostname]：追加方法に応じて、ホスト名または IP アドレスが表示されます。Spectrum Expert の詳細ページにアクセスするには、ホスト名をクリックします。
- [Active Interferers]：Spectrum Expert により検出された現在の干渉源の数。
- [Affected APs]：検出された干渉源が潜在的な影響を及ぼしていると Spectrum Expert により確認されたアクセス ポイントの数。
- [Alarms]：Spectrum Expert から送信された Active Interference トラップの数。クリックすると、この Spectrum Expert のアクティブ アラームに対してフィルタリングされている [Alarm] ページへアクセスします。
- [Reachability Status]：Spectrum Expert が動作し Prime Infrastructure にデータを送信している場合は、緑色で「Reachable」と表示され、そうでない場合は赤で「Unreachable」と表示されます。
- [Location]：Spectrum がワイヤレス クライアントの場合は、Spectrum Expert の場所を示すリンクが表示されます。Spectrum Expert の周囲の赤いボックスは、有効な範囲を示します。クリックすると、マップに配置された最も近いアクセス ポイントにアクセスできます。

干渉源の概要

[Interferers] > [Summary] ページには、30 日間隔で検出されたすべての干渉源の一覧が表示されます。この表には、次のような干渉源の情報が記載されています。

- [Interferer ID]：異なる Spectrum Expert 間で一意の ID。これは、疑似乱数によって生成される ID です。MAC アドレスに似ていますが、実際のアドレスではなく、干渉デバイスの検出に使用できます。

- [Category]：干渉源のカテゴリ。カテゴリには、[Bluetooth]、[Cordless Phones]、[Microwave Ovens]、[802.11 FH]、[Generic - Fixed-Frequency]、[Jammers]、[Generic - Frequency-Hopped]、[Generic - Continuous] があります。
- [Type]：干渉源の種類を示します。クリックすると、種類の説明のポップアップにアクセスできます。
- [Status]：[Active] または [Inactive] を示します。
  - [Active]：干渉源が現在 Spectrum Expert で検出されていることを示します。
  - [Inactive]：Spectrum Expert で干渉源が検出されなくなったこと、または干渉源を検出した Spectrum Expert が Prime Infrastructure から到達不能になったことを示します。
- [Discover Time]：検出の時刻を示します。
- [Affected Channels]：影響を受けるチャネルを示します。
- [Number of APs Affected]：アクセス ポイントは、次の条件を満たす場合に [Affected] と表示されます。
  - アクセス ポイントが Prime Infrastructure で管理されている。
  - Spectrum Expect がアクセス ポイントを検出している。
  - Spectrum Expect がアクセス ポイントの稼働チャネル上の干渉源を検出している。
- [Power]：dBm で示されます。
- [Duty Cycle]：パーセントで示されます。

（注）　100 % は最悪値を示します。

- [Severity]：干渉源の重大度ランキングを示します。

（注）　100 % は最悪値を示し、0 は干渉源がないことを示します。

干渉源の検索

Prime Infrastructure の検索機能を使用して、特定の干渉源を検索することや、カスタム検索を作成して保存することができます。追加情報については、次のいずれかのトピックを参照してください。

- 「検索機能の使用方法」（P.2-54）
- 「Quick Search」（P.2-54）
- 「Advanced Search」（P.2-55）
- 「Saved Search」（P.2-67）

Spectrum Expert の詳細

[Spectrum Expert Details] ページには、単一の Spectrum Expert からの干渉源の詳細がすべて表示されます。このページは 20 秒ごとに更新され、リモート Spectrum Expert の状況がリアルタイムに表示されます。次の項目が含まれています。

- [Total Interferer Count]：特定の Spectrum Expert で検出された干渉源の数を示します。
- [Active Interferers Count Chart]：カテゴリごとに干渉源をグループ化した円グラフを表示します。

- [Active Interferer Count Per Channel]：別々のチャネル上のカテゴリごとにグループ化された干渉源の数を表示します。
- [AP List]：Spectrum Expert によってアクティブな干渉源が検出されたチャネル上にある、Spectrum Expert によって検出されたアクセス ポイントの一覧が表示されます。
- [Affected Clients List]：アクセス ポイント リストに表示されているいずれかのアクセス ポイントの無線に対して現在認証または関連付けられているクライアントの一覧が表示されます。

WiFi TDOA レシーバのモニタリング

WiFi TDOA レシーバをモニタするには、次の手順に従います。

ステップ 1　[Monitor] > [WiFi TDOA Receivers] の順に選択します。[WiFi TDOA Receiver] 概要ページに、マッピングされているすべての WiFI TDOA レシーバが表示されます。

ステップ 2　長いリストが表示された場合に検索条件を微調整するには、MAC アドレスまたはロケーション センサー名で検索できます。

a. MAC アドレスで TDOA レシーバの検索を開始するには、Prime Infrastructure で [Advanced Search] リンクをクリックします。[Search Category] ドロップダウン リストから [WiFi TDOA Receiver] を選択し、[Search by] ドロップダウン リストから [MAC Address] を選択します。TDOA レシーバの MAC アドレスをテキスト ボックスに入力し、[Search] をクリックします。

b. 名前で TDOA レシーバの検索を開始するには、Prime Infrastructure で [Advanced Search] リンクをクリックします。[Search Category] ドロップダウン リストから [WiFi TDOA Receiver] を選択し、[Search by] ドロップダウン リストから [WiFi TDOA Receivers] を選択します。TDOA レシーバの名前をテキスト ボックスに入力し、[Search] をクリックします。

一致するものがない場合、その旨を示すメッセージがページに表示されます。そうでない場合は検索結果が表示されます。

（注）　Prime Infrastructure の検索機能の詳細については、「検索機能の使用方法」（P.2-54）または「Advanced Search」（P.2-55）を参照してください。

[WiFi TDOA Receivers] ページには、次の情報が表示されます。

- MAC Address
- WiFi TDOA Receiver Name
- [Static IP]：WiFi TDOA レシーバのスタティック IP アドレス。
- [Oper Status]：[Up] または [Down]。
- [Map Location]：[Map Location] リンクをクリックすると、この WiFi TDOA レシーバのフロア マップが表示されます。Prime Infrastructure フロア マップの詳細については、「フロア領域のモニタリング」を参照してください。

（注）　WiFi TDOA レシーバの追加、設定、編集の詳細については、「Wi-Fi TDOA 受信機の設定」（P.6-197）を参照してください。

メディア ストリームのモニタリング

メディア ストリームの設定をモニタするには、次の手順を実行します。

ステップ 1　[Monitor] > [Media Streams] の順に選択します。[Media Streams] ページが開き、コントローラ全体で設定されているメディア ストリームの一覧が表示されます。

[Media Streams] ページには、次の列を含む表が表示されます。

- [Stream Name]：メディア ストリーム名。
- [Start IP]：Multicast Direct 機能が有効になっているメディア ストリームの開始 IP アドレス。
- [End IP]：Multicast Direct 機能が有効になっているメディア ストリームの終了 IP アドレス。
- [State]：メディア ストリームの動作状態。
- [Max Bandwidth]：メディア ストリームに割り当てられている最大帯域幅を示します。
- [Priority]：メディア ストリームに設定されているプライオリティ ビットを示します。プライオリティは 1 ～ 8 の任意の数字です。値が小さいほど、プライオリティは高くなります。たとえば、プライオリティ 1 が最も高く、値 8 は最も低くなります。
- [Violation]：違反の場合に実行すべき処置を示します。表示される値は次のとおりです。
  - [Drop]：定期的な再評価時にストリームがドロップされることを示します。
  - [Best Effort]：定期的な再評価時にストリームがベストエフォート クラスにデモートされることを示します。
- [Policy]：メディア ストリーム ポリシーを示します。取り得る値は [Admit] または [Deny] です。
- [Controllers]：指定されたメディア ストリームを使用するコントローラの数を示します。
- [Clients]：指定されたメディア ストリームを使用するクライアントの数を示します。

ステップ 2　メディア ストリームの詳細を表示するには、[Stream] 列のメディア ストリーム名をクリックします。[Media Streams] ページが表示されます。

[Media Streams] ページには、次のグループ ボックスが表示されます。

- [Media Stream Details]：メディア ストリームの設定情報が表示されます。これには、[Name]、[Start Address]、[End Address]、[Maximum Bandwidth]、[Operational Status]、[Average Packet Size]、[RRC Updates]、[Priority]、および [Violation] が含まれます。
- [Statistics]：選択したメディア ストリームを使用するコントローラとクライアントの数が表示されます。コントローラ数をクリックすると、選択したメディア ストリームを使用するコントローラの一覧にアクセスできます。
- [Error]：エラー、最低 AP、およびその AP に対応するフロア マップが表示されます。
- [Client Counts]：各期間のクライアント数が表示されます。
- [Failed Client Counts]：各期間に障害になったクライアント数が表示されます。

（注）　クライアント情報は、時間ベースのグラフに表示されます。時間ベースのグラフでは、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。

無線リソース管理（RRM）のモニタリング

オペレーティング システムのセキュリティ ソリューションでは、無線リソース管理（RRM）機能を使用して、すべての近隣アクセス ポイントを継続的にもモニタし、不正アクセス ポイントを自動的に検出します。

無線リソース管理（RRM）は Cisco Unified Wireless Network に組み込まれており、RF 環境で見つかったパフォーマンス上の問題をモニタし動的に修正します。

Prime Infrastructure は、アクセス ポイントの送信電力またはチャネルが変化したときにトラップを受信します。こうしたトラップ イベントまたは RF の再グループ化などの同様のイベントは、Prime Infrastructure イベントに通知として記録され、イベント ディスパッチャによって保持されました。近隣のアクセス ポイントからの信号、干渉、ノイズ、負荷など、送信電力またはチャネルの変化の理由は明らかではありませんでした。これらのイベントや統計を表示してトラブルシューティングを実行できませんでした。

無線リソース管理（RRM）統計情報は、問題のある箇所を特定するために役立ち、チャネルまたは電力レベルの変化の理由を提供します。ダッシュボードは、ネットワーク全体の RRM パフォーマンスの統計を示し、イベントのグループ化（パフォーマンスが最も悪いアクセス ポイント、同一 RF グループ内のコントローラ間の設定の不一致、しきい値に基づいてアクセス ポイントによって検出されたカバレッジ ホール、コントローラで検出されたプレカバレッジ ホール、最大電力で動作しているアクセス ポイントの割合など）に基づいてチャネルの変更を予測します。

（注）　RRM ダッシュボードの情報は、Lightweight アクセス ポイントのみで使用できます。

ここでは、次の内容について説明します。

- 「チャネルの変更通知」（P.5-124）
- 「送信電力変更通知」（P.5-125）
- 「RF グループ化通知」（P.5-125）
- 「RRM ダッシュボードの表示」（P.5-125）

チャネルの変更通知

チャネルが変更されると、Prime Infrastructure RRM ダッシュボードに通知が送信されます。チャネルの変更は、モードを [auto] または [on demand] に設定できる動的チャネル割り当て（DCA）設定によって異なります。モードが [auto] の場合、この操作を許可するすべての Lightweight アクセス ポイントに対し、チャネル割り当てが定期的に更新されます。モードが [on demand] に設定されている場合、要求に基づいてチャネル割り当てが更新されます。DCA が静的である場合、動的チャネル割り当ては行われず、値はグローバル デフォルトに設定されます。

チャネル変更のトラップが受信され、チャネル変更が前に行われている場合、イベントは [Channel Revised] とマークされます。そうでない場合、[Channel Changed] とマークされます。チャネル変更の各イベントには、いくつかの理由があります。原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。たとえば、チャネル変更が信号、干渉、またはノイズによって発生するとします。原因コードが通知として受信されたときに、すべての原因を対象として原因コードの係数が変更されます。そのイベントの理由が 3 つある場合は、原因コードの係数は理由 1 つあたり 1/3 または 0.33 に変更されます。10 件のチャネル変更イベントが同じ原因コードで受信された場合、3 つの原因コードすべてに同じ係数が与えられて、チャネル変更の原因が判定されます。

送信電力変更通知

送信電力が変更されると、Prime Infrastructure RRM ダッシュボードに通知が送信されます。送信電力変更の各イベントには、いくつかの理由があります。原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。

RF グループ化通知

RRM がコントローラに実行されると、動的グループ化が行われ、新しいグループ リーダーが選択されます。動的グループ化には、Automatic、Off、および Leader の 3 つのモードがあります。グループ化を Off にすると、動的グループ化は行われなくなり、各スイッチは自身の Lightweight アクセス ポイント パラメータのみを最適化します。グループ化を Automatic にすると、スイッチはグループを形成し、リーダーを選択してより適切な動的パラメータの最適化を実行します。グループ化を Automatic にすると、設定した間隔（秒）はグループ化アルゴリズムが実行される期間を示します。（グループ化アルゴリズムは、グループに変更があり、自動グループ化が有効である場合にも実行されます）。

RRM ダッシュボードの表示

RRM ダッシュボードにアクセスするには、[Monitor] > [Radio Resource Management] の順に選択します。

このダッシュボードは、次の部分で構成されています。

- [RRM RF Group Summary] には、異なる RF グループの数が表示されます。

  （注）　最新の RF グループ数を取得するには、設定の同期バックグラウンド タスクを実行する必要があります。

- [RRM Statistics] 部分には、ネットワーク全体の統計が表示されます。
- [Channel Change Reason] 部分には、802.11a/b/g/n 無線のチャネルが変更した理由が表示されます。
  - 信号：他のいくつかの近隣する無線のチャネル品質が改善されたためにチャネルが変更されました。他のいくつかの近隣無線のチャネル品質の改善により、アルゴリズムによって評価されるシステムのチャネル計画が改善しました。
  - WiFi 干渉
  - ロード
  - レーダー
  - ノイズ
  - 固定的 Non-WiFi 干渉
  - 主要な電波品質イベント
  - その他
- [Channel Change] には、完了したすべてのイベントが原因とともに表示されます。
- [Configuration Mismatch] 部分には、リーダーとメンバの比較が表示されます。
- [Coverage Hole] 部分には、カバレッジ ホールがどれほど深刻かを評価し、その位置を示します。
- [Percent Time at Maximum Power] には、アクセス ポイントが最大電力に達した時間の割合が表示され、これらのアクセス ポイントを示します。

次の統計情報が表示されます。

- [Total Channel Changes]：チャネルが更新または変更されたかどうかに関係なく、802.11a/b/g/n 無線のチャネル変更数の合計。カウントは、24 時間および 7 日間の期間に分割されます。割合のリンクまたは [24-hour] 列の下にあるリンクをクリックすると、そのアクセス ポイントのみの詳細を示すページが表示されます。
- [Total Configuration Mismatches]：24 時間に検出された設定の不一致数の合計。
- [Total Coverage Hole Events]：24 時間および 7 日間のカバレッジ ホール イベント数の合計。
- [Number of RF Groups]：RF グループの総数（現在 Prime Infrastructure によって管理されているすべてのコントローラから計算されます）。
- [Configuration Mismatch]：24 時間に発生した設定の不一致を RF グループごとにグループ リーダーの詳細とともに表示します。
- [APs at MAX Power]：802.11a/n 無線のアクセス ポイントの割合を、最大電力に達したすべてのアクセス ポイントの割合の合計として表示します。最大電力レベルはプリセットされ、プリセット値を基準にして計算されます。

（注） 最大電力は、RRM ダッシュボードの 3 つの領域に表示されます。この最大電力の部分には、現在の値が表示され、ポーリングされます。

- [Channel Change Causes]：802.11a/n 無線のグラフィック棒グラフ。グラフは、チャネル変更が行われた理由に基づいて作成されます。グラフは 2 つの部分に分割され、それぞれ 24 時間および 7 日間に発生するイベントを引き起こす理由の重み付けされた理由の割合を示します。チャネル変更の各イベントにはいくつかの理由があり、その重みはそれらの理由に均等に分けられます。ネット原因コードは、イベントが発生した理由の数に関係なく、1 という係数が与えられます。
- [Channel Change - APs with channel changes]：チャネル変更の各イベントには、Lightweight アクセス ポイントの MAC アドレスが含まれます。各理由コードについて、チャネル イベントの重み付き理由に基づいて 802.11a/n アクセス ポイントに発生したチャネル変更の多くが表示されます。カウントは、24 時間および 7 日間の期間に分割されます。
- [Coverage Hole - APs reporting coverage holes]：カバレッジ ホール イベント（しきい値に基づく）を生成した、IF Type 11 a/n でフィルタされた上位 5 つのアクセス ポイントが表示されます。
- [Aggregated Percent Max Power APs]：カバレッジ ホール イベントを調整するために最大電力で動作している 802.11a/n Lightweight アクセス ポイントの割合の合計を示すグラフィカルな進捗状況グラフ。カウントは、24 時間および 7 日間の期間に分割されます。

（注） この最大電力の部分には、最近 24 時間の値が表示され、ポーリング主導となります。これは、15 分ごとまたは無線パフォーマンスの設定に応じて発生します。

- [Percent Time at Maximum Power]：最大電力で動作している上位 5 つの 802.11a/n Lightweight アクセス ポイントのリスト。

（注） この最大電力の部分には、最近 24 時間の値が表示され、イベント ドリブンのみです。

クライアントとユーザのモニタリング

Monitor Clients and Users 情報は、クライアントの問題の識別、診断、解決に役立ちます。Monitor Clients and Users 機能を使用して、クライアント アソシエーション履歴と統計情報を表示できます。また、クライアントの履歴上の問題をトラブルシューティングすることもできます。これらのツールは、ユーザがラップトップ コンピュータを持って建物の中を移動したときに、ネットワークのパフォーマンスについて苦情があった場合に有用です。この情報は、カバレッジが一貫していないエリアや、カバレッジがドロップする可能性があるエリアを評価するために役立ちます。詳細については、「クライアントの管理」（P.10-559）を参照してください。

アラームのモニタリング

ここでは、次の内容について説明します。

アラームとイベントの概要

イベントとは、ネットワーク内やその周辺である状態が発生すること、およびこれを検出することです。たとえば、しきい値を超えた無線干渉、新たな不正アクセス デバイスの検出、コントローラのリブートなどが報告されます。

イベントは、パターンの一致が発生するたびにコントローラによって生成されるわけではありません。パターンに一致するものの中には、報告間隔内に特定の回数発生しなければ攻撃の可能性があると見なされないものもあります。このようなパターン マッチのしきい値は、シグニチャ ファイルで設定します。イベントが発生するとアラームが生成されます。さらに、そのように設定されている場合は、電子メール通知を生成することもできます。

アラームは、1 つ以上の関連イベントへの Prime Infrastructure 応答です。イベントの重大度（重大、やや重大、比較的重大でない、または警告）が高いと見なされた場合、Prime Infrastructure はその状態が発生しなくなるまでアラームを発生させます。たとえば、不正アクセス ポイントが検出されている間はアラームが発生する場合がありますが、不正アクセス ポイントが数時間検出されないと、アラームは終了します。

1 つまたは複数のイベントで、発生するアラームが 1 つの場合もあります。アラームへのイベントのマッピングでは、それらの相関関係が作用します。たとえば、Intrusion Detection System（IDS; 侵入検知システム）のいくつかのイベントはネットワーク規模と見なされるため、どのアクセス ポイントからイベントが報告されているかに関係なく、その種類のすべてのイベントは、1 つのアラームにマップされます。その一方で、ほかの IDS イベントはクライアント固有のイベントです。これらの場合、特定のクライアント MAC アドレスのその種類のすべてのイベントは、複数のアクセス ポイントが同じ IDS 違反を報告したとしても、そのクライアント MAC アドレス固有のアラームにマップされます。同じ種類の IDS 違反が異なるクライアントに発生した場合は、異なるアラームが発生します。

現時点では、Prime Infrastructure 管理者は、どのイベントでアラームを生成するか、またはいつそれらをタイムアウトするかについては制御できません。コントローラ上では、個々の種類のイベントを有効または無効にできます（管理、SNMP、トラップ制御など）。

アラームの一覧の表示

アラームの一覧が表示された [Alarm Browser] ページにアクセスするには、[Monitor] > [Alarms] に順に選択します。また、Prime Infrastructure ページの下部にあるツールバーの [Alarm Browser] にマウス カーソルを合わせることでも、[Alarm Browser] ページを表示できます。

[Alarm Browser] には、各アラームの次の情報が表示されます。

- [Severity] : アラームの重大度。次のものがあります。
  - Critical
  - Major
  - Minor
  - Warning
  - Informational
- [Status] : アラームのステータス。
- [Timestamp] : アラームが発生した日時。
- [Category] : アラームに割り当てられているカテゴリ。不正 AP、コントローラ、スイッチ、セキュリティなどがあります。
- [Condition] : アラームの原因となった条件。
- [Owner] : このアラームが割り当てられている個人の名前（入力されている場合）。
- [Message] : アラームに関するメッセージ。
- [Failure Source] : イベントのソース（名前や MAC アドレスを含む）を示します。

（注）　デフォルトでは、認知済みのアラームは [Alarm Browser] ページに表示されません。この動作を変更するには、[Administration] > [Settings] > [Alarms] の順に選択し、[Hide Acknowledged Alarms] チェックボックスをオフにします。[Prime Infrastructure Alarm Summary] およびアラーム リスト ページに認知済みアラームを表示する場合は、このチェックボックスをオフにする必要があります。

チェックボックスを使用して 1 つ以上のアラームを選択します。[Alarm Browser] に表示されているすべてのアラームを選択するには、一番上のボックスをクリックします。詳細については、「アラームの変更」（P.5-131）を参照してください。

アラームのフィルタリング

[Monitor] > [Alarms] ページで、[Alarm Browser] に表示されるアラームをフィルタリングできます。

[Monitor] > [Alarms] の順に選択し、[Show] ドロップダウン リストから、次のいずれかのフィルタを選択します。

- [Quick Filter]：入力したテキストを含むアラームを表示するには、いずれかのボックスにテキストを入力します。たとえば、[Category] フィールドに AP と入力した場合、AP アラームと不正 AP アラームが表示されます。有線アラームとワイヤレス アラームのフィルタリングされたビューがオプションで表示されます。
- [Advance Filter]：このフィルタは、高度なアラーム検索機能を提供します。さまざまな条件（「含む」、「含まない」、「～で始まる」、「～で終わる」など）を使用して、特定のフィールドを検索できます。また、高度なフィルタでは、AND/OR 条件のネストが可能です。カテゴリと演算子を選択し、テキスト フィールドに比較のための条件を入力し、次のいずれかを実行します。
  - [+] をクリックしてフィルタを追加するか、[-] をクリックして指定したフィルタを削除します。
  - フィルタを適用するには [Go] をクリックします。
  - 入力したエントリをクリアするには [Clear Filter] をクリックします。
  - フィルタを保存するには [disc] アイコンをクリックします。保存するフィルタの名前を入力し、[Save] をクリックします。

（注）　プリセット フィルタを選択してフィルタ ボタンをクリックすると、フィルタ条件は無効になります。フィルタ条件は表示されるものの、変更できません。[All] を選択してすべてのエントリを表示した場合、フィルタ ボタンをクリックすると [Quick Filter] オプションが表示され、フィルタ可能なフィールドを使用してデータをフィルタリングできます。また、自由形式のボックスを使用して、表をフィルタリングするためのテキストを入力できます。

- [All]：すべてのアラームが表示されます。
- [Manage Preset Filter]：以前保存したフィルタの表示と、以前保存したフィルタの編集および削除が可能です。
- [Assigned to Me]：自分に割り当てられたすべてのアラームが表示されます。
- [Unassigned Alarms]：割り当てられていないすべてのアラームが表示されます。
- Alarms in Last 5 Minutes
- Alarms in Last 15 Minutes
- Alarms in Last 30 Minutes
- Alarms in the last hour
- Alarms in the last 8 hours
- Alarms in the last 24 hours
- Alarms in last 7 days
- [All wired alarms]：有線デバイスのすべてのアラームが表示されます。

- [All wireless alarms]：ワイヤレス デバイスのすべてのアラームが表示されます。

アラームのエクスポート

アラームのリストを簡単に CSV ファイル（各値がカンマで区切られたスプレッドシート形式のファイル）にエクスポートできます。

（注）　アラームの表に表示されている列のみが CSV ファイルにエクスポートされます。

アラームのリストをエクスポートするには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] の順に選択します。

ステップ 2　ツールバーで アイコンをクリックします。ポップアップ ウィンドウが表示されます。

ステップ 3　[File Download] ウィンドウで、[Save] をクリックしてファイルを保存します。

アラーム詳細の表示

[Monitor] > [Alarms] ページの左端にある、詳細を表示するアラームの展開アイコンをクリックすることで、[Monitor] > [Alarms] ページでアラームの詳細を表示できます。表示される内容は、選択したアラームの種類によって異なります（表 5-63 を参照）。

表 5-63　アラーム詳細の表示

セクション	フィールド	説明
General Info[1]	Failure Source	イベントのソース（名前や MAC アドレスを含む）を示します。
	Owner	このアラームの担当者の名前または空欄。
	Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。
	Category	アラームのカテゴリ（AP、Rogue AP、Security など）。
	Created	アラームが作成された日時（月、日、年、時、分、秒、AM/PM）。
	Modified	最後にアラームが修正された日時（月、日、年、時、分、秒、AM または PM）。
	Generated By	アラームの発生原因となったデバイス。
	Severity	セキュリティのレベル：重大、やや重大、比較的重大でない、警告、クリア、情報。
	Previous Severity	最近のポーリング サイクルの後のアラームの重大度。

表 5-63　アラーム詳細の表示 （続き）

セクション	フィールド	説明
Device Info	Device Name	デバイスの名前。
	Device Address	デバイスの IP アドレス。
	Device Contact	デバイスの連絡先担当者の情報。
	Device Location	デバイスの場所。
	Device Status	デバイスのステータス。
Messages		ログ メッセージから取得されるデバイス情報。
Annotation		この不正アクセス ポイントに関する現在の注釈が表示されます。新しい注釈を追加するには、[New Annotation] をクリックします。注釈を入力し、[Post] をクリックして注釈を保存および表示するか、[Cancel] をクリックして、注釈を保存せずにページを閉じます。

1.全般情報は、アラームのタイプによって異なる場合があります。たとえば、アラーム詳細の中に、ロケーションおよびスイッチ ポート トレーシング情報を含む場合もあります。

[Alarms] リスト ページでは、「アラームに関連するイベントの表示」（P.5-131）で説明するように、選択したアラームのイベントも表示されます。

アラームに関連するイベントの表示

[Monitor] > [Alarms] ページを選択すると、[Severity] 列のアラーム重大度にマウス カーソルを合わせ、表示されたアイコンをクリックすることで、アラーム概要情報が表示されます。

ダイアログが開き、選択したアラームに関連する上位 5 個のイベントが表示されます。

[Events] をクリックすると、選択したアラームに関連付けられたすべてのイベントが表示されます。

アラームの変更

[Monitor] > [Alarms] ページでは、アラームの横のチェックボックスをオンにし、[Alarm Browser] ページ上部のいずれかのタスクをクリックして、アラームを変更できます。

（注）　[Monitor] > [Alarms] ページに表示されるアラームは、[Administration] > [Settings] ページで指定した設定に応じて変わります。詳細については、「アラーム設定の変更」（P.5-134）を参照してください。

- [Change Status]：アラームのステータスを次のいずれかに変更します。
  - [Acknowledge]：アラームを認知できます。デフォルトでは、認知済みのアラームは [Alarm Browser] ページに表示されません。認知済みのアラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、認知済みのすべてのアラームを検索できます。詳細については、「アラームの認知」（P.5-136）を参照してください。
  - [UnAcknowledge]：すでに認知しているアラームの認知を解除できます。

  - [Clear]：選択したアラームをクリアします。アラームが [Alarm Browser] から削除されます。クリアされたアラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、クリアされたすべてのアラームを検索できます

（注）　デフォルトでは、重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。この設定は、[Administration] > [Settings] ページで変更できます。

- [Assign]：選択したアラームについて、次の操作を実行できます。
  - [Assign to me]：アラームを指定したユーザに割り当てます。
  - [Unassign]：指定した所有者をアラームから削除します。
- [Annotation]：選択したアラームの注釈を入力し、[Post] をクリックします。入力した注釈はアラームの詳細を表示するときに表示されます。
- [Delete]：選択したアラームを削除します。アラームがどのデバイスでも検出されなくなったことを示します。

アラームの電子メール通知の指定

[Monitor] > [Alarms] ページで、アラームのカテゴリと重大度に基づき、アラームの電子メール通知を設定できます。

ステップ 1　[Monitor] > [Alarms] の順に選択し、[Email Notification] をクリックします。

ステップ 2　電子メール通知を設定するアラーム カテゴリの横の [Enable] チェックボックスをオンにし、[Save] をクリックします。

Prime Infrastructure は、指定したカテゴリのアラームが発生したときに電子メール通知を送信します。

Alarm Browser の変更

アラームの一覧を表示するには、[Monitor] > [Alarms] の順に選択します。Prime Infrastructure ホームページの下部にあるツールバーの [Alarm Browser] をクリックすることもできます。Alarm Browser に表示される次の情報を変更できます。

- 列の順序を変更するには、列の見出しを任意の位置にドラッグ アンド ドロップします。
- 列見出しをクリックすると、その列で表を並べ替えることができます。デフォルトでは、列は降順に並べ替えられます。もう一度列見出しをクリックすると、列が昇順に並べ替えられます。

（注）　一部の列は並べ替え不可です。列見出しにマウス カーソルを合わせると、Prime Infrastructure はその列が並べ替え可能かどうかを表示します。

- 表示される列をカスタマイズするには、[Settings] アイコンをクリックし、[Columns] をクリックします。表示する列の横のチェックボックスをオンにし、[Alarm Browser] ページに表示しない列のボックスをオフにします。

アラームの概要の表示

Prime Infrastructure がコントローラ、スイッチ、または Prime Infrastructure からアラーム メッセージを受信すると、[Alarm Summary] にアラーム インジケータが表示されます。[Alarm Summary] は、Prime Infrastructure ホーム ページの下部にあり、現在 Prime Infrastructure によって検出されている重大、やや重大、比較的重大でない警告の総数を表示します。[Alarm Summary] にマウス カーソルを合わせると、アラームの詳細が表示されます。

（注）　[Alarm Summary] ページと [Monitor] > [Alarms] ページに表示されるアラームは、[Administration] > [Settings] ページで指定した設定に応じて変わります。デフォルトでは、承認済みアラームは表示されません。詳細については、「アラーム設定の変更」（P.5-134）を参照してください。

アラームのカラー コードは、次のとおりです。

- 赤：重大なアラーム
- オレンジ：やや重大なアラーム
- 黄：比較的重大でないアラーム

アラームは、エレメントの現在の障害またはステートを示し、通常、1 つ以上のイベントにより生成されます。アラームをクリアすることはできますが、イベントは残ります。アラームの詳細については、「アラームとイベントの概要」（P.5-127）を参照してください。

（注）　デフォルトでは、アラーム カウントは 1 分ごとに更新されます。アラームの更新頻度は、[Administration] > [User Preferences] ページで変更できます。

[Alarm Summary] にマウス カーソルを合わせると、ポップアップ ページが開き、各アラーム カテゴリの重大、やや重大、比較的重大でないの各アラームの数が表示されます。[Alarm Summary] に表示されるアラーム カテゴリは、[Administration] > [User Preferences] ページで指定できます。デフォルトでは、すべてのカテゴリが表示されます。

- [Alarm Summary]：すべてのアラーム カテゴリの合計アラームの要約が表示されます。
- [AP]：AP Disassociated from controller、Thresholds violation for Load、Noise or Interference、AP Contained as Rogue、AP Authorization Failure、AP regulatory domain mismatch、Radio card Failure などの AP アラームのカウントが表示されます。
- Context-Aware Notifications
- [Controller]：Prime Infrastructure からの到達可能性の問題や、他のコントローラ障害（ファン障害、POE コントローラ障害、AP ライセンス期限切れ、リンク ダウン、温度センサー障害、低温検知）など、コントローラ アラームのカウントが表示されます。
- [Coverage Hole]：しきい値によって設定された十分なカバレッジがないクライアントが接続されたアクセス ポイントに対して生成された、カバレッジ ホールのカウントが表示されます。詳細については、「マップのモニタリング」（P.6-153）を参照してください。
- [Mesh Links]：SNR の低下、コンソール ログイン、過剰な親の変更、承認失敗、過剰なアソシエーションの失敗など、メッシュ リンク アラームのカウントが表示されます。
- [Mobility Services]：Prime Infrastructure からの到達可能性の問題やロケーション通知（In/Out Area、Movement from Marker、Battery Level）など、ロケーション アラームのカウントが表示されます。
- [Prime Infrastructure]：Prime Infrastructure アラームのカウントが表示されます。

- [Performance]：パフォーマンス アラームのカウントが表示されます。
- [Rogue AP]：悪意のある不正アクセス ポイント アラームのカウントが表示されます。
- [Rogue Adhoc]：未分類の不正アクセス ポイント アラームのカウントが表示されます。
- [Security]：Signature Attacks、AP Threats/Attacks、Client Security Events などのセキュリティ アラームのカウントが表示されます。
- [Switch]：認証エラーなどのスイッチ アラームのカウントが表示されます。

アラーム設定の変更

アラームの次の設定を変更できます。

- [Alarm count refresh rate]：「アラーム カウント更新頻度の変更」（P.5-134）を参照してください。
- [Alarm severity levels]：「アラーム重大度の設定」（P.5-134）を参照してください。

アラーム カウント更新頻度の変更

デフォルトでは、アラーム カウントは 1 分ごとに更新されます。更新頻度を変更するには、[Administration] > [User Preferences] の順に選択し、[Alarm Summary Every] メニューから [Refresh Alarm Count] の新しい値を選択します。

アラーム重大度の設定

[Administration] > [Settings] > [Severity Configuration] ページでは、新たに生成されたアラームの重大度を変更できます。

（注）　既存のアラームは変更されません。

新たに生成されるアラームの重大度を再設定するには、次の手順を実行します。

ステップ 1　[Administration] > [Settings] の順に選択します。

ステップ 2　左側のサイドバー メニューから [Severity Configuration] を選択します。

ステップ 3　重大度を変更するアラーム状態のチェックボックスをオンにします。

ステップ 4　[Configure Security Level] ドロップダウン リストから、次の重大度を選択します。

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Informational**
- **Reset to Default**

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして変更内容を確定するか、[Cancel] をクリックしてセキュリティ レベルを変更前のままにします。

アラームの処理

Prime Infrastructure を使用し、アクセス ポイントおよびモビリティ サービス エンジン上で、アラームとイベントを表示、割り当て、クリアできます。

ここでは、アラームの電子メール通知を送信する方法についても説明します。次のトピックが含まれます。

アラームの割り当てと割り当て解除

自分にアラームを割り当てたり割り当て解除したりするには、次の手順を実行します。

ステップ 1　アクセス ポイント アラームについて高度な検索を実行します。詳細については、「Advanced Search」（P.2-55）を参照してください。

ステップ 2　対応するチェックボックスをオンにすることで、自分に割り当てるアラームを選択します。

（注）　自分に割り当てられているアラームを割り当て解除するには、適切なアラームの横にあるチェックボックスをオフにします。他の人に割り当てられているアラームの割り当ては解除できません。

ステップ 3　[Select a command] ドロップダウン リストから、[Assign to Me]（または [Unassign]）を選択し、[Go] をクリックします。

[Assign to Me] を選択した場合、自分のユーザ名が [Owner] 欄に表示されます。[Unassign] を選択した場合、ユーザ名の欄は空白になります。

アラームの削除とクリア

モビリティ サービス エンジンからアラームを削除またはクリアするには、次の手順を実行します。

ステップ 1　[Monitor] > [Alarms] ページで、対応するチェックボックスをオンにして、削除またはクリアするアラームを選択します。

（注）　アラームを削除すると、アラームは Prime Infrastructure によってデータベースから削除されます。アラームをクリアすると、Prime Infrastructure データベースには残りますが、[Clear] 状態になります。アラームは、その原因となった状況が存在しなくなったときにクリアします。

ステップ 2　[Select a command] ドロップダウン リストから、[Delete] または [Clear] を選択し、[Go] をクリックします。

（注）　古いアラームとクリアされたアラームのクリーンアップを設定するには、[Administration] > [Settings] > [Alarms] の順に選択します。詳細については、「アラームとイベントの設定」（P.15-852）を参照してください。

アラームの認知

状況によっては、特定のアラームを [Alarms] リストから削除した方がよい場合があります。たとえば、802.11g インターフェイス上で特定のアクセス ポイントから干渉アラームを継続的に受信している場合は、[Alarm Summary] ページまたはその他のアラーム リストで、そのアクセス ポイントがアクティブなアラームとしてカウントされないように設定しておくと便利です。そのためには、[Alarms] リストで 802.11g インターフェイスのアラームを探し、チェックボックスをオンにして、[Select a command] ドロップダウン リストから [Acknowledge] を選択します。

これで、そのアクセス ポイントが同じインターフェイスで新しい違反を検出しても、Prime Infrastructure によって新しいアラームが生成されず、[Alarm Summary] ページにも新しいアラームが表示されません。ただし、802.11a など別のインターフェイス上では干渉違反が検出され、新しいアラームが生成されます。

デフォルトでは、認知されたアラームは [Alarm Summary] ページにもアラーム リスト ページにも表示されません。さらに、アラームを認知済みとしてマークした場合は、これらのアラームの電子メール メッセージも生成されません。デフォルトでは、認知済みアラームは検索対象となりません。このデフォルト動作を変更するには、[Administration] > [Settings] > [Alarms] ページを選択し、[Hide Acknowledged Alarms] チェックボックスをオフにします。

アラームを認知すると、この機能を無効にしない限り、問題が再発しても別のアラームは生成されないことを示す次の警告が通知として表示されます。

（注）　アラームを認知すると、この機能を無効にしない限り、問題が再度発生しても別のアラームが生成されない旨の注意を促すために、警告が表示されます。この警告メッセージを無効にするには、[Administration] > [User Preferences] ページを選択します。

また、以前の認知済みアラームをすべて検索して、過去 7 日間に認知されたアラームを表示することもできます。Prime Infrastructure は、7 日以上経過した解除済みアラートを自動的に削除するため、検索結果として表示されるのは最近 7 日間のアクティビティのみです。既存のアラームが削除されるまで、Prime Infrastructure がすでにアラームを生成している管理対象エンティティに対して新しいアラームを生成できません。

アクセス ポイント アラームのモニタリング

[Access Point Alarms] ページには、ネットワーク上のアクセス ポイントに基づくアラームが表示されます。

AP アラーム ページを表示するには、次のいずれかの手順を実行します。

- AP アラームの検索を実行します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- [Alarm Summary] ボックスの [Access Point] 番号のリンクをクリックします。

[Monitor AP Alarms] ページには次のフィールドがあります。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Failure Source]：アラームを生成したデバイス。
- [Owner]：このアラームに割り当てられている個人の名前またはブランク。
- [Date/Time]：アラームが生成された時間。
- [Message]：Prime Infrastructure アラーム ブラウザに表示される関連するメッセージ。
- [Category]：アラームに割り当てられているカテゴリを示します。不正 AP、コントローラ、スイッチ、セキュリティなどがあります。
- [Condition]：アラームの原因となった条件。
- [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。詳細については、「アラームの認知」（P.5-136）を参照してください。

電波品質アラームのモニタリング

[Air Quality Alarms] ページには、ネットワーク上の電波品質アラームが表示されます。

[Air Quality Alarms] ページを表示するには、次のいずれかの手順を実行します。

- パフォーマンス アラームの検索を実行します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- [Alarm Summary] ボックスの [Performance number] リンクをクリックします。

[Monitor Air Quality Alarms] ページには次のフィールドがあります。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Failure Source]：アラームを生成したデバイス。
- [Owner]：このアラームに割り当てられている個人の名前またはブランク。
- [Date/Time]：アラームが生成された時間。
- [Message]：Prime Infrastructure アラーム ブラウザに表示される関連するメッセージ。
- [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。詳細については、「アラームの認知」（P.5-136）を参照してください。

[Select a command] メニュー

対応するチェックボックスを選択して 1 つ以上のアラームを選択するか、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Clear]：選択したアラームをクリアします。
- [Delete]：選択したアラームを削除します。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。詳細については、「アラームの認知」（P.5-136）を参照してください。

（注）　アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。詳細については、「RFID タグのモニタリング」（P.5-113）を参照してください。

CleanAir セキュリティ アラームのモニタリング

[CleanAir Security Alarms] ページには、ネットワーク上のセキュリティ アラームが表示されます。

セキュリティ アラーム ページを表示するには、次のいずれかの手順を実行します。

- セキュリティ アラームの検索を実行します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。
- [Alarm Summary] ボックスの [Security number] リンクをクリックします。

[Monitor CleanAir Security Alarms] ページには次のフィールドがあります。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Failure Source]：アラームを生成したデバイス。
- [Owner]：このアラームに割り当てられている個人の名前またはブランク。
- [Date/Time]：アラームが生成された時間。
- [Message]：Prime Infrastructure アラーム ブラウザに表示される関連するメッセージ。
- [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。詳細については、「アラームの認知」（P.5-136）を参照してください。

[Select a command] メニュー

対応するチェックボックスを選択して 1 つ以上のアラームを選択するか、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Clear]：選択したアラームをクリアします。
- [Delete]：選択したアラームを削除します。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。詳細については、「アラームの認知」（P.5-136）を参照してください。

（注）　アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。

- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。詳細については、「RFID タグのモニタリング」（P.5-113）を参照してください。

電子メール通知のモニタリング

Prime Infrastructure には、組み込み電子メール通知機能が含まれており、重大なアラームが発生したときにネットワーク オペレータに通知できます。

[Email Notification] ページでは、各アラート カテゴリのフィルタを追加できます。アラート カテゴリが有効な場合、重大度はデフォルトで重大に設定されますが、カテゴリごとに異なる重大度を選択できます。電子メール通知は、設定された重大度についてのみ生成されます。

電子メール通知を設定する手順は、次のとおりです。

ステップ 1　[Monitor] > [Alarms] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Email Notification] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[Alarm Category] をクリックして、重大度と電子メール通知の受信者を編集します。

ステップ 5　通知を送信する重大度に該当するチェックボックス（[Critical]、[Major]、[Minor]、または [Warning]）をオンにします。

ステップ 6　[To] テキスト ボックスに、通知受信者の電子メール アドレスを入力します。

（注）　複数の電子メール アドレスを入力する場合は、各アドレスをカンマで区切ります。

ステップ 7　[OK] をクリックします。

ステップ 8　該当するアラーム カテゴリの [Enabled] チェックボックスをオンにして、電子メール通知の配信を有効にします。

ステップ 9　[OK] をクリックします。

モニタリングの重大度の設定

新しく生成されるアラームの重大度を変更できます。

（注）　既存のアラームは変更されません。

新しく生成されるアラームの重大度を変更する手順は、次のとおりです。

ステップ 1　[Administration] > [Setting] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Severity Configuration] を選択します。

ステップ 3　重大度を変更するアラーム状態のチェックボックスをオンにします。

ステップ 4　[Configure Severity Level] ドロップダウン リストから、新しい重大度（[Critical]、[Major]、[Minor]、[Warning]、[Informational]、[Reset to Default]）を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、変更を確定します。

Cisco Adaptive wIPS のアラームのモニタリング

Cisco Adaptive wIPS DoS（サービス拒絶）およびセキュリティ ペネトレーション攻撃からのアラームは、セキュリティ アラームとして分類されます。これらの wIPS アラームとその詳細は、[Monitor] > [Alarms] ページで参照できます。

wIPS DoS およびセキュリティ ペネトレーション攻撃のアラームの一覧を表示するには、次の手順を実行します。

ステップ 1　Advanced Search 機能を使用して、セキュリティ アラームの検索を行います。高度な検索の実行の詳細については、「Advanced Search」（P.2-55）を参照してください。

wIPS アラームに関する次の情報が表示されます。

- [Severity]：重大度には、重大、やや重大、情報、警告、およびクリアがあります。
- [Failure Object]：アラームの生成原因となったオブジェクトの名前と IP アドレスまたは MAC アドレスが表示されます。[Failure Object]：をクリックすると、アラームの詳細が表示されます。wIPS アラームの詳細の表示については、「Cisco Adaptive wIPS アラームの詳細のモニタリング」（P.5-141）を参照してください。
- [Date/Time]：アラームが発生した日時が表示されます。
- [Message]：アラームが発生した理由の説明（該当する wIPS ポリシーなど）を含むメッセージが表示されます。
- [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。
- [Category]：このアラームのカテゴリ（Security など）を示します。
- [Condition]：このアラームが生成された原因の説明が表示されます。

アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

テーブルで列の追加、削除、または並べ替えを行うには、[Edit View] リンクをクリックして、[Edit View] ページに移動します。

Select a command

[Select a command] ドロップダウン リストを使用して、選択したアラームに対し次の操作を実行できます。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。

- [Acknowledge] : [Alarm Summary] ページに表示されないように、アラームを承認します。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge] : すでに認知したアラームの認知を解除できます。
- [Email Notification] : 電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。

選択したアラームに対してアクションを実行するには、次の手順を実行します。

ステップ 1　チェックボックスをオンにしてアラームを選択します。

ステップ 2　[Select a command] ドロップダウン リストから、該当するコマンドを選択します。

ステップ 3　[Go] をクリックします。

Cisco Adaptive wIPS アラームの詳細のモニタリング

選択した Cisco wIPS アラームの詳細を表示するには、[Monitor] > [Alarms] > [*failure object*] の順に選択します。Cisco Adaptive wIPS アラームについて、次のアラームの詳細が表示されます。

- General
  - [Detected By wIPS AP] : アラームを検出したアクセス ポイント。
  - [wIPS AP IP Address] : wIPS アクセス ポイントの IP アドレス。
  - [Owner] : このアラームに割り当てられている個人の名前またはブランク。
  - [Acknowledged] : アラームがユーザによって承認されているかどうかを表示します。
  - [Category] : wIPS の場合、アラーム カテゴリは [Security] です。
  - [Created] : アラームが作成された日時（月、日、年、時、分、秒、AM/PM）。
  - [Modified] : アラームが最後に変更された日時（月、日、年、時、分、秒、AM/PM）。
  - [Generated By] : アラーム イベントの生成方法（NMS またはトラップから）を示します。

    [NMS (Network Management System - Prime Infrastructure)] : ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。

    [Trap] : コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。
  - [Severity] : 重大度（重大、やや重大、情報、警告、およびクリア）。
  - [Last Disappeared] : 潜在的な攻撃が最後になくなった日時。
  - [Channel] : 潜在的な攻撃が発生したチャネル。
  - [Attacker Client/AP MAC] : 攻撃を開始したクライアントまたはアクセス ポイントの MAC アドレス。
  - [Attacker Client/AP IP Address] : 攻撃を開始したクライアントまたはアクセス ポイントの IP アドレス。
  - [Target Client/AP IP Address] : 攻撃者により攻撃対象となったクライアントまたはアクセス ポイントの IP アドレス。

  - [Controller IP Address] : アクセス ポイントがアソシエートされているコントローラの IP アドレス。
  - [MSE] : 関連付けられているモビリティ サービス エンジンの IP アドレス。
  - [Controller MAC Address] : アクセス ポイントがアソシエートされているコントローラの MAC アドレス。
  - wIPS access point MAC address
  - Forensic File
  - [Event History] :「アラームのモニタリング」ページに移動し、このアラームのすべてのイベントを表示します。
- [Annotations] : このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、アラームが更新されます。注釈は [Annotations] 表示領域に表示されます。
- [Messages] : アラームに関する情報が表示されます。
- [Audit Report] : クリックすると設定監査アラームの詳細が表示されます。このレポートは、設定監査アラームにだけ使用できます。

  監査の矛盾が設定グループに施行されると、設定監査アラームが生成されます。

  （注） 施行が失敗すると、設定グループに重大なアラームが生成されます。施行が成功すると、設定グループに比較的重大でないアラームが生成されます。
  アラームには監査レポートへのリンクがあり、各コントローラの矛盾のリストを表示できます。

- [Rogue Clients] : 障害が発生したオブジェクトが不正なアクセス ポイントの場合、不正なクライアントに関する情報が表示されます。

Select a command

対応するチェックボックスをオンにして 1 つ以上のアラームを選択し、[Go] をクリックします。

- [Assign to me] : 選択したアラームを現在のユーザに割り当てます。
- [Unassign] : 選択したアラームの割り当てを解除します。
- [Delete] : 選択したアラームを削除します。
- [Clear] : 選択したアラームをクリアします。
- [Acknowledge] : [Alarm Summary] ページに表示されないように、アラームを承認します。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge] : すでに認知したアラームの認知を解除できます。
- [Email Notification] : 電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Event History] : [Monitor Alarms] > [Events] ページに移動し、不正アラームのイベントを表示します。

イベントのモニタリング

1 つ以上のイベントによって、異常ステートまたはアラームが生成されることがあります。アラームはクリアできますが、イベントは残ります。[Events] ページにアクセスするには、[Monitor] > [Events] の順に選択します。このページには次の情報が表示されます。

- [Description]：イベントの詳細を示します。
- [Time]：イベントが生成された日時を示します。
- [Severity]：イベントの重大度には、[Critical]、[Major]、[Minor]、[Warning]、[Cleared]、[Information] があります。
- [Failure Source]：イベントのソース（名前や MAC アドレスを含む）を示します。
- [Category]：[Rogue AP]、[Security]、[AP] などのイベントの種類。

列見出し行をクリックして、その列で並べ替えられます。

イベントの詳細を表示するには、クイックビュー アイコンを使用します。イベントの追加情報は、一般的な情報とメッセージに分かれています。一般的な情報では、障害のソース、カテゴリ、重大度、生成された時刻、IP アドレスが含まれます。イベントのメッセージも表示されます。

（注） イベントにも、アラームと同様に、プリセット フィルタ、クイック フィルタ、高度なフィルタがあります。これらのフィルタは、アラームのフィルタと同様に機能します。

検索機能を使用して表をフィルタリングすると、[Events] ページに追加情報が表示されることがあります。検索の実行の詳細については、「Advanced Search」（P.2-55）（イベントの Advanced Search の結果）を参照してください。追加情報には次のものがあります。

- Coverage Hole Events
  - Access Point Name
  - [Failed Clients]：カバレッジ ホールにより障害となったクライアントの数。
  - [Total Clients]：カバレッジ ホールによって影響を受けるクライアントの総数。
  - [Radio Type]：該当するアクセス ポイントの無線の種類（802.11b/g または 802.11a）。
  - Coverage Threshold
- Rogue AP Events
  - [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
  - [Classification Type]：不正アクセス ポイントの種類（Malicious、Friendly、Unclassified）。
  - [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
  - [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
  - [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
  - [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。

（注）　不正アクセス ポイントのイベントの詳細については、「不正アラーム イベントのモニタリング」（P.5-109）または「不正 AP イベントの詳細の表示」（P.5-110）を参照してください。

- Adhoc Rogue Events
  - [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
  - [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
  - [Radio Type]：この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
  - [State]：アラームの状態を示します。アドホック不正の可能な状態には、[Threat]、[Alert]、[Internal]、[External]、[Contained]、[Contained Pending]、および [Removed] があります。
  - [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- Interference
  - [Detected By]：干渉源を検出したデバイスの IP アドレス。
  - [ID]：干渉源を検出したデバイスの ID。
- Mesh Links
- Client
- Context-Aware Notifications
- Pre Coverage Hole
  - [Client MAC Address]：プレ カバレッジ ホールの影響を受けるクライアントの MAC アドレス。
  - [AP MAC Address]：該当するアクセス ポイントの MAC アドレス。
  - [Radio Type]：該当するアクセス ポイントの無線の種類（802.11b/g または 802.11a）。
  - [Power Level]：アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。
  - [Client Type]：クライアントの種類（laptop(0)、pc(1)、pda(2)、dot11mobilephone(3)、dualmodephone(4)、wgb(5)、scanner(6)、tabletpc(7)、printer(8)、projector(9)、videoconfsystem(10)、camera(11)、gamingsystem(12)、dot11deskphone(13)、cashregister(14)、radiotag(15)、rfidsensor(16)、server(17)）。
  - WLAN Coverage Hole Status

複数のイベント ページがある場合、ページ番号が、両側面のスクロール矢印とともに表示されます。これらのスクロール矢印を使用して、その他のイベントを表示します。

ここでは、次の内容について説明します。

- 「イベントの検索」（P.5-145）
- 「障害のあるオブジェクトのモニタリング」（P.5-145）
- 「不正 AP のイベントのモニタリング」（P.5-146）

- 「アドホック不正イベントの詳細の表示」（P.5-111）
- 「Cisco Adaptive wIPS イベントのモニタリング」（P.5-148）
- 「イベントの使用」（P.5-151）

イベントの検索

Prime Infrastructure の検索機能を使用して、特定のイベントを検索することや、カスタム検索を作成して保存することができます。追加情報については、次のいずれかのトピックを参照してください。

- 「検索機能の使用方法」（P.2-54）
- 「Quick Search」（P.2-54）
- 「Advanced Search」（P.2-55）
- 「Saved Search」（P.2-67）

イベントのエクスポート

イベントのリストをすばやく CSV ファイル（各値がカンマで区切られたスプレッドシート形式のファイル）にエクスポートできます。

（注）　イベントの表に表示されている列のみが CSV ファイルにエクスポートされます。

イベントのリストをエクスポートするには、次の手順を実行します。

ステップ 1　[Monitor] > [Events] を選択します。

ステップ 2　ツールバーで アイコンをクリックします。ポップアップ ウィンドウが表示されます。

ステップ 3　[File Download] ウィンドウで、[Save] をクリックしてファイルを保存します。

障害のあるオブジェクトのモニタリング

（注）　イベント カテゴリ Location Servers と Location Notifications は、Cisco NCS Location バージョンのみに表示されます。

[Monitor] > [Events] の順に選択し、[Monitor] > [Events] ページの左端にある、詳細を表示するイベントの展開アイコンをクリックします。イベントの詳細が表示されます。選択したイベントの種類に応じて、関連付けられている詳細が異なります。

- General Info
  - [Failure Source]：イベントのソース（名前や MAC アドレスを含む）を示します。
  - [Category]：[Security]、[AP] などのアラームの種類。
  - [Generated]：イベントが生成された日時。
  - [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。

[NMS (Network Management System - Prime Infrastructure)] : ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。

[Trap] : コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。

- [Device IP Address] : アラームを生成するデバイスの IP アドレス。
- [Severity] : 重大度（重大、やや重大、情報、警告、およびクリア）。

- [Messages] : イベントが発生した理由を説明したメッセージ。

不正 AP のイベントのモニタリング

[Monitor] > [Events] を選択します。[Description] 欄の項目をクリックし、不正アクセス ポイント無線のアラーム イベントを表示します。不正アクセス ポイント無線は、コントローラによって検出された無許可のアクセス ポイントです。次のフィールドが表示されます。

General

- Rogue MAC Address
- Vendor
- [On Network] : 不正が検出された方法を示します。
  - [Controller] : コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace] : 不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Owner] : このアラームに割り当てられている個人の名前または（ブランク）。
- [State] : この無線の、ネットワークまたはポートに対する状態。不正アクセス ポイント無線は、ポートで最初にスキャンされたときは [Alert] と表示され、オペレーティング システムの ID をまだ確認中の場合は [Pending] と表示されます。
- [SSID] : 不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Containment Level] : 封じ込められているアクセス ポイントは、まったくサービスを提供できないか、非常に低速なサービスを提供します。封じ込め活動に関連付けられているレベルがあります。これは、脅威を封じ込めるために使用する Cisco 1000 シリーズ Lightweight アクセス ポイントの数を示します。このサービスは、管理者が開始および停止する必要があります。[Containment Type] : 不正アクセス ポイント クライアントが Update Status でレベル 1 ～ 4 で封じ込められた場合は [Contained]、そうでない場合は [Unassigned] になります。
- [Channel] : アドホック不正がブロードキャストしている帯域を示します。
- [Radio Type] : この不正アクセス ポイントに適用されるすべての無線タイプをリストします。
- [Created] : イベントが発生した日付と時刻。
- [Generated By] : アラーム イベントの生成方法（NMS またはトラップから）を示します。
  - [NMS (Network Management System - Prime Infrastructure)] : ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。

  - [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。
- [Device IP Address]：アラームを生成するデバイスの IP アドレス。
- [Severity]：重大度（Critical、Major、Minor、Warning、Clear、Info）。色分けして表示されます。

[Message]：アラームに関する説明が表示されます。

[Help]：アラームに関する情報が表示されます。

（注）　特定のイベントを検索するには Advance Search 機能を使用します。詳細については、「Advanced Search」（P.2-55）を参照してください。

アドホック不正イベントのモニタリング

[Monitor] > [Events] を選択します。[Description] 欄の項目をクリックして、アドホック不正イベントの詳細を表示します。

General

- Rogue MAC Address
- Vendor
- [On Network]：不正が検出された方法を示します。
  - [Controller]：コントローラが不正を検出しました（Yes または No）。
  - [Switch Port Trace]：不正がスイッチ ポート トレースによって検出されました。[Traced but not found]、[Traced and found]、[Not traced] のいずれかで示されます。
- [Owner]：このアラームに割り当てられている個人の名前または（ブランク）。
- [State]：この無線の、ネットワークまたはポートに対する状態。不正アクセス ポイント無線は、ポートで最初にスキャンされたときは [Alert] と表示され、オペレーティング システムの ID をまだ確認中の場合は [Pending] と表示されます。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
- [Containment Level]：封じ込められているアクセス ポイントは、まったくサービスを提供できないか、非常に低速なサービスを提供します。封じ込め活動に関連付けられているレベルがあります。これは、脅威を封じ込めるために使用する Cisco 1000 シリーズ Lightweight アクセス ポイントの数を示します。このサービスは、管理者が開始および停止する必要があります。[Containment Type]：不正アクセス ポイント クライアントが Update Status でレベル 1 ～ 4 で封じ込められた場合は [Contained]、そうでない場合は [Unassigned] になります。
- [Channel]：アドホック不正がブロードキャストしている帯域を示します。
- [Created]：イベントが発生した日付と時刻。
- [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。
  - [NMS (Network Management System - Prime Infrastructure)]：ポーリングによって生成されます。Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。Prime Infrastructure は、トラップを無効にするか、これらのイベントのトラップが失われるとイベントを生成します。この場合、[Generated by] は [NMS] です。

  - [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、[Generated by] は [Controller] です。
- [Device IP Address]：アラームを生成するデバイスの IP アドレス。
- [Severity]：重大度（Critical、Major、Minor、Warning、Clear、Info）。色分けして表示されます。

[Message]：アラームに関する説明が表示されます。

[Help]：アラームに関する情報が表示されます。

Cisco Adaptive wIPS イベントのモニタリング

wIPS イベントを表示するには、[Monitor] > [Events] の順に選択します。1 つ以上のイベントによって、異常ステートまたはアラームが生成されることがあります。アラームはクリアできますが、イベントは残ります。イベントのモニタリングの詳細については、「イベントのモニタリング」（P.5-143）を参照してください。

以降の項では、Cisco Adaptive wIPS の詳細について説明します。

- wIPS プロファイルの設定
- Prime Infrastructure サービス
- wIPS ポリシー アラーム リファレンス

モビリティ サービス エンジンまたはセキュリティのイベントのみに結果を絞り込むには、イベント検索を実行します。モビリティ サービスエンジンまたはセキュリティ イベントを表示するには、[Monitor] > [Events] の順に選択します。

（注）　複数のイベント ページがある場合、ページ番号が、両側面のスクロール矢印とともに表示されます。これらのスクロール矢印を使用して、その他のイベントを表示します。

CleanAir 電波品質イベントのモニタリング

Prime Infrastructure を使用して、ワイヤレス ネットワークの電波品質に関して生成されたイベントを表示できます。

電波品質のイベントを表示するには、次の手順を実行します。

ステップ 1　Prime Infrastructure で [Advanced Search] をクリックします。

[New Search] ページが表示されます。

ステップ 2　[New Search] ページで、[Search Category] ドロップダウン リストから [Events] を選択します。

ステップ 3　[Severity] ドロップダウン リストから、電波品質イベントを検索する重大度の種類を選択します。

ステップ 4　[Event Category] ドロップダウン リストから、[Performance] を選択します。

ステップ 5　[Go] をクリックします。

[Air Quality Events] ページに、次の情報が表示されます。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Failure Source]：アラームを生成したデバイス。

- [Date/Time]：アラームが生成された時間。

電波品質イベントの詳細の表示

電波品質イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Air Quality Events] ページの [Failure Source] で項目をクリックし、アラームの詳細ページにアクセスします。「CleanAir 電波品質イベントのモニタリング」（P.5-148）を参照してください。

ステップ 2　[Air Quality Events] ページには、次の情報が表示されます。

- [Failure Source]：アラームを生成したデバイス。
- [Category]：このイベントのカテゴリ。この場合は [Performance] になります。
- [Created]：イベントが生成されたタイム スタンプ。
- [Generated By]：イベントを生成したデバイス。
- [Device IP Address]：イベントを生成したデバイスの IP アドレス。
- [Severity]：イベントの重大度。
- [Alarm Details]：このイベントに関連付けられたアラームへのリンク。アラームの詳細を表示するには、リンクをクリックします。
- [Message]：このアクセス ポイント上の電波品質の指標を示します。

干渉セキュリティ リスク イベントのモニタリング

Prime Infrastructure を使用して、ワイヤレス ネットワークで生成されたセキュリティ イベントを表示できます。

干渉セキュリティのイベントを表示するには、次の手順を実行します。

ステップ 1　Prime Infrastructure で [Advanced Search] をクリックします。

[New Search] ページが表示されます。

ステップ 2　[New Search] ページで、[Search Category] ドロップダウン リストから [Events] を選択します。

ステップ 3　[Severity] ドロップダウン リストから、電波品質イベントを検索する重大度の種類を選択します。

ステップ 4　[Event Category] ドロップダウン リストから、[Security] を選択します。

ステップ 5　[Go] をクリックします。

干渉セキュリティ イベントのページには、次の情報が表示されます。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Failure Source]：アラームを生成したデバイス。
- [Date/Time]：アラームが生成された時間。

干渉セキュリティ リスク イベントの詳細の表示

干渉セキュリティ イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Interferer Security Event] 詳細ページの [Failure Source] で項目をクリックし、アラームの詳細ページにアクセスします。「干渉セキュリティ リスク イベントのモニタリング」（P.5-149）を参照してください。

ステップ 2　[Air Quality Events] ページには、次の情報が表示されます。

- [Failure Source]：アラームを生成したデバイス。
- [Category]：このイベントのカテゴリ。この場合は [Security] になります。
- [Created]：イベントが生成されたタイム スタンプ。
- [Generated By]：イベントを生成したデバイス。
- [Device IP Address]：イベントを生成したデバイスの IP アドレス。
- [Severity]：イベントの重大度。
- [Alarm Details]：このイベントに関連付けられたアラームへのリンク。アラームの詳細を表示するには、リンクをクリックします。
- [Message]：アクセス ポイントに影響を与えている干渉デバイスを示します。

ヘルス モニタ イベントのモニタリング

Prime Infrastructure を使用して、ヘルス モニタによって生成されたイベントを表示できます。

ヘルス モニタ イベントを表示するには、次の手順を実行します。

ステップ 1　Prime Infrastructure で [Advanced Search] をクリックします。

[New Search] ページが表示されます。

ステップ 2　[New Search] ページで、[Search Category] ドロップダウン リストから [Events] を選択します。

ステップ 3　[Severity] ドロップダウン リストから、ヘルス モニタ イベントを検索する重大度の種類を選択します。

ステップ 4　[Event Category] ドロップダウン リストから、[Prime Infrastructure] を選択します。

ステップ 5　[Go] をクリックします。

[Health Monitor Events] ページに、次の情報が表示されます。

- [Severity]：アラームの重大度を示します。重大度インジケータ アイコンの一覧については、表 5-62 を参照してください。
- [Failure Source]：アラームを生成したデバイス。
- [Date/Time]：アラームが生成された時間。
- [Message]：稼働状態の詳細を示します。

ヘルス モニタ イベントの詳細の表示

ヘルス モニタ イベントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Health Monitor Events] ページの [Failure Source] で項目をクリックし、アラームの詳細ページにアクセスします。「ヘルス モニタ イベントのモニタリング」（P.5-150）を参照してください。

ステップ 2　[Health Monitor Events] ページに、次の情報が表示されます。

- [Failure Source]：アラームを生成したデバイス。
- [Category]：このイベントのカテゴリ。この場合は、[Prime Infrastructure] です。
- [Created]：イベントが生成されたタイム スタンプ。
- [Generated By]：イベントを生成したデバイス。
- [Device IP Address]：イベントを生成したデバイスの IP アドレス。
- [Severity]：イベントの重大度。
- [Alarm Details]：このイベントに関連付けられたアラームへのリンク。アラームの詳細を表示するには、リンクをクリックします。
- [Message]：メッセージを通じてイベントについて説明します。

イベントの使用

Prime Infrastructure を使用して、モビリティ サービス エンジンとアクセス ポイントのイベントを表示できます。重大度（重大、やや重大、比較的重大でない、警告、クリア、情報）およびイベント カテゴリに基づいてイベントを検索および表示できます。また、モビリティ サービス エンジンとアクセス ポイントを、その IP アドレス、MAC アドレス、または名前で検索できます。

イベントの検索に成功すると、イベントの重大度、障害オブジェクト、イベントの日付と時刻、各イベントのメッセージが表示されます。

イベントを表示するには、次の手順を実行します。

ステップ 1　Prime Infrastructure で、[Monitor] > [Events] をクリックします。

ステップ 2　[Events] ページで、次の手順を実行します。

- 特定の要素のイベントを表示し、その IP アドレス、MAC アドレス、または名前がわかっている場合は、その値を [Quick Search] テキスト ボックス（左ペイン）に入力します。[Go] をクリックします。
- 重大度とカテゴリでイベントを表示するには、[Severity and Event Category] ドロップダウン リスト（左ペイン）から適切なオプションを選択します。[Search] をクリックします。

ステップ 3　Prime Infrastructure は検索条件に一致するイベントを見つけると、それらのイベントを一覧表示します。

（注）　イベントの詳細を表示するには、イベントに関連付けられている障害オブジェクトをクリックします。また、イベントの概要を各列見出しで並べ替えることができます。

サイト マップのモニタリング

マップでは、キャンパス、ビルディング、屋外領域、およびフロア上にあるすべての管理対象システムの概要を表示できます。Prime Infrastructure データベースを使用すると、マップを追加して、リアルなキャンパス、ビルディング、およびフロア マップ上で管理対象のシステムを確認できます。詳細については、「マップのモニタリング」（P.6-153）を参照してください。

Google Earth マップのモニタリング

モビリティ サーバでロケーション表示を有効にすると、シスコのデフォルト設定（キャンパス、ビルディング、フロア、XY 座標）以外の拡張都市ロケーション情報（市町村、州、郵便番号、国）および GEO ロケーション情報（経度、緯度）を表示できます。クライアントは、ロケーションベースのサービスとアプリケーションで使用するために、オンデマンド ベースでこの情報を要求できます。新しいキャンパス、ビルディング、フロア、または屋外領域が後で追加または設定されるときに、ロケーション表示を設定できます。詳細については、「Google Earth マップのモニタリング」（P.6-235）を参照してください。

マップのモニタリング

この章では、マップを追加およびモニタする方法について説明します。ここで説明する内容は、次のとおりです。

マップについて

マップでは、キャンパス、ビルディング、屋外領域、およびフロア上にあるすべての管理対象システムの概要を表示できます。

従来のマップ機能に加えて、Cisco Prime Infrastructure 1.2 では、次世代マップの機能を使用することができます。次世代マップ機能は、デフォルトで有効になっています。この機能を無効または有効にするには、[Administration] > [User Preferences] ページを使用します。

次世代マップ機能には、次のような利点があります。

- マップで大量の情報を表示します。多数のクライアント、干渉、およびアクセス ポイントがある場合、Prime Infrastructure のマップ ページの表示が乱れる場合があります。また、ページのロードが遅くなります。Prime Infrastructure 1.2 は情報のクラスタリングおよび階層化を導入しています。情報のクラスタにより、高レベルでノイズを軽減し、オブジェクトをクリックすると、より多くの情報を表します。詳細については、「フロア領域のモニタリング」（P.6-176）を参照してください。
- AP をマップに追加するプロセスを効率化し、迅速化します。従来のマップでは、マップへのアクセス ポイントの追加プロセスは手作業で手間がかかります。Prime Infrastructure 1.2 では、階層の自動作成を使用し、アクセス ポイントを追加して名前を付けることができます。詳細については、「マップ作成のための自動階層の使用方法」（P.6-181）を参照してください。
- 容易なナビゲーションとズーム/パン コントロールによる高品質なマップ イメージを提供します。従来のマップでは、マップ イメージの品質が低く、ナビゲーション、ズーム、パンが低速です。Prime Infrastructure 1.2 では、次世代「タイル対応」マップ エンジンを使用して、マップのロードが早く、ズーム/パンを容易に行えます。また、次世代マップにより、管理者は高解像度のマップをより高速にロードし、マップ中を移動できます。詳細については、「次世代マップを使用したパンおよびズーム」（P.6-176）を参照してください。

表 6-1　　マップと連動するプロセス

プロセス	説明
1. 新しいキャンパスおよびビルディングのマップの追加	[Monitor] > [Site Maps] を選択します。[Select a Command] ドロップダウン リストから [New Campus] または [New Building] を選択します。
2. フロア マップの追加	[Monitor] > [Site Maps] を選択します。[Select a command] ドロップダウン リストから、[New Floor Area] を選択します。
3. Map Editor の使用	[Monitor] > [Site Maps] を選択します。[Select a command] ドロップダウン リストから [Map Editor] を選択します。

キャンパス マップの追加

（注） [Monitor] > [Site Maps] に移動すると、「未割り当てのキャンパス」領域が表示されます。これは、サイトの分類情報が使用できない場合の保証データ用領域です。すべてのエンドポイントまたはホスト データが未割り当てのキャンパスに集約されます。[Unassigned] は Prime Infrastructure で利用可能なデフォルト サイトです。

単一のキャンパス マップを Prime Infrastructure データベースに追加するには、次の手順を実行します。

ステップ 1　マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。

（注）　マップは任意のサイズにできます。これは、Prime Infrastructure が作業領域に適合するようマップを自動的にサイズ変更するためです。

ステップ 2　ファイル システムの任意の場所にあるマップを参照して、インポートします。

ステップ 3　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 4　[Select a command] ドロップダウン リストから [New Campus] を選択し、[Go] をクリックします。

ステップ 5　[Maps] > [New Campus] ページで、キャンパス名とキャンパスの連絡先の名前を入力します。

ステップ 6　キャンパス マップが含まれているイメージ ファイル名を参照および選択してから、[Open] をクリックします。

ステップ 7　[Maintain Aspect Ratio] チェックボックスをオンにして、Prime Infrastructure でマップのサイズが変更されたときに、縦横比が変わらないようにします。

ステップ 8　マップの水平方向スパンと垂直方向スパンをフィート単位で入力します。

（注）　測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。水平方向スパンと垂直方向スパンは、キャンパスに追加するビルディングやフロア図面よりも大きい値にする必要があります。

ステップ 9　[OK] をクリックして、このキャンパス マップを Prime Infrastructure データベースに追加します。Prime Infrastructure に、データベース内のマップ、マップの種類、およびキャンパスのステータスの一覧を含む [Maps] ページが表示されます。

ステップ 10　（任意）位置プレゼンス情報を割り当てるには、[Monitor] > [Site Maps] ページで新たに作成したキャンパスのリンクをクリックします。

（注）　システム キャンパスは、明示的にそれぞれの仮想ドメインに追加されているかどうかにかかわらず、各仮想ドメインに常に存在します。システム キャンパスを仮想ドメインに明示的に追加しても、同じ仮想ドメインにその子のビルディングおよびフロアがすべて含まれることはありません。

キャンパス マップへのビルディングの追加

Prime Infrastructure データベース内のキャンパス マップにビルディングを追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　目的のキャンパスをクリックします。[Site Maps] > [Campus Name] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 4　[Campus Name] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a.　ビルディング名を入力します。

b. ビルディング問い合わせ先の名前を入力します。

c. 地上のフロア数と地下のフロア数を入力します。

d. 水平位置（ビルディングの四角形の隅からキャンパス マップの左端までの距離）と垂直位置（ビルディングの四角形の隅からキャンパス マップの上端までの距離）をフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

e. ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

ヒント Ctrl キーを押した状態でクリックすることで、キャンパス マップの左上隅にある境界領域のサイズを変更できます。境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。

f. [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更されたビルディングの四角形が作成されます。

g. ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

h. [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。Prime Infrastructure では、キャンパス マップ上のビルディングの四角形の中にビルディング名が保存されます。

（注） ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5　（任意）新しい屋外領域に位置プレゼンス情報を割り当てる手順は、次のとおりです。

a. [Select a command] ドロップダウン リストから、[Edit Location Presence Info] を選択します。[Go] をクリックします。[Location Presence] ページが表示されます。

（注）　デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパス マップにビルディングを追加する際は、キャンパスのロケーション情報をインポートできます。
チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。
1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

b. [Civic Address] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注）　選択した各フィールドには、上記のすべてが含まれています。たとえば、[Advanced] を選択した場合、クライアントからの要求により Civic 位置情報も提供できます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

c. デフォルトでは、[Override Child's Presence Information] チェックボックスはオンになっています。独立したビルディングについては、この設定を変更する必要はありません。

ステップ 6　[Save] をクリックします。

独立したビルディングの追加

Prime Infrastructure データベースに独立したビルディングを追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　[Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 3　[Maps] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a. ビルディング名を入力します。

b. ビルディング問い合わせ先の名前を入力します。

（注）　新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

c. 地上のフロア数と地下のフロア数を入力します。

d. ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注）　測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

（注）　水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

e. [OK] をクリックして、このビルディングをデータベースに保存します。

ステップ 4　（任意）新しいビルディングに位置プレゼンス情報を割り当てる手順は、次のとおりです。

a. [Select a command] ドロップダウン リストから、[Location Presence] を選択します。[Go] をクリックします。[Location Presence] ページが表示されます。

b. [Civic] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注）　選択した各フィールドには、上記のすべてが含まれています。たとえば、[Advanced] を選択した場合、クライアントからの要求により Civic 位置情報も提供できます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

c. デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパス マップにビルディングを追加する際は、ロケーション情報をインポートできます。チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

ステップ 5　[Save] をクリックします。

（注）　独立したビルディングは、システム キャンパス内に自動的に配置されます。

フロア領域の追加

ここでは、Prime Infrastructure データベース内のキャンパスのビルディングまたは独立したビルディングにフロア図面を追加する方法を説明します。内容は次のとおりです。

- 「アクセス ポイントの配置」（P.6-180）

キャンパスのビルディングへのフロア領域の追加

ビルディングをキャンパス マップに追加したら、ビルディングに個々のフロア図面と地下のマップを追加できます。

（注） マップ ビューのサイズの拡大または縮小、およびマップ グリッド（マップ サイズをフィートまたはメートル単位で表示したもの）の表示または非表示を行うには、キャンパス イメージ上部にあるズーム コントロールを使用します。

キャンパスのビルディングにフロア領域を追加するには、次の手順を実行します。

ステップ 1　フロア図面マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） auto-cad ファイルの変換に問題がある場合は、エラー メッセージが表示されます。Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。ネイティブ ライブラリをロードできない場合、Prime Infrastructure は「unable to convert the auto-cad file」というメッセージを表示します。

（注） インポートされた auto-cad ファイルは、拡大するとぼやけて表示される場合があります。拡大しなければ、元の auto-cad ファイルと同じくらい明瞭に表示されます。関連するすべてのセクションが元の auto-cad ファイル（DWG/DXF）ではっきりと表示されていることを確認した後に、auto-cad ファイルを .JPEG および .JPG ではなく .PNG/.GIF 形式にインポートします。

（注） フロア マップ イメージがズームとパン機能のために拡張されています。フロア イメージは、この操作が完了するまで完全に表示されません。ズームインおよびズームアウトして、マップ イメージ全体を表示できます。たとえば、サイズが約 60 MB の高解像度のイメージがある場合は（約 181 メガピクセル）、マップに表示されるまでに 2 分かかることがあります。

ステップ 2　[Monitor] > [Site Maps] を選択します。

ステップ 3　[Maps Tree View] または [Monitor] > [Site Maps] リストから、該当するキャンパスのビルディングを選択し、[Building View] ページを開きます。

ステップ 4　マウス カーソルを既存ビルディングの四角形の中にある名前の上に移動して、強調表示します。

（注） [Campus View] ページからビルディングにアクセスすることもできます。[Campus View] ページで、ビルディング名をクリックし、[Building View] ページを開きます。

ステップ 5　[Select a command] ドロップダウン リストから、[New Floor Area] を選択します。

ステップ 6　[Go] をクリックします。[New Floor Area] ページが表示されます。

ステップ 7　[New Floor Area] ページで、関連するフロア図面マップを整理するためにフロアをビルディングに追加するには、次の手順を実行します。

a. フロア領域と連絡先の名前を入力します。

b. [Floor] ドロップダウン リストから、フロアまたは地下の数を選択します。

c. フロアまたは地下のタイプ（RF Model）を選択します。

d. フロア間の高さをフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

e. [Image or CAD File] チェックボックスを選択します。

f. 目的のフロアまたは地下のイメージまたは CAD ファイル名を参照および選択してから、[Open] をクリックします。

（注） CAD ファイルをインポートする場合は、[Convert CAD File] ドロップダウン リストを使用し、変換するイメージ ファイルを決定します。

ヒント auto-cad 変換に .JPEG（.JPG）形式を使用することは推奨しません。JPEG が特別に必要でない限り、高品質な画像には .PNG 形式または .GIF 形式を使用します。

g. [Next] をクリックします。CAD ファイルが指定されている場合、この時点でデフォルトのイメージ プレビューが生成されて読み込まれます。

（注） Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。ネイティブ ライブラリのロードに問題があるとき、Prime Infrastructure は次のエラーを表示します。「Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library.」詳細については、Prime Infrastructure オンライン ヘルプまたは Prime Infrastructure のドキュメントを参照してください。

CAD ファイル レイヤの名前が一覧表示されます。有効になっているレイヤには、イメージの右側にあるチェックボックスがオンになっています。

（注） フロアまたは地下のイメージ ファイル名を選択すると、Prime Infrastructure はビルディングのサイズに合わせたグリッド内にイメージを表示します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） マップは .PNG、.JPG、.JPEG、または .GIF 形式で保存する必要があります。

h. CAD ファイル レイヤがある場合、いくつでも選択または選択解除し、[Preview] をクリックして更新したイメージを表示できます。選択したレイヤで次に進む準備ができたら、[Next] をクリックします。

フロア領域に関する残りのパラメータを入力します。

i. 元のイメージの縦横比を維持するには、[Maintain Aspect Ratio] チェックボックスをオンのままにし、イメージの縦横比を変更するにはチェックボックスをオフにします。

j. フロアまたは地下のおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 水平方向スパンと垂直方向スパンは、Prime Infrastructure データベース内のビルディングの水平方向スパンおよび垂直方向スパンと同じサイズかそれ以下にする必要があります。

k. 必要に応じて、水平位置（屋外領域の四角形の隅からキャンパス マップの左端までの距離）と垂直位置（屋外領域の四角形の隅からキャンパス マップの上端までの距離）をフィートまたはメートル単位で入力します。

ヒント ビルディングのサイズに合わせてグリッド内のイメージのサイズを変更するには、Ctrl キーを押した状態でクリックします。

l. 必要に応じて [Launch Map Editor after floor creation] チェックボックスを選択し、フロアの縮尺を変更し、壁を描画します。

m. [OK] をクリックして、このフロア図面をデータベースに保存します。フロアは [Maps Tree View] と [Monitor] > [Site Maps] リストに追加されます。

（注） ビルディングごとに異なるフロア名を使用します。キャンパス マップに複数のビルディングを追加する場合、別のビルディングに存在するフロア名を使用しないでください。フロア名が重複すると、フロアとビルディング間のマッピング情報が不正確になります。

ステップ 8　フロア図面または地下のマップを表示するには、フロアまたは地下のイメージをクリックします。

（注） マップを拡大または縮小してさまざまなサイズで表示したり、アクセス ポイントを追加したりできます。

独立したビルディングへのフロア図面の追加

独立したビルディングを Prime Infrastructure データベースに追加したら、個々のフロア図面マップをビルディングに追加できます。

独立したビルディングにフロア図面を追加するには、次の手順を実行します。

ステップ 1　フロア図面マップを .PNG、.JPG、または .GIF 形式で保存します。

（注）　マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

ステップ 2　ファイル システムの任意の場所にあるフロア図面マップを参照して、インポートします。DXF または DWG 形式の CAD ファイル、またはステップ 1 で作成した形式のうちどの CAD ファイルでもインポートできます。

（注）　auto-cad ファイルの変換に問題がある場合は、エラー メッセージが表示されます。Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。ネイティブ ライブラリをロードできない場合、Prime Infrastructure は「unable to convert the auto-cad file」というメッセージを表示します。

ステップ 3　[Monitor] > [Site Maps] を選択します。

ステップ 4　[Maps Tree View] または左側のサイドバー メニューの [Monitor] > [Site Maps] から、目的のビルディングを選択し、[Building View] ページを表示します。

ステップ 5　[Select a command] ドロップダウン リストから、[New Floor Area] を選択します。

ステップ 6　[Go] をクリックします。

ステップ 7　[New Floor Area] ページで、次の情報を追加します。

- フロア領域と連絡先の名前を入力します。
- [Floor] ドロップダウン リストから、フロアまたは地下の数を選択します。
- フロアまたは地下のタイプ（RF Model）を選択します。
- フロア間の高さをフィート単位で入力します。
- [Image or CAD File] チェックボックスを選択します。
- 目的のフロアまたは地下のイメージまたは CAD ファイルを参照および選択してから、[Open] をクリックします。

（注）　CAD ファイルをインポートする場合は、[Convert CAD File] ドロップダウン リストを使用し、変換するイメージ ファイルを決定します。

ヒント　auto-cad 変換に .JPEG（.JPG）形式を使用することは推奨しません。.JPEG が特別に必要でない限り、高品質な画像には .PNG 形式または .GIF 形式を使用します。

ステップ 8　[Next] をクリックします。CAD ファイルが指定されている場合、この時点でデフォルトのイメージ プレビューが生成されて読み込まれます。

（注）　Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。ネイティブ ライブラリのロードに問題があるとき、Prime Infrastructure は次のエラーを表示します。「Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. 詳細については、Prime Infrastructure オンライン ヘルプまたは Prime Infrastructure のドキュメントを参照してください。

CAD ファイル レイヤの名前が一覧表示されます。有効になっているレイヤには、イメージの右側にあるチェックボックスがオンになっています。

（注） フロアまたは地下のイメージ ファイル名を選択すると、Prime Infrastructure はビルディングのサイズに合わせたグリッド内にイメージを表示します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） マップは .PNG、.JPG、.JPEG、または .GIF 形式で保存する必要があります。

CAD ファイル レイヤがある場合、いくつでも選択または選択解除し、[Preview] をクリックして更新したイメージを表示できます。選択したレイヤで次に進む準備ができたら、[Next] をクリックします。

ステップ 9　フロア領域に関する残りのパラメータを入力します。

- 元のイメージの縦横比を維持するには、[Maintain Aspect Ratio] チェックボックスをオンのままにし、イメージの縦横比を変更するにはチェックボックスをオフにします。
- フロアまたは地下のおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 水平方向スパンと垂直方向スパンは、Prime Infrastructure データベース内のビルディングの水平方向スパンおよび垂直方向スパンと同じサイズかそれ以下にする必要があります。

- 必要に応じて、水平位置（屋外領域の四角形の隅からキャンパス マップの左端までの距離）と垂直位置（屋外領域の四角形の隅からキャンパス マップの上端までの距離）をフィートまたはメートル単位で入力します。

ヒント ビルディングのサイズに合わせてグリッド内のイメージのサイズを変更するには、Ctrl キーを押した状態でクリックします。

- [Launch Map Editor] の横のチェックボックスを選択して、Prime Infrastructure の Map Editor でフロアの特性を調整します。Map Editor 機能の詳細については、「Map Editor の使用」（P.6-184）を参照してください。

ステップ 10　[OK] をクリックして、このフロア図面をデータベースに保存します。フロアは [Maps Tree View] と [Monitor] > [Site Maps] リストに追加されます。

ステップ 11　フロア図面または地下のマップを表示するには、フロアまたは地下のイメージをクリックします。

（注） マップを拡大または縮小してさまざまなサイズで表示したり、アクセス ポイントを追加したりできます。

フロア設定の構成

さまざまなフロア設定のチェックボックスをオンまたはオフにすることにより、フロア マップの外観を変更できます。オンにしたフロア設定はマップ イメージに表示されます。

[Floor Settings] オプションには次の項目が含まれます。

- Access Point
- AP Heatmaps
- AP Mesh Info
- Clients
- 802.11 Tags
- Rogue APs
- Rogue Adhocs
- Rogue Clients
- Coverage Areas
- Location Regions
- Rails
- Markers
- Chokepoints
- Wi-Fi TDOA Receivers
- Interferers

青色の矢印を使用して、アクセス ポイント、アクセス ポイント ヒートマップ、クライアント、802.11 タグ、不正アクセス ポイント、不正アドホック、および不正クライアントに関するフロア設定フィルタにアクセスします。フィルタリング オプションを選択したら、[OK] をクリックします。

最後のドロップダウン リスト内の [Show MSE data] を使用して、モビリティ サービス エンジンのデータの期間を選択します。過去 2 分間から最大 24 時間の範囲で、モビリティ サービス エンジンのデータを表示できます。このオプションは、モビリティ サービス エンジンが Prime Infrastructure に存在する場合のみ表示されます。

[Save Settings] をクリックすると、現在のビューとフィルタ設定がすべてのマップに対する新しいデフォルトになります。

フロア上の包含リージョンと除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含める領域（包含領域）と計算に含めない領域（除外領域）を定義できます。

たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外して、作業領域（小個室、研究室、製造現場など）を含めることができます。

（注） フロアが同期している MSE が Aeroscout タグ エンジンを実行している場合、タグに対する包含リージョンと除外リージョンは計算されません。

フロア コンポーネント詳細の表示

[Floor View] に表示されているコンポーネントの詳細を表示するには、マウス カーソルを該当するアイコンの上に移動します。詳細情報を含むダイアログボックスが表示されます。表 6-2 に、フロア マップのアイコンを示します。

表 6-2　フロア マップ アイコン

アイコン	説明
	アクセス ポイントのアイコン。円の色は Cisco Radio のアラーム ステータスを示します。 **（注）** 各アクセス ポイントには 2 つの Cisco Radio が搭載されています。[Access Point filter] ページで 1 つのプロトコルが選択されているときは、アイコン全体がこの無線を表します。両方のプロトコルが選択されている場合は、アイコンの上半分が 802.11a/n 無線のステートを表し、下半分が 802.11b/g/n 無線のステートを表します。 **（注）** Cisco Radio が無効になっている場合は、小さい「x」がアイコンの中央に表示されます。 **（注）** モニタ モードのアクセス ポイントは、他のアクセス ポイントと区別するために灰色のラベルで表示されます。
	AP ヒートマップのアイコン。
	クライアントのアイコン。クライアントの詳細を表示するには、マウス カーソルをアイコンの上に移動します。
	タグのアイコン。タグの詳細を表示するには、マウス カーソルをアイコンの上に移動します。
	不正アクセス ポイントのアイコン。アイコンの色は、不正アクセス ポイントのタイプを示します。たとえば、赤色は悪意のある不正アクセス ポイントを示し、青色は不明なタイプを示します。 不正アクセス ポイントの詳細を表示するには、マウス カーソルをアイコンの上に移動します。
	不正アドホックのアイコン。 不正アドホックの詳細を表示するには、マウス カーソルをアイコンの上に移動します。
	不正クライアントのアイコン。 不正クライアントの詳細を表示するには、マウス カーソルをアイコンの上に移動します。
	カバレッジのアイコン。
	ロケーション リージョンのアイコン。
	レールのアイコン。

表 6-2　フロア マップ アイコン （続き）

アイコン	説明
	マーカーのアイコン。
	チョークポイントのアイコン。
	Wi-Fi TDOA 受信機のアイコン。
	干渉デバイスのアイコン。
	Prime Infrastructure の Web 認証 WLAN 経由で設定されたゲスト クライアントを識別します。 （注）　コントローラに Guest WLAN を作成しそのコントローラを MSE に割り当てると、そのコントローラからのゲストはゲスト アイコンとしてのみ表示されます。

Cisco 1000 シリーズ Lightweight アクセス ポイントのアイコン

アイコンは、アクセス ポイントの現在のステータスを示します。アイコンの円部分は水平方向に半分に分割できます。2 つの Cisco 無線 の色のうちより重大な方が、大きい三角形ポインタの色を決定します。

（注）　アイコンが 802.11a/n と 802.11b/n を表している場合は、上半分が 802.11a/n ステータスを示し、下半分が 802.11b/g/n ステータスを示します。アイコンが 802.11b/g/n のみを表している場合は、アイコン全体が 802.11b/g/n ステータスを示します。三角形はより重大な色を示します。

表 6-3 に、Prime Infrastructure ユーザ インターフェイスのマップ画面で使用されるアイコンを示します。

表 6-3　アクセス ポイント アイコンの説明

アイコン	説明
	緑色のアイコンは、障害のないアクセス ポイント（AP）を示します。円の上半分は、オプションの 802.11a Cisco 無線 を表します。円の下半分は、802.11b/g Cisco 無線 のステートを示します。
	黄色のアイコンは、比較的重大でない障害があるアクセス ポイントを示します。円の上半分は、オプションの 802.11a Cisco 無線 を表します。円の下半分は、802.11b/g Cisco 無線 のステートを示します。 （注）　黄色の点滅するアイコンは、802.11a または 802.11b/g の干渉、ノイズ、カバレッジ、または負荷プロファイル違反があることを示します。黄色の点滅するアイコンは、802.11a および 802.11b/g のプロファイル違反があることを示します。

表 6-3　アクセス ポイント アイコンの説明 （続き）

アイコン	説明
	赤色のアイコンは、やや重大な障害または重大な障害があるアクセス ポイント（AP）を示します。円の上半分は、オプションの 802.11a Cisco 無線 を表します。円の下半分は、802.11b/g Cisco 無線 のステートを示します。
	疑問符が中央に付いている灰色のアイコンは、到達不能なアクセス ポイントを表します。ステータスが判断できないため、灰色になっています。
	疑問符が中央に付いていない灰色のアイコンは、アソシエートされていないアクセス ポイントを表します。
	円の中央に赤い「x」が付いているアイコンは、管理目的で無効にされているアクセス ポイントを表します。
	上半分が緑色で下半分が黄色のアイコンは、障害のないオプションの 802.11a Cisco 無線（上）と、比較的重大でない障害がある 802.11b/g Cisco 無線（下）を示します。2 つの Cisco 無線 の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が緑色で下半分が赤色のアイコンは、障害がなく正常に動作している、オプションの 802.11a Cisco 無線（上）と、やや重大な障害または重大な障害がある 802.11b/g Cisco 無線（下）を示します。2 つの Cisco 無線 の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が黄色で下半分が赤色のアイコンは、比較的重大でない障害がある、オプションの 802.11a Cisco 無線（上）と、やや重大な障害または重大な障害がある 802.11b/g Cisco 無線（下）を示します。2 つの Cisco 無線 の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が黄色で下半分が緑色のアイコンは、比較的重大でない障害がある、オプションの 802.11a Cisco 無線（上）と、障害がなく正常に動作している 802.11b/g Cisco 無線（下）を示します。2 つの Cisco 無線 の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が赤色で下半分が緑色のアイコンは、やや重大な障害または重大な障害がある、オプションの 802.11a Cisco 無線（上）と、障害がなく正常に動作している 802.11b/g Cisco 無線（下）を示します。2 つの Cisco 無線 の色のうちより重大な方が、大きい三角形ポインタの色を決定します。

表 6-3　アクセス ポイント アイコンの説明 （続き）

アイコン	説明
	上半分が赤色で下半分が黄色のアイコンは、やや重大な障害または重大な障害がある、オプションの 802.11a Cisco 無線（上）と、比較的重大でない障害がある 802.11b/g Cisco 無線（下）を示します。2 つの Cisco 無線 の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
     	上半分（オプションの 802.11a）に赤い「x」が付いているアイコンは、示されている Cisco 無線 が管理目的で無効にされていることを表します。記載されている 6 つのカラー コーディングが存在します。

各アクセス ポイント アイコンには、内部の Side A アンテナの方向を示す、小さい黒矢印があります。

表 6-4 に、Prime Infrastructure ユーザ インターフェイスのマップ画面で使用される矢印の例を示します。

表 6-4　矢印

矢印の例	方向
	0 度、またはマップ上の右方向。
	45 度、またはマップ上の右下方向。
	90 度、またはマップ上の下方向。
これらは、矢印の角度を 45 度ずつ増加させた例の最初の 3 つ分を示しています。45 度ずつ増加させた例はあと 5 つあります。	

アクセス ポイントのフロア設定のフィルタリング

アクセス ポイントのフロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、フィルタリング オプションを含む [Access Point Filter] ダイアログボックスが表示されます。

アクセス ポイントのフィルタリング オプションには、次の項目が含まれます。

- [Show]：このオプション ボタンを選択すると、無線ステータスまたはアクセス ポイントのステータスが表示されます。

（注）　アクセス ポイント アイコンの色はアクセス ポイントのステータスに基づいており、選択されているステータスによってアイコンの色は異なります。フロア マップのデフォルトは無線ステータスです。

- [Protocol]：ドロップダウン リストから、表示する無線タイプを選択します（802.11a/n、802.11b/g/n、または両方）。

（注）　表示されるヒートマップは、選択した無線タイプに対応します。

- [Display]：ドロップダウン リストから、マップ イメージ上に表示されるアクセス ポイントの識別情報を選択します。
  - [Channels]：Cisco 無線 のチャネル番号を表示するか、「Unavailable」（アクセス ポイントが接続されていない場合）を表示します。
  - [TX Power Level]：現在の Cisco 無線 の送信電力レベル（1 が高い）または「Unavailable」（アクセス ポイントが接続されていない場合）を表示します。

（注）　電力レベルはアクセス ポイントのタイプによって異なります。1000 シリーズのアクセス ポイントでは 1 ～ 5 の値、1230 アクセス ポイントでは 1 ～ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ～ 8 の値をとります。

表 6-5 は、送信電力レベル番号と対応する電力設定を示しています。

表 6-5　送信電力レベル値

送信電力レベル番号	電力設定
1	国コード設定で許可される最大の電力
2	50% の電力
3	25% の電力
4	12.5 ～ 6.25 % の電力
5	6.25 ～ 0.195% の電力

（注）　電力レベルは、国コードの設定によって定義され、各国で規制されています。詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

- [Channel and Tx Power] : チャネルと送信電力レベルの両方（またはアクセス ポイントが接続されていない場合は「Unavailable」）を表示します。
- [Coverage Holes] : 接続が切断されるまでに信号が弱くなったクライアントの割合を表示します。接続されていないアクセス ポイントに対しては「Unavailable」を表示し、monitor-only モードのアクセス ポイントに対しては「MonitorOnly」を表示します。

（注）　カバレッジ ホールとは、クライアントがワイヤレス ネットワークから信号を受信できない領域のことです。無線ネットワークを展開する場合、初期ネットワーク展開のコストとカバレッジ ホール領域の割合を考慮する必要があります。展開するにあたってのカバレッジ ホールの妥当な条件とは、2 ～ 10% です。これは、100 か所のランダムに選択したテスト ロケーションのうち、2 ～ 10 か所でサービスが制限される可能性があることを意味します。展開後、Cisco Unified Wireless Network Solution の無線リソース管理（RRM）によってこれらのカバレッジ ホール領域が特定され、IT マネージャに報告されます。IT マネージャはユーザからの要求に基づいてカバレッジ ホールに対応します。

- [MAC Addresses] : アクセス ポイントがコントローラにアソシエートされているかどうかに関係なく、アクセス ポイントの MAC アドレスを表示します。
- [Names] : アクセス ポイント名を表示します。768 ビットは、デフォルト値です。
- [Controller IP] : アクセス ポイントがアソシエートされているコントローラの IP アドレスを表示します。アソシエーションを解除されたアクセス ポイントでは、「Not Associated」を表示します。
- [Utilization] : アソシエートされたクライアント デバイスで使用されている帯域幅の割合（受信、送信、およびチャネル使用率を含む）を表示します。アソシエーションを解除されたアクセス ポイントでは [Unavailable]、monitor-only モードのアクセス ポイントでは [MonitorOnly] が表示されます。
- [Profiles] : 対応するオペレータ定義のしきい値の負荷、ノイズ、干渉、およびカバレッジ コンポーネントを表示します。超えていないしきい値には「Okay」、超えているしきい値には「Issue」、接続されていないアクセス ポイントには「Unavailable」を表示します。

（注）　[Profile Type] ドロップダウン リストを使用して、[Load]、[Noise]、[Interference]、または [Coverage] を選択します。

- [CleanAir Status] : アクセス ポイントの CleanAir ステータスと、アクセス ポイントで CleanAir が有効かどうかを表示します。
- [Average Air Quality] : このアクセス ポイントの平均電波品質を表示します。詳細には、帯域と平均電波品質が含まれます。
- [Minimum Air Quality] : このアクセス ポイントの最小電波品質を表示します。詳細には、帯域と最小電波品質が含まれます。
- [Average and Minimum Air Quality] : このアクセス ポイントの平均電波品質と最小電波品質を表示します。詳細には、帯域、平均電波品質、および最小電波品質が含まれます。
- [Associated Clients] : アソシエートされているクライアントの数を表示します。接続されていないアクセス ポイントに対しては「Unavailable」を表示し、monitor-only モードのアクセス ポイントに対しては「MonitorOnly」を表示します。
- Bridge Group Names

- [RSSI Cutoff]：ドロップダウン リストから、RSSI Cutoff レベルを選択します。RSSI Cutoff の範囲は -60 dBm ～ -90 dBm です。
- [Show Detected Interferers]：チェックボックスをオンにすると、アクセス ポイントで検出されるすべての干渉を表示します。
- [Max.Interferers/label]：ドロップダウン リストから、ラベルごとに表示される干渉の最大数を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

アクセス ポイント ヒートマップのフロア設定のフィルタリング

RF ヒートマップは、変数から取得した値をマップに色として表した、RF ワイヤレス データのグラフィック表示です。現在のヒートマップは、RSSI 予測モデル、アンテナの方向、および AP 送信電力に基づいて計算されます。

[Access Point Heatmap] フロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、ヒートマップのフィルタリング オプションを含む [Contributing APs] ダイアログが表示されます。

Prime Infrastructure ではダイナミック ヒートマップが導入されました。ダイナミック ヒートマップを有効にすると、Prime Infrastructure は変更された RSSI 値を表すためにヒートマップを再計算します。

アクセス ポイント ヒートマップのフィルタリング オプションには、次の項目が含まれます。

- [Heatmap Type] : [Coverage] または [Air Quality] を選択します。[Air Quality] を選択した場合は、アクセス ポイントのヒート マップ タイプを平均電波品質または最小電波品質でさらにフィルタリングできます。該当するオプション ボタンを選択します。

（注） フロア計画にモニタ モード アクセス ポイントがある場合、IDS ヒートマップ タイプまたはカバレッジ ヒートマップ タイプのいずれかを選択できます。カバレッジ ヒートマップでは、モニタ モード アクセス ポイントは除外されます。

（注） カバレッジ ヒートマップおよび電波品質ヒートマップには、ローカル モード、FlexConnect モード、またはブリッジ モードの AP のみが関係します。

- [Total APs]：マップに配置されているアクセス ポイントの数を表示します。
- アクセス ポイントのチェックボックスをオンにして、イメージ マップ上に表示するヒートマップを決定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

[AP Mesh Info] のフロア設定のフィルタリング

（注） [AP Mesh Info] チェックボックスは、ブリッジ アクセス ポイントがフロアに追加されているときのみ表示されます。

このチェックボックスをオンにすると、Prime Infrastructure はコントローラと通信を開始し、ブリッジ アクセス ポイントの情報を表示します。次の情報が表示されます。

- 子アクセス ポイントと親アクセス ポイントとの間のリンク。
- 子アクセス ポイントから親アクセス ポイントへの方向を示す矢印。

- 信号対雑音比（SNR）を示す、色分けされたリンク。緑色のリンクは高い SNR（25 dB 超）を表し、オレンジ色のリンクは許容範囲内の SNR（20 ～ 25 dB）を表し、赤色のリンクは非常に低い SNR（20 dB 未満）を表します。

[AP Mesh Info] フロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、メッシュのフィルタリング オプションを含む [Mesh Parent-Child Hierarchical View] ページが表示されます。

マップ上に表示するアクセス ポイントを選択することにより、マップ ビューを更新できます。[Quick Selections] ドロップダウン リストから、ルート アクセス ポイントのみを選択するか、1 番めのホップから 4 番めのホップの間のさまざまなホップを選択するか、またはすべてのアクセス ポイントを選択します。

（注） 子アクセス ポイントを表示するには、その親が選択されている必要があります。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

クライアントのフロア設定のフィルタリング

（注） [Clients] オプションは、モビリティ サーバが Prime Infrastructure に追加されている場合のみ表示されます。

[Clients] フロア設定を有効にし、右側の青い矢印をクリックすると、[Client Filter] ダイアログボックスが表示されます。

クライアントのフィルタリング オプションには、次の項目が含まれます。

- [Show All Clients]：チェックボックスをオンにすると、マップ上のすべてのクライアントが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各クライアントのアイコンが表示されます。

（注） [Show All Clients] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。

[Small Icons] チェックボックスをオフにすると、ラベルに MAC アドレス、IP アドレス、ユーザ名、アセット名、アセット グループ、またはアセット カテゴリを表示するかどうか選択できます。

[Show All Clients] チェックボックスをオフにすると、クライアントをフィルタリングする方法を指定して、特定の SSID を入力できます。

- [Display]：マップ上に表示するクライアントの識別子（IP アドレス、ユーザ名、MAC アドレス、アセット名、アセット グループ、またはアセット カテゴリ）を選択します。
- [Filter By]：クライアントをフィルタリングするパラメータを選択します（IP アドレス、ユーザ名、MAC アドレス、アセット名、アセット グループ、アセット カテゴリ、またはコントローラ）。選択したら、特定のデバイスをテキスト ボックスに入力します。

（注） クライアントに複数の IPv6 アドレスが存在する場合は、いずれか 1 つの IP アドレスを指定して、クライアントを一意に識別できます。

- [SSID]：入力可能なテキスト ボックスにクライアントの SSID を入力します。
- [Protocol]：ドロップダウン リストから [All]、[802.11a/n]、または [802.11b/g/n] を選択します。
  - [All]：領域内のすべてのアクセス ポイントを表示します。
  - [802.11a/n]：802.11a/n 無線通信機を使用するクライアントに対するカバレッジ パターンを示す色付きのオーバーレイを表示します。色は、赤（-35dBm）～濃い青（-85dBm）までの受信信号強度を表します。
  - [802.11b/g/n]：802.11b/g/n 無線通信機を使用するクライアントに対するカバレッジ パターンを示す色付きのオーバーレイを表示します。色は、赤（-35dBm）～濃い青（-85dBm）までの受信信号強度を表します。768 ビットは、デフォルト値です。
- [State]：ドロップダウン リストから [All]、[Idle]、[Authenticated]、[Probing]、または [Associated] を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

802.11 タグのフロア設定のフィルタリング

[802.11 Tags] フロア設定を有効にし、右側の青い矢印をクリックすると、[Tag Filter] ダイアログが表示されます。

タグのフィルタリング オプションには、次の項目が含まれます。

- [Show All Tags]：チェックボックスをオンにすると、マップ上のすべてのタグが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各タグのアイコンが表示されます。

（注）　[Show All Tags] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。

[Small Icons] チェックボックスをオフにすると、ラベルに MAC アドレス、アセット名、アセット グループまたはアセット カテゴリを表示するかどうか選択できます。

[Show All Tags] チェックボックスをオフにすると、タグをフィルタリングする方法を指定できます。

- [Display]：マップ上に表示するタグの識別子（MAC アドレス、アセット名、アセット グループ、またはアセット カテゴリ）を選択します。
- [Filter By]：クライアントをフィルタリングするパラメータを選択します（MAC アドレス、アセット名、アセット グループ、アセット カテゴリ、またはコントローラ）。選択したら、特定のデバイスをテキスト ボックスに入力します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正 AP のフロア設定のフィルタリング

[Rogue APs] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue AP filter] ダイアログ ボックスが表示されます。

不正 AP のフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue APs]：チェックボックスをオンにすると、マップ上のすべての不正アクセス ポイントが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正アクセス ポイントのアイコンが表示されます。

（注）　[Show All Rogue APs] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。

[Show All Rogue APs] チェックボックスをオフにすると、不正アクセス ポイントをフィルタリングする方法を指定できます。

- [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Known]、[Acknowledged]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。
- [On Network]：ドロップダウン リストを使用して、ネットワーク上の不正アクセス ポイントを表示するかどうか指定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正アドホックのフロア設定のフィルタリング

[Rogue Adhocs] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue Adhoc filter] ダイアログが表示されます。

不正アドホックのフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue Adhocs]：チェックボックスをオンにすると、マップ上のすべての不正アドホックが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正アドホックのアイコンが表示されます。

（注）　[Show All Rogue Adhocs] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。

[Show All Rogue Adhocs] チェックボックスをオフにすると、不正アドホックをフィルタリングする方法を指定できます。

- [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Known]、[Acknowledged]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。
- [On Network]：ドロップダウン リストを使用して、ネットワーク上の不正アドホックを表示するかどうか指定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正クライアントのフロア設定のフィルタリング

[Rogue Clients] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue Clients filter] ダイアログが表示されます。

不正クライアントのフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue Clients]：チェックボックスをオンにすると、マップ上のすべての不正クライアントが表示されます。

- [Small Icons] : チェックボックスをオンにすると、マップ上の各不正クライアントのアイコンが表示されます。

（注）　[Show All Rogue Clients] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。[Show All Rogue Clients] チェックボックスをオフにすると、不正クライアントをフィルタリングする方法を指定できます。

- [Assoc. Rogue AP MAC Address] : 特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State] : ドロップダウン リストを使用して、[Alert]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

干渉設定のフィルタリング

[Interferer] フロア設定を有効にし、右側の青い矢印をクリックすると、[Interferers filter] ダイアログボックスが表示されます。

干渉のフィルタリング オプションには、次の項目が含まれます。

- [Show active interferers only] : チェックボックスをオンにすると、すべてのアクティブな干渉が表示されます。
- [Small Icons] : チェックボックスをオンにすると、マップ上の各干渉のアイコンが表示されます。
- [Show Zone of Impact] : おおまかな干渉の影響領域を表示します。円の不透明度はその重大度を示します。赤一色の円は Wi-Fi 通信を妨害する可能性がある非常に強い干渉を表し、薄いピンク色の円は弱い干渉を表します。
- 該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

マップおよび AP ロケーション データのインポート

Autonomous から Lightweight アクセス ポイントに、および WLSE から Prime Infrastructure に変換する場合、変換手順の 1 つとして、アクセス ポイント関連情報を手動で Prime Infrastructure に再入力する方法があります。この処理を高速化するために、WLSE からアクセス ポイントに関する情報をエクスポートして、Prime Infrastructure にインポートすることができます。

（注）　Prime Infrastructure は、.tar ファイルを想定しているため、ファイルをインポートする前に .tar 拡張子かどうかをチェックします。インポートしようとしているファイルが .tar ファイルでない場合は、Prime Infrastructure にエラー メッセージが表示され、別のファイルをインポートするためのプロンプトが表示されます。

（注）　WLSE データ エクスポート機能（WLSE バージョン 2.15）の詳細については、次の URL を参照してください。
http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp

Prime Infrastructure Web インターフェイスを使用して、プロパティをマップし、WLSE データを含む tar ファイルをインポートするには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Import Maps] を選択し、[Go] をクリックします。

ステップ 3　[WLSE Map and AP Location Data] オプションを選択して、[Next] をクリックします。

ステップ 4　[Import WLSE Map and AP Location Data] ページで、[Browse] をクリックしてインポートするファイルを選択します。

ステップ 5　インポートする .tar ファイルを見つけて選択し、[Open] をクリックします。

Prime Infrastructure では、[Import From] テキスト ボックスにファイルの名前が表示されます。

ステップ 6　[Import] をクリックします。

Prime Infrastructure によってファイルがアップロードされ、ファイルが処理されている間は一時的にローカル ディレクトリに保存されます。ファイルに処理できないデータが含まれている場合、Prime Infrastructure は問題を修正して再試行するようユーザに促します。ファイルのロードが完了すると、Prime Infrastructure に追加された内容を示すレポートが Prime Infrastructure に表示されます。レポートには、追加できない内容とその理由も記載されます。

インポートするデータの一部がすでに存在している場合、Prime Infrastructure では、キャンパスの場合は既存のデータを使用し、ビルディングとフロアの場合はインポートされたデータで既存のデータを上書きします。

（注）　WLSE サイトとビルディングの組み合わせ、および Prime Infrastructure キャンパス（または最上位レベルのビルディング）とビルディングの組み合わせの間に重複する名前がある場合、Prime Infrastructure の実行前インポート レポートに、既存のビルディングを削除することを示すメッセージが表示されます。

ステップ 7　[Import] をクリックして、WLSE データをインポートします。

Prime Infrastructure にインポートされた内容を示すレポートが表示されます。

ステップ 8　インポートされたデータを表示するには、[Monitor] > [Site Maps] を選択します。

フロア領域のモニタリング

フロア領域とは、ロビー、地下、エレベータ シャフトを含み、集合住宅ビルディングではすべての共通スペースを含む、外壁の外側の表面まで測定されたビルディングの各フロアの領域を指します。

ここでは、次の内容について説明します。

- 「次世代マップを使用したパンおよびズーム」（P.6-176）
- 「アクセス ポイントのフロア領域への追加」（P.6-178）
- 「アクセス ポイントの配置」（P.6-180）

次世代マップを使用したパンおよびズーム

パン

マップを移動するには、左マウス ボタンをクリックしたまま、新しい場所にマッピングをドラッグします。

また、パン矢印を使用して、マップを東西南北に移動することもできます。これはマップの左上隅にあります（図 6-1 を参照）。

図 6-1　　パン コントロール

（注）　キーボードの矢印キーを使用してパン操作を実行することもできます。

ズームインとズームアウト：スケールの変更

ズーム レベルは画像の解像度によって異なります。高解像度のイメージの場合、ズーム レベルが高くなります。さまざまなスケールでマップの表示状態を変えるたびにズーム レベルが変わり、表示が詳細になったり、広範になったりします。マップの中にはスケールを小さくしても大きくしても、同じ状態のマップもあります。

マップをさらに詳細に表示するには、ズームインする必要があります。マップの左側のズーム バーを使用してこれを行うことができます（図 6-2 を参照）。ズーム バーの上部にある [+] 記号をクリックします。ある場所を中心にズームインするには、その場所をダブルクリックします。マップを広い範囲で表示するには、ズームアウトする必要があります。これを行うには、ズーム バーの下部にある [-] 記号をクリックします。

図 6-2　　ズーム コントロール

（注）　マウスまたはキーボードを使用してズーム操作を実行できます。キーボードを使用して、[+] または [-] の記号をクリックし、ズームインまたはズームアウトします。マウスの場合は、マウスのスクロール ホイールを使用してズームインまたはズームアウトします。あるいは、ダブルクリックしてズームインします。

フロア ビュー ナビゲーション

[Floor View] メイン ナビゲーション ペインでは、複数のマップ機能にアクセスできます。

このナビゲーション ペインには、次の機能が含まれます。

- [Zoom In/Zoom]：「次世代マップを使用したパンおよびズーム」（P.6-176）を参照してください。
- [Map Size]：「次世代マップを使用したパンおよびズーム」（P.6-176）を参照してください。
- [Show Grid]：クリックすると、マップ上の距離をフィート単位で表示するグリッドが表示されたり、非表示になったりします。
- [RSSI Legend]：マウス カーソルを RSSI 凡例アイコンの上に移動すると、RSSI の色彩設計（赤色 /-35 dBm から紺青色 /-90 dBm までの範囲）が表示されます。
- [Add Access Points]：クリックすると、[Add Access Points] ページが開きます。詳細については、「アクセス ポイントのフロア領域への追加」（P.6-178）を参照してください。

- [Remove Access Points]：クリックすると、[Remove Access Points] ページが開きます。削除するアクセス ポイントを選択し、[OK] をクリックします。
- [Position Access Points]：クリックすると、[Position Access Points] ページが開きます。
- [Add Chokepoints]：クリックすると、[Add Chokepoints] ページが開きます。詳細については、『*Cisco Context-Aware Services Configuration Guide*』を参照してください。
- [Add WiFi TDOA Receivers]：クリックすると、[Add Wi-Fi TDOA Receivers] ページが開きます。詳細については、『*Cisco Context-Aware Services Configuration Guide*』を参照してください。
- [Auto Refresh]：ドロップダウン リストから、システム リフレッシュ間の時間の長さを選択します。
- [Refresh from Network]：クリックすると、現在のデータの即時リフレッシュを開始します。
- [Planning Mode]：クリックすると、[Planning Mode] ウィンドウが開きます。詳細については、「プランニング モードの使用」（P.6-221）を参照してください。
- [Map Editor]：クリックすると、[Map Editor] ウィンドウが開きます。

アクセス ポイントのフロア領域への追加

.PNG、.JPG、.JPEG、または .GIF 形式のフロア図面と屋外領域のマップを Prime Infrastructure データベースに追加した後に、Lightweight アクセス ポイント アイコンをマップ上に配置して、ビルディング内の設定位置を示すことができます。アクセス ポイントをフロア領域と屋外領域に追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Maps Tree View] または左側のサイドバーのメニューの [Monitor] > [Site Maps] から、目的のフロアを選択し、[Floor View] ページを開きます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Access Points] を選択し、[Go] をクリックします。

ステップ 4　[Add Access Points] ページで、フロア領域に追加するアクセス ポイントのチェックボックスをオンにします。

（注）　アクセス ポイントを検索する場合は、AP 名または MAC アドレス（イーサネット / 無線）/IP を [Search AP] の [Name/MacAddress (Ethernet/Radio)/IP] テキスト ボックスに入力して、[Search] をクリックします。検索では大文字と小文字は区別されません。

（注）　フロアおよび屋外領域にまだ割り当てられていないアクセス ポイントのみがリストに表示されます。

（注）　リストの上部にあるチェックボックスをオンにして、すべてのアクセス ポイントを選択します。

（注）　Prime Infrastructure では、フロア マップあたり最大 100 個のアクセス ポイントを設定できます。

ステップ 5　該当するすべてのアクセス ポイントが選択されたら、アクセス ポイント リストの下部にある [OK] をクリックします。

[Position Access Points] ページが表示されます。

フロア マップに追加するために選択した各アクセス ポイントは、灰色の円で表され（アクセス ポイント名や MAC アドレスにより区別）、フロア マップの左上部分に並べられます。

ステップ 6　各アクセス ポイントをクリックし、適切な位置にドラッグします。アクセス ポイントは選択されると青色に変わります。

（注）　マップ上にアクセス ポイントをドラッグすると、[Horizontal] テキスト ボックスと [Vertical] テキスト ボックスにアクセス ポイントの水平位置と垂直位置が表示されます。

（注）　各アクセス ポイントの横の小さい黒矢印は各アクセス ポイントの Side A を表し、各アクセス ポイントの矢印は、アクセス ポイントが設置された方向と一致する必要があります。Side A はそれぞれの 1000 シリーズ アクセス ポイント上で明確に記されており、802.11a/n 無線とは関係ありません。方向の矢印を調整するには、[Antenna Angle] ドロップダウン リストから適切な方向を選択します。

アクセス ポイントを選択すると、そのアクセス ポイントの詳細がページの左側に表示されます。アクセス ポイントの詳細には、次の情報が含まれます。

- [AP Model]：選択したアクセス ポイントのモデル タイプを示します。
- [Protocol]：ドロップダウン リストから、このアクセス ポイントのプロトコルを選択します。
- [Antenna]：ドロップダウン リストから、このアクセス ポイントの適切なアンテナ タイプを選択します。
- [Antenna/AP Image]：[Antenna] ドロップダウン リストから選択したアンテナがアンテナ イメージに反映されます。アンテナ イメージの右上の矢印をクリックすると、画像のサイズが拡大します。
- [Antenna Orientation]：アンテナ タイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。

  （注）　[Omnidirectional] アンテナのパターンでは方位角が存在しなくなるため、[Azimuth] オプションは表示されません。

  （注）　内部アンテナでは、同じ垂直方向の角度が両方の無線に適用されます。

  アンテナの角度は、マップの X 軸に対して相対的です。X（水平）座標および Y（垂直）座標の原点はマップの左上の角であるため、0 度はアクセス ポイントの Side A を右に、90 度は Side A を下に、180 度は Side A を左に向けることになります。

  アンテナの Elevation（垂直面）は、最大 90 度までアンテナを垂直（上下）に移動するために使用されます。

（注）　各アクセス ポイントがマップ上の正しい位置に設置されていること、またアンテナの方向が正しいことを確認します。マップを使って、カバレッジ ホールや不正アクセス ポイントを発見するときは、正確なアクセス ポイントの位置決めが重要です。

アンテナの垂直方向の角度および方位角のパターンの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

ステップ 7　各アクセス ポイントの配置と調整が完了したら、[Save] をクリックします。

（注）　[Save] をクリックすると、アクセス ポイントのアンテナ ゲインが選択したアンテナに一致します。これにより、無線がリセットされる可能性があります。

Prime Infrastructure によって、カバレッジ領域の RF 予測が計算されます。この RF 予測は、カバレッジ領域マップ上の RF 信号の相対強度を示しているため、一般的には「*ヒート マップ*」として知られています。

（注）　ここでは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値だけが表示されています。

（注）　アンテナ ゲインの設定はヒートマップおよびロケーションの計算には影響を与えません。アンテナ ゲインはアンテナ名に暗黙的に関連付けられます。このため、次の条件が適用されます。
- アンテナが Prime Infrastructure で「Other」として使用およびマークされている場合は、すべてのヒートマップおよびロケーションの計算で無視されます。
- アンテナが Prime Infrastructure で Cisco アンテナとして使用およびマークされている場合は、コントローラに設定されているゲインに関係なく、そのアンテナ ゲインの設定（Prime Infrastructure 上の内部値）が使用されます。

（注）　マップ上へのアクセス ポイントの配置の詳細については、「アクセス ポイントの配置」（P.6-180）を参照してください。

（注）　ファイルをインポートまたはエクスポートすることにより、アクセス ポイントの位置を変更できます。詳細については、「Wi-Fi TDOA 受信機の配置」（P.6-198）を参照してください。

アクセス ポイントの配置

無線 LAN のカバレッジ領域での全デバイスの最適な位置を判断するには、アクセス ポイントの密度と位置を考慮する必要があります。

少なくとも 3 個、可能な場合は 4 個か 5 個のアクセス ポイントが、デバイス位置を必要とする各領域にカバレッジを提供していることを確認します。デバイスを検出するアクセス ポイントは多いほうが効果があります。この高水準のガイドラインが生み出す最良の実施例は次のとおりです。優先度順に並べられています。

1. 最も重要なのは、アクセス ポイントが目的の位置を囲むことです。
2. 50 ～ 70 リニア フィート（約 17 ～ 20m）ごとに 1 つのアクセス ポイントが配置される必要があります。これは変換すると、2,500 ～ 5,000 平方フィート（230 ～ 450 平方メートル）ごとに 1 つのアクセス ポイントとなります。

（注）　アクセス ポイントは、20 フィート未満の高さで設置する必要があります。性能を最も引き出すためには、10 フィートで設置すると理想的です。

これらのガイドラインに従うと、アクセス ポイントが追跡したデバイスをより検出しやすくなります。2 つの物理環境が同じ RF 特性を持つことはほとんどありません。ユーザは特定の環境や要件に合わせてこれらのパラメータを変更しなければならない場合があります。

（注）　コントローラが情報を Location Appliance に転送するために、-75dBm を超える信号でデバイスを検出する必要があります。3 つ以上のアクセス ポイントが、-75dBm 以下の信号でデバイスを検出できなければなりません。

（注）　全方向性アンテナを内蔵した天井マウント型 AP がある場合は、Prime Infrastructure でアンテナの方向を必ずしも設定する必要はありません。ただし、同じ AP を壁にマウントする場合は、アンテナの方向を 90 度に設定する必要があります。

表 6-6 では、アクセス ポイントの方向について説明します。

表 6-6　　アクセス ポイントのアンテナ方向

アクセス ポイント	アンテナの方向
1140（天井に取り付けた場合）	Cisco ロゴは床面に向いている必要があります。 垂直方向：0 度。
1240（天井に取り付けた場合）	アンテナはアクセス ポイントと垂直にする必要があります。 垂直方向：0 度。
1240（壁面に取り付けた場合）	アンテナはアクセス ポイントと平行にする必要があります。 垂直方向：0 度。 アンテナが AP と垂直な場合、角度は 90 度になります（ダイポール アンテナは全方向性のため、方向の上下は関係ありません）。

マップ作成のための自動階層の使用方法

自動階層作成はすばやくマップを作成し、Prime Infrastructure のマップにアクセス ポイントを割り当てる方法です。ワイヤレス LAN コントローラを Prime Infrastructure 追加し、アクセス ポイントに名前を付けたら、自動階層作成を使用してマップを作成できます。また、ネットワークにアクセス ポイントを追加した後、自動階層作成をしようして、Prime Infrastructure のマップにアクセス ポイントを割り当てることができます。

（注）　自動階層作成機能を使用するには、マップのキャンパス、ビルディング、フロア、または屋外領域名を指定する、ワイヤレス アクセス ポイントに対して確立された命名パターンを必要とします。

たとえば、San Jose-01-GroundFloor-AP3500i1 などです。

ステップ 1　[Monitor] > [Automatic Hierarchy Creation] を選択して、[Automatic Hierarchy Creation] ページを表示します。

ステップ 2　テキスト ボックスに、システムのアクセス ポイントの名前を入力します。または、リストから名前を 1 つ選択できます。

この名前は、マップを作成する正規表現を作成するために使用されます。

（注）　以前に作成した正規表現を更新するには、式の横の [Load and Continue] をクリックし、式を適宜更新します。正規表現を削除するには、式の横にある [Delete] をクリックします。

ステップ 3　[Next] をクリックします。

ステップ 4　アクセス ポイントの名前にデリミタが含まれる場合は、それをテキスト ボックスに入力し、[Generate basic regex based on delimiter] をクリックします。システムではデリミタに基づいてアクセス ポイントの名前と一致する正規表現が作成されます。

たとえば、ダッシュ（-）のデリミタをアクセス ポイント名、San Jose-01-GroundFloor-AP3500i1 で使用すると、正規表現 /(.*)-(.*)-(.*)-(.*)/ が作成されます。
より複雑なアクセス ポイント名がある場合は、手動で正規表現を入力できます。

（注）　先頭と末尾のスラッシュを入力する必要はありません。

（注）　規則として、Prime Infrastructure ではスラッシュ内に正規表現を表示します。

ステップ 5　[Test] をクリックします。システムは、アクセス ポイント名に対して作成されたマップと、入力された正規表現を表示します。

ステップ 6　[Group] フィールドを使用して、階層型に一致するグループを割り当てます。

たとえば、アクセス ポイントに SJC14-4-AP-BREAK-ROOM の名前が付けられた場合

この例では、キャンパス名が SJC、ビルディング名が 14、フロア名が 4、AP 名が AP-BREAK-ROOM です。

正規表現 /([A-Z]+)(\d+)-(\d+)-(.*)/ を使用します。

AP 名から、次のグループが抽出されます。

1. SJC
2. 14
3. 4
4. AP-BREAK-ROOM

一致するグループは、1 から始めて、左から右へ割り当てられます。

一致するグループを階層要素と一致させるには、各グループ番号のドロップダウン リストを使用して、適切な階層要素を選択します。

これにより、アクセス ポイント名内の位置は、ほとんどどのような順番でも可能になります。

たとえば、アクセス ポイントに EastLab-Atrium2-3-SanFrancisco の名前が付けられた場合

正規表現 /(.*)-(.*)-(.*)-(.*)/ を使用して、

次のグループ マッピングを併用する場合：

1. Building
2. Device Name
3. Floor
4. Campus

自動階層作成では、SanFrancisco というキャンパス、EastLab というビルディング、EastLab の 3 というフロアを作成します。

（注） デバイス名がない、またはデバイスが影響を与えない 2 つの階層タイプでは、他の目的で一致するグループを使用する必要がある場合は、グループを省略できます。

自動階層作成では、アクセス ポイントを配置するマップを計算するためにマップする次のグループが必要です。

キャンパス グループは一致しているか？	ビルディング グループは一致しているか？	フロア グループは一致しているか？	結果の位置
Yes	Yes	Yes	キャンパス > ビルディング > フロア
Yes	Yes	No	不一致
Yes	No	Yes	キャンパス > フロア（フロアが屋外領域の場合）
Yes	No	No	不一致
No	Yes	Yes	システム キャンパス > ビルディング > フロア
No	Yes	No	不一致
No	No	Yes	不一致
No	No	No	不一致

自動階層作成では、フロア名からフロア インデックスを推測しようとします。フロア名が数値の場合、AHC はフロアを正数のフロア インデックスに割り当てます。フロア名が負の数値または文字 B で始まる場合（b1、-4、または B2 など）、AHC はフロアを負数のフロア インデックスに割り当てます。これは、フロアが地下であることを示します。

アクセス ポイントを配置する既存のマップを検索する場合、AHC は、アクセス ポイントの名前と同じフロア インデックスを持つアクセス ポイントのビルディング内のフロアを考慮します。

たとえば、SF > MarketStreet > Sublevel1 というマップがあり、フロア インデックスが -1 の場合、そのフロアにはアクセス ポイント SF-MarketStreet-b1-MON1 が割り当てられます。

ステップ 7　[Next] をクリックします。アクセス ポイントの対象を増やしてテストできます。[Add more device names to test against] フィールドにアクセス ポイントを入力して [Add] をクリックすると、より多くのアクセス ポイントに対する正規表現と一致グループのマッピングをテストできます。

次に、[Test] をクリックして、テーブル内の各アクセス ポイント名をテストします。各テストの結果がテーブルに表示されます。

必要に応じて、現在の正規表現の正規表現またはグループ マッピングを編集するには、前のステップに戻ります。

ステップ 8　[Next] をクリックしてから、[Save and Apply] をクリックします。これでシステムに正規表現が適用されます。システムはマップに割り当てられていないすべてのアクセス ポイントを処理します。

（注）　フロア イメージ、正しい寸法などを含めるようにマップを編集できます。自動階層作成でマップを作成する場合は、20 フィート X 20 フィートのデフォルト寸法が使用されます。正しい寸法などの属性を指定するには、作成されたマップを編集する必要があります。

自動階層作成を使用して作成されるマップは、*不完全な*アイコンがマップ リストに表示されます。マップの編集を完了すると、*不完全な*アイコンが消えます。[Edit View] リンクをクリックして、不完全なマップの列を非表示にできます。

Map Editor の使用

Map Editor を使って、フロア図面情報を定義、描画、および拡張します。また、Map Editor では、アクセスポイントに対する RF 予測ヒートマップを計算するときに反映できるように、障害物を作成できます。その特定の領域にあるクライアントとタグを特定する、Location Appliances のカバレッジ領域を追加することもできます。

プランニング モードでは、プランニング ツールが起動されるブラウザ ウィンドウで Map Editor を開きます。元のブラウザ ウィンドウがフロアのページから移動している場合は、フロアのページに戻って、Map Editor を起動する必要があります。

ここでは、次の内容について説明します。

Map Editor の使用に関するガイドライン

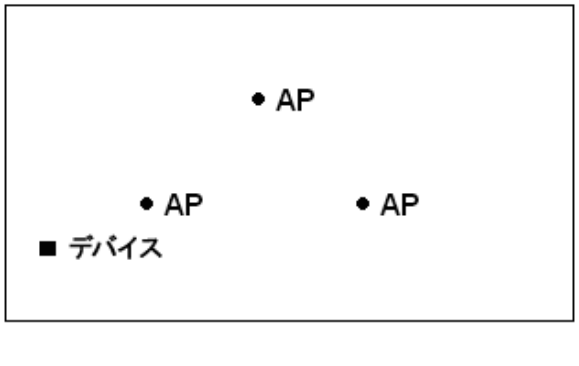
Map Editor を使用してビルディングまたはフロア マップを変更する際には、次の内容を考慮してください。

- 以前の Floor Plan Editor から .FPE ファイルをインポートするのではなく、Map Editor を使用して壁やその他の障害物を描画することを推奨します。
  - 必要に応じて .FPE ファイルをインポートすることはできます。そのためには、目的のフロア領域に移動します。[Select a command] ドロップダウン リストから、[Edit Floor Area] を選択し、[Go] をクリックします。[FPE File] チェックボックスをオンにしてから、.FPE ファイルを参照して選択します。
- Map Editor でフロア図面に追加できる壁の数に制限はありません。ただし、クライアント ワークステーションの処理能力およびメモリによって、Prime Infrastructure でのリフレッシュやレンダリングが制限されることがあります。
  - RAM が 1 GB 以下のコンピュータでは、実用的な制限として、フロアごとの壁数を 400 個までにすることを推奨します。
- すべての壁は、Prime Infrastructure が RF カバレッジ ヒートマップを生成する際に使用されます。
- WCS から 99999 より大きいマップ（長さもしくは幅が）をインポートした場合、エラーが発生します。したがって、Prime Infrastructure にインポートする前にマップのサイズを変更します。

アクセス ポイントの配置に関するガイドライン

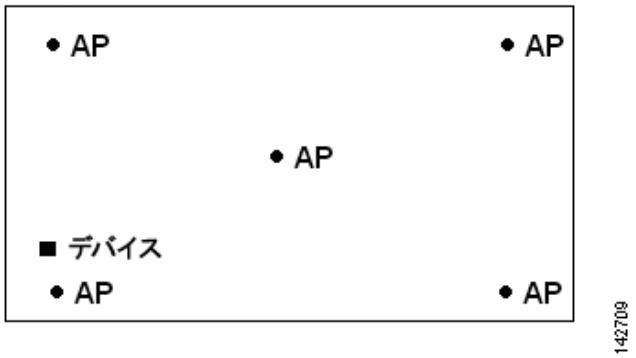
部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿ってアクセス ポイントを設置します。このようなカバレッジ領域の中心に設置されたアクセス ポイントからは、場合によっては他の全アクセス ポイントから等距離に見えてしまうデバイスに関しても有益なデータが得られます。

図 6-3　　一塊に集めたアクセス ポイント



全体のアクセス ポイントの密度を高め、アクセス ポイントをカバレッジ領域の周辺方向へ移動することにより、位置精度が大幅に向上します。

図 6-4　密度を高めることによる位置精度の向上



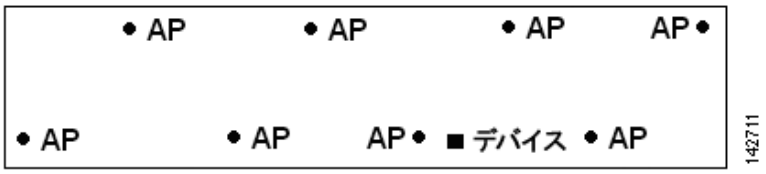
細長いカバレッジ領域では、直線的にアクセス ポイントを配置しないようにします。各アクセス ポイントでデバイス ロケーションのスナップショットが他と異なるように、それらを交互にずらします。

図 6-5　直線的な配置を控える

この計画では高い帯域幅のアプリケーションに十分なアクセス ポイント密度が提供されますが、ある 1 つのデバイスに対する、各アクセス ポイントからの見え方があまり変化しないため、ロケーションの特定が困難になるという問題があります。

アクセス ポイントをカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。

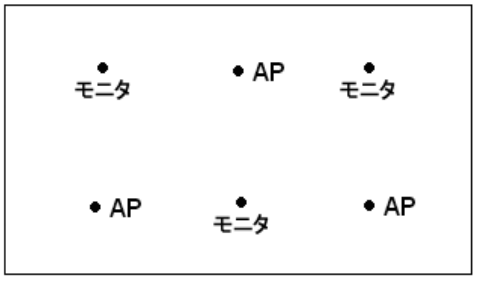
図 6-6　周辺で交互にずらすことで向上する位置精度



最も一般的な無線端末は、3 つの重複しないチャネルだけを提供する 802.11b/n しかサポートしていません。そのため、電話に対して設計された無線 LAN は、データを伝送するために計画されたものより密度が低い傾向があります。また、トラフィックが Platinum QoS バケット（通常は音声トラフィック、および遅延の影響を受けやすい他のトラフィック用に予約されている）にキューイングされると、Lightweight アクセス ポイントはスキャン機能を延期します。これにより、スキャン機能は他のチャネルで最大となり、アクセス ポイントは他の情報と共にデバイスの位置情報を収集します。ユーザは、monitor-only モードに設定したアクセス ポイントで無線 LAN 展開を補完できます。モニタリング機能だけを実行するアクセス ポイントは、クライアントにサービスを提供せず、干渉は引き起こしません。電波をスキャンしてデバイス情報を取得するだけです。

音声ネットワークなどの低密度の無線 LAN の導入では、それらの位置精度が、モニタ アクセス ポイントの追加および適切な配置によって非常に高まることがわかります。

図 6-7　　低密度の無線 LAN の導入



無線ラップトップ、ハンドヘルド、または電話を使用してカバレッジを検証し、3 つ以上のアクセス ポイントがデバイスによって検出されることを確認します。クライアントとアセット タグのロケーションを確認するには、指定した精度の範囲内（10 m、90 %）で、Prime Infrastructure がクライアントのデバイスとタグを報告することを確認します。

（注） 全方向性アンテナを内蔵した天井マウント型 AP がある場合は、Prime Infrastructure でアンテナの方向を必ずしも設定する必要はありません。ただし、同じ AP を壁にマウントする場合は、アンテナの方向を 90 度に設定する必要があります。

フロア上の包含領域と除外領域に関するガイドライン

包含領域と除外領域は多角形で表され、最低 3 点で構成される必要があります。

フロア上の包含リージョンを 1 つだけ定義できます。デフォルトでは、各フロアの包含リージョンは、そのリージョンが Prime Infrastructure に追加されるときに定義されます。包含リージョンは水色の実線で示され、通常はリージョンの輪郭を描きます。

フロア上の除外リージョンを複数定義できます。

新たに定義された包含リージョンと除外リージョンは、モビリティ サービス エンジンによってロケーションが再計算された後にヒートマップ上に表示されます。

Map Editor の表示

Map Editor を使用するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Map Design] を選択します。

ステップ 2　目的のキャンパスをクリックします。[Site Maps] > [Campus Name] ページが表示されます。

ステップ 3　キャンパスをクリックし、次にビルディングをクリックします。

ステップ 4　目的のフロア領域をクリックします。[Site Maps] > [Campus Name] > [Building Name] > [Floor Area Name] ページが表示されます。

ステップ 5　[Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。[Map Editor] ページが表示されます。

Map Editor アイコン

表 6-7　次世代マップのアイコン

アイコン	説明
	フロアのスケーリング：線の描画を開始するマップ上の任意の場所をクリックします。ダブルクリックすると線を終了し、表示されるポップアップに新しい行の長さを入力します。これでフロア寸法を新しい寸法に変更します。
	距離の測定：線の描画を開始するマップ上の任意の場所をクリックします。ダブルクリックすると線を終了します。測定した線の長さはフィート / メートル単位で上部に表示されます。
	障害物のコピー / 移動：マップ上にボックスを描画するか、障害物をクリックして、障害物を選択します。障害物をコピーするには、[Copy] をクリックします。これで、選択された障害物のすぐ上に新しい障害物が作成されます。障害物を移動するには、選択した障害物を新しい位置にドラッグします。マップ上の任意の場所をクリックすると、すべての要素が選択解除されます。
	削除モード：マップ上にボックスを描画するか、各要素をクリックして、削除する要素を選択します。複数の要素を選択するには、Shift キーを使用します。要素の選択 / 選択解除を切り替えるには、Ctrl キーを 1 回ずつ使用します。マップ上の任意の場所をクリックすると、すべての要素が選択解除されます。選択した要素を削除するには、[Delete] をクリックします。
	変更モード：要素をクリックし、変形させる頂点をクリックするか、要素をドラッグして新しい位置まで移動します。マップ上の任意の場所をクリックすると、選択した要素が選択解除されます。
	カバレッジ領域の描画
	ロケーション リージョンの描画
	レールの描画
	障害物の描画：線の描画を開始するマップ上の任意の場所をクリックします。ダブルクリックすると描画を終了します。現在の描画を取り消す場合は Ctrl-z を、やり直す場合は Ctrl-y を、キャンセルする場合は Esc キーを使用します。
	マーカーの配置
	ナビゲーション：描画や編集など選択したモードをすべて削除し、ナビゲーション モードに切り替えます。このモードでは、マップを表示し、ズームまたはパンを実行できます。

Map Editor を使用したカバレッジ領域の描画

長方形以外のビルディングがある場合、またはフロア内に長方形以外の領域をマークする場合には、Map Editor を使用してカバレッジ領域を描画できます。

ステップ 1　フロア図面が Prime Infrastructure にまだ表示されていない場合は、フロア図面を追加します。

ステップ 2　[Monitor] > [Site Maps] を選択します。

ステップ 3　編集する屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 4　[Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。

ステップ 5　[Map Editor] ページで、ツールバーの [Draw Coverage Area] アイコンをクリックします。

ポップアップが表示されます。

ステップ 6　定義する領域の名前を入力します。[OK] をクリックします。

描画ツールが表示されます。

ステップ 7　輪郭を描く領域に描画ツールを移動します。

- 左マウス ボタンをクリックして、線の描画を開始および終了します。
- 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。

マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。

ステップ 8　ツールバーのディスク アイコンをクリックして、新たに描画した領域を保存します。

Map Editor を使用した障害物の描画

表 6-10 では、障害のカラー コーディングについて説明します。

表 6-8　　障害のカラー コーディング

障害のタイプ	カラー コーディング	損失（dB）
厚い壁		13
薄い壁		2
重いドア		15
軽いドア		4
パーティション		1
ガラス		1.5

フロア上の包含リージョンの定義

包含領域を定義するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域の名前をクリックします。

ステップ 3　[Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　マップで、ツールバーの水色のボックスをクリックします。

（注）　一度に 1 つの包含領域のみ定義できることを示すメッセージ ボックスが表示されます。新しい包含リージョンを定義すると、以前に定義されていた包含リージョンは自動的に削除されます。デフォルトでは、各フロアの包含リージョンは、そのリージョンが Prime Infrastructure に追加されるときに定義されます。包含リージョンは水色の実線で示され、通常はリージョンの輪郭を描きます。

ステップ 6　表示されるメッセージ ボックスで [OK] をクリックします。包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7　包含領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8　含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。再びクリックすると、次の境界線を定義できます。

ステップ 9　領域の輪郭が描画されるまでステップ 8 を繰り返したら、描画アイコンをダブルクリックします。水色の実線によって包含領域が定義されます。

ステップ 10　[Command] メニューから [Save] を選択するか、ツールバーの**ディスク** アイコンをクリックして、包含リージョンを保存します。

（注）　包含領域を誤って定義した場合は、領域をクリックします。選択された領域の輪郭が水色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 11　[Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。これをすべてのフロア マップに適用する場合は、[Save settings] をクリックします。[Layers configuration] ページを閉じます。

ステップ 12　Prime Infrastructure データベースと MSE データベースを再同期するには、[Services] > [Synchronize Services] を選択します。

（注）　2 つの DB がすでに同期されている場合は、変更があるたびに自動的に再同期が実行されます。明示的に再同期する必要はありません。

ステップ 13　[Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

（注）　新たに定義された包含リージョンと除外リージョンは、モビリティ サービス エンジンによってロケーションが再計算された後にヒートマップ上に表示されます。

フロア上の除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外できます。通常、除外領域は包含領域の境界内に定義されます。

除外領域を定義するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域の名前をクリックします。

ステップ 3　[Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　マップで、ツールバーの紫色のボックスをクリックします。

ステップ 6　表示されるメッセージ ボックスで [OK] をクリックします。除外領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7　除外領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8　除外する領域の境界に沿って描画アイコンを移動させます。1 回クリックして境界線を開始し、再びクリックして境界線を終了します。

ステップ 9　領域の輪郭が描画されるまでステップ 8 を繰り返したら、描画アイコンをダブルクリックします。定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。除外された領域は紫色で網掛けされます。

ステップ 10　追加の除外リージョンを定義するには、ステップ 5 ～ ステップ 9 を繰り返します。

ステップ 11　すべての除外領域を定義したら、[Command] メニューから [Save] を選択するか、ツールバーの**ディスク** アイコンをクリックして、除外リージョンを保存します。

（注）　除外領域を削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 12　完了したら、[Location Regions] チェックボックスがまだオンになっていない場合にはオンにし、[Save settings] をクリックし、[Layers configuration] ページを閉じます。

ステップ 13　Prime Infrastructure データベースとロケーション データベースを再同期するには、[Services] > [Synchronize Services] を選択します。

ステップ 14　[Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

フロアでのレール ラインの定義

フロア上にコンベヤ ベルトを表すレール ラインを定義できます。また、レール領域の周囲にスナップ幅とも呼ばれる、ロケーション計算を一層サポートする領域を定義できます。この領域は、クライアントが表示されると予測される領域を表します。スナップ幅の領域内に配置されたクライアントは、レール ライン上に表示されるか（多数）、スナップ幅領域の外側に表示されます（少数）。

（注） レール ラインの設定はタグには適用されません。

スナップ幅領域は、フィートまたはメートル（ユーザ定義）単位で定義され、レールの片側（東および西、または北および南）からモニタされる距離を表します。

レールをフロアに定義するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域の名前をクリックします。

ステップ 3　[Select a command] ドロップダウン リストから、[Map Editor] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　マップで、ツールバーの**レール** アイコン（紫色の除外アイコンの右側）をクリックします。

ステップ 6　表示されるメッセージ ダイアログボックスで、レールのスナップ幅（フィートまたはメートル）を入力し、[OK] をクリックします。描画アイコンが表示されます。

ステップ 7　レール ラインの開始ポイントで**描画**アイコンをクリックします。ラインの描画を停止するときやラインの方向を変えるときは、再びクリックします。

ステップ 8　フロア マップ上にレール ラインを完全に描画したら、**描画**アイコンを 2 回クリックします。レール ラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。

（注） レール ラインを削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 9　フロア マップで、[Layers] ドロップダウン リストを選択します。

ステップ 10　完了したら、[Rails] チェックボックスがまだオンになっていない場合はオンにし、[Save settings] をクリックして、[Layers configuration] ペインを閉じます。

ステップ 11　Prime Infrastructure とモビリティ サービス エンジンを再同期するには、[Services] > [Synchronize Services] を選択します。

ステップ 12　[Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

屋外領域の追加

（注）　屋外領域マップをデータベースに追加したことがあるかどうかに関係なく、屋外領域を Prime Infrastructure データベース内のキャンパス マップに追加することができます。

屋外領域をキャンパス マップに追加するには、次の手順を実行します。

ステップ 1　屋外領域のマップをデータベースに追加する場合は、マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。ファイル システムの特定の場所にあるマップを参照して、インポートします。

（注）　屋外領域を追加するのにマップは必要ありません。屋外領域をデータベースに追加するため、領域の寸法を定義する必要があるだけです。Prime Infrastructure では、作業領域に合わせてマップのサイズが自動的に調整されるため、マップは任意のサイズにすることができます。

ステップ 2　[Monitor] > [Site Maps] を選択します。

ステップ 3　目的のキャンパスをクリックすると、[Monitor] > [Site Maps] > [Campus View] ページが表示されます。

ステップ 4　[Select a command] ドロップダウン リストから、[New Outdoor Area] を選択します。

ステップ 5　[Go] をクリックします。[Create New Area] ページが表示されます。

ステップ 6　[New Outdoor Area] ページで、次の情報を入力します。

- [Name]：新しい屋外領域のユーザ定義の名前。
- [Contact]：ユーザ定義の連絡先の名前。
- [Area Type (RF Model)]：[Cubes And Walled Offices]、[Drywall Office Only]、[Outdoor Open Space]（デフォルト）。
- [AP Height (feet)]：アクセス ポイントの高さを入力します。
- [Image File]：屋外領域マップを含むファイルの名前。[Browse] をクリックしてファイルを検索します。

ステップ 7　[Next] をクリックします。

ステップ 8　[Place] をクリックして、屋外領域をキャンパス マップ上に配置します。Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更された屋外領域の四角形が作成されます。

ステップ 9　屋外領域の四角形をクリックし、キャンパス マップ上の目的の位置までドラッグします。

ステップ 10　[Save] をクリックして、この屋外領域とキャンパス上の位置をデータベースに保存します。

（注）　屋外領域には、該当する [Maps] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 11　（任意）新しい屋外領域に位置プレゼンス情報を割り当てるには、[Edit Location Presence Info] を選択し、[Go] をクリックします。

（注）　デフォルトでは、[Override Child Element Presence Info] チェックボックスがオンになっています。屋外領域については、この設定を変更する必要はありません。

チョークポイントを使用したタグの位置報告の精度の向上

チョークポイントを設置すると、精度の高い RFID タグの位置情報を取得できます。アクティブな Cisco Compatible Extensions バージョン 1 準拠の RFID タグがチョークポイントの範囲に入ると、チョークポイントにより誘導されます。その後、このチョークポイントの MAC アドレスが、誘導されたタグにより送信される次のビーコンに含められます。このタグ ビーコンを検出したすべてのアクセス ポイントはその後、情報をコントローラと Location Appliance に転送します。

アクティブな Compatible Extensions 準拠のタグと一緒にチョークポイントを使用すると、タグとそのアセットに関する位置情報が即座に提供されます。Cisco Compatible Extension タグがチョークポイントの範囲外に出ると、後続のビーコン フレームには、チョークポイントの識別情報が何も含まれません。タグの位置はデフォルトで、タグにアソシエートされているアクセス ポイントにより報告される RSSI に基づいた標準の計算方法で決定されます。

ここでは、次の内容について説明します。

Prime Infrastructure データベースへのチョークポイントの追加

チョークポイントは、チョークポイントのベンダーによって推奨されるとおりに設置および設定されます。チョークポイントのインストールが完了して動作可能になったら、チョークポイントをロケーション データベースに入力して、Prime Infrastructure マップ上に表示できます。

Prime Infrastructure データベースにチョークポイントを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Chokepoints] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　チョークポイントの MAC アドレスと名前を入力します。

ステップ 5　[Entry/Exit Chokepoint] チェックボックスをオンにします。

ステップ 6　チョークポイントのカバレッジ範囲を入力します。

（注）　チョークポイントの範囲は視覚的に表示されるだけです。これは製品固有です。実際の範囲は、該当するチョークポイント ベンダー ソフトウェアを使用して別個に設定する必要があります。

ステップ 7　[OK] をクリックします。

（注）　データベースにチョークポイントを追加したら、適切な Prime Infrastructure フロア マップに配置できます。

Prime Infrastructure マップへのチョークポイントの追加

チョークポイントをマップに追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Maps] ページで、チョークポイントのフロアの位置に対応するリンクを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 4　[Go] をクリックします。

（注）　[Add Chokepoints] 概要ページには、データベースには存在しているが、まだマップされていない、最近追加されたチョークポイントがすべて一覧表示されます。

ステップ 5　マップ上に配置するチョークポイントの横にあるチェックボックスを選択します。

ステップ 6　[OK] をクリックします。

チョークポイント アイコンが左上隅に配置されたマップが表示されます。これで、マップ上にチョークポイントを配置する準備ができました。

ステップ 7　チョークポイント アイコンを左クリックし、適切な位置までドラッグします。

（注）　チョークポイント アイコンを配置するためにクリックすると、左側のダイアログボックスにチョークポイントの MAC アドレス、名前、およびカバレッジ範囲が表示されます。

ステップ 8　[Save] をクリックします。

フロア マップに戻ると、マップ上に追加されたチョークポイントが表示されます。

（注）　新たに作成されたチョークポイント アイコンは、そのフロアの表示設定に応じて、マップに表示される場合と表示されない場合があります。

（注）　チョークポイントの周囲の輪は、カバレッジ領域を示しています。CCX タグとそのアセットがカバレッジ領域内を通過すると、位置の詳細がブロードキャストされ、タグはチョークポイント カバレッジ円上に自動的にマップされます。タグがチョークポイントの範囲外に出ると、その位置は以前と同様に計算されるので、チョークポイントの輪の上にはマップされなくなります。

（注）　チョークポイントのマップ アイコンの上にマウス カーソルを移動すると、チョークポイントの MAC アドレス、名前、Entry/Exit チョークポイント、スタティック IP アドレス、および範囲が表示されます。

ステップ 9　チョークポイントがマップ上に表示されない場合は、[Floor Settings] メニューにある [Chokepoints] チェックボックスを選択します。

（注）　すべてのマップに対してこの表示条件を保存しない場合には、[Save Settings] をクリックしないでください。

（注）　ネットワーク設計をモビリティ サービス エンジンまたはロケーション サーバに同期して、チョークポイント情報をプッシュする必要があります。

チョークポイントの配置

チョークポイントをマップ上に配置するには、次の手順を実行します。

ステップ 1　**チョークポイント** アイコンを左クリックし、適切な位置までドラッグします。

（注）　チョークポイント アイコンを配置するためにクリックすると、左側のダイアログボックスにチョークポイントの MAC アドレス、名前、およびカバレッジ範囲が表示されます。

ステップ 2　アイコンが正しくマップに配置されたら、[Save] をクリックします。

ステップ 3　新たに作成されたチョークポイント アイコンは、そのフロアの表示設定に応じて、マップに表示される場合と表示されない場合があります。

（注）　チョークポイントの周囲の輪は、カバレッジ領域を示しています。Cisco Compatible Extensions タグとそのアセットがカバレッジ領域内を通過すると、位置の詳細がブロードキャストされ、タグはチョークポイント カバレッジ円上に自動的にマップされます。チョークポイントの範囲は表示されるだけですが、実際に範囲を設定するにはチョークポイントのベンダー ソフトウェアが必要です。タグがチョークポイントの範囲外に出ると、その位置は以前と同様に計算されるので、チョークポイントの輪の上にはマップされなくなります。

（注）　チョークポイントのマップ アイコンの上にマウス カーソルを移動すると、チョークポイントの MAC アドレス、名前、および範囲が表示されます。

ステップ 4　チョークポイントがマップ上に見当たらない場合、[Layers] を選択して、マップ上で表示できる要素のドロップダウン リストを表示します。[Chokepoints] チェックボックスをオンにします。

（注）　すべてのマップに対してこの表示条件を保存しない場合には、[Save Settings] をクリックしないでください。

（注）　ファイルをインポートまたはエクスポートすることにより、チョークポイントの位置を変更できます。

Wi-Fi TDOA 受信機の設定

ここでは、次の内容について説明します。

Prime Infrastructure データベースへの Wi-Fi TDOA 受信機の追加

Wi-Fi TDOA 受信機を Prime Infrastructure データベースに追加するには、次の手順を実行します。

ステップ 1　[Configure] > [WiFi TDOA Receivers] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add WiFi TDOA Receivers] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　Wi-Fi TDOA 受信機の MAC アドレス、名前、およびスタティック IP アドレスを入力します。

（注）　Wi-Fi TDOA 受信機は、ベンダー ソフトウェアを使用して個別に設定されます。

ステップ 5　[OK] をクリックして、Wi-Fi TDOA 受信機のエントリをデータベースに保存します。

（注）　データベースに Wi-Fi TDOA 受信機が追加されたら、適切な Prime Infrastructure フロア マップに配置します。詳細については、「Prime Infrastructure データベースへの Wi-Fi TDOA 受信機の追加」（P.6-197）を参照してください。

マップへの Wi-Fi TDOA 受信機の追加

WiFi TDOA 受信機をマップに追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　Wi-Fi TDOA 受信機のフロアの位置に対応するリンクを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add WiFi TDOA Receivers] を選択します。

ステップ 4　[Go] をクリックします。

（注）　[Add WiFi TDOA Receivers] 概要ページには、データベースには存在しているが、まだマップされていない、最近追加された Wi-Fi TDOA 受信機がすべて一覧表示されます。

ステップ 5　マップに追加する Wi-Fi TDOA 受信機の隣のチェックボックスをオンにします。

ステップ 6　[OK] をクリックします。

緑色の Wi-Fi TDOA 受信機アイコンが左上隅に配置されたマップが表示されます。これで、マップ上に Wi-Fi TDOA 受信機を配置する準備ができました。

Wi-Fi TDOA 受信機の配置

Wi-Fi TDOA 受信機をマップ上に配置するには、次の手順を実行します。

ステップ 1　**Wi-Fi TDOA 受信機**アイコンを左クリックし、適切な位置までドラッグします。

（注）　Wi-Fi TDOA 受信機アイコンを配置するためにクリックすると、左側のペインに Wi-Fi TDOA 受信機の MAC アドレスと名前が表示されます。

ステップ 2　アイコンが正しくマップに配置されたら、[Save] をクリックします。

（注）　Wi-Fi TDOA 受信機のマップ アイコンの上にマウス カーソルを移動すると、Wi-Fi TDOA 受信機の MAC アドレスが表示されます。

ステップ 3　チョークポイントがマップ上に見当たらない場合、[Layers] をクリックして、マップ上で表示できる要素のドロップダウン リストを表示します。[WiFi TDOA Receivers] チェックボックスを選択します。

（注）　すべてのマップに対してこの表示条件を保存しない場合には、[Save Settings] を選択しないでください。

（注）　ファイルをインポートまたはエクスポートすることにより、Wi-Fi TDOA 受信機の位置を変更できます。

RF キャリブレーション モデルの管理

指定した RF モデルがフロアのレイアウトを十分に表していない場合は、フロアに適用するキャリブレーション モデルを作成し、そのフロアの減衰特性をより正確に表すことができます。キャリブレーション モデルは、別々のフロア領域に適用できる測定済みの RF 信号特性を使用して RF オーバーレイとして使用されます。これによって Cisco WLAN Solution インストール チームは複数フロア領域の 1 フロアをレイアウトし、RF キャリブレーション ツールを使用して新しいキャリブレーション モデルとしてそのフロアの RF 特性を測定して保存し、そのキャリブレーション モデルを同一の物理レイアウトを備えるすべての他のフロアに適用できます。

2 つの方法のいずれかを使用してキャリブレーションのデータを収集できます。

- ポイント モード データ収集：キャリブレーション ポイントを選択して、そのカバレッジ領域を一度に 1 つのロケーションについて計算します。
- リニア モード データ収集：一連の直線状のパスを選択して、パスをたどりながら計算します。通常、このアプローチはポイント モード データ収集よりも速く計算できます。また、ポイント モード データ収集を使用すると、直線状のパスで見つからないロケーションに対するデータ収集を増やすことができます。

（注）　キャリブレーション モデルは、クライアント、不正なクライアント、および不正なアクセス ポイントのみに適用できます。タグのキャリブレーションには、AeroScout システム マネージャを使用します。タグのキャリブレーションの詳細については、http://support.aeroscout.com を参照してください。

（注）　802.11a/n 無線と 802.11b/g/n 無線の両方をサポートするクライアント デバイスを使用して、両方の周波数帯のキャリブレーションを迅速に処理することを推奨します。

ラップトップやその他のワイヤレス デバイスを使用して、Prime Infrastructure サーバへのブラウザを開き、キャリブレーション プロセスを実行します。

ここでは、次の内容について説明します。

- 「キャリブレーション」（P.6-204）
- 「フロアへのモデルの適用」（P.6-204）
- 「キャリブレーション モデルの削除」（P.6-205）

現在のキャリブレーション モデルへのアクセス

現在のキャリブレーション モデルにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[RF Calibration Models] を選択します。各キャリブレーション モデルの [Model Name] と [Status] が表示されます。

ステップ 3　特定のキャリブレーション モデルにアクセスするには、モデル名をクリックします。

マップへのキャリブレーション モデルの適用

現在のキャリブレーション モデルをマップに適用するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[RF Calibration Models] を選択します。

ステップ 3　該当するキャリブレーション モデルにアクセスするには、モデル名をクリックします。

ステップ 4　[Select a command] ドロップダウン リストから、[Apply to Maps] を選択します。

ステップ 5　[Go] をクリックします。

キャリブレーション モデル プロパティの表示

現在のキャリブレーション モデルを表示または編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[RF Calibration Models] を選択します。

ステップ 3　該当するキャリブレーション モデルにアクセスするには、モデル名をクリックします。

ステップ 4　[Select a command] ドロップダウン リストから、[Properties] を選択します。

ステップ 5　[Go] をクリックして、キャリブレーション モデルの詳細を表示または編集します。詳細については、「キャリブレーション モデル プロパティの表示」（P.6-200）を参照してください。

キャリブレーション モデルの詳細の表示

キャリブレーション モデルの詳細を編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[RF Calibration Models] を選択します。

ステップ 3　該当するキャリブレーション モデルにアクセスするには、モデル名をクリックします。

ステップ 4　[Select a command] ドロップダウン リストから、[Properties] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　次のパラメータを編集できます。

- [Sweep Client Power for Location]：有効にするにはクリックします。アクセス ポイントが高密度に存在し、送信電力が低下しているか、または不明である場合に有効にすると効果的です。クライアントの送信電力におけるスイープ範囲の精度は高まりますが、拡張性は低下します。
- [HeatMap Binsize]：ドロップダウン リストから、[4]、[8]、[16]、または [32] を選択します。
- [HeatMap Cutoff]：ヒートマップ カットオフを決定します。特にアクセス ポイント密度が高く、RF 伝播条件が良好な場合は、低いヒートマップ カットオフを設定することを推奨します。高いカットオフ値により、拡張性は高まりますが、クライアントの検索が難しくなる可能性があります。

ステップ 7　必要な変更が完了した場合やページを終了する場合は、[OK] をクリックします。

新しいキャリブレーション モデルの作成

新しいキャリブレーション モデルを作成するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[RF Calibration Models] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[Select a command] ドロップダウン リストから、[Create New Model] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　モデル名を入力し、[OK] をクリックします。

[Not Yet Calibrated] ステータスの他の RF キャリブレーション モデルとともに、新しいモデルが表示されます。

キャリブレーション プロセスの開始

キャリブレーション プロセスを開始するには、次の手順を実行します。

ステップ 1　[Calibration Model] > [Model Name] ページを開くには、モデル名をクリックします。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Data Points] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　キャリブレーションの実行に使用しているデバイスの MAC アドレスを入力します。手動で入力する MAC アドレスはコロンで区切る必要があります（例：FF:FF:FF:FF:FF:FF）。

（注）　このプロセスが Cisco Centralized アーキテクチャを介して Prime Infrastructure に接続されたモバイル デバイスから実行されている場合は、MAC アドレス テキスト ボックスに自動的にデバイスのアドレスが読み込まれます。

ステップ 5　キャリブレーションが実行される適切なキャンパス、ビルディング、フロア、または屋外領域を選択します。

（注）　屋外領域のキャリブレーションはリリース 1.0.x 以降でサポートされています。このオプションを使用して、キャリブレーション データ ポイントを屋外領域に追加できます。キャリブレーションと同様の手順を使用して、データ ポイントを屋外領域に追加できます。

ステップ 6　[Next] をクリックします。

ステップ 7　選択したフロア マップおよびアクセス ポイントの位置が表示されるときには、キャリブレーションのためのデータ収集を実行した位置がプラス マーク（+）のグリッドで表されます。

これらの位置をガイドラインとして使用して、[Calibration Point] ポップアップ（ポイント収集の場合）または [Start]/[Finish] ポップアップ（リニア収集の場合）のいずれかを適切に配置することにより、データのポイント収集またはリニア収集のいずれかを実行できます。これらのポップアップは、それぞれのオプションが表示されるとマップ上に表示されます。

キャリブレーション データのポイント収集を実行するには、次の手順を実行します。

a. [Collection Method] ドロップダウン リストから [Point] を選択し、[Show Data points] チェックボックスがまだオンになっていない場合にはオンにします。マップ上に [Calibration Point] ポップアップが表示されます。

b. データ ポイント（+）に [Calibration Point] ポップアップの先端を配置し、[Go] をクリックします。データ収集の進捗を示すダイアログボックスが表示されます。

（注）　近辺にあるすべてのアクセス ポイントでクライアントが均等に受信されるように、データ収集中のキャリブレーション クライアント ラップトップを回転させます。

c. 選択したデータ ポイントでデータ収集が完了し、カバレッジ領域がマップ上に表示されたら、[Calibration Point] ポップアップを別のデータ ポイントに移動して [Go] をクリックします。

（注）　マップ上に表示されたカバレッジ領域は色分けされ、そのデータを収集するために使用した特定の無線 LAN 規格に対応します。カラー コーディングに関する情報は、ページの左側の凡例に示されます。また、キャリブレーション処理の進捗は、凡例の上の 2 つのステータス バーに示されます。1 つは 802.11a/n 用、もう 1 つは 802.11b/g/n 用です。

（注）　誤って選択した位置のデータ ポイントを削除するには、[Delete] をクリックして適切なデータ ポイント上に表示される黒の四角形を移動します。必要に応じて、**Ctrl** キーを押しながらマウスを移動し、四角形のサイズを変更します。

d. 関連する周波数帯（802.11a/n、802.11b/g/n）のキャリブレーション ステータス バーの表示が「done」になるまで、ポイント収集のステップ a. ～ c. を繰り返します。

（注）　キャリブレーション ステータス バーは、約 50 か所の異なる位置と 150 個の測定結果を収集すると、キャリブレーション用のデータ収集の完了を表示します。キャリブレーション プロセスで保存されたそれぞれの位置で、複数のデータ ポイントが収集されます。キャリブレーション処理の進捗は、凡例の上の 2 つのステータス バーに示されます。1 つは 802.11b/g/n 用、もう 1 つは 802.11a/n 用です。

キャリブレーション データのリニア収集を実行するには、次の手順を実行します。

a. [Collection Method] ドロップダウン リストから [Linear] を選択し、[Show Data points] チェックボックスがまだオンになっていない場合にはオンにします。[Start] ポップアップと [Finish] ポップアップの両方と共に、マップ上に線が表示されます。

b. 開始データ ポイントに [Start] ポップアップの先端を配置します。

c. 終了データ ポイントに [Finish] ポップアップを配置します。

d. 開始データ ポイントにラップトップを持って立ち、[Go] をクリックします。定義されたパスに沿って終了ポイントに向かって一定のペースで歩きます。データ収集が処理中であることを示すダイアログボックスが表示されます。

（注）　データ収集バーが完了を示したとしても、終了ポイントに到達するまでデータ収集を中止しないでください。

（注）　Intel 製およびシスコ製のアダプタのみテスト済みです。[Cisco Compatible Extension Options] で、[Enable Cisco Compatible Extensions] と [Enable Radio Management Support] が有効になっていることを確認します。

e. 終了ポイントに到達したら、スペース バー（またはデータ収集パネル上の [Done]）を押します。収集ペインには、収集したサンプル数が表示されます。収集ペインが閉じると、マップが表示されます。マップには、データが収集されたすべてのカバレッジ領域が表示されます。

（注）　誤って選択した位置のデータ ポイントを削除するには、[Delete] をクリックして適切なデータ ポイント上に表示される黒の四角形を移動します。必要に応じて、Ctrl キーを押しながらマウスを移動し、四角形のサイズを変更します。

（注）　カバレッジ領域は色分けされ、そのデータを収集するために使用した特定の無線 LAN 規格に対応します。カラー コーディングに関する情報は、ページの左側の凡例に示されます。

f. 各周波数帯のステータス バーが [done] になるまで、リニア収集のステップ b ～ e を繰り返します。

（注）　リニア収集に加えてポイント モード データ収集を実行すると、見つからないカバレッジ領域に対応できます。

ステップ 8　ページ上部のキャリブレーション モデルの名前をクリックすると、そのモデルのメインページに戻り、データ ポイントを調整できます。

ステップ 9　[Select a command] ドロップダウン リストから [Calibrate] を選択し、[Go] をクリックします。

ステップ 10　キャリブレーションが完了したら、[Inspect Location Quality] リンクをクリックします。RSSI 測定値を示すマップが表示されます。

ステップ 11　新しく作成されたキャリブレーション モデルを使用するには、それが作成されたフロアにそのモデル適用する必要があります（また、類似する減衰特性を持つその他のフロアについても同様）。[Monitor] > [Site Maps] を選択して、モデルを適用する特定のフロアを見つけます。フロア マップのインターフェイスで、ドロップダウン リストから [Edit Floor Area] を選択し、[Go] をクリックします。

ステップ 12　[Floor Type (RF Model)] ドロップダウン リストから、新たに作成したキャリブレーション モデルを選択します。[OK] をクリックして、フロアにモデルを適用します。

（注）　このプロセスを、必要なモデルとフロアの数に応じて繰り返します。モデルをフロアに適用すると、そのフロアで実行される位置判定はすべて、キャリブレーション モデルから収集した特定の減衰データを使用して実行されます。

キャリブレーション

収集したデータ ポイントを計算するには、次の手順を実行します。

ステップ 1　[Calibration Model] > [Model Name] ページを開くには、モデル名をクリックします。

ステップ 2　[Calibration Model] > [Model Name] ページで、[Select a command] ドロップダウン リストから [Calibrate] を選択します。

ステップ 3　[Go] をクリックします。

フロアへのモデルの適用

新たに作成されたキャリブレーション モデルを使用するには、それが作成されたフロアにモデルを適用する必要があります（類似する減衰特性を持つ他のフロアについても同様）。

フロアにモデルを適用するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　モデルを適用する特定のフロアを見つけます。

ステップ 3　[Select a command] ドロップダウン リストから、[Edit Floor Area] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[Floor Type (RF Model)] ドロップダウン リストから、新たに作成したキャリブレーション モデルを選択します。

ステップ 6　[OK] をクリックして、フロアにモデルを適用します。

このプロセスを、必要なモデルとフロアの数に応じて繰り返します。モデルをフロアに適用すると、そのフロアで実行される位置判定はすべて、キャリブレーション モデルから収集した特定の減衰データを使用して実行されます。

キャリブレーション モデルの削除

キャリブレーション モデルを削除するには、次の手順を実行します。

ステップ 1　[Calibration Model] > [Model Name] ページを開くには、モデル名をクリックします。

ステップ 2　[Select a command] ドロップダウン リストから [Delete Model] を選択します。

ステップ 3　[Go] をクリックします。

位置プレゼンス情報の管理

モビリティ サービス エンジンでロケーション表示を有効にすると、シスコのデフォルト設定（キャンパス、ビルディング、フロア、XY 座標）以外の拡張 Civic ロケーション情報（市町村、州、郵便番号、国）および GEO ロケーション情報（経度、緯度）を表示できます。クライアントは、ロケーションベースのサービスとアプリケーションで使用するために、オンデマンド ベースでこの情報を要求できます。位置プレゼンスの有効化の詳細については、「モビリティ サービスのロケーション表示の有効化」（P.16-996）を参照してください。

現在のマップの位置プレゼンス情報を表示または編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　マップのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Location Presence] を選択します。

ステップ 4　[Go] をクリックします。

[Location Presence] ページが表示されます。

（注）　現在のマップのロケーション情報（[Area Type]、[Campus]、[Building]、および [Floor]）では、[Monitor] > [Site Maps] ページで選択したマップの情報が表示されます。別のマップを選択するには、[Select a Map to Update Presence Information] ドロップダウン リストを使用して、新しいマップ位置を選択します。

ステップ 5　[Civic Address] タブ、[GPS Markers] タブ、または [Advanced] タブをクリックします。

- [Civic Address]：名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパス、ビルディング、またはフロアを特定します。
- [GPS Markers]：経度と緯度でキャンパス、ビルディング、またはフロアを特定します。
- [Advanced]：近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパス、ビルディング、またはフロアを特定します。

（注）　選択した各フィールドには、上記のすべてが含まれています。たとえば、[Advanced] を選択した場合、ユーザからの要求により GPS および Civic 位置情報も提供されます。選択した設定は、モビリティ サービス エンジン レベルでの設定と一致する必要があります。詳細については、「モビリティ サービスのロケーション表示の有効化」（P.16-996）を参照してください。

（注）　クライアントが、キャンパスに対して [GPS Markers] フィールドで設定されていないビルディング、フロア、または屋外領域などのロケーション情報を要求した場合、エラー メッセージが表示されます。

（注）　デフォルトでは、[Override Child Element Presence Info] チェックボックスがオンになっています。

マップの検索

[Search Maps] ページで、次のパラメータを使用できます。

- Search for
- Map Name
- Search in
- Save Search
- Items per page

[Go] をクリックすると、マップ検索結果ページが表示されます（表 6-9 を参照）。

表 6-9　Map Search Results

フィールド	オプション
Name	[Name] 列の項目をクリックすると、各フロアに対する個々のフロア領域マップとともに既存のビルディングのマップが表示されます。
Type	キャンパス、ビルディングまたはフロア領域。
Total APs	検出された Cisco Radio の合計数が表示されます。
a/n Radios	802.11a/n Cisco Radio の数が表示されます。
b/g/n Radios	802.11b/g/n Cisco Radio の数が表示されます。

Map Editor の使用

Prime Infrastructure の Map Editor を使って、フロア図面情報を定義、描画、および拡張することができます。ここでは、次の内容について説明します。

- 「Map Editor の表示」（P.6-207）
- 「Map Editor を使用した多角形領域の描画」（P.6-207）
- 「フロア上の包含リージョンの定義」（P.6-208）
- 「フロア上の除外リージョンの定義」（P.6-210）
- 「フロアでのレール ラインの定義」（P.6-211）

Map Editor の表示

Map Editor を使用するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2　目的のキャンパスをクリックします。[Site Maps] > [Campus Name] ページが表示されます。

ステップ 3　キャンパスをクリックし、次にビルディングをクリックします。

ステップ 4　目的のフロア領域をクリックします。[Site Maps] > [Campus Name] > [Building Name] > [Floor Area Name] ページが表示されます。

ステップ 5　[Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。[Map Editor] ページが表示されます。

（注）　外壁より外部の空白部分がすべてなくなるように、フロア図面のイメージが適切に縮尺されていることを確認してください。フロアの寸法が正確かどうかを確かめるには、ツールバーの**コンパス ツール**をクリックします。

ステップ 6　基準長を配置します。実行すると、指定した線の長さの [Scale] メニューが表示されます。基準長の寸法（幅と高さ）を入力して、[OK] をクリックします。

ステップ 7　[Antenna Mode] ドロップダウン リストから、伝播パターンを決定します。

ステップ 8　アンテナ方向バーを目的の度の方向へスライドさせて、アンテナ調整をします。

ステップ 9　目的のアクセス ポイントを選択します。

ステップ 10　[Save] をクリックします。

Map Editor を使用した多角形領域の描画

長方形以外のビルディングがある場合、またはフロア内に長方形以外の領域をマークする場合には、Map Editor を使用して多角形の領域を描画できます。

ステップ 1　フロア図面が Prime Infrastructure にまだ表示されていない場合は、フロア図面を追加します（「フロア領域の追加」（P.6-158）を参照）。

ステップ 2　[Monitor] > [Site Maps] を選択します。

ステップ 3　編集する屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 4　[Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。

ステップ 5　[Map Editor] ページで、ツールバーの [Add Perimeter] アイコンをクリックします。

ポップアップが表示されます。

ステップ 6　定義する領域の名前を入力します。[OK] をクリックします。

描画ツールが表示されます。

ステップ 7　輪郭を描く領域に描画ツールを移動します。

- 左マウス ボタンをクリックして、線の描画を開始および終了します。

- 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。

マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。

ステップ 8　ツールバーのディスク アイコンをクリックして、新たに描画した領域を保存します。

ステップ 9　[Command] > [Exit] を選択して、ウィンドウを閉じます。元のフロア図面に戻ります。

（注）　Map Editor を終了して元のフロア図面ビューに戻ると、新たに描画した領域は表示されません。ただし、要素を追加する際に、[Planning Model] ページには表示されます。

ステップ 10　[Select a command] ドロップダウン リストから [Planning Mode] を選択して、新たに定義した多角形領域に要素を追加し始めます。

表 6-10 では、障害のカラー コーディングについて説明します。

表 6-10　障害のカラー コーディング

障害のタイプ	カラー コーディング	損失（dB）
厚い壁		13
薄い壁		2
重いドア		15
軽いドア		4
パーティション		1
ガラス		1.5

（注）　アクセス ポイントの RF 予測ヒートマップは、実際の RF 信号強度を近似したものです。このヒートマップでは Map Editor を使用して描画された障害物の減衰が考慮されていますが、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されません。13 dB の損失を与える厚い壁（オレンジに色分けされている）では、ヒートマップの壁を超える RF 信号を十分に封じ込められない場合があります。

フロア上の包含リージョンの定義

包含領域を定義するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域の名前をクリックします。

ステップ 3　[Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　マップで、ツールバーの水色のボックスをクリックします。

（注）　一度に 1 つの包含領域のみ定義できることを示すメッセージ ボックスが表示されます。新しい包含リージョンを定義すると、以前に定義されていた包含リージョンは自動的に削除されます。デフォルトでは、各フロアの包含リージョンは、そのリージョンが Prime Infrastructure に追加されるときに定義されます。包含リージョンは水色の実線で示され、通常はリージョンの輪郭を描きます。

ステップ 6　表示されるメッセージ ボックスで [OK] をクリックします。包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7　包含領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8　含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。再びクリックすると、次の境界線を定義できます。

ステップ 9　領域の輪郭が描画されるまでステップ 8 を繰り返したら、描画アイコンをダブルクリックします。水色の実線によって包含領域が定義されます。

ステップ 10　[Command] メニューから [Save] を選択するか、ツールバーの**ディスク** アイコンをクリックして、包含リージョンを保存します。

（注）　包含領域を誤って定義した場合は、領域をクリックします。選択された領域の輪郭が水色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 11　フロア マップに戻ってヒートマップ上で包含リージョンを有効にするには、[Command] メニューから [Exit] を選択します。

ステップ 12　[Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。これをすべてのフロア マップに適用する場合は、[Save settings] をクリックします。[Layers configuration] ページを閉じます。

ステップ 13　Prime Infrastructure データベースと MSE データベースを再同期するには、[Services] > [Synchronize Services] を選択します。

（注）　2 つの DB がすでに同期されている場合は、変更があるたびに自動的に再同期が実行されます。明示的に再同期する必要はありません。

ステップ 14　[Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

（注）　新たに定義された包含リージョンと除外リージョンは、モビリティ サービス エンジンによってロケーションが再計算された後にヒートマップ上に表示されます。

フロア上の除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外できます。通常、除外領域は包含領域の境界内に定義されます。

除外領域を定義するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域の名前をクリックします。

ステップ 3　[Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　マップで、ツールバーの紫色のボックスをクリックします。

ステップ 6　表示されるメッセージ ボックスで [OK] をクリックします。除外領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7　除外領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8　除外する領域の境界に沿って描画アイコンを移動させます。1 回クリックして境界線を開始し、再びクリックして境界線を終了します。

ステップ 9　領域の輪郭が描画されるまでステップ 8 を繰り返したら、描画アイコンをダブルクリックします。定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。除外された領域は紫色で網掛けされます。

ステップ 10　追加の除外リージョンを定義するには、ステップ 5 ～ ステップ 9 を繰り返します。

ステップ 11　すべての除外領域を定義したら、[Command] メニューから [Save] を選択するか、ツールバーの**ディスク** アイコンをクリックして、除外リージョンを保存します。

（注）　除外領域を削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 12　フロア マップに戻ってヒートマップ上で除外リージョンを有効にするには、[Command] メニューから [Exit] を選択します。

ステップ 13　完了したら、[Location Regions] チェックボックスがまだオンになっていない場合にはオンにし、[Save settings] をクリックし、[Layers configuration] ページを閉じます。

ステップ 14　Prime Infrastructure データベースとロケーション データベースを再同期するには、[Services] > [Synchronize Services] を選択します。

ステップ 15　[Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

フロアでのレール ラインの定義

フロア上にコンベヤ ベルトを表すレール ラインを定義できます。また、レール領域の周囲にスナップ幅とも呼ばれる、ロケーション計算を一層サポートする領域を定義できます。この領域は、クライアントが表示されると予測される領域を表します。スナップ幅の領域内に配置されたクライアントは、レール ライン上に表示されるか（多数）、スナップ幅領域の外側に表示されます（少数）。

（注） レール ラインの設定はタグには適用されません。

スナップ幅領域は、フィートまたはメートル（ユーザ定義）単位で定義され、レールの片側（東および西、または北および南）からモニタされる距離を表します。

レールをフロアに定義するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域の名前をクリックします。

ステップ 3　[Select a command] ドロップダウン リストから、[Map Editor] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　マップで、ツールバーの**レール** アイコン（紫色の除外アイコンの右側）をクリックします。

ステップ 6　表示されるメッセージ ダイアログボックスで、レールのスナップ幅（フィートまたはメートル）を入力し、[OK] をクリックします。描画アイコンが表示されます。

ステップ 7　レール ラインの開始ポイントで**描画**アイコンをクリックします。ラインの描画を停止するときやラインの方向を変えるときは、再びクリックします。

ステップ 8　フロア マップ上にレール ラインを完全に描画したら、**描画**アイコンを 2 回クリックします。レール ラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。

（注） レール ラインを削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 9　フロア マップに戻ってヒートマップ上でレールを有効にするには、[Command] メニューから [Exit] を選択します。

ステップ 10　フロア マップで、[Layers] ドロップダウン リストを選択します。

ステップ 11　完了したら、[Rails] チェックボックスがまだオンになっていない場合にはオンにし、[Save settings] をクリックし、[Layers configuration] パネルを閉じます。

ステップ 12　Prime Infrastructure とモビリティ サービス エンジンを再同期するには、[Services] > [Synchronize Services] を選択します。

ステップ 13　[Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

位置の準備状態と品質の調査

Prime Infrastructure を設定することで、既存のアクセス ポイント展開の能力を確認し、少なくとも 90 % の確率で、10 m 以内にあるクライアント、不正クライアント、不正アクセス ポイント、またはタグの真の位置を推定できます。位置の準備状態の計算は、アクセス ポイントの数と配置に基づいています。

また、位置の品質と指定の位置の能力を確認し、実際の調査とキャリブレーションの際に収集されたデータ ポイントに基づいて、位置の仕様（10 m、90 %）を満たすこともできます。

位置の準備状態の調査

Inspect Location Readiness 機能は距離ベースの予測ツールで、アクセス ポイントを配置した場合に起こる問題領域を指摘できます。

Inspect Location Readiness ツールを表示する手順は、次のとおりです。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域名をクリックして、マップを表示します。

（注）　RSSI が表示されない場合は、左側のサイドバー メニューの [AP Heatmaps] チェックボックスをオンにして、AP ヒートマップを有効にできます。

（注）　クライアント、タグ、およびアクセス ポイントが表示されない場合は、左側のサイドバー メニューでそれぞれのチェックボックスがオンになっていることを確認します。また、クライアントとタグをそれぞれ追跡するには、クライアントとタグの両方のライセンスを購入済みである必要もあります。

ステップ 3　[Select a command] ドロップダウン リストから、[Inspect Location Readiness] を選択します。

ステップ 4　[Go] をクリックします。

10 m、90 % の位置仕様を満たす領域（[Yes] で示される）と満たさない領域（[No] で示される）を示す、色分けされたマップが表示されます。

キャリブレーション データを使用した位置の品質の調査

領域を実際に調査する際に生成されたデータ ポイントに基づくキャリブレーション モデルが完了すると、アクセス ポイントの位置品質を調査できます。

キャリブレーションに基づき位置品質を調査するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[RF Calibration Model] を選択します。[Go] をクリックします。

キャリブレーション モデルの一覧が表示されます。

ステップ 3　適切なキャリブレーション モデルをクリックします。

最後のキャリブレーションの日付、キャリブレーションに使用される信号タイプ別（802.11a、802.11 b/g）のデータ ポイントの数、位置、およびカバレッジを含むキャリブレーションの詳細が表示されます。

ステップ 4　同じページの [Calibration Floors] 見出しの下にある [Inspect Location Quality] リンクをクリックします。

位置エラーの割合を示す、色分けされたマップが表示されます。

（注）　選択されている距離を変更して、位置エラーへの影響を確認できます。

VoWLAN の準備状態の調査

VoWLAN Readiness（音声の準備状態）ツールでは、RF カバレッジを確認し、音声のニーズを十分に満たすかどうか判断できます。このツールは、アクセス ポイントをインストールした後の RSSI レベルを確認します。

VoWLAN Readiness ツール（VRT）を表示する手順は、次のとおりです。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　該当するフロア領域名をクリックします。

ステップ 3　[Select a command] ドロップダウン リストから、[Inspect VoWLAN Readiness] を選択します。

ステップ 4　ドロップダウン リストから、[Band]、[AP Transmit Power]、および [Client] パラメータのうち、該当するものを選択します。

（注）　デフォルトでは、地域マップには Cisco 電話ベースの RSSI しきい値に対する b/g/n 帯域が表示されます。別の設定は保存できません。

ステップ 5　選択したクライアントによっては、次の RSSI 値が編集不可になる場合があります。

- [Cisco Phone]：RSSI 値を編集できません。
- [Custom]：RSSI 値を次の範囲で編集できます。
  - 低しきい値：-95 dBm ～ -45 dBm
  - 高しきい値：-90 dBm ～ -40 dBm

ステップ 6　領域が Voice Ready かどうかは、次の色で表示されます。

- 緑色：はい
- 黄色：しきい値周辺
- 赤色：いいえ

（注）　緑色 / 黄色 / 赤色のリージョンの精度は、RF 環境およびフロアが調整されているかどうかによって異なります。フロアが調整されている場合、リージョンの精度は高まります。

音声 RF カバレッジ問題のトラブルシューティング

- キャリブレーション データまたは未キャリブレーション データが存在するフロアは、次のように扱われます。
  - [AP Transmit] フィールドを [Max] に設定します（最大ダウンリンク電力設定）。マップに黄色か赤色の地域がまだ表示される場合は、フロアをカバーするのにアクセス ポイントを増やす必要があります。
  - 調整されたモデルが赤色または黄色のリージョン（音声が導入される予定のリージョン）を示し、[AP Transmit] フィールドが [Current] に設定されている場合は、アクセス ポイントの電力レベルを増やすことが効果的である場合があります。

マップを使用したメッシュ ネットワークのモニタリング

Prime Infrastructure のメッシュ ネットワーク マップから、次の要素の詳細にアクセスして表示することができます。

- メッシュ リンクの統計
- メッシュ アクセス ポイント
- メッシュ アクセス ポイント ネイバー

ここでは、これらの各アイテムに関する情報へのアクセスおよび表示方法の詳細について説明します。ここでは、次の内容について説明します。

- 「マップを使用したメッシュ リンクの統計のモニタリング」（P.6-214）
- 「マップを使用したメッシュ アクセス ポイントのモニタリング」（P.6-216）
- 「マップを使用したメッシュ アクセス ポイント ネイバーのモニタリング」（P.6-217）
- 「メッシュ ネットワーク階層の表示」（P.6-218）
- 「メッシュ フィルタを使用したマップ画面およびメッシュ リンクの修正」（P.6-219）

マップを使用したメッシュ リンクの統計のモニタリング

特定のメッシュ ネットワーク リンクの SNR と、そのリンク上で送受信されたパケットの数を表示し、[Monitor] > [Site Maps] ページからリンク テストを開始できます。

2 つのメッシュ アクセス ポイント間またはメッシュ アクセス ポイントとルート アクセス ポイント間の特定のメッシュ リンクに関する詳細を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　モニタする屋外領域、キャンパス、ビルディングまたはフロアに対応するマップ名をクリックします。

ステップ 3　左側のサイドバーのメニューから、[AP Mesh Info] の右側の矢印をクリックします。[Mesh Filter] ダイアログボックスが表示されます。

ステップ 4　各メッシュ アクセス ポイントの子の横の色付きドットの上にカーソルを移動して、これとその親間のリンクの詳細を表示します。表 6-11 に、表示されるパラメータをまとめています。

また、ドットの色は、次のように、SNR 強度のクイック リファレンス ポイントを示します。

- 緑のドットは、SNR が高いことを表します（25dB 以上）。
- 黄のドットは、SNR が許容範囲内にあることを表します（20 ～ 25dB）。
- 赤のドットは、SNR が低いことを表します（20dB 以下）。
- 黒のドットは、ルート アクセス ポイントを示します。

ブリッジ リンク情報が表示されます。

表 6-11　ブリッジ リンク情報

フィールド	説明
Information fetched on	情報を集めた日時
Link SNR	リンクの Signal to Noise Ratio（SNR）
Link Type	階層化されたリンク関係
SNR Up	アップリンクの Signal to Noise Ratio（dB）
SNR Down	ダウンリンクの Signal to Noise Ratio（dB）
PER	リンクのパケット エラー率
Tx Parent Packets	親として動作する際のノードに対する TX パケット
Rx Parent Packets	親として動作する際のノードに対する RX パケット
Time of Last Hello	最後のハローの日時

ステップ 5　[Link Test]、[Child to Parent] または [Link Test]、[Parent to Child] のいずれかをクリックします。リンク テストが完了すると、結果のページが表示されます。

（注）　リンク テストは 30 秒間稼働します。

（注）　リンク テストを両方のリンク（子対親と親対子）に同時に実行できません。

ステップ 6　SNR 統計をある期間にわたってグラフィカルに表示するには、リンク上の矢印をクリックします。複数の SNR グラフを含むページが表示されます。

表示されるリンクのグラフは、次のとおりです。

- [SNR Up]：アクセス ポイントの視点からのネイバーの RSSI 値を描画します。
- [SNR Down]：ネイバーがアクセス ポイントへレポートする RSSI 値を描画します。
- [Link SNR]：SNR Up 値に基づく重み付けされフィルタ処理された測定を描画します。
- [Adjusted Link Metric]：ルート アクセス ポイントへの最小コストのパスを決定するために使用された値を描画します。この値は、屋上アクセス ポイントに到達することの容易さを表し、ホップ カウントを計上します。この値が低くなるほど、パスは使用されにくくなります。

- [The Unadjusted Link Metric]：ホップ カウントによって未調整のルート アクセス ポイントに到達する最小コストのパスを描画します。未調整のリンクの値が高くなるほど、パスは効果的になります。

マップを使用したメッシュ アクセス ポイントのモニタリング

メッシュ ネットワーク マップから、次のメッシュ アクセス ポイントの概要を表示することができます。

- 親
- 子の数
- ホップ カウント
- ロール
- グループ名
- バックホール インターフェイス
- データ レート
- チャネル

（注） この情報は、すべてのアクセス ポイントに表示される情報（MAC アドレス、アクセス ポイント モデル、コントローラ IP アドレス、位置、アクセス ポイントの高さ、アクセス ポイントの稼働時間、および LWAPP の稼働時間）に追加して表示されます。

（注） 詳細な設定を確認して、マップからアラームとイベント情報にアクセスすることもできます。表示されるアラームとイベントの詳細については、「アラームおよびイベント一覧」（P.13-771）を参照してください。

メッシュ アクセス ポイントの設定情報の概要と詳細をメッシュ ネットワーク マップから表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　モニタするアクセス ポイントの屋外領域、キャンパス、ビルディングまたはフロアの位置に対応する [Map Name] をクリックします。

ステップ 3　アクセス ポイントの設定情報の概要を表示するには、マウス カーソルをモニタするアクセス ポイント上に移動します。選択したアクセス ポイントの設定情報が記載されたダイアログボックスが表示されます。

ステップ 4　アクセス ポイントの設定情報の詳細を表示するには、マップに表示されているアクセス ポイントをダブルクリックします。アクセス ポイントの設定の詳細が表示されます。

（注） アクセス ポイントのダイアログボックスにある [View Mesh Neighbors] リンクの詳細については、「マップを使用したメッシュ アクセス ポイント ネイバーのモニタリング」（P.6-217）を参照してください。アクセス ポイントに IP アドレスがある場合には、メッシュ アクセス ポイント ダイアログボックスの下部に [Run Ping Test] リンクも表示されます。

ステップ 5　[Access Point Details] 設定ページで次の手順に従って、メッシュ アクセス ポイントの設定詳細を表示します。

a. [General] タブをクリックし、AP 名、MAC アドレス、AP の稼働時間、アソシエートされているコントローラ（登録済みおよびプライマリ）の動作ステータス、ソフトウェア バージョンなど、メッシュ アクセス ポイントの全般的な設定を表示します。

（注） メッシュ アクセス ポイントのソフトウェア バージョンには、*m* の文字と *mesh* という単語をカッコで囲んだものが付加されます。

b. [Interface] タブをクリックし、メッシュ アクセス ポイントでサポートされるインターフェイスの設定詳細を表示します。インターフェイスのオプションは無線とイーサネットです。

c. [Mesh Links] タブをクリックし、メッシュ アクセス ポイントの親およびネイバーの詳細（名前、MAC アドレス、パケット エラー率、およびリンク詳細）を表示します。このページからリンク テストを開始することもできます。

d. [Mesh Statistics] タブをクリックし、メッシュ アクセス ポイントのブリッジ、キュー、およびセキュリティの統計に関する詳細を表示します。メッシュの統計の詳細については、「[Mesh Statistics] タブ」（P.5-79）を参照してください。

マップを使用したメッシュ アクセス ポイント ネイバーのモニタリング

メッシュ アクセス ポイントのネイバーの詳細をメッシュ ネットワーク マップから表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　モニタする屋外領域、キャンパス、ビルディングまたはフロアに対応するマップ名をクリックします。

ステップ 3　メッシュ アクセス ポイントのメッシュ リンクに関する詳細を表示するには、アクセス ポイント ラベルの矢印部分をクリックします。[Access Points] ページが表示されます。

ステップ 4　[Mesh Links] タブをクリックします。

（注） アクセス ポイント設定概要ダイアログボックスの [Mesh] タブにある [View Mesh Neighbors] リンクをクリックして、選択したアクセス ポイントのネイバーのメッシュ リンク詳細を表示することもできます。このダイアログボックスはマップ上のアクセス ポイントの上にマウス カーソルを移動すると表示されます。

（注） 信号対雑音比（SNR）が [View Mesh Neighbors] ダイアログボックスに表示されます。

（注） 表示されるダイアログボックスには現在および過去のネイバーの一覧に加えて、選択したアクセス ポイント、ネイバー アクセス ポイント、および子アクセス ポイントを特定するためのラベルが、メッシュ アクセス ポイント マップのアイコンに追加されます。選択したアクセス ポイントの [clear] リンクをクリックして、マップから関係を示すラベルを削除します。

（注）　メッシュ ネイバー ページの上部にあるドロップダウン リストには、表示されたマップの解像度（100 %）と表示された情報の更新間隔（5 分おき）が示されます。これらのデフォルト値は変更することができます。

メッシュ ネットワーク階層の表示

メッシュ ネットワーク内のメッシュ アクセス ポイントの親子関係を、移動が容易な画面に表示できます。興味のあるアクセス ポイントを選択するだけで、マップ ビューに表示されるアクセス ポイントをフィルタリングすることもできます。

選択したネットワークのメッシュ ネットワーク階層を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　表示するマップ名をクリックします。

ステップ 3　左側のサイドバー メニューにある [AP Mesh Info] チェックボックスがまだオンになっていない場合にはオンにします。

（注）　[AP Mesh Info] チェックボックスは、メッシュ アクセス ポイントがマップ上に存在する場合にだけ選択できます。メッシュ階層を表示するには、このチェックボックスをオンにする必要があります。

ステップ 4　[AP Mesh Info] の右側の青い矢印をクリックして、[Mesh Parent-Child Hierarchical View] を表示します。

ステップ 5　メッシュ アクセス ポイントの横に表示された**プラス（+）**の記号をクリックして、その子を表示します。

マイナス記号（-）が親メッシュ アクセス ポイントのエントリの横に表示されている場合には、すべての下位メッシュ アクセス ポイントが表示されます。たとえば、アクセス ポイントの *indoor-mesh-45-rap2* には *indoor-mesh-44-map2* という子が 1 つだけ存在します。

ステップ 6　各メッシュ アクセス ポイントの子の横の色付きドットの上にマウス カーソルを移動して、子と親の間のリンク詳細を表示します。表 6-12 に、表示されるパラメータをまとめています。

また、ドットの色は、SNR 強度のクイック リファレンス ポイントを示します。

- 緑のドットは、SNR が高いことを表します（25dB 以上）。
- 黄のドットは、SNR が許容範囲内にあることを表します（20 ～ 25dB）。
- 赤のドットは、SNR が低いことを表します（20dB 以下）。
- 黒のドットは、ルート アクセス ポイントを示します。

表 6-12　ブリッジ リンク情報

フィールド	説明
Information fetched on	情報を集めた日時
Link SNR	リンクの Signal to Noise Ratio（SNR）
Link Type	階層化されたリンク関係
SNR Up	アップリンクの Signal to Noise Ratio（dB）
SNR Down	ダウンリンクの Signal to Noise Ratio（dB）
PER	リンクのパケット エラー率
Tx Parent Packets	親として動作する際のノードに対する TX パケット
Rx Parent Packets	親として動作する際のノードに対する RX パケット
Time of Last Hello	最後のハローの日時

メッシュ フィルタを使用したマップ画面およびメッシュ リンクの修正

メッシュ階層ページでは、ホップ値およびメッシュ リンクに表示するラベルに基づいて、マップ上に表示するメッシュ アクセス ポイントを決定するメッシュ フィルタを定義することもできます。

メッシュ アクセス ポイントとそのルート アクセス ポイント間のホップ カウントによって、メッシュ アクセス ポイントがフィルタ処理されます。

メッシュ フィルタリングを使用する手順は、次のとおりです。

ステップ 1　メッシュ リンクのラベルおよび色の表示を変更する手順は、次のとおりです。

a. [Mesh Parent-Child Hierarchical View] で、[Link Label] ドロップダウン リストからオプションを選択します。オプションは、[None]、[Link SNR]、および [Packet Error Rate] です。

b. [Mesh Parent-Child Hierarchical View] で、[Link Color] ドロップダウン リストからオプションを選択し、マップのメッシュ リンクの色を決定するパラメータ（[Link SNR] または [Packet Error Rate]）を定義します。

（注）　リンクの色は、SNR 強度またはパケット エラー率のクイック リファレンス ポイントを示します。表 6-13 では、さまざまなリンクの色を定義しています。

表 6-13　SNR およびパケット エラー率のリンクの色の定義

リンクの色	リンク SNR	パケット エラー率（PER）
緑	SNR が 25dB を超えている（高い値）ことを表します。	PER が 1% 以下であることを表します。
オレンジ	SNR が 20 ～ 25dB（許容値）であることを表します。	PER が 1% より大きく 10% 未満であることを表します。
赤	SNR が 20dB を下回っている（低い値）ことを表します。	PER が 10% より大きいことを表します。

（注）　リンクのラベルおよび色の設定は、ただちにマップ上に反映されます。SNR と PER の両方の値を同時に表示することができます。

ステップ 2　メッシュ アクセス ポイントとその親との間のホップ カウントに基づいて、表示するメッシュ アクセス ポイントを変更する手順は、次のとおりです。

a. [Mesh Parent-Child Hierarchical View] で、[Quick Selections] ドロップダウン リストから適切なオプションを選択します。表 6-14 は、オプションの説明を示しています。

表 6-14　[Quick Selections] オプション

フィールド	説明
Select only Root APs	マップ ビューにルート アクセス ポイントだけを表示したい場合は、この設定を選択します。
Select up to 1st hops	マップ ビューに 1 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 2nd hops	マップ ビューに 2 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 3rd hops	マップ ビューに 3 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 4th hops	マップ ビューに 4 番めのホップだけを表示したい場合は、この設定を選択します。
Select All	マップ ビューにすべてのアクセス ポイントを表示したい場合は、この設定を選択します。

b. [Update Map View] をクリックして画面をリフレッシュし、選択したオプションでマップ ビューを表示します。

（注）　マップ ビュー情報は Prime Infrastructure データベースから取得され、15 分おきに更新されます。

（注）　メッシュ階層ビューで、アクセス ポイントのチェックボックスをオンまたはオフにし、表示するメッシュ アクセス ポイントを変更することもできます。子アクセス ポイントを表示するには、ルート アクセス ポイントへの親アクセス ポイントを選択する必要があります。

（注）　[Monitor] > [Site Maps] ページで MAC アドレスをクライアント ロゴとともに表示するには、次の手順を実行します。
a) [Maps Tree View] に移動します。
b) [Clients] の隣の [>] をクリックします。
c) [Small Icons] チェックボックスをオフにします。

マップを使用したタグのモニタリング

Prime Infrastructure マップでは、タグ付きのアセットの信号を生成したアクセス ポイントの名前、その信号の強度、およびアセットのロケーション情報が最後に更新された日時を確認できます。この情報は、マップ上のアセット タグ アイコンの上にマウス カーソルを移動するだけで表示されます。

マップ上でタグの位置ステータスを有効にするには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Campus] > [Building] > [Floor] を選択し、該当するモビリティ サービス エンジンとタグを選択します。

ステップ 3　[Floor Settings] ペイン（左側）の [802.11 Tags] チェックボックスがまだオンになっていない場合にはオンにします。

（注）　すべてのマップに対して [Floor Settings] に加えた変更を保存しない場合には、[Save Settings] をクリックしないでください。

ステップ 4　タグ アイコン（黄色のタグ）の上にマウス カーソルを移動すると、そのタグの設定概要がダイアログ ボックスに表示されます。

ステップ 5　新しいウィンドウでタグの詳細を表示するには、**タグ** アイコンをクリックします。

プランニング モードの使用

データ トラフィック、音声トラフィック、および位置がそれぞれアクティブかどうかに基づいて、アクセス ポイントの推奨される数および位置を計算できます。

（注）　プランニング モードでは、各プロトコル（802.11a または 802.11 b/g）に指定されるスループットに基づいて、ネットワーク内で最適カバレッジを提供するために必要な合計アクセス ポイント数が計算されます。

プランニング モードへのアクセス

プランニング モード機能にアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Name] リストから目的のキャンパスまたはビルディングを選択します。

ステップ 3　[Building] で目的のフロア領域をクリックします。

ステップ 4　[Select a command] ドロップダウン リストから [Planning Mode] を選択します。

ステップ 5　[Go] をクリックします。

（注）　プランニング モードでは、必要なアクセス ポイント数の計算に AP タイプおよびアンテナ パターン情報を使用しません。計算はアクセス ポイントのカバレッジ領域または各アクセス ポイントのユーザ数に基づいています。

プランニング モードのオプション：

- [Add APs]：マップへのアクセス ポイントの追加を可能にします。詳細については、「プランニング モードを使用したアクセス ポイント要件の計算」（P.6-222）を参照してください。
- [Delete APs]：選択したアクセス ポイントを削除します。
- [Map Editor]：[Map Editor] ウィンドウを開きます。詳細については、「Map Editor の使用」（P.6-206）を参照してください。
- [Synchronize with Deployment]：プランニング モードのアクセス ポイントを現在の導入シナリオと同期します。
- [Generate Proposal]：現在のアクセス ポイント導入のプランニング概要を表示します。
- [Planned AP Association Tool]：Excel または CSV ファイルから AP アソシエーションの追加、削除、またはインポートを実行できます。アクセス ポイントを定義したら、[Planned AP Association Tool] を使用して、そのアクセス ポイントをベース無線の MAC アドレスにアソシエートできます。AP が検出されない場合はスタンバイ バケットに送られ、AP が検出されたときにアソシエートされます。

（注）　AP アソシエーションには、AP はフロアまたは屋外領域に属さないという制限があります。AP がすでにフロアまたは屋外領域に割り当てられている場合は、スタンバイ バケットが AP を保持し、フロアまたは屋外領域から AP が削除されたときに、指定されたフロアに配置されます。1 つの MAC アドレスを複数のフロアまたは屋外領域のバケットに入力することはできません。

（注）　マップの同期は、AP がベース無線の MAC アドレスにアソシエートされている場合のみ動作し、イーサネット MAC アドレスにアソシエートされている場合は動作しません。

プランニング モードを使用したアクセス ポイント要件の計算

Prime Infrastructure プランニング モードを使用すると、マップ上に架空のアクセス ポイントを配置してカバレッジ領域が表示できるようになるため、領域をカバーするのに必要なアクセス ポイント数を計算できます。プランニング モードでは、各プロトコル（802.11a/n または 802.11b/g/n）に指定されるスループットに基づいて、ネットワーク内で最適カバレッジを提供するために必要な合計アクセス ポイント数が計算されます。次の条件に基づいて、アクセス ポイントの推奨される数および位置を計算できます。

- ネットワーク上でアクティブなトラフィックのタイプ：データ トラフィック、音声トラフィック、または両方
- 位置精度の要件
- アクティブなユーザ数
- 1 平方フィートごとのユーザ数

特定の配置におけるアクセス ポイントの推奨される数および配置を計算する手順は、次のとおりです。

ステップ 1　[Monitor] > [Site Maps] を選択します。

[Site Map] ページが表示されます。

ステップ 2　表示されるリストから、該当する位置のリンクを選択します。

インストールされているすべての要素（アクセス ポイント、クライアント、タグ）の配置および相対的な信号強度を示した、色分けされたマップが表示されます。

ステップ 3　[Select a command] ドロップダウン リスト（右上）から、[Planning Mode] を選択し、[Go] をクリックします。空白のフロア マップが表示されます。

ステップ 4　[Add APs] をクリックします。

ステップ 5　表示されるページで、破線の四角形を、推奨されるアクセス ポイントを計算するマップ位置にドラッグします。

（注）　四角形の端を選択し、Ctrl キーを押したままにして、四角形のサイズまたは配置を調整します。必要に応じてマウスを動かし、目的の位置の輪郭を描きます。次世代マップ モードを使用する場合、四角形の辺と頂点にあるハンドルをドラッグすると、サイズを変更できます。

ステップ 6　[Add APs] ドロップダウン リストから [Automatic] を選択します。

ステップ 7　[AP Type] と、そのアクセス ポイントに対して適切なアンテナおよびプロトコルを選択します。

ステップ 8　アクセス ポイントのターゲット スループットを選択します。

ステップ 9　フロアで使用される**サービス**の隣のチェックボックスをオンにします。オプションには、[Data/Coverage (default)]、[Voice]、[Location]、および [Location with Monitor Mode APs] があります。（表 6-15 を参照）。

（注）　少なくとも 1 つのサービスを選択しないと、エラーが発生します。

（注）　[Advanced Options] チェックボックスをオンにした場合、[Demand] と [Override Coverage per AP] の 2 つのアクセス ポイント プランニング オプションが追加で表示されます。また、[Data/Coverage] および [Voice] セーフティ マージン オプションに対しては、[Safety Margin] フィールドが表示されます。

表 6-15　サービス オプションの定義

<table>
<tr><th>サービス オプション</th><th>説明</th></tr>
<tr><td>Data/Coverage</td><td>データ トラフィックが無線 LAN 上で送信される場合は、このチェックボックスをオンにします。次の定義は、帯域およびデータ レートに応じて使用されます。
<table>
<tr><th>帯域</th><th>パス損失モデル（dBm）</th><th>データ レート（Mb/s）</th><th>領域（平方フィート）</th></tr>
<tr><td>802.11a</td><td>–3.3</td><td>10 ～ 12</td><td>6000</td></tr>
<tr><td>802.11a</td><td>–3.3</td><td>15 ～ 18</td><td>4500</td></tr>
<tr><td>802.11a</td><td>-3.5</td><td>10 ～ 12</td><td>5000</td></tr>
<tr><td>802.11a</td><td>-3.5</td><td>15 ～ 18</td><td>3250</td></tr>
<tr><td>802.11bg</td><td>–3.3</td><td>5</td><td>6500</td></tr>
<tr><td>802.11bg</td><td>–3.3</td><td>6</td><td>4500</td></tr>
<tr><td>802.11bg</td><td>-3.5</td><td>5</td><td>5500</td></tr>
<tr><td>802.11bg</td><td>-3.5</td><td>6</td><td>3500</td></tr>
</table>
[Advanced Options] チェックボックスをオンにした場合、データの信号強度のしきい値について、希望するセーフティ マージン（[Aggressive]、[Safe]、または [Very Safe]）を選択できます。
• Aggressive = 最小（-3 dBm）
• Safe = 中（0 dBm）
• Very Safe = 最大（+3 dBm）</td></tr>
</table>

表 6-15　サービス オプションの定義 （続き）

サービス オプション	説明
Voice	音声トラフィックが無線 LAN 上で送信される場合は、[Voice] チェックボックスをオンにします。 [Advanced Options] チェックボックスをオンにした場合、音声の信号強度のしきい値について、希望するセーフティ マージン（[Aggressive]、[Safe]、[Very Safe]、または [7920-enabled]）を選択できます。 • Aggressive = 最小 [-78 dBm (802.11a/b/g)] • Safe = 中 [-75 dBm (802.11a/b/g)] • Very Safe = 最大 [-72 dBm (802.11a/b/g)] • 7920_enabled = [-72 dBm (802.11a); -67 dBm (802.11b/g)]
Location	このチェックボックスをオンにすると、推奨されるアクセス ポイントの計算において、少なくとも 90 % の確率で、10 m 以内にある要素の真の位置が提供されるようになります。 条件を満たすために、各アクセス ポイントを、他のアクセス ポイントから 70 フィート以内に配置します。アクセス ポイントの周囲を六角形に区切り、その六角形を互い違いに組み合わせた形式の配置にします。 **（注）** 各サービス オプションには、そのオプションの上に示されているすべてのサービスが含まれます。たとえば、[Location] チェックボックスをオンにした場合、計算では、必要なアクセス ポイントの最適数を決定する際に、データ / カバレッジ、音声、および位置が考慮されます。

表 6-16　Advanced Services の定義

<table>
<tr><th>サービス オプション</th><th>説明</th></tr>
<tr><td>Data/Coverage</td><td>データ トラフィックが無線 LAN 上で送信される場合は、このチェックボックスをオンにします。次の定義は、帯域およびデータ レートに応じて使用されます。
<table>
<tr><th>帯域</th><th>パス損失モデル（dBm）</th><th>データ レート（Mb/s）</th><th>領域（平方フィート）</th></tr>
<tr><td>802.11a</td><td>–3.3</td><td>10 ～ 12</td><td>6000</td></tr>
<tr><td>802.11a</td><td>–3.3</td><td>15 ～ 18</td><td>4500</td></tr>
<tr><td>802.11a</td><td>-3.5</td><td>10 ～ 12</td><td>5000</td></tr>
<tr><td>802.11a</td><td>-3.5</td><td>15 ～ 18</td><td>3250</td></tr>
<tr><td>802.11bg</td><td>–3.3</td><td>5</td><td>6500</td></tr>
<tr><td>802.11bg</td><td>–3.3</td><td>6</td><td>4500</td></tr>
<tr><td>802.11bg</td><td>-3.5</td><td>5</td><td>5500</td></tr>
<tr><td>802.11bg</td><td>-3.5</td><td>6</td><td>3500</td></tr>
</table>
[Advanced Options] チェックボックスをオンにした場合、データの信号強度のしきい値について、希望するセーフティ マージン（[Aggressive]、[Safe]、または [Very Safe]）を選択できます。
• Aggressive = 最小（-3 dBm）
• Safe = 中（0 dBm）
• Very Safe = 最大（+3 dBm）</td></tr>
<tr><td>Voice</td><td>音声トラフィックが無線 LAN 上で送信される場合は、[voice] チェックボックスをオンにします。
[Advanced Options] チェックボックスをオンにした場合、音声の信号強度のしきい値について、希望するセーフティ マージン（[Aggressive]、[Safe]、[Very Safe]、または [7920-enabled]）を選択できます。
• Aggressive = 最小 [-78 dBm (802.11a/b/g)]
• Safe = 中 [-75 dBm (802.11a/b/g)]
• Very Safe = 最大 [-72 dBm (802.11a/b/g)]
7920_enabled = [-72 dBm (802.11a); -67 dBm (802.11b/g)]</td></tr>
<tr><td>Location</td><td>このチェックボックスをオンにすると、推奨されるアクセス ポイントの計算において、少なくとも 90 % の確率で、10 m 以内にある要素の真の位置が提供されるようになります。
条件を満たすために、各アクセス ポイントを、他のアクセス ポイントから 70 フィート以内に配置します。アクセス ポイントの周囲を六角形に区切り、その六角形を互い違いに組み合わせた形式の配置にします。
（注）　各サービス オプションには、そのオプションの上に示されているすべてのサービスが含まれます。たとえば、[Location] チェックボックスをオンにした場合、計算では、必要なアクセス ポイントの最適数を決定する際に、データ / カバレッジ、音声、および位置が考慮されます。</td></tr>
</table>

表 6-16　Advanced Services の定義 （続き）

サービス オプション	説明
Demand	アクセス ポイント計算の基準として、合計ユーザ数またはアクセス ポイントごとのユーザ比率を使用する場合は、このチェックボックスをオンにします。
Override Coverage per AP	アクセス ポイントのカバレッジの基準として、平方フィートのカバレッジを指定する場合は、このチェックボックスをオンにします。
Safety Margin	アクセス ポイントの計算において、データおよび音声サービスの相対的な信号強度の要件を制限するには、このチェックボックスをオンにします。オプションは [Aggressive]、[Safe]、[Very Safe]、および [7920-enabled]（音声のみ）です。計算において最小限の信号強度要件を必要とするには [Aggressive] を選択し、最大限の信号強度を要求するには [Very Safe] を選択します。

ステップ 10　[Calculate] をクリックします。

選択されたサービスに対して推奨されるアクセス ポイントの数が表示されます。

（注）　推奨される計算では、[Advanced Options] の [Safety Margin] で下方に調整されていない限り、常に強力な信号が必要であると見なされます。場合によっては、必要なアクセス ポイントが推奨される数より少ないこともあります。

（注）　プランニング モードの計算では、壁は使用または考慮されません。

ステップ 11　[Apply] をクリックして、選択されたサービスおよびパラメータに基づいて、選択された領域において推奨されるアクセス ポイントの配置案を示すマップを生成します。

ステップ 12　[Generate Proposal] を選択して、指定された入力に基づいて推奨されるアクセス ポイントの数および配置のレポートを、テキストおよびグラフィックで表示します。

リフレッシュ オプション

無線 LAN をモニタする準備をするには、マップに対するさまざまなリフレッシュ オプションを十分に理解してください。

- [Load] : 左側のサイド バーのメニューの [Load] オプションは、Prime Infrastructure データベースからマップ データをオンデマンドでリフレッシュします。
- [Auto Refresh] : [Auto Refresh] オプションでは、データベースからマップ データをリフレッシュする頻度を設定するための間隔を選べるドロップダウン リストを提供しています。
- [Refresh from network] : [Auto Refresh] ドロップダウン リストの右側の [Refresh from network] アイコンをクリックすることで、作成後 5 ～ 15 分経過している Prime Infrastructure データベースからポーリングされるデータではなく、SNMP フェッチを介してコントローラから直接マップ ステータスと統計をリフレッシュできます。

（注）　フロア計画にモニタ モード アクセス ポイントがある場合、IDS ヒートマップ タイプまたはカバレッジ ヒートマップ タイプのいずれかを選択できます。カバレッジ ヒートマップでは、モニタ モード アクセス ポイントが除外され、IDS ヒートマップでは含められます。

- [Refresh browser]：マップの上の [Logout and Print] オプションの横にあります。もう 1 つのリフレッシュ オプションです。これをクリックするとページ全体がリフレッシュされます。マップ ページ上でクリックした場合、マップとそのステータスおよび統計がリフレッシュされます。

ネットワーク設計の作成

アクセス ポイントを設置してコントローラに接続し、そのコントローラを管理するように Prime Infrastructure を設定したら、ネットワーク設計を設定します。*ネットワーク設計*は、施設全体にわたるアクセス ポイントの物理配置を Prime Infrastructure 内で表現したものです。1 つのキャンパス、そのキャンパスを構成するビルディング、および各ビルディングのフロアという階層構造が、1 つのネットワーク設計を構成します。これらの手順は、その環境のデバイスを追跡するために、Location Appliance がそのネットワーク内のコントローラをポーリングするように設定され、特定のネットワーク設計と同期するように設定されていると仮定します。Prime Infrastructure とモビリティ サービス エンジン間の同期を実行する概念と手順については、『*Cisco 3350 Mobility Services Engine Configuration Guide*』を参照してください。

ネットワークの設計

ネットワークを設計するには、次の手順を実行します。

ステップ 1　Prime Infrastructure Web インターフェイスを開いてログインします。

（注）　ネットワーク設計を作成または編集するには、Prime Infrastructure にログインし、SuperUser、Admin、または ConfigManager アクセス権限を持つ必要があります。

ステップ 2　[Monitor] > [Site Maps] を選択します。

ステップ 3　ネットワーク設計のサイズおよびマップの構成に応じて、右側のドロップダウン リストから、[New Campus] または [New Building] を選択します。[New Campus] を選択する場合は、ステップ 4 に進みます。キャンパスなしでビルディングを作成するには、ステップ 14 に進みます。

ステップ 4　[Go] をクリックします。

ステップ 5　キャンパスのネットワーク設計の名前、問い合わせ先の名前、およびキャンパスのイメージ ファイルへのファイル パスを入力します。.bmp と .jpg をインポート可能です。

（注）　[Browse...] ボタンを使用して、位置を指定できます。

ステップ 6　[Next] をクリックします。

ステップ 7　[Maintain Aspect Ratio] チェックボックスをオンにします。このチェックボックスをオンにすると、キャンパスの水平方向スパンが約 5,000 フィートになり、イメージ ファイルの縦横比に従って垂直方向スパンが調整されます。水平方向または垂直方向のスパンを調整すると、画像の比率に従ってほかのフィールドが変更されます。

この自動調整を優先したい場合は、[Maintain Aspect Ratio] チェックボックスをオフにする必要があります。その後で、両方のスパンを実際のキャンパスの寸法に合うように調整できます。

ステップ 8　[OK] をクリックします。

ステップ 9　[Monitor] > [Site Maps] ページで、前の手順で作成したキャンパス マップに関連付けられたハイパーリンクをクリックします。新しいキャンパス イメージを示すページが表示されます。

ステップ 10　ページの右上の [Select a command] メニューから、[New Building] を選択し、[Go] をクリックします。

ステップ 11　ビルディング名、連絡先担当者、ビルディングの地上のフロア数と地下のフロア数、および寸法を入力します。[OK] をクリックします。

ステップ 12　キャンパス イメージの左上の青い四角形をクリックし、それを目的の位置にドラッグして、キャンパス マップのどのビルディングが適切なビルディングかを示します。青い四角形のサイズを変更するには、Ctrl キーを押した状態でクリックしてドラッグし、その水平サイズを調整します。また、ビルディングの寸法を [Horizontal Span] と [Vertical Span] フィールドに数値で入力して [Place] をクリックすることもできます。サイズ変更した後で、青い四角形をクリックして目的の位置にドラッグすることで、必要に応じて再配置できます。[Save] をクリックします。

ステップ 13　その後 Prime Infrastructure は、緑色の四角形の中で強調表示された、新たに作成されたビルディングを備えたキャンパス イメージに戻ります。**緑色の四角形**をクリックします。

ステップ 14　キャンパスなしでビルディングを作成するには、[New Building] を選択して [Go] をクリックします。

ステップ 15　ビルディングの名前、連絡先情報、地上のフロア数と地下のフロア数、および寸法情報を入力します。[Save] をクリックします。Prime Infrastructure が [Monitor] > [Site Maps] ページに戻ります。

ステップ 16　新しく作成されたビルディングに関連付けられたハイパーリンクをクリックします。

ステップ 17　[Monitor] > [Site Maps] > [*Campus Name*] > [*Building Name*] ページで、ドロップダウン リストから [New Floor Area] を選択します。[Go] をクリックします。

ステップ 18　アクセス ポイントを設置するフロア名、問い合わせ先、フロア番号、フロアの種類、高さを入力し、フロア画像のパスを入力します。[Next] をクリックします。

（注）　[Floor Type]（RF Model）フィールドは、その指定したフロアの環境の種類を指定します。この RF Model は、そのフロア上の予想される RF 信号の減衰量を示します。使用可能なモデルがフロアの構造を正しく表していない場合に、フロアの減衰特性に特有の RF モデルを作成する方法の詳細については、『*Cisco 3350 Mobility Services Engine Configuration Guide*』を参照してください。

ステップ 19　フロア領域がビルディングの面積と異なる場合は、[Dimensions] 見出しの下のテキスト フィールドの数値を変更するか、Ctrl キーを押した状態でクリックしてフロア画像の周りの青い四角形をドラッグし、フロアの面積を調整します。フロアの位置がビルディングの左上隅からオフセットしている場合は、青い四角形をクリックして目的の位置にドラッグするか、[Coordinates of top left corner] 見出しの下の数値を変更して、ビルディング内のフロアの配置を変更します。いずれかの数値を変更した後は、[Place] をクリックします。

ステップ 20　[Launch Map Editor] の横のチェックボックスを選択して、Prime Infrastructure の Map Editor でフロアの特性を調整します。Map Editor の機能については、「Map Editor の使用」（P.6-206）を参照してください。

ステップ 21　新しいフロアのイメージ（[Monitor] > [Site Maps] > [*CampusName*] > [*BuildingName*] > [*FloorName*]）で、右上のドロップダウン リストから [Add Access Points] を選択します。[Go] をクリックします。

ステップ 22　コントローラに接続しているすべてのアクセス ポイントが表示されます。管理のために Prime Infrastructure は設定されているがまだ別のフロア マップに追加されていないコントローラでも表示されます。アクセス ポイント エントリの左側のチェックボックスをオンにして、特定のフロア マップ上に配置するアクセス ポイントを選択します。[Name] 列の左側のチェックボックスをオンにしてすべてのアクセス ポイントを選択します。[OK] をクリックします。

ステップ 23　フロア マップに追加するために選択した各アクセス ポイントは、灰色の円で表され（アクセス ポイント名や MAC アドレスにより区別）、フロア マップの左上部分に並べられます。各アクセス ポイントを適切な位置にドラッグします （アクセス ポイントは、クリックして再配置すると青色に変わる）。各アクセス ポイントの横の小さい黒矢印は各アクセス ポイントの Side A を表し、各アクセス ポイントの矢印は、アクセス ポイントが設置された方向と一致する必要があります。（Side A はそれぞれの 1000 シリーズ アクセス ポイント上で明確に記されており、802.11a/n 無線とは関連なし）。

ステップ 24　方向の矢印を調整するには、[Antenna Angle] ドロップダウン リストで適切な方向を選択します。各アクセス ポイントの配置と方向の調整が完了したら、[Save] をクリックします。

（注）　アクセス ポイントの配置と方向は、実際のアクセス ポイントの展開に直接反映する必要があります。反映しない場合は、システムはデバイス位置を特定できません。

ステップ 25　それぞれのデバイス位置がネットワーク設計で適切に詳しく表されるまで、これらの手順を繰り返してキャンパス、ビルディング、およびフロアを作成します。

WLSE マップ データのインポートまたはエクスポート

アクセス ポイントを Autonomous から CAPWAP に、および WLSE から Prime Infrastructure に変換する場合、変換手順の 1 つとして、アクセス ポイント情報を手動で Prime Infrastructure に再入力する方法があります。これは、時間のかかる手順となる場合があります。処理を高速化するために、WLSE からアクセス ポイントに関する情報をエクスポートして、Prime Infrastructure にインポートすることができます。

（注）　Prime Infrastructure は、.tar ファイルを想定しているため、ファイルをインポートする前に .tar 拡張子かどうかをチェックします。インポートしようとしているファイルが .tar ファイルでない場合は、Prime Infrastructure にエラー メッセージが表示され、別のファイルをインポートするためのプロンプトが表示されます。

Prime Infrastructure Web インターフェイスを使用して、プロパティをマップし、WLSE データを含む tar ファイルをインポートするには、次の手順を実行します。WLSE データ エクスポート機能（WLSE バージョン 2.15）の詳細については、次の URL を参照してください。
http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp

ステップ 1　[Monitor] > [Site Maps] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから [Properties] を選択し、[Go] をクリックします。

ステップ 3　[Export/Import AP/LS/SP Placement] で、[Browse] をクリックしてインポートするファイルを選択します。

ステップ 4　インポートする .tar ファイルを見つけて選択し、[Open] をクリックします。

Prime Infrastructure では、[Import From] フィールドにファイルの名前が表示されます。

ステップ 5　[Import] をクリックします。

Prime Infrastructure によってファイルがアップロードされ、ファイルが処理されている間は一時的にローカル ディレクトリに保存されます。ファイルに処理できないデータが含まれている場合、Prime Infrastructure は問題を修正して再試行するようユーザに促します。ファイルのロードが完了すると、Prime Infrastructure に追加された内容を示すレポートが Prime Infrastructure に表示されます。レポートには、追加できない内容とその理由も記載されます。

インポートするデータの一部がすでに存在している場合、Prime Infrastructure では、キャンパスの場合は既存のデータを使用し、ビルディングとフロアの場合はインポートされたデータで既存のデータを上書きします。

WLSE サイトとビルディングの組み合わせ、および Prime Infrastructure キャンパス（または最上位レベルのビルディング）とビルディングの組み合わせの間に重複する名前がある場合、Prime Infrastructure の実行前インポート レポートに、既存のビルディングを削除することを示すメッセージが表示されます。

ステップ 6　[Import] をクリックして、WLSE データをインポートします。

Prime Infrastructure にインポートされた内容を示すレポートが表示されます。

（注） WLSE ファイルにはフロア番号情報がないため、WLSE が Prime Infrastructure にインポートされた後のフロア インデックス計算の構造は降順になります。フロア イメージをクリックすると、適切なフロア ページに直接移動できます。

ステップ 7　インポートされたデータを確認するには、[Monitor] > [Site Maps] を選択します。

デバイス詳細のモニタリング

アクセス ポイント詳細

アクセス ポイントの詳細を表示するには、マウス カーソルをアクセス ポイント アイコンの上に移動します。適切なタブをクリックして、アクセス ポイントと無線情報を表示します。

（注） モニタ モードのアクセス ポイントは、他のアクセス ポイントと区別するために灰色のラベルで表示されます。

[AP Info] タブには、次のアクセス ポイントの情報が含まれます。

- MAC アドレス
- アクセス ポイントのモデル
- コントローラ
- ロケーション
- アクセス ポイントの高さ
- アクセス ポイントの稼働時間
- LWAPP の稼働時間

（注）　[AP Info] タブの [Run Ping Test] リンクをクリックして、ping テストを実行できます。

[802.11] タブには、次の無線情報が含まれます。

- チャネル番号
- 拡張チャネル
- チャネル幅
- 送信電力レベル
- クライアント数

（注）　アクセス ポイントにアソシエートされているクライアントの数は、クライアントの総数と一致しない場合があります。

- 送受信の使用率
- チャネル使用率

（注）　合計使用率 = (受信 + 送信 + チャネル使用率) を 100 % までの割合で表したもの。

- アンテナの名前および角度
- 垂直方向の角度

（注）　いずれかの [802.11] タブの該当するリンク（[View Rx Neighbors] または [View Radio Details]）をクリックして、このアクセス ポイントの受信ネイバーと無線の詳細を表示できます。

- 802.11n が有効かどうか
- [CleanAir Status] : アクセス ポイントの CleanAir ステータスと、アクセス ポイントで CleanAir が有効かどうかを表示します。
- [Average Air Quality] : このアクセス ポイントの平均電波品質を表示します。
- [Minimum Air Quality] : このアクセス ポイントの最小電波品質を表示します。

クライアント詳細

クライアントの詳細を表示するには、マウス カーソルをクライアント アイコンの上に移動します。

クライアント詳細情報には、次の項目が含まれます。

- ユーザ名
- IP アドレス
- アセットの名前、グループ、およびカテゴリ
- ステータス
- 認証
- SSID

- アクセス ポイント名
- プロトコル
- ポート番号
- 最後に検索された日時

タグ詳細

タグの詳細を表示するには、マウス カーソルをタグ アイコンの上に移動します。

タグ詳細には、次の項目が含まれます。

- アセットの名前、グループ、およびカテゴリ
- タイプ
- バッテリ寿命
- 最後に検索された日時

不正アクセス ポイントの詳細

不正アクセス ポイントの詳細を表示するには、マウス カーソルをアクセス ポイント アイコンの上に移動します。

不正アクセス ポイントの詳細には、次の情報が含まれます。

- 分類タイプ：[Friendly]、[Malicious]、または [Unknown]。
- 状態
- 検出したアクセス ポイント
- タイプ
- 不正クライアント
- 最初に発見された日時
- 最後に発見された日時
- ネットワーク上にあるかどうか
- 最後に検索された日時

不正アドホックの詳細

不正アドホックの詳細を表示するには、マウス カーソルをアクセス ポイント アイコンの上に移動します。

不正クライアントの詳細

不正クライアントの詳細を表示するには、マウス カーソルをアクセス ポイント アイコンの上に移動します。

干渉の詳細

干渉の詳細を表示するには、マウス カーソルを干渉アイコンの上に移動します。干渉の詳細には、次の項目が含まれます。

- [Interferer Name]：干渉デバイスの名前。
- [Affected Channels]：干渉デバイスが影響を与えているチャネル。
- [Detected Time]：干渉源が検出された時刻。
- [Severity]：干渉デバイスの重大度インデックス。
- [Duty Cycle]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- [RSSI (dBm)]：干渉しているデバイスの受信信号強度。

不正クライアントの詳細には、次の項目が含まれます。

- 状態
- アソシエートされている不正アクセス ポイント
- 検出したアクセス ポイント
- 最初に発見された日時
- 最後に発見された日時
- 最後に検索された日時

フロア ビュー ナビゲーション

[Floor View] メイン ナビゲーション ペインでは、複数のマップ機能にアクセスできます。

このナビゲーション ペインには、次の機能が含まれます。

- [Zoom In/Zoom Out]：プラス記号（+）の付いた虫眼鏡アイコンをクリックすると、マップ ビューが拡大します。マイナス記号（-）の付いた虫眼鏡アイコンをクリックすると、マップ ビューのサイズが縮小します。
- [Map Size]：「次世代マップを使用したパンおよびズーム」（P.6-176）を参照してください。
- [Show Grid]：クリックすると、マップ上の距離をフィート単位で表示するグリッドが表示されたり、非表示になったりします。
- [RSSI Legend]：マウス カーソルを RSSI 凡例アイコンの上に移動すると、RSSI の色彩設計（赤色/-35 dBm から紺青色/-90 dBm までの範囲）が表示されます。
- [Add Access Points]：クリックすると、[Add Access Points] ページが開きます。詳細については、「アクセス ポイントのフロア領域への追加」（P.6-178）を参照してください。
- [Remove Access Points]：クリックすると、[Remove Access Points] ページが開きます。削除するアクセス ポイントを選択し、[OK] をクリックします。
- [Position Access Points]：クリックすると、[Position Access Points] ページが開きます。
- [Add Chokepoints]：クリックすると、[Add Chokepoints] ページが開きます。詳細については、『*Cisco Context-Aware Services Configuration Guide*』を参照してください。
- [Add WiFi TDOA Receivers]：クリックすると、[Add Wi-Fi TDOA Receivers] ページが開きます。詳細については、『*Cisco Context-Aware Services Configuration Guide*』を参照してください。
- [Auto Refresh]：ドロップダウン リストから、システム リフレッシュ間の時間の長さを選択します。

- [Refresh from Network]：クリックすると、現在のデータの即時リフレッシュを開始します。
- [Planning Mode]：クリックすると、[Planning Mode] ウィンドウが開きます。詳細については、「プランニング モードの使用」（P.6-221）を参照してください。
- [Map Editor]：クリックすると、[Map Editor] ウィンドウが開きます。

[Full Screen]：クリックすると、マップのサイズが全画面に拡大します。このときに、[Exit Full Screen] をクリックすると標準のビューに戻ります。

RF ヒートマップの計算について

無線周波ヒート マップは、RF 信号の強度をグラフィカルに表示したものです。WLAN は非常に動的で非決定性を備えているため、管理者は特定の瞬間のカバレッジを確実に把握することは困難です。この課題への対処をサポートするため、Prime Infrastructure では、フロアの Wi-Fi カバレッジに関して、視覚的な指示を含むフロア図面のマップを提供しています。これらのマップは、海洋学や地理科学でさまざまなレベルの温度を示す際に使用される色付きマップと似ていることから、ヒートマップと呼ばれます。色はさまざまなレベルの信号強度を示すために使用されます。「ヒートマップ」のさまざまな色合いは、異なる信号強度を反映しています。

この色による視覚的な表示は非常に便利です。ひと目で、現在のカバレッジの状態、信号強度、および WLAN のすき間や「穴」がわかります。カバレッジの状態を歩き回って測定する必要はありません。フロア図面とヒート マップは非常に直感的であるため、このシステムを使用することで、所属する組織へのサポートと特定の問題のトラブルシューティングにかかる時間と手間が大幅に削減されます。

RF ヒートマップの計算は内部グリッドに基づいています。グリッド内の障害物の正確な場所に応じて、障害物から数フィートまたは数メートルの範囲において、RF ヒートマップが障害物による減衰を考慮できるかどうかが異なります。

詳細には、交差する障害物に部分的に影響を受けているグリッドの正方形が障害物の減衰を反映できるかどうかは、アクセス ポイント、障害物、およびグリッドの配置によって異なります。

たとえば、グリッドの正方形に交差する壁があるとします。グリッドの正方形の中心点は AP から見ると壁の背後にあります。このため、グリッドの正方形では、実際には壁の前にある左上隅も含めて（残念ながら）、全体に減衰を示す色が設定されます。

グリッドの正方形の中心点は壁に対して AP と同じ側にあります。このため、グリッドの正方形では、実際には AP から見て壁の背後にある右下隅も含めて（残念ながら）、全体に減衰を示す色は設定されません。

ダイナミック ヒートマップ計算

RF ヒートマップの計算は、静的または動的に実行できます。デフォルトでは、動的に計算されます。静的に設定するには、[Map Properties] ページでダイナミック ヒートマップ オプションを無効にします。Prime Infrastructure サーバはすべての AP に対するすべての AP の RSSI 強度の最新の一覧を保持しています。近隣 AP の RSSI 強度は、すべての AP の RF ヒートマップを修正するために使用されます。ダイナミック ヒートマップ機能の主な目的は、障害物による RF ヒートマップの再計算を行うことです。

Google Earth マップのモニタリング

[Monitor] > [Google Earth Maps] では、屋外位置の作成、ファイルのインポート、Google Earth マップの表示、Google Earth パラメータの設定を行えます。

ここでは、次の内容について説明します。

Google Earth を使用した屋外位置の作成

アクセス ポイントを屋外位置に基づいてグループ化するには、各アクセス ポイントの緯度/経度座標を使用します。これらの座標を指定するには次の 2 つの方法があります。

- KML（Google Keyhole Markup Language）ファイルをインポートする
- CSV ファイル（各値がカンマで区切られたスプレッドシート形式のファイル）をインポートする

ここでは、次の内容について説明します。

Google Earth の地理座標について

各アクセス ポイントについて、次の地理情報が必要です。

（注）　標準マップに AP を関連付けることなく、その AP を Google Earth マップに追加しても、Google Earth 内の AP を表示したときにヒートマップは表示されません。

- [Longitude]（東経または西経）：グリニッジ子午線を基準とする角距離（度数）。子午線より西側の値の範囲は -180 ～ 0 度。子午線より東側の値の範囲は 0 ～ 180 度。デフォルト値は 0 です。

  度、分、秒、方位による座標表記
  - 度（–180 ～ 180）
  - 分（0 ～ 59）
  - 秒（00.00 ～ 59.99）
  - 方位：東（E）または西（W）

  10 進法表記（「度分秒」表記から変換）
  - 経度の範囲は -179.59.59.99 W ～ 179.59.59.99 E
- [Latitude]（北緯または南緯）：赤道を基準とする角距離（度数）。赤道より南側の値の範囲は -90 ～ 0 度。赤道より北側の値の範囲は 0 ～ 90 度。デフォルト値は 0 です。

  度、分、秒、方位による座標表記
  - 度（–90 ～ 90）
  - 分（0 ～ 59）
  - 秒（00.00 ～ 59.99）
  - 方位：北（N）または南（S）

10 進法表記（「度分秒」表記から変換）

  - 緯度の範囲は -89.59.59.99 S ～ 89.59.59.99 N

- [Altitude]：地表からアクセス ポイントまでの高さまたは距離（メートル）。指定しない場合は、デフォルト値の 0 が適用されます。値の範囲は 0 ～ 99,999 です。
- [Tilt]：0 ～ 90 度（負の値は指定できません）。<tilt> 値が 0 度の場合は、アクセス ポイントを真上から眺めることができます。<tilt> 値が 90 度の場合は、水平線に沿った眺めになります。値の範囲は 0 ～ 90 です。デフォルトの方位角は 0 です。
- [Range]：[Longitude] と [Latitude] で指定した地点から、アクセス ポイントを眺める視点までの距離をメートルで指定します（海面からのカメラ高度）。値の範囲は 0 ～ 99,9999 です。
- [Heading]：コンパス方位を度数で指定します。デフォルトは 0（北）です。値の範囲は 0 ～ ± 180 度です。
- [Altitude Mode]：<LookAt> で指定した <altitude> の解釈方法を指定します。
  - [Clamped to ground]：<altitude> の指定を無視し、地表面に <LookAt> 位置（視点）を配置します。これはデフォルトです。
  - [Relative to ground]：<altitude> を、地表面から測定した高度値（メートル）と見なします。
  - [Absolute]：<altitude> を、海面からの高度値（メートル）と見なします。
- [Extend to ground]：アクセス ポイントをマストにアタッチするかどうかを指定します。

Google Earth での座標の作成およびインポート（KML ファイル）

地理座標を Google Earth で作成してインポートすることができます。その場合、フォルダを作成する方法と、目印を個別に作成する方法があります。フォルダを作成する方法の利点は、すべての目印を 1 つのフォルダにまとめ、そのフォルダ自体を KML（XML）ファイルとして保存できることです。目印を作成する場合は、それらを個別に保存する必要があります。

Google Earth でフォルダを作成する手順は、次のとおりです。

ステップ 1　Google Earth を起動します。

ステップ 2　左側のサイドバー メニューの [Places] ページで、[My Places] または [Temporary Places] を選択します。

ステップ 3　[Temporary Places] を右クリックして、ドロップダウン リストから [Add] > [Folder] を選択します。

（注）　KML ファイルを使用すると、フォルダをその深さに制限なく階層的に作成できます。たとえば、国、都市、州、郵便番号別に構成されたフォルダと目印を作成できます。
これは CSV には該当しません。CSV で作成できる階層は 1 レベルだけです。

ステップ 4　次の情報を入力します（任意）。

- [Name]：フォルダ名
- [Description]：フォルダの説明
- [View]：緯度、経度、範囲、機首方位、傾斜を指定します。

（注）　[View] で座標（緯度、経度、範囲、機首方位、傾斜）を指定した場合、Google Earth の最初の読み込み時に正しい場所へ「飛行」または移動するときに、これらの情報が使用されます。
座標を指定しない場合は、このグループまたはフォルダに属するすべてのアクセス ポイントの最小緯度、最小経度、最大緯度、および最大経度に基づいて位置情報が取得されます。

ステップ 5　[OK] をクリックして、フォルダを保存します。フォルダを作成した後は、そのフォルダを [Places] ページで選択して目印を作成できます。

目印を作成する手順は、次のとおりです。

ステップ 1　Google Earth を起動します。

ステップ 2　左側のサイドバーの [Places] ページで、[My Places] または [Temporary Places] を選択します。

ステップ 3　前に作成したフォルダを選択します。

ステップ 4　作成したフォルダを右クリックして、ドロップダウン リストから [Add] > [Placemark] を選択します。

ステップ 5　必要に応じて、次のパラメータを設定します。

- [Name]：目印名には、該当するアクセス ポイントの名前、MAC アドレス、または IP アドレスが含まれている必要があります。

（注）　MAC アドレスは、イーサネット MAC ではなくベース無線 MAC を指しています。

- [Latitude]：目印をフォルダ内に作成した場合は、そのフォルダの現在の座標。それ以外の場合は目印の座標。このフィールドは、マップ上に配置した黄色い目印アイコンの位置に基づいて自動的に設定されます。マウスを使用して、目印を正しい場所まで移動します。または、[Latitude] テキスト ボックスに正しい座標を入力します。
- [Longitude]：目印をフォルダ内に作成した場合は、そのフォルダの現在の座標。それ以外の場合は目印の座標。このフィールドは、マップ上に配置した黄色い目印アイコンの位置に基づいて自動的に設定されます。マウスを使用して、目印を正しい場所まで移動します。または、[Longitude] テキスト ボックスに正しい座標を入力します。
- [Description]（任意）：Prime Infrastructure ではこのフィールドは無視されます。
- [Style, Color]（任意）：Prime Infrastructure ではこのフィールドは無視されます。
- [View]：経度、緯度、範囲、機首方位、傾斜を設定できます。これらの地理座標の詳細については、「Google Earth の地理座標について」（P.6-236）を参照してください。
  - 緯度と経度は、マップ上の黄色い目印アイコンの位置に応じて自動的に設定されます。目印をクリックして、正しい位置までドラッグします。
  - これらの座標はすべて手動で入力できます。
- [Altitude]：テキスト ボックスに標高（単位はメートル）を入力します。または、[Ground to Space] スライド バーを使用して標高を指定します。
  - [Clamped to ground]：「視点」位置を地上に配置します。これはデフォルトです。
  - [Relative to ground]：<altitude> を、地表面から測定した高度値（メートル）と見なします。
  - [Absolute]：<altitude> を、海面からの高度値（メートル）と見なします。

– [Extend to ground] : [Relative to ground] または [Absolute] を選択した場合、アクセス ポイントをマストにアタッチするかどうかを指定します。

ステップ 6　すべての座標を入力したら、[Snapshot current view] をクリックします。または、[Reset] をクリックして元の座標設定に戻します。

（注）　Google Earth の詳細については、Google Earth のオンライン ヘルプを参照してください。

ステップ 7　[OK] をクリックします。

ステップ 8　追加するすべての目印について、上記の手順を繰り返します。

ステップ 9　すべての目印を作成したら、そのフォルダを .kmz ファイル（KML Zip ファイル）または .kml ファイルとして保存します

（注）　.kmz ファイルに追加できる .kml ファイルは 1 つだけです。

（注）　フォルダを保存するには、目的のフォルダを右クリックして、ドロップダウン リストから [Save as] を選択します。次に、適切な保存先を指定して [Save] をクリックします。.kmz ファイルと .kml ファイルの両方を Prime Infrastructure にインポートできます。

CSV ファイルとしての座標の作成とインポート

Prime Infrastructure へインポートする CSV ファイルを作成するには、次の手順を実行します。

ステップ 1　フラット ファイルを開き、必要な情報をカンマ区切りリストとして指定します。表 6-17 に、設定可能なデータ、任意または必須の区別、およびデータのパラメータを示します。

（注）　表 6-17 に示す地理座標の詳細については、「Google Earth の地理座標について」（P.6-236）を参照してください。

表 6-17　CSV ファイルのフィールド

"FolderName"	"Value Optional"	最大長：32
"FolderState"	"Value Optional"	設定可能な値：true/false
"FolderLongitude"	"Value Optional"	範囲：0 ～ ± 180
"FolderLatitude"	"Value Optional"	範囲：0 ～ ± 90
"FolderAltitude"	"Value Optional"	範囲：0 ～ 99999
"FolderRange"	"Value Optional"	範囲：0 ～ 99999
"FolderTilt"	"Value Optional"	範囲：0 ～ 90
"FolderHeading"	"Value Optional"	範囲：0 ～ ± 180
"FolderGeoAddress"	"Value Optional"	最大長：128

表 6-17　CSV ファイルのフィールド （続き）

"FolderGeoCity"	"Value Optional"	最大長：64
"FolderGeoState"	"Value Optional"	最大長：40
"FolderGeoZip"	"Value Optional"	最大長：12
"FolderGeoCountry"	"Value Optional"	最大長：64
"AP_Name"	"Value Required"	最大長：32
"AP_Longitude"	"Value Required"	範囲：0 ～ ±180
"AP_Latitude"	"Value Required"	範囲：0 ～ ±90

ステップ 2　.csv ファイルを保存します。これで、このファイルを Prime Infrastructure へインポートできるようになりました。

Prime Infrastructure へのファイルのインポート

Google KML または CSV を Prime Infrastructure の Google Earth マップ機能へインポートするには、次の手順を実行します。

ステップ 1　Prime Infrastructure にログインします。

ステップ 2　[Monitor] > [Google Earth Maps] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Import Google KML] または [Import CSV] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[Browse] ボタンをクリックして、コンピュータ上に保存されている .kml ファイル、.kmz ファイル、または .csv ファイルを選択します。

ステップ 6　目的のファイルの名前とパスがテキスト ボックスに表示されたら、[Next] をクリックします。

選択したファイルが解析され、次の処理が行われます。

- アップロードしたファイルで指定されているアクセス ポイントの有効性（指定されたアクセス ポイントが Prime Infrastructure 内で使用できること）が検証されます。
- 傾斜、機首方位、範囲、および他の地理座標フィールドに対して、範囲の検証が実行されます。経度および緯度が指定されると、範囲の検証が実行されます。指定されていない場合、値はデフォルトで 0 になります。

（注）　KML では、経度と緯度の範囲は 10 進法でのみ入力できます。CSV では、さまざまな形式がサポートされています（[Google Maps] > [Import CSV] にある CSV の例を参照）。

（注）　入力ファイルの有効性に問題がある場合は、エラー ページが表示されます。すべてのエラーを修正しない限り、アップロードした情報を保存できません。

ステップ 7　有効性チェックが正常に終了したら、ファイルの詳細を確認して [Save] をクリックします。

以前に同じ情報をアップロードして、保存している場合は、その情報が次のように上書きされます。

- 以前にフォルダをアップロードした場合は、そのフォルダの座標が更新されます。
- 以前にアクセス ポイントをアップロードした場合は、そのアクセス ポイントの座標が更新されます。
- フォルダ内の既存のアクセス ポイントは削除されません。
- 必要に応じて、新しいフォルダが作成され、配置されます。

Google Earth マップの表示

Google Earth マップを表示する手順は、次のとおりです。

ステップ 1　Prime Infrastructure にログインします。

ステップ 2　[Monitor] > [Google Earth Maps] の順に選択します。[Google Earth Maps] ページが開き、すべてのフォルダと、各フォルダに含まれるアクセス ポイントの数が表示されます。

ステップ 3　表示するマップの [Launch] をクリックします。Google Earth が起動して新しいページが開き、ロケーションとそのアクセス ポイントが表示されます。

（注）　この機能を使用するには、コンピュータに Google Earth をインストールし、サーバからデータを受け取った時点で自動的に起動するように設定しておく必要があります。Google Earth は、Google ウェブサイト（http://www.google.com/earth/index.html）からダウンロードできます。

Google Earth マップの詳細の表示

Google Earth Map フォルダの詳細を表示する手順は、以下のとおりです。

ステップ 1　[Google Earth Map] ページで、目的のフォルダの名前をクリックします。そのフォルダの詳細ページが開きます。[Google Earth Details] ウィンドウでは、アクセス ポイント名と、MAC アドレスまたは IP アドレスを確認できます。

（注）　アクセス ポイントを削除するには、該当するチェックボックスをオンにして [Delete] をクリックします。
フォルダ全体を削除するには、[<Folder Name>] の隣のチェックボックスをオンにして [Delete] をクリックします。フォルダを削除すると、そのフォルダ内のすべてのサブフォルダとアクセス ポイントが削除されます。

ステップ 2　[Cancel] をクリックして、詳細ページを閉じます。

[Access Point] ページへの [Google Earth Location] 起動ポイントの追加

[Google Earth Location] 起動ポイントを [Access Point] 概要および詳細ページに追加することで、Prime Infrastructure 内の [Google Earth Location] 起動ポイントの数を増やすことができます。

[Google Earth Location] 起動ポイントを [Access Point] 概要および詳細ページに追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Access Points] の順に選択します。

ステップ 2　[Access Point] 概要ページで、ページ見出しの隣の [Edit View] リンクをクリックします。

ステップ 3　[Edit View] ページで、左側の列の [Google Earth Location] を強調表示します。[Show] をクリックします。

[Google Earth Location] 列見出しは [View Information] 列内に移動します。

（注）　[View Information] の上から下へのリストは、[Access Point] 概要ページで表示される列の左から右への順序を反映しています。

ステップ 4　列の表示順序を変更するには、[Google Earth Location] エントリを強調表示し、必要に応じて [Up] および [Down] ボタンをクリックします。[Submit] をクリックします。

[Access Points] 概要ページに戻り、Google Earth 起動リンクが画面に表示されます。

（注）　起動リンクは、[Access Points] 詳細ページの一般概要ページにも表示されます（[Monitor] > [Access Points] > [*AP Name*]）。

Google Earth の設定

アクセス ポイント関連の設定は、[Google Earth Settings] ページから定義できます。Google Earth Maps 機能に対してアクセス ポイントを設定する手順は、以下のとおりです。

ステップ 1　[Monitor] > [Google Earth Maps] の順に選択します。

ステップ 2　次のパラメータを設定します。

- [Refresh Settings] : オンデマンド更新を有効にするには、[Refresh from Network] チェックボックスをオンにします。このオプションは一度だけ適用されて、無効になります。

注意　この更新がネットワークから直接実行された場合、アクセス ポイントの数によっては、データ収集に長い時間かかることがあります。

- [Layers] : アクセス ポイント、アクセス ポイント ヒート マップ、およびアクセス ポイント メッシュ情報のレイヤ フィルタを選択して保存できます。チェックボックスをオンにして適切なレイヤをアクティブにし、[>] をクリックしてフィルタ ページを開きます。

（注）　Google Earth が次の更新要求を送信する時点で、これらの設定が適用されます。

- [Access Points] : [AP Filter] ドロップダウン リストから、表示する情報（チャネル、Tx 電力レベル、カバレッジ ホール、MAC アドレス、名前、コントローラ IP、使用率、プロファイル、またはクライアント）を選択します。

  （注）　アクセス ポイント レイヤがオンになっていない場合は、データが返されず、エラー メッセージ（アイコンのない目印）が Google Earth に返されます。

- [AP Heatmap] : [Protocol] ドロップダウン リストから、[802.11a/n]、[802.11b/g/n]、[802.11a/n & 802.11b/g/n]、または [None] を選択します。[RSSI Cutoff] ドロップダウン リストからカットオフを選択します（-60 ～ -90 dBm）。

  （注）　802.11a/n プロトコルと 802.11b/g/n プロトコルを 2 つとも選択した場合は、これら両方のヒート マップが生成され、互いに重なり合って配置されます。重なり順序は指定できません。この重なりを防ぐには、Google Earth でオーバーレイを個別にオフにするか、Prime Infrastructure の [Google Earth Settings] でオーバーレイを変更する必要があります。

- [AP Mesh Info] : [Link Label] ドロップダウン リストから、[Link SNR]、[Packet Error Rate]、または [none] を選択します。[Link Color] ドロップダウン リストから、[Link SNR] または [Packet Error Rate] を選択します。

  （注）　[AP Mesh Info] チェックボックスがオンの場合、[Mesh Links] も自動的に表示されます。

ステップ 3　[Save Settings] をクリックして、変更内容を保存します。変更を保存せずにページを閉じる場合は、[Cancel] をクリックします。

ユーザ アカウントの管理

Cisco Prime Infrastructure 管理によって、タスクのスケジューリング、アカウントの管理、ローカルおよび外部の認証や許可の設定が行えます。また、ロギング オプションの設定、メール サーバの設定、およびデータ保持期間の設定に関連するデータの管理も実行できます。Prime Infrastructure ライセンスの種類やライセンスのインストール方法についての情報を利用できます。

組織では、単一の管理プラットフォームを使用したワイヤレス ネットワーク セグメントの管理や制御を行える、簡単でコスト効率の優れた方法が必要となります。各管理者が管理や制御を行う無線 LAN を限定できるようなソリューションが必要です。

この章では、Prime Infrastructure を使って実行する管理タスクについて説明します。ここで説明する内容は、次のとおりです。

Prime Infrastructure ユーザ アカウントの管理

この項では、グローバル電子メール パラメータの設定方法と Prime Infrastructure ユーザ アカウントの管理方法について説明します。次の項目について説明します。

Prime Infrastructure ユーザ アカウントの設定

この項では、Prime Infrastructure ユーザを設定する方法を説明します。AAA フレームワークのアカウンティング部分は、この時点では実装しません。完全なアクセス以外に、特定のユーザ グループに対して異なる権限の管理アクセスを付与できます。Prime Infrastructure はこれらのアクセス制限を使用して外部ユーザの認証をサポートし、TACACS+ サーバおよび RADIUS サーバに対してユーザを認証します。

インストール時に入力したユーザ名とパスワードは、常に認証されますが、ここで取る手順では追加のスーパーユーザが作成されます。パスワードを消失したり忘れたりした場合には、ユーティリティを実行して別のユーザ定義パスワードにリセットする必要があります。

Prime Infrastructure に新しいユーザ アカウントを設定するには、次の手順を実行します。

ステップ 1　「Prime Infrastructure サーバの起動」（P.2-20）の手順に従って、Prime Infrastructure サーバを起動します。

ステップ 2　Prime Infrastructure ユーザ インターフェイスに *root* としてログインします。

（注）　新しいスーパーユーザを作成して SuperUsers グループに割り当てることを推奨します。

ステップ 3　[Administration] > [AAA] の順に選択します。[Change Password] ページが表示されます。

ステップ 4　[Old Password] テキストボックスに、変更する現在のパスワードを入力します。

ステップ 5　新しい Prime Infrastructure ユーザ アカウントのユーザ名とパスワードを入力します。パスワードは 2 回入力する必要があります。

（注）　これらの項目では、大文字と小文字が区別されます。

ステップ 6　左側のサイドバーのメニューから、[User Groups] を選択します。[All Groups] ページに次のグループ名が表示されます。

（注）　一部のユーザグループは、別のユーザグループと組み合わせることができません。たとえば、[Lobby Ambassador] と [Monitor Lite] の両方を選択できません。

- [System Monitoring]：Prime Infrastructure の動作をモニタできます。
- [ConfigManagers]：Prime Infrastructure の動作をモニタおよび設定できます。
- [Admin]：Prime Infrastructure の動作をモニタおよび設定し、すべてのシステム管理タスクを実行できます。

  （注）　admin アカウントを選択してコントローラにログインする場合は、[Local Net Admin] の下のゲスト ユーザを確認することもできます。

- [SuperUsers]：Prime Infrastructure の動作をモニタおよび設定し、Prime Infrastructure のユーザ アカウントとパスワードの管理を含むすべてのシステム管理タスクを実行できます。スーパーユーザのタスクは、変更できます。
- [Users Assistant]：ローカル ネット ユーザの管理だけを実行できます。ユーザ アシスタントではコントローラを設定またはモニタできません。[Configure] > [Controller] ページの順に選択して、これらのローカル ネット機能を設定する必要があります。

（注）　作成した User Assistant ユーザとしてログインし、[Monitor] > [Controller] と選択すると、「permission denied」メッセージが表示されます。これは正常な動作です。

- [Lobby Ambassador]：ゲスト ユーザのユーザ アカウントの設定と管理のためだけのアクセスが許可されます。
- [Monitor lite]：アセットの位置をモニタできます。
- [Root]：Prime Infrastructure の動作をモニタおよび設定し、パスワードの変更などのすべてのシステム管理タスクを実行できます。このグループに割り当てることができるユーザは 1 つだけで、インストールの際に決定されます。このユーザをシステムから削除でません。また、このユーザに対してタスクを変更できません。

ステップ 7　新しいユーザ アカウントを割り当てたユーザ グループの名前をクリックします。[Group Detail] > [User Group] ページに、そのグループに許可された操作のリストが表示されます。

このページから、ログインおよびログアウト パターンの監査証跡の表示や、タスク リストのエクスポートが行えます。

ステップ 8　タスクの許可やメンバーのチェックボックスを適宜選択または選択解除して、必要な変更を行います。

（注）　加える変更は、このユーザ グループのすべてのメンバーに影響します。

（注）　[Monitor] > [Client details] ページの詳細をすべて表示し、無線測定などの操作を実行するには、User Defined グループのユーザに Monitor Clients、View Alerts & Events、Configure Controllers、Client Location の権限が必要です。

ステップ 9　[Submit] をクリックして変更内容を保存するか、または [Cancel] をクリックして設定変更を取り消します。

Prime Infrastructure ユーザ アカウントの削除

Prime Infrastructure ユーザ アカウントを削除するには、次の手順に従ってください。

ステップ 1　「Prime Infrastructure サーバの起動」（P.2-20）の手順に従って、Prime Infrastructure サーバを起動します。

ステップ 2　SuperUsers グループに割り当てられたユーザとして Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 3　[Administration] > [AAA] の順に選択します。

ステップ 4　左のサイドバー メニューで、[Users] を選択し [Users] を表示します。

ステップ 5　削除するユーザ アカウントの左側のチェックボックスをオンにします。

ステップ 6　[Select a command] ドロップダウン リストから、[Delete User(s)] を選択し、[Go] をクリックします。

プロンプトが表示されたら、[OK] をクリックして選択を確定します。ユーザ アカウントが削除され、使用できなくなります。

パスワードの変更

Prime Infrastructure ユーザ アカウントのパスワードを変更するには、次の手順を実行します。

ステップ 1　「Prime Infrastructure サーバの起動」（P.2-20）の手順に従って、Prime Infrastructure サーバを起動します。

ステップ 2　SuperUsers グループに割り当てられたユーザとして Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 3　[Administration] > [AAA] の順に選択して、[Change Password] ページを表示します。

ステップ 4　古いパスワードを入力します。

ステップ 5　[New Password] と [Confirm New Password] テキストボックスの両方に新しいパスワードを入力します。

ステップ 6　[Save] をクリックして変更を保存します。ユーザ アカウントのパスワードが変更され、すぐに使用できる状態になりました。

CLI を使用したルート ユーザ パスワードの変更

コマンドライン インターフェイスを使用してルート ユーザのパスワードを変更するには、次の手順に従います。

ステップ 1　administrator としてシステムにログインします。

ステップ 2　コマンドライン インターフェイス（CLI）を使用して、次のコマンドを入力します。

```
VMNCS/admin# ncs password ?
  ftpuser  Modifies ftp username and password
  root     Modifies root user login password

VMNCS/admin# ncs password root ?
  password  Modifies root user login password

VMNCS/admin# ncs password root password ? <password>
  <WORD>  Type in root user login password (Max Size - 80)
```

アクティブ セッションのモニタリング

アクティブ ユーザの一覧を表示するには、次の手順に従います。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Active Sessions] を選択します。[Active Sessions] ページが表示されます。

赤で表示されているユーザは、現在ログインしていることを表しています。列見出しがハイパーリンクの場合、列見出しをクリックするとアクティブ セッションの一覧をその列の降順または昇順で並べ替えることができます。並べ替えの方向は、ハイパーリンクをクリックするたびに切り替わります。

[Active Sessions] ページの列は、次のとおりです。

- [Username]：ログインしているユーザ名。

- [IP/Host Name] : ブラウザが稼働しているマシンの IP アドレスまたはホスト名。ユーザ マシンのホスト名が DNS にない場合、IP アドレスが表示されます。
- [Login Time] : ユーザが Prime Infrastructure にログインした時刻。すべての時刻は、Prime Infrastructure サーバのマシンの時刻に基づいています。
- [Last Access Time] : ユーザが最後に Prime Infrastructure にアクセスした時刻。すべての時刻は、Prime Infrastructure サーバのマシンの時刻に基づいています。

（注）　この列に表示されている時刻は、通常、使用しているシステムの時刻より数秒遅れています。これは、[Alarm Status] ダッシュレットの更新によって、[Last Access Time] が頻繁に更新されるためです。

- [Login Method] :
  - [Regular] : ブラウザを使用して直接 Prime Infrastructure にログインするユーザに対して作成されたセッション
- [User Groups] : ユーザが所属するグループの一覧。
- 監査証跡アイコン : そのユーザの監査証跡（以前のログイン時刻）を表示するページへのリンク。

ユーザ アカウント情報の表示または編集

ユーザの所属グループを参照する、またはユーザのパスワードや所属グループを調整するには、次の手順に従います。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　[User Name] 列でユーザをクリックします。[User Detail : *User Group*] ページが表示されます。

ユーザの所属グループを確認したり、パスワードや所属グループを変更したりすることが可能です。

Lobby Ambassador のデフォルトの設定

[User Name] 列で [Lobby Ambassador] を選択した場合、[Lobby Ambassador Defaults] タブが表示されます。Lobby Ambassador で作成されたすべてのゲスト ユーザ アカウントには、デフォルトでこのようなクレデンシャルが備わっています。デフォルト値が指定されていない場合、Lobby Ambassador には必要なゲスト ユーザ クレデンシャルのフィールドが表示されるはずです。

（注）　デフォルトのプロファイルがこのタブで選択されていないと、デフォルト値はこの Lobby Ambassador に適用されません。Lobby Ambassador アカウントは作成されず、選択した任意のクレデンシャルを持つユーザを作成する可能性があります。

ステップ 1　[Profile] ドロップダウン リストを使用して、接続するゲスト ユーザを選択します。

有線ゲストは、有線 LAN ポートから発信されるトラフィックを示すように定義されたプロファイルの一例です。「有線ゲスト アクセスの設定」（P.9-332）を参照してください。

ステップ 2　ユーザ ロールを選択して、ネットワーク内の特定のユーザに割り当てられた帯域幅の量を管理します。これは管理者により事前に定義され、ゲストのアクセス（契約者、顧客、代理店、ベンダー、ビジターなど）に関連付けられています。

ステップ 3　[Lifetime] オプション ボタンで [Limited] または [Unlimited] を選択します。

- [Limited] オプションでは、時間および分のドロップダウン リストを使用して、ゲスト ユーザ アカウントをアクティブにする期間を選択します。[Limited] のデフォルト値は、1 日（8 時間）です。
- [Unlimited] を選択すると、ゲスト アカウントの有効期限の日付は存在しません。

ステップ 4　[Apply] ドロップダウン リストを使用して、次のオプションから選択します。選択したオプションによって、表示される追加パラメータが決まります。

- [Indoor area]：キャンパス、ビルディングまたはフロア領域。
- [Outdoor area]：キャンパスまたは屋外領域。
- [Controller list]：作成済みのプロファイルのうち選択されたものが表示されたコントローラの一覧。
- [Config Group]：Prime Infrastructure で設定された設定グループの名前。

ステップ 5　ゲスト アカウント クレデンシャルの送信先のホストの電子メール ID を入力します。

ステップ 6　アカウントの簡単な説明を入力します。

ステップ 7　免責事項テキストを入力する場合には、[Disclaimer] に入力します。

Lobby Ambassador のこれらの設定済みデフォルトを上書きできるようにする場合は、[Defaults Editable] チェックボックスをオンにします。こうすることで、[Lobby Ambassador] ポータルからゲスト アカウントを作成するときに、ゲスト ユーザのデフォルト設定を Lobby Ambassador が編集できるようになります。

（注）　デフォルトのプロファイルがこのタブで選択されていない場合、デフォルト値はこの Lobby Ambassador に適用されません。ただし、Lobby Ambassador アカウントは作成され、Lobby Ambassador により必要に応じてクレデンシャルを持ったユーザを作成できます。

ステップ 8　[Max User Creations Allowed] チェックボックスをオンにして、Lobby Ambassador が指定する期間内に作成可能なゲスト ユーザの上限を設定します。期間は、時間、日、または週で定義します。

ステップ 9　[Preview Current Logo] リンクをクリックして、現在使用されているロゴを参照します。クリックして有効にするか、別の場所を参照してロゴを更新できます。

ステップ 10　ページ ヘッダー テキストを追加するには、[Print Page Header Text] フィールドに入力します。

ステップ 11　[Submit] をクリックします。

グループ情報の表示または編集

定義されたグループ内でユーザによる実行の許可されている具体的なタスクを参照するか、タスクに変更を加えるには、次の手順に従ってください。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　[Member Of] 列で、グループ リンクをクリックします。[Group Detail: *User Group*] ページが表示されます。

（注）　詳細事項を記載したページは、選択したグループに応じて異なります。

定義済みグループでユーザに許可された特定のタスクを参照する、またはタスクに変更を加えることが可能です。

ゲスト ユーザのクレデンシャルの編集

クレデンシャルを編集するゲスト ユーザの Prime Infrastructure ユーザ名をクリックします。[Lobby Ambassador Default] タブが表示され、クレデンシャルを変更できます。

（注）　編集の際、*Profile* の選択が削除されている場合（[Select a profile] に変更されている場合）、この Lobby Ambassador のデフォルト値は削除されています。デフォルト値を再び有効にするには、設定し直す必要があります。

監査証跡の表示

[Users] ページの  アイコンをクリックして、各ユーザが設定に加えた変更を表示します。[Audit Trail] ページが表示されます。

このページでは、次のデータを表示できます。

- [User]：ユーザのログイン名。
- [Operation]：監査された操作の種類。
- [Time]：操作が監査された時刻。
- [Status]：成功または失敗。
- [Reason]：ログイン失敗の理由（無効なパスワードなど）。
- [Configuration Changes]：設定が変更されている場合、このフィールドに [Details] リンクが表示されます。個々のユーザによる設定の変更の詳細を確認するには [Details] リンクをクリックします。Prime Infrastructure とコントローラとの間の個々のパラメータの値に加えられた変更が、エントリとして一覧表示されます。監査証跡詳細について詳しくは、「[Audit Trail Details] ページ」（P.7-251）を参照してください。

（注）　個々のコントローラの変更について、監査証跡のエントリがログに記録されている場合があります。たとえば、あるテンプレートが複数のコントローラに適用される場合、そのテンプレートが適用された各コントローラ用として複数の監査エントリが存在することになります。

[Audit Trail Details] ページ

設定に変更がある場合、[Audit Trail] 一覧ページの [Configuration Changes] 列に [Details] リンクが含まれます。[Details] リンクをクリックすると、特定のユーザの [Audit Trail Details] が表示されます。ユーザによるテンプレートからまたは設定側からの設定変更があるとき、[Audit Trail Details] ダイアログボックスには相違点が属性レベルで表示されます。

表 7-1 に [Audit Trail Details] ダイアログボックスのフィールドについて説明します。

表 7-1　[Audit Trail Details] ページのフィールド

フィールド	説明
Prime Infrastructure Username	監査証跡を生成したユーザの名前。
Object Name	監査証跡を生成したオブジェクトの名前。
Operation Time	監査エントリが作成された日付と時刻。
Configuration Changes	ユーザによる Prime Infrastructure とコントローラでの操作の結果、変更された属性を一覧表示します。 たとえば、次のような属性です。 • Quality of service • Admin Status • MAC Filters

ゲスト ユーザ アカウントの作成

Cisco Lobby Ambassador を使用して、Prime Infrastructure のゲスト ユーザ アカウントを作成できます。企業によって提供されるゲスト ネットワークは、ホストを危険にさらすことなく、ゲストがインターネットにアクセスできるようにします。Web 認証はサプリカントまたはクライアントの有無にかかわらず提供されます。そのため、ゲストはそれらの目的の宛先への VPN トンネルを開始する必要があります。

有線および無線の両方のゲスト ユーザ アクセスが、サポートされています。有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。

ネットワーク管理者は、まず Lobby Ambassador アカウントを設定する必要があります。ゲスト ユーザ アカウントは、ネットワーク アクセスを必要とする訪問者、臨時職員用などです。Lobby Ambassador アカウントは制限された設定権限を持ち、ゲスト ユーザ アカウントの設定と管理に使用する画面へのアクセスだけを許可します。

Lobby Ambassador では、次の種類のゲスト ユーザ アカウントを作成できます。

- ライフタイムの期限があるゲスト ユーザ アカウント。指定した時間が経過すると、ゲスト ユーザ アカウントは自動的に失効します。
- ライフタイムの期限がないゲスト ユーザ アカウント。このアカウントには有効期限がありません。
- 事前に定義された将来の時刻にアクティブ化されるゲスト ユーザ アカウント。Lobby Ambassador では、有効期間の開始と終了が定義されています。

Prime Infrastructure でゲスト ユーザ アカウントを作成するには、次の手順を実行します。

（注） SuperUser/ 管理者権限を持つグループ（デフォルト）が Lobby Ambassador アカウントを作成できます。管理者は、複数の Lobby Ambassador アカウントを作成して、それぞれ異なるプロファイルおよび権限を設定することができます。

（注）　インストールの際に作成されるルート グループに割り当てられたユーザは 1 つだけです。インストール後に、ユーザを追加して割り当てることはできません。このルート ユーザは変更できません。また、スーパーユーザとは異なり、タスクを変更することもできません。

ステップ 1　管理者として Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Administration] > [AAA] の順に選択します。

ステップ 3　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add User] を選択し、[Go] をクリックします。[Users] ページが表示されます。

ステップ 5　ユーザ名を入力します。

ステップ 6　パスワードを入力します。最小文字数は 6 文字です。確認のため、同じパスワードをもう一度入力します。

（注）　4 種類の要素（小文字、大文字、数字、特殊文字）のうち、3 種類以上の要素を使用してパスワードを作成する必要があります。

ステップ 7　[Groups Assigned to this User] セクションで、[LobbyAmbassador] チェックボックスをオンにすると、[Lobby Ambassador Defaults] タブが表示されます。

ステップ 8　「Lobby Ambassador のデフォルトの設定」（P.7-249）の手順を実行します。

Prime Infrastructure ゲスト ユーザ アカウントの管理

Prime Infrastructure ゲスト ユーザ アカウントは、テンプレートを使用して管理されます。この項では、Prime Infrastructure ユーザ アカウントの管理方法について説明します。次の項目について説明します。

- 「ゲスト ユーザ テンプレートの設定」（P.11-662）
- 「Prime Infrastructure ゲスト ユーザ アカウントのスケジュール」（P.7-253）
- 「Prime Infrastructure ゲスト ユーザの詳細の印刷または電子メール送信」（P.7-255）
- 「ゲスト アカウントのデバイスへの保存」（P.7-255）

Prime Infrastructure ゲスト ユーザ アカウントのスケジュール

Lobby Ambassador は、ゲスト ユーザ アカウントの自動作成をスケジュールできます。アカウントの有効性と自動更新を定義できます。オプションとして、スケジュールごとに新しいパスワードを生成できます。有効にするには、チェックボックスをオンにします。スケジュールされたユーザの場合、パスワードは自動的に生成され、ゲストのホストへ電子メールが自動的に送信されます。ホストの電子メール アドレスは [New User] ページで設定します。[Save] をクリックすると、[Guest User Details] ページにパスワードが表示されます。このページから、アカウントのクレデンシャルの電子メール送信や、印刷が可能です。

Prime Infrastructure でゲスト ユーザ アカウントの繰り返しをスケジュールするには、次の手順を実行します。

ステップ 1　Lobby Ambassador として Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Guest User] ページで [Schedule Guest User] を選択します。

（注）　ゲスト ユーザのスケジュールは、[Configure] > [Controller Template Launch Pad] > [Security] > [Guest User] オプションからも実行できます。

ステップ 3　[Guest Users] > [Scheduling] ページで、ゲスト ユーザ名を入力します。最大文字数は 24 文字です。

ステップ 4　チェックボックスをオンにして、スケジュールごとにユーザ名とパスワードを生成します。これを有効化すると、異なるパスワードが毎日（選択した日数分）支給されます。これを無効化すると（オフにする）、1 つのパスワードが選択した日数の間支給されます。オプションとして、スケジュールごとに新しいパスワードを生成できます。

ステップ 5　ドロップダウン リストから [Profile ID] を選択します。これは、このゲスト ユーザが適用する SSID であり、レイヤ 3 認証ポリシーが設定されている WLAN でなければなりません。使用する Profile ID については管理者に問い合わせてください。

ステップ 6　ゲスト ユーザ アカウントの説明を入力します。

ステップ 7　[limited] または [unlimited] を選択します。

- [Limited] : ドロップダウン リストから、このゲスト ユーザ アカウントのライフタイムを日数、時間数、または分数で選択します。最大文字数は 35 文字です。
  - [Start time] : ゲスト ユーザ アカウントを開始する日付と時刻。
  - [End time] : ゲスト ユーザ アカウントが期限切れとなる日付と時刻。
- [Unlimited] : このユーザ アカウントには有効期限がありません。
- [Days of the week] : このゲスト ユーザ アカウントに適用する曜日をチェックボックスでオンにします。

ステップ 8　[Apply To] を選択し、キャンパス、ビルディング、またはフロアを選択してゲスト ユーザを限定領域に制限します。それにより、適用されたときにそれらのコントローラおよびアソシエートされたアクセス ポイントだけが使用できるようになります。ブロードキャストする SSID を決定する AP グルーピングを使用して、アクセス ポイント レベルの制限を強化できます。アクセス ポイントがそれぞれのフロアに割り当てられるようになります。また、ゲスト ユーザを、一覧に記載された特定のコントローラまたは設定グループに制限することもできます。この際、コントローラのグループは管理者により事前に設定されています。

ドロップダウン リストから、次のいずれかを選択します。

- [Controller List] : ゲスト ユーザ アカウントが関連するコントローラのチェックボックスをオンにします。
- [Indoor Area] : 適用できるキャンパス、ビルディング、およびフロアを選択します。
- [Outdoor Area] : 適用できるキャンパスおよび屋外領域を選択します。
- [Config group] : ゲスト ユーザ アカウントが所属する設定グループを選択します。

ステップ 9　電子メール アドレスを入力して、ゲスト ユーザ アカウントのクレデンシャルを送信します。スケジュールされた時刻になるたびに、ゲスト ユーザ アカウントのクレデンシャルが指定された電子メール アドレスへ送信されます。

ステップ 10　免責事項の情報を確認します。スクロール バーを使用して、上下に移動します。

ステップ 11　[Save] をクリックして変更内容を保存するか、または [Cancel] をクリックして設定変更を取り消します。

Prime Infrastructure ゲスト ユーザの詳細の印刷または電子メール送信

Lobby Ambassador では、ゲスト ユーザ アカウントの詳細を印刷したり、ゲストを受け入れるホストや個人にこの情報を電子メールで送信できます。

電子メールおよび印刷には、次の詳細が表示されます。

- [Username]：ゲスト ユーザのアカウント名。
- [Password]：ゲスト ユーザ アカウントのパスワード。
- [Start time]：ゲスト ユーザ アカウントを開始する日付と時刻。
- [End time]：ゲスト ユーザ アカウントが期限切れとなる日付と時刻。
- [Profile ID]：ゲスト ユーザに割り当てられるプロファイル。使用する Profile ID については管理者に問い合わせてください。
- [Disclaimer]：ゲスト ユーザ向けの免責事項情報。

ゲスト ユーザ アカウントを作成して、コントローラ、領域、または設定グループの一覧にそのアカウントを適用すると、リンクが生成され、ゲスト ユーザ アカウントの詳細を電子メールで送信したり、印刷できるようになります。[Guest Users List] ページからもゲスト ユーザ アカウントの詳細を印刷できます。

[Guest Users List] ページからゲスト ユーザの詳細情報を印刷するには、次の手順に従います。

ステップ 1　Lobby Ambassador として Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Guest User] ページで、[User Name] の横のチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Print/E-mail User Details] を選択して、[Go] をクリックします。

- 印刷する場合には、[Print] ページで [Print] をクリックし、プリンタを選択して [Print] または [Cancel] をクリックします。
- 電子メールの場合には、[E-mail] ページで [E-mail] をクリックして、件名と受信者の電子メール アドレスを入力します。[Send] または [Cancel] をクリックします。

（注）　ユーザの詳細情報の印刷や電子メール送信は、[Configure] > [Controller Template Launch Pad] > [Security] > [Guest User] オプションからも実行できます。

ゲスト アカウントのデバイスへの保存

[Save Guest Accounts on Device] チェックボックスをオンにして、ゲスト アカウントを WLC フラッシュに保存すると、WLC リブート時にもアカウントを保持できます。

（注）　[Configure] > [Controller Template Launch Pad] > [Security] > [Guest] ページで、[Select a command] ドロップダウン リストから [Save Guest Accounts on device] を選択します。

ゲスト ユーザのクレデンシャルの編集

クレデンシャルを編集するゲスト ユーザの Prime Infrastructure ユーザ名をクリックします。[Lobby Ambassador Default] タブが表示され、クレデンシャルを変更できます。

編集の際、*Profile* の選択が削除されている場合（[Select a profile] に変更されている場合）、この Lobby Ambassador のデフォルト値は削除されています。デフォルト値を再び有効にするには、設定し直す必要があります。

新しいユーザの追加

[Add User] ページを使用して、管理者はユーザ名、パスワード、ユーザに割り当てられるグループ、ユーザの仮想ドメインなど、新しいユーザ ログインを設定できます。

（注）　自分で新しく作成したユーザにだけ、仮想ドメインを割り当てることができます。仮想ドメインをユーザに割り当てることによって、ユーザはこれらの仮想ドメインに適切な情報に制限されます。

ここでは、次の内容について説明します。

- 「ユーザ名、パスワード、グループの追加」（P.7-256）
- 「仮想ドメインの割り当て」（P.7-257）

ユーザ名、パスワード、グループの追加

新規ユーザを追加する手順は、次のとおりです。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add User] を選択します。

ステップ 4　[Go] をクリックします。[Users] ページが表示されます。

ステップ 5　[Username] に新しいユーザ名を入力します。

ステップ 6　このアカウントのパスワードを入力して確定します。

ステップ 7　ユーザが割り当てられているグループのチェック ボックスをオンにします。

（注）　ユーザが Lobby Ambassador、Monitor Lite、Northbound API、または Users Assistant グループに属する場合、ユーザは別のグループにも属するということはできません。

- [Admin]：Prime Infrastructure の動作をモニタおよび設定し、すべてのシステム管理タスクを実行できます。
- [ConfigManagers]：Prime Infrastructure の動作をモニタおよび設定できます。
- [System Monitoring]：Prime Infrastructure の動作をモニタできます。
- [Users Assistant]：ローカル ネット ユーザの管理だけを実行できます。
- [Lobby Ambassador]：ゲストのアクセスで許可されるのは、ユーザ アカウントの設定と管理だけです。[Lobby Ambassador] を選択すると、[Lobby Ambassador Defaults] タブが表示されます。

- [Monitor Lite]：アセットの位置をモニタできます。
- [North Bound API User]：Prime Infrastructure Web サービス コンシューマで使用されるユーザ グループ。つまり、すべての North Bound API です。

（注）　TACACS または RADIUS から North Bound API User を作成する場合、デフォルト ユーザ ドメインを *root* にする必要があります。

（注）　North Bound API User には、仮想ドメインを割り当てられません。North Bound API グループを選択すると、[Virtual Domains] タブを使用できなくなります。

- [SuperUsers]：Prime Infrastructure の動作をモニタおよび設定し、Prime Infrastructure のユーザ アカウントとパスワードの管理を含むすべてのシステム管理タスクを実行できます。スーパーユーザのタスクは、変更できます。
- [Root]：このグループは「root」ユーザにだけ割り当てでき、その割り当てを変更できません。
- User Defined

仮想ドメインの割り当て

ユーザに仮想ドメインを割り当てるには、次の手順に従います。

ステップ 1　[Virtual Domains] タブをクリックします。このタブには、このユーザが使用できる仮想ドメインおよび割り当てられている仮想ドメインがすべて表示されます。

（注）　[Virtual Domains] タブを使用して、管理者は仮想ドメインを各ユーザに割り当てることができます。仮想ドメインをユーザに割り当てることによって、ユーザはこれらの仮想ドメインに適切な情報に制限されます。

（注）　North Bound API User には、仮想ドメインを割り当てられません。North Bound API グループを選択すると、[Virtual Domains] タブを使用できなくなります。

ステップ 2　[Available Virtual Domains] リストで、このユーザに割り当てる仮想ドメインをクリックして強調表示します。

（注）　Shift キーまたは Ctrl キーを押したまま、複数の仮想ドメインを選択できます。

ステップ 3　[Add >] をクリックします。仮想ドメインが [Available Virtual Domains] リストから [Selected Virtual Domains] リストに移動します。

仮想ドメインを [Selected Virtual Domains] リストから削除するには、[Selected Virtual Domains] リストのドメインをクリックして強調表示し、[Remove] をクリックします。仮想ドメインが [Selected Virtual Domains] リストから [Available Virtual Domains] リストに移動します。

ステップ 4　[Submit] をクリックして変更を保存するか、[Cancel] で現在のユーザの追加または編集を保存せずにページを閉じます。

Lobby Ambassador アカウントの管理

Cisco Lobby Ambassador を使用して、Prime Infrastructure のゲスト ユーザ アカウントを作成できます。企業によって提供されるゲスト ネットワークは、ホストを危険にさらすことなく、ゲストがインターネットにアクセスできるようにします。Web 認証はサプリカントまたはクライアントの有無にかかわらず提供されます。そのため、ゲストはそれらの目的の宛先への VPN トンネルを開始する必要があります。

有線および無線の両方のゲスト ユーザ アクセスが、サポートされています。有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。

ネットワーク管理者は、まず Lobby Ambassador アカウントを設定する必要があります。ゲスト ユーザ アカウントは、ネットワーク アクセスを必要とする訪問者、臨時職員用などです。Lobby Ambassador アカウントは制限された設定権限を持ち、ゲスト ユーザ アカウントの設定と管理に使用するページへのアクセスだけを許可します。

Lobby Ambassador では、次の種類のゲスト ユーザ アカウントを作成できます。

- ライフタイムの期限があるゲスト ユーザ アカウント。指定した時間が経過すると、ゲスト ユーザ アカウントは自動的に失効します。
- ライフタイムの期限がないゲスト ユーザ アカウント。このアカウントには有効期限がありません。
- 事前に定義された将来の時刻にアクティブ化されるゲスト ユーザ アカウント。Lobby Ambassador では、有効期間の開始と終了が定義されています。

ここでは、次の内容について説明します。

- 「Lobby Ambassador アカウントの作成」（P.7-258）
- 「Lobby Ambassador アカウントの編集」（P.7-260）
- 「Lobby Ambassador として Prime Infrastructure ユーザ インターフェイスへログインする方法」（P.7-260）
- 「Lobby Ambassador アクティビティのロギング」（P.7-261）

Lobby Ambassador アカウントの作成

（注）　SuperUser/ 管理者権限を持つグループ（デフォルト）が Lobby Ambassador アカウントを作成できます。

Prime Infrastructure で Lobby Ambassador アカウントを作成するには、次の手順を実行します。

ステップ 1　管理者として Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Administration] > [AAA] の順に選択します。

ステップ 3　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add User] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　ユーザ名を入力します。

ステップ 7　パスワードを入力します。確認のため、同じパスワードをもう一度入力します。パスワードには、次のような要求事項があります。

- パスワードには少なくとも 8 文字必要です。
- 小文字、大文字、数字、特殊文字の 4 種類の文字から 3 種類以上を使用してパスワードを作成する必要があります。

ステップ 8　[Groups Assigned to this User] セクションで、[LobbyAmbassador] チェックボックスをオンにすると、[Lobby Ambassador Defaults] タブが表示されます。

[Lobby Ambassador Defaults] タブには、次のパラメータがあります。

- [Profile]：ゲスト ユーザが接続するデフォルト プロファイル。
- [Lifetime]：「Limited」または「Unlimited」。

  （注）　デフォルトでは、ライフタイムは 8 時間までに限定されています。

- [Apply to]：ドロップダウン リストから、次のいずれかを選択します。
  - [Indoor Area]：キャンパス、ビルディング、フロア。
  - [Outdoor Area]：キャンパス、屋外領域。
  - [Controller List]：選択されたプロファイルが作成されたコントローラの一覧。
  - [Config Group]：Prime Infrastructure で設定された設定グループの名前。
- [Email ID]：ゲスト アカウント クレデンシャルの送信先のホストの電子メール ID を入力します。
- [Description]：アカウントの簡単な説明。
- [Disclaimer]：デフォルトの免責事項テキスト。
- [Defaults Editable]：Lobby Ambassador にこれらの設定済みデフォルトの上書きを許可する場合、このチェックボックスをオンにします。こうすることで、Lobby Ambassador が [Lobby Ambassador] ポータルからゲスト アカウントを作成する際にこれらのゲスト ユーザ アカウントのデフォルト設定を編集できるようになります。

  （注）　デフォルトのプロファイルがこのタブで選択されていない場合、デフォルト値はこの Lobby Ambassador に適用されません。ただし、Lobby Ambassador アカウントは作成され、Lobby Ambassador は必要に応じてクレデンシャルを持ったユーザを作成できます。

- [Max User Creation Allowed]：このチェックボックスをオンにして、Lobby Ambassador が指定する期間内に作成可能なゲスト ユーザの上限を設定します。期間は、時間、日、または週で定義します。
- [Submit] をクリックします。新しい Lobby Ambassador アカウントの名前が一覧に表示され、アカウントはすぐに使用できる状態になります。

Lobby Ambassador アカウントの編集

Lobby Ambassador デフォルト クレデンシャルは、Prime Infrastructure ユーザの一覧ページのユーザ名のリンクから編集できます。

Lobby Ambassador デフォルト クレデンシャルを編集する手順は、次のとおりです。

ステップ 1　管理者として Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　[Administration] > [AAA] の順に選択します。

ステップ 3　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 4　[User Name] 列から使用できる Lobby Ambassador アカウントをクリックします。

ステップ 5　[Lobby Ambassador Defaults] ページから、必要に応じてクレデンシャルを編集します。

（注）　編集の際、Profile の選択が削除されている場合（[Select a profile] に変更されている場合）、この Lobby Ambassador のデフォルト値は削除されています。デフォルト値を再び有効にするには、設定し直す必要があります。

ステップ 6　[Submit] をクリックします。

Lobby Ambassador として Prime Infrastructure ユーザ インターフェイスへログインする方法

Lobby Ambassador としてログインすると、Prime Infrastructure のゲスト ユーザ テンプレートのページにアクセスできます。そこでテンプレートを通してゲスト ユーザ アカウントを設定できます。

Web ブラウザを介して Prime Infrastructure ユーザ インターフェイスにログインするには、次の手順を実行します。

ステップ 1　コンピュータで Internet Explorer 8 またはそれ以降のバージョンを起動します。

（注）　Windows ワークステーション上で Internet Explorer 8 以降以外の Web ブラウザを使用した場合、一部の Prime Infrastructure 機能が適切に機能しない場合があります。

ステップ 2　ブラウザのアドレス欄に、**https://***Prime Infrastructure-ip-address*（https://1.1.1.1 など）と入力します。ここで、*Prime Infrastructure-ip-address* は Prime Infrastructure がインストールされているコンピュータの IP アドレスです。この IP アドレスは管理者が知っています。

ステップ 3　Prime Infrastructure ユーザ インターフェイスに [Login] ウィンドウが表示されたら、ユーザ名とパスワードを入力します。

（注）　入力する文字はすべて、大文字と小文字が区別されます。

（注）　Lobby Ambassador は、ゲスト ユーザ テンプレートだけを定義できます。

ステップ 4　[Submit] をクリックして、Prime Infrastructure にログインします。Prime Infrastructure ユーザ インターフェイスは、これでアクティブになり、使用可能になります。[Guest Users] ページが表示されます。このページには、作成したすべての Guest User の概要が表示されます。

Prime Infrastructure ユーザ インターフェイスを終了するには、ブラウザ ウィンドウを閉じるか、ページの右上隅にある [Logout] をクリックします。Prime Infrastructure ユーザ インターフェイス セッションを終了しても、サーバ上の Prime Infrastructure はシャットダウンされません。

（注）　Prime Infrastructure セッション中にシステム管理者が Prime Infrastructure サーバを停止すると、セッションが終了し、Web ブラウザに「`The page cannot be displayed.`」というメッセージが表示されます。サーバが再起動される際に、セッションは Prime Infrastructure に再アソシエートされません。Prime Infrastructure セッションを再起動する必要があります。

Lobby Ambassador アクティビティのロギング

各 Lobby Ambassador アカウントの次のアクティビティが記録されます。

- [Lobby ambassador login] : Prime Infrastructure では、すべてのユーザの認証操作結果が記録されます。
- [Guest user creation] : Lobby Ambassador がゲスト ユーザ アカウントを作成すると、Prime Infrastructure はゲスト ユーザ名を記録します。
- [Guest user deletion] : Lobby Ambassador がゲスト ユーザ アカウントを削除すると、Prime Infrastructure は削除されたゲスト ユーザ名を記録します。
- [Account updates] : Prime Infrastructure はゲスト ユーザ アカウントに対して実行されたすべての更新の詳細を記録します。たとえば、ライフタイムの延長などです。

Lobby Ambassador のアクティビティを表示するには、次の手順に従います。

（注）　このウィンドウを開くには、管理者権限が必要です。

ステップ 1　管理者として Prime Infrastructure ユーザ インターフェイスにログインします。

ステップ 2　左側のサイドバーのメニューから [Administration] > [AAA] > [Groups] と選択して、[All Groups] ページを表示します。

ステップ 3　[All Groups] ページで、表示する Lobby Ambassador アカウントの [Audit Trail] アイコンをクリックします。Lobby Ambassador の [Audit Trail] ページが表示されます。

このページで、Lobby Ambassador アクティビティ一覧を時系列表示できます。

- [User] : ユーザのログイン名
- [Operation] : 監査された操作の種類
- [Time] : 操作が監査された時刻
- [Status] : 成功または失敗

ステップ 4　監査証跡をクリアするには、[Select a Command] ドロップダウン リストから [Clear Audit Trail] を選択し、[Go] をクリックします。

モビリティ グループの設定

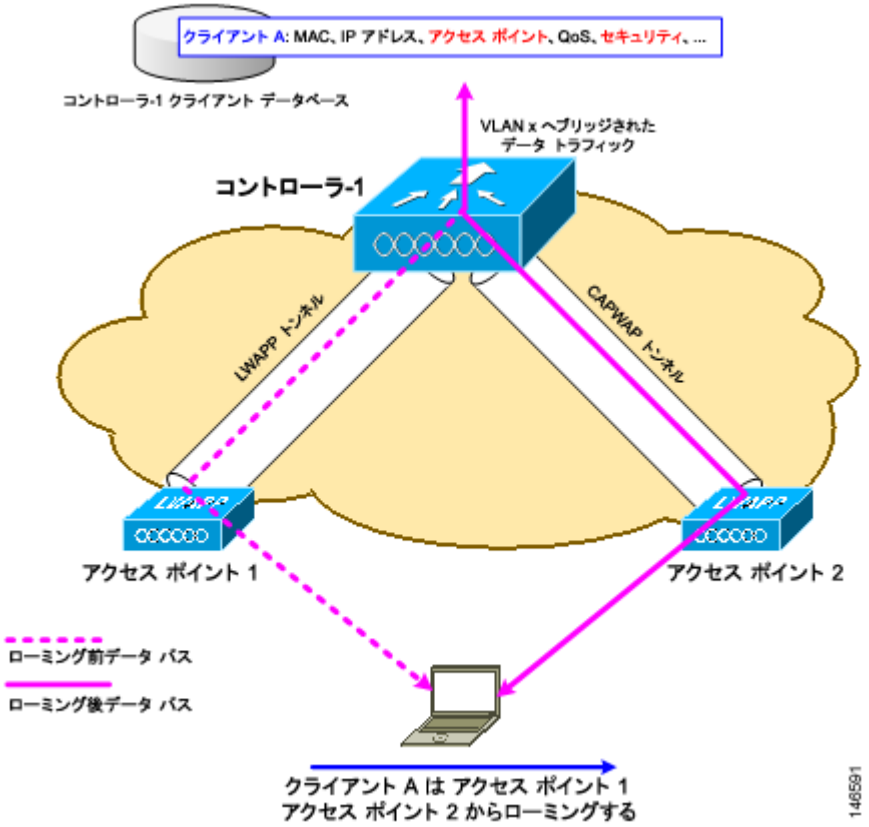
この章では、モビリティ グループについて説明し、Cisco Prime Infrastructure でモビリティ グループを設定する方法を説明します。ここで説明する内容は、次のとおりです。

モビリティについて

モビリティ（ローミング）は、できるだけ遅れることなく、確実かつスムーズに、あるアクセス ポイントから別のアクセス ポイントへアソシエーションを維持するワイヤレス クライアントの機能です。この項では、コントローラが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントがアクセス ポイントにアソシエートして認証すると、コントローラは、クライアント データベースにそのクライアントに対するエントリを設定します。このエントリにはクライアントの MAC アドレスと IP アドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、アソシエートされているアクセス ポイントなどが含まれます。コントローラはこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。図 8-1 には、2 つのアクセス ポイントが同一のコントローラに接続されている場合の両アクセス ポイント間における無線クライアント ローミングの様子が示されています。

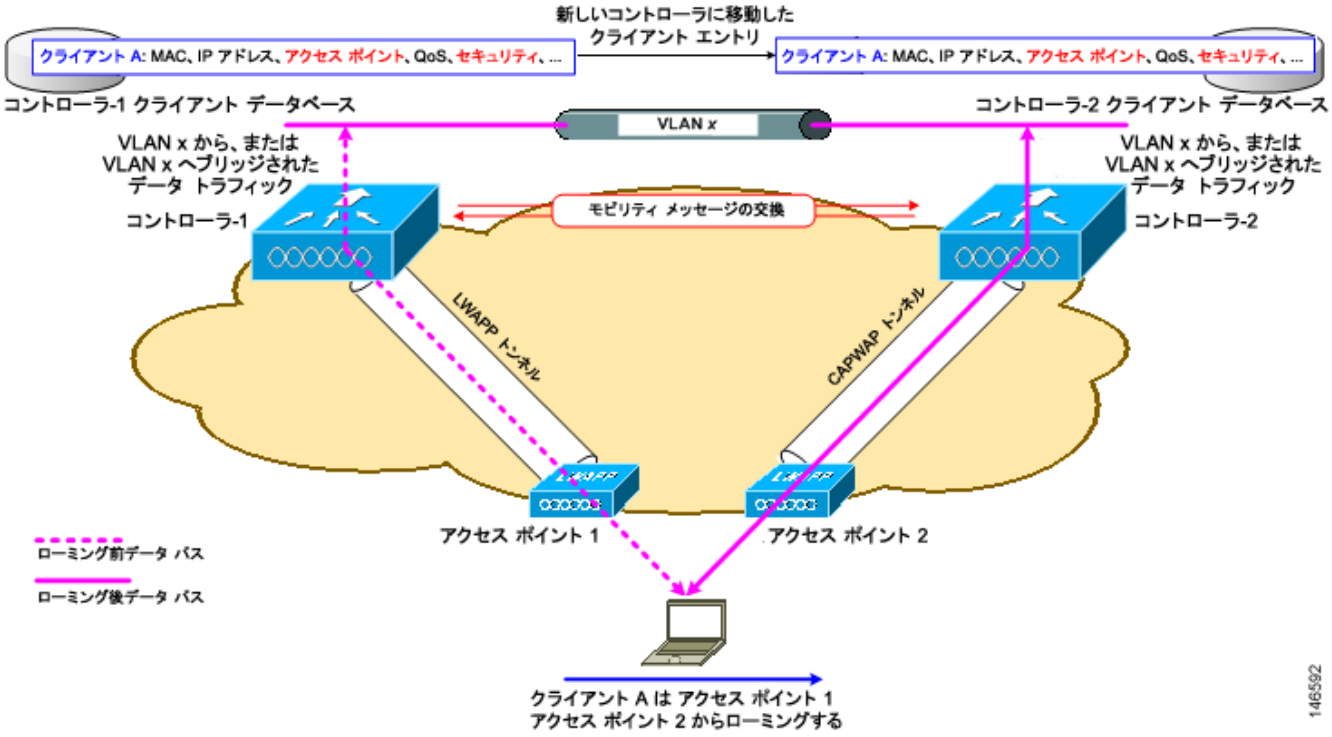
図 8-1　コントローラ内ローミング



ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントへ移動する場合、コントローラはクライアントのデータベースを新たにアソシエートするアクセス ポイントでアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。

しかし、クライアントが 1 つのコントローラに join されたアクセス ポイントから別のコントローラに join されたアクセス ポイントにローミングする際には、プロセスはより複雑になります。また、プロセスは、コントローラが同一サブネット上で動作しているかどうかによって変わります。図 8-2 は、コントローラの無線 LAN インターフェイスが同じ IP サブネット上に存在する場合に発生する *コントローラ間ローミング*を表したものです。

図 8-2　コントローラ間ローミング

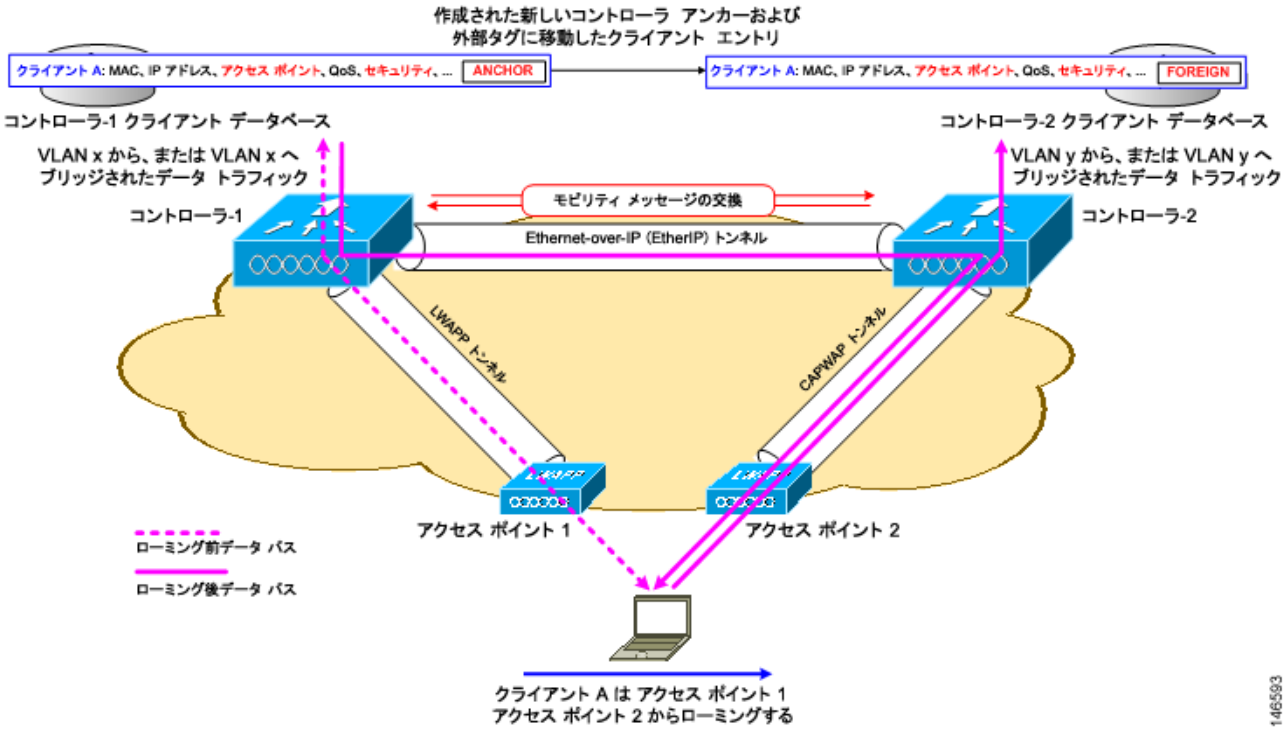


クライアントが新たなコントローラに join されたアクセス ポイントへアソシエートする場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たなアクセス ポイントに対してアップデートされます。このプロセスはユーザには見えません。

（注）　802.1X/Wi-Fi Protected Access（WPA）セキュリティで設定したすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

図 8-3 は、コントローラの無線 LAN インターフェイスが異なる IP サブネット上に存在する場合に発生する *サブネット間ローミング*を表したものです。

図 8-3　サブネット間ローミング



*サブネット間ローミング*は、コントローラがクライアントのローミング方法に関するモビリティ メッセージを交換する点で、コントローラ間ローミングと似ています。ただし、クライアントのデータベース エントリを新しいコントローラに移動するのではなく、元のコントローラのクライアント データベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベース エントリが新しいコントローラのクライアント データベースにコピーされ、新しいコントローラ内で「外部」エントリのマークが付けられます。ローミングは無線クライアントには見えません。また、クライアントはその元の IP アドレスを保持します。

サブネット間ローミングの後は、データは無線クライアントとの間で非対称のトラフィック パスで転送されます。クライアントからネットワークへのトラフィックは、外部コントローラでネットワークへ直接転送されます。クライアントへのトラフィックはアンカー コントローラに到達し、ここで EtherIP トンネルで外部コントローラへ転送されます。外部コントローラは、そのデータをクライアントへ転送します。無線クライアントが新たな外部コントローラへローミングする場合、クライアントのデータベース エントリは元の外部コントローラから新しい外部コントローラへ移動されますが、元のアンカー コントローラは常に保持されます。クライアントは元のコントローラに戻ると、再びローカルになります。

サブネット間ローミングでは、アンカーと外部の両コントローラの WLAN に同一のネットワーク アクセス権限を設定し、ソースベースのルーティングやソースベースのファイアウォールを設定しないでおく必要があります。そうしないと、ハンドオフ後にクライアントにネットワーク接続の問題が発生する場合があります。

（注） 現時点では、サブネット間ローミングの際にマルチキャスト トラフィックは伝送できません。この点を考慮して、サブネット間ネットワークの設計には Push-to-Talk を使用する際にマルチキャスト トラフィックを送信する必要のある Spectralink の電話を組み込まないようにします。

（注）　コントローラ間ローミングもサブネット間ローミングも、コントローラを同一のモビリティ グループ内に設置する必要があります。モビリティ グループの説明と設定の手順については、次の 2 つの項を参照してください。

シンメトリック トンネリング

シンメトリック モビリティ トンネリングを使用すると、コントローラでは 1 つのアクセス ポイントから無線 LAN 内の別のアクセス ポイントへローミングするクライアントに対して、サブネット間のモビリティが提供されます。有線ネットワーク上のクライアント トラフィックは、外部コントローラによって直接ルーティングされます。ルータでリバース パス フィルタリング（RPF）が有効になっている場合、着信パケットで追加確認が実行され、通信はブロックされます。RPF が有効になっている場合でも、シンメトリック モビリティ トンネリングによって、アンカーとして指定されたコントローラにクライアント トラフィックが到達できるようになります。[Configure] > [Controller] の順に選択し、左側のサイドバーのメニューから [System] > [General] の順に選択すると、シンメトリック トンネリングを有効または無効にできます。

（注）　モビリティ グループのすべてのコントローラは、同一のシンメトリック トンネリング モードを備えている必要があります。

（注）　シンメトリック トンネリングを有効にするには、リブートする必要があります。

このゲスト トンネリングの N+1 冗長機能を使用すると、コントローラのエラー後にクライアントが別のアクセス ポイントに接続するためにかかる時間が短縮されます。エラーがすばやく特定され、クライアントが問題発生のコントローラから移動し、別のコントローラに接続されるためです。

この機能をテンプレート内で設定する方法については、「コントローラ テンプレートの設定」（P.11-604）を参照してください。

モビリティ グループの概要

コントローラのセットを*モビリティ グループ*として設定すると、コントローラのグループ内でクライアントのローミングをスムーズに実行できるようになります。モビリティ グループを作成すると、ネットワーク内で複数のコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータ トラフィックを転送できるようになります。コントローラは、クライアント デバイスのコンテキストと状態およびコントローラのロード情報を共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。

（注）　クライアントは、モビリティ グループ間のローミングは行いません。

図 8-4 はモビリティ グループの例を示しています。

図 8-4　シングル モビリティ グループ

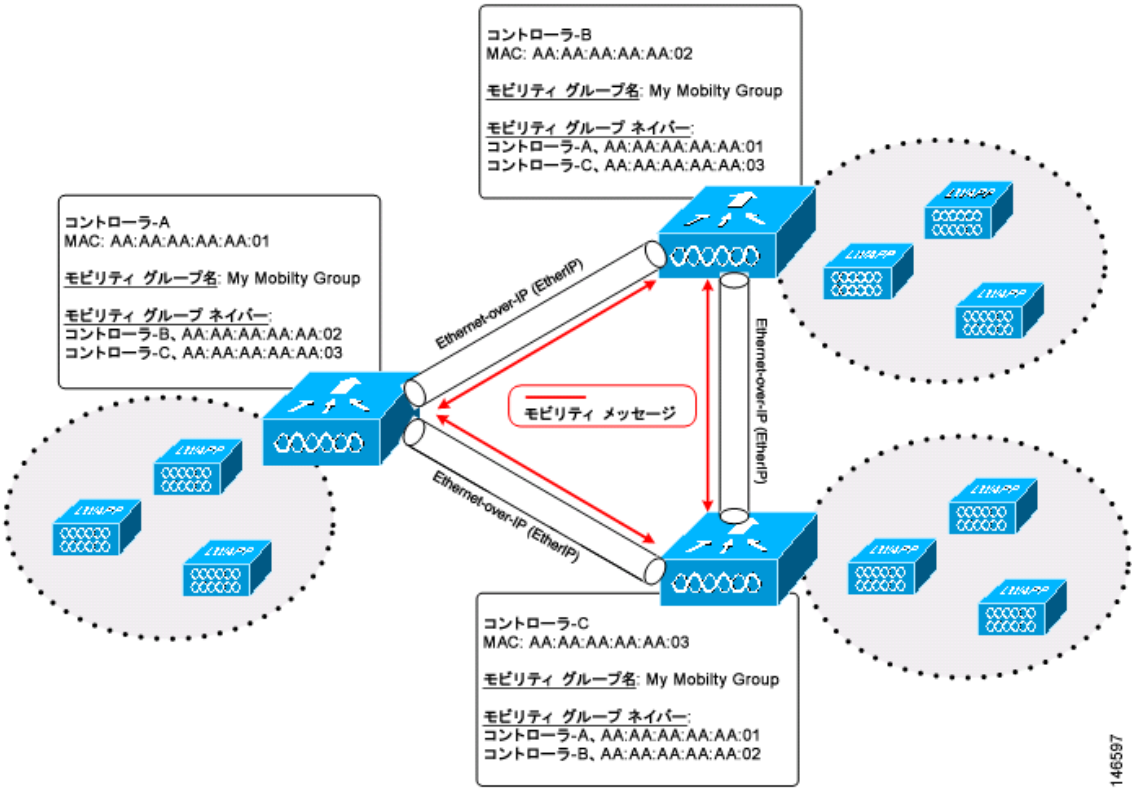


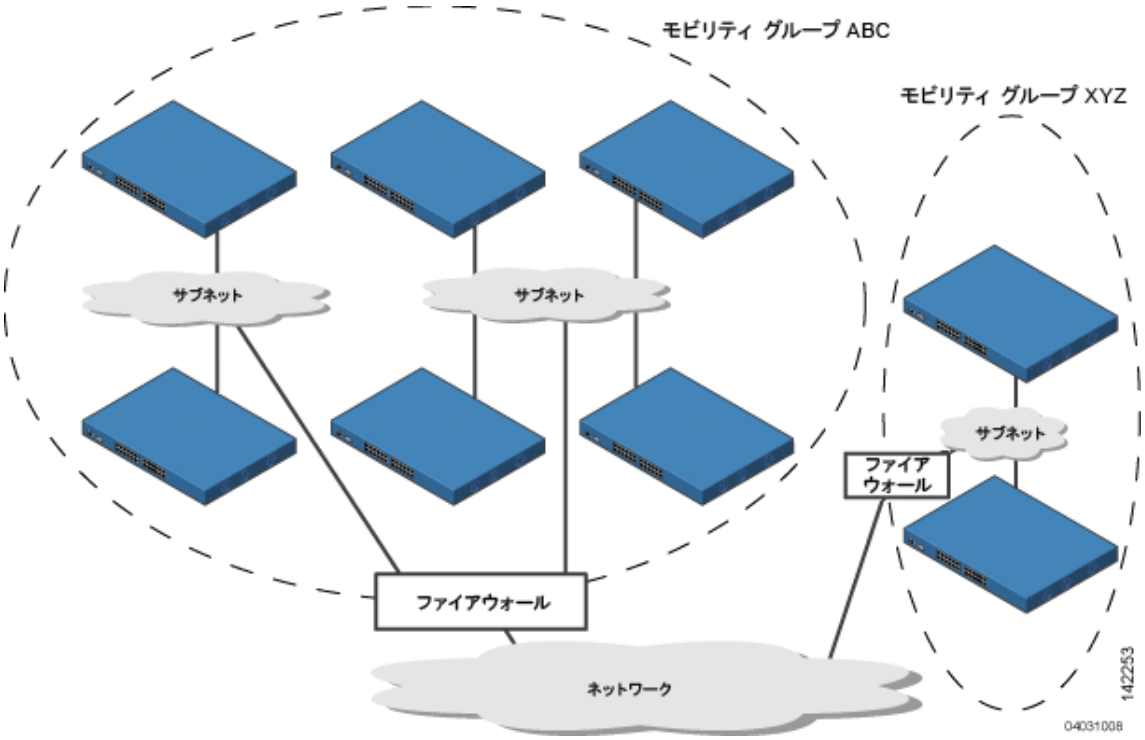
図 8-4 に示したように、各コントローラはモビリティ グループの別メンバのリストを使用して設定されています。新たなクライアントがコントローラに追加されると、コントローラはユニキャスト メッセージをそのモビリティ グループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを送信します。コントローラ間のすべてのモビリティ交換トラフィックが CAPWAP トンネルで実行されます。

次に、例を示します。

1. 4404-100 コントローラは、最大 100 台のアクセス ポイントをサポートします。したがって、24 個の 4404-100 コントローラで構成されているモビリティ グループは、最大 2400 個のアクセス ポイント（24 * 100 = 2400 アクセス ポイント）をサポートします。
2. 4402-25 コントローラは最大 25 台のアクセス ポイントをサポートし、4402-50 コントローラは最大 50 台のアクセス ポイントをサポートします。したがって、12 個の 4402-25 コントローラと 12 個の 4402-50 コントローラで構成されたモビリティ グループは最大 900 個のアクセス ポイント（12 * 25 + 12 * 50 = 300 + 600 = 900 アクセス ポイント）をサポートします。

異なるモビリティ グループ名を同じ無線ネットワーク内の異なるコントローラに割り当てると、モビリティ グループによって、1 つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。図 8-5 には、2 つのコントローラ グループに異なるモビリティ グループ名を作成した結果が示されています。

図 8-5　　2 つのモビリティ グループ



ABC モビリティ グループのコントローラは、アクセス ポイントと共有サブネットを使用して相互に認識しあい、通信します。ABC モビリティ グループのコントローラは、異なるモビリティ グループの XYZ コントローラを認識せず、通信を行いません。同様に、XYZ モビリティ グループのコントローラは、ABC モビリティ グループのコントローラを認識せず、通信を行いません。この機能により、ネットワークでのモビリティ グループの切り離しが確実に行われます。

（注）　クライアントは、異なるモビリティ グループのアクセス ポイントを検出できる場合は、そのアクセス ポイント間のローミングを行う場合があります。ただし、そのセッション情報は異なるモビリティ グループのコントローラ間では伝送されません。

モビリティ グループにコントローラを追加するタイミング

ネットワーク内の無線クライアントが、あるコントローラに接続したアクセス ポイントから、別のコントローラに接続したアクセス ポイントへローミングできるとしたら、どちらのコントローラも同じモビリティ グループに属しているはずです。

モビリティ グループ内でのメッセージング

コントローラでは、モビリティ メッセージを他のメンバ コントローラに送信することにより、クライアントにサブネット間モビリティが提供されます。リリース 5.1 以降のコントローラ ソフトウェアでは、モビリティ リストで 72 台までのコントローラをサポートします。すべてのリリースにわたって、

モビリティ グループで 24 台までのコントローラをサポートしています。Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、モビリティ メッセージングに対して 2 つの改良が行われました。いずれも、モビリティ メンバの全リストにメッセージを送信する場合に役立ちます。

- Mobile Announce メッセージを、まず同じグループ内に送信してから、リスト内の他のグループに送信する

  コントローラは、新しいクライアントがアソシエートされるたびに、モビリティ リスト内のメンバに Mobile Announce メッセージを送信します。Prime Infrastructure および 5.0 よりも前のコントローラ ソフトウェア リリースでは、コントローラは所属グループに関係なく、このメッセージをリスト内のすべてのメンバに送信します。しかし、コントローラ ソフトウェア リリース 5.0 では、コントローラは自分と同じグループに属するメンバーに対してだけメッセージを送信し、その後、再試行を送信しながら、他のメンバーをすべて加えます。

- ユニキャストではなくマルチキャストを使用して Mobile Annouce メッセージを送信する

  Prime Infrastructure および 5.0 よりも前のコントローラ ソフトウェア リリースでは、コントローラはマルチキャストを使用して、Mobile Announce メッセージを送信するように設定される場合がありますが、これには、すべてのモビリティ メンバにメッセージのコピーを送信する必要があります。多くのメッセージ（Mobile Announce、PMK Update、AP List Update、IDS Shun など）はグループ内のすべてのメンバに向けられたものなので、この動作は効率的ではありません。Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、コントローラでマルチキャスト モードを使用して Mobile Announce メッセージを送信します。これにより、コントローラからネットワークに送られるメッセージは 1 コピーのみになります。このコピーはモビリティ メンバすべてを含むマルチキャスト グループに宛てて送られます。マルチキャスト メッセージングを最大限生かすには、グループ メンバすべてに対してこの機能を有効または無効にすることを推奨します。

モビリティ グループの設定

この項では、モビリティ グループを設定する方法について説明します。

（注） コントローラを使用してモビリティ グループを設定することもできます。手順については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

前提条件

コントローラをモビリティ グループに追加する前に、グループに追加するコントローラすべてについて、次の要件が満たされていることを確認する必要があります。

- すべてのコントローラには同じ LWAPP モードを設定する必要があります（レイヤ 2 またはレイヤ 3）。

  （注） [System] > [General] ページで LWAPP 転送モードを確認し、必要に応じて LWAPP 転送モードを変更できます。

- すべてのデバイスの管理インターフェイス間に IP 接続が存在する必要があります。

  （注） コントローラに対し Ping することで、IP 接続を確認できます。

- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。

（注）　Cisco WiSM の場合、300 のアクセス ポイント間のルーティングをシームレスにするために両方のコントローラを同じモビリティ グループ名で設定してください。

- すべてのデバイスを、同じ仮想インターフェイス IP アドレスに設定する必要があります。

（注）　モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイスを使用していない場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

- モビリティ グループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報は、すべてのコントローラにモビリティ グループの他のすべてのメンバの MAC アドレスと IP アドレスを設定するために必要です。

（注）　モビリティ グループに追加する他のコントローラの MAC アドレスと IP アドレスは、[Configure] > [Controllers] ページにあります。

モビリティ グループにそれぞれの WLC コントローラを追加して設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

このページでは、ステップ 1 で追加したすべてのコントローラの一覧が表示されます。モビリティ グループ名、および現在モビリティ グループのメンバーとなっている各コントローラの IP アドレスが一覧表示されます。

ステップ 2　WLC IP アドレスをクリックして最初のコントローラを選択します。その後、管理しているコントローラのコントローラ テンプレートのインターフェイスにアクセスします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Mobility Groups] の順に選択します。既存のモビリティ グループ メンバがページに一覧表示されます。

ステップ 4　使用可能なコントローラの一覧が表示されます。画面右上の [Select a command] ドロップダウン リストから [Add Group Members] を選択し、[Go] をクリックします。

ステップ 5　モビリティ グループに追加するコントローラが見つからない場合は、[To add members manually to the Mobility Group click here] リンクをクリックして手動でメンバを追加できます。[Mobility Group Member] ページが表示されます。

ステップ 6　[Member MAC Address] テキスト ボックスに、追加するコントローラの MAC アドレスを入力します。

ステップ 7　[Member IP Address] テキスト ボックスに、追加するコントローラの管理インターフェイスの IP アドレスを入力します。

（注）　ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

ステップ 8　マルチキャスト モビリティ メッセージに使用するマルチキャスト グループ IP アドレスを [Multicast Address] テキスト ボックスに入力します。ローカル モビリティ メンバのグループ アドレスは、ローカル コントローラのグループ アドレスと同じである必要があります。

ステップ 9　[Group Name] テキスト ボックスに、モビリティ グループ名を入力します。

ステップ 10　[Save] をクリックします。

ステップ 11　残りの WLC デバイスに対してステップ 1 ～ 9 を繰り返します。

モビリティ スケーラビリティ パラメータの設定

モビリティ メッセージ パラメータを設定するには、次の手順を実行します。

（注）　モビリティ スケーラビリティ パラメータを設定する前に、「モビリティ グループの設定」（P.8-270）の手順を実行する必要があります。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　ソフトウェア バージョンが 5.0 以降のコントローラの IP アドレスを選択します。

ステップ 3　左側のサイドバーのメニューから、[System] > [Multicast] の順に選択します。[Multicast] ページが表示されます。

ステップ 4　[Ethernet Multicast Support] ドロップダウン リストから、コントローラがマルチキャスト モードを使用して Mobile Announce メッセージをモビリティ メンバに送信する機能を無効にするかどうかを指定します。または、ドロップダウン リストから [Multicast] または [Unicast] を選択します。

ステップ 5　ステップ 4 でマルチキャストを選択した場合、[Multicast Group Address] フィールドでグループ IP アドレスを入力してマルチキャスト モビリティ メッセージングを開始する必要があります。この IP アドレスをローカル モビリティ グループに対して設定する必要がありますが、モビリティ リスト内のその他のグループではオプションとなります。その他の（非ローカル）グループに IP アドレスを設定しない場合、コントローラはユニキャスト モードを使用してこれらのメンバーにモビリティ メッセージを送信します。

ステップ 6　[Global Multicast Mode] チェックボックスをオンにして、マルチキャスト モードがグローバルに使用できるようにします。

ステップ 7　[Enable IGMP Snooping] チェックボックスをオンにして、IGMP スヌーピングを有効にします。

ステップ 8　[Multicast Mobility Mode] ドロップダウン リストから [Enable] を選択して、IGMP スヌーピング ステータスを変更するか、または IGMP タイムアウトを設定します。IGMP スヌーピングが有効の場合、コントローラはクライアントから IGMP レポートを収集した後、いずれかのマルチキャスト グループをリッスンしているクライアントのリストをアクセス ポイントに送信します。その後、アクセス ポイントはこれらのクライアントのみにマルチキャスト パケットを転送します。

タイムアウト間隔の範囲は 3 ～ 300 で、デフォルト値は 60 です。タイムアウトが経過すると、コントローラはすべての WLAN に対してクエリーを送信します。その後、マルチキャスト グループ内でリッスンしているクライアントは、コントローラにパケットを送り返します。

ステップ 9　マルチキャスト モビリティ モードを有効にしている場合は、モビリティ グループ マルチキャスト アドレスを入力します。

ステップ 10　[Multicast Direct] チェックボックスをオンにして、ワイヤレス ネットワークでビデオがストリームされるようにします。

ステップ 11　セッション バナー情報を指定します。これは、クライアントがメディア ストリームから拒否またはドロップされた場合に、クライアントに送信されるエラー情報です。

a. [State] : セッション バナーをアクティブにする場合は、このチェックボックスをオンにします。アクティブにしない場合、セッション バナーはクライアントに送信されません。

b. [URL] : クライアントにレポートされる Web アドレス

c. [Email] : クライアントにレポートされる電子メール アドレス

d. [Phone] : クライアントにレポートされる電話番号

e. [Note] : クライアントにレポートされる注意

（注）　コントローラ上のすべてのメディア ストリームは、この設定を共有します。

ステップ 12　[Save] をクリックします。

モビリティ アンカー

モビリティ アンカーは、WLAN のアンカー コントローラとして指定されるモビリティ グループのサブセットです。この機能は、クライアントのネットワークへのエントリ ポイントに関係なく、WLAN を 1 つのサブネットに制限する際に使用されます。これによって、ユーザは企業全体にわたりパブリック WLAN やゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。また、WLAN は建物の特定のセクション（ロビー、レストランなど）を表すことができるため、ゲスト WLAN で地理的ロード バランシングを実現できます。

クライアントが WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティ グループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが、WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、ローカル セッションがクライアントのために作成され、コントローラは同じモビリティ グループの別のコントローラへ通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに連絡をとり、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは EtherIP を使用してモビリティ トンネルを介してカプセル化され、アンカー コントローラに送信されます。ここでカプセルを解除されて有線ネットワークへ配信されます。クライアントへのパケットは、アンカー コントローラで受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットのカプセルを解除し、クライアントへ転送します。

（注）　2000 シリーズ コントローラを WLAN のアンカーとして指定できません。ただし、2000 シリーズ コントローラ上に作成された WLAN に 4100 シリーズ コントローラまたは 4400 シリーズ コントローラをアンカーとして指定できます。

（注）　L2TP レイヤ 3 セキュリティ ポリシーは、モビリティ アンカーで設定された WLAN には使用できません。

モビリティ アンカーの設定

WLAN の新しいモビリティ アンカーを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　IP アドレスをクリックしてコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。

ステップ 4　目的の WLAN ID URL のチェックボックスをオンにします。

ステップ 5　WLAN ID を選択すると、タブ付きのページが表示されます。[Advanced] タブをクリックします。

ステップ 6　ページ下部の [Mobility Anchors] リンクをクリックします。[Mobility Anchors] ページが表示されます。

ステップ 7　モビリティ アンカーとして指定するコントローラの IP アドレス チェックボックスをオンにして、[Save] をクリックします。

ステップ 8　ステップ 6 とステップ 7 を繰り返し、その他のコントローラをこの WLAN のアンカーとして設定します。

ステップ 9　モビリティ グループのすべてのコントローラに同じセットのアンカー コントローラを設定します。

複数の国コードの設定

1 つまたは複数の国をコントローラに設定できます。国をコントローラに設定すると、対応する 802.11a/n DCA チャネルが選択可能になります。少なくとも 1 つの DCA チャネルを、802.11a/n ネットワークに対して選択する必要があります。国コードが変更されると、DCA チャネルも連携して自動的に変更されます。

（注）　コントローラの 802.11a/n および 802.11b/n のネットワークとアクセス ポイントを無効にしてから、コントローラ上で国を設定してください。802.11a/n または 802.11b/n のネットワークを無効にするには、[Configure] > [Controllers] の順に選択し、無効にする目的のコントローラを選択し、[802.11a/n] または [802.11b/g/n] を左側のサイドバーのメニューから選択して、さらに [Parameters] を選択します。[Network Status] が最初のチェックボックスです。

（注）　モビリティ グループ外の複数の国コードを設定するには、「セキュリティ パラメータの設定」（P.9-379）を参照してください。

設定グループで定義された複数のコントローラを追加して DCA チャネルを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから [Add Config Groups] を選択し、[Go] をクリックします。

ステップ 3　グループ名およびモビリティ グループ名を入力して、設定グループを作成します。

ステップ 4　[Save] をクリックします。[Config Groups] ページが表示されます。

ステップ 5　[Controllers] タブをクリックします。[Controllers] ページが表示されます。

ステップ 6　追加するコントローラを強調表示して、[Add] をクリックします。コントローラが [Group Controllers] ページに追加されます。

ステップ 7　[Country/DCA] タブをクリックします。[Country/DCA] ページが表示されます。DCA により、コントローラに接続された管理対象デバイスの中から妥当なチャネルの割り当てが自動的に選択されます。

ステップ 8　[Update Country/DCA] チェックボックスをオンにして、選択する国の一覧を表示します。

ステップ 9　同じモビリティ グループのコントローラ上で現在設定されている DCA チャネルが、[Select Country Codes] ページに表示されます。選択した国に割り当て可能な対応チャネル（802.11a/n および 802.11b/n）も表示されます。一覧に記載されているチャネルを追加または削除するには、チャネルを選択または選択解除して、[Save Selection] をクリックします。

（注）　最低 1 か国および最高 20 か国を、1 つのコントローラに設定できます。

コントローラ設定グループの設定

設定グループを作成することで、同じモビリティ グループ名および類似する設定を持つ必要のあるコントローラをグループ化できます。テンプレートをグループに割り当てて、テンプレートをグループ内のすべてのコントローラに適用できます。設定グループを追加、削除、または解除することができ、ソフトウェア、IDS シグニチャ、またはカスタマイズした Web 認証ページを、選択した設定グループのコントローラにダウンロードできます。また、現在の設定を、選択した設定グループのコントローラの不揮発性（フラッシュ）メモリに保存することもできます。

（注）　コントローラは、複数のモビリティ グループのメンバーにはできません。コントローラをあるモビリティ グループに追加すると、すでにメンバーとなっている別のモビリティ グループからそのコントローラが削除されます。

個々のコントローラまたは選択した設定グループのコントローラへのテンプレートの適用の詳細については、「テンプレートの使用」（P.11-601）を参照してください。

[Configure] > [Controller Config Groups] を選択すると、Prime Infrastructure データベースのすべての設定グループの概要を表示できます。[Select a command] ドロップダウン リストから [Add Config Groups] を選択すると、ページに次の列を持つ表が表示されます。

- [Group Name]：設定グループの名前。
- [Templates]：設定グループに適用するテンプレートの数。
-

新しいグループの追加

設定グループを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Config Group] を選択し、[Go] をクリックします。[Add New Group] ページが表示されます。

ステップ 3　新しい設定グループ名を入力します。これは全グループで一意である必要があります。[Enable Background Audit] を選択すると、この設定グループのネットワークとコントローラの監査が発生します。[Enable Enforcement] を選択すると、何らかの矛盾が見つかった場合、監査中にテンプレートが自動的に適用されます。

（注）　[Enable Background Audit] オプションを選択すると、この設定グループのネットワークとコントローラの監査が実行されます。

ステップ 4　Prime Infrastructure で作成されたその他のテンプレートを、設定グループに割り当てることができます。同じ WLAN テンプレートを、1 つ以上の設定グループに割り当てできます。次の中から選択します。

- [Select and add later]：後でテンプレートを追加するためにクリックします。
- [Copy templates from a controller]：別のコントローラからテンプレートをコピーするためにクリックします。現在のコントローラ一覧からコントローラを選択して、それに適用されているテンプレートを新しい設定グループにコピーします。テンプレートだけがコピーされます。

（注）　無線テンプレートを使用する場合、テンプレートの順序が重要になります。たとえば、テンプレート リストに無線テンプレートが含まれ、無線パラメータを適用する前に無線ネットワークを無効にする必要がある場合、まず無線ネットワークを無効にするテンプレートをテンプレートに追加する必要があります。

ステップ 5　[Save] をクリックします。[Config Groups] ページが表示されます。

設定グループの設定

設定グループを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択して、[Group Name] 列でグループ名をクリックします。[Config Group] ページが表示されます。

ステップ 2　[General] タブをクリックします。次のような設定グループのオプションが表示されます。

- [Group Name]：設定グループの名前。
  - [Enable Background Audit]：このグループに含まれるすべてのテンプレートが、ネットワークとコントローラの監査中にコントローラに対して監査されます。
  - [Enable Enforcement] ：何らかの矛盾が見つかった場合、監査中にテンプレートが自動的に適用されます。

    （注）　選択した監査モードが [Template based audit] の場合、設定グループのテンプレートの監査と施行が行われます。

  - [Enable Mobility Group]：モビリティ グループ名がグループ内のすべてのコントローラに適用されます。
- [Mobility Group Name]：グループ内のすべてのコントローラに適用されるモビリティ グループ名。モビリティ グループ名はここで変更することもできます。

（注）　コントローラを複数の設定グループに含むことができます。

- [Last Modified]：設定グループを最後に変更した日付と時刻。
- [Last Applied]：最後に変更を適用した日付と時刻。

ステップ 3　[Apply/Schedule] タブをクリックして、指定したモビリティ グループ名をグループのコントローラに配信し、グループの各コントローラでモビリティ グループ メンバを作成する必要があります。

ステップ 4　[Save] をクリックします。

設定グループのコントローラの追加または削除

設定グループのコントローラを追加または削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択して、[Group Name] 列でグループ名をクリックします。

ステップ 2　[Controllers] タブをクリックします。このテーブルの列にはコントローラの IP アドレス、コントローラが含まれる設定グループの名前、コントローラのモビリティ グループ名が表示されます。

ステップ 3　グループに追加したいコントローラの行をクリックして強調表示させます。

ステップ 4　[Add] をクリックします。

（注）　グループからコントローラを削除する場合は、[Group Controllers] ボックスのコントローラを強調表示させ、[Remove] ボタンをクリックします。

ステップ 5　設定グループのコントローラを追加または削除するには、[Apply/Schedule] タブをクリックしてから [Apply] をクリックする必要があります。

ステップ 6　[Save Selection] をクリックします。

設定グループのテンプレートの追加または削除

設定グループのテンプレートを追加または削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択して、[Group Name] 列でグループ名をクリックします。

ステップ 2　[Templates] タブをクリックします。[Remaining Templates] テーブルに、使用可能なすべてのテンプレートの項目番号、テンプレート名、およびテンプレートの種類と使用方法が表示されます。

ステップ 3　グループに追加したいテンプレートの行をクリックして強調表示させます。

ステップ 4　[Add] をクリックして、強調表示されたテンプレートを [Group Templates] 列に移動します。

（注）　グループからテンプレートを削除する場合は、[Remaining Templates] ボックスのテンプレートを強調表示させ、[Remove] をクリックします。

ステップ 5　設定グループのテンプレートを追加または削除するには、[Apply/Schedule] タブをクリックしてから [Apply] をクリックする必要があります。

ステップ 6　[Save Selection] をクリックします。

設定グループの適用またはスケジューリング

（注）　スケジューリング機能を使用して、プロビジョニングの開始日および開始時刻をスケジューリングできます。

モビリティ グループ、モビリティ メンバ、およびテンプレートを設定グループのすべてのコントローラに適用するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択して、[Group Name] 列でグループ名をクリックします。

ステップ 2　[Apply/Schedule] タブをクリックして、このページにアクセスします。

ステップ 3　[Apply] をクリックして、モビリティ グループ、モビリティ メンバー、およびテンプレートのプロビジョニングを、設定グループのすべてのコントローラに対して開始します。適用後には、このページを離れたり、Prime Infrastructure からログアウトすることができます。プロセスは継続され、後でこのページに戻りレポートを表示できます。

（注）　プロビジョニングの適用時は、その他の設定グループの機能は実行しないでください。

レポートが生成され、[Recent Apply Report] ページに表示されます。どのモビリティ グループ、モビリティ メンバー、またはテンプレートが各コントローラに適用されたかが表示されます。

（注）　ページに表示されたとおりにレポートを印刷するには、ページの印刷の向きに横を選択する必要があります。

ステップ 4　テキスト ボックスに開始日を入力するか、カレンダーのアイコンを使用して開始日を選択します。

ステップ 5　開始時刻を、[hours] および [minutes] ドロップダウン リストを使用して選択します。

ステップ 6　[Schedule] をクリックして、スケジューリングした時間にプロビジョニングを開始します。

設定グループの監査

[Config Groups Audit] ページを使用して、コントローラの設定がグループのテンプレートおよびモビリティ グループに従っているかどうかを確認します。監査中は、この画面を離れたり、Prime Infrastructure からログアウトしたりできます。プロセスは継続され、後でこのページに戻りレポートを表示できます。

（注）　監査中は、その他の設定グループの機能は実行しないでください。

設定グループ監査を実行するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択して、[Group Name] 列でグループ名をクリックします。

ステップ 2　[Audit] タブをクリックして、このページにアクセスします。

ステップ 3　[Controllers] タブからコントローラをクリックして強調表示し、[>> (Add)] および [Save Selection] を選択します。

ステップ 4　[Templates] タブからテンプレートをクリックして強調表示し、[>> (Add)] および [Save Selection] を選択します。

ステップ 5　[Audit] をクリックして、監査プロセスを開始します。

レポートが生成され、各コントローラの現在の設定が設定グループのテンプレートに準拠します。レポートには監査ステータス、同期テンプレートの数、非同期テンプレートの数が表示されます。

（注）　この監査では、デバイスに対して Prime Infrastructure 設定は強制されません。矛盾の識別だけを行います。

ステップ 6　[Details] をクリックして、[Controller Audit Report] の詳細を表示します。

ステップ 7　項目をダブルクリックして、[Attribute Differences] ページを開きます。このページには属性、Prime Infrastructure の属性値、コントローラの属性値が表示されます。

（注）　[Retain Prime Infrastructure Value] をクリックして、[Attribute Differences] ページのすべての属性をデバイスに適用します。

ステップ 8　[Close] をクリックして、[Controller Audit Report] ページに戻ります。

•

設定グループのリブート

設定グループをリブートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択して、[Group Name] 列でグループ名をクリックします。

ステップ 2　[Reboot] タブをクリックします。

ステップ 3　一度に 1 つのコントローラをリブートして、そのコントローラが起動されるまで次のコントローラのリブートを待つ場合は、[Cascade Reboot] チェックボックスをオンにします。

ステップ 4　[Reboot] をクリックして、設定グループのすべてのコントローラを一度にリブートします。リブート中は、このページを離れたり、Prime Infrastructure からログアウトしたりできます。プロセスは継続され、後でこのページに戻りレポートを表示できます。

[Recent Reboot Report] ページに、各コントローラがリブートされた時間、リブート後のコントローラのステータスが表示されます。Prime Infrastructure がコントローラをリブートできない場合は、失敗が表示されます。

（注）　ページに表示されたとおりにレポートを印刷するには、ページの印刷の向きに横を選択する必要があります。

設定グループのレポート

指定のグループ名で最近適用されたすべてのレポートを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択して、[Group Name] 列でグループ名をクリックします。

ステップ 2　[Report] タブをクリックします。[Recent Apply Report] ページには、適用ステータス、適用が開始された日時、テンプレート数などを示す、最近適用されたレポートがすべて表示されます。各 IP アドレスに関する次の情報が表示されます。

- [Apply Status] : Success（成功）、Partial Success（一部成功）、Failure（失敗）、Not Initiated（未開始）を示します。
- [Successful Templates] : 該当する IP アドレスに関連する正常なテンプレートの数を示します。
- [Failures] : コントローラに対するモビリティ グループ、モビリティ メンバー、およびテンプレートのプロビジョニングの失敗数を示します。
- [Details] : [Details] をクリックすると、それぞれの失敗と関連するエラー メッセージが表示されます。

ステップ 3　スケジューリングされたタスク レポートを表示するには、ページ下部の [click here] リンクをクリックします。すると、[Configure] > [Scheduled Configuration Tasks] > [Config Group] メニューにリダイレクトし、スケジューリングされた設定グループのレポートを表示できます。

ソフトウェアのダウンロード

設定グループの作成後に、選択したグループのすべてのコントローラにソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択します。

ステップ 2　[Config Groups] ページで、選択する 1 つ以上の設定グループ名のチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから次のいずれかを選択し、[GO] をクリックします。

- Download Software (TFTP)
- Download Software (FTP)
- Download Software (SFTP)

[Download Software to Controller] ページが表示されます。バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。[File is Located On] フィールドから [local machine] を選択します。

ステップ 4　ダウンロード タイプを指定します。

ステップ 5　TFTP、FTP、SFTP サーバのサーバ詳細を入力します。

ステップ 6　[Download] をクリックします。

IDS シグニチャのダウンロード

設定グループからローカル TFTP サーバへ侵入検知システム（IDS）のシグニチャ ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択します。

ステップ 2　[Config Groups] ページで、選択する 1 つ以上の設定グループのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Download IDS Signatures] を選択し、[Go] をクリックします。

ステップ 4　[Download IDS Signatures to Controller] ページが表示されます。バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。[File is Located On] フィールドから [local machine] を選択します。

ステップ 5　[Maximum Retries] フィールドに、コントローラがシグニチャ ファイルのダウンロードを試みる最大回数を入力します。

ステップ 6　[Timeout] フィールドに、シグニチャ ファイルのダウンロードを試行する際、コントローラがタイムアウトになるまでの最大時間を秒単位で入力します。

ステップ 7　ファイルは /localdisk/tftp ディレクトリにアップロードされます。そのディレクトリ内のローカル ファイル名を指定するか、[Browse] をクリックしてナビゲートします。コントローラはベース ネームとしてこのローカル ファイル名を使用してから、サフィクスとして _custom.sgi を追加します。

何らかの理由で転送がタイムアウトになった場合、単に [File Is Located On] フィールドで [TFTP server] オプションを選択できます。サーバ ファイル名が自動的に入力され、再試行されます。

ステップ 8　[OK] をクリックします。

カスタマイズされた WebAuth のダウンロード

カスタマイズされた Web 認証をダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択します。

ステップ 2　[Config Groups] ページで、選択する 1 つ以上の設定グループのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Download Customized WebAuth] を選択し、[Go] をクリックします。

ステップ 4　[Download Customized Web Auth Bundle to Controller] ページが表示されます。バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。

ステップ 5　[File is Located On] フィールドから [local machine] を選択します。

デバイスの設定

この章では、Prime Infrastructure データベースにデバイスを設定する方法について説明します。ここで説明する内容は、次のとおりです。

コントローラの設定

ここでは、Prime Infrastructure データベースにコントローラを設定する方法について説明します。

[Configure] > [Controllers] を選択して、次にアクセスします。

- Prime Infrastructure データベースのすべてのコントローラの概要。
- 選択したコントローラを追加、削除、およびリブートする機能。
- 選択したコントローラに Prime Infrastructure サーバからソフトウェアをダウンロードする機能。
- 選択したコントローラ上の不揮発性（フラッシュ）メモリに現在の設定を保存する機能。
- 選択したコントローラの監査レポートを表示する機能。

コントローラのデータ テーブルには、次の列が含まれています。

- [Check box]：該当するコントローラを選択します。
- [IP Address]：コントローラ管理インターフェイスのローカル ネットワーク IP アドレス。

  - タイトルをクリックすると、リスト項目がソートされます。
  - いずれかのリスト項目をクリックすると、その IP アドレスのパラメータが表示されます。「コントローラのプロパティの設定」（P.9-308）を参照してください。
  - IP アドレスの右側のアイコンをクリックすると、コントローラの Web ユーザ インターフェイスが新しいブラウザ ウィンドウで表示されます。
- [Device Name]：コントローラの名前を示します。[Controller Name] リンクをクリックすると、コントローラ名でリストがソートされます。
- [Device Type]：クリックすると、タイプでソートされます。デバイス タイプは、シリーズでグループ化されています。次に例を示します。
  - [WLC2100]：21xx シリーズ ワイヤレス LAN コントローラ
  - [2500]：25xx シリーズ ワイヤレス LAN コントローラ
  - [4400]：44xx シリーズ ワイヤレス LAN コントローラ
  - [5500]：55xx シリーズ ワイヤレス LAN コントローラ
  - [7500]：75xx シリーズ ワイヤレス LAN コントローラ
  - [WiSM]：WiSM（スロット番号、ポート番号）
  - [WiSM2]：WiSM2（スロット番号、ポート番号）
- [Location]：コントローラの場所を示します。
- [Software Version]：現在コントローラで実行されているコードのオペレーティング システム release.version.dot.maintenance 番号。
- [Mobility Group Name]：モビリティまたは WPS グループの名前。
- [Reachability Status]：到達可能または到達不能。

（注）　デバイス ステータスのバックグラウンド タスクの最後の実行情報に基づいて、到達可能性ステータスが更新されます。現在のステータスをアップデートするには、[Administration] > [Background Tasks] を選択して、[Select a command] ドロップダウン リストから [Execute Now] を選択します。

- Audit Status
  - [Not Available]：このスイッチでは監査は実行されていません。
  - [Identical]：設定の相違は見つかりませんでした。
  - [Mismatch]：設定の相違が見つかりました。

  [Audit Status] リンクをクリックして、監査レポートにアクセスします。[Audit Report] ページで [Select a command] ドロップダウン リストから [Audit Now] を選択して、このコントローラに対して新たに監査を実行します。監査レポートの詳細については、「コントローラ監査レポートについて」（P.9-285）を参照してください。

（注）　監査ステータスは、設定の同期バックグラウンド タスクまたは [Controllers] ページの [Audit Now] オプションのいずれかの、最新の実行情報に基づいてアップデートされます。現在のステータスを確認するには、[Administration] > [Background Tasks] を選択し、[Select a command] ドロップダウン リストから [Execute Now] または [Audit Now] を選択します。

（注）　特定のコントローラを検索するには、検索機能を使用します。詳細については、「検索機能の使用方法」（P.2-54）を参照してください。

ここでは、次の内容について説明します。

コントローラ監査レポートについて

コントローラ監査レポートには、[Administration] > [Settings] > [Audit] で選択した監査のタイプ、および監査の実行で使用されたパラメータに基づいて、次の情報が表示されます。

- 適用されたテンプレートの矛盾（Template Based Audit のみ）
- 設定グループのテンプレートの矛盾（Template Based Audit のみ）
- バックグラウンドの監査が有効な設定グループの全体の施行（Template Based Audit のみ）
  - 全体の施行数が 0 より大きい場合、この数値はリンクとして表示されます。このリンクをクリックすると、Prime Infrastructure から行われた施行のリストが表示されます。
- バックグラウンドの監査が有効な設定グループの障害（Template Based Audit のみ）
  - 全体の障害数が 0 より大きい場合、この数値はリンクとして表示されます。リンクをクリックすると、デバイスから返された障害が表示されます。
- その他の Prime Infrastructure の矛盾

（注）　コントローラ監査レポートには、監査がすべてのパラメータに基づいて実行されたか、または選択された一部のパラメータに基づいて実行されたかが示されます。

（注）　2 種類の監査、および監査の特定のパラメータを管理する方法に関する詳細については、「監査の設定」（P.15-853）を参照してください。

現在のコントローラ監査レポートには、[Configure] > [Controllers] ページの [Audit Status] 列で値をクリックすることでアクセスできます。

[Configure] > [Controllers] ページの [Select a command] ドロップダウン リストから [Audit Now] を選択するか（詳細は「[Audit Now] 機能の使用」（P.9-305）を参照してください）、またはコントローラ監査レポートで [Audit Now] をクリックすると、コントローラを監査できます。

コントローラの追加

コントローラは 1 つずつまたはバッチで追加することができます。

コントローラを追加する手順は次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Controllers] を選択し、[Go] をクリックします。[Add Controller] ページが表示されます。

ステップ 3　次のいずれかを選択します。

1 つのコントローラを追加するか、カンマを使用して複数のコントローラを区切る場合は、[Add Format Type] ドロップダウン リストを [Device Info] のままにします。

CSV ファイルのインポートにより複数のコントローラを追加する場合は、[Add Format Type] ドロップダウン リストから [File] を選択します。CSV ファイルを使用すると、独自のインポート ファイルを生成して必要に応じてデバイスを追加できます。

（注）　システムからコントローラが削除されても、アソシエートされたアクセス ポイントは自動的に削除されず、システムに残ります。これらのアソシエーションが解除されたアクセス ポイントは、手動で削除する必要があります。

（注）　パケットを複数のフラグメントに分割し、IPsec を利用して GRE リンクを越える、または小さい MTU のリンクを越えて Prime Infrastructure にコントローラを追加する場合は、Maximum VarBinds per Get PDU および Maximum VarBinds per Set PDU の調整が必要な場合があります。設定されている値が高すぎる場合は、Prime Infrastructure へのコントローラの追加は失敗する場合があります。Maximum VarBinds per Get PDU または Maximum VarBinds per Set PDU を調整するには、Prime Infrastructure を停止し、[Administration] > [Settings] > [SNMP Settings] の順に選択して、[Maximum VarBinds per Get PDU] および [Maximum VarBinds per Set PDU] の値を 50 以下に編集します。

（注）　[Maximum VarBinds per Get PDU] または [Maximum VarBinds per Set PDU] の値を下げると、デバイスへの設定の適用が失敗する場合があります。

ステップ 4　[Device Info] を選択した場合は、追加するコントローラの IP アドレスを入力します。複数のコントローラを追加するには、IP アドレスの文字列の間にカンマを使用します。

（注）　可変長サブネット マスクとしては正しいホスト アドレスであっても、可変長サブネット マスクを考慮しないバイト境界のブロードキャスト アドレスとして見なされ、Prime Infrastructure へのコントローラの追加には制限があります。たとえば、10.0.2.255/23 は追加できませんが、10.0.2.254/23 は追加できます。

[File] を選択した場合は、[Browse] をクリックしてインポートする CSV ファイルの場所を探します。

CSV ファイルの最初の行は、含まれている列の説明に使用されます。CSV ファイルの最初の行は、含まれている列の説明に使用されます。IP アドレス列は必須です。次に、CSV ファイルの例を示します。

```
ip_address,network_mask,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmp
v3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,snmp_retries,snmp_timeout,pro
tocol,telnet_username,telnet_password,enable_password,telnet_timeout
209.165.200.225,255.255.255.224,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
209.165.200.226,255.255.255.224,v2,public,,,,,,3,10,,cisco,cisco,cisco,60
209.165.200.227,255.255.255.224,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
```

CSV ファイルには、次のフィールドを含めることができます。

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

ステップ 5　このコントローラで Telnet/SSH クレデンシャルを確認する場合は、[Verify Telnet/SSH Credentials] チェックボックスをオンにします。デバイスの検出には相当の時間がかかるため、これを選択しない（または無効の）ままにすることもできます。

（注）　書き込みアクセスに対応する SNMP パラメータ（使用できる場合）を入力します。読み取り専用アクセス パラメータを入力した場合、コントローラは追加されますが、Prime Infrastructure は設定を変更することはできず、また Prime Infrastructure をそのコントローラのトラップ レシーバとして登録することもできません。

ステップ 6　[Version] ドロップダウン リストから、[v1]、[v2]、[v3] のいずれかを選択します。

ステップ 7　[Retries] テキスト ボックスに、コントローラの検出を試行する回数を入力します。

ステップ 8　クライアントのセッション タイムアウト値を秒単位で入力します。この値により、クライアントの再認証が強制されるまでの最大時間が決定されます。

ステップ 9　[Community] フィールドに、public または private のいずれかを入力します（v1 および v2 の場合のみ）。

（注）　後でコミュニティ モードを変更する場合は、そのコントローラに対して設定リフレッシュを実行する必要があります。

ステップ 10　認証タイプについて、[None]、[HMAC-SHA]、[HMAC-MD5]（v3 の場合のみ）のいずれかを選択します。

ステップ 11　認証パスワードを入力します（v3 の場合のみ）。

ステップ 12　プライバシー タイプについて、[None]、[CBC-DES]、[CFB-AES-128]（v3 の場合のみ）のいずれかを入力します。

ステップ 13　プライバシー パスワードを入力します（v3 の場合のみ）。

ステップ 14　コントローラの Telnet クレデンシャル情報を入力します。[File] オプションを選択して複数のコントローラを追加した場合は、指定したコントローラすべてにこの情報が適用されます。CSV ファイルからコントローラを追加した場合は、ユーザ名およびパスワード情報は、CSV ファイルから取得されます。

（注）　Telnet/SSH のユーザ名は、CLI テンプレートでコマンドを実行するために十分な権限を持っている必要があります。

デフォルトのユーザ名とパスワードは admin です。

ステップ 15　再試行の回数およびタイムアウトの値を入力します。デフォルトの再試行回数は 3、デフォルトの再試行タイムアウトは 1 分です。

ステップ 16　[OK] をクリックします。

（注）　Prime Infrastructure へのデバイスの追加に失敗し、エラーメッセージ「Sparse table not supported」が表示された場合は、Prime Infrastructure と WLC のバージョンに互換性があるかどうかを確認して再試行します。バージョンの互換性の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html

（注）　コントローラが Prime Infrastructure に追加されると、Prime Infrastructure はトラップ レシーバとして動作し、802.11 ディスアソシエーション、802.11 認証解除、および 802.11 認証のトラップがコントローラで有効になります。

（注）　複数のコントローラのクレデンシャルを一括してアップデートするには、[Select a command] ドロップダウン リストから [Bulk Update Controllers] を選択します。[Bulk Update Controllers] ページが表示されます。CSV ファイルを選択できます。CSV ファイルには、アップデートするコントローラのリストを含めます（1 行につき 1 個のコントローラを記述）。各行には、コントローラの属性がカンマ区切りでリストします。最初の行は、含まれている属性の説明です。IP アドレス属性は必須です。

（注）　追加後のコントローラは、Prime Infrastructure が、追加されたコントローラとの通信を試行する間、一時的に [Monitor] > [Unknown Devices] ページに配置されます。コントローラとの通信が正常に確立されると、コントローラは [Monitor] > [Unknown Devices] ページから [Monitor] > [Controllers] ページに移動されます。Prime Infrastructure がコントローラと正常に通信できない場合、そのコントローラは [Monitor] > [Unknown Devices] に残り、エラー状態およびエラー メッセージが表示されます。[Unknown Devices] ページにアクセスするには、[Configure] > [Unknown Devices] を選択します。

コントローラ クレデンシャルの一括アップデート

CSV ファイルをインポートすることで、複数のコントローラのクレデンシャルをアップデートできます。

コントローラの情報を一括アップデートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Bulk Update Controller] を選択します。[Bulk Update Controllers] ページが表示されます。

ステップ 4　[Select CSV File] テキスト ボックスに CSV ファイル名を入力するか、または [Browse] をクリックして目的のファイルを特定します。

ステップ 5　[Update and Sync] をクリックします。

コントローラ クレデンシャルのバルク アップデート用 CSV ファイルの例

CSV ファイルの最初の行は、含まれている列の説明に使用されます。IP アドレス列は必須です。次に、CSV ファイルの例を示します。

```
ip_address,network_mask,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmp
v3_auth_password,snmpv3_privacy_type,snmpv3_privacy_password,snmp_retries,snmp_timeout,pro
tocol,telnet_username,telnet_password,enable_password,telnet_timeout
209.165.200.225,255.255.255.224,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
209.165.200.226,255.255.255.224,v2,public,,,,,,3,10,,,cisco,cisco,cisco,60
209.165.200.227,255.255.255.224,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
```

CSV ファイルには、次のフィールドを含めることができます。

- ip_address

- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- protocol
- telnet_username
- telnet_password
- enable_password
- telnet_timeout

Prime Infrastructure からのコントローラの削除

コントローラを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Remove Controllers] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　ポップアップ ダイアログボックスで [OK] をクリックして、削除を確定します。

（注）　システムからコントローラが削除されても、アソシエートされたアクセス ポイントは自動的に削除されず、システムに残ります。これらのアソシエーションが解除されたアクセス ポイントは、手動で削除する必要があります。

コントローラのリブート

コントローラをリブートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Reboot Controllers] を選択します。

ステップ 4　[Go] をクリックします。[Reboot Controllers] ページが表示されます。

（注）　リブートする前に、現在のコントローラの設定を保存します。

ステップ 5　適用する必要のある [Reboot Controller] オプションを選択します。

- [Save Config to Flash]：データはコントローラの不揮発性 RAM（NVRAM）に保存され、電源の再投入時にも保持されます。コントローラをリブートした場合、設定が保存されていないと、適用した変更はすべて失われます。
- [Reboot APs]：何らかのアップデートが実行された後、アクセス ポイントがリブートされるようにするには、このチェックボックスをオンにします。
- [Swap AP Image]：AP イメージをスワップした際に、コントローラおよび AP をリブートするかどうかを示します。[Yes] または [No] のいずれかになります。

（注）　[Reboot APs] チェックボックスがオンの場合以外は、オプションは無効になっています。

ステップ 6　[OK] をクリックして、オプションの設定を選択した状態でコントローラをリブートします。

コントローラへのソフトウェアのダウンロード

Prime Infrastructure では、ファイルのアップロードおよびダウンロードに、ファイル転送プロトコル（FTP）および Trivial File Transfer Protocol（TFTP）の両方がサポートされています。前のソフトウェア リリースでは、TFTP のみがサポートされました。

ここでは、次の内容について説明します。

- 「ソフトウェアのダウンロード（TFTP）」（P.9-291）
- 「ソフトウェアのダウンロード（FTP）」（P.9-293）
- 「ソフトウェアのダウンロード（FTP）」（P.9-293）
- 「コントローラからの IPaddr アップロード設定 / ログの設定」（P.9-298）

ソフトウェアのダウンロード（TFTP）

コントローラにソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Download Software (TFTP)] を選択します。

ステップ 4　[Go] をクリックします。

（注）　[Configure] > [Controllers] > [*IPaddr*] > [System] > [Commands] > [Upload/Download Commands] > [Download Software] の順に選択することでも、ソフトウェアをダウンロードできます。

コントローラの IP アドレスおよび現在のステータスが、[Download Software to Controller] ページに表示されます。

ステップ 5　ダウンロード タイプを選択します。

（注）　事前ダウンロード オプションは、選択したすべてのコントローラがリリース 7.0.x.x 以降を使用している場合のみ表示されます。

- [Now]：ソフトウェアのダウンロードをただちに開始します。このオプションを選択した場合は、ステップ 7 に進みます。

  （注）　ダウンロードが成功したら、コントローラをリブートして、新しいソフトウェアを有効にします。

- [Scheduled]：スケジュール設定するダウンロードオプションを指定します。
  - [Download software to controller]：ソフトウェアをコントローラにダウンロードするようにスケジュール設定するには、このオプションを選択します。
  - [Pre-download software to APs]：ソフトウェアを AP に事前ダウンロードするようにスケジュール設定するには、このオプションを選択します。AP にイメージがダウンロードされ、コントローラのリブート時に、AP もリブートされます。

    （注）　AP ごとの [Image Predownload] ステータスを確認するには、[Administration] > [Background Task] > [AP Image Predownload Task] ページでタスクを有効にし、[Report Launch Pad] から AP Image Predownload レポートを実行します。

ステップ 6　[Download type] の下で [Scheduled] オプションを選択した場合は、スケジュールの詳細を入力します。

- [Task Name]：スケジュール設定済みタスク名を入力して、当該のスケジュール設定済みソフトウェア ダウンロード タスクを特定します。
- [Reboot Type]：リブート タイプが手動、自動、またはスケジュール設定済みかどうかを示します。

  （注）　[Download software to controller] オプションだけを選択した場合は、[Reboot Type] を自動に設定できます。

- [Download date/time]：表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。
- [Reboot date/time]：このオプションは、リブート タイプで [Scheduled] を選択した場合のみ表示されます。表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、コントローラをリブートする日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。

  （注）　すべての AP がソフトウェアの事前ダウンロードを完了できるように、ダウンロードとリブートの間に十分な時間（少なくとも 30 分）をスケジュール設定します。

（注）　スケジュール設定されたリブート時刻に、いずれかの AP で事前ダウンロードが進行中の場合、コントローラはリブートしません。そのような場合は、すべての AP の事前ダウンロードが終了するまで待機し、コントローラを手動でリブートします。

- [Notification]（任意）：電子メールで通知を送信する受信者の電子メール アドレスを入力します。

（注）　電子メール通知を受信するには、[Administration] > [Settings] > [Mail Server Configuration] ページで Prime Infrastructure メール サーバを設定します。

ステップ 7　[File is located on] フィールドで、[Local machine] または [TFTP server] を選択します。

（注）　TFTP サーバを選択した場合は、デフォルト サーバを選択するか、[Server Name] ドロップダウン リストを使用して新しいサーバを追加します。

ステップ 8　[Maximum Retries] フィールドに、コントローラによるソフトウェアのダウンロードの最大試行回数を入力します。

ステップ 9　[Timeout] フィールドに、コントローラがソフトウェアのダウンロードを試行する際の、タイムアウトするまでの最大時間（秒単位）を入力します。

（注）　ソフトウェア ファイルは、インストール中に指定した TFTP ディレクトリにアップロードされます。

ステップ 10　ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。

（注）　TFTP サーバを選択している場合は、サーバ ファイル名を指定します。

ステップ 11　[Download] をクリックします。

ヒント　何らかの理由で転送がタイムアウトした場合には、[File is located on] フィールドで [TFTP server] オプションを選択すると、サーバ ファイル名が読み込まれ、再試行されます。

ソフトウェアのダウンロード（FTP）

コントローラにソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Download Software (FTP)] を選択します。

ステップ 4　[Go] をクリックします。

（注）　[Configure] > [Controllers] > [*IPaddr*] > [System] > [Commands] > [Upload/Download Commands] > [Download Software] の順に選択することでも、ソフトウェアをダウンロードできます。

コントローラの IP アドレスおよび現在のステータスが、[Download Software to Controller] ページに表示されます。

ステップ 5　ダウンロード タイプを選択します。

（注）　事前ダウンロード オプションは、選択したすべてのコントローラがリリース 7.0.x.x 以降を使用している場合のみ表示されます。

- [Now]：ソフトウェアのダウンロードをただちに開始します。このオプションを選択した場合は、ステップ 7 に進みます。

  （注）　ダウンロードが成功したら、コントローラをリブートして、新しいソフトウェアを有効にします。

- [Scheduled]：スケジュール設定するダウンロードオプションを指定します。
  - [Schedule download to controller]：ソフトウェアをコントローラにダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。
  - [Pre-download software to APs]：ソフトウェアを AP に事前ダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。AP にイメージがダウンロードされ、コントローラのリブート時に、AP もリブートされます。

    （注）　AP ごとの [Image Predownload] ステータスを確認するには、[Administration] > [Background Task] > [AP Image Predownload Task] ページでタスクを有効にし、[Report Launch Pad] から AP Image Predownload レポートを実行します。

ステップ 6　[Download type] の下で [Scheduled] オプションを選択した場合は、スケジュールの詳細を入力します。

- [Task Name]：スケジュール設定済みタスク名を入力して、当該のスケジュール設定済みソフトウェア ダウンロード タスクを特定します。
- [Reboot Type]：リブート タイプが手動、自動、またはスケジュール設定済みかどうかを示します。

  （注）　[Download software to controller] オプションだけを選択した場合は、[Reboot Type] を自動に設定できます。

- [Download date/time]：表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。
- [Reboot date/time]：このオプションは、リブート タイプで [Scheduled] を選択した場合のみ表示されます。表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、コントローラをリブートする日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。

（注）　すべての AP がソフトウェアの事前ダウンロードを完了できるように、ダウンロードとリブートの間に十分な時間（少なくとも 30 分）をスケジュール設定します。

（注）　スケジュール設定されたリブート時刻に、いずれかの AP で事前ダウンロードが進行中の場合、コントローラはリブートしません。そのような場合は、すべての AP の事前ダウンロードが終了するまで待機し、コントローラを手動でリブートします。

- [Notification]（任意）：電子メールで通知を送信する受信者の電子メール アドレスを入力します。

（注）　電子メール通知を受信するには、[Administration] > [Settings] > [Mail Server Configuration] ページで Prime Infrastructure メール サーバを設定します。

ステップ 7　ユーザ名、パスワード、およびポートを含めて、FTP クレデンシャルを入力します。

（注）　$、'、\、%、&、(、)、;、"、<、>、,、?、および | などの特殊文字は FTP パスワードの一部として使用できません。@、#、^、*、~、_、-、+、=、{、}、[、]、:、.、および / などの特殊文字をパスワードには使用できます。特殊文字「!」（感嘆符）は、パスワード ポリシーが無効の場合に動作します。パスワード ポリシーの詳細については、「ローカル パスワード ポリシーの設定」（P.15-890）を参照してください。

ステップ 8　[File is located on] オプションで、[Local machine] または [FTP Server] オプション ボタンのいずれかを選択します。

（注）　[FTP Server] を選択した場合は、[Server Name] ドロップダウン リストから [Default Server] または [New] を選択します。

（注）　ソフトウェア ファイルは、インストール中に指定した FTP ディレクトリにアップロードされます。

ステップ 9　ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。

（注）　FTP サーバを選択している場合は、サーバ ファイル名を指定します。

ステップ 10　[Download] をクリックします。

（注）　何らかの理由で転送がタイムアウトした場合には、[File is located on] フィールドで [FTP server] オプションを選択すると、サーバ ファイル名が読み込まれ、再試行されます。

ソフトウェアのダウンロード（SFTP）

コントローラにソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Download Software (SFTP)] を選択します。

ステップ 4　[Go] をクリックします。

（注）　[Configure] > [Controllers] > [*IPaddr*] > [System] > [Commands] > [Upload/Download Commands] > [Download Software] の順に選択することでも、ソフトウェアをダウンロードできます。

コントローラの IP アドレスおよび現在のステータスが、[Download Software to Controller] ページに表示されます。

ステップ 5　ダウンロード タイプを選択します。

（注）　事前ダウンロード オプションは、選択したすべてのコントローラがリリース 7.0.x.x 以降を使用している場合のみ表示されます。

- [Now]：ソフトウェアのダウンロードをただちに開始します。このオプションを選択した場合は、ステップ 7 に進みます。

  （注）　ダウンロードが成功したら、コントローラをリブートして、新しいソフトウェアを有効にします。

- [Scheduled]：スケジュール設定するダウンロードオプションを指定します。
  - [Schedule download to controller]：ソフトウェアをコントローラにダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。
  - [Pre-download software to APs]：ソフトウェアを AP に事前ダウンロードするようにスケジュール設定するには、このチェックボックスをオンにします。AP にイメージがダウンロードされ、コントローラのリブート時に、AP もリブートされます。

    （注）　AP ごとの [Image Predownload] ステータスを確認するには、[Administration] > [Background Task] > [AP Image Predownload Task] ページでタスクを有効にし、[Report Launch Pad] から AP Image Predownload レポートを実行します。

ステップ 6　[Download type] の下で [Scheduled] オプションを選択した場合は、スケジュールの詳細を入力します。

- [Task Name]：スケジュール設定済みタスク名を入力して、当該のスケジュール設定済みソフトウェア ダウンロード タスクを特定します。
- [Reboot Type]：リブート タイプが手動、自動、またはスケジュール設定済みかどうかを示します。

  （注）　[Download software to controller] オプションだけを選択した場合は、[Reboot Type] を自動に設定できます。

- [Download date/time] : 表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。
- [Reboot date/time] : このオプションは、リブート タイプで [Scheduled] を選択した場合のみ表示されます。表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、コントローラをリブートする日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。

（注） すべての AP がソフトウェアの事前ダウンロードを完了できるように、ダウンロードとリブートの間に十分な時間（少なくとも 30 分）をスケジュール設定します。

（注） スケジュール設定されたリブート時刻に、いずれかの AP で事前ダウンロードが進行中の場合、コントローラはリブートしません。そのような場合は、すべての AP の事前ダウンロードが終了するまで待機し、コントローラを手動でリブートします。

- [Notification]（任意）: 電子メールで通知を送信する受信者の電子メール アドレスを入力します。

（注） 電子メール通知を受信するには、[Administration] > [Settings] > [Mail Server Configuration] ページで Prime Infrastructure メール サーバを設定します。

ステップ 7　ユーザ名、パスワード、およびポートなどの SFTP クレデンシャルを入力します。

ステップ 8　[File is located on] オプションで、[Local machine] または [SFTP Server] オプション ボタンのいずれかを選択します。

（注） [SFTP Server] を選択した場合は、[Server Name] ドロップダウン リストから [Default Server] または [New] を選択します。

（注） ソフトウェア ファイルは、インストール中に指定した SFTP ディレクトリにアップロードされます。

ステップ 9　ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。

（注） SFTP サーバを選択している場合は、サーバ ファイル名を指定します。

ステップ 10　[Download] をクリックします。

（注） 何らかの理由で転送がタイムアウトした場合には、[File is located on] フィールドで [SFTP server] オプションを選択すると、サーバ ファイル名が読み込まれ、再試行されます。

コントローラからの *IPaddr* アップロード設定 / ログの設定

コントローラからファイルをアップロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4　[TFTP] 、[FTP] 、または [SFTP] オプション ボタンを選択します。

ステップ 5　[Upload/Download Commands] ドロップダウン リストから、[Upload File from Controller] を選択します。

ステップ 6　このページにアクセスするには、[Go] をクリックします。

- [FTP Credentials Information] : FTP オプション ボタンを選択している場合は、FTP ユーザ名、パスワード、ポートを入力します。
- TFTP、FTP、または SFTP サーバの情報：
  - [Server Name] : ドロップダウン リストから、[Default Server] または [New] を選択します。
  - [IP Address] : コントローラの IP アドレス。これは、デフォルトのサーバを選択すると自動的に入力されます。
  - [File Type] : コンフィギュレーション、イベント ログ、メッセージ ログ、トラップ ログ、クラッシュ ファイル、シグニチャ ファイル、PAC のいずれかを選択します。
  - [Upload to File] で、/(root)/Prime Infrastructure-tftp/ または /(root)/Prime Infrastructure-ftp/ ファイル名を入力します。
  - 設定のバックアップ前に、Prime Infrastructure で情報を保存するかどうかを選択します。

ステップ 7　[OK] をクリックします。選択したファイルが、[File Name] テキスト ボックスに入力した名前で TFTP、FTP、または SFTP サーバにアップロードされます。

IDS シグニチャのダウンロード

侵入検知システム（IDS）シグニチャ ファイルをコントローラにダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Download IDS Signatures] を選択します。

ステップ 4　[Go] をクリックします。

（注）　[Configure] > [Controllers] > [IPaddr] > [System] > [Commands] > [Upload/Download Commands] > [Download IDS Signatures] の順に選択することでも、IDS シグニチャ ファイルをダウンロードできます。

[Download IDS Signatures to Controller] ページに、コントローラの IP アドレスおよび現在のステータスが表示されます。

ステップ 5　シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 6　[File is located on] オプションで、[Local machine] オプション ボタンを選択します。

（注）　ファイル名および、サーバのルート ディレクトリに対して相対的なパスがわかる場合は、[TFTP server] オプション ボタンを選択することもできます。

ステップ 7　[Maximum Retries] テキスト ボックスに、コントローラによるシグニチャ ファイルのダウンロードの最大試行回数を入力します。

ステップ 8　[Timeout] テキスト ボックスに、コントローラがシグニチャ ファイルのダウンロードを試行する際の、タイムアウトするまでの最大時間（秒単位）を入力します。

（注）　ファイルは /localdisk/tftp ディレクトリにアップロードされます。

ステップ 9　ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。コントローラはベース ネームとしてこのローカル ファイル名を使用してから、サフィクスとして _custom.sgi を追加します。

（注）　TFTP サーバを選択している場合は、サーバ ファイル名を指定します。

ステップ 10　[Download] をクリックします。

ヒント　何らかの理由で転送がタイムアウトした場合には、[File is located on] フィールドで [TFTP server] オプションを選択すると、サーバ ファイル名が読み込まれ、再試行されます。

（注）　ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure 独自の組み込みの TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、ダウンロードした Web ページで自動的にそのファイル名が読み込まれます。

コントローラへのカスタマイズ Web 認証バンドルのダウンロード

カスタマイズ Web 認証バンドルをコントローラにダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Download Customized WebAuth] を選択します。

ステップ 4　[Go] をクリックします。

（注）　カスタマイズ Web 認証バンドルは、[Configure] > [Controllers] > [IPaddr] > [System] > [Commands] > [Upload/Download Commands] > [Download Customized Web Auth] からダウンロードすることも可能です。

[Download Customized WebAuth bundle to Controller] ページに、コントローラの IP アドレスおよび現在のステータスが表示されます。

ステップ 5　[File is located on] フィールドで、[Local machine] オプション ボタンを選択します。

（注）　ファイル名および、サーバのルート ディレクトリに対して相対的なパスがわかる場合は、[TFTP server] オプション ボタンを選択することもできます。

（注）　ローカル マシンのダウンロードには、.zip または .tar のファイル オプションがありますが、Prime Infrastructure では自動的に .zip を .tar に変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイルだけを指定します。

ステップ 6　[Maximum Retries] テキスト ボックスに、コントローラによるファイルのダウンロードの最大試行回数を入力します。

ステップ 7　[Timeout] テキスト ボックスに、コントローラがファイルのダウンロードを試行する際の、タイムアウトするまでの最大時間（秒単位）を入力します。

（注）　[Prime Infrastructure Server Files In field] は Prime Infrastructure サーバ ファイルのある場所を指定します。

ステップ 8　ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。コントローラはベース ネームとしてこのローカル ファイル名を使用してから、サフィクスとして _custom.sgi を追加します。

ステップ 9　[Download] をクリックします。

ヒント　何らかの理由で転送がタイムアウトした場合には、[File is located on] フィールドで [TFTP server] オプション ボタンを選択すると、サーバ ファイル名が読み込まれ、再試行されます。

ステップ 10　ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure 独自の組み込みの TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、ダウンロードした Web ページで自動的にそのファイル名が読み込まれます。

ステップ 11　ダウンロードが完了すると、新しいページに接続され、認証できます。

ベンダー デバイス証明書のダウンロード

各無線デバイス（コントローラ、アクセス ポイント、およびクライアント）には独自のデバイスの証明書があります。ご自身のベンダー固有のデバイス証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。

ベンダー デバイス証明書をコントローラにダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　証明書は 2 種類の方法でダウンロードできます。

a.　該当するコントローラのチェックボックスをオンにします。

b.　[Select a command] ドロップダウン リストから、[Download Vendor Device Certificate] を選択します。

c.　[Go] をクリックします。

または

a.　目的のコントローラの IP アドレスをクリックします。

b.　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

c.　[Upload/Download Commands] ドロップダウン リストから、[Download Vendor Device Certificate] を選択します。

d.　[Go] をクリックします。

ステップ 3　[Certificate Password] テキスト ボックスに、証明書の保護に使用されたパスワードを入力します。

ステップ 4　[Confirm Password] テキスト ボックスにパスワードを再入力します。

ステップ 5　[File is located on] フィールドで、[Local machine] または [TFTP server] オプション ボタンを選択します。

（注）　証明書が TFTP サーバにある場合は、サーバ ファイル名を入力します。ローカル マシンにある場合は、[Browse] をクリックして、ローカル ファイル名を入力します。

ステップ 6　[Server Name] フィールドに TFTP サーバ名を入力します。デフォルトは Prime Infrastructure サーバです。

ステップ 7　サーバの IP アドレスを入力します。

ステップ 8　[Maximum Retries] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 9　[Timeout] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 10　[Local File Name] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 11　[Server File Name] テキスト ボックスに、証明書の名前を入力します。

ステップ 12　[Download] をクリックします。

ベンダー CA 証明書のダウンロード

コントローラとアクセス ポイントには、デバイスの証明書の署名と確認に使用される認証局（CA）の証明書があります。コントローラには、シスコによりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時にワイヤレス クライアントを認証するために、（PAC を使用していない場合）EAP-TLS と EAP-FAST により使用される場合があります。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。

ベンダー CA 証明書をコントローラにダウンロードするには、次の手順に従います。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　証明書は 2 種類の方法でダウンロードできます。

a.　該当するコントローラのチェックボックスをオンにします。

b.　[Select a command] ドロップダウン リストから、[Download Vendor CA Certificate] を選択します。

c.　[Go] をクリックします。

または

a.　目的のコントローラの IP アドレスをクリックします。

b.　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

c.　[Upload/Download Commands] ドロップダウン リストから、[Download Vendor CA Certificate] を選択します。

d.　[Go] をクリックします。

ステップ 3　[File is located on] フィールドで、[Local machine] または [TFTP server] オプション ボタンを選択します。

（注）　証明書が TFTP サーバにある場合は、サーバ ファイル名を入力します。ローカル マシンにある場合は、[Browse] をクリックして、ローカル ファイル名を入力します。

ステップ 4　[Server Name] テキスト ボックスに TFTP サーバ名を入力します。デフォルトは Prime Infrastructure サーバです。

ステップ 5　サーバの IP アドレスを入力します。

ステップ 6　[Maximum Retries] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 7　[Timeout] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 8　[Local File Name] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 9　[Server File Name] テキスト ボックスに、証明書の名前を入力します。

ステップ 10　[OK] をクリックします。

フラッシュへの設定の保存

設定をフラッシュ メモリに保存するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Save Config to Flash] を選択します。

ステップ 4　[Go] をクリックします。

コントローラからの設定のリフレッシュ

Refresh Config from Controller コマンドはコントローラで指定されたカスタムの不正 AP ルールがある場合は機能しません。

コントローラから設定をリフレッシュするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Refresh Config from Controller] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[Configuration Change] プロンプトで、[Retain] または [Delete] オプション ボタンを選択します。

ステップ 6　[Go] をクリックします。

コントローラからのテンプレートの検出

リリース 5.1 よりも前のソフトウェアでは、コントローラが検出されるとテンプレートも検出され、コントローラの Prime Infrastructure で検出された設定にはすべてアソシエートされたテンプレートがありました。現在、コントローラが検出されてもテンプレートは自動的に検出されず、テンプレートをアソシエートする Prime Infrastructure 設定を指定できます。

（注）　検出されたテンプレートは、管理またはローカル ユーザ パスワードを取得しません。

テンプレート検出には次のルールが適用されます。

- テンプレート検出では、Prime Infrastructure で見つからないテンプレートが検出されます。
- 既存のテンプレートは検出されません。
- テンプレート検出では、コントローラの動的インターフェイスの設定を取得しません。コントローラで動的インターフェイスの設定を適用するには、新しいテンプレートを作成する必要があります。

現在のテンプレートを検出するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　テンプレートを検出するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Discover Templates from Controller] を選択します。

ステップ 4　[Go] をクリックします。[Discover Templates] ページには、検出されたテンプレートの数、各テンプレートのタイプ、および各テンプレートの名前が表示されます。

（注）　[Enabling this option will create association between discovered templates and the device listed above] チェックボックスをオンにすると、検出されたテンプレートがデバイスの設定にアソシエートされ、当該のコントローラに適用されていることが表示されます。

（注）　テンプレートの検出を実行した場合、実際に検出が実行される前に、コントローラから設定が更新されます。検出を続行するには、警告ダイアログボックスで [OK] をクリックします。

（注）　TACACS+ サーバ テンプレートの場合、サーバ IP アドレスおよびポート番号が同じで、サーバ タイプが異なるコントローラの設定は、単一のテンプレートに集約されます。このとき、対応するサーバ タイプが検出されたテンプレートに設定されます。TACACS+ サーバ テンプレートの場合、検出されたテンプレートの管理ステータスには、最初に見つかったサーバ IP アドレスおよびポート番号が同じコントローラの設定の管理ステータスが反映されます。

Prime Infrastructure のクレデンシャルのアップデート

複数のコントローラの Prime Infrastructure の SNMP/Telnet クレデンシャルの詳細を一括にアップデートする設定はありません。この一括アップデートを実行するには、各デバイスで SNMP および Telnet クレデンシャルをアップデートする必要があります。

SNMP/Telnet クレデンシャルをアップデートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　SNMP/Telenet クレデンシャルをアップデートする各コントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Update Credentials in Prime Infrastructure] を選択します。[Update Credentials in Prime Infrastructure] ページが表示されます。

ステップ 4　[SNMP Parameters] チェックボックスをオンにして、次のパラメータを設定します。

（注）　コントローラの設定を変更するには、SNMP 書き込みアクセス パラメータが必要です。読み取り専用アクセス パラメータの場合、設定は表示されるのみです。

- [Version] : [v1]、[v2]、または [v3] から選択します。
- [Retries] : コントローラの検出試行回数を示します。
- [Timeout] : プロセスがタイムアウトになるまでに許可される時間（秒単位）を示します。有効な範囲は 2 ～ 90 秒です。デフォルトは 2 秒です。
- [Community] : [Public] または [Private]。
- [Verify SNMP Credentials] : SNMP クレデンシャルを確認するには、このチェックボックスをオンにします。

ステップ 5　[Telnet/SSH Parameters] チェックボックスをオンにして、次のパラメータを設定します。

- [User Name]：ユーザ名を入力します。
- [Password]/[Confirm Password]：パスワードを入力して、確認します。
- [Timeout]：プロセスがタイムアウトになるまでに許可される時間（秒単位）を示します。有効な範囲は 2 ～ 90 秒です。デフォルトは 60 秒です。

コントローラに適用されているテンプレートの表示

特定のコントローラに現在適用されているすべてのテンプレートを表示できます。

（注）　このパーティション内に適用されているテンプレートのみが表示されます。

適用されているテンプレートを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Templates Applied to a Controller] を選択します。

ステップ 4　[Go] をクリックします。[Templates Applied to a Controller] ページに、適用されている各テンプレート名、テンプレート タイプ、テンプレートの最終保存日、およびテンプレートの最終適用日が表示されます。

（注）　テンプレート名のリンクをクリックして、テンプレートの詳細を表示します。詳細については、「テンプレートの使用」（P.11-601）を参照してください。

[Audit Now] 機能の使用

[Configure] > [Controllers] ページの [Select a command] ドロップダウン リストで [Audit Now] を選択するか、または [Select a command] ドロップダウン リストで [Audit Now] を直接選択すると、コントローラを監査できます。

（注）　現在のコントローラ監査レポートには、[Configure] > [Controllers] ページの [Audit Status] 列で値をクリックすることでアクセスできます。

コントローラを監査する手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Audit Now] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　データベース内の設定オブジェクトからテンプレート アソシエーションを削除し、同時にアソシエートされている設定グループから当該のコントローラのテンプレート アソシエーションも削除する場合（Template based audit のみ）は、ポップアップ ダイアログボックスで [OK] をクリックします。

監査レポートには、次の内容が表示されます。

- デバイス名
- 監査の時刻
- 監査ステータス
- 適用テンプレートと設定グループ テンプレートの矛盾の情報には、次の内容が含まれます。
  - テンプレートの種類（テンプレート名）
  - テンプレート適用方法
  - 監査ステータス（不一致、同一など）
  - テンプレートの属性
  - Prime Infrastructure の値
  - コントローラの値
- 次を含む、その他の Prime Infrastructure の矛盾：
  - 設定の種類（名前）
  - 監査ステータス（不一致、同一など）
  - 属性
  - Prime Infrastructure の値
  - コントローラの値
- バックグラウンド監査が有効な設定グループの施行数の合計：バックグラウンド監査が有効な設定グループに関する監査の際に矛盾が検出された場合、そして施行が有効である場合、このセクションにコントローラの監査中の施行が表示されます。バックグラウンド監査有効化の詳細は、「設定グループの設定」（P.9-524）を参照してください。
- バックグラウンド監査が有効な設定グループの失敗した施行：リンクをクリックして、デバイスに返された障害の詳細（障害の理由など）リストを表示します。バックグラウンド監査（ConfigAuditSet）有効化の詳細については、「設定グループの設定」（P.9-524）を参照してください。
- [Restore Prime Infrastructure Values to Controller or Refresh Config from Controller] : 監査の結果として設定の相違が見つかった場合は、[Restore Prime Infrastructure Values to controller] または [Refresh Config from controller] をクリックして、Prime Infrastructure 設定をコントローラと同期させます。
  - [Restore Prime Infrastructure Values to Controller] を選択して、矛盾をデバイスにプッシュします。
  - [Refresh Config from Controller] を選択して、デバイスからこの設定を取得します。

（注）　[Refresh Config from Controller] をクリックしても、テンプレートはリフレッシュされません。

最新のネットワーク監査レポートの表示

Network Audit Report には、監査の時刻、選択したコントローラの IP アドレス、および同期ステータスが表示されます。

（注）　この方法では、ネットワーク監査タスクからのレポートが表示され、コントローラごとのオンデマンドの監査は表示されません。

選択したコントローラに対する最新のネットワーク監査レポートを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[View Latest Network Configuration Audit Report] を選択します。

ステップ 4　[Go] をクリックします。

[Audit Summary] には、監査の時刻、選択したコントローラの IP アドレス、および監査ステータスが表示されます。該当する場合、[Audit Details] に設定の相違が表示されます。

（注）　[General and Schedule] タブを使用して、Audit Report パラメータを変更します。

コマンド ボタン

- [Save]：現在パラメータに対して加えられている変更を保存する場合にクリックします。
- [Save and Run]：現在パラメータに対して加えられている変更を保存し、レポートを実行する場合にクリックします。
- [Run Now]：既存のパラメータに基づいて監査レポートを実行する場合にクリックします。
- [Export Now]：レポート結果をエクスポートする場合にクリックします。サポートされるエクスポート形式は PDF および CSV です。
- [Cancel]：既存のパラメータに対して加えられた変更をキャンセルする場合にクリックします。

（注）　[All Controllers] ページから、[Audit Status] 列の値をクリックして、選択したコントローラの最新の監査詳細ページを表示します。この方法で表示される情報は、[Reports] メニューの Network Audit レポートと似ていますが、このレポートはインタラクティブでコントローラごとになっています。

（注）　オンデマンドの監査レポートを実行するには、レポートを実行させるコントローラを選択し、[Select a command] ドロップダウン リストから [Audit Now] を選択します。オンデマンド監査レポートを実行して設定の相違が検出されると、既存のコントローラの値か Prime Infrastructure の値のどちらを保持するかを選択できます。

既存のコントローラの設定

ここでは、次の内容について説明します。

コントローラのプロパティの設定

現在のコントローラのプロパティを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Properties] > [Settings] の順に選択します。次のパラメータが表示されます。

- General Parameters：
  - [Name]：コントローラに割り当てられている名前。
  - [Type]：コントローラのタイプ。
  - [Restore on Cold Start Trap]：コールド スタート トラップでの復元を有効にする場合に選択します。
  - [Auto Refresh on Save Config Trap]：Save Config トラップでの自動リフレッシュを有効にする場合に選択します。
  - [Trap Destination Port]：読み取り専用。
  - [Software Version]：読み取り専用。
  - [Location]：コントローラの場所。

- [Contact]：このコントローラの連絡先担当者。
- [Most Recent Backup]：最新のバックアップ日時。
- [Save Before Backup]：バックアップの前の保存を有効にする場合に選択します。

• SNMP Parameters：

（注）　コントローラの設定を変更するには、SNMP 書き込みアクセス パラメータが必要です。読み取り専用アクセス パラメータの場合、設定は表示されるのみです。

- [Version]：[v1]、[v2]、または [v3] から選択します。
- [Retries]：コントローラの検出試行回数を示します。
- [Timeout (seconds)]：クライアント セッションのタイムアウト。クライアントの再認証が強制されるまでの最大時間を設定します。
- [Community]：[Public] または [Private]。
- [Access Mode]：[Read Write]

（注）　Community の設定は、[v1] および [v2] のみに適用されます。

- [User Name]：ユーザ名を入力します。
- [Auth.Type]：ドロップダウン リストから認証タイプを選択するか、[None] を選択します。
- [Auth.Password]：認証パスワードを入力します。
- [Privacy Type]：ドロップダウン リストからプライバシー タイプを選択するか、[None] を選択します。
- [Privacy Password]：プライバシー パスワードを入力します。

（注）　ユーザ名、認証タイプ、認証パスワード、プライバシー タイプ、およびプライバシー パスワードは v3 の場合にのみ表示されます。

• Telnet/SSH Parameters：

- [User Name]：ユーザ名を入力します。（デフォルトのユーザ名は admin です）。

（注）　Telnet/SSH のユーザ名は、CLI テンプレートでコマンドを実行するために十分な権限を持っている必要があります。

- [Password]/[Confirm Password]：パスワードを入力して、確認します。（デフォルトのパスワードは admin です）。
- [Retries]：許可されている再試行回数を示します。デフォルトは 3 です。
- [Timeout]：プロセスがタイムアウトになるまでに許可される時間（秒単位）を示します。デフォルトは 60 秒です。

（注）　Telnet/SSH パラメータが空白のままの場合は、デフォルト値が使用されます。

ステップ 4　このコントローラのプロパティを変更した場合は、[Save] をクリックして変更を確定するか、[Reset] をクリックして以前またはデフォルトの設定に戻すか、または [Cancel] をクリックして設定に変更を加えずに [Configure] > [Controllers] ページに戻ります。

コントローラ システム パラメータの設定

ここでは、コントローラ システム パラメータの設定方法について説明します。内容は次のとおりです。

コントローラの一般システム プロパティの管理

現在のコントローラの一般システム パラメータを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [General] の順に選択します。次のパラメータが表示されます。

- [802.3x Flow Control Mode]：無効または有効。詳細については、「802.3x フロー制御」（P.9-314）を参照してください。
- [802.3 Bridging]：無効または有効。詳細については、「802.3 ブリッジの設定」（P.9-314）を参照してください。
- [Web Radius Authentication]：[PAP]、[CHAP]、[MD5-CHAP] のいずれかを選択します。
  - [PAP]：パスワード認証プロトコル。クリア テキストでユーザ情報（ユーザ名およびパスワード）が送信される 認証方法。

  - [CHAP]：チャレンジ ハンドシェイク認証プロトコル。ユーザ情報を送信用に暗号化する認証方式。
  - [MD5-CHAP]：Message Digest 5 チャレンジ ハンドシェイク認証プロトコル。MD5 では、パスワードは Message Digest 5 アルゴリズムを使用してハッシュされます。
- [AP Primary Discovery Timeout]：30 ～ 3600 秒の間の値を入力します。

  アクセス ポイントはバックアップ コントローラのリストを維持し、リスト上の各エントリに対して定期的にプライマリ ディスカバリ要求を送信します。設定されている場合、プライマリ ディスカバリ要求タイマーは、アクセス ポイントからのプライマリ ディスカバリ要求に対して応答する時間を指定します。この時間を超えても応答がない場合は、アクセス ポイントはそのコントローラは接続できないと見なし、次にリストされているコントローラからのディスカバリ応答を待ちます。
- [CAPWAP Transport Mode]：[Layer 3] または [Layer 2]。詳細については、「Lightweight Access Point Protocol 転送モード」（P.9-314）を参照してください。
- [Current LWAPP Operating Mode]：自動的に入力されます。
- [Broadcast Forwarding]：無効または有効。
- [LAG Mode]：LAG を無効にするには、[Disable] を選択します。

  リンク集約（LAG）は、802.3ad ポート集約標準の部分的な実装です。コントローラのすべてのディストリビューション システム ポートが 1 つの 802.3ad ポート チャネルにまとめられるので、コントローラのポートの設定に必要な IP アドレスの数を減らすことができます。LAG が有効である場合、ポートの冗長性は動的に管理され、アクセス ポイントはユーザからは透過的にロード バランシングされます。

  （注）　Cisco 5500 および 4400 シリーズ コントローラでは LAG はデフォルトで無効化されていますが、Cisco WiSM コントローラおよび Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラではデフォルトで有効化されます。

  詳細については、「リンク集約」（P.9-316）を参照してください。
- Ethernet Multicast Support
  - [Disable]：コントローラでのマルチキャスト サポートを無効にする場合に選択します。
  - [Unicast]：マルチキャスト パケットを受信した場合に、コントローラがパケットをアソシエートされたアクセス ポイントすべてに転送する場合に選択します。

    （注）　FlexConnect は、ユニキャスト モードのみをサポートしています。
  - [Multicast]：コントローラでのマルチキャスト サポートを有効にする場合に選択します。
- [Aggressive Load Balancing]：無効または有効。ロード バランシングの詳細については、「アグレッシブ ロード バランシング」（P.9-316）を参照してください。
- Peer to Peer Blocking Mode
  - [Disable]：同じサブネットのクライアントはこのコントローラを使用して通信します。
  - [Enable]：同じサブネットのクライアントは上位レベルのルータを使用して通信します。
- [Over Air Provision AP Mode]：無効または有効。

  無線プロビジョニング（OTAP）は、Cisco 5500 および 4400 シリーズ コントローラでサポートされています。この機能がコントローラ上で有効にされると、アソシエートされたアクセス ポイントすべてはワイヤレス CAPWAP または LWAPP ネイバー メッセージを送信し、新しいアクセス

ポイントはこれらのメッセージからコントローラの IP アドレスを受信します。この機能はデフォルトでは無効です。すべてのアクセス ポイントをインストールする際は、無効のままにしておいてください。

（注）　コントローラ上で OTAP を無効にしても、アクセス ポイント上では OTAP は無効になりません。OTAP はアクセス ポイント上で無効化できません。

（注）　OTAP についての詳細は、次の URL を参照してください。
http://www.ciscosystems.com/en/US/products/ps6366/products_tech_note09186a008093d74a.shtml

- [AP Fallback]：無効または有効。

（注）　AP フォールバックを有効にすると、プライマリ コントローラの接続が切断されたアクセス ポイントがプライマリ コントローラの復帰と同時に自動的にサービスに戻ります。

- [AP Failover Priority]：無効または有効。

（注）　アクセス ポイントのフェールオーバー優先度設定を設定するには、まず AP Failover Priority 機能を有効にする必要があります。詳細については、「AP フェールオーバー優先度」（P.9-313）を参照してください。

- [AppleTalk Bridging]：無効または有効。
- [Fast SSID change]：無効または有効。

  コントローラ上で Fast SSID Change が有効になっているときは、クライアントは SSID 間で移動することができます。クライアントが異なる SSID の新しいアソシエーションを送信すると、コントローラの通信テーブルのクライアント エントリがクリアされてから、新しい SSID にクライアントが追加されます。Fast SSID Change が無効のときは、コントローラは一定の遅延時間が経過した後でクライアントに新しい SSID への移動を許可します。

（注）　有効にすると、クライアントは SSID 間で接続をほとんど中断せずにコントローラに瞬時に接続します。

- [Master Controller Mode]：無効または有効。

（注）　マスター コントローラは、通常、展開されたネットワークで使用されないため、マスター コントローラの設定は、リブートまたは OS コードのアップグレード時に自動的に無効になります。

- [Wireless Management]：無効または有効。詳細については、「ワイヤレス管理」（P.9-316）を参照してください。
- Symmetric Tunneling Mode
- [ACL Counters]：無効または有効。ヒット数は、[ACL Rule] ページに表示されます。詳細については、「アクセス コントロール リストの設定」（P.9-395）または「[IPaddr] > [Access Control List] > [listname Rules] の設定」（P.9-396）を参照してください。

- [Multicast Mobility Mode]：無効または有効。詳細については、「モビリティ スケーラビリティ パラメータの設定」（P.9-339）を参照してください。
- [Default Mobility Domain Name]：ドメイン名を入力します。
- [Mobility Anchor Group Keep Alive Interval]：クライアントが別のアクセス ポイントへの接続を試みるまでに許可される遅延時間を入力します。詳細については、「モビリティ アンカー グループのキープアライブ インターバル」（P.9-317）を参照してください。

ヒント マウス カーソルをパラメータのテキスト ボックスの上に移動すると、そのフィールドの有効な範囲が表示されます。

- [Mobility Anchor Group Keep Alive Retries]：試行可能回数を入力します。

ヒント マウス カーソルをパラメータのテキスト ボックスの上に移動すると、そのフィールドの有効な範囲が表示されます。

- [RF Network Name]：ネットワーク名を入力します。
- [User Idle Timeout (seconds)]：タイムアウトを秒単位で入力します。
- [ARP Timeout (seconds)]：タイムアウトを秒単位で入力します。

ここでは、次の内容について説明します。

- 「AP フェールオーバー優先度」（P.9-313）
- 「802.3 ブリッジの設定」（P.9-314）
- 「802.3x フロー制御」（P.9-314）
- 「Lightweight Access Point Protocol 転送モード」（P.9-314）
- 「アグレッシブ ロード バランシング」（P.9-316）
- 「リンク集約」（P.9-316）
- 「ワイヤレス管理」（P.9-316）
- 「モビリティ アンカー グループのキープアライブ インターバル」（P.9-317）

AP フェールオーバー優先度

コントローラに障害が発生した場合、アクセス ポイントに設定されたバックアップ コントローラがすぐに多くの検出と接続要求を受信します。コントローラが過負荷になった場合、一部のアクセス ポイントが拒否される場合があります。

フェールオーバー優先順位をアクセス ポイントに割り当てることによって、拒否されるアクセス ポイントを制御します。バックアップ コントローラが過負荷になった場合、優先度が高く設定されているアクセス ポイントの接続リクエストの方が、優先度の低いアクセス ポイントよりも優先されます。

アクセス ポイントのフェールオーバー優先度設定を設定するには、まず AP Failover Priority 機能を有効にする必要があります。

AP Failover Priority 機能を有効にする手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [General] の順に選択します。

ステップ 4　[AP Failover Priority] ドロップダウン リストから、[Enabled] を選択します。

アクセス ポイント フェールオーバーの優先度を設定する手順は、次のとおりです。

ステップ 1　[Configure] > [Access Points] > [*AP Name*] を選択します。

ステップ 2　[AP Failover Priority] ドロップダウン リストから、適切な優先度（[Low]、[Medium]、[High]、[Critical]）を選択します。

（注）　デフォルトの優先度は [Low] です。

802.3 ブリッジの設定

コントローラは、一般的にレジやレジ サーバで使用されるような 802.3 フレームおよびそれらを使用するアプリケーションをサポートしています。ただし、これらのアプリケーションをコントローラとともに使用するには、802.3 のフレームがコントローラ上でブリッジされている必要があります。

802.3 Raw フレームのサポートを有効にすると、IP 上では実行されないアプリケーションの非 IP フレームをコントローラがブリッジできるようになります。この未加工の 802.3 フレームの形式だけが、現在サポートされています。

Prime Infrastructure Release 4.1 以降を使用して 802.3 ブリッジを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　[System] > [General] の順に選択して、[General] ページにアクセスします。

ステップ 4　[802.3 Bridging] ドロップダウン リストから [Enable] を選択してコントローラ上の 802.3 ブリッジを有効にするか、[Disable] を選択してこの機能を無効にします。デフォルト値は [Disable] です。

ステップ 5　[Save] をクリックして変更を確定します。

802.3x フロー制御

フロー制御は、モデムなどの送信エンティティにより、データを持つ受信エンティティが過負荷にならないようにする手法です。受信側デバイスのバッファに空きがない場合、メッセージが送信側デバイスに送信され、バッファ内のデータが処理されるまで伝送は一時停止されます。

デフォルトでは、フロー制御は無効に設定されています。ポーズ フレームを受信しても送信できないように Cisco スイッチを設定できるだけです。

Lightweight Access Point Protocol 転送モード

Lightweight Access Point Protocol 転送モードは、コントローラとアクセス ポイント間の通信レイヤを示します。選択肢は Layer 2 または Layer 3 です。

Prime Infrastructure ユーザ インターフェイスを使用して Cisco Unified Wireless Network ソリューションをレイヤ 3 からレイヤ 2 Lightweight アクセス ポイント転送モードに変換するには、次の手順を実行します。

（注）　Cisco IOS ベースの Lightweight アクセス ポイントは、レイヤ 2 Lightweight アクセス ポイント モードはサポートしていません。このようなアクセス ポイントは、レイヤ 3 でしか実行できません。

（注）　この手順を実行すると、コントローラが再度ブートしてアクセス ポイントがコントローラと再アソシエートするまで、アクセス ポイントはオフラインになります。

ステップ 1　コントローラとアクセス ポイントはすべて同じサブネット上に配置するようにします。

（注）　変換を実行する前に、コントローラおよびアソシエートしているアクセス ポイントをレイヤ 2 モードで動作するように設定する必要があります。

ステップ 2　Prime Infrastructure ユーザ インターフェイスにログインします。Lightweight アクセス ポイント転送モードをレイヤ 3 からレイヤ 2 に変換する手順は、次のとおりです。

a. [Configure] > [Controllers] の順に選択します。

b. 該当するコントローラの IP アドレスをクリックします。

c. [System] > [General] の順に選択して、[General] ページにアクセスします。

d. Lightweight アクセス ポイント転送モードを [Layer2] に変更し、[Save] をクリックします。

e. Prime Infrastructure で次のメッセージが表示された場合、[OK] をクリックします。

```
Please reboot the system for the CAPWAP Mode change to take effect.
```

ステップ 3　Prime Infrastructure を再起動するには、次の手順を実行します。

a. [System] > [Commands] の順に選択します。

b. [Administrative Commands] ドロップダウン リストから [Save Config To Flash] を選択して [Go] をクリックし、変更した設定をコントローラに保存します。

c. [OK] をクリックして作業を続行します。

d. [Administrative Commands] ドロップダウン リストから [Reboot] を選択して [Go] をクリックし、コントローラをリブートします。

e. [OK] をクリックし、設定を保存してリブートすることを確認します。

ステップ 4　コントローラがリブートしたら、次の手順に従って CAPWAP 転送モードがレイヤ 2 になっていることを確認します。

a. [Configure] > [Controllers] の順に選択します。

b. 該当するコントローラの IP アドレスをクリックします。

c. [general] ドロップダウン リストで、現在の CAPWAP 転送モードがレイヤ 2 であることを確認します。

これで、レイヤ 3 からレイヤ 2 への CAPWAP 転送モードの変換が完了しました。オペレーティング システムのソフトウェアによって、同じサブネット上のコントローラとアクセス ポイントとの間におけるすべての通信が制御されます。

アグレッシブ ロード バランシング

ルーティングでは、ロード バランシングは、宛先アドレスからの距離が同じすべてのネットワーク ポートでトラフィックを分配するルータの機能を示します。優れたロードバランシング アルゴリズムでは、回線速度と信頼性の両方の情報を使用します。ロード バランシングを行うと、ネットワーク セグメントの使用が増加するため、効率的なネットワーク帯域幅が増加します。

アグレッシブ ロード バランシングは、モバイル クライアントとアソシエートされたアクセス ポイントの間で負荷をアクティブに分散させます。

リンク集約

リンク集約によって、物理ポートをすべてグループ化して link aggregation group（LAG; リンク集約グループ）を作成し、コントローラ上のポートを構成するために必要な IP アドレスの数を削減できます。4402 モデルでは、LAG を形成するために 2 つのポートが組み合わされます。4404 モデルでは、4 つのポートすべてが LAG を形成するため組み合わされます。

LAG がコントローラ上で有効な場合、次の設定が変更されます。

- 作成した動的インターフェイスは削除されます。これは、インターフェイス データベース内での設定の矛盾を避けるためです。
- インターフェイスを「Dynamic AP Manager」フラグを設定して作成できません。

（注） コントローラ上では、複数の LAG を作成できません。

LAG の作成には、次のようなメリットがあります。

- リンクの 1 つがダウンした場合に、常にトラフィックが LAG 内の他のリンクに移動します。物理ポートの 1 つが動作している限り、システムは機能し続けます。
- 各インターフェイスに対して個別にバックアップ ポートを設定する必要がありません。
- アプリケーションは論理ポートを 1 つしか認識しないため、複数の AP-manager インターフェイスは必要ありません。

（注） LAG 設定に変更を加えると、変更を有効にするためにコントローラをリブートする必要があります。

ヒント マウス カーソルをパラメータのテキスト ボックスの上に移動すると、そのフィールドの有効な範囲が表示されます。

ワイヤレス管理

IPsec 動作により、ワイヤレスによる管理は WPA、静的 WEP、または VPN パススルー WLAN でログインしているオペレータだけが実行できます。ワイヤレス管理は、IPsec WLAN を経由してログインしようとしているクライアントは実行できません。

モビリティ アンカー グループのキープアライブ インターバル

クライアントが別のアクセス ポイントへの接続を試みるまでの遅延時間を指定します。この機能を使用することで、エラーがすばやく特定され、クライアントが問題発生のコントローラから移動し、別のコントローラに接続されるため、コントローラのエラー後にクライアントが別のアクセス ポイントに接続するためにかかる時間が短縮されます。

ヒント　マウス カーソルをパラメータのテキスト ボックスの上に移動すると、そのフィールドの有効な範囲が表示されます。

コントローラ システム コマンドの設定

現在のコントローラのシステム コマンド パラメータを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。次のパラメータが表示されます。

- 管理
  - [Reboot]：このコマンドを使用すると、設定変更の保存した後にご使用のコントローラを再起動することを確定できます。システム接続が失われないようにするため、新しいセッションを開いて確定し、コントローラにログインします。
  - [Save Config to Flash]：データはコントローラの不揮発性 RAM（NVRAM）に保存され、電源の再投入時にも保持されます。コントローラをリブートした場合、設定が保存されていないと、適用した変更はすべて失われます。
  - [Reset to Factory Default]：コントローラを元の設定に戻すには、このコマンドを選択します。詳細については、「出荷時の初期状態の復元」（P.9-319）を参照してください。
  - [Ping From Controller]：ネットワーク要素に ping を送信します。このポップアップ ダイアログボックスを使用して、コントローラから指定した IP アドレスに ping 要求を送信するように命令できます。これは、コントローラと特定の IP ステーション間に接続があるかどうかを判別する場合に有効です。[OK] をクリックすると、3 つの ping が送信され、ping の結果がポップアップに表示されます。ping に対する応答がない場合は、「No Reply Received from IP xxx.xxx.xxx.xxx」と表示されます。それ以外の場合は、「Reply received from IP xxx.xxx.xxx.xxx: (send count =3, receive count = n)」と表示されます。
- 設定
  - [Audit Config]：「最新のネットワーク監査レポートの表示」（P.9-307）を参照してください。
  - [Refresh Config From Controller]：「コントローラからの設定のリフレッシュ」（P.9-303）を参照してください。
  - [Restore Config To Controller]：Prime Infrastructure データベースからコントローラに設定を復元するには、このコマンドを選択します。
  - [Set System Time]：「コントローラの時刻と日付の設定」（P.9-319）を参照してください。
- Upload/Download コマンド

（注）　[FTP] または [TFTP] オプション ボタンを選択します。Prime Infrastructure では、ファイルのアップロードおよびダウンロードに、ファイル転送プロトコル（FTP）および Trivial Transfer Protocol（TFTP）の両方がサポートされています。前のソフトウェア リリースでは、TFTP のみがサポートされました。

  - [Upload File from Controller] :「コントローラからの設定およびログのアップロード」（P.9-319）を参照してください。
  - [Download Config] :「コントローラへの設定のダウンロード」（P.9-320）を参照してください。
  - [Download Software] : 選択したコントローラにソフトウェアをダウンロードする場合、または設定グループを構築してから選択したグループのすべてのコントローラにソフトウェアをダウンロードする場合は、このコマンドを選択します。「コントローラへのソフトウェアのダウンロード」（P.9-321）を参照してください。
  - [Download Web Auth Cert] : [Download Web Auth Certificate to Controller] ページにアクセスする場合は、このコマンドを選択します。「コントローラへの Web 管理証明書のダウンロード」（P.9-322）を参照してください。
  - [Download Web Admin Cert] : [Download Web Admin Certificate to Controller] ページにアクセスする場合は、このコマンドを選択します。「コントローラへの Web 管理証明書のダウンロード」（P.9-322）を参照してください。
  - [Download IDS Signatures] : 現在コントローラ上に存在するシグニチャ ファイルに、カスタマイズ シグニチャをダウンロードする場合は、このコマンドを選択します。詳細については、「シグニチャ ファイルのダウンロード」（P.9-405）を参照してください。
  - [Download Customized Web Auth] : カスタマイズ Web 認証ページをコントローラにダウンロードする場合は、このコマンドを選択します。カスタマイズ Web ページは、ユーザ Web アクセス用のユーザ名とパスワードを設定するために作成されます。「コントローラへのカスタマイズ Web 認証バンドルのダウンロード」（P.9-299）を参照してください。
  - [Download Vendor Device Certificate] : ユーザ自身のベンダー固有デバイス証明書をコントローラにダウンロードして、現在のワイヤレス デバイス証明書と置き換える場合は、このコマンドを選択します。「ベンダー デバイス証明書のダウンロード」（P.9-301）を参照してください。
  - [Download Vendor CA Certificate] : ユーザ自身のベンダー固有認証局（CA）をコントローラにダウンロードして、現在の CA と置き換える場合は、このコマンドを選択します。「ベンダー CA 証明書のダウンロード」（P.9-302）を参照してください。

- RRM コマンド
  - [RRM 802.11a/n Reset] : 802.11a/n Cisco Radio のリモート無線管理をリセットします。
  - [802.11b/g/n Reset] : 802.11b/g/n Cisco Radio のリモート無線管理をリセットします。
  - [802.11a/n Channel Update] : 802.11a/n Cisco Radio のアクセス ポイントの動的チャネル アルゴリズムをアップデートします。
  - [802.11b/g/n Channel Update] : 802.11b/g/n Cisco Radio のアクセス ポイントの動的チャネル アルゴリズムをアップデートします。
  - [802.11a/n Power Update] : 802.11a/n Cisco Radio のアクセス ポイントの動的送信電力アルゴリズムをアップデートします。
  - [802.11b/g/n Power Update] : 802.11b/g/n Cisco Radio のアクセス ポイントの動的送信電力アルゴリズムをアップデートします。

出荷時の初期状態の復元

[Configure] > [Controllers] を選択して、[IP Address] 列で IP アドレスをクリックします。このページにアクセスするには、左側のサイドバーのメニューから [System] > [Commands] の順に選択し、[Administrative Commands] ドロップダウン リストから [Reset to Factory Default] を選択して [Go] をクリックします。

このコマンドを使用することで、コントローラの設定を出荷時の初期状態にリセットできます。この操作により、すべての適用および保存されている設定パラメータが上書きされます。コントローラの再初期化を確認するプロンプトが表示されます。

すべての設定データ ファイルが削除され、リブート時にコントローラが元の未設定状態に復元されます。これにより、すべての IP 設定が削除されるため、シリアル接続で基本設定を復元する必要があります。

（注）　設定の削除を確定した後に、コントローラをリブートし、[Reboot Without Saving] オプションを選択する必要があります。

コントローラの時刻と日付の設定

[Configure] > [Controllers] を選択して、[IP Address] 列で IP アドレスをクリックします。このページにアクセスするには、左側のサイドバーのメニューから [System] > [Commands] の順に選択し、[Configuration Commands] ドロップダウン リストから [Set System Time] を選択して [Go] をクリックします。

このコマンドを使用して、コントローラの現在の時刻および日付を手動設定します。ネットワーク タイム サーバを使用して現在の時刻を設定またはリフレッシュする場合は、「NTP サーバ テンプレートの設定」（P.11-609）を参照してください。次のパラメータが表示されます。

- [Current Time]：システムで現在使用されている時刻を表示します。
- [Month/Day/Year]：ドロップダウンリストから、月、日、年を選択します。
- [Hour/Minutes/Seconds]：ドロップダウンリストから、時、分、秒を選択します。
- [Delta (hours)]：GMT（グリニッジ標準時）からのオフセットをプラスまたはマイナス時間で入力します。
- [Delta (minutes)]：GMT（グリニッジ標準時）からのオフセットをプラスまたはマイナス分で入力します。
- [Daylight Savings]：夏時間を有効にする場合は、選択します。

コマンド ボタン

- Set Date and Time
- Set Time Zone
- Cancel

コントローラからの設定およびログのアップロード

コントローラからファイルをアップロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Upload File from Controller] を選択します。

ステップ 5　このページにアクセスするには、[Go] をクリックします。

このコマンドを使用して、コントローラからローカル TFTP（Trivial File Transfer Protocol）サーバにファイルをアップロードします。次のフィールドが表示されます。

- [IP Address]：コントローラの IP アドレス。
- [Status]：NOT_INITIATED またはその他のアップロード状態。
- TFTP サーバ名を入力するか、[New] をクリックして新しい TFTP サーバ名を入力します。
- TFTP サーバの IP アドレスを確認および / または入力します。
- [Select the file type]：コンフィギュレーション ファイル、イベント ログ、メッセージ ログ、トラップ ログ、クラッシュ ファイル。
- [Upload to File] で、/(root)/Prime Infrastructure-tftp/ ファイル名を入力します。
- 設定のバックアップ前に、Prime Infrastructure で保存するかどうかを選択します。

ステップ 6　[OK] をクリックします。選択したファイルが、[File Name] テキスト ボックスに入力した名前で TFTP サーバにアップロードされます。

（注） Prime Infrastructure は統合 TFTP サーバを使用します。これは、サードパーティ製の TFTP サーバは Prime Infrastructure と同じワークステーション上では実行できないことを意味します。Cisco Prime Infrastructure とサードパーティ製の TFTP サーバが、同一の通信ポートを使用するためです。

コントローラへの設定のダウンロード

コンフィギュレーション ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Download Config] を選択します。

ステップ 5　このページにアクセスするには、[Go] をクリックします。

このコマンドを使用して、ローカル TFTP（Trivial File Transfer Protocol）サーバからコントローラにコンフィギュレーション ファイルをダウンロードしてインストールします。次のパラメータが表示されます。

（注） Prime Infrastructure は統合 TFTP サーバを使用します。これは、サードパーティ製の TFTP サーバは Prime Infrastructure と同じワークステーション上では実行できないことを意味します。Prime Infrastructure とサードパーティ製 TFTP サーバが、同一の通信ポートを使用するためです。

- [IP Address]：コントローラの IP アドレス。

- [Status]：証明書のステータス（例：NOT_INITIATED）。

TFTP サーバ

- [Server Name]：ドロップダウン リストから [Default Server] または [New] を選択します。[New] を選択した場合は、IP アドレスを入力します。
- [Server Address]：サーバの IP アドレス
- [Maximum Retries]：ダウンロードが失敗した場合の再試行回数。
- [Timeout]：再試行するまでに許可される時間。
- [File Name]：ダウンロードするファイル名を入力するか、または [Browse] をクリックして選択します。

コントローラへのソフトウェアのダウンロード

ソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Download Software] を選択します。

ステップ 5　このページにアクセスするには、[Go] をクリックします。

このコマンドを使用して、ローカル TFTP（Trivial File Transfer Protocol）サーバからコントローラに新しいオペレーティング システム ソフトウェアをダウンロードしてインストールします。

（注）　Prime Infrastructure は統合 TFTP サーバを使用します。これは、サードパーティ製の TFTP サーバは Prime Infrastructure と同じワークステーション上では実行できないことを意味します。Prime Infrastructure とサードパーティ製 TFTP サーバが、同一の通信ポートを使用するためです。

- [IP Address]：ソフトウェアを受信するコントローラの IP アドレス。
- [Current Software Version]：コントローラで現在実行されているソフトウェアのバージョン。
- [Status]：ソフトウェアのステータス（例：NOT_INITIATED）。
- [TFTP Server on Cisco Prime Infrastructure System]：組み込み Cisco Prime Infrastructure TFTP サーバを有効にする場合は、このチェックボックスをオンにします。
- [Server IP Address]：組み込み Prime Infrastructure TFTP サーバを無効にした場合に、コントローラにソフトウェアを送信する TFTP サーバの IP アドレスを示します。
- [Maximum Retries]：ダウンロードが放棄されるまでの試行の失敗回数の上限。
- [Timeout]：ダウンロードが放棄されるまでの最大秒数。
- [File Name]：ダウンロードするファイル名を入力するか、または [Browse] をクリックして選択します。

コントローラへの Web 管理証明書のダウンロード

Web 管理証明書をダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Download WEB Admin Cert] を選択します。

ステップ 5　このページにアクセスするには、[Go] をクリックします。

このページでは、コントローラに Web 管理証明書をダウンロードできます。次のパラメータが表示されます。

注意　各証明書には、可変長 RSA キーが組み込まれています。RSA キーの長さは、比較的安全性の低い 512 ビットから、非常に安全性の高い数千ビットまでさまざまです。認証局（Microsoft CA など）から新しい証明書を取得する場合は、証明書に組み込まれている RSA キーが 768 ビット以上であることを確認してください。

- [IP Address]：証明書を受信するコントローラの IP アドレス。
- [Status]：証明書のステータス（例：NOT_INITIATED）。

TFTP サーバ

- [Server Name]：ドロップダウン リストを使用して、[Default Server] または [New] を選択します。[New] を選択した場合は、IP アドレスを入力します。
- [Server Address]：サーバの IP アドレス
- [Maximum Retries]：各ダウンロード動作を試行できる最大回数。
- [Timeout (seconds)]：各ダウンロード動作に許可される時間。
- [File Name]：証明書のファイル名。
- [Password]：証明書にアクセスするパスワード。

IDS シグニチャのダウンロード

IDS シグニチャをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Download IDS Signatures] を選択します。

ステップ 5　このページにアクセスするには、[Go] をクリックします。

このコマンドを使用して、ローカル TFTP（Trivial File Transfer Protocol）サーバからコントローラに IDS（侵入検知システム）シグニチャ ファイルをダウンロードします。次のパラメータが表示されます。

- [IP Address]：コントローラの IP アドレス。
- [Status]：NOT_INITIATED、TRANSFER_SUCCESSFUL、またはその他のダウンロード状態。

カスタマイズ Web 認証バンドルのコントローラへのダウンロード

カスタマイズ Web 認証ページをコントローラにダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 4　[Upload/Download Commands] ドロップダウン リストから、[Download Customized Web Auth] を選択します。

次のパラメータが表示されます。

- [IP Address]：バンドルを受信するコントローラの IP アドレス。
- [Status]：ダウンロード状態（NOT_INITIATED、TRANSFER_SUCCESSFUL、TRANSFER_FAILED、NOT_RESPONDING）。

カスタマイズ Web 認証バンドルをダウンロードする前に、次の手順を実行します。

ステップ 1　示されているリンクをクリックして、サーバから login.tar サンプル バンドル ファイルをダウンロードします。

リンクは、ページの下部に表示されている「here」という強調表示された単語です。

ステップ 2　Login.html を編集し、これを .tar または .zip ファイルとして保存します。

ステップ 3　.tar または .zip ファイルをコントローラにダウンロードします。

このファイルには、Web 認証の表示に必要なページおよびイメージ ファイルが含まれています。

（注）　コントローラでは、サイズが 1 MB 以下の .tar または .zip ファイルを受け入れます。1MB の制限には、バンドル内の圧縮されていないファイルの合計サイズが含まれます。

TFTP サーバ

1 つ以上の TFTP サーバを設定するには、次のパラメータを設定します。

- [File is located on]：[Local machine] または [TFTP server] を選択します。デフォルトは、ローカル マシン（Prime Infrastructure 内部サーバ）です。
- [Server Name]：ドロップダウン リストを使用して、次のいずれかを選択します。

  - [New]：新しいサーバを設定します。表示されるテキスト ボックスに、サーバ名および IP アドレスを入力します。
  - [Default Server]：サーバ名（編集可能）および IP アドレス（読み取り専用）は自動的に追加されます。
- [Server IP Address]：サーバの IP アドレス。
- [Maximum Retries]：ダウンロードが放棄されるまでの試行の失敗回数の上限。
- [Timeout]：ダウンロードが放棄されるまでの最大秒数。
- [Prime Infrastructure Server Files In]：ローカル マシン上の C:\tftp またはその他の指定ファイル ディレクトリ。
- [Local File Name]：ローカル マシン上の Web 認証バンドルのファイル名。[Browse] をクリックしてファイルを検索します。
- [Server File Name]：リモート TFTP サーバ上のファイル名。

これらのフィールドを入力すると、ページに設定した内容が自動的に再入力されるため、再度入力する必要はありません。

コマンド ボタン

- [OK]：[File Name] テキスト ボックスに表示された名前のローカル マシンまたは TFTP サーバから、ファイルがダウンロードされます。
- Cancel

コントローラ システム インターフェイスの設定

ここでは、コントローラ システム インターフェイスの設定方法について説明します。内容は次のとおりです。

- 「インターフェイスの追加」（P.9-325）
- 「現在のインターフェイスの詳細表示」（P.9-326）
- 「ダイナミック インターフェイスの削除」（P.9-327）
- 「NAC 統合」（P.9-330）
- 「有線ゲスト アクセスの設定」（P.9-332）

既存のインターフェイスを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。次のパラメータが表示されます。

- [Check box]：削除するダイナミック インターフェイスを選択します。[Select a command] ドロップダウン リストから [Delete Dynamic Interfaces] を選択します。
- [Interface Name]：このインターフェイスに対するユーザ定義の名前（例：Management、Service-Port、Virtual）。
- [VLAN Identifier]：0（タグなし）～ 4096 の VLAN ID、または N/A。
- [Quarantine]：インターフェイスに隔離 VLAN ID が設定されている場合は、このチェックボックスをオンにします。

- [IP Address]：このインターフェイスの IP アドレス。
- [Interface Type]：スタティック（管理、AP-Manager、サービス ポート、および仮想インターフェイス）またはダイナミック（オペレータ定義インターフェイス）。
- [AP Management Status]：AP 管理インターフェイスのステータスを表示します。このパラメータには、Enabled、Disabled、および N/A が含まれます。

（注） 管理ポートだけがリダンダンシー マネジメント インターフェイスのポートとして設定できます。

インターフェイスの追加

インターフェイスを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Interface] を選択します。

ステップ 5　必要なパラメータを入力します。

- [Interface Name]：このインターフェイスのユーザ定義名（Management、Service-Port、Virtual、VLAN n）。
- [Wired Interface]：インターフェイスを有線としてマークする場合は、このチェックボックスをオンにします。
- Interface Address
  - [VLAN Identifier]：1 ～ 4096、または 0（タグなし）。
  - [Quarantine]：VLAN の隔離を有効または無効にします。チェックボックスをオンにすると有効になります。
  - [IP Address]：インターフェイスの IP アドレス。
  - [Gateway]：インターフェイスのゲートウェイ アドレス。
- Physical Information
  - [Port Number]：インターフェイスにより使用されるポート。
  - [Primary Port Number (active)]：現在インターフェイスにより使用されているポート。
  - [Secondary Port Number]：プライマリ ポートがダウンした場合に、インターフェイスにより使用されるポート。

（注） プライマリおよびセカンダリ ポート番号は、Cisco 4400 シリーズ Wireless LAN Controller の場合のみ存在します。

（注）　セカンダリ ポートは、プライマリ ポートがシャットダウンした場合に使用されます。プライマリ ポートが再アクティブ化されると、Cisco 4400 シリーズ Wireless LAN Controller は、インターフェイスをプライマリ ポートに転送されます。

  - [AP Management] : アクセス ポイント管理を有効にする場合に選択します。
- DHCP Information
  - [Primary DHCP Server] : プライマリ DHCP サーバの IP アドレス。
  - [Secondary DHCP Server] : セカンダリ DHCP サーバの IP アドレス。
  - [DHCP Proxy Mode] : 次のいずれかの DHCP プロキシ モードを選択できるドロップダウン リストです。

    [Global] : コントローラでグローバル DHCP プロキシ モードを使用します。

    [Enabled] : インターフェイスで DHCP プロキシ モードを有効にします。コントローラ上で DHCP プロキシを有効にした場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。少なくとも 1 つの DHCP サーバを、WLAN に関連付けられたインターフェイスか WLAN に設定する必要があります。

    [Disabled] : インターフェイスで DHCP プロキシ モードを無効にします。コントローラの DHCP プロキシを無効にすると、クライアントとの間で送受信されるそれらの DHCP パケットは、パケットの IP 部分が変更されることなくコントローラによってブリッジされます。クライアントから受信したパケットは CAPWAP トンネルから削除され、アップストリーム VLAN 上で送信されます。クライアント宛の DHCP パケットは、アップストリーム VLAN 上で受信され、802.11 に変換されて、CAPWAP トンネルを通ってクライアントに送信されます。したがって、DHCP プロキシが無効になっている場合は、内部 DHCP サーバは使用できません。
- [Access Control List] : ユーザ定義の ACL 名（または指定しない）。
- [mDNS Profile] : ユーザが mDNS プロファイルを選択できるドロップダウン リスト。デフォルトのオプションは [none] です。

現在のインターフェイスの詳細表示

現在のインターフェイスの詳細を表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

ステップ 4　該当するインターフェイスのインターフェイス名を選択します。[Interface Details] ページが表示されます。

ステップ 5　次のインターフェイス パラメータを表示または編集します。

（注）　インターフェイス パラメータを変更すると、WLAN が一時的に無効になり、一部のクライアントの接続が失われる場合があります。

- Interface Address
  - [VLAN Identifier] : 1 ～ 4096、または 0（タグなし）。

- Guest LAN
- [Quarantine]：VLAN の隔離を有効または無効にします。チェックボックスをオンにすると有効になります。
- [IP Address]：インターフェイスの IP アドレス。
- [Gateway]：インターフェイスのゲートウェイ アドレス。

• Physical Information
- [Primary Port Number (active)]：現在インターフェイスにより使用されているポート。
- [Secondary Port Number]：プライマリ ポートがダウンした場合に、インターフェイスにより使用されるポート。

（注）　プライマリおよびセカンダリ ポート番号は、Cisco 4400 シリーズ Wireless LAN Controller の場合のみ存在します。

（注）　セカンダリ ポートは、プライマリ ポートがシャットダウンした場合に使用されます。プライマリ ポートが再アクティブ化されると、Cisco 4400 シリーズ Wireless LAN Controller は、インターフェイスをプライマリ ポートに転送されます。

- [AP Management]：アクセス ポイント管理を有効にする場合に選択します。

• DHCP Information
- [Primary DHCP Server]：プライマリ DHCP サーバの IP アドレス。
- [Secondary DHCP Server]：セカンダリ DHCP サーバの IP アドレス。

• アクセス コントロール リスト
- [ACL Name]：アクセス コントロール リストのユーザ定義名（または指定しない）。

ステップ 6　行った変更を確定するには [Save] をクリックします。デバイス値を監査するには、[Audit] をクリックします。

ダイナミック インターフェイスの削除

ダイナミック インターフェイスを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

ステップ 4　削除するダイナミック インターフェイスのチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから [Delete Dynamic Interfaces] を選択します。

ステップ 6　[OK] をクリックして、削除を実行します。

（注）　インターフェイス グループに割り当てられているダイナミック インターフェイスは、削除できません。

コントローラ システム インターフェイス グループの設定

（注）　インターフェイス グループ機能はコントローラ ソフトウェア リリース 7.0.116.0 以降でサポートされます。

ここでは、コントローラ システム インターフェイス グループの設定方法について説明します。内容は次のとおりです。

- 「インターフェイス グループの追加」（P.9-328）
- 「インターフェイス グループの削除」（P.9-329）
- 「インターフェイス グループの表示」（P.9-329）

インターフェイス グループの追加

インターフェイス グループを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interface Groups] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add Interface Group] を選択します。

ステップ 5　必要なパラメータを入力します。

- [Name]：このインターフェイス グループのユーザ定義名（group1、group2）。
- [Description]：（任意）インターフェイス グループの説明。
- [Quarantine]：VLAN の隔離を有効または無効にします。チェックボックスをオンにすると有効になります。
- [mDNS Profile]：ユーザが mDNS プロファイルを選択できるドロップダウン リスト。デフォルトのオプションは [none] です。

ステップ 6　[Add] をクリックします。

[Interface] ダイアログボックスが表示されます。

ステップ 7　グループに追加するインターフェイスを選択して、[OK] をクリックします。

[Interface Group] ページからインターフェイスを削除するには、インターフェイスを選択して [Remove] をクリックします。

ステップ 8　[Interface Group] ページへのインターフェイスの追加が完了したら、次のいずれかのボタンをクリックします。

- [Save] で行った変更を確定します。
- [Cancel] で変更を廃棄します。

（注）
- インターフェイス グループに追加できるインターフェイスの数は、コントローラのタイプに応じて異なります。
- ゲスト LAN インターフェイスは、インターフェイス グループに含めることはできません。
- インターフェイス グループ名は、インターフェイス名とは別にする必要があります。

インターフェイス グループの削除

インターフェイス グループを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interface Groups] の順に選択します。

ステップ 4　削除するインターフェイス グループのチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから、[Delete Interface Group] を選択し、[Go] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

（注）
- WLAN に割り当てられているインターフェイス グループは、削除できません。
- AP グループに割り当てられているインターフェイス グループは、削除できません。
- WLAN の外部コントローラ マッピングに割り当てられているインターフェイス グループは、削除できません。
- WLAN テンプレートに割り当てられているインターフェイス グループ テンプレートは、削除できません。
- AP グループ テンプレートに割り当てられているインターフェイス グループ テンプレートは、削除できません。
- インターフェイス グループに割り当てられているインターフェイスの隔離は、有効または無効にできません。

インターフェイス グループの表示

既存のインターフェイス グループを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interface Groups] の順に選択します。次のパラメータが表示されます。
- [Name]：インターフェイス グループのユーザ定義名（例：group1、group2）。
- [Description]：（任意）インターフェイス グループの説明。

- [Interfaces]：グループに属しているインターフェイスの数。

ステップ 4　インターフェイス グループ名のリンクをクリックします。

[Interface Groups Details] ページが表示され、インターフェイス グループの詳細と、特定のインターフェイス グループの一部を構成するインターフェイスの詳細が示されます。

NAC 統合

Cisco NAC アプライアンス（Cisco Clean Access（CCA）とも呼ばれます）は、ネットワーク管理者がユーザにネットワークへの接続を許可する前に、有線および無線経由のユーザ、リモートのユーザおよびそのマシンを許可、承認、評価、感染修復するネットワーク アドミッション コントロール（NAC）製品です。Cisco NAC アプライアンスは、マシンがセキュリティ ポリシーに準拠しているかどうかを判別し、脆弱性を修復してから、ネットワークへのアクセスを許可します。NAC アプライアンスは、インバンド モードとアウトオブバンド モードの 2 つのモードで利用できます。お客様は、必要ならば両方のモードを導入して、それぞれが特定のタイプのアクセスを担当するようにすることもできます。たとえば、インバンドで無線接続ユーザをサポートし、アウトオブバンドで有線接続ユーザを担当するといった構成も可能です。

ここでは、次の内容について説明します。

- 「SNMP NAC を使用する際のガイドライン」（P.9-330）
- 「NAC アウトオブバンド統合（SNMP NAC）の設定」（P.9-331）

SNMP NAC を使用する際のガイドライン

SNMP NAC アウトオブバンド統合を使用する場合は、次のガイドラインに従ってください。

- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。したがって、複数の NAC アプライアンスの導入を必要とする場合があります。
- NAC アプライアンスでは静的な VLAN マッピングがサポートされているため、コントローラ上で設定されているインターフェイスごとに一意の隔離 VLAN を設定する必要があります。たとえば、コントローラ 1 で 110 という隔離 VLAN を設定し、コントローラ 2 で 120 という隔離 VLAN を設定します。ただし、2 つの WLAN またはゲスト LAN が、コントローラのダイナミック インタフェースとして同一の VLAN を使用している場合、ネットワーク内に導入された NAC アプライアンスが 1 つならば、同じ隔離 VLAN を使用する必要があります。NAC アプライアンスは、一意の隔離 - アクセス VLAN マッピングをサポートします。
- セッションの失効に基づくポスチャ再評価の場合、NAC アプライアンスと WLAN の両方にセッション タイムアウトを設定し、WLAN でのセッションの失効が NAC アプライアンスでの失効より大きいことを確認します。
- オープン WLAN でセッション タイムアウトが設定されると、Quarantine 状態にあるクライアントのタイムアウトは NAC アプライアンスのタイマーによって判定されます。Web 認証を使用する WLAN においてセッションがタイムアウトすると、クライアントはコントローラから認証解除されるので、ポスチャ検証を再度実行する必要があります。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。
- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。

- NAC アウトオブバンド統合は、WLAN AAA Override 機能では使用できません。
- レイヤ 2 およびレイヤ 3 認証はすべて、隔離 VLAN で実行されます。外部 Web 認証を使用するには、外部 Web サーバからの HTTP トラフィックおよび外部 Web サーバへの HTTP トラフィックを許可するとともに、隔離 VLAN でのリダイレクト URL を許可するように NAC アプライアンスを設定する必要があります。

（注）　設定手順については、次の URL にある Cisco NAC アプライアンスのコンフィギュレーション ガイドを参照してください。
http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

RADIUS NAC を使用する際のガイドライン

RADIUS NAC を使用する場合には、次のガイドラインに従ってください。

- RADIUS NAC は、802.1x/WPA/WPA2 レイヤ 2 セキュリティを備えた WLAN のみが使用できます。
- RADIUS NAC は、FlexConnect ローカル スイッチングが有効の場合は有効にできません。
- RADIUS NAC を設定する場合は、AAA オーバーライドを有効にしてください。

NAC アウトオブバンド統合（SNMP NAC）の設定

SNMP NAC アウトオブバンド統合を設定するには、次の手順を実行します。

ステップ 1　動的インターフェイスに隔離 VLAN を設定する手順は、次のとおりです。

a. [Configure] > [Controller] の順に選択します。

b. [IP Address] 列でアウトオブバンド統合の設定を行うコントローラをクリックして選択します。

c. 左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。

d. [Select a command] ドロップダウン リストから [Add Interface] を選択します。

e. [Interface Name] テキスト ボックスに、"quarantine" など、このインターフェイスの名前を入力します。

f. [VLAN Identifier] テキスト ボックスに、"10" など、アクセス VLAN ID の 0 以外の値を入力します。

g. インターフェイスに隔離 VLAN ID が設定されている場合は、[Quarantine] チェックボックスをオンにします。

（注）　ネットワーク全体で一意の隔離 VLAN を設定することを推奨します。同じモビリティ グループ内に複数のコントローラが設定されており、すべてのコントローラのアクセス インターフェイスが同じサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、同じ隔離 VLAN を保持する必要があります。同じモビリティ グループ内に複数のコントローラが設定されており、すべてのコントローラのアクセス インターフェイスが別々のサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、別々の隔離 VLAN を保持する必要があります。

h. このインターフェイスの残りのフィールド（IP アドレス、ネットマスク、デフォルト ゲートウェイなど）を設定します。

i. プライマリおよびセカンダリ DHCP サーバの IP アドレスを入力します。

j. [Save] をクリックします。これで、NAC を有効にしたの WLAN またはゲスト LAN を作成する準備ができました。

ステップ 2　WLAN またはゲスト LAN で NAC アウトオブバンド サポートを設定する手順は、次のとおりです。

a. 左側のサイドバーのメニューから、[WLANs] > [WLAN] の順に選択します。

b. [Select a command] ドロップダウン リストから [Add a WLAN] を選択し、[Go] をクリックします。

c. このコントローラに適用する作成済みのテンプレートがある場合には、ドロップダウン リストからゲスト LAN テンプレート名を選択します。そうでない場合には、[click here] リンクをクリックして新しいテンプレートを作成します。テンプレートの設定の詳細については、「有線ゲスト アクセスの設定」（P.9-332）のセクションを参照してください。

d. [Advanced] タブをクリックします。

e. この WLAN またはゲスト LAN に SNMP NAC サポートを設定するには、[NAC Stage] ドロップダウン リストから [SNMP NAC] を選択します。SNMP NAC サポートを無効にするには、[NAC Stage] ドロップダウン リストから [None]（デフォルト値）を選択します。

f. [Apply] をクリックして、変更を確定します。

ステップ 3　特定の AP グループに NAC アウトオブバンド サポートを設定するには、次の手順を実行します。

a. 左側のサイドバーのメニューから、[WLANs] > [AP Groups VLAN] の順に選択し、[AP Groups] ページを表示します。

（注） AP グループ（5.2 以降のコントローラ）は、5.2 よりも前のコントローラでは AP グループ VLAN と呼ばれます。

b. 目的の AP グループの名前をクリックします。

c. [Interface Name] ドロップダウン リストから、隔離を有効にしたインターフェイスを選択します。

d. この AP グループに SNMP NAC サポートを設定するには、[Nac State] ドロップダウン リストから [SNMP NAC] を選択します。NAC アウトオブバンドのサポートを無効にするには、[NAC State] ドロップダウン リストから [None]（デフォルト値）を選択します。

e. [Apply] をクリックして、変更を確定します。

ステップ 4　クライアントの現在の状態（Quarantine または Access）を表示する手順は、次のとおりです。

a. [Monitor] > [Clients] を選択して、[Clients] を開きます。クライアントの検索を実行します。

b. 目的のクライアントの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。[Security Information] セクションの下に NAC ステートが [Access]、[Invalid]、または [Quarantine] と表示されます。

有線ゲスト アクセスの設定

有線ゲスト アクセスでは、ゲスト ユーザがゲスト アクセス用に指定および設定された有線イーサネット接続からゲスト アクセス ネットワークへ接続できます。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。

無線ゲスト ユーザ アカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。「ゲスト アカウントの設定」（P.15-861）を参照してください。

有線ゲスト アクセスは、スタンドアロン設定、またはアンカーおよび外部のコントローラを配置したデュアル コントローラ設定で設定することができます。この後者の設定は、有線ゲスト アクセス トラフィックをさらに隔離するために使用されますが、有線ゲスト アクセスの展開には必須ではありません。

有線ゲスト アクセス ポートは、最初、レイヤ 2 アクセス スイッチか、有線ゲストのアクセス トラフィック用 VLAN インターフェイスで設定されたスイッチ ポートで終端します。

有線ゲスト トラフィックは、その後、アクセス スイッチから無線 LAN コントローラへトランキングされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。

2 つのコントローラが使用されている場合、外部コントローラがスイッチから有線ゲスト トラフィックを受信し、次に有線ゲスト トラフィックをアンカーコントローラへ転送します。アンカーコントローラも有線ゲストのアクセスに対して設定されています。有線ゲスト トラフィックがアンカー コントローラへ正常に渡されると、外部コントローラとアンカー コントローラ間に双方向の Ethernet over IP（EoIP）トンネルが確立され、このトラフィックを処理します。

（注） 2 つのコントローラが展開されるとき、有線ゲスト アクセスはアンカーと外部アンカーによって管理されますが、有線ゲスト アクセス クライアントではモビリティがサポートされていません。この場合、DHCP およびクライアントの Web 認証は、アンカー コントローラによって処理されます。

（注） ロールと帯域幅コントラクトを設定して割り当てることで、ネットワーク内の有線ゲスト ユーザに割り当てる帯域幅の量を指定できます。これらの機能の設定の詳細については、「ゲスト アカウントの設定」（P.15-861）を参照してください。

ネットワークの有線ゲスト ユーザのアクセスを設定して有効にするには、次の手順を実行します。

ステップ 1　有線ゲスト ユーザ アクセス用のダイナミック インターフェイスを設定するには、[Configure] > [Controllers] を選択し、IP アドレスを選択してから、[System] > [Interfaces] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから [Add Interface] を選択し、[Go] をクリックします。

ステップ 3　新しいインターフェイスの名前と VLAN ID を入力します。

ステップ 4　[Guest LAN] チェックボックスをオンにします。

ステップ 5　プライマリ ポート番号とセカンダリ ポート番号を入力します。

ステップ 6　[Save] をクリックします。これで、ゲスト アクセス用の有線 LAN を作成できるようになりました。

ステップ 7　ゲスト ユーザ アクセス用の有線 LAN を設定するには、左側のサイドバーのメニューから [WLANs] > [WLAN configuration] の順に選択します。

ステップ 8　[Select a command] ドロップダウン リストから [Add a WLAN] を選択し、[Go] をクリックします。

ステップ 9　このコントローラに適用する作成済みのテンプレートがある場合には、ドロップダウン リストからゲスト LAN テンプレート名を選択します。そうでない場合には、[click here] リンクをクリックして新しいテンプレートを作成します。

ステップ 10　[WLAN] > [New Template] の [General] ページで、ゲスト LAN を特定する [Profile Name] テキストボックスに名前を入力します。入力する名前には、スペースを使用しないでください。

ステップ 11　[WLAN Status] フィールドの [Enabled] チェックボックスをオンにします。

ステップ 12　[Ingress Interface] ドロップダウン リストから、ステップ 3 で作成した VLAN を選択します。この VLAN は、レイヤ 2 アクセス スイッチを経由して、有線ゲスト クライアントとコントローラとの間のパスを提供します。

ステップ 13　[Egress Interface] ドロップダウン リストから、インターフェイスの名前を選択します。この WLAN は、有線ゲスト クライアント トラフィックのコントローラから送信されるパスを提供します。

（注）　設定でコントローラが 1 つしかない場合は、[Egress Interface] ドロップダウン リストから [management] を選択します。

ステップ 14　[Security] > [Layer 3] タブをクリックして、デフォルトのセキュリティ ポリシー（Web 認証）を変更するか、または WLAN 固有の Web 認証（ログイン、ログアウト、ログイン失敗）ページとサーバ ソースを割り当てます。

a.　セキュリティ ポリシーをパススルーに変更するには、[Web Policy] チェックボックスをオンにして、[Passthrough] オプション ボタンを選択します。これでユーザは、ユーザ名やパスワードを入力しなくてもネットワークにアクセスできます。

[Email Input] チェックボックスが表示されます。ユーザがネットワークに接続しようとしたとき、電子メール アドレスの入力を求める場合は、このチェックボックスをオンにします。

b.　カスタムな Web 認証ページを指定するには、[Global WebAuth Configuration] の [Enabled] チェックボックスをオフにします。

[Web Auth Type] ドロップダウン リストが表示されたら、次のいずれかのオプションを選択して、無線ゲスト ユーザ用の Web ログイン ページを定義します。

[Default Internal]：コントローラのデフォルト Web ログイン ページを表示します。768 ビットは、デフォルト値です。

[Customized Web Auth]：カスタム Web ログイン ページ、ログイン失敗ページ、およびログアウト ページを表示します。[Customized] オプションを選択した場合は、ログイン ページ、ログイン失敗ページ、およびログアウト ページを選択するための 3 つのドロップダウン リストが表示されます。これらすべてのオプションについてカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン リストで [None] を選択します。

これらオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。カスタム ページのダウンロードの詳細は、「コントローラへのカスタマイズ Web 認証バンドルのダウンロード」（P.9-299）を参照してください。

[External]：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

外部認証を行う場合は、[Security] > [AAA] ペインで RADIUS サーバまたは LDAP サーバを選択できます。その場合は、ステップ 17 に進んでください。

（注）　[Security] > [AAA] ペインで選択できるように、RADIUS 外部サーバと LDAP 外部サーバを事前に設定しておく必要があります。[RADIUS Authentication Servers]、[TACACS+ Authentication Servers]、および [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 15　ステップ 15 の [Web Authentication Type] で [External] を選択した場合は、[Security] > [AAA] を選択して、ドロップダウン リストから RADIUS サーバまたは LDAP サーバを 3 つまで選択します。

ステップ 16　[Save] をクリックします。

ステップ 17　2 番めの（アンカー）コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

入力インターフェイスの作成

入力インターフェイスを作成するには、次の手順を実行します。

ステップ 1　[Select a command] ドロップダウン リストから [Add Interface] を選択し、[Go] をクリックします。

ステップ 2　インターフェイス名をクリックします。[Interfaces Details : New Config] ページが表示されます。

ステップ 3　[Interface Name] テキスト ボックスに、guestinterface など、このインターフェイスの名前を入力します。

ステップ 4　新しいインターフェイスの VLAN ID を入力します。

ステップ 5　[Guest LAN] チェックボックスをオンにします。

ステップ 6　プライマリ ポート番号とセカンダリ ポート番号を入力します。

ステップ 7　[Save] をクリックします。

出力インターフェイスの作成

出力インターフェイスを作成するには、次の手順を実行します。

ステップ 1　[Select a command] ドロップダウン リストから [Add Interface] を選択し、[Go] をクリックします。

ステップ 2　インターフェイス名をクリックします。[Interfaces Details : New Config] ページが表示されます。

ステップ 3　[Interface Name] テキスト ボックスに、quarantine など、このインターフェイスの名前を入力します。

ステップ 4　[VLAN Identifier] テキスト ボックスに、10 など、アクセス VLAN ID の 0 以外の値を入力します。

ステップ 5　[Quarantine] チェックボックスをオンにし、隔離 VLAN ID に 110 など 0 以外の値を入力します。

（注）　[Quarantine] が有効なインターフェイスの場合、[WLAN or guest WLAN template Advanced] タブで NAC サポートを有効にできます。

ステップ 6　IP アドレス、ネットマスク、デフォルト ゲートウェイを入力します。

ステップ 7　プライマリ ポート番号とセカンダリ ポート番号を入力します。

ステップ 8　プライマリおよびセカンダリ DHCP サーバの IP アドレスを入力します。

ステップ 9　インターフェイスの残りのフィールドを設定し、[Save] をクリックします。

これで、ゲスト アクセス用の有線 LAN を作成できるようになりました。

コントローラのネットワーク ルートの設定

[Network Route] ページでは、コントローラのサービス ポートにルートを追加できます。このルートを使用することで、すべてのサービス ポート トラフィックを指定した管理 IP アドレスに送ることができます。

- 「既存のネットワーク アドレスの表示」（P.9-336）
- 「ネットワーク ルートの追加」（P.9-336）

既存のネットワーク アドレスの表示

既存のネットワーク ルートを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Network Route] の順に選択します。次のパラメータが表示されます。

- [IP Address]：ネットワーク ルートの IP アドレス。
- [IP Netmask]：ルートのネットワーク マスク。
- [Gateway IP Address]：ネットワーク ルートのゲートウェイ IP アドレス。

ネットワーク ルートの追加

ネットワーク ルートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Network Route] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add Network Route] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　IP アドレス、IP ネットマスク、およびゲートウェイ IP アドレスの情報を入力します。

ステップ 7　[Save] をクリックします。

コントローラのスパニングツリー プロトコル パラメータの設定

スパニングツリー プロトコル（STP）は、ネットワーク内の有害なループを防止しながら、パスの冗長性を実現するリンク管理プロトコルです。

現在の STP パラメータを表示または管理するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Spanning Tree Protocol] の順に選択します。[Spanning Tree Protocol] ページに、次のパラメータが表示されます。

- [Protocol Spec]：現在のプロトコル仕様。
- [Admin Status]：有効にする場合は、このチェックボックスをオンにします。
- [Priority]：最適なスイッチのプライオリティ番号。
- [Maximum Age (seconds)]：ポートに対して記録された受信プロトコル情報が廃棄されるまでの時間（秒単位）。

- [Hello Time (seconds)]：スイッチが hello メッセージをその他のスイッチにブロードキャストする頻度（秒単位）を特定します。
- [Forward Delay (seconds)]：スイッチのポートがラーニング / リスニング ステートでの経過時間（秒単位）。

コントローラのモビリティ グループの設定

モビリティ グループを作成すると、複数のネットワーク コントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータ トラフィックを転送できるようになります。コントローラは、クライアント デバイスのコンテキストと状態およびコントローラのロード情報を共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。

（注）　ネットワーク内の無線クライアントが、あるコントローラに接続したアクセス ポイントから、別のコントローラに接続したアクセス ポイントへローミングできるとしたら、どちらのコントローラも同じモビリティ グループに属しているはずです。

- 「モビリティ グループ内でのメッセージング」（P.9-337）
- 「モビリティ グループの前提条件」（P.9-337）
- 「現在のモビリティ グループ メンバの表示」（P.9-338）
- 「コントローラのリストからのモビリティ グループ メンバの追加」（P.9-338）
- 「モビリティ グループ メンバの手動追加」（P.9-338）
- 「モビリティ スケーラビリティ パラメータの設定」（P.9-339）

モビリティ グループ内でのメッセージング

コントローラでは、モビリティ メッセージを他のメンバ コントローラに送信することにより、クライアントにサブネット間モビリティが提供されます。

- リリース 5.1 以降のコントローラ ソフトウェアでは、モビリティ リストで 72 台までのコントローラをサポートします。すべてのリリースにわたって、モビリティ グループで 24 台までのコントローラをサポートしています。
- コントローラは、新しいクライアントがアソシエートされるたびに、モビリティ リスト内のメンバに Mobile Announce メッセージを送信します。
- Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、コントローラでマルチキャスト モードを使用して Mobile Announce メッセージを送信します。これにより、コントローラからネットワークに送られるメッセージはメンバ数にかかわらず、ただ 1 つになります。このコピーはモビリティ メンバすべてを含むマルチキャスト グループに宛てて配信されます。

モビリティ グループの前提条件

コントローラをモビリティ グループに追加する前に、グループに追加するコントローラすべてについて、次の要件が満たされていることを確認する必要があります。

- すべてのコントローラには同じ CAPWAP モードを設定する必要があります（レイヤ 2 またはレイヤ 3）。
- すべてのデバイスの管理インターフェイス間に IP 接続が存在する必要があります。

- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。
- すべてのデバイスを、同じ仮想インターフェイス IP アドレスに設定する必要があります。
- モビリティ グループに含める各コントローラの MAC および IP アドレスが使用可能である必要があります（コントローラにその他すべてのモビリティ グループ メンバの MAC アドレスおよび IP アドレスを設定するため）。

現在のモビリティ グループ メンバの表示

現在のモビリティ グループ メンバを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Mobility Groups] の順に選択します。

（注）　グループ メンバを削除するには、該当するグループ メンバのチェックボックスをオンにして [Delete Group Members] を選択し、[Go] をクリックします。

コントローラのリストからのモビリティ グループ メンバの追加

既存のコントローラのリストからモビリティ グループ メンバを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Mobility Groups] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Group Members] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　モビリティ グループに追加するコントローラのチェックボックスをオンにします。

ステップ 7　[Save] をクリックします。

モビリティ グループ メンバの手動追加

モビリティ グループに追加するコントローラが見つからない場合は、手動でメンバを追加できます。モビリティ グループに手動でメンバを追加するには、次の手順を実行します。

ステップ 1　[Mobility Group Member] の [Details] ページで [click here] リンクをクリックします。

ステップ 2　[Member MAC Address] テキスト ボックスに、追加するコントローラの MAC アドレスを入力します。

ステップ 3　[Member IP Address] テキスト ボックスに、追加するコントローラの管理インターフェイスの IP アドレスを入力します。

（注）　ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する場合は、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

ステップ 4　マルチキャスト モビリティ メッセージに使用するマルチキャスト グループ IP アドレスを [Multicast Address] テキスト ボックスに入力します。ローカル モビリティ メンバのグループ アドレスは、ローカル コントローラのグループ アドレスと同じである必要があります。

ステップ 5　[Group Name] テキスト ボックスに、モビリティ グループ名を入力します。

ステップ 6　[Save] をクリックします。

ステップ 7　残りの WLC デバイスに対して、ステップ 1 ～ 6 を繰り返します。

モビリティ スケーラビリティ パラメータの設定

（注）　モビリティ スケーラビリティ パラメータを設定する前に、モビリティ グループを設定しておく必要があります。

モビリティ メッセージ パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　ソフトウェア バージョンが 5.0 以降のコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [General] の順に選択します。

ステップ 4　[Multicast Mobility Mode] ドロップダウン リストで、マルチキャスト モードを使用してモビリティ メンバに Mobile Announce メッセージを送信する機能を、このコントローラに対して有効または無効にするかを指定します。

ステップ 5　マルチキャスト モビリティ モードを有効に設定してマルチキャスト メッセージングを有効にした場合は、[Mobility Group Multicast-address] フィールドにグループ IP アドレスを入力してマルチキャスト モビリティ メッセージングを開始する必要があります。この IP アドレスの設定はローカル モビリティ グループに対しては必須ですが、モビリティ リスト内のその他のグループに対してはオプションです。その他の（非ローカル）グループに IP アドレスを設定しない場合、コントローラはユニキャスト モードを使用してこれらのメンバーにモビリティ メッセージを送信します。

ステップ 6　[Save] をクリックします。

コントローラのネットワーク タイム プロトコルの設定

新しい NTP サーバを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Network Time Protocol] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add NTP Server] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[Select a template to apply to this controller] ドロップダウン リストから、このコントローラに適用する適切なテンプレートを選択します。

コマンド ボタン

- Apply
- Cancel

NTP サーバ用の新しいテンプレートを作成するには、[click here] リンクを使用して、テンプレート作成ページにアクセスします（[Configure NTP Servers] > [New Template]）。

NTP の一般パラメータには、次のものがあります。

- [Template Name] : 新しい NTP テンプレート名を入力します。

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- [Server Address] : NTP サーバの IP アドレスを入力します。
- [No.of Controllers Applied To] : このテンプレートを適用するコントローラの数（読み取り専用）。

メッシュ ネットワークの 1510 でのバックグラウンド スキャン

バックグラウンド スキャンにより、Cisco Aironet 1510 アクセス ポイントは、より最適なパスと親を探すために、能動的に連続して別のネイバーがいるチャネルをモニタできます。アクセス ポイントは現在のチャネルだけでなくネイバー チャネル上でも検索を実行するため、最適な代替パスおよび親のリストは大きくなります。

親を喪失する前にこの情報を特定すると、より高速な転送速度およびそのアクセス ポイントにとって最適なリンクが実現します。さらに、新しいチャネル上のリンクが、ホップの少なさ、信号対雑音比（SNR）の強さなどの点で、現在のチャネルよりも良好であると判明した場合は、アクセス ポイントはそのチャネルに切り替わる場合があります。

その他のチャネル上でのバックグラウンド スキャンおよびそれらのチャネル上のネイバーからのデータ収集は、2 つのアクセス ポイント間のプライマリ バックホール上で実行されます。

1510 のプライマリ バックホールは、802.11a リンク上で動作します。

バックグラウンド スキャンは、アクセス ポイントのアソシエートされたコントローラ上でグローバルに有効化されます。

（注）　音声コールが新しいチャネルに切り替わると、遅延が大きくなる場合があります。

（注）　EMEA 規制区域では、DFS 要件が前提となるため、その他のチャネル上でのネイバーの検索に時間がかかる場合があります。

バックグラウンド スキャンのシナリオ

バックグラウンド スキャンの動作をより詳しく説明するために、いくつかのシナリオを示します。

図 9-1 では、メッシュ アクセス ポイント（MAP1）は、最初にアップしたときに両方のルート アクセス ポイント（RAP1 および RAP2）を、親になる可能性があると認識しています。ここでは、ホップ、SNR などの点で RAP2 を経由したルートの方が良好であるため、RAP2 が親として選択されています。リンクの確立後、バックグラウンド スキャン（有効にした場合）は、すべてのチャネルを継続的にモニタし、より最適なパスおよび親を検索します。RAP2 は、リンクがダウンするか、より最適なパスが別のチャネルで見つかるまで、MAP1 の親としての動作を継続し、チャネル 2 上で通信を続けます。

図 9-1　　メッシュ アクセス ポイント（MAP1）による親の選択

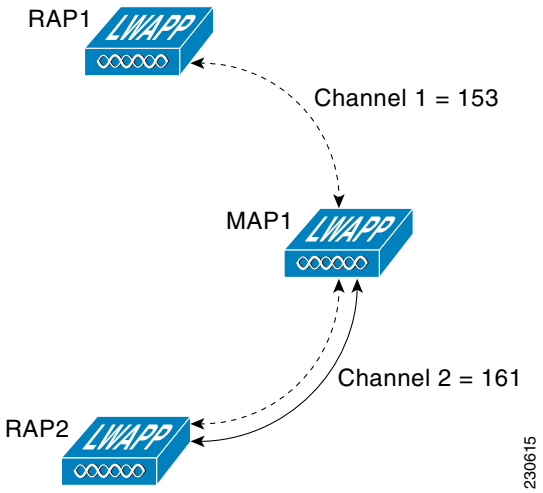
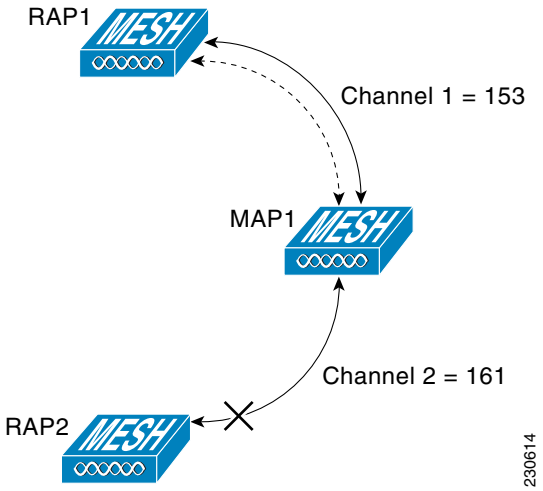


図 9-2 では、MAP1 と RAP2 間のリンクが失われています。現在実行中のバックグラウンド スキャンからのデータにより、RAP1 と Channel 1 が、MAP1 にとって 2 番めに最適な親および通信パスであると識別されるため、RAP2 とのリンクがダウンした後に、追加のスキャンなしでリンクがただちに確立されます。

図 9-2　　バックグラウンド スキャンによる新しい親の識別



バックグラウンド スキャンの有効化

AP1510 RAP または MAP でバックグラウンド スキャンを有効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

（注）　これは、コントローラのテンプレートでも有効にできます。「メッシュ テンプレートの設定」（P.11-718）を参照してください。

ステップ 2　左側のサイドバーのメニューから、[Mesh] > [Mesh Settings] の順に選択します。[Mesh Settings] ページが表示されます。

ステップ 3　バックグラウンド スキャンを有効にする場合は [Background Scanning] チェックボックスをオンにし、この機能を無効にする場合はオフにします。デフォルト値は [disabled] です。

ステップ 4　[Save] をクリックします。

コントローラ QoS プロファイルの設定

QoS プロファイルを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [QoS Profiles] の順に選択します。次のパラメータが表示されます。

- [Bronze]：バックグラウンド用
- [Gold]：ビデオ アプリケーション用
- [Platinum]：音声アプリケーション用
- [Silver]：ベスト エフォート用

ステップ 4　該当するプロファイルをクリックして、プロファイル パラメータを表示または編集します。

ステップ 5　[Per-User Bandwidth Contracts] グループ ボックスで次の値を設定します（デフォルトはすべて 0 つまりオフ）。

- [Average Data Rate]：非 UDP トラフィックの平均データ レート。
- [Burst Data Rate]：非 UDP トラフィックのピーク データ レート。
- [Average Real-time Rate]：UDP トラフィックの平均データ レート。
- [Burst Real-time Rate]：UDP トラフィックのピーク データ レート。

ステップ 6　[Over-the-Air QoS] グループ ボックスで次の値を設定します。

- [Maximum QoS RF Usage Per AP (%)]：クライアントが使用できる最大無線帯域幅。デフォルトは 100% です。
- [QoS Queue Depth]：クライアントのクラスのキュー深度。これより大きな値のパケットは、アクセス ポイントでドロップされます。

ステップ 7　[WLAN QoS] グループ ボックスで次の値を設定します。

- 最大プライオリティ

- ユニキャストのデフォルト プライオリティ
- マルチキャストのデフォルト プライオリティ

ステップ 8　[Wired QoS Protocol] グループ ボックスで次の値を設定します。

- [Wired QoS Protocol]：802.1P プライオリティ タグをアクティブにするには [802.1P] を選択し、802.1P プライオリティ タグを非アクティブ化するには [None] を選択します。

ステップ 9　[Save] をクリックします。

コントローラ DHCP スコープの設定

ここでは、次の内容について説明します。

- 「現在の DHCP スコープの表示」（P.9-343）
- 「新しい DHCP スコープの追加」（P.9-343）

現在の DHCP スコープの表示

現在の DHCP（Dynamic Host Configuration Protocol）スコープを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [DHCP Scopes] の順に選択します。

次の DHCP スコープの情報が表示されます。

- プール アドレス
- リース時間
- ステータス

新しい DHCP スコープの追加

新しい DHCP スコープを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [DHCP Scopes] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add DHCP Scope] を選択します。

ステップ 5　次の情報を入力します。

- スコープ名
- リース時間（秒単位）
- ネットワーク
- ネットマスク
- プールの開始アドレス

- プールの終了アドレス
- DNS ドメイン名
- ステータス
- ルータ アドレス：いずれの IP アドレスがすでに使用中であり、そのため除外する必要があるか入力します。たとえば、会社のルータの IP アドレスを入力します。この場合、この IP アドレスは他のクライアントが使用できないようにブロックされます。
- DNS サーバ：DNS サーバの IP アドレスを入力します。各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。
- NetBios サーバ：Windows インターネット ネーム サービス（WINS）サーバなど、Microsoft Network Basic Input Output System（NetBIOS）ネーム サーバの IP アドレスを入力します。

ステップ 6　[Save] をクリックします。

コントローラのユーザ ロールの設定

ここでは、次の内容について説明します。

- 「現在のローカル ネット ユーザ ロールの表示」（P.9-344）
- 「新しいローカル ネット ユーザ ロールの追加」（P.9-345）

現在のローカル ネット ユーザ ロールの表示

現在のローカル ネット ユーザ ロールを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [User Roles] の順に選択します。

次の Local Net User Role パラメータが表示されます。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- Role Name
- [Average Data Rate]：非 UDP トラフィックの平均データ レート。
- [Burst Data Rate]：非 UDP トラフィックのピーク データ レート。
- [Average Real-time Rate]：UDP トラフィックの平均データ レート。
- [Burst Real-time Rate]：UDP トラフィックのピーク データ レート。

ステップ 4　テンプレート名をクリックして、ユーザ ロールの詳細を表示します。

新しいローカル ネット ユーザ ロールの追加

新しいローカル ネット ユーザ ロールを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [User Roles] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add User Role] を選択します。

ステップ 5　[Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6　[Apply] をクリックします。

（注）　ローカル ネット ユーザ ロールに新しいテンプレートを作成するには、[click here] リンクをクリックしてテンプレート作成ページにアクセスします。ユーザ ロール テンプレートの詳細については、「ユーザ ロール コントローラ テンプレートの設定」（P.11-610）を参照してください。

グローバル アクセス ポイント パスワードの設定

[AP Username Password] ページでは、すべてのアクセス ポイントがコントローラに接続する際に継承する、グローバル パスワードを設定できます。また、アクセス ポイントを追加するときに、このグローバル ユーザ名およびパスワードを受け入れるか、アクセス ポイント単位で上書きするかを選択できます。グローバル パスワードの表示場所およびアクセス ポイント単位での上書き方法については、「AP 設定テンプレートの設定」（P.11-736）を参照してください。

さらにコントローラ ソフトウェア リリース 5.0 では、アクセス ポイントをコントローラに接続すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、アクセス ポイントのコンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

グローバル ユーザ名とパスワードを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　リリース 5.0 以降のコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [AP Username Password] の順に選択します。

ステップ 4　コントローラに接続するアクセス ポイントで継承されるユーザ名およびパスワードを入力します。

（注）　Cisco IOS アクセス ポイントの場合は、イネーブル パスワードも入力して確認する必要があります。

ステップ 5　[Save] をクリックします。

グローバル CDP の設定

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。

（注）　CDP は、イーサネット ポートおよび無線ポート上で、デフォルトで有効になっています。

（注）　グローバル インターフェイス CDP 設定は、AP レベルで CDP を有効にした AP のみに適用されます。

グローバル CDP を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　必要なコントローラの IP アドレスを選択します。

ステップ 3　左側のサイドバーのメニューから、[System] > [Global CDP Configuration] の順に選択します。[Global CDP Configuration] ページが表示されます。

ステップ 4　[Global CDP] グループ ボックスで、次のパラメータを設定します。

- [CDP on controller]：コントローラで CDP を有効にするか、無効にするかを選択します。

  （注）　この設定は、WiSM2 コントローラには適用できません。

- [Global CDP on APs]：アクセス ポイントで CDP を有効にするか、無効にするかを選択します。
- [Refresh-time Interval (seconds)]：[Refresh Time Interval] フィールドに、CDP メッセージが生成される時間を秒単位で入力します。デフォルト値は 60 です。
- [Holdtime (seconds)]：CDP ネイバー エントリの期限が切れるまでの時間を秒単位で入力します。デフォルト値は 180 です。
- [CDP Advertisement Version]：使用する CDP プロトコルのバージョンを入力します。デフォルトは v1 です。

ステップ 5　[CDP for Ethernet Interfaces] グループ ボックスで、CDP を有効にするイーサネット インターフェイスのスロットを選択します。

（注）　[CDP for Ethernet Interfaces] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 6　[CDP for Radio Interfaces] グループ ボックスで、CDP を有効にする無線インターフェイスのスロットを選択します。

（注）　[CDP for Radio Interfaces] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 7　[Save] をクリックします。

AP 802.1X サプリカント クレデンシャルの設定

Lightweight アクセス ポイントとスイッチ間の 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。すべてのアクセス ポイントがコントローラ接続時に継承するグローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。

必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセス ポイントに割り当てることができます。詳細については、「アクセス ポイントの詳細の設定」（P.9-477）を参照してください。

グローバル サプリカント クレデンシャルを有効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　必要なコントローラの IP アドレスを選択します。

ステップ 3　左側のサイドバーのメニューから、[System] > [AP 802.1X Supplicant Credentials] の順に選択します。

ステップ 4　[Global Supplicant Credentials] チェックボックスをオンにします。

ステップ 5　サプリカント ユーザ名を入力します。

ステップ 6　適切なパスワードを入力して確定します。

ステップ 7　[Save] をクリックします。

（注）　保存後に、[Audit] をクリックして、このコントローラで監査を実行できます。詳細については、「コントローラ監査レポートについて」（P.9-285）または「監査の設定」（P.15-853）を参照してください。

コントローラ DHCP の設定

コントローラの DHCP（Dynamic Host Configuration Protocol）情報を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　必要なコントローラの IP アドレスを選択します。

ステップ 3　左側のサイドバーのメニューから、[System] > [DHCP] の順に選択します。

ステップ 4　次のパラメータを追加または変更します。

- [DHCP Option 82 Remote Id Field Format]：DHCP オプション 82 はネットワークで DHCP リレーエージェント（WLC）が DHCP サーバへクライアントの接続ポイントの情報を渡すことができるようにするために使用されます。ドロップダウン リストから、次のいずれかを選択します。
  - AP-MAC
  - AP-MAC-SSID

- AP-ETHMAC
- AP-NAME-SSID
- AP-GROUP-NAME
- FLEX-GROUP-NAME
- AP-LOCATION
- AP-MAC-VLAN-ID
- AP-ETHMAC-SSID

（注）　DHCP オプション 82 の RemoteID フィールドのフォーマットを設定する場合
Ap-Mac を選択した場合、RemoteID フォーマットは [*AP-Mac*] に設定します。
Ap-Mac-ssid を選択した場合、RemoteID フォーマットは [*AP-Mac:SSID*] に設定します。

- [DHCP Proxy]：プロキシで DHCP を有効にする場合は、このチェックボックスをオンにします。

（注）　DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。そのため、少なくとも 1 つの DHCP サーバが、WLAN にアソシエートされたインターフェイスか WLAN 自体で設定されている必要があります。

ステップ 5　[DHCP Timeout] を秒単位で入力します。この時間を過ぎると DHCP 要求がタイムアウトします。デフォルト設定は 5 です。有効値の範囲は 5 ～ 120 秒です。

（注）　DHCP タイムアウトは、リリース 7.0.114.74 以降のコントローラで適用できます。

ステップ 6　[Save] をクリックします。

（注）　保存後に、[Audit] をクリックして、このコントローラで監査を実行できます。詳細については、「コントローラ監査レポートについて」（P.9-285）または「監査の設定」（P.15-853）を参照してください。

コントローラのマルチキャスト モードの設定

Prime Infrastructure では、コントローラ上の IGMP（インターネット グループ管理プロトコル）スヌーピングおよびタイムアウト値を設定するオプションが提供されています。

コントローラのマルチキャスト モードおよび IGMP スヌーピングを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　目的のコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Multicast] の順に選択します。

ステップ 4　[Ethernet Multicast Support] ドロップダウン リストから、[Disable]、[Unicast]、[Multicast] のいずれかを選択します。

（注）　IGMP スヌーピングおよびタイムアウトは、イーサネット マルチキャスト モードが有効の場合のみ設定できます。

ステップ 5　[Multicast] を選択した場合は、マルチキャスト グループ IP アドレスを入力します。

ステップ 6　マルチキャスト モードをグローバルで使用可能にする場合は、[Enable Global Multicast Mode] チェックボックスをオンにします。

ステップ 7　IGMP スヌーピングを選択して有効にします。

ステップ 8　[Multicast Mobility Mode] ドロップダウン リストから [Enable] を選択して、IGMP スヌーピング ステータスを変更するか、または IGMP タイムアウトを設定します。IGMP スヌーピングが有効の場合、コントローラはクライアントから IGMP レポートを収集した後、いずれかのマルチキャスト グループをリッスンしているクライアントのリストをアクセス ポイントに送信します。その後、アクセス ポイントはこれらのクライアントのみにマルチキャスト パケットを転送します。

タイムアウト間隔の範囲は 3 ～ 300 で、デフォルト値は 60 です。タイムアウトが経過すると、コントローラはすべての WLAN に対してクエリーを送信します。その後、マルチキャスト グループ内でリッスンしているクライアントは、コントローラにパケットを送り返します。

ステップ 9　マルチキャスト モビリティ モードを有効にしている場合は、モビリティ グループ マルチキャスト アドレスを入力します。

ステップ 10　ワイヤレス ネットワークを介したビデオのストリームを有効にする場合は、[Multicast Direct feature] チェックボックスをオンにします。

ステップ 11　[Multicast Mobility Mode] ドロップダウン リストから [Enable] を選択して、MLD 設定を変更します。

ステップ 12　IPv6 MLD スヌーピングを有効にする場合は、[Enable MLD Snooping] チェックボックスをオンにします。このチェックボックスを選択した場合は、次のパラメータを設定します。

- [MLD Timeout] : MLD タイムアウト値を秒単位で入力します。タイムアウトの範囲は 3 ～ 7200 で、デフォルト値は 60 です。
- [MLD Query Interval] : MLD クエリー間隔のタイムアウト値を秒単位で入力します。間隔の範囲は 15 ～ 2400 で、デフォルト値は 20 です。

（注）　インターネット グループ管理プロトコル（IGMP）スヌーピングを使用することにより、IPv4 のマルチキャスト トラフィックのフラッディングを抑制できます。IPv6 の場合は、Multicast Listener Discovery（MLD）スヌーピングが使用されます。

ステップ 13　セッション バナー情報を指定します。これは、クライアントがメディア ストリームから拒否またはドロップされた場合に、クライアントに送信されるエラー情報です。

a. [State] : セッション バナーをアクティブにする場合は、このチェックボックスをオンにします。アクティブにしない場合、セッション バナーはクライアントに送信されません。

b. [URL] : クライアントにレポートされる Web アドレス

c. [Email] : クライアントにレポートされる電子メール アドレス

d. [Phone] : クライアントにレポートされる電話番号

e. [Note] : クライアントにレポートされる注意

（注）　コントローラ上のすべてのメディア ストリームは、この設定を共有します。

ステップ 14　[Save] をクリックします。

（注）　保存後に、[Audit] をクリックして、このコントローラで監査を実行できます。詳細については、「コントローラ監査レポートについて」（P.9-285）または「監査の設定」（P.15-853）を参照してください。

アクセス ポイント タイマーの設定

Prime Infrastructure のコントローラでは、FlexConnect およびローカル モードの拡張タイマーが設定できます。

（注）　この機能は、リリース 6.0 以降のコントローラのみでサポートされています。

- 「拡張タイマーの設定」（P.9-350）
- 「ローカル モードのアクセス ポイント タイマー設定」（P.9-350）
- 「FlexConnect モードのアクセス ポイント タイマー設定」（P.9-350）

拡張タイマーの設定

拡張タイマーを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　タイマーを設定するコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[System] > [AP Timers] の順に選択します。

ステップ 4　該当するアクセス ポイント モード（ローカル モードまたは FlexConnect モード）を選択します。

ステップ 5　各モードの設定の詳細については、「ローカル モードのアクセス ポイント タイマー設定」（P.9-350）または「FlexConnect モードのアクセス ポイント タイマー設定」（P.9-350）を参照してください。

ローカル モードのアクセス ポイント タイマー設定

障害検出時間を短縮するには、高速ハートビート間隔（コントローラとアクセス ポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの期限（ハートビート間隔ごとの）を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラへ送信します。この場合、10 ～ 15 秒の値を入力できます。

FlexConnect モードのアクセス ポイント タイマー設定

選択した場合、FlexConnect タイムアウト値を設定できます。[AP Primary Discovery Timeout] チェックボックスをオンにして、タイムアウト値を有効にします。30 ～ 3600 秒の値を入力します。

（注）　5500 シリーズ コントローラは、1 ～ 10 の範囲のアクセス ポイント高速ハートビート タイマー値を受け入れます。

コントローラ WLAN の設定

コントローラは 512 WLAN 設定をサポートできるため、Prime Infrastructure は、特定のコントローラに対して、指定した時刻に複数の WLAN を有効または無効にする効率的な方法が提供しています。

ネットワーク上に設定した SSID（WLAN）のサマリーを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。[Configure WLAN Summary] ページが表示されます。この [WLAN Configuration] ページには、表 9-1 に示されている値が含まれます。

表 9-1　[WLAN Configuration Summary] ページ

フィールド	説明
Check box	削除する WLAN を選択します。[Select a command] ドロップダウン リストから [Delete WLANs] を選択します。
WLAN ID	WLAN の識別番号。
Profile Name	WLAN テンプレートの作成時に指定したユーザ定義のプロファイル名。プロファイル名は WLAN 名です。
SSID	ブロードキャストされている Service Set Identifier。
WLAN/Guest LAN	WLAN かゲスト LAN かを指定します。
Security Policies	WLAN で有効になっているセキュリティ ポリシー。
Status	WLAN のステータスは有効または無効のいずれかです。
Task List	[Configure] > [Scheduled Configuration Tasks] でタスクがスケジュール設定されている場合は、スケジュール設定された設定タスクを表示するリンクが表示されます。

WLAN の詳細の表示

WLAN の詳細を表示するには、[WLANs] を選択します。[WLAN Details] ページが表示されます。

タブ（[General]、[Security]、[QoS]、[Advanced]）を使用して、WLAN のパラメータを表示または編集します。

ここでは、次の内容について説明します。

- 「[General] タブ」（P.9-352）
- 「[Security] タブ」（P.9-352）

- 「[QoS] タブ」（P.9-359）
- 「[Advanced] タブ」（P.9-360）

[General] タブ

[General] タブには、次の情報が含まれています。

（注）　このコントローラで使用されている WLAN テンプレートに応じて、使用できるパラメータと使用できないパラメータがあります。

- [Guest LAN]：この WLAN がゲスト LAN かどうかを示します。
- Profile Name
- SSID
- [Status]：[Enabled] チェックボックスをオンにしてこの WLAN を有効にします。

（注）　WLAN ステータスが有効になる開始時間を設定するには、[Schedule Status] チェックボックスをオンにします。ドロップダウン リストから時間と分を選択します。カレンダー アイコンをクリックして、該当する日付を選択します。

- Schedule Status
- [Security Policies]：[Security] タブを使用して設定したセキュリティ ポリシーを示します（None、802.1X、静的 WEP、静的 WEP-802.1X、WPA+WPA2、CKIP などのセキュリティ ポリシーを含む）。セキュリティ ポリシーの変更は、ページの保存後に表示されます。
- [Radio Policy]：ドロップダウン リストから、次のいずれかを選択します。
  - [All]、[802.11a only]、[802.11g only]、[802.11b/g only]、[802.11a/g only]。
- [Interface/Interface Group]：ドロップダウン リストから選択します。
- [Broadcast SSID]：チェックボックスをオンにすると有効になります。
- [Egress Interface]：該当するインターフェイスの名前を選択します。この WLAN は、有線ゲスト クライアント トラフィックのコントローラから送信されるパスを提供します。

（注）　設定でコントローラが 1 つしかない場合は、[Egress Interface] ドロップダウン リストから [Management] を選択します。

- [Ingress Interface]：ドロップダウン リストから該当する VLAN を選択します。このインターフェイスは、レイヤ 2 アクセス スイッチを経由して、有線ゲスト クライアントとコントローラとの間のパスを提供します。

[Security] タブ

[Security] タブには、[Layer 2]、[Layer 3]、[AAA Servers] の 3 つの追加タブが含まれます。

Layer 2 Security

[Layer 2 Security] ドロップダウン リストを使用して、[None]、[802.1x]、[Static WEP]、[Cranite]、[Static WEP-802.1x]、[WPA1+WPA2]、[CKIP] のいずれかを選択します。これらのパラメータは、表 9-2 で説明されています。

[Mac Filtering] : MAC アドレスによりクライアントをフィルタリングする場合は、このチェックボックスをオンにします。

（注）　FlexConnect ローカル認証では、[PMac Filtering]、[Max-Clients]、および [Client Profiling] はサポートされていません。

表 9-2　Layer 2 Security オプション

フィールド	説明
None	• レイヤ 2 の選択はありません。 – [FT Enable] : アクセス ポイント間の高速移行（FT）を有効にする場合は、このチェックボックスをオンにします。 （注）　高速移行機能は FlexConnect モードではサポートされません。 – [Over the DS] : 分散システムでの高速移行を有効にする場合は、このチェックボックスをオンにします。 – [Reassociation Timeout] : 高速移行の再アソシエーションがタイムアウトになるまでの時間（秒単位）。デフォルトは 20 秒です。有効範囲は 1 ～ 100 です。 （注）　[Over the DS] または [Reassociation Timeout] を有効にするには、高速移行を有効にする必要があります。
802.1x	802.11 Data Encryption : • [Type] : WEP • [Key Size] : 40、104、または 128 ビット。
Static WEP	802.11 Data Encryption : • Type • [Key Size] : 設定なしか、40、104、または 128 ビット。 • [Key Index] : 1 ～ 4。 • Encryption Key • [Encryption Key Format] : ASCII または HEX。 • [Allowed Shared Key Authentication] : チェックボックスをオンにすると、共有キー認証が有効になります。
Cranite	FIPS140-2 準拠の Cranite Wireless Wall Software Suite を使用するように WLAN を設定します。ここでは、AES 暗号化および VPN トンネルを使用し、Cisco Wireless LAN Solution により伝送されるすべてのデータ フレームの暗号化および確認を行います。

表 9-2　Layer 2 Security オプション （続き）

フィールド	説明
Static WEP-802.1X	この設定により、静的 WEP と 802.1X の両方のポリシーを有効にします。このオプションを選択すると、静的 WEP と 802.1X のパラメータがページの下部に表示されます。 静的 WEP 暗号化パラメータ： • 802.11 Data Encryption – Type – [Key Size]：設定なしか、40、104、または 128 ビット。 – [Key Index]：1 ～ 4。 – Encryption Key – [Encryption Key Format]：ASCII または HEX。 • [Allowed Shared Key Authentication]：チェックボックスをオンにすると有効になります。

表 9-2　Layer 2 Security オプション （続き）

フィールド	説明
WPA+WPA2	この設定により、WPA、WPA2、またはその両方を有効にします。WPA は、TKIP-MIC データ暗号化または AES を使用する Wi-Fi Protected Access を有効にします。[WPA+WPA2] を選択すると、クライアントがアクセス ポイント間をローミングする際に迅速な交換が可能となる Cisco Centralized Key Management（CCKM）認証キー管理を使用できます。 レイヤ 2 セキュリティ ポリシーとして [WPA+WPA2] を選択し、事前共有キーを有効にしている場合は、CCKM または 802.1X を有効にできません。ただし、CCKM と 802.1X の両方を同時に有効にすることは可能です。 • [Mac Filtering]：MAC アドレス フィルタリングを有効にします。 （注）　FlexConnect ローカル認証では、[Mac Filtering] および [Max-Clients] はサポートされていません。 • [FT Enable]：アクセス ポイント間の高速移行を有効にする場合は、このチェックボックスをオンにします。 （注）　高速移行は FlexConnect モードではサポートされません。 – [Over the DS]：分散システムでの高速移行を有効にする場合は、このチェックボックスをオンにします。 – [Reassociation Timeout]：高速移行の再アソシエーションがタイムアウトになるまでの時間（秒単位）。デフォルトは 20 秒です。有効範囲は 1 ～ 100 です。 （注）　[Over the DS] または [Reassociation Timeout] を有効にするには、高速移行を有効にする必要があります。 [WPA+WPA2] のパラメータ： • [WPA1]：WPA1 を有効にする場合は、チェックボックスをオンにします。 • [WPA2]：WPA2 を有効にする場合は、チェックボックスをオンにします。 認証キー管理： • [FT802.1X]：FT802.1X を有効にする場合は、チェックボックスをオンにします。 • [802.1X]：802.1X を有効にする場合は、チェックボックスをオンにします。 • [CCKM]：CCKM を有効にする場合は、チェックボックスをオンにします。 • [PSK]：PSK を有効にする場合は、チェックボックスをオンにします。 • [FT PSK]：ASCII または 16 進（HEX）形式を選択でき、これによって Fast Transition に対する事前共有キーを入力します。 • [PMF 802.1X]：管理フレームの保護（PMF）の 802.1X 認証。 • [PMF PSK]：PMF の事前共有キー（PSK）。ASCII または 16 進形式（HEX）を選択し、Fast Transition の事前共有キーを入力します。 （注）　[FT802.1X] または [FTPSK] を設定するには、WPA2 および高速移行を有効にします。

表 9-2　Layer 2 Security オプション （続き）

フィールド	説明
Protected Management Frame	[Protected Management Frame]：次を選択できるドロップダウン リストです。 • [Disabled]：WLAN の 802.11w MFP 保護を無効にします。 • [Optional]：WLAN の 802.11w MFP 保護を有効にします。 • [Required]：クライアントが WLAN の 802.11w MFP 保護をネゴシエートすることを要求します。 802.11w では、ブロードキャストまたはマルチキャストの管理フレームを保護するために使用される Integrity Group Temporal Key（IGTK）が導入されています。IGTK は、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用するオーセンティケータ ステーション（コントローラ）によって割り当てられる、ランダムな値です。802.11w IGTK キーは、4 ウェイ ハンドシェイクを使用して取得され、レイヤ 2 で WPA または WPA2 セキュリティによって設定されている WLAN でのみ使用されます。 **（注）** PMF を有効にするために、PMF AKM のいずれか 1 つと WPA2 が有効になっている必要があります。
Association Comeback Timer	アソシエーション復帰間隔（秒単位）。このタイマーは、アソシエーションされたクライアントがステータス コード 30 で拒否された後にアソシエーションを再試行するまで待機する必要のある間隔です。ステータス コード 30 のメッセージは、Association request rejected temporarily; Try again later です。 有効な範囲は 1 ～ 10 秒です。デフォルト値は 1 秒です。
SA Query Retry Timeout	ミリ秒単位のセキュリティ アソシエーション（SA）のクエリー間隔。このタイムアウトはアソシエーションを再試行する前に、すでにアソシエーションされているクライアントへのアソシエーション応答で特定される間隔です。アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかが確認されます。クライアントがこの時間内に応答しない場合は、クライアント アソシエーションがコントローラから削除されます。 範囲は 100 ～ 500 ミリ秒です。デフォルト値は 200 ミリ秒です。
CKIP	Cisco Key Integrity Protocol。Cisco のアクセス ポイントは、ビーコンおよびプローブの応答パケットで CKIP のサポートをアドバタイズします。CKIP は、Aironet IE が WAN で有効な場合にだけ設定できます。 **（注）** CKIP は、10xx アクセス ポイントではサポートされていません。 CKIP パラメータ： • 802.11 Data Encryption – Type – [Key Size]：設定なしか、40、104、または 128 ビット。 – [Key Index]：1 ～ 4。 – Encryption Key – [Encryption Key Format]：ASCII または HEX。 • [MMH Mode]：チェックボックスをオンにすると有効になります。 • [Key Permutation]：チェックボックスをオンにすると有効になります。

Layer 3 Security

[Layer 3 Security] ドロップダウン リストを使用して、[None]、[VPN Pass Through]、[IPsec]（**インターネット プロトコル セキュリティ**）のいずれかを選択します。選択肢によって、ページ パラメータが変わります。WLAN のタイプに応じて、使用できるレイヤ 3 パラメータと使用できないレイヤ 3 パラメータがあります。

（注） [VPN Pass Through] を選択した場合は、VPN ゲートウェイ アドレスを入力する必要があります。

（注） IPsec は、データ ストリーム内の各 IP パケットを認証および/または暗号化して、IP 通信のセキュリティを確保するプロトコル スイートです。また、IPsec には、暗号キーを確立するためのプロトコルも含まれます。

次の情報を設定します。

- [Web Policy]：認証、パススルー、条件付き Web リダイレクト、または [WebAuth on MAC Filter Failure] などのポリシーを指定するには、このチェックボックスをオンにします。また、このセクションではゲスト ユーザに対してカスタマイズしたログイン ページが表示されるようにもできます。

  （注） パススルーを選択した場合は、[Email Input] チェックボックスが表示されます。ユーザがネットワークに接続しようとしたとき、電子メール アドレスの入力を求める場合は、このチェックボックスをオンにします。

- [Preauthentication ACL]：クライアントとコントローラ間のトラフィックに使用される IPv4、IPv6、および WebAuth ACL のリストを示します。

  （注） WLAN の IPv6 ACL マッピングは、リリース 7.2.x 以降のコントローラでサポートされています。

- [Sleeping Client Enable]：スリープ状態にあるクライアントのサポートを有効にするには、このチェックボックスを選択します。この機能は、リモートおよびゲスト LAN には適用できません。
- [Sleeping ClientTimeout]：スリープ状態にあるクライアントが強制的に再認証されるまでの、アイドル タイムアウト後の最大時間数（時間単位）。範囲は 1 ～ 720 時間です。デフォルト値は 12 時間です。このフィールドは [Sleeping Client] チェックボックスをオンにした場合にだけ表示されます。また、スリープと再起動時間の間、クライアントは同じモビリティ グループ内で 1 つのコントローラから別のコントローラに移動した場合、ログイン資格情報を入力する必要はありません。
- [Global WebAuth Configuration]：カスタム Web 認証ページを指定するには、このチェックボックスをオフにします。
- [Web Auth Type]：[Web Auth Type] ドロップダウン リストが表示されたら、次のいずれかのオプションを選択して、無線ゲスト ユーザ用の Web ログイン ページを定義します。
  - [Default Internal]：ゲスト ユーザに対して、デフォルトのログイン ページが表示されます。

– [Customized WebAuth] : [Upload/Download Commands] ページから、カスタマイズされたログイン ページをダウンロードできます。詳細については、「カスタマイズ Web 認証ページのダウンロード」（P.11-668）を参照してください。

  ドロップダウン リストから、[Web Auth Login Page]、[Web Auth Login Failure Page]、[Web Auth Logout Page] のいずれかを選択します。

  カスタマイズしたページを表示しないオプションに対しては、任意のドロップダウン リストで [None] を選択します。

– [External] : ゲスト ユーザは、外部のログイン ページにリダイレクトされます。[External Web Auth URL] テキスト ボックスに、ログイン ページの URL を入力します。

（注）　[External] を選択した場合、[Security] > [AAA] ページで最大 3 つの RADIUS および LDAP サーバを選択できます。詳細については、「AAA サーバ」（P.9-358）を参照してください。

AAA サーバ

現在の WLAN で RADIUS および LDAP サーバを選択して、デフォルト サーバの使用を上書きします。

– [RADIUS Servers] : ドロップダウン リストを使用して、認証サーバおよびアカウンティング サーバを選択します。それを選択することで、指定した WLAN のデフォルトの RADIUS サーバが選択され、ネットワークに対して設定されている RADIUS サーバは上書きされます。3 つすべての RADIUS サーバが特定の 1 つの WLAN に対して設定されている場合、優先順位はサーバ 1 が最も高くなります。

– [LDAP Servers] : ドロップダウン リストで LDAP サーバを選択しない場合は、Prime Infrastructure はデータベースのデフォルトの LDAP サーバ順序を使用します。

– [Local EAP Authorization] : ユーザおよびワイヤレス クライアントのローカル認証を可能にします。この方式は、バックエンド システムが妨害されたり、外部認証サーバでエラーが発生した場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。

  EAP プロファイルを設定している場合は、このチェックボックスをオンにして有効にします。ドロップダウン リストから、プロファイルを選択します。

– [Allow AAA Override] : この機能が有効になっていて、クライアントの AAA とコントローラの WLAN の認証パラメータが競合する場合、クライアント認証は AAA サーバで実行されます。

  この認証の一部として、オペレーティング システムはクライアントをデフォルトの Cisco WLAN ソリューションから、AAA サーバにより返され、コントローラのインターフェイス設定で事前定義された VLAN に移動します（MAC フィルタリング、802.1X、または WPA 動作用に設定されている場合のみ）。

  すべての場合において、オペレーティング システムはまた、QoS、および AAA サーバにより提供される ACL がコントローラ インターフェイス設定で事前に定義されている限り、これらを使用します。（この AAA オーバーライドによる VLAN スイッチングは、*ID ネットワーキング*とも呼ばれます）。

  AAA オーバーライドを無効にすると、コントローラの認証パラメータ設定がすべてのクライアント認証においてデフォルトで使用され、コントローラ WLAN にクライアント固有の認証パラメータがない場合は、AAA サーバのみによって認証が実行されます。

[QoS] タブ

- [Quality of service (QoS)]：ドロップダウン リストから、[Platinum (voice)]、[Gold (video)]、[Silver (best effort)]、[Bronze (background)] のいずれかを選択します。
  - VoIP などのサービスは、[Gold] に設定する必要があります。テキスト メッセージなど差別的ではないサービスは [Bronze] に設定できます。
- [NBAR Visibility]：チェックボックスをオンにすると、アプリケーションの分類を、Network Based Application Recognition（NBAR）のディープ パケット インスペクション テクノロジーに基づいて表示できます。
- [AVC Profile]：ドロップダウン リストから、WLAN の Application Visibility and Control（AVC）プロファイルを選択できます。
- [Netflow Monitor]：ドロップダウン リストから、WLAN の NetFlow モニタを選択できます。
- [Override Per-User Rate Limits]：ワイヤレス レート制限は、アップストリームおよびダウンストリーム トラフィックの両方に定義できます。データ レートをユーザ単位で定義するには、次の項目を設定します。
  - [Average Data Rate]：[Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックの平均データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
  - [Burst Data Rate]：[Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。
  - [Average Real-Time Rate]：[Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
  - [Burst Real-Time Rate]：[Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-realtime-rate は average-realtime-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。
- [Override Per-SSID Rate Limits]：データ レートを SSID 単位で定義するには、次の項目を設定します。
  - [Average Data Rate]：[Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックの平均データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
  - [Burst Data Rate]：[Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。
  - [Average Real-Time Rate]：[Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。

  - [Burst Real-Time Rate] : [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-realtime-rate は average-realtime-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。

- WMM パラメータ
  - [WMM Policy] : [Disabled]、[Allowed]（クライアントが WLAN と通信できるようにする）、または [Required]（クライアントが通信で WMM を有効にすることを必須とする）を選択します。
  - [7920 AP CAC] : Cisco 7920 電話でサポートを有効にする場合は、このチェックボックスをオンにします。
  - [7920 Client CAC] : 7920 電話で WLAN に旧バージョンのソフトウェアをサポートさせる場合は、このチェックボックスをオンにして有効にします。CAC の制限は、より新しいバージョンのソフトウェアのアクセス ポイントで設定されます。

[Advanced] タブ

- [FlexConnect Local Switching] : FlexConnect ローカル スイッチングを有効にする場合は、このチェックボックスをオンにします。これを有効にすると、FlexConnect のアクセス ポイントはクライアント認証を処理し、クライアント パケットをローカルにスイッチングします。詳細については、「FlexConnect の設定」（P.12-761）を参照してください。

  （注）　FlexConnect ローカル スイッチングは、Cisco 1130/1240/1250 シリーズ アクセス ポイントのみに適用されます。L2TP、PPTP、CRANITE、FORTRESS 認証ではサポートされていません。WLAN ID 9 ～ 16 には適用されません。

- [FlexConnect Local Auth] チェックボックスをオンにして、FlexConnect ローカル認証を有効にします。

  ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位（MTU）が 500 バイトを下回らない、最小帯域幅が 128 kbps のリモート オフィス設定の基準を維持できない場合に役立ちます。ローカル スイッチングでは、認証機能はアクセス ポイント自体に存在します。そのため、ローカル認証によって、ブランチ オフィスの遅延要件が軽減されます。

  （注）　ローカル認証は、ローカル スイッチング モードの FlexConnect AP の WLAN のみで有効にできます。

  ローカル認証は、次のシナリオではサポートされません。
  - FlexConnect ローカル認証を有効にした WLAN では、ゲスト認証は実行できません。
  - RRM 情報は、FlexConnect ローカル認証を有効にした WLAN のコントローラでは使用不可です。
  - ローカル RADIUS はサポートされません。
  - クライアントがいったん認証されると、WLC およびグループ内の他の FlexConnect がクライアント情報で更新された後だけ、ローミングがサポートされます。

- [Session Timeout (secs)] : クライアント セッションが再認証を必要とせずに続行できる最大時間を設定します。

- [Override Interface ACL]：この WLAN 上のインターフェイスに対して設定されている ACL を上書きする、IPv4 および IPv6 アクセス コントロール リスト（ACL）のリストを表示します。
- [Learn Client IP Address]：H-REAP ローカル スイッチングを有効にした場合、[Learn Client IP Address] チェックボックスはデフォルトで有効になります。ただし、クライアントが Fortress レイヤ 2 暗号化を使用するように設定されている場合は、コントローラがそのクライアント IP アドレスを知ることができないので、コントローラはクライアントの接続を定期的に切断します。コントローラがクライアント IP アドレスを知らなくてもクライアント接続を維持できるように、このオプションを無効にしてください。このオプションを無効にできるのは、H-REAP ローカル スイッチングを行うように設定されているときだけです。H-REAP 中央スイッチングを行う場合は、無効にすることはできません。
- [VLAN Based Central Switching] : [VLAN based Central Switching] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上での AAA でオーバーライドされた VLAN に基づく中央スイッチングを有効または無効にします。
- [Central DHCP Processing] : [Central DHCP Processing] チェックボックスをオンまたはオフにして、機能を有効または無効にします。この機能を有効にすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。
- [Override DNS] : [Override DNS] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバ アドレスのオーバーライドを有効または無効にします。中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
- [NAT-PAT] : [NAT-PAT] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換（NAT）およびポートアドレス変換（PAT）を有効または無効にします。NAT および PAT をイネーブルにするには、[Central DHCP Processing] を有効にする必要があります。
- [Aironet IE]：この WLAN の Aironet 情報要素（IE）を有効にする場合は、このチェックボックスをオンにします。
  - Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの番号などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントがアソシエーション要求内の Aironet IE 0x85 を受信する場合、コントローラは、Aironet IE 0x85 および 0x95（コントローラの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション要求に格納して送信します。
- [IPv6]：IPv6 を有効にする場合は、チェックボックスをオンにします。

  （注） IPv6 を有効にするには、[Layer 3 Security] は [None] に設定する必要があります。

- [Diagnostic Channel]：診断を有効にする場合はクリックします。有効にした場合、クライアントは診断の目的でこの WLAN に接続できます。

  （注） 診断テストの結果は SNMP テーブルに格納され、Prime Infrastructure はこれらのテーブルをポーリングして結果を表示します。

- [Override Interface ACL]：ドロップダウン リストから定義済みのアクセス コントロール リスト（ACL）を選択します。ACL を選択した場合、WLAN は ACL を WLAN にアソシエートします。

（注）　ACL の選択は任意であり、デフォルトは [None] です。

詳細については、「アクセス コントロール リスト テンプレートの設定」（P.11-671）を参照してください。

- [Peer to Peer Blocking]：ドロップダウン リストから、[Disable]、[Drop]、[Forward-Up Stream] のいずれかを選択します。
  - このオプションを使用することで、すべての WLAN クライアントについてユニバーサルにピアツーピア ブロックを設定するのではなく、各クライアントについて設定できるようになります。

（注）　コントローラ リリース 7.2.x 以降では、[Forward Up Stream] はローカルでスイッチするクライアントの [Drop] と同じです。

- [Wi-Fi Direct Client Policy]：Wi-Fi Direct 対応のデバイス同士は、迅速かつ簡単に直接接続して、印刷、同期、データの共有などのタスクを実行できます。Wi-Fi Direct デバイスは、複数のピアツーピア（P2P）デバイスおよびインフラストラクチャ無線 LAN（WLAN）に同時にアソシエートしている場合があります。コントローラを使用して、WLAN ごとに Wi-Fi Direct クライアント ポリシーを設定できます。ここでは、Wi-Fi デバイスとインフラストラクチャ WLAN とのアソシエーションを許可または禁止したり、WLAN の Wi-Fi Direct クライアント ポリシーをすべて無効にしたりできます。[Wi-Fi Direct Clients Policy] ドロップダウン リストから、次のいずれかのオプションを選択します。
  - [Disabled]：WLAN の Wi-Fi Direct クライアント ポリシーを無効にして、すべての Wi-Fi Direct 対応クライアントを認証解除します。
  - [Allow]：Wi-Fi Direct クライアントとインフラストラクチャ WLAN とのアソシエーションを許可します。
  - [Not-Allow]：Wi-Fi Direct クライアントとインフラストラクチャ WLAN とのアソシエーションを禁止します。

（注）　Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。

（注）　Wi-Fi Direct クライアント ポリシーは、リリース 7.2.x 以降のコントローラに適用できます。

- [Client Exclusion]：自動クライアント除外を有効にする場合は、このチェックボックスをオンにします。これを有効にした場合、無効にしたクライアント マシンに対して、タイムアウト値を秒単位で設定します。
  - クライアント マシンは MAC アドレスで除外され、そのステータスは監視できます。
  - 0 のタイムアウト設定は、クライアントを再度有効にするには管理制御が必要であることを示します。

（注）　セッション タイムアウトが設定されていない場合、除外されたクライアントはそのまま残り、除外状態からタイムアウトすることはありません。除外機能が無効であることを意味するのではありません。

- [Media Session Snooping] : メディア セッション スヌーピングを有効にする場合は、このチェックボックスをオンにします。この機能により、アクセス ポイントは音声コールの確立、終了、および失敗を検出し、それをコントローラおよび Prime Infrastructure にレポートできます。WLAN ごとに有効化または無効化できます。

  メディア セッション スヌーピングを有効にした場合、アクセス ポイント無線により、Session Initiation Protocol（SIP）音声パケットに対してこの WLAN スヌープがアドバタイズされます。ポート番号 5060 に宛てた、またはポート番号 5060 からのパケットはいずれも、詳細検査の対象として考慮されます。アクセス ポイントは、Wi-Fi マルチメディア（WMM）および非 WMM クライアントがコールを確立中か、すでにアクティブなコール上にあるか、またはコールの終了処理中であるかをトラッキングし、コントローラに対して主要なコール イベントを通知します。

- [KTS based CAC] : WLAN 単位で KTS ベースの CAC サポートを有効にする場合は、このチェックボックスをオンにします。

  WLC は、TSPEC ベースの CAC および SIP ベースの CAC をサポートしています。ただし、異なる CAC のプロトコルで稼働する特定の電話があります。これらは、Key Telephone System（KTS）をベースとします。CAC および KTS ベースの SIP クライアントをサポートするには、WLC はこのプロトコルの一部として、特定のその他のメッセージを処理して送信することに加えて、これらのクライアントからの帯域幅要求メッセージを理解して処理し、AP 無線上に要求された帯域幅を割り当てる必要があります。

（注）　KTS CAC 設定は、コントローラ ソフトウェア リリース 7.2.x を実行する Cisco 5508、7500、WISM2、2500 コントローラのみでサポートされています。この機能は、Cisco 4400 シリーズ コントローラではサポートされません。

（注）　音声パラメータは、[QoS] タブの [quality of service (QoS)] ドロップダウン リストで [Platinum (voice)] を選択した場合のみ表示されます。

- [NAC State] : [NAC State] ドロップダウン リストから、[SNMP NAC] または [Radius NAC] を選択します。検出された SIP エラーにより、[Client Troubleshooting] および [Alarms] ページに表示されるトラップが生成されます。コントローラはアウトオブバンドの NAC アプライアンスと統合できます。NAC アプライアンスは、クライアントが分析および解除されるまでデータ パス内に保持されます。アウトオブバンド モードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。詳細については、「NAC 統合」（P.9-330）を参照してください。

  （注）　オープン認証の WLAN 上の RADIUS NAC および MAC フィルタリングを有効にできます。RADIUS NAC によるローカル Web 認証を使用している場合は、レイヤ 3 Web 認証も有効にする必要があります。

- [Passive Client] : このチェックボックスをオンにした場合、WLAN 上のパッシブ クライアントが有効になります。

パッシブ クライアントは、スケールおよびプリンタなどの、スタティック IP アドレスが設定されたワイヤレス デバイスです。これらのクライアントは、アクセス ポイントとのアソシエーション中に、IP アドレス、サブネット マスク、ゲートウェイ情報などの IP 情報を一切送信しません。その結果、パッシブ クライアントが使用されている場合、DHCP が使用されている場合を除き、クライアントは IP アドレスを認識できません。

現在、Wireless LAN Controller は ARP 要求のプロキシとして動作します。ARP 要求を受信すると、コントローラはクライアントに直接要求を渡すのではなく、ARP 応答で応答します。これには、2 つの利点があります。

- クライアントに ARP 要求を送信するアップストリーム デバイスは、クライアントの場所を特定できません。
- すべての ARP 要求に応答する必要がないため、携帯電話およびプリンタなどのバッテリ駆動のデバイスの消費電力を節約できます。

ワイヤレス コントローラは、パッシブ クライアントについての IP を一切持っていないため、いずれの ARP 要求にも応答できません。現在の動作では、ARP 要求のパッシブ クライアントへの転送は許可されていません。そのため、パッシブ クライアントへのアクセスを試行するアプリケーションは、すべて失敗します。

この機能は、ARP 要求と応答を、VLAN/WLAN ごとに有線およびワイヤレス クライアント間で交換できるようにします。この機能により、ユーザは目的の WLAN にプロキシ ARP が存在するかをマークできます。これにより、クライアントが RUN 状態になるまで、コントローラが ARP 要求を渡すことができるようになります。

（注） この機能は、5500 および 2100 シリーズ コントローラのみでサポートされています。

- [DTIM Period (in beacon intervals)] : 802.11a/n および 802.11b/g/n の場合、ワイヤレス媒体での DTIM パケットの送信頻度を指定します。この期間は、バージョン 6.0 以降のすべてのコントローラで、すべての WLAN（ゲスト WLAN を除く）に対して設定できます。
- DHCP
  - [DHCP Server] : DHCP サーバを上書きする場合は、このチェックボックスをオンにして、DHCP サーバの IP アドレスを入力します。

    （注） 一部の WLAN 設定では、この設定は必須です。

  - [DHCP Addr.Assignment] : [Required] チェックボックスをオンにした場合、この WLAN に接続しているクライアントは、デフォルトの DHCP サーバから IP アドレスを取得します。
- 管理フレーム保護（MFP）
  - [MFP Signature Generation] : このチェックボックスがオンの場合、この WLAN にアソシエートされているアクセス ポイントにより送信される 802.11 管理フレームのシグニチャ生成が可能です。シグニチャ生成によって、侵入者による送信された管理フレームへの変更が、検出および報告されます。
  - [MFP Client Protection] : 個別の WLAN 設定について、ドロップダウン リストから [Enabled]、[Disabled]、[Required] のいずれかを選択します。

    （注） [Enabled] なパラメータは、WLC グラフィカル ユーザ インターフェイスの [MFP Client Protection] ドロップダウン リストで選択する [Optional] パラメータと同じです。

- [MFP Version]：管理フレーム保護のバージョンを表示します。

（注）　クライアント側の MFP は、CCXv5（以降）のクライアントをサポートするように設定された WLAN のみに対して使用できます。また、最初に WPA1 を設定する必要があります。

- [Foreign Controller Mapping]：外部コントローラのマッピングを設定する場合は、このリンクをクリックします。外部コントローラ設定ページに移動します。この設定ページでは、[Foreign Controller] ドロップダウン リストから外部コントローラを選択し、[Interface/Interface Group] ドロップダウン リストからインターフェイスまたはインターフェイス グループを選択します。必要なオプションを選択したら、[Add] をクリックして外部コントローラの追加を完了します。
- [Client Profiling] : WLAN に関連付けられたすべてのクライアントのプロファイリングを有効または無効にする場合は、このチェックボックスを選択します。

（注）　FlexConnect ローカル認証では、[Client Profiling] はサポートされていません。

（注）　[Client Profiling] は、[DHCP Address Assignment] チェックボックスをオンにした場合のみ設定できます。

（注）　[Client profiling] は、コントローラ リリース 7.2.x でサポートされます。

- [mDNS Snooping] : WLAN の mDNS スヌーピングを有効にする場合は、[mDNS Snooping] チェックボックスをオンにします。
- [mDNS Profile] : [mDNS Profile] ドロップダウン リストから、WLAN の mDNS プロファイルを選択できます。デフォルト値は default-mdns-profile です。

モバイル コンシェルジュの設定（802.11u）

モバイル コンシェルジュは、外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュ機能は、クライアントにサービスのアベイラビリティに関する情報を提供し、使用可能なネットワークをアソシエートするのに役立ちます。

ネットワークから提供されるサービスは、次の 2 つのプロトコルに大きく分類できます。

- 802.11u MSAP
- 802.11u HotSpot 2.0

モバイル コンシェルジュには、次のガイドラインと制限事項が適用されます。

- モバイル コンシェルジュは FlexConnect アクセス ポイントではサポートされません。
- 802.11u 設定アップロードはサポートされません。設定のアップグレードを実行し、設定をコントローラにアップロードすると、WLAN の HotSpot の設定は失われます。

モバイル コンシェルジュ（802.11u）グループを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。

ステップ 4　[Hot Spot] タブをクリックします。

ステップ 5　[General] タブで、次のフィールドを設定します。

- [802.11u Status] チェックボックスをオンにして WLAN の 802.11u を有効にします。
- [Internet Access] チェックボックスを選択して、この WLAN からインターネット サービスを提供できるようにします。
- [Network Type] ドロップダウン リストから、この WLAN に設定する 802.11u を表すネットワークタイプを選択します。次のオプションを使用できます。
  - **Private Network**
  - **Private Network with Guest Access**
  - **Chargeable Public Network**
  - **Free Public Network**
  - **Emergency Services Only Network**
  - **Personal Device Network**
  - **Test or Experimental**
  - **Wildcard**
- このネットワークの 802.11u パラメータ用に設定する認証タイプを選択します。
  - Not configured
  - Acceptance of Terms and Conditions
  - Online Enrollment
  - HTTP/HTTPS Redirection
- [HESSID] フィールドに、Homogenous Extended Service Set Identifier 値を入力します。HESSID は、HESS を識別する 6 オクテットの MAC アドレスです。

ステップ 6　[Others] タブで、次のフィールドを設定します。

- [OUI List] グループ ボックスで、次の詳細情報を入力します。
  - OUI name
  - Is Beacon
  - OUI Index

  [Add] をクリックして、OUI（組織固有識別子）エントリをこの WLAN に追加します。
- [Domain List] グループ ボックスで、次の詳細情報を入力します。
  - [Domain Name] : 802.11 アクセス ネットワークで稼働するドメイン名。
  - [Domain Index] : ドロップダウン リストからドメイン インデックスを選択します。

  [Add] をクリックして、ドメイン エントリをこの WLAN に追加します。

ステップ 7　[Realm] タブで、次のフィールドを設定します。

- [OUI List] セクションで、次の詳細情報を入力します。
  - [Realm Name] : レルム名。
  - [Realm Index] : レルム インデックス。

  [Add] をクリックして、ドメイン エントリをこの WLAN に追加します。

ステップ 8　[Service Advertisement] タブで、次のフィールドを設定します。

- [MSAP Enable] チェックボックスをオンにし、サービス アドバタイズメントを有効にします。

- 前のステップで MSAP を有効にした場合は、サーバ インデックスを提供する必要があります。この WLAN のサーバ インデックスを入力します。サーバのインデックス フィールドによって、BSSID を使用して到達可能である場所を提供する MSAP サーバ インスタンスを一意に識別します。

（注）　MSAP（Mobility Services Advertisement Protocol）は、ネットワーク接続を確立するためのポリシー セットを使用して設定されたモバイル デバイスで主に使用するために設計されています。これらのサービスは、上位層サービスを提供するデバイス、つまりサービス プロバイダー経由で有効にされるネットワーク サービス向けです。サービス アドバタイズメントは、MSAP を使用して、Wi-Fi アクセス ネットワークへのアソシエーションの前にサービスをモバイル デバイスに提供します。この情報はサービス アドバタイズメントで伝送されます。シングルモードまたはデュアルモード モバイル デバイスは、アソシエーションの前にサービス ネットワークをネットワークにクエリーします。デバイスによるネットワークの検出および選択機能では、ネットワークに join する判断においてサービス アドバタイズメントを使用する場合があります。

ステップ 9　[HotSpot 2.0] タブで、次のフィールドを設定します。

- [HotSpot2 Enable] ドロップダウン リストから [Enable] オプションを選択します。
- [WAM Metrics] グループ ボックスで、次の項目を指定します。
  - [WAN Link Status]：リンク ステータス。有効な範囲は 1 ～ 3 です。
  - [WAN SIM Link Status]：対称リンク ステータス。たとえば、アップリンクとダウンリンクに異なる速度または同じ速度を設定できます。
  - [Down Link Speed]：ダウンリンク速度。最大値は 4,194,304 kbps です。
  - [Up Link Speed]：アップリンク速度。最大値は 4,194,304 kbps です。
- [Operator Name List] グループ ボックスで、次の項目を指定します。
  - [Operator Name]：802.11 オペレータの名前を指定します。
  - [Operator Index]：オペレータ インデックスを選択します。範囲は 1 ～ 32 です。
  - [Language Code]：言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。

  [Add] をクリックして、オペレータの詳細を追加します。オペレータの詳細が表形式で表示されます。
- [Port Config List] で、次の項目を指定します。
  - [IP Protocol]：有効にしたい IP プロトコル。次のオプションは、ESP、FTP、ICMP、および IKEV2 です。
  - [Port No]：この WLAN で有効になっているポート番号。
  - [Status]：ポートのステータス。

ステップ 10　[Policy Configuration] タブで、次のフィールドを設定します。

- [Policy Name]：ポリシー名。
- [Policy Priority]：1 ～ 16 のポリシー プライオリティを設定します。2 個のポリシーが同じプライオリティを持つことはできません。

（注）　WLAN あたり 16 ポリシー マッピングまでです。マッピングに選択されたポリシー テンプレートは、コントローラにポリシーがない場合に最初に適用されます。

ステップ 11　[Save] をクリックします。

WLAN の追加

WLAN を追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。
ステップ 2　該当するコントローラの IP アドレスをクリックします。
ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。
ステップ 4　[Select a command] ドロップダウン リストから、[Add a WLAN] を選択します。
ステップ 5　[Go] をクリックして、[WLAN Details: Add from Template] ページを開きます。
ステップ 6　[Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。
ステップ 7　[Apply] をクリックします。

（注）　WLAN のテンプレートを作成するには、このページの [click here] リンクを使用するか、[Configure] > [Controller Template Launch Pad] > [WLANs] > [WLAN] の順に選択します。

WLAN の削除

WLAN を削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。
ステップ 2　該当するコントローラの IP アドレスをクリックします。
ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。
ステップ 4　削除する WLAN のチェックボックスをオンにします。
ステップ 5　[Select a command] ドロップダウン リストから [Delete a WLAN] を選択します。
ステップ 6　[Go] をクリックします。
ステップ 7　[OK] をクリックして、削除を実行します。

WLAN ステータス スケジュールの管理

Prime Infrastructure では、特定のコントローラ上で、複数の WLAN のステータスを一度に変更できます。複数の WLAN を選択して、そのステータスが変更される日時を選択できます。

複数の WLAN のステータス変更をスケジュールするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。
ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。

ステップ 4　ステータス変更をスケジュールする WLAN のチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから、[Schedule Status] を選択して [WLAN Schedule Task Detail] ページを開きます。

選択した WLAN は、ページの上部にリストされます。

ステップ 6　スケジュール設定済みタスク名を入力して、このステータス変更スケジュールを特定します。

ステップ 7　ドロップダウン リストから、新しい管理ステータス（[Enabled] または [Disabled]）を選択します。

ステップ 8　スケジュール時刻を、[hours] および [minutes] ドロップダウン リストを使用して選択します。

ステップ 9　カレンダー アイコンをクリックしてスケジュール日を選択するか、テキスト ボックスに日付を入力します（MM/DD/YYYY 形式）。

ステップ 10　適切な [Recurrence] オプション ボタンを選択して、ステータス変更の頻度を決めます（[Daily]、[Weekly]、または [No Recurrence]）。

ステップ 11　[Submit] をクリックしてステータス変更スケジュールを開始します。

（注）　WLAN 設定のスケジュール済みタスクの結果の詳細については、「WLAN 設定のスケジュール設定されたタスク結果の表示」（P.9-526）を参照してください。

モビリティ アンカー

モビリティ アンカーは、WLAN のアンカーとして定義された、1 つ以上のコントローラです。クライアント（ラップトップなどの 802.11 モバイル ステーション）は、常にいずれかのアンカーに接続しています。

この機能は、クライアントのネットワークへのエントリ ポイントに関係なく、WLAN を 1 つのサブネットに制限する際に使用されます。これによって、ユーザは企業全体にわたりパブリック WLAN やゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。また、WLAN は建物の特定のセクション（ロビー、レストランなど）を表すことができるため、ゲスト WLAN で地理的ロード バランシングを実現できます。

クライアントが WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティ グループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが、WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、ローカル セッションがクライアントのために作成され、コントローラは同じモビリティ グループの別のコントローラへ通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに連絡をとり、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは暗号化され、有線ネットワークに配信されます。クライアントへのパケットは、アンカー コントローラで受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットのカプセルを解除し、クライアントへ転送します。

（注）　2000 シリーズ コントローラを WLAN のアンカーとして指定できません。ただし、2000 シリーズ コントローラ上に作成された WLAN に 4100 シリーズ コントローラまたは 4400 シリーズ コントローラをアンカーとして指定できます。

（注）　L2TP レイヤ 3 セキュリティ ポリシーは、モビリティ アンカーで設定された WLAN には使用できません。

特定の WLAN のモビリティ アンカーのステータスをリアルタイムで表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。

ステップ 4　[WLAN ID] をクリックして、特定の WLAN のパラメータを表示します。

ステップ 5　[Advanced] タブをクリックします。

ステップ 6　[Mobility Anchors] リンクをクリックします。表 9-3 では、表示されるパラメータについて説明します。

表 9-3　　モビリティ アンカー

フィールド	説明
Mobility Anchor	アンカーの IP アドレス。
Status	アンカーの現在のステータス。たとえば、[reachable] または [unreachable] です。

WLAN AP グループの設定

サイト固有の VLAN または AP グループは、WLAN を異なるブロードキャスト ドメインにセグメント化することで、ブロードキャスト ドメインを最小に制限します。これには、ロード バランシングおよび帯域割り当てをより効率的に管理できるなどの利点があります。

このページを開くには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLAN] > [AP Groups] の順に選択します。

このページには、ネットワーク上に設定されている AP グループのサマリーが表示されます。ここで、AP グループの追加、削除、詳細の表示が可能です。[Access Points] タブで AP グループ名をクリックして、そのアクセス ポイントを表示または編集します。[WLAN Profiles] タブをクリックして、WLAN プロファイルを表示、編集、追加、または削除します。

アクセス ポイント グループの追加

新しいアクセス ポイント グループを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLAN] > [AP Groups] の順に選択します。

（注）　AP グループ（5.2 以降のコントローラ）は、5.2 よりも前のコントローラでは AP グループ VLAN と呼ばれます。

ステップ 4　[Select a command] ドロップダウン リストから、[Add AP Groups] を選択します。

ステップ 5　[Go] をクリックします。

[AP Groups] の [Details] ページで、このアクセス ポイント グループにアクセス ポイントおよび WLAN プロファイルを追加できます。

ステップ 6　アクセス ポイント グループの名前およびグループの説明を入力します。

（注）　グループの説明はオプションです。

ステップ 7　グループにアクセス ポイントを追加するには、次の手順を実行します。

a.　[Access Points] タブをクリックします。

b.　[Add] をクリックします。アクセス ポイント ページには、使用できるアクセス ポイントのパラメータが表示されます。アクセス ポイントの名前をクリックして、使用できるアクセス ポイントのいずれか 1 つのパラメータを表示または編集します。

c.　追加するアクセス ポイントのチェックボックスをオンにします。

d.　[Select] をクリックします。

ステップ 8　WLAN プロファイルを追加するには、[WLAN Profiles] タブをクリックして、次のパラメータを設定します。

a.　[Add] をクリックします。

（注）　使用可能なすべての WLAN プロファイル名を表示するには、テキスト ボックスから現在の WLAN プロファイル名を削除します。テキスト ボックスから現在の WLAN プロファイルの名前を削除すると、使用可能なすべての WLAN プロファイルがドロップダウン リストに表示されます。

（注）　各アクセス ポイントは 16 個の WLAN プロファイルに限定されます。各アクセス ポイントは、WLAN override 機能が有効にされない限り、すべての WLAN プロファイルをブロードキャストします。WLAN override 機能によって、アクセス ポイントごとに 16 個の任意の WLAN プロファイルを無効にできます。

（注）　WLAN override 機能は、512 WLAN 機能をサポートしていない（最大 512 個の WLAN プロファイルをサポートできる）古いコントローラのみに適用されます。

b. WLAN プロファイル名を入力するか、[WLAN Profile Name] ドロップダウン リストからいずれか 1 つを選択します。

c. インターフェイス/インターフェイス グループを入力するか、[Interface/Interface Group] ドロップダウン リストからいずれか 1 つを選択します。

（注）　使用できるすべてのインターフェイスを表示するには、[Interface] テキスト ボックスから現在のインターフェイスを削除します。[Interface] テキスト ボックスから現在のインターフェイスを削除すると、使用可能なすべてのインターフェイスがドロップダウン リストに表示されます。

d. 該当する場合は、[NAC Override] チェックボックスをオンにします。デフォルトでは、NAC の上書きは無効になっています。

e. [Add/Edit] リンクをクリックして、ポリシー設定パラメータを指定します。

- [Policy Name]：ポリシー名。
- [Policy Priority]：1 ～ 16 のポリシー プライオリティを設定します。2 個のポリシーが同じプライオリティを持つことはできません。

（注）　WLAN あたり 16 ポリシー マッピングまでです。マッピングに選択されたポリシー テンプレートは、コントローラにポリシーがない場合に最初に適用されます。

f. アクセス ポイントおよび WLAN プロファイルを追加したら、[Save] をクリックします。

ステップ 9　RF プロファイルを追加するには、[RF Profiles] タブをクリックして、次のパラメータを設定します。

- [802.11a]：ドロップダウン リストから、802.11a 無線 AP の RF プロファイルを選択できます。
- [802.11b]：ドロップダウン リストから、802.11b 無線 AP の RF プロファイルを選択できます。
- RF プロファイルを追加したら、[Save] をクリックします。

（注）　新しい RF プロファイルを追加するには、[Click here] リンクを使用します。詳細については、「RF プロファイル テンプレートの設定（802.11）」（P.11-688）を参照してください。

（注）　AP グループの WLAN インターフェイス マッピングを変更すると、このグループの FlexConnect AP のローカル VLAN マッピングが削除されます。これらのマッピングは、この変更を適用した後に再度設定する必要があります。

ステップ 10　場所グループを追加する場合は、[Venue Group] タブをクリックし、次のパラメータを設定します。

- [Venue Group]：アクセス ポイントが属する場所カテゴリ。次のオプションを使用できます。
  - Unspecified
  - Assembly
  - Business
  - Educational
  - Factory and Industrial
  - Institutional
  - Mercantile
  - Residential
  - Storage
  - Utility and Misc
  - Vehicular
  - Outdoor
- [Venue Type]：選択する場所グループに基づいて場所のタイプを選択できるドロップダウン リスト。
- [Operator Class]：AP グループの運用クラス。使用可能な運用クラスは、81、83、84、112、113、115、116、117、118、119、120、121、122、123、124、125、126、127 です。
- [Venue Language]：この場所で使用される言語を定義する ISO-639 エンコード文字列。この文字列は 3 文字の言語コードです。たとえば、英語の場合は ENG と入力します。
- [Venue Name]：この AP グループの場所の名前。この名前は、基本サービス セット（BSS）に関連付けられ、SSID で場所に関する十分な情報が得られないときに使用されます。場所の名前は最大 252 文字の英数字で、大文字と小文字を区別します。

ステップ 11　[Save] をクリックします。

アクセス ポイント グループの削除

アクセス ポイント グループを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLAN] > [AP Groups] の順に選択します。

ステップ 4　削除するアクセス ポイント グループのチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから [Delete AP Groups] を選択します。

ステップ 6　[OK] をクリックして、削除を実行します。

アクセス ポイント グループの監査

アクセス ポイント グループを監査して、Prime Infrastructure とデバイスの値が異なるかどうかを特定できます。

アクセス ポイント グループを監査するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[WLAN] > [AP Groups] の順に選択します。

ステップ 4　監査するアクセス ポイント グループの名前をクリックします。

（注）　ページの一番下にある [Audit] をクリックします。

コントローラでのポリシーの設定

[Policy Configuration Templates] ページでは、コントローラにデバイス ベースのポリシーを設定することができます。ネットワーク上のユーザまたはデバイス用のポリシーを設定できます。設定できるポリシーの最大数は 64 です。ポリシー設定テンプレートの詳細については、「ポリシー設定テンプレートの設定」（P.11-644）を参照してください。

（注）　AAA オーバーライドがコントローラに設定されている場合は、ポリシーは WLAN および AP グループに適用されません。

ポリシー設定のテンプレートを設定するには、次の手順に従ってください。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Policy Configuration] をクリックするか、左側のサイドバーのメニューから [WLANs] > [Policy Configuration] を選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。

ステップ 4　次のフィールドを設定します。

- [Policy Name]：ポリシー名。
- [Policy Role]：ユーザの属するユーザ タイプまたはユーザ グループ。たとえば、学生、従業員。
- [EAP Type]：クライアントが使用する EAP 認証方式。使用可能なタイプは次のとおりです。
  - LEAP
  - EAP-FAST
  - EAP-TLS
  - PEAP
- [Device Type]：デバイスのタイプを選択できるドロップダウン リスト。
- [VLAN]：ポリシーに関連付けられている VLAN。
- [ACL]：ポリシーの IPv4 ACL を選択できるドロップダウン リスト。
- [QoS]：次の QoS ポリシーのうちの 1 つを選択できるドロップダウン リスト。
  - [Platinum (Voice)]：Voice over Wireless の高い QoS を保証します。
  - [Gold (Video)]：高品質のビデオ アプリケーションをサポートします。

  - [Silver (Best Effort)]：クライアントの通常の帯域幅をサポートします。
  - [Bronze (Background)]：ゲスト サービス用の最小の帯域幅を提供します。
- [Session Timeout]：クライアントが強制的に再認証されるまでの最大時間数（秒単位）。デフォルト値は 0 秒です。
- [Sleeping Client Timeout]：ゲスト クライアントが強制的に再認証されるまでの最大時間数（時間単位）。デフォルト値は 12 時間です。範囲は 1 ～ 720 時間です。

FlexConnect パラメータの設定

FlexConnect により、顧客は各オフィスにコントローラを導入しなくても、本社オフィスからワイドエリア ネットワーク（WAN）リンク経由で、支社またはリモート オフィスのアクセス ポイントを設定および制御できるようになります。ロケーションごとに導入できる FlexConnect のアクセス ポイント数は無制限です。FlexConnect アクセス ポイントは、クライアント データ トラフィックをローカルで切り替えて、コントローラへの接続が失われるとクライアント認証をローカルで実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

- 「FlexConnect AP グループの設定」（P.9-375）
- 「FlexConnect グループの監査」（P.9-379）

FlexConnect AP グループの設定

既存の FlexConnect AP グループのリストを表示するには、次の手順に従います。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[FlexConnect] > [FlexConnect AP Groups] の順に選択します。[FlexConnect AP Groups] ページが開きます。

- [Group Name]：FlexConnect AP グループの名前。グループ名をクリックすると、その詳細が表示されます。

（注）　削除するグループを選択するには、チェックボックスを使用します。

FlexConnect AP グループの設定

FlexConnect アクセス ポイント グループを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[FlexConnect] > [FlexConnect AP Groups] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add FlexConnect AP Group] をクリックして [FlexConnect AP Group] > [Add From Template] ペインを開きます。

ステップ 5　[Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6　[Apply] をクリックします。

（注）　既存の FlexConnect AP Group を変更するには、[FlexConnect AP Group] ページの [Group Name] 列で既存のグループをクリックします。
既存のグループを削除するには、削除するグループのチェックボックスをオンにして、[Select a command] ドロップダウン リストから [Delete FlexConnect AP Group] を選択します。

ステップ 7　[General] タブで、次のフィールドを設定します。

- [Template Name]：このコントローラに適用されているテンプレートの名前。
- [Primary Radius]：ドロップダウン リストから、コントローラ上に存在するプライマリ RADIUS 認証サーバを選択します。

（注）　RADIUS 認証サーバがコントローラ（7.4 より前のリリースの WLC）上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。また、7.4 以降のリリースを使用すると、コントローラ上にない FlexConnect グループ（サイト レベル）のローカル RADIUS サーバを設定できます。

（注）　Prime Infrastructure から FlexConnectRADIUS サーバ設定を適用する前に、コントローラ（WLC 7.3 以前のリリース）に RADIUS サーバ設定を設定する必要があります。

- [Secondary Radius]：ドロップダウン リストから、コントローラ上に存在するセカンダリ RADIUS 認証サーバを選択します。

（注）　RADIUS 認証サーバがコントローラ（7.4 より前のリリースの WLC）上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。また、7.4 以降のリリースを使用すると、コントローラ上にない FlexConnect グループ（サイト レベル）のローカル RADIUS サーバを設定できます。

ステップ 8　[FlexConnectAP] タブで、次のフィールドを設定します。

（注）　AP のイーサネット MAC アドレスは、同じコントローラ上の複数の FlexConnect グループには存在できません。AP イーサネット MAC が別の FlexConnect グループにすでに存在する場合、その AP イーサネット MAC を FlexConnect グループに設定することは、コントローラでは許可されていません。

- [Add AP]：クリックして、既存の FlexConnect グループに追加の FlexConnect AP（Prime Infrastructure に存在しているもの）を追加します。[Add AP] をクリックした場合、この FlexConnect グループの一部であるアクセス ポイントのみがリストされます。

ステップ 9　[Local Authentication] タブで、次のフィールドを設定します。

（注）　[General] タブで、[Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。

- この FlexConnect グループのローカル認証を有効にするには、[FlexConnect Local Authentication Enable] チェックボックスをオンにします。デフォルト値はオフです。

- FlexConnect アクセス ポイントが LEAP を使用してクライアントを認証することができるようにするには、[LEAP Authentication] チェックボックスを選択します。AP ローカル認証が設定されている場合にだけ LEAP 認証を設定できます。
- FlexConnect アクセス ポイントが EAP-FAST を使用してクライアントを認証することができるようにするには、[EAP Fast Authentication] チェックボックスを選択します。AP ローカル認証が設定されている場合にだけ EAP Fast 認証を設定できます。
- 自動的にサーバ キーを生成するには、[Auto key Generation] チェックボックスを選択します。
- [EAP-FAST Authentication] チェックボックスを選択した場合は、EAP-FAST キーを指定して、EAP-FAST キーを確定する必要があります。
- Protected Access Credential（PAC）をプロビジョニングする方法に応じて、次のいずれかを実行します。
  - 手動の PAC プロビジョニングを使用するには、[EAP-FAST Key] テキスト ボックスと [Confirm EAP-FAST Key] テキスト ボックスに、PAC の暗号化と暗号化解除に使用するキーを入力します。キーは 32 桁の 16 進数文字である必要があります。
  - PAC プロビジョニング中に PAC のないクライアントに自動的に PAC を送信できるようにするには、[Auto key generation] チェックボックスをオンにします。
- [EAP-FAST Key] テキスト ボックスに、EAP-FAST サーバの認証局 ID を入力します。識別子は 32 桁の 16 進数文字である必要があります。
- [EAP-FAST Authority ID] テキスト ボックスに EAP-FAST サーバの認証局 ID をテキスト形式で入力します。32 桁までの 16 進数文字を入力できます。
- [EAP-FAST Authority Info] テキスト ボックスに EAP-FAST サーバの認証局情報を入力します。
- [EAP-FAST Pac Timeout] テキスト ボックスの編集ボックスに PAC が表示され続ける秒数を入力することにより、PAC タイムアウト値を指定します。有効範囲は 2 ～ 4095 秒です。
- FlexConnect アクセス ポイントが PEAP を使用してクライアントを認証することができるようにするには、[PEAP Authentication] チェックボックスを選択します。AP ローカル認証が設定されている場合にだけ PEAP 認証を設定できます。
- FlexConnect アクセス ポイントが EAP-TLS を使用してクライアントを認証することができるようにするには、[EAP-TLS Authentication] チェック ボックスを選択します。AP ローカル認証が設定されている場合にだけ EAP-TLS 認証を設定できます。
- アクセス ポイントへの EAP ルートおよびデバイス証明書をダウンロードするには、[EAP TLS Certificate Download] チェックボックスを選択します。このオプションは、[EAP-TLS Authentication] チェックボックスを選択した場合にのみ使用できます。

  [EAP TLS Certificate Download] チェックボックスを選択してコントローラにこれを適用しようとした後で、EAP 証明書がコントローラに使用可能でない場合、エラー メッセージが表示されることがあります。コントローラに証明書をダウンロードして適用しても、その状態は Prime Infrastructure には保持されません。また、この情報は FlexConnect 監査レポートでは使用できません。

（注）　FlexConnect のローカル認証が有効な場合にだけ、LEAP、EAP-FAST、PEAP、または EAP-TLS 認証を設定できます。

ステップ 10　[Image Upgrade] タブをクリックし、次の項目を設定します。

- [FlexConnect AP Upgrade] : FlexConnect アクセス ポイントをアップグレードする場合は、このチェックボックスをオンにします。

- [Slave Maximum Retry Count] : スレーブが FlexConnect グループ内のマスターからのダウンロード開始を試行する最大回数を指定します。このオプションは、[FlexConnect AP Upgrade] チェックボックスをオンにした場合のみ使用できます。

（注）　[General] タブで [FlexConnect AP Upgrade] チェックボックスが有効になっている場合に限り、アクセス ポイントをマスター アクセス ポイントとして追加できます。

ステップ 11　[ACL Mapping] タブで、次のフィールドを設定します。

- [VLAN-ACL Mapping] タブをクリックして、VLAN ACL マッピングを表示、追加、編集、または削除します。
  - [Add Row] をクリックします。
  - VLAN ID を入力します。有効な VLAN ID の範囲は 1 ～ 4094 です。
  - [Ingress ACL] ドロップダウン リストから、入力 ACL を選択します。
  - [Egress AC] ドロップダウン リストから、出力 ACL を選択します。
  - [Save] をクリックします。
- [WLAN-ACL Mapping] タブをクリックし、外部 Web 認証用の FlexConnect アクセス コントロール リストを選択します。
  - [Add Row] をクリックします。
  - [WLAN Profile Name] ドロップダウン リストから、WLAN プロファイルを選択します。
  - [WebAuth ACL] ドロップダウン リストから、WebAuth ACL を選択します。
  - [Save] をクリックします。

（注）　最大 16 個の WebAuth ACL を追加できます。

- Web ポリシーとして追加するには、[Policies] タブをクリックし [FlexConnect] アクセス コントロール リストを選択します。
  - [Add Row] をクリックします。
  - [Web-Policy ACL] ドロップダウン リストから、WebPolicy ACL を選択します。
  - [Save] をクリックします。

（注）　最大 16 個の Web-Policy ACL を追加できます。

- [Local Split] タブをクリックして、Local Split ACL マッピングを表示、追加、編集、または削除します。
  - [Add Row] をクリックします。
  - [WLAN Profile Name] ドロップダウン リストから、WLAN プロファイルを選択します。

（注）　FlexConnect 中央スイッチング WLAN だけが [WLAN Profile Name] ドロップダウン リストに表示されます。

  - [Local-Split ACL] ドロップダウン リストから、FlexConnect ACL を選択します。
  - [Save] をクリックします。

ステップ 12　[Central DHCP] タブをクリックして、中央 DHCP の処理を表示、追加、編集、または削除します。

- [Add Row] をクリックします。
- [WLAN Profile Name] ドロップダウン リストから、WLAN プロファイルを選択します。

（注）　FlexConnect ローカル スイッチング WLAN だけが [WLAN Profile Name] ドロップダウン リストに表示されます。

- [Central DHCP] ドロップダウン リストから、[Enable] または [Disable] を選択します。この機能を有効にすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。
- [Override DNS] ドロップダウン リストから、[Enable] または [Disable] を選択します。ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバ アドレスのオーバーライドを有効または無効にできます。中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
- [NAT-PAT] ドロップダウン リストで、[Enable] または [Disable] を選択します。ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）を有効または無効にできます。NAT および PAT をイネーブルにするには、[Central DHCP Processing] を有効にする必要があります。
- [Save] をクリックします。

ステップ 13　[WLAN-VLAN Mapping] タブで、VLAN ID を FlexConnect アクセス ポイントに割り当て、ローカルにスイッチされた WLAN に VLAN マッピングを設定します。

- [WLAN Profile Name]：WLAN の名前。
- [VLAN ID]：ローカル スイッチングを行う際にクライアントが受信する IP アドレスを送信する VLAN の番号。

ステップ 14　[Save] をクリックします。

FlexConnect グループの監査

FlexConnect 設定が Prime Infrastructure またはコントローラ上で時間とともに変化した場合は、設定を監査できます。変更は、後続のページで表示できます。Prime Infrastructure またはコントローラをリフレッシュして設定を同期するように指定できます。

セキュリティ パラメータの設定

ここでは、次の内容について説明します。

- 「コントローラのファイル暗号化の設定」（P.9-380）
- 「[Controllers] > [IPaddr] > [Security] > [AAA] の設定」（P.9-380）
- 「[Controllers] > [IPaddr] > [Security] > [Local EAP] の設定」（P.9-391）
- 「ユーザ ログイン ポリシーの設定」（P.9-394）
- 「手動で無効にしたクライアントの管理」（P.9-394）
- 「アクセス コントロール リストの設定」（P.9-395）
- 「CPU アクセス コントロール リストの設定」（P.9-398）

- 「IDS センサー リストの設定」（P.9-398）
- 「CA 証明書の設定」（P.9-399）
- 「ID 証明書の設定」（P.9-400）
- 「[Controllers] > [IPaddr] > [Security] > [Web Auth Certificate] の設定」（P.9-401）
- 「ワイヤレス保護ポリシーの設定」（P.9-401）
- 「不正ポリシーの設定」（P.9-402）
- 「不正 AP ルールの設定」（P.9-403）
- 「クライアント除外ポリシーの設定」（P.9-403）
- 「コントローラの標準シグニチャ パラメータの設定」（P.9-404）
- 「カスタム シグニチャの設定」（P.9-408）
- 「AP 認証および MFP の設定」（P.9-409）

コントローラのファイル暗号化の設定

コントローラのファイル暗号化を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [File Encryption] の順に選択します。ファイル暗号化により、TFTP サーバへのコントローラ コンフィギュレーション ファイルのアップロードまたはダウンロードの際に、データが必ず暗号化されるようになります。

ファイル暗号化パラメータは次のとおりです。

- [File Encryption]：このオプションを有効にした場合、コントローラ コンフィギュレーション ファイルが TFTP サーバを介してアップロードまたはダウンロードされる際に、コントローラ コンフィギュレーション ファイル内のデータが暗号化されます。
- [Encryption Key]：正確に 16 文字のテキスト文字列。
- [Confirm Encryption Key]：暗号キーを入力します。

[Controllers] > [*IPaddr*] > [Security] > [AAA] の設定

ここでは、コントローラのセキュリティ AAA パラメータの設定方法について説明します。内容は次のとおりです。

- 「AAA の一般パラメータの設定」（P.9-381）
- 「AAA RADIUS 認証サーバの設定」（P.9-381）
- 「AAA RADIUS アカウンティング サーバの設定」（P.9-382）
- 「AAA RADIUS フォールバック パラメータの設定」（P.9-383）
- 「AAA LDAP サーバの設定」（P.9-383）
- 「AAA TACACS+ サーバの設定」（P.9-385）
- 「AAA ローカル ネット ユーザの設定」（P.9-386）
- 「AAA MAC フィルタリングの設定」（P.9-387）

- 「AAA AP/MSE 許可の設定」（P.9-388）
- 「AAA Web 認証の設定」（P.9-389）
- 「AAA Web 認証の設定」（P.9-389）

AAA の一般パラメータの設定

[General] ページでは、コントローラ上のローカル データベース エントリを設定できます。

ローカル データベース エントリを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [General] の順に選択します。

ステップ 4　許可されるデータベース エントリの最大数を入力します。この数は、次回リブート時に有効になります。有効な範囲は 512 ～ 2048 です。

AAA RADIUS 認証サーバの設定

既存の RADIUS 認証サーバのサマリーを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [RADIUS Auth Servers] の順に選択します。次の RADIUS Auth Servers パラメータが表示されます。

- [Server Index] : RADIUS サーバのアクセス プライオリティ番号（表示のみ）。[Configure IPaddr] > [RADIUS Authentication Server] の順にクリックして移動します。
- [Server Address] : RADIUS サーバの IP アドレス（読み取り専用）。
- [Port Number] : コントローラ ポート番号（読み取り専用）。
- [Admin Status] : [Enabled] または [Disabled]。
- [Network User] : [Enabled] または [Disabled]。
- [Management User] : [Enabled] または [Disabled]。

認証サーバの追加

認証サーバを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [RADIUS Auth Servers] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Auth Server] 選択して、[Radius Authentication Server] > [Add From Template] ページを開きます。

ステップ 5　[Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6　[Apply] をクリックします。

（注）　RADIUS 認証サーバのテンプレートを新規作成するには、[Configure] > [Controller Templates] > [Security] > [RADIUS Auth Servers] の順に選択します。

AAA RADIUS アカウンティング サーバの設定

既存の RADIUS アカウンティング サーバのサマリーを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [RADIUS Acct Servers] の順に選択します。RADIUS Acct Server パラメータには、次のようなものがあります。

- [Server Index] : RADIUS サーバのアクセス プライオリティ番号（読み取り専用）。クリックして [Radius Acct Servers Details] ページを開きます。

  （注）　現在のアカウンティング サーバのパラメータを編集または監査するには、該当するアカウンティング サーバのサーバ インデックスをクリックします。

- [Server Address] : RADIUS サーバの IP アドレス（読み取り専用）。
- [Port Number] : コントローラ ポート番号（読み取り専用）。
- [Admin Status] : [Enabled] または [Disabled]。
- [Network User] : [Enabled] または [Disabled]。

コマンド ボタン

- Save
- Audit

アカウンティング サーバの追加

アカウンティング サーバを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [RADIUS Acct Servers] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Acct Server] 選択して、[Radius Acct Servers Details] > [Add From Template] ページを開きます。

ステップ 5　[Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6　ドロップダウン リストから、このテンプレートに適用するコントローラを選択します。

ステップ 7　[Apply] をクリックします。

（注）　RADIUS アカウンティング サーバのテンプレートを新規作成するには、[Configure] > [Controller Templates Launch Pad] > [Security] > [RADIUS Acct Servers] の順に選択します。

アカウンティング サーバの削除

アカウンティング サーバを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [RADIUS Acct Servers] の順に選択します。

ステップ 4　該当するアカウンティング サーバのチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから [Delete Acct Server] を選択します。

ステップ 6　[Go] をクリックします。

ステップ 7　ポップアップ ダイアログボックスで [OK] をクリックして、削除を確定します。

AAA RADIUS フォールバック パラメータの設定

RADIUS フォールバック パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [RADIUS Fallback] の順に選択します。

ステップ 4　次のパラメータを追加または変更します。

- RADIUS:FallbackMode
- Username
- Time Interval

ステップ 5　[Save] をクリックします。

（注）　[Audit] をクリックして、Prime Infrastructure およびコントローラの現在の設定ステータスをチェックします。

AAA LDAP サーバの設定

このページでは、このコントローラに対して LDAP サーバを追加および削除できます。

[LDAP Servers] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [LDAP Servers] の順に選択します。

このページには、現在このコントローラが使用している LDAP サーバが表示されます。次のパラメータが含まれます。

- [Check box]：チェックボックスをオンにして、削除する LDAP サーバを選択します。
- [Server Index]：LDAP サーバを識別するために割り当てられた番号。

（注）　LDAP サーバの設定ページに移動するには、インデックス番号をクリックします。

- [Server Address]：LDAP サーバの IP アドレス。
- [Port Number]：LDAP サーバとの通信に使用されるポート番号。
- [Admin Status]：サーバ テンプレートのステータス。

  LDAP サーバ テンプレートの使用が有効か無効かを示します。

（注）　列のタイトルがリンクの場合は、そのリンクをクリックして昇順と降順を切り替えできます。

（注）　現在、Prime Infrastructure では匿名バインドおよび認証済みバインドの両方の LDAP 設定がサポートされています。詳細については、「新しい LDAP バインド要求の設定」（P.9-385）を参照してください。

LDAP サーバの [Select a command] ドロップダウン リスト オプション

LDAP サーバの追加

LDAP サーバを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [LDAP Servers] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add LDAP Server] を選択します。

ステップ 5　[Go] をクリックします。

LDAP サーバの削除

LDAP サーバを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [LDAP Servers] の順に選択します。

ステップ 4　削除する LDAP サーバのチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから [Delete LDAP Servers] を選択します。

ステップ 6　[Go] をクリックします。

新しい LDAP バインド要求の設定

現在、Prime Infrastructure では匿名バインドおよび認証済みバインドの両方の LDAP 設定がサポートされています。バインドは、検索処理を実行する空きソケットです。

LDAP バインド要求を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Security] > [AAA] > [LDAP Servers] の順に選択します。

ステップ 3　[Bind Type] ドロップダウン リストから、[Authenticated] または [Anonymous] を選択します。[Authenticated] を選択した場合、バインド ユーザ名およびパスワードも入力する必要があります。

ステップ 4　[Server User Base DN] テキスト ボックスに、ユーザすべてのリストを含む LDAP サーバ内のサブツリーの識別名を入力します。

ステップ 5　[Server User Attribute] テキスト ボックスに LDAP サーバのユーザ名を含む属性を入力します。

ステップ 6　[Server User Type] テキスト ボックスにユーザを識別する ObjectType 属性を入力します。

ステップ 7　[Retransmit Timeout] テキスト ボックスに再転送までの時間を秒単位で入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

ステップ 8　LDAP サーバに管理権限を持たせる場合は、[Admin Status] チェックボックスをオンにします。

ステップ 9　[Save] をクリックします。

AAA TACACS+ サーバの設定

このページでは、このコントローラに対して TACACS+ サーバを追加および削除できます。

[TACACS+ Servers] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [TACACS+ Servers] の順に選択します。

このページには、現在このコントローラが使用している TACACS+ サーバが表示されます。次のパラメータが含まれます。

- [Check box]：チェックボックスをオンにして、削除する TACACS+ サーバを選択します。
- [Server Type]：TACACS+ のサーバ タイプ（アカウンティング、許可、または認証）。

- [Server Index]：TACACS+ サーバを識別し、使用プライオリティを設定するために割り当てられた番号。TACACS+ サーバの設定ページに移動するには、インデックス番号をクリックします。
- [Server Address]：TACACS+ サーバの IP アドレス。
- [Port Number]：TACACS+ サーバとの通信に使用されるポート番号。
- [Admin Status]：サーバ テンプレートのステータス。

  TACACS+ サーバ テンプレートの使用が有効かを示します。

列のタイトルがリンクの場合は、そのリンクをクリックして昇順と降順を切り替えできます。

[Select a command] ドロップダウン リストには、次のオプションが表示されます。

- [Add TACACS+ Server]：このオプションを選択して [Go] をクリックすると、TACACS+ サーバがコントローラに追加されます。
- [Delete TACACS+ Servers]：このオプションを選択して [Go] をクリックすると、チェックボックスがオンになっているすべての TACACS+ サーバがコントローラから削除されます。

AAA ローカル ネット ユーザの設定

このページには、特定の WLAN へのアクセスが許可されているクライアントの、既存のローカル ネットワーク ユーザ コントローラのサマリーが表示されます。これは、RADIUS 認証プロセスの管理バイパスです。レイヤ 3 Web 認証を有効にする必要があります。クライアント情報は、まず RADIUS 認証サーバに渡され、クライアント情報が RADIUS データベースのエントリと一致しない場合は、ローカル データベースに対してポーリングが実行されます。RADIUS 認証が失敗した場合、または存在しない場合は、このデータベースで見つかったクライアントがネットワーク サービスへのアクセスを付与されます。

- 「ローカル ネット ユーザの追加」（P.9-386）
- 「ローカル ネット ユーザの削除」（P.9-387）

既存のローカル ネットワーク ユーザを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [Local Net Users] の順に選択します。[Local Net Users] ページには、次のローカル ネット ユーザ パラメータが表示されます。

- [Username]：ユーザ定義の ID。
- [WLAN ID]：任意の WLAN ID（1 ～ 16）。すべての WLAN の場合は 0、このローカル ネット ユーザがアクセスできるサードパーティ製 WLAN の場合は 17。
- [Description]：オプションのユーザが定義した説明

ローカル ネット ユーザの追加

ローカル ネット ユーザを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [Local Net Users] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Local Net User] を選択して [Local Net User] > [Add From Template] ページを開きます。

ステップ 5　[Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6　[Apply] をクリックします。

（注）　ローカル ネット ユーザのテンプレートを新規作成するには、[Configure] > [Controller Templates] > [Security] > [Local Net Users] の順に選択します。詳細については、「ローカル ネットワーク ユーザ テンプレートの設定」（P.11-660）を参照してください。

ローカル ネット ユーザの削除

ローカル ネット ユーザを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [Local Net Users] の順に選択します。

ステップ 4　該当するローカル ネット ユーザのチェックボックスを選択します。

ステップ 5　[Select a command] ドロップダウン リストから、[Delete Local Net Users] を選択します。

ステップ 6　[Go] をクリックします。

ステップ 7　ダイアログボックスで [OK] をクリックして、削除を確定します。

AAA MAC フィルタリングの設定

このページには、MAC フィルタ情報を表示できます。

（注）　ブロードキャスト用の MAC アドレスを使用できません。

[MAC Filtering] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [MAC Filtering] の順に選択します。[MAC Filtering] ページには、次のパラメータが表示されます。

- MAC フィルタ パラメータ
  - [RADIUS Compatibility Mode]：ユーザ定義の RADIUS サーバの互換性（[Cisco ACS]、[FreeRADIUS]、または [Other]）。
  - [MAC Delimiter]：MAC デリミタは、RADIUS サーバの要件に応じて、コロン（xx:xx:xx:xx:xx:xx）、ハイフン（xx-xx-xx-xx-xx-xx）、シングル ハイフン（xxxxxx-xxxxxx）、またはデリミタなし（xxxxxxxxxxxx）に設定できます。

- MAC Filters
  - [MAC Address]：クライアント MAC アドレス。クリックして [Configure *IPaddr*] > [MAC Filter] を開きます。
  - [WLAN ID]：1 ～ 16。17 = サードパーティ製 AP WLAN、0 = すべての WLAN。
  - [Interface]：アソシエートされたインターフェイス名を表示します。
  - [Description]：オプションのユーザ定義の説明を表示します。

ステップ 4　[Select a command] ドロップダウン リストから [Add MAC Filters] を選択して MAC フィルタを追加するか、[Delete MAC Filters] を選択してテンプレートを削除するか、[Edit MAC Filter Parameters] を選択して MAC フィルタを編集します。

ステップ 5　[Go] をクリックします。

AAA AP/MSE 許可の設定

[AP/MSE Authorization] ページには、アクセス ポイント ポリシーおよび許可されたアクセス ポイントのリストが表示されます。このリストには、アクセス ポイントで許可に使用する証明書のタイプも示されます。

（注）　ブロードキャスト用の MAC アドレスを使用できません。

[AP/MSE Authorization] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [AP/MSE Authorization] の順に選択します。[AP/MSE Authorization] ページに次のパラメータが表示されます。

- AP Policies
  - [Authorize APs]：有効または無効。
  - [Accept SSC-APs]：有効または無効。
- AP/MSE Authorization
  - [AP/MSE Base Radio MAC Address]：許可されたアクセス ポイントの MAC アドレス。

    （注）　[AP/MSE Base Radio MAC Address] をクリックすると、AP/MSE 許可の詳細が表示されます。

  - Type
  - [Certificate Type]：MIC または SSC。
  - [Key Hash]：40 文字の長さの 16 進数 SHA1 キー ハッシュ。

    （注）　キー ハッシュは、証明書のタイプが SSC の場合のみ表示されます。

コマンド ボタン

- [Add AP/MSE Auth Entry] : このコマンドを選択して [Go] をクリックします。「アクセス ポイント許可または MSE 許可テンプレートの設定」（P.11-664）を参照してください。
- [Delete AP/MSE Auth Entries] : 1 つ以上のアクセス ポイントを選択してこのコマンドを選択し、[Go] をクリックして、AP 許可リストから選択したアクセス ポイントを削除します。
- [Edit AP Policies] : このコマンドを選択して [Go] をクリックします。「AP ポリシーの編集」（P.9-389）を参照してください。

AP ポリシーの編集

AP/MSE 許可アクセス ポイント ポリシーを編集するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [AP/MSE Authorization] の順に選択します。

ステップ 4　[Edit AP Policies] ページで、必要に応じて次のパラメータを編集します。

- [Authorize APs] : アクセス ポイント許可を有効にする場合は、このチェックボックスをオンにします。
- [Accept SSC-APs] : SSE アクセス ポイントの承認を有効にする場合は、このチェックボックスをオンにします。

ステップ 5　[Save] をクリックして変更を確定するか、[Audit] をクリックしてこれらのデバイス値の監査を実行するか、[Cancel] をクリックしてこのページを変更せずに閉じます。

AAA Web 認証の設定

[Web Auth Configuration] ページでは、Web 認証の設定タイプを設定できます。このタイプをカスタマイズに設定した場合は、コントローラにより提供された内部 Web 認証ページが、ユーザのダウンロードした Web 認証に置き換わります。

[Web Auth Configuration] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [Web Auth Configuration] の順に選択します。

ステップ 4　[Web Authentication] ページで、ドロップダウン リストから Web 認証タイプを選択します。Web 認証オプションには、デフォルトの内部 Web ページ、カスタマイズ Web 認証ページ、または外部 Web ページが含まれます。

ステップ 5　選択したタイプに応じて、Web 認証パラメータを設定します。

- デフォルトの内部
  - [Logo Display] : ロゴの表示を有効または無効にします。
  - [Web Auth Page Title] : Web 認証ページに表示されるタイトル。
  - [Web Auth Page Message] : 認証ページに表示されるメッセージ。

  - [Custom Redirect URL]：認証が成功した後にユーザがリダイレクトされる URL。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

- カスタマイズ Web 認証

  サンプルのログイン ページをダウンロードして、そのページをカスタマイズするオプションがあります。カスタマイズ Web 認証ページを使用する場合は、サーバからサンプルの login.tar バンドル ファイルをダウンロードし、login.html ファイルを編集して .tar または .zip ファイルとして保存してから、.tar または .zip ファイルをコントローラにダウンロードする必要があります。

  プレビュー イメージをクリックして、このサンプル ログイン ページを TAR としてダウンロードします。HTML の編集後にここをクリックすると [Download Web Auth] ページにリダイレクトされます。詳細については、「コントローラへのカスタマイズ Web 認証バンドルのダウンロード」（P.9-299）を参照してください。

- External

  - [External Redirect URL]：ネットワーク上の外部サーバにある login.html の場所。

    外部 Web 認証サーバが設定されていない場合は、外部 Web 認証サーバを設定するオプションがあります。

    [No external Web Auth Server(s) configured]。外部 Web 認証サーバを設定する場合は、このオプションを選択します。

（注）　外部 Web サーバ テンプレートを設定する場合は、「外部 Web 認証サーバ テンプレートの設定」（P.11-670）を参照してください。

コマンド ボタン

- [Save]：現在の設定をコントローラに保存します。
- [Audit]：Prime Infrastructure およびコントローラの現在の設定ステータスをチェックします。

AAA パスワード ポリシーの設定

このページでは、パスワード ポリシーを決定できます。

既存のパスワード ポリシーを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [AAA] > [Password Policy] の順に選択します。

ステップ 4　パスワード ポリシーのパラメータを必要に応じて変更します。

ステップ 5　[Save] をクリックします。

（注）　パスワード ポリシー オプションを無効にすると、「Disabling the strong password check(s) will be a security risk as it allows weak passwords」というメッセージが表示されます。

[Controllers] > [*IPaddr*] > [Security] > [Local EAP] の設定

ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンド システムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。

ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバから独立します。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザの資格情報を取得して、ユーザを認証します。

ローカル EAP の一般パラメータの設定

このページでは、ローカル EAP のタイムアウト値を指定できます。その後、このタイムアウト値を持つテンプレートを追加したり、既存のテンプレートを変更できます。

（注） コントローラ上で RADIUS サーバが設定されている場合は、コントローラはまず RADIUS サーバを使用してワイヤレス クライアントを認証しようとします。ローカル EAP は、RADIUS サーバがタイムアウトしていたり、RADIUS サーバが設定されていない場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番めの RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番めの RADIUS サーバを試行し、次に 4 番めの RADIUS サーバ、その次にローカル EAP を試行します。

ローカル EAP のタイムアウト値を指定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Local EAP] > [General - Local EAP] の順に選択します。

ステップ 4　[Local Auth Active Timeout] テキスト ボックスにローカル認証アクティブ タイムアウトを入力します（秒単位）。

（注） ローカル認証アクティブ タイムアウトは、すべての RADIUS サーバが失敗した後、ローカル EAP が必ず使用されるタイムアウト時間を指します。

ステップ 5　EAP-FAST、手動パスワード入力、ワンタイム パスワード、または 7920/7921 電話を使用する際は、次の値を調整する必要があります。

（注） 自動プロビジョニングを使用している PAC をクライアントで取得する場合、コントローラで 802.1x のタイムアウト値を大きくする必要があります（デフォルトは 2 秒）。Cisco ACS サーバでは、デフォルトの 20 秒を推奨します。

- Local EAP Identify Request Timeout =1（秒単位）
- Local EAP Identity Request Maximum Retries=20（秒単位）
- Local EAP Dynamic Wep Key Index=0
- Local EAP Request Timeout=20（秒単位）

- Local EAP Request Maximum Retries=2
- EAPOL-Key Timeout=1000（ミリ秒単位）
- EAPOL-Key Max Retries=2
- Max-Login Ignore Identity Response

（注）　複数のコントローラで次の値が同じに設定されていないと、ローミングが失敗します。

ステップ 6　[Save] をクリックします。

コマンド ボタン

- [Save]：クリックして現在のテンプレートを保存します。
- [Apply to Controllers]:クリックして現在のテンプレートをコントローラに適用します。[Apply to Controllers] ページで該当するコントローラを選択し、[OK] をクリックします。
- [Delete]：クリックして現在のテンプレートを削除します。現在コントローラにそのテンプレートが適用されている場合は、[OK] をクリックして、テンプレートが適用されている選択したコントローラから、テンプレートを削除することを確定します。
- [Cancel]：クリックして現在のテンプレート作成または現在のテンプレートの変更をキャンセルします。

ローカル EAP プロファイルの設定

このページでは、ローカル EAP プロファイルへのテンプレートの適用、または既存のテンプレートの変更が可能です。

（注）　LDAP バックエンド データベースは、次のローカル EAP メソッドだけをサポートします。証明書による EAP-TLS および EAP-FAST。LDAP バックエンド データベースでは、LEAP および PAC による EAP-FAST はサポートされません。

- 「既存のローカル EAP プロファイルの表示」（P.9-392）
- 「ローカル ネット ユーザの追加」（P.9-393）

既存のローカル EAP プロファイルの表示

既存のローカル EAP プロファイルを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Local EAP] > [Local EAP Profiles] の順に選択します。[Local EAP Profiles] ページには、次のパラメータが表示されます。

- [EAP Profile Name]：ユーザ定義の ID。
- [LEAP]：Cisco Key Integrity Protocol（CKIP）と MMH Message Integrity Check（MIC）を使用してデータを保護する認証タイプ。ユーザ名とパスワードを使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。

- [EAP-FAST] : 3 段階のトンネル認証プロセスを使用して高度な 802.1x EAP 相互認証を実行する認証タイプ（Flexible Authentication via Secure Tunneling）。ユーザ名、パスワード、および PAC（保護されたアクセス クレデンシャル）を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。
- [TLS] : クライアント アダプタおよび RADIUS サーバの動的セッション ベースの暗号鍵を使用してデータを暗号化する認証タイプ。認証のためには、クライアント証明書が必要です。
- [PEAP] : 保護拡張認証プロトコル。

ローカル ネット ユーザの追加

ローカル EAP プロファイルを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Local EAP] > [Local EAP Profile] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Local EAP Profile] を選択して [Local EAP Profile] > [Add From Template] ページを開きます。

ステップ 5　[Select a template to apply to this controller] ドロップダウン リストからテンプレートを選択します。

ステップ 6　[Apply] をクリックします。

（注）　ローカル EAP プロファイルのテンプレートを新規作成するには、[Configure] > [Controller Templates] > [Security] > [Local EAP Profiles] の順に選択します。

ローカル EAP の一般 EAP-FAST パラメータの設定

この認証のタイプ（Flexible Authentication via Secure Tunneling）は、3 段階のトンネル認証プロセスを使用して高度な 802.1x EAP 相互認証を実行します。ユーザ名、パスワード、および PAC を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。

EAP-FAST パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Local EAP] > [EAP-FAST Parameters] の順に選択します。

ステップ 4　次のパラメータを入力します。

- [Time to live for the PAC] : PAC の有効日数。有効な範囲は 1 ～ 1000 日で、デフォルトの設定は 10 日です。
- [Authority ID] : 16 進数文字で表したローカル EAP-FAST サーバの認証局 ID。最大 32 文字の 16 進数文字を入力できますが、文字数は偶数である必要があります。
- [Authority Info] : テキスト形式で表したローカル EAP-FAST サーバの認証局 ID に関する情報。

- [Server Key]：PAC の暗号化と暗号化解除に使用するキー（16 進数文字）。
- [Confirm Server Key]：再度入力して正しいサーバ キーを確認します。
- [Anonymous Provision]：匿名プロビジョニングを有効にする場合は、このチェックボックスをオンにします。

（注）　この機能を使用すると、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。この機能を無効にすると、PAC を手動でプロビジョニングする必要があります。

ステップ 5　[Save] をクリックします。

ローカル EAP の一般ネットワーク ユーザ プライオリティの設定

LDAP とローカル データベースがユーザ クレデンシャル情報を取得するために使用する順序を指定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Local EAP] > [Network Users Priority] の順に選択します。

ステップ 4　左右の矢印を使用して、右端のリストにネットワーク クレデンシャルを入れたり、除外することができます。

ステップ 5　上下のボタンを使用してクレデンシャルを試行する順序を指定します。

ステップ 6　[Save] をクリックします。

ユーザ ログイン ポリシーの設定

ユーザ ログイン ポリシーを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [User Login Policies] の順に選択します。

ステップ 4　1 つのユーザ名で同時にログインできる最大数を入力します。

ステップ 5　[Save] をクリックします。

手動で無効にしたクライアントの管理

[Disabled Clients] ページでは、除外された（ブラックリストに掲載された）クライアントの情報を表示できます。

アソシエートを試行した際に、3 回認証に失敗したクライアントはオペレータが定義したタイムアウトの間、再度アソシエートを試行できないように、自動的にブロック（または除外）されます。除外タイムアウトが経過すると、クライアントは認証の再試行を許可され、アソシエートすることができます。このとき、認証に失敗すると再び除外されます。

（注）　ブロードキャスト用の MAC アドレスを使用できません。

[Manually Disabled Clients] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Manually Disabled Clients] の順に選択します。[Manually Disabled Clients] ページには、次のパラメータが表示されます。

- [MAC Address]：無効にされたクライアントの MAC アドレス。リスト項目をクリックして、無効にされたクライアントの説明を編集します。
- [Description]：無効にされたクライアントのオプションの説明。

手動で無効にされたクライアントの [Select a command] ドロップダウン リスト オプション

- [Add Manually Disabled Client]：ドロップダウン リストからこのオプションを選択して [Go] をクリックします。「手動による無効化クライアント テンプレートの設定」（P.11-665）を参照してください。
- [Delete Manually Disabled Clients]：該当するコントローラのチェックボックスをオンにし、ドロップダウン リストからこのオプションを選択して、[Go] をクリックします。

アクセス コントロール リストの設定

[Access Control Lists] ページには、このコントローラで使用できるアクセス コントロール リスト（ACL）が表示されます。また、適用されているアクセス コントロール リストに新しいルールを追加したり、既存のルールを編集したりできます。

[Access Control Lists] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で該当する IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Access Control Lists] の順に選択します。

- [Check box]：チェックボックスを使用して、削除する ACL を 1 つ以上選択します。
- [ACL Name]：ユーザ定義のこのテンプレートの名前。ACL 項目をクリックすると、そのパラメータを表示できます。「[IPaddr] > [Access Control List] > [listname Rules] の設定」（P.9-396）を参照してください。

[*IPaddr*] > [Access Control List] > [*listname* Rules] の設定

このページには、このアクセス コントロール リスト（ACL）に適用されている、現在のアクセス コントロール リスト ルールが表示されます。

[Access Control Lists Rules] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　[IP Address] 列で該当する IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Access Control Lists] の順に選択します。

ステップ 4　ACL 名をクリックします。

- [Check box]：アクセス コントロール リストのルールを選択して削除します。
- [Seq#]：オペレータは、各 ACL に対して最大 64 個のルールを定義できます。各 ACL のルールは、1 ～ 64 の連続した順序で一覧表示されます。つまり、ルール 29 を追加するときにすでにルール 1 ～ 4 が定義されている場合、このルールはルール 5 となります。

（注）　連番を追加または変更する場合、オペレーティング システムは連続した順序が維持されるようその他のルールの連番を調整します。たとえば、連番 1 ～ 7 が定義されていて、7 番を 5 番に変更する場合、オペレーティング システムは自動的に 6 番を 7 番に、5 番を 6 番に割り当て直します。

- [Action]：許可、拒否。
- [Source IP/Mask]：送信元 IP アドレスおよびマスク。
- [Destination IP/Mask]：送信先 IP アドレスおよびマスク。
- [Protocol]：この ACL を使用するプロトコル。
  - [Any]：すべてのプロトコル
  - [TCP]：トランスミッション コントロール プロトコル
  - [UDP]：ユーザ データグラム プロトコル
  - [ICMP]：インターネット制御メッセージ プロトコル
  - [ESP]：IP カプセル化セキュリティ ペイロード
  - [AH]：認証ヘッダー
  - [GRE]：Generic Routing Encapsulation
  - [IP]：インターネット プロトコル
  - [Eth Over IP]：Ethernet over Internet Protocol
  - [Other Port OSPF]：Open Shortest Path First
  - [Other]：その他の任意の IANA プロトコル（http://www.iana.org/）

  TCP または UDP を選択すると、Source Port および Dest Port パラメータが表示されます。
  - [Source Port]：送信元ポート。[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を指定できます。

  - [Dest Port]：宛先ポート。[TCP] または [UDP] が選択されている場合、[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を選択できます。
- [DSCP (Differentiated Services Code Point)]：Any、または 0 ～ 255。

新しい ACL ルールを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Access Control Lists] の順に選択します。

ステップ 4　ACL 名をクリックします。

ステップ 5　該当する [Seq#] をクリックするか、[Add New Rule] を選択してこのページにアクセスします。

FlexConnect アクセス コントロール リストの設定

FlexConnect 上の ACL は、ローカルでスイッチされた、アクセス ポイントからのデータ トラフィックの保護および完全性のために、FlexConnect アクセス ポイントで必要とされるアクセス コントロールを提供するメカニズムを提供します。

ここでは、次の内容について説明します。

- 「FlexConnect アクセス コントロール リストの追加」（P.9-397）
- 「FlexConnect アクセス コントロール リストの削除」（P.9-398）

FlexConnect アクセス コントロール リストの追加

FlexConnect アクセス ポイントのアクセス コントロール リストを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [FlexConnect ACLs] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add FlexConnect ACLs] を選択します。

ステップ 5　[Go] をクリックします。

（注）　テンプレートが作成されていない場合は、FlexConnect ACL は追加できません。使用できるテンプレートが存在しない状態で FlexConnect ACL の作成を試行した場合は、[New Controller Templates] ページにリダイレクトされます。ここで、FlexConnect ACL 用のテンプレートを作成できます。

[FlexConnect ACLs Details] ページが表示されます。

ステップ 6　ドロップダウン リストからコントローラに適用するテンプレートを選択して、[Apply] をクリックします。

作成した FlexConnect ACL が、[Configure] > [Controllers] > [*IP Address*] > [Security] > [FlexConnect ACLs] に表示されます。

FlexConnect アクセス コントロール リストの削除

FlexConnect ACL を削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [FlexConnect ACLs] の順に選択します。

ステップ 4　[FlexConnect ACLs] ページから、削除する FlexConnect ACL を 1 つ以上選択します。

ステップ 5　[Select a command] ドロップダウン リストから [Delete FlexConnect ACLs] を選択します。

ステップ 6　[Go] をクリックします。

CPU アクセス コントロール リストの設定

アクセス コントロール リスト（ACL）は、コントローラの CPU に適用して、その CPU へのトラフィックを制御できます。

[Access Control Lists Rules] ページには、選択したコントローラに適用された CPU アクセス コントロール リストのテンプレートの名前が表示されます。

[Access Control Lists Rules] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [CPU Access Control Lists] の順に選択します。

ステップ 4　[Enable CPU ACL] チェックボックスをオンにして、CPU ACL を有効にします。

このチェックボックスをオンにした場合、次のパラメータを使用できます。

- [ACL Name] : [ACL Name] ドロップダウン リストから使用する ACL を選択します。
- [CPU ACL Mode] : この CPU ACL リストで制御するデータ トラフィックの方向を選択します。

  選択肢は、[The wired side of the data traffic]、[the wireless side of the data traffic]、または [both wired and wireless] です。

IDS センサー リストの設定

センサーが攻撃を識別した場合は、攻撃しているクライアントを回避するようにコントローラに警告します。新しい IDS（侵入検知システム）センサーを追加した場合は、回避したクライアントのレポートをセンサーがコントローラに送信できるように、コントローラをその IDS センサーに登録します。また、コントローラは定期的にセンサーをポーリングします。

IDS センサーを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [IDS Sensor Lists] の順に選択します。

[IDS Sensor] ページには、このコントローラに設定されているすべての IDS センサーのリストが表示されます。IP アドレスをクリックして、特定の IDS センサーの詳細を表示します。

CA 証明書の設定

CA 証明書は、1 つの認証局（CA）から別の認定 CA に対して発行されるデジタル証明書です。

- 「CA 証明書のインポート」（P.9-399）
- 「CA 証明書の直接貼り付け」（P.9-399）

CA 証明書のインポート

ファイルから CA 証明書をインポートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [IP Sec Certificates] > [CA Certificate] の順に選択します。

ステップ 4　[Browse] をクリックして該当する証明書ファイルにナビゲートします。

ステップ 5　[Open] をクリックします。

ステップ 6　[Save] をクリックします。

CA 証明書の直接貼り付け

CA 証明書を直接貼り付けるには、次の手順を実行します。

ステップ 1　コンピュータのクリップボードに CA 証明書をコピーします。

ステップ 2　[Configure] > [Controllers] の順に選択します。

ステップ 3　適切な IP アドレスをクリックします。

ステップ 4　左側のサイドバーのメニューから、[Security] > [IP Sec Certificates] > [CA Certificate] の順に選択します。

ステップ 5　[Paste] チェックボックスをオンにします。

ステップ 6　証明書をテキスト ボックスに直接貼り付けます。

ステップ 7　[Save] をクリックします。

ID 証明書の設定

このページには、既存のネットワーク ID 証明書が、証明書の名前順にリストされます。ID 証明書は、Web サーバのオペレータが、安全なサーバの動作を確保するために使用します。ここでは、次の内容について説明します。

- 「ID 証明書のインポート」（P.9-400）
- 「ID 証明書の貼り付け」（P.9-400）

ID 証明書のインポート

ファイルから ID 証明書をインポートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [IP Sec Certificates] > [ID Certificate] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Certificate] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　名前とパスワードを入力します。

ステップ 7　[Browse] をクリックして該当する証明書ファイルにナビゲートします。

ステップ 8　[Open] をクリックします。

ステップ 9　[Save] をクリックします。

ID 証明書の貼り付け

ID 証明書を直接貼り付けるには、次の手順を実行します。

ステップ 1　コンピュータのクリップボードに ID 証明書をコピーします。

ステップ 2　[Configure] > [Controllers] の順に選択します。

ステップ 3　適切な IP アドレスをクリックします。

ステップ 4　左側のサイドバーのメニューから、[Security] > [IP Sec Certificates] > [ID Certificate] の順に選択します。

ステップ 5　[Select a command] ドロップダウン リストから [Add Certificate] を選択します。

ステップ 6　[Go] をクリックします。

ステップ 7　名前とパスワードを入力します。

ステップ 8　[Paste] チェックボックスをオンにします。

ステップ 9　証明書をテキスト ボックスに直接貼り付けます。

ステップ 10　[Save] をクリックします。

（注）　ID 証明書は、コントローラが Cisco Unified Wireless Network のソフトウェア バージョン 3.2 以降を実行している場合のみ、使用できます。

（注）　証明書を削除するには、その証明書を選択し、[Select a command] ドロップダウン リストから [Delete Certificates] を選択して [Go] をクリックします。

[Controllers] > [*IPaddr*] > [Security] > [Web Auth Certificate] の設定

このページでは、Web 許可証明書のダウンロード、または内部生成 Web 許可証明書の再生成を実行できます。

[Web Auth Certificate] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Web Auth Certificate] の順に選択します。

注意　各証明書には、可変長 RSA キーが組み込まれています。RSA キーは、比較的安全性の低い 512 ビットから、非常に安全性の高い数千ビットまでさまざまです。認証局（Microsoft CA など）から新しい証明書を取得する場合は、証明書に組み込まれている RSA キーが 768 ビット以上であることを確認してください。

- [Download Web Auth Certificate]：クリックして [Download Web Auth Certificate to Controller] ページにアクセスします。追加情報については、「コントローラへの Web 認証または Web 管理証明書のダウンロード」（P.9-450）を参照してください。

コマンド ボタン

- [Regenerate Cert]：内部生成された Web 認証証明書を再生成します。

ワイヤレス保護ポリシーの設定

ここでは、ワイヤレス保護ポリシーの設定について説明します。内容は次のとおりです。

不正ポリシーの設定

このページでは、不正アクセス ポイントのポリシーを設定できます。

[Rogue Policies] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Rogue Policies] の順に選択します。次のパラメータが表示されます。

- [Rogue Location Discovery Protocol]：RLDP は、企業の有線ネットワークへの不正な接続の有無を判断します。ドロップダウン リストから、次のいずれかのオプションを選択します。
  - [Disable]：すべてのアクセス ポイント上で RLDP を無効にします。768 ビットは、デフォルト値です。
  - [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。
  - [Monitor Mode APs]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。

（注）　必要なアクセス ポイントで不正検出が有効になっていることを確認します。コントローラに接続されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効化されます（OfficeExtend アクセス ポイントを除く）。ただし、Prime Infrastructure ソフトウェア リリース 6.0 以降では、[Access Point Details] ページで [Rogue Detection] チェックボックスをオンまたはオフにすることにより、アクセス ポイントごとに不正検出を有効または無効にできます。詳細については、「アクセス ポイントの設定」（P.9-463）を参照してください。

（注）　家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。

- Rogue APs
  - [Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)]：不正なアクセス ポイントおよびクライアントのエントリがリストから削除されるまでの秒数を入力します。

    有効な範囲は 240 ～ 3600 秒で、デフォルト値は 1200 秒です。

    （注）　不正なアクセス ポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

  - [Rogue Detection Report Interval]：AP からコントローラに不正検出レポートを送信する間隔を秒数で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。この機能は、モニタ モードの AP のみに適用されます。
  - [Rogue Detection Minimum RSSI]：AP で検出するために不正に必要であり、かつコントローラで不正エントリが作成されるために必要な最小 RSSI 値を入力します。有効な範囲は -70 ～ -128 dBm で、デフォルト値は -128 dBm です。この機能は、すべての AP モードに適用できます。

（注）　非常に RSSI 値が低く、不正解析にとって有益な情報とならない不正が多く存在する可能性があります。そのため、このオプションを使用して AP が不正を検出する最小 RSSI 値を指定することで、不正をフィルタできます。

  - [Rogue Detection Transient Interval]：最初に不正がスキャンされた後、AP が継続的に不正をスキャンする必要のある間隔を入力します。一時的な間隔を入力することで、AP が不正をスキャンする間隔を制御できます。AP は、一時的な間隔の値に基づいて、不正をフィルタできます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。この機能は、モニタ モードの AP のみに適用されます。

- Rogue Clients
  - [Validate rogue clients against AAA]：このチェックボックスをオンにし、AAA サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントかどうかを検証します。デフォルト値はオフです。
  - [Detect and report Adhoc networks]：このチェックボックスをオンにして、アドホック不正検出およびレポートを有効にします。デフォルト値はオンです。

コマンド ボタン

- [Save]：クライアント除外ポリシーへの変更を保存して、前のページに戻ります。
- [Audit]：コントローラで使用される値と Prime Infrastructure の値を比較します。

不正 AP ルールの設定

このページでは、現在の不正 AP ルールを表示および編集できます。

[Rogue AP Rules] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Rogue AP Rules] の順に選択します。[Rogue AP Rules] に、不正 AP ルール、ルール タイプ（[Malicious] または [Friendly]）、およびルールの順序が表示されます。

ステップ 4　ルールの詳細を表示または編集するには、[Rogue AP Rule] をクリックします。詳細については、「不正 AP ルール テンプレートの設定」（P.11-680）を参照してください。

クライアント除外ポリシーの設定

このページでは、コントローラに適用されているクライアント除外ポリシーを設定、有効化、または無効化できます。

[Client Exclusion Policies] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Client Exclusion Policies] の順に選択します。次のパラメータが表示されます。

- [Excessive 802.11a Association Failures]：有効にした場合、クライアントは 802.11 アソシエーションの試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.11a Authentication Failures]：有効にした場合、クライアントは 802.11 認証の試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.11x Authentication Failures]：有効にした場合、クライアントは 802.1X 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [Excessive 802.11 Web Authentication Failures]：有効にした場合、クライアントは Web 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [IP Theft Or Reuse]：有効にした場合、IP アドレスがすでに別のデバイスに割り当てられていると、クライアントが除外されます。

ステップ 4　[Save] をクリックし、クライアント除外ポリシーに行われた変更を保存して前のページに戻るか、[Audit] をクリックしてコントローラで使用された値と Prime Infrastructure の値を比較します。

IDS シグニチャの設定

コントローラ上で、IDS シグニチャ、つまり、受信 802.11 パケットにおけるさまざまなタイプの攻撃を特定するのに使用されるビット パターンのマッチング ルールを設定することができます。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が取られます。

シスコでは、標準シグニチャとカスタムなシグニチャのページで示すように、コントローラで 17 個の標準シグニチャをサポートします。

- 「コントローラの標準シグニチャ パラメータの設定」（P.9-404）
- 「カスタム シグニチャの設定」（P.9-408）
- 「AP 認証および MFP の設定」（P.9-409）

コントローラの標準シグニチャ パラメータの設定

[Standard Signature Parameters] ページには、現在コントローラ上にあるシスコ提供のシグニチャの一覧が表示されます。ここでは、次の内容について説明します。

- 「シグニチャ ファイルのダウンロード」（P.9-405）
- 「シグニチャ ファイルのアップロード」（P.9-406）
- 「標準シグニチャおよびカスタム シグニチャのグローバル設定」（P.9-407）

[Standard Signatures] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Standard Signatures] の順に選択します。このページには、次のパラメータが表示されます。

- [Precedence]：コントローラがシグニチャ チェックを実行する順序。

- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータ フレームの種類。
- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。次に例を示します。
  - [None]：アクションが実行されません。
  - [Report]：検出をレポートします。
- [State]：有効または無効。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。

（注）　シグニチャの名前をクリックして各パラメータを表示し、シグニチャを有効または無効にします。

シグニチャ ファイルのダウンロード

シグニチャ ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Standard Signatures] または [Security] > [Wireless Protection Policies] > [Custom Signatures] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Download Signature Files] を選択します。

（注）　この機能には、[System] > [Commands] > [Upload/Download Commands] > [Download IDS Signatures] を選択することでもアクセスできます。

ステップ 5　[Go] をクリックします。

ステップ 6　シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 7　[File is Located On] から [Local Machine] を選択します。ファイル名および、サーバのルート ディレクトリに対して相対的なパスがわかる場合は、[TFTP server] を選択することもできます。

ステップ 8　[Maximum Retries] に、コントローラがシグニチャ ファイルのダウンロードを試みる最大回数を入力します。

ステップ 9　[Timeout] に、シグニチャ ファイルのダウンロードを試行する際、コントローラがタイムアウトになるまでの最大時間を秒単位で入力します。

ステップ 10　ファイルは /localdisk/tftp ディレクトリにアップロードされます。そのディレクトリ内のローカル ファイル名を指定するか、[Browse] をクリックしてナビゲートします。シグニチャ ファイルの「revision」行で、ファイルがシスコ提供の標準のシグニチャ ファイルか、またはサイトに合わせたカスタム シグニチャ ファイルかを指定します（カスタム シグニチャ ファイルには revision=custom が必須）。

（注）　何らかの理由で転送がタイムアウトになった場合、単に [File Is Located On] フィールドで [TFTP server] オプションを選択できます。サーバ ファイル名が自動的に入力され、再試行されます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure 独自の組み込みの TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、ダウンロードした Web ページで自動的にそのファイル名が読み込まれます。

ステップ 11　[OK] をクリックします。

シグニチャ ファイルのアップロード

コントローラからシグニチャ ファイルをアップロードするには、次の手順を実行します。

ステップ 1　シスコからシグニチャ ファイルを入手します（以降、標準シグニチャ ファイル）。「シグニチャ ファイルのダウンロード」（P.9-405）に従い、独自のシグニチャ ファイル（カスタム シグニチャ ファイル）を作成することもできます。

ステップ 2　シグニチャのダウンロードに Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティングできないため、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Prime Infrastructure と同じコンピュータ上で実行できません。

ステップ 3　[Configure] > [Controllers] の順に選択します。

ステップ 4　適切な IP アドレスをクリックします。

ステップ 5　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Standard Signatures] または [Security] > [Wireless Protection Policies] > [Custom Signatures] の順に選択します。

ステップ 6　[Select a Command] ドロップダウン リストから、[Upload Signature Files from controller] を選択します。

（注）　この機能には、[Security] > [Custom Signatures] > [Select a command] > [Upload Signature Files from controller] または [System] > [Commands] > [Upload/Download Commands] > [Upload File from Controller] を選択することでもアクセスできます。

ステップ 7　転送に使用している TFTP サーバ名を指定します。

ステップ 8　TFTP サーバが新しい場合は、[Server IP Address] フィールドで TFTP IP アドレスを入力します。

ステップ 9　[File Type] ドロップダウン リストから [Signature Files] を選択します。

ステップ 10　このシグニチャ ファイルは、TFTP サーバによる使用に対して設定されたルート ディレクトリにアップロードされます。[Upload to File] フィールドで別のディレクトリに変更できます（このフィールドは、[Server Name] がデフォルト サーバの場合のみ表示）。コントローラはベース ネームとしてこのローカル ファイル名を使用し、標準シグニチャ ファイルのサフィクスとして _std.sig を、カスタム シグニチャ ファイルのサフィクスとして _custom.sig を追加します。

ステップ 11　[OK] をクリックします。

標準シグニチャおよびカスタム シグニチャのグローバル設定

このコマンドは、個々に選択して有効にしたシグニチャすべてを有効にします。このチェックボックスをオフのままにすると、以前に有効にしていても、すべてのファイルは無効になります。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。

現在コントローラ上にあるすべての標準シグニチャおよびカスタム シグニチャを有効にするには、次の手順を実行します。

ステップ 1　[Select a command] ドロップダウン リストから [Edit Signature Parameters] を選択します。

ステップ 2　[Go] をクリックします。

ステップ 3　[Enable Check for All Standard and Custom Signatures] チェックボックスをオンにします。

ステップ 4　[Save] をクリックします。

シグニチャを個別に有効または無効にするには、次の手順を実行します。

ステップ 1　有効または無効にする攻撃のタイプの、該当する名前をクリックします。

[Standard Signature parameters] ページには、現在コントローラ上にあるシスコ提供のシグニチャの一覧が表示されます。[Custom Signatures] ページには、現在コントローラ上に存在する、カスタマー提供のシグニチャのリストが表示されます。次のパラメータは、両方のシグニチャ ページおよび詳細シグニチャ ページに表示されます。

- [Precedence]：コントローラがシグニチャ チェックを行う順序、または優先順位。
- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータフレームの種類。
- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。なにも処置をとらない場合は [None]、検出を報告する場合は [Report] となります。
- [Frequency]：シグニチャの頻度。攻撃が検出される前に、アクセス ポイント レベルの検出において識別する必要のある、間隔ごとのシグニチャと一致するパケット数です。有効な範囲は間隔あたり 1 ～ 32,000 パケットです。デフォルト値は間隔あたり 50 パケットです。
- [Quiet Time]：各アクセス ポイント レベルで攻撃が検出されなくなってから、アラームを停止するまでの時間の長さ（秒単位）。この設定は、次項の [MAC Information] の設定が [all] もしくは [both] の場合にだけ表示されます。有効な範囲は 60 ～ 32,000 秒で、デフォルト値は 300 秒です。
- [MAC Information]：アクセス ポイント レベルの検出においてシグニチャをネットワークごとまたは MAC アドレスごと、または両方で追跡するどうか。

- [MAC Frequency]：シグニチャ MAC の頻度。攻撃が検出される前に、コントローラ レベルにおいて識別する必要のある、間隔ごとのシグニチャと一致するパケット数です。有効な範囲は間隔あたり 1 ～ 32,000 パケットです。デフォルト値は間隔あたり 30 パケットです。
- [Interval]：シグニチャの検出頻度がしきい値に達したかどうかをチェックする間隔（秒単位）を入力します。有効な範囲は 1 ～ 3600 秒で、デフォルト値は 1 秒です。
- [Enable]：このシグニチャによりセキュリティ攻撃が検出されるようにする場合はこのチェックボックスをオンにし、このシグニチャを無効にする場合はオフにします。
- [Signature Patterns]：セキュリティ攻撃の検出に使用されるパターン。

ステップ 2　[Enable] ドロップダウン リストから、[Yes] を選択します。カスタマイズされたシグニチャをダウンロードしているため、_custom.sgi という名前の付いたファイルを有効にし、同じ名前で異なる拡張子を持つ標準シグニチャを無効にする必要があります。たとえば、ブロードキャスト プローブ フラッドをカスタマイズしている場合に、ブロードキャスト プローブ フラッドを標準シグニチャでは無効にし、カスタム シグニチャでは有効にする場合です。

ステップ 3　[Save] をクリックします。

カスタム シグニチャの設定

[Custom Signature] ページには、現在コントローラ上に存在する、ユーザ提供のシグニチャのリストが表示されます。

シグニチャの詳細については、次の項を参照してください。

- 「シグニチャ ファイルのダウンロード」（P.9-405）
- 「シグニチャ ファイルのアップロード」（P.9-406）
- 「標準シグニチャおよびカスタム シグニチャのグローバル設定」（P.9-407）

[Custom Signatures] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [Custom Signatures] の順に選択します。このページには、次のパラメータが表示されます。

- [Precedence]：コントローラがシグニチャ チェックを実行する順序。
- [Name]：シグニチャによって検出を試みる攻撃の種類。
- [Frame Type]：シグニチャによってセキュリティ攻撃の調査が行われる管理フレームまたはデータ フレームの種類。
- [Action]：シグニチャによって攻撃が検出されたときに実行する、コントローラへの指示。次に例を示します。
  - [None]：アクションが実行されません。
  - [Report]：検出をレポートします。
- [State]：有効または無効。
- [Description]：シグニチャによって検出を試みる攻撃の種類の詳細説明。

（注）　シグニチャの名前をクリックして各パラメータを表示し、シグニチャを有効または無効にします。

AP 認証および MFP の設定

このページでは、アクセス ポイントの認証ポリシーを設定できます。

[AP Authentication and MFP (Management Frame Protection)] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [Wireless Protection Policies] > [AP Authentication and MFP] の順に選択します。

このページには、次のフィールドが表示されます。

- [RF Network Name]：このテキスト ボックスは編集できません。General パラメータ ページ（[Configure IPaddr] > [General] を参照）で入力した RF ネットワーク名がここに表示されます。
- [Protection Type]：ドロップダウン リストから、次のいずれかの認証ポリシーを選択します。
  - [None]：アクセス ポイント認証ポリシーなし。
  - [AP Authentication]：認証ポリシーを適用します。
  - [MFP]：管理フレーム保護を適用します。詳細については、「管理フレーム保護のモニタリング」（P.5-18）を参照してください。
- [Alarm Trigger Threshold]：（[Protection Type] で [AP Authentication] を選択した場合のみ表示）。アラームを発生させるまでに無視する、未知のアクセス ポイントからのヒット数を設定します。

  有効な範囲は 1 ～ 255 です。デフォルト値は 255 です。

コマンド ボタン

- Save
- Audit

Cisco アクセス ポイントの設定

[Configure] > [Controllers] ページを使用して、特定のコントローラ用の Cisco アクセス ポイントを表示して設定できます。

[Cisco APs] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから [Access Points] > [シスコ APs] の順に選択します。[Cisco APs] ページが開き、次のパラメータが表示されます。

- [AP Name]：アクセス ポイント名をクリックして、アクセス ポイントの詳細を表示または設定します。
- Base Radio MAC
- Admin Status
- AP Mode
- Software Version
- Primary Controller Name

ステップ 4　アクセス ポイント名をクリックして、アクセス ポイントの詳細を表示または設定します。表示される情報は、アクセス ポイントのタイプに応じて異なります。

（注）　詳細については、「アクセス ポイントの設定」（P.9-463）を参照してください。

コマンド ボタン

- [Save]：現在の設定を保存します。
- [Audit]：このアクセス ポイントの現在のステータスを検出します。

スニファ機能

アクセス ポイントでスニファ機能を有効にした場合、そのアクセス ポイントはスニファとして機能し、特定チャネル上のすべてのパケットを取得して、AiroPeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

（注）　スニファ機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合だけ有効になります。AiroPeek の詳細は、次の URL を参照してください。www.wildpackets.com/products/airopeek/overview

スニファ機能の使用に関する前提条件

スニファ機能を使用する前に、次の作業を完了しておく必要があります。

- リモート サイトで、スニファ モードでアクセス ポイントを設定します。スニファ モードでのアクセス ポイントの設定の詳細については、「Web ユーザ インターフェイスを使用したスニッファ モードでの AP の設定」（P.9-411）を参照してください。
- Windows XP マシンで AiroPeek バージョン 2.05 以降をインストールします。

（注）　次の dll ファイルをダウンロードするには、WildPackets のメンテナンス メンバーである必要があります。次の URL を参照してください。

https://wpdn.wildpackets.com/view_submission.php?id=30

- 次の dll ファイルをコピーします。
  - socket.dll ファイルを Plugins フォルダ（C:\ProgramFiles\WildPackets\AiroPeek\Plugins など）へ

- socketres.dll ファイルを PluginRes フォルダ（C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes など）へ

リモート マシンでの AiroPeek の設定

リモート マシンで AiroPeek を設定するには、次の手順を実行します。

ステップ 1　AiroPeek アプリケーションを開始して、[Tools] タブで [Options] をクリックします。

ステップ 2　[Options] ページで [Analysis Module] をクリックします。

ステップ 3　ページ内を右クリックして、[Disable All] オプションを選択します。

ステップ 4　[Cisco remote module] 列を見つけて、有効にします。[OK] をクリックして変更を保存します。

ステップ 5　[New capture] をクリックして、[capture option] ページを表示します。

ステップ 6　アダプタ モジュールのリストからリモート Cisco アダプタを選択します。

ステップ 7　展開して、新しいリモート アダプタ オプションを見つけます。ダブルクリックして新規ページを開き、表示されるテキスト ボックスに名前を入力して、[IP address] 列にコントローラ管理インターフェイス IP を入力します。

ステップ 8　[OK] をクリックします。新しいアダプタがリモート Cisco アダプタに追加されます。

ステップ 9　アクセス ポイントを使用してリモートの airopeek キャプチャ用の新規アダプタを選択します。

ステップ 10　[capture] ページで [start socket capture] をクリックして、リモート キャプチャ プロセスを開始します。

ステップ 11　コントローラの CLI からアクセス ポイントを起動して、**config ap mode sniffer** *ap-name* コマンドを入力してスニファ モードに設定します。

アクセス ポイントがリブートし、スニファ モードでアップ状態になります。

Web ユーザ インターフェイスを使用したスニッファ モードでの AP の設定

Web ユーザ インターフェイスを使用してスニッファ モードで AP を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] を選択して、[AP Name] 列で項目をクリックしてこのページにナビゲートします。

ステップ 2　[General] グループ ボックスで、ドロップダウン リストを使用して AP モードを [Sniffer] に設定し、[Apply] をクリックします。

ステップ 3　[Radio Interfaces] グループ ボックスの [Protocol] 列でプロトコル（802.11a/802.11b/g）をクリックします。これによって、設定ページが開きます。

ステップ 4　[Sniff] パラメータを表示するには、[Sniff] チェックボックスを選択します。スニファ対象チャネルを選択し、サーバ（AiroPeek が実行されているリモート マシン）の IP アドレスを入力します。

ステップ 5　変更を保存するには、[Save] をクリックします。

802.11 パラメータの設定

- 「802.11 コントローラの一般パラメータの設定」（P.9-412）

- 「セキュリティ パラメータの設定」（P.9-379）
- 「アグレッシブ ロード バランシングの設定」（P.9-413）
- 「帯域選択の設定」（P.9-414）
- 「802.11 のメディア パラメータの設定」（P.9-416）
- 「RF プロファイル（802.11）の設定」（P.9-416）

802.11 コントローラの一般パラメータの設定

このページでは、802.11 コントローラでの国選択とタイマー情報を編集できます。このページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11] > [General] の順に選択します。ページが開き、次のパラメータが表示されます。

- Country
  - [Country]：許可される国およびプロトコル。

    （注）　選択できる国の最大数は 20 です。

  - [Selected Countries]：現在選択されている国を表示します。
- Timers
  - [Authentication Response Timeout]：802.11 認証応答タイムアウト（秒単位）を設定します。

複数の国コードの設定

モビリティ グループの一部ではない単一のコントローラを、複数の国をサポートするように設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　国を追加するコントローラをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11] > [General] の順に選択します。

ステップ 4　チェックボックスを選択して、追加する国を選択します。アクセス ポイントは、さまざまな規制要件を持つ多くの国で使用できるように設計されています。国の規制に準拠するように国コードを設定できます。

（注）　運用する国向けに設計されていない場合、アクセス ポイントは正しく動作しない可能性があります。たとえば、部品番号が AIR-AP1030-A-K9（米国の規制区域に含まれている）のアクセス ポイントは、オーストラリアでは使用できません。必ず自国の規制区域に合ったアクセス ポイントを購入するようにしてください。製品ごとにサポートされる国コードの完全なリストについては、次の URL を参照してください。
http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html。

ステップ 5　認証応答がタイムアウトになるまでの時間（秒単位）を入力します。

ステップ 6　[Save] をクリックします。

アグレッシブ ロード バランシングの設定

コントローラ上でアグレッシブ ロード バランシングを有効にすると、無線クライアントの負荷を Lightweight アクセス ポイント間で分散することができます。

（注）　クライアントの負荷は、同じコントローラ上のアクセス ポイント間で分散されます。別のコントローラ上のアクセス ポイントとの間では、ロード バランシングは行われません。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエーション応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。このコードは、アクセス ポイントがそれ以上アソシエーションを受け付けることが可能かどうかを示します。アクセス ポイントへの負荷が高すぎる場合は、クライアントはそのエリア内の別のアクセス ポイントへのアソシエートを試みます。アクセス ポイントの負荷が高いかどうかは、そのクライアントからアクセス可能な、近隣の他のアクセス ポイントと比べて相対的に判断されます。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロード バランシング ウィンドウの和を上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントが AP1 にアソシエートしようとすると、ステータス コード 17 が含まれている 802.11 応答パケットがクライアントに送信されます。アクセス ポイントの負荷が高いことがこのステータス コードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

10 回までクライアント アソシエーションを拒否するようコントローラを設定できます（クライアントが 11 回アソシエーションを試行した場合、11 回目の試行ではアソシエーションが許可されます）。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指定できます。これは、特定のクライアント グループ（遅延に敏感な音声クライアントなど）に対してロード バランシングを無効にする場合に便利です。

アグレッシブ ロード バランシングを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　設定する必要があるコントローラを選択します。

ステップ 3　左側のサイドバー メニューから、[802.11] > [Load Balancing] の順に選択します。[Load Balancing] ページが表示されます。

ステップ 4　クライアントのウィンドウ サイズとして 1 ～ 20 までの値を入力します。このページ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ページ＋最も負荷が低い AP 上のクライアント アソシエーション数＝ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアントのページ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこのしきい値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数がしきい値を下回るアクセス ポイントだけとなります。

ステップ 5　拒否の最大数として 0 ～ 10 までの値を入力します。拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

ステップ 6　[Save] をクリックします。

ステップ 7　特定の WLAN でアグレッシブ ロード バランシングを有効または無効にするには、[WLAN Configuration] ページを参照して、[Advanced] タブをクリックします。[WLAN Configuration] ページの使用について詳しくは、「コントローラ WLAN の設定」（P.9-351）を参照してください。

帯域選択の設定

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。これらの干渉の原因を緩和して、ネットワーク全体のパフォーマンスを向上させるには、コントローラで帯域選択を設定できます。

帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。

帯域選択をコントローラ上でグローバルに有効にすることも、特定の WLAN 上の帯域選択を有効または無効にすることもできます。後者は、特定のクライアントのグループ（遅延に敏感な音声クライアントなど）に対して帯域選択を無効にする場合に便利です。

（注）　帯域選択が有効になっている WLAN では、ローミングの遅延が発生するので、音声や映像のような、遅延に敏感なアプリケーションはサポートされません。

帯域選択の使用に関するガイドライン

帯域選択を使用する際には、次のガイドラインに従ってください。

- 帯域選択を使用できるのは、アクセス ポイントが Cisco Aironet 1140 または 1250 シリーズである場合だけです。
- 帯域選択が動作するのは、コントローラに接続されたアクセス ポイントに対してのみです。コントローラに接続しない FlexConnect アクセス ポイントは、リブート後に帯域選択を実行しません。
- 帯域選択アルゴリズムによるデュアル バンド クライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。
- コントローラ上で帯域選択とアグレッシブ ロード バランシングの両方を有効にすることができます。これらは独立して動作し、相互に影響を与えることはありません。

設定手順

帯域選択を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　設定する必要があるコントローラを選択します。

ステップ 3　左側のサイドバー メニューから、[802.11] > [Band Select] の順に選択します。[Band Select] ページが表示されます。

ステップ 4　プローブ サイクル回数として 1 ～ 10 までの値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。

ステップ 5　スキャン サイクル期間のしきい値として 1 ～ 1000 ミリ秒までの値を入力します。この設定は、クライアントからの新しいプローブ要求が新しいスキャン サイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は 200 ミリ秒です。

ステップ 6　[age out suppression] フィールドに 10 ～ 200 秒までの値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 7　[age out dual band] フィールドに 10 ～ 300 秒までの値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンド クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 60 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 8　[acceptable client RSSI] フィールドに –20 ～ –90 dBm までの値を入力します。このフィールドは、クライアントがプローブに応答するための最大 RSSI を設定します。デフォルト値は -80 dBm です。

ステップ 9　[Save] をクリックします。

ステップ 10　特定の WLAN で帯域選択を有効または無効にするには、[WLAN Configuration] ページを参照して、[Advanced] タブをクリックします [WLAN Configuration] ページの使用について詳しくは、「コントローラ WLAN の設定」（P.9-351）を参照してください。

優先コールの設定

優先コール機能を使用すると、特定の番号に対して行う SIP コールに最高の優先度を指定できます。高い優先度を設定するには、設定済みの音声プールに使用可能な音声帯域幅がない場合でも、そのような優先 SIP コールに帯域幅を割り当てます。この機能は、WCS または WLC で帯域幅割り当てに SIP ベースの CAC を使用するクライアントのみでサポートされます。

（注）　コントローラごとに最大 6 個の番号を設定できます。

優先コール サポートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11] > [Preferred Call] の順に選択します。既存の優先コールがある場合は、次のフィールドが表示されます。

- [Description]：優先コールの説明。
- [Number Id]：コントローラの固有識別子を示し、コントローラに割り当てられている 6 個の優先コール番号の 1 つを示します。
- [Preferred Number]：優先コール番号を示します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add Number] を選択します。

ステップ 5　このコントローラに適用するテンプレートを選択します。

（注）　選択したコントローラに適用するテンプレートを選択する必要があります。優先コール番号用の新しいテンプレートを作成するには、「優先コール テンプレートの設定」（P.11-687）を参照してください。

ステップ 6　[Apply] をクリックします。

（注）　優先コールを削除するには、該当する優先コール番号のチェックボックスを選択して、[Select a command] ドロップダウン リストから [Delete] を選択します。[Go] をクリックし、[OK] をクリックして削除を確認します。

802.11 のメディア パラメータの設定

802.11 のメディア パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11] > [Media Stream] の順に選択します。

ステップ 4　[Media Stream Configuration] セクションで、次のパラメータを設定します

- Media Stream Name
- [Multicast Destination Start IP]：マルチキャストまでのメディア ストリームの開始 IP アドレス
- [Multicast Destination End IP]：マルチキャストまでのメディア ストリームの終了 IP アドレス
- [Maximum Expected Bandwidth]：メディア ストリームが使用できる最大帯域幅

ステップ 5　[Resource Reservation Control (RRC) Parameters] グループ ボックスで、次のパラメータを設定します。

- [Average Packet Size]：メディア ストリームが使用できる平均パケット サイズ。
- [RRC Periodical Update]：定期的に更新されるリソース予約コントロールの計算。無効にすると、RRC の計算は、クライアントがメディア ストリームに加入したときに、1 回のみ行われます。
- [RRC Priority]：最高が 1、最低が 8 の RRC の優先度。
- [Traffic Profile Violation]：ストリームが QoS ビデオ プロファイルに違反したときに、ストリームがドロップされるか、ベスト エフォート キューに入れられる場合に表示されます。
- [Policy]：メディア ストリームが許可されるか拒否される場合に表示されます。

ステップ 6　[Save] をクリックします。

RF プロファイル（802.11）の設定

[RF Profiles] ページでは、AP グループに関連付けられる RF プロファイルを作成または変更できます。

コントローラの RF プロファイルを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　[RF Profiles] をクリックするか、左側のサイドバー メニューから [802.11] > [RF Profiles] を選択します。[RF Profiles] ページが表示されます。このページには、既存の RF プロファイル テンプレートがリストされます。

ステップ 3　RF プロファイルを追加する場合は、[Select a command] ドロップダウン リストから [Add RF Profile] を選択します。

ステップ 4　[Go] をクリックします。[New Controller Template] ページが表示されます。

ステップ 5　次の情報を設定します。

- General
  - [Template Name]：テンプレートのユーザ定義の名前。
  - [Profile Name]：現在のプロファイルのユーザ定義の名前。
  - [Description]：テンプレートの説明。
  - [Radio Type]：アクセス ポイントの無線タイプ。これは、802.11a または 802.11b 無線がある AP の RF プロファイルを選択できるドロップダウン リストです。
- TCP（送信電力制御）
  - [Minimum Power Level Assignment (-10 to 30 dBm)]：割り当てられている最小電力を示します。範囲は -10 ～ 30 dB で、デフォルト値は 30 dB です。
  - [Maximum Power Level Assignment (-10 to 30 dBm)]：割り当てられている最大電力を示します。範囲は -10 ～ 30 dB で、デフォルト値は 30 dB です。
  - [Power Threshold v1(-80 to -50 dBm)]：送信電力しきい値を示します。
  - [Power Threshold v2(-80 to -50 dBm)]：送信電力しきい値を示します。
- データ レート：アクセス ポイントとクライアント間でデータを送信できるレートを指定するには、[Data Rates] ドロップダウン リストを使用します。次のデータ レートが使用可能です。
  - [802.11a]：6、9、12、18、24、36、48、および 54 Mbps。
  - [802.11b/g]：1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps。

  各データ レートに対して、次のオプションのいずれかを選択します。
  - [Mandatory]：このコントローラ上のアクセス ポイントに関連付けるには、クライアントがこのデータ レートをサポートしている必要があります。
  - [Supported]：関連付けられたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信できます。ただし、クライアントがこのレートを使用できなくても、関連付けは可能です。
  - [Disabled]：通信に使用するデータ レートは、クライアントが指定します。

ステップ 6　[Save] をクリックします。

SIP スヌーピングの設定

SIP スヌーピングを使用する際は、次のガイドラインを考慮します。

- SIP は、Cisco 5500 シリーズ コントローラ、1240、1130、および 11n アクセス ポイント上でのみ使用できます。
- SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話に対してのみ使用してください。

- SIP CAC は、SIP スヌーピングが有効になっている場合にのみサポートされます。

コントローラの SIP スヌーピングを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[802.11] > [SIP Snooping] の順に選択します。

ステップ 4　次のフィールドを設定します。

- Port Start
- Port End

ステップ 5　[Save] をクリックします。

（注）　単一ポートを使用する場合は、開始ポートおよび終了ポートのフィールドを同じ番号で設定します。

802.11a/n パラメータの設定

ここでは、次の内容について説明します。

802.11a/n の一般パラメータの設定

特定のコントローラの 802.11a/n パラメータを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n Parameters] を選択して、次のパラメータを表示します。

- General

- [802.11a/n Network Status]：有効にするには、このチェックボックスを選択します。
- [Beacon Period]：ビーコン間の時間。有効範囲は 100 ～ 600 ミリ秒です。
- [DTIM Period]：配送数フィールドが 0 のトラフィック インジケータ メッセージ（TIM）要素を含むビーコン フレームの送信間に経過したビーコン間隔。
- [Fragmentation Threshold (in bytes)]：パケットを断片化するサイズ。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。
- Template Applied

- 802.11a/n Band Status
  - [Low]、[Medium]、および [High Bands]（読み取り専用）。
- 802.11a/n Power Status
  - [Dynamic Assessment]：[Automatic]、[On Demand]、または [Disabled]。
  - [Current Tx Level]：範囲には、1（国コード設定別に許可される最大電力）、2（50 % の電力）、3（25 % の電力）、4（6.25 ～ 12.5 % の電力）、および 5（0.195 ～ 6.25 % の電力）。

（注） 電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。

  - [Control Interval]：秒単位（読み取り専用）。
  - [Dynamic Treatment Power Control]：有効にするには、このチェックボックスを選択します。
- 802.11a/n Channel Status
  - [Assignment Mode]：[Automatic]、[On Demand]、または [Disabled]。
  - [Update Interval]：秒単位。
  - [Avoid Foreign AP Interference]：有効にすると、RRM がチャネルを割り当てる際に、外部 Cisco アクセス ポイント（RF/ モビリティ ドメイン外の Cisco 以外のアクセス ポイント）からの干渉が考慮されます。
  - [Avoid Cisco AP load]：有効にすると、コントローラがアクセス ポイントにチャネルを割り当てる際に、各アクセス ポイントによって使用されるトラフィック帯域幅が考慮されます。
  - [Avoid non 802.11 Noise]：有効にすると、アクセス ポイントは、アクセス ポイント以外のソース（電子レンジや Bluetooth デバイスなど）からの干渉があるチャネルを回避します。RRM にこの干渉を無視させるには、このフィールドを無効にします。
  - [Signal Strength Contribution]：設定不可。
  - Avoid Persistent Non-WiFi interface
- Data Rates
  - [Ranges between 6 Mbps and 54 Mbps]：[Supported]、[Mandatory]、または [Disabled]。
- Noise/Interference/Rogue Monitoring Channels
  - [Channel List]：[All Channels]、[Country Channels]、[DCA Channels]。

（注） 動的チャネル割り当て（DCA）により、コントローラに接続された管理対象デバイス セットの中から妥当なチャネルの割り当てが自動的に選択されます。

- [CCX Location Measurement]：有効にすると、クライアントの位置精度が向上します。
  - [Mode]：有効にするには、このチェックボックスを選択します。
  - [Interval]：秒単位。

（注）　[CCX Location Measurement] の [Interval] は、測定モードが有効の場合のみ変更できます。

コマンド ボタン

- [Save]：行った変更を保存します。
- [Audit]：コントローラで使用される値と Prime Infrastructure の値を比較します。

802.11a/n RRM しきい値の設定

802.11a/n RRM しきい値コントローラを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [RRM Thresholds] の順に選択します。

ステップ 4　[Coverage Level]、[Load Thresholds]、および [Threshold For Traps] に対して変更が必要な場合には、変更します。

（注）　[Coverage Thresholds Min SNR Level (dB)] フィールドを調整すると、[Signal Strength (dB)] の値にこの変更が自動的に反映されます。[Signal Strength (dB)] フィールドにより、SNR 値を調整する際のカバレッジしきい値の対象範囲に関する情報が提供されます。

ステップ 5　[Save] をクリックします。

802.11a/n RRM 間隔の設定

個々のコントローラに対する 802.11b/g/n RRM 間隔を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [RRM Intervals] または [802.11b/g/n] > [RRM Intervals] を選択します。

（注）　次の 4 つの RRM 間隔パラメータのデフォルトは 300 秒です。

ステップ 4　各アクセス ポイントに対して強度測定を行う間隔を入力します。

ステップ 5　各アクセス ポイントに対してノイズおよび干渉測定を行う間隔を入力します。

ステップ 6　各アクセス ポイントに対して負荷測定を行う間隔を入力します。

ステップ 7　各アクセス ポイントに対してカバレッジ測定を行う間隔を入力します。

ステップ 8　[Save] をクリックします。

802.11a/n RRM 送信電力コントロールの設定

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。通常は、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、3 番めに送信電力の強いネイバーによるアクセス ポイントの認識に応じて、アクセス ポイントの送信電力のバランスを取ろうとします。

送信電力コントロール（TPC）アルゴリズムは、RF 環境での変更に応じてアクセス ポイントの電力の増大と低減の両方を行います。ほとんどの場合、TPC は干渉を減らすためにアクセス ポイントの電力を下げようとしますが、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になるなど、RF カバレッジで急な変更が発生した場合、TPC は周辺のアクセス ポイントで電力を増大することもあります。この機能は、カバレッジ ホール検出とは異なります。カバレッジ ホールの検出は主にクライアントと関係がありますが、TPC はアクセス ポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジ レベルを達成するため、十分な RF パワーを提供する必要があります。

送信電力コントロール バージョン 2（TPCv2）は、Cisco AP ネットワークからの同一チャネルの干渉を減らそうとします。前のバージョンの TPC は、より大きい送信電力を使用する傾向のある強い信号カバレッジを提供するよう設計されています。その結果、密に展開されたネットワークで電波が強すぎる状態が発生していました。

802.11a/n の RRM TPC を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n-RRM] > [TPC] の順に選択します。

ステップ 4　次の TPC パラメータを設定します。

- [Template Applied]：このコントローラに適用されるテンプレートの名前。
- [Template Version]：TPC バージョンを示します。

  [TPCv2] オプションは、リリース 7.2.x 以降を実行するコントローラのみで適用できます。
- [Dynamic Assignment]：[Dynamic Assignment] ドロップダウン リストで、次の 3 つのモードのうち 1 つを選択します。
  - [Automatic]：この動作を許可するすべてのアクセス ポイントに対し、送信電力が定期的に更新されます。
  - [On Demand]：[Assign Now] ボタンが選択されると送信電力が更新されます。
  - [Disabled]：動的な送信電力割り当ては発生せず、値はグローバル デフォルトに設定されます。
- [Maximum Power Assignment]：割り当てられている最大電力を示します。
  - 範囲：-10 ～ 30 dB
  - デフォルト：30 dB
- [Minimum Power Assignment]：割り当てられている最小電力を示します。
  - 範囲：-10 ～ 30 dB
  - デフォルト：30 dB
- [Dynamic Tx Power Control]：動的な送信電力コントロールを有効にするかどうかを決定します。

- [Transmitted Power Threshold]：送信電力しきい値を -50 ～ -80 の間で入力します。
- [Control Interval]：秒単位（読み取り専用）。

ステップ 5　[Save] をクリックします。

802.11a/n RRM 動的チャネル割り当ての設定

[Radio Resource Management (RRM) Dynamic Channel Assignment (DCA)] ページを使用して、このコントローラのチャネル幅のほか、DCA チャネルを選択できます。

RRM DCA は、5 GHz 帯域で 802.11n 40 MHz チャネルをサポートします。より高い帯域幅を使用すると、瞬間的データ レートが高くなります。

（注）　大きい帯域幅を選択すると、オーバーラッピングしないチャネルが減少するため、展開によっては全体のネットワーク スループットが低下することがあります。

各コントローラに 802.11 a/n RRM DCA チャネルを設定する手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[802.11a/n] > [RRM DCA] の順に選択します。[802.11a/n RRM DCA] ページが表示されます。

（注）　[Configure] > [Access Points] を選択し、[Radio] 列で [802.11a/n] リンクをクリックし、アクセス ポイントのページでチャネル幅を設定することもできます。[Current RF Channel Assignment] が表示され、[Global] 割り当て方式を選択するか、[Custom] を選択してチャネルを指定できます。

ステップ 4　[Channel Width] ドロップダウン リストから、[20 MHz]、[40 MHz]、または [80 MHz] を選択します。40 MHz の場合、無線の瞬間データ レートが高くなる場合がありますが、チャネル幅が大きいとオーバーラップしないチャネル数が少なくなるため、導入によっては全体のネットワーク スループットが低下することがあります。

（注）　802.11ac では 80 MHz チャネル幅が提供されます。

（注）　20 MHz デバイスと 40 MHz デバイスが混在する展開の場合は注意が必要です。40 MHz デバイスのチャネル アクセス ルールが若干異なるため、20 MHz デバイスに悪影響を与える場合があります。

（注）　アクセス ポイントの無線のチャネル幅を表示するには、[Monitor] > [Access Points] > [*name*] > [Interfaces] タブに移動します。[Configure] > [Access Points] を選択して、[Radio] 列で該当する無線をクリックして、チャネル幅とアンテナの選択肢を表示することもできます。

ステップ 5　該当する DCA チャネルのチェックボックスを選択します。選択したチャネルが、[Selected DCA channels] リストにリストされます。

ステップ 6　次のパラメータを使用して、イベント駆動型無線リソース管理（ED-RRM; Event-Driven Radio Resource Management）を有効または無効にします。CleanAir 対応アクセス ポイントが重大なレベルの干渉を検出すると、イベント駆動型 RRM が使用されます。

- [Event Driven RRM]：スペクトル イベント駆動型 RRM を有効または無効にします。デフォルトでは、[Event Driven RRM] は有効です。
- [Sensitivity Threshold]：[Event Driven RRM] が有効の場合、このフィールドには、イベント駆動型 RRM が生成されるしきい値レベルが表示されます。値は、[Low]、[Medium]、または [High] のいずれかになります。アクセス ポイントの干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセス ポイント無線のチャネルを変更します。[Low] は、環境の変更に対する感度を下げることを表すのに対して、[High] は、感度を上げることを表します。

ステップ 7　[Save] をクリックします。

802.11a/n RRM 無線のグループ化の設定

個々のコントローラに対する 802.11b/g/n RRM 無線のグループ化を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [RRM] > [RF Grouping] の順に選択します。

ステップ 4　ドロップダウン リストからグループ化モードを選択します。次のパラメータが表示されます。

- [Automatic]：自動的な RRM グループ化アルゴリズムをアクティブ化できます。これは、デフォルトのモードです。
- [Off]：自動グループ化を非アクティブ化できます。
- [Leader]：グループにメンバーを割り当てることができます。

ステップ 5　ドロップダウン リストからグループ更新間隔（秒）を選択します。グループ化がオンになっている場合、この間隔（秒単位）は、グループ化アルゴリズムがグループ リーダーによって実行される期間を表します。グループ化アルゴリズムは、グループの内容が変更され、自動グループ化が有効であるときも実行されます。動的グループ化は、システム管理者からの要求時に開始できます。デフォルト値は 600 秒です。

ステップ 6　[RF Group Members] グループ ボックスで、[Add >] をクリックします。選択したコントローラは、[Available Controllers] から [RF Group Members] リストに移動されます。

（注）　[RF Group Members] グループ ボックスは、グループ化モードが [Leader] に設定されている場合のみ表示されます。

（注）　RF グループに追加できるコントローラの最大数は 20 です。

ステップ 7　[Save] をクリックします。

802.11a/n のメディア パラメータの設定

802.11a/n のメディア パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [Media Parameters] の順に選択します。

ステップ 4　[Voice] タブで、次のパラメータを設定します。

- [Admission Control (ACM)] : アドミッション制御を有効にするには、このチェックボックスを選択します。

  VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、コール アドミッション制御（CAC）が必要です。アクセス ポイントでの CAC により、アクセス ポイントは、ネットワークの輻輳時でも QoS が制御された状態を維持し、許容する最大の通話数を許容できる数に保つことができます。
- [CAC Method] : [Admission Control (ACM)] が有効になっている場合、CAC 方式を負荷ベースまたはスタティックに指定します。

  負荷ベースの CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

  負荷ベース CAC では、RF チャネル、チャネル干渉、およびアクセス ポイントが許容できるその他のコールが、アクセス ポイントによって定期的に測定および更新されます。アクセス ポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。このようにすることで、負荷ベースの CAC は、チャネルのオーバーサブスクリプションを防ぎ、WLAN の負荷および干渉のあらゆる状況下で QoS を維持します。
- [Maximum Bandwidth Allowed] : 許容される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 5 ～ 85 です。
- [Reserved Roaming Bandwidth] : 予約済みのローミング帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 です。
- [Expedited Bandwidth] : 緊急コール用に CAC の拡張として緊急帯域幅を有効にするには、このチェックボックスを選択します。

  より高い優先度が TSPEC 要求に与えられるように、CCXv5 準拠の優先帯域幅が必要となります。
- [SIP CAC] : SIP CAC を有効にするには、このチェックボックスを選択します。

  SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話のみに使用する必要があります。
- [SIP Codec] : この無線で使用するコーデック名を指定します。使用可能なオプションは、[G.711]、[G.729]、および [User Defined] です。
- [SIP Call Bandwidth] : ネットワークで SIP コールごとに割り当てる帯域幅（キロビット / 秒単位）を指定します。このフィールドは、選択されている [SIP Codec] が [User Defined] である場合のみ設定できます。
- [SIP Sample Interval] : コーデックを動作させる必要があるサンプルの間隔（ミリ秒）を指定します。

- [Max Voice Calls per Radio]：無線ごとに行うことができるボイスコールの最大数を指定します。
- [Max Roaming Reserved Calls per Radio]：無線ごとに予約できるローミング コールの最大数を指定します。

（注）　[Max Voice Calls per Radio] および [Max Roaming Reserved Calls per Radio] オプションは、[CAC Method] が [Static] として指定され、SIP CAC が有効になっている場合にだけ使用できます。

- [Metric Collection]：メトリック収集を有効にするには、このチェックボックスを選択します。

  トラフィック ストリーム メトリックは、ワイヤレス LAN での VoIP に関する一連の統計情報で、ワイヤレス LAN の QoS を通知します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは、関連付けられたすべてのアクセス ポイントから、90 秒ごとに 802.11b/g インターフェイスに関する統計情報データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にする必要があります。

ステップ 5　[Video] タブで、次のパラメータを設定します。

- [Admission Control (ACM)]：アドミッション制御を有効にするには、このチェックボックスを選択します。
- [Maximum Bandwidth Allowed]：許容される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。コントローラ バージョン 6.0.188.0 以前の場合、有効な範囲は 0 ～ 100 です。コントローラ バージョン 6.0.188.1 以降の場合、有効な範囲は 5 ～ 85 です。
- [Reserved Roaming Bandwidth]：予約済みのローミング帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 で、デフォルトは 0 です。
- [Static CAC method] : [SIP Codec] ドロップダウン リストから、次のいずれかのオプションを選択して CAC 方式を設定します。デフォルト値は [G.711] です。オプションは次のとおりです。
  - Load-Based
  - Static

（注）　スタティック CAC 方式は無線ベースで、負荷ベースの CAC 方式はチャネル ベースです

- [SIP CAC] : スタティック CAC のサポートを有効にするには、[SIP CAC] チェックボックスを選択します。デフォルトでは、このチェックボックスはディセーブルになっています。

（注）　SIP CAC は、SIP スヌーピングが有効になっている場合にのみサポートされます。

- [Unicast Video Redirect] : ビデオ キュー内のすべての非メディア ストリーム パケットがベスト エフォート キューにリダイレクトされるようにするには、[Unicast Video Redirect] チェックボックスを選択します。無効にすると、ビデオ マーキングのあるパケットはすべてのビデオ キューに保持されます。
- [Client Minimum Phy Rate]：クライアントがメディア ストリームに加入するために必要な物理データ レートを [Client Minimum Phy Rate] ドロップダウン リストから選択します。
- [Multicast Direct Enable]：この無線でどの WLAN でも Media Direct を有効にするには、[Multicast Direct Enable] チェックボックスを選択します。
- [Maximum Number of Streams per Radio]：許可される無線ごとのストリームの最大数を指定します。

- [Maximum Number of Streams per Client]：許可されるクライアントごとのストリーム最大数を指定します。
- [Best Effort QOS Admission]：新しいクライアント要求をベスト エフォート キューにリダイレクトするには、[Best Effort QOS Admission] チェックボックスを選択します。これは、すべてのビデオ帯域幅が使用されている場合のみ発生します。

（注）　無効になっており、最大のビデオ帯域幅が使用されている場合、新しいクライアント要求は拒否されます。

ステップ 6　[General] タブで、次のフィールドを設定します。

- [Maximum Media Bandwidth (0 to 85%)]：許可される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。

ステップ 7　[Save] をクリックします。

（注）　SIP は、コントローラ 4400 および 5500 のみで使用可能です。また、SIP は、アクセス ポイント 1240、1130、および 11n のみで使用可能です。

コマンド ボタン

- [Save]：行った変更を保存します。
- [Audit]：コントローラで使用される値と Prime Infrastructure の値を比較します。

802.11a/n の EDCA パラメータの設定

802.11b/g/n に対する EDCA パラメータ（EDCA プロファイル設定と Streaming MAC Enable 設定）は、個々のコントローラまたはコントローラ テンプレートのいずれかを使用して、音声 QoS サポートを向上させるように設定できます。

個々のコントローラの [802.11b/g/n EDCA] パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11b/g/n] > [EDCA Parameters] を選択します。

ステップ 4　ドロップダウン リストから [EDCA Profile] を選択します。

（注）　プロファイルには、Wi-Fi Multimedia (WMM)、Spectralink Voice Priority (SVP)、Voice Optimized、および Voice & Video Optimized が含まれます。WMM がデフォルトの EDCA プロファイルです。

（注）　無線インターフェイスをシャットダウンしてから、EDCA パラメータを設定してください。

ステップ 5　[Enable Streaming MAC] チェックボックスを選択にして、この機能を有効にします。

（注）　ネットワーク上のすべてのクライアントが WMM 準拠の場合にだけ、Streaming MAC を有効にしてください。

802.11a/n のローミング パラメータの設定

個々のコントローラの [802.11b/g/n EDCA] パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [Roaming Parameters] の順に選択します。

ステップ 4　[Mode] ドロップダウン リストから、[Default values] または [Custom values] を選択します。

- [Default values] : テキスト ボックスにデフォルト値（読み取り専用）が自動的に表示されます。
- [Custom values] : ローミング パラメータの編集を可能にするには、テキスト ボックスをアクティブ化します。

ステップ 5　[Minimum RSSI] テキスト ボックスには、クライアントがアクセス ポイントにアソシエートするときに必要な受信信号強度（RSSI）の最小値を入力します。

- 範囲：-80 ～ -90 dBm
- デフォルト：-85 dBm

（注）　クライアントの平均の受信信号の強度がこのしきい値よりも低い場合、通常信頼できる通信は不可能です。RSSI の最小値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。

ステップ 6　[Hysteresis] テキスト ボックスに、クライアントがローミングするために必要な隣接するアクセス ポイントの信号強度を示す値を入力します。

このフィールドは、クライアントが物理的に 2 つのアクセス ポイント間の境界上やその近くにある場合に、アクセス ポイント間の「ピンポン」の量を減らすためのものです。

- 範囲：2 ～ 4 dB
- デフォルト：3 dB

ステップ 7　[Adaptive Scan Threshold] テキスト ボックスに、クライアントがアソシエートしたアクセス ポイントの RSSI 値を入力します。これよりも小さい場合、クライアントは指定された移行時間内に隣接するアクセス ポイントにローミングできる必要があります。

このフィールドは、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法を提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。

- 範囲：-70 ～ -77 dB
- デフォルト：-72 dB

ステップ 8　[Transition Time] テキスト ボックスには、クライアントがアソシエートしているアクセス ポイントからの RSSI がスキャンしきい値を下回った場合には常に、ローミングに適した近隣のアクセス ポイントを検出してローミングを完了するまでの最大許容時間を入力します。

[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

- 範囲：1 ～ 10 秒
- デフォルト：5 秒

ステップ 9　[Save] をクリックします。

802.11a/n 802.11h パラメータの設定

個々のコントローラの 802.11h パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [802.11h] を選択します。

ステップ 4　[Power Constraint] チェックボックスを選択して TPC を有効にします。

ステップ 5　[Channel Announcement] チェックボックスを選択してチャネル通知を有効にします。チャネル通知は、新しいチャネルや新しいチャネル番号に切り替わった場合に、アクセス ポイントが通知するメソッドです。

ステップ 6　[Save] をクリックします。

802.11a/n のハイ スループット（802.11n）パラメータの設定

802.11b/g/n のハイ スループット パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11b/g/n] > [High Throughput] を選択します。

ステップ 4　高いスループットを可能にするには、[802.11n Network Status Enabled] チェックボックスを選択します。

ステップ 5　802.11ac 無線で高いスループットを可能にするには、[802.11ac Network Status Enabled] チェックボックスを選択します。

ステップ 6　[MCS (Data Rate) Settings] で、サポートするデータ レートのレベルを選択します。MCS は、802.11a データ レートと似た変調符号化方式です。デフォルトでは、20MHz のショート ガード インターバルが使用されます。

（注）　[Supported] チェックボックスを選択すると、選択した数値が [Selected MCS Indexes] ページに表示されます。

ステップ 7　[Save] をクリックします。

802.11a/n の CleanAir パラメータの設定

802.11a/n の CleanAir パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [CleanAir] を選択して、次の情報を表示します。

- [CleanAir]：このチェックボックスを選択して 802.11 a/n ネットワークで CleanAir 機能を有効にするか、選択解除して CleanAir 機能を無効にします。デフォルト値はオンです。
- [Reporting Configuration]：レポートで含める干渉デバイスを設定するには、このセクションのパラメータを使用します。
  - [Report]：[report interferers] チェックボックスを選択して、CleanAir システムが干渉源を報告して検出できるようにするか、選択解除して、コントローラが干渉を報告しないようにします。デフォルト値はオンです。
  - CleanAir システムで検出および報告する必要がある干渉源が、[Interferences to Detect] テキスト ボックスに表示され、検出する必要がない干渉源が [Interferers to Ignore] テキスト ボックスに表示されることを確認します。[>] および [<] ボタンを使用して、これらの 2 つのテキスト ボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が検出されます。
  - CleanAir で検出できる持続性デバイスに関する情報を伝播できるようにするには、[Persistent Device Propagation] チェックボックスを選択します。持続性デバイスの伝播によって、干渉タイプに関する情報を指定して、この情報を近隣のアクセス ポイントに伝播できます。ある場所には持続的な干渉源が存在し、常に検出可能ではない場合でも WLAN の動作に干渉します。
- [Alarm Configuration]：このセクションでは、電波品質アラームの生成を設定できます。
  - [Air Quality Alarm]：[Air Quality Alarm] チェックボックスを選択して電波品質アラームの生成を有効にするか、このチェックボックスを選択解除してこの機能を無効にします。デフォルト値はオンです。
  - [Air Quality Alarm Threshold]：[Air Quality Alarm] チェックボックスを選択した場合は、[Air Quality Alarm Threshold] テキスト ボックスに 1 ～ 100 までの値を入力して、電波品質アラームが生成されるしきい値を指定します。電波品質がしきい値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は 35 です。
  - [Air Quality Unclassified category Alarm]：未分類の干渉源カテゴリについてアラームを生成できるようにするには、[Air Quality Unclassified category Alarm] チェックボックスを選択します。CleanAir は、未分類の干渉源を検出してモニタできます。未分類の干渉源は、検出はされるものの、既知のいずれの干渉タイプにも対応しない干渉源です。

    未分類カテゴリのアラームは、未分類の重大度が設定済みのしきい値を上回るか、Air Quality インデックスが設定済みのしきい値を下回ると生成されます。
  - [Air Quality Unclassified Category Severity Threshold]：[Air Quality Unclassified category Alarm] チェックボックスを選択した場合、[Air Quality Unclassified Severity Threshold] テキスト ボックスに 1 ～ 99 までの間の値を入力して、未分類カテゴリのアラームを生成するしきい値を指定します。デフォルト値は 20 です。

  - [Interferers For Security Alarm] : [Interferers For Security Alarm] チェックボックスを選択して、コントローラが指定されたデバイス タイプを検出したときに干渉アラームを生成するか、選択解除してこの機能を無効にします。デフォルト値はオンです。
  - 干渉アラームを生成する必要があるすべての干渉源が [Interferers Selected for Security Alarms] テキスト ボックスに表示され、干渉アラームを生成する必要がないすべての干渉源が [Interferers Ignored for Security Alarms] テキスト ボックスに表示されることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が干渉アラームを生成します。
- [Event Driven RRM] : CleanAir 対応アクセス ポイントが重大なレベルの干渉を検出したときに実行するスペクトル イベント駆動型無線リソース管理（RRM）を生成するには、次の手順を実行します。
  - [Event Driven RRM] : スペクトル イベント駆動型 RRM の現在のステータスを表示します。
  - [Sensitivity Threshold] : [Event Driven RRM] が有効の場合、このテキスト ボックスには、イベント駆動型 RRM が生成されるしきい値レベルが表示されます。値は、[Low]、[Medium]、または [High] のいずれかになります。アクセス ポイントの干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセス ポイント無線のチャネルを変更します。[Low] は、環境の変更に対する感度を下げることを表すのに対して、[High] は、感度を上げることを表します。

コマンド ボタン

- [Save] : 行った変更を保存します。
- [Audit] : コントローラで使用される値と Prime Infrastructure の値を比較します。

802.11b/g/n パラメータの設定

ここでは、次の内容について説明します。

802.11b/g/n の一般パラメータの設定

特定のコントローラの 802.11b/g/n パラメータを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから [802.11b/g/n Parameters] を選択して、次のパラメータを表示します。

- General
  - [802.11b/g Network Status]：有効にするには、このチェックボックスを選択します。
  - [802.11g Support]：有効にするには、このチェックボックスを選択します。
  - [Beacon Period]：ミリ秒単位。
  - [DTIM Period]：配送数フィールドが 0 のトラフィック インジケータ メッセージ（TIM）要素を含むビーコン フレームの送信間に経過したビーコン間隔。
  - [Fragmentation Threshold]：バイト単位。
  - [Short Preamble]：有効にするチェックボックスを選択します。
  - [Template Applied]。
- 802.11a/n Power Status
  - [Dynamic Assessment]：[Automatic]、[On Demand]、または [Disabled]。
  - [Current Tx Level]。
  - [Control Interval]：秒単位（読み取り専用）。
  - [Dynamic Treatment Power Control]：有効にするには、このチェックボックスを選択します。
- 802.11a/n Channel Status
  - [Assignment Mode]：[Automatic]、[On Demand]、または [Disabled]。
  - [Update Interval]：秒単位。
  - [Avoid Foreign AP Interference]：有効にするには、このチェックボックスを選択します。
  - [Avoid Cisco AP load]：有効にするには、このチェックボックスを選択します。
  - [Avoid non 802.11 Noise]：有効にするには、このチェックボックスを選択します。
  - [Signal Strength Contribution]：有効にするには、このチェックボックスを選択します。
- Data Rates
  - [Ranges between 1 Mbps and 54 Mbps]：[Supported]、[Mandatory]、または [Disabled]。
- Noise/Interference/Rogue Monitoring Channels
  - [Channel List]：[All Channels]、[Country Channels]、[DCA Channels]。
- CCX Location Measurement
  - [Mode]：有効にするには、このチェックボックスを選択します。
  - [Interval]：秒単位。

（注）　[CCX Location Measurement] の [Interval] は、測定モードが有効の場合のみ変更できます。

コマンド ボタン

- [Save]：行った変更を保存します。

- [Audit]：コントローラで使用される値と Prime Infrastructure の値を比較します。

802.11b/g/n RRM しきい値の設定

802.11b/g/n RRM しきい値コントローラを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[802.11b/g/n] > [RRM Thresholds] の順に選択します。

ステップ 4　[Coverage Level]、[Load Thresholds]、および [Threshold For Traps] に対して変更が必要な場合には、変更します。

（注）　[Coverage Thresholds Min SNR Level (dB)] フィールドを調整すると、[Signal Strength (dB)] の値にこの変更が自動的に反映されます。[Signal Strength (dB)] フィールドにより、SNR 値を調整する際のカバレッジしきい値の対象範囲に関する情報が提供されます。

ステップ 5　[Save] をクリックします。

802.11b/g/n RRM 間隔の設定

個々のコントローラに対する 802.11b/g/n RRM 間隔を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11a/n] > [RRM Intervals] または [802.11b/g/n] > [RRM Intervals] を選択します。

（注）　次の 4 つの RRM 間隔パラメータのデフォルトは 300 秒です。

ステップ 4　各アクセス ポイントに対して強度測定を行う間隔を入力します。

ステップ 5　各アクセス ポイントに対してノイズおよび干渉測定を行う間隔を入力します。

ステップ 6　各アクセス ポイントに対して負荷測定を行う間隔を入力します。

ステップ 7　各アクセス ポイントに対してカバレッジ測定を行う間隔を入力します。

ステップ 8　[Save] をクリックします。

802.11b/g/n RRM 送信電力コントロールの設定

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。通常は、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、3 番めに送信電力の強いネイバーによるアクセス ポイントの認識に応じて、アクセス ポイントの送信電力のバランスを取ろうとします。

送信電力コントロール（TPC）アルゴリズムは、RF 環境での変更に応じてアクセス ポイントの電力の増大と低減の両方を行います。ほとんどの場合、TPC は干渉を減らすためにアクセス ポイントの電力を下げようとしますが、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になるなど、RF カバレッジで急な変更が発生した場合、TPC は周辺のアクセス ポイントで電力を増大することもあります。この機能は、カバレッジ ホール検出とは異なります。カバレッジ ホールの検出は主にクライアントと関係がありますが、TPC はアクセス ポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジ レベルを達成するため、十分な RF パワーを提供する必要があります。

802.11b/g/n RRM TPC を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[802.11b/g/n-RRM] > [TPC] の順に選択します。

ステップ 4　次の TPC パラメータを設定します。

- [Template Applied]：このコントローラに適用されるテンプレートの名前。
- [Dynamic Assignment] : [Dynamic Assignment] ドロップダウン リストで、次の 3 つのモードのうち 1 つを選択します。
  - [Automatic]：送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。
  - [On Demand]：送信電力は、[Assign Now] ボタンを選択したときに更新されます。
  - [Disabled]：動的な送信電力割り当ては行われず、値はグローバル デフォルトに設定されます。
- [Maximum Power Assignment]：割り当てられている最大電力を示します。
  - 範囲：-10 ～ 30 dB
  - デフォルト：30 dB
- [Minimum Power Assignment]：割り当てられている最小電力を示します。
  - 範囲：-10 ～ 30 dB
  - デフォルト：30 dB
- [Dynamic Tx Power Control]：動的な送信電力コントロールを有効にするかどうかを決定します。
- [Transmitted Power Threshold]：送信電力しきい値を -50 ～ -80 の間で入力します。
- [Control Interval]：秒単位（読み取り専用）。

ステップ 5　[Save] をクリックします。

802.11b/g/n RRM 動的チャネル割り当ての設定

個々のコントローラに対する 802.11b/g/n RRM DCA チャネルを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11b/g/n-RRM] > [DCA] の順に選択します。

ステップ 4　該当する DCA チャネルのチェックボックスを選択します。選択したチャネルが、[Selected DCA channels] テキスト ボックスに表示されます。

ステップ 5　イベント駆動型無線リソース管理（RRM）を有効または無効にします。CleanAir 対応アクセス ポイントが重大なレベルの干渉を検出すると、イベント駆動型 RRM が使用されます。次の手順を実行します。

- [Event Driven RRM]：スペクトル イベント駆動型 RRM を有効または無効にします。デフォルトでは、[Event Driven RRM] は有効です。
- [Sensitivity Threshold]：[Event Driven RRM] が有効の場合、このテキスト ボックスには、イベント駆動型 RRM が生成されるしきい値レベルが表示されます。値は、[Low]、[Medium]、または [High] のいずれかになります。アクセス ポイントの干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセス ポイント無線のチャネルを変更します。[Low] は、環境の変更に対する感度を下げることを表すのに対して、[High] は、感度を上げることを表します

ステップ 6　[Save] をクリックします。

802.11b/g/n RRM 無線のグループ化の設定

個々のコントローラに対する 802.11b/g/n RRM 無線のグループ化を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[802.11b/g/n] > [RRM] > [RF Grouping] の順に選択します。

ステップ 4　ドロップダウン リストからグループ化モードを選択します。次のパラメータが表示されます。

- [Automatic]：自動的な RRM グループ化アルゴリズムをアクティブ化できます。これは、デフォルトのモードです。
- [Off]：自動グループ化を非アクティブ化できます。
- [Leader]：グループにメンバーを割り当てることができます。

ステップ 5　ドロップダウン リストからグループ更新間隔（秒）を選択します。グループ化がオンになっている場合、この間隔（秒単位）は、グループ化アルゴリズムがグループ リーダーによって実行される期間を表します。グループ化アルゴリズムは、グループの内容が変更され、自動グループ化が有効であるときも実行されます。動的グループ化は、システム管理者からの要求時に開始できます。デフォルト値は 600 秒です。

ステップ 6　[RF Group Members] グループ ボックスで、[Add >] をクリックします。選択したコントローラは、[Available Controllers] から [RF Group Members] リストに移動されます。

（注）　[RF Group Members] グループ ボックスは、グループ化モードが [Leader] に設定されている場合のみ表示されます。

（注）　RF グループに追加できるコントローラの最大数は 20 です。

ステップ 7　[Save] をクリックします。

802.11b/g/n のメディア パラメータの設定

802.11b/g/n のメディア パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11b/g/n] > [Media Parameters] の順に選択します。

ステップ 4　[Voice] タブで、次のパラメータを設定します。

- [Admission Control (ACM)] : アドミッション制御を有効にするには、このチェックボックスを選択します。

  VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、コール アドミッション制御（CAC）が必要です。アクセス ポイントでの CAC により、アクセス ポイントは、ネットワークの輻輳時でも QoS が制御された状態を維持し、許容する最大の通話数を許容できる数に保つことができます。
- [CAC Method] : [Admission Control (ACM)] が有効になっている場合、CAC 方式を負荷ベースまたはスタティックに指定します。

  負荷ベースの CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

  負荷ベース CAC では、RF チャネル、チャネル干渉、およびアクセス ポイントが許容できるその他のコールが、アクセス ポイントによって定期的に測定および更新されます。アクセス ポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。このようにすることで、負荷ベースの CAC は、チャネルのオーバーサブスクリプションを防ぎ、WLAN の負荷および干渉のあらゆる状況下で QoS を維持します。
- [Maximum Bandwidth Allowed] : 許容される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 5 ～ 85 です。
- [Reserved Roaming Bandwidth] : 予約済みのローミング帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 です。
- [Expedited Bandwidth] : 緊急コール用に CAC の拡張として緊急帯域幅を有効にするには、このチェックボックスを選択します。

  より高い優先度が TSPEC 要求に与えられるように、CCXv5 準拠の優先帯域幅が必要となります。
- [SIP CAC] : SIP CAC を有効にするには、このチェックボックスを選択します。

  SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話のみに使用する必要があります。
- [SIP Codec] : この無線で使用するコーデック名を指定します。使用可能なオプションは、[G.711]、[G.729]、および [User Defined] です。
- [SIP Call Bandwidth] : ネットワークで SIP コールごとに割り当てる帯域幅（キロビット / 秒単位）を指定します。このフィールドは、選択されている [SIP Codec] が [User Defined] である場合のみ設定できます。
- [SIP Sample Interval] : コーデックを動作させる必要があるサンプルの間隔（ミリ秒）を指定します。

- [Max Voice Calls per Radio]：無線ごとに行うことができるボイスコールの最大数を示します。

（注）　[Max Voice Calls per Radio] の値は設定できません。これは、選択された CAC 方式、許容される最大帯域幅、ローミング帯域幅に基づいて自動的に計算されます。

- [Max Roaming Reserved Calls per Radio]：無線ごとに予約できるローミング コールの最大数を示します。

（注）　[Max Voice Calls per Radio] および [Max Roaming Reserved Calls per Radio] オプションは、[CAC Method] が [Static] として指定され、SIP CAC が有効になっている場合にだけ使用できます。

- [Metric Collection]：メトリック収集を有効にするには、このチェックボックスを選択します。

  トラフィック ストリーム メトリックは、ワイヤレス LAN での VoIP に関する一連の統計情報で、ワイヤレス LAN の QoS を通知します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは、関連付けられたすべてのアクセス ポイントから、90 秒ごとに 802.11b/g インターフェイスに関する統計情報データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にする必要があります。

ステップ 5　[Video] タブで、次のパラメータを設定します。

- [Admission Control (ACM)]：アドミッション制御を有効にするには、このチェックボックスを選択します。
- [Maximum Bandwidth]：許可される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。コントローラ バージョン 6.0.188.0 以前の場合、有効な範囲は 0 ～ 100 です。コントローラ バージョン 6.0.188.1 以降の場合、有効な範囲は 5 ～ 85 です。
- [Reserved Roaming Bandwidth]：予約済みのローミング帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 です。
- [Unicast Video Redirect]：ビデオ キュー内のすべての非メディア ストリーム パケットがベスト エフォート キューにリダイレクトされるようにするには、[Unicast Video Redirect] チェックボックスを選択します。無効にすると、ビデオ マーキングのあるパケットはすべてのビデオ キューに保持されます。
- [Client Minimum Phy Rate]：クライアントがメディア ストリームに加入するために必要な物理データ レートを [Client Minimum Phy Rate] ドロップダウン リストから指定します。
- [Multicast Direct Enable]：この無線でどの WLAN でも Media Direct を有効にするには、[Multicast Direct Enable] チェックボックスを選択します。
- [Maximum Number of Streams per Radio]：許可される無線ごとのストリームの最大数を指定します。
- [Maximum Number of Streams per Client]：許可されるクライアントごとのストリーム最大数を指定します。
- [Best Effort QOS Admission]：新しいクライアント要求をベスト エフォート キューにリダイレクトするには、[Best Effort QOS Admission] チェックボックスを選択します。これは、すべてのビデオ帯域幅が使用されている場合のみ発生します。

（注）　無効になっており、最大のビデオ帯域幅が使用されている場合、新しいクライアント要求は拒否されます。

ステップ 6　[General] タブで、次のフィールドを設定します。

- [Maximum Media Bandwidth (0 to 85%)] : 許可される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。

ステップ 7　[Save] をクリックします。

（注）　SIP は、コントローラ 4400 および 5500 のみで使用可能です。また、SIP は、アクセス ポイント 1240、1130、および 11n のみで使用可能です。

コマンド ボタン

- [Save] : 行った変更を保存します。
- [Audit] : コントローラで使用される値と Prime Infrastructure の値を比較します。

802.11b/g/n の EDCA パラメータの設定

802.11b/g/n に対する EDCA パラメータ（EDCA プロファイル設定と Streaming MAC Enable 設定）は、個々のコントローラまたはコントローラ テンプレートのいずれかを使用して、音声 QoS サポートを向上させるように設定できます。

個々のコントローラの [802.11b/g/n EDCA] パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11b/g/n] > [EDCA Parameters] を選択します。

ステップ 4　ドロップダウン リストから [EDCA Profile] を選択します。

（注）　プロファイルには、Wi-Fi Multimedia (WMM)、Spectralink Voice Priority (SVP)、Voice Optimized、および Voice & Video Optimized が含まれます。WMM がデフォルトの EDCA プロファイルです。

（注）　無線インターフェイスをシャットダウンしてから、EDCA パラメータを設定してください。

ステップ 5　[Enable Streaming MAC] チェックボックスを選択にして、この機能を有効にします。

（注）　ネットワーク上のすべてのクライアントが WMM 準拠の場合にだけ、Streaming MAC を有効にしてください。

802.11b/g/n のローミング パラメータの設定

個々のコントローラの [802.11b/g/n EDCA] パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューで、[802.11b/g/n] > [Roaming Parameters] を選択します。

ステップ 4　[Mode] ドロップダウン リストから、[Default values] または [Custom values] を選択します。

- [Default values] : テキスト ボックスにデフォルト値（読み取り専用）が自動的に表示されます。
- [Custom values] : ローミング パラメータの編集を可能にするには、テキスト ボックスをアクティブ化します。

ステップ 5　[Minimum RSSI] テキスト ボックスには、クライアントがアクセス ポイントにアソシエートするときに必要な受信信号強度（RSSI）の最小値を入力します。

- 範囲：-80 ～ -90 dBm
- デフォルト：-85 dBm

（注）　クライアントの平均の受信信号の強度がこのしきい値よりも低い場合、通常信頼できる通信は不可能です。RSSI の最小値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。

ステップ 6　[Hysteresis] テキスト ボックスに、クライアントが近隣のアクセス ポイントにローミングするために必要なアクセス ポイントの信号強度を示す値を入力します。

このフィールドは、クライアントが物理的に 2 つのアクセス ポイント間の境界上やその近くにある場合に、アクセス ポイント間の「ピンポン」の量を減らすためのものです。

- 範囲：2 ～ 4 dB
- デフォルト：3 dB

ステップ 7　[Adaptive Scan Threshold] テキスト ボックスに、クライアントがアソシエートしたアクセス ポイントの RSSI 値を入力します。これよりも小さい場合、クライアントは指定された移行時間内に隣接するアクセス ポイントにローミングできる必要があります。

このフィールドは、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法を提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。

- 範囲：-70 ～ -77 dB
- デフォルト：-72 dB

ステップ 8　[Transition Time] テキスト ボックスには、クライアントがアソシエートしているアクセス ポイントからの RSSI がスキャンしきい値を下回った場合には常に、ローミングに適した近隣のアクセス ポイントを検出してローミングを完了するまでの最大許容時間を入力します。

[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

- 範囲：1 ～ 10 秒
- デフォルト：5 秒

ステップ 9　[Save] をクリックします。

802.11b/g/n のハイ スループット（802.11n）パラメータの設定

802.11b/g/n のハイ スループット パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11b/g/n] > [High Throughput] を選択します。

ステップ 4　高いスループットを可能にするには、[802.11n Network Status Enabled] チェックボックスを選択します。

ステップ 5　[MCS (Data Rate) Settings] で、サポートするデータ レートのレベルを選択します。MCS は、802.11a データ レートと似た変調符号化方式です。デフォルトでは、20MHz のショート ガード インターバルが使用されます。

（注）　[Supported] チェックボックスを選択すると、選択した数値が [Selected MCS Indexes] ページに表示されます。

ステップ 6　[Save] をクリックします。

802.11b/g/n の CleanAir パラメータの設定

802.11b/g/n の CleanAir パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[802.11b/g/n] > [CleanAir] を選択して、次の情報を表示します。

- [CleanAir] : このチェックボックスを選択して 802.11b/g/n ネットワークで CleanAir 機能を有効にするか、選択解除してコントローラがスペクトラム干渉を検出しないようにします。デフォルト値はオンです。
- [Reporting Configuration] : レポートで含める干渉デバイスを設定するには、このセクションのパラメータを使用します。
  - [Report] : [report interferers] チェックボックスを選択して、CleanAir システムが干渉源を報告して検出できるようにするか、選択解除して、コントローラが干渉を報告しないようにします。デフォルト値はオンです。
  - CleanAir システムで検出および報告する必要がある干渉源が、[Interferences to Detect] テキスト ボックスに表示され、検出する必要がない干渉源が [Interferers to Ignore] テキスト ボックスに表示されることを確認します。[>] および [<] ボタンを使用して、これらの 2 つのテキスト ボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が検出されます。
  - CleanAir で検出できる持続性デバイスに関する情報を伝播できるようにするには、[Persistent Device Propagation] チェックボックスを選択します。持続性デバイスの伝播によって、干渉タイプに関する情報を指定して、この情報を近隣のアクセス ポイントに伝播できます。永続型の干渉源は、検出されない場合でも、常にいずれかに存在し、WLAN の動作に干渉しています。
- [Alarm Configuration] : このグループ ボックスでは、電波品質アラームの生成を設定できます。

- [Air Quality Alarm] : [Air Quality Alarm] チェックボックスを選択して電波品質アラームの生成を有効にするか、このチェックボックスを選択解除してこの機能を無効にします。デフォルト値はオンです。
- [Air Quality Alarm Threshold] : [Air Quality Alarm] チェックボックスを選択した場合は、[Air Quality Alarm Threshold] テキスト ボックスに 1 ～ 100 までの値を入力して、電波品質アラームが生成されるしきい値を指定します。電波品質がしきい値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は 35 です。
- [Air Quality Unclassified category Alarm] : 未分類の干渉源カテゴリについてアラームを生成できるようにするには、[Air Quality Unclassified category Alarm] チェックボックスを選択します。Cisco CleanAir は、未分類の干渉源を検出してモニタできます。未分類の干渉源は、検出はされるものの、既知のいずれの干渉タイプにも対応しない干渉源です。

  未分類カテゴリのアラームは、未分類の重大度が設定済みのしきい値を上回るか、Air Quality インデックスが設定済みのしきい値を下回ると生成されます。
- [Air Quality Unclassified Category Severity Threshold] : [Air Quality Unclassified category Alarm] チェックボックスを選択した場合、[Air Quality Unclassified Severity Threshold] テキスト ボックスに 1 ～ 99 までの間の値を入力して、未分類カテゴリのアラームを生成するしきい値を指定します。デフォルト値は 20 です。
- [Interferers For Security Alarm] : [Interferers For Security Alarm] チェックボックスを選択して、コントローラが指定されたデバイス タイプを検出したときに干渉アラームを生成するか、選択解除してこの機能を無効にします。デフォルト値はオンです。
- 干渉アラームを生成する必要があるすべての干渉源が [Interferers Selected for Security Alarms] テキスト ボックスに表示され、干渉アラームを生成する必要がないすべての干渉源が [Interferers Ignored for Security Alarms] テキスト ボックスに表示されることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのテキスト ボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が干渉アラームを生成します。

- [Event Driven RRM] : CleanAir 対応アクセス ポイントが重大なレベルの干渉を検出したときに実行するスペクトル イベント駆動型無線リソース管理（RRM）を起動するには、次のパラメータを使用します。
  - [Event Driven RRM] : スペクトル イベント駆動型 RRM の現在のステータスを表示します。
  - [Sensitivity Threshold] : [Event Driven RRM] が有効の場合、このテキスト ボックスには、イベント駆動型 RRM が生成されるしきい値レベルが表示されます。値は、[Low]、[Medium]、または [High] のいずれかになります。アクセス ポイントの干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセス ポイント無線のチャネルを変更します。[Low] は、環境の変更に対する感度を下げることを表すのに対して、[High] は、感度を上げることを表します。

コマンド ボタン

- [Save] : 行った変更を保存します。
- [Audit] : コントローラで使用される値と Prime Infrastructure の値を比較します。

メッシュ パラメータの設定

個々のコントローラのメッシュ パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Mesh] > [Mesh Settings] を選択します。

ステップ 4　次のメッシュ パラメータを表示または編集します。

- [RootAP to MeshAP Range (150 - 13200 ft)] : デフォルトでは、この値は 12,000 フィートです。150 ～ 132,000 フィートの値を入力できます。ルート アクセス ポイントとメッシュ アクセス ポイント間の適切な距離をフィート単位で入力します。このグローバル フィールドは、コントローラにアクセス ポイントが接続されるとすべてのアクセス ポイントに適用され、ネットワーク内に存在するすべての既存のアクセス ポイントにも適用されます。
- [Client Access on Backhaul Link] : この機能を有効にすると、802.11a バックホールを介してメッシュ アクセス ポイントを 802.11a ワイヤレス クライアントに関連付けることができます。802.11a バックホールでは、ルートとメッシュ アクセス ポイント間の既存の通信に加えて、クライアント アソシエーションが行われます。この機能は 2 つの無線のあるアクセス ポイントだけに適用されます。詳細については、「1524SB デュアル バックホールでのクライアント アクセス」（P.9-441）を参照してください。

  （注）　バックホール クライアント アクセスを変更すると、すべてのメッシュ アクセス ポイントがリブートされます。

- [Mesh DCA Channels] : 有効または無効にします。このオプションは、デフォルトで無効です。DCA チャネル リストを使用してコントローラでバックホール チャネルを選択解除できるようにするには、このオプションを有効にします。コントローラ DCA リスト内のチャネルに対する変更はすべて、関連付けられたアクセス ポイントに適用されます。このオプションは、1524SB メッシュ アクセス ポイントのみに適用可能です。この機能の詳細については、「Prime Infrastructure を使用したバックホール チャネルの選択解除」（P.9-442）を参照してください。
- [Background Scanning] : [Background Scanning] チェックボックスを選択してバックグラウンド スキャンを有効にするか、選択解除してこの機能を無効にします。デフォルト値は [disabled] です。バックグラウンド スキャンにより、Cisco Aironet 1510 アクセス ポイントは、より最適なパスと親を探すために、能動的に連続して別のネイバーがいるチャネルをモニタできます。
- [Security Mode] : [Security Mode] ドロップダウン リストから [EAP]（拡張認証プロトコル）または [PSK]（事前共有キー）を選択します。

  （注）　セキュリティを変更すると、すべてのメッシュ アクセス ポイントがリブートされます。

ステップ 5　[Save] をクリックします。

1524SB デュアル バックホールでのクライアント アクセス

1524 シリアル バックホール（SB）アクセス ポイントは、3 つの無線スロットで構成されます。スロット 0 の無線は、クライアント アクセスに使用される 2.4 GHz の周波数帯域で動作します。スロット 1 とスロット 2 の無線は 5.8 GHz 帯域で動作し、主にバックホールに使用されます。ただし、ユニバーサル クライアント アクセス機能を使用すると、スロット 1 とスロット 2 の無線でもクライアント アクセスが可能です。

2 つの 802.11a バックホール無線は、同じ MAC アドレスを使用します。同じ WLAN が複数のスロット内の同じ BSSID にマップされることがあります。

デフォルトでは、両方のバックホール無線によるクライアント アクセスは無効です。

無線スロットを有効または無効にするには、次のガイドラインに従う必要があります。

- スロット 2 でのクライアント アクセスが無効の場合でも、スロット 1 でクライアント アクセスを有効にできます。
- スロット 1 でのクライアント アクセスが有効の場合のみ、スロット 2 でクライアント アクセスを有効にできます。
- スロット 1 でクライアント アクセスを無効にすると、スロット 2 でのクライアント アクセスは自動的に無効になります。
- クライアント アクセスを有効または無効にすると常に、すべてのメッシュ アクセス ポイントがリブートされます。

次のいずれかから、バックホール無線によるクライアント アクセスを設定できます。

- コントローラのコマンドライン インターフェイス（CLI）
- コントローラのグラフィカル ユーザ インターフェイス（GUI）
- Prime Infrastructure GUI。詳細については、「Prime Infrastructure の GUI を使用したクライアント アクセスの設定」（P.9-442）を参照してください。

（注）　CLI および GUI を使用したクライアント アクセスの設定手順は、『*Controller Configuration Guide*』に記載されています。

Prime Infrastructure の GUI を使用したクライアント アクセスの設定

2 つのバックホール無線でクライアント アクセスを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] > [Controller IP] > [Mesh] > [Mesh Settings] を選択します。

ステップ 2　[Client Access on Backhaul Link] チェックボックスを選択します。

ステップ 3　拡張したバックホール クライアント アクセスを有効にする場合は、[Extended Backhaul Client Access] チェックボックスを選択します。

ステップ 4　[Save] をクリックします。

警告メッセージが表示されます。

```
Enabling client access on both backhaul slots will use same BSSIDs on both the slots.
Changing Backhaul Client Access will reboot all Mesh APs.
```

ステップ 5　[OK] をクリックします。

ユニバーサル クライアント アクセスが、両方の無線で設定されます。

Prime Infrastructure を使用したバックホール チャネルの選択解除

バックホール チャネルの選択解除を設定するには、次の手順を実行します。

ステップ 1　最初に、コントローラでメッシュ DCA チャネル フラグを設定する必要があります。詳細については、「Prime Infrastructure を使用したコントローラでのメッシュ DCA チャネル フラグの設定」（P.9-443）を参照してください。

ステップ 2　次に、設定グループを使用してチャネル リストを変更します。詳細については、「設定グループを使用したチャネル リストの変更」（P.9-443）を参照してください。

ここでは、次の内容について説明します。

- 「Prime Infrastructure を使用したコントローラでのメッシュ DCA チャネル フラグの設定」（P.9-443）
- 「設定グループを使用したチャネル リストの変更」（P.9-443）

Prime Infrastructure を使用したコントローラでのメッシュ DCA チャネル フラグの設定

1 つ以上のコントローラでの各チャネルの変更を、関連付けられたすべての 1524SB アクセス ポイントに適用するよう、メッシュ DCA チャネル フラグを設定できます。この機能を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] > [*ip address of controller*] > [Mesh] > [Mesh Settings] を選択して、特定のコントローラ用にこのフラグを設定します。

または

[Configure] > [Controller Template Launch Pad] > [Mesh] > [Mesh Settings] を選択して、コントローラのリスト用にこのフラグを設定します。

[Mesh Settings] ページが表示されます。

ステップ 2　[general] オプションで、[Mesh DCA Channels] オプションを選択して、チャネルの選択を有効にします。このオプションは、デフォルトでは選択解除されています。

これで、コントローラでのチャネルの変更が、関連付けられた 1524SB アクセス ポイントに適用されます。

設定グループを使用したチャネル リストの変更

コントローラの設定グループを使用して、バックホール チャネルの選択解除を設定できます。設定グループを作成して、必要なコントローラをグループに追加し、[Country/DCA] タブを使用してそのグループ内のコントローラのチャネルを選択または選択解除できます。

設定グループを使用してバックホール チャネルの選択解除を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Config Groups] を選択します。

ステップ 2　設定グループの詳細を表示する設定グループを選択します。

ステップ 3　[Config Group detail] ページで、[Country/DCA] タブをクリックします。

ステップ 4　設定グループのチャネルを選択または選択解除します。

（注）　コントローラからバックホール チャネルの選択解除を設定することもできます。詳細については、コントローラのオンライン ヘルプまたは『*Controller User Guide*』を参照してください。

ポート パラメータの設定

個々のコントローラのポート パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Ports] > [Port Settings] を選択します。

ステップ 4　該当するポート番号をクリックして、[Port Settings Details] ページを開きます。次のパラメータが表示されます。

- 一般的なパラメータ：
  - [Port Number]：読み取り専用。
  - [Admin Status]：ドロップダウン リストから [Enabled] または [Disabled] を選択します。
  - [Physical Mode]：[Auto Negotiate] または [Full Duplex 1 Gbps] を選択します。
  - [STP Mode]：[802.1D]、[Fast]、または [Off] を選択します。
  - [Mirror Mode]：[Enabled] または [Disabled] を選択します。
  - [Link Traps]：[Enabled] または [Disabled] を選択します。
  - Power Over Ethernet
  - [Multicast Application Mode]：[Enabled] または [Disabled] を選択します。
- スパニングツリー プロトコル パラメータ：
  - [Priority]：最適なスイッチのプライオリティ番号。
  - [Path Cost]：ネットワーク管理者によって割り当てられ、インターネットワーク環境で最も望ましいパス（コストが低いほど、適したパスになります）を判別するために使用される値（通常、ホップ カウント、メディア帯域幅、またはその他の測定に基づく）。

ステップ 5　[General] または [Spanning Tree Protocol] 設定で [Save] または [Audit] を選択します。

コントローラ管理パラメータの設定

ここでは、次の内容について説明します。

トラップ レシーバの設定

ここでは、次の内容について説明します。

- 「個々のコントローラのトラップ レシーバの設定」（P.9-445）
- 「新規レシーバの追加」（P.9-445）

個々のコントローラのトラップ レシーバの設定

個々のコントローラのトラップ レシーバを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Trap Receivers] の順に選択します。

ステップ 4　現在のトラップ レシーバについて、次のパラメータが表示されます。

- [Template Name]：このテンプレートのユーザ定義の名前。
- [IP Address]：サーバの IP アドレス。
- [Admin Status]：SNMP トラップをレシーバに送信するには、ステータスを有効にする必要があります。

ステップ 5　詳細にアクセスするには、レシーバ名をクリックします。

ステップ 6　トラップ レシーバを有効にするには、[Admin Status] チェックボックスを選択します。トラップ レシーバを無効にするには、このチェックボックスを選択解除します。

ステップ 7　[Save] をクリックします。

新規レシーバの追加

新規レシーバを追加するには、次の手順を実行します。

ステップ 1　[Select a command] ドロップダウン リストから [Add Receiver] を選択します。

ステップ 2　[Go] をクリックします。

ステップ 3　[Select a template to apply to this controller] ドロップダウン リストから、このコントローラに適用する適切なテンプレートを選択します。

（注）　トラップ レシーバの新規テンプレートを作成するには、[click here] リンクを使用して、適切なテンプレート作成ページにアクセスします。

ステップ 4　[Apply] をクリックします。

トラップ制御パラメータの設定

個々のコントローラのトラップ制御パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Trap Control] の順に選択します。

適用されるテンプレートが特定されます（該当する場合）。詳細については、「トラップ制御テンプレートの設定」（P.11-720）を参照してください。

このコントローラの次のトラップを有効にできます。

- 一般的なトラップ
  - [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。

    （注）　SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。

  - [Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。
  - [Multiple Users]：2 人のユーザが同じログイン ID でログインしています。
  - [Spanning Tree]：スパニングツリー トラップ。個々のパラメータについては、STP 仕様を参照してください。
  - [Rogue AP]：不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。以前に検出された不正アクセス ポイントが存在しなくなっている場合は、このトラップが送信されます。
  - [Config Save]：コントローラ設定が変更されると送信される通知。
  - [RFID Limit Reached Threshold]：RFID 到達限度をこのチェックボックスで有効にして、しきい値のパーセントを設定します。これによって RFID タグがこのしきい値をまたいだときに Prime Infrastructure に通知が送信されます。デフォルトでは、警告が有効で、しきい値は 90 に設定されています。しきい値の有効範囲は 80 ～ 100 で単位は 1 です。
- クライアント関連トラップ
  - [802.11 Association]：クライアントがアソシエーション フレームを送信すると、アソシエーション通知が送信されます。
  - [802.11 Disassociation]：クライアントがディスアソシエーション フレームを送信すると、ディスアソシエーション通知が送信されます。
  - [802.11 Deauthentication]：クライアントが認証解除フレームを送信すると、認証解除通知が送信されます。
  - [802.11 Failed Authentication]：クライアントが「成功」以外のステータス コードの認証フレームを送信すると、認証エラー通知が送信されます。
  - [802.11 Failed Association]：クライアントが「成功」以外のステータス コードのアソシエーション フレームを送信すると、アソシエーション エラー通知が送信されます。
  - [Excluded]：クライアントが除外されると、アソシエーション エラー通知が送信されます。
  - [MaxClients Limit Reached Threshold]：MaxClients 到達限度をこのチェックボックスで有効にして、しきい値のパーセントを設定します。これによってクライアントの限度がこのしきい値をまたいだときに Prime Infrastructure に通知が送信されます。デフォルトでは、警告が有効で、しきい値は 90 に設定されています。しきい値の有効範囲は 80 ～ 100 で単位は 1 です。
- Cisco AP トラップ
  - [AP Register]：アクセス ポイントがコントローラに関連付けられるか、関連付け解除されると送信される通知。
  - [AP Interface Up/Down]：アクセス ポイント インターフェイス（802.11a または 802.11b/g）のステータスがアップまたはダウンになると送信される通知。
- 自動 RF プロファイル トラップ

- [Load Profile] : [Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Noise Profile] : [Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Interference Profile] : [Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Coverage Profile] : [Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

- 自動 RF 更新トラップ
  - [Channel Update] : アクセス ポイントの動的チャネル アルゴリズムが更新されると送信される通知。
  - [Tx Power Update] : アクセス ポイントの動的送信電力アルゴリズムが更新されると送信される通知。
- AAA トラップ
  - [User Auth Failure] : このトラップは、クライアントの RADIUS 認証の失敗が発生したことを通知します。
  - [RADIUS Server No Response] : このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。
- IP セキュリティ トラップ
  - [ESP Authentication Failure] : 無効なハッシュを持つ IPsec パケットが着信 ESP SA で見つかりました。
  - [ESP Replay Failure] : 無効なシーケンス番号を持つ IPsec パケットが着信 ESP SA で見つかりました。
  - [Invalid SPI] : 不明な SPI を持つパケットが、指定されたプロトコルを使用する指定された SPI を持つ指定されたピアから検出されました。
  - [IKE Negotiation Failure] : フェーズ 1 IKE SA のネゴシエーションの試行が失敗しました。ネゴシエーション エラーの総数カウンタの現在の値とともに、トラップの一部として通知回数も送信されます。
  - [IKE Suite Failure] : 指定されたセレクタのフェーズ 2 SA スイートのネゴシエーションの試行が失敗しました。この障害に関係した通知の通知タイプ回数とともに、現在の合計障害回数が渡されます。
  - [Invalid Cookie] : 指定された宛先への無効な cookie がある ISAKMP パケットが、指定された送信元から検出されました。発信側と送信側の cookie もトラップとともに送信されます。
- 802.11 セキュリティ トラップ
  - [WEP Decrypt Error] : コントローラが WEP 復号エラーを検出すると送信される通知。
- WPS トラップ
  - [Rogue Auto Containment] : 不正アクセス ポイントが自動的に封じ込められると送信される通知。

ステップ 4　該当するパラメータの選択後に、[Save] をクリックします。

Telnet SSH パラメータの設定

個々のコントローラの Telnet SSH（セキュア シェル）パラメータを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Telnet SSH] の順に選択します。

適用されるテンプレートが特定されます（該当する場合）。詳細については、「Telnet SSH テンプレートの設定」（P.11-722）を参照してください。

次のパラメータを設定できます。

- [Session Timeout]：ログオフされるまでに Telnet セッションが非アクティブの状態を継続できる分数を示します。0 は、タイムアウトしないことを意味します。0 ～ 160 までの数値で指定できます。工場出荷時のデフォルトは 5 です。
- [Maximum Sessions]：ドロップダウン リストから、0 ～ 5 までの値を選択します。このオブジェクトは、許可される同時 Telnet セッションの数を示します。

（注）　DS（ネットワーク）ポートでは、新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。

- [Allow New Telnet Sessions]：[no] に設定すると、DS ポートでは新しい Telnet セッションが許可されないことを示します。工場出荷時のデフォルト値は [no] です。

（注）　DS（ネットワーク）ポートでは、新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。

- [Allow New SSH Sessions]：[no] に設定すると、新しいセキュア シェル Telnet セッションが許可されないことを示します。工場出荷時のデフォルト値は [yes] です。

ステップ 4　該当するパラメータの設定後に、[Save] をクリックします。

個々のコントローラの Syslog の設定

個々のコントローラの Syslog を有効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Syslog] の順に選択します。

適用されるテンプレートが特定されます（該当する場合）。詳細については、「レガシー Syslog テンプレートの設定」（P.11-723）を参照してください。

- [Syslog Enabled]：Syslog を有効にするには、このチェックボックスを選択します。

ステップ 4　[Save] をクリックします。

複数の Syslog サーバの設定

リリース 5.0.148.0 以降のコントローラでは、WLAN コントローラで複数（3 つまで）の Syslog サーバを設定できます。それぞれのメッセージが記録されると、メッセージの重大度が設定済みの Syslog フィルタ重大度レベル以上である場合、コントローラは、メッセージのコピーを設定済みの各 Syslog ホストに送信します。

個々のコントローラの Syslog を有効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Multiple Syslog] の順に選択します。

適用されるテンプレートが示されます。

[Syslog Server Address] : 該当する Syslog のサーバ アドレスを示します。

ステップ 4　[Save] をクリックします。

WEB 管理の設定

この項では、ディストリビューション システム ポートを Web ポート（HTTP を使用）またはセキュア Web ポート（HTTPS を使用）として有効にする手順について説明します。HTTPS を有効化すると、GUI との通信を保護できます。HTTPS は、Secure Socket Layer（SSL）プロトコルを使用して HTTP ブラウザ セッションを保護します。HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。また、外部で生成された証明書をダウンロードすることもできます。

個々のコントローラの WEB 管理パラメータを有効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Web Admin] の順に選択します。

次のパラメータを設定できます。

- [Web Mode] : ドロップダウン リストから [Enable] または [Disable] を選択します。有効にすると、ユーザは、*https://ip-address* を使用してコントローラの GUI にアクセスできます。デフォルトでは無効になっています。

  （注）　Web モードの接続は、セキュリティで保護されません。

- [Secure Web Mode] : ドロップダウン リストから [Enable] または [Disable] を選択します。有効にすると、ユーザは、*https://ip-address* を使用してコントローラの GUI にアクセスできます。デフォルトは [Enabled] です。

  （注）　セキュア Web モードの接続は、セキュリティで保護されています。

- Certificate Type

- [Download Web Admin Certificate] : [Download Web Admin Certificate to Controller] ページにアクセスする場合にクリックします。追加情報については、「コントローラへの Web 認証または Web 管理証明書のダウンロード」（P.9-450）を参照してください。

（注）　新しい Web 管理証明書を有効にするには、コントローラをリブートする必要があります。

コマンド ボタン

- Save
- Audit
- Regenerate Cert

コントローラへの Web 認証または Web 管理証明書のダウンロード

Web 認証または Web 管理証明書をコントローラにダウンロードするには、次の手順を実行します。

ステップ 1　[Download Web Admin Certificate] リンクをクリックします。

ステップ 2　[File is located on] フィールドで、ローカル マシンまたは TFTP サーバを指定します。

（注）　証明書が TFTP サーバにある場合は、サーバ ファイル名を入力します。ローカル マシンにある場合は、[Browse] をクリックして、ローカル ファイル名を入力します。

ステップ 3　[Server Name] テキスト ボックスに TFTP サーバ名を入力します。デフォルトは Prime Infrastructure サーバです。

ステップ 4　サーバの IP アドレスを入力します。

ステップ 5　[Maximum Retries] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 6　[Timeout] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 7　[Local File Name] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 8　[Server File Name] テキスト ボックスに、証明書の名前を入力します。

ステップ 9　[Password] テキスト ボックスにパスワードを入力します。

ステップ 10　[OK] をクリックします。

ローカル管理ユーザの設定

このページには、ローカル管理ユーザの名前やアクセス権限の一覧が表示されます。

[Local Management Users] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Local Management Users] の順に選択します。

ステップ 4　ユーザ名をクリックします。

- [User Name (read-only)] : ユーザの名前。
- [Access Level (read-only)] : [Read Write] または [Read Only]。

認証の優先順位の設定

このページで、コントローラの管理ユーザの認証に使用する認証サーバの順序を制御できます。

[Authentication Priority] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Management] > [Authentication Priority] の順に選択します。

ステップ 4　最初にローカル データベースが検索されます。RADIUS または TACACS+ のどちらかを次の検索対象に選択します。ローカル データベースを使用した認証に失敗した場合に、コントローラは次の種類のサーバを使用します。

ステップ 5　[Save] をクリックします。

コマンド ボタン

- [Save] : 管理ユーザの認証順序に行った変更を保存して、前のページに戻ります。
- [Audit] : コントローラで使用される値と Prime Infrastructure の値を比較します。

ロケーションの設定

[Location Configuration] ページで、有効期限、通知間隔、およびその他の詳細設定オプションなど、ロケーション パラメータを設定できます。

ロケーション テンプレートでは、次の一般パラメータと詳細パラメータを設定できます。

- General パラメータ : RFID タグの収集の有効化、調整クライアントまたは通常の（非調整）クライアントのロケーション パス損失の設定、クライアント、タグ、および不正アクセス ポイントの測定通知の設定、クライアント、タグ、および不正アクセス ポイントの RSSI 有効期限タイムアウト値の設定を行います。
- Advanced パラメータ : RFID タグ データ タイムアウト値の設定、調整クライアントのマルチバンドのロケーション パス損失設定の有効化を行います。

個々のコントローラのロケーションを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Location Configuration] > [Location Configuration] を選択します。

[Location Configuration] ページには、[General] と [Advanced] の 2 つのタブが表示されます。

ステップ 4　次の General パラメータを追加または変更します。

- [RFID Tag Data Collection]：タグでデータの収集を有効にするには、このチェックボックスを選択します。

  ロケーション サーバがコントローラからアセット タグ データを収集する前に、コントローラで CLI コマンド **config rfid status enable** を使用して、アクティブ RFID タグの検出を有効にする必要があります。

- Location Path Loss Configuration
  - [Calibrating Client]：クライアントの調整を有効にするには、[Enabled] チェックボックスを選択します。コントローラは、クライアントを調整するために、アクセス ポイントを介して（クライアントの機能に応じて）通常の S36 または S60 要求を送信します。パケットは、すべてのチャネルで送信されます。すべてのアクセス ポイントが、それぞれの場所でクライアントから RSSI データを収集します。これらの追加送信およびチャネル変更は、同時に発生する音声またはビデオ トラフィックの質が低下する場合があります。

    （注）　使用可能なすべての無線（802.11a/b/g/n）を使用するには、[Advanced] ページでマルチバンドを有効にする必要があります。

  - [Normal Client]：非調整クライアントを使用するには、[Enabled] チェックボックスを選択します。S36 要求はクライアントに送信されません。

    （注）　S36 および S60 は、特定の Cisco Compatible Extensions との互換性があるクライアント ドライバです。S36 には CCXv2 以降との互換性があります。S60 には CCXv4 以降との互換性があります。詳細については、次の URL を参照してください。
    http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml

- Measurement Notification Interval (in secs)
  - [Tags, Clients, and Rogue APs/Clients]：クライアント、タグ、および不正に関する NMSP 測定通知間隔を設定できます。見つかった要素（タグ、クライアント、および不正アクセス ポイントやクライアント）が通知されるまでの秒数を指定します。

    コントローラでこの値を設定すると、[Synchronize Servers] ページで表示できる同期外れ通知が生成されます。コントローラとモビリティ サービス エンジン間に別の測定間隔が存在する場合、2 つの設定のうち最長の間隔設定がモビリティ サービス エンジンによって採用されます。

    このコントローラがモビリティ サービス エンジンと同期されると、モビリティ サービス エンジンで新しい値が設定されます。

    （注）　測定通知間隔に変更を行う場合は、モビリティ サービス エンジンに同期する必要があります。

- RSS Expiry Timeout (in secs)
  - [For Clients]：通常の（非調整）クライアントの RSSI 測定を廃棄するまでの秒数を入力します。
  - [For Calibrating Clients]：調整クライアントの RSSI 測定を廃棄するまでの秒数を入力します。
  - [For Tags]：タグの RSSI 測定を廃棄するまでの秒数を入力します。

– [For Rogue APs]：不正アクセス ポイントの RSSI 測定を廃棄するまでの秒数を入力します。

ステップ 5　次の Advanced パラメータを追加または変更します。

- [RFID Tag Data Timeout (in secs)] : RFID タグ データ タイムアウトを設定するための値（秒単位）を入力します。
- Location Path Loss Configuration
  - [Calibrating Client Multiband]：すべてのチャネルで S36 および S60 パケット（該当する場合）を送信するには、[Enabled] チェックボックスを選択します。[general] ページで調整クライアントを有効にする必要があります。

（注）　使用可能なすべての無線（802.11a/b/g/n）を使用するには、マルチバンドを有効にする必要があります。

ステップ 6　[Save] をクリックします。

コマンド ボタン

- [Save]：管理ユーザの認証順序に行った変更を保存して、前のページに戻ります。
- [Audit]：コントローラで使用される値と Prime Infrastructure の値を比較します。

IPv6 の設定

ここでは、次の内容について説明します。

- 「ネイバーのバインディング タイマーの設定」（P.9-453）
- 「[RA Throttle Policy] の設定」（P.9-454）
- 「RA ガードの設定」（P.9-454）

ネイバーのバインディング タイマーの設定

[Down Lifetime]、[Reachable Lifetime]、[Stale Lifetime]、および対応する間隔など、[IPv6 Router Neighbor Binding Timers] パラメータを設定できます。

[Neighbor Binding Timers] を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[IPv6] > [Neighbor Binding Timers] を選択します。[IPv6] > [Neighbor Binding Timers] ページが表示されます。

ステップ 4　[Down Lifetime] タイマーを有効にするには、[Enable] チェックボックスを選択します。このチェックボックスを選択した場合は、[Down Lifetime Interval] 値を指定します。これは、最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。

ステップ 5　[Reachable Lifetime] タイマーを有効にするには、[Enable] チェックボックスを選択します。このチェックボックスを選択した場合は、[Reachable Lifetime Interval] 値を指定します。これは、最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。

ステップ 6　[Stale Lifetime] タイマーを有効にするには、[Enable] チェックボックスを選択します。このチェックボックスを選択した場合は、[Stale Lifetime Interval] 値を指定します。これは、最大時間（秒単位）を示します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 です。

ステップ 7　[Save] をクリックします。

[RA Throttle Policy] の設定

[RA Throttle Policy] を使用すると、ワイヤレス ネットワークで循環するマルチキャスト ルータ アドバタイズメント（RA）の量を制限できます。[RA Throttle Policy]、[Throttle Period]、およびその他のオプションなど、[IPv6 Router Advertisement] パラメータを設定できます。

[RA Throttle Policy] を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[IPv6] > [RA Throttle Policy] の順に選択します。[IPv6] > [RA Throttle Policy] ページが表示されます。

ステップ 4　RA スロットル ポリシーを有効にするには、[Enable] チェックボックスを選択し、次のパラメータを設定します。

- [Throttle Period]：スロットル期間（秒単位）。指定できる範囲は 10 ～ 86,400 秒です。
- [Max Through]：ある期間または無制限の期間にわたって通過する RA の数。
- [Interval Option]：RA で間隔オプションが指定されている場合の動作を示します。
  - Ignore
  - Passthrough
  - Throttle
- [Allow At-least]：ルータ単位で抑制されない RA の最小数を示します。
- [Allow At-most]：ルータ単位で抑制されない RA の最大数または無制限数を示します。

ステップ 5　[Save] をクリックします。

RA ガードの設定

RA ガードは、ワイヤレス クライアントから RA をドロップするための Unified Wireless のソリューションです。これはグローバルに設定され、デフォルトで有効です。[IPv6 Router Advertisement] パラメータを設定できます。

RA ガードを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[IPv6] > [RA Guard] の順に選択します。[IPv6] > [RA Guard] ページが表示されます。

ステップ 4　[Router Advertisement Guard] を有効にするには、[Enable] チェックボックスを選択します。

ステップ 5　[Save] をクリックします。

プロキシ モバイル IPv6 の設定

プロキシ モバイル IPv6 は、任意の IP モビリティ関連シグナリングでモバイル ノードのプロキシとして動作することによってモバイル ノードをサポートする、ネットワーク ベースのモバイル管理プロトコルです。ネットワークのモビリティ エンティティは、モバイル ノードの移動を追跡し、モビリティ シグナリングを起動して必要なルーティング状態を設定します。

主要な機能エンティティは Local Mobility Anchor（LMA）とモバイル アクセス ゲートウェイ（MAG）です。LMA はモバイル ノードの到達可能性状態を維持し、モバイル ノードの IP アドレス用のトポロジ アンカー ポイントです。MAG はモバイル ノードの代わりにモビリティ管理を行います。MAG はモバイル ノードがアンカーされているアクセス リンクに存在します。コントローラは MAG 機能を実装します。

PMIP グローバル設定の構成

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[PMIP] > [Global Config] の順に選択します。

ステップ 4　次のフィールドを設定します。

- [Domain Name]
- [Maximum Bindings Allowed] : コントローラが MAG に送信できるバインディング アップデートの最大数。有効な範囲は 0 ～ 40000 です。
- [Binding Lifetime] : コントローラのバインディング エントリのライフタイム。有効な範囲は 10 ～ 65535 秒です。デフォルト値は 65535 です。バインディング ライフタイムは 4 秒の倍数であることが必要です。
- [Binding Refresh Time] : コントローラのバインディング エントリのリフレッシュ時間。有効な範囲は 4 ～ 65535 秒です。デフォルト値は 300 秒です。バインディング リフレッシュ時間は 4 秒の倍数であることが必要です。
- [Binding Initial Retry Timeout] : コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の初期タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 1000 秒です。
- [Binding Maximum Retry Timeout] : コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の最大タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 32000 秒です。
- [Replay Protection Timestamp] : 受信したプロキシ バインディング確認のタイムスタンプと現在の日時との時間差の上限。有効範囲は 1 ～ 255 ミリ秒です。デフォルト値は 7 ミリ秒です。
- [Minimum BRI Retransmit Timeout] : コントローラが BRI メッセージを再送信するまでに待機する時間の最小値。有効な範囲は 500 ～ 65535 秒です。
- [Maximum BRI Retransmit Timeout] : コントローラが Binding Revocation Indication（BRI）メッセージを再送信するまでに待機する時間の最大値。有効な範囲は 500 ～ 65535 秒です。デフォルト値は 2000 秒です。

ステップ 5　[Save] をクリックします。

LMA 設定の構成

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[PMIP] > [LMA Config] の順に選択します。

ステップ 4　次のフィールドを設定します。

- [LMA Name]：コントローラに接続された LMA の名前。
- [LMA IP Address]：コントローラに接続された LMA の IP アドレス。

ステップ 5　[Save] をクリックします。

PMIP プロファイルの設定

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[PMIP] > [PMIP Profile] の順に選択します。

ステップ 4　プロファイル名を入力します。

ステップ 5　[Add] をクリックし、次のフィールドを設定します。

- [Network Access Identifier]：プロファイルにアソシエートされたネットワーク アクセス識別子（NAI）の名前。
- [LMA Name]：プロファイルをアソシエートする LMA の名前。
- [Access Point Node]：コントローラに接続されているアクセス ポイント ノードの名前。

ステップ 6　[Save] をクリックします。

mDNS の設定

マルチキャスト DNS（mDNS）サービス ディスカバリは、ローカル ネットワークでサービスを通知し、検出する手段を提供します。mDNS は IP マルチキャストを介して DNS クエリーを実行します。mDNS はゼロ設定の IP ネットワーキングをサポートします。

mDNS テンプレート、ガイドライン、および制約事項については、「mDNS テンプレートの設定」（P.11-732）を参照してください。

コントローラが mDNS サービスについて学習し、すべてのクライアントにこれらのサービスをアドバタイズできるように mDNS を設定できます。

[Services] と [Profiles] の 2 個のタブがあります。

- [Services] タブ：このタブでは、グローバル mDNS パラメータを設定し、Master Services データベースを更新できます。

- [Profiles] タブ：このタブでは、コントローラに設定されている mDNS プロファイルを表示し、新しい mDNS プロファイルを作成できます。新しいプロファイルを作成した後、インターフェイス グループ、インターフェイス、または WLAN にプロファイルをマッピングする必要があります。クライアントはプロファイルに関連付けられたサービスだけのサービス アドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。デフォルトで、コントローラには mDNS プロファイル default-mdns-profile があります。このデフォルト プロファイルは削除できません。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[mDNS] > [mDNS] の順に選択します。

ステップ 4　[Services] タブで、次のパラメータを設定します。

- [Template Applied]：このコントローラに適用されるテンプレートの名前。
- [mDNS Global Snooping]：mDNS パケットのスヌーピングを有効にするチェックボックス。

（注）　コントローラは mDNS スヌーピングを有効にしても、IPv6 mDNS パケットをサポートしません。

- [Query Interval]（10 ～ 120）：ユーザが設定できる mDNS クエリー間隔（分単位）。この間隔は、WLC によって、サービス アドバタイズメントを自動的に送信しないサービスに対して、そのサービスが開始された後に定期的な mDNS クエリー メッセージを送信するために使用されます。範囲は 10 ～ 120 分です。デフォルト値は 15 分です。
- [Master Services]：[Add Row] をクリックし、次のフィールドを設定します。
  - [Master Service Name]：ドロップダウン リストから、照会可能なサポートされているサービスを選択できます。次のサービスを使用できます。
  - AirTunes
  - AirPrint
  - AppleTV
  - HP Photosmart Printer1
  - HP Photosmart Printer2
  - Apple File Sharing Protocol（AFP）
  - Scanner
  - Printer
  - FTP
  - iTunes Music Sharing
  - iTunes Home Sharing
  - iTunes Wireless Device Syncing
  - Apple Remote Desktop
  - Apple CD/DVD Sharing
  - Time Capsule Backup

（注）　新しいサービスを追加するには、サービス名を入力または選択し、そのサービス文字列を入力して、サービス ステータスを選択します。

- [Service Name] : mDNS サービスの名前。
- [Service String] : mDNS サービスに関連付けられた一意の文字列。たとえば、_airplay._tcp.local. は AppleTV に関連付けられたサービス文字列です。
- [Query Status] : サービスの mDNS クエリーを有効にするために選択するチェックボックス。

（注）　定期的な mDNS クエリー メッセージは、クエリーのステータスが有効な場合だけ、WLC によって、サービスに対して設定されたクエリー間隔で送信されます。それ以外の場合、サービスは、クエリーのステータスが無効になっているその他のサービス（たとえば AppleTV）に自動的にアドバタイズする場合があります。

ステップ 5　[Profiles] タブで、次のパラメータを設定します。

- [Profiles] : [Add Profile] をクリックし、次のフィールドを設定します。
  - [Profile Name] : mDNS プロファイルの名前。最大 16 個のプロファイルを作成できます。
  - [Services] : mDNS プロファイルにマップするサービスを選択します（チェックボックスを使用）。

ステップ 6　[Save] をクリックします。

AVC プロファイルの設定

Application Visibility and Control（AVC）は、Network Based Application Recognition（NBAR）ディープ パケット インスペクション テクノロジーを使用して、使用するプロトコルに基づいてアプリケーションを分類します。AVC を使用して、コントローラはレイヤ 4 ～レイヤ 7 の 1400 を超えるプロトコルを検出できます。AVC では、リアルタイム分析を実施して、ネットワークの輻輳、高価なネットワーク リンクの使用、およびインフラストラクチャのアップグレードを減らすためにポリシーを作成することができます。

AVC は、Cisco 2500 および 5500 シリーズ コントローラ、Cisco Flex 7500 および Cisco 8500 シリーズ コントローラでだけサポートされています。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Application Visibility And Control] > [AVC Profiles] の順に選択します。

ステップ 4　設定する AVC プロファイル名をクリックします。

ステップ 5　AVC ルールを作成するには、[AVC Rule List] の下にある [Add Row] をクリックします。

ステップ 6　次のパラメータを設定します。

- [Application Name] : アプリケーションの名前。
- [Application Group Name] : アプリケーションが属するアプリケーション グループの名前。
- [Action] : ドロップダウン リストから、次の項目を選択できます。

- [Drop]：選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをドロップします。
- [Mark]：[Differentiated Services Code Point (DSCP)] ドロップダウン リストで指定する DSCP 値と選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをマークします。DSCP 値により QoS レベルに基づいて差別化サービスを提供します。

  デフォルト アクションは、すべてのアプリケーションの許可です。

- [DSCP]：インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コード。DSCP 値は次の QoS レベルにマッピングされます。
  - [Platinum (Voice)]：Voice over Wireless の高い QoS を保証します。
  - [Gold (Video)]：高品質のビデオ アプリケーションをサポートします。
  - [Silver (Best Effort)]：クライアントの通常の帯域幅をサポートします。
  - [Bronze (Background)]：ゲスト サービス用の最小の帯域幅を提供します。
- [DSCP Value]：[Custom] を選択し、DSCP 値を指定することもできます。範囲は 0 ～ 63 です。

ステップ 7　[Save] をクリックします。

NetFlow の設定

NetFlow は、ネットワーク ユーザとアプリケーション、ピーク時の使用時間、およびトラフィック ルーティングに関する貴重な情報を提供するプロトコルです。このプロトコルは、トラフィックをモニタするためにネットワーク デバイスから IP トラフィック情報を収集します。Netflow アーキテクチャは次のコンポーネントで構成されています。

- コレクタ：さまざまなネットワーク要素から IP トラフィック情報をすべて収集するエンティティ。
- エクスポータ：IP トラフィック情報を使用してテンプレートをエクスポートするネットワーク エンティティ。コントローラは、エクスポータとして機能します。

ここでは、次の内容について説明します。

- 「NetFlow モニタの設定」（P.9-459）
- 「NetFlow エクスポータの設定」（P.9-460）

NetFlow モニタの設定

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[NetFlow] > [Monitor] の順に選択します。

ステップ 4　次のパラメータを設定します。

- [Monitor Name]：NetFlow モニタの名前。モニタ名は最大 127 文字の英数字で、大文字と小文字を区別します。コントローラでは 1 つのみモニタを設定できます。
- [Record Name]：NetFlow レコードの名前。コントローラの NetFlow レコードには、特定のフロー内のトラフィックに関する次の情報が含まれます。
  - クライアントの MAC アドレス。
  - クライアント送信元 IP アドレス

- WLAN ID
- アプリケーション ID
- データの着信バイト数
- データの発信バイト数
- 着信パケット
- 発信パケット
- 着信 DSCP
- 発信 DSCP
- 最後の AP の名前。

ステップ 5　[Exporter Name] : エクスポータの名前。コントローラでは 1 つのみモニタを設定できます。

ステップ 6　[Exporter IP] : コレクタの IP アドレス。

ステップ 7　[Port] : NetFlow レコードをコントローラからエクスポートする UDP ポート。

ステップ 8　[Save] をクリックします。

NetFlow エクスポータの設定

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　適切な IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[NetFlow] > [Exporter] の順に選択します。

ステップ 4　次のパラメータを設定します。

- [Exporter Name] : エクスポータの名前。
- [Exporter IP] : エクスポータの IP アドレス。
- [Port Number] : NetFlow レコードをコントローラからエクスポートする UDP ポート。

ステップ 5　[Save] をクリックします。

サードパーティのコントローラおよびアクセス ポイントの設定

Prime Infrastructure では、サードパーティのコントローラおよびアクセス ポイントを追加することができます。この機能の一部として、次の機能を実行できます。

- Prime Infrastructure にサードパーティのコントローラを追加します。
- サードパーティのコントローラの状態をモニタします。
- サードパーティのコントローラと、アソシエートされたアクセス ポイントのインベントリ情報を取得します。
- サードパーティのコントローラおよびアクセス ポイントの動作ステータスを表示するには、バックグラウンド タスクを使用します。

ここでは、次の内容について説明します。

サードパーティのコントローラの追加

サードパーティのコントローラを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Third Party Controllers] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Controller] を選択し、[Go] をクリックします。

ステップ 3　[Add Controller] ページで、コントローラの IP アドレス、ネットワーク マスク、および必要な SNMP 設定を入力します。

ステップ 4　[Add] をクリックします。

サードパーティのコントローラの動作ステータスの表示

[Third Party Controller Operational Status] ページを表示するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Third Party Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Third Party Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Tasks] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Third Party Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Tasks] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3　タスクを変更するには、[Background Tasks] 列の [Third Party Controller Operational Status] リンクをクリックします。

[Third Party Controller Operational Status] ページには、次の情報が表示されます。

- 最後の実行情報

- 開始時刻および終了時刻。
- タスクの経過時間（秒）。
- [Result]：成功またはエラー。
- [Message]：このタスクに関するテキスト メッセージ。

ステップ 4　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Interval]：タスクの頻度（分）を示します。デフォルトは 3 時間です。

ステップ 5　完了したら、[Save] をクリックしてタスクの変更を確定します。

サードパーティのアクセス ポイントの詳細の表示

サードパーティのアクセス ポイントは、サードパーティのコントローラを追加すると検出されます。

サードパーティのアクセス ポイントの設定を表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Third Party Access Points] を選択します。

ステップ 2　[AP Name] リンクをクリックして、サードパーティのアクセス ポイントの詳細を表示します。そのサードパーティのアクセス ポイントの [General] タブが表示されます。

（注）　表内の列の追加、削除、並べ替えを行うには、[Edit View] リンクをクリックします。

サードパーティのアクセス ポイントの削除

サードパーティのアクセス ポイントを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Third Party Access Points] を選択します。

ステップ 2　削除するアクセス ポイントのチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Remove APs] を選択します。

サードパーティのアクセス ポイントの動作ステータスの表示

[Third Party Access Point Operational Status] ページを表示するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

[Third party Access Point Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

または

- タスクを有効にする。

  [Third party Access Point Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Tasks] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Third party Access Point Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Tasks] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3　タスクを変更するには、[Background Tasks] 列の [Third party Access Point Operational Status] リンクをクリックします。

[Third Party Controller Operational Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - タスクの経過時間（秒）。
  - [Result]：成功またはエラー。
  - [Message]：このタスクに関するテキスト メッセージ。

ステップ 4　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Interval]：タスクの頻度（分）を示します。デフォルトは 3 時間です。

ステップ 5　完了したら、[Save] をクリックしてタスクの変更を確定します。

アクセス ポイントの設定

ここでは、Prime Infrastructure データベースでのアクセス ポイントの設定方法について説明します。ここでは、次の内容について説明します。

- 「アクセス ポイントの削除」（P.9-495）
- 「無線ステータスのスケジュール設定」（P.9-496）
- 「監査ステータスの表示（アクセス ポイント）」（P.9-497）
- 「メンテナンス モード アクセス ポイントのアラームのフィルタリング」（P.9-497）
- 「アクセス ポイントの検索」（P.9-498）
- 「メッシュ リンクの詳細の表示」（P.9-499）
- 「不正アクセス ポイント分類ルールの表示または編集」（P.9-500）
- 「Spectrum Expert の設定」（P.9-510）
- 「OfficeExtend アクセス ポイント」（P.9-513）
- 「アクセス ポイントのリンク遅延の設定」（P.9-514）

AP フェールオーバー優先度の設定

コントローラに障害が発生した場合、アクセス ポイントに設定されたバックアップ コントローラがすぐに多くの検出と接続要求を受信します。これにより、コントローラは飽和ポイントに達し、いくつかのアクセス ポイントを拒否する可能性があります。

優先順位をアクセス ポイントに割り当てることによって、拒否されるアクセス ポイントを制御します。フェールオーバー時にバックアップ コントローラが飽和している状況では、優先度の低いアクセス ポイントの接続を切断することによって優先度の高いアクセス ポイントがバックアップ コントローラに接続できるようになります。

アクセス ポイントの優先度設定を設定するには、まず AP Priority 機能を有効にする必要があります。AP Priority 機能を有効にする手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　該当するコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [General] の順に選択します。

ステップ 4　[AP Failover Priority] ドロップダウン リストから、[Enable] 選択します。

アクセス ポイントの優先度を設定するには、「アクセス ポイントの詳細の設定」（P.9-477）を参照してください。

アクセス ポイントのグローバル クレデンシャルの設定

Cisco Autonomous アクセス ポイントには、工場出荷時にデフォルトのイネーブル パスワード *Cisco* が設定されています。ユーザはこのパスワードを使用して、非特権モードにログインし、show および debug コマンドを実行することができますが、これはセキュリティに対する脅威となります。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートからコンフィギュレーション コマンドを実行できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

Prime Infrastructure およびリリース 5.0 よりも前のコントローラ ソフトウェアでは、現在コントローラに接続されているアクセス ポイントに対してだけ、アクセス ポイントのイネーブル パスワードを設定できます。Prime Infrastructure およびコントローラ ソフトウェア リリース 5.0 では、グローバルなユーザ名、パスワード、イネーブル パスワードを設定できます。これらは、コントローラに追加されるときに、すべてのアクセス ポイントが継承する情報です。これには、コントローラに現在接続され

ているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。アクセス ポイントを追加するとき、このグローバル ユーザ名とパスワードを使用するか、（グローバル ユーザ名とパスワードを使用せずに）そのアクセス ポイント独自のユーザ名、パスワード、イネーブル パスワードを設定するかを選択できます。グローバル パスワードが表示される場所、およびアクセス ポイント単位でグローバル パスワードを上書きする方法を確認するには、「AP 設定テンプレートの設定」（P.11-736）を参照してください。

さらにコントローラ ソフトウェア リリース 5.0 では、アクセス ポイントをコントローラに接続すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、アクセス ポイントのコンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

（注） コントロール ソフトウェア リリース 5.0 の機能は、Lightweight モードに変換されているすべてのアクセス ポイントで利用できます（1100 シリーズ以外）。VxWorks アクセス ポイントはサポートされていません。

コントローラで設定したグローバル資格情報はコントローラやアクセス ポイントをリブートした後も保持されます。この情報が上書きされるのは、アクセス ポイントを、グローバル ユーザ名およびパスワードが設定された新しいコントローラに join した場合のみです。グローバル資格情報を使って新しいコントローラを設定しなかった場合、このアクセス ポイントは最初のコントローラに設定されているグローバル ユーザ名とパスワードをそのまま保持します。

（注） アクセス ポイントにより使用される資格情報は常に把握している必要があります。そうではない場合、アクセス ポイントのコンソール ポートにログインできない可能性があります。必要であれば、アクセス ポイントの設定をクリアして、ユーザ名とパスワードをデフォルト設定に戻すことができます。

グローバル ユーザ名とパスワードを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] または [Configure] > [Access Points] の順に選択します。

ステップ 2　ソフトウェア リリース 5.0 以降を使用しているコントローラの IP アドレス、またはソフトウェア リリース 5.0 以降に関連付けられているアクセス ポイントを選択します。

ステップ 3　左側のサイドバーのメニューから、[System] > [AP Username Password] の順に選択します。[AP Username Password] ページが表示されます。

ステップ 4　[AP Username] テキスト ボックスに、そのコントローラに追加するすべてのアクセス ポイントが継承するユーザ名を入力します。

ステップ 5　[AP Password] テキスト ボックスに、そのコントローラに追加するすべてのアクセス ポイントが継承するパスワードを入力します。[Confirm AP Password] テキスト ボックスにパスワードを再度入力します。

ステップ 6　Cisco Autonomous アクセス ポイントの場合は、イネーブル パスワードも入力する必要があります。[AP Enable Password] テキスト ボックスに、そのコントローラに追加するすべてのアクセス ポイントが継承するイネーブル パスワードを入力します。[Confirm Enable Password] テキスト ボックスにパスワードを再度入力します。

ステップ 7　[Save] をクリックします。

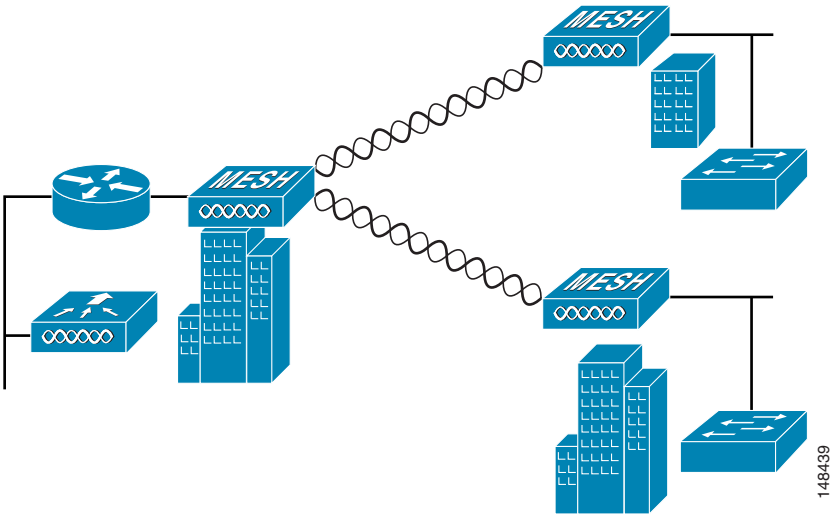
イーサネット ブリッジングおよびイーサネット VLAN タギングの設定

イーサネット ブリッジングは、2 つのメッシュ ネットワークのシナリオで使用されます。

1. MAP 間のポイントツーポイントおよびポイントツーマルチポイント ブリッジング（タグなしパケット）。一般的なトランク アプリケーションではキャンパス内のビルディング間のトラフィックをブリッジングすることがあります（図 9-3 を参照）。

（注）　ポイントツーポイントおよびポイントツーマルチポイント ブリッジング導入でイーサネット ブリッジングを使用するのに、VLAN タギングを設定する必要はありません。

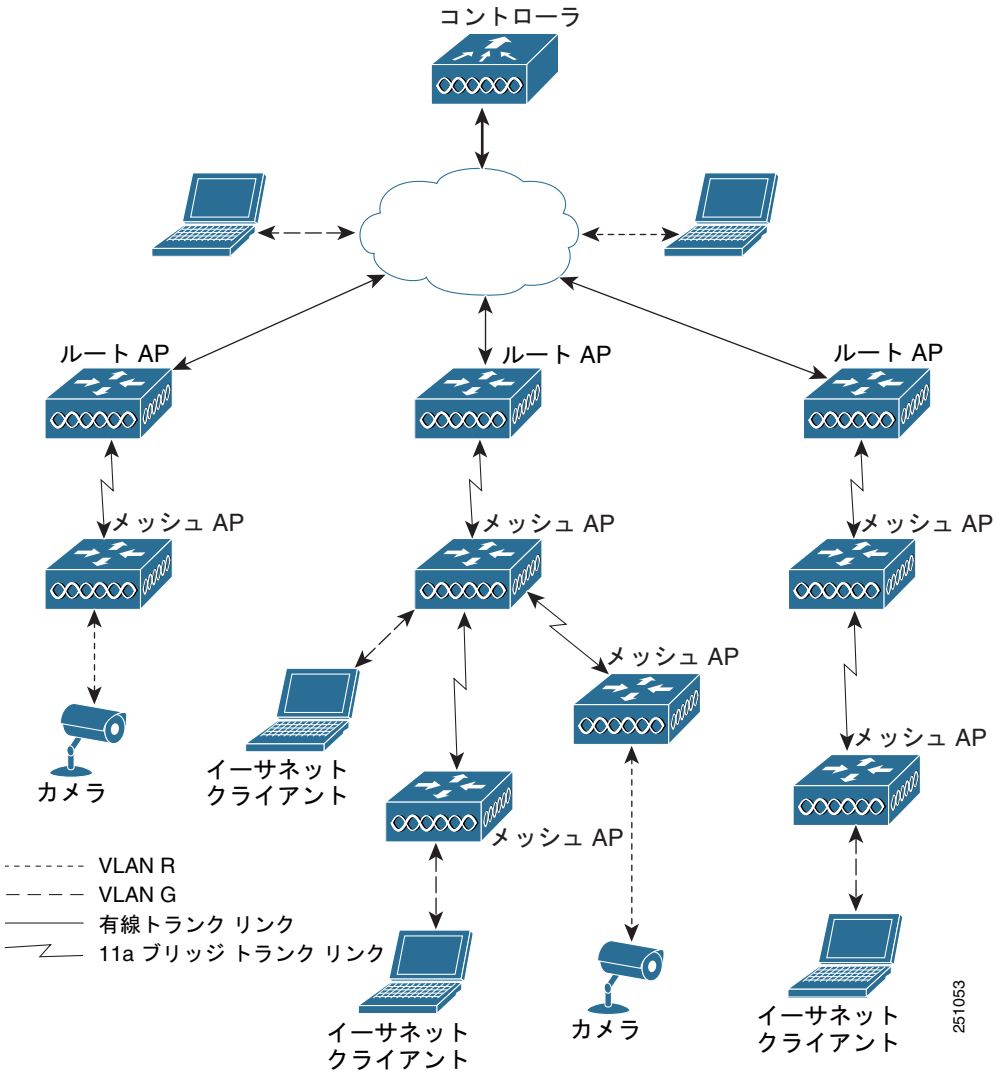
図 9-3　　ポイントツーマルチポイント ブリッジング



2. イーサネット VLAN タギングを使用すると、無線メッシュ ネットワーク内で特定のアプリケーション トラフィックをセグメント化して、有線 LAN に転送（ブリッジング）するか（アクセス モード）、別の無線メッシュ ネットワークにブリッジングすることができます（トランク モード）。

イーサネット VLAN タギングを使用した一般的な公共安全アクセス アプリケーションには、市内のさまざまな屋外の場所へのビデオ監視カメラの配置があります。これらのビデオ カメラはすべて MAP に有線で接続されています。さらに、これらのカメラのビデオはすべてワイヤレス バックホールを介して有線ネットワークにある中央の指令本部にストリーミングされます（図 9-4 を参照）。

図 9-4　　イーサネット VLAN タギング



イーサネット VLAN タギングのガイドライン

- セキュリティの理由で、メッシュ アクセス ポイント（RAP および MAP）にあるイーサネット ポートはデフォルトでは無効です。メッシュ アクセス ポイント ポートでイーサネット ブリッジングを設定すると、有効になります。
- イーサネット VLAN タギングが動作するためには、メッシュ ネットワークのすべてのアクセス ポイントでイーサネット ブリッジングを有効にする必要があります。
- VLAN モードは非 VLAN トランスペアレントに設定する必要があります（[global mesh] フィールド）。「イーサネット ブリッジングおよびイーサネット VLAN タギングの設定」（P.9-466）を参照してください。
  - VLAN トランスペアレントは、デフォルトで有効になっています。非 VLAN トランスペアレントとして設定するには、[Global Mesh Parameters] ページで [VLAN transparent] オプションを選択解除する必要があります。

- メッシュ アクセス ポイントの VLAN 設定が適用されるのは、すべてのアップリンク メッシュ アクセス ポイントがその VLAN をサポートできる場合だけです。
  - アップリンク アクセス ポインがその VLAN をサポートできない場合は、その設定は適用されるのではなく、格納されます。
- VLAN タギングはイーサネット インターフェイスでだけ設定できます。
  - 152x メッシュ アクセス ポイントでは、4 つのうち 3 つのポート（*ポート 0-PoE 入力*、*ポート 1-PoE 出力*、*およびポート 3 光ファイバ*）*をセカンダリ イーサネット インターフェイス*として使用します。*ポート 2 ケーブル*をセカンダリ イーサネット インターフェイスとして設定することはできません。
  - イーサネット VLAN タギングでは、RAP の*ポート 0-PoE 入力*は、有線ネットワークのスイッチのトランク ポートに接続します。MAP の*ポート 1-PoE 出力*は、ビデオ カメラなどの外部デバイスを接続します。
- バックホール インターフェイス（802.11a 無線）は、*プライマリ イーサネット インターフェイス*として機能します。バックホールはネットワーク内のトランクとして機能し、無線ネットワークと有線ネットワークとの間のすべての VLAN トラフィックを伝送します。プライマリ イーサネット インターフェイスを設定する必要はありません。
- RAP に接続されている有線ネットワークのスイッチ ポート（*ポート 0–PoE 入力*）は、トランク ポートでタグ付きパケットを許可するように設定する必要があります。RAP は、メッシュ ネットワークから受信したすべてのタグ付きパケットを有線ネットワークに転送します。
- 802.11a バックホール イーサネット インターフェイスで VLAN タギングをサポートするための設定は、メッシュ ネットワーク内では必要ありません。
  - これには RAP アップリンク イーサネット ポートが含まれます。登録メカニズムを使用して、必要な設定が自動的に行われます。
  - バックホールとして動作する 802.11a イーサネット リンクへの設定の変更はすべて無視され、警告が表示されます。イーサネット リンクがバックホールとして動作しなくなると、変更した設定が適用されます。
- 152x アクセス ポイントのポート 02 ケーブル モデム ポートでは VLAN を設定できません。ポート 0（PoE 入力）、1（PoE 出力）、および 3（光ファイバ）で VLAN を設定してください。
- 2 つの MAP 間でブリッジングする場合、ブリッジングする 2 つのアクセス ポイント間の距離（メッシュ範囲）を入力します。（MAP に接続されているトラフィックを RAP にアクセス モードで転送しているアプリケーションには該当しません）。
- 各セクタでは、最大 16 の VLAN がサポートされます。そのため、RAP の子（MAP）によってサポートされる VLAN の累計が 16 を超えることはできません。
- アクセス ポイントのイーサネット ポートは、イーサネット タギング展開内の*標準*ポート、*アクセス* ポート、または *トランク* ポートのいずれかとして機能します。
  - 通常モード：このモードでは、イーサネット インターフェイスはデフォルトで VLAN トランスペアレントであり、タグ付きパケットを送受信しません。クライアントからのタグ付きフレームは破棄されます。タグなしフレームは、RAP トランク ポート上のネイティブ VLAN に転送されます。
  - アクセス モード：このモードでは、タグなしパケットのみが許可されます。アクセス VLAN と呼ばれるユーザ設定の VLAN ですべてのパケットをタグ付けする必要があります。このモードが有効になるには、グローバル VLAN モードが非 VLAN 透過である必要があります。

    このオプションは、カメラや PC などの MAP に接続されているデバイスから情報を収集し、RAP に転送するアプリケーションに使用します。次に、RAP はタグを適用し、トラフィックを有線ネットワーク上のスイッチに転送します。

  - トランク モード : このモードでは、ユーザがネイティブ VLAN および許可された VLAN リストを設定する必要があります（デフォルトではありません）。このモードではタグ付きのパケットとタグなしパケットの両方が許可されます。タグなしパケットを許可し、ユーザ指定のネイティブ VLAN でそれらのパケットにタグ付けすることができます。許可される VLAN リスト内の VLAN でタグ付けされる場合はタグ付きパケットを許可できます。このモードが有効になるには、グローバル VLAN モードが非 VLAN 透過である必要があります。

    このオプションは、ブリッジング アプリケーションに使用します。たとえば、キャンパス内の別々のビルディングにある 2 つの MAP 間でトラフィックを転送する場合です。

- RAP に接続されるスイッチ ポートはトランクである必要があります。
  - スイッチのトランク ポートと RAP トランク ポートは一致している必要があります。
- MAP イーサネット ポートで設定した VLAN は、管理 VLAN として機能できません。
- RAP は常にスイッチのネイティブ VLAN（ID 1）に接続する必要があります。
  - RAP のプライマリ イーサネット インターフェイスはデフォルトではネイティブ VLAN 1 です。

イーサネット ブリッジングと VLAN タギングの有効化

RAP または MAP でイーサネット ブリッジングと VLAN タギングを有効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　イーサネット ブリッジングを有効にするメッシュ アクセス ポイントの名前をクリックします。アクセス ポイントの設定ページが表示されます。

ステップ 3　[Bridging Information] グループ ボックスで、[Data Rate] ドロップダウン リストから適切なバックホール レートを選択します。802.11a バックホール インターフェイスのデフォルト値は 24 Mbps です。

ステップ 4　[Bridging Information] セクションで、[Ethernet Bridging] ドロップダウン リストから [Enable] を選択します。

ステップ 5　適切なイーサネット インターフェイス リンク（[FastEthernet] や [gigabitEthernet1] など）をクリックします。

ステップ 6　[Ethernet interface] ページで、次のいずれかを実行します。

（注）　設定オプションは、VLAN モード（標準、アクセス、およびトランク）ごとに異なります。

a. MAP および RAP の標準ポートを設定するときに、[FastEthernet0] を選択した場合は、[VLAN Mode] ドロップダウン リストから [Normal] を選択します。

このモードでは、イーサネット インターフェイスはデフォルトで VLAN トランスペアレントであり、タグ付きパケットを送受信しません。クライアントからのタグ付きフレームは破棄されます。タグなしフレームは、RAP トランク ポート上のネイティブ VLAN に転送されます。

b. MAP アクセス ポートを設定するときに、[gigabitEthernet1]（ポート 1-PoE 出力）を選択した場合：

1. [VLAN Mode] ドロップダウン リストから [Access] を選択します。
2. VLAN ID を入力します。VLAN ID には 1 ～ 4095 の任意の値を入力できます。
3. [Save] をクリックします。

（注）　VLAN ID 1 はデフォルト VLAN として予約されていません。

（注）　RAP のすべての下位 MAP では、合計で最大 16 の VLAN がサポートされます。

c. RAP または MAP トランク ポートを設定し、[gigabitEthernet0]（または [FastEthernet0]）（ポート 0-PoE 入力）を選択した場合：

1. [VLAN Mode] ドロップダウン リストから [trunk] を選択します。
2. *incoming* トラフィックのネイティブ VLAN ID を入力します。ネイティブ VLAN ID には 1 ～ 4095 の任意の値を入力できます。ユーザ VLAN（アクセス）に割り当てた値を割り当てないでください。
3. *outgoing* トラフィックのトランク VLAN ID を入力して、[Add] をクリックします。

   追加されたトランクが許可される VLAN ID のサマリー列に表示されます。

   *タグなし*パケットを転送する場合は、デフォルトのトランク VLAN ID 値であるゼロを変更しないでください（MAP-to-MAP ブリッジング、キャンパス環境など）。

   *タグ付き*パケットを転送する場合、まだ割り当てられていない VLAN ID（1 ～ 4095）を入力します（RAP から有線ネットワークのスイッチなど）。

   （注）　リストから VLAN を削除するには、[Delete] をクリックします。

4. [Save] をクリックします。

   （注）　メッシュ ネットワークでは、少なくとも 1 つのメッシュ アクセス ポイントが [RootAP] に設定されている必要があります。

Autonomous から Lightweight への移行のサポート

Autonomous から Lightweight への移行サポート機能には、現在の Lightweight アクセス ポイントとともに Autonomous アクセス ポイントの基本的なモニタを実行できる共通のアプリケーションが備わっています。次の Autonomous アクセス ポイントがサポートされています。

- Cisco Aironet 1130 Access Point
- Cisco Aironet 1200 Access Point
- Cisco Aironet 1240 Access Point
- Cisco Aironet 1310 Bridge
- Cisco Aironet 1410 Bridge

Autonomous アクセス ポイントを Lightweight に変換するよう選択することもできます。アクセス ポイントを Lightweight に変換すると、アクセス ポイントの前のステータスまたは設定は保持されません。

Prime Infrastructure から、Autonomous アクセス ポイントを管理する際に次の機能を使用できます。

- 「Prime Infrastructure への Autonomous アクセス ポイントの追加」（P.9-471）

- 「Prime Infrastructure への Autonomous アクセス ポイントの表示」（P.9-475）
- [Monitor] > [Maps] ページからの Autonomous アクセス ポイントの追加および表示（詳しくは、「マップのモニタリング」（P.6-153）を参照してください）
- 関連付けられているアラームのモニタリング
- Autonomous アクセス ポイントのバックグラウンド タスクの実行
  - Prime Infrastructure によって管理される Autonomous アクセス ポイントのステータスを確認します。
  - 到達不能の Autonomous アクセス ポイントが検出された場合に、Critical アラームを生成します。
- Autonomous アクセス ポイントのレポートの実行
  - [Reports] > [Inventory Reports] および [Reports] > [Client Reports] > [Client Count] で詳細を確認します。
- 「Work Group Bridge（WGB）モードにおける Autonomous アクセス ポイントのサポート」（P.9-477）
- 「Autonomous アクセス ポイントの Lightweight アクセス ポイントへの移行」（P.11-750）

Prime Infrastructure への Autonomous アクセス ポイントの追加

Prime Infrastructure から、Autonomous アクセス ポイントを追加するには、次の方法を使用できます。

- 「デバイス情報による Autonomous アクセス ポイントの追加」（P.9-471）（IP アドレスとクレデンシャル）。
- 「CSV ファイルによる Autonomous アクセス ポイントの追加」（P.9-472）
- 「Autonomous アクセス ポイントの削除」（P.9-475）

デバイス情報による Autonomous アクセス ポイントの追加

デバイス情報によって Autonomous アクセス ポイントを Prime Infrastructure に追加するには、カンマ区切りの IP アドレスとクレデンシャルを使用します。

デバイス情報を使用して Autonomous アクセス ポイントを追加する手順は、次のとおりです。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Autonomous APs] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[Add Format Type] ドロップダウン リストから [Device Info] を選択します。

ステップ 5　Autonomous アクセス ポイントのカンマ区切り IP アドレスを入力します。

ステップ 6　次の [SNMP Parameters] パラメータを入力します。

- [Version]：[v1]、[v2]、または [v3] から選択します。
- [Retries]：コントローラの検出試行回数を示します。
- [Timeout]：プロセスがタイムアウトになるまでに許可される時間（秒単位）を示します。有効な範囲は 2 ～ 90 秒です。デフォルトは 10 秒です。
- [Community]：[Public] または [Private]。

ステップ 7　次の Telnet/SSH パラメータを入力します。

（注）　Telnet/SSH パラメータが空白のままの場合は、デフォルト値が使用されます。

- [Protocol]：使用するプロトコルを選択します（[Telenet] または [SSH] のいずれか）。
- [User Name]：ユーザ名を入力します。（デフォルトのユーザ名は admin です）。

（注）　Telnet/SSH のユーザ名は、CLI テンプレートでコマンドを実行するために十分な権限を持っている必要があります。

- [Password]/[Confirm Password]：パスワードを入力して、確認します。（デフォルトのパスワードは admin です）。
- [Enable Password]/[Confirm Password]：イネーブル パスワードを入力して、確認します。
- [Telnet Timeout]：プロセスがタイムアウトになるまでに許可される時間（秒単位）を示します。デフォルトは 60 秒です。

（注）　AAP Download Software タスクを実行する前に、最大 Telnet/SSH のタイムアウト値を設定する必要があります。

（注）　Cisco Autonomous アクセス ポイントには、工場出荷時にデフォルトのイネーブル パスワード *Cisco* が設定されています。ユーザはこのパスワードを使用して、非特権モードにログインし、show および debug コマンドを実行することができますが、これはセキュリティに対する脅威となります。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートからコンフィギュレーション コマンドを実行できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

ステップ 8　[Add] をクリックします。

（注）　AP を追加して、インベントリ収集が完了すると、[Access Point] リスト ページ（[Configure] > [Access Points]）に表示されます。[Access Points] リストにない場合は、[Configure] > [Unknown Device] ページを選択して、ステータスを確認します。詳細については、「不明デバイスの設定」（P.9-510）を参照してください。

（注）　Autonomous アクセス ポイントは、ライセンスの合計デバイス数に含まれません。

CSV ファイルによる Autonomous アクセス ポイントの追加

Autonomous アクセス ポイントを Prime Infrastructure に追加するには、WLSE からエクスポートした CSV ファイルを使用します。

CSV ファイルを使用して Autonomous アクセス ポイントを追加する手順は、次のとおりです。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Autonomous APs] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[Add Format Type] ドロップダウン リストから [File] を選択します。

ステップ 5　該当する CSV ファイルを入力するか、参照して選択します。

次に、V2 デバイス用の CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,,3,4,Cisco,Cisco,2,10
```

（注）　SNMP、telnet、または SSH クレデンシャルは必須です。

次に、V3 デバイス用の CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

CSV ファイルには、次のフィールドを含めることができます。

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

ステップ 6　[OK] をクリックします。

Autonomous アクセス ポイントの一括更新

CSV ファイルをインポートすることで、複数の Autonomous アクセス ポイントのクレデンシャルを更新できます。

Autonomous アクセス ポイント情報を一括で更新するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　該当するコントローラのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Bulk Update APs] を選択します。[Bulk Update Autonomous Access Points] ページが表示されます。

ステップ 4　[Choose File] をクリックして CSV ファイルを選択し、インポートする CSV ファイルの場所を見つけます。

ステップ 5　[Update and Sync] をクリックします。

Autonomous アクセス ポイントの一括更新用の CSV ファイルの例

次に、V2 デバイス用の CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries, snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,,3,4,Cisco,Cisco,2,10
```

（注）　SNMP、telnet、または SSH クレデンシャルは必須です。

次に、V3 デバイス用の CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.224,v3,default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2
,10
```

CSV ファイルには、次のフィールドを含めることができます。

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries

- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Autonomous アクセス ポイントの削除

（注） 何らかの理由により、Autonomous アクセス ポイントを交換する場合は、代替のアクセス ポイントをネットワークにインストールする前に Prime Infrastructure から Autonomous アクセス ポイントを削除します。

Prime Infrastructure から Autonomous アクセス ポイントを削除するには、次の手順を実行します。

ステップ 1　削除するアクセス ポイントのチェックボックスを選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Remove APs] を選択します。

Prime Infrastructure への Autonomous アクセス ポイントの表示

Autonomous アクセス ポイントが追加されると、[Monitor] > [Access Points] ページに表示されます。

Autonomous アクセス ポイントをクリックすると、次のような詳細が表示されます。

- アクセス ポイントの操作ステータス
- 無線情報、チャネル、電力、無線上のクライアント数などの主要な属性
- CDP 近隣情報

Autonomous アクセス ポイントは、[Monitor] > [Maps] でも表示できます。

Autonomous アクセス ポイントをフロア領域に追加するには、[Monitor Maps] > [*floor area*] を選択して、[Select a command] ドロップダウン リストから [Add Access Points] を選択します。

Autonomous アクセス ポイントへのイメージのダウンロード（TFTP）

Lightweight アクセス ポイント イメージは、コントローラ イメージにバンドルされており、コントローラによって管理されます。Autonomous アクセス ポイント イメージは、WLSE、CiscoWorks、または Prime Infrastructure などの NMS システムで処理する必要があります。

（注） AAP Download Software タスクを実行する前に、最大 Telnet/SSH のタイムアウト値を設定する必要があります。

TFTP を使用してイメージを Autonomous アクセス ポイントにダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　イメージをダウンロードする Autonomous アクセス ポイントのチェックボックスを選択します。[AP Type] 列には、Autonomous と Lightweight のいずれのアクセス ポイントであるかが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Download Autonomous AP Image (TFTP)] を選択します。[Download images to Autonomous APs] ページが表示されます。

ステップ 4　次のパラメータを設定します。

- [File is located on] : [Local machine] または [TFTP server] を選択します。
- [Server Name] : デフォルト サーバを選択するか、[Server Name] ドロップダウン リストから新しいサーバを追加します。
- [IP address] : TFTP サーバの IP アドレスを指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- [Prime Infrastructure Server Files In] : Prime Infrastructure サーバ ファイルのある場所を指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- [Server File Name] : サーバ ファイル名を指定します。

ステップ 5　[Download] をクリックします。

ヒント　一部の TFTP サーバでは、32 MB を超えるファイルはサポートされません。

Autonomous アクセス ポイントへのイメージのダウンロード（FTP）

（FTP を使用して）イメージを Autonomous アクセス ポイントにダウンロードするには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　イメージをダウンロードする Autonomous アクセス ポイントのチェックボックスを選択します。[AP Type] 列には、Autonomous と Lightweight のいずれのアクセス ポイントであるかが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Download Autonomous AP Image (FTP)] を選択します。[Download images to Autonomous APs] ページが表示されます。

ステップ 4　ユーザ名とパスワードを含む FTP クレデンシャルを入力します。

ステップ 5　次のパラメータを設定します。

- [File is located on] : [Local machine] または [FTP server] を選択します。
- [Server Name] : デフォルト サーバを選択するか、[Server Name] ドロップダウン リストから新しいサーバを追加します。
- [IP address] : FTP サーバの IP アドレスを指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- [Prime Infrastructure Server Files In] : Prime Infrastructure サーバ ファイルのある場所を指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- [Server File Name] : サーバ ファイル名を指定します。

ステップ 6　[Download] をクリックします。

Work Group Bridge（WGB）モードにおける Autonomous アクセス ポイントのサポート

Workgroup Bridge（WGB）モードは、Autonomous アクセス ポイントがワイヤレス クライアントとして機能して、Lightweight アクセス ポイントに接続する特殊なモードです。AP モードが [Bridge] に設定され、アクセス ポイントがブリッジ対応である場合、WGB とその有線クライアントは、Prime Infrastructure にクライアントとしてリストされます。

WGB であるすべての Prime Infrastructure クライアントのリストを表示するには、[Monitor] > [Clients] を選択します。[Show] ドロップダウン リストから [WGB Clients] を選択して、[Go] をクリックします。[Clients (detected as WGBs)] ページが表示されます。ユーザをクリックして、特定の WGB とその有線クライアントに関する詳細な情報を表示します。

（注）　Prime Infrastructure は、Autonomous アクセス ポイントが Prime Infrastructure によって管理されているかどうかにかかわらず、Autonomous アクセス ポイントの WGB クライアント情報を提供します。WGB アクセス ポイントも Prime Infrastructure によって管理されている場合、Prime Infrastructure は他の Autonomous アクセス ポイントに類似したアクセス ポイントに対する基本的なモニタリング機能を提供します。

アクセス ポイントの詳細の設定

[Configure] > [Access Points] の順に選択して、Prime Infrastructure データベース内のすべてのアクセス ポイントのサマリーを表示します。表示されるサマリー情報は、次のとおりです。

- イーサネット MAC
- IP アドレス
- 無線
- マップ ロケーション
- AP タイプ
- コントローラ
- オペレーション ステータス
- アラーム ステータス
- 監査ステータス

（注）　マウス カーソルを監査ステータスの値の上に置くと、最新監査の時刻が表示されます。

（注）　AP 設定テンプレートの設定の詳細については、「AP 設定テンプレートの設定」（P.11-736）を参照してください。

（注）　[AP Mode]、[Channel Width]、[Client Count] などの列の追加、削除、または並べ替えを行うには、[Edit View] リンクをクリックします。詳細については、「検索結果の表示（[Edit View]）の設定」（P.2-68）を参照してください。

ステップ 1　[AP Name] 列のリンクをクリックして、そのアクセス ポイント名についての詳細情報を表示します。[Access Point Detail] ページが表示されます。

（注）　オペレーティング システムのソフトウェアによってアクセス ポイントが自動的に検出され、Prime Infrastructure データベース内の既存のコントローラに関連付けられると Prime Infrastructure データベースに追加されます。

（注）　[Access point] パラメータは、アクセス ポイント タイプによって異なることがあります。

ページの一部のパラメータは、自動的に入力されます。

- [General] グループ ボックスには、イーサネット MAC、ベース無線 MAC、IP アドレス、およびステータスが表示されます。
- このページの [Versions] グループ ボックスには、ソフトウェアおよびブート バージョンが表示されます。
- [Inventory Information] グループ ボックスには、モデル、AP タイプ、AP 証明書タイプ、シリアル番号、および REAP モード サポートが表示されます。
- [Ethernet Interfaces] グループ ボックスには、インターフェイス名、スロット ID、管理ステータス、および CDP ステートなどの情報が表示されます。
- [Radio Interfaces] グループ ボックスには、管理ステータス、チャネル番号、電力レベル、アンテナ モード、アンテナ ダイバーシティ、アンテナの種類など、802.11a/n、802.11b/g/n 無線、および 802.11a/b/g/n の現在のステータスが表示されます。

設定可能なパラメータを設定するには、次の手順を実行します。

（注）　アクセス ポイントのパラメータを変更すると、アクセス ポイントが一時的に無効になり、これによって一部のクライアントで接続が失われる可能性があります。

ステップ 2　アクセス ポイントに割り当てられた名前を入力します。

ステップ 3　ドロップダウン リストを使用して国コードを選択して、複数国のサポートを設定します。アクセス ポイントは、さまざまな規制要件を持つ多くの国で使用できるように設計されています。国の規制にアクセス ポイントが準拠するように国コードを設定できます。国コードを設定する際には、次の内容を考慮してください。

- コントローラごとに 20 までの国を設定できます。
- 自動 RF エンジンが 1 つと、使用可能なチャネルの一覧が 1 つしか存在しないため、複数国の設定は、共通チャネル内で自動 RF が使用できるチャネルに制限されます。共通チャネルとは、設定したすべての国において合法的なものです。
- 複数の国用にアクセス ポイントを設定する場合は、自動 RF チャネルは、設定したすべての国で使用できる最も高い電力レベルに制限されます。特定のアクセス ポイントはこれらの制限を超えるよう設定される場合があります（または、これらの制限を超えるレベルを手動で設定する場合があります）。ただし、自動 RF が自動で共通チャネル以外を選択することや、すべての国で使用できるレベルを超えた電力レベルに上げることはありません。

（注）　運用する国向けに設計されていない場合、アクセス ポイントは正しく動作しない可能性があります。たとえば、（-A）米国規制区域に含まれる部分番号 AIR-AP1030-A-K9 のアクセス ポイントは、ヨーロッパ（-E）では使用できません。必ず、自国の規制ドメインに合ったアクセス ポイントを購入してください。製品ごとにサポートされる国コードの完全なリストについては、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html。

ステップ 4　管理目的でアクセス ポイントを有効にする場合は、[Enable] チェックボックスを選択します。

ステップ 5　[AP Static IP] チェックボックスの [Enable] をクリックする場合は、リブート時に動的に IP アドレスを取得するのではなく、常にスタティック IP アドレスがアクセス ポイントに割り当てられます。

ステップ 6　[AP Mode] ドロップダウン リストから、アクセス ポイントのロールを選択します。モニタ モードを選択した場合を*除き*、モードの変更後にリブートする必要はありません。[Save] をクリックすると、リブートに関するメッセージが表示されます。使用できるモードは、次のとおりです。

- [Local]：これがアクセス ポイントの通常動作であり、[AP Mode] のデフォルト値です。このモードでは、設定したチャネルをスキャンしてノイズと不正を探す間、データ クライアントが提供されます。アクセス ポイントは 50 ミリ秒間、チャネルの不正をリッスンします。Auto RF 設定の下で指定された期間の間、各チャネルを巡回します。

  [AP Sub Mode]：AP モードが [Local] に設定されている場合、[WIPS] に [AP Sub Mode] を設定できます。

- [FlexConnect]：最大 6 個のアクセス ポイントに対して FlexConnect を有効にするには、[AP Mode] ドロップダウン リストから [FlexConnect] を選択します。FlexConnect アクセス ポイントは、クライアント データ トラフィックをローカルで切り替えて、コントローラへの接続が失われるとクライアント認証をローカルで実行できます。

  （注）　Cisco 適応型 wIPS 機能用にローカルまたは FlexConnect アクセス ポイントを設定するには、[Local] または [FlexConnect] を選択して、[Enhanced wIPS Engine Enabled] チェックボックスを選択します。

  [AP Sub Mode]：AP モードが [FlexConnect] に設定されている場合、[AP Sub Mode] を次のいずれかに設定できます。

  - WIPS
  - [PPPOE]：アクセス ポイント上での Point-to-Point Protocol over Ethernet（PPPoE）サブモードを設定します。
  - [PPPOE-WIPS]：アクセス ポイント上での Point-to-Point Protocol over Ethernet（PPPoE）サブモードと wIPS サブモードの両方を設定します。

- [Monitor]：これは無線受信のみのモードであり、設定したすべてのチャネルをアクセス ポイントが 12 秒ごとにスキャンできるようになります。このように設定されたアクセス ポイントのある空間では認証解除のパケットだけが送信されます。モニタ モードのアクセス ポイントは不正を検出しますが、RLDP パケットの送信準備のために不審なものにクライアントとしては接続できません。

  [AP Sub Mode]：AP モードが [Monitor] に設定されている場合、[AP Sub Mode] を [WIPS] に設定できます。

（注）　トラッキング最適化モニタ モード（TOMM）機能を有効にすることで、タグのモニタ モードを拡張して、位置計算を追加できます。TOMM を有効にするときは、アクセス ポイントの 2.4 GHz 帯（802.11b/g 無線）内で、4 つのうちいずれかチャネルを使用してタグをモニタするかを指定できます。これによって、ネットワーク内でこれまでにタグが検出されたチャネルだけを対象にチャネル スキャンを実行できます（チャネル 1、チャネル 6、チャネル 11 など）。TOMM を有効にするには、アクセス ポイントの 802.11b/g 無線をさらに編集する必要があります。設定の詳細については、「Tracking Optimized Monitor Mode を使用するためのアクセス ポイント無線の設定」（P.9-494）を参照してください。

（注）　TOMM と wIPS の両方を同時に有効にすることはできません。TOMM は、wIPS が無効の場合のみ有効にできます。

（注）　Cisco 適応型 wIPS 機能用にアクセス ポイントを設定するには、[Monitor] を選択して、[Enhanced wIPS Engine Enabled] チェックボックスを選択し、[Monitor Mode Optimization] ドロップダウン リストから [wIPS] を選択します。

- [Rogue Detector]：このモードでは、アクセス ポイントの無線がオフに切り替わり、アクセス ポイントは有線トラフィックのみをリッスンします。このモードで動作するコントローラは、不正アクセス ポイントをモニタします。コントローラはすべての不正アクセス ポイントとクライアントの MAC アドレスのリストを不正検出器に送信して、不正検出器がこの情報を WLC に転送します。MAC アドレスの一覧は、WLC アクセス ポイントが予測した内容と比較されます。MAC アドレスが一致する場合は、どの不正アクセス ポイントが有線ネットワークに接続されるかを判別できます。
- [Sniffer]：スニファ モードで動作し、アクセス ポイントは特定チャネル上のすべてのパケットを取得して、Airopeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。この機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合のみ有効にできます。AiroPeek の詳細については、次の URL を参照してください。www.wildpackets.com。
- [Bridge]：ブリッジ モードは、Autonomous アクセス ポイントがワイヤレス クライアントとして機能して、Lightweight アクセス ポイントに接続する特殊なモードです。AP モードが [Bridge] に設定され、アクセス ポイントがブリッジ対応である場合、ブリッジとその有線クライアントは、Prime Infrastructure にクライアントとしてリストされます。
- [SE-Connect]：このモードでは、CleanAir 対応のアクセス ポイントをすべてのモニタ対象チャネルでの干渉検出に広く使用できます。IDS スキャンや Wi-Fi などのその他の機能はすべて一時停止されます。

（注）　このオプションは、アクセス ポイントが CleanAir 対応の場合のみ表示されます。

（注）　AP モードを変更すると、アクセス ポイントがリブートします。

ステップ 7　アクセス ポイント無線をすべて無効にします。

ステップ 8　[AP Failover Priority] ドロップダウン リストから、アクセス ポイントのフェールオーバー優先度を示す [Low]、[Medium]、[High]、または [Critical] を選択します。デフォルトの優先度は [Low] です。詳細については、「AP フェールオーバー優先度の設定」（P.9-464）を参照してください。

ステップ 9　[Primary Controller] フィールド、[Secondary Controller] フィールド、および [Tertiary Controller] フィールドで、アクセスするコントローラの順序を定義できます。

ステップ 10　[AP Group Name] ドロップダウン メニューには、[WLANs] > [AP Group VLANs] を使用して定義されているすべてのアクセス ポイント グループ名が表示されます。また、このアクセス ポイントをいずれかのグループに関連付けるかどうかを指定できます。

（注）　4.2.132.0 および 5.0.159.0 よりも前のバージョンの WLC では、アクセス ポイント グループ名は 31 文字までです。

ステップ 11　アクセス ポイントが配置されている物理位置の説明を入力します。

ステップ 12　[Stats Collection Period] フィールドには、アクセス ポイントが .11 の統計をコントローラに送信する時間を入力します。有効範囲は 0 ～ 65535 秒です。値 0 は統計を送信しないことを意味します。

ステップ 13　単一のクライアント デバイスまたはアクセス ポイントで発信されるか終了するすべてのトラフィックを（別のポートに）複製する場合は、[Mirror Mode] に [Enable] を選択します。ミラー モードは特定のネットワーク問題を診断する際には役立ちますが、このポートへの接続には反応しなくなるため、使用されていないポートだけで有効にする必要があります。

ステップ 14　コントローラ上でグローバルに管理フレーム保護（MFP）を設定できます。その場合、管理フレームの保護と検証は、接続している各アクセス ポイントに対してデフォルトで有効になります。また、アクセス ポイント認証は自動で無効になります。MFP をコントローラ上でグローバルに有効にした後は、個々の WLAN とアクセス ポイントに対してそれを無効にすることや再度有効にすることができます。

クリックして MFP Frame Validation を有効にする場合は、次の 3 つの主要な機能が実行されます。

- 管理フレーム保護：管理フレーム保護を有効にすると、アクセス ポイントはメッセージ整合性チェック情報要素（MIC IE）を各フレームに追加することにより、送信する管理フレームを保護します。フレームのコピー、変更、または再生を試みると、MIC が整合性チェックに失敗し、MFP フレームを検出するように設定された受信アクセス ポイントはその矛盾を報告します。
- 管理フレーム検証：管理フレーム検証を有効にすると、アクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。発信側が MFP フレームを送信するよう設定されている場合、MIC IE が存在し、管理フレームの中身が一致していることを確認できます。正当な MIC IE が含まれていないフレームを受信した場合は、その矛盾がネットワーク管理システムに報告されます。この矛盾を報告するには、アクセス ポイントは MFP フレームを送信するように設定されている必要があります。同様に、タイムスタンプが適切に機能するには、すべてのコントローラでネットワーク タイム プロトコル（NTP）が同期されている必要があります。
- イベント報告：アクセス ポイントは異常を検出するとコントローラに通知し、コントローラは受信した異常イベントを集積して、ネットワーク マネージャに警告するために SNMP トラップ経由で結果を報告します。

ステップ 15　CDP を有効にするには、[Cisco Discovery Protocol] チェックボックスを選択します。CDP は、シスコで製造されたルータ、ブリッジ、通信サーバなどのすべての機器で実行されるデバイス検出プロトコルです。各デバイスは、隣接デバイスについて知るために、マルチキャスト アドレスに定期メッセージを送信して、他のデバイスが送信したメッセージをリッスンします。デバイスの起動時には、要求した電力が供給されるように、デバイスがインライン パワーに対応するかどうかを指定する CDP パケットを送信します。

（注）　アクセス ポイント パラメータを変更すると、一時的にアクセス ポイントが無効になり、いくつかのクライアントへの接続を失う場合があります。

ステップ 16　不正検出を有効にするには、チェックボックスを選択します。

（注）　家庭環境に導入されるアクセス ポイントは、多数の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出は自動的に無効にされます。OfficeExtend アクセス ポイントの詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

ステップ 17　暗号化を有効にするには、[Encryption] チェックボックスを選択します。

（注）　暗号化機能を有効または無効にすると、アクセス ポイントがリブートし、クライアントは接続を失います。

（注）　DTLS データ暗号化は、セキュリティを維持するために OfficeExtend アクセス ポイントに対しては自動的に有効になりますが、他のすべてのアクセス ポイントに対してはデフォルトで無効になります。

（注）　Cisco 5500 コントローラは、AS_5500_LDPE_x_x_x_x.aes または AS_5500_x_x_x_x.aes の 2 つのタイプのイメージのうちの 1 つとともにロードできます。以前のイメージとともにロードされる 5500 コントローラの場合は、暗号化を示すために DTLS ライセンスが必要です。

（注）　WiSM2 および 2500 コントローラでは、暗号化を示すために DTLS ライセンスは必須です。

ステップ 18　不正検出を有効にすると、アクセス ポイントの無線がオフに切り替わり、アクセス ポイントは有線トラフィックのみをリッスンします。このモードで動作するコントローラは、不正アクセス ポイントをモニタします。コントローラはすべての不正アクセス ポイントとクライアントの MAC アドレスのリストを不正検出器に送信して、不正検出器がこの情報を WLC に転送します。MAC アドレスの一覧は、WLC アクセス ポイントが予測した内容と比較されます。MAC アドレスが一致する場合は、どの不正アクセス ポイントが有線ネットワークに接続されるかを判別できます。

ステップ 19　SSH アクセスを有効にするには、[SSH Access] チェックボックスを選択します。

ステップ 20　Telnet アクセスを有効にするには、[Telnet Access] チェックボックスを選択します。

（注）　OfficeExtend アクセス ポイントは、デフォルトのパスワードがアクセス ポイントで使用されている場合に外部アクセスを許可する WAN に直接接続されていることがあります。そのため、Telnet および SSH アクセスは、OfficeExtend アクセス ポイントに対しては自動的に無効になります。

ステップ 21　[AP LED] チェックボックスをオンにして、アクセス ポイントの LED を有効にします。多くの AP が導入されていて、特定の AP を指定する場合、すべての AP の LED を無効にしてから検索する AP の LED を有効にできます。これによって、LED が有効になっている AP が簡単に識別できます。

ステップ 22　このアクセス ポイントについてクレデンシャルを上書きする場合は、[Override Global Username Password] チェックボックスを選択します。その後、このアクセス ポイントで割り当てる新しいサプリカント AP ユーザ名、AP パスワード、およびイネーブル パスワードを入力できます。

（注）　[System] > [AP Username Password] ページでは、コントローラへの接続時に継承するすべてのアクセス ポイントのグローバル クレデンシャルを設定できます。設定したこれらのクレデンシャルは、[AP Parameters] タブ ページの右下に表示されます。

入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。

ステップ 23　[Enable Link Latency] チェックボックスを選択して、このアクセス ポイントのリンク遅延を有効にするか、または選択解除して、エコー応答受信ごとにアクセス ポイントがコントローラにラウンドトリップ時間を送信しないようにします。リンク遅延の詳細については、「アクセス ポイントのリンク遅延の設定」（P.9-514）を参照してください。

ステップ 24　コントローラに直接アクセスする必要なく、Prime Infrastructure からパワー インジェクタ設定を操作できるようになりました。先行標準またはパワー インジェクタ ステートを有効にするには、[Power Over Ethernet Settings] セクションでチェックボックスを選択します。

アクセス ポイントが高性能のシスコ スイッチによって電力供給される場合は、[Pre-standard] が選択されます。それ以外の場合は、無効にされます。パワー インジェクタのステートを選択すると、[power injector] オプションが表示されます。可能な値がインストールまたは上書きされます。上書きを選択した場合は、MAC アドレスを入力するか、WLC によって指定されるよう空のままにできます。

（注）　Prime Infrastructure を実行している電源を判別するには、[Monitor] > [Access Points] を選択して、[Edit View] をクリックし、[POE Status] を選択して [View Information] ボックスに移動します。[Submit] のクリック後に、POE ステータスが最後の列に表示されます。デバイスがインジェクタによって電源供給される場合は、POE ステータスは [Not Applicable] と表示されます。

ステップ 25　次の FlexConnect 設定を有効にするには、[Enable] チェックボックスを選択します。

（注）　アクセス ポイントが有効の場合、FlexConnect 設定は変更できません。

- [OfficeExtend AP]：デフォルトは [Enabled] です。

  （注）　このチェックボックスを選択解除すると、単にこのアクセス ポイントの OfficeExtend モードが無効になります。アクセス ポイントでのすべての設定が取り消されることはありませんが、アクセス ポイントがリモートで配置される状態になるため、危険にさらされます。アクセス ポイントの設定をクリアして、工場出荷時のデフォルト設定に戻すには、[access point details] ページの下部にある [Clear Config] をクリックします。アクセス ポイントの個人 SSID のみをクリアする場合は、アクセス ポイント詳細ページ下部にある [Reset Personal SSID] をクリックします。

[Enabled for the OfficeExtend AP] を選択すると、警告メッセージによって次の情報が提供されます。

- 自動的に発生した設定変更。[Encryption] と [Link Latency] は有効です。[Rogue Detection]、[SSH Access]、および [Telnet Access] は無効です。
- 少なくとも 1 つのプライマリ、セカンダリ、およびターシャリ コントローラ（名前と IP アドレスを含む）を設定するよう求めるリマインダ。

（注）　通常、アクセス ポイントは追加するプライマリ コントローラを最初に検索します。その後、コントローラはセカンダリを試行し、次にターシャリ コントローラを試行します。これらのどのコントローラも設定されていない場合、アクセス ポイントは、見つかったどのコントローラでも追加しようとして、デフォルトのディスカバリ モードに切り替えます。

OfficeExtend アクセス ポイントは、追加するプライマリ、セカンダリ、またはターシャリ コントローラのみを検索します。設定されているコントローラについてこれ以上の検索は行いません。このため、少なくとも 1 つのプライマリ、セカンダリ、またはターシャリ コントローラの名前と IP アドレスを設定することが重要です。

  - 暗号化を有効にする警告によって、アクセス ポイントがリブートされ、クライアントは接続を失います。

- [Least Latency Controller Join] : 有効にすると、アクセス ポイントは、優先度順の検索（プライマリ、セカンダリ、次にターシャリ コントローラ）から、遅延測定が最善（最短の遅延）のコントローラの検索に切り替えます。遅延が最短のコントローラが、最善のパフォーマンスを提供します。

（注）　アクセス ポイントは、コントローラを初めて追加したときにこの検索を一度のみ実行します。追加後は、測定が変更されたかどうかを確認するために、プライマリ、セカンダリ、およびターシャリ コントローラの遅延測定を再計算しません。

- [VLAN Support] : 選択する場合は、ネイティブ VLAN ID を入力します。

  [Enable VLAN] が選択されると、Prime Infrastructure は WLAN-VLAN マッピングを表示します。WLAN ID にマップされた VLAN ID のみを編集できます。
- [WLAN-VLAN Mapping] : [WLAN-VLAN Mapping] ダイアログ ボックスにアクセスするには、このリンクをクリックします。ここから、WLAN-VLAN マッピングを編集できます。WLAN プロファイル名を選択し、[Edit] をクリックします。
  - [WLAN Profile Name] : WLAN プロファイル名を示します。
  - [VLAN ID] : VLAN の ID 番号を指定できます。
  - [Inheritance Type] : グループ固有、WLAN 固有、または AP 固有などの継承タイプを示します。マッピングが FlexConnect グループに追加されると、継承タイプはグループ固有に表示されます。マッピングが FlexConnect グループに追加されると、継承タイプは WLAN- 固有に表示されます。

    AP 固有に継承タイプを変更するには、WLAN プロファイルを選択し、次に [Make AP specific] をクリックします。

    グループ固有に継承タイプを変更するには、WLAN プロファイルを選択し、次に [Remove AP specific] をクリックします。
- [AP level VLAN ACL Mapping] : このグループ ボックスは、VLAN サポートが有効にされた FlexConnect モードのアクセス ポイントのみで表示されます。VLAN ID にマップされた入力および出力 ACL のみを編集できます。

（注）　Prime Infrastructure で入力した VLAN ID が、関連付けられたコントローラのアクセス ポイントの [AP Level VLAN ACL Mapping] セクションで使用可能な場合のみ、[AP level VLAN ACL Mapping] 設定がアクセス ポイントに適用されます。

- [Group level VLAN ACL Mapping]：このグループ ボックスは、VLAN サポートが有効にされた FlexConnect モードのアクセス ポイントのみで表示されます。FlexConnect ACL グループの [ACL] タブで指定したグループ レベルの VLAN ACL マッピングを表示できます。
- PreAuthentication ACL Mappings
  - [Web-Authentication and Web-Policy ACLs]：WebAuth および Web ポリシー ACL マッピングをアクセス ポイント レベルで表示するには、[External WebAuthentication ACLs] リンクをクリックします。[ACL Mappings] ページには、WLAN ACL マッピングおよび Web ポリシー ACL の詳細が一覧表示されます。

ステップ 26　[Role] ドロップダウン リストからメッシュ アクセス ポイントのロールを選択します。デフォルトの設定は MAP です。

（注）　メッシュ ネットワークのアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）として機能します。

ステップ 27　アクセス ポイントが属するブリッジ グループの名前を入力します。名前には最大 10 文字が使用できます。

（注）　ブリッジ グループは、メッシュ アクセス ポイントを論理的にグループ化して、同一チャネル上の 2 つのネットワークが互いに通信しないようにするために使用されます。

（注）　メッシュ アクセス ポイントが通信するためには、同じブリッジ グループ名が付いている必要があります。

（注）　複数の RAP を使用する設定の場合は、ある RAP から別の RAP へフェールオーバーできるように、すべての RAP に同じブリッジ グループ名が付いていることを確認してください。

（注）　別々のセクタが必要な設定の場合は、各 RAP およびそれがアソシエートしている MAP に別々のブリッジ グループ名が付いていることを確認してください。

[Type] フィールドには、メッシュ アクセス ポイントの種類（屋内または屋外）が表示されます。[Backhaul Interface] フィールドには、アクセス ポイントのバックホールとして使用されているアクセス ポイントの無線が表示されます。

ステップ 28　ドロップダウン リストから、バックホール インターフェイスのデータ レートを選択します。使用可能なデータ レートは、バックホール インターフェイスによって指示されます。デフォルトのレートは 18Mbps です。

（注）　このデータ レートは、メッシュ アクセス ポイント間で共有され、メッシュ ネットワーク全体に対して固定されます。

（注）　展開したメッシュ ネットワーク ソリューションに対してデータ レートを変更しないでください。

ステップ 29　[Ethernet Bridging] ドロップダウン リストから [Enable] を選択し、メッシュ アクセス ポイントに対してイーサネット ブリッジを有効にします。

ステップ 30　[Save] をクリックして、設定を保存します。

ステップ 31　アクセス ポイントの無線を再度有効にします。

ステップ 32　このアクセス ポイントをリセットする必要がある場合は、[Reset AP Now] をクリックします。

ステップ 33　OfficeExtend アクセス ポイントの個人 SSID を工場出荷時のデフォルト設定にリセットするには、[Reset Personal SSID] をクリックします。

ステップ 34　アクセス ポイントの設定をクリアする必要がある場合や、すべての値を工場出荷時のデフォルト設定にリセットする必要がある場合は、[Clear Config] をクリックします。

イーサネット インターフェイスの設定

（注）　152x メッシュ アクセス ポイントは、ポート 0-PoE 入力、ポート 1-PoE 出力、ポート 2 ケーブル、およびポート 3 光ファイバの 4 つのポートのうちのいずれか 1 つで設定されます。その他の AP（1130、1140、1240、1250 など）はポート 2 ケーブルで設定されます。

イーサネット インターフェイスを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[AP Name] の下のリンクをクリックして、そのアクセス ポイント名についての詳細情報を表示します。[Access Point Detail] ページが表示されます。

（注）　[Access Point Details] ページに、イーサネット インターフェイスのリストが表示されます。

ステップ 3　[Interface] の下のリンクをクリックすると、そのインターフェイスに関する詳細情報が表示されます。[Ethernet Interface] ページが表示されます。

このページには、次のパラメータが表示されます。

- [AP Name] : アクセス ポイントの名前。
- [Slot Id] : スロット番号を示します。
- [Admin Status] : アクセス ポイントの管理ステートを示します。
- [CDP State] : CDP ステートを有効にするには、[CDP State] チェックボックスを選択します。

ステップ 4　[Save] をクリックします。

AP 設定のインポート

現在のアクセス ポイントのコンフィギュレーション ファイルをインポートするには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Import AP Config] を選択します。

すべての Unified AP が CSV ファイルのみからインポートされることを示すポップアップ アラート ボックスが表示されます。Excel および XML ファイルからの Unified AP はインポートされません。

ステップ 3　[OK] をクリックして、ポップアップ アラート ボックスを閉じます。

ステップ 4　[Go] をクリックします。

ステップ 5　テキスト ボックスに CSV ファイルのパスを入力するか、[Browse] をクリックして、コンピュータで CSV ファイルにナビゲートします。

CSV ファイルの最初の行は、含まれている列の説明に使用されます。[AP Ethernet Mac Address] 列は必須です。このページのパラメータは、CSV ファイルで定義されていない列に使用されます。

ファイル ヘッダーの例：

```
AP Name,Ethernet MAC,Location,Primary Controller,Secondary Controller,Tertiary Controller
ap-1, 00:1c:58:74:8c:22, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3
```

CSV ファイルには、次のフィールドを含めることができます。

- [AP Ethernet MAC Address]：必須
- [AP Name]：省略可能
- [Location]：省略可能
- [Primary Controller]：省略可能
- [Secondary Controller]：省略可能
- [Tertiary Controller]：省略可能

省略可能フィールドは空のままにできます。[AP Config Import] は、空の省略可能フィールド値を無視します。ただし、primaryMwar と secondaryMwar エントリが空の場合は、Unified アクセス ポイントの更新は実行されません。

- [Ethernet MAC]：AP イーサネット MAC アドレス
- [AP Name]：AP 名
- [Location]：AP ロケーション
- [Primary Controller]：プライマリ コントローラ名
- [Secondary Controller]：セカンダリ コントローラ名
- [Tertiary Controller]：ターシャリ コントローラ名

（注）　省略可能フィールドは空のままにできます。[AP Config Import] は、空の省略可能フィールド値を無視します。ただし、primaryMwar と secondaryMwar エントリが空の場合は、Unified アクセス ポイントの更新は実行されません。

ステップ 6　適切な CSV ファイルのパスが [Select CSV File] テキスト ボックスに表示されたら、[OK] をクリックします。

AP 設定のエクスポート

現在のアクセス ポイントのコンフィギュレーション ファイルをエクスポートするには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Export AP Config] を選択します。

すべての Unified AP が CSV/EXCEL/XML ファイルにエクスポートされることを示すポップアップ アラート ボックスが表示されます。

ステップ 3　[OK] をクリックして、ポップアップ アラート ボックスを閉じます。

ステップ 4　次のものを含む現在の AP 設定を表示するには、[Go] をクリックします。

- AP 名
- イーサネット MAC
- 位置
- プライマリ コントローラ
- セカンダリ コントローラ
- ターシャリ コントローラ

ステップ 5　アクセス ポイント設定をエクスポートするには、ファイル オプション（CSV、Excel、XML）を選択します。

ステップ 6　[File Download] ウィンドウで、[Save] をクリックしてファイルを保存します。

アクセス ポイント 802.11n アンテナの設定

Prime Infrastructure には、特定のアンテナの使用を有効または無効にする機能があります。デフォルトでは、すべてのアンテナが有効になっています。

（注）　少なくとも 1 つの送信アンテナと 1 つの受信アンテナが有効である必要があります。すべての送信アンテナおよび受信アンテナを一度に無効にできません。

[Configure] > [Access Points] を選択して、[Radio] 列から [802.11n] 項目を選択すると、次のページが表示されます。

ここでは、次のフィールドについて説明します。

（注）　いずれかのフィールドを変更すると、無線が一時的に無効になり、一部のクライアントの接続が失われる場合があります。

General

- [AP Name]：アクセス ポイントのオペレータ定義名。
- [AP Base Radio MAC]：アクセス ポイントのベース無線の MAC アドレス。
- [Admin Status]：アクセス ポイントの管理ステートを有効するには、ボックスを選択します。

- [CDP State]：CDP を有効にするには、[CDP State] チェックボックスを選択します。
- [Controller]：コントローラの IP アドレス。詳細については、コントローラの IP アドレスをクリックします。
- [Site Config ID]：サイトの識別番号。
- [CleanAir Capable]：アクセス ポイントが CleanAir 対応かどうかが表示されます。
- [CleanAir]：ユーザが有効または無効に設定できるアクセス ポイントのスペクトラム センサーの CleanAir 管理ステータス。このフィールドを次のオプションに設定できます。
  - [Both Enabled]：2.4 GHz と 5 GHz の両方の無線の CleanAir を有効にします。
  - [Both Disabled]：2.4 GHz と 5 GHz の両方の無線の CleanAir を無効にします。
  - [2.4-GHz Enabled]：2.4 GHz 無線の CleanAir だけを有効にします。
  - [5-GHz Enabled]：5 GHz 無線の CleanAir だけを有効にします。

Antenna

- [Antenna Type]：外部アンテナまたは内部アンテナかを示します。
- [Antenna Diversity]：[Right]、[Left]、または [Enabled] を選択します。

（注） アンテナ ダイバーシティは、アクセス ポイントが 2 つの統合アンテナ ポートから無線信号をサンプリングし、適切なアンテナを選択する Cisco Aironet アクセス ポイント機能を指します。このダイバーシティ オプションは、マルチパスの歪みがあるエリアで信頼性を確保するために設計されています。

外部アンテナの場合は、次のいずれかを選択します。

  - [Enabled]：アクセス ポイントの左右両方のコネクタでダイバーシティを有効にする場合に選択します。
  - [Left]：アクセス ポイントに取り外し可能なアンテナがあり、そのアクセス ポイントの左コネクタに高利得アンテナが取り付けられている場合は、この設定を使用します。
  - [Right]：アクセス ポイントに取り外し可能なアンテナがあり、そのアクセス ポイントの右コネクタに高利得アンテナが取り付けられている場合、この設定を使用します。

内部アンテナの場合は、次のいずれかを選択します。

  - [Enabled]：Side A と Side B の両方でダイバーシティを有効にする場合に選択します。
  - [Side A]：Side A（前面アンテナ）のみでダイバーシティを有効にする場合は、この設定を使用します。
  - [Side B]：Side B（背面アンテナ）のみでダイバーシティを有効にする場合は、この設定を使用します。
- [External Antenna]：ドロップダウン リストから [external antenna] または [Other] を選択します。

（注） 802.11a/b/g/n 無線の場合、アンテナ タイプは [Internal] で、外部アンテナは [Internal-3rdRadio] です。

- [Antenna Gain]：テキスト ボックスに望ましいアンテナ ゲインを入力します。

（注）　無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 X 0.5 = 2dBi のゲインであることを意味します。

- [Current Gain (dBi)]：現在のゲイン（dBi）を示します。

  アンテナの dBi 値については『Cisco Aironet Antenna Reference Guide』を参照してください。

WLAN Override

次の [802.11a WLAN Override] フィールドが表示されます。

- [WLAN Override]：ドロップダウン リストから [Enable] または [Disable] を選択します。

（注）　[WLAN Override] を有効にすると、オペレーティング システムには、現在の Cisco WLAN ソリューション WLAN がすべて示された表が表示されます。この表で、この 802.11a Cisco 無線について WLAN 操作有効にする WLAN を選択し、WLAN 操作を禁止する WLAN を選択解除します。

（注）　WLAN の上書きは、512 WLAN 機能をサポートするアクセス ポイントには適用されません。

Performance Profile

[URL] をクリックして、このアクセス ポイントのインターフェイスのパフォーマンス プロファイル パラメータを表示または編集します。

- [ClientLink]：インターフェイスごとにアクセス ポイントの無線のクライアント リンクを有効または無効にします。この機能は、従来の（直交周波数分割多重）OFDM レートのみでサポートされます。インターフェイスでは ClientLink がサポートされる必要があり、OFDM レートを有効にする必要があります。また、複数のアンテナを送信可能にして、3 つすべてのアンテナを受信可能にする必要があります。

（注）　サポートされるクライアントの最大数は 15 です。アンテナ設定により操作が 1 本の送信アンテナに制限されている場合、あるいは OFDM レートが無効になっている場合、ClientLink は使用できません。

RF Channel Assignment

次の [802.11a RF Channel Assignment] パラメータが表示されます。

- [Current Channel]：アクセス ポイントのチャネル番号。
- [Assignment Method]：次のいずれかを選択します。
  - [Global]：アクセス ポイントのチャネルがコントローラによってグローバルに設定される場合は、この設定を使用します。
  - [Custom]：アクセス ポイントのチャネルがローカルで設定されている場合は、この設定を使用します。ドロップダウン リストからチャネルを選択します。

    たとえば、カスタムの電力として [2(17 dBm)] を選択する場合、2 は電力レベルに対応し、17 は絶対電力（dBm）に対応します。

- [Channel width] : ドロップダウン リストからチャネル幅を選択します。[20]、[above 40]、および [below 40] を選択できます。

  RF チャネル割り当てでは、5 GHz 帯域で 802.11n 40 MHz チャネル幅がサポートされます。40-MHz チャネル化により、無線では瞬間的データ レートが高くなります。

（注）　大きい帯域幅を選択すると、オーバーラッピングしないチャネルが減少するため、展開によっては全体のネットワーク スループットが低下することがあります。

（注）　アクセス ポイントの電力レベルとチャネル数は、監査されません。

Tx Power Level Assignment

- [Current Tx Power Level] : 現在の送信電力レベルを示します。
- [Assignment Method] : 次のいずれかを選択します。
  - [Global] : 電力レベルがコントローラによってグローバルに設定されている場合は、この設定を使用します。
  - [Custom] : アクセス ポイントの電力レベルがローカルで設定されている場合は、この設定を使用します。ドロップダウン リストから電力レベルを選択します。

11n Antenna Selection

Prime Infrastructure には、特定のアンテナの使用を有効または無効にする機能があります。デフォルトでは、すべてのアンテナが有効になっています。

（注）　少なくとも 1 つの送信アンテナと 1 つの受信アンテナが有効である必要があります。すべての送信アンテナおよび受信アンテナを一度に無効にできません。

次のいずれかの [11n Antenna Selection] パラメータを設定します。

- Antenna A
- Antenna B
- Antenna C
- Antenna D

[11n] パラメータ

次の [11n] フィールドが表示されます。

- [11n Supported] : 802.11n の無線がサポートされているかどうかを示します。
- [11ac Supported] : 802.11ac 無線がサポートされいないかどうかを示します。
- [Client Link] : クライアント リンクを有効または無効にするには、このオプションを使用します。ドロップダウン リストから [Enable]、[Disable]、または [Not Applicable] を選択します。

アクセス ポイントの 802.11ac 無線インターフェイスの設定

Prime Infrastructure には、802.11ac 無線管理状態を有効にする機能があります。。

[Configure] > [Access Points] を選択して、[Radio] 列から [802.11ac] 項目を選択すると、次のページが表示されます。

ここでは、次のフィールドについて説明します。

（注）　いずれかのフィールドを変更すると、無線が一時的に無効になり、一部のクライアントの接続が失われる場合があります。

General

- [AP Name] : アクセス ポイントのオペレータ定義名。
- [AP Base Radio MAC] : アクセス ポイントのベース無線の MAC アドレス。
- [Admin Status] : このボックスをオンにして 802.11ac 無線インターフェイスの管理状態を有効にします。
- [Controller] : コントローラの IP アドレス。詳細については、コントローラの IP アドレスをクリックします。
- [Site Config ID] : サイトの識別番号。
- [CleanAir Capable] : アクセス ポイントが CleanAir 対応かどうかが表示されます。802.11ac インターフェイスは CleanAir 機能ではありません。

Antenna

- [Antenna Type] : 外部アンテナまたは内部アンテナかを示します。802.11ac アンテナのタイプは、常に内部です。

Performance Profile

[URL] をクリックして、このアクセス ポイントのインターフェイスのパフォーマンス プロファイル パラメータを表示または編集します。

- [ClientLink] : インターフェイスごとにアクセス ポイントの無線のクライアント リンクを有効または無効にします。この機能は、従来の（直交周波数分割多重）OFDM レートのみでサポートされます。インターフェイスでは ClientLink がサポートされる必要があり、OFDM レートを有効にする必要があります。また、複数のアンテナを送信可能にして、3 つすべてのアンテナを受信可能にする必要があります。

（注）　サポートされるクライアントの最大数は 15 です。アンテナ設定により操作が 1 本の送信アンテナに制限されている場合、あるいは OFDM レートが無効になっている場合、ClientLink は使用できません。

RF Channel Assignment

次の [RF Channel Assignment] パラメータが表示されます。

- [Current Channel] : アクセス ポイントのチャネル番号。

- [Assignment Method]：チャネル割り当て方式が、[Global] または [Custom] のどちらかで表示されます。
- [Channel width]：ドロップダウン リストからチャネル幅を選択します。選択肢には、20 MHz、40 MHz、および 80 MHz があります。

（注）　802.11a/n 無線のチャネル割り当て方法がカスタムの場合のみチャネル幅を選択できます。

Tx Power Level Assignment

- [Current Tx Power Level]：現在の送信電力レベルを示します。

（注）　802.11ac 無線の現在の TX 電力のレベルは 802.11an 無線と同じです。

- [Assignment Method]：チャネル割り当て方式が、[Global] または [Custom] のどちらかで表示されます。

11n Antenna Selection

Prime Infrastructure には、特定のアンテナの使用を有効または無効にする機能があります。デフォルトでは、すべてのアンテナが有効になっています。

（注）　少なくとも 1 つの送信アンテナと 1 つの受信アンテナが有効である必要があります。すべての送信アンテナおよび受信アンテナを一度に無効にできません。

次のいずれかの [11n Antenna Selection] パラメータを設定します。

- Antenna A
- Antenna B
- Antenna C
- Antenna D

[11n] パラメータ

次の [11n] フィールドが表示されます。

- [11n Supported]：802.11n の無線がサポートされているかどうかを示します。
- [11ac Supported]：802.11ac 無線がサポートされいないかどうかを示します。
- [Client Link]：クライアント リンクを有効または無効にするには、このオプションを使用します。ドロップダウン リストから [Enable]、[Disable]、または [Not Applicable] を選択します。

CDP の設定

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。

（注）　CDP は、デフォルトでイーサネットと、ブリッジの無線ポートで有効です。

アクセス ポイントへの CDP の設定

無線またはイーサネット インターフェイスで CDP を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　ソフトウェア リリース 5.0 以降のコントローラに関連付けられたアクセス ポイントを選択します。

ステップ 3　CDP を有効にする無線またはイーサネット インターフェイスのスロットをクリックします。

ステップ 4　インターフェイスで CDP を有効にするには、[CDP State] チェックボックスを選択します。

ステップ 5　[Save] をクリックします。

Tracking Optimized Monitor Mode を使用するためのアクセス ポイント無線の設定

タグのモニタと位置計算を最適化するには、アクセス ポイントの 2.4GHz 帯（802.11b/g 無線）内で、最高 4 つのチャネルに対して Tracking Optimized Monitor Mode（TOMM）を有効にします。これによって、タグが機能するようにプログラミングされているチャネルだけを対象にチャネル スキャンを実行できます（チャネル 1、チャネル 6、チャネル 11 など）。

アクセス ポイント レベルでモニタ モードを有効にした後、TOMM を有効にして、そのアクセス ポイントの 802.11b/g 無線にモニタ チャネルを割り当てる必要があります。

（注）　アクセス ポイントでモニタ モードを有効にする方法については、「アクセス ポイントの詳細の設定」（P.9-477）のステップ 6 を参照してください。

アクセス ポイント無線で TOMM を有効にして、モニタ チャネルを割り当てるには、次の手順を実行します。

ステップ 1　アクセス ポイント レベルでモニタ モードを有効にした後、[Configure] > [Access Points] の順に選択します。

ステップ 2　[Access Points] ページで、適切なアクセス ポイントの [802.11 b/g Radio] リンクをクリックします。

ステップ 3　[General] グループ ボックスで、チェックボックスを選択解除して [Admin Status] を無効にします。無線が無効になります。

ステップ 4　[TOMM] チェックボックスを選択します。このチェックボックスは、モニタ モードの AP の場合のみ表示されます。設定可能な 4 つの各チャネルのドロップダウン リストが表示されます。

ステップ 5　アクセス ポイントによるタグのモニタを有効にする 4 つのチャネルを選択します。

（注）　モニタ対象として 4 つすべてのチャネルを選択する必要はありません。モニタ チャネルを削除するには、チャネルのドロップダウン リストから [None] を選択します。

ステップ 6　[Save] をクリックします。チャネル選択が保存されます。

ステップ 7　[Radio] パラメータ ページで、[Admin Status] チェックボックスを選択して無線を再度有効にします。

ステップ 8　[Save] をクリックします。これで、アクセス ポイントが TOMM アクセス ポイントとして設定されました。

[Monitor] > [Access Points] ページに、AP モードが [Monitor/TOMM] と表示されます。

アクセス ポイントのコピーおよび交換

[Copy and Replace AP] 機能は、アクセス ポイントをネットワークから削除して、新しいアクセス ポイントと交換する必要がある場合に役立ちます。AP モード、名前、およびマップ ロケーションなどのすべてのアクセス ポイント情報を古いアクセス ポイントから新しいアクセス ポイントにコピーする必要があります。

[Copy and Replace AP] 機能にアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Copy and Replace AP] を選択します。

ステップ 4　[Go] をクリックします。

最初に古いアクセス ポイントをネットワークから削除する必要があります。その後、このアクセス ポイントは、すべてのコントローラに対する関連付けが解除されます。新しいアクセス ポイントを接続すると、そのアクセス ポイントがコントローラに関連付けられ、Prime Infrastructure によって情報が更新されます。この時点で、関連付けを解除された古いアクセス ポイントを選択して、設定を新しいアクセス ポイントにコピーして交換することを選択します。

（注）　別のアクセス ポイント タイプを使用して、古いアクセス ポイントを交換する場合は、適用される設定パラメータのみがコピーされます。

アクセス ポイントの削除

関連付けられていないアクセス ポイントを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Remove APs] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[OK] をクリックして、削除を確定します。

無線ステータスのスケジュール設定および表示

この項では、次のトピックを扱います。

無線ステータスのスケジュール設定

無線ステータスの変更（有効または無効）のスケジュールを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Schedule Radio Status] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[Admin Status] ドロップダウン リストから、[Enable] または [Disable] を選択します。

ステップ 6　[Hours] および [Minutes] ドロップダウン リストを使用して、スケジュール時間を決定します。

ステップ 7　カレンダー アイコンをクリックして、ステータス変更の予定日を選択します。

ステップ 8　タスクを周期的に繰り返して実行する場合は、[Daily] または [Weekly] を選択します。タスクを一度だけ実行する場合は、[No Recurrence] を選択します。

ステップ 9　[Save] を選択して、スケジュール設定したタスクを確定します。

スケジュール設定したタスクの表示

現在スケジュール設定されている無線ステータス タスクを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　該当するアクセス ポイントのチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[View Scheduled Radio Task(s)] を選択します。

ステップ 4　[Go] をクリックします。

スケジュール設定済みのタスクに関する次の情報が表示されます。

- [Scheduled Task(s)]：そのアクセス ポイントとアクセス ポイント無線を表示するタスクを選択します。
- [Scheduled Radio adminStatus]：ステータス変更（Enable または Disable）を示します。
- [Schedule Time]：スケジュール タスクの発生時間を示します。
- [Execution status]：タスクがスケジュール設定されているかどうかを示します。
- [Recurrence]：タスクが繰り返し実行されるようにスケジュール設定している場合は、その周期（Daily または Weekly）を示します。
- [Next Execution]：タスクの次の実行日時を示します。
- [Last Execution]：タスクの最後の実行日時を示します。

- [Unschedule]：スケジュール設定されているタスクをキャンセルする場合は、[Unschedule] をクリックします。[OK] をクリックして、キャンセルを確定します。

監査ステータスの表示（アクセス ポイント）

[Configure] > [Access Points] ページの [Audit Status] 列には、各アクセス ポイントの監査ステータスが表示されます。選択したアクセス ポイントの監査レポートも確認できます。レポートには、監査の時刻、選択したアクセス ポイントの IP アドレス、および同期ステータスが表示されます。

監査ステータスを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Points] の順に選択します。

ステップ 2　[Audit Status] 列の値をクリックして、選択したアクセス ポイントの最新の監査詳細ページへ移動します。このレポートは、インタラクティブでアクセス ポイントごとになっています。

（注）　マウス カーソルを [Audit Status] 列の値の上に置くと、最新監査の時刻が表示されます。

アクセス ポイントのオンデマンドの監査レポートを実行するには、レポートを実行する目的のアクセス ポイントを選択し、[Select a command] ドロップダウン リストから [Audit Now] を選択します。4.1 よりも前のバージョンでは、監査は [AP Details and AP Interface Details] ページのパラメータに限られていました。リリース 4.1 では、この監査レポートはアクセス ポイント全体レベルの監査を対象としています。監査結果はデータベースに保存されるので、もう一度監査を実行しなくても最新の監査レポートを確認できます。

（注）　監査は、コントローラに関連付けられているアクセス ポイント上でだけ実行できます。

メンテナンス モード アクセス ポイントのアラームのフィルタリング

Prime Infrastructure は、Critical アラームを使用して、管理対象アクセス ポイントがダウンしているかどうかを追跡します。コントローラは、次のことが発生した場合に、3 つの異なるアラームを送信します。

- アクセス ポイントがダウンになる
- アクセス ポイントの無線 A がダウンになる
- アクセス ポイントの無線 B または G がダウンになる

リリース 7.0.172.0 以降では、これらの 3 つのアラームは単一のアラームにグループ化されます。

アクセス ポイントの技術メンテナンス中は、Critical アラームの優先順位付けを解除する必要があります。アクセス ポイントのアラームの重大度の優先順位付けを解除するには、[Configure] > [Access Points] ページを使用します。アクセス ポイントをメンテナンス ステートに移行すると、そのアクセス ポイントのアラーム ステータスは黒色で表示されます。

この項では、次のトピックを扱います。

- 「アクセス ポイントのメンテナンス ステートへの移行」（P.9-498）

- 「メンテナンス ステートからのアクセス ポイントの削除」（P.9-498）

アクセス ポイントのメンテナンス ステートへの移行

アクセス ポイントをメンテナンス ステートに移行するには、次の手順を実行します。

ステップ 1　[Prime Infrastructure] > [Configure] > [Access Points] を選択します。

[Access Points] ページが表示されます。

ステップ 2　ドロップダウン リストから [Place in Maintenance State] を選択して、[Go] をクリックします。

アクセス ポイントがメンテナンス ステートに移行されます。

アクセス ポイントがメンテナンス ステートに移行されると、アクセス ポイント ダウン アラームは、重大よりも低い重大度で処理されます。

メンテナンス ステートからのアクセス ポイントの削除

アクセス ポイントをメンテナンス ステートから削除するには、次の手順を実行します。

ステップ 1　[Prime Infrastructure] > [Configure] > [Access Points] を選択します。

[Access Points] ページが表示されます。

ステップ 2　ドロップダウン リストから [Remove from Maintenance State] を選択して、[Go] をクリックします。

アクセス ポイントがメンテナンス ステートから削除されます。

アクセス ポイントの検索

カスタム検索を作成して保存するには、ページの右上隅にある検索オプションを使用します。

- [New Search] : IP アドレス、名前、SSID、または MAC を入力して、[Search] をクリックします。
- [Saved Searches] : [Saved Search] をクリックして、カテゴリ、保存したカスタム検索を選択するか、ドロップダウン リストから他の検索基準を選択します。
- [Advanced Search] : 詳細検索では、さまざまなカテゴリとフィルタに基づいてデバイスを検索できます。

詳細については、「検索機能の使用方法」（P.2-54）を参照してください。

[Go] をクリックすると、アクセス ポイントの検索結果が表示されます（表 9-4 を参照）。

表 9-4　アクセス ポイントの検索結果

フィールド	オプション
IP Address	アクセス ポイントの IP アドレス。
Ethernet MAC	アクセス ポイントの MAC アドレス。

表 9-4　アクセス ポイントの検索結果 （続き）

AP Name	アクセス ポイントに割り当てられた名前。詳細を表示するには、アクセス ポイント名の項目をクリックします。
Radio	アクセス ポイントのプロトコルは、802.11a/n または 802.11b/g/n のどちらかです。
Map Location	キャンパス、ビルディング、またはフロアの位置。
Controller	コントローラの IP アドレス。
AP Type	アクセス ポイントの無線周波数の種類。
Operational Status	シスコ製無線通信機の動作ステータスを表示します（Up または Down）。
Alarm Status	アラームのカラー コードは、次のとおりです。 • 透明 = アラームなし • 赤 = Critical アラーム • オレンジ = Major アラーム • 黄 = Minor アラーム
Audit Status	アクセス ポイントの監査ステータス。
Serial Number	アクセス ポイントのシリアル番号。
AP Mode	Local、FlexConnect、Monitor、Rogue Detector、Sniffer、Bridge、または SE-Connect など、アクセス ポイント モードのロールを示します。

メッシュ リンクの詳細の表示

メッシュ リンクの詳細には、次のいくつかの方法でアクセスできます。

- Prime Infrastructure ホーム ページで [Mesh] ダッシュボードをクリックします
- [Monitor] > [Access Points] を選択して、[Mesh Links] タブをクリックしてから、[Details] リンクをクリックします
- Google Earth から KML ファイルをインポートした後で、[AP Mesh] リンクをクリックします

ページの上部に、現在の統計、その後に特定の統計の図が表示されます。

- [SNR Graph] : [SNR Up] および [SNR Down] グラフは 1 つのグラフに結合されています。各データ セットは、別の色で表されます。
- [Link Metrics Graph] : [Adjusted Link Metric] と [Unadjusted Link Metric] は 1 つのグラフに結合されています。各データ セットは、別の色で表されます。
- [Packet Error Rate Graph] : パケット エラー レートをグラフで表示します。
- [Link Events] : リンクの最近 5 つのイベントが表示されます。
- [Mesh Worst SNR Links] : 最低信号対雑音比（SNR）リンクが表示されます。
- [AP Uptime] : これらの統計は、アクセス ポイントが頻繁にリブートされるかどうかを判別するために役立ちます。

- [LWAPP Join Taken Time]：これらの統計は、アクセス ポイントの追加に要する時間を判別します。
- [Location Links]：Prime Infrastructure マップまたは Google Earth のロケーションに移動できます。

不正アクセス ポイント分類ルールの表示または編集

単一の WLC で、不正アクセス ポイントの現在の分類ルールを表示または編集できます。詳細については、「不正 AP ルール テンプレートの設定」（P.11-680）を参照してください。

不正アクセス ポイント分類ルールにアクセスするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　[IP Address] 列で IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Security] > [Rogue AP Rules] の順に選択します。[Rogue AP Rules] 画面に、不正アクセス ポイントの分類ルール、ルール タイプ（[Malicious] または [Friendly]）、およびルールの順序が表示されます。

ステップ 4　ルールの詳細を表示または編集するには、[Rogue AP Rule] を選択します。

スイッチの設定

スイッチを Prime Infrastructure データベースに追加して、全体的なスイッチ ヘルスとエンドポイントのモニタを表示して、スイッチポート トレースを実行できます。このスイッチ機能は Prime Infrastructure の [Configuration] メニューに表示されますが、Prime Infrastructure システムを設定しているのであって、スイッチを設定しているわけではありません。Prime Infrastructure を使用してスイッチ機能を設定することはできません。

Prime Infrastructure を使用して次を実行できます。

- [Configure] > [Switches] ページでスイッチを追加して、CLI および SNMP クレデンシャルを指定します。詳細については、「スイッチの追加」（P.9-503）を参照してください。
- [Monitor] > [Switches] を選択してスイッチをモニタします。詳細については、「スイッチのモニタリング」（P.5-31）を参照してください。
- [Reports] メニューを使用してスイッチ関連レポートを実行します。

（注）　[Configure] > [Switches] ページで、モビリティ サービス エンジンと Prime Infrastructure で有線クライアントを追跡するためにロケーション対応スイッチを追加することもできます。

ここでは、次の内容について説明します。

- 「スイッチの設定」（P.9-500）
- 「Spectrum Expert の設定」（P.9-510）

（注）　サポートされているスイッチは、3750、3560、3750E、3560E、および 2960 です。

スイッチ タイプ別に使用可能な機能

スイッチを Prime Infrastructure に追加する際には、スイッチの管理方法を指定します。スイッチの管理を指定する方法に基づいて、Prime Infrastructure は使用可能な機能を判別します。

- [Monitored switches]：スイッチを追加（[Configure] > [Switches] を選択）して、スイッチの動作をモニタ（[Monitor] > [Switches] を選択）できます。それぞれのスイッチは、ライセンスの合計デバイス数に対して 1 つのデバイスとしてカウントされます。ライセンス エンジンで使用可能な未使用のデバイス数がある場合は、スイッチを Prime Infrastructure に追加できます。使用可能なデバイス数が残っていない場合は、別のスイッチを Prime Infrastructure に追加できません。
- [Switch Port Tracing (SPT) only switches]：スイッチは、スイッチ ポート トレースのみを実行します。SPT 専用スイッチは、[Configure] > [Switches] ページとインベントリ レポートに表示されますが、SPT 専用スイッチは [Monitor] > [Switches] ページまたはダッシュボードには表示されません。ライセンスは SPT スイッチには適用されません。

スイッチの表示

Prime Infrastructure データベースですべてのスイッチのサマリーを表示するには、[Configure] > [Switches] を選択します。表示されるサマリー情報は、次のとおりです。

- [Management IP Address]：スイッチの IP アドレス。詳細を取得するには、スイッチの IP アドレスをクリックします。詳細については、「スイッチの詳細の表示」（P.9-501）を参照してください。
- [Device Name]：スイッチの名前。
- [Device Type]：スイッチのタイプ。
- [Reachability Status]：スイッチが到達可能な場合は [Reachable]、スイッチが到達不能な場合は [Unreachable] を示します。
- [Inventory Collection Status]：最後のインベントリ収集のステータス。可能な値は、[OK]、[Partial]、[Failed]、[NA]（SPT 専用スイッチの場合）、または [In Progress] です。
- [Inventory Status Detail]：最新のインベントリ収集のステータスを指定します。インベントリ収集が正常に行われなかった場合は、失敗の考えられる理由がリストされます。
- [Last Inventory Collection Date]：インベントリが収集された最後の日付が表示されます。
- [Creation Time]：スイッチが Prime Infrastructure に追加された日付と時刻。
- [License Status]：スイッチのライセンス ステータスを示します。これは、[Full Support] または [SPT only] です。詳細については、「スイッチ タイプ別に使用可能な機能」（P.9-501）を参照してください。

任意の列見出しをクリックして、その列で情報をソートします。列見出しを複数回クリックすることで、昇順のソートと降順のソートを切り替えることができます。

スイッチの詳細の表示

Prime Infrastructure データベースですべてのスイッチのサマリーを表示するには、[Configure] > [Switches] を選択します。スイッチに関する詳細情報を表示するには、[Management IP Address] 列で IP アドレスをクリックします。表 9-5 で、表示される要約情報について説明します。

表 9-5　[Configure] > [Switches Summary Information]

General パラメータ	
IP Address	スイッチの IP アドレス。
Device Name	スイッチ名。
Last Inventory Collection Date	最後のインベントリ収集の日付と時刻。
Inventory Collection Status	最後のインベントリ収集のステータス。可能な値は、[OK]、[Partial]、または [Failed] です。
Software Version	スイッチで実行されているソフトウェアのバージョン。
Location	スイッチの場所。
Contact	スイッチの担当者名。
Reachability Status	スイッチが到達可能な場合は [Reachable]、スイッチが到達不能な場合は [Unreachable] を示します。
SNMP パラメータ	
Version	SNMP バージョン番号、これは、[v1]、[v2c]、または [v3] です。 **（注）** SNMP v3 で設定されたスイッチのスイッチ ポート トレーシングを正常に実行するには、該当する VLAN のコンテキストをスイッチで設定する必要があります。詳細については、「スイッチでの SNMPv3 の設定」（P.9-505）を参照してください。
Retries	プロセスが成功せずに停止するまでに許可される再試行値（秒単位）。
Timeout	SNMP タイムアウト値（秒単位）。
[Version] ドロップダウン リストで [v3] を選択した場合は、次のフィールドが表示されます。	
Username	ユーザ名
Auth.Type	認証タイプは、[None]、[HMAC-SHA]、または [HMAC-HD5] です。
Auth.Password	認証パスワード。
Privacy Type	プライバシー タイプは、[None]、[CBC-DES]、または [CFB-AES-128] です。
Privacy Password	プライバシー パスワード。
Community	[v1] または [v2c] を選択した場合は、このフィールドは SNMP コミュニティ ストリングを示します。
Telnet/SSH パラメータ	
Protocol	使用されるプロトコル。
User Name	ユーザ名。
Password	パスワード。
Confirm Password	パスワードを再度入力して確認します。
Enable Password	イネーブル パスワード。
Confirm Password	パスワードを再度入力して確認します。
Timeout	タイムアウト値（秒単位）です。

SNMP パラメータの変更

スイッチの SNMP パラメータを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Switches] を選択して、SNMP クレデンシャルを変更するスイッチの IP アドレスをクリックします。

ステップ 2　必要な [SNMP Parameters] フィールドを変更して、次をクリックします。

- [Reset]：以前に保存したパラメータを復元します。
- [Save]：行った変更を保存して適用します。
- [Cancel]：変更を保存せずに終了して、前の画面に戻ります。

Telnet/SSH パラメータの変更

スイッチの Telnet または SSH パラメータを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Switches] を選択して、Telnet または SSH クレデンシャルを変更するスイッチの IP アドレスをクリックします。

ステップ 2　必要な [Telnet/SSH Parameters] フィールドを変更して、次をクリックします。

- [Reset]：以前に保存したパラメータを復元します。
- [Save]：行った変更を保存して適用します。
- [Cancel]：変更を保存せずに終了して、前の画面に戻ります。

スイッチの追加

Prime Infrastructure データベースにスイッチを追加すると、デフォルトでは、Prime Infrastructure はスイッチの SNMP クレデンシャルを検査します。デバイスのクレデンシャルが正しくない場合、SNMP 失敗メッセージが表示されますが、スイッチは Prime Infrastructure データベースに追加されます。

スイッチを Prime Infrastructure に追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Switches] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Switches] を選択し、[Go] をクリックします。

ステップ 3　表 9-6 の説明に従って、フィールドに入力します。

表 9-6　スイッチの追加

フィールド	説明
General Parameters	
Add Format Type	次を選択します。 • [Device Info] : イーサネット スイッチの IP アドレスをカンマで区切って手動で入力します。 • [CSV File] : 複数のスイッチの IP アドレスが含まれている CSV ファイルをインポートします。テキスト ボックスに CSV ファイルのパスを入力するか、[Browse] をクリックして、コンピュータで CSV ファイルにナビゲートします。詳細については、「スイッチでの SNMPv3 の設定」（P.9-505）を参照してください。
IP Addresses	[Device Info] を選択した場合は、イーサネット スイッチの IP アドレスをカンマで区切って入力します。
License Level	次を選択します。 • **Full** • [SPT only] : スイッチ ポート トレーシング サポートのみを指定します。
SNMP Parameters **（注）** 書き込みアクセスに対応する SNMP パラメータ（使用できる場合）を入力します。読み取り専用アクセス パラメータを入力すると、スイッチは追加されますが、Prime Infrastructure は設定を変更できません。	
Version	SNMP バージョン番号を入力します。これは、[v1]、[v2c]、または [v3] です。 **（注）** SNMP v3 で設定されたスイッチのスイッチ ポート トレーシングを正常に実行するには、該当する VLAN のコンテキストをスイッチで設定する必要があります。詳細については、「スイッチでの SNMPv3 の設定」（P.9-505）を参照してください。
Retries	プロセスが成功せずに停止するまでに許可される再試行値（秒単位）を入力します。
SNMP Timeout (in secs)	SNMP タイムアウト値（秒単位）を入力します。
[Version] ドロップダウン リストで [v1] または [v2c] を選択した場合は、[Community] フィールドが表示されます。	
Community	SNMP コミュニティ ストリングを入力します。
[Version] ドロップダウン リストで [v3] を選択した場合は、次のフィールドが表示されます。	
Username	ユーザ名を入力します。
Auth.Type	[None]、[HMAC-SHA]、または [HMAC-HD5] の認証タイプを入力します。
Auth.Password	認証パスワードを入力します。
Privacy Type	[None]、[CBC-DES]、または [CFB-AES-128] のプライバシー タイプを入力します。
Privacy Password	プライバシー パスワードを入力します。
Telnet/SSH Parameters	
Protocol	プロトコルを選択します。
User Name	ユーザ名を入力します。
Password	パスワードを入力します。
Confirm Password	パスワードを再度入力して確認します。
Enable Password	イネーブル パスワードを入力します。
Confirm Password	イネーブル パスワードを再度入力して確認します。
Timeout (in secs)	タイムアウト値（秒単位）を入力します。

ステップ 4　[Add] をクリックして、スイッチを追加します。

ステップ 5　操作をキャンセルして、スイッチのリストに戻るには、[Cancel] をクリックします。

（注）　追加後のスイッチは、Prime Infrastructure が、追加されたコントローラとの通信を試行する間、一時的に [Monitor] > [Unknown Devices] ページに配置されます。スイッチとの通信が正常に行われると、スイッチは [Monitor] > [Unknown Devices] ページから [Monitor] > [Switches] ページに表示されます。Prime Infrastructure がスイッチと正常に通信できない場合、そのコントローラは [Monitor] > [Unknown Devices] に残り、エラー状態およびエラーメッセージが表示されます。[Unknown Devices] ページにアクセスするには、[Configure] > [Unknown Devices] を選択します。

スイッチでの SNMPv3 の設定

次に、スイッチでの SNMPv3 の設定例を示します。

```
snmp-server view v3default iso included
snmp-server group v3group v3 auth write v3default snmp-server user <username>
<v3group> v3 auth <md5 or sha> <authentication password>
```

スイッチに VLAN がある場合、各 VLAN を設定する必要があります。設定しないと、スイッチ ポート トレーシングは失敗します。次に、スイッチに VLAN 1 および 20 がある場合の例を示します。

```
snmp-server group v3group v3 auth context vlan-1  write v3default
snmp-server group v3group v3 auth context vlan-20 write v3default

snmp-server group v3group v3 auth context vlan-20 write v3default
```

（注）　SNMP v3 ビューの作成時に、すべての OID を含めてください。

スイッチをインポートするための CSV ファイルの例

CSV ファイルの最初の行は、含まれている列の説明に使用されます。IP アドレス列は必須です。次に、CSV ファイルの例を示します。

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name,
snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password,
snmp_retries,
snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
16.1.1.3,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
16.1.1.4,255.255.255.0,v2,public,,,,,,3,10,ssh2,cisco,cisco,cisco,60
16.1.1.5,255.255.255.0,v2,public,,,,,,3,10,,cisco,cisco,cisco,60
16.1.1.6,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
3.3.3.3,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4
4.4.4.4,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4,telnet,cisco,cisco,
cisco,60
```

CSV ファイルには、次のフィールドを含めることができます。

- ip_address：IP アドレス
- network_mask：ネットワーク マスク
- snmp_version：SNMP クレデンシャル バージョン。v1、v2、または v3 です。
- snmp_community：SNMP コミュニティ（v2 では必須）。

- snmpv2_community：SNMP V2 コミュニティ。
- snmpv3_user_name：SNMP V3 ユーザ名（v3 では必須）。
- snmpv3_auth_type：SNMP V3 認証タイプ。None、HMAC-MD5、または HMAC-SHA です（v3 では必須）。
- snmpv3_auth_password：SNMP V3 認証パスワード（v3 では必須）。
- snmpv3_privacy_type：SNMP V3 プライバシー タイプ。None、DES、または CFB-AES-128 です（v3 では必須）。
- snmpv3_privacy_password：SNMP V3 プライバシー パスワード（v3 では必須）。
- snmp_retries：SNMP 再試行回数
- snmp_timeout：SNMP タイムアウト
- protocol：telnet、ssh2
- telnet_username：設定されている場合、スイッチおよび AP のユーザ名（設定されている場合は必須）。
- telnet_password：スイッチと AP のパスワード（必須）
- enable_password
- telnet_timeout

スイッチ NMSP およびロケーションの設定

[Prime Infrastructure] > [Configure] > [Switches] > [*Switch IP Address*] > [NMSP & Location] を選択して、スイッチの NMSP およびロケーション情報を表示します。

（注）　NMSP は次のものによってサポートされます。

- Cisco Catalyst 3000 および 4000 シリーズ スイッチ
- Cisco IOS Release 12.50 以降

次の項の説明に従って、NMSP ステータスを有効または無効にして、スイッチとスイッチ ポートのロケーションを設定できます。

- スイッチの NMSP の有効化および無効化
- スイッチ ロケーションの設定
- スイッチ ポート ロケーションの設定

スイッチの NMSP の有効化および無効化

[Prime Infrastructure] > [Configure] > [Switches] > [*Switch IP Address*] > [NMSP & Location] > [NMSP Status] を選択することで、スイッチの NMSP を有効または無効にできます。

表 9-7 に、[NMSP Status] ページで使用可能なオプションをリストします。

表 9-7　[NMSP Status] ページのパラメータ

フィールド	説明
NMSP	スイッチの NMSP を有効または無効にするには、このオプションを選択または選択解除します。
MSE IP Address	スイッチが MSE に関連付けられている場合に、MSE の IP アドレスを表示します。このスイッチを MSE に関連付けるには、[Go to Synchronize] をクリックします。これによって [Synchronization] ページが表示されます。このスイッチを MSE と同期できます。または、[Prime Infrastructure] > [Services] > [Synchronize Services] > [Wired Switches] を選択して、スイッチを MSE に同期することもできます。 同期の詳細については、「サービスの同期化」（P.16-950）を参照してください。

スイッチ ロケーションの設定

[Switch Location] オプションを使用して、スイッチのロケーションを設定できます。

ステップ 1　[Prime Infrastructure] > [Configure] > [Switches] > [*Switch IP Address*] > [NMSP & Location] > [Switch Location] を選択します。

ステップ 2　[Map Location] ペインで、ドロップダウン リストから次を選択します。

- **Campus**
- **Building**
- **Floor**

ステップ 3　[Import Civic] をクリックして、スイッチに Civic 情報をインポートします。

[Civic Location] ペイン内のフィールドには、Civic 情報のインポート後に値が取り込まれます。

スイッチ ポート ロケーションの設定

[Switch Port Location] オプションを使用して、スイッチ ポートのロケーションを設定できます。

ステップ 1　[Prime Infrastructure] > [Configure] > [Switches] > [*Switch IP Address*] > [NMSP & Location] > [Switch Port Location] を選択します。

ステップ 2　ロケーションを設定するポートを 1 つ以上選択します。

ステップ 3　ドロップダウン リストから、[Configure Location] を選択して、[Go] をクリックします。

[Switch Port Location Configuration] ページが表示されます。

[Switch Ports] ペインには、ロケーションを選択するために選択したポートがリストされます。

ステップ 4　[Map Location] ペインで、ドロップダウン リストから次を選択します。

- **Campus**
- **Building**
- **Floor**

ステップ 5　[Import Civic] をクリックして、スイッチ ポートに Civic 情報をインポートします。

[Civic Location] ペイン内のフィールドには、Civic 情報のインポート後に値が取り込まれます。

スイッチの削除

Prime Infrastructure データベースからスイッチを削除すると、次の機能が実行されます。

- そのスイッチのインベントリ情報が、データベースから削除されます。
- スイッチのアラームは、ステータスが [Clear] のデータベース内に残ります。デフォルトでは、クリアされたアラームは Prime Infrastructure インターフェイスに表示されません。
- 保存したレポートは、レポートを実行したスイッチが削除されてもデータベースに残ります。

スイッチを Prime Infrastructure から削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Switches] を選択します。
ステップ 2　削除するスイッチのチェックボックスを選択します。
ステップ 3　[Select a command] ドロップダウン リストから、[Remove Switches] を選択します。
ステップ 4　[Go] をクリックします。
ステップ 5　[OK] をクリックして、削除を確認します。

スイッチ設定の更新

デフォルトでは、インベントリ情報が 6 時間ごとに収集されます。設定の変更を行った場合に、次のインベントリ収集を待たずに変更を即時に表示するには、次の手順で示すように、スイッチを更新できます。

ステップ 1　[Configure] > [Switches] を選択します。
ステップ 2　設定を更新するスイッチのチェックボックスを選択します。
ステップ 3　[Select a command] ドロップダウン リストで、[Refresh Config from Switch] を選択します。
ステップ 4　[Go] をクリックします。

有線クライアントの検出のためのスイッチでのトラップと Syslog の有効化

ここでは、クライアントの接続または切断時にクライアントを検出するために、Prime Infrastructure にトラップと syslog を送信するようスイッチを設定する方法について説明します。

この項では、次のトピックを扱います。

- 「トラップの MAC 通知（アイデンティティ クライアント以外の検出で使用）」（P.9-509）
- 「Syslog の設定」（P.9-509）

トラップの MAC 通知（アイデンティティ クライアント以外の検出で使用）

この Cisco IOS スイッチ機能は、MAC 通知のために SNMP トラップをスイッチから Prime Infrastructure サーバに転送します（802.1x 以外のクライアントの場合）。

Cisco IOS の設定例：

```
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of Prime Infrastructure server> version 2c <community-string>
mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change


interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface level config for MAC Notification
  snmp trap mac-notification change removed <- interface level config for MAC Notification
```

debug コマンド

```
debug snmp packets
```

show コマンド

```
show mac address-table notification change
```

参照

MAC 変更通知トラップの設定の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/swadmin.html#wp1246821

Syslog の設定

（注）　この機能は、アイデンティティ クライアント検出に使用されます。

syslog 設定は、syslog メッセージを Catalyst スイッチから Prime Infrastructure サーバに転送します。

Cisco IOS の設定例：

```
archive
 log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of Prime Infrastructure server>
```

詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/swlog.html

不明デバイスの設定

不明デバイスを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Unknown Devices] を選択します。[Unknown Devices] ページが表示されます。表示されるサマリー情報は、次のとおりです。

- [IP Address] : デバイスの IP アドレス。
- [Device Type] : デバイスのタイプ。
- [Reachability Status] : デバイスが到達可能な場合は [Reachable]、デバイスが到達不能な場合は [Unreachable] を示します。
- [Inventory Collection Status] : 最後のインベントリ収集のステータス。可能な値は、[OK]、[Partial]、[Failed]、[NA]、または [In Progress] です。
- [Inventory Status Detail] : 最新のインベントリ収集のステータスを指定します。インベントリ収集が正常に行われなかった場合は、失敗の考えられる理由がリストされます。
- [Creation Time] : デバイスが Prime Infrastructure に追加された日付と時刻。

ステップ 2　[Unknown Devices] ページから、次の機能を実行できます。

- [Remove Devices] : [unknown devices] 表からデバイスを削除するには、デバイスを選択して、[Select a command] ドロップダウン リストから [Remove Devices] を選択します。
- [Update Device Credentials] : デバイスのデバイス クレデンシャルを更新するには、デバイスを選択して、[Select a command] ドロップダウン リストから [Update Device Credentials] を選択します。[Update Device Credentials] ページが表示されます。
- [Bulk Update Devices] : デバイス クレデンシャルを一括更新するには、[Select a command] ドロップダウン リストから [Bulk Update Devices] を選択します。[Bulk Update Devices] ページが表示されます。CSV ファイルを選択できます。

（注）　CSV ファイルには、更新するデバイスのリスト（1 行に 1 つのデバイス）が含まれています。各行は、デバイス属性のカンマ区切りのリストです。最初の行は、含まれている属性の説明です。IP アドレス属性は必須です。

Spectrum Expert の設定

Spectrum Expert クライアントは、リモート干渉センサーとして機能し、動的な干渉データを Prime Infrastructure に送信します。この機能により、Prime Infrastructure はネットワーク内の Spectrum Expert から詳細な干渉データを収集、モニタ、およびアーカイブできます。

Spectrum Expert を設定するには、[Configure] > [Spectrum Experts] の順に選択します。このページには、次の項目を含むすべての Spectrum Expert の一覧が表示されます。

- [Hostname] : Spectrum Expert ラップトップのホスト名または IP アドレス。
- [MAC Address] : ラップトップのスペクトラム センサー カードの MAC アドレス。
- [Reachability Status] : Spectrum Expert が正常に稼働し、情報を Prime Infrastructure に送信しているかどうかを指定します。ステータスは、[Reachable] または [Unreachable] と表示されます。

ここでは、次の内容について説明します。

Spectrum Expert の追加

Spectrum Expert を追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Spectrum Experts] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Spectrum Expert] を選択します。

（注）　このリンクは、Spectrum Expert が 1 つも追加されていない場合にだけ表示されます。[Select a command] ドロップダウン リストから [Add a Spectrum Expert] を選択しても、[Add a Spectrum Expert] ページにアクセスできます。

ステップ 3　Spectrum Expert のホスト名または IP アドレスを入力します。ホスト名を使用する場合、Spectrum Expert を Prime Infrastructure に追加するには DNS に登録する必要があります。

（注）　Spectrum Expert として正しく追加するには、Spectrum Expert クライアントが稼働しており、Prime Infrastructure に通信するように設定されていなければなりません。

Spectrum Expert のモニタ

Spectrum Expert をモニタするためのオプションもあります。

Spectrum Expert をモニタするには、次の手順を実行します。

ステップ 1　[Monitor] > [Spectrum Experts] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Spectrum Experts] ページと [Interferers-SEs] ページにアクセスできます。

[Spectrum Experts Summary] の表示

[Spectrum Experts] ページには、システムに追加された Spectrum Expert の表が表示されます。この表には、次の Spectrum Expert の情報が記載されています。

[Hostname]：ホスト名または IP アドレス。

[Active Interferers]：Spectrum Expert により検出された現在の干渉源の数。

[Alarms APs]：検出された干渉が潜在的な影響を及ぼしていると Spectrum Expert により確認されたアクセス ポイントの数。

[Alarms]：Spectrum Expert から送信された Active Interference トラップの数。クリックすると、この Spectrum Expert のアクティブ アラームに対してフィルタリングされている [Alarm] ページへアクセスします。

[Reachability Status]：Spectrum Expert が稼働していて、データを Prime Infrastructure に送信している場合は、緑で [Reachable] と表示されます。それ以外の場合は、[Unreachable] と赤で表示されます。

[Location]：Spectrum Expert が無線クライアントの場合、場所へのリンクが使用できます。それによって、Spectrum Expert の場所が有効範囲を示す赤いボックス付きで表示されます。

[Interferers Summary] の表示

[Interferers-SEs] ページには、30 日間隔で検出されたすべての干渉源の一覧が表示されます。この表には、次のような干渉源の情報が記載されています。

- [Interferer ID]：異なる Spectrum Expert 間で一意の ID。これは、疑似乱数によって生成される ID です。MAC アドレスに似ていますが、実際のアドレスではなく、干渉デバイスの検出に使用できます。
- [Category]：干渉源のカテゴリ。[Categories include]：Bluetooth、コードレス電話、電子レンジ、802.11 FH、その他一般：周波数ホッピング、その他一般：連続、およびアナログ ビデオ。
- [Type]：Active は、干渉源が現在 Spectrum Expert で検出されていることを示します。[Inactive] は、干渉源が検出されなくなったこと、または Prime Infrastructure が到達できる干渉源はなくなったと Spectrum Expert が確認したことを示します。
- [Discover Time]：干渉源が発見された時刻を示します。
- [Affected Channels]：影響を受けるチャネルを示します。
- [Number of APs Affected]：Spectrum Expert が検出した Prime Infrastructure により管理されるアクセス ポイントの数、または Spectrum Expert がアクセス ポイントのチャネル上で検出した干渉源の数。アクティブな干渉源だけが表示されます。次の条件のすべてが適合する場合、そのアクセス ポイントには [affected] とラベルが付けられます。
  - アクセス ポイントが Prime Infrastructure で管理されている。
  - Spectrum Expect がアクセス ポイントを検出している。
  - Spectrum Expect がアクセス ポイントの稼働チャネル上の干渉源を検出している。
- [Power]：dBm で示されます。
- [Duty Cycle]：パーセントで示されます。100% は最低値です。
- [Severity]：干渉源の重大度ランキングを示します。100 は最低値、0 は干渉がないことを表しています。

[Spectrum Experts Details] の表示

[Spectrum Expert] ページには、単一の Spectrum Expert からの干渉源の詳細がすべて表示されます。このページは 20 秒ごとに更新され、リアルタイムにリモートの Spectrum Expert を確認できます。このページに表示される項目は、次のとおりです。

- [Total Interferer Count]：特定の Spectrum Expert から報告されます。
- [Active Interferers Count Chart]：カテゴリごとの干渉源をグループ化した円グラフを表示します。
- [Active Interferer Count Per Channel]：別々のチャネル上のカテゴリごとにグループ化された干渉源の数を表示します。
- [AP List]：Spectrum Expert によって検出されたアクセス ポイントの一覧を表示します。これらのアクセス ポイントは、アクティブな干渉源が検出されたチャネル上にあります。

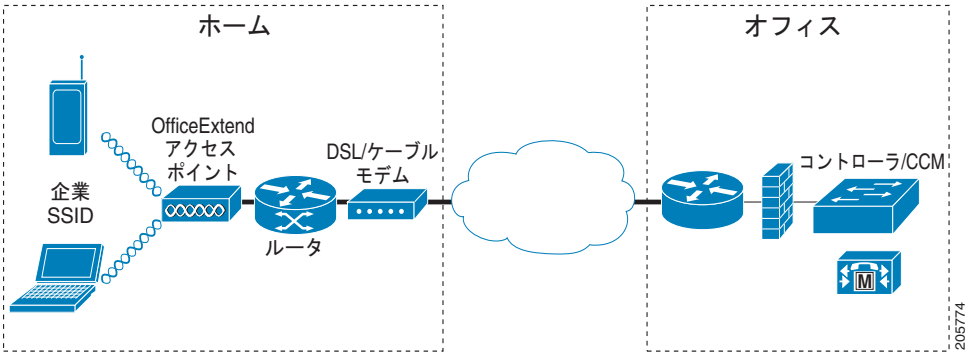
- [Affected Clients List] : アクセス ポイントに現在認証されているクライアントの一覧を表示します 外部認証を行う場合は、[Security] > [AAA] ページで特定の RADIUS サーバまたは LDAP サーバを選択できます。

OfficeExtend アクセス ポイント

OfficeExtend アクセス ポイントは、リモート ロケーションでコントローラからアクセス ポイントへの安全な通信を提供し、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。ホーム オフィスでのテレワーカーのエクスペリエンスは、本社オフィスでのエクスペリエンスとまったく同じです。アクセス ポイントとコントローラの間の Datagram Transport Layer Security（DTLS; データグラム トランスポート層セキュリティ）による暗号化は、すべての通信のセキュリティを最高レベルにします。

図 9-5 は、一般的な OfficeExtend アクセス ポイント セットアップを示します。

図 9-5　一般的な OfficeExtend アクセス ポイント セットアップ



（注） OfficeExtend アクセス ポイントは、ルータまたはネットワーク アドレス変換（NAT）を使用するその他のゲートウェイ デバイスを越えて動作するよう設計されています。NAT により、ルータなどのデバイスはインターネット（パブリック）と個人ネットワーク（プライベート）間のエージェントとして動作でき、これにより、コンピュータのグループ全体を単一の IP アドレスとすることができます。コントローラ リリース 6.0 では、単一の NAT デバイスの後方では単一の OfficeExtend アクセス ポイントのみを展開可能です。

現時点では、WPLUS ライセンスにより Cisco 5500 シリーズのコントローラに接続された Cisco Aironet 1130 シリーズおよび 1140 シリーズのアクセス ポイントだけを OfficeExtend アクセス ポイントとして設定できます。

（注） ファイアウォールは、アクセス ポイントからの CAPWAP を使用するトラフィックを許可するよう設定されている必要があります。UDP ポート 5246 および 5247 が有効であり、アクセス ポイントがコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。

OfficeExtend アクセス ポイントのライセンシング

5500 シリーズ コントローラに WPlus ライセンスがインストールされていることを確認します。ライセンスのインストール後、1130 シリーズまたは 1140 シリーズ アクセス ポイントで OfficeExtend モードを有効化できます。

（注）　オペレーティング システムのソフトウェアによってアクセス ポイントが自動的に検出され、Prime Infrastructure データベース内の既存のコントローラに関連付けられると Prime Infrastructure データベースに追加されます。

アクセス ポイントのリンク遅延の設定

コントローラでリンク遅延を設定して、アクセス ポイントおよびコントローラの間のリンクを計測できます。この機能は、コントローラに接続されたすべてのアクセス ポイントで使用できますが、特に、リンクの速度が低いか、信頼性の低い WAN 接続の可能性がある FlexConnect アクセス ポイントで役立ちます。

（注）　リンク遅延は、接続モードが FlexConnect アクセス ポイントのみでサポートされます。スタンドアロン モードの FlexConnect アクセス ポイントはサポートされません。

リンク遅延は、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントにおける CAPWAP ハートビート パケット（エコー要求および応答）のラウンドトリップ時間をモニタします。この時間は、ネットワーク リンク速度およびコントローラの処理負荷によって異なります。アクセス ポイントは、コントローラへの発信エコー要求およびコントローラから受信するエコー応答をタイムスタンプ記録します。アクセス ポイントはこのデルタ時間をシステムのラウンドトリップ時間としてコントローラに送信します。アクセス ポイントは、30 秒のデフォルト間隔でコントローラにハートビート パケットを送信します。

（注）　リンク遅延はアクセス ポイントとコントローラ間の CAPWAP 応答時間を計算します。ネットワーク遅延や ping 応答は計測しません。

コントローラにより、現在のラウンドトリップ時間および継続的な最短および最長ラウンドトリップ時間が表示されます。最短および最長時間はコントローラが動作している限り維持され、クリアして再開することもできます。

リンク遅延を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Access Point] 詳細ページで、[Enable Link Latency] チェックボックスを選択して、このアクセス ポイントのリンク遅延を有効にするか、選択解除して、エコー応答を受信するたびにアクセス ポイントがコントローラにラウンドトリップ時間を送信しないようにします。デフォルト値はオフです。

ステップ 2　[Save] をクリックして変更を保存します。

リンク遅延の結果は、[Enable Link Latency] チェックボックスの下に表示されます。

- [Current] : アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの現在のラウンドトリップ時間（ミリ秒単位）。

- [Minimum]：リンク遅延が有効になったか、またはリセットされたことが原因の、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最短ラウンドトリップ時間（ミリ秒単位）。
- [Maximum]：リンク遅延が有効になったか、またはリセットされたことが原因の、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最長ラウンドトリップ時間（ミリ秒単位）。

ステップ 3　このアクセス ポイントのコントローラ上の現在、最短、および最長リンク遅延統計をクリアするには、[Reset Link Latency] をクリックします。[Minimum] フィールドおよび [Maximum] フィールドに更新された統計情報が表示されます。

チョークポイントの設定

チョークポイントは、低周波の送信デバイスです。配置されたチョークポイントの範囲内でタグが渡されると、低周波電磁界がタグを認識し、チョークポイント デバイス ID を含むメッセージを Cisco Unified Wireless Network 経由で送信します。送信されるメッセージには、センサー情報（温度や圧力など）が含まれます。チョークポイント ロケーション システムは、部屋レベルの精度（ベンダーによって数インチから 2 フィートまで）を提供します。

チョークポイントは、チョークポイントのベンダーによって推奨されるとおりに設置および設定されます。チョークポイントのインストールが完了して動作可能になったら、チョークポイントをロケーション データベースに入力して、Prime Infrastructure マップ上に表示できます。

ここでは、次の内容について説明します。

- 「新しいチョークポイントの設定」（P.9-515）
- 「現在のチョークポイントの編集」（P.9-518）

新しいチョークポイントの設定

ここでは、次の内容について説明します。

- 「Prime Infrastructure データベースへのチョークポイントの追加」（P.9-515）
- 「Prime Infrastructure マップへのチョークポイントの追加」（P.9-516）
- 「Prime Infrastructure マップからのチョークポイントの削除」（P.9-517）
- 「Prime Infrastructure からのチョークポイントの削除」（P.9-517）

Prime Infrastructure データベースへのチョークポイントの追加

Prime Infrastructure データベースにチョークポイントを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Chokepoints] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　チョークポイントの MAC アドレスと名前を入力します。

ステップ 5　これが [Entry/Exit Chokepoint] であることを示すには、チェックボックスを選択します。

ステップ 6　チョークポイントのカバレッジ範囲を入力します。

（注）　チョークポイントの範囲は、視覚的な表示のみです。これは製品固有です。実際の範囲は、該当するチョークポイント ベンダー ソフトウェアを使用して別個に設定する必要があります。

ステップ 7　[OK] をクリックします。

（注）　データベースにチョークポイントを追加したら、適切な Prime Infrastructure フロア マップに配置できます。

Prime Infrastructure マップへのチョークポイントの追加

チョークポイントをマップに追加するには、次の手順を実行します。

ステップ 1　[Monitor] > [Maps] を選択します。

ステップ 2　[Maps] ページで、チョークポイントのフロアの位置に対応するリンクをクリックします。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 4　[Go] をクリックします。

（注）　[Add Chokepoints] サマリー ページには、データベースに追加されていてもまだマップされていない、最近追加されたチョークポイントがすべて一覧表示されます。

ステップ 5　マップ上に配置するチョークポイントの横にあるチェックボックスを選択します。

ステップ 6　[OK] をクリックします。

チョークポイント アイコンが左上角に配置されて、マップが表示されます。これで、マップ上にチョークポイントを配置する準備ができました。

ステップ 7　チョークポイント アイコンを左クリックして、適切な位置までドラッグして配置します。

（注）　チョークポイント アイコンを配置するためにクリックすると、選択したチョークポイントの詳細ページにチョークポイントの MAC アドレス、名前、およびカバレッジ範囲が表示されます。

ステップ 8　[Save] をクリックします。

フロア マップに戻ると、マップ上に追加されたチョークポイントが表示されます。

（注）　新たに作成されたチョークポイント アイコンは、そのフロアの表示設定に応じて、マップに表示される場合と表示されない場合があります。

（注）　チョークポイントの周囲の輪は、カバレッジ領域を示しています。CCX タグとそのアセットがカバレッジ領域内を通過すると、位置の詳細がブロードキャストされ、タグはチョークポイント カバレッジ円上に自動的にマップされます。タグがチョークポイントの範囲外に出ると、その位置は以前と同様に計算されるので、チョークポイントの輪の上にはマップされなくなります。

（注）　マウスをマップ アイコンの上に移動すると、チョークポイントの MAC アドレス、名前、Entry/Exit チョークポイント、スタティック IP アドレス、および範囲が表示されます。

ステップ 9　チョークポイントがマップ上に表示されない場合は、[Floor Settings] メニューにある [Chokepoints] チェックボックスを選択します。

（注）　すべてのマップに対してこの表示条件を保存しない場合には、[Save Settings] チェックボックスを選択しないでください。

（注）　チョークポイント情報を適用するには、ネットワーク設計をモビリティ サービス エンジンまたはロケーション サーバと同期する必要があります。

Prime Infrastructure マップからのチョークポイントの削除

マップからチョークポイントを削除するには、次の手順を実行します。

ステップ 1　[Monitor] > [Maps] を選択します。

ステップ 2　[Maps] ページで、チョークポイントのフロアの位置に対応するリンクを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Remove Chokepoints] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[OK] をクリックして、削除を実行します。

Prime Infrastructure からのチョークポイントの削除

Prime Infrastructure からチョークポイントを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Chokepoints] を選択します。

ステップ 2　削除するチョークポイントのチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Remove Chokepoints] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[OK] をクリックして、削除を実行します。

現在のチョークポイントの編集

Prime Infrastructure データベースと該当するマップで現在のチョークポイントを編集するには、次の手順を実行します。

ステップ 1　[Configure] > [Chokepoints] を選択します。[Configure] > [Chokepoints] ページに、現在の各チョークポイントに関する情報（MAC アドレス、チョークポイント名、Entry/Exit チョークポイントの範囲、スタティック IP アドレス、チョークポイントのマップの位置）が表示されます。

ステップ 2　編集するチョークポイントを [MAC Address] 列でクリックします。

ステップ 3　必要に応じて、次のパラメータを編集します。

- Name
- [Entry/Exit Chokepoint]：有効にする場合にクリックします。
- [Range]：チョークポイントのカバレッジ範囲。

（注）　チョークポイントの範囲は製品固有であり、チョークポイントのベンダーにより供給されます。

- Static IP Address

ステップ 4　[Save] をクリックします。

Wi-Fi TDOA 受信機の設定

ここでは、次の内容について説明します。

Wi-Fi TDOA レシーバを使用したタグ位置レポートの強化

Wi-Fi TDOA レシーバは、追跡対象のタグ付き資産から送信される信号を受信するように設計された外部システムです。その後これらの信号は、資産の位置計算に役立つよう、モビリティ サービス エンジンに転送されます。TDOA レシーバは、到達時間差（TDOA）の方法を使用して、タグの位置を計算します。この方法は、最小で 3 つの TDOA レシーバからのデータを使用して、タグ付き資産の位置を生成します。

（注）
- TDOA レシーバが使用中ではなく、パートナー エンジン ソフトウェアがモビリティ サービス エンジンにある場合は、タグの位置計算は、アクセス ポイントからの RSSI の読み取りを使用して生成されます。
- シスコのタグ エンジンは、アクセス ポイントからの RSSI 読み取りを使用してタグの位置を計算できます。

Cisco Unified Wireless Network 内で TDOA レシーバを使用する前に、次の手順を実行する必要があります。

1. ネットワークでモビリティ サービス エンジンをアクティブにします。

   モビリティ サービス エンジンの追加の詳細については、「モビリティ サービス エンジンの追加」（P.16-943）を参照してください。

2. TDOA レシーバを Prime Infrastructure データベースとマップに追加します。

   Prime Infrastructure への TDOA レシーバの追加の詳細については、「Prime Infrastructure およびマップへの Wi-Fi TDOA レシーバの追加」（P.9-519）を参照してください。

3. Prime Infrastructure を使用して MSE でパートナー エンジン サービスをアクティブ化または開始します。

4. Prime Infrastructure およびモビリティ サービス エンジンを同期します。

   同期の詳細は、「サービスの同期化」（P.16-950）を参照してください。

5. AeroScout システム マネージャを使用して TDOA レシーバを設定します。

（注）　設定の詳細については、次の URL にある『*AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide*』を参照してください。
http://support.aeroscout.com。

Prime Infrastructure およびマップへの Wi-Fi TDOA レシーバの追加

AeroScout システム マネージャによって Wi-Fi TDOA レシーバをインストールして設定し、パートナー ソフトウェアをモビリティ サービス エンジンにダウンロードすると、TDOA レシーバをモビリティ サービス エンジン データベースに追加して、Prime Infrastructure マップ上に配置することができます。

TDOA レシーバを Prime Infrastructure マップに追加した後で、Prime Infrastructure ではなく、AeroScout システム マネージャ アプリケーションを使用して TDOA レシーバに対する設定の変更を続行します。

（注）　設定オプションの詳細については、次の URL にある『*AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide*』を参照してください。
http://support.aeroscout.com。

TDOA レシーバを Prime Infrastructure データベースと適切なマップに追加するには、次の手順を実行します。

ステップ 1　[Configure] > [WiFi TDOA Receivers] を選択して、[All WiFi TDOA Receivers] 概要ページを開きます。

（注）　現在の WiFi TDOA レシーバの詳細を表示または編集するには、[MAC Address] リンクをクリックして、詳細ページを開きます。

ステップ 2　[Select a command] ドロップダウン リストから、[Add WiFi TDOA Receivers] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　TDOA レシーバの MAC アドレス、名前、およびスタティック IP アドレスを入力します。

ステップ 5　[OK] をクリックして、TDOA レシーバ エントリをデータベースに保存します。

（注）　TDOA レシーバをデータベースに追加したら、適切な Prime Infrastructure フロア マップに TDOA レシーバを配置できます。その場合は、ステップ 6 に進んでください。

（注）　WiFi TDOA レシーバは、レシーバ ベンダー ソフトウェアを使用して別個に設定する必要があります。

ステップ 6　TDOA レシーバをマップに追加するには、[Monitor] > [Maps] を選択します。

ステップ 7　[Maps] ページで、TDOA レシーバのフロアの位置に対応するリンクを選択します。

ステップ 8　[Select a command] ドロップダウン リストから、[Add WiFi TDOA receivers] を選択します。

ステップ 9　[Go] をクリックします。

（注）　[All WiFi TDOA Receivers] サマリー ページに、データベースには追加されていても、まだマップされていない、最近追加したすべての TDOA レシーバがリストされます。

ステップ 10　マップに追加するには、各 TDOA レシーバの横にあるチェックボックスを選択します。

ステップ 11　[OK] をクリックします。TDOA レシーバ アイコンが左上隅に配置されて、マップが表示されます。これで、マップ上に TDOA レシーバを配置する準備ができました。

ステップ 12　TDOA レシーバ アイコンを左クリックして、フロア マップ上の適切な場所にドラッグして配置します。

（注）　TDOA レシーバ アイコンを配置のためにクリックすると、TDOA レシーバの MAC アドレスと名前が左側のペインに表示されます。

ステップ 13　アイコンが正確にマップに配置されたら、[Save] をクリックします。追加された TDOA レシーバがフロア ヒート マップに表示されます。

（注）　新たに追加された TDOA レシーバのアイコンは、そのフロアの表示設定によって、マップに表示される場合と表示されない場合があります。アイコンが表示されなかった場合は、ステップ 14 に進んでください。

ステップ 14　TDOA レシーバがマップ上に見当たらない場合、[Layers] をクリックして、マップ上で表示できる要素の選択メニューを折りたたみます。

ステップ 15　[WiFi TDOA Receivers] チェックボックスを選択します。TDOA レシーバがマップに表示されます。

（注）　マップ上の TDOA レシーバの上にカーソルを置くと、そのレシーバの設定の詳細が表示されます。

ステップ 16　[Layers] ページを閉じるには、[X] をクリックします。

（注）　すべてのマップについてこの表示基準を保存する場合を除き、[Layers] メニューから [Save Settings] を選択しないでください。

ステップ 17　これで、モビリティ サービス エンジンにパートナー エンジン ソフトウェアをダウンロードできます。

現在の Wi-Fi TDOA レシーバの表示または編集

現在の TDOA レシーバを Prime Infrastructure データベースに表示するには、次の手順を実行します。

ステップ 1　[Configure] > [WiFi TDOA Receivers] を選択して、[All WiFi TDOA Receivers] 概要ページを開きます。

ステップ 2　[MAC Address] リンクをクリックして、MAC アドレス、名前、およびスタティック IP アドレスを含む TDOA レシーバの詳細を表示します。

ステップ 3　レシーバ名または IP アドレスに変更を行った場合は、[Save] をクリックしてこれらの変更を確認します。

（注）　WiFi TDOA レシーバは、レシーバ ベンダー ソフトウェアを使用して別個に設定する必要があります。

Prime Infrastructure およびマップからの Wi-Fi TDOA レシーバの削除

1 つ以上の WiFi TDOA レシーバを同時に削除できます。マップから TDOA レシーバを削除すると、Prime Infrastructure データベース内には残りますが、未割り当てのラベルが付けられます。

Prime Infrastructure から TDOA レシーバを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [WiFi TDOA Receivers] を選択して、[All WiFi TDOA Receivers] 概要ページを開きます。

ステップ 2　削除する各 TDOA レシーバの横にあるチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Remove WiFi TDOA Receivers] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　TDOA レシーバの削除を確認するには、ダイアログボックスで [OK] をクリックします。

[All WiFi TDOA Receivers] ページで、メッセージによって削除を確認します。削除された TDOA レシーバは、ページにリストされなくなります。

スケジュール設定タスクの設定

スケジュール設定タスク機能を使用して、スケジュール設定されたアクセス ポイントのテンプレートおよび設定グループのタスクを表示、変更、および削除できます。[Scheduled Configuration Tasks] ページにアクセスするには、[Configure] > [Scheduled Configuration Tasks] の順に選択します。

ここでは、次の内容について説明します。

- 「AP テンプレート タスク」（P.9-522）
- 「設定グループの設定」（P.9-524）
- 「WLAN 設定のスケジュール設定されたタスク結果の表示」（P.9-526）
- 「ソフトウェア ダウンロード タスク」（P.9-527）

AP テンプレート タスク

[AP Template Tasks] ページを使用して、現在のアクセス ポイント テンプレート タスクを表示、変更、削除、有効化、または無効化できます。[AP Template Tasks] ページにアクセスして現在のアクセス ポイント テンプレート タスクを表示するには、[Configure] > [Scheduled Configuration Tasks] の順に選択します。

- 「現在の AP テンプレート タスクの変更」（P.9-522）
- 「スケジュール設定されたタスクの AP ステータス レポートの表示」（P.9-523）
- 「現在の AP テンプレート タスクの有効化または無効化」（P.9-523）
- AP テンプレート タスク履歴の表示
- 「現在の AP テンプレート タスクの削除」（P.9-524）

現在の AP テンプレート タスクの変更

現在のアクセス ポイント テンプレートのタスクを変更する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　該当するタスクのテンプレート名を選択します。

ステップ 3　[AP Radio/Template] ページで、[Apply/Schedule] タブをクリックします。

ステップ 4　現在のスケジュールまたはアクセス ポイント テンプレートに必要な変更を行い、[Schedule] をクリックします。

スケジュール設定されたタスクの AP ステータス レポートの表示

スケジュール設定されたタスクの AP ステータス レポートには、次の情報が含まれます。

- [AP Name]：スケジュール設定されたアクセス ポイント テンプレートのタスクに含まれるすべてのアクセス ポイントを示します。
- [Ethernet MAC]：該当するアクセス ポイントのイーサネット MAC アドレスを示します。
- [Controller]：該当するアクセス ポイントにアソシエートされたコントローラを示します。
- [Map]：該当するアクセス ポイントのマップの位置を表示します。
- [Status]：アクセス ポイント テンプレートが正常に適用されたかどうかを示します。表示されるステートは、[Not Initiated]、[Success]、[Failure]、[Partial Failure]、および [Not Reachable] です。
- [Task Execution Time]：該当するアクセス ポイントのスケジュール設定されたタスクの実行時間を示します。

スケジュール設定されたタスクに含まれるアクセス ポイントのステータス レポートを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　該当するタスクの [AP Status Report] を選択します。

現在の AP テンプレート タスクの有効化または無効化

現在のアクセス ポイント テンプレート タスクを有効または無効にする手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　有効または無効にするスケジュール済みタスクのチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、必要に応じて [Enable Schedule] または [Disable Schedule] を選択します。

ステップ 4　[Go] をクリックします。

AP テンプレート タスク履歴の表示

以前スケジュール設定したタスク レポートを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　該当するスケジュール済みタスクのチェックボックスを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[View History] を選択します。

ステップ 4　[Go] をクリックします。

現在の AP テンプレート タスクの削除

スケジュール設定されたアクセス ポイント テンプレートのタスクを削除する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。
ステップ 2　該当するスケジュール済みタスクのチェックボックスを選択します。
ステップ 3　[Select a command] ドロップダウン リストから [Delete Task(s)] を選択します。
ステップ 4　[Go] をクリックします。
ステップ 5　[OK] をクリックして、削除を実行します。

設定グループの設定

[Config Group Tasks] ページを使用して、現在の設定グループ タスクを表示、変更、削除、有効化、または無効化できます。[Config Group Tasks] ページにアクセスして、現在の設定グループ タスクを表示する場合、[Configure] > [Scheduled Configuration Tasks] > [ConfigGroup] を選択します。

- 「現在の設定グループ タスクの変更」（P.9-524）
- 「スケジュール設定されたタスクのコントローラ ステータス レポートの表示」（P.9-524）
- 「現在の設定グループ タスクの有効化または無効化」（P.9-525）
- 「設定グループ タスク履歴の表示」（P.9-525）
- 「現在の設定グループ タスクの削除」（P.9-526）

現在の設定グループ タスクの変更

現在の設定グループ タスクを変更する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。
ステップ 2　左側のサイドバー メニューから、[ConfigGroup] を選択します。
ステップ 3　該当するタスクのグループ名を選択します。
ステップ 4　[Config Groups] ページで、[Apply/Schedule] タブをクリックします。
ステップ 5　現在のスケジュールに必要な変更を加えて、[Schedule] をクリックします。

スケジュール設定されたタスクのコントローラ ステータス レポートの表示

スケジュール設定されたタスクのコントローラ ステータス レポートには、次の情報が含まれます。

- [Group Name]：設定グループの名前。
- [Schedule]：タスクが有効か、無効か、または有効期限切れかを示します。
- [Last Run Time]：最後にスケジュール設定されたタスクの日付と時刻を示します。
- [Next Scheduled Run]：次にスケジュール設定されたタスクの日付と時刻を示します。

- [Controller Status Report]：この設定グループのステータス レポートの番号を示します。ステータス レポートを表示するには、番号リンクをクリックします。

コントローラ ステータス レポートを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[ConfigGroup] を選択します。

ステップ 3　該当するタスクの [Controller Status Report] を選択します。[Controller Status Report] には、次の情報があります。

- コントローラ
- タスクのステータス（[Not Initiated]、[Success]、[Failure]、[Partial Failure]、[Partial Success]、[Not Reachable]）
- 適用されているテンプレートの数
- 失敗したテンプレートの数
- タスク実行の日付と時刻

現在の設定グループ タスクの有効化または無効化

現在の設定グループのタスクを有効または無効にする手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[ConfigGroup] を選択します。

ステップ 3　有効または無効にするスケジュール済みタスクのチェックボックスを選択します。

ステップ 4　[Select a command] ドロップダウン リストから、必要に応じて [Enable Schedule] または [Disable Schedule] を選択します。

ステップ 5　[Go] をクリックします。

設定グループ タスク履歴の表示

以前スケジュール設定したタスク レポートを表示する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[ConfigGroup] を選択します。

ステップ 3　該当するスケジュール済みタスクのチェックボックスを選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[View History] を選択します。

ステップ 5　[Go] をクリックします。

現在の設定グループ タスクの削除

スケジュール設定された設定グループ タスクを削除する手順は、次のとおりです。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[ConfigGroup] を選択します。

ステップ 3　該当するスケジュール済みタスクのチェックボックスを選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Delete Task(s)] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

WLAN 設定のスケジュール設定されたタスク結果の表示

（注）　WLAN 設定用のドロップダウン コマンド リストはありません。

スケジュール設定されたすべての WLAN タスクを Prime Infrastructure で表示および管理するには、次の手順を実行します。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから [WLAN Configuration] を選択して、[WLAN Configuration Task List] ページを開きます。

ステップ 3　スケジュール設定された設定タスクが使用可能な場合は、[WLAN Configuration Task List] ページに次のパラメータが表示されます。

- [Schedule Task Name]：スケジュール設定された新規タスクのユーザ定義の名前。
- [Schedule]：スケジュール設定されたタスクのステータスを示します。
- [WLAN Status]：WLAN のステータスを示します。
- [Controller IP Address]：コントローラの IP アドレスを示します。
- [Last Run Time]：最後にスケジュール設定されたタスクの日付と時刻を示します。
- [Next Scheduled Run]：次にスケジュール設定されたタスクの日付と時刻を示します。
- [Recurrence]：タスクが繰り返し実行されるようにスケジュール設定している場合は、その周期（Daily または Weekly）を示します。

ステップ 4　[WLAN Schedule Detail] ページを開くには、[Task Name] リンクを選択します。このページで、スケジュール設定されたタスクの日付と時刻を変更できます。詳細については、「WLAN ステータス スケジュールの管理」（P.9-368）を参照してください。

ステップ 5　スケジュール設定されたタスクのチェックボックスを選択して、[WLAN Configuration Task List] ページにある [Select a command] ドロップダウン リストを使用して、選択したタスクを有効化、無効化、または削除します。

- [Enable Schedule]：サーバでスケジュールが無効になっている場合に、タスクを有効にします。
- [Disable Schedule]：サーバでスケジュール設定されたタスクの実行を無効にします。無効にすると、タスクはスケジュールした時間に実行されません。タスクは後で再度有効にできます。

- [View History]：失敗の理由を含め、個別の WLAN タスクの実行結果を表示します。
- [Delete Task(s)]：選択したタスクを Prime Infrastructure サーバから削除します。

ソフトウェア ダウンロード タスク

この機能を使用すると、ソフトウェアをコントローラにダウンロードするためのタスクをスケジュール設定できます。[Download Software Tasks] ページでは、スケジュール設定されたソフトウェア ダウンロード タスクを追加、削除、表示、有効化、無効化できます。[Download Software Tasks] ページにアクセスし、現在のソフトウェア ダウンロード タスクを表示するには、[Configure] > [Scheduled Configuration Tasks] > [Download Software] の順に選択します。

ここでは、次の内容について説明します。

- 「ソフトウェア ダウンロード タスクの追加」（P.9-527）
- 「ソフトウェア ダウンロード タスクの変更」（P.9-529）
- 「ソフトウェア ダウンロード タスクのコントローラの選択」（P.9-530）
- 「ソフトウェア ダウンロード結果の表示」（P.9-530）
- 「ソフトウェア ダウンロード タスクの削除」（P.9-531）
- 「ソフトウェア ダウンロード タスクの有効化と無効化」（P.9-531）

ソフトウェア ダウンロード タスクの追加

ソフトウェア ダウンロード タスクを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[Download Software] を選択し、[Download Software Task List] ページを開きます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Download Software Task] を選択します。

ステップ 4　[Go] をクリックします。[New Download Software Task] ページが表示されます。

ステップ 5　次の情報を設定します。

- General
  - [Task Name]：スケジュール設定済みタスク名を入力して、当該のスケジュール設定済みソフトウェア ダウンロード タスクを特定します。
- Schedule Details
  - [Download Type]：ダウンロード タイプを選択します。[Download software to controller] チェックボックスをオンにして、コントローラへのソフトウェア ダウンロードをスケジュール設定するか、[Pre-download software APs] チェックボックスをオンにして、ソフトウェア AP の事前ダウンロードをスケジュール設定します。[Download software to controller] を選択した場合、イメージの詳細を指定します。

（注）　事前ダウンロード オプションは、選択したすべてのコントローラがリリース 7.0.x.x 以降を使用している場合のみ表示されます。

（注）　AP ごとの [Image Predownload] ステータスを確認するには、[Administration] > [Background Task] > [AP Image Predownload Task] ページでタスクを有効にし、[Report Launch Pad] から AP Image Predownload レポートを実行します。

- [Reboot Type]：リブート タイプが手動、自動、またはスケジュール設定済みかどうかを示します。

（注）　[Reboot Type] として [Automatic] を設定できるのは、[Download software to controller] オプションが選択されている場合のみです。

- [Download date/time]：表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。
- [Reboot date/time]：このオプションは、[Reboot Type] として [Scheduled] を選択した場合のみ表示されます。表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、コントローラをリブートする日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。

（注）　すべての AP がソフトウェアの事前ダウンロードを完了できるように、ダウンロードとリブートの間に十分な時間（少なくとも 30 分）をスケジュール設定します。

（注）　スケジュール設定されたリブート時刻に、いずれかの AP で事前ダウンロードが進行中の場合、コントローラはリブートしません。そのような場合は、すべての AP の事前ダウンロードが終了するまで待機し、コントローラを手動でリブートします。

- [Notification]（任意）：電子メールで通知を送信する受信者の電子メール アドレスを入力します。

（注）　電子メール通知を受信するには、[Administration] > [Settings] > [Mail Server Configuration] ページで Prime Infrastructure メール サーバを設定します。

- [Image Details]：TFTP、FTP、または SFTP サーバの次の情報を指定します。

（注）　[Schedule Details] グループ ボックスで [Download software to controller] オプションを選択した場合、次の内容を入力します。

[TFTP]：TFTP サーバ情報を指定します。

- [File is Located on] ドロップダウン リストから、[Local machine] または [TFTP server] を選択します。

（注）　TFTP サーバを選択した場合は、[Default Server] を選択するか、[Server Name] ドロップダウン リストから**新しいサーバを追加**します。

- TFTP サーバの IP アドレスを指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。
- 上で [TFTP server] を選択した場合、ファイル名を指定します。

[FTP] : FTP サーバ情報を指定します。

- [FTP Credentials Information] : [FTP] オプション ボタンを選択した場合は、FTP ユーザ名、パスワード、およびポートを入力します。
- [File is Located on] ドロップダウン リストから、[Local machine] または [FTP server] を選択します。

（注） FTP サーバを選択した場合は、[Default Server] を選択するか、[Server Name] ドロップダウン リストから**新しいサーバを追加**します。

- FTP サーバの IP アドレスを指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。
- 上で [FTP server] を選択した場合は、ファイル名を指定します。

[SFTP] : SFTP サーバ情報を指定します。

- [SFTP Credentials Information] : [SFTP] オプション ボタンを選択した場合は、SFTP ユーザ名、パスワード、およびポートを入力します。
- [File is Located on] ドロップダウン リストから､[Local machine] または [SFTP server] を選択します。

（注） SFTP サーバを選択した場合は、[Default Server] を選択するか、[Server Name] ドロップダウン リストから**新しいサーバを追加**します。

- SFTP サーバの IP アドレスを指定します。これは、デフォルトのサーバを選択すると自動的に入力されます。
- ローカル ファイル名を指定するか、[Browse] をクリックして該当するファイルにナビゲートします。
- 上で [SFTP server] を選択した場合は、ファイル名を指定します。

ステップ 6　[Save] をクリックします。

ソフトウェア ダウンロード タスクの変更

ソフトウェア ダウンロード タスクを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[Download Software] を選択します。

ステップ 3　[Task Name] リンクを選択して、[Download Software Task] ページを開きます。

ステップ 4　必要な変更を加えます。

（注）　Enabled 状態のタスクの [Download Type]（[Download]/[Pre-download]）または [Server Type]（[FTP]/[TFTP]）を変更した場合、タスクが Disabled 状態に設定され、既存のすべてのコントローラがタスクから関連付け解除されます。

ステップ 5　[Save] をクリックします。

ソフトウェア ダウンロード タスクのコントローラの選択

このページには、スケジュール設定されたイメージのダウンロードまたは事前ダウンロード タスクで選択できる、サポートされているすべてのコントローラの一覧が表示されます。

スケジュール設定されたイメージのダウンロード用のコントローラを選択するには、次の手順を実行します。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[Download Software] を選択します。

ステップ 3　[Controller] をクリックし、[Download Software Task] 詳細ページを開きます。

ステップ 4　[Download Software Task] 詳細ページで、[Select Controller] をクリックしてコントローラ リストを表示します。

（注）　[Select Controllers] ページにアクセスするためのもう 1 つの方法は、[Configure] > [Scheduled Configuration Tasks] > [Download Software] の順に選択し、Enabled、Disabled、または Expired 状態のダウンロード タスクの [Select Controller] 欄のハイパーリンクをクリックすることです。

（注）　タスクで事前ダウンロード オプションを選択した場合、ソフトウェア リリースが 7.0.x.x 以降のコントローラのみが表示されます。

（注）　到達可能性ステータスが「Unreachable」のコントローラは、ソフトウェア ダウンロード タスクで選択できません。

ステップ 5　必要な変更を加えます。

ステップ 6　[Save] をクリックします。

ソフトウェア ダウンロード結果の表示

[Schedule Run Results] レポートを表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[Download Software] を選択します。

ステップ 3　[Task Name] チェックボックスを選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Schedule Run Results] を選択します。

ステップ 5　[Go] をクリックします。[Schedule Run Results] ページには、次の情報が表示されます。

- [IP Address]：ソフトウェアのダウンロード先のコントローラの IP アドレス。
- [Controller Name]：コントローラの名前。
- [Scheduled Run Time]：ダウンロード処理のスケジュール設定された時刻。
- [Last Updated Time]：スケジュール ダウンロード ステータス（または結果）の最終更新時刻。
- [Transfer Status]：コントローラ内のイメージの現在のダウンロード ステータス。たとえば、[Not Initiated]、[Wrong file Type]、[Writing the code into flash]、[Transfer Successful] になります。
- [Reboot Status]：コントローラのリブート ステータス。たとえば、[NA]（リブート タイプが「Manual」の場合）、[Reboot failed]、[Reboot Successful] になります。
- [Details]：ダウンロードおよびリブート処理に関する詳細ステータス。

ソフトウェア ダウンロード タスクの削除

スケジュール設定されたソフトウェア ダウンロード タスクを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[Download Software] を選択します。

ステップ 3　該当するスケジュール済みタスクのチェックボックスを選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Delete Download Software Task] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

ソフトウェア ダウンロード タスクの有効化と無効化

ソフトウェア ダウンロード タスクを有効または無効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Scheduled Configuration Tasks] を選択します。

ステップ 2　左側のサイドバー メニューから、[Download Software] を選択します。

ステップ 3　有効または無効にするスケジュール済みタスクのチェックボックスを選択します。

ステップ 4　[Select a command] ドロップダウン リストから、必要に応じて [Enable Schedule] または [Disable Schedule] を選択します。

ステップ 5　[Go] をクリックします。

コントローラの自動プロビジョニングの設定

自動プロビジョニングでは、Prime Infrastructure によるワイヤレス LAN コントローラ（WLC）の新規設定や切り替えを自動化できます。Prime Infrastructure の自動プロビジョニング機能を使用すれば、多数のコントローラで構成された顧客環境を簡素化できます。

（注）　自動プロビジョニングの権限を有効にするには、Admin、Root、または SuperUser ステータスでログインしている必要があります。

（注）　ユーザの自動プロビジョニング権限を有効または無効にするには、Prime Infrastructure の [Administration] > [AAA] > [User Groups] > [*group name*] > [List of Tasks Permitted] で、許可されているタスクを編集します。各チェックボックスをオンまたはオフにして、これらの権限の有効と無効を切り替えます。

（注）　コントローラの無線および b/g ネットワークは、Prime Infrastructure のダウンロードされたスタートアップ コンフィギュレーション ファイルで最初は無効になっています。必要に応じて、テンプレートを使用し、それらの無線ネットワークを有効にできます。テンプレートは、自動化されたテンプレートの 1 つとして含まれている必要があります。

（注）　自動プロビジョニング フィルタ コンテンツを指定するには、アプリケーションに直接詳細を入力するか、CSV ファイルから詳細をインポートします。自動プロビジョニング機能は、5500 シリーズのコントローラと 5500 シリーズ以外のコントローラをサポートしています。5500 シリーズ以外のコントローラでは、AP マネージャ インターフェイスのコンフィギュレーション情報が定義されているのに対し、5500 シリーズのコントローラにはこの情報がありません。

Auto Provisioning 機能にアクセスするには、[Configure] > [Controller Auto Provisioning] の順に選択します。

- 自動プロビジョニング デバイス管理（自動プロビジョニング フィルタ リスト）：自動プロビジョニング フィルタを作成および編集し、Prime Infrastructure による自動プロビジョニングまたは自動モニタを有効にするデバイスのリストを定義できるようになります。
- 自動プロビジョニング プライマリ検索キー設定：一致条件の検索順序を設定できるようになります。

自動プロビジョニング デバイス管理（自動プロビジョニング フィルタ リスト）

この機能を使用して、自動プロビジョニング フィルタを作成および編集し、Prime Infrastructure による自動プロビジョニングまたは自動モニタを有効にするデバイスのリストを定義できるようになります。

フィルタ パラメータには、次のものがあります。

- [Filter Name]：フィルタの名前を示します。
- [Filter Enable]：フィルタが有効かどうかを示します。

（注）　有効にしたフィルタだけを自動プロビジョニング プロセスに追加できます。

- [Monitor Only]：選択した場合、このフィルタで定義された WLC は Prime Infrastructure で管理されますが、自動プロビジョニング処理中に WLC が Prime Infrastructure と通信する場合、Prime Infrastructure で設定されることはありません。
- [Filter Mode]：このフィルタの検索モード（[Host Name]、[MAC Address]、または [Serial Number]）を示します。
- [Config Group Name]：設定グループ名を示します。

（注）　自動プロビジョニング フィルタで使用されるすべての設定グループで、コントローラが定義されていてはなりません。

自動プロビジョニングのオプション

[Select a command] ドロップダウン リストには、次のオプションが表示されます。

- [Add Filter]：自動プロビジョニング フィルタを追加します。詳細については、「自動プロビジョニング フィルタの追加」（P.9-533）を参照してください。
- [Delete Filter(s)]：選択した自動プロビジョニング フィルタを削除します。詳細については、「自動プロビジョニング フィルタの削除」（P.9-537）を参照してください。
- [List Filter(s) Device Info]：選択した自動プロビジョニング フィルタの詳細を表示します。詳細については、「自動プロビジョニング フィルタのデバイス情報の一覧表示」（P.9-537）を参照してください。
- [List All Filter(s) Device Info]：すべての自動プロビジョニング フィルタの詳細を表示します。詳細については、「すべての自動プロビジョニング フィルタのデバイス情報の一覧表示」（P.9-538）を参照してください。
- [Export Filter(s) Config (CSV)]：選択した自動プロビジョニング フィルタの詳細をエクスポートできます。詳細については、「自動プロビジョニング フィルタのエクスポート」（P.9-538）を参照してください。
- [Export All Filter(s) Config (CSV)]：すべての自動プロビジョニング フィルタの詳細をエクスポートできます。詳細については、「すべての自動プロビジョニング フィルタのエクスポート」（P.9-539）を参照してください。

ここでは、次の内容について説明します。

自動プロビジョニング フィルタの追加

自動プロビジョニング フィルタを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。[Auto Provisioning Filter List] ページが表示されます

ステップ 2　[Select a command] ドロップダウン リストから [Add Filter] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[Go] をクリックします。[Auto Provisioning Filters] > [New Filter] ページが表示されます。

ステップ 5　次の情報を設定します。

- General
  - [Enable Filter]：新しいフィルタを有効にするには、このチェックボックスをオンにします。

（注）　有効にしたフィルタだけを自動プロビジョニング プロセスに追加できます。

  - [Filter Name]：フィルタ名を入力します。
- Filter Properties
  - [Monitor Only]：選択した場合、このフィルタで定義された WLC は Prime Infrastructure で管理されますが、自動プロビジョニング処理中に WLC が Prime Infrastructure と通信する場合、Prime Infrastructure で設定されることはありません。
  - [Filter Mode]：ドロップダウン リストから、このフィルタの検索モード（[Host Name]、[MAC Address]、または [Serial Number]）を選択します。
  - [Config Group Name]：ドロップダウン リストから設定グループ名を選択します。
- Filter Member Management - Add Member
  - [Input Type]：ドロップダウン リストから、[Single Device] または [CSV File] を選択します。

    [Single Device] を選択した場合は、ホスト名を入力し、LAG 設定を有効にし（該当する場合）、管理インターフェイスの IP アドレス、管理インターフェイスのネットマスク、管理インターフェイスのゲートウェイ、AP マネージャ インターフェイスの IP アドレス、AP マネージャ インターフェイスのネットマスク、AP マネージャ インターフェイスのゲートウェイ、および DHCP IP アドレスを入力します。

    [CSV File] を選択した場合は、CSV ファイルを入力するか、[Browse] ボタンをクリックして目的の CSV ファイルを選択します。

（注）　[Download a sample CSV File] リンクを選択して、サンプル CSV ファイルをコンピュータにダウンロードし、さまざまな設定をカスタマイズできます。

（注）　MS-Excel では、CSV ファイルを編集したときに追加のカンマが挿入されることがあるため、CSV ファイルは通常のテキスト エディタ アプリケーションを使用して編集してください。

CSV ファイルには次のセクションが含まれています。

** 最初の部分は一般的な設定のセクションであり、コントローラのスタートアップ コンフィギュレーション ファイルを構成するために使用されるパラメータが含まれています。
** CSV ファイルの先頭行はキーワードであることが必要です

"!!deviceId, LAG, managementIP, managementVlanId, managementNetmask, managementGateway, apManagerIP, apManagerVlanId, apManagerNetmask,

apManagerGateway, dhcpServerIP"

deviceId：ホスト名、MAC アドレス、シリアル番号のいずれか。
LAG：コントローラの LAG コンフィギュレーション（true または false）。
managementIP：コントローラの管理インターフェイスの IP アドレス。
managementVlanId：コントローラの管理インターフェイスの VLAN ID（0= タグなし）。
managementNetmask：コントローラの管理インターフェイスのネットワーク マスク。
managementGateway：コントローラの管理インターフェイスのゲートウェイ IP。
apManagerIP：コントローラの AP マネージャ インターフェイスの IP アドレス（5500 シリーズ コントローラでは任意）。
apManagerVlanId：コントローラの AP マネージャ インターフェイスの VLAN ID（0= タグなし）（5500 シリーズ コントローラでは任意）。
apManagerNetmask：コントローラの AP マネージャ インターフェイスのネットマスク（5500 シリーズ コントローラでは任意）。
apManagerGateway：コントローラの AP マネージャ インターフェイスのゲートウェイ（5500 シリーズ コントローラでは任意）。
dhcpServerIP：コントローラの DHCP IP アドレス。

** 2 番めの部分は、コントローラの動的インターフェイス パラメータが格納されている動的インターフェイス セクションです。これは任意のセクションです。
** 動的インターフェイスを設定するには、最初の 8 個のパラメータは必須であり、最後の 4 個のパラメータは任意です。

"!!deviceId, interfaceName, vlanId, quarantineVlanId, interfaceIP, interfaceNetmask, gateway, primaryPort, secondaryPort, primaryDHCP, secondaryDHCP, aclName"
deviceId：この deviceId は、セクション 1 で定義されている必要があります。
interfaceName：動的インターフェイスの名前。
vlanId：このインターフェイスで使用される VLAN ID。
quarantineVlanId：このインターフェイスで使用される隔離 VLAN ID。
interfaceIP：動的インターフェイスの IP アドレス。
interfaceNetmask：動的インターフェイスのネットワーク マスク。
gateway：動的インターフェイスのゲートウェイの IP アドレス。
primaryPort：動的インターフェイスで使用される物理プライマリ ポート番号。
secondaryPort：動的インターフェイスで使用される物理セカンダリ ポート番号（任意のフィールド）。
primaryDHCP：動的インターフェイスで使用されるプライマリ DHCP の IP アドレス（任意のフィールド）。
secondaryDHCP：動的インターフェイスで使用されるセカンダリ DHCP の IP アドレス（任意のフィールド）。

** 3 番めの部分は、デバイス固有の設定のセクションであり、自動プロビジョニング中には任意である、その他のデバイス固有の設定パラメータが格納されています。

"!!deviceId, countryCode, mobilityGroupName, mobilityGroupMembers"
deviceId：この deviceId は、セクション 1 で定義されている必要があります。
countryCode：コントローラの国コード（任意のフィールド）。
mobilityGroupName：このコントローラが属するモビリティ グループのデフォルト名（任意のフィールド）。この属性が指定されていない場合、既存のデフォルト モビリティ グループ名が使用されます。
mobilityGroupMembers：セミコロンで区切った、コントローラのモビリティ グループ メンバの IP アドレス、MAC アドレス、およびモビリティ グループ名（任意のフィールド）。モビリ

ティ グループ メンバには、スラッシュで区切った IP アドレスと MAC アドレスの両方が必要です。モビリティ グループ名は、このフィールドの任意の属性です。モビリティ グループ名が存在しない場合、このコントローラのデフォルトのモビリティ グループ名が使用されます。

- [Single Device] オプションを選択した場合、次のオプションを設定します。
  - [Device Type]：ドロップダウン リストから、[5500 Controller] または [non-5500 Controller] を選択します。
  - Host Name
  - [LAG Configuration]：有効または無効。
  - Management Interface IP Address
  - [Management Interface VLAN Id]（0= タグなし）
  - Management Interface Netmask
  - Management Interface Gateway
  - AP Manager Interface IP Address
  - [AP Manager Interface VLAN Id]（0= タグなし）
  - AP Manager Interface Netmask
  - AP Manager Interface Gateway
  - [DHCP IP Address]：リセット後にコントローラが起動したときに、この IP アドレスを使用して DHCP アドレスを取得し、その TFTP サーバを認識し、そこからコンフィギュレーション ファイルを選択します。
  - [Virtual IP Address]：ルーティング可能でないアドレスであり、ワイヤレス クライアントへの仮想 IP アドレスにある DHCP サーバとして、通常は 209.105.170.1 として設定されます。

ステップ 6　[Submit] をクリックします。

（注）　動的インターフェイス コンフィギュレーションとデバイス固有コンフィギュレーションの詳細は、CSV ファイルを入力するときのみ指定します。これら 2 つは、グラフィカル ユーザ インターフェイスでは設定できません。

自動プロビジョニング フィルタの編集

自動プロビジョニング フィルタを編集するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。

ステップ 2　編集するフィルタのフィルタ名を選択します。

ステップ 3　必要に応じて、現在のフィルタ パラメータを変更します。

（注）　フィルタ メンバの詳細情報を表示するには、表示するメンバの [Device ID] チェックボックスをオンにします。
フィルタ メンバを削除するには、次の手順を実行します。[Filter Member Management - Delete Member] グループ ボックスで、削除するメンバのチェックボックスをオンにします。[Submit] をクリックすると、そのメンバが削除されます。

ステップ 4　[Submit] をクリックします。

自動プロビジョニング フィルタの削除

自動プロビジョニング フィルタを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。

ステップ 2　削除するフィルタのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Delete Filter(s)] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[OK] をクリックして、削除を実行します。

自動プロビジョニング フィルタのデバイス情報の一覧表示

個々の自動プロビジョニング フィルタの詳細を表示には、次の手順を実行します。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。

ステップ 2　表示するフィルタのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [List Filter(s) Device Info] を選択します。

ステップ 4　[Go] をクリックします。[Detailed Auto Provisioning Device Information] ページが表示されます。

選択したフィルタに関する次の情報が表示されます。

- [Filter Name]：フィルタ名を示します。
- [Device ID]：デバイス ID を示します。
- [LAG]：コントローラの LAG ステータスを true または false で示します。
- [Management IP]：コントローラの管理インターフェイスの IP アドレスを示します。
- [Management VlanId]：コントローラの管理 VLAN ID を示します。
- [Management Netmask]：コントローラの管理インターフェイスのネットマスク マスクを示します。
- [Management Gateway]：コントローラの管理インターフェイスのネットマスク ゲートウェイを示します。
- [AP Mgr IP]：アクセス ポイント マネージャの IP アドレスを示します。
- [AP Mgr Vlan Id]：アクセス ポイント マネージャの VLAN ID を示します。
- [AP Mgr Netmask]：アクセス ポイント マネージャのネットマスク マスクを示します。
- [AP Mgr Gateway]：アクセス ポイント マネージャのゲートウェイの IP アドレスを示します。
- [Status]：[Idle]、[Trap Received]、[Failed In Trap Processing]、[Failed In Applying Templates]、[Failed In Discovery Switch]、[Managed]、[Managed partially applied templates]、または [Unknown Error] のいずれかです。
- [Country]：国を示します。

- [Mobility Grp]：モビリティ グループの名前を示します。
- [Mobility Grp Members]：モビリティ グループのメンバを示します。
- [Timestamp]：情報の日時を示します。

すべての自動プロビジョニング フィルタのデバイス情報の一覧表示

すべての自動プロビジョニング フィルタの詳細を表示するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから [List All Filter(s) Device Info] を選択します。

ステップ 3　[Go] をクリックします。

選択したフィルタに関する次の情報が表示されます。

- [Filter Name]：フィルタ名を示します。
- [Device ID]：デバイス ID を示します。
- [LAG]：コントローラの LAG ステータスを true または false で示します。
- [Management IP]：コントローラの管理インターフェイスの IP アドレスを示します。
- [Management VlanId]：コントローラの管理 VLAN ID を示します。
- [Management Netmask]：コントローラの管理インターフェイスのネットマスク マスクを示します。
- [Management Gateway]：コントローラの管理インターフェイスのネットマスク ゲートウェイを示します。
- [AP Mgr IP]：アクセス ポイント マネージャの IP アドレスを示します。
- [AP Mgr Vlan Id]：アクセス ポイント マネージャの VLAN ID を示します。
- [AP Mgr Netmask]：アクセス ポイント マネージャのネットマスク マスクを示します。
- [AP Mgr Gateway]：アクセス ポイント マネージャのゲートウェイの IP アドレスを示します。
- [Status]：[Idle]、[Trap Received]、[Failed In Trap Processing]、[Failed In Applying Templates]、[Failed In Discovery Switch]、[Managed]、[Managed partially applied templates]、または [Unknown Error] のいずれかです。
- [Country]：国を示します。
- [Mobility Grp]：モビリティ グループの名前を示します。
- [Mobility Grp Members]：モビリティ グループのメンバを示します。
- [Timestamp]：情報の日時を示します。

自動プロビジョニング フィルタのエクスポート

自動プロビジョニング フィルタをエクスポートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。

ステップ 2　エクスポートするフィルタのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Export Filter(s) Config (CSV)] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　表示される [File Download] ダイアログボックスで、[Save] をクリックしてファイルをコンピュータに保存します。

すべての自動プロビジョニング フィルタのエクスポート

すべての自動プロビジョニング フィルタをエクスポートするには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから [Export All Filter(s) Config (CSV)] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　表示される [File Download] ダイアログボックスで、[Save] をクリックしてファイルをコンピュータに保存します。

自動プロビジョニング プライマリ検索キー設定

[Primary Search Key Setting] では、一致条件の検索順序を設定できます。

検索キー順序を指定する手順は、次のとおりです。

ステップ 1　[Configure] > [Controller Auto Provisioning] を選択します。

ステップ 2　左側のサイドバーのメニューから、[Setting] を選択します。

ステップ 3　該当する検索キーをクリックして、選択します。

ステップ 4　[Move Up] ボタンまたは [Move Down] ボタンを使用して、選択した検索キーの優先順位を変更します。

ステップ 5　[Save] をクリックして変更を確定するか、[Cancel] をクリックして変更を取り消します。

コントローラの冗長性の設定

Prime Infrastructure では、冗長性という用語は、コントローラのハイ アベイラビリティ（HA）フレームワークを指します。ワイヤレス ネットワークの冗長性により、ネットワークのダウンタイムを減らすことができます。冗長性アーキテクチャでは、1 台のコントローラがアクティブ状態で、2 台目のコントローラはスタンバイ状態です。このようにして、冗長ポート経由で常にアクティブ状態のコントローラの稼働状態をモニタします。両方のコントローラは管理インターフェイスの IP アドレスを含め、同じ設定を共有します。

スタンバイ状態またはアクティブ状態のコントローラは、製造時に発注される固有デバイス識別情報（UDI）である、冗長在庫管理単位（SKU）に基づいています。冗長 SKU UDI を持つコントローラは、起動されて永続カウント ライセンスを実行するコントローラとペアになる場合、最初はスタンバイ状態です。永続カウント ライセンスを持つコントローラの場合、コントローラがアクティブ状態であるか、スタンバイ状態であるかを手動で設定できます。

（注）　クライアントのステートフル スイッチオーバーはサポートされていないため、FlexConnect モードのアクセス ポイントでローカルでスイッチされる WLAN 上のクライアントを除く、すべてのクライアントが認証解除され、アクティブ状態の新しいコントローラで強制的に再アソシエーションされることになります。

ここでは、次の内容について説明します。

冗長性の前提条件と制限事項

冗長性を設定する前に、以下の前提条件および制限事項を検討する必要があります。

- 冗長性は、5500、7500、8500、および Wism2 のコントローラでサポートされます。
- プライマリおよびセカンダリ コントローラは、同じハードウェア モデルである必要があります。
- プライマリおよびセカンダリ コントローラは、同じコントローラ ソフトウェア リリースを実行している必要があります。
- 管理、冗長管理、およびピア冗長管理インターフェイスの IP アドレスは、同じサブネット内である必要があります。
- サービス ポートの IP アドレスおよびルート情報はデバイスごとに維持されます。
- 冗長性がコントローラ上で有効な場合、Prime Infrastructure やその他のデバイスでもスタンバイ コントローラを管理できません。
- コントローラがサービス ポートを経由して Prime Infrastructure に追加された場合、コントローラの冗長性は有効にできません。コントローラの冗長性を有効にするには、コントローラを削除し、管理インターフェイスを通じてそのコントローラを追加する必要があります。
- コントローラと Prime Infrastructure 間に監査の不一致がある場合、コントローラでは Prime Infrastructure から冗長パラメータを復元しないでください。ただし、Prime Infrastructure の冗長パラメータを更新できます。
- 冗長性を有効にする前に、各デバイスの証明書をダウンロードする必要があります。
- 設定がネットワークからアクティブ コントローラにダウンロードされ、続いて、詳細が冗長インターフェイス経由でスタンバイ コントローラに転送されます。

- 古いアクティブ コントローラが新しいアクティブ コントローラとペアになると、古いアクティブ コントローラには制御が移らず、新しいアクティブ コントローラのスタンバイ コントローラになります。

冗長インターフェイスの設定

冗長管理インターフェイスと冗長ポート インターフェイスの 2 つの冗長インターフェイスがあります。冗長管理インターフェイスは、管理インターフェイスのサブネット マスク、ゲートウェイ、および VLAN ID を共有するローカル物理管理インターフェイスです。プライマリおよびセカンダリ コントローラの冗長性を有効にするには、冗長管理インターフェイスの IP アドレスだけを設定する必要があります。冗長ポート インターフェイスの IP アドレスは自動生成され、内部的に使用されます。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　プライマリ コントローラとして選択したコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Interfaces] の順に選択します。[Interfaces] リスト ページが表示されます。

ステップ 4　**冗長管理**インターフェイスをクリックします。冗長管理インターフェイスの詳細ページが表示されます。

ステップ 5　[IP Address] フィールドに、管理インターフェイスのサブネットに属している IP アドレスを入力します。

ステップ 6　[Save] をクリックします。

（注）　[Global Configuration] 詳細ページでも冗長管理の IP アドレスを設定できます。[Global Configuration] 詳細ページにアクセスするには、[Configure] > [Controllers] > [*Ctrl IP addr*] > [Redundancy] > [Global Configuration] を選択します。

プライマリ コントローラの冗長性の設定

プライマリまたはアクティブ コントローラの冗長性を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　冗長管理インターフェイスの IP アドレスを設定したプライマリ コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[Global Configuration] 詳細ページが表示されます。

ステップ 4　プライマリ コントローラの冗長モードを有効にする前に、次のパラメータを設定する必要があります。

- [Redundancy-Management IP]：冗長管理インターフェイスの詳細ページで設定した、ローカル物理管理インターフェイスの IP アドレスが表示されます。また、IP アドレスを変更することもできます。
- [Peer Redundancy-Management IP]：ピアの冗長管理インターフェイスの IP アドレスを入力します。
- [Redundant Unit]：[Primary] を選択します。

- [Mobility MAC Address]：冗長ペアの仮想 MAC アドレスを入力します。入力するモビリティ MAC アドレスがプライマリおよびセカンダリの両方のコントローラで同じであることを確認します。

ステップ 5　[Save] をクリックします。冗長モードの [Enabled] チェックボックスが編集可能になります。

ステップ 6　プライマリ コントローラの冗長性を有効にするには、冗長モードの [Enabled] チェックボックスをオンにします。

（注）　冗長性を有効にした後、冗長管理 IP、ピアの冗長管理 IP、冗長装置、およびモビリティ MAC アドレスは変更できません。

（注）　冗長ペアの処理中にこのコントローラを設定できません。

ステップ 7　SSO のドロップダウン リストから [Enable] を選択して AP とクライアント SSO を有効にします。

WLC リリース 7.5 の場合、AP およびクライアント SSO の両方が有効になります。WLC 7.4 および WLC 7.3 の場合、AP SSO のみが有効になります。

SSO をイネーブルにした後、プライマリおよびセカンダリの両方のコントローラがリブートされます。リブート プロセス中に、コントローラは設定に基づいて冗長ポートを介して HA ロールをネゴシエートします。コントローラが冗長ポートまたは冗長マネジメント インターフェイスを介して相互に接続できない場合、スタンバイ コントローラはメンテナンス モードになります。

ステップ 8　[Save] をクリックします。設定が保存され、システムがリブートされます。

セカンダリ コントローラの冗長性の設定

セカンダリまたはスタンバイ コントローラの冗長性を設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　セカンダリ コントローラとして選択したコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[Global Configuration] 詳細ページが表示されます。

ステップ 4　セカンダリ コントローラの冗長モードを有効にする前に、次のパラメータを設定する必要があります。

- [Redundancy-Management IP]：ローカル物理管理インターフェイスの IP アドレスを入力します。この IP アドレスは、プライマリ コントローラのピアの冗長管理インターフェイスの IP アドレスと同じである必要があります。
- [Peer Redundancy-Management IP]：ピアの物理管理インターフェイスの IP アドレスを入力します。この IP アドレスは、プライマリ コントローラのローカル物理冗長管理インターフェイスの IP アドレスと同じである必要があります。
- [Redundant Unit]：[Secondary] を選択します。
- [Mobility MAC Address]：冗長ペアの仮想 MAC アドレスを入力します。入力するモビリティ MAC アドレスがプライマリおよびセカンダリの両方のコントローラで同じであることを確認します。

ステップ 5　[Save] をクリックします。冗長モードの [Enabled] チェックボックスが編集可能になります。

ステップ 6　セカンダリ コントローラの冗長性を有効にするには、冗長モードの [Enabled] チェックボックスをオンにします。

（注）　冗長性を有効にした後、冗長管理 IP、ピアの冗長管理 IP、冗長装置、およびモビリティ MAC アドレスは変更できません。

（注）　冗長ペアの処理中にプライマリ コントローラを設定できません。

ステップ 7　[Save] をクリックします。設定が保存され、システムがリブートされます。

冗長ステートのモニタリングとトラブルシューティング

冗長モードがプライマリおよびセカンダリ コントローラで有効になると、システムがリブートされます。両方のコントローラの冗長ステートは、[Controllers] リスト ページで [Enabled] になります。

（注）　[Controllers] リスト ページの [Redundancy] 列を表示するには、[Edit View] をクリックし、[Show] ボタンを使用して、[Redundancy] を [Hide Information] リスト ボックスから [View Information] リスト ボックスに移動します。[Submit] をクリックします。[Redundancy] 列が [Controllers] リスト ページに表示されます。

スタンバイ コントローラが新しいアクティブ コントローラになると、スイッチ オーバー アクティビティがトリガーされた旨のトラップがトリガーされ、ピア ステートが「Disabled」から「StandbyCold」に、さらに「StandbyHot」に変化すると、プライマリまたはアクティブ コントローラによって冗長コントローラの進行通知トラップがトリガーされます。

アクティブとスタンバイ コントローラ間で矛盾する場合があります。その結果、冗長に失敗します。冗長性障害イベント トラップがトリガーされます。

アラームおよびイベントの詳細情報については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps12239/prod_technical_reference_list.html

ローカルおよびピアのステート、装置、冗長管理の IP アドレス、ピアの冗長管理、冗長ポート、ピアの冗長ポート、ペアのコントローラのピア サービス ポートなど、冗長ステートの詳細を表示できます。これらの詳細を表示するには、[Monitor] > [Controllers] > [*Ctrl IP addr*] > [Redundancy] > [Redundancy States] を選択します。

ピアのステートが [StandbyCold] から [StandbyHot] に変わると、Prime Infrastructure で冗長トラップを見逃すことがります。その結果、冗長ペアの処理を完了できません。この問題を解決するには、冗長ステータスのバックグラウンド タスクを手動で実行する必要があります。

冗長ステータスのバックグラウンド タスクを実行するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　[Other Background Tasks] セクションで、[Redundancy Status] バックグラウンド タスクを選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Execute Now] を選択します。

ステップ 4　[Go] をクリックします。

Prime Infrastructure でトラップを見逃した場合は、このバックグラウンド タスクを実行して、次を完了する必要があります。

- Prime Infrastructure からスタンバイ コントローラを削除します。
- ピア ネットワーク ルート テーブル エントリと、ネットワーク ルート テーブル エントリをスワップします。
- 冗長ステート情報およびシステム インベントリ情報を更新します。

冗長ペアの処理が完了すると、アクティブ コントローラの冗長ステートが [Paired] になり、スタンバイ コントローラは Prime Infrastructure から削除されます。

ピア サービス ポートの IP およびサブネット マスクの設定

ピア コントローラのステートが [StandbyHot] の場合にだけ、ピア サービス ポートの IP アドレスおよびサブネット マスクを設定できます。ピア サービス ポートの IP アドレスを設定する前に、DHCP がローカル サービス ポートで無効になっていることを確認します。

ピア サービス ポートの IP およびサブネット マスクを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　プライマリまたはアクティブ コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[Global Configuration] 詳細ページが表示されます。

ステップ 4　[Peer Service Port IP] フィールドに、ピア サービス ポートの IP アドレスを入力します。

ステップ 5　[Peer Service Netmask IP] フィールドに、ピア サービス サブネット マスクの IP アドレスを入力します。

ステップ 6　[Save] をクリックします。

ピア ネットワーク ルートの追加

ピア コントローラのステートがコントローラがピアになっていることを示す [StandbyHot] の場合にだけ、アクティブ コントローラでピア ネットワーク ルートを追加できます。新しいネットワーク ルート テーブルが維持されます。スタンバイ コントローラがアクティブになると、ネットワーク ルート テーブルのエントリは、ピア ネットワーク ルート テーブルのエントリとスワップされます。

ピア ネットワーク ルートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　冗長管理インターフェイスの IP アドレスを設定したプライマリ コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Redundancy] > [Peer Network Route] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add Peer Network Route] を選択します。

ステップ 5　[Go] をクリックします。[Peer Network Route Details] ページが表示されます。

ステップ 6　次のフィールドを設定します。

- [IP Address]：ピア ネットワーク ルートの IP アドレスを入力します。
- [IP Netmask]：ピア ネットワーク ルートのサブネット マスクを入力します。
- [Gateway IP Address]：ピア ネットワーク ルート ゲートウェイの IP アドレスを入力します。

ステップ 7　[Save] をクリックします。ピア ネットワーク ルートが追加されます。

冗長性のための管理コマンド

スタンバイ コントローラが [StandbyHot] 状態（スタンバイ コントローラがピア）のときに、冗長ペアの処理が完了した場合、**Reset Standby** コマンドを使用してスタンバイ コントローラをリセットできます。また、**Upload File from Standby Controller** コマンドを使用して、スタンバイ コントローラから FTP/TFTP サーバにファイルをアップロードできます。これらのコマンドにアクセスするには、[Configure] > [Controllers] > [*Ctrl IP addr*] > [Redundancy] > [Redundancy Commands] を選択します。

（注）　現在、Prime Infrastructure では SFTP を使用したスタンバイ コントローラからファイルのアップロードはサポートしていません。

コントローラの冗長性の無効化

コントローラの冗長性を無効にするには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　冗長性を無効にするコントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Redundancy] > [Global Configuration] の順に選択します。[Global Configuration] 詳細ページが表示されます。

ステップ 4　選択したコントローラの冗長性を無効にするには、冗長モードの [Enabled] チェックボックスをオフにします。

ステップ 5　[Save] をクリックします。設定が保存され、システムがリブートされます。

コントローラの冗長性を無効にすると、アクティブおよびスタンバイの両方のコントローラがリブートされます。冗長パラメータの監査の不一致を解消するには、デバイスから設定を更新する必要があります。アクティブ コントローラはスタンドアロン コントローラになり、スタンバイ コントローラはポートがすべて無効に設定されてリブートします。

wIPS プロファイルの設定

Prime Infrastructure には、いくつかの定義済みプロファイルが用意されており、そこからプロファイルを選択できます。これらのプロファイル（カスタマー タイプ、ビルディング タイプ、業界タイプなどに基づきます）を使用すると、Cisco Adaptive wIPS を通じて使用可能な追加のワイヤレスの脅威保護をすばやくアクティブにできます。プロファイルは「そのまま」使用することも、要件に合わせてカスタマイズすることもできます。

ヒント　Cisco Adaptive wIPS 機能の詳細については、Cisco.com にアクセスして、マルチメディア プレゼンテーションをご覧ください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールがあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

定義済みのプロファイルには次のものがあります。

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

[wIPS Profiles] ページでは、wIPS プロファイル リストと SSID グループ リストにアクセスできます。[wIPS Profile] ページにアクセスするには、[Configure] > [wIPS Profiles] の順に選択します。

左側のサイドバー メニューから、現在の wIPS プロファイル リストと SSID グループ リストにアクセスできます。

[wIPS Profiles] ページには、デフォルトで [Profile List] が表示されます。[SSID Group List] ページには、左側のサイドバー メニューからアクセスできます。

（注）　Adaptive wIPS は、Prime Infrastructure パーティショニング機能をサポートしていません。

プロファイル リスト

[wIPS Profiles] > [Profile List] ページでは、現在の wIPS プロファイルの表示、編集、適用、削除を行ったり、新しいプロファイルを追加したりできます。

ヒント　Cisco Adaptive wIPS 機能の詳細については、Cisco.com にアクセスして、マルチメディア プレゼンテーションをご覧ください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

Prime Infrastructure の wIPS プロファイル リストにアクセスするには、[Configure] > [wIPS Profiles] の順に選択します。ページのデフォルトは、[wIPS Profiles] > [Profile List] です。[Profile List] が現在表示されていない場合は、左側のサイドメニュー バー [wIPS Profiles] から [Profile List] を選択します。

[Profile List] には、各プロファイルの次の情報が表示されます。

- [Profile Name]：現在のプロファイルのユーザ定義名を示します。プロファイルの詳細を表示または編集するには、プロファイル名をクリックします。

（注）　マウス カーソルをプロファイル名に合わせると、プロファイル ID とバージョンが表示されます。

- [MSE(s) Applied To]：このプロファイルが適用されているモビリティ サービス エンジン（MSE）の数を示します。MSE 番号をクリックすると、プロファイルの割り当ての詳細が表示されます。
- [Controller(s) Applied To]：このプロファイルが適用されているコントローラの数を示します。コントローラ番号をクリックすると、プロファイルの割り当ての詳細が表示されます。

ここでは、次の内容について説明します。

- 「プロファイルの追加」（P.9-547）
- 「プロファイルの削除」（P.9-551）
- 「現在のプロファイルの適用」（P.9-551）

プロファイル エディタを使用すると、新しいプロファイルの作成や現在のプロファイルの変更が可能です。詳細については、「プロファイル エディタ」（P.9-548）を参照してください。

プロファイルの追加

デフォルトまたは事前設定されたプロファイルを使用して、新しい wIPS プロファイルを作成できます。

ヒント　Cisco Adaptive wIPS 機能の詳細については、Cisco.com にアクセスして、マルチメディア プレゼンテーションをご覧ください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

wIPS プロファイルを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] の順に選択します。ページのデフォルトは、[wIPS Profiles] > [Profile List] です。

ステップ 2　[Select a command] ドロップダウン リストから [Add Profile] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[Profile Parameters] ページの [Profile Name] テキスト ボックスにプロファイル名を入力します。

ステップ 5　ドロップダウン リストから、該当する定義済みのプロファイルを選択するか、[Default] を選択します。定義済みのプロファイルには次のものがあります。

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

ステップ 6　次のいずれかを選択します。

- [Save]：プロファイルを、モビリティ サービス エンジンやコントローラを割り当てずに、変更なしで Prime Infrastructure データベースに保存します。プロファイルはプロファイル リストに表示されます。
- [Save and Edit]：プロファイルを保存し、編集します。
- [Cancel]：プロファイルを作成せずに [Profile Parameters] ページを閉じます。

プロファイル エディタ

ヒント　Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

プロファイル エディタを使用すると、次のものを含むプロファイルの詳細を設定できます。

- SSID グループ：SSID グループを追加、編集、または削除します。
- ポリシーの包含：プロファイルに含めるポリシーを決定します。
- ポリシー レベル設定：しきい値、重大度、通知の種類、ACL または SSID グループなど、各ポリシーの設定を行います。
- MSE またはコントローラ アプリケーション：プロファイルを適用するモビリティ サービス エンジンまたはコントローラを選択します。

プロファイルの詳細を設定するには、次の手順を実行します。

ステップ 1　プロファイル エディタにアクセスします。これには、次の 2 つの方法があります。

- 新しいプロファイルを作成するときは、[Profile Parameters] ページで [Save and Edit] をクリックします。
- [Profile List] ページからプロファイル名をクリックします。

ステップ 2　[SSID Groups] ページから、現在のグループの編集および削除、または新しいグループの追加を行うことができます。SSID グループの追加、編集、または削除の詳細については、「[Configure] > [wIPS] > [SSID Group List]」（P.9-552）を参照してください。

ステップ 3　SSID グループを必要に応じて追加または編集した後、次のいずれかを選択します。

- [Save]：SSID グループに対して行った変更を保存します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。
- [Next]：[Profile Configuration] ページに進みます。

ステップ 4　[Profile Configuration] ページでは、現在のプロファイルに含めるポリシーを決定できます。ポリシー ツリーのチェックボックス（左側の [Select Policy] ペインにあります）は、現在のプロファイルで有効または無効になっているポリシーを示します。該当するブランチまたはポリシーのチェックボックスをオンにすることで、必要に応じてブランチ全体または個別のポリシーを有効または無効にできます。

（注）　デフォルトでは、すべてのポリシーが選択されています。

（注）　各 wIPS ポリシーの詳細については、「wIPS ポリシー アラーム リファレンス」（P.18-1071）を参照してください。

ステップ 5　[Profile Configuration] ページで、個々のポリシーをクリックしてポリシーの説明を表示したり、現在のポリシー ルール設定を表示または変更します。

各ポリシーで次のオプションを使用できます。

- [Add]：このポリシーに新しいルールを作成するには、[Add] をクリックして [Policy Rule Configuration] ページにアクセスします。
- [Edit]：このルールの設定を編集するには、該当するルールのチェックボックスをオンにし、[Edit] をクリックして [Policy Rule Configuration] ページにアクセスします。
- [Delete]：削除するルールのチェックボックスをオンにし、[Delete] をクリックします。[OK] をクリックして、削除を実行します。

  （注）　1 つ以上のポリシー ルールが存在する必要があります。リスト内で唯一のポリシー ルールは削除できません。

- [Move Up]：リスト内で上に移動するルールのチェックボックスをオンにします。[Move Up] をクリックします。
- [Move Down]：リスト内で下に移動するルールのチェックボックスをオンにします。[Move Down] をクリックします。

ポリシー レベルで次の設定を行うことができます。

- [Threshold]（すべてのポリシーに適用されるわけではありません）：選択したポリシーに関連付けられたしきい値または上限を示します。ポリシーのしきい値に達すると、アラームが生成されます。

（注）　すべてのポリシーに 1 つ以上のしきい値が含まれている必要があるため、標準的なワイヤレス ネットワークの問題に基づいて、各ポリシーにデフォルトのしきい値が定義されています。

（注）　しきい値オプションは、選択したポリシーに応じて異なります。

（注）　Cisco Adaptive wIPS DoS およびセキュリティ ペネトレーション攻撃からのアラームは、セキュリティ アラームとして分類されます。これらの攻撃の概要は [Security Summary] ページにあります。このページにアクセスするには、[Monitor] > [Security] の順に選択します。wIPS の攻撃は [Threats and Attacks] セクションにあります。

- [Severity]：選択したポリシーの重大度を示します。パラメータとしては、[critical]、[major]、[info]、および [warning] があります。このフィールドの値は、ワイヤレス ネットワークに応じて変わります。
- [Notification]：しきい値に関連付けられた通知の種類を示します。
- [ACL/SSID Group]：このしきい値が適用される ACL または SSID グループを示します。

（注）　選択されたグループに対してのみポリシーが適用されます。

ステップ 6　プロファイルの設定が完了したら、次のいずれかを選択します。

- [Save]：現在のプロファイルに対して行った変更を保存します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。
- [Back]：[SSID Groups] ページに戻ります。
- [Next]：[MSE/Controller(s)] ページに進みます。

ステップ 7　[Apply Profile] ページで、現在のプロファイルを適用するモビリティ サービス エンジンとコントローラのチェックボックスをオンにします。

ステップ 8　該当するモビリティ サービス エンジンとコントローラが選択されている場合、次のいずれかを選択します。

- [Apply]：現在のプロファイルを、選択されたモビリティ サービス エンジンまたはコントローラに適用します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。

（注）　作成したプロファイルは、プロファイル リストから直接適用することもできます。[Profile List] ページから、適用するプロファイルのチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Apply Profile] をクリックします。[Apply Profile] ページにアクセスするには、[Go] をクリックします。

プロファイルの削除

wIPS プロファイルを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。ページのデフォルトは、[wIPS Profiles] > [Profile List] です。

ステップ 2　削除する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Delete Profile] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[OK] をクリックして、削除を実行します。

（注）　プロファイルがコントローラに適用されている場合、そのプロファイルは削除できません。

現在のプロファイルの適用

ヒント　Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

wIPS プロファイルを適用するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。ページのデフォルトは、[wIPS Profiles] > [Profile List] です。

ステップ 2　適用する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Apply Profile] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　プロファイルを適用するモビリティ サービス エンジンとコントローラを選択します。

（注）　新しい割り当てが現在の割り当てと異なる場合、プロファイルを異なる名前で保存するよう求められます

ステップ 6　該当するモビリティ サービス エンジンとコントローラが選択されている場合、次のいずれかを選択します。

- [Apply]：現在のプロファイルを、選択されたモビリティ サービス エンジンまたはコントローラに適用します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。

[Configure] > [wIPS] > [SSID Group List]

SSID（Service Set IDentifier）は、802.11（Wi-Fi）ネットワークを識別するトークンまたはキーです。802.11 ネットワークに参加するには、SSID を知っている必要があります。SSID は、SSID グループリスト機能を使用して、グループとして wIPS プロファイルに関連付けることができます。

SSID グループは、[Global SSID Group List] ページ（[Configure] > [wIPS Profiles] > [SSID Group List]）からインポートするか、[SSID Groups] ページから直接追加することで、プロファイルに追加できます。

ここでは、次の内容について説明します。

- 「グローバル SSID グループ リスト」（P.9-552）
- 「SSID グループ」（P.9-554）

ヒント　Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

グローバル SSID グループ リスト

[SSID Group List] ページでは、グローバル SSID グループを追加または設定できます。このグローバル SSID グループは、後で該当する wIPS プロファイルにインポートできます。

ヒント　Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

[SSID Group List] ページにアクセスするには、[Configure] > [wIPS Profiles] の順に選択します。左側のサイドバー メニューから、[SSID Group List] を選択します。[SSID Group List] ページには、現在の SSID グループとそれに関連付けられた SSID が表示されます。

ここでは、次の内容について説明します。

- 「グループの追加」（P.9-552）
- 「グループの編集」（P.9-553）
- 「グループの削除」（P.9-553）

グループの追加

SSID グループを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。

ステップ 2　左側のサイドバー メニューから、[SSID Group List] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから [Add Group] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　SSID 設定ページで、テキスト ボックスに SSID グループ名を入力します。

ステップ 6　[SSID List] テキスト ボックスに SSID を入力します。SSID が複数ある場合は復帰改行で区切ります。

ステップ 7　終了したら、次のいずれかを選択します。

- [Save]：SSID グループを保存し、SSID グループ リストに追加します。
- [Cancel]：新しい SSID グループを保存せずに SSID 設定ページを閉じます。

（注）　SSID グループをプロファイルにインポートするには、[Configure] > [wIPS Profile] の順に選択します。[SSID Groups] ページを開くには、該当するプロファイルのプロファイル名をクリックします。[Select a command] ドロップダウン リストから、[Add Groups from Global List] を選択します。インポートする SSID グループのチェックボックスをオンにし、[Save] をクリックします。

グループの編集

現在の SSID グループを編集するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。

ステップ 2　左側のサイドバー メニューから、[SSID Group List] を選択します。

ステップ 3　編集する SSID グループのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから [Edit Group] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　SSID 設定ページで、SSID グループ名または SSID リストに必要な変更を行います。

ステップ 7　終了したら、次のいずれかを選択します。

- [Save]：現在の変更内容を保存し、SSID 設定ページを閉じます。
- [Cancel]：変更内容を保存せずに SSID 設定ページを閉じます。

グループの削除

現在の SSID グループを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。

ステップ 2　左側のサイドバー メニューから、[SSID Group List] を選択します。

ステップ 3　削除する SSID グループのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから [Delete Group] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

SSID グループ

[SSID Groups] ページは、プロファイル エディタにアクセスしたときに表示される最初のページです。このページには、現在の wIPS プロファイルに含まれている SSID グループが表示されます。

このページから、現在のプロファイルの SSID グループを追加、インポート、編集、または削除できます。

ヒント　Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html
Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

ここでは、次の内容について説明します。

- 「グループの追加」（P.9-554）
- 「グローバル リストからのグループの追加」（P.9-554）
- 「グループの編集」（P.9-555）
- 「グループの削除」（P.9-555）

グループの追加

SSID グループを現在の wIPS プロファイルに追加するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。
ステップ 2　左側のサイドバー メニューから、[Profile List] を選択します。
ステップ 3　該当する wIPS プロファイルのプロファイル名をクリックします。
ステップ 4　[Select a command] ドロップダウン リストから [Add Group] を選択します。
ステップ 5　[Go] をクリックします。
ステップ 6　SSID 設定ページで、テキスト ボックスに SSID グループ名を入力します。
ステップ 7　[SSID List] テキスト ボックスに SSID を入力します。SSID が複数ある場合はカンマで区切ります。
ステップ 8　終了したら、次のいずれかを選択します。

- [Save]：SSID グループを保存し、SSID グループ リストに追加します。
- [Cancel]：新しい SSID グループを保存せずに SSID 設定ページを閉じます。

グローバル リストからのグループの追加

SSID グループは、グローバル SSID グループ リストからインポートして追加することもできます。グローバル SSID グループ リストの作成の詳細については、「グローバル SSID グループ リスト」（P.9-552）を参照してください。

SSID グループをプロファイルにインポートするには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profile] の順に選択します。

ステップ 2　[SSID Groups] ページを開くには、該当するプロファイルのプロファイル名をクリックします。
ステップ 3　[Select a command] ドロップダウン リストから、[Add Groups from Global List] を選択します。
ステップ 4　インポートする SSID グループのチェックボックスをオンにします。
ステップ 5　[Save] をクリックします。

グループの編集

現在の SSID グループを編集するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。
ステップ 2　左側のサイドバー メニューから、[Profile List] を選択します。
ステップ 3　該当する wIPS プロファイルのプロファイル名をクリックします。
ステップ 4　編集する SSID グループのチェックボックスをオンにします。
ステップ 5　[Select a command] ドロップダウン リストから [Edit Group] を選択します。
ステップ 6　[Go] をクリックします。
ステップ 7　SSID 設定ページで、SSID グループ名または SSID リストに必要な変更を行います。
ステップ 8　終了したら、次のいずれかを選択します。

- [Save]：現在の変更内容を保存し、SSID 設定ページを閉じます。
- [Cancel]：変更内容を保存せずに SSID 設定ページを閉じます。

グループの削除

現在の SSID グループを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [wIPS Profiles] を選択します。
ステップ 2　左側のサイドバー メニューから、[Profile List] を選択します。
ステップ 3　該当する wIPS プロファイルのプロファイル名をクリックします。
ステップ 4　削除する SSID グループのチェックボックスをオンにします。
ステップ 5　[Select a command] ドロップダウン リストから [Delete Group] を選択します。
ステップ 6　[Go] をクリックします。
ステップ 7　[OK] をクリックして、削除を実行します。

ACS View Server の設定

Prime Infrastructure と ACS View Server との間の通信を容易にし、[ACS View Server] タブにアクセスするには、クレデンシャルを使用して View サーバを追加する必要があります。

（注）　Prime Infrastructure では、ACS View Server 5.1 以降のみがサポートされます。

ACS View Server クレデンシャルを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [ACS View Server] を選択します。

ステップ 2　追加する ACS View Server のポート番号を入力します。（一部の ACS View Server は、HTTPS を実行するポートを変更できません）。

ステップ 3　ACS View Server サーバに設定されたパスワードを入力します。パスワードを確認します。

ステップ 4　認証要求がタイムアウトし、コントローラが再送信を試みるまでの時間を秒単位で指定します。

ステップ 5　再試行の回数を指定します。

ステップ 6　[Submit] をクリックします。

ACS View Server クレデンシャルの設定

Prime Infrastructure と ACS View Server との間の通信を容易にし、[ACS View Server] タブにアクセスするには、クレデンシャルを使用して View サーバを追加する必要があります。

ACS View Server クレデンシャルを設定するには、次の手順を実行します。

（注）　Prime Infrastructure では、ACS View Server 5.1 以降のみがサポートされます。

ステップ 1　[Configure] > [ACS View Server] を選択します。

ステップ 2　追加する ACS View Server のポート番号を入力します。（一部の ACS View Server は、HTTPS を実行するポートを変更できません）。

ステップ 3　ACS View Server サーバに設定されたパスワードを入力します。パスワードを確認します。

ステップ 4　再試行の回数を指定します。

ステップ 5　[Submit] をクリックします。

TFTP、FTP、SFTP サーバの設定

TFTP サーバ、FTP サーバ、または SFTP サーバを Prime Infrastructure に追加または削除するには、[Configure] > [TFTP/FTP/SFTP Servers] の順に選択します。

（注）　Prime Infrastructure は統合 TFTP/FTP/SFTP サーバを使用します。これは、サードパーティ製の TFTP サーバ、FTP サーバ、または SFTP サーバも、Prime Infrastructure と同じワークステーション上では実行できないことを意味します。Prime Infrastructure とサードパーティ製 TFTP サーバ、FTP サーバ、または SFTP サーバが同一の通信ポートを使用するためです。

ここでは、次の内容について説明します。

- 「TFTP、FTP、SFTP サーバの追加」（P.9-557）
- 「TFTP、FTP、または SFTP サーバの削除」（P.9-557）

TFTP、FTP、SFTP サーバの追加

TFTP、FTP、SFTP を追加するには、次のステップを実行します。

ステップ 1　[Configure] > [TFTP/FTP/SFTP Servers] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add TFTP/FTP/SFTP Server] を選択します。

ステップ 3　[Server Type] ドロップダウン リストから、[TFTP]、[FTP]、[SFTP]、または [ALL] を選択します。

ステップ 4　TFTP/FTP/SFTP サーバ名を入力します。これは、サーバのユーザ定義名です。

ステップ 5　TFTP/FTP/SFTP サーバの IP アドレスを入力します。

ステップ 6　[Save] をクリックします。

TFTP、FTP、または SFTP サーバの削除

TFTP サーバ、FTP サーバ、または SFTP サーバを削除するには、該当するサーバのチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Delete TFTP/FTP/SFTP Servers] を選択します。[Go] をクリックし、[OK] をクリックして削除を確認します。

CHAPTER 10

クライアントの管理

クライアントは、アクセス ポイントまたはスイッチに接続されたデバイスです。Prime Infrastructure は、有線クライアントとワイヤレス クライアントの両方をサポートしています。コントローラおよびスイッチを Prime Infrastructure に追加すると、クライアント検出プロセスが開始されます。ワイヤレス クライアントは、管理対象のコントローラまたは Autonomous アクセス ポイントから検出されます。ワイヤレス クライアント数には、Autonomous 型のクライアントも含まれます。Prime Infrastructure では、スイッチの場合に限り、デバイスの追加直後にクライアントをポーリングします。コントローラの場合、デバイスは定期的なクライアント ステータス ポーリング時にポーリングされます。Prime Infrastructure では、スイッチからクライアント情報を取得し、データベースにこの情報を更新します。有線クライアントの場合、クライアント アソシエーションを検出するためのクライアント ステータス ポーリングは、2 時間ごとに行われます（デフォルトの場合）。すべてのスイッチについて、接続されているすべての有線クライアントの完全な情報をポーリングする完全ポーリングが、毎日 2 回実施されます。

Prime Infrastructure では、バックグラウンド タスクを使用して、データ ポーリング操作を実行します。クライアントと関連するタスクは 3 つあります。

1. Autonomous AP Client Status
2. Lighweight Client Status
3. Wired Client Status

（注） [Administration] > [Background Tasks] ページからデータ収集タスクをリフレッシュできます（ポーリング間隔など）。詳細については、「バックグラウンド タスクの実行」（P.15-797）を参照してください。

（注） Prime Infrastructure を使用すると、クライアントを追跡でき、このクライアントがネットワークに接続したときに通知を受けることができます。詳細については、「クライアントの追跡」（P.10-587）を参照してください。

（注） 有線クライアントの検出用にスイッチ上でトラップおよび Syslog を有効にするときの詳細については、「クライアントの追跡」（P.10-587）を参照してください。

802.1x を介して認証されないユーザやデバイス（プリンタなど）もあります。その場合は、ネットワーク管理者がデバイスにユーザ名を割り当てできます。詳細については、「不明デバイスの設定」（P.9-510）を参照してください。

クライアント デバイスが Web 認証を介してネットワークに認証される場合、Prime Infrastructure では、クライアントのユーザ名情報を取得できないことがあります（有線クライアントのみ該当）。

クライアント ステータス（有線クライアントのみ該当）は、接続、切断、または不明で示されます。

- [Connected clients]：有線スイッチに接続しているアクティブなクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの SNMP 接続が失われた時点で、不明としてマークされたクライアント。

（注）　クライアントの追跡の詳細については、「不明デバイスの設定」（P.9-510）を参照してください。

Prime Infrastructure は、アイデンティティと非アイデンティティの両方の有線クライアントをサポートしています。有線クライアントのサポートは、アイデンティティ サービスに基づきます。アイデンティティ サービスによって、ユーザおよびデバイスに対するセキュアなネットワーク アクセスが実現される他、ネットワーク管理者は、ユーザの職務権限に基づいて、サービスとリソースをユーザにプロビジョニングできるようになります。

この章の内容は、次のとおりです。

- 「クライアント ロケーション履歴の表示」（P.10-599）
- 「クライアントの音声メトリックの表示」（P.10-599）

[General] ダッシュボード上のクライアント ダッシュレット

（注）　ダッシュボード上のダッシュレットは、インタラクティブ グラフとして表示されます。詳細については、「インタラクティブ グラフ」（P.2-37）を参照してください。

Prime Infrastructure にログインすると、[General] ダッシュボードに、クライアント関連のいくつかのダッシュレットが表示されます。

- [Client Count By Association/Authentication]：選択した期間について、Prime Infrastructure でのアソシエーションおよび認証ごとのクライアントの総数が表示されます。
  - [Associated client]：認証されているかどうかに関係なく接続されているすべてのクライアント。
  - [Authenticated client]：接続されて、認証、許可、およびその他のポリシーをパスし、ネットワークを使用できる状態になったすべてのクライアント。
- [Client Count By Wireless/Wired]：選択した期間について、Prime Infrastructure での有線およびワイヤレスのクライアントの総数が表示されます。

[Client] ダッシュボード

（注）　ダッシュボード上のダッシュレットは、インタラクティブ グラフとして表示されます。詳細については、「インタラクティブ グラフ」（P.2-37）を参照してください。

Prime Infrastructure ホーム ページの [Client] ダッシュボード（ を参照）には、クライアント関連のダッシュレットが表示されます。これらのダッシュレットにより、ネットワーク上のクライアントをモニタできます。グラフ用のデータも定期的にポーリングおよび更新されて、Prime Infrastructure データベースに保存されます。一方、[Client Details] ページにある情報の大部分は、コントローラまたはスイッチから直接ポーリングされます。

[Edit Content] リンクをクリックして、[Client] ダッシュボードに表示するダッシュレットを選択します。[Available dashlets] リストからダッシュレットを選択してクリックすることにより、左方または右方の列に追加できます。[Edit Content] リンクの使用の詳細については、「ダッシュボード」（P.2-23）を参照してください。たとえば、[General] ダッシュボードと [Client] ダッシュボードの両方でクライアント数を参照する場合は、同じダッシュレットを両方に追加できます。

カスタマイズ前の元の [Client] ダッシュボードに戻すには、[Edit Tabs] をクリックしてから、[Reset to Factory Default] をクリックします。

ここでは、[Client] ダッシュボードのダッシュレットについて説明します。内容は次のとおりです。

- 「[Client Troubleshooting] ダッシュレット」（P.10-562）
- 「Client Distribution ダッシュレット」（P.10-562）
- 「[Client Alarms and Events Summary] ダッシュレット」（P.10-563）
- 「[Client Traffic] ダッシュレット」（P.10-564）

- 「[Wired Client Speed Distribution] ダッシュレット」（P.10-564）
- 「Top 5 SSIDs by Client Count」（P.10-564）
- 「Top 5 Switches by Switch Count」（P.10-565）
- 「[Client Posture Status] ダッシュレット」（P.10-565）
- 「Client Count By IP Address Type」（P.10-565）
- 「IPv6 Assignment Distribution」（P.10-565）
- 「User Auth Failure Count」（P.10-565）
- 「Client Protocol Distribution」（P.10-565）
- 「Client EAP Type Distribution」（P.10-566）
- 「Guest Users Count」（P.10-566）
- 「Client CCX Distribution」（P.10-566）
- 「Top N Client Count」（P.10-566）
- 「Client Mobility Status Distribution」（P.10-566）
- 「Client 11u Distribution」（P.10-566）
- 「11u Client Count」（P.10-566）
- 「11u Client Traffic」（P.10-566）
- 「PMIP Clients Distribution」（P.10-566）
- 「PMIP Client Count」（P.10-567）
- 「Top APs By Client Count」（P.10-567）
- 「Most Recent Client Alarms」（P.10-567）
- 「Recent 5 Guest User Accounts」（P.10-567）
- 「Latest 5 logged in Guest Users」（P.10-567）
- 「Clients Detected by Context-Aware Service」（P.10-567）

[Client Troubleshooting] ダッシュレット

クライアントをトラブルシューティングするには、クライアント MAC アドレスを入力し、[Troubleshoot] をクリックします。プロパティ情報が表示されます。

（注）　クライアントが現在アソシエートされていない場合、大部分の情報は表示されません。

クライアントのトラブルシューティングの詳細については、「クライアントのトラブルシューティング」（P.10-580）を参照してください。

Client Distribution ダッシュレット

このダッシュレットには、現在ネットワーク上にあるクライアントの数が表示されます。クライアントの分散方法をプロトコル、EAP タイプ、および認証タイプ別に参照できます。

- Protocol

- [802.11] : ワイヤレス クライアント プロトコル
- [802.3] : 有線クライアント プロトコル

（注）　プロトコルをクリックすると、そのプロトコルに属しているユーザのリストにアクセスできます。たとえば、802.3 プロトコルをクリックすると、[Clients and Users] ページの有線クライアントとユーザのリストに直接アクセスできます。

- [EAP-Type] : EAP-FAST、PEAP などの拡張認証プロトコル（EAP）タイプを表します。
- [Authentication Type] : WPA（TKIP）、WPA2（AES）、オープンなどのタイプを表します。

この情報は、選択により、表形式または円グラフで表示できます。これらの円グラフはクリックできます。円グラフの特定の部分にマウス カーソルを合わせると、見出しと割合が表示されます。円グラフの扇形の 1 つをクリックすると、フィルタされたリストが開きます。[Client Distribution] で示された数（[Client Distribution] ヘッダーの横）をクリックすると、この数によって示されているクライアントのリストが表示されます（[Monitor] > [Clients and Users] を選択した場合と同じページ）。[Dashlet Options] アイコンをクリックし、コントローラ、IP、SSID、またはフロア領域のいずれかを選択することにより、クライアントの分布状況に表示されるデータをフィルタできます。

（注）　[Client Distribution] の数の横に [Edited] というラベルがあれば、ダッシュレットはカスタマイズされています。デフォルト ページにリセットすると、[Edited] ラベルはクリアされます。

クライアント認証タイプの分布

この [Client Authentication Type] グラフには、認証タイプごとのクライアント数が表示されます。この情報は、選択により、表形式または円グラフで表示できます。[Total Clients] で示された数をクリックすると、この数によって示されているクライアントのリストが表示されます（[Monitor] > [Clients and Users] を選択した場合と同じページ）。[Dashlet Options] アイコンをクリックし、コントローラ、IP、SSID、またはフロア領域のいずれかを選択することにより、クライアントの認証タイプの分布状況に表示されるデータをフィルタできます。

[Client Alarms and Events Summary] ダッシュレット

このダッシュレットには、有線とワイヤレスの両方のクライアントについて、最新のクライアント アラームが表示されます。

- クライアント アソシエーションの失敗
- クライアント認証の失敗
- クライアント WEP キー復号化エラー
- クライアント WPA MIC エラー カウンタのアクティブ化
- クライアントの除外
- Autonomous AP クライアント認証の失敗
- 有線クライアント認証の失敗
- 有線クライアント許可の失敗
- 有線クライアントのクリティカル VLAN 割り当て
- 有線クライアントの認証失敗 VLAN 割り当て

- 有線クライアントのゲスト VLAN 割り当て
- 有線クライアントのセキュリティ違反

（注）　アラームおよびイベントの詳細については、「アラームおよびイベント一覧」（P.13-771）を参照してください。

[Total] 列の数字をクリックすると、[Events] ページ（[Monitor] > [Events] を選択した場合と同じページ）が開きます。

[Client Traffic] ダッシュレット

コントローラでは、クライアントごとの転送および受信バイト数のカウンタを保持しています。Prime Infrastructure では、15 分ごとにこの数を読み取り、直前のポーリングと比較して差異を計算します。このクライアント トラフィック データは、次に 1 時間ごと、1 日ごと、および 1 週ごとに集約されます。ダウンストリームとアップストリームの両方のトラフィックについて、平均値および最大値がメガバイト/秒単位で表示されます。この情報は、表形式または面グラフで表示できます。フロアをベースとするグラフを生成する場合、Prime Infrastructure では、このフロア上の全クライアント トラフィックを合算します。[Dashlet Options] アイコンをクリックし、コントローラ、IP、SSID、またはフロア領域のいずれかを選択することにより、クライアント トラフィックに表示されるデータをフィルタできます。

ワイヤレス クライアントの場合、クライアントのトラフィック情報はコントローラから取得します。有線クライアントの場合、クライアントのトラフィック情報は ISE から取得するため、スイッチ上でアカウンティング情報およびその他に必要な機能を有効にする必要があります。

[View History] をクリックすると、さまざまなタイム フレームに対する [Client Traffic Historical Charts] ダッシュレットが表示されます。[Client Traffic Historical Charts] ダッシュレットには、過去 6 時間、過去 1 日間、過去 1 週間、過去 1 ヵ月、および過去 1 年間のクライアント トラフィックが表示されます。青色の線は認証されたクライアントの数を示し、オレンジ色の線はアソシエートされたクライアントの数を示します。右上隅には、グラフの最終更新時刻が表示されます。

[Wired Client Speed Distribution] ダッシュレット

このダッシュレットは、有線クライアントの速度と、速度ごとのクライアント数を表示します。クライアントの実行速度は 3 種類あります。

- 10 Mbps
- 100 Mbps
- 1 Gbps

（注）　ポートは、デフォルトでは、自動ネゴシエーション モードです。たとえば、100 Mbps の速度で稼働するクライアントに対しては、100 Mbps の速度になります。

Top 5 SSIDs by Client Count

このダッシュレットには、現在アソシエートされているクライアントおよび認証されているクライアントの数が表示されます。この情報は、選択により、表形式または面グラフで表示できます。

（注）　Prime Infrastructure 1.0 の場合、WGB、有線ゲスト、および OEAP 600（Office Extended Access Point 600）は、ワイヤレス クライアントとして追跡されます。

Top 5 Switches by Switch Count

このダッシュレットは、クライアントの数が最も多い 5 つのスイッチ、およびスイッチにアソシエートされたクライアントの数を表示します。

[Client Posture Status] ダッシュレット

Prime Infrastructure では、アイデンティティ サービス エンジン（ISE）からポスチャ ステータス情報を収集します。許可と認証のために、ISE を追加する必要があります。ISE の追加については、「アイデンティティ サービス エンジンの追加」（P.16-1050）を参照してください。ISE で、必要な機能を有効にすると、Prime Infrastructure の [Client Posture Status] ダッシュレットにデータが表示されます。

このダッシュレットは、クライアント ポスチャ ステータスと、次の各ステータス カテゴリのクライアント数を表示します。

- Compliant
- Non-compliant
- Unknown
- Pending
- Not Applicable
- Error

Client Count By IP Address Type

このダッシュレットは、各種 IP アドレス タイプ別にクライアント数のトレンドを時系列で示すグラフを表示します。タイプには、IPv4、IPv6、Dual-Stack、および unknown が含まれます。

IPv6 Assignment Distribution

このダッシュレットは、IPv6 アドレスがどのように割り当てられるかに基づき、すべてのクライアントの分布を示す円グラフを表示します。タイプには、Unknown、DHCPv6、Self-Assigned、および SLACC または Static が含まれます。

User Auth Failure Count

このダッシュレットは、ユーザ認証の失敗数のトレンドを時系列で示すグラフを表示します。

Client Protocol Distribution

このダッシュレットは、現在のクライアント数の分散をプロトコル別に表示します。

Client EAP Type Distribution

このダッシュレットは、EAP タイプに基づいた数を表示します。

Guest Users Count

このダッシュレットは、指定した期間にわたるゲスト クライアント数を表示します。

Client CCX Distribution

このダッシュレットは、各種 CCX バージョン間でのクライアントの分布を示す円グラフを表示します。

Top N Client Count

このダッシュレットは、クライアント数に基づいて、上位 N 個の要素を示す棒グラフを表示します。要素には、SSID、AP、コントローラ、エンドポイント タイプ、ベンダー、スイッチ、アンカー コントローラが含まれます。これは異なる個別の Top N グラフを置き換える汎用 Top N グラフです。

Client Mobility Status Distribution

このダッシュレットは、ローカル（非アンカー）とアンカー間でのクライアント分布を示す円グラフを表示します。

Client 11u Distribution

このダッシュレットは、非 11u クライアント上の 11u クライアントを示す円グラフを表示します。

11u Client Count

このダッシュレットは、11u クライアント数のトレンドを時系列で示すグラフを表示します。

11u Client Traffic

このダッシュレットは、11u クライアント トラフィックのトレンドを時系列で示すグラフを表示します。

PMIP Clients Distribution

このダッシュレットは、非 PMIP クライアント上の PMIP クライアントを示す円グラフを表示します。

PMIP Client Count

このダッシュレットは、PMIP クライアント数のトレンドを時系列で示すグラフを表示します。

Top APs By Client Count

このダッシュレットは、上位の AP をクライアント数別に表示します。

Most Recent Client Alarms

このダッシュレットは、最新のクライアント アラームを表示します。

Recent 5 Guest User Accounts

このダッシュレットは、作成または変更された最新のゲスト ユーザ アカウントを表示します。

Latest 5 logged in Guest Users

このダッシュレットは、ログインする最新のゲスト ユーザを表示します。

Clients Detected by Context-Aware Service

このダッシュレットは、過去 15 分間以内にコンテキスト認識型サービスによって検出されたクライアント数を表示します。

クライアントとユーザのモニタリング

クライアントとユーザのモニタ機能を使用すると、ネットワーク内のすべてのクライアント（有線とワイヤレスの両方）を表示できます。クライアント アソシエーション履歴と統計情報を表示することもできます。これらのツールは、ユーザがラップトップ コンピュータを持って建物の中を移動したときに、ネットワークのパフォーマンスについて苦情があった場合に有用です。この情報は、カバレッジが一貫していないエリアや、カバレッジがドロップする可能性があるエリアを評価するために役立ちます。

[Client Detail] ページには、時間ベースのデータを表すためのアソシエーション履歴グラフが表示されます。この情報は、クライアントの問題の特定、診断、および解決に役立ちます。

（注） この章で説明されている機能の一部（無効化、削除など）は、有線クライアントには適用されません。

[Monitor] > [Clients and Users] を選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。[Clients and Users] ページが表示されます。[Clients and Users] ページには、クライアントが表形式で表示されており、表の上部にあるさまざまなツールを使用できます。

ここでは、次の内容について説明します。

クライアントとユーザのフィルタリング

デフォルトの [Clients and Users] リスト ページには、アソシエートされているすべてのクライアントが表示されます。プリセットされた 17 個のフィルタがあり、クライアントのサブセットを表示できます（表 10-1 を参照）。

（注）　WGB、有線ゲスト、および OEAP 600（Office Extended Access Point 600）は、ワイヤレス クライアントとして追跡されます。

（注）　インデックスなしの列でソートを行うと、クライアント一覧ページをロードする際に、重大なパフォーマンスの問題が発生します。Prime Infrastructure では、MAC アドレス、IP アドレス、ユーザ名、AP MAC アドレス、SSID など、インデックス付きの列のソートのみ記憶されます。それでも任意の列でテーブルをソートすることはできます。ただし、列にインデックスが付加されていない場合、このページから移動した後、Prime Infrastructure では、最後に使用した列のソートは記憶されません。

表 10-1 に、[Clients and Users] ページで使用可能なプリセット フィルタを示します。[Show] ドロップダウン リストから、表示するフィルタを選択します。

表 10-1　　クライアント リスト フィルタ

フィルタ	結果
All	非アクティブなクライアントを含むすべてのクライアント。 （注）　通常、「All」フィルタは、フィルタなしを意味します。すべての SSID で、PMIP、WGB、有線ゲスト クライアントなど、すべてのコントローラに接続されているすべてのクライアントが返されます。
2.4 GHz Clients	2.4 GHz 無線帯域を使用しているすべてのクライアント。
5 GHz Clients	5.0 GHz 無線帯域を使用しているすべてのクライアント。
All Lightweight Clients	Lightweight AP に接続されたすべてのクライアント。
All Autonomous Clients	Autonomous AP に接続されたすべてのクライアント。
All Wired Clients	Prime Infrastructure によって管理されているスイッチに直接接続されたすべてのクライアント。

表 10-1　クライアント リスト フィルタ （続き）

フィルタ	結果
Associated Clients	認証されているかどうかにかかわらず、ネットワークに接続されているすべてのクライアントが表示されます。
Clients detected by MSE	有線クライアントおよびワイヤレス クライアントを含め、MSE で検出されたすべてのクライアントが表示されます。
Clients detected in last 24 hours	過去 24 時間に検出されたすべてのクライアント。
Clients Known by ISE	ISE で認証されたすべてのクライアントが表示されます。
Clients with Problems	アソシエートされている一方で、ポリシーが完了していないクライアント。
Excluded Clients	コントローラによって除外された、すべての Lightweight ワイヤレス クライアント。
FlexConnect Locally Authenticated	FlexConnect AP に接続され、ローカルで認証されたクライアント。
New Clients detected in last 24 hours	過去 24 時間に検出された新規クライアント。
On Network Clients	認証および許可を完了しており、データを送受信できるクライアント。つまり、設定されたすべてのポリシーを完了しており、ネットワーク上にあるクライアントです。クライアントはアイデンティティ クライアントではなく、常に「On Network」と表示されます。
WGB Clients	すべての WGB クライアント。 **（注）** ブリッジ機能を持つアクセス ポイントの AP モードに [Bridge] を設定すると、クライアントを WGB として識別して表示できます。WGB クライアントは、無線を有線にブリッジします。Cisco IOS アクセス ポイントはすべて、有線クライアントが接続された無線クライアントとして、WGB のロールを果たすことができます。この WGB についての情報はコントローラに伝えられ、Prime Infrastructure と WLC の両方でクライアントとして表示されます。
All IPv4 Address Clients	IPv4 アドレスを持つクライアント（有線およびワイヤレス）。
All IPv6 Address Clients	IPv6 アドレスを持つクライアント（有線およびワイヤレス）。
All Dual-Stack Clients	IPv4 と IPv6 の両方のアドレスを持つクライアント（有線およびワイヤレス）。

フィルタ アイコン（）を使用して、フィルタのルールと一致するレコードをフィルタすることもできます。フィルタのルールを指定するには、[Show] ドロップダウン リストから [All] を選択してから をクリックします。

（注）　プリセット フィルタを選択してフィルタ アイコンをクリックすると、フィルタ条件は無効になります。そのフィルタ基準は参照可能ですが変更できません。[All] オプションを選択してすべてのエントリを表示し、フィルタ アイコンをクリックすると、クイック フィルタのオプションが表示されます。ここで、フィールドを使用してデータをフィルタできます。自由形式のテキスト ボックスに、表のフィルタリング用のテキストを入力することもできます。

（注）　IPv6 アドレスに対する詳細クライアント フィルタリングを実行する場合、指定する各オクテットは、完全なオクテットである必要があります。オクテットの一部を指定した場合は、フィルタリングで正しい結果が表示されないことがあります。次に、IPv6 アドレスに対する詳細クライアント フィルタリングの動作の例を示します。
この例は、システムに次の IP アドレスがあることを前提としています。

```
10.10.40.1
10.10.40.2
10.10.40.3
10.10.240.1
Fec0::40:20
Fe80::240:20
```

40 を含むすべての IP アドレスを検索すると、次の結果が得られます。

```
10.10.40.1
10.10.40.2
10.10.40.3
Fec0::40:20
```

このフィルタリング機能では、完全なオクテットを入力することを前提としているため、240 を含む IP アドレスはフィルタ基準と一致しません。

クライアントとユーザの表示

（注）　詳細検索機能を使用して、特定のカテゴリおよびフィルタに基づいて、クライアント リストを絞り込むことができます。詳細については、「検索機能の使用方法」（P.2-54）または「Advanced Search」（P.2-55）を参照してください。
[Show] ドロップダウン リストを使用して、現在のリストをフィルタリングすることもできます。詳細については、「クライアントとユーザのフィルタリング」（P.10-568）を参照してください。

（注）　他の使用可能なクライアント パラメータについては、「検索結果表示の設定」（P.10-589）を参照してください。このクライアント リストのフィルタリングについては、「クライアントとユーザのフィルタリング」（P.10-568）を参照してください。

（注）　[Monitor] > [Clients and Users] ページで完全な詳細を表示したり、無線測定などの操作を実行したりするには、ユーザ定義グループのユーザは、[Monitor Clients]、[View Alerts & Events]、[Configure Controllers]、および [Client Location] のページにアクセスする前に権限を必要とします。

クライアントおよびユーザを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。[Clients and Users] ページが表示されます。

[Clients and Users] テーブルにはデフォルトでいくつかの列が表示されます。使用可能な追加の列を表示するには、 をクリックし、[Columns] をクリックします。使用可能な列が表示されます。[Clients and Users] 表に表示する列を選択します。列内の任意の場所をクリックすると、その列が選択され、クライアントの詳細が表示されます。

[Clients and Users] テーブルには、次の列があります。

- [MAC Address] : クライアント MAC アドレス。
- [IP Address] : クライアント IP アドレス。

  [IP Address] 列に表示される IP アドレスは、定義済みの優先順位によって決まります。使用可能な最初の IP アドレスが次の順番で [IP address] フィールドに表示されます。
  - IPv4 アドレス。
  - IPv6 固有グローバル アドレス。このタイプのアドレスが複数ある場合は、クライアントが受信した最新の IPv6 アドレスが表示されます。ユーザがグローバル IPv6 アドレスを 2 つ持っていても、いずれかが期限切れになっている古いルータ アドバタイズメントによって取得したアドレスである場合があるためです。
  - IPv6 固有ローカル アドレス。IPv6 固有ローカル アドレスが複数存在する場合は、最新のアドレスが使用されます。
  - IPv6 リンクローカル アドレス。IPv6 クライアントは、常にリンクローカル アドレスを少なくとも 1 つ持ちます。

  次のようなさまざまな IPv6 アドレス タイプがあります。
  - リンクローカル ユニキャスト：リンクローカル アドレスは、自動アドレス設定、ネイバー探索、ルータが存在しないときなどのために、単一リンクでのアドレス指定に使用するように設計されています。
  - サイトローカル ユニキャスト：サイトローカル アドレスは、グローバル プレフィックスには必要のない、サイト内部でのアドレス指定に使用するように設計されています。
  - グローバル ユニキャスト：グローバル ユニキャスト アドレスは、グローバル ネットワーク内でクライアントを一意に識別します。パブリック IPv4 アドレスと同等です。クライアントは複数のグローバル ユニキャスト アドレスを持つことができます。

  （注）　同じタイプの IP アドレスが複数ある場合は、そのタイプで最新の IP アドレスのみが表示され、それ以外のアドレスは、[QuickView (+)] アイコンにマウス カーソルを合わせたときに [QuickView] ページに表示されます。

- [IP Address Type] : IPv4、IPv6 などの IP アドレス タイプ。
- [PMIP Client] : クライアントが PMIP クライアントかどうかを指定します。
- [PMIP State] : PMIP クライアントの状態。あり得る状態は次のとおりです。
  - [Unknown] : クライアントの状態を判定できないことを示します。
  - [Activated] : クライアントがトンネルを確立する準備ができていることを示します。
  - [Tunneled] : 二方向トンネルが確立されていることを示します。
- [Global Unique] : IPv6 アドレスの集約グローバル ユニキャスト アドレス。このフィールドには、クライアントにグローバル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。

- [Unique Local]：IPv6 アドレスのローカル ユニキャスト アドレス。このフィールドには、クライアントにローカル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
- [Link Local]：IPv6 アドレスのリンクローカル ユニキャスト アドレス。このフィールドには、クライアントにリンクローカル IPv6 アドレスが割り当てられている場合のみ値が入力されます。
- [User Name]：802.1x 認証または Web 認証に基づくユーザ名。ユーザ名を使用しないで接続されたクライアントの場合は [Unknown] と表示されます。
- [Type]：クライアント タイプを示します。
  - Lightweight クライアントを示します
  - 有線クライアントを示します
  - Autonomous クライアントを示します
- [Vendor]：OUI から導き出されたデバイス ベンダー。
- [AP Name]：ワイヤレスのみ
- [Device Name]：WLC、スイッチなどのネットワーク認証デバイス名。
- [Location]：接続しているデバイスのマップ位置。
- [ISE]：[Yes] または [No]。この列は、Prime Infrastructure に追加されている ISE を使用してクライアントが認証されているかどうかを示します。
- [Endpoint Type]：ISE が追加されている場合に限り適用される、ISE によって報告されるエンドポイント タイプ（iPhone、iPad、Windows ワークステーションなど）。

（注）　ポリシーが設定されている場合、ISE が設定されていない場合でもエンドポイント タイプを表示することができます。

- [Posture]：最新のクライアント ポスチャ ステータス
- [SSID]：ワイヤレスのみ
- [Profile Name]：ワイヤレスのみ
- [VLAN]：このクライアントのアクセス VLAN ID を示します。
- [Status]：現在のクライアントのステータス。
  - [Idle]：正常の動作。クライアント アソシエーション要求は拒否されていません。
  - [Auth Pending]：AAA トランザクションを実行しています。
  - [Authenticated]：802.11 認証完了。
  - [Associated]：802.11 アソシエーションが完了しています。これは、現在クライアントがネットワークに接続されていることを示すために有線クライアントでも使用されます。
  - [Power Save]：クライアントを省電力モードで実行しています。
  - [Disassociated]：802.11 ディスアソシエーションが完了しています。これは、現在クライアントがネットワーク上に存在しないことを示すために有線クライアントでも使用されます。
  - [To Be Deleted]：ディスアソシエーション後に削除されるクライアント。
  - [Excluded]：セキュリティの脅威と見なされたため、システムによって自動的に無効化されています。
- [Interface]：クライアントが接続するコントローラ インターフェイス（ワイヤレス）またはスイッチ インターフェイス（有線）。
- Protocol
  - 802.11a

  - 802.11b
  - 802.11g
  - 802.11n (2.4 GHz)
  - 802.11n (5 GHz)
  - 802.11ac
  - [802.3]：有線
  - Mobile
- [Speed]：イーサネット ポートの速度（有線のみ）。ワイヤレスの場合は「N/A」が表示されます。
- [Association Time]：最後のアソシエーションの開始時間（ワイヤレス クライアントの場合）。有線クライアントの場合、これは、クライアントがスイッチ ポートに接続した時間です。クライアントがアソシエートされているが、ネットワーク上で問題がある場合、この列は空になります。
- [Session Length]：セッションの長さ。
- [First Seen]：クライアントが最初に検出された日時が表示されます。
- [Authentication Type]：WPA、WPA2、802.1x、MAC 認証バイパス、または Web 認証。
- [Authorization Profile Names]：ISE によってこのクライアントに適用された許可プロファイル。ISE が追加されており、クライアントが ISE によって認証されている場合に限り、データを含みます。
- [Traffic (MB)]：このセッションの MB 単位のトラフィック（送信または受信）
- [Average Session Throughput (kbps)]：kbps 単位の平均セッション スループット。
- [Automated Test Run]：クライアントが自動テスト モードかどうかを示します。ワイヤレス クライアントのみに適用されます。
- [AP MAC Address]：ワイヤレスのみ。
- [AP IP Address]：ワイヤレスのみ。
- [Anchor Controller]：Lightweight ワイヤレスのみ。
- [On Network]：関連付けられており、必要に応じて認証が正常に完了しているクライアントに対して [Yes] が表示されます。
- [CCX]：Lightweight ワイヤレスのみ。
- [Client Host Name]：有線およびワイヤレス。DNS 逆引きの結果です。
- [Device IP Address]：接続されたデバイスの IP アドレス（WLC、スイッチ、または Autonomous AP）。
- [Port]：WLC 上のスイッチ ポート。
- [E2E]：Lightweight ワイヤレスのみ。
- [Encryption Cipher]：ワイヤレスのみ。
- [MSE]：このクライアントを管理している MSE サーバ。
- [RSSI]：ワイヤレスのみ。
- [SNR]：ワイヤレスのみ。
- [Router Advertisements Dropped]：特定のセッションを対象とする、クライアントごとのドロップされたルータ アドバタイズメントの数。
- [Session ID]：ISE およびスイッチで使用される監査セッション ID。
- [FlexConnect Local Authentication]：このクライアントに対して FlexConnect ローカル認証が有効かどうかを示します。

- [WGB Status]：Work Group Bridge（WGB）モードのステータスを示します。
- [Client Policy Name]：ポリシー名。
- [Policy AAA Role]：ユーザが属するユーザ タイプまたはユーザ グループを指定します。たとえば、学生、従業員。
- [Mobility Status]：ワイヤレス クライアントのモビリティ ステータスを示します。
- [SNMP NAC State]：アウトオブバンド モードの NAC アプライアンスのステータスを示します。

ステップ 2　クライアントまたはユーザを選択します。次の情報が表示されます。

- 「クライアント属性」（P.10-574）
- 「クライアント統計情報」（P.10-576）

（注） [Client Statistics] には、クライアント詳細の表示に続いて統計情報が表示されます。

- 「クライアント アソシエーション履歴」（P.10-576）
- 「クライアント イベント情報」（P.10-577）
- 「クライアント ロケーション情報」（P.10-577）
- 「有線ロケーション履歴」（P.10-577）
- 「クライアント CCXv5 情報」（P.10-578）

次の属性は、ISE が Prime Infrastructure に追加された場合にのみ設定されます。

- ISE
- エンドポイント タイプ
- ポスチャ
- 許可プロファイル名

（注） Prime Infrastructure は、このデータを設定するために、最近 24 時間のクライアント認証レコードを ISE に問い合わせます。Prime Infrastructure での検出の 24 時間前にクライアントがネットワークに接続されていた場合、ISE 関連データはこのテーブルには表示されない場合があります。このデータは、クライアント詳細ページに表示される可能性があります。これを回避するには、クライアントをネットワークに接続し直します。次回のクライアント バックグランド タスクの実行後に、ISE 情報がテーブルに表示されます。

クライアント属性

[Clients and Users] リストからクライアントを選択すると、[Clients and Users] リストにクライアント属性が表示されます。クライアントは、MAC アドレスを使用して特定されます。

（注） [Client Attributes] グループ ボックスに表示される詳細情報はデバイスから取得される一方で、[Clients and Users] リストに表示される詳細情報はデータベースから取得されます。したがって、[Clients and Users] リストと [Client Attributes] グループ ボックスでは、表示される詳細情報が食い違うこと場合があります。

（注）　有線クライアントの場合、この情報はスイッチから取得されます。また、詳細ページに表示されるデータは、コントローラ/スイッチ/ISE からオンデマンドで収集されたライブ データです。

これらの詳細には、次のクライアント詳細が含まれます。

- [General]：ユーザ名、MAC アドレスなどの生成情報をリストします。

  （注）　ユーザ名の横にある アイコンをクリックすると、ユーザの関連するユーザにアクセスします。

- [Session]：クライアント セッション情報をリストします。
- [Security]（ワイヤレス クライアントおよびアイデンティティ有線クライアントのみ）：セキュリティ ポリシー、認証情報、および EAP タイプをリストします。

  （注）　アイデンティティ クライアントは、認証タイプが 802.1x、MAC 認証バイパス、または Web 認証のクライアントです。アイデンティティ クライアント以外の認証タイプは N/A です。

  （注）　[Client Attributes] グループ ボックスに表示されるデータは、クライアントのタイプ、つまりアイデンティティ クライアントなのか非アイデンティティ クライアントなのかに応じて異なります。アイデンティティ クライアントの場合は、認証ステータス、監査セッション ID などのセキュリティ情報を確認できます。

- [Statistics]（ワイヤレスのみ）
- [Traffic]：クライアントのトラフィック情報を表示します。

  （注）　ワイヤレス クライアントの場合、クライアントのトラフィック情報はコントローラから取得します。有線クライアントの場合、クライアントのトラフィック情報は ISE から取得するため、スイッチ上でアカウンティング情報およびその他の必要な機能を有効にする必要があります。

クライアント IPv6 アドレス

[Clients and Users] リストから IPv6 クライアントを選択すると、クライアント IPv6 アドレスの詳細が表示されます。この詳細情報は、コントローラから直接取得されています。

IPv6 アドレスを持つ有線クライアントの場合、Prime Infrastructure では、スイッチ上の IPv6 ネイバーテーブルからクライアント アドレスを検出します。

この詳細には、次の情報が含まれます。

- IP アドレス：クライアントの IPv6 アドレス。
- スコープ
- アドレス タイプ
- 検出時間

クライアント統計情報

クライアント統計情報には、選択したクライアントの次の情報が含まれます。

- クライアント AP アソシエーション履歴
- クライアント RSSI 履歴（dBm）：クライアントがアソシエートされたアクセス ポイントで検出された RSSI（受信信号強度インジケータ）の履歴。
- クライアント SNR 履歴：クライアントがアソシエートされたアクセス ポイントで検出された SNR（クライアント RF セッションの信号対雑音比）の履歴。
- 送受信バイト（Kbps）：アソシエートされたアクセス ポイントで送受信したバイト数。
- 送受信パケット（毎秒）：アソシエートされたアクセス ポイントで送受信したパケット数。
- 経時データ レート

（注）　グラフ上にマウス カーソルを合わせると、その他の統計情報が表示されます。

（注）　この情報は、インタラクティブ グラフで表示されます。詳細については、「インタラクティブ グラフ」（P.2-37）を参照してください。

クライアント アソシエーション履歴

[Association History] ダッシュレットには、選択したクライアントの過去 10 件のアソシエーション時間に関する情報が表示されます。この情報は、クライアントのトラブルシューティングに役立つことがあります。

- クライアント アソシエーション履歴（ワイヤレス クライアントの場合）には、次の情報が含まれます。
  - アソシエーションの日付と時刻
  - アソシエーションの期間
  - ユーザ名
  - IP アドレス
  - アクセス ポイント名
  - コントローラ名
  - SSID
  - プロトコル
  - トラフィックの量（MB）
  - ホスト名
  - ローミング理由（*コントローラから認識されなくなった*、*新規アソシエーションを検出した*など）
- クライアント アソシエーション履歴（有線クライアントの場合）には、次の情報が含まれます。
  - アソシエーションの日付と時刻
  - アソシエーションの期間
  - ユーザ名

- IP アドレス
- アクセス ポイントおよびコントローラ名
- マップ ロケーション
- SSID
- プロトコル
- トラフィックの量（MB）
- ホスト名
- ローミング理由（*コントローラから認識されなくなった*、*新規アソシエーションを検出した*など）

（注）　[Current Associated Clients] テーブルの列を追加、削除、順序変更するには、[Edit View] リンクをクリックします。[Edit View] から追加できる以外の新規パラメータの追加については、「アクセス ポイント リストの表示の設定」（P.5-45）を参照してください。

クライアント イベント情報

[Client Details] ページの [Client Event] ダッシュレットには、イベント タイプやイベントの日時など、このクライアントのすべてのイベントが表示されます。

イベント タイプの詳細を表示するには、イベント タイプをクリックします。詳細については、「障害のあるオブジェクトのモニタリング」（P.5-145）を参照してください。

クライアント ロケーション情報

選択したクライアントの次のロケーション パラメータが表示されます（該当する場合）。

- [Map Area]：クライアントが最後に検出されたマップ領域。
- [ELIN]：緊急ロケーション識別番号。MSE によって検出される有線クライアントのみに適用されます。
- [Civic Address]：[Civic Address] タブにあるフィールドは、クライアントの Civic アドレスがインポートされている場合のみ入力されます。MSE によって検出される有線クライアントのみに適用されます。
- [Advanced]：クライアントの詳細情報。このタブにあるフィールドは、クライアントの Civic アドレスがインポートされている場合のみ入力されます。

クライアントの Civic 情報をインポートするときに詳細については、「スイッチ ロケーションの設定」（P.9-507）を参照してください。

有線ロケーション履歴

有線クライアントのロケーション履歴を表示できます。

（注）　有線クライアントは MSE によって検出されている必要があり、有線クライアントの履歴が MSE で有効化されている必要があります。

クライアントに関する次のロケーション履歴情報が表示されます。

- タイムスタンプ
- ステート
- ポート タイプ
- スロット
- モジュール
- ポート
- ユーザ名
- IP アドレス
- スイッチ IP
- サーバ名
- マップ ロケーション
- 都市ロケーション

ワイヤレス ロケーション履歴

ワイヤレス クライアントのロケーション履歴を表示できます。

（注）　ワイヤレス クライアントは MSE によって検出されている必要があり、有線クライアントの履歴が MSE で有効化されている必要があります。

クライアント CCXv5 情報

CCXv5 クライアントは、Cisco Compatible Extensions バージョン 5（CCXv5）をサポートするクライアント デバイスです。CCXv5 クライアントに固有のレポートにより、クライアントの診断およびトラブルシューティングを強化するクライアントの詳細が提供されます。

（注）　CCXv5 製造元情報は、CCXv5 クライアントの場合のみ表示されます。

特定のクライアント詳細を表示するには、該当する検索パラメータを使用して、クライアント検索を実行します。クライアント検索の実行の詳細については、「クライアント CCXv5 情報」（P.10-578）または 「Advanced Search」（P.2-55）を参照してください。

CCXv5 情報は、[Monitor Clients] > [Client Details] ページに表示されます。CCXv5 情報には次のような内容が含まれます。

CCXv5 製造元情報：

- [Organizationally Unique Identifier]：IEEE によって割り当てられた組織固有識別子。無線ネットワーク接続デバイスの MAC アドレスの最初の 3 バイトなど。
- [ID]：無線ネットワーク アダプタの製造業者 ID。
- [Model]：無線ネットワーク アダプタのモデル。
- [Serial Number]：無線ネットワーク アダプタのシリアル番号。
- [Radio]：クライアントの無線の種類。
- [MAC Address]：クライアントに割り当てられた MAC アドレス。

- [Antenna Type]：無線ネットワーク アダプタに接続されるアンテナの種類。
- [Antenna Gain]：無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 X 0.5 = 2dBi のゲインであることを意味します。

（注）　次の付加的な CCXv5 パラメータを表示するには、[More] をクリックします。

[Automated Troubleshooting Report]：自動テストが実行された場合、このレポートには、自動トラブルシューティングのログである AUTO_TS_LOG<ClientMac>.txt の場所が表示されます。自動テストが実行されていない場合は [Not Exists] が表示されます。

- [Export] をクリックして .zip ファイルを保存します。ファイルには、自動トラブルシューティング レポート、フレーム ログ、およびウォッチ リスト ログの 3 つのログが含まれます。

（注）　[Settings] > [Client] ページでは、診断チャネル上で自動クライアント トラブルシューティングを有効にできます。これらの機能は、Cisco Compatible Extensions クライアント バージョン 5 だけでサポートされています。詳細については、「診断トラップの処理」（P.15-856）を参照してください。

[Radio Receiver Sensitivity]：次の情報を含む、ワイヤレス ネットワーク アダプタの受信装置の感度が表示されます。

- 無線
- データ レート
- 最小および最大 RSSI

[CCXV5 Capability Information]：CCXv5 クライアントに限り、Capability Information パラメータが表示されます。

- Radio
- [Client Status]：成功または失敗。
- [Service Capability]：音声、ストリーミング（一方向）ビデオ、インタラクティブ（双方向）ビデオなどのサービス機能。

[Radio Channels]：該当する各無線のチャネルを識別します。

[Transmit Data Rates]：各無線の伝送データ レート（Mbps）を識別します。

[Transmit Power Values]：次の情報を含む送信電力を示します。

- 電源モード
- 無線
- 電力（dBm）

クライアントとユーザのエクスポート

クライアントとユーザのリストを CSV ファイル（カンマ区切りの値を含むスプレッドシート形式）に簡単にエクスポートできます。

（注）　[Clients and Users] テーブルに表示される列は、CSV ファイルのみにエクスポートされます。

クライアントとユーザのリストをエクスポートするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　ツールバーで アイコンをクリックします。ダイアログボックスが表示されます。

ステップ 3　[File Download] ダイアログボックスで、[Save] をクリックします。

クライアントのトラブルシューティング

トラブルシューティングは、[Client] ダッシュボードで MAC アドレスを入力する、検索機能を使用する、または [Monitor] > [Clients and Users] ページで行を選択するという、複数の方法で開始できます。これらの方法のいずれかにより、クライアントの履歴問題をトラブルシューティングするために必要なすべての情報が提供されます。接続のステータスのモニタ、ユーザの現在および過去のロケーションの確認、クライアントの接続に関する問題のトラブルシューティングができます。クライアント トラブルシューティング オプションは、ユーザが接続の問題を繰り返し経験する場合などに必要になります。[Client Details] ページには、SNR の経時変化、RSSI の経時変化、クライアントの再アソシエーション、クライアントの再認証、およびすべての RRM イベントが表示されます。管理者は、再アソシエーションと再認証を関連付け、問題がネットワークにあるか、クライアントにあるかを判別できます。

（注）　トラブルシューティングできるのは、現在のクライアントの問題のみです。クライアントの履歴上の問題は、トラブルシューティングできません。ただし、ロケーション アシストされるクライアントの場合、ロケーション履歴を確認できます。

（注）　クライアントのトラブルシューティング機能は、アイデンティティ有線クライアントに対してのみ使用できます。この機能は、非アイデンティティ有線クライアントに対しては使用できません。

Prime Infrastructure では、有線およびワイヤレスのデバイスまたはクライアントを統合管理できます。有線クライアントとワイヤレス クライアントの両方をモニタおよびトラブルシューティングできます。SNMP は、クライアントの検出とクライアント データの収集に使用されます。クライアント統計情報およびその他の属性を収集して、関連するダッシュボードのダッシュレットおよびレポートにデータを入力するために、ISE は定期的にポーリングされます。ISE がシステムに追加されており、デバイスを ISE で認証している場合は、[Client Details] ページにセキュリティ情報が表示されます。

[Client Troubleshooting] ツールを起動するには、クライアントを選択してから、トラブルシューティングする IP アドレスの上に表示されている アイコンをクリックします。[Troubleshooting Client] ページが表示されます。

トラブルシューティング ページには、有線クライアントの次の状態が表示されます。

- リンク接続
- 802.1X 認証
- MAC 認証
- Web 認証
- IP 接続
- 許可

- 正常接続

（注）　表示される正確な状態は、そのクライアントで使用しているセキュリティのレベルによって異なります。

クライアントでは、次のセキュリティ メカニズムが使用されます。

- 802.1X
- MAC 認証
- Web 認証

表 10-2 に、セキュリティ タイプに対して有効な状態をまとめてあります。状態は、クライアントのたどる順に並べてあります。

表 10-2　セキュリティ メカニズム

セキュリティ / クライアント状態	リンク接続	802.1X 認証	MAC 認証	Web 認証	IP 接続	許可
802.1X	X	X	–	–	X	X
MAC 認証	X	–	X	–	X	X
Web 認証	X	–	–	X	X	X

表 10-3 に、クライアントが失敗したときの状態に応じた問題と推奨措置をリストします。

表 10-3　クライアントの状態、問題、および推奨措置

クライアントの状態	問題	推奨措置
Link Connectivity	ネットワークでクライアントが見つからない	• クライアントのケーブルがネットワークに接続されているかどうかを確認します。 • クライアントで適切なケーブルを使用してネットワークに接続しているかどうかを確認します。 • クライアントの接続先のポートが管理目的で無効になっていないことを確認します。 • クライアントの接続先のポートがエラーによって無効になっていないことを確認します。 • クライアントの接続先のポートで、速度およびデュプレックスが自動に設定されているかどうかを確認します。
	認証の進行中	• クライアントが長時間この状態の場合は、次の点を確認します。 – クライアント上のサプリカントが必要に応じて適切に設定されているかどうかを確認します。 – 認証方式に関連するタイマーを変更し、再試行します。 – そのクライアントで機能する認証方式が不明な場合は、フォールバック認証機能を使用します。 – 切断と再接続を試行します。
802.1X Authentication	802.1X 認証の失敗	• スイッチから RADIUS サーバに到達可能かどうかを確認します。 • クライアントで選択されている EAP が RADIUS サーバでサポートされているかどうかを確認します。 • クライアントのユーザ名、パスワード、証明書が有効かどうかを確認します。 • RADIUS サーバで使用している証明書をクライアントで受け入れているかどうかを確認します。
MAC Authentication	MAC 認証の失敗	• スイッチから RADIUS サーバに到達可能かどうかを確認します。 • クライアントの MAC アドレスが RADIUS サーバにある既知クライアントのリストにあるかどうかを確認します。 • クライアントの MAC アドレスが除外されたクライアントのリストにないことを確認します。

表 10-3　クライアントの状態、問題、および推奨措置 （続き）

クライアントの状態	問題	推奨措置
Web Authentication	Web/ ゲスト インターフェイスを介してクライアントを認証できない	• ゲスト クレデンシャルが有効であり、期限が切れていないことを確認します。 • クライアントをログイン ページにリダイレクトできるかどうかを確認します。 • RADIUS サーバに到達可能かどうかを確認します。 • ポップアップがブロックされていないことを確認します。 • クライアント上の DNS 解決が機能することを確認します。 • クライアントでいずれのプロキシ設定も使用していないことを確認します。 • クライアントで https://<virtual-ip>/login.html にアクセスできるかどうかを確認します。 • クライアントのブラウザで、コントローラの提供する自己署名証明書を受け入れるかどうかを確認します。
IP Connectivity	クライアントで DHCP インタラクションを完了できない	• DHCP サーバに到達可能かどうかを確認します。 • その WLAN で使用できるように DHCP サーバが設定されているかどうかを確認します。 • DHCP スコープをすべて使用したかどうかを確認します。 • 複数の DHCP サーバでオーバーラップするスコープが設定されているかどうかを確認します。 • DHCP ブリッジ モードが有効にされている（このサーバをセカンドに移動）場合に、ローカル DHCP サーバがあることを確認します。DHCP サーバからアドレスを取得するようにクライアントが設定されていることを確認します。 • クライアントに静的 IP が設定されており、クライアントで IP トラフィックを生成しているかどうかを確認します。
Authorization	許可の失敗	• 許可用に定義されている VLAN がスイッチで使用可能であることを確認します。 • デフォルト ポート ACL が ACL 許可用に設定されていることを確認します。
Successful Connection	なし	なし。

検索機能を使用したクライアントのトラブルシューティング

クライアント検索の主目的はクライアントの場所を見つけることです。検索機能の詳細説明については、「検索機能の使用方法」（P.2-54）を参照してください。

検索機能を使用してクライアントをトラブルシューティングするには、次の手順に従います。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Advanced Search] テキスト ボックスにクライアント MAC アドレスの全体または一部を入力して、[Search] をクリックします。[Search Results] ページが表示されます。

ステップ 3　[View List] をクリックすると、検索基準と一致するクライアントが [Clients] ページに表示されます。[Monitor] > [Clients and Users] ページが表示されます。

（注）　[Reset] リンクをクリックすると、テーブルをデフォルト表示に設定して、検索基準の適用をやめることができます。

ステップ 4　クライアントを選択してから、トラブルシューティングする IP アドレスの上に表示されている  アイコンをクリックします。[Troubleshooting Client] ページが表示されます。Cisco Compatible Extension v5 クライアント（ワイヤレス）をトラブルシューティングする場合は、[Troubleshooting Client] ページに追加のタブが表示されます。

（注）　クライアントがいずれのアクセス ポイントにも接続されていないというメッセージを受け取る場合は、クライアントを接続し直して [Refresh] をクリックします。

（注）　ページの右上隅にある [detach]/[clone] アイコンを使用すると、現在のページを新しいウィンドウまたはタブとして切り離すことができます。

（注）　クライアント トラブルシューティングを起動したページに戻るには、[Go back] をクリックします。たとえば、リスト ページからクライアントのトラブルシューティングを起動した場合、そのリスト ページに戻ることができます。

要約ページでは、問題が簡単に説明され、一連の操作を行うよう推奨されます。

（注）　Windows ワークステーションで Mozilla Firefox 11.0 以降または Internet Explorer 8 以降以外の Web ブラウザを使用している場合、一部の Cisco Compatible Extension 機能は正しく動作しません。

ステップ 5　クライアントに対して記録されたログ メッセージを表示するには、[Log Analysis] タブをクリックします。

ステップ 6　クライアントに関するログ メッセージをコントローラから取得するには、[Start] をクリックします。ログ メッセージの取得を停止するには、[Stop] をクリックします。すべてのログ メッセージをクリアするには、[Clear] をクリックします。

（注）　ログ メッセージは 10 分間取得され、自動的に停止されます。続行するには、[Start] をクリックする必要があります。

ステップ 7　表示するログ メッセージを選択するには、[Select Log Messages] の下にあるいずれかのリンクをクリックします（カッコ内の数字はメッセージの数を示します）。メッセージはグループ ボックス内に表示されます。メッセージに含まれる情報は、次のとおりです。

- ステータス メッセージ
- コントローラの時刻
- 情報またはエラーの重大度レベル（エラーの表示は赤）
- クライアントに接続されているコントローラ

ステップ 8　クライアントのイベント履歴を表示するには、[Event History] タブをクリックします。

[Event History] には、このクライアントの接続イベントに関連するメッセージが表示されます。この例では、クライアントは正常に認証できませんでした。日時情報は、ネットワーク管理者によるこのクライアントのトラブルシューティング用です。

ステップ 9　イベント ログを表示するには、[Event Log] タブをクリックします。クライアントからのログ メッセージの取得を開始するには、[Start] をクリックします。十分な数のメッセージが収集されたら、[Stop] をクリックします。

（注）　クライアント トラブルシューティング イベント ログおよびメッセージング機能は、Management Service のバージョンが 2 以降の場合のみ CCX バージョン 6 クライアントに対して使用できます。

ステップ 10　[ACS View Server] タブをクリックすると、Cisco Access Control System（ACS）View Server と対話できます。このタブには、ACS View サーバまたはアイデンティティ サービス エンジン（ISE）のいずれか（Prime Infrastructure に設定されている方）から受信した最新の認証レコードが表示されます。このタブにアクセスする前に、View Server クレデンシャルを確立する必要があります。（View Server が設定されていない場合、このタブには空白のサーバ リストが表示されます）。クレデンシャル確立の手順は、「ACS View Server クレデンシャルの設定」（P.9-556）を参照してください。

ACS View サーバがすでに設定されている場合は、期間を選択し、[Submit] をクリックして、ACS View サーバから認証レコードを取得できます。Prime Infrastructure では、記録の取得に ACS View NS API が使用されます。

ステップ 11　[Identity Services Engine] タブをクリックすると、ISE 認証に関する情報を表示できます。過去の認証および許可に関する情報を取得する日付と時刻の範囲を入力し、[Submit] をクリックします。照会の結果は、ページの [Authentication Records] 部分に表示されます。

ステップ 12　[CleanAir] タブをクリックすると、電波品質パラメータおよび CleanAir 対応のアクセス ポイントに対するアクティブな干渉に関する情報を表示できます。このタブには、CleanAir 対応のアクセス ポイントによって検出された電波品質に関する次の情報があります。

- [AP Name]：アクセス ポイントの詳細を表示する場合にクリックします。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-56）を参照してください。
- AP MAC Address
- Radio
- [CleanAir Capable]：アクセス ポイントが CleanAir 対応かどうかを示します。
- [CleanAir Enabled]：アクセス ポイントで CleanAir が有効になっているかどうかを示します。
- [Admin Status]：有効または無効。

- [Operational Status]：Cisco Radio の動作ステータス（[Up] または [Down]）を表示します。
- [Channel]：Cisco 無線がブロードキャストしているチャネル。
- [Extension Channel]：Cisco Radio がブロードキャストしているセカンダリ チャネルを示します。
- [Channel Width]：この無線インターフェイスのチャネル帯域幅を示します。チャネル帯域幅の設定の詳細については、「802.11a/n RRM 動的チャネル割り当ての設定」（P.9-422）を参照してください。
- [Power Level]：アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。
- 電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。
- [Average AQ Index]：Air Quality インデックスの平均値。
- [Minimum AQ Index]：Air Quality インデックスの最小値。

アクティブな干渉に関する次の情報が表示されます。

- [Interferer Name]：干渉デバイスの名前。
- [Affected Channels]：干渉デバイスが影響を与えているチャネル。
- [Detected Time]：干渉源が検出された時刻。
- [Severity]：干渉デバイスの重大度インデックス。
- [Duty Cycle(%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- [RSSI(dBm)]：干渉しているデバイスの受信信号強度。
- Air Quality インデックスの詳細を参照するには、[CleanAir Details] をクリックします。

ステップ 13　（任意）Cisco Compatible Extension バージョン 5 またはバージョン 6 クライアントが使用可能な場合、[Test Analysis] タブをクリックできます。

（注）　クライアント トラブルシューティング テスト解析機能は、Management Service のバージョンが 2 以降の場合のみ CCX バージョン 6 クライアントに対して使用できます。

[Test Analysis] タブにより、クライアントでさまざまな診断テストを実行することができます。適用可能な診断テストのチェックボックスをオンにし、該当するすべての入力情報を入力して、[Start] をクリックします。次のような診断テストが用意されています。

- [DHCP]：完全な DHCP の Discover/Offer/Request/ACK 交換を実行し、コントローラとクライアント間で DHCP が正常に動作しているかどうかを判別します。
- [IP Connectivity]：クライアントに DHCP テストで取得したデフォルト ゲートウェイの ping テストを実行させ、ローカル サブネットに IP 接続が存在しているかどうかを確認します。
- [DNS Ping]：クライアントに DHCP テストで取得した DNS サーバの ping テストを実行させ、DNS サーバとの IP 接続が存在しているかどうかを確認します。
- [DNS Resolution]：DNS クライアントに解決可能であることがわかっているネットワーク名の解決を試行させ、名前解決が正常に機能しているかどうかを確認します。
- [802.11 Association]：特定のアクセス ポイントとのアソシエーションを完了させ、クライアントが指定した WLAN と適切にアソシエートできるかどうかを確認します。
- [802.1X Authentication]：特定のアクセス ポイントとのアソシエーションおよび 802.1X 認証を完了させ、クライアントが適切に 802.1X 認証を完了できるかどうかを確認します。

- [Profile Redirect]：診断システムは、いつでもクライアントに対して、設定済み WLAN プロファイルのいずれかをアクティブにし、そのプロファイルにより動作を継続するよう指示できます。

（注）　プロファイルの診断テストを実行する場合、クライアントは診断チャネル上になければなりません。このテストでは、プロファイル番号を入力として使用します。ワイルドカード リダイレクトを指定するには、0 を入力します。このリダイレクトによって、クライアントは診断チャネルとのアソシエーションを解除し、任意のプロファイルとアソシエートすることを求められます。また、有効なプロファイル ID を入力することもできます。テストが実行されているときにクライアントが診断チャネル上にあるため、プロファイル リストで返されるプロファイルは 1 つだけです。プロファイル リダイレクト テストでは、このプロファイル ID を使用する必要があります（ワイルドカード リダイレクトが必要でない場合）。

ステップ 14　（任意）Cisco Compatible Extension バージョン 5 またはバージョン 6 クライアントが使用可能な場合は、[Messaging] タブが表示されます。このタブを使用して、即時にテキスト メッセージをこのクライアントのユーザに送信できます。[Message Category] ドロップダウン リストからメッセージを選択し、[Send] をクリックします。

（注）　クライアント トラブルシューティング イベント ログおよびメッセージング機能は、Management Service のバージョンが 2 以降の場合のみ CCX バージョン 6 クライアントに対して使用できます。

ステップ 15　[Identity Services Engine] タブをクリックすると、アイデンティティ サービス パラメータに関する情報を表示できます。このタブにアクセスするには、まずアイデンティティ サービス エンジン（ISE）を設定する必要があります。（ISE が設定されていない場合、このタブのサーバ リストは空になります）。

（注）　ISE が設定されていない場合は、ISE を Prime Infrastructure に追加するためのリンクが表示されます。

ISE では、REST API を介して Prime Infrastructure に認証レコードを渡します。ネットワーク管理者は ISE から認証レコードを取得するための期間を選択できます。

ステップ 16　クライアント ロケーションの履歴を表示するには、[Context-Aware History] タブをクリックします。

ステップ 17　[Troubleshooting Client] ページを閉じます。

クライアントの追跡

この機能を使用すると、クライアントを追跡でき、このクライアントがネットワークに接続したときに通知を受けることができます。

クライアントを追跡するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。

ヒント このテーブルは、最大 2000 行に対応しています。新規の行を追加またはインポートするには、古いエントリをいくつか削除する必要があります。

ステップ 3　単一のクライアントを追跡するには、[Add] をクリックしてから、次のパラメータを入力します。

- Client MAC address
- [Expiration] : [Never] を選択するか、日付を入力します。

ステップ 4　複数のクライアントを追跡するには、[Import] をクリックします。これにより、CSV ファイルからクライアント リストをインポートできます。MAC アドレスおよびユーザ名を入力します。

データ形式を規定した、サンプル CSV ファイルをダウンロードできます。

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

通知設定

クライアント追跡用の通知設定を指定するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。

ステップ 3　通知設定を指定する、追跡されるクライアントを選択します。

ステップ 4　通知設定を指定します。通知のオプションは 3 つあります。

a. [Purged Expired Entries] : 追跡対象クライアントを Prime Infrastructure データベースに保持する期間を設定できます。クライアントは、次の期間で削除できます。

- 1 週間後
- 2 週間後
- 1 ヵ月後
- 2 ヵ月後
- 6 ヵ月後
- 無期限で保持

b. [Notification Frequency] : Prime Infrastructure で追跡対象クライアントの通知をいつ送信するかを指定できます。

- 最初の検出時
- 検出ごと

c. [Notification Method] : 追跡対象クライアント イベントによりアラームを生成するか、電子メールを送信するか指定できます。

ステップ 5　[Save] をクリックします。

不明ユーザの識別

802.1x を介して認証されないユーザやデバイス（プリンタなど）もあります。その場合は、ネットワーク管理者がデバイスにユーザ名を割り当てできます。

クライアント デバイスが Web 認証を介してネットワークに認証される場合、Prime Infrastructure では、クライアントのユーザ名情報を取得できないことがあります（有線クライアントのみ該当）。

クライアントは、有線スイッチとの NMSP 接続が失われた時点で、不明としてマークされます。クライアント ステータス（有線クライアントのみ該当）は、接続、切断、または不明で示されます。

- [Connected clients]：有線スイッチに接続しているアクティブなクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、不明としてマークされたクライアント。

不明なデバイスを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Identify Unknown Users] をクリックします。

ステップ 3　クライアント MAC アドレスをユーザ名に割り当てるには、[Add] をクリックします。

ステップ 4　MAC アドレスおよびユーザ名を入力します。

（注）　クライアントおよび MAC アドレスが追加されると、Prime Infrastructure では、MAC アドレスの照合に基づくクライアントの検索に、このデータが使用されます。

ステップ 5　[Add] をクリックします。

ステップ 6　ステップ 3 からステップ 5 を繰り返して、各クライアントの MAC アドレスおよび対応するユーザ名を入力します。

ステップ 7　[Save] をクリックします。

（注）　このテーブルは、最大 10,000 行に対応しています。新規の行を追加またはインポートするには、古いエントリをいくつか削除する必要があります。

検索結果表示の設定

[Edit View] ページでは、[Clients] テーブルの列を追加、削除、または並べ替えができます。

[Clients] テーブルの使用可能な列を編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Edit View] リンクをクリックします。

ステップ 3　[Clients] テーブルに新しい列を追加するには、左側の領域で、追加する列見出しをクリックして選択します。[Show] をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が [Clients] テーブルに表示されます。

ステップ 4　[Clients] テーブルから列を削除するには、右側の領域で、削除する列見出しをクリックして選択します。[Hide] をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目は [Clients] テーブルに表示されません。

ステップ 5　[Up] ボタンと [Down] ボタンを使用して、表内での情報の並び順を指定します。目的の列見出しを選択し、[Up] または [Down] をクリックして、現在のリスト内での位置を変更します。

ステップ 6　デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7　[Submit] をクリックして、変更内容を確定します。

（注）　付加的なクライアント パラメータには、AP MAC Address、Anchor Controller、Authenticated、CCX、Client Host Name、Controller IP Address、Controller Port、E2E、Encryption Cipher、MSE、RSSI、SNR、および FlexConnect Local Authentication があります。

自動クライアント トラブルシューティングの有効化

[Settings] > [Client] ページでは、診断チャネルでの自動クライアント トラブルシューティングを有効にできます。これらの機能は、Cisco Compatible Extensions クライアント バージョン 5 だけでサポートされています。

自動クライアント トラブルシューティングを有効にするには、次の手順を実行します。

ステップ 1　[Administration] > [Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Client] を選択します。

ステップ 3　[Automatically troubleshoot client on diagnostic channel] チェックボックスをオンにします。

（注）　このチェックボックスがオンの場合、Prime Infrastructure は診断アソシエーション トラップを処理します。このチェックボックスがオフの場合、Prime Infrastructure はトラップを発生させますが、自動トラブルシューティングは開始されません。

ステップ 4　[Save] をクリックします。

アクセス ポイント ページでのクライアント詳細の表示

アクセス ポイント ページからクライアント情報を表示することもできます。[Monitor] > [Access Points] の順に選択します。アクセス ポイントの詳細を参照するには、その列のアクセス ポイント URL をクリックします。[Current Associated Clients] タブをクリックします。

現在アソシエートされているクライアントの表示

スイッチ詳細ページから現在アソシエートされているクライアント（有線）を表示することもできます。[Monitor] > [Controllers] の順に選択し、IP アドレスを選択し、左側のサイドバーのメニューから [Clients] > [Current Associated Clients] を選択します。

クライアント レポートの実行

Busiest Clients、Client Count、Client Sessions、Client Summary、Throughput、Unique Clients と v5 クライアントの統計などクライアント レポートをレポート ラウンチ パッドから実行できます。「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。

ISE レポートの実行

レポート ラウンチ パッドから ISE レポートを起動することもできます。「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。ISE レポートの実行の詳細については、ISE オンライン ヘルプを参照してください。

クライアント設定の指定

[Administration] > [Settings] > [Client] ページでは、さまざまなクライアント設定を指定できます。詳細については、「クライアントの設定」（P.15-856）を参照してください。

クライアントの無線測定の受信

クライアント ページで、無線測定を受信できるのは、クライアントが Cisco Compatible Extensions v2（以上）であり、Associated 状態（有効な IP アドレスを持つ）である場合だけです。測定が問い合わせられたときクライアントがビジー状態の場合、測定を引き受けるかどうかが検討されます。クライアントが測定の実行を拒否する場合、クライアントからのデータは表示されません。

（注） この機能は、Foundation サービスのバージョンが 1 以降の場合のみ、CCX バージョン 6 クライアントで使用できます。

無線測定を受信するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

（注） Prime Infrastructure 検索機能を使用して特定のクライアントの検索を実行することもできます。詳細については、「検索機能の使用方法」（P.2-54）または「Advanced Search」（P.2-55）を参照してください。

ステップ 3　[Test] ドロップダウン リストから [Radio Measurement] を選択します。

（注）　[Radio Measurement] オプションは、クライアントが Cisco Compatible Extensions v2（以上）であり、Associated 状態（有効な IP アドレスを持つ）である場合に限り表示されます。

ステップ 4　このチェックボックスをオンにして、ビーコンの測定、フレームの測定、チャネルの負荷、またはノイズ ヒストグラムを指定するかどうかを示します。

ステップ 5　[Initiate] をクリックします。測定が異なると、生成される結果も異なります。詳細については、「クライアントの無線測定の結果」（P.10-592）を参照してください。

（注）　測定には、約 5 ミリ秒かかります。Prime Infrastructure からのメッセージにより、進捗状況が示されます。クライアントが測定を実行しないと選択した場合は、そのことが通知されます。

クライアントの無線測定の結果

要求した測定のタイプに応じて、次のような情報が表示されます。

- Beacon Response
  - [Channel]：この測定に対するチャネル数
  - [BSSID]：ビーコンまたはプローブの応答を送信したステーションの 6 バイトの BSSID
  - [PHY]：物理メディアの種類（FH、DSS、OFDM、高いデータレートの DSS または ERP）
  - [Received Signal Power]：ビーコンまたはプローブの応答フレームの dBm 単位の強度
  - [Parent TSF]：サービス中のアクセス ポイントの TSF 値の下位 4 バイト
  - [Target TSF]：ビーコンまたはプローブの応答に含まれている 8 バイトの TSF 値
  - [Beacon Interval]：受信したビーコンまたはプローブの応答に含まれる 2 バイトのビーコン間隔
  - [Capability information]：ビーコンまたはプローブの応答に含まれている情報
- Frame Measurement
  - [Channel]：この測定に対するチャネル番号
  - [BSSID]：受信したデータ フレームの MAC ヘッダーに含まれる BSSID
  - [Number of frames]：送信アドレスから受信したフレームの数
  - [Received Signal Power]：802.11 フレームの dBm での信号強度
- Channel Load
  - [Channel]：この測定に対するチャネル数
  - [CCA busy fraction]：上限と定義された測定時間のうち、チャネルがビジーであると CCA が示した時間の長さの割合（チャネルがビジーであると CCA が示した時間の長さに 255 を乗算して測定時間で除算した数値）
- Noise Histogram
  - [Channel]：この測定に対するチャネル数
  - 8 つの各電力範囲における RPI 密度

クライアント V5 統計の表示

[Statistics request] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[Test] ドロップダウン リストから [V5 Statistics] を選択します。

（注）　このメニューは、CCX v5 以降のクライアントだけに表示されます。

ステップ 4　[Go] をクリックします。

ステップ 5　必要な統計のタイプ（[Dot11 Measurement] または [Security Measurement]）を選択します。

ステップ 6　[Initiate] をクリックして測定を開始します。

（注）　測定期間は 5 秒間です。

ステップ 7　要求した V5 統計のタイプに応じて、次のカウンタが結果ページに表示されます。

- Dot11 測定
  - 送信フラグメント数
  - マルチキャスト送信フレーム数
  - 失敗数
  - 再試行数
  - 複数再試行数
  - フレーム重複数
  - Rts 成功数
  - Rts 失敗数
  - Ack 失敗数
  - 受信フラグメント数
  - マルチキャスト受信フレーム数
  - FCS エラー数 : このカウンタは、受信した MPDU で FCS エラーが検出されたときに増分されます。
  - 送信フレーム数
- セキュリティ
  - ペアワイズ暗号
  - Tkip ICV エラー数
  - Tkip ローカル MIC 失敗数
  - Tkip 再試行数
  - Ccmp 再試行数
  - Ccmp 復号化エラー数
  - 管理統計 Tkip ICV エラー数

- 管理統計 Tkip ローカル MIC 失敗数
- 管理統計 Tkip 再試行数
- 管理統計 Ccmp 再試行数
- 管理統計 Ccmp 復号化エラー数
- 管理統計 Tkip MHDR エラー数
- 管理統計 Ccmp MHDR エラー数
- 管理統計ブロードキャスト アソシエーション解除数
- 管理統計ブロードキャスト認証解除数
- 管理統計ブロードキャスト アクション フレーム数

クライアント動作パラメータの表示

特定のクライアント動作パラメータを表示するには、次の手順に従います。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[Test] ドロップダウン リストから [Operational Parameters] を選択します。

次の情報が表示されます。

動作パラメータ：

- [Device Name]：デバイスのユーザ定義の名前。
- [Client Type]：クライアントの種類は次のいずれかになります。
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
  - projector(9)
  - videoconfsystem(10)
  - camera(11)
  - gamingsystem(12)
  - dot11deskphone(13)
  - cashregister(14)
  - radiotag(15)
  - rfidsensor(16)

  - server(17)
- [SSID]：クライアントで使用している SSID。
- [IP Address Mode]：静的設定、DHCP などの IP アドレス モード。
- [IPv4 Address]：クライアントに割り当てられた IPv4 アドレス。
- [IPv4 Subnet Address]：クライアントに割り当てられた IPv4 サブネット アドレス。
- [IPv6 Address]：クライアントに割り当てられた IPv6 アドレス。
- [IPv6 Subnet Address]：クライアントに割り当てられた IPv6 サブネット アドレス。
- [Default Gateway]：このクライアントで選択されているデフォルト ゲートウェイ。
- [Operating System]：ワイヤレス ネットワーク アダプタを使用しているオペレーティング システムを識別します。
- [Operating System Version]：ワイヤレス ネットワーク アダプタを使用しているオペレーティング システムのバージョンを識別します。
- [WNA Firmware Version]：クライアントに現在インストールされているファームウェアのバージョン。
- [Driver Version]：
- [Enterprise Phone Number]：クライアントの企業電話番号。
- [Cell Phone Number]：クライアントの携帯電話番号。
- [Power Save Mode]：省電力モードとして awake、normal、または maxPower のいずれかが表示されます。
- System Name
- ローカリゼーション

無線情報：

- [Radio Type]：次の無線の種類が使用可能です。
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- [Radio Channel]：使用中の無線チャネル。

DNS/WNS 情報：

- [DNS Servers]：DNS サーバの IP アドレス。
- [WNS Servers]：WNS サーバの IP アドレス。

セキュリティ情報：

- [Credential Type]：クライアントに設定されているクレデンシャルの方法を示します。
- [Authentication Method]：クライアントで使用する認証方式。
- [EAP Method]：クライアントで使用する拡張認証プロトコル（EAP）の方式。
- [Encryption Method]：クライアントで使用する暗号化方式。

- [Key Management Method]：クライアントで使用するキー管理方式。

クライアント プロファイルの表示

特定のクライアント プロファイル情報を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Profiles] を選択します。

次の情報が表示されます。

- [Profile Name]：ハイパーリンクになったプロファイル名のリスト。クリックすると、プロファイルの詳細が表示されます。
- [SSID]：このクライアントをアソシエートする WLAN の SSID。

現在のクライアントの無効化

現在のクライアントを無効にするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　無効にするクライアントを選択します。

ステップ 3　[Disable] をクリックします。[Disable Client] ページが表示されます。

ステップ 4　[Description] テキスト ボックスに説明を入力します。

ステップ 5　[OK] をクリックします。

（注）　無効にしたクライアントは、コントローラ上のいずれのネットワークおよび SSID にも接続できません。クライアントを再度有効にするには、[Configure] > [Controllers] > [IP Address] > [Security] > [Manually Disabled Clients] の順に選択し、クライアントのエントリを削除します。

現在のクライアントの削除

現在のクライアントを削除するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　削除するクライアントを選択します。

ステップ 3　[Remove] を選択します。

ステップ 4　[Remove] をクリックして、削除を実行します。

ミラー モードの有効化

ミラー モードを有効にすると、単一のクライアント デバイスまたはアクセス ポイントが起点または終点であるすべてのトラフィックを（別のポートに）複製できます。

（注）　ミラー モードは特定のネットワーク問題を診断する際には役立ちますが、このポートへの接続には反応しなくなるため、使用されていないポートだけで有効にする必要があります。

ミラー モードを有効にするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Enable Mirror Mode] を選択します。

ステップ 4　[Go] をクリックします。

クライアントの最近のロケーションを示す高レゾリューション マップの表示

クライアントの最近のロケーションを示す高レゾリューション マップを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Recent Map (High Resolution)] を選択します。

ステップ 4　[Go] をクリックします。

クライアントの現在のロケーションを示す高レゾリューション マップの表示

クライアントの現在のロケーションを示す高レゾリューション マップを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Present Map (High Resolution)] を選択します。

ステップ 4　[Go] をクリックします。

クライアントのクライアント セッション レポートの実行

このクライアントの最新のクライアント セッション レポートを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Client Sessions Report] を選択します。

ステップ 4　[Go] をクリックします。Client Session レポートの詳細が表示されます。詳細については、「クライアント レポート」（P.14-779）を参照してください。

クライアントのローミング理由レポートの表示

このクライアントの最新のローミング レポートを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Roam Reason] を選択します。

ステップ 4　[Go] をクリックします。

このページには、クライアントの最新のローミング レポートが表示されます。各ローミング レポートには、次の情報が含まれます。

- 新規 AP MAC アドレス
- 旧（前）AP MAC アドレス
- 前の AP SSID
- 前の AP チャネル
- 遷移時間：クライアントを新しいアクセス ポイントにアソシエートするためにかかった時間。
- ローミング理由：クライアントのローミング理由。

検出アクセス ポイントの詳細の表示

信号強度、SNR など、クライアントと通信できるアクセス ポイントの詳細を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Detecting APs] を選択します。

ステップ 4　[Go] をクリックします。

クライアント ロケーション履歴の表示

RF フィンガープリントに基づくクライアント ロケーションの履歴を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Location History] を選択します。

ステップ 4　[Go] をクリックします。

クライアントの音声メトリックの表示

このクライアントのトラフィック ストリーム メトリックを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Voice Metrics] を選択します。

ステップ 4　[Go] をクリックします。

次の情報が表示されます。

- [Time]：アクセス ポイントから統計情報が収集された時刻。
- QoS
- AP Ethernet MAC
- Radio
- [% PLR (Downlink)]：90 秒の間隔中にダウンリンク（アクセス ポイントからクライアント）で失われたパケットの割合。
- [% PLR (Uplink)]：90 秒の間隔中にアップリンク（クライアントからアクセス ポイント）で失われたパケットの割合。
- [Avg Queuing Delay (ms) (Uplink)]：アップリンクの平均キューイング遅延（ミリ秒）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
- [% Packets > 40 ms Queuing Delay (Downlink)]：40 ms を超えるキューイング遅延パケットの割合。

- [% Packets 20ms-40ms Queuing Delay (Downlink)] : 20 ms を超えるキューイング遅延パケットの割合。
- [Roaming Delay] : ローミング遅延（ミリ秒）。クライアントによって測定されるローミング遅延は、古いアクセス ポイントから最後のパケットを受信した時点から、ローミングが正常に行われた後で新しいアクセス ポイントから最初のパケットを受信した時点まで測定されます。

CHAPTER 11

テンプレートの使用

この章では、テンプレートを追加および適用する方法を説明します。テンプレートを利用すると、複数のデバイスにパラメータを適用するときに共通の情報を再入力する必要がなくなります。この章の内容は、次のとおりです。

テンプレートについて

Controller Template Launch Pad は、すべてのコントローラ テンプレートのハブです。この Template Launch Pad から、コントローラ テンプレートを追加および適用、テンプレートを表示、または既存のテンプレートを変更できます。この章では、コントローラ テンプレートの適用と削除、およびアクセス ポイント テンプレートの作成や変更についても説明します。

（注） テンプレートの情報は、個々のデバイスで上書きされる場合があります。

Controller Template Launch Pad へのアクセス

Controller Template Launch Pad にアクセスするには、[Configure] > [Controller Template Launch Pad] の順に選択します。

Controller Template Launch Pad では、1 つのページからすべての Prime Infrastructure テンプレートにアクセスできます。このページから、現在のコントローラ テンプレートを表示したり、新しいテンプレートを作成および保存したりできます。

ヒント　テンプレート タイプの横にあるツール チップにマウス カーソルを合わせると、テンプレートの詳細を表示できます。

コントローラ テンプレートの追加

新規コントローラ テンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　テンプレート名を入力します。

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

ステップ 4　テンプレートの説明を入力します。

ステップ 5　[Save] をクリックします。

コントローラ テンプレートの削除

コントローラ テンプレートを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　テンプレート タイプをクリックして、テンプレート リスト ページを開きます。

ステップ 3　削除するテンプレートのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから [Delete Templates] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。このテンプレートがコントローラにされている場合には、[Remove Template Confirmation] ページが開き、このテンプレートを現在適用しているすべてのコントローラがリストされます。

ステップ 7　テンプレートを削除する各コントローラのチェックボックスをオンにします。

ステップ 8　[OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてテンプレートを削除せずにこのページを閉じます。

コントローラ テンプレートの適用

コントローラ テンプレートは、選択した設定グループの 1 つ以上のコントローラに直接適用できます。

コントローラ テンプレートを適用するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　左側のサイドバーのメニューを使用して、適用するテンプレートのカテゴリを選択します。

ステップ 3　コントローラに適用するテンプレートのテンプレート名をクリックします。

ステップ 4　[Apply to Controllers] をクリックして、[Apply to Controllers] ページを開きます。

ステップ 5　テンプレートを適用する各コントローラのチェックボックスをオンにします。

（注）　すべてのコントローラを選択するには、コントローラ テーブルの左隅に表示されるチェックボックスをオンにします。

（注）　[Ignore errors on Apply template to Controllers] チェックボックスをオンにすると、エラーを無視して、テンプレートのすべてのコマンドをコントローラに適用できます。このチェックボックスがオフの場合、テンプレートのコマンドをコントローラに適用するときにエラーが発生すると、残りのコマンドは適用されません。

ステップ 6　テンプレートを直接適用する対象として、選択した設定グループの 1 つまたはすべてのコントローラより選択ください。

テンプレートを 1 つのコントローラ（もしくは、すべてのコントローラ）に直接適用するには、次の手順を実行します。

a.　[Apply to controllers selected directly] オプション ボタン を選択します。[Apply to Controllers] ページに、コントローラ名および設定グループ名（該当する場合）とともに、使用できる各コントローラの IP アドレスがリストされます。

b.　テンプレートを適用する各コントローラのチェックボックスをオンにします。

（注）　[Ignore errors on Apply template to Controllers] チェックボックスをオンにすると、エラーを無視して、テンプレートのすべてのコマンドをコントローラに適用できます。このチェックボックスがオフの場合、テンプレートのコマンドをコントローラに適用するときにエラーが発生すると、残りのコマンドは適用されません。

選択した設定グループのすべてのコントローラにテンプレートを適用するには、次の手順を実行します。

a.　[Apply to controllers in the selected Config Groups] オプション ボタン を選択します。[Apply to Controllers] ページに、モビリティ グループ名および含まれるコントローラ数とともに、各設定グループの名前がリストされます。

b.　テンプレートを適用する各設定グループのチェックボックスをオンにします。

（注）　コントローラのない設定グループには、テンプレートを適用できません。

ステップ 7　次の追加操作を実行できます。

- [Save Config to Flash after apply] チェックボックスをオンにした場合は、テンプレートが正常に適用されると、save config to Flash コマンドが実行されます。

- [Reboot Controller after apply] チェックボックスをオンにした場合は、テンプレートが正常に適用されると、コントローラがリブートします。

（注）　この設定結果は、[View Save Config / Reboot Results] オプションを有効にして、[Template Results] ページで表示できます。

ステップ 8　[Save] をクリックします。

（注）　[Template List] ページから直接、テンプレートを適用できます。適用するテンプレートのチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Apply Templates] を選択し、[Go] をクリックして、[Apply to Controllers] ページを開きます。このテンプレートを適用するコントローラのチェックボックスをオンにして、[OK] をクリックします。

コントローラ テンプレートの設定

ここでは、次の内容について説明します。

システム テンプレートの設定

ここでは、次の内容について説明します。

汎用テンプレートの設定

汎用テンプレートを追加、または既存の汎用テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

[General] をクリックするか、左側のサイドバーのメニューから [System] > [General] を選択します。[System] > [General Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 2　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[General template] ページが表示されます。

ステップ 3　[802.3x Flow Control Mode] ドロップダウン リストを使用して、フロー コントロール モードを有効または無効にします。

ステップ 4　[802.3x Bridging] ドロップダウン リストを使用して、802.3 ブリッジングを有効または無効にします。

（注）　この 802.3 ブリッジング オプションは、5500 および 2106 シリーズのコントローラでは使用できません。

ステップ 5　[Web RADIUS Authentication] ドロップダウン リストを使用して、目的の Web RADIUS 認証を選択します。ユーザ資格情報の交換時に、コントローラとクライアント間の認証用に、PAP、CHAP、または MD5-CHAP の使用を選択できます。

ステップ 6　AP Primary Discovery タイムアウトの秒数を指定します。デフォルトは 120 秒です。有効範囲は 30 ～ 3600 です。

ステップ 7　バックアップ プライマリおよびセカンダリ コントローラの詳細（コントローラ IP アドレスおよびコントローラ名）を指定します。

ステップ 8　レイヤ 2 またはレイヤ 3 転送モードを指定します。レイヤ 3 に設定した場合、Lightweight アクセス ポイントは IP アドレスを使用してアクセス ポイントと通信します。これらの IP アドレスは必須の DHCP サーバから収集します。レイヤ 2 に設定した場合、Lightweight アクセス ポイントは専用コードを使用してアクセス ポイントと通信します。

（注）　リリース 5.2 までのコントローラでは LWAPP が使用され、新しいコントローラ リリースでは CAPWAP が使用されます。

ステップ 9　ブロードキャスト転送を有効または無効にします。デフォルトでは無効になっています。

ステップ 10　[LAG Mode] ドロップダウン リストから [Enable] または [Disable] を選択します。リンク集約によって、物理ポートをすべてグループ化して link aggregation group（LAG; リンク集約グループ）を作成し、コントローラ上のポートを構成するために必要な IP アドレスの数を削減できます。

LAG がコントローラで有効にされている場合、インターフェイス データベース内での設定の矛盾を避けるため、作成したダイナミック インターフェイスが削除されます。LAG 設定に変更を加えると、変更を有効にするためにコントローラをリブートする必要があります。

（注）　インターフェイスは Dynamic AP Manager フラグを設定した状態では作成できません。また、コントローラ上では複数の LAG を作成できません。

ステップ 11　ピアツーピア ブロック モードを有効にするか無効にするかを選択します。[Disable] を選択すると、同じサブネットのクライアントはすべてこのコントローラを使用して通信します。[Enable] を選択すると、同じサブネットのクライアントはすべて上位レベルのルータを使用して通信します。

ステップ 12　[Over Air AP Provision Mode] ドロップダウン リストから、[enable] または [disable] を選択します。

ステップ 13　[AP Fallback] ドロップダウン リストで、[enable] または [disable] を選択します。フォールバックを有効にすると、プライマリ コントローラの接続を切断されたアクセス ポイントがプライマリ コントローラの復帰と同時に自動的にサービスに戻ります。

ステップ 14　コントローラに障害が発生した場合、アクセス ポイントに設定されたバックアップ コントローラがすぐに多くの検出と接続要求を受信します。これにより、コントローラは飽和ポイントに達し、いくつかのアクセス ポイントを拒否する可能性があります。優先順位をアクセス ポイントに割り当てることによって、拒否されるアクセス ポイントを制御します。フェールオーバー時にバックアップ コントローラが飽和している状況では、優先度の低いアクセス ポイントの接続を切断すると、優先度の高いアクセス ポイントがバックアップ コントローラに接続できるようになります。この機能を有効にする場合、[AP Failover Priority] ドロップダウン リストから [enable] を選択します。

ステップ 15　AppleTalk ブリッジングを有効にするか無効にするかを選択します。

（注）　この AppleTalk ブリッジング オプションは、5500 シリーズ コントローラでは使用できません。

ステップ 16　[Fast SSID Change] オプションを有効にするか無効にするかを選択します。このオプションを有効にすると、クライアントは SSID 間で接続をほとんど中断せずにコントローラに瞬時に接続します。通常、各クライアントは SSID に特定された特定の WLAN に接続します。クライアントが接続したアクセス ポイントの範囲外に移動した場合、クライアントは別のアクセス ポイントを使用してコントローラに再接続する必要があります。この通常のプロセスは、DHCP サーバが IP アドレスをクライアントに割り当てる必要があるため、少し時間がかかります。

ステップ 17　マスター コントローラは、通常、展開されたネットワークで使用されないため、マスター コントローラの設定は、リブートまたはオペレーティング システム コードのアップグレード時に自動的に無効になります。コントローラをマスター コントローラとして [Master Controller Mode] ドロップダウン リストから有効にする場合もあります。

ステップ 18　無線クライアントからコントローラ管理インターフェイスへのアクセスを有効にするか無効にするかを選択します。IPsec 動作により、無線による管理は WPA または静的 WEP 全体にログインしているオペレータだけが実行できます。ワイヤレス管理は、IPsec WLAN を経由してログインしようとしているクライアントは実行できません。

ステップ 19　シンメトリック トンネリング モードを有効にするか無効にするかを選択します。シンメトリック モビリティ トンネリングを使用すると、コントローラでは 1 つのアクセス ポイントから無線 LAN 内の別のアクセス ポイントへローミングするクライアントに対して、サブネット間のモビリティが提供されます。有線ネットワーク上のクライアント トラフィックは、外部コントローラによって直接ルーティングされます。ルータでリバース パス転送（RPF）が有効になっている場合、受信パケットで追加確認が実行され、通信はブロックされます。RPF が有効になっている場合でも、シンメトリック モビリティ トンネリングによって、アンカーとして指定されたコントローラにクライアント トラフィックが到達できるようになります。

（注）　モビリティ グループのすべてのコントローラは、同一のシンメトリック トンネリング モードを備えている必要があります。

（注）　シンメトリック トンネリングを有効にするには、リブートする必要があります。

ステップ 20　[ACL Counters] ドロップダウン リストを使用して、ACL カウンタを有効または無効にします。各コントローラの ACL ルールごとの値を表示できます。

ステップ 21　[Default Mobility Domain Name] テキスト ボックスにオペレータが定義した RF モビリティ グループ名を入力します。

ステップ 22　[Mobility Anchor Group Keep Alive Interval] でクライアントが別のアクセス ポイントへの接続を試みるまでの遅延時間を指定します。このゲスト トンネリングの N+1 冗長機能を使用すると、コントローラのエラー後にクライアントが別のアクセス ポイントに接続するためにかかる時間が短縮されます。エラーがすばやく特定され、クライアントが問題発生のコントローラから移動し、別のコントローラに接続されるためです。

（注）　マウス カーソルをフィールドの上に移動すると、値の有効な範囲が表示されます。

ステップ 23　[Mobility Anchor Group Keep Alive Retries] でクライアントが到達不能と判断するまでのアンカーへのクエリーの数を指定します。

ステップ 24　8 ～ 19 文字の RF ネットワーク グループ名を入力します。無線リソース管理（RRM）ネイバー パケットは RF ネットワーク グループ内のアクセス ポイントに分散されます。Cisco アクセス ポイントは、この RF ネットワーク名で送信された RRM ネイバー パケットだけを受け入れます。別の RF ネットワーク名で送信された RRM ネイバー パケットはドロップされます。

ステップ 25　アイドル クライアントのタイムアウトを指定します。デフォルトは 300 秒です。タイムアウトを過ぎると、クライアントは認証を失い、アクセス ポイントから一時的にアソシエート解除し、再アソシエートして、再度認証を行います。

ステップ 26　アドレス解決プロトコルのタイムアウトを秒単位で指定します。デフォルトは 300 秒です。

ステップ 27　[Global TCP Adjust MSS] チェックボックスをオンにすると、クライアントから送信される TCP パケットが、TCP SYN/TCP ACK パケットおよび MSS 値に対してチェックされ、アップストリームおよびダウンストリーム側の設定値にリセットされます。

ステップ 28　手動プロキシ設定がクライアントのブラウザで設定されている場合、[Web Auth Proxy Redirect Mode] の [enable] または [disable] を選択します。このクライアントから送信されるすべての Web トラフィックは、ブラウザで設定されている PROXY IP および PORT に送信されます。

ステップ 29　[Web Auth Proxy Redirect Port] に値を入力します。デフォルトのポートは、8080 および 3128 です。範囲は 0 ～ 65535 です。

ステップ 30　[AP Retransmit Count] および [AP Retransmit Interval] に値を入力します。[AP Retransmit Count] のデフォルト値は 5 で、範囲は 3 ～ 8 です。[AP Retransmit Interval] のデフォルト値は 3 です。指定できる範囲は 2 ～ 5 です。

ステップ 31　[Save] をクリックします。

SNMP コミュニティ コントローラ テンプレートの設定

コントローラでの SNMP コミュニティの設定用のテンプレートを作成または変更します。コミュニティは、SNMP v1、v2 または v3 を使用して、読み取り専用または読み取りと書き込み権限を指定できます。

WLC（ワイヤレス LAN コントローラ）上に SNMP コミュニティを設定する場合、IP アドレスおよびサブネットを指定することができます。指定したコミュニティ ストリングを使用してすべてのホストに SNMP アクセスを開く 0.0.0.0 が両方のデフォルトです。デフォルトの 0.0.0.0 以外を指定した場合、IP アドレスとサブネット マスクに指定した設定に SNMP アクセスが限定されます。255.255.255.255 のサブセットによって IP アドレスで指定した特定のホスト ID に制限されます。

コントローラの SNMP コミュニティ情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のフィールドを設定します。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- Community Name
- [Confirm Community Name]：コミュニティ名を再入力します。
- [IP Address]：サーバの IP アドレス。
- Netmask
- [Access Mode]：ドロップダウン リストから [Read Only] または [Read Write] を選択します。

  - [Read Only]：編集できません。
  - [Read Write]：編集できます。
- [Admin Status]：チェックボックスをオンにすると、このテンプレートおよび [Update Discover Community] オプションが有効になります。
- [Update Discover Community]：チェックボックスをオンにすると、SNMP バージョンが v2 で更新されます。これにより、適用されるコントローラのテンプレート コミュニティ名で読み取り / 書き込みコミュニティが更新されます。

（注）　[Access Mode] オプションを [Read Only] に設定すると、このテンプレートの適用後、Prime Infrastructure のコントローラへのアクセス権は読み取り専用になります。

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

（注）　テンプレートが正常に適用され、[Update Discover Community] オプションが有効にされると、適用されるコミュニティ名が、その適用コントローラの Prime Infrastructure データベースで更新されます。また、Prime Infrastructure は、コントローラとの今後の通信に、このコミュニティ名を使用します。

NTP サーバ テンプレートの設定

（注）　NTP は、コンピュータのクロックをインターネット上で同期させるときに使用します。

NTP テンプレートを追加する、または既存の NTP テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Network Time Protocol] をクリックするか、左側のサイドバー メニューから [System] > [Network Time Protocol] を選択します。[System] > [NTP Server Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Network Time Protocol Template] ページが表示されます。

ステップ 4　NTP サーバの IP アドレスを入力します。

ステップ 5　[Save] をクリックします。

ユーザ ロール コントローラ テンプレートの設定

ここでは、ユーザ ロール設定用のテンプレートを作成または変更する方法について説明します。ユーザ ロールは、ネットワークが使用できる帯域幅の量を決定します。ゲスト ユーザに割り当てる帯域幅には、4 つの QoS レベル（プラチナ、ブロンズ、ゴールドおよびシルバー）を使用できます。ゲスト ユーザには、ロール（契約者、顧客、代理店、ベンダー、ビジター、その他）が事前に割り当てられます。また、それぞれの帯域幅は、管理者により設定されます。これらの役割は、新しいゲスト ユーザを追加するときに適用できます。ゲスト ユーザの追加の詳細については、「ゲスト ユーザ テンプレートの設定」（P.11-662）を参照してください。

コントローラのユーザ ロールを含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のフィールドを設定します。

- Role Name
- [Average Data Rate] : 非 UDP（ユーザ データグラム プロトコル）トラフィックの平均データ レート。
- [Burst Data Rate] : 非 UDP トラフィックのピーク データ レート。
- [Average Real-time Rate] : UDP トラフィックの平均データ レート。
- [Burst Real-time Rate] : UDP トラフィックのピーク データ レート。

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページから、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

AP ユーザ名パスワード コントローラ テンプレートの設定

アクセス ポイントのユーザ名およびパスワードを設定するテンプレートを作成または変更します。すべてのアクセス ポイントは、コントローラに接続されるときにパスワードを継承します。これらのクレデンシャルは、コンソールまたは Telnet/SSH を介してアクセス ポイントにログインするときに使用されます。

（注）　グローバル パスワードの詳細については、「グローバル アクセス ポイント パスワードの設定」（P.9-345）を参照してください。

[AP Username Password] ページでは、すべてのアクセス ポイントがコントローラに接続する際に継承する、グローバル パスワードを設定できます。また、アクセス ポイントを追加するときに、このグローバル ユーザ名およびパスワードを受け入れるか、アクセス ポイント単位で上書きするかを選択できます。グローバル パスワードが表示される場所、およびアクセス ポイント単位でグローバル パスワードを上書きする方法を確認するには、「AP 設定テンプレートの設定」（P.11-736）を参照してください。

さらにコントローラ ソフトウェア リリース 5.0 では、アクセス ポイントをコントローラに接続すると、そのアクセス ポイントのコンソール ポート セキュリティが有効になり、アクセス ポイント コンソール ポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

コントローラの AP ユーザ名パスワード情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のフィールドを設定します。

- [AP Username]：コントローラに接続するすべてのアクセス ポイントが継承するユーザ名を入力します。
- [AP Password]：コントローラに接続するすべてのアクセス ポイントが継承するパスワードを入力します。
- [Confirm Password]：アクセス ポイントのパスワードを再入力します。
- Enable Password

（注）　Cisco IOS アクセス ポイントの場合は、イネーブル パスワードも入力して確認する必要があります。

- Confirm Enable Password

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

（注）　グローバル パスワードの詳細については、「グローバル アクセス ポイント パスワードの設定」（P.9-345）を参照してください。

AP 802.1X サプリカント クレデンシャルの設定

Lightweight アクセス ポイントとスイッチ間の 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。すべてのアクセス ポイントがコントローラ接続時に継承するグローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。

既存の AP 802.1X サプリカント クレデンシャル テンプレートを追加または変更するには、次の手順を実行します。

（注）　必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセス ポイントに割り当てることができます。詳細については、「アクセス ポイントの設定」（P.9-463）を参照してください。

ステップ 1　[Configure] > [Controller Templates Launch Pad] の順に選択します。

ステップ 2　[AP 802.1X Supplicant Credentials] をクリックするか、左側のサイドバー メニューから [System] > [AP 802.1X Supplicant Credentials] を選択します。[AP 802.1X Supplicant Credentials Templates] ページに、現在保存されているすべての AP 802.1X サプリカント クレデンシャル テンプレートが表示されます。また、各テンプレートが適用されるコントローラ数および仮想ドメイン数も表示されます。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　テンプレート名をクリックして、[Controller Template] リスト ページを開きます。ここから、現在のテンプレート フィールドを編集できます。

ステップ 4　[Save] をクリックします。

グローバル CDP 設定テンプレートの設定

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。

（注）　CDP は、デフォルトでイーサネットと、ブリッジの無線ポートで有効です。

グローバル CDP 設定テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Global CDP Configuration] をクリックするか、左側のサイドバー メニューから [System] > [Global CDP Configuration] を選択します。[Global CDP Configuration Templates] ページには、現在保存されているすべてのグローバル CDP 設定テンプレートが表示されます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Global CDP Configuration template] ページが表示されます。

ステップ 4　新しい CDP テンプレート名を入力します。

ステップ 5　ページの [Global CDP] グループ ボックスで、次のフィールドを設定します。

- [CDP on controller]：コントローラで CDP を有効にするか、無効にするかを選択します。

  （注）　この設定は、WiSM2 コントローラには適用できません。

- [Global CDP on APs]：アクセス ポイントで CDP を有効にするか、無効にするかを選択します。
- [Refresh-time Interval (seconds)]：[Refresh Time Interval] フィールドに、CDP メッセージが生成される時間を秒単位で入力します。デフォルト値は 60 です。
- [Holdtime (seconds)]：CDP ネイバー エントリの期限が切れるまでの時間を秒単位で入力します。デフォルト値は 180 です。

- [CDP Advertisement Version] : 使用する CDP プロトコルのバージョンを入力します。デフォルトは v1 です。

ステップ 6　ページの [CDP for Ethernet Interfaces] グループ ボックスで、CDP を有効にするイーサネット インターフェイスのスロットを選択します。

（注）　[CDP for Ethernet Interfaces] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 7　ページの [CDP for Radio Interfaces] グループ ボックスで、CDP を有効にする無線インターフェイスのスロットを選択します。

（注）　[CDP for Radio Interfaces] フィールドは、リリース 7.0.110.2 以降のコントローラでサポートされています。

ステップ 8　[Save] をクリックします。

（注）　グローバル インターフェイス CDP 設定は、AP レベルで CDP を有効にした AP のみに適用されます。

DHCP テンプレートの設定

DHCP テンプレートを追加、または既存の DHCP テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[DHCP] をクリックするか、左側のサイドバーのメニューから [System] > [DHCP] の順に選択します。[System] > [DHCP Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[DHCP template] ページが表示されます。

ステップ 4　DHCP プロキシを WLAN ベースではなく、グローバルで有効または無効にできます。DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。少なくとも 1 つの DHCP サーバが、WLAN にアソシエートされたインターフェイスか WLAN 自体で設定されている必要があります。DHCP プロキシは、デフォルトで有効になっています。

ステップ 5　[DHCP Timeout] を秒単位で入力します。この時間を過ぎると DHCP 要求がタイムアウトします。デフォルト設定は 5 です。有効値の範囲は 5 ～ 120 秒です。

（注）　DHCP タイムアウトは、リリース 7.0.114.74 以降のコントローラで適用できます。

ステップ 6　[Save] をクリックします。

ダイナミック インターフェイス テンプレートの設定

ダイナミック インターフェイス テンプレートを追加するか、既存のインターフェイス設定を変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Dynamic Interface] をクリックするか、左側のサイドバーのメニューから [System] > [Dynamic Interface] を選択します。[System] > [Dynamic Interface Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Dynamic Interface template] ページが表示されます。

ステップ 4　[Guest LAN] チェックボックスをオンにして、インターフェイスに有線マークを付けます。

ステップ 5　インターフェイスのネット マスク アドレスを入力します。

ステップ 6　インターフェイスに現在使用されているポートを入力します。

ステップ 7　プライマリ ポートがダウンしているときにインターフェイスにより使用されるセカンダリ ポートを入力します。プライマリ ポートが再アクティブ化されると、Cisco 4400 シリーズ Wireless LAN Controller は、インターフェイスをプライマリ ポートに転送されます。

（注）　プライマリおよびセカンダリ ポート番号は、Cisco 4400 Series Wireless LAN コントローラのみに存在します。

ステップ 8　プライマリ DHCP サーバの IP アドレスを入力します。

ステップ 9　セカンダリ DHCP サーバの IP アドレスを入力します。

ステップ 10　[DHCP Proxy Mode] ドロップダウン リストから、DHCP プロキシ モードを選択します。

- [Global] : コントローラでグローバル DHCP プロキシ モードを使用します。
- [Enabled] : インターフェイスで DHCP プロキシ モードを有効にします。コントローラ上で DHCP プロキシを有効にした場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。少なくとも 1 つの DHCP サーバを、WLAN に関連付けられたインターフェイスか WLAN に設定する必要があります。
- [Disabled] : インターフェイスで DHCP プロキシ モードを無効にします。コントローラの DHCP プロキシを無効にすると、クライアントとの間で送受信されるそれらの DHCP パケットは、パケットの IP 部分が変更されることなくコントローラによってブリッジされます。クライアントか

ら受信したパケットは CAPWAP トンネルから削除され、アップストリーム VLAN 上で送信されます。クライアント宛の DHCP パケットは、アップストリーム VLAN 上で受信され、802.11 に変換されて、CAPWAP トンネルを通ってクライアントに送信されます。したがって、DHCP プロキシが無効になっている場合は、内部 DHCP サーバは使用できません。

ステップ 11　[ACL Name] ドロップダウン リストの定義済みの名前のリストから名前を選択します。

ステップ 12　[mDNS Profile] ドロップダウン リストから、[mDNS] プロファイルを選択します。デフォルトのオプションは [none] です。

ステップ 13　[Add Interface Format Type] グループ ボックスの [Add Format Type] ドロップダウン リストから、[Device Info] または [File] のいずれかを選択します。[Device Info] を選択する場合、各コントローラのデバイス固有フィールドを設定する必要があります。[File] を選択する場合、CSV ファイルで指定されているすべての管理対象コントローラの CSV デバイス固有フィールド（[Interface Name]、[VLAN Identifier]、[Quarantine VLAN Identifier]、[IP Address]、[Gateway]）を設定する必要があります（表 11-1 を参照）。[Device Info] を選択した場合は、ステップ 12 に進みます。

サンプル CSV ファイルを次に示します。

表 11-1　サンプル CSV ファイル

ip_address	interface_name	vlan_id	quarantine_ vlan_id	interface_ ip_address	gateway
209.165.200.224	dyn-1	1	2	209.165.200.228	209.165.200.229
209.165.200.225	interface-1	4	2	209.165.200.230	209.165.200.231
209.165.200.226	interface-2	5	3	209.165.200.232	209.165.200.233
209.165.200.227	dyna-2	2	3	209.165.200.234	209.165.200.235

CSV ファイルの最初の行は、含まれている列の説明に使用されます。CSV ファイルには、次のフィールドを含めることができます。

- ip_address
- interface_name
- vlan_id
- quarantine_vlan_id
- interface_ip_address
- gateway

ステップ 14　[Apply to Controllers] を選択した場合、[Apply To] ページに進みます。このページで、各コントローラのデバイス固有フィールドを設定できます。

ステップ 15　[Add] および [Remove] オプションを使用して、各コントローラのデバイス固有フィールドを設定します。[Edit] をクリックすると、現在のパラメータ入力を示すダイアログボックスが表示されます。

ステップ 16　ダイアログボックスで必要な変更を行い、[OK] をクリックします。

（注）　インターフェイス フィールドを変更する場合、WLAN が一時的に無効になるため、一部のクライアントとの接続が切断されることがあります。インターフェイス フィールドの変更は、コントローラに正常に適用された後で保存されます。

（注）　ここでインターフェイスを削除すると、インターフェイスは、コントローラではなく、テンプレートからのみ削除されます。

ダイナミック インターフェイス テンプレートのコントローラへの適用

ダイナミック インターフェイス テンプレートをコントローラに適用するには、次の手順を実行します。

ステップ 1　[Dynamic Interface controller template] ページで、[Apply to Controllers] をクリックします。

ステップ 2　[Manage Interfaces] オプションを使用して、次のデバイス固有フィールドを設定します。

- [Add] : [Add] をクリックして、[Add Interface] ダイアログボックスを開きます。インターフェイス名、VLAN 識別子、IP アドレス、ゲートウェイを入力します。すべてのフィールドを入力したら、[Done] をクリックします。
- [Edit] : [Edit] をクリックして、現在のインターフェイスを変更します。
- [Remove] : [Remove] をクリックして、現在のインターフェイスを削除します。

ステップ 3　このテンプレートを適用する各コントローラのチェックボックスをオンにします。

ステップ 4　[Apply] をクリックします。

（注）　インターフェイス フィールドを変更すると、WLAN が一時的に無効になるため、一部のクライアントの接続が切断される場合があります。

（注）　インターフェイス フィールドの変更またはこのページでの設定は、コントローラに正常に適用された場合のみ保存されます。

（注）　このページから削除したインターフェイスは、コントローラではなく、このテンプレートからのみ削除されます。

（注）　ダイナミック インターフェイス コントローラ テンプレートの詳細については、「ダイナミック インターフェイス テンプレートの設定」（P.11-614）を参照してください。

QoS テンプレートの設定

QoS（Quality of Service）プロファイルを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[QoS Profiles] をクリックするか、左側のサイドバーのメニューから [System] > [QoS Profiles] を選択します。[System] > [QoS Profiles] ページが表示されます。テンプレートが適用されるコントローラと仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　ブロンズ、ゴールド、プラチナまたはシルバー QoS プロファイルを編集する場合、編集するプロファイルの [Name] 列をクリックします。[Edit QoS Profile Template] ページが表示されます。

ステップ 4　[Per-User Bandwidth Contracts] グループ ボックスで次の値を設定します。すべてに 0 または Off のデフォルトがあります。

- [Average Data Rate] : 非 UDP トラフィックの平均データ レート。
- [Burst Data Rate] : 非 UDP トラフィックのピーク データ レート。
- [Average Real-time Rate] : UDP トラフィックの平均データ レート。
- [Burst Real-time Rate] : UDP トラフィックのピーク データ レート。

ステップ 5　[Over-the-Air QoS] グループ ボックスで次の値を設定します。

- Maximum QoS RF Usage per AP：クライアントが使用できる最大無線帯域幅。デフォルトは 100% です。
- QoS Queue Depth：クライアントのクラスのキュー深度。これより大きな値のパケットは、アクセス ポイントでドロップされます。

（注）　無線 QoS 設定は、コントローラ リリース 7.0 以前のリリースに適用できます。

ステップ 6　[Wired QoS Protocol] グループ ボックスで次の値を設定します。

- Wired QoS Protocol：802.1P プライオリティ タグをアクティブにするには [802.1P] を選択し、802.1P プライオリティ フラグを非アクティブにするには [None] を選択します。
- 802.1P Tag：有線接続の 802.1P プライオリティ タグを 0 ～ 7 から選択します。このタグは、トラフィックおよび CAPWAP パケットに使用されます。

ステップ 7　[Save] をクリックします。

AP タイマー テンプレートの設定

FlexConnect の一部の拡張タイマー設定およびローカル モードは、Prime Infrastructure のコントローラで使用できます。

AP タイマーのテンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[AP Timers] をクリックするか、左側のサイドバーのメニューから [System] > [AP Timers] を選択します。[System] > [AP Timers] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Access Point Mode] 列の値は、リンクです。リンクをクリックすると、[Controller Template *access point mode*] ページが表示されます。[Access Point Mode] は自動的に設定されます。

ステップ 3　[AP Fast Heartbeat Timer State] チェックボックスをオンにして、[AP Fast Heartbeat Timeout] を有効にします。

ステップ 4　[AP Fast Heartbeat Timeout] に値を入力します。有効な範囲は 1 ～ 15 秒です。デフォルトは 10 秒です。推奨されるタイムアウト値を次に示します。

- 7500 シリーズ コントローラ：10 ～ 15 秒
- リリース 7.0.98.0 以前の 5500 シリーズ コントローラ：10 ～ 15 秒
- リリース 7.0.98.0 以降の 5500 シリーズ コントローラ：1 ～ 10 秒
- その他のコントローラ：1 ～ 10 秒

ステップ 5　[Save] をクリックします。

インターフェイス グループ テンプレートの設定

[Interface Group Template] ページでは、インターフェイスのリストを選択したり、グループを作成したりできます。このページを使用して、インターフェイスを作成することはできません。

（注）　インターフェイス グループ機能はコントローラ ソフトウェア リリース 7.0.116.0 以降でサポートされます。

インターフェイス グループ テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Interface Groups] をクリックするか、左側のサイドバーのメニューから [System] > [Interface Groups] を選択します。[System] > [Interface Groups] ページが表示されます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[New Controller Template] ページが表示されます。

ステップ 4　次の詳細を指定します。

- [Name]：インターフェイス グループ名。
- [Description(optional)]：インターフェイス グループの詳細な説明。
- [Quarantine]：インターフェイス グループに追加できるインターフェイスのタイプを示します。このオプションが有効な場合、隔離 VLAN ID を設定したインターフェイスを追加できます。このオプションが無効な場合、隔離 VLAN ID が設定されていないインターフェイスを追加できます。
- [mDNS Profile]：ユーザが mDNS プロファイルを選択できるドロップダウン リスト。デフォルトのオプションは [none] です。

ステップ 5　グループに追加するコントローラまたはインターフェイスを選択します。

ステップ 6　[Save] をクリックします。

トラフィック ストリーム メトリック QoS テンプレートの設定

トラフィック ストリーム メトリックは、無線 LAN での VoIP に関する一連の統計で、無線 LAN の QoS について報告します。これらの統計は、VoIP システムにより提供されるエンドツーエンドの統計とは異なります。エンドツーエンドの統計は、コール パスからなるすべてのリンクをカバーする、パケット損失および遅延に関する情報を提供します。しかし、トラフィック ストリーム メトリックは、コールの WLAN セグメントだけの統計です。このためシステム管理者は、音声の問題が WLAN によるものであるのか、コールに関与するその他のネットワーク要素によるものであるのかを、迅速に判断できます。どのアクセス ポイントの QoS が低下しているかを監視することにより、システム管理者は問題の発生している物理領域を迅速に特定できます。無線のカバレッジ不足または過度の干渉が根本的な問題である場合は、これが重要となります。

音声コールの音声品質に影響を与える可能性のある 4 つの QoS の値（パケット遅延、パケット ジッタ、パケット損失、ローミング時間）がモニタされます。このプロセスには、すべての無線 LAN コンポーネントが関与しています。アクセス ポイントおよびクライアントでメトリックを測定し、アクセス ポイントで計測結果を収集してこれらをコントローラに送信します。アクセス ポイントでは、90 秒ごとにコントローラのトラフィック ストリーム メトリック情報を更新し、一度に 10 分間分のデータが格納されます。Prime Infrastructure はコントローラにメトリックを問い合わせ、[Traffic Stream Metrics QoS Status] にこれらを表示します。これらのメトリックはしきい値と比較され、ステータス レベルが決定されます。統計のいずれかのステータス レベルが可（黄色）または低下（赤）と表示された場合には、管理者は無線 LAN の QoS を調査します。

アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックがコントローラで有効であることが必要です。

トラフィック ストリーム メトリック QoS テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Traffic Stream Metrics QoS] をクリックするか、左側のサイドバーのメニューから [System] > [Traffic Stream Metrics QoS] を選択します。[Traffic Stream Metrics QoS Controller Templates] ページが表示されます。

[Traffic Stream Metrics QoS Controller Configuration] ページにいくつかの QoS 値が示されます。管理者は、音声およびビデオの次の品質をモニタできます。

- アップストリーム遅延
- アップストリーム パケット損失率
- ローミング時間
- ダウンストリーム パケット損失率
- ダウンストリーム遅延

Packet Loss Rate（PLR; パケット損失率）は音声の明瞭さに影響を与えます。パケット遅延は、明瞭さと接続におけるやり取りの品質の両方に影響を与える可能性があります。過度のローミング時間は音声に望ましくないギャップが生じます。

測定レベルは 3 つあります。

- Normal：正常な QoS（緑）
- Fair：一応は満足できる QoS（黄色）
- Degraded：低下した QoS（赤）

緑、黄色、および赤のアラーム レベルを設定する際、システム管理者は何らかの判断を採る必要があります。考慮すべきファクタは次のとおりです。

- PLR に影響を与える可能性のある干渉および無線のカバレッジを含む環境ファクタ。

- モバイル デバイスでの音声品質に対するエンド ユーザの期待およびシステム管理者の要求（音声品質が低いほど高い PLR が可能）。
- 電話により使用されるコーデックの種類が異なると、パケット損失の許容値は異なる。
- すべてのコールがモバイル間のコールとは限らず、そのため、中には無線 LAN に関する PLR 要件があまり厳しくないものがある。

WLAN テンプレートの設定

ここでは、次の内容について説明します。

WLAN テンプレートの設定

WLAN テンプレートを利用すると、複数のコントローラに適用するためのさまざまな WLAN プロファイルを定義できます。

同じ SSID の WLAN を複数設定できます。この機能によって、同じ無線 LAN 内で別のレイヤ 2 セキュリティ ポリシーを割り当てられます。プロファイル名が一意の識別名として使用されていた以前のリリースとは異なり、リリース 5.1 の場合、テンプレート名が識別名となります。

次の制限は、同じ SSID で複数の WLAN を設定する場合に適用されます。

- 同じ SSID の WLAN は、クライアントがビーコンおよびプローブ内のアドバタイズされた情報に基づいて WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを持っている必要があります。利用できるレイヤ 2 セキュリティ ポリシーは次のとおりです。
  - なし（オープン WLAN）
  - 静的 WEP または 802.1
  - CKIP
  - WPA/WPA2
- SSID を共有する WLAN 上で Broadcast SSID を有効にする必要があります。これによって、アクセス ポイントがこれらの WLAN のプローブ応答を生成できます。
- FlexConnect アクセス ポイントは、複数の SSID をサポートしません。

WLAN テンプレートを追加、または既存の WLAN テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[WLAN] をクリックするか、左側のサイドバーのメニューから [WLANs] > [WLAN Configuration] を選択します。[WLAN Template] ページに既存のすべての定義済み WLAN の概要が表示されます。[WLAN Template General] ページに表示される WLAN を定義するために、次の情報見出しが使用されます。

- [Template Name]：テンプレートのユーザ定義名。名前をクリックすると、このフィールドのパラメータが表示されます。
- [Profile Name]：同じ SSID の WLAN を区別するときに使用されるユーザ定義プロファイル名。

- [SSID]：WLAN の名前を表示します。
- [WLAN/Guest LAN]：ゲスト LAN または WLAN かを決定します。
- [Security Policies]：選択されているセキュリティ ポリシーを示します。None は 802.1X が有効ではないことを示します。
- [WLAN Status]：WLAN が有効かどうかを決定します。
- [Applied to Controllers]：WLAN テンプレートが適用されるコントローラの数。[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。
- [Applied to Virtual Domains]：WLAN テンプレートが適用される仮想ドメインの数。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。
- [Last Saved At]：テンプレートがいつ最後に保存されたかを示します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[WLAN template] ページが表示されます。

ステップ 4　[Wired LAN] チェックボックスをオンにし、この WLAN が有線 LAN かどうかを示します。

（注）　ゲスト アクセスに指定および設定したイーサネット接続から有線ゲスト アクセスをゲスト ユーザに設定するかどうかを指定します。有線ゲスト アクセス ポートは、ゲストのオフィスまたは会議室の特定のポートで使用できます。Lobby Ambassador ポータルを使用してアカウントがネットワークに追加されます。（「ゲスト ユーザ アカウントの作成」（P.7-252）を参照してください）。

（注）　出力または入力インターフェイス設定は、有線 LAN のみで使用できます。

ステップ 5　[Type] ドロップダウン リストを使用して、有線 LAN のタイプを選択します。

- [Guest LAN]：有線 LAN がゲスト LAN であることを示します。

  （注）　[Guest LAN] オプションを選択した場合、任意のゲスト LAN に割り当てられていない入力インターフェイスを選択する必要があります。

- [Remote LAN]：有線 LAN がリモート LAN であることを示します。

ステップ 6　WLAN またはゲスト LAN を示す [Profile Name] テキスト ボックスに名前を入力します。入力する名前には、スペースを使用しないでください。

ステップ 7　WLAN SSID の名前を入力します。SSID は、ゲスト LAN には必要ありません。

同じ SSID の WLAN は、クライアントがビーコンおよびプローブ内のアドバタイズされた情報に基づいて WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを持っている必要があります。

ステップ 8　[Status] フィールドで [Enable] チェックボックスをオンにします。

ステップ 9　[Radio Policy] ドロップダウン リストを使用して、適用する WLAN ポリシーを [All]（802.11a/b/g/n）、[802.11a only]、[802.11g only]、[802.11b/g only]、または [802.11a/g only] に設定します。

ステップ 10　[Interface/Interface Group] ドロップダウン リストを使用して、[Controller] > [Interfaces] モジュールにより作成された使用可能なインターフェイス名から選択します。

ステップ 11　[Egress Interface] ドロップダウン リストから、「出力インターフェイスの作成」（P.9-335）で作成した出力インターフェイスを選択します。これは、有線ゲスト クライアントのトラフィックを処理するコントローラから外部へのパスに相当します。

ステップ 12　[Ingress Interface] ドロップダウン リストから、「入力インターフェイスの作成」（P.9-335）で作成した入力インターフェイスを選択します。この VLAN は、レイヤ 2 アクセス スイッチを使用した有線ゲスト クライアントとコントローラ間のパスを提供します。

ステップ 13　[Enable] チェックボックスをオンにし、マルチキャスト VLAN 機能を有効にします。

ステップ 14　[Multicast VLAN Interface] ドロップダウン リストから、適切なインターフェイス名を選択します。このリストは、マルチキャスト VLAN 機能を有効にすると自動的に読み込まれます。

ステップ 15　[Broadcast SSID] をクリックし、この WLAN の SSID ブロードキャストをアクティブにします。

ステップ 16　[Save] をクリックします。

ステップ 17　WLAN テンプレートをさらに設定するには、次から選択します。

- この WLAN 上のデフォルト サーバを上書きできる AAA とレイヤ 2 および 3 のセキュリティ モードを設定するには、[Security] タブをクリックします。「[Security] タブ」（P.11-622）に進みます。
- この WLAN でのサービスの質を設定するには、[QoS] タブをクリックします。「[QoS] タブ」（P.11-630）に進みます。
- DHCP の割り当てや Management Frame Protection など、WLAN についてのその他の詳細を設定するには、[Advanced] タブをクリックします。「[Advanced] タブ」（P.11-632）に進みます。

[Security] タブ

[Security] を選択すると、さらに 3 つのタブが表示されます。[Layer 2]、[Layer 3]、および [AAA Servers] です。

[Layer 2] タブ

[Layer 2] タブをクリックすると、[Layer 2] タブが表示されます。

（注）　タブには、[Layer 2 Security] ドロップダウン リストで選択したオプションに応じてさまざまな内容が表示されます。

[Layer 2] タブを設定するには、次の手順を実行します。

ステップ 1　[Layer 2 Security] ドロップダウン リストを使用して、表 11-2 で説明されているように、[None]、[802.1X]、[Static WEP]、[Static WEP-802.1X]、[WPA + WPA2] または [CKIP] を選択します。

表 11-2　レイヤ 2 セキュリティのオプション

フィールド	説明
None	レイヤ 2 の選択はありません。 • [FT Enable]：アクセス ポイント間の高速移行（FT）を有効にする場合は、このチェックボックスをオンにします。 （注）　高速移行は FlexConnect モードではサポートされません。 – [Over the DS]：分散システムでの高速移行を有効にする場合は、このチェックボックスをオンにします。 – [Reassociation Timeout]：高速移行の再アソシエーションがタイムアウトになるまでの時間（秒単位）。デフォルトは 20 秒です。有効範囲は 1 ～ 100 です。 （注）　[Over the DS] または [Reassociation Timeout] を有効にするには、高速移行を有効にする必要があります。
802.1X	WEP 802.1X データ暗号化タイプ（注 1）： 40/64 ビット キー 104 ビット キー 152 ビット キー
Static WEP	静的 WEP 暗号化フィールド： [Key sizes]：設定なし、40/64、104 および 152 ビット キー サイズ [Key Index]：1 ～ 4（注 2） [Encryption Key]：暗号キーは必須です。 [Key Format]：ASCII または HEX [Allowed Shared Key Authentication]：チェックボックスをオンにすると、共有キー認証が有効になります。 （注）　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。

表 11-2　レイヤ 2 セキュリティのオプション （続き）

フィールド	説明
Static WEP-802.1X	この設定により、静的 WEP と 802.1X の両方のポリシーを有効にします。このオプションを選択すると、静的 WEP と 802.1X のフィールドがページの下部に表示されます。 静的 WEP 暗号化フィールド： [Key sizes]：設定なし、40/64、104 および 152 ビット キー サイズ [Key index]：1 ～ 4（注 2） [Encryption Key]：暗号キーを入力します。 [Key Format]：ASCII または HEX [Allowed Shared Key Authentication]：チェックボックスをオンにすると有効になります。 802.1 データ暗号化：40/64 ビット キー、104 ビット キー、152 ビット キー

表 11-2　レイヤ 2 セキュリティのオプション （続き）

フィールド	説明
WPA+WPA2	この設定により、WPA、WPA2、またはその両方を有効にします。WPA は、TKIP-MIC データ暗号化または AES を使用する Wi-Fi Protected Access を有効にします。[WPA+WPA2] を選択すると、クライアントがアクセス ポイント間をローミングする際に迅速な交換が可能となる Cisco Centralized Key Management（CCKM）認証キー管理を使用できます。レイヤ 2 セキュリティ ポリシーとして [WPA+WPA2] を選択し、事前共有キーを有効にしている場合は、CCKM または 802.1X を有効にできません。ただし、CCKM と 802.1X の両方を同時に有効にすることは可能です。 • [Mac Filtering] : MAC アドレス フィルタリングを有効にします。 （注） FlexConnect ローカル認証では、[Mac Filtering] および [Max-Clients] はサポートされていません。 • [FT Enable] : アクセス ポイント間の高速移行を有効にする場合は、このチェックボックスをオンにします。 （注） 高速移行は FlexConnect モードではサポートされません。 – [Over the DS] : 分散システムでの高速移行を有効にする場合は、このチェックボックスをオンにします。 – [Reassociation Timeout] : 高速移行の再アソシエーションがタイムアウトになるまでの時間（秒単位）。デフォルトは 20 秒です。有効範囲は 1 ～ 100 です。 （注） [Over the DS] または [Reassociation Timeout] を有効にするには、高速移行を有効にします。 [WPA+WPA2] のパラメータ： • [WPA1] : WPA1 を有効にする場合は、チェックボックスをオンにします。 • [WPA2] : WPA2 を有効にする場合は、チェックボックスをオンにします。 認証キー管理： • [FT802.1X] : FT802.1X を有効にする場合は、チェックボックスをオンにします。 • [802.1X] : 802.1X を有効にする場合は、チェックボックスをオンにします。 • [CCKM] : CCKM を有効にする場合は、チェックボックスをオンにします。 • [PSK] : PSK を有効にする場合は、チェックボックスをオンにします。 • [FT PSK] : ASCII または 16 進（HEX）形式を選択でき、これによって Fast Transition に対する事前共有キーを入力します。 • [PMF 802.1X] : 管理フレームの保護（PMF）の 802.1X 認証。 • [PMF PSK] : PMF の事前共有キー（PSK）。ASCII または 16 進形式（HEX）を選択し、Fast Transition の事前共有キーを入力します。 （注） [FT802.1X] または [FTPSK] を設定するには、WPA2 および高速移行を有効にします。

表 11-2　レイヤ 2 セキュリティのオプション （続き）

フィールド	説明
Protected Management Frame	[Protected Management Frame]：次を選択できるドロップダウン リスト。 • [Disabled]：WLAN の 802.11w MFP 保護を無効にします。 • [Optional]：WLAN の 802.11w MFP 保護を有効にします。 • [Required]：クライアントが WLAN の 802.11w MFP 保護をネゴシエートすることを要求します。 802.11w では、ブロードキャストまたはマルチキャストの管理フレームを保護するために使用される Integrity Group Temporal Key（IGTK）が導入されています。IGTK は、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用するオーセンティケータ ステーション（コントローラ）によって割り当てられる、ランダムな値です。802.11w IGTK キーは、4 ウェイ ハンドシェイクを使用して取得され、レイヤ 2 で WPA または WPA2 セキュリティによって設定されている WLAN でのみ使用されます。 **（注）** PMF を有効にするために、PMF AKM のいずれか 1 つと WPA2 が有効になっている必要があります。
Association Comeback Timer	アソシエーション復帰間隔（秒単位）。このタイマーは、アソシエーションされたクライアントがステータス コード 30 で拒否された後にアソシエーションを再試行するまで待機する必要のある間隔です。ステータス コード 30 のメッセージは、Association request rejected temporarily; Try again later です。 有効な範囲は 1 ～ 10 秒です。デフォルト値は 1 秒です。

表 11-2　レイヤ 2 セキュリティのオプション （続き）

フィールド	説明
SA Query Retry Timeout	ミリ秒単位でのセキュリティ アソシエーション（SA）クエリー間隔です。このタイムアウトはアソシエーションを再試行する前に、すでにアソシエーションされているクライアントへのアソシエーション応答で特定される間隔です。アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかが確認されます。クライアントがこの時間内に応答しない場合は、クライアント アソシエーションがコントローラから削除されます。 範囲は 100 ～ 500 ミリ秒です。デフォルトの値は 200 ミリ秒です。
CKIP	Cisco Key Integrity Protocol（CKIP）。Cisco のアクセス ポイントは、ビーコンおよびプローブの応答パケットで CKIP のサポートをアドバタイズします。CKIP は、Aironet IE が WLAN で有効な場合にだけ設定できます。 （注）　CKIP は 10xx AP ではサポートされていません。 選択すると、これらの CKIP フィールドが表示されます。 [Key size] : 設定なし、40 または 104 [Key Index] : 1 ～ 4 [Encryption Key] : 暗号キーを指定します。 [Key Format] : ASCII または HEX （注）　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。 [MMH Mode] : チェックボックスをオンにして有効にします。 [Key Permutation] : チェックボックスをオンにして有効にします。

ステップ 2　MAC アドレスによりクライアントをフィルタリングする場合は、[MAC Filtering] チェックボックスをオンにします。

（注）　MAC フィルタ リスト内で指定されていなくてもコントローラに接続できるのは、メッシュ アクセス ポイントだけです。

（注）　4.1.82.0 以前のリリースでは、メッシュ アクセス ポイントは MAC フィルタ リストで定義されていない限り、コントローラに接続しません。

新しく追加されたアクセス ポイントがコントローラに接続できるようにするには、MAC フィルタ リストを無効にします。MAC フィルタ リストを再度有効にする前に、新しいアクセス ポイントの MAC アドレスを入力する必要があります。

ステップ 3　目的の種類の認証キー管理を選択します。802.1X、CCKM または PSK を選択できます。

（注）　PSK を選択した場合は、共有キーと種類（ASCII または 16 進数）を入力する必要があります。

（注）　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。

ステップ 4　[Save] をクリックします。

[Layer 3] タブ

[Layer 3 Security] ドロップダウン リストを使用して、[None]、[VPN Pass Through]、[IPsec]（**インターネット プロトコル セキュリティ**）のいずれかを選択します。選択肢によって、ページ パラメータが変わります。WLAN のタイプに応じて、使用できるレイヤ 3 パラメータと使用できないレイヤ 3 パラメータがあります。

（注）　[VPN Pass Through] を選択した場合は、VPN ゲートウェイ アドレスを入力する必要があります。

（注）　IPsec は、データ ストリーム内の各 IP パケットを認証および/または暗号化して、IP 通信のセキュリティを確保するプロトコル スイートです。また、IPsec には、暗号キーを確立するためのプロトコルも含まれます。

次の情報を設定します。

- [Web Policy] : 認証、パススルー、条件付き Web リダイレクト、または [WebAuth on MAC Filter Failure] などのポリシーを指定するには、このチェックボックスをオンにします。また、このセクションではゲスト ユーザに対してカスタマイズしたログイン ページが表示されるようにもできます。

  （注）　パススルーを選択した場合は、[Email Input] チェックボックスが表示されます。ユーザがネットワークに接続しようとしたとき、電子メール アドレスの入力を求める場合は、このチェックボックスをオンにします。

- [Preauthentication ACL] : クライアントとコントローラ間のトラフィックに使用される IPv4、IPv6、および WebAuth ACL のリストを示します。

  （注）　WLAN の IPv6 ACL マッピングは、リリース 7.2.x 以降のコントローラでサポートされています。

- [Sleeping Client Enable] : スリープ状態にあるクライアントのサポートを有効にするには、このチェックボックスを選択します。この機能は、リモートおよびゲスト LAN には適用できません。

- [Sleeping ClientTimeout]：スリープ状態にあるクライアントが強制的に再認証されるまでの、アイドル タイムアウト後の最大時間数（時間単位）。範囲は 1 ～ 720 時間です。デフォルト値は 12 時間です。このフィールドは [Sleeping Client] チェックボックスをオンにしている場合にだけ表示されます。また、スリープと再起動時間の間、クライアントは同じモビリティ グループ内で 1 つのコントローラから別のコントローラに移動した場合、ログイン資格情報を入力する必要はありません。
- [Global WebAuth Configuration]：カスタムの Web 認証ページを指定するには、このチェックボックスをオフにします。
- [Web Auth Type]：[Web Auth Type] ドロップダウン リストが表示されたら、次のいずれかのオプションを選択して、無線ゲスト ユーザ用の Web ログイン ページを定義します。
  - [Default Internal]：ゲスト ユーザに対して、デフォルトのログイン ページが表示されます。
  - [Customized WebAuth]：[Upload/Download Commands] ページから、カスタマイズされたログイン ページをダウンロードできます。詳細については、「カスタマイズ Web 認証ページのダウンロード」（P.11-668）を参照してください。

    ドロップダウン リストから、[Web Auth Login Page]、[Web Auth Login Failure Page]、[Web Auth Logout Page] のいずれかを選択します。

    カスタマイズしたページを表示しないオプションに対しては、任意のドロップダウン リストで [None] を選択します。
  - [External]：ゲスト ユーザは、外部のログイン ページにリダイレクトされます。[External Web Auth URL] テキスト ボックスに、ログイン ページの URL を入力します。

    （注）　[External] を選択した場合、[Security] > [AAA] ページで最大 3 つの RADIUS および LDAP サーバを選択できます。

AAA サーバ

[AAA Servers] タブをクリックすると、[AAA Servers] タブが表示されます。

[AAA Servers] タブを設定するには、次の手順を実行します。

ステップ 1　[Radius Server Overwrite Interface] チェックボックスをオンにして、WLAN で設定されているダイナミック インターフェイスを介してクライアント認証要求を送信します。[Radius Server Overwrite Interface] オプションを有効にすると、WLC は、その WLAN で設定されているダイナミック インターフェイスを使用して、WLAN のすべての RADIUS トラフィックを送信します。

（注）　[Diagnostic Channel] が有効な場合、[Radius Server Overwrite Interface] を有効にすることはできません。

（注）　[Radius Server Overwrite Interface] オプションは、コントローラ リリース 7.0.x 以降でサポートされます。

ステップ 2　[Enable] チェックボックスをオンにして、RADIUS および LDAP サーバ セクションのドロップダウン リストを使用して、認証およびアカウンティング サーバを選択します。これによって、指定した WLAN のデフォルトの RADIUS サーバが選択され、ネットワークに対して設定されている RADIUS サーバは上書きされます。3 つすべての RADIUS サーバが特定の 1 つの WLAN に対して設定されている場合、優先順位はサーバ 1 が最も高くなります。

LDAP サーバをここで選択しないと、Prime Infrastructure はデータベースのデフォルトの LDAP サーバ順序を使用します。

ステップ 3　RADIUS サーバ アカウンティングの暫定アップデートを有効にする場合は、[Interim Update] チェックボックスをオンにします。このチェックボックスをオンにした場合、[Interim Interval] 値を指定します。範囲は 180 ～ 3600 秒で、デフォルト値は 0 です。

（注）　[Interim Interval] は、[Interim Update] を有効にした場合にのみ入力できます。

ステップ 4　有効にする EAP プロファイルをすでに設定している場合は、[Local EAP Authentication] チェックボックスをオンにします。ローカル EAP は、ユーザと無線クライアントがローカルで認証できる認証メソッドです。この方式は、バックエンド システムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。

ステップ 5　AAA Override が有効で、クライアントにおいて AAA とコントローラ WLAN 認証フィールドが競合している場合、クライアント認証は AAA サーバにより行われます。この認証の一部として、オペレーティング システムはクライアントをデフォルトの Cisco WLAN ソリューション から、AAA サーバにより返され、コントローラのインターフェイス設定で事前定義された VLAN に移動します（MAC フィルタリング、802.1X、または WPA 動作用に設定されている場合のみ）。すべての場合において、オペレーティング システムは、QoS、および AAA サーバにより提供される ACL がコントローラ インターフェイス設定で事前に定義されている限り、これらも使用します。（この AAA オーバーライドによる VLAN スイッチングは、ID ネットワーキングとも呼ばれます）。

たとえば、企業の WLAN が主に VLAN 2 に割り当てられた管理インターフェイスを使用し、AAA Override が VLAN 100 へのリダイレクトを返す場合、物理ポートが VLAN 100 に割り当てられているかどうかは関係なく、オペレーティング システムは、すべてのクライアント転送を VLAN 100 にリダイレクトします。

AAA Override が無効の場合、すべてのクライアント認証はデフォルトのコントローラの認証パラメータ設定となり、コントローラの WLAN にクライアント固有の認証パラメータが含まれていない場合、認証のみ AAA サーバによって行われます。

AAA オーバーライド値は、たとえば RADIUS サーバから取り込まれます。

ステップ 6　[Save] をクリックします。

[QoS] タブ

[WLAN Template] ページの [QoS] タブをクリックすると、[QoS] タブが表示されます。

QoS フィールドを設定するには、次の手順を実行します。

ステップ 1　[QoS] ドロップダウン リストから、[Platinum]（音声）、[Gold]（ビデオ）、[Silver]（ベストエフォート）、または [Bronze]（バックグラウンド）のいずれかを選択します。VoIP などのサービスは [Gold] に設定する必要がありますが、テキスト メッセージなど差別的ではないサービスは [Bronze] に設定できます。

ステップ 2　ネットワークベース アプリケーション認識（NBAR）のディープ パケット インスペクション テクノロジーに基づいてアプリケーションの分類を表示するには、[NBAR Visibility] チェックボックスをオンにします。

ステップ 3　[AVC Profile] ドロップダウン リストから、WLAN の Application Visibility and Control（AVC）プロファイルを選択できます。

ステップ 4　[Netflow Monitor] ドロップダウン リストから、WLAN の Netflow モニタを選択できます。

ステップ 5　[Override Per-User Rate Limits] グループ ボックスで、次のフィールドを設定します。

（注）　ワイヤレス レート制限は、アップストリームおよびダウンストリーム トラフィックの両方に定義できます。

- [Average Data Rate] : [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックの平均データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
- [Burst Data Rate] : [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。
- [Average Real-Time Rate] : [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
- [Burst Real-Time Rate] : [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-realtime-rate は average-realtime-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

ステップ 6　[Override Per-SSID Rate Limits] グループ ボックスで、次のフィールドを設定します。

- [Average Data Rate] : [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックの平均データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
- [Burst Data Rate] : [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。
- [Average Real-Time Rate] : [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。
- [Burst Real-Time Rate] : [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザまたは SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。値 0 は、プロファイルに帯域幅の制限を課しません。burst-realtime-rate は average-realtime-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。

ステップ 7　[WMM Policy] ドロップダウン リストから、[Disabled]、[Allowed]（クライアントが WLAN と通信できるようにする）、または [Required]（クライアントが通信で WMM を有効にすることを必須とする）を選択します。

ステップ 8　Cisco 7920 電話でサポートを有効にする場合は、[7920 AP CAC] チェックボックスをオンにします。

ステップ 9　7920 電話で WLAN に旧バージョンのソフトウェアをサポートさせる場合は、[7920 Client CAC] チェックボックスをオンにして有効にします。CAC の制限は、より新しいバージョンのソフトウェアのアクセス ポイントで設定されます。

ステップ 10　[Save] をクリックします。

[Advanced] タブ

ステップ 1　FlexConnect ローカル スイッチングを有効にする場合は、[FlexConnect local switching] チェックボックスをオンにします。FlexConnect の詳細については、「FlexConnect の設定」（P.12-761）を参照してください。これを有効にすると、FlexConnect のアクセス ポイントは、クライアント認証を処理し、クライアント データ パケットをローカルにスイッチングします。FlexConnect ローカル スイッチングは、Cisco 1130/1240/1250 シリーズのアクセス ポイントに対してだけ適用可能です。これは、L2TP または PPTP 認証ではサポートされていません。また、WLAN ID 9 ～ 16 には適用できません。

ステップ 2　FlexConnect ローカル認証を有効にする場合は、[FlexConnect Local Auth] チェックボックスをオンにします。

ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位（MTU）が 500 バイトを下回らない、最小帯域幅が 128 kbps のリモート オフィス設定の基準を維持できない場合に役立ちます。ローカル スイッチングでは、認証機能はアクセス ポイント自体に存在します。そのため、ローカル認証によって、ブランチ オフィスの遅延要件が軽減されます。

（注）　ローカル認証は、ローカル スイッチング モードの FlexConnect AP の WLAN のみで有効にできます。

ローカル認証は、次のシナリオではサポートされません。

- FlexConnect ローカル認証を有効にした WLAN では、ゲスト認証は実行できません。
- RRM 情報は、FlexConnect ローカル認証を有効にした WLAN のコントローラでは使用不可です。
- ローカル RADIUS はサポートされません。
- クライアントが認証されると、グループの WLC およびその他の FlexConnect でクライアント情報が更新された後で、ローミングがサポートされます。

ステップ 3　H-REAP ローカル スイッチングを有効にすると、[Learn Client IP Address] チェックボックスがデフォルトで有効になります。ただし、クライアントが Fortress レイヤ 2 暗号化を使用するように設定されている場合は、コントローラがそのクライアント IP アドレスを知ることができないので、コントローラはクライアントの接続を定期的に切断します。コントローラがクライアント IP アドレスを知らなくてもクライアント接続を維持できるように、このオプションを無効にしてください。このオプションを無効にできるのは、H-REAP ローカル スイッチングを行うように設定されているときだけです。
H-REAP 中央スイッチングを行う場合は、無効にすることはできません。

ステップ 4　[VLAN based Central Switching] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上での AAA Override VLAN に基づく中央スイッチングを有効または無効にします。次に、この機能の機能および制約事項について説明します。

- オーバーライドされたインターフェイス上でのマルチキャストはサポートされていません。
- この機能は、WLAN がローカルでスイッチされる WLAN 単位でのみ使用できます。
- IPv6 ACL、CAC、NAC、および IPv6 はサポートされていません。
- IPv4 ACL は、VLAN に基づく中央スイッチング有効な場合にのみサポートされ、無線 LAN 上の中央スイッチングのクライアントにのみ適用できます。
- この機能は、ローカルでスイッチされる WLAN の FlexConnect モードの AP に適用できます。
- この機能は、ローカル モードの AP には適用できません。

- この機能は、中央でスイッチされる WLAN の FlexConnect モードの AP ではサポートされません。
- この機能は、中央認証だけでサポートされます。
- この機能は、Web 認証セキュリティ クライアント上ではサポートされません。
- ローカル スイッチング クライアントのレイヤ 3 ローミングはサポートされません。

ステップ 5　[Central DHCP Processing] チェックボックスをオンまたはオフにして、機能を有効または無効にします。この機能を有効にすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。

ステップ 6　[Override DNS] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバ アドレスのオーバーライドを有効または無効にします。中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。

ステップ 7　[NAT-PAT] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換（NAT）およびポートアドレス変換（PAT）を有効または無効にします。NAT および PAT をイネーブルにするには、[Central DHCP Processing] を有効にする必要があります。

ステップ 8　選択して診断チャネル機能を有効にするか、そのままにして機能を無効にします。診断チャネル機能により、WLAN とのクライアント通信に関する問題のトラブルシューティングが可能になります。問題のあるクライアントにより診断チャネルが開始されると、通信への障害物が最も少なく、最も堅牢な通信方法が提供されます。

ステップ 9　この WLAN の Aironet 情報要素（IE）のサポートを有効にする場合は、[Aironet IE] チェックボックスをオンにします。Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの番号などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、コントローラは、Aironet IEs 0x85 および 0x95（コントローラの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション要求に格納して送信します。

ステップ 10　[IPv6] チェックボックスをオンにします。同じ WLAN 上で IPv6 ブリッジおよび IPv4 Web 認証を設定できます。

ステップ 11　[Session Timeout] チェックボックスをオンにして、クライアント セッションが再許可を必要とせずに続行できる最大時間を設定します。

ステップ 12　この WLAN で Coverage Hold Detection（CHD）を有効または無効にするか選択します。デフォルトでは、CHD は、コントローラのすべての WLAN で有効です。WLAN で CHD を無効にした場合、カバレッジ ホールの警告はコントローラに送信されますが、カバレッジ ホールを解消するためのそれ以外の処理は行われません。この機能は、モバイル利用率の高いゲストが短期間だけネットワークに接続するゲスト WLAN で役に立ちます。

ステップ 13　[Override Interface] ドロップダウン リストは、定義済みのアクセス コントロール リスト（ACL）のリストを提供します。（ACL を定義する手順については、「アクセス コントロール リスト テンプレートの設定」（P.11-671）を参照してください）。リストから ACL を選択すると、WLAN は ACL を WLAN にアソシエートします。ACL の選択はオプションで、このフィールドのデフォルトは、[None] です。

ステップ 14　すべての WLAN にステータスを適用するのではなく、WLAN ごとにピアツーピア ブロックを設定できます。[Peer to Peer Blocking] ドロップダウン リストから、次のいずれかを選択します。

- [Disable]：ピアツーピア ブロックは無効にされています。トラフィックは可能な場合はローカルでブリッジされます。
- [Drop]：パケットは廃棄されます。
- [Forward Up Stream]：パケットはアップストリーム VLAN 上に転送され、そのパケットをどうするかが決定されます。

（注）　コントローラ リリース 7.2.x 以降では、[Forward Up Stream] はローカルでスイッチするクライアントの [Drop] と同じです。

WLAN の FlexConnect ローカル スイッチングが有効になっている（トラフィックがコントローラを通過するのを防ぐ）場合は、このドロップダウン リストが灰色になります。

（注）　ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。

ステップ 15　[Wi-Fi Direct Clients Policy] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [Disabled] : WLAN の Wi-Fi Direct クライアント ポリシーを無効にして、すべての Wi-Fi Direct 対応クライアントを認証解除します。デフォルトでは無効になっています。
- [Allow] : Wi-Fi Direct クライアントとインフラストラクチャ WLAN とのアソシエーションを許可します。
- [Not-Allow] : Wi-Fi Direct クライアントとインフラストラクチャ WLAN とのアソシエーションを禁止します。

（注）　Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。

（注）　Wi-Fi Direct クライアント ポリシーは、リリース 7.2.x 以降のコントローラに適用できます。

ステップ 16　クライアントの自動的な除外を有効にする場合は、[Client Exclusion] チェックボックスをオンにします。

ステップ 17　クライアントの除外を有効にする場合、無効となるクライアント マシンの [Timeout Value] を秒単位で設定することも必要です。クライアント マシンは MAC アドレスで除外され、そのステータスは監視できます。0 のタイムアウト設定は、クライアントを再度有効にするには管理制御が必要であることを示します。

（注）　セッションのタイムアウトが設定されていない場合、除外されたクライアントはそのまま残り、除外された状態からタイムアウトすることはありません。除外機能が無効であることを意味するのではありません。

ステップ 18　[Maximum Clients] テキスト ボックスに、WLAN に関連付けられるクライアントの最大数を入力します。有効な範囲は 0 ～ 7000 です。デフォルト値は 0 です

（注）　値を 0 にすると、WLAN に関連付けられるクライアント数が無限になります。

ステップ 19　[Static IP Tunneling] チェックボックスをオンにして、スタティック IP クライアントのダイナミック アンカリングを有効にします。

ステップ 20　[Media Session Snooping] チェックボックスをオンにします。この機能により、アクセス ポイントは音声コールの確立、終了、および失敗を検出し、それをコントローラおよび Prime Infrastructure にレポートできます。WLAN ごとに有効化または無効化できます。

メディア セッション スヌーピングが有効な場合、この WLAN をアドバタイズするアクセス ポイント無線は、Session Initiation Protocol（SIP）音声パケットをスヌープします。ポート番号 5060 に宛てた、またはポート番号 5060 からのパケットはいずれも、詳細検査の対象として考慮されます。アクセス ポイントは、Wi-Fi マルチメディア（WMM）および非 WMM クライアントがコールを確立中か、すでにアクティブなコール上にあるか、またはコールの終了処理中であるかをトラッキングし、コントローラに対して主要なコール イベントを通知します。

ステップ 21　[KTS based CAC] チェックボックスをオンにして、WLAN ごとの KTS ベース CAC サポートを有効にします。

WLC は、TSPEC ベースの CAC および SIP ベースの CAC をサポートしています。ただし、異なる CAC のプロトコルで稼働する特定の電話があります。これらは、KTS（Key Telephone System）をベースとします。CAC および KTS ベースの SIP クライアントをサポートするには、WLC はこのプロトコルの一部として、特定のその他のメッセージを処理して送信することに加えて、これらのクライアントからの帯域幅要求メッセージを理解して処理し、AP 無線上に要求された帯域幅を割り当てる必要があります。

（注）　KTS CAC 設定は、コントローラ ソフトウェア リリース 7.2.x を実行する Cisco 5508、7500、WISM2、2500 コントローラのみでサポートされています。この機能は、Cisco 4400 シリーズ コントローラではサポートされません。

ステップ 22　[NAC State] : [NAC State] ドロップダウン リストから、[SNMP NAC] または [Radius NAC] を選択します。検出された SIP エラーにより、クライアントのトラブルシューティングおよびアラーム画面に表示されるトラップが生成されます。コントローラはアウトオブバンドの NAC アプライアンスと統合できます。NAC アプライアンスは、クライアントが分析および解除されるまでデータ パス内に保持されます。アウトオブバンド モードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。詳細については、「NAC 統合」（P.9-330）を参照してください。

ステップ 23　[Off-Channel Scanning Defer] は、ノイズや干渉など代替チャネル選択に関する情報を収集する RRM を使用するときに重要となります。また、[Off-Channel Scanning Defer] は、不正検出を行います。[Off-Channel Scanning Defer] を提供する必要があるデバイスは、可能な限り、同じ WLAN を使用する必要があります。このようなデバイスが多くある場合（この機能を使用して Off-Channel Defer スキャンが完全に無効化されている可能性があります）、モニタ アクセス ポイントや、この WLAN が割り当てられていない同じ位置にあるその他のアクセス ポイントなど、代わりにローカル AP で [Off-Channel Scanning Defer] を実装する必要があります。

QoS ポリシー（ブロンズ、シルバー、ゴールド、プラチナ）の WLAN への割り当ては、クライアントからアップリンクでどのように受信されたかに関係なく、パケットがアクセス ポイントからのダウンリンク接続でどのようにマーキングされるかに影響します。UP=1,2 は最低の優先順位で、UP=0,3 はその次に高い優先順位です。各 QoS ポリシーのマーキング結果は次のとおりです。

- ブロンズは、すべてのダウンリンク トラフィックを UP= 1 にマーキングします。
- シルバーは、すべてのダウンリンク トラフィックを UP= 0 にマーキングします。
- ゴールドは、すべてのダウンリンク トラフィックを UP= 4 にマーキングします。
- プラチナは、すべてのダウンリンク トラフィックを UP= 6 にマーキングします。

優先順位引数をクリックして [Scan Defer Priority] を設定し、[Scan Defer Interval] テキスト ボックスに時間をミリ秒単位で設定します。有効な値は、0 ～ 60000 です。デフォルト値は 100 ミリ秒です。

ステップ 24　802.11a/n ネットワークおよび 802.11b/g/n ネットワークの場合、Lightweight アクセス ポイントは、Delivery Traffic Indication Map（DTIM）と同期する一定間隔でビーコンをブロードキャストします。アクセス ポイントでビーコンがブロードキャストされると、DTIM period で設定した値に基づいて、バッファされたブロードキャスト フレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャスト データやマルチキャスト データが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11a/n または 802.11b/g/n のネットワークのビーコン期間が 100ms で DTIM 値が 1 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 5 回送信します。ブロードキャスト フレームおよびマルチキャスト フレームの頻度を考慮して、VoIP を含むアプリケーションに適したいずれかの設定を使用できます。

ただし、802.11a/n または 802.11b/g/n のすべてのクライアントで省電力モードが有効になっている場合は、DTIM 値を最大 255 まで設定できます（ブロードキャスト フレームおよびマルチキャスト フレームは 255 回のビーコンで 1 回送信）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100ms で DTIM 値が 100 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを 10 秒おきに送信するので、省電力クライアントを再起動してブロードキャストとマルチキャストをリッスンするまでのスリープ時間が長くなり、結果的にバッテリー寿命が長くなります。

多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。省電力クライアントをサポートしている 802.11a/n ネットワークおよび 802.11b/g/n ネットワークでは、DTIM 値を小さく設定することを推奨します。

DTIM Period の下の 802.11a/n フィールドと 802.11b/g/n フィールドに 1 ～ 255 までの値を入力します。デフォルト値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）です。

ステップ 25　DHCP サーバを上書きするチェックボックスをオンにすると、別のパラメータが表示され、ここで DHCP サーバの IP アドレスを入力できます。一部の WLAN 設定では、これは必須です。有効な 3 つの設定は、次のとおりです。

- DHCP Required および有効な DHCP サーバの IP アドレスを設定 : すべての WLAN クライアントは DHCP サーバから IP アドレスを取得します。
- DHCP は不要とし、有効な DHCP サーバの IP アドレスを設定 : すべての WLAN クライアントは、DHCP サーバから IP アドレスを取得するか、固定 IP アドレスを使用します。
- DHCP は不要とし、DHCP サーバの IP アドレスを 0.0.0.0 に設定 : すべての WLAN クライアントは強制的に固定 IP アドレスを使用します。すべての DHCP 要求はドロップされます。

DHCP のアドレス割り当てを要求した後に DHCP サーバの IP アドレスの入力を選択できません。

ステップ 26　[MFP Signature Generation] チェックボックスがオンの場合、この WLAN にアソシエートされているアクセス ポイントにより送信される 802.11 管理フレームのシグニチャ生成が可能です。シグニチャ生成によって、侵入者による送信された管理フレームへの変更が、確実に検出および報告されます。

ステップ 27　[MFP Client Protection] ドロップダウン リストから、コントローラの個別の WLAN の設定のために [Enabled]、[Disabled]、または [Required] を選択します。インフラストラクチャ MFP が有効でない場合、このドロップダウン リストは使用できません。

（注）　[Enabled] なパラメータは、WLC グラフィカル ユーザ インターフェイスの [MFP Client Protection] ドロップダウン リストで選択する [Optional] パラメータと同じです。

（注）　クライアント側 MFP は、Cisco Compatible Extensions（バージョン 5 以降）クライアントをサポートするよう設定されている WLAN でだけ使用でき、WPA2 が最初に設定されている必要があります。

ステップ 28　ビーコン間隔として 1 ～ 255 の値を、このページの [802.11a/n DTIM Period] グループ ボックスに入力します。コントローラは、ビーコン間隔の入力値に従い、この WLAN の 802.11a/n 無線で DTIM パケットを送信します。

ステップ 29　ビーコン間隔として 1 ～ 255 の値を、このページの [802.11b/g/n DTIM Period] グループ ボックスに入力します。コントローラは、ビーコン間隔の入力値に従い、この WLAN の 802.11b/g/n 無線で DTIM パケットを送信します。

（注）　DTIM 設定は、ゲスト LAN には適していません。

ステップ 30　[PMIP Mobility Type] ドロップダウン リストから、次のオプションのモビリティ タイプを選択します。

- [None]：簡易 IP を使用して WLAN を設定します。
- [Mixed]：簡易 IP および PMIPv6 を使用して WLAN を設定します。
- [PMIPv6]：PMIPv6 のみを使用して WLAN を設定します。

ステップ 31　WLAN で mDNS スヌーピングを有効にするには、[mDNS Snooping] チェックボックスをオンにします。デフォルトで、このオプションは有効になっています。

ステップ 32　[mDNS Profile] ドロップダウン リストから、WLAN の mDNS プロファイルを選択できます。デフォルト値は default-mdns-profile です。

ステップ 33　[Save] をクリックします。

[Policy Configuration] タブ

ステップ 1　[Policy Configuration] タブで、次のフィールドを設定します。

- [Policy Name]：ポリシー名。
- [Policy Priority]：1 ～ 16 のポリシー プライオリティを設定します。2 つのポリシーが同じプライオリティを持つことはできません。

（注）　WLAN あたりのポリシー マッピングは 16 だけです。そのマッピング用に選択したポリシーのテンプレートが、コントローラにポリシーがない場合に最初に適用されます。

クライアント プロファイルの設定

クライアントが WLAN にアソシエートしようとする場合、プロセスで受信した情報からクライアント タイプを決定することができます。コントローラは情報のコレクタとして機能し、必要なデータとともに最適な形式で ISE を送信します。

クライアント プロファイルを設定する場合、次のガイドラインに従います。

デフォルトで、クライアントのプロファイルはすべての WLAN 上で無効です。

- クライアント プロファイルは、ローカル モードと FlexConnect モードのアクセス ポイントでサポートされます。
- プロファイルは、次のシナリオのクライアントではサポートされません。

  - スタンドアロン モードで FlexConnect モード AP とアソシエートしているクライアント。
  - ローカル スイッチングが有効な状態でローカル認証が行われる場合に FlexConnect モード AP とアソシエートしているクライアント。
- コントローラでは DHCP プロキシと DHCP ブリッジ モードの両方がサポートされます。
- WLAN のアカウンティング サーバの設定は、1.1 MnR 以降のリリースを実行する ISE を指している必要があります。Cisco の ACS では、クライアント プロファイルはサポートされていません。
- 使用されている DHCP サーバのタイプは、クライアントのプロファイルに影響しません。
- DHCP_REQUEST のパケットに ISE プロファイル済みデバイス リストで見つかった文字列が含まれている場合、クライアントは自動的にプロファイルされます。
- クライアントは、Accounting request パケットで送信される MAC アドレスに基づいて識別されます。
- プロファイルが有効になると MAC アドレスだけがアカウンティング パケットの発信側ステーション ID として送信されます。
- ローカル スイッチングの FlexConnect モードの AP でプロファイルが有効である場合、VLAN オーバーライドだけが AAA Override 属性としてサポートされます。

クライアント プロファイルを設定するには、次の手順に従います。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[WLAN] をクリックするか、左側のサイドバーのメニューから [WLANs] > [WLAN Configuration] を選択します。

ステップ 3　[Advanced] タブをクリックします。

ステップ 4　DHCP プロファイルを有効にするには、[DHCP Profiling] チェックボックスをオンにします。

ステップ 5　HTTP プロファイルを有効にするには、[HTTP Profiling] チェックボックスをオンにします。

（注）　HTTP クライアント プロファイルは、コントローラ バージョン 7.3.1.31 以降でサポートされます。

ステップ 6　[Save] をクリックします。

モバイル コンシェルジュの設定（802.11u）

モバイル コンシェルジュは、外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュ機能は、クライアントにサービスのアベイラビリティに関する情報を提供し、使用可能なネットワークをアソシエートするのに役立ちます。

ネットワークから提供されるサービスは、次の 2 つのプロトコルに大きく分類できます。

- 802.11u MSAP
- 802.11u HotSpot 2.0

モバイル コンシェルジュには、次のガイドラインと制限事項が適用されます。

- モバイル コンシェルジュは FlexConnect アクセス ポイントではサポートされません。
- 802.11u 設定アップロードはサポートされません。設定のアップグレードを実行し、設定をコントローラにアップロードすると、WLAN の HotSpot の設定は失われます。

モバイル コンシェルジュ（802.11u）グループを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[WLAN] をクリックするか、左側のサイドバーのメニューから [WLANs] > [WLAN Configuration] を選択します。

ステップ 3　[Hot Spot] タブをクリックします。

ステップ 4　[802.11u Configuration] タブで、次のフィールドを設定します。

- [802.11u Status] チェックボックスをオンにして WLAN の 802.11u を有効にします。
- [Internet Access] チェックボックスを選択して、この WLAN からインターネット サービスを提供できるようにします。
- [Network Type] ドロップダウン リストから、この WLAN に設定する 802.11u を表すネットワークタイプを選択します。次のオプションを使用できます。
  - **Private Network**
  - **Private Network with Guest Access**
  - **Chargeable Public Network**
  - **Free Public Network**
  - **Emergency Services Only Network**
  - **Personal Device Network**
  - **Test or Experimental**
  - **Wildcard**
- このネットワークの 802.11u パラメータ用に設定する認証タイプを選択します。
  - **Not configured**
  - **Acceptance of Terms and Conditions**
  - **Online Enrollment**
  - **HTTP/HTTPS Redirection**
- [HESSID] フィールドに、Homogenous Extended Service Set Identifier 値を入力します。HESSID は、HESS を識別する 6 オクテットの MAC アドレスです。

ステップ 5　[Others] タブで、次のフィールドを設定します。

- [OUI List] グループ ボックスで、次の詳細情報を入力します。
  - OUI name
  - Is Beacon
  - OUI Index

  [Add] をクリックして、OUI（組織固有識別子）エントリをこの WLAN に追加します。
- [Domain List] グループ ボックスで、次の詳細情報を入力します。
  - [Domain Name]：802.11 アクセス ネットワークで稼働するドメイン名。
  - [Domain Index]：ドロップダウン リストからドメイン インデックスを選択します。

  [Add] をクリックして、ドメイン エントリをこの WLAN に追加します。

ステップ 6　[Realm] タブで、次のフィールドを設定します。

- [OUI List] セクションで、次の詳細情報を入力します。
  - [Realm Name]：レルム名。

- [Realm Index]：レルム インデックス。

[Add] をクリックして、ドメイン エントリをこの WLAN に追加します。

ステップ 7　[Service Advertisement] タブで、次のフィールドを設定します。

- [MSAP Enable] チェックボックスをオンにし、サービス アドバタイズメントを有効にします。
- 前のステップで MSAP を有効にした場合は、サーバ インデックスを提供する必要があります。この WLAN のサーバ インデックスを入力します。サーバのインデックス フィールドによって、BSSID を使用して到達可能である場所を提供する MSAP サーバ インスタンスを一意に識別します。

（注）　MSAP（Mobility Services Advertisement Protocol）は、ネットワーク接続を確立するためのポリシー セットを使用して設定されたモバイル デバイスで主に使用するために設計されています。これらのサービスは、上位層サービスを提供するデバイス、つまりサービス プロバイダー経由で有効にされるネットワーク サービス向けです。サービス アドバタイズメントは、MSAP を使用して、Wi-Fi アクセス ネットワークへのアソシエーションの前にサービスをモバイル デバイスに提供します。この情報はサービス アドバタイズメントで伝送されます。シングルモードまたはデュアルモード モバイル デバイスは、アソシエーションの前にサービス ネットワークをネットワークにクエリーします。デバイスによるネットワークの検出および選択機能では、ネットワークに join する判断においてサービス アドバタイズメントを使用する場合があります。

ステップ 8　[HotSpot] タブで、次のフィールドを設定します。

- [HotSpot2 Enable] ドロップダウン リストから [Enable] オプションを選択します。
- [WAM Metrics] グループ ボックスで、次の項目を指定します。
  - [WAN Link Status]：リンク ステータス。有効な範囲は 1 ～ 3 です。
  - [WAN SIM Link Status]：対称リンク ステータス。たとえば、アップリンクとダウンリンクに異なる速度または同じ速度を設定できます。
  - [Down Link Speed]：ダウンリンク速度。最大値は 4,194,304 kbps です。
  - [Up Link Speed]：アップリンク速度。最大値は 4,194,304 kbps です。
- [Operator Name List] グループ ボックスで、次の項目を指定します。
  - [Operator Name]：802.11 オペレータの名前を指定します。
  - [Operator Index]：オペレータ インデックスを選択します。範囲は 1 ～ 32 です。
  - [Language Code]：言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。

  [Add] をクリックして、オペレータの詳細を追加します。オペレータの詳細が表形式で表示されます。
- [Port Config List] で、次の項目を指定します。
  - [IP Protocol]：有効にしたい IP プロトコル。次のオプションは、ESP、FTP、ICMP、および IKEV2 です。
  - [Port No]：この WLAN で有効になっているポート番号。
  - [Status]：ポートのステータス。

ステップ 9　[Save] をクリックします。

WLAN AP グループ テンプレートの設定

サイト固有の VLAN または AP グループは、WLAN を異なるブロードキャスト ドメインにセグメント化することで、ブロードキャスト ドメインを最小に制限します。このようにすることで、ロード バランシングおよび帯域幅割り当てを効果的に管理できるというメリットがあります。

WLAN AP グループを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[AP Groups] をクリックするか、左側のサイドバーのメニューから [WLAN] > [AP Groups] を選択します。[WLAN] > [AP Groups] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[AP Groups template] ページが表示されます。

このページには、ネットワーク上に設定されている AP グループのサマリーが表示されます。このページで、AP グループの詳細を追加、削除、編集または表示できます。[Edit] 列をクリックして、そのアクセス ポイントを編集します。[WLAN Profile Name] 列のチェックボックスをオンにし、[Remove] をクリックして、WLAN プロファイルを削除します。

（注）　[Description] テキスト ボックスに入力できる最大数は 256 文字です。

アクセス ポイント グループの追加

WLAN プロファイルを AP グループに分割するテンプレートを作成または変更できます。

新しいアクセス ポイント グループを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[AP Group VLANs] をクリックするか、左側のサイドバーのメニューから [WLAN] > [AP Group VLANs] を選択します。

（注）　[AP Groups]（コントローラ リリース 5.2 以降）は、リリース 5.2 よりも前のコントローラでは [AP Group VLANs] です。

ステップ 3　[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。

ステップ 4　アクセス ポイント グループの名前およびグループの説明を入力します。

（注）　グループの説明はオプションです。

ステップ 5　WLAN プロファイルを追加する場合は、[WLAN Profiles] タブをクリックし、次のフィールドを設定します。

a. [Add] をクリックします。

（注） 使用可能なすべての WLAN プロファイル名を表示するには、テキスト ボックスから現在の WLAN プロファイル名を削除します。テキスト ボックスから現在の WLAN プロファイルの名前を削除すると、使用可能なすべての WLAN プロファイルがドロップダウン リストに表示されます。

（注） 各アクセス ポイントは 16 個の WLAN プロファイルに限定されます。各アクセス ポイントは、WLAN override 機能が有効にされない限り、すべての WLAN プロファイルをブロードキャストします。WLAN override 機能によって、アクセス ポイントごとに 16 個の任意の WLAN プロファイルを無効にできます。

（注） WLAN override 機能は、512 WLAN 機能をサポートしていない（最大 512 個の WLAN プロファイルをサポートできる）古いコントローラのみに適用されます。

b. WLAN プロファイル名を入力するか、[WLAN Profile Name] ドロップダウン リストからいずれか 1 つを選択します。

c. インターフェイス/インターフェイス グループを入力するか、[Interface/Interface Group] ドロップダウン リストからいずれか 1 つを選択します。

（注） 使用できるすべてのインターフェイスを表示するには、[Interface] テキスト ボックスから現在のインターフェイスを削除します。[Interface] テキスト ボックスから現在のインターフェイスを削除すると、使用可能なすべてのインターフェイスがドロップダウン リストに表示されます。

d. 該当する場合は、[NAC Override] チェックボックスをオンにします。NAC の上書き機能は、デフォルトでは無効です。

e. [Add/Edit] リンクをクリックして、ポリシー設定パラメータを指定します

- [Policy Name]：ポリシー名。
- [Policy Priority]：1 ～ 16 のポリシー プライオリティを設定します。2 つのポリシーが同じプライオリティを持つことはできません。

（注） WLAN あたりのポリシー マッピングは 16 だけです。そのマッピング用に選択したポリシーのテンプレートが、コントローラにポリシーがない場合に最初に適用されます。

f. アクセス ポイントおよび WLAN プロファイルを追加したら、[Save] をクリックします。

ステップ 6　RF プロファイルを追加する場合は、[RF Profiles] タブをクリックし、次のフィールドを設定します。

- [802.11a]：ドロップダウン リストから、802.11a 無線 AP の RF プロファイルを選択できます。
- [802.11b]：ドロップダウン リストから、802.11b 無線 AP の RF プロファイルを選択できます。
- RF プロファイルを追加したら、[Save] をクリックします。

（注）　[Click here] リンクをクリックして、新しい RF プロファイルを追加します。詳細については、「RF プロファイル テンプレートの設定（802.11）」（P.11-688）を参照してください。

ステップ 7　場所グループを追加する場合は、[Venue Group] タブをクリックし、次のパラメータを設定します。

- [Venue Group]：このアクセス ポイントが属する場所のカテゴリ。次のオプションを使用できます。
  - Unspecified
  - Assembly
  - Business
  - Educational
  - Factory and Industrial
  - Institutional
  - Mercantile
  - Residential
  - Storage
  - Utility and Misc
  - Vehicular
  - Outdoor
- [Venue Type]：上で選択した場所のカテゴリに応じて、[Venue Type] ドロップダウン リストに場所のタイプのオプションが表示されます。
- [Operator Class]：AP グループの運用クラス。使用可能な運用クラスは、81、83、84、112、113、115、116、117、118、119、120、121、122、123、124、125、126、127 です。
- [Venue Language]：この場所で使用される言語を定義するの ISO-639 エンコード文字列。この文字列は 3 文字の言語コードです。たとえば、英語の場合は ENG と入力します。
- [Venue Name]：この AP グループの場所の名前。この名前は、基本サービス セット（BSS）に関連付けられ、SSID で場所に関する十分な情報が得られないときに使用されます。場所の名前は最大 252 文字の英数字で、大文字と小文字を区別します。

ステップ 8　[Save] をクリックします。

アクセス ポイント グループの削除

アクセス ポイント グループを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[AP Groups] をクリックするか、左側のサイドバーのメニューから [WLAN] > [AP Groups] を選択します。

ステップ 3　[Remove] をクリックします。

ポリシー設定テンプレートの設定

[Policy Configuration Templates] ページでは、コントローラにデバイス ベースのポリシーを設定することができます。ネットワーク上のユーザまたはデバイス用のポリシーを設定できます。設定できるポリシーの最大数は 64 です。

（注）　AAA オーバーライドがコントローラに設定されている場合は、ポリシーは WLAN および AP グループに適用されません。

ポリシー設定のテンプレートを設定するには、次の手順に従ってください。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Policy Configuration] をクリックするか、左側のサイドバーのメニューから [WLANs] > [Policy Configuration] を選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。

ステップ 4　次のフィールドを設定します。

- [Policy Name]：ポリシー名。
- [Policy Role]：ユーザが属するユーザ タイプまたはユーザ グループを指定します。たとえば、学生、従業員。
- [EAP Type]：クライアントが使用する EAP 認証方式。使用できる方法は、次のとおりです。
  - LEAP
  - EAP-FAST
  - EAP-TLS
  - PEAP
- [Device Type]：デバイス タイプを選択できるドロップダウン リスト。
- [VLAN]：ポリシーに関連付けられている VLAN。
- [ACL]：ポリシーの IPv4 ACL を選択できるドロップダウン リスト。
- [QoS]：次の QoS ポリシーのうちの 1 つを選択できるドロップダウン リスト。
  - [Platinum (Voice)]：Voice over Wireless の高い QoS を保証します。
  - [Gold (Video)]：高品質のビデオ アプリケーションをサポートします。
  - [Silver (Best Effort)]：クライアントの通常の帯域幅をサポートします。
  - [Bronze (Background)]：ゲスト サービス用の最小の帯域幅を提供します。
- [Session Timeout]：クライアントが強制的に再認証されるまでの最大時間数（秒単位）。デフォルト値は 0 秒です。
- [Sleeping Client Timeout]：ゲスト クライアントが強制的に再認証されるまでの最大時間数（時間単位）。デフォルト値は 12 時間です。範囲は 1 ～ 720 時間です。

FlexConnect テンプレートの設定

ここでは、次の内容について説明します。

- 「FlexConnect AP グループ テンプレートの設定」（P.11-645）
- 「FlexConnect ユーザの設定」（P.11-648）

FlexConnect AP グループ テンプレートの設定

FlexConnect を使用すると、ブランチ オフィスまたはリモート オフィスにあるアクセス ポイントを本社のオフィスからワイドエリア ネットワーク（WAN）リンクを使用して、各オフィスでコントローラを導入せずに、設定および制御できます。ロケーションごとに展開できる FlexConnect のアクセス ポイント数は無制限ですが、ブランチ オフィスは同じ設定を共有していることが多いため、フロアごとにアクセス ポイントを組織化してグループ化し、ビルディングごとに 25 程度に制限できます。

FlexConnect AP グループを設定するには、次の手順に従います。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[FlexConnect AP Groups] をクリックするか、左側のサイドバーのメニューから [FlexConnect] > [FlexConnect AP Groups] を選択します。[FlexConnect] > [FlexConnect AP Groups] ページが表示されます。また、プライマリおよびセカンダリ RADIUS、さらに、テンプレートが適用されるコントローラおよび仮想ドメインの数（自動的に読み込まれます）が表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　[General] タブで、次のフィールドを設定します。

- [Template Name] : FlexConnect アクセス ポイント グループに割り当てるテンプレートの名前を入力します。
- [Primary RADIUS] : 各グループのプライマリ RADIUS 認証サーバを選択します。また、コントローラに存在しない FlexConnect グループ上（サイト レベルで）のローカル RADIUS サーバも設定できます。FlexConnect グループは、グループあたり最大 100 の RADIUS サーバをサポートします。
- 各グループのセカンダリ RADIUS 認証サーバを選択します。また、コントローラに存在しない FlexConnect グループ上（サイト レベルで）のローカル RADIUS サーバも設定できます。FlexConnect グループは、グループあたり最大 100 の RADIUS サーバをサポートします。

ステップ 5　[FlexConnect AP] タブで、次のフィールドを設定します。

（注）　アクセス ポイントのイーサネット MAC アドレスは、同じコントローラ上の複数の FlexConnect グループに存在できません。複数のグループが同じコントローラに適用されている場合は、[Ethernet MAC] チェックボックスをオンにして、グループの 1 つのアクセス ポイントの選択を解除します。この変更を保存するか、コントローラに適用する必要があります。

- [Add AP] : クリックして、既存の FlexConnect グループに追加の FlexConnect AP（Prime Infrastructure に存在しているもの）を追加します。[Add AP] をクリックした場合、この FlexConnect グループの一部であるアクセス ポイントのみがリストされます。

ステップ 6　[Local Authentication] タブで、次のフィールドを設定します。

（注）　[General] タブで、[Primary RADIUS Server] フィールドと [Secondary RADIUS Server] フィールドが [None] に設定されていることを確認します。

- [FlexConnect Local Authentication] : [FlexConnectLocal Authentication] チェックボックスをオンにして、この FlexConnect グループに対してローカル認証を有効にします。

  （注）　FlexConnect ユーザを作成できるのは、FlexConnect AP Group を保存した後だけです。

- [LEAP Authentication] : [LEAP Authentication] チェックボックスをオンにして、FlexConnect アクセス ポイントが LEAP を使用してクライアントを認証できるようにします。AP ローカル認証が設定されている場合にだけ LEAP 認証を設定できます。
- [EAP-FAST Authentication] : [EAP FAST Authentication] チェックボックスをオンにして、FlexConnect アクセス ポイントが EAP-FAST を使用してクライアントを認証できるようにします。AP ローカル認証が設定されている場合にだけ EAP Fast 認証を設定できます。
- [Auto Key Generation] : 自動的にサーバ キーを生成するには、[Auto key Generation] チェックボックスを選択します。

  [EAP-FAST Authentication] チェックボックスを選択した場合は、EAP-FAST キーを指定して、EAP-FAST キーを確定する必要があります。
- Protected Access Credential（PAC）をプロビジョニングする方法に応じて、次のいずれかを実行します。
  - 手動の PAC プロビジョニングを使用するには、[EAP-FAST Key] テキスト ボックスと [Confirm EAP-FAST Key] テキスト ボックスに、PAC の暗号化と暗号化解除に使用するキーを入力します。キーは 32 桁の 16 進数文字である必要があります。
  - PAC プロビジョニング中に PAC のないクライアントに自動的に PAC を送信できるようにするには、[Auto key generation] チェックボックスをオンにします。
- [EAP-FAST Key] : [EAP-FAST Key] テキスト ボックスに、EAP-FAST サーバの権限識別子を入力します。識別子は 32 桁の 16 進数文字である必要があります。
- [EAP-FAST Authority ID] : [EAP-FAST Authority ID] テキスト ボックスに EAP-FAST サーバの権限 ID をテキスト形式で入力します。32 桁までの 16 進数文字を入力できます。
- [EAP-FAST Authority Info] : [EAP-FAST Authority Info] テキスト ボックスに、EAP-FAST サーバの権限情報を入力します。
- [EAP-FAST PAC Timeout（2-4095）] : [EAP-FAST Pac Timeout] テキスト ボックスの編集ボックスに PAC が表示され続ける秒数を入力することにより、PAC タイムアウト値を指定します。有効範囲は 2 ～ 4095 秒です。
- [PEAP Authentication] : [PEAP Authentication] チェックボックスをオンにして、FlexConnect アクセス ポイントが PEAP を使用してクライアントを認証できるようにします。AP ローカル認証が設定されている場合にだけ PEAP 認証を設定できます。
- [EAP-TLS Authentication] : [EAP-TLS Authentication] チェックボックスをオンにして、FlexConnect アクセス ポイントが EAP-TLS を使用してクライアントを認証できるようにします。AP ローカル認証が設定されている場合にだけ EAP-TLS 認証を設定できます。
- [EAP-TLS Certificate Download] : EAP ルートおよびデバイス証明書をアクセス ポイントへダウンロードするには [EAP TLS Certificate Download] チェックボックスをオンにします。このオプションは、[EAP-TLS Authentication] チェックボックスをオンにした場合にだけ使用できます。

[EAP TLS Certificate Download] チェックボックスをオンにしてコントローラに適用しようとした後で、EAP 証明書がそのコントローラで使用できない場合、エラー メッセージが表示されることがあります。コントローラに証明書をダウンロードして適用しても、その状態は Prime Infrastructure には保持されません。また、この情報は FlexConnect 監査レポートに使用できません。

（注）　FlexConnect のローカル認証が有効な場合にだけ、LEAP、EAP-FAST、PEAP、または EAP-TLS 認証を設定できます。

ステップ 7　[Image Upgrade] タブで、次のフィールドを設定します。

- [FlexConnect AP Upgrade] : FlexConnect アクセス ポイントをアップグレードする場合は、このチェックボックスをオンにします。
- [Slave Maximum Retry Count] : スレーブが FlexConnect グループ内のマスターからのダウンロード開始を試行する最大回数を入力します。このオプションは、[FlexConnect AP Upgrade] チェックボックスをオンにした場合のみ使用できます。

（注）　[Image Upgrade] タブで [FlexConnect AP Upgrade] チェックボックスが有効になっている場合に限り、アクセス ポイントをマスター アクセス ポイントとして追加できます。

ステップ 8　[ACL Mapping] タブで、次のフィールドを設定します。

- [VLAN-ACL Mapping] タブをクリックして、VLAN ACL マッピングを表示、追加、編集、または削除します。
  - [Add Row] をクリックします。
  - VLAN ID を入力します。有効な VLAN ID の範囲は 1 ～ 4094 です。
  - [Ingress ACL] ドロップダウン リストから、入力 ACL を選択します。
  - [Egress AC] ドロップダウン リストから、出力 ACL を選択します。
  - [Save] をクリックします。
- [WLAN-ACL Mapping] タブをクリックして、WLAN ACL マッピングを表示、追加、編集、削除します。
  - [Add Row] をクリックします。
  - [WLAN Profile Name] ドロップダウン リストから、WLAN プロファイルを選択します。
  - [WebAuth ACL] ドロップダウン リストから、WebAuth ACL を選択します。
  - [Save] をクリックします。

（注）　最大 16 個の WebAuth ACL を追加できます。

- [Policies] タブをクリックして、WebPolicy ACL マッピングを表示、追加、編集、削除します。
  - [Add Row] をクリックします。
  - [Web-Policy ACL] ドロップダウン リストから、WebPolicy ACL を選択します。
  - [Save] をクリックします。

（注）　最大 16 個の Web-Policy ACL を追加できます。

- [Local Split] タブをクリックして、Local Split ACL マッピングを表示、追加、編集、または削除します。
  - [Add Row] をクリックします。
  - [WLAN Profile Name] ドロップダウン リストから、WLAN プロファイルを選択します。

    （注）　FlexConnect 中央スイッチング WLAN だけが [WLAN Profile Name] ドロップダウン リストに表示されます。

  - [Local-Split ACL] ドロップダウン リストから、FlexConnect ACL を選択します。
  - [Save] をクリックします。

ステップ 9　[Central DHCP] タブをクリックして、中央 DHCP の処理を表示、追加、編集、または削除します。

- [Add Row] をクリックします。
- [WLAN Profile Name] ドロップダウン リストから、WLAN プロファイルを選択します。

  （注）　FlexConnect ローカル スイッチング WLAN だけが [WLAN Profile Name] ドロップダウン リストに表示されます。

- [Central DHCP] ドロップダウン リストから、[Enable] または [Disable] を選択します。この機能を有効にすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。
- [Override DNS] ドロップダウン リストから、[Enable] または [Disable] を選択します。ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバ アドレスのオーバーライドを有効または無効にできます。中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
- [NAT-PAT] ドロップダウン リストで、[Enable] または [Disable] を選択します。ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）を有効または無効にできます。NAT および PAT をイネーブルにするには、[Central DHCP Processing] を有効にする必要があります。
- [Save] をクリックします。

ステップ 10　[WLAN-VLAN Mapping] タブで、VLAN ID を FlexConnect アクセス ポイントに割り当て、ローカルにスイッチした WLAN に対する VLAN マッピングを設定します。

- [WLAN Profile Name]：WLAN の名前。
- [VLAN ID]：ローカル スイッチングを行う際にクライアントが受信する IP アドレスを送信する VLAN の番号。

ステップ 11　[Save] をクリックします。

FlexConnect ユーザの設定

（注）　FlexConnect ユーザを作成できるのは、FlexConnect AP Group を保存した後だけです。

（注）　コントローラ リリース 5.2.x.x 以降では、最大 100 の FlexConnect ユーザがサポートされます。コントローラ リリース 5.2.0.0 以前では、20 の FlexConnect ユーザのみサポートされます。

FlexConnect ユーザを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[FlexConnect AP Groups] をクリックするか、左側のサイドバーのメニューから [FlexConnect] > [FlexConnect AP Groups] を選択します。[FlexConnect] > [FlexConnect AP Groups] ページが表示されます。

ステップ 3　[FlexConnect Configuration] タブをクリックして、FlexConnect グループのローカル認証を有効にします。

ステップ 4　この FlexConnect グループのローカル認証を有効にするには、[FlexConnect Local Authentication] チェックボックスをオンにします。

ステップ 5　[Users configured in the group] リンクをクリックします。[FlexConnect Users] ページが表示されます。

ステップ 6　新しいユーザを追加する場合は、[Select a command] ドロップダウン リストから [Add User] を選択し、[Go] をクリックします。[Add User] ページが表示されます。

ステップ 7　[User Name] テキスト ボックスに、FlexConnect ユーザ名を入力します。

ステップ 8　[Password] テキスト ボックスに、パスワードを入力します。

ステップ 9　[Confirm Password] テキスト ボックスにパスワードを再入力します。

ステップ 10　[Save] をクリックします。

（注）　FlexConnect ユーザを削除するには、[FlexConnect Users] リストからユーザを選択して、[Delete] をクリックします。

セキュリティ テンプレートの設定

ここでは、次の内容について説明します。

- 「ローカル ネットワーク ユーザ テンプレートの設定」（P.11-660）
- 「ゲスト ユーザ テンプレートの設定」（P.11-662）
- 「ユーザ ログイン ポリシー テンプレートの設定」（P.11-663）
- 「MAC フィルタ テンプレートの設定」（P.11-663）
- 「アクセス ポイント許可または MSE 許可テンプレートの設定」（P.11-664）
- 「手動による無効化クライアント テンプレートの設定」（P.11-665）
- 「クライアント除外ポリシー テンプレートの設定」（P.11-665）
- 「アクセス ポイント認証および MFP テンプレートの設定」（P.11-666）
- 「Web 認証テンプレートの設定」（P.11-667）
- 「外部 Web 認証サーバ テンプレートの設定」（P.11-670）

汎用セキュリティ コントローラ テンプレートの設定

コントローラの汎用セキュリティ情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のフィールドを設定します。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- [Maximum Local Database Entries (on next reboot)]:許可されるデータベース エントリの最大数を入力します。この数は、次回リブート時に有効になります。

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

ファイル暗号化テンプレートの設定

このページでは、ファイル暗号化テンプレートの追加、または既存のファイル暗号化テンプレートの変更が可能です。

ファイル暗号化テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[File Encryption] をクリックするか、左側のサイドバーのメニューから [Security] > [File Encryption] を選択します。[Security] > [File Encryption] ページが開きます。テンプレートが適用されるコントローラと仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[File Encryption template] ページが表示されます。

ステップ 4　ファイル暗号化を有効にする場合、[File Encryption] をオンにします。

ステップ 5　ちょうど 16 個の ASCII 文字から成る暗号キー テキスト文字列を入力します。

ステップ 6　暗号キーを再入力します。

ステップ 7　[Save] をクリックします。

RADIUS 認証テンプレートの設定

このページでは、RADIUS 認証テンプレートの追加、または既存のテンプレートの変更が可能です。これらのサーバ テンプレートを設定した後、CLI または GUI を経由してコントローラにログインしているコントローラ ユーザが認証されます。

RADIUS 認証テンプレートを設定するには、次の手順に従います。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RADIUS Auth Servers] をクリックするか、左側のサイドバーのメニューから [Security] > [RADIUS Auth Servers] を選択します。[Security] > [RADIUS Auth Servers] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。RADIUS サーバの IP アドレスとインターフェイス プロトコルのポート番号および admin ステータスも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[RADIUS Auth Servers template] ページが表示されます。

ステップ 4　[Shared Secret Format] ドロップダウン リストから、[ASCII] または [hex] を選択します。

（注）　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。

ステップ 5　指定のサーバで使用する RADIUS 共有秘密を入力します。

ステップ 6　キー ラップを有効にする場合は、チェックボックスをオンにします。このチェックボックスが有効な場合、認証要求は次の Key Encryption Key（KEK）および Message Authenticator Code Keys（MACK）が設定されている RADIUS サーバに送信されます。有効にされている場合、次のフィールドが表示されます。

- [Shared Secret Format]：ASCII または 16 進数を入力します。

（注）　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。

- [KEK Shared Secret]：KEK 共有秘密を入力します。
- [MACK Shared Secret]：MACK 共有秘密を入力します。

（注）　コントローラが共有秘密の通知を受けるたびに、既存の共有秘密は新しい共有秘密に上書きされます。

ステップ 7　管理権限を有効にする場合は、[Admin Status] チェックボックスをオンにします。

ステップ 8　RFC 3576 のサポートを有効にする場合はクリックします。RFC 3576 は、Remote Authentication Dial In User Service（RADIUS）プロトコルの拡張版です。これは、ユーザ セッションに対する動的な変更を可能とし、ユーザの接続解除やユーザ セッションに適用できる許可の変更に対するサポートを含みます。これらの許可と共に、[Disconnect] および [Change-of-Authorization]（CoA）メッセージのサポートが提供されます。[Disconnect] メッセージはユーザ セッションをただちに終了させ、CoA メッセージはデータ フィルタなどセッションの許可属性を変更します。

ステップ 9　ネットワーク ユーザ認証を有効にする場合は、[Network User] チェックボックスをオンにします。このオプションが有効な場合、このエントリがネットワーク ユーザの RADIUS 認証サーバと見なされます。

ステップ 10　管理認証を有効にする場合は、[Management User] チェックボックスをオンにします。このオプションが有効な場合、このエントリが管理ユーザの RADIUS 認証サーバと見なされます。

ステップ 11　RADIUS 認証要求がタイムアウトし、コントローラが再転送を試みるまでの時間を秒単位で指定します。2 ～ 30 秒の値を指定できます。

ステップ 12　[IPsec] チェックボックスをオンにして IP セキュリティ メカニズムを有効にすると、追加の IP セキュリティ フィールドがページに追加され、ステップ 13 からステップ 19 までの操作が必要になります。これを無効にする場合は、[Save] をクリックします。ステップ 13 ～ 19 までの操作は必要ありません。

ステップ 13　ドロップダウン リストを使用して、使用する IP セキュリティ認証プロトコルを選択します。オプションは [HMAC-SHA1]、[HMAC-MD5]、および [None] です。

秘密キーを共有する 2 者間では、やり取りされる情報を検証するために、Message Authentication Codes（MAC; メッセージ認証コード）が使用されます。HMAC（ハッシュ MAC）は、暗号ハッシュ関数に基づいたメカニズムで、反復された任意の暗号ハッシュ関数の組み合わせで使用できます。HMAC-MD5 と HMAC-SHA1 は、MD5 ハッシュ関数と SHA1 ハッシュ関数を使用した HMAC の 2 つの構造です。また、HMAC では、メッセージ認証値の計算と検証に秘密キーを使用します。

ステップ 14　使用する IP セキュリティ暗号化メカニズムを設定します。オプションは次のとおりです。

- [DES]：Data Encryption Standard（DES; データ暗号化規格）は、プライベート（秘密）キーを使用するデータ暗号化の方法です。DES では、56 ビットのキーを 64 ビットのデータ ブロックごとに適用します。
- [Triple DES]：3 つのキーを連続で適用するデータ暗号規格。

- [AES 128 CBC] : Advanced Encryption Standard（AES; 高度暗号化規格）は 128、192、または 256 ビットの長さのキーを使用して 128、192、または 256 ビットの長さのブロックを暗号化します。AES 128 CBC では、Cipher Block Chaining（CBC; 暗号ブロック連鎖）モードで 128 ビットのデータ パスを使用します。
- [None] : IP セキュリティ暗号化メカニズムはありません。

ステップ 15　インターネット キー エクスチャンジ（IKE）認証は、編集可能なテキスト ボックスではありません。Internet Key Exchange プロトコルは、セッション キー（暗号化と認証）を配信し、VPN エンドポイントにデータの保護方法に合意する方法を提供するメソッドです。IKE はセキュリティ アソシエーション（SA）のバンドルを各接続に割り当てることによって、接続を追跡します。

ステップ 16　[IKE phase 1] ドロップダウン リストを使用して [aggressive] または [main] を選択します。これによって、IKE プロトコルが設定されます。IKE phase 1 は、IKE の保護方法をネゴシエートするために使用されます。Aggressive モードは、少ないパケットでより多くの情報を渡し、若干高速の接続になる利点がありますが、セキュリティ ゲートウェイの ID を暗号化せずに転送する欠点があります。

ステップ 17　[Lifetime] フィールドでセッションが無効になるまでのタイムアウト間隔（秒単位）を設定します。

ステップ 18　IKE Diffie Hellman グループを設定します。オプションは、[group 1]（768 ビット）、[group 2]（1024 ビット）、または [group 5]（1536 ビット）です。Diffie-Hellman 技術は、対称キーを生成するために 2 つのデバイスによって使用されます。これによって、値を公に交換し、同じ対称キーを生成できます。

3 つのグループのすべてで従来の攻撃に対するセキュリティが確保されますが、キーのサイズが大きいことから、Group 5 の安全性がより高くなります。ただし、Group 1 および Group 2 のキーを使用した計算は、素数サイズがより小さいために、多少高速に実行される可能性があります。

ステップ 19　[Save] をクリックします。

RADIUS アカウンティング テンプレートの設定

このページでは、新しい RADIUS アカウンティング テンプレートの追加、または既存の RADIUS アカウンティング テンプレートの変更が可能です。

RADIUS アカウンティング テンプレートを設定するには、次の手順に従います。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RADIUS Acct Servers] をクリックするか、左側のサイドバーのメニューから [Security] > [RADIUS Acct Servers] を選択します。[Security] > [RADIUS Acct Servers] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。RADIUS サーバの IP アドレスとインターフェイス プロトコルのポート番号および admin ステータスも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[RADIUS Accounting Server template] ページが表示されます。

ステップ 4　[Shared Secret Format] ドロップダウン リストを使用し、[ASCII] または [hexadecimal] を選択します。

（注）　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定する必要があります。

ステップ 5　指定のサーバで使用する RADIUS 共有秘密を入力します。

ステップ 6　共有秘密を再入力します。

ステップ 7　サーバの管理権限を確立する場合は、[Admin Status] をオンにします。

ステップ 8　ネットワーク ユーザ認証を有効にする場合は、[Network User] チェックボックスをオンにします。このオプションが有効な場合、このエントリがネットワーク ユーザの RADIUS 認証サーバと見なされます。

ステップ 9　RADIUS 認証要求がタイムアウトし、コントローラが再転送を試みるまでの時間を秒単位で指定します。2 ～ 30 秒の値を指定できます。

ステップ 10　[Save] をクリックします。

RADIUS フォールバック テンプレートの設定

このページでは、新しい RADIUS フォールバック テンプレートの追加、または既存の RADIUS フォールバック テンプレートの変更が可能です。

RADIUS フォールバック テンプレートを設定するには、次の手順に従います。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RADIUS Fallback] をクリックするか、左側のサイドバーのメニューから [Security] > [RADIUS Fallback] を選択します。[Security] > [RADIUS Fallback] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[RADIUS Fallback template] ページが表示されます。

ステップ 4　[RADIUS Fallback Mode] ドロップダウン リストから、[Off]、[Passive] または [Active] を選択します。

- [Off]：フォールバックを無効にします。
- [Passive]：時間間隔を入力する必要があります。
- [Active]：ユーザ名および時間間隔を入力する必要があります。

ステップ 5　[Save] をクリックします。

LDAP サーバ テンプレートの設定

この項では、Lightweight Directory Access Protocol（LDAP）サーバを、RADIUS データベースやローカル ユーザ データベースに類似したバックエンド データベースとして設定する方法について説明します。LDAP バックエンド データベースを使用すると、コントローラで、特定のユーザの資格情報（ユーザ名およびパスワード）を LDAP サーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザ クレデンシャルを取得するために、バックエンド データベースとして LDAP サーバを使用する場合があります。

LDAP サーバ テンプレートを追加する、または既存の LDAP サーバ テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[LDAP Servers] をクリックするか、左側のサイドバーのメニューから [Security] > [LDAP Servers] を選択します。[Security] > [LDAP Servers] ページが表示されます。LDAP サーバの IP アドレスとインターフェイス プロトコルのポート番号も表示されます。また、値を自動的に入力するためにテンプレートが適用されるコントローラと仮想ドメインの数も表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[LDAP Server template] ページが表示されます。

ステップ 4　アクセス ポイントが接続されているコントローラのポート番号。

ステップ 5　[Bind Type] ドロップダウン リストから、[Authenticated] または [Anonymous] を選択します。[Authenticated] を選択した場合、バインド ユーザ名およびパスワードも入力する必要があります。バインドは、検索処理を実行する空きソケットです。匿名のバインド要求は拒否されます。

ステップ 6　[Server User Base DN] テキスト ボックスに、ユーザすべてのリストを含む LDAP サーバ内のサブツリーの識別名を入力します。

ステップ 7　[Server User Attribute] テキスト ボックスに LDAP サーバのユーザ名を含む属性を入力します。

ステップ 8　[Server User Type] テキスト ボックスにユーザを識別する ObjectType 属性を入力します。

ステップ 9　[Retransmit Timeout] テキスト ボックスに再転送までの時間を秒単位で入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

ステップ 10　LDAP サーバに管理権限を持たせる場合は、[Admin Status] チェックボックスをオンにします。

ステップ 11　[Save] をクリックします。

TACACS+ サーバ テンプレートの設定

このページでは、TACACS+ サーバ テンプレートの追加、または既存の TACACS+ サーバ テンプレートの変更が可能です。これらのサーバ テンプレートを設定した後、CLI または GUI を経由してコントローラにログインしているコントローラ ユーザが認証されます。

TACACS+ Server テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[TACACS+ Server] をクリックするか、左側のサイドバーのメニューから [Security] > [TACACS+ Server] を選択します。[Security] > [TACACS+ Servers] ページが開きます。TACACS+ テンプレートの IP アドレスとポート番号および admin が表示されます。また、値を自動的に入力するためにテンプレートが適用されるコントローラと仮想ドメインの数も表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[TACACS+ Servers template] ページが表示されます。

ステップ 4　チェックボックスをオンにして、1 つ以上のサーバ タイプを選択します。次のサーバ タイプが使用可能です。

- [authentication]：ユーザ認証 / 許可サーバ
- [authorization]：ユーザ許可専用サーバ
- [accounting]：RADIUS ユーザ アカウンティング サーバ

ステップ 5　サーバの IP アドレスを入力します。

ステップ 6　サーバのポート番号を入力します。デフォルトは 49 です。

ステップ 7　ドロップダウン リストから、[ASCII] または [hex] を選択します。

（注）　選択した形式に関係なく、セキュリティ上の理由で、ASCII のみが WLC（および Prime Infrastructure）に表示されます。そのため、自動プロビジョニング時にテンプレートを使用しても、別のコントローラの設定を複製できません。検出されたテンプレートが別のデバイスに適用される場合、テンプレートでもう一度キー形式を設定します。

ステップ 8　[Shared Secret] テキスト ボックスに、指定サーバにより使用される TACACS+ 共有秘密を入力します。

ステップ 9　[Confirm Shared Secret] テキスト ボックスに共有秘密をもう一度入力します。

ステップ 10　TACACS+ サーバに管理権限を持たせる場合は、[Admin Status] チェックボックスをオンにします。

ステップ 11　[Retransmit Timeout] テキスト ボックスに、TACACS+ 認証要求がタイムアウトになり、コントローラにより再送信が試行されるまでの時間を秒数で入力します。

ステップ 12　[Save] をクリックします。

ローカル EAP 汎用テンプレートの設定

このページでは、ローカル EAP のタイムアウト値を指定できます。次に、既存のローカル EAP 汎用テンプレートに変更を追加すること、またはこのテンプレートを変更することができます。

（注）　コントローラで RADIUS サーバが設定されている場合は、コントローラは最初に RADIUS サーバを使用してワイヤレス クライアントを認証しようとします。ローカル EAP は、RADIUS サーバがタイムアウトしていたり、RADIUS サーバが設定されていない場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番めの RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番めの RADIUS サーバを試行し、次に 4 番めの RADIUS サーバ、その次にローカル EAP を試行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Local EAP General] をクリックするか、左側のサイドバーのメニューから [Security] > [Local EAP General] を選択します。[Security] > [Local EAP General] ページが表示されます。テンプレートが適用されるコントローラと仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Local EAP General controller template] ページが表示されます。

ステップ 4　[Local Auth Active Timeout] テキスト ボックスに、設定された RADIUS サーバのペアが失敗した後、コントローラがローカル EAP を使用して無線クライアントを認証しようとする時間を秒単位で入力します。有効な範囲は 1 ～ 3600 秒で、デフォルト設定は 1000 秒です。

ステップ 5　EAP-FAST、手動パスワード入力、ワンタイム パスワード、または 7920/7921 電話を使用する際は、次の値を調整する必要があります。自動プロビジョニングを使用している PAC をクライアントで取得する場合、コントローラで 802.1x のタイムアウト値を大きくする必要があります（デフォルトは 2 秒）。Cisco ACS サーバでの推奨およびデフォルトのタイムアウトは 20 秒です。

（注）　複数のコントローラで次の値が同じに設定されていないと、ローミングが失敗します。

- Local EAP Identify Request Timeout =1
- Local EAP Identity Request Maximum Retries=20
- Local EAP Dynamic WEP Key Index=0
- Local EAP Request Timeout=20
- Local EAP Request Maximum Retries=2

ステップ 6　[Save] をクリックします。

ローカル EAP プロファイル テンプレートの設定

このページでは、ローカル EAP プロファイル テンプレートの追加、または既存のテンプレートの変更が可能です。ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンド システムが妨害されたり、外部認証サーバがダウンした場合

でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバへの依存が排除されます。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザの資格情報を取得して、ユーザを認証します。

（注）　LDAP バックエンド データベースは、次のローカル EAP メソッドだけをサポートします。証明書による EAP-TLS および EAP-FAST。LDAP バックエンド データベースでは、LEAP および PAC による EAP-FAST はサポートされません。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Local EAP Profiles] をクリックするか、左側のサイドバーのメニューから [Security] > [Local EAP Profiles] を選択します。[Security] > [Local EAP Profiles] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。また、EAP プロファイル名、および LEAP、EAP-FAST、TLS または PEAP が使用されているかどうかも示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Local EAP Profiles template] ページが表示されます。

ステップ 4　EAP プロファイルはそれぞれ、認証の種類にアソシエートされる必要があります。目的の認証タイプを選択します。

- [LEAP]：この認証のタイプは Cisco Key Integrity Protocol（CKIP）と MMH Message Integrity Check（MIC）を使用してデータを保護します。ユーザ名とパスワードを使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。
- [EAP-FAST]：この認証のタイプ（Flexible Authentication via Secure Tunneling）は、3 段階のトンネル認証プロセスを使用して高度な 802.1X EAP 相互認証を実行します。ユーザ名、パスワード、および PAC（保護されたアクセス クレデンシャル）を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。
- [TLS]：この認証のタイプは、クライアント アダプタおよび RADIUS サーバの動的セッション ベースの暗号鍵を使用してデータを暗号化します。認証のためには、クライアント証明書が必要です。
- [PEAP]：この認証の種類は EAP-TLS 認証に基づいていますが、認証にクライアント証明書ではなくパスワードを使用します。PEAP は、クライアント アダプタおよび RADIUS サーバの動的セッション ベースの暗号鍵を使用してデータを暗号化します。

ステップ 5　[Certificate Issuer] ドロップダウン リストを使用して、認証のための証明書を発行したのがシスコであるか他のベンダーであるかを指定します。証明書が必要なのは、EAP-FAST と TLS だけです。

ステップ 6　クライアントからの受信証明書をコントローラ上の認証局（CA）証明書に対して検証するには、[Check Against CA Certificates] チェックボックスをオンにします。

ステップ 7　受信証明書の（CN）を CA 証明書の共通名に対して検証するには、[Verify Certificate CN Identity] チェックボックスをオンにします。

ステップ 8　受信デバイス証明書が有効で期限が切れていないことをコントローラで確認するには、[Check Against Date Validity] チェックボックスをオンにします。

ステップ 9　ローカル証明書が必要な場合は、チェックボックスをオンにします。

ステップ 10　クライアント証明書が必要な場合は、チェックボックスをオンにします。

ステップ 11　[Save] をクリックします。

ステップ 12　ローカル EAP を有効にするには、次の手順を実行します。

a.　左側のサイドバーのメニューから、[WLAN] > [WLAN Configuration] の順に選択します。

b.　目的の WLAN のプロファイル名をクリックします。

c.　[Security] > [AAA Servers] タブを選択して [AAA Servers] ページにアクセスします。

d.　[Local EAP Authentication] チェックボックスをオンにして、この WLAN に対してローカル EAP を有効にします。

ステップ 13　[Save] をクリックします。

EAP-FAST テンプレートの設定

この認証のタイプ（Flexible Authentication via Secure Tunneling）は、3 段階のトンネル認証プロセスを使用して高度な 802.1X EAP 相互認証を実行します。ユーザ名、パスワード、および PAC を使用し、アクセス ポイントを介して RADIUS サーバと相互認証を行います。このページでは、EAP-FAST テンプレートの追加、または既存の EAP-FAST テンプレートの変更が可能です。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[EAP-FAST Parameters] をクリックするか、左側のサイドバーのメニューから [Security] > [EAP-FAST Parameters] を選択します。[Security] > [EAP-FAST Parameters] ページが表示されます。テンプレートが適用されるコントローラと仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[EAP-FAST Parameters template] ページが表示されます。

ステップ 4　[Time to Live for the PAC] テキスト ボックスに、PAC の有効日数を入力します。有効な範囲は 1 ～ 1000 日で、デフォルトの設定は 10 日です。

ステップ 5　[Authority ID] テキスト ボックスに、ローカル EAP-FAST サーバの認証局 ID を 16 進数文字で入力します。最大 32 文字の 16 進数文字を入力できますが、文字数は偶数である必要があります。

ステップ 6　[Authority Info] テキスト ボックスにローカル EAP-FAST サーバの認証局 ID に関する情報をテキスト形式で入力します。

ステップ 7　[Server Key] テキスト ボックスおよび [Confirm Server Key] フィールドに、PAC の暗号化と暗号化解除に使用するキー（16 進数文字）を入力します。

ステップ 8　匿名プロビジョニングを有効にするには、[Anonymous Provision] チェックボックスをオンにします。この機能を使用すると、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。この機能を無効にすると、PAC を手動でプロビジョニングする必要があります。

ステップ 9　[Save] をクリックします。

ネットワーク ユーザ優先度テンプレートの設定

LDAP とローカル データベースがユーザ クレデンシャル情報を取得するために使用する順序を指定できます。このページでは、ネットワーク ユーザ クレデンシャル取得優先度テンプレートを追加、または既存のテンプレートを変更できます。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Network Users Priority] をクリックするか、左側のサイドバー メニューから [Security] > [Network Users Priority] を選択します。[Security] > [Network User Credential Retrieval Priority] ページが表示されます。ネットワーク取得順序およびテンプレートが適用されるコントローラと仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Network Users Priority template] ページが表示されます。

ステップ 4　左右の矢印を使用して、右側のページにネットワーク ユーザ クレデンシャルを入れたり、除外したりすることができます。

ステップ 5　上下のボタンを使用してクレデンシャルを試行する順序を指定します。

ステップ 6　[Save] をクリックします。

ローカル ネットワーク ユーザ テンプレートの設定

このテンプレートでは、ローカル ネットワーク ユーザ全員のクレデンシャル（ユーザ名とパスワード）を保存できます。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザ クレデンシャルを取得するために、バックエンド データベースとしてローカル ユーザ データベースを使用する場合があります。このページでは、ローカル ネットワーク ユーザ テンプレートを追加、または既存のテンプレートを変更できます。Web 認証クライアントとしてログインする際は、ローカル ネット ユーザを作成し、パスワードを定義する必要があります。

ローカル ネットワーク ユーザ テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Local Net Users] をクリックするか、左側のサイドバーのメニューから [Security] > [Local Net Users] を選択します。[Security] > [Local Net Users] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Local Net Users template] ページが表示されます。

ステップ 4　[Import From File] を有効のままとする場合は、ファイル パスを入力するか、[Browse] をクリックしてファイル パスに移動する必要があります。次にステップ 11 に進みます。インポートを無効にする場合はステップ 5 に進みます。

（注）　インポートできるのは .csv ファイルだけです。その他のファイル形式はサポートされていません。

ファイルの最初の行はヘッダーです。Prime Infrastructure はヘッダーのデータを読み取りません。ヘッダーは空白でも入力してもかまいません。Prime Infrastructure は 2 行目以降のデータを読み取ります。

ステップ 5　ユーザ名とパスワードを入力します。すべての行でユーザ名とパスワードを入力する必要があります。

ステップ 6　プロファイルを入力します。[Profile] 列が空白（または「*Any Profile*」と表示）の場合、任意のプロファイルのクライアントがこのアカウントを使用できることを示します。

ステップ 7　プロファイルの説明を入力します。

ステップ 8　ドロップダウン リストを使用してこのローカル ユーザに適用される SSID を選択するか、[any SSID] オプションを選択します。

ステップ 9　ユーザが定義したこのインターフェイスの説明を入力します。ステップ 11 に進みます。

ステップ 10　既存のテンプレートを上書きする場合は、[Override existing templates] チェックボックスをオンにします。

ステップ 11　[Save] をクリックします。

ゲスト ユーザ テンプレート

[Configure] > [Controller Template Launch Pad] > [Security] > [Guest Users] の順に選択して、[Guest Users list] ページにアクセスします。

（注）　画面を見やすくするために、Prime Infrastructure では期限切れのテンプレートはデフォルトでは表示されません。ステータス（active、scheduled、expired、not active、または none）に基づき、どのゲスト ユーザをフィルタリングするか指定できます。[Select a Status Filter] ドロップダウン リストを使用して、フィルタ基準を決定します。

（注）　[Guest Users] テーブルの列を追加、削除、または順序変更するには、[Edit View] リンクをクリックします。

ゲスト ユーザ テンプレートの設定

このページでは、ゲスト ユーザ テンプレートの追加、または既存のゲスト ユーザ テンプレートの変更が可能です。ゲスト ユーザ アカウントの目的は、一定の時間だけ有効なユーザ アカウントを用意することです。Lobby Ambassador は、ゲスト ユーザ アカウントがアクティブとなる特定の時間フレームを設定できます。指定した時間が経過すると、ゲスト ユーザ アカウントは自動的に失効します。ゲスト アクセスの詳細は、「ゲスト ユーザ アカウントの作成」（P.7-252）を参照してください。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Guest Users] をクリックするか、左側のサイドバー メニューから [Security] > [Guest Users] を選択します。[Security] > [Guest User] ページが表示されます。

（注）　画面を見やすくするために、Prime Infrastructure では期限切れのテンプレートはデフォルトでは表示されません。ステータス（active、scheduled、expired、not active、または none）に基づき、どのゲスト ユーザをフィルタリングするか指定できます。[Select a Status Filter] ドロップダウン リストを使用して、フィルタ基準を決定します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Guest Users template] ページが表示されます。

ステップ 4　ゲスト ユーザ名を [User Name] テキスト ボックスに入力します。最大長は 24 文字です。

ステップ 5　このユーザ名のパスワードを [Password] テキスト ボックスに入力します。

ステップ 6　[Advanced] タブをクリックします。

ステップ 7　[Profile] ドロップダウン リストを使用して、接続するゲスト ユーザを選択します。

ステップ 8　ドロップダウン リストからゲスト ユーザのユーザ ロールを選択します。ユーザ ロールは、管理者により事前に定義され、ゲストのアクセス（契約者、顧客、代理店、ベンダー、ビジターなど）にアソシエートされています。

ユーザ ロールを使用して、ネットワーク内の特定のユーザに割り当てられた帯域幅の量を管理します。

ステップ 9　ゲスト ユーザ アカウントをアクティブにしておく期間を定義するには、[Lifetime] オプションで [Limited] または [Unlimited] のいずれかを選択します。

- [Limited] オプションでは、時間および分のドロップダウン リストを使用して、ゲスト ユーザ アカウントをアクティブにする期間を選択します。[Limited] のデフォルト値は、1 日（8 時間）です。
- [Unlimited] を選択した場合は、ゲスト アカウントの有効期限の日付はありません。

ステップ 10　ゲスト ユーザのトラフィックが制限される領域（屋内、屋外）、コントローラの一覧、または設定グループを [Apply to] ドロップダウン リストから選択します。

コントローラ一覧のオプションを選択すると、コントローラの IP アドレスの一覧が表示されます。

ステップ 11　（任意）必要に応じて、[General] タブでデフォルトのゲスト ユーザの説明を変更します。

ステップ 12　（任意）必要に応じて、[General] タブで [Disclaimer] のテキストを変更します。入力されたテキストをデフォルトにする場合は、[Make this Disclaimer default] チェックボックスをオンにします。

ステップ 13　[Save] をクリックします。

ユーザ ログイン ポリシー テンプレートの設定

このページでは、ユーザ ログイン テンプレートの追加、または既存のユーザ ログイン ポリシー テンプレートの変更が可能です。このテンプレートでは、各ユーザが可能な同時ログインの最大数を設定します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[User Login Policies] をクリックするか、左側のサイドバーのメニューから [Security] > [User Login Policies] を選択します。[Security] > [User Login Policies] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[User Login Policies template] ページが表示されます。

ステップ 4　ユーザ 1 人あたりの同時ログインの最大数を調整できます。

ステップ 5　このテンプレートを保存するには、[Save] をクリックします。

MAC フィルタ テンプレートの設定

このページでは、新しい MAC フィルタ テンプレートの追加、または既存の MAC フィルタ テンプレートの変更が可能です。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[MAC Filtering] をクリックするか、左側のサイドバーのメニューから [Security] > [MAC Filtering] を選択します。[Security] > [MAC Filtering] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[MAC Filtering template] ページが表示されます。

ステップ 4　[Import From File] を有効のままとする場合は、ファイル パスを入力するか、[Browse] をクリックしてファイル パスに移動する必要があります。インポート ファイルは MAC アドレス、プロファイル名、インターフェイス、および説明を示した CSV ファイルである必要があります（例：00:11:22:33:44:55,Profile1,management,test filter）。[Import from File] チェックボックスをオフにした場合は、ステップ 5 に進みます。そうでない場合は、ステップ 8 に進みます。

クライアントの MAC アドレスが表示されます。

ステップ 5　この MAC フィルタが適用されるプロファイル名を選択するか、[any Profile] オプションを選択します。

ステップ 6　ドロップダウン リストを使用して、使用可能なインターフェイス名から選択します。

ステップ 7　ユーザが定義したこのインターフェイスの説明を入力します。ステップ 9 に進みます。

ステップ 8　既存のテンプレートを上書きする場合は、[Override existing templates] チェックボックスをオンにします。

ステップ 9　[Save] をクリックします。

（注）　ブロードキャスト用の MAC アドレスを使用できません。

アクセス ポイント許可または MSE 許可テンプレートの設定

MSE 許可を追加するか、既存のアクセス ポイントまたは MSE 許可テンプレートを変更して、次の手順を実行します。

（注）　これらのテンプレートは、Cisco IOS から Lightweight アクセス ポイントに変換された Cisco 11xx/12xx シリーズのアクセス ポイント、またはブリッジ モードで接続される 1030 アクセス ポイント用に考案されています。詳細については、『*Cisco Mobility Services Engine Configuration Guide*』を参照してください。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[AP/MSE Authorization] をクリックするか、左側のサイドバーのメニューから [Security] > [AP/MSE Authorization] を選択します。[Security] > [AP/LBS Authorization Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、Base Radio MAC および認証タイプとキーも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[AP/MSE Authorization template] ページが表示されます。

ステップ 4　アクセス ポイント MAC アドレスを含むファイルをインポートする場合は、[Import From File] チェックボックスをオンにします。

（注）　インポートできるのは .csv ファイルだけです。.csv ファイル形式は GUI のフィールドに対応しており、したがってアクセス ポイントのベース無線 MAC、種類、証明書タイプ（MIC または SSC）、およびキー ハッシュが含まれます（例：00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx）。その他のファイル形式はサポートされていません。

ステップ 5　目的のファイルのパスを入力するか、[Browse] をクリックしてファイルをインポートします。

ステップ 6　[Save] をクリックします。

（注）　ブロードキャスト用の MAC アドレスを使用できません。

手動による無効化クライアント テンプレートの設定

このページでは、新しい手動による無効化クライアント テンプレートの追加、または既存の無効化クライアント テンプレートの変更が可能です。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Disable Clients] をクリックするか、左側のサイドバーのメニューから [Security] > [Disabled Clients] を選択します。[Security] > [Disabled Clients] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Manually Disabled template] ページを表示されます。

ステップ 4　無効にするクライアントの MAC アドレスを入力します。

ステップ 5　無効に設定するクライアントの説明を入力します。

ステップ 6　[Save] をクリックします。

（注）　ブロードキャスト範囲では MAC アドレスを使用できません。

クライアント除外ポリシー テンプレートの設定

クライアント除外ポリシー テンプレートを追加するか、既存のクライアント除外ポリシー テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Client Exclusion Policies] をクリックするか、左側のサイドバーのメニューから [Security] > [Client Exclusion Policies] を選択します。[Security] > [Client Exclusion Policies] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Client Exclusion Policies template] ページが表示されます。

ステップ 4　フィールドを設定して、クライアント除外ポリシー テンプレートを編集します（表 11-3 を参照）。

表 11-3　ポリシー テンプレート フィールド

フィールド	説明
Template Name	クライアント除外ポリシーの名前を入力します。
Excessive 802.11 Association Failures	過剰な 802.11 のアソシエーションの失敗によるクライアントの除外を有効にします。
Excessive 802.11 Authentication Failures	過剰な 802.11 認証の失敗によるクライアントの除外を有効にします。
Excessive 802.1X Authentication Failures	過剰な 802.1X 認証の失敗によるクライアントの除外を有効にします。
Excessive 802.11 Web Authentication Failures	過剰な 802.11 Web 認証の失敗によるクライアントの除外を有効にします。
IP Theft or Reuse	IP の盗難または再使用の症状を示すクライアントの除外を有効にします。

ステップ 5　[Save] をクリックします。

アクセス ポイント認証および MFP テンプレートの設定

管理フレーム保護（MFP）は、無線ネットワーク インフラストラクチャによる 802.11 管理フレームの認証を提供します。DoS 攻撃を引き起こし、アソシエーションおよびプローブでネットワークをフラッディングさせ、不正アクセス ポイントをさしはさみ、QoS および無線測定フレームの攻撃によりネットワーク パフォーマンスに影響を与える敵対者を検出するため、管理フレームを保護できます。

有効にすると、アクセス ポイントは Message Integrity Check Information Element（MIC IE）を各フレームに追加することにより、送信する管理フレームを保護します。フレームのコピー、変更、再送が試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。MFP フレームを送信するには、アクセス ポイントは WDS のメンバーであることが必要です。

MFP 検出が有効な場合、アクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。MIC IE が存在しており（送信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身に一致していることを確認します。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの正当な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。

アクセス ポイント認証および管理フレーム保護（MFP）テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[AP Authentication and MFP] をクリックするか、左側のサイドバーのメニューから [Security] > [AP Authentication and MFP] を選択します。[Security] > [AP Authentication Policy] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[AP Authentication and MFP template] ページが表示されます。

ステップ 4　[Protection Type] ドロップダウン リストから、次の認証ポリシーのいずれかを選択します。

- [None]：アクセス ポイント認証ポリシーなし。
- [AP Authentication]：認証ポリシーを適用します。
- [MFP]：管理フレーム保護を適用します。

アラームが生成されるしきい値は、保護の種類として AP 認証が選択されている場合にだけ表示されます。アラームを発生させるまでに無視する、未知のアクセス ポイントからのヒット数を設定します。

有効な範囲は 1 ～ 255 です。デフォルト値は 255 です。

ステップ 5　[Save] をクリックします。

Web 認証テンプレートの設定

Web 認証により、ゲストはブラウザを起動すると自動的に Web 認証ページにリダイレクトされます。ゲストは、この Web ポータルから WLAN にアクセスできます。この認証メカニズムを使用している無線 LAN 管理者は、ゲスト ユーザによるアクセスに対して、暗号化通信と非暗号化通信のどちらを設定するかを選択できます。ゲスト ユーザは、SSL で暗号化される有効なユーザ名とパスワードを使用して無線ネットワークにログインできます。Web 認証アカウントはローカルに作成するか、RADIUS サーバで管理できます。Cisco Wireless LAN Controller は Web 認証クライアントをサポートするように設定できます。このテンプレートを使用して、コントローラで提供される Web 認証ページを置き換えることができます。

Web 認証テンプレートを追加、または既存の Web 認証テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Web Auth Configuration] をクリックするか、左側のサイドバーのメニューから [Security] > [Web Auth Configuration] を選択します。[Security] > [Web Authentication] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Web Authentication template] ページが表示されます。

ステップ 4　ドロップダウン リストから適切な Web 認証のタイプを選択します。選択肢は、デフォルトの内部、カスタマイズ Web 認証、または外部です。

- デフォルトの内部を選択する場合、さらにページ タイトル、メッセージ、リダイレクト URL、およびロゴを表示するかどうかを変更できます。ステップ 5 に進みます。
- カスタマイズ Web 認証を選択する場合は、[Save] をクリックしてこのテンプレートをコントローラに適用します。Web 認証バンドルをダウンロードするプロンプトが表示されます。

（注）　カスタマイズ Web 認証を選択する前に、まず [Config] > [Controller] の順にクリックし、[Select a command] ドロップダウン リストから [Download Customized Web Authentication] を選択して [Go] をクリックすることにより、バンドルをダウンロードする必要があります。

- 外部を選択する場合は、認証に成功した後でリダイレクトする URL を入力する必要があります。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 5　会社のロゴを表示する場合は、[Logo Display] チェックボックスをオンにします。

ステップ 6　Web 認証ページに表示するタイトルを入力します。

ステップ 7　Web 認証ページに表示するメッセージを入力します。

ステップ 8　認証に成功した後でユーザがリダイレクトされる URL を指定します。たとえば、このテキスト ボックスに入力した値が http://www.example.com の場合、ユーザはこの会社のホーム ページに接続されます。

ステップ 9　[Save] をクリックします。

カスタマイズ Web 認証ページのダウンロード

カスタマイズされた Web 認証ページをコントローラにダウンロードできます。カスタマイズ Web ページでは、ユーザ Web アクセス用のユーザ名とパスワードを設定できます。

カスタマイズ Web 認証をダウンロードするときは、次のガイドラインに従う必要があります。

- ユーザ名を提供する。
- パスワードを提供する。
- リダイレクト URL は、元の URL から引用した後、非表示の入力項目として保持する。
- 操作 URL は、元の URL から引用および設定する。
- リターン ステータス コードをデコードするスクリプトを提供する。

ダウンロード前に、次の手順を実行します。

ステップ 1　サーバからサンプルの login.html バンドル ファイルをダウンロードします。この .html ファイルを 図 11-1 に示します。Web 認証がオンの場合、最初に WLAN にアクセスすると、ログイン ページが Web ユーザに表示されます。

図 11-1　Login.html

ステップ 2　Login.html を編集し、これを .tar または .zip ファイルとして保存します。

（注）　[Submit] ボタンのテキストを「Accept terms and conditions and Submit」（条件を承諾して送信）と変更できます。

ステップ 3　ダウンロードに Trivial File Transfer Protocol（TFTP）サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。ただし、管理ポートがダウンしている間、TFTP サーバを別のネットワークに配置する場合は、サービス ポートのあるサブネットにゲートウェイがあれば、スタティック ルートを追加します（config route add *IP address of TFTP server*）。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure の組み込み TFTP サーバとサードパーティの TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバを Prime Infrastructure と同じコンピュータ上で実行することはできません。

ステップ 4　.tar または .zip ファイルをコントローラにダウンロードします。

（注）　コントローラでは、Web 認証の表示に必要なページおよびイメージ ファイルを含む、1 MB までの .tar ファイルをダウンロードできます。1MB の制限には、バンドル内の圧縮されていないファイルの合計サイズが含まれます。

これでダウンロードを続行できます。

ステップ 5　ファイルを TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 6　[Configure] > [Controllers] の順に選択します。

ステップ 7　該当する IP アドレスの URL をクリックすることにより、コントローラを選択します。複数の IP アドレスを選択する場合は、カスタマイズ Web 認証ページが複数のコントローラにダウンロードされます。

ステップ 8　左側のサイドバーのメニューから、[System] > [Commands] の順に選択します。

ステップ 9　[Upload/Download Commands] ドロップダウン リストから、[Download Customized Web Auth] を選択し、[Go] をクリックします。

ステップ 10　バンドルを受信するコントローラの IP アドレスとその現在のステータスが表示されます。

ステップ 11　[File is Located On] フィールドから [local machine] を選択します。ファイル名および、サーバのルート ディレクトリに対して相対的なパスがわかる場合は、TFTP サーバを選択することもできます。

（注）　ローカル マシンのダウンロードには、.zip または .tar のファイル オプションがありますが、Prime Infrastructure では自動的に .zip を .tar に変換します。TFTP サーバのダウンロードを選択した場合は、.tar ファイルだけを指定します。

ステップ 12　[Maximum Retries] フィールドに、コントローラがファイルのダウンロードを試みる最大回数を入力します。

ステップ 13　[Timeout] フィールドに、ファイルをダウンロードする際、コントローラがタイムアウトするまでの最大時間を秒単位で入力します。

ステップ 14　ファイルは c:\tftp ディレクトリにアップロードされます。そのディレクトリ内のローカル ファイル名を指定するか、[Browse] をクリックしてナビゲートします。

ステップ 15　[OK] をクリックします。

転送がタイムアウトした場合には、[File Is Located On] フィールドの TFTP サーバ オプションを選択すると、サーバ ファイル名が読み込まれます。ローカル マシン オプションでは 2 段階の動作が起動されます。最初に、ローカル ファイルが管理者のワークステーションから Prime Infrastructure の組み込み TFTP サーバにコピーされます。次にコントローラがそのファイルを取得します。後の操作では、ファイルはすでに Prime Infrastructure サーバの TFTP ディレクトリにあるため、[download web] ページには、自動的にファイル名が入力されます。

ステップ 16　[Click here to download a sample tar file] リンクをクリックし、login.tar ファイルを開くか、保存するオプションを選択します。

ステップ 17　ダウンロードが完了すると、新しいページに接続され、認証できます。

外部 Web 認証サーバ テンプレートの設定

外部 Web 認証サーバ テンプレートを作成するか、既存の外部 Web 認証サーバ テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Templates Launch Pad] の順に選択します。

ステップ 2　[External Web Auth Server] をクリックするか、左側のサイドバーのメニューから [Security] > [External Web Auth Server] を選択します。[External Web Auth Server Controller Templates] ページに、現在保存されているすべての外部 Web 認証サーバ テンプレートが表示されます。また、各テンプレートが適用されるコントローラ数および仮想ドメイン数も表示されます。

ステップ 3　テンプレート名をクリックして、[Controller Template] リスト ページを開きます。このページで、現在のテンプレート フィールドを編集できます。

セキュリティ パスワード ポリシー テンプレートの設定

このページでは、セキュリティ パスワード ポリシーを設定できます。

パスワード ポリシー テンプレートを追加、または既存のパスワード ポリシー テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Password Policy] をクリックするか、左側のサイドバーのメニューから [Security] > [Password Policy] を選択します。[Security] > [Password Policy] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Password Policy template] ページが表示されます。

ステップ 4　テンプレート名を入力します。

ステップ 5　次の設定を有効または無効にできます。

- パスワードには、大文字、小文字、数字、特殊文字など、少なくとも 3 つのクラスの文字を含める必要があります。
- 同じ文字を 4 回以上連続して使用することはできません。
- パスワードには、cisco や admin などのデフォルトの単語は使用できません。

（注） パスワードには、「cisco」、「ocsic」、「admin」、または「nimda」は使用できません。また、これらの単語は、大文字と小文字を変えたり、「i」を「1」、「|」、「!」、「o」を「0」、または「s」を「$」に変えても使用できません。

- パスワードには、ユーザ名やユーザ名を逆にしたものを使用できません。

ステップ 6　[Save] をクリックします。

セキュリティ アクセス コントロール テンプレートの設定

ここでは、次の内容について説明します。

- 「アクセス コントロール リスト テンプレートの設定」（P.11-671）
- 「FlexConnect アクセス コントロール リスト テンプレートの設定」（P.11-674）
- 「ACL IP グループ テンプレートの設定」（P.11-676）
- 「ACL プロトコル グループ テンプレートの設定」（P.11-677）

アクセス コントロール リスト テンプレートの設定

許可されるトラフィックのタイプを、プロトコル、方向、トラフィックの送信元や宛先により設定する ACL テンプレートを作成または変更できます。

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。ACL は無線クライアントとのデータ トラフィックとコントローラの中央処理装置（CPU）へのすべてのトラフィックに適用でき、再使用可能な IP アドレス グループと再使用可能なプロトコルをサポートできるようになりました。テンプレートで ACL が設定された後、これらを管理インターフェイス、AP-manager インターフェイス、またはクライアント データ トラフィックのための任意の動的インターフェイス、コントローラ CPU へのトラフィックのためのネットワーク処理装置（NPU）インターフェイス、または WAN に適用できます。

このリリースの Prime Infrastructure は、IPv6 ACL をサポートします。

ACL テンプレートを追加、または既存の ACL テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Access Control Lists] をクリックするか、左側のサイドバーのメニューから [Security] > [Access Control] > [Access Control Lists] を選択します。[Security] > [Access Control List] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいアクセス コントロール リスト テンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。[New Controller Template] ページが表示されます。このページで、次のフィールドを指定します。

- [Access Control List Name] : テンプレートのユーザ定義名。
- [ACL Type] : [IPv4] または [IPv6] を選択します。

（注）　IPv6 ACL は、コントローラ リリース 7.2.x からサポートされます。

ステップ 4　再使用可能な IP アドレス グループとプロトコルを作成するには、左側のサイドバーのメニューから [Access Control] > [IP Groups] を選択します。

ステップ 5　IP アドレス グループがすべて一覧表示されます。IP アドレス グループ 1 つで最高 128 の IP アドレスとネットマスクの組み合わせを格納できます。新しい IP アドレス グループを定義する場合は、[Select a command] ドロップダウン リストから [Add IP Group] を選択し、[Go] をクリックします。既存の IP アドレス グループを表示または変更するには、IP アドレス グループの URL をクリックします。[IP address group] ページが開きます。

（注）　IP アドレスが「any」の場合用に、「*any*」グループが定義されています。

ステップ 6　[ACL IP Groups details] ページで、現在の IP グループ フィールドを編集できます。

- IP Group Name
- IP Address
- [Netmask OR CIDR Notation] : ネットマスクまたは CIDR 表記を入力して、[Add] をクリックします。IP アドレスまたはネットマスクのリストが、[IP Address/Netmasks] テキスト ボックスに表示されます。

  CIDR 表記を入力すると、1 つのクライアント オブジェクトを設定するだけで、サブネット範囲に存在する大量のクライアントを追加できます。

  ネットマスクを入力すると、IP アドレス プロパティの CIDR 表記ではなく、ドット区切り 10 進数表記でサブネット マスクを設定できます。

  - [Netmask] : 範囲内の IP アドレスを持つマシンだけにインターネット サービスへのアクセスを許可するために定義された IP アドレスの範囲。
  - [CIDR] : Classless InterDomain Routing（クラスレス ドメイン間ルーティング）。複数の連続するブロックでのクラス C IP アドレスの割り当てを可能にするプロトコル。
- BroadCast/Network

- [List of IP Addresses/Netmasks] : [Move Up] および [Move Down] ボタンを使用して、リスト項目の順序を変更します。[Delete] ボタンを使用すると、IP アドレスまたはネットマスクを削除できます。

ステップ 7　標準の事前に定義されたものでない追加プロトコルを定義するには、左側のサイドバーのメニューから [Access Control] > [Protocol Groups] を選択します。プロトコル グループとその送信元ポートおよび宛先ポートと DSCP の一覧が表示されます。

ステップ 8　新しいプロトコル グループを作成する場合は、[Select a command] ドロップダウン リストから [Add Protocol Group] を選択し、[Go] をクリックします。既存のプロトコル グループを表示または変更するには、グループの URL をクリックします。[Protocol Groups] ページが表示されます。

ステップ 9　既存のルールの場合はルール名が表示され、新しいルールの場合は名前を入力できます。ルールを定義するために ACL は必要ありません。パケットがルールのすべてのパラメータに一致すると、このルールに対する動作が実行されます。

ステップ 10　ドロップダウン リストからプロトコルを選択します。

- [Any] : すべてのプロトコル
- [TCP] : トランスミッション コントロール プロトコル
- [UDP] : ユーザ データグラム プロトコル
- [ICMP] : インターネット制御メッセージ プロトコル
- [ESP] : IP カプセル化セキュリティ ペイロード
- [AH] : 認証ヘッダー
- [GRE] : Generic Routing Encapsulation
- [IP] : インターネット プロトコル
- [Eth Over IP] : Ethernet over Internet Protocol
- [Other Port OSPF] : Open Shortest Path First
- [Other] : その他の任意の IANA プロトコル（http://www.iana.org/）

ステップ 11　一部のプロトコル（TCP または UDP など）を選択すると、追加の送信元ポートおよび宛先ポート GUI エレメントが表示されます。

- [Source Port] : この ACL が適用されるパケットの送信元を指定します。[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を選択できます。
- [Dest Port] : この ACL が適用されるパケットの宛先を指定します。[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を選択できます。

ステップ 12　[DSCP (Differentiated Services Code Point)] ドロップダウン リストから、[any] または [specific] を選択します。[specific] を選択した、DSCP（0 ～ 255）を入力します。

（注）　DSCP は、インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コードです。

ステップ 13　[Save] をクリックします。

ステップ 14　ここで、定義済みの IP アドレス グループとプロトコル グループから新しいマッピングを作成できます。新しいマッピングを定義するには、新しいグループをマップする ACL テンプレートを選択します。すべての ACL マッピングがページの最上部に表示され、すべての ACL ルールが下部に表示されます。

ステップ 15　新しいマッピングを定義するには、[Select a command] ドロップダウン リストから [Add Rule Mappings] を選択します。[Add Rule Mapping] ページが表示されます。

ステップ 16　次のフィールドを設定します。

- [Source IP Group]：IPv4 および IPv6 の事前定義グループ。
- [Destination IP Group]：IPv4 および IPv6 の事前定義グループ。
- [Protocol Group]：ACL で使用するプロトコル グループ。
- [Direction]：[Any]、[Inbound (from client)]、または [Outbound (to client)]。
- [Action]：[Deny] または [Permit]。デフォルトのフィルタでは、ルールで明示的に許可されていない限り、すべてのアクセスを拒否します。

ステップ 17　[Add] をクリックします。新しいマッピングによって下部のテーブルにデータが表示されます。

ステップ 18　[Save] をクリックします。

ステップ 19　ここで、作成したルール マッピングから自動的にルールを生成できます。ルールを生成するマッピングを選択して、[Generate] をクリックします。これによって、ルールが自動的に作成されます。これらのルールは、連続した順序で生成されます。つまり、ルール 29 を追加するときにすでにルール 1 ～ 4 が定義されている場合、このルールはルール 5 となります。

既存の ACL テンプレートは新しい ACL テンプレートに複製されます。この複製は、ソース ACL テンプレートで定義した ACL ルールとマッピングをすべてコピーします。

FlexConnect アクセス コントロール リスト テンプレートの設定

許可されるトラフィックのタイプを、プロトコル、トラフィックの送信元や宛先により設定する FlexConnect ACL ACL テンプレートを作成または変更できます。

（注）　FlexConnect ACL は、IPv6 アドレスをサポートしません。

ここでは、次の内容について説明します。

- 「FlexConnect アクセス コントロール リストの設定および適用」（P.11-674）
- 「FlexConnect アクセス コントロール リストの削除」（P.11-675）

FlexConnect アクセス コントロール リストの設定および適用

アクセス コントロール リスト テンプレートを設定およびコントローラに適用するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバー メニューから、[Security] > [Access Control] > [FlexConnect ACLs] を選択します。

ステップ 4　[Select a command] ドロップダウン リストから、[Add a Template] を選択します。

ステップ 5　[Go] をクリックします。

[New Controller Template] ページが表示されます。

ステップ 6　新しい FlexConnect ACL の名前を [FlexConnect ACL Name] テキスト ボックスに入力します。

ステップ 7　[Save] をクリックします。

FlexConnect ACL テンプレートが作成されます。ここで、定義済みの IP アドレス グループとプロトコル グループから新しいマッピングを作成できます。新しいマッピングを定義するには、新しいグループをマップする ACL テンプレートを選択します。すべての FlexConnect ACL マッピングがページ上部に表示され、すべての FlexConnect ACL ルールがページ下部に表示されます。

ステップ 8　[Select a command] ドロップダウン リストから、[Add Rule Mappings] を選択し、[Go] をクリックします。

ステップ 9　[FlexConnect ACL IP Protocol Map] ページが表示されます。

ステップ 10　次のフィールドを設定します。

- [Source IP Group] : IPv4 および IPv6 の事前定義グループ。
- [Destination IP Group] : IPv4 および IPv6 の事前定義グループ。
- [Protocol Group] : ACL で使用するプロトコル グループ。
- [Action] : [Deny] または [Permit]。デフォルトのフィルタでは、ルールで明示的に許可されていない限り、すべてのアクセスを拒否します。

ステップ 11　[Add] をクリックします。新しいマッピングによって下部のテーブルにデータが表示されます。

ステップ 12　[Save] をクリックします。

ステップ 13　ここで、作成したルール マッピングから自動的にルールを生成できます。ルールを生成するマッピングを選択して、[Generate] をクリックします。これによって、ルールが自動的に作成されます。これらのルールは、連続した順序で生成されます。つまり、ルール 29 を追加するときにすでにルール 1 ～ 4 が定義されている場合、このルールはルール 5 となります。

既存の FlexConnect ACL テンプレートは新しい FlexConnect ACL テンプレートに複製されます。この複製は、ソース FlexConnect ACL テンプレートで定義した FlexConnect ACL ルールとマッピングをすべてコピーします。

ステップ 14　[FlexConnect ACL] ページの [Select a command] ドロップダウン リストから、[Apply Templates] を選択します。

[Apply to Controllers] ページが表示されます。

ステップ 15　[Save Config to Flash after apply] チェックボックスをオンにして、FlexConnect ACL をコントローラに適用した後で設定をフラッシュに保存します。

ステップ 16　[Reboot Controller after apply] チェックボックスをオンにして、FlexConnect ACL が適用された後でコントローラをリブートします。このチェックボックスを使用できるのは、[Save Config to Flash after apply] チェックボックスをオンにしている場合だけです。

ステップ 17　1 つ以上のコントローラを選択し、[OK] をクリックして、FlexConnect ACL テンプレートを適用します。

作成された FlexConnect ACL は、[Configure] > [Controller Template Launch Pad] > [IP Address] > [Security] > [Access Control] > [FlexConnect ACLs] に表示されます。

FlexConnect アクセス コントロール リストの削除

FlexConnect ACL を削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Controllers] を選択します。

ステップ 2　コントローラの IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、[Security] > [FlexConnect ACLs] の順に選択します。

ステップ 4　[FlexConnect ACLs] ページから、削除する FlexConnect ACL を 1 つ以上選択します。

ステップ 5　[Select a command] ドロップダウン リストから [Delete FlexConnect ACLs] を選択します。

ステップ 6　[Go] をクリックします。

ACL IP グループ テンプレートの設定

再使用可能な IP アドレス グループを作成するには、次の手順に従います。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　左側のサイドバー メニューから、[Security] > [Access Control] > [IP Groups] の順に選択します。

ステップ 3　IPv4 および IPv6 グループを含む IP アドレス グループがすべて一覧表示されます。IP アドレス グループ 1 つで最高 128 の IP アドレスとネットマスクの組み合わせを格納できます。新しい IP アドレス グループを定義する場合は、[Select a command] ドロップダウン リストから [Add IP Group] または [Add IPv6 Group] を選択し、[Go] をクリックします。

（注）　IP アドレスが「any」の場合用に、「*any*」グループが定義されています。

（注）　any の IPv6 アドレス場合、*any* グループは、IP アドレス タイプが IPv6 で事前に定義されます。

ステップ 4　次のフィールドを設定します。

- IP Group Name
- [IP Address] : [IP Group] に IPv4 アドレス形式を入力します。IPv6 グループの場合、IPv6 アドレス形式を入力します。
- [Netmask OR CIDR Notation] : ネットマスクまたは CIDR 表記を入力して、[Add] をクリックします。IP アドレスまたはネットマスクのリストが、[IP Addresses/Netmasks] テキスト ボックスに表示されます。

  （注）　これらのフィールドは、IPv6 グループでは使用できません。

  CIDR 表記を入力すると、1 つのクライアント オブジェクトを設定するだけで、サブネット範囲に存在する大量のクライアントを追加できます。

  ネットマスクを入力すると、IP アドレス プロパティの CIDR 表記ではなく、ドット区切り 10 進数表記でサブネット マスクを設定できます。

  - [Netmask] : 範囲内の IP アドレスを持つマシンだけにインターネット サービスへのアクセスを許可するために定義された IP アドレスの範囲。
  - [CIDR] : Classless InterDomain Routing（クラスレス ドメイン間ルーティング）。複数の連続するブロックでのクラス C IP アドレスの割り当てを可能にするプロトコル。

- BroadCast/Network

（注）　これらのフィールドは、IPv6 グループでは使用できません。

- [Prefix Length]：IPv6 アドレスのプレフィックス（0 ～ 128）。
- [List of IP Addresses/Netmasks]：[Move Up] および [Move Down] ボタンを使用して、リスト項目の順序を変更します。[Delete] ボタンを使用すると、IP アドレスまたはネットマスクを削除できます。

ステップ 5　[Save] をクリックします。保存されると、IP グループは、[Template List] ページに表示されます。

ここで、定義済みの IP アドレス グループとプロトコル グループから新しいマッピングを作成できます。新しいマッピングを定義するには、新しいグループをマップする ACL テンプレートを選択します。ACL マッピングがすべてページの最上部に表示され、ACL ルールがすべて下部に表示されます。詳細については、「アクセス コントロール リスト テンプレートの設定」（P.11-671）を参照してください。

プロトコル グループの定義については、「ACL プロトコル グループ テンプレートの設定」（P.11-677）を参照してください。

ACL プロトコル グループ テンプレートの設定

標準の事前定義プロトコルではない別のプロトコルを定義するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　左側のサイドバー メニューから、[Access Control] > [Protocol Groups] の順に選択します。

ステップ 3　次のフィールドを設定します。

- [Rule Name]：既存のルールの場合はルール名が表示され、新しいルールの場合は名前を入力できます。ルールを定義するために ACL は必要ありません。パケットがルールのすべてのフィールドに一致すると、このルールに対する動作が実行されます。

（注）　ACL の詳細については、「アクセス コントロール リスト テンプレートの設定」（P.11-671）を参照してください。

- [Protocol]：ドロップダウン リストからプロトコルを選択します。
  - [Any]：すべてのプロトコル
  - [TCP]：トランスミッション コントロール プロトコル
  - [UDP]：ユーザ データグラム プロトコル
  - [ICMP]：インターネット制御メッセージ プロトコル
  - [ESP]：IP カプセル化セキュリティ ペイロード
  - [AH]：認証ヘッダー
  - [GRE]：Generic Routing Encapsulation
  - [IP]：インターネット プロトコル
  - [Eth Over IP]：Ethernet over Internet Protocol
  - [Other Port OSPF]：Open Shortest Path First

  - [Other]：その他の任意の IANA プロトコル（http://www.iana.org/）
- [Source Port]：[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を選択できます。
- [Dest Port]：宛先ポート。[TCP] または [UDP] が選択されている場合、[Any]、[HTTP]、[HTTPS]、[Telnet]、[RADIUS]、[DHCP Server]、[DHCP Client]、[DNS]、[L2TP]、[PPTP control]、[FTP control]、[SMTP]、[SNMP]、[LDAP]、[Kerberos]、[NetBIOS NS]、[NetBIOS DS]、[NetBIOS SS]、[MS Dir Server]、[Other]、[Port Range] を選択できます。
- [DSCP (Differentiated Services Code Point)]：ドロップダウン リストから [Any] または [Specific] を選択します。[Specific] を選択した、DSCP（0 ～ 255）を入力します。

（注）　DSCP は、インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コードです。

ステップ 4　[Save] をクリックします。保存されると、IP グループは [Template List] ページに表示されます。

ここで、定義済みの IP アドレス グループとプロトコル グループから新しいマッピングを作成できます。新しいマッピングを定義するには、新しいグループをマップする ACL テンプレートを選択します。ACL マッピングがすべてページの最上部に表示され、ACL ルールがすべて下部に表示されます。詳細については、「アクセス コントロール リスト テンプレートの設定」（P.11-671）を参照してください。

IP グループの定義については、「ACL IP グループ テンプレートの設定」（P.11-676）を参照してください。

セキュリティ CPU アクセス コントロール リスト テンプレートの設定

（注）　IPv6 での CPU ACL 設定は、このリリースではサポートされません。これは、仮想インターフェイスを除き、インターフェイスのコントローラのすべての IP アドレスが IPv4 を使用するためです。

CPU アクセス コントロール リスト（ACL）テンプレートの設定

「アクセス コントロール リスト テンプレートの設定」（P.11-671）で確立された既存の ACL は、中央処理装置（CPU）とネットワーク処理装置（NPU）間のトラフィック制御を設定するために使用されます。

CPU ACL テンプレートを追加、または既存の CPU ACL テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[CPU Access Control Lists] をクリックするか、左側のサイドバーのメニューから [Security] > [CPU Access Control] > [CPU Access Control Lists] を選択します。[Security] > [CPU Access Control List] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[CPU Access Control List template] ページが表示されます。

ステップ 4　チェックボックスをオンにして CPU ACL を有効にすると、さらに 2 つのフィールドが表示されます。CPU ACL が有効になり、コントローラに適用されると、Prime Infrastructure はそのコントローラに対する CPU ACL の詳細を表示します。

ステップ 5　[ACL Name] ドロップダウン リストの定義済みの名前のリストから名前を選択します。

ステップ 6　[CPU ACL Mode] ドロップダウン リストでこの CPU ACL リストが制御するデータ トラフィック方向を選択します。選択肢は、データ トラフィックの有線サイド、データ トラフィックの無線サイド、または有線と無線の両方です。

ステップ 7　[Save] をクリックします。

セキュリティ不正テンプレートの設定

ここでは、次の内容について説明します。

- 「不正ポリシー テンプレートの設定」（P.11-679）
- 「不正 AP ルール テンプレートの設定」（P.11-680）
- 「不正 AP ルール グループ テンプレートの設定」（P.11-682）
- 「危険性のないアクセス ポイント テンプレートの設定」（P.11-683）

不正ポリシー テンプレートの設定

このページでは、コントローラに適用される（アクセス ポイントとクライアントに対する）不正ポリシーを設定できます。

テンプレートを追加、または既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Rogue Policies] をクリックするか、左側のサイドバーのメニューから [Security] > [Rogue] > [Rogue Policies] を選択します。[Security] > [Rogue Policy Setup] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Rogue Policies template] ページが表示されます。

ステップ 4　Rogue Location Discovery Protocol（RLDP）が企業の有線ネットワークに接続しているかどうかを判断します。ドロップダウン リストから、次のいずれかのオプションを選択します。

- [Disable]：すべてのアクセス ポイント上で RLDP を無効にします。
- [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。
- [Monitor Mode APs]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。

（注）　RLDP が有効の場合、コントローラは管理対象のアクセス ポイントに対して、不正アクセス ポイントをアソシエートし、特殊なパケットをコントローラへ送信するよう指示します。コントローラがこのパケットを受信すると、不正アクセス ポイントが企業ネットワークに接続されます。この方法は、暗号化を有効にしていない不正アクセス ポイントに対して機能します。

ステップ 5　不正アクセス ポイント エントリの失効タイムアウトを秒単位で設定します。

ステップ 6　[Rogue Detection Report Interval] テキスト ボックスに、AP が不正検出レポートをコントローラに送信するまでの時間間隔を秒数で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。この機能は、モニタ モードの AP のみに適用されます。

ステップ 7　[Rogue Detection Minimum RSSI] テキスト ボックスに、AP により検出され、不正エントリがコントローラに作成する RSSI の最小値を入力します。有効な範囲は -70 ～ -128 dBm で、デフォルト値は -128 dBm です。この機能は、すべての AP モードに適用できます。

（注）　非常に RSSI 値が低く、不正解析にとって有益な情報とならない不正が多く存在する可能性があります。そのため、このオプションを使用して AP が不正を検出する最小 RSSI 値を指定することで、不正をフィルタできます。

ステップ 8　[Rogue Detection Transient Interval] テキスト ボックスに、不正が AP により最初にスキャンされてから、必ずスキャンされる時間間隔を入力します。一時的な間隔を入力することで、AP が不正をスキャンする間隔を制御できます。AP は、一時的な間隔の値に基づいて、不正をフィルタできます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。この機能は、モニタ モードの AP のみに適用されます。

ステップ 9　[Validate rogue clients against AAA] チェックボックスをオンにして、不正クライアントの AAA 検証を有効にします。

ステップ 10　[Detect and report Adhoc networks] チェックボックスをオンにして、アドホック ネットワーキングに参加している不正クライアントの検出とレポートを有効にします。

ステップ 11　[Save] をクリックします。

不正 AP ルール テンプレートの設定

不正アクセス ポイントのルールを使用すると、不正アクセス ポイントを自動的に分類するルールを定義できます。Prime Infrastructure では、不正アクセス ポイントの分類ルールをコントローラに適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

（注）　不正アクセス ポイントのルールは、誤アラームを減らすのにも役立ちます。

現在の分類ルール テンプレート、ルール タイプおよびこれらが適用されるコントローラの数を表示するには、[Configure] > [Controller Template Launch Pad] > [Security] > [Rogue] > [Rogue AP Rules] を選択します。不正アクセス ポイントのルールを表示する方法については、「不正アクセス ポイント分類ルールの表示または編集」（P.9-500）を参照してください。

（注）　不正クラスには以下の種類があります。
Malicious Rogue：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。
Friendly Rogue：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
Unclassified Rogue：検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

不正アクセス ポイントの新しい分類ルール テンプレートを追加または作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　左側のサイドバーのメニューから、[Security] > [Rogue] > [Rogue AP Rules] の順に選択します。[Rogue AP Rules Controller template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Classification Rule] を選択し、[Go] をクリックします。[Rogue AP Rules] > [New Template] ページが表示されます。既存の不正アクセス ポイント ルール テンプレートを変更するか、現在のテンプレートをコントローラに適用するには、[Configure] > [Controller Template Launch Pad] > [Security] > [Rogue] > [Rogue AP Rules] を選択して、テンプレート名をクリックします。

ステップ 4　[General] グループ ボックスで、次のフィールドを設定します。

- [Rule Name]：テキスト ボックスにルールの名前を入力します。
- [Rule Type]：ドロップダウン リストから [Malicious] または [Friendly] を選択します。検出されたアクセス ポイントがユーザ定義の Malicious ルールと合致した場合、または危険性のない AP カテゴリから手動で移動された場合には、悪意のある不正と見なされます。不正が既知、認知済み、または信頼されたアクセス ポイントである場合、または検出されたアクセス ポイントがユーザ定義の Friendly ルールと一致している場合、危険性がない不正と見なされます。
- [Match Type]：ドロップダウン リストから [Match All Conditions] または [Match Any Condition] を選択します。

ステップ 5　ページの [Malicious Rogue Classification Rule] グループ ボックスで、次のフィールドを設定します。

- [Open Authentication]：オープン認証を有効にするには、このチェックボックスをオンにします。
- [Match Managed AP SSID]：管理対象 AP の SSID との一致を有効にするには、このチェックボックスをオンにします。

（注）　管理対象 SSID は、WLAN に対して設定された SSID で、システムが既知のものです。

- [Match User Configured SSID]：ユーザが設定した SSID との一致を有効にするには、このチェックボックスをオンにします。

（注）　ユーザが設定した SSID は、手動で追加された SSID です。[Match User Configured SSID] テキスト ボックスに、ユーザ設定の SSID を（1 行に 1 つずつ）入力します。

- [Minimum RSSI]：最小 RSSI しきい値制限を有効にするには、このチェックボックスをオンにします。

（注）　テキスト ボックスに RSSI しきい値の最小レベル（dB 単位）を入力します。検出されたアクセス ポイントがここで指定した RSSI しきい値を超えていると、そのアクセス ポイントは悪意のあるものとして分類されます。

- [Time Duration]：時間制限を有効にするには、このチェックボックスをオンにします。

（注）　テキスト ボックスに制限時間（秒単位）を入力します。検出されたアクセス ポイントが指定した制限時間よりも長く表示されているとき、そのアクセス ポイントは悪意のあるものとして分類されます。

- [Minimum Number Rogue Clients]：悪意のあるクライアントの最小数の制限を有効にするには、このチェックボックスをオンにします。悪意のあるクライアントを許可する最小数を入力します。検出されたアクセス ポイントにアソシエートされたクライアントの数が指定した値以上になると、そのアクセス ポイントは悪意のあるものとして分類されます。

ステップ 6　[Save] をクリックします。

不正 AP ルール グループ テンプレートの設定

不正アクセス ポイント ルール グループ テンプレートを使用すると、複数の不正アクセス ポイント ルールをコントローラに統合できます。

現在の不正アクセス ポイント ルール グループ テンプレートを表示するか、新しいルール グループを作成するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Rogue AP Rule Groups] をクリックするか、左側のサイドバーのメニューから [Security] > [Rogue] > [Rogue AP Rule Groups] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Rogue Rule Group] をクリックします。

ステップ 4　[Go] をクリックします。[Rogue AP Rule Groups] > [New Template] ページが表示されます。

（注）　既存の不正ポリシー テンプレートを変更するか、現在のテンプレートをコントローラに適用するには、[Configure] > [Controller Template Launch Pad] > [Security] > [Rogue] > [Rogue AP Rule Groups] を選択して、テンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5　ページの [General] グループ ボックスにルール グループの名前を入力します。

ステップ 6　Rogue AP ルールを追加するには、左の列のルールをクリックして強調表示します。[Add] をクリックして、強調表示したルールを右側の列に移動します。

（注）　不正アクセス ポイント ルールは、[Rogue Access Point Rules] セクションから追加できます。詳細については、「不正 AP ルール テンプレートの設定」（P.11-680）を参照してください。

ステップ 7　不正アクセス ポイント ルールを削除するには、右の列のルールをクリックして強調表示します。[Remove] をクリックして、強調表示したルールを左側の列に移動します。

ステップ 8　[Move Up]/[Move Down] ボタンをクリックして、ルールが適用される順序を指定します。任意のルールを強調表示し、[Move Up] または [Move Down] をクリックして、現在のリストで上下に移動させます。

ステップ 9　不正アクセス ポイント ルール リストを保存するには、[Save] をクリックします。

ステップ 10　現在のリストに変更を加えずにページを終了するには [Cancel] をクリックします。

（注）　コントローラに適用されたルールを表示または編集するには、[Configure] > [Controller] を選択してコントローラ名をクリックします。

危険性のないアクセス ポイント テンプレートの設定

このテンプレートを使用すると、危険性のない内部アクセス ポイントをインポートできます。危険性のないアクセス ポイントをインポートすると、非 Lightweight アクセス ポイントが不正アクセス ポイントとして識別されるのを防ぐことができます。

（注）　*危険性のない内部*アクセス ポイントは、以前は*既知の AP* と呼ばれていました。

（注）　[Friendly AP] ページでは、アクセス ポイントの MAC アドレス、ステータス、コメント、このアクセス ポイントに対するアラームの抑制有無が確認できます。

危険性のないアクセス ポイントの現在のリストを表示または編集するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Friendly AP] をクリックするか、左側のサイドバーのメニューから [Security] > [Rogue] > [Friendly AP] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから [Add Friendly] を選択します。

ステップ 4　[Go] をクリックします。[Friendly AP] ページが表示されます。

（注）　既存の危険性のないアクセス ポイントを変更するには、[Configure] > [Controller Template Launch Pad] > [Security] > [Rogue] > [Friendly Internal] を選択して、アクセス ポイントの MAC アドレスをクリックします。アクセス ポイントに必要な変更を加えて、[Save] をクリックします。

ステップ 5　危険性のないアクセス ポイントは、アクセス ポイントをインポートするか、アクセス ポイント情報を手動で入力することにより追加できます。

- インポート機能を使用してアクセス ポイントをインポートするには、次の手順を実行します。
  - [Import from File] チェックボックスをオンにします。
  - ファイルのパスを入力するか、[Browse] をクリックしてインポートするファイルを選択します。

（注）　MAC アドレスを区切るには改行してください。たとえば、次のように、MAC アドレスを入力します。
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46

- アクセス ポイントを手動で追加するには、次の手順を実行します。
  - [Import from File] チェックボックスをオフにします。
  - アクセス ポイントの MAC アドレスを入力します。
  - [Status] ドロップダウン リストから [Internal] アクセス ポイントを選択します。
  - このアクセス ポイントに関するコメントを必要に応じて入力します。
  - [Suppress Alarms] チェックボックスをオンにして、このアクセス ポイントのすべてのアラームを抑制します。
- このアクセス ポイントを保存するには [Save]、アクセス ポイントをリストに追加しないでページを終了するには [Cancel] をクリックします。

無視される不正 AP テンプレートの設定

[Ignored Rogue AP Template] ページでは、無視されるアクセス ポイントをインポートするテンプレートを作成または変更できます。[Ignored AP] リストのアクセス ポイントは、不正アクセス ポイントと識別されません。

（注）　無視される不正 AP テンプレートは、コントローラに適用されません。コントローラが不正 AP を Prime Infrastructure に報告するときに、無視される不正 AP テンプレートに不正 MAC アドレスがあり、この MAC アドレスがコントローラの不正 AP 無視リストに追加される場合、不正 AP/アドホック アラームが抑制されます。

無視される不正アクセス ポイントを追加または編集するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Ignored Rogue AP] をクリックするか、左側のサイドバーのメニューから [Security] > [Rogue] > [Ignored Rogue AP] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Ignored Rogue AP] を選択します。

ステップ 4　[Go] をクリックします。[Ignored Rogue AP] ページが表示されます。

ステップ 5　無視される不正アクセス ポイントは、アクセス ポイントをインポートするか、アクセス ポイント情報を手動で入力することにより追加できます。

- インポート機能を使用して無視される不正アクセス ポイントをインポートする手順は、次のとおりです。
  - [Import from File] チェックボックスをオンにします。
  - ファイルのパスを入力するか、[Browse] ボタンを使用してインポートするファイルを選択します。インポート ファイルは、MAC アドレスを含む（1 行に MAC アドレス 1 つ）CSV ファイルにする必要があります。

  （注）　たとえば、次のように、MAC アドレスを入力します。
  00:00:11:22:33:44
  00:00:11:22:33:45
  00:00:11:22:33:46

- 無視される不正アクセス ポイントを手動で追加するには、次の手順を実行します。
  - [Import from File] チェックボックスをオフにします。
  - 不正アクセス ポイントの MAC アドレスおよびコメントを入力します。
- このアクセス ポイントを保存するには [Save]、無視される不正アクセス ポイントをリストに追加しないでページを終了するには [Cancel] をクリックします。

（注）　既存の危険性のないアクセス ポイントを変更するには、[Configure] > [Controller Template Launch Pad] > [Security] > [Rogue] > [Ignored Rogue AP] を選択して、無視される不正アクセス ポイントの MAC アドレスをクリックします。必要な変更を行って、[Save] をクリックします。

（注）　MAC アドレスを [Ignored AP] リストから削除すると、MAC アドレスは、コントローラの不正 AP 無視リストから削除されます。

802.11 テンプレートの設定

ここでは、次の内容について説明します。

ロード バランシング テンプレートの設定

ロード バランシング テンプレートを設定するには、次の手順に従ってください。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Load Balancing] をクリックするか、左側のサイドバーのメニューから [802.11] > [Load Balancing] を選択します。[Load Balancing] ページが表示されます。

ステップ 3　クライアントのウィンドウ サイズとして 1 ～ 20 までの値を入力します。このページ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ページ + 最も負荷が低い AP 上のクライアント アソシエーション数 = ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアントのページ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこのしきい値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数がしきい値を下回るアクセス ポイントだけとなります。

ステップ 4　拒否の最大数として 0 ～ 10 までの値を入力します。拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

ステップ 5　[Save] をクリックします。

帯域選択テンプレートの設定

帯域選択テンプレートを設定するには、次の手順に従ってください。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Band Select] をクリックするか、左側のサイドバーのメニューから [802.11] > [Band Select] を選択します。[Band Select] ページが表示されます。

ステップ 3　プローブ サイクル回数として 1 ～ 10 までの値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。

ステップ 4　スキャン サイクル期間のしきい値として 1 ～ 1000 ミリ秒までの値を入力します。この設定は、クライアントからの新しいプローブ要求が新しいスキャン サイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は 200 ミリ秒です。

ステップ 5　[age out suppression] フィールドに 10 ～ 200 秒までの値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 6　[age out dual band] フィールドに 10 ～ 300 秒までの値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンド クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 60 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 7　[acceptable client RSSI] フィールドに –20 ～ –90 dBm までの値を入力します。このフィールドは、クライアントがプローブに応答するための最大 RSSI を設定します。デフォルト値は -80 dBm です。

ステップ 8　[Save] をクリックします。

優先コール テンプレートの設定

このページでは、優先コールを設定するテンプレートを作成または変更できます。

優先コール テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Preferred Call] をクリックするか、左側のサイドバーのメニューから [802.11] > [Preferred Call] を選択します。[Preferred Call Controller Templates] ページが表示されます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[New Controller Template] ページが表示されます。

ステップ 4　次の優先コール パラメータを設定します。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- [Number Id]：優先番号を識別する値を入力します。優先コール番号は最大 6 つまで入力できます。有効な範囲は 1 ～ 6 です。デフォルト値は、1 です
- [Preferred Number]：優先コール番号を入力します。

ステップ 5　[Save] をクリックします。

コントローラ テンプレートのメディア ストリームの設定（802.11）

802.11 無線のコントローラ テンプレートのメディア ストリームを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[802.11] グループ ボックスで、[Media Stream] の横の [New] をクリックします。[New Controller Template] ページが表示されます。

ステップ 3　[General] グループ ボックスで、テンプレートに適切な名前を指定します。

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

ステップ 4　[Media Stream Configuration] グループ ボックスで、次のフィールドを指定します。

- Media Stream Name
- [Multicast Destination Start IP]：マルチキャストするメディア ストリームの開始 IP アドレス。
- [Multicast Destination End IP]：マルチキャストするメディア ストリームの終了 IP アドレス。

（注）　開始 IP および終了 IP は、コントローラ リリース 7.2.x より、IPv4 または IPv6 マルチキャスト アドレスにすることができます。

- [Maximum Expected Bandwidth]：メディア ストリームが使用できる最大帯域幅。

ステップ 5　[Resource Reservation Control (RRC) Parameters] グループ ボックスで、次のフィールドを指定します。

- [Average Packet Size]：メディア ストリームが使用できる平均パケット サイズ。
- [RRC Periodical Update]：定期的に更新されるリソース予約コントロールの計算。無効にすると、RRC の計算は、クライアントがメディア ストリームに加入したときに、1 回のみ行われます。
- [RRC Priority]：最高が 1、最低が 8 の RRC の優先度。
- [Traffic Profile Violation]：ストリームが QoS ビデオ プロファイルに違反したときに、ストリームがドロップされるか、ベスト エフォート キューに入れられる場合に表示されます。
- [Policy]：メディア ストリームが許可されるか拒否される場合に表示されます。

ステップ 6　[Save] をクリックします。

保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

RF プロファイル テンプレートの設定（802.11）

[RF Profiles] ページでは、AP グループに関連付けられる RF プロファイルを作成または変更できます。

802.11 無線のコントローラ テンプレートの RF プロファイルを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RF Profiles] をクリックするか、左側のサイドバー メニューから [802.11] > [RF Profiles] を選択します。[RF Profiles] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 4　[Go] をクリックします。[New Controller Template] ページが表示されます。

ステップ 5　次の情報を設定します。

- General
  - [Template Name]：テンプレートのユーザ定義の名前。
  - [Profile Name]：現在のプロファイルのユーザ定義の名前。
  - [Description]：テンプレートの説明。
  - [Radio Type]：アクセス ポイントの無線タイプ。これは、802.11a または 802.11b 無線がある AP の RF プロファイルを選択できるドロップダウン リストです。
- TPC（送信電力制御）
  - [Minimum Power Level Assignment (-10 to 30 dBm)]：割り当てられている最小電力を示します。範囲は -10 ～ 30 dBm で、デフォルトは -10 dBm です。
  - [Maximum Power Level Assignment (-10 to 30 dBm)]：割り当てられている最大電力を示します。範囲は -10 ～ 30 dBm で、デフォルトは 30 dBm です。

- [Power Threshold v1(-80 to -50 dBm)]：送信電力しきい値を示します。
- [Power Threshold v2(-80 to -50 dBm)]：送信電力しきい値を示します。

- データ レート：アクセス ポイントとクライアント間でデータを送信できるレートを指定するには、[Data Rates] ドロップダウン リストを使用します。次のデータ レートが使用可能です。
  - [802.11a]：6、9、12、18、24、36、48、および 54 Mbps。
  - [802.11b/g]：1、2、5.5、6、9、11、12、18、24、36、48、または 54Mbps

  各データ レートに対して、次のオプションのいずれかを選択します。
  - [Mandatory]：このコントローラ上のアクセス ポイントに関連付けるには、クライアントがこのデータ レートをサポートしている必要があります。
  - [Supported]：関連付けられたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信できます。ただし、クライアントがこのレートを使用できなくても、関連付けは可能です。
  - [Disabled]：通信に使用するデータ レートは、クライアントが指定します。
- [Band Select]：帯域選択機能により、混雑した講堂または競技場内の数百のクライアントに AP がサービスする場合に、クライアントへの無線サービスの分配のバランスを取ることができます。帯域選択により、クライアント機能が検出され、2.4 GHz と 5GHz の両方の周波数帯にクライアントを関連付けることができるかどうかが確認されます。WLAN で帯域選択を有効にすると、AP は 2.4GHz でのプローブ抑制の実行を強制され、最終的にデュアル バンド クライアントは 5Ghz 周波数帯に移行します。[Band Select] グループ ボックスで、以下を指定します。
  - Probe Response
  - Cycle Count(1 to 10 Cycles)
  - Cycle Threshold(1 to 1000 msecs)
  - Suppression Expire(10 to 200 secs)
  - Dual Band Expire(10 to 300 secs)
  - Client RSSI(-90 to -20 dBm)
- High Density Configurations
  - [Maximum Clients]：クライアントの最大数を指定します。
- Multicast Configurations
  - [Multicast Data Rate]：[Multicast Data Rate] ドロップダウン リストから、データ レートを選択します。値「auto」は、AP が自動的にクライアントのデータ レートを調整することを示します。
- Coverage Hole Detection
  - [Data RSSI(-90 to -60 dBm)]：アクセス ポイントが受信するデータ パケットの最小受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホール（またはカバレッジが不完全な領域）を特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータ キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は –90 ～ –60 dBm で、デフォルト値は –80 dBm です。アクセス ポイントでは、データ RSSI が 5 秒おきに測定され、それらが 90 秒間隔でコントローラにレポートされます。
  - [Voice RSSI(-90 to -60 dBm)]：アクセス ポイントが受信する音声パケットの最小受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホールを特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットが音声キューに受信される場合、潜在的なカバレッジ ホールが検出されて

います。有効な値の範囲は –90 ～ –60dBm で、デフォルト値は –75dBm です。アクセス ポイントでは、音声 RSSI が 5 秒おきに測定され、それらが 90 秒間隔でコントローラにレポートされます。

- [Coverage Exception(1 to 75 Clients)] : データ以下の RSSI 値または音声 RSSI しきい値を使用するアクセス ポイントのクライアントの最小数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 3 です。
- [Coverage Level(0 to 100 %)] : [Coverage Exception Level per AP] テキスト ボックスに、信号レベルが低い一方で、他のアクセス ポイントにローミングできないアクセス ポイントのクライアントの割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

- Load Balancing
  - [Window(0 to 20 Clients)] : 1 ～ 20 までの値を入力します。このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。
  - [Denial(1 to 10)] : 0 ～ 10 までの値を入力します。拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

ステップ 6　[Save] をクリックします。

SIP スヌーピングの設定

SIP スヌーピングを使用する際は、次のガイドラインを考慮します。

- SIP は、Cisco 5500 シリーズ コントローラ、1240、1130、および 11n アクセス ポイント上でのみ使用できます。
- SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話に対してのみ使用してください。
- SIP CAC は、SIP スヌーピングが有効になっている場合にのみサポートされます。

コントローラの SIP スヌーピングを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[SIP Snooping] をクリックするか、左側のサイドバーのメニューから [802.11] > [SIP Snooping] の順に選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 4　[Go] をクリックします。[New Controller Template] ページが表示されます。

ステップ 5　次のフィールドを設定します。

- Port Start
- Port End

ステップ 6　[Save] をクリックします。

（注）　単一ポートを使用する場合は、開始ポートおよび終了ポートのフィールドを同じ番号で設定します。

無線テンプレートの設定（802.11a/n）

ここでは、次の内容について説明します。

802.11a/n パラメータ テンプレートの設定

無線テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Parameters] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [Parameters] を選択します。[802.11a/n Parameters template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、802.11 ネットワーク ステータスと、チャネルおよび電源モードが表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n Parameters template] ページが表示されます。

ステップ 4　802.11a/n ネットワーク ステータスを有効にする場合は、チェックボックスをオンにします。

ステップ 5　[ClientLink] ドロップダウン リストを使用して、ClientLink をサポートするすべてのアクセス ポイント 802.11a/n 無線で ClientLink を有効にします。それ以外の場合、[Disable] を選択します。

ステップ 6　送信電力しきい値を -50 ～ -80 の間で入力します。

ステップ 7　ビーコンの間隔をキロマイクロ秒単位で入力します。有効範囲は 20 ～ 1000 ミリ秒です。

ステップ 8　配送数テキスト ボックスが 0 のトラフィック インジケータ メッセージ（TIM）要素を含むビーコン フレームの送信間に経過した、ビーコン間隔を入力します。この値は、ビーコン フレームの DTIM 間隔フィールドで送信されます。DTIM を追加したビーコンをクライアント デバイスが受信すると、通常は、保留中のパケットをチェックするためにクライアント デバイスが再起動します。DTIM の間隔が長くなると、クライアントのスリープ時間が長くなり、電力を節約できます。反対に、DTIM の間隔が短くなるとパケットの受信の遅延を抑えられますが、クライアントが頻繁に起動するためバッテリ残量が消費されます。

ステップ 9　[Fragmentation Threshold] フィールドで、パケットを断片化する（1 ブロックではなく、いくつかの断片として送信する）サイズを指定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。

ステップ 10　802.11e の最大帯域幅のパーセンテージを入力します。

ステップ 11　短いプリアンブルを有効にする場合は、チェックボックスをオンにします。

ステップ 12　[Dynamic Assignment] ドロップダウン リストから、次の 3 つのモードのいずれかを選択します。

- [Automatic]：送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。
- [On Demand]：送信電力は、[Assign Now] ボタンを選択したときに更新されます。
- [Disabled]：動的な送信電力割り当ては行われず、値はグローバル デフォルトに設定されます。

ステップ 13　[Dynamic Tx Power Control] を有効にするかどうかを決定します。電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。

ステップ 14　[Assignment Mode] ドロップダウン リストには 3 つの動的チャネル モードがあります。

- [Automatic]：この動作を許可するすべてのアクセス ポイントに対し、チャネル割り当てが定期的に更新されます。これはデフォルトのモードです。
- [On Demand]：チャネル割り当ては、必要に応じて更新されます。
- [OFF]：動的チャネル割り当ては発生せず、値はグローバル デフォルトに設定されます。

ステップ 15　外部 AP 干渉の回避を有効にするには、[Avoid Foreign AP Interference] チェックボックスをオンにします。このフィールドを有効にすると、RRM がチャネルを割り当てる際に、外部 Cisco アクセス ポイント（RF/モビリティ ドメイン外の Cisco 以外のアクセス ポイント）からの干渉が考慮されます。[Radio Resource Management (RRM)] フィールドは、外部 802.11 干渉をモニタします。RRM でこの干渉を無視するには、このチェックボックスをオフにします。

外部アクセス ポイントからの干渉エネルギー（dB）および負荷（使用率）が著しい特定の状況では、RRM は、この外部アクセス ポイントの近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するために、チャネル割り当てを調整することがあります。これにより、Cisco WLAN ソリューション のキャパシティが増加し、変動性が減少します。

ステップ 16　AP 負荷の回避を有効にするには、[Avoid シスコ AP Load] チェックボックスをオンにします。この RRM 帯域幅認識フィールドを有効にすると、コントローラがチャネルをアクセス ポイントに割り当てる際に、各アクセス ポイントで使用されるトラフィック帯域幅が考慮されます。RRM でこの値を無視するには、このチェックボックスをオフにします。

特定の状況でより高密度に展開されている場合、完全なチャネルの再使用を適切に作成するには、チャネルが十分に存在しないことがあります。このような状況で、RRM は、より大きなトラフィック負荷を伝送するアクセス ポイントに、より良い再使用パターンを割り当てることができます。

ステップ 17　これを有効にするには、[Avoid non 802.11 Noise] チェックボックスをオンにします。この RRM ノイズ モニタリング フィールドを有効にすると、電子レンジや Bluetooth デバイスなど、アクセス ポイントでないソースからの干渉のあるチャネルが回避されます。RRM でこの干渉を無視するには、このチェックボックスをオフにします。

非 802.11 ノイズ源からの干渉エネルギー（dB）が著しい特定の状況では、このノイズ源の近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するため、RRM がチャネル割り当てを調整することがあります。これにより、Cisco WLAN ソリューション のキャパシティが増加し、変動性が減少します。

ステップ 18　[Signal Strength Contribution] チェックボックスは常にオンです（設定不可）。RRM は常に、RF/モビリティ ドメイン内のすべてのアクセス ポイントの相対位置をモニタし、最適に近いチャネルの再使用を保証します。その結果、Cisco WLAN ソリューション キャパシティについては増加、チャネル相互および隣接チャネルの干渉については減少となります。

ステップ 19　クライアントおよびコントローラは、データ レートをネゴシエートします。データ レートが [Mandatory] に設定されている場合、クライアントはネットワークを使用するには、そのデータ レートをサポートしている必要があります。データ レートがコントローラにより [Supported] として設定されている場合、同じレートをサポートする、アソシエートされているクライアントは、そのレートを使用してアクセス ポイントと通信する可能性があります。しかし、アソシエートするために、サポートさ

れるすべてのレートをクライアントが使用する必要はありません。それぞれのレートについて、[Mandatory] または [Supported] のドロップダウン リストが使用可能です。各データ レートは、[Disabled] に設定し、クライアントの設定に合わせることもできます。

ステップ 20　[Noise/Interference/Rogue Monitoring Channels] セクションの [Channel List] ドロップダウン リストから、必要なモニタリング レベルに基づいて、すべてのチャネル、各国のチャネル、または DCA チャネルから選択します。DCA により、コントローラに接続された管理対象デバイスの中から妥当なチャネルの割り当てが自動的に選択されます。

ステップ 21　Cisco Compatible Extension の位置測定間隔を変更できるのは、測定モードで無線測定要求をブロードキャストできる場合だけです。有効な場合、これによってクライアントの位置の正確さが向上します。

ステップ 22　[Save] をクリックします。

メディア パラメータ コントローラ テンプレートの設定（802.11a/n）

このページでは、コール アドミッション制御およびトラフィック ストリーム メトリックなど、802.11a/n 音声フィールドを設定するテンプレートを作成または変更できます。

コントローラの 802.11a/n 音声フィールド情報（コール アドミッション制御およびトラフィック ストリーム メトリック）を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　テンプレートに適切な名前を指定します。

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

ステップ 4　[Voice] タブで、次のフィールドを設定します。

- [Admission Control (ACM)] : アドミッション制御を有効にするには、このチェックボックスを選択します。

  VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、コール アドミッション制御（CAC）が必要です。アクセス ポイントでの CAC により、アクセス ポイントは、ネットワークの輻輳時でも QoS が制御された状態を維持し、許容する最大の通話数を許容できる数に保つことができます。

- [CAC Method] : [Admission Control (ACM)] が有効になっている場合、CAC 方式を負荷ベースまたはスタティックに指定します。

  負荷ベースの CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

- [Maximum Bandwidth Allowed] : 許容される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。コントローラのバージョンが 6.0.188.0 以前の場合、有効な範囲は 40 ～ 85 です。コントローラのバージョンが 6.0.188.1 以降の場合、有効な範囲は 5 ～ 85 で、デフォルトは 75 です。

- [Reserved Roaming Bandwidth] : 予約済みのローミング帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 で、デフォルトは 6 です。

- [Expedited Bandwidth]：緊急コール用に CAC の拡張として緊急帯域幅を有効にするには、このチェックボックスを選択します。

  より高い優先度が TSPEC 要求に与えられるように、CCXv5 準拠の優先帯域幅の IE が必要となります。
- [SIP CAC]：SIP CAC を有効にするには、このチェックボックスを選択します。

  SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話のみに使用する必要があります。
- [SIP Codec]：この無線で使用するコーデック名を指定します。使用可能なオプションは、[G.711]、[G.729]、および [User Defined] です。
- [SIP Call Bandwidth]：ネットワークで SIP コールごとに割り当てる帯域幅（キロビット / 秒単位）を指定します。このフィールドは、選択されている [SIP Codec] が [User Defined] である場合のみ設定できます。
- [SIP Sample Interval]：コーデックを動作させる必要があるサンプルの間隔（ミリ秒）を指定します。
- [Max Number of Calls per Radio]：無線ごとのコールの最大数を指定します。
- [Metric Collection]：メトリック収集を有効にするには、このチェックボックスを選択します。

  トラフィック ストリーム メトリックは、ワイヤレス LAN での VoIP に関する一連の統計情報で、ワイヤレス LAN の QoS を通知します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは、関連付けられたすべてのアクセス ポイントから、90 秒ごとに 802.11b/g インターフェイスに関する統計情報データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にする必要があります。

ステップ 5　[Video] タブで、次のフィールドを設定します。

- [Admission Control (ACM)]：アドミッション制御を有効にするには、このチェックボックスを選択します。
- [Maximum Bandwidth]：許可される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。コントローラ バージョン 6.0.188.0 以前の場合、有効な範囲は 0 ～ 100 です。コントローラ バージョン 6.0.188.1 以降の場合、有効な範囲は 5 ～ 85 です。
- [Reserved Roaming Bandwidth]：予約済みのローミング帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 です。
- [Static CAC method] : [SIP Codec] ドロップダウン リストから、次のいずれかのオプションを選択して CAC 方式を設定します。デフォルト値は [G.711] です。オプションは次のとおりです。
  - Load-Based
  - Static

  （注）　スタティック CAC 方式は無線ベースで、負荷ベースの CAC 方式はチャネル ベースです
- [SIP CAC]：スタティック CAC のサポートを有効にするには、[SIP CAC] チェックボックスを選択します。デフォルトでは、このチェックボックスはディセーブルになっています。

  （注）　SIP CAC は、SIP スヌーピングが有効になっている場合にのみサポートされます。

- [Unicast Video Redirect]：ビデオ キュー内のすべての非メディア ストリーム パケットがベスト エフォート キューにリダイレクトされるようにするには、[Unicast Video Redirect] チェックボックスを選択します。無効にすると、ビデオ マーキングのあるパケットはすべてのビデオ キューに保持されます。
- [Client Minimum Phy Rate]：クライアントがメディア ストリームに加入するために必要な物理データ レートを [Client Minimum Phy Rate] ドロップダウン リストから指定します。
- [Multicast Direct Enable]：この無線でどの WLAN でも Media Direct を有効にするには、[Multicast Direct Enable] チェックボックスを選択します。
- [Maximum Number of Streams per Radio]：許可される無線ごとのストリームの最大数を指定します。
- [Maximum Number of Streams per Client]：許可されるクライアントごとのストリーム最大数を指定します。
- [Best Effort QOS Admission]：新しいクライアント要求をベスト エフォート キューにリダイレクトするには、[Best Effort QOS Admission] チェックボックスを選択します。これは、すべてのビデオ帯域幅が使用されている場合のみ発生します。

（注） 無効になっており、最大のビデオ帯域幅が使用されている場合、新しいクライアント要求は拒否されます。

ステップ 6　[General] タブで、次のフィールドを指定します。

- [Maximum Media Bandwidth (0 to 85%)]：許可される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。

ステップ 7　[Save] をクリックします。

保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

コントローラ テンプレートによる EDCA パラメータの設定（802.11a/n）

Enhanced Distributed Channel Access（EDCA）パラメータは、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。

コントローラ テンプレートを介して 802.11a/n EDCA パラメータを追加または設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[EDCA Parameters] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [EDCA Parameters] を選択します。[EDCA Parameters template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、EDCP プロファイルおよび低遅延 MAC が表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n EDCA Parameters template] ページが表示されます。

ステップ 4　[EDCA Profile] ドロップダウン リストで、次のいずれかのオプションを選択します。

- [WMM] : Wi-Fi Multimedia（WMM）のデフォルト パラメータを有効にします。768 ビットは、デフォルト値です。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
- [Spectralink Voice Priority] : Spectralink 音声優先パラメータを有効にします。通話の質を向上するため、ネットワークに Spectralink 電話技術を実装している場合に、このオプションを選択します。
- [Voice Optimized] : 音声用に最適化された EDCA プロファイル パラメータを有効にします。Spectralink 以外の音声サービスをネットワーク上で展開している場合に、このオプションを選択します。
- [Voice & Video Optimized] : 音声とビデオ用に最適化された EDCA プロファイル パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。

（注）　ビデオ サービスは、Admission Control（ACM; アドミッション制御）とともに展開する必要があります。ACM なしのビデオ サービスはサポートされていません。

（注）　無線インターフェイスをシャットダウンしてから、EDCA パラメータを設定してください。

ステップ 5　この機能を有効にするには、[Low Latency MAC] チェックボックスをオンにします。

（注）　ネットワーク上のすべてのクライアントが WMM 準拠の場合にだけ、低遅延 MAC を有効にしてください。

ローミング パラメータ テンプレートの設定（802.11a/n）

ローミング パラメータ テンプレートを追加、または既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Roaming Parameters] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [Roaming Parameters] を選択します。[Roaming Parameters template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページでは、最小 RSSI、ローミング ヒステリシス、適応可能なスキャンのしきい値および移行時間も表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n Roaming Parameters template] ページが表示されます。

ステップ 4　[Mode] ドロップダウン リストを使用して、[Default values] および [Custom values] のいずれかのコンフィギュレーション モードを選択します。[Default values] オプションを選択すると、ローミング パラメータは変更不可能になり、テキスト ボックスにデフォルト値が表示されます。[Custom values] オプションを選択すると、テキスト ボックスでローミング パラメータを編集できます。パラメータを編集するには、ステップ 5 に進みます。

ステップ 5　[Minimum RSSI] フィールドには、クライアントがアクセス ポイントにアソシエートするときに必要な受信信号強度インジケータ（RSSI）の最小値を入力します。クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。

範囲：-80 ～ -90 dBm

デフォルト：-85 dBm

ステップ 6　[Roaming Hysteresis] フィールドに、クライアントがローミングするために必要なネイバー アクセス ポイントの信号強度を示す値を入力します。このフィールドは、クライアントが物理的に 2 つのアクセス ポイントの境界上やその近くにある場合に、アクセス ポイント間のピンポンの量を減らすためのものです。

範囲：2 ～ 4 dB

デフォルト：2 dB

ステップ 7　[Adaptive Scan Threshold] フィールドに、クライアントのアソシエートされたアクセス ポイントの RSSI 値を入力します。これ以下の場合、クライアントは指定された移行時間内にネイバー アクセス ポイントにローミングできる必要があります。このフィールドはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。

範囲：-70 ～ -77 dB

デフォルト：-72 dB

ステップ 8　[Transition Time] フィールドには、クライアントがアソシエートしているアクセス ポイントからの RSSI がスキャンしきい値を下回ったときに、適切なネイバー アクセス ポイントを検出してローミングを完了するまでの最大許容時間を入力します。

[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

範囲：1 ～ 10 秒

デフォルト：5 秒

ステップ 9　[Save] をクリックします。

802.11h テンプレートの設定

802.11h では、チャネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。802.11h パラメータ（電力制限およびチャネル コントローラ通知）を設定するテンプレートを作成または変更し、これらの設定を複数のコントローラに適用します。

802.11h テンプレートを追加、または既存の 802.11h テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[802.11h] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [802.11h] を選択します。[802.11h Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページでは、ローカル電力制約およびチャネル通知のクワイエット モードも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11h template] ページが表示されます。

ステップ 4　アクセス ポイントによる現在のチャネルでの転送を停止する場合、[Power Constraint] チェックボックスをオンにします。

ステップ 5　[Channel Announcement] チェックボックスを選択してチャネル通知を有効にします。チャネル通知は、新しいチャネルや新しいチャネル番号に切り替わった場合に、アクセス ポイントが通知するメソッドです。

ステップ 6　[Save] をクリックします。

ハイ スループット テンプレートの設定（802.11a/n）

802.11a/n ハイ スループット テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[High Throughput (802.11n)] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [High Throughput] を選択します。[802.11n Parameters for 2.4 GHz Template] または [802.11n Parameters for 5 GHz Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページでは、802.11n ネットワーク ステータスが表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n High Throughput template] ページが表示されます。

ステップ 4　高いスループットを可能にするには、[802.11n Network Status Enabled] チェックボックスを選択します。

ステップ 5　802.11ac 無線で高スループットを可能にするには、[802.11ac Network Status Enabled] チェックボックスを選択します。

ステップ 6　[MCS (Data Rate) Settings] 列で、サポートするデータ レートのレベルを選択します。Modulation Coding Schemes（MCS; 変調符号化方式）は 802.11a データ レートと類似しています。デフォルトでは、20MHz のショート ガード インターバルが使用されます。

（注）　[Supported] チェックボックスを選択すると、選択した数値が [Selected MCS Indexes] ページに表示されます。

ステップ 7　[Save] をクリックします。

CleanAir コントローラ テンプレートの設定（802.11a/n）

802.11a/n 無線の CleanAir パラメータを設定するテンプレートを作成または変更します。テンプレートを設定して、コントローラの CleanAir、レポーティングおよびアラームを有効または無効にできます。また、レポートおよびアラームに含める干渉デバイスのタイプを設定できます。

コントローラの 802.11a/n CleanAir 情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　左側のサイドバーのメニューから、[802.11a/n] > [CleanAir] の順に選択します。[802.11a/n CleanAir Controller Templates] ページに、現在保存されているすべての 802.11a/n CleanAir テンプレートが表示されます。また、各テンプレートが適用されるコントローラおよび仮想ドメインの数も表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add a Template] を選択し、[Go] をクリックします。

[New Controller Template] ページが表示されます。

ステップ 4　次のフィールドを設定します。

- [Template Name] : テンプレート名を入力します。
- [CleanAir] : チェックボックスをオンにして、802.11 b/g/n ネットワークで CleanAir を有効にします。または、オフにして、コントローラによるスペクトラム干渉の検出を停止します。

（注）　[CleanAir] を有効にした場合、[Reporting Configuration] および [Alarm Configuration] グループ ボックスが表示されます。

- [Reporting Configuration]：このグループ ボックスのフィールドを使用して、レポートに含める干渉デバイスを設定します。

  [Report Interferers]：[report interferers] チェックボックスをオンにして、CleanAir システムによる干渉源のレポートおよび検出を有効にします。または、オフにして、コントローラによる干渉デバイスのレポートを停止します。デフォルト値はオンです。

  CleanAir システムに検出およびレポートされる必要のある干渉源が [Interferences to Detect] ボックスに表示され、検出される必要のない干渉源が [Interferers to Ignore] ボックスに表示されていることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が無視されます。

- [Alarm Configuration]：このグループ ボックスでは、電波品質アラームの生成を設定できます。
  - [Air Quality Alarm]：[Air Quality Alarm] チェックボックスを選択して電波品質アラームの生成を有効にするか、このチェックボックスを選択解除してこの機能を無効にします。
  - [Air Quality Alarm Threshold]：[Air Quality Alarm] チェックボックスを選択した場合は、[Air Quality Alarm Threshold] フィールドに 1 ～ 100 までの値を入力して、電波品質アラームが生成されるしきい値を指定します。電波品質がしきい値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は、1 です
  - [Interferers For Security Alarm]：[Interferers For Security Alarm] チェックボックスを選択して、コントローラが指定されたデバイス タイプを検出したときに干渉アラームを生成するか、選択解除してこの機能を無効にします。デフォルト値はオフです。
  - 干渉デバイス アラームを生成する必要のある干渉源が [Interferers Selected for Security Alarms] ボックスに表示され、干渉デバイス アラームを生成する必要のない干渉源が [Interferers Ignored for Security Alarms] ボックスに表示されていることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、セキュリティ アラームに対してすべての干渉源が無視されます。

ステップ 5　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの設定」（P.11-604）を参照してください。

802.11a/n RRM テンプレートの設定

ここでは、次の内容について説明します。

RRM しきい値テンプレートの設定（802.11a/n）

802.11a/n または 802.11b/g/n RRM しきい値テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RRM Thresholds] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [RRM Thresholds] を選択します。[802.11a/n RRM Thresholds Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、ノイズしきい値、最大クライアント数および RF 使用率も表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n RRM Threshold template] ページが表示されます。

ステップ 4　現在コントローラにアソシエートされている故障したクライアントの最小数を入力します。

ステップ 5　カバレッジしきい値の対象範囲を入力します。

ステップ 6　[Data RSSI]（–60 ～ –90 dBm）を入力します。この数値は、クライアントがアクセス ポイントにアソシエートするために必要なデータの最小受信信号強度インジケータ（RSSI）の値を示します。

（注）　これらの RRM しきい値フィールドを適用する前に、802.11a/n ネットワークを無効にする必要があります。

ステップ 7　[Voice RSSI]（–60 ～ –90 dBM）を入力します。この数値は、クライアントがアクセス ポイントにアソシエートするために必要な音声の最小受信信号強度インジケータ（RSSI）の値を示します。

ステップ 8　現在コントローラにアソシエートされている故障したクライアントの最大数を入力します。

ステップ 9　[RF Utilization] テキスト ボックスに、802.11a/n のしきい値の割合を入力します。

ステップ 10　干渉しきい値の割合を入力します。

ステップ 11　ノイズしきい値を -127 ～ 0dBm の範囲で入力します。このしきい値を超えると、コントローラは Prime Infrastructure にアラームを送信します。

ステップ 12　カバレッジ例外レベルの割合を入力します。最小クライアント数に設定されたカバレッジから、この割合分減少した場合、カバレッジ ホールが生成されます。

ステップ 13　[Save] をクリックします。

RRM 間隔テンプレートの設定（802.11a/n）

802.11a/n RRM 間隔テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RRM Intervals] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [RRM Intervals] を選択します。[802.11a/n or 802.11b/g/n RRM Threshold Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、ネイバー パケット頻度、ノイズ測定間隔および負荷測定間隔も表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n or 802.11b/g/n RRM Intervals template] ページが表示されます。

ステップ 4　[Neighbor Packet Frequency] テキスト ボックスに、各アクセス ポイントで信号強度が測定される間隔を入力します。デフォルトは 300 秒です。

ステップ 5　各アクセス ポイントに対してノイズおよび干渉測定を行う間隔を入力します。デフォルトは 300 秒です。

ステップ 6　各アクセス ポイントに対して負荷測定を行う間隔を入力します。デフォルトは 300 秒です。

ステップ 7　[Coverage Measurement Interval] フィールドに、各アクセス ポイントで行うカバレッジ測定の間隔を入力します。デフォルトは 300 秒です。

ステップ 8　[Save] をクリックします。

RRM ダイナミック チャネル割り当てテンプレートの設定（802.11a/n）

[Radio Resource Management (RRM) Dynamic Channel Assignment (DCA)] ページを使用して、このコントローラのチャネル幅のほか、DCA チャネルを選択できます。

RRM DCA は、5 GHz 帯域で 802.11n 40 MHz チャネルをサポートします。より高い帯域幅を使用すると、瞬間的データ レートが高くなります。

（注）　大きい帯域幅を選択すると、オーバーラッピングしないチャネルが減少するため、展開によっては全体のネットワーク スループットが低下することがあります。

802.11 a/n RRM DCA テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[DCA] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [DCA] を選択します。[802.11a/n DCS Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n TPC template] ページが表示されます。

ステップ 4　次のフィールドを設定します。

- [Template Name] : テンプレート名を入力します。

- [Assignment Mode]：[Dynamic Assignment] ドロップダウン リストから、次の 3 つのモードのいずれかを選択します。
  - [Automatic]：送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。
  - [On Demand]：送信電力は、[Assign Now] をクリックすると更新されます。
  - [Disabled]：動的な送信電力割り当ては行われず、値はグローバル デフォルトに設定されます。
- 有効にするには、[Avoid Foreign AP Interference] チェックボックスをオンにします。このチェックボックスを有効にすると、RRM がチャネルを割り当てる際に、外部 Cisco アクセス ポイント（RF/ モビリティ ドメイン外の Cisco 以外のアクセス ポイント）からの干渉が考慮されます。この外部 802.11 は干渉しています。RRM でこの干渉を無視するには、このチェックボックスをオフにします。

  外部アクセス ポイントからの干渉エネルギー（dB）および負荷（使用率）が著しい特定の状況では、RRM は、この外部アクセス ポイントの近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するために、チャネル割り当てを調整することがあります。これによって、キャパシティが増加し、Cisco WLAN ソリューションの変動性が減少します。
- AP 負荷の回避を有効にするには、[Avoid Cisco AP Load] チェックボックスをオンにします。この帯域幅認識フィールドを有効にすると、コントローラがチャネルをアクセス ポイントに割り当てる際に、各アクセス ポイントで使用されるトラフィック帯域幅が考慮されます。RRM でこの値を無視するには、このチェックボックスをオフにします。

  特定の状況でより高密度に展開されている場合、完全なチャネルの再使用を適切に作成するには、チャネルが十分に存在しないことがあります。このような状況で、RRM は、より大きなトラフィック負荷を伝送するアクセス ポイントに、より良い再使用パターンを割り当てることができます。
- これを有効にするには、[Avoid non 802.11 Noise] チェックボックスをオンにします。このノイズ モニタリング フィールドを有効にすると、電子レンジや Bluetooth デバイスなど、アクセス ポイントでないソースからの干渉のあるチャネルが回避されます。RRM でこの干渉を無視するには、このチェックボックスをオフにします。

  非 802.11 ノイズ源からの干渉エネルギー（dB）が著しい特定の状況では、このノイズ源の近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するため、RRM がチャネル割り当てを調整することがあります。これによって、キャパシティが増加し、Cisco WLAN ソリューションの変動性が減少します。
- [Signal Strength Contribution] チェックボックスは常にオンです（設定不可）。これは常に、RF/ モビリティ ドメイン内のすべてのアクセス ポイントの相対位置をモニタし、最適に近いチャネルの再使用を保証します。その結果、Cisco WLAN Solution キャパシティについては増加、チャネル相互および隣接チャネルの干渉については減少となります。
- [Channel Width] ドロップダウン リストから、[20 MHz]、[40 MHz]、または [80 MHz] を選択します。40 MHz の場合、無線の瞬間データ レートが高くなる場合がありますが、チャネル幅が大きいとオーバーラップしないチャネル数が少なくなるため、導入によっては全体のネットワーク スループットが低下することがあります。802.11ac では 80 MHz チャネル幅が提供されます。
- 次のフィールドを使用して、イベント駆動型無線リソース管理（ED-RRM; Event-Driven Radio Resource Management）を有効または無効にします。CleanAir 対応アクセス ポイントが重大なレベルの干渉を検出すると、イベント駆動型 RRM が使用されます。
  - [Event Driven RRM]：スペクトル イベント駆動型 RRM を有効または無効にします。デフォルトでは、[Event Driven RRM] は有効です。
  - [Sensitivity Threshold]：[Event Driven RRM] が有効の場合、このフィールドには、イベント駆動型 RRM が生成されるしきい値レベルが表示されます。値は、[Low]、[Medium]、または [High] のいずれかになります。アクセス ポイントの干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワークのパフォーマン

スを改善するために可能な場合は影響を受けるアクセス ポイント無線のチャネルを変更します。[Low] は、環境の変更に対する感度を下げることを表すのに対して、[High] は、感度を上げることを表します。

ステップ 5　[Save] をクリックします。

RRM 送信電力コントロール テンプレートの設定（802.11a/n）

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。通常は、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、3 番めに送信電力の強いネイバーによるアクセス ポイントの認識に応じて、アクセス ポイントの送信電力の調整を試行します。

送信電力コントロール（TPC）アルゴリズムは、RF 環境での変更に応じてアクセス ポイントの電力の増大と低減の両方を行います。ほとんどの場合、TPC は干渉を減らすためにアクセス ポイントの電力を下げようとしますが、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になるなど、RF カバレッジで急な変更が発生した場合、TPC は周辺のアクセス ポイントで電力を増大することもあります。この機能は、カバレッジ ホール検出とは異なります。カバレッジ ホールの検出は主にクライアントと関係がありますが、TPC はアクセス ポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジ レベルを達成するため、十分な RF パワーを提供する必要があります。

802.11a/n RRM TPC テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[TPC] をクリックするか、左側のサイドバーのメニューから [802.11a/n] > [TPC] を選択します。[802.11a/n TPC Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11a/n TPC template] ページが表示されます。

ステップ 4　次のフィールドを設定します。

- [Template Name] : テキスト ボックスにテンプレート名を入力します。
- [TPC Version] : [TPCv1] または [TPCv2] を選択します。

（注）　[TPCv2] オプションは、リリース 7.2.x 以降を実行するコントローラのみで使用できます。

- [Dynamic Assignment] : [Dynamic Assignment] ドロップダウン リストから、次の 3 つのモードのいずれかを選択します。
  - [Automatic] : 送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。
  - [On Demand] : 送信電力は、[Assign Now] をクリックすると更新されます。

  - [Disabled]：動的な送信電力割り当ては行われず、値はグローバル デフォルトに設定されます。
- [Maximum Power Assignment]：割り当てられている最大電力を示します。
  - 範囲：-10 ～ 30 dB
  - デフォルト：30 dB
- [Minimum Power Assignment]：割り当てられている最小電力を示します。
  - 範囲：-10 ～ 30 dB
  - デフォルト：30 dB
- [Dynamic Tx Power Control]：動的な送信電力コントロールを有効にするかどうかを決定します。
- [Transmitted Power Threshold]：送信電力しきい値を -50 ～ -80 の間で入力します。
- [Control Interval]：秒単位（読み取り専用）。

ステップ 5　[Save] をクリックします。

無線テンプレートの設定（802.11b/g/n）

ここでは、次の内容について説明します。

802.11b/g/n パラメータ テンプレートの設定

802.11b/g/n パラメータ（電源およびチャネル ステータス、データ レート、チャネル リストおよび CCX 位置測定など）を設定するテンプレートを作成または変更して、これらの設定をコントローラに適用します。

コントローラの 802.11b/g/n パラメータに関する情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次の一般パラメータを設定します。

- [Policy Name]：実施中のセキュリティ ポリシー。
- 802.11b/g Network Status
- [Beam Forming]：ドロップダウン リストから、[Enable] または [Disable] を選択します。

（注）　ビーム フォーミングは、信号の送受信の方を制御するときに使用される一般的な信号処理技術です。

- [Transmitted Power Threshold]：有効な範囲は -50 ～ -80 です。
- [Beacon Period]：SSID がアクセス ポイントによりブロードキャストされるレート（ビーコン間隔）。有効範囲は 100 ～ 600 ミリ秒です。
- [DTIM Period]：配送数フィールドが 0 のトラフィック インジケータ メッセージ（TIM）要素を含むビーコン フレームの送信間に経過したビーコン間隔。この値は、ビーコン フレームの DTIM Period フィールドで送信されます。

  DTIM を追加したビーコンをクライアント デバイスが受信すると、通常は、保留中のパケットをチェックするためにクライアント デバイスが「再起動」します。DTIM の間隔が長くなると、クライアントのスリープ時間が長くなり、電力を節約できます。反対に、DTIM の間隔が短くなるとパケットの受信の遅延を抑えられますが、クライアントが頻繁に起動するためバッテリ残量が消費されます。

（注）　DTIM の間隔は、コントローラ リリース 5.0.0.0 以降では使用できません。

- [Fragmentation Threshold]：パケットを断片化する（1 ブロックではなく、いくつかの断片として送信する）サイズを指定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。デフォルト値は 2346 です。
- [802.11e Max Bandwidth]：802.11e 最大帯域幅の割合。デフォルト値は 100 です。

ステップ 4　次の [802.11b/g Power Status] パラメータを設定します。

- [Dynamic Assignment]：[Dynamic Assignment] ドロップダウン リストから、次の動的送信電力割り当てモードのいずれかを選択します。
  - [Automatic]：送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。
  - [On Demand]：送信電力は、[Assign Now] をクリックすると更新されます。
  - [Disabled]：動的な送信電力割り当ては発生せず、値はグローバル デフォルトに設定されます。デフォルトは Automatic です。

（注）　電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。

- [Dynamic Tx Power Control]：このチェックボックスをオンにして、DTPC サポートを有効にします。このオプションが有効な場合、無線の送信電力レベルは、ビーコンにアドバタイズされ、プローブが応答します。

ステップ 5　次の [802.11b/g Channel Status] パラメータを設定します。

- [Assignment Mode]：[Assignment Mode] ドロップダウン リストから、次の動的チャネル割り当てモードのいずれかを選択します。
  - [Automatic]：この動作を許可するすべてのアクセス ポイントに対し、チャネル割り当てが定期的に更新されます。
  - [On Demand]：チャネル割り当ては、必要に応じて更新されます。
  - [Disabled]：動的チャネル割り当ては発生せず、値はグローバル デフォルトに設定されます。

（注）　デフォルトは Automatic です。

- [Avoid Foreign AP Interference] : この Radio Resource Management（RRM）外部 802.11 干渉モニタリング パラメータを有効にすると、無線リソース管理がチャネルを シスコ アクセス ポイントに割り当てるときに、外部（RF/ モビリティ ドメイン外の シスコ 非アクセス ポイント）アクセス ポイントからの干渉が考慮されます。

  無線リソース管理にこの干渉を無視させるには、このフィールドを無効にします。

  （注）　外部アクセス ポイントからの干渉エネルギー（dB）および負荷（使用率）が著しい特定の状況では、無線リソース管理は、この外部アクセス ポイントの近くの シスコ アクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するために、チャネル割り当てを調整することがあります。これにより、Cisco WLAN ソリューションのキャパシティが増加し、変動性が減少します。

- [Avoid Cisco AP Load] : この Radio Resource Management（RRM）帯域幅認識パラメータを有効にすると、コントローラがチャネルをアクセス ポイントに割り当てる際に、各アクセス ポイントで使用されるトラフィック帯域幅が考慮されます。

  無線リソース管理にこの値を無視させるには、このフィールドを無効にします。

  （注）　特定の状況でより高密度に展開されている場合、完全なチャネルの再使用を適切に作成するには、チャネルが十分でない場合があります。このような状況で、無線リソース管理は、より大きなトラフィック負荷を伝送する AP に、より良い再使用パターンを割り当てることができます。

- [Avoid non 802.11 Noise] : この Radio Resource Management（RRM）ノイズ モニタリング フィールドを有効にすると、電子レンジや Bluetooth デバイスなど、アクセス ポイントでないソースからの干渉のあるチャネルが回避されます。

  無線リソース管理にこの干渉を無視させるには、このフィールドを無効にします。

  （注）　非 802.11 ノイズ源からの干渉エネルギー（dB）が著しい特定の状況では、このノイズ源の近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するため、無線リソース管理がチャネル割り当てを調整することがあります。これにより、Cisco WLAN ソリューションのキャパシティが増加し、変動性が減少します。

- [Signal Strength Contribution] : このチェックボックスは常にオンです（設定不可）。Radio Resource Management（RRM）は常に、RF/ モビリティ ドメイン内のすべてのアクセス ポイントの相対位置をモニタし、最適に近いチャネルの再使用が保証されます。その結果、Cisco WLAN ソリューション キャパシティについては増加、チャネル相互および隣接チャネルの干渉については減少となります。

ステップ 6　データ レート パラメータを設定します。

データ レート セットは、クライアントとコントローラ間でネゴシエートされます。データ レートが [Mandatory] に設定されている場合、クライアントはネットワークを使用するには、そのデータ レートをサポートしている必要があります。データ レートがコントローラにより [Supported] として設定されている場合、同じレートをサポートする、アソシエートされているクライアントは、そのレートを使用してアクセス ポイントと通信する可能性があります。しかし、6、9、12、18、24、36、48、54 Mbps

をアソシエートするために、サポートされるすべてのレートをクライアントが使用する必要はありません。それぞれのレートについて、[Mandatory] または [Supported] のドロップダウン リスト選択が可能です。各データ レートは、[Disabled] に設定し、クライアントの設定に合わせることもできます。

ステップ 7　[Noise/Interference/Rogue Monitoring Channels] パラメータを設定します。

必要なモニタリング レベルに基づいて、すべてのチャネル、カントリー チャネルまたは DCA チャネルを選択します。Dynamic Channel Allocation（DCA）により、コントローラに接続された管理対象デバイスの中から妥当なチャネルの割り当てが自動的に選択されます。

ステップ 8　[CCX Location Measurement] パラメータを設定します。

- [Mode]：ブロードキャスト無線測定要求を有効または無効にします。有効な場合、これによってクライアントの位置の正確さが向上します。
- [Interval]：要求間の秒数での間隔。

（注）　Cisco Compatible Extension 位置測定間隔は、測定モードが有効な場合だけ変更できます。

ステップ 9　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

メディア パラメータ コントローラ テンプレートの設定（802.11b/g/n）

コール アドミッション制御およびトラフィック ストリーム メトリックなど 802.11b/g/n ボイス パラメータを設定するテンプレートを作成または変更します。

コントローラの 802.11b/g/n ボイス パラメータ情報（コール アドミッション制御およびトラフィック ストリーム メトリックなど）を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　テンプレートに適切な名前を指定します。

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

ステップ 4　[Voice] タブで、次のパラメータを設定します。

- [Admission Control (ACM)]：アドミッション制御を有効にするには、このチェックボックスを選択します。

  VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、コール アドミッション制御（CAC）が必要です。アクセス ポイントでの CAC により、アクセス ポイントは、ネットワークの輻輳時でも QoS が制御された状態を維持し、許容する最大の通話数を許容できる数に保つことができます。
- [CAC Method]：[Admission Control (ACM)] が有効になっている場合、CAC 方式を負荷ベースまたはスタティックに指定します。

負荷ベースの CAC で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって同一チャネル アクセス ポイントで消費される帯域幅や、同一チャネルの干渉によって消費される帯域幅が考慮されています。load-based の CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

- [Maximum Bandwidth Allowed]：許容される最大帯域幅の割合を入力します。このオプションは、CAC が有効の場合のみ使用可能です。コントローラのバージョンが 6.0.188.0 以前の場合、有効な範囲は 40 ～ 85 です。コントローラのバージョンが 6.0.188.1 以降の場合、有効な範囲は 5 ～ 85 で、デフォルトは 75 です。
- [Reserved Roaming Bandwidth]：予約済みのローミング帯域幅の割合を入力します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 で、デフォルトは 6 です。
- [Expedited Bandwidth]：緊急コール用に CAC の拡張として緊急帯域幅を有効にするには、このチェックボックスを選択します。

  より高い優先度が TSPEC 要求に与えられるように、CCXv5 準拠の優先帯域幅の IE が必要となります。
- [SIP CAC]：SIP CAC を有効にするには、このチェックボックスを選択します。

  SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話のみに使用する必要があります。
- [SIP Codec]：[SIP Codec] ドロップダウン リストから、この無線で使用するコーデック名を選択します。使用可能なオプションは、[G.711]、[G.729]、および [User Defined] です。
- [SIP Call Bandwidth]：ネットワークで SIP コールごとに割り当てる帯域幅（キロビット / 秒単位）を入力します。このフィールドは、選択されている [SIP Codec] が [User Defined] である場合のみ設定できます。
- [SIP Sample Interval]：コーデックを動作させる必要があるサンプルの間隔（ミリ秒）を入力します。
- [Max Number of Calls per Radio]：無線ごとのコールの最大数を入力します。
- [Metric Collection]：メトリック収集を有効にするには、このチェックボックスを選択します。

  トラフィック ストリーム メトリックは、ワイヤレス LAN での VoIP に関する一連の統計情報で、ワイヤレス LAN の QoS を通知します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは、関連付けられたすべてのアクセス ポイントから、90 秒ごとに 802.11b/g インターフェイスに関する統計情報データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にする必要があります。

ステップ 5　[Video] タブで、次のパラメータを設定します。

- [Admission Control (ACM)]：アドミッション制御を有効にするには、このチェックボックスを選択します。
- [Maximum Bandwidth]：許可される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。コントローラ バージョン 6.0.188.0 以前の場合、有効な範囲は 0 ～ 100 です。コントローラ バージョン 6.0.188.1 以降の場合、有効な範囲は 5 ～ 85 です。
- [Reserved Roaming Bandwidth]：予約済みのローミング帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。有効な範囲は 0 ～ 25 で、デフォルトは 0 です。
- [Unicast Video Redirect]：ビデオ キュー内のすべての非メディア ストリーム パケットがベスト エフォート キューにリダイレクトされるようにするには、[Unicast Video Redirect] チェックボックスを選択します。無効にすると、ビデオ マーキングのあるパケットはすべてのビデオ キューに保持されます。
- [Client Minimum Phy Rate]：クライアントがメディア ストリームに加入するために必要な物理データ レートを [Client Minimum Phy Rate] ドロップダウン リストから選択します。

- [Multicast Direct Enable]：この無線でどの WLAN でも Media Direct を有効にするには、[Multicast Direct Enable] チェックボックスを選択します。
- [Maximum Number of Streams per Radio]：許可される無線ごとのストリームの最大数を指定します。
- [Maximum Number of Streams per Client]：許可されるクライアントごとのストリーム最大数を指定します。
- [Best Effort QOS Admission]：新しいクライアント要求をベスト エフォート キューにリダイレクトするには、[Best Effort QOS Admission] チェックボックスを選択します。これは、すべてのビデオ帯域幅が使用されている場合のみ発生します。

（注）　無効になっており、最大のビデオ帯域幅が使用されている場合、新しいクライアント要求は拒否されます。

ステップ 6　[General] タブで、次のフィールドを指定します。

- [Maximum Media Bandwidth (0 to 85%)]：許可される最大帯域幅の割合を指定します。このオプションは、CAC が有効の場合のみ使用可能です。

ステップ 7　[Save] をクリックします。

保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

EDCA パラメータ コントローラ テンプレートの設定（802.11b/g/n）

802.11b/g/n EDCA パラメータを設定するテンプレートを作成または変更します。EDCA パラメータは、ボイスおよびビデオの MAC 層で事前設定プロファイルを指定します。

コントローラの 802.11b/g/n EDCA パラメータ情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のパラメータを設定します。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- [EDCA Profile]：プロファイルには、Wi-Fi Multimedia（WMM）、Spectralink Voice Priority（SVP）、Voice Optimized、および Voice & Video Optimized が含まれます。WMM がデフォルトの EDCA プロファイルです。

（注）　無線インターフェイスをシャットダウンしてから、EDCA パラメータを設定してください。

- [Streaming MAC]：ネットワーク上のすべてのクライアントが WMM 準拠の場合にだけ、Streaming MAC を有効にしてください。

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

ローミング パラメータ コントローラ テンプレートの設定（802.11b/g/n）

802.11b/g/n 無線のローミング パラメータを設定するテンプレートを作成または変更します。

コントローラの 802.11b/g/n ローミング パラメータ情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のパラメータを設定します。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- [Mode]：ドロップダウン リストから [Default Values] または [Custom Values] を選択します。
  - [Default Values]：ローミング パラメータは使用できません。デフォルト値が表示されます。
  - [Custom Values]：次のローミング パラメータを編集できます。
- [Minimum RSSI]：フィールドには、クライアントがアクセス ポイントにアソシエートするときに必要な受信信号強度インジケータ（RSSI）の最小値を入力します。

  クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。
  - 範囲：-80 ～ -90 dBm
  - デフォルト：-85 dBm
- [Roaming Hysteresis]：クライアントがローミングするために必要な隣接するアクセス ポイントの信号強度を示す値を入力します。このフィールドは、クライアントが物理的に 2 つのアクセス ポイント間の境界上やその近くにある場合に、アクセス ポイント間の「ピンポン」の量を減らすためのものです。
  - 範囲：2 ～ 4 dB
  - デフォルト：2 dB
- [Adaptive Scan Threshold]：クライアントのアソシエートされたアクセス ポイントの RSSI 値を入力します。これ以下の場合、クライアントは指定された移行時間内に隣接するアクセス ポイントにローミングできる必要があります。

  このフィールドはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。

  - 範囲：-70 ～ -77 dB
  - デフォルト：-72 dB
- [Transition Time]：クライアントのアソシエートされたアクセス ポイントからの RSSI がスキャンのしきい値より低くなった場合に、クライアントがローミングに適したネイバー アクセス ポイントの検出およびローミングにかけられる最大許容時間を入力します。
  - 範囲：1 ～ 10 秒
  - デフォルト：5 秒

（注）　[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

ハイ スループット（802.11n）コントローラ テンプレートの設定（802.11b/g/n）

MCS（データ レート）設定およびインデックスなどのハイ スループット パラメータを設定し、これらの 802.11n 設定を複数のコントローラに適用するテンプレートを作成または変更します。

コントローラのハイ スループット（802.11n）情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のフィールドを設定します。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- [802.11n Network Status]：このチェックボックスをオンにして、ハイ スループットを有効にします。
- [MCS (Data Rate) Settings]：サポートするデータ レートのレベルを選択します。MCS は、802.11a データ レートと似た変調符号化方式です。

（注）　デフォルトでは、20MHz のショート ガード インターバルが使用されます。

（注）　[Supported] チェックボックスを選択すると、選択した数値が [Selected MCS Indexes] ページに表示されます。

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

CleanAir コントローラ テンプレートの設定（802.11 b/g/n）

802.11 b/g/n 無線の CleanAir パラメータを設定するテンプレートを作成または変更します。テンプレートを設定して、コントローラの CleanAir、レポーティングおよびアラームを有効または無効にできます。また、レポートおよびアラームに含める干渉デバイスのタイプを設定できます。

コントローラの 802.11b/g/n CleanAir 情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　左側のサイドバーのメニューから、[802.11b/g/n] > [CleanAir] の順に選択します。[802.11b/g/n CleanAir Controller Templates] ページに、現在保存されているすべての 802.11b/g/n CleanAir テンプレートが表示されます。また、各テンプレートが適用されるコントローラおよび仮想ドメインの数も表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add a Template] を選択し、[Go] をクリックします。

[New Controller Template] ページが表示されます。

ステップ 4　次のフィールドを設定します。

- [Template Name]：テキスト ボックスにテンプレート名を入力します。
- [CleanAir]：チェックボックスをオンにして、802.11 b/g/n ネットワークで CleanAir を有効にします。または、オフにして、コントローラによるスペクトラム干渉の検出を停止します。デフォルト値はオンです。

（注）　[CleanAir] を有効にした場合、[Reporting Configuration] および [Alarm Configuration] グループ ボックスが表示されます。

- [Reporting Configuration]：このグループ ボックスのパラメータを使用して、レポートに含める干渉デバイスを設定します。
  - [Report Interferers]：[report interferers] チェックボックスをオンにして、CleanAir システムによる干渉源のレポートおよび検出を有効にします。または、オフにして、コントローラによる干渉デバイスのレポートを停止します。デフォルト値はオンです。
  - CleanAir システムに検出およびレポートされる必要のある干渉源が [Interferences to Detect] ボックスに表示され、検出される必要のない干渉源が [Interferers to Ignore] ボックスに表示されていることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が無視されます。
- [Alarm Configuration]：このグループ ボックスでは、電波品質アラームの生成を設定できます。
  - [Air Quality Alarm]：[Air Quality Alarm] チェックボックスを選択して電波品質アラームの生成を有効にするか、このチェックボックスを選択解除してこの機能を無効にします。
  - [Air Quality Alarm Threshold]：[Air Quality Alarm] チェックボックスを選択した場合は、[Air Quality Alarm Threshold] テキスト ボックスに 1 ～ 100 までの値を入力して、電波品質アラームが生成されるしきい値を指定します。電波品質がしきい値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は、1 です

- [Interferers For Security Alarm] : [Interferers For Security Alarm] チェックボックスをオンにして、コントローラが指定されたデバイス タイプを検出したときに干渉アラームを生成するか、選択解除してこの機能を無効にします。デフォルト値はオフです。
- 干渉デバイス アラームを生成する必要のある干渉源が [Interferers Selected for Security Alarms] ボックスに表示され、干渉デバイス アラームを生成する必要のない干渉源が [Interferers Ignored for Security Alarms] ボックスに表示されていることを確認してください。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、セキュリティ アラームに対してすべての干渉源が無視されます。

ステップ 5　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの追加」（P.11-602）を参照してください。

802.11b/g/n RRM テンプレートの設定

ここでは、次の内容について説明します。

RRM しきい値コントローラ テンプレートの設定（802.11b/g/n）

負荷、干渉、ノイズおよびカバレッジなど、さまざまな RRM しきい値を設定するテンプレートを作成または変更します。

コントローラの 802.11b/g/n RRM しきい値情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のテンプレート名を追加または変更します。

（注） テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

ステップ 4　次の [Coverage Hole Algorithm] パラメータを設定します。

- [Min.Failed Clients (#)] : 現在コントローラに関連付けられている故障したクライアントの最小数を入力します。
- [Coverage Level] : カバレッジしきい値（dB）の対象範囲を入力します。
- [Signal Strength] : [Coverage Level] フィールドを調整すると、[Signal Strength (dBm)] の値が自動的にこの変更に反映されます。[Signal Strength] フィールドにより、カバレッジ レベルを調整するときの信号強度に関する情報が提供されます。
- [Data RSSI] : データ RSSI を入力します（-60 ～ -90 dBm）。この数値は、クライアントがアクセス ポイントにアソシエートするために必要なデータの最小受信信号強度インジケータ（RSSI）の値を示します。

- [Voice RSSI]：音声 RSSI を入力します（-60 ～ -90 dBm）。この数値は、クライアントがアクセス ポイントにアソシエートするために必要な音声の最小受信信号強度インジケータ（RSSI）の値を示します。

ステップ 5　次の [Load Thresholds] パラメータを設定します。

- [Max.Clients]：現在コントローラにアソシエートできるクライアントの最大数を入力します。
- [RF Utilization]：この無線タイプのしきい値の割合を入力します。

ステップ 6　次の [Threshold for Traps] パラメータを設定します。

- [Interference Threshold]：干渉しきい値を 0 ～ 100 % の範囲で入力します。
- [Noise Threshold]：ノイズしきい値を -127 ～ 0dBm の範囲で入力します。このしきい値を超えると、コントローラは Prime Infrastructure にアラームを送信します。
- [Coverage Exception Level]：カバレッジ例外レベルの割合を入力します。最小クライアント数に設定されたカバレッジから、この割合分減少した場合、カバレッジ ホールが生成されます。

ステップ 7　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

RRM 間隔コントロール テンプレートの設定（802.11b/g/n）

802.11b/g/n 無線の RRM 間隔を設定するテンプレートを作成または変更します。

コントローラの 802.11b/g/n RRM 間隔情報を含む新しいテンプレートを追加するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　追加するテンプレートの横にある [New] をクリックします。

ステップ 3　次のパラメータを設定します。

- Template Name

（注）　テンプレート名は、テンプレートを特定するために使用される一意のキーです。同じキー属性を持つ 2 つのテンプレートを区別するため、テンプレート名は必須です。

- [Neighbor Packet Frequency]：各アクセス ポイントに対して信号強度測定を行う間隔を入力します。デフォルトは 300 秒です。
- [Noise Measurement Interval]：各アクセス ポイントに対してノイズおよび干渉測定を行う間隔を入力します。デフォルト値は 180 秒です。
- [Load Measurement Interval]：各アクセス ポイントに対して負荷測定を行う間隔を入力します。デフォルトは 300 秒です。
- [Channel Scan Duration]：各アクセス ポイントで行うカバレッジ測定の間隔を入力します。デフォルトは 300 秒です。

ステップ 4　[Save] をクリックします。保存後に、テンプレートが [Template List] ページに表示されます。[Template List] ページで、このテンプレートをコントローラに適用できます。詳細については、「コントローラ テンプレートの適用」（P.11-602）を参照してください。

RRM 動的チャネル割り当てテンプレートの設定（802.11b/g/n）

[Radio Resource Management (RRM) Dynamic Channel Assignment (DCA)] ページを使用して、このコントローラのチャネル幅のほか、DCA チャネルを選択できます。

RRM DCA は、5 GHz 帯域で 802.11n 40 MHz チャネルをサポートします。より高い帯域幅を使用すると、瞬間的データ レートが高くなります。

（注）　大きい帯域幅を選択すると、オーバーラッピングしないチャネルが減少するため、展開によっては全体のネットワーク スループットが低下することがあります。

802.11b/g/n RRM DCA テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[DCA] をクリックするか、左側のサイドバーのメニューから [802.11b/g/n] > [DCA] を選択します。[802.11b/g/n DCS Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11b/g/n TPC template] ページが表示されます。

ステップ 4　次のパラメータを設定します。

- [Template Name] : テンプレート名を入力します。
- [Assignment Mode] : [Dynamic Assignment] ドロップダウン リストから、次の 3 つのモードのいずれかを選択します。
  - [Automatic] : 送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。
  - [On Demand] : 送信電力は、[Assign Now] をクリックすると更新されます。
  - [Disabled] : 動的な送信電力割り当ては行われず、値はグローバル デフォルトに設定されます。
- 有効にするには、[Avoid Foreign AP Interference] チェックボックスをオンにします。このフィールドを有効にすると、RRM がチャネルを割り当てる際に、外部 Cisco アクセス ポイント（RF/ モビリティ ドメイン外の Cisco 以外のアクセス ポイント）からの干渉が考慮されます。この外部 802.11 は干渉しています。RRM でこの干渉を無視するには、このチェックボックスをオフにします。

  外部アクセス ポイントからの干渉エネルギー（dB）および負荷（使用率）が著しい特定の状況では、RRM は、この外部アクセス ポイントの近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するために、チャネル割り当てを調整することがあります。これによって、キャパシティが増加し、Cisco WLAN ソリューションの変動性が減少します。
- AP 負荷の回避を有効にするには、[Avoid Cisco AP Load] チェックボックスをオンにします。この帯域幅認識フィールドを有効にすると、コントローラがチャネルをアクセス ポイントに割り当てる際に、各アクセス ポイントで使用されるトラフィック帯域幅が考慮されます。RRM でこの値を無視するには、このチェックボックスをオフにします。

特定の状況でより高密度に展開されている場合、完全なチャネルの再使用を適切に作成するには、チャネルが十分に存在しないことがあります。このような状況で、RRM は、より大きなトラフィック負荷を伝送するアクセス ポイントに、より良い再使用パターンを割り当てることができます。

- これを有効にするには、[Avoid non 802.11 Noise] チェックボックスをオンにします。このノイズ モニタリング フィールドを有効にすると、電子レンジや Bluetooth デバイスなど、アクセス ポイントでないソースからの干渉のあるチャネルが回避されます。RRM でこの干渉を無視するには、このチェックボックスをオフにします。

  非 802.11 ノイズ源からの干渉エネルギー（dB）が著しい特定の状況では、このノイズ源の近くのアクセス ポイントのこれらのチャネル（および場合により隣接チャネル）を回避するため、RRM がチャネル割り当てを調整することがあります。これによって、キャパシティが増加し、Cisco WLAN ソリューションの変動性が減少します。

- [Signal Strength Contribution] チェックボックスは常にオンです（設定不可）。RRM は常に、RF/モビリティ ドメイン内のすべてのアクセス ポイントの相対位置をモニタし、最適に近いチャネルの再使用が保証されます。その結果、Cisco WLAN Solution キャパシティについては増加、チャネル相互および隣接チャネルの干渉については減少となります。

- 次のパラメータを使用して、イベント駆動型無線リソース管理（ED-RRM; Event-Driven Radio Resource Management）を有効または無効にします。CleanAir 対応アクセス ポイントが重大なレベルの干渉を検出すると、イベント駆動型 RRM が使用されます。

  - [Event Driven RRM]：スペクトル イベント駆動型 RRM を有効または無効にします。デフォルトでは、[Event Driven RRM] は有効です。
  - [Sensitivity Threshold]：[Event Driven RRM] が有効の場合、このフィールドには、イベント駆動型 RRM が生成されるしきい値レベルが表示されます。値は、[Low]、[Medium]、または [High] のいずれかになります。アクセス ポイントの干渉が閾値レベルを上回ると、RRM はローカルの動的チャネル割り当て（DCA）の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセス ポイント無線のチャネルを変更します。[Low] は、環境の変更に対する感度を下げることを表すのに対して、[High] は、感度を上げることを表します。

ステップ 5　[Save] をクリックします。

RRM 送信電力コントロール テンプレートの設定（802.11b/g/n）

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。通常は、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、3 番めに送信電力の強いネイバーによるアクセス ポイントの認識に応じて、アクセス ポイントの送信電力のバランスを取ろうとします。

送信電力コントロール（TPC）アルゴリズムは、RF 環境での変更に応じてアクセス ポイントの電力の増大と低減の両方を行います。ほとんどの場合、TPC は干渉を減らすためにアクセス ポイントの電力を下げようとしますが、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になるなど、RF カバレッジで急な変更が発生した場合、TPC は周辺のアクセス ポイントで電力を増大することもあります。この機能は、カバレッジ ホール検出とは異なります。カバレッジ ホールの検出は主にクライアントと関係がありますが、TPC はアクセス ポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジ レベルを達成するため、十分な RF パワーを提供する必要があります。

802.11b/g/n RRM TPC テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[TPC] をクリックするか、左側のサイドバーのメニューから [802.11b/g/n] > [TPC] を選択します。[802.11b/g/n TPC Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[802.11b/g/n TPC template] ページが表示されます。

ステップ 4　次のパラメータを設定します。

- [Template Name] : テキスト ボックスにテンプレート名を入力します。
- [TPC Version] : ドロップダウン リストから [TPCv1] または [TPCv2] を選択します。

  （注）　[TPCv2] オプションは、リリース 7.2.x 以降のコントローラのみで使用できます。

- [Dynamic Assignment] : [Dynamic Assignment] ドロップダウン リストから、次の 3 つのモードのいずれかを選択します。
  - [Automatic] : 送信電力は、この操作を許可するすべてのアクセス ポイントで定期的に更新されます。
  - [On Demand] : 送信電力は、[Assign Now] をクリックすると更新されます。
  - [Disabled] : 動的な送信電力割り当ては行われず、値はグローバル デフォルトに設定されます。
- [Maximum Power Assignment] : 割り当てられている最大電力を示します。
  - 範囲 : -10 ～ 30 dB
  - デフォルト : 30 dB
- [Minimum Power Assignment] : 割り当てられている最小電力を示します。
  - 範囲 : -10 ～ 30 dB
  - デフォルト : 30 dB
- [Dynamic Tx Power Control] : 動的な送信電力コントロールを有効にするかどうかを決定します。
- [Transmitted Power Threshold] : 送信電力しきい値を -50 ～ -80 の間で入力します。
- [Control Interval] : 秒単位（読み取り専用）。

ステップ 5　[Save] をクリックします。

メッシュ テンプレートの設定

メッシュ設定テンプレートの設定

アクセス ポイントを設定してコントローラとの接続を確立できます。

メッシュ テンプレートを追加、または既存のメッシュ テンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Mesh Configuration] をクリックするか、左側のサイドバーのメニューから [Mesh] > [Mesh Configuration] を選択します。[Mesh Configuration Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、rootAP から MeshAP の範囲、バックホール リンクでのクライアント アクセスおよびセキュリティ モードも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Mesh Configuration template] ページが表示されます。

ステップ 4　[Root AP to Mesh AP Range] はデフォルトで 12,000 フィートです。ルート アクセス ポイントとメッシュ アクセス ポイント間の適切な距離をフィート単位で入力します。このグローバル フィールドは、コントローラにアクセス ポイントが接続されるとすべてのアクセス ポイントに適用され、ネットワーク内に存在するすべての既存のアクセス ポイントにも適用されます。

ステップ 5　[Client Access on Backhaul Link] チェックボックスは、デフォルトでオンになっていません。このオプションが有効の場合、メッシュ アクセス ポイントは 802.11a/n 無線クライアントと 802.11a/n バックホールを介してアソシエートできます。このクライアント アソシエーションは、ルートとメッシュ アクセス ポイント間の 802.11a/n バックホール上の既存の通信に追加されます。

（注）　この機能は 2 つの無線のあるアクセス ポイントだけに適用されます。

ステップ 6　[Mesh DCA Channels] チェックボックスは、デフォルトでオンになっていません。このオプションをオンにして、コントローラで設定されている DCA チャネル リストを使用したコントローラでのバックホール チャネル選択解除を有効にします。コントローラ DCA リスト内のチャネルに対する変更はすべて、関連付けられたアクセス ポイントに適用されます。この機能は、1524SB メッシュ アクセス ポイントだけに適用されます。この機能の詳細については、『*Controller Configuration Guide*』を参照してください。

ステップ 7　バックグラウンド スキャンを有効にする場合は [Background Scanning] チェックボックスをオンにし、この機能を無効にする場合はオフにします。デフォルト値は [disabled] です。バックグラウンド スキャンにより、Cisco Aironet 1510 アクセス ポイントは、より最適なパスと親を探すために、能動的に連続して別のネイバーがいるチャネルをモニタできます。詳細については、「メッシュ ネットワークの 1510 でのバックグラウンド スキャン」（P.9-340）を参照してください。

ステップ 8　[Security Mode] ドロップダウン リストから、[EAP]（拡張認証プロトコル）または [PSK]（事前共有キー）を選択します。

ステップ 9　[Save] をクリックします。

管理テンプレートの設定

ここでは、次の内容について説明します。

トラップ レシーバ テンプレートの設定

ネットワーク上に SNMP トラップを受信するモニタリング デバイスがある場合、トラップ レシーバ テンプレートを追加できます。

トラップ レシーバ テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Trap Receivers] をクリックするか、左側のサイドバーのメニューから [Management] > [Trap Receivers] を選択します。

ステップ 3　[Management] > [Trap Receiver] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページでは、IP アドレスおよび管理ステータスも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 4　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Trap Receivers template] ページが表示されます。

ステップ 5　テキスト ボックスにサーバの IP アドレスを入力します。

ステップ 6　SNMP トラップをレシーバに送信する場合は、[Admin Status] チェックボックスをオンにして、管理者ステータスを有効にします。

ステップ 7　[Save] をクリックします。

トラップ制御テンプレートの設定

トラップ制御テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Trap Control] をクリックするか、左側のサイドバーのメニューから [Management] > [Trap Control] を選択します。[Management] > [Trap Control] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、リンク ポート アップまたはダウンおよび不正 AP も表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Trap Control template] ページが表示されます。

ステップ 4　適切なチェックボックスをオンにして、次のその他のトラップを有効にします。

- [SNMP Authentication] : SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。
- [Link (Port) Up/Down] : リンクの状態がアップまたはダウンから変わります。
- [Multiple Users] : 2 人のユーザが同じログイン ID でログインします。
- [Spanning Tree] : スパニングツリー トラップ。個々のパラメータの説明については、STP の仕様を参照してください。
- [Rogue AP] : 不正アクセス ポイントが検出されるたび、または以前検出された不正アクセス ポイントが存在しなくなると、このトラップがその MAC アドレスとともに送信されます。
- [Controller Config Save] : 設定が変更されると送信される通知です。
- [RFID Limit Reached Threshold] : RFID 到達限度をこのチェックボックスで有効にして、しきい値のパーセントを設定します。これによって RFID タグがこのしきい値をまたいだときに Prime Infrastructure に通知が送信されます。デフォルトでは、警告が有効で、しきい値は 90 に設定されています。しきい値の有効範囲は 80 ～ 100 で、単位は 1 です。

ステップ 5　適切なチェックボックスをオンにして、次のクライアントに関するトラップを有効にします。

- [802.11 Association] : クライアントが WLAN にアソシエートされるとトラップが送信されます。このトラップは、クライアントが認証されることを保証しません。
- [802.11 Disassociation] : クライアントがディスアソシエーション フレームを送信すると、ディスアソシエーション通知が送信されます。
- [802.11 Deauthentication] : クライアントが認証解除フレームを送信すると、認証解除通知が送信されます。
- [802.11 Failed Authentication] : クライアントが成功以外のステータス コードの認証フレームを送信すると、認証エラー通知が送信されます。
- [802.11 Failed Association] : クライアントが成功以外のステータス コードのアソシエーション フレームを送信すると、アソシエーション エラー通知が送信されます。
- [Excluded] : クライアントが除外されると、アソシエーション エラー通知が送信されます。
- [MaxClients Limit Reached Threshold] : MaxClients 到達限度をこのチェックボックスで有効にして、しきい値のパーセントを設定します。これによってクライアントの限度がこのしきい値をまたいだときに Prime Infrastructure に通知が送信されます。デフォルトでは、警告が有効で、しきい値は 90 に設定されています。しきい値の有効範囲は 80 ～ 100 で、単位は 1 です。

ステップ 6　適切なチェックボックスをオンにして、次のアクセス ポイント トラップを有効にします。

- [AP Register]：アクセス ポイントがコントローラとアソシエートまたはアソシエート解除すると送信される通知です。
- [AP Interface Up/Down]：アクセス ポイント インターフェイス（802.11a/n または 802.11b/g/n）のステータスがアップまたはダウンになると送信される通知です。

ステップ 7　適切なチェックボックスをオンにして、次の自動 RF プロファイル トラップを有効にします。

- [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Interference Profile]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

ステップ 8　適切なチェックボックスをオンにして、次の自動 RF 更新トラップを有効にします。

- [Channel Update]：アクセス ポイントの動的チャネル アルゴリズムが更新されると送信される通知です。
- [Tx Power Update]：アクセス ポイントの動的送信電力アルゴリズムが更新されると送信される通知です。

ステップ 9　適切なチェックボックスをオンにして、次の AAA トラップを有効にします。

- [User Auth Failure]：このトラップは、クライアント RADIUS 認証エラーが発生したことを通知します。
- [RADIUS Server No Response]：このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。

ステップ 10　適切なチェックボックスをオンにして、次の IP セキュリティ トラップを有効にします。

- ESP Authentication Failure
- ESP Replay Failure
- Invalid SPI
- IKE Negotiation Failure
- IKE Suite Failure
- Invalid Cookie

ステップ 11　適切なチェックボックスをオンにして、次の 802.11 セキュリティ トラップを有効にします。

- [WEP Decrypt Error]：コントローラが WEP 復号化エラーを検出すると送信される通知です。
- Signature Attack

ステップ 12　[Save] をクリックします。

Telnet SSH テンプレートの設定

Telnet SSH 設定テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Telnet SSH] をクリックするか、左側のサイドバーのメニューから [Management] > [Telnet SSH] を選択します。[Management] > [Telnet SSH Configuration] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページでは、セッション タイムアウト、最大セッション数、および Telnet または SSH セッションが許可されているかどうかも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Telnet SSH template] ページが表示されます。

ステップ 4　ログオフされるまでに Telnet セッションが非アクティブの状態を継続できる時間を分単位で入力します。0 は、タイムアウトしないことを意味します。有効な範囲は 0 ～ 160 で、デフォルトは 5 です。

ステップ 5　[Maximum Sessions] フィールドに、許容される Telnet の同時セッション数を入力します。有効な範囲は 0 ～ 5 で、デフォルトは 5 です。DS（ネットワーク）ポートでは、新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。

ステップ 6　[Allow New Telnet Session] ドロップダウン リストを使用して、DS ポートで新しい Telnet セッションを許可するかどうかを指定します。DS（ネットワーク）ポートでは、新しい Telnet セッションを許可または禁止できます。サービス ポートでは、新しい Telnet セッションは常に許可されます。デフォルトは [No] です。

ステップ 7　[Allow New SSH Session] ドロップダウン リストを使用して、Secure Shell Telnet セッションを許可するかどうかを指定します。デフォルトは yes です。

ステップ 8　[Save] をクリックします。

レガシー Syslog テンプレートの設定

レガシー Syslog 設定テンプレートを追加または変更するには、次の手順を実行します。

（注）　レガシー Syslog は、5.0.6.0 以前のコントローラ リリースに適用されます。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Legacy Syslog] をクリックするか、左側のサイドバーのメニューから [Management] > [Legacy Syslog] を選択します。[Management] > [Legacy Syslog] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Legacy Syslog templat] ページが表示されます。

ステップ 4　テンプレート名を入力します。このテンプレートが適用されるコントローラの数が表示されます。

ステップ 5　[Syslog] チェックボックスをオンにすると、syslog が有効になります。有効にすると、[Syslog Host IP Address] テキスト ボックスが表示されます。

ステップ 6　[Save] をクリックします。

マルチ Syslog テンプレートの設定

マルチ syslog 設定テンプレートを追加または変更するには、次の手順を実行します。

（注）　syslog サーバ テンプレートは最大 3 つ入力できます。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Multiple Syslog] をクリックするか、左側のサイドバーのメニューから [Management] > [Multiple Syslog] を選択します。[Management] > [Multiple Syslog] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページでは、syslog サーバ アドレスも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Multiple Syslog template] ページが表示されます。

ステップ 4　テキスト ボックスにテンプレート名および syslog サーバ IP アドレスを入力します。

ステップ 5　[Save] をクリックします。

ローカル管理ユーザ テンプレートの設定

ローカル管理ユーザ テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Local Management Users] をクリックするか、左側のサイドバーのメニューから [Management] > [Local Management Users] を選択します。[Management] > [Local Management Users Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページでは、ユーザ名およびアクセス レベルも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Local Management Users template] ページが表示されます。

ステップ 4　テンプレート名を入力します。

ステップ 5　テンプレート ユーザ名を入力します。

ステップ 6　このローカル管理ユーザ テンプレートのパスワードを入力します。

ステップ 7　パスワードを再度入力します。

ステップ 8　[Access Level] ドロップダウン リストを使用して、[Read Only] または [Read Write] を選択します。

ステップ 9　[Update Telnet Credentials] チェックボックスをオンにして、Telnet/SSH アクセスの Prime Infrastructure のユーザ クレデンシャルを更新します。

（注）　テンプレートが正常に適用され、[Update Telnet Credentials] オプションが有効な場合、適用される管理ユーザ クレデンシャルが、その適用コントロールへの Telnet/SSH クレデンシャルの Prime Infrastructure で使用されます。

ステップ 10　[Save] をクリックします。

ユーザ認証優先度テンプレートの設定

管理ユーザ認証優先度テンプレートは、認証サーバがコントローラの管理ユーザの認証に使用される順序を制御します。

ユーザ認証優先度テンプレートを追加したり、既存のテンプレートを変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Authentication Priority] をクリックするか、左側のサイドバーのメニューから [Management] > [Authentication Priority] を選択します。[Management] > [Local Management Users Template] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。この初期ページには、認証優先度リストも表示されます。最後の列は、テンプレートがいつ最後に保存されたかを示します。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Local Management Users template] ページが表示されます。

ステップ 4　テンプレート名を入力します。

ステップ 5　最初にローカル サーバが試行されます。ローカル認証が失敗した場合に試行するサーバをドロップダウン リストから [RADIUS] または [TACACS+] を選択します。

ステップ 6　[Save] をクリックします。

CLI テンプレートの設定

CLI コマンドのセットの適用

CLI コマンドのセットを含むテンプレートを作成し、Prime Infrastructure から 1 つ以上のコントローラにこれらを適用できます。これらのテンプレートは、SNMP サポートまたはカスタム Prime Infrastructure ユーザ インターフェイスがない複数のコントローラに機能をプロビジョニングします。テンプレート コンテンツは、コマンド配列の文字列です。置換変数、条件式などはサポートされていません。

デバイスの CLI セッションは、ユーザ プリファレンスに基づいて確立されます。デフォルト プロトコルは SSH です。プロトコル ユーザ プリファレンスについては、「CLI セッションのプロトコル設定」（P.15-858）を参照してください。

CLI テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[CLI] > [General] をクリックするか、左側のサイドバーのメニューから [CLI] > [General] を選択します。[CLI] > [General] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Command-Line Interface General template] ページが表示されます。

ステップ 4　新しいテンプレートを追加する場合、コマンドの文字列に指定する名前をテキスト ボックスに入力します。既存のテンプレートを変更する場合、[Template Name] テキスト ボックスは変更できません。

ステップ 5　[Commands] ページで、一連の CLI コマンドを入力します。

ステップ 6　[Refresh Config after Apply] チェックボックスをオンにして、CLI テンプレートが正常に適用されたら、コントローラで refresh config を実行します。

ステップ 7　CLI コマンドを選択したコントローラに適用せずに Prime Infrastructure データベースに保存する場合は [Save] をクリックし、コマンドを選択したコントローラに適用し、Prime Infrastructure データベースに保存する場合は [Apply to Controllers] をクリックします。[Apply to Controllers] をクリックする場合、テンプレートを適用するコントローラの IP アドレスを選択します。

（注）　テンプレートが選択コントローラに適用されると、ステータス画面が表示されます。テンプレートを適用するときにエラーが発生した場合、エラー メッセージが表示されます。[Session Output] 列のアイコンをクリックして、セッション全体を出力します。

（注）　コントローラで正しいユーザ名およびパスワードが設定されているが、ユーザ名およびパスワードが無効なため、Controller Telnet クレデンシャル チェックが失敗するか、コントローラ CLI テンプレートが失敗した場合、コントローラが CLI 接続の最大数を超えていないか確認してください。接続数が最大数を超えている場合、CLI セッションの最大数を増やすか、コントローラの既存の CLI セッションを終了してから、操作を再試行してください。

位置設定テンプレートの設定

位置設定テンプレートを追加または変更するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Location] > [Location Configuration] をクリックするか、左側のサイドバーのメニューから [Location] > [Location Configuration] を選択します。[Location] > [Location Configuration] ページが表示され、テンプレートが適用されるコントローラおよび仮想ドメインの数が自動的に読み込まれます。

[Applied to Controllers] の数字はリンクになっています。数字をクリックすると、[Applied to Controllers] ページが開きます。このページには、そのテンプレートが適用されているコントローラ名と IP アドレス、および適用された時刻とステータスが表示されます。[Applied to Virtual Domains] の数字もリンクになっています。このリンクをクリックすると、すべてのパーティション名が表示された [Applied to Virtual Domains] ページが開きます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Location Configuration template] ページが表示されます。

ステップ 4　[RFID Tag Data Collection] チェックボックスをオンにして、タグ コレクションを有効にします。モビリティ サービス エンジンがコントローラからアセット タグ データを収集する前に、コントローラで CLI コマンド **config rfid status enable** を使用して、アクティブ RFID タグの検出を有効にする必要があります。

ステップ 5　[Calibrating Client] チェックボックスをオンにして、クライアントの校正を有効にします。コントローラは、アクセス ポイントから校正クライアントに通常の S36 または S60 要求を送信します（クライアント機能に異なります）。パケットは、すべてのチャネルで送信されます。チャネルに関係なくすべてのアクセス ポイント（チャネル変更なし）が、RSSI データを各位置のクライアントから収集します。これらの追加送信およびチャネル変更は、同時に発生する音声またはビデオ トラフィックの質が低下する場合があります。

（注）　使用可能なすべての無線（802.11a/b/g/n）を使用するには、[Advanced] ページでマルチバンドを有効にする必要があります。

ステップ 6　[Normal Client] チェックボックスをオンにして、非校正クライアントを使用します。S36 要求はクライアントに送信されません。

（注）　S36 および S60 は、特定の Cisco Compatible Extensions との互換性があるクライアント ドライバです。S36 には CCXv2 以降との互換性があります。S60 には CCXv4 以降との互換性があります。詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps9806/products_qanda_item09186a0080af9513.shtml

ステップ 7　検出要素（タグ、クライアント、不正 AP/クライアント）を通知するまでの時間を秒単位で指定します。

ステップ 8　クライアントの RSSI 測定が廃棄される時間を秒単位で入力します。

ステップ 9　校正クライアントの RSSI 測定が廃棄される時間を秒単位で入力します。

ステップ 10　タグの RSSI 測定が廃棄される時間を秒単位で入力します。

ステップ 11　不正アクセス ポイントの RSSI 測定が廃棄される時間を秒単位で入力します。

ステップ 12　[Advanced] タブをクリックします。

ステップ 13　値を秒数で入力して、RFID タグ データ タイムアウトを設定します。

ステップ 14　[Calibrating Client Multiband] チェックボックスをオンにして、すべてのチャネルで S36 および S60 パケット（該当する場合）を送信します。校正クライアントは、[General] グループ ボックスで有効にする必要があります。

ステップ 15　[Save] をクリックします。

IPv6 テンプレートの設定

ここでは、次の内容について説明します。

- 「ネイバー バインディング タイマー テンプレートの設定」（P.11-728）
- 「RA スロット ポリシー テンプレートの設定」（P.11-729）
- 「RA ガード テンプレートの設定」（P.11-729）

ネイバー バインディング タイマー テンプレートの設定

ダウンライフタイム、到達可能ライフタイム、ステイル ライフタイムおよび対応する間隔など、IPv6 ルータ ネイバー バインディング タイマーを設定するテンプレートを作成または変更できます。

ネイバー バインディング タイマー テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Neighbor Binding Timers] をクリックするか、左側のサイドバーのメニューから [IPv6] > [Neighbor Binding Timers] を選択します。[IPv6] > [Neighbor Binding Timers] ページが表示されます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[Neighbor Binding Timers template] ページが表示されます。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　ダウン ライフタイムを有効にする場合は、[Enable] チェックボックスをオンにします。このチェックボックスをオンにした場合、[Down Lifetime Interval] テキスト ボックスに値を指定します。これは、エントリが削除されるまで、またはエントリが到達可能であることの証明を受け取るまでに、ダウン インターフェイスから学習されたエントリがバインディング テーブルで保持される最大時間（秒単位）です。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 秒です。

ステップ 6　到達可能ライフタイムを有効にする場合は、[Enable] チェックボックスをオンにします。このチェックボックスをオンにした場合、[Reachable Lifetime Interval] テキスト ボックスに値を指定します。これは、到達可能という証明（トラッキングを介した直接的な到達可能、またはネイバー探索プロトコル

（NDP）検査を介した間接的な到達可能性）を受け取らずにエントリが到達可能と見なされる最大時間（秒単位）です。この時間が経過すると、エントリはステイルに移行します。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 秒です。

ステップ 7　ステイル ライフタイムを有効にする場合は、[Enable] チェックボックスをオンにします。このチェックボックスをオンにした場合、[Stale Lifetime Interval] テキスト ボックスに値を指定します。これは、エントリが削除されるまで、またはエントリが到達可能であることの証明を受け取るまでに、ステイル エントリがバインディング テーブルで保持される最大時間（秒単位）です。範囲は 0 ～ 86,400 秒で、デフォルト値は 0 秒です。

ステップ 8　[Save] をクリックします。

RA スロット ポリシー テンプレートの設定

[RA Throttle Policy] を使用すると、ワイヤレス ネットワークで循環するマルチキャスト ルータ アドバタイズメント（RA）の量を制限できます。RA スロット ポリシー、スロット期間およびその他のオプションなど IPv6 ルータ アドバタイズメント パラメータを設定するテンプレートを作成または変更できます。

RA スロット ポリシー テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RA Throttle Policy] をクリックするか、左側のサイドバーのメニューから [IPv6] > [RA Throttle Policy] を選択します。[IPv6] > [RA Throttle Policy] ページが表示されます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[RA Throttle Policy template] ページが表示されます。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　ダウン ライフタイムを有効にする場合は、[Enable] チェックボックスをオンにします。このチェックボックスを選択した場合は、次のパラメータを設定します。

- [Throttle Period]：スロットル期間（秒単位）。指定できる範囲は 10 ～ 86,400 秒です。
- [Max Through]：秒単位での一定期間で通過する RA の数。
- [Interval Option]：RA で間隔オプションが指定されている場合の動作を示します。
- [Allow At-least]：ルータ単位で抑制されない RA の最小数を示します。
- [Allow At-most]：ルータ単位で抑制されない RA の最大数を示します。

ステップ 6　[Save] をクリックします。

RA ガード テンプレートの設定

RA ガードは、RA をワイヤレス クライアントからドロップするときに使用される Unified Wireless ソリューションです。これはグローバルに設定され、デフォルトで有効です。IPv6 ルータ アドバタイズメント パラメータを設定するテンプレートを作成または変更できます。

RA ガード テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[RA Guard] をクリックするか、左側のサイドバーのメニューから [IPv6] > [RA Guard] を選択します。[IPv6] > [RA Guard] ページが表示されます。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。[RA Guard template] ページが表示されます。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　[Router Advertisement Guard] を有効にするには、[Enable] チェックボックスを選択します。

ステップ 6　[Save] をクリックします。

プロキシ モバイル IPv6 テンプレートの設定

プロキシ モバイル IPv6 は、任意の IP モビリティ関連シグナリングでモバイル ノードのプロキシとして動作することによってモバイル ノードをサポートする、ネットワーク ベースのモバイル管理プロトコルです。ネットワークのモビリティ エンティティは、モバイル ノードの移動を追跡し、モビリティ シグナリングを起動して必要なルーティング状態を設定します。

主要な機能エンティティは Local Mobility Anchor（LMA）とモバイル アクセス ゲートウェイ（MAG）です。LMA はモバイル ノードの到達可能性状態を維持し、モバイル ノードの IP アドレス用のトポロジ アンカー ポイントです。MAG はモバイル ノードの代わりにモビリティ管理を行います。MAG はモバイル ノードがアンカーされているアクセス リンクに存在します。コントローラは MAG 機能を実装します。

PMIP グローバル設定の構成

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Global Config] をクリックするか、左側のサイドバーのメニューから [PMIP] > [Global Config] の順に選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　次のフィールドを設定します。

- [Domain Name]
- [Maximum Bindings Allowed] : コントローラが MAG に送信できるバインディング アップデートの最大数。有効な範囲は 0 ～ 40000 です。
- [Binding Lifetime] : コントローラのバインディング エントリのライフタイム。有効な範囲は 10 ～ 65535 秒です。デフォルト値は 65535 です。バインディング ライフタイムは 4 秒の倍数であることが必要です。
- [Binding Refresh Time] : コントローラのバインディング エントリのリフレッシュ時間。有効な範囲は 4 ～ 65535 秒です。デフォルト値は 300 秒です。バインディング リフレッシュ時間は 4 秒の倍数であることが必要です。
- [Binding Initial Retry Timeout] : コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の初期タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 1000 秒です。

- [Binding Maximum Retry Timeout] : コントローラがプロキシ バインディング確認（PBA）を受信しない場合のプロキシ バインディング アップデート（PBU）間の最大タイムアウト。有効な範囲は 100 ～ 65535 秒です。デフォルト値は 32000 秒です。
- [Replay Protection Timestamp] : 受信したプロキシ バインディング確認のタイムスタンプと現在の日時との時間差の上限。有効範囲は 1 ～ 255 ミリ秒です。デフォルト値は 7 ミリ秒です。
- [Minimum BRI Retransmit Timeout] : コントローラが BRI メッセージを再送信するまでに待機する時間の最小値。有効な範囲は 500 ～ 65535 秒です。
- [Maximum BRI Retransmit Timeout] : コントローラが Binding Revocation Indication（BRI）メッセージを再送信するまでに待機する時間の最大値。有効な範囲は 500 ～ 65535 秒です。デフォルト値は 2000 秒です。

ステップ 6　[Save] をクリックします。

LMA 設定の構成

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[LMA Config] をクリックするか、左側のサイドバーのメニューから [PMIP] > [LMA Config] の順に選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　次のフィールドを設定します。

- [LMA Name] : コントローラに接続された LMA の名前。
- [LMA IP Address] : コントローラに接続された LMA の IP アドレス。

ステップ 5　[Save] をクリックします。

PMIP プロファイルの設定

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Profile] をクリックするか、左側のサイドバーのメニューから [PMIP] > [Profile] の順に選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　プロファイル名を入力します。

ステップ 5　[Add] をクリックし、次のフィールドを設定します。

- [Network Access Identifier] : プロファイルにアソシエートされたネットワーク アクセス識別子（NAI）の名前。
- [LMA Name] : プロファイルをアソシエートする LMA の名前。
- [Access Point Node] : コントローラに接続されているアクセス ポイント ノードの名前。

ステップ 6　[Save] をクリックします。

mDNS テンプレートの設定

マルチキャスト DNS（mDNS）サービス ディスカバリは、ローカル ネットワークでサービスを通知し、検出する手段を提供します。mDNS は IP マルチキャストを介して DNS クエリーを実行します。mDNS はゼロ設定の IP ネットワーキングをサポートします。

以下は、mDNS のテンプレートに関する注意事項および制約事項です。

- mDNS サービスが 1 つ以上のプロファイルにマップされている場合、その mDNS サービスは削除できません。
- プロファイル名およびサービス名は最大 31 文字です。
- サービス文字列の長さは最大 255 文字です。
- デフォルト プロファイル（default-mdns-profile）は削除できません。
- プロファイルがインターフェイス、インターフェイス グループ、または WLAN にマップされている場合、それらのプロファイルは削除できません。
- mDNS サービスがインターフェイス、インターフェイス グループ、または WLAN にマップされている場合、プロファイルからそれらの mDNS サービスを削除できません。新しいサービスを追加できます。
- mDNS テンプレートを作成して適用すると、コントローラの現在の設定が上書きされます。
- FlexConnect ローカル スイッチングがオンの場合、WLAN の mDNS スヌーピングを有効にできません。
- 「AP Management」が有効の場合、インターフェイスに mDNS プロファイルをアタッチできません。

コントローラが mDNS サービスを認識し、すべてのクライアントにこれらのサービスをアドバタイズできるようにするために mDNS テンプレートを作成できます。

[Services] と [Profiles] の 2 個のタブがあります。

- [Services] タブ：このタブでは、グローバル mDNS パラメータを設定し、Master Services データベースを更新できます。
- [Profiles] タブ：このタブでは、コントローラに設定されている mDNS プロファイルを表示し、新しい mDNS プロファイルを作成できます。新しいプロファイルを作成した後、インターフェイス グループ、インターフェイス、または WLAN にプロファイルをマッピングする必要があります。クライアントはプロファイルに関連付けられたサービスだけのサービス アドバタイズメントを受信します。コントローラはインターフェイス グループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイス プロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。デフォルトで、コントローラには mDNS プロファイル default-mdns-profile があります。このデフォルト プロファイルは削除できません。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[mDNS] をクリックするか、左側のサイドバーのメニューから [mDNS] > [mDNS] の順に選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　[Services] タブで、次のパラメータを設定します。

- [Template Name]：このテンプレートのユーザ定義の名前。
- [mDNS Global Snooping]：mDNS パケットのスヌーピングを有効にするチェックボックス。

（注） コントローラは mDNS スヌーピングを有効にしても、IPv6 mDNS パケットをサポートしません。

- [Query Interval]（10 ～ 120）：ユーザが設定できる mDNS クエリー間隔（分単位）。この間隔は、WLC によって、サービス アドバタイズメントを自動的に送信しないサービスに対して、そのサービスが開始された後に定期的な mDNS クエリー メッセージを送信するために使用されます。範囲は 10 ～ 120 分です。デフォルト値は 15 分です。
- [Master Services]：[Add Row] をクリックし、次のフィールドを設定します。
  - [Master Service Name]：ドロップダウン リストから、照会可能なサポートされているサービスを選択できます。次のサービスを使用できます。
  - AirTunes
  - AirPrint
  - AppleTV
  - HP Photosmart Printer1
  - HP Photosmart Printer2
  - Apple File Sharing Protocol（AFP）
  - スキャナ
  - プリンタ
  - FTP
  - iTunes Music Sharing
  - iTunes Home Sharing
  - iTunes Wireless Device Syncing
  - Apple Remote Desktop
  - Apple CD/DVD Sharing
  - Time Capsule Backup

（注） 新しいサービスを追加するには、サービス名を入力または選択し、そのサービス文字列を入力して、サービス ステータスを選択します。

- [Service Name]：mDNS サービスの名前。
- [Service String]：mDNS サービスに関連付けられた一意の文字列。たとえば、_airplay._tcp.local. は AppleTV に関連付けられたサービス文字列です。
- [Query Status]：サービスの mDNS クエリーを有効にするために選択するチェックボックス。

（注） 定期的な mDNS クエリー メッセージは、クエリーのステータスが有効な場合だけ、WLC によって、サービスに対して設定されたクエリー間隔で送信されます。それ以外の場合、サービスは、クエリーのステータスが無効になっているその他のサービス（たとえば AppleTV）に自動的にアドバタイズする場合があります。

ステップ 5　[Profiles] タブで、次のパラメータを設定します。

- [Profiles] : [Add Profile] をクリックし、次のフィールドを設定します。
  - [Profile Name] : mDNS プロファイルの名前。最大 16 個のプロファイルを作成できます。
  - [Services] : mDNS プロファイルにマップするサービスを選択します（チェックボックスを使用）。

ステップ 6　[Save] をクリックします。

AVC プロファイル テンプレートの設定

Application Visibility and Control（AVC）は、Network Based Application Recognition（NBAR）ディープ パケット インスペクション テクノロジーを使用して、使用するプロトコルに基づいてアプリケーションを分類します。AVC を使用して、コントローラはレイヤ 4 ～レイヤ 7 の 1400 を超えるプロトコルを検出できます。AVC では、リアルタイム分析を実施して、ネットワークの輻輳、高価なネットワーク リンクの使用、およびインフラストラクチャのアップグレードを減らすためにポリシーを作成することができます。

AVC は、Cisco 2500 および 5500 シリーズ コントローラ、WiSM 2 コントローラ、Cisco Flex 7500 および Cisco 8500 シリーズ コントローラでのみサポートされます。

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[AVC Profiles] をクリックするか、左側のサイドバーのメニューから [Application Visibility And Control] > [AVC Profiles] の順に選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　AVC プロファイルの名前を入力します。

（注）　1 つの WLAN には AVC プロファイルを 1 つだけ設定できます。また各 AVC プロファイルに最大 32 のルールを設定できます。各ルールでは、アプリケーションのマーキング アクションまたはドロップ アクションを示します。これにより、WLAN ごとに最大 32 のアプリケーション アクションを設定できます。コントローラ 1 台に最大 16 の AVC プロファイルを設定し、AVC プロファイル 1 つを複数の WLAN に関連付けることができます。

ステップ 6　[AVC Rule List] で、[Add Row] をクリックして AVC ルールを作成します。

- [Application Name] : アプリケーションの名前。
- [Application Group Name] : アプリケーションが属するアプリケーション グループの名前。
- [Action] : ドロップダウン リストから、次の項目を選択できます。
  - [Drop] : 選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをドロップします。
  - [Mark] : [Differentiated Services Code Point (DSCP)] ドロップダウン リストで指定する DSCP 値と選択されたアプリケーションに対応するアップストリームおよびダウンストリーム パケットをマークします。DSCP 値により QoS レベルに基づいて差別化サービスを提供します。

デフォルト アクションは、すべてのアプリケーションの許可です。

- [DSCP]：インターネットでのサービスの質を定義するために使用できるパケット ヘッダー コード。DSCP 値は次の QoS レベルにマッピングされます。
  - [Platinum (Voice)]：Voice over Wireless の高い QoS を保証します。
  - [Gold (Video)]：高品質のビデオ アプリケーションをサポートします。
  - [Silver (Best Effort)]：クライアントの通常の帯域幅をサポートします。
  - [Bronze (Background)]：ゲスト サービス用の最小の帯域幅を提供します。
- [DSCP Value]：[Custom] を選択し、DSCP 値を指定することもできます。範囲は 0 ～ 63 です。

ステップ 7　[Save] をクリックします。

NetFlow テンプレートの設定

NetFlow は、ネットワーク ユーザとアプリケーション、ピーク時の使用時間、およびトラフィック ルーティングに関する貴重な情報を提供するプロトコルです。このプロトコルは、トラフィックをモニタするためにネットワーク デバイスから IP トラフィック情報を収集します。Netflow アーキテクチャは次のコンポーネントで構成されています。

- コレクタ：さまざまなネットワーク要素から IP トラフィック情報をすべて収集するエンティティ。
- エクスポータ：IP トラフィック情報を使用してテンプレートをエクスポートするネットワーク エンティティ。コントローラは、エクスポータとして機能します。

ここでは、次の内容について説明します。

- 「NetFlow モニタ テンプレートの設定」（P.11-735）
- 「NetFlow エクスポータ テンプレートの設定」（P.11-736）

NetFlow モニタ テンプレートの設定

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Monitor] をクリックするか、左側のサイドバーのメニューから [NetFlow] > [Monitor] の順に選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　次のパラメータを設定します。

- [Monitor Name]：NetFlow モニタの名前。モニタ名は最大 127 文字の英数字で、大文字と小文字を区別します。コントローラでは 1 つのみモニタを設定できます。
- [Record Name]：NetFlow レコードの名前。コントローラの NetFlow レコードには、特定のフロー内のトラフィックに関する次の情報が含まれます。
  - クライアント MAC アドレス
  - クライアント送信元 IP アドレス
  - WLAN ID

- アプリケーション ID
- データの着信バイト数
- データの発信バイト数
- 着信パケット
- 発信パケット
- 着信 DSCP
- 発信 DSCP
- 最後の AP の名前。

ステップ 6　[Exporter Name]：エクスポータの名前。

ステップ 7　[Save] をクリックします。

NetFlow エクスポータ テンプレートの設定

ステップ 1　[Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2　[Exporters] をクリックするか、左側のサイドバーのメニューから [NetFlow] > [Exporters] の順に選択します。

ステップ 3　新しいテンプレートを追加する場合は、[Select a command] ドロップダウン リストから [Add Template] を選択し、[Go] をクリックします。既存のテンプレートを変更するには、テンプレート名をクリックします。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　次のパラメータを設定します。

- [Exporter Name]：エクスポータの名前。
- [Exporter IP]：エクスポータの IP アドレス。
- [Port Number]：NetFlow レコードをコントローラからエクスポートする UDP ポート。

ステップ 6　[Save] をクリックします。

（注）　コントローラあたり 1 つの NetFlow エクスポータのみ設定できます。

AP 設定テンプレートの設定

このメニューは、アクセス ポイント テンプレート概要の詳細へのアクセスを提供します。セレクタ グループ ボックスを使用して、個々のテンプレートの詳細にアクセスし設定します。

（注）　テンプレート名を選択して、現在のアクセス ポイント テンプレートのパラメータを表示または編集します。アクセス ポイント テンプレート パラメータの詳細については、「新しい Lightweight アクセス ポイント テンプレートの設定」（P.11-737）で適切なステップを参照してください。

ここでは、次の内容について説明します。

Lightweight アクセス ポイント テンプレートの設定

ここでは、次の内容について説明します。

新しい Lightweight アクセス ポイント テンプレートの設定

新しい Lightweight アクセス ポイント テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Lightweight AP Configuration Templates] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　テキスト ボックスにテンプレート名を入力します。

ステップ 5　テキスト ボックスにテンプレートの説明を入力します。

ステップ 6　[Save] をクリックします。

ステップ 7　ロードされると、[Lightweight AP Template Detail] ページが表示されます。ここでは、[Lightweight AP Template Detail] ページについて説明します。内容は次のとおりです。

[AP Parameters] タブ

適用する必要があるアクセス ポイント パラメータのチェックボックスをオンにします。

- [Location] : [Location] テキスト ボックスに位置を入力します。
- [Admin Status] : [Admin and Enabled] チェックボックスをオンにして、管理ステータスを有効にします。

（注）　エネルギーを節約するために、アクセス ポイントを作業時間以外の指定された時間にオフにすることができます。[Enabled] チェックボックスをオンにすると、アクセス ポイントをオンにしたりオフにしたりします。

- [AP Mode]：ドロップダウン リストから、次のいずれかを選択します。
  - [Local]：デフォルト。
  - [Monitor]：モニタ モードのみ。

    （注）　[Monitor] をオンにして、Cisco Adaptive wIPS のアクセス ポイント テンプレートを有効にします。[Monitor] を選択した場合、[Enhanced WIPS Engine] チェックボックスおよび [Enabled] チェックボックスをオンにします。[AP Monitor Mode Optimization] チェックボックスをオンにして、[AP Monitor Mode Optimization] ドロップダウン リストから [WIPS] を選択します。Cisco Adaptive wIPS の詳細については、「wIPS プロファイルの設定」（P.9-546）または「wIPS ポリシー アラーム リファレンス」（P.18-1071）および「Prime Infrastructure サービス」（P.16-937）を参照してください。

  - [FlexConnect]：Cisco 1030 IEEE 802.11a/b/g/n リモート エッジ Lightweight アクセス ポイントで使用される Cisco 1030 リモート エッジ Lightweight アクセス ポイント（REAP）。

    （注）　OfficeExtend アクセス ポイントを設定するには、[FlexConnect] を選択する必要があります。AP モードが [FlexConnect] の場合、[OfficeExtend AP] および [Least Latency Controller Join] を有効にするオプションなど、[FlexConnect] 設定オプションが表示されます。詳細については、「FlexConnect の設定」（P.12-761）を参照してください。

  - [Rogue Detector]：不正アクセス ポイントをモニタしますが、不正アクセス ポイントを送信したり、封じ込め処理をすることはありません。
  - Bridge
  - [Sniffer]：アクセス ポイントは、所定のチャネルで無線を「スニファ」します。アクセス ポイントは、そのチャネル上のクライアントからのすべてのパケットを取得し、AiroPeek（IEEE 802.11 無線 LAN のパケット アナライザ）を実行するリモート マシンに転送します。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。動作モードとして [Sniffer] を選択する場合、AP/ 無線テンプレートの [802.11b/g/n Parameters] または [802.11a/n Parameters] タブでチャネルとサーバ IP アドレスの入力を要求されます。

    （注）　スニファ機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合だけ有効になります。AiroPeek の詳細については、http://www.wildpackets.com を参照してください。

  - [SE-Connect]：このモードでは、CleanAir 対応のアクセス ポイントをすべてのモニタ対象チャネルでの干渉検出に広く使用できます。IDS スキャンや Wi-Fi などのその他の機能はすべて一時停止されます。

    （注）　このオプションは、アクセス ポイントが CleanAir 対応の場合のみ表示されます。

（注）　AP モードを変更すると、アクセス ポイントがリブートします。

- [Enhanced wIPS Engine]：[Enhanced wIPS Engine] および [Enabled] チェックボックスをオンにして有効にします。
- [AP Sub Mode]：ドロップダウン リストからオプションを選択します。
- [AP Height (feet)]：アクセス ポイントの高さ（フィート）をテキスト ボックスに入力します。
- [Mirror Mode]：[Enabled] チェックボックスをオンにして、ミラー モードを有効にします。
- [Country Code]：適切な国コードをドロップダウン リストから選択します。

（注）　国コードを変更すると、アクセス ポイントがリブートされる場合があります。

- [Stats Collection Interval]：状態収集間隔をテキスト ボックスに入力します。
- [Cisco Discovery Protocol]：[Enabled] チェックボックスをオンにして、Cisco Discovery Protocol を有効にします。
- [AP Failover Priority]：ドロップダウン リストから [Low]、[Medium]、[High] または [Critical] を選択して、アクセス ポイント フェールオーバー優先度を示します。デフォルトの優先度は [Low] です。詳細については、「AP フェールオーバー優先度の設定」（P.9-464）を参照してください。
- Pre-Standard 802.3af Switches
- [Power Injector State]：有効にすると、コントローラに直接移動せずに、Prime Infrastructure を介してパワー インジェクタ設定を操作できます。[Enable Power Injector State] を選択した場合、パワー インジェクタ オプションが表示されます。
- [Power Injector Selection]：ドロップダウン リストから [installed] または [override] を選択します。
- [Injector Switch MAC Address]：インジェクタ スイッチの MAC アドレスを入力します。
- [Primary, Secondary, and Tertiary Controller IP]：プライマリ、セカンダリ、ターシャリ コントローラ IP は、コントローラの管理 IP です。
- [Domain Name]
- [Domain Name Server IP Address]：ドメイン ネーム サーバ IP およびドメイン ネームは、スタティック IP を持つ AP だけで設定できます。
- [Encryption]：[Encryption] チェックボックスをオンにして、暗号化を有効にします。

（注）　暗号化機能を有効または無効にすると、アクセス ポイントがリブートし、クライアントの接続が失われます。

（注）　DTLS データ暗号化は、セキュリティを維持するため、OfficeExtend アクセス ポイントで自動的に有効になります。暗号化は、Plus ライセンスが設定された 5500 シリーズ コントローラにアクセス ポイントが接続されている場合のみ使用できます。暗号化は、すべてのアクセス ポイント モデルで使用できるわけではありません。

（注）　暗号化を有効にすると、パフォーマンスが低下することがあります。

- [Rogue Detection]：チェックボックスをオンにして、不正検出を有効にします。

（注）　家庭環境に導入されるアクセス ポイントは、多数の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出は自動的に無効にされます。OfficeExtend アクセス ポイントの詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

- [SSH Access]：[SSH Access] チェックボックスをオンにして、SSH アクセスを有効にします。
- [Telnet Access]：[Telnet Access] チェックボックスをオンにして、Telnet アクセスを有効にします。

（注）　OfficeExtend アクセス ポイントは、デフォルトのパスワードがアクセス ポイントで使用されている場合に外部アクセスを許可する可能性がある WAN に直接接続されていることがあります。このため、Telnet と SSH アクセスは、OfficeExtend アクセス ポイントでは自動的に無効になります。

- [Link Latency]：コントローラでリンク遅延を設定して、アクセス ポイントおよびコントローラの間のリンクを計測できます。この機能はコントローラに接続されたすべてのアクセス ポイントで使用できますが、特に、リンクの速度が低い場合のある FlexConnect アクセス ポイント、および信頼性の低い WAN 接続で役立ちます。詳細については、「アクセス ポイントのリンク遅延の設定」（P.9-514）を参照してください。

（注）　リンク遅延は、接続モードが FlexConnect アクセス ポイントのみでサポートされます。スタンドアロン モードの FlexConnect アクセス ポイントはサポートされません。

- [Reboot AP]：チェックボックスをオンにして、他の更新後のアクセス ポイントのリブートを有効にします。
- [TCP Adjust MSS]：[TCP Adjust MSS] チェックボックスをオンにして、TCP を有効にして MSS を調整します。
- [AP Failover Priority]：ドロップダウン リストから [Low]、[Medium]、[High] または [Critical] を選択して、アクセス ポイント フェールオーバー優先度を示します。デフォルトの優先度は [Low] です。詳細については、「AP フェールオーバー優先度の設定」（P.9-464）を参照してください。
- [Controllers]：[Controllers] チェックボックスをオンにして、プライマリ、セカンダリおよびターシャリ コントローラ名のドロップダウン リストを有効にします。
- [Group VLAN name]：適切なグループ VLAN 名をドロップダウン リストから選択します。
- [Override Global Username Password]：チェックボックスをオンにして、グローバル ユーザ名およびパスワードの上書きを有効にします。新しいアクセス ポイント ユーザ名およびパスワードを、該当するテキスト ボックスに入力し確認します。グローバル ユーザ名およびパスワードの詳細については、「グローバル アクセス ポイント パスワードの設定」（P.9-345）を参照してください。

（注）　[System] > [AP Username Password] ページでは、コントローラへの接続時に継承するすべてのアクセス ポイントのグローバル クレデンシャルを設定できます。設定したクレデンシャルは、[AP Parameter] タブ ページの右下に表示されます。

- [Override Supplicant Credentials] : [Override Supplicant Credentials] チェックボックスをオンにして、このアクセス ポイントがコントローラから認証ユーザ名およびパスワードを継承しないようにします。デフォルト値はオフです。[Override Supplicant Credentials] オプションは、コントローラ リリース 6.0 以降でサポートされます。
  - [Username]、[Password]、および [Confirm Password] テキスト ボックスに、このアクセス ポイントに割り当てる一意のユーザ名およびパスワードを入力します。

（注）　入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。

- [AP LED] : アクセス ポイントの LED を有効または無効にするチェックボックスです。多くの AP が導入されていて、特定の AP を検索する場合、すべての AP の LED を無効にした後、検索対象の AP の LED を有効にできます。これによって、LED が有効になっている AP を簡単に識別できます。

[Mesh] タブ

[Mesh] タブを使用して、メッシュ アクセス ポイントの次のパラメータを設定します。

- [Bridge Group Name] : ブリッジ グループ名（最大 10 文字）をテキスト ボックスに入力します。

（注）　ブリッジ グループは、メッシュ アクセス ポイントを論理的にグループ化して、同一チャネル上の 2 つのネットワークが互いに通信しないようにするために使用されます。

（注）　メッシュ アクセス ポイントが通信するためには、同じブリッジ グループ名が付いている必要があります。

（注）　複数の RAP を使用する設定の場合は、ある RAP から別の RAP へフェールオーバーできるように、すべての RAP に同じブリッジ グループ名が付いていることを確認してください。

- [Data Rate (Mbps)] : バックホール インターフェイスのデータ レートをドロップダウン リストから選択します。使用可能なデータ レートは、バックホール インターフェイスによって指示されます。デフォルトのレートは 18Mbps です。

（注）　このデータ レートは、メッシュ アクセス ポイント間で共有され、メッシュ ネットワーク全体に対して固定されます。

（注）　展開したメッシュ ネットワーク ソリューションに対してデータ レートを変更しないでください。

- [Ethernet Bridging] : [Enable] チェックボックスをオンにします。[Ethernet Bridging] ドロップダウン リストから、メッシュ アクセス ポイントの Ethernet ブリッジングを有効にします。
- [Role] : メッシュ アクセス ポイントのロールをドロップダウン リストから選択します（[MAP] または [RAP]）。デフォルトの設定は MAP です。

（注）　メッシュ ネットワークのアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）として機能します。

[802.11a/n] タブ

適用する必要がある 802.11a/n パラメータのチェックボックスをオンにします。

- Channel Assignment
- Admin Status
- Antenna Mode
- Antenna Diversity
- Antenna Name
- Power Assignment
- WLAN Override
- 11n Antenna Selection
- CleanAir
- Channel Width for 802.11ac
- Admin Status for 802.11ac

[802.11a SubBand] タブ

適用する必要がある 802.11a Sub Band オプション（4.9 または 5.8 パラメータ）を選択します。

（注）　フィールド左側のチェックボックスがオンでない限り、オプションは無効です。

- Admin Status
- [Channel Assignment] : チェックボックスをオンにして、該当するチャネルをドロップダウン リストから選択します。

  （注）　チャネル番号は、その無線でサポートされているチャネル一覧に対して検証されます。

- [Power Assignment] : チェックボックスをオンにして、該当する電力レベルをドロップダウン リストから選択します。

  （注）　電力レベルは、その無線でサポートされている電力レベル一覧に対して検証されます。

- [WLAN Override] : チェックボックスをオンにして、ドロップダウン リストから [Disable] または [Enable] を選択します。

  （注）　WLAN の上書きについての変更を有効にするためには、このアクセス ポイントをリセットする必要があります。

- [Antenna Type]：チェックボックスをオンにして、アンテナ タイプをドロップダウン リストから選択します。
- [Antenna Name]：[Antenna Type] チェックボックスをオンにして、適切なアンテナ名をドロップダウン リストから選択します。

（注）　アクセス ポイントのタイプによっては、一部のアンテナ モデルしかサポートしていないものもあります。

[802.11b/g/n] タブ

適用する必要がある 802.11b/g/n パラメータのチェックボックスをオンにします。

- Channel Assignment
- Admin Status
- Antenna Mode
- Antenna Diversity
- Antenna Name
- Power Assignment
- WLAN Override
- Tracking Optimized Monitor Mode
- 11n Antenna Selection
- CleanAir

[CDP] タブ

- [Cisco Discovery Protocol on Ethernet Interfaces] グループ ボックスで、CDP を有効にするイーサネット インターフェイスのスロットのチェックボックスをオンにします。
- [Cisco Discovery Protocol on Radio Interfaces] グループ ボックスで、CDP を有効にする無線インターフェイスのスロットを選択します。

[FlexConnect] タブ

- [FlexConnect Configuration]：チェックボックスをオンにして、FlexConnect 設定（VLAN サポート、ネイティブ VLAN ID およびプロファイル名 VLAN マッピングなど）を有効にします。

（注）　これらのオプションは、FlexConnect モードのアクセス ポイントだけで使用できます。

  - [OfficeExtend]：デフォルトは [Enabled] です。

（注）　このチェックボックスを選択解除すると、単にこのアクセス ポイントの OfficeExtend モードが無効になります。アクセス ポイントの設定すべてが取り消されることはありません。アクセス ポイント設定をクリアし、工場出荷時設定に戻す場合、アクセス ポイント詳細ページ下部の [Clear Config] をクリックします。アクセス ポイント パーソナル SSID だけをクリアする場合、アクセス ポイント詳細ページ下部の [Reset Personal SSID] をクリックします。詳細については、「出荷時の初期状態の復元」（P.9-319）を参照してください。

（注）　[Enable for the OfficeExtend AP] を選択した場合、いくつかの設定が自動的に変更されます。たとえば、暗号化およびリンク遅延が有効になり、不正検出、SSH アクセス、Telnet アクセスが無効になります。

（注）　OfficeExtend アクセス ポイントを有効にする場合、少なくとも 1 つのプライマリ、セカンダリ、ターシャリ コントローラ（名前および IP アドレスを含む）を設定する必要があります。

- [Least Latency Controller Join] : 有効にすると、アクセス ポイントは、優先度順の検索（プライマリ、セカンダリ、次にターシャリ コントローラ）から、遅延測定が最善（最短の遅延）のコントローラの検索に切り替えます。遅延が最短のコントローラが、最善のパフォーマンスを提供します。

（注）　アクセス ポイントは、コントローラを初めて追加したときにこの検索を一度のみ実行します。接続後は、プライマリ、セカンダリおよびターシャリの遅延測定を再計算して、遅延測定が変わったかどうかを確認されることはありません。

- VLAN Support
- Native VLAN ID

（注）　ネイティブの VLAN ID の有効な範囲は 1 ～ 4094 です。モードを REAP に変更するときに、アクセス ポイントがまだ REAP モードでない場合、他のすべての REAP パラメータはそのアクセス ポイントに適用されません。

[Show/Add VLAN ACL Mapping] リンクをクリックして、VLAN ID を追加または削除して、入力 ACL および出力 ACL にマッピングします。

- [VLAN ID ACL Mapping] : VLAN ID を入力して、ドロップダウン リスト ボックスから [Ingress and Egress ACLs] を選択して、指定 VLAN ID にマッピングします。

[Show/Add WebAuth ACL Mapping] リンクをクリックして、WLAN プロファイルおよび WebAuth ACL マッピングを追加または削除します。

- [WLAN Profile to ACL Mapping]: ドロップダウン リスト ボックスから WLAN プロファイルおよび WebAuth ACL を選択して、WebAuth ACL マッピングを追加します。

[Show/Add WebPolciy ACL] リンクをクリックして、Web ポリシー ACL を追加または削除します。

[Local Split ACL Mapping] リンクをクリックして、Local Split ACL マッピングを追加または削除します。

- [WLAN Profile Name] ドロップダウン リストから、WLAN プロファイルを選択します。

（注）　FlexConnect 中央スイッチング WLAN だけが [WLAN Profile Name] ドロップダウン リストに表示されます。

- [Local Split ACL] ドロップダウン リストから、FlexConnect ACL を選択します。

（注）　中央でスイッチされる WLAN に関連付けられた WAN リンクに接続するクライアントが、ローカル サイトに存在するデバイスに一部のトラフィックを送信する必要がある場合、クライアントは、CAPWAP 経由でトラフィックをコントローラに送信し、CAPWAP 経由または帯域外の接続を使用して、ローカル サイトに同じトラフィックを戻す必要があります。このプロセスは不必要に WAN リンク帯域幅を消費します。この問題を回避するには、パケットの内容に基づいたクライアントによる送信トラフィックの分類を可能にする、スプリット トンネリング機能を使用できます。一致するパケットはローカルでスイッチされ、残りのトラフィックは中央でスイッチされます。ローカル サイトに存在するデバイスの IP アドレスと一致するクライアントによって送信されるトラフィックを、ローカルでスイッチされるトラフィックとして分類し、残りのトラフィックを中央でスイッチされるトラフィックとして分類できます。

[Select APs] タブ

[Search APs] ドロップダウン リストを使用して、[Last Applied AP(s)]、[Scheduled AP(s)]、[All]、[All Mesh MAP AP(s)]、[All Mesh RAP AP(s)]、[By Controller]（ドロップダウン リストからコントローラを選択）、[By Controller Name]（ドロップダウン リストからコントローラ名を選択）、[By Floor Area]（ドロップダウン リストからキャンパス、ビルディングおよびフロアを選択）、[By Outdoor Area]（ドロップダウン リストからキャンパスおよび屋外領域を選択）、[By Model]（ドロップダウン リストからモデルを選択）、[By AP MAC Address]（MAC アドレスを入力）、[By AP Name]（完全な AP 名または AP 名の開始文字を入力）および [By AP IP Address Range]（IP アドレスを入力）を検索します。

（注）　IP アドレス検索の入力テキストは、X.X.X.* または X.X.X.[0-255] の 2 つの形式を使用できます。たとえば、10.10.10.* または 10.10.10.[20-50] は、10.10.10.10 ～ 10.10.10.50 IP アドレス範囲の AP を検索します。

（注）　[All Applied APs] および [Scheduled APs] 検索フィルタは、過去 24 時間の AP データを一覧表示します。

（注）　[AP(s) unassigned to Map(s)] 検索フィルタは、マッピングに割り当てられていない AP をリストします。

- [Save] をクリックして、パラメータ選択を保存します。
- [Apply] をクリックして、検索から選択したアクセス ポイントに [AP/Radio] パラメータを保存および適用します。

[Apply/Schedule] タブ

現在のテンプレートを保存、現在のテンプレートをすぐに適用、または適切な時間にプロビジョニングを開始するように現在のテンプレートをスケジュールできます。

- [Save] : [Save] をクリックして、現在のテンプレート設定を保存します。
- [Apply] : [Apply] をクリックして、テンプレートを保存して、選択アクセス ポイントへのテンプレートのプロビジョニングを開始します。

（注）　ページから移動し、Prime Infrastructure からログアウトした場合でも、このプロビジョニング プロセスは完了するまで続行します。

- [Schedule]：スケジュールした時間にプロビジョニングを設定および開始できます。
  - [Enable schedule]：[Enable schedule] チェックボックスをオンにして、スケジュール機能をアクティブにします。
  - [Start Date]：テキスト ボックスに開始日を入力するか、カレンダーのアイコンを使用して開始日を選択します。
  - [Start Time]：開始時刻を、[hours] および [minutes] ドロップダウン リストを使用して選択します。
  - [Recurrence]：[no recurrence]、[hourly]、[daily] または [weekly] から選択して、プロビジョニングの発生頻度を指定します。プロビジョニングの発生頻度（日数）を入力します。
  - [Schedule]：[Schedule] をクリックして、スケジューリングした時間にプロビジョニングを開始します。

[Report] タブ

最近適用されたすべてのレポートを、適用ステータスおよび適用日時とともに表示します。各アクセス ポイントに関する次の情報が表示されます。

- [Status]：Success（成功）、Partial Success（一部成功）、Failure（失敗）、Not Initiated（未開始）を示します。失敗した、または一部成功したプロビジョニングでは、[Details] をクリックして失敗の詳細（失敗したプロビジョニングおよび失敗した理由など）を表示できます。
- [Ethernet MAC]：該当するアクセス ポイントのイーサネット MAC アドレスを示します。
- [Controller]：該当するアクセス ポイントのコントローラ IP アドレスを示します。
- [Map]：アクセス ポイントのマップの位置を示します。

（注）　[Report] ページ下部の [click here] リンクをクリックして、スケジュールされたタスク レポートを表示します。

現在の Lightweight アクセス ポイント テンプレートの編集

現在の Lightweight アクセス ポイント テンプレートを編集するには、次の手順を実行します。

ステップ 1　[Configure] > [Lightweight AP Configuration Templates] を選択します。

ステップ 2　[Template Name] 列で該当するテンプレートをクリックします。

ステップ 3　次のタブで必要なパラメータを編集します。

- [AP Parameters]：適用する必要があるアクセス ポイント パラメータのチェックボックスをオンにします。
- Mesh
- [802.11a/n Parameters]：適用する必要がある 802.11a/n パラメータのチェックボックスをオンにします。

- [802.11b/g/n Parameters]：適用する必要がある 802.11b/g/n パラメータのチェックボックスをオンにします。
- [APs] を選択します
  - [Search APs] ドロップダウン リストを使用して、[Last Applied APs]、[All APs]、[All MAP(s)] または [All RAP(s)] を検索します。
  - [Save] をクリックして、パラメータ選択を保存します。
  - [Apply] をクリックして、検索から選択したアクセス ポイントに [AP/Radio] パラメータを保存および適用します。
  - [Apply Report]：適用テンプレートからレポートを表示します。

Autonomous アクセス ポイント テンプレートの設定

[Configuring] > [Autonomous Access Point Templates] ページでは、Autonomous アクセス ポイントの CLI テンプレートを設定できます。

ここでは、次の内容について説明します。

- 「新しい Autonomous アクセス ポイント テンプレートの設定」（P.11-747）
- 「AP 設定テンプレートの Autonomous アクセス ポイントへの適用」（P.11-747）
- 「現在の Autonomous AP 移行テンプレートの編集」（P.11-751）

新しい Autonomous アクセス ポイント テンプレートの設定

新しい Autonomous アクセス ポイント テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Configure] > [Autonomous AP Configuration Templates] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　テンプレート名を入力します。

ステップ 5　該当する CLI コマンドを入力します。

（注）　show コマンドは [CLI commands] テキスト ボックスに含めないでください。show コマンドはサポートされていません。

ステップ 6　[Save] をクリックします。

AP 設定テンプレートの Autonomous アクセス ポイントへの適用

AP 設定テンプレートを Autonomous アクセス ポイントに適用するには、次の手順を実行します。

ステップ 1　[Configure] > [Autonomous AP Configuration Templates] を選択します。

ステップ 2　テンプレート名リンクをクリックして、テンプレートを選択して、Autonomous アクセス ポイントに適用します。[New Autonomous AP Configuration template] ページが表示されます。

ステップ 3　テンプレート名を入力します。

ステップ 4　該当する CLI コマンドを入力します。

ステップ 5　[Save] をクリックします。

ステップ 6　[Apply to Autonomous Access Points] をクリックします。[Apply to Autonomous Access Points] ページが表示されます。

ステップ 7　目的の Autonomous アクセス ポイントを選択します。

ステップ 8　[OK] をクリックします。

（注）　[Ignore errors on Apply template to Controllers] チェックボックスをオンにすると、エラーを無視して、テンプレートのすべてのコマンドを Autonomous AP に適用できます。このチェックボックスがオフの場合、テンプレートのコマンドを Autonomous AP に適用するときにエラーが発生すると、残りのコマンドは適用されません。

テンプレート結果の表示

Autonomous AP 設定テンプレートをアクセス ポイントに適用するときの結果を表示するには、次の手順を実行します。

ステップ 1　[Configure] > [AP Configuration Templates] > [Autonomous AP] を選択します。

ステップ 2　テンプレート名リンクをクリックして、テンプレートを選択して、Autonomous アクセス ポイントに適用します。[Autonomous AP Configuration template] ページが表示されます。

ステップ 3　テンプレート名を入力します。

ステップ 4　該当する CLI コマンドを入力します。

ステップ 5　[Save] をクリックします。

ステップ 6　[Apply to Autonomous Access Points] をクリックします。[Apply to Autonomous Access Points] ページが表示されます。

ステップ 7　目的の Autonomous アクセス ポイントを選択します。

ステップ 8　[OK] をクリックします。[Template Results] ページが表示されます。次のパラメータが表示されます。

- [IP Address]：アクセス ポイントの IP アドレス。
- [AP Name]：アクセス ポイントの名前。
- [Apply Status]：Success（成功）、Failure（失敗）、Initiated（開始）または Not Initiated（未開始）を示します。
- [Operation Status]：動作ステータス、[Success] または [Failure] を表示します。
- [Reason]：失敗した理由を示します。
- Session Output

スイッチ位置設定テンプレートの設定

スイッチ位置設定テンプレートを使用して、スイッチの位置テンプレートを設定できます。

スイッチの位置テンプレートを設定するには、次の手順を実行します。

ステップ 1　[Prime Infrastructure] > [Configure] > [Switch Location Configuration Template] の順に選択します。

[Switch Location Configuration template] ページが表示されます。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Template] を選択し、[Go] をクリックします。

[New Template] ページが表示されます。

表 11-4 に、[New Template] ページのフィールドを一覧で表示します。

表 11-4　[New Template] ページのフィールド

フィールド	説明
General	
Template Name	テンプレートの名前。
Map Location	
Campus	スイッチまたはスイッチ ポートのマップ位置のキャンパスを選択します。
Building	スイッチまたはスイッチ ポートのマップ位置のビルディングを選択します。
Floor	スイッチまたはスイッチ ポートのマップ位置のフロアを選択します。
Import	選択したキャンパス、ビルディングおよびフロアの Civic 情報をインポートします。
ELIN and Civic Location	
ELIN	緊急ロケーション識別番号。
[Civic Address] タブ	スイッチ/スイッチ ポートで使用できる Civic 住所情報。
[Advanced] タブ	スイッチ/スイッチ ポート位置に関する詳細情報。
NMSP	スイッチの NMSP を有効または無効にするには、このチェックボックスをオンまたはオフにします。
ボタン	
Save	テンプレートを保存します。
Cancel	テンプレート作成を廃棄します。

Autonomous AP 移行テンプレートの設定

ここでは、次の内容について説明します。

- 「Autonomous アクセス ポイントの Lightweight アクセス ポイントへの移行」（P.11-750）

- 「Cisco IOS アクセス ポイントの現在のステータスの表示」（P.11-755）

Autonomous アクセス ポイントの Lightweight アクセス ポイントへの移行

Autonomous ソリューションから Unified アーキテクチャへ移行するには、Autonomous アクセス ポイントを Lightweight アクセス ポイントへ変換する必要があります。移行ユーティリティは、既存テンプレートが一覧に記載されている [Configure] > [Autonomous AP Migration Templates] ページから使用できます。

[Autonomous AP Migration Templates] リスト ページには、次の情報が表示されます。

- [Name]：テンプレート名。
- [Description]：テンプレートの説明。
- [AP Count]：移行に選択された Autonomous アクセス ポイントの数。
- [Schedule Run]：タスクの実行スケジュール時刻。
- [Status]：次のいずれかのタスク ステータスを示します。
  - [Not initiated]：テンプレートの移行が未開始ですが、スケジュールされた時刻に開始します。
  - [Disabled]：テンプレートが無効で、スケジュールされた時刻に実行しません。これは、Autonomous アクセス ポイントを選択せずに作成された場合のテンプレートのデフォルト状態です。
  - [Expired]：テンプレートは、スケジュールされた時刻に実行しませんでした（Prime Infrastructure サーバがダウンしていた可能性があります）。
  - [Enabled]：テンプレートの移行が未開始ですが、スケジュールされた時刻に開始します。
  - [In progress]：テンプレートは、現在、選択した Autonomous アクセス ポイントを CAPWAP に変換しています。
  - [Success]：テンプレートは、Autonomous アクセス ポイントの CAPWAP への移行を正常に完了しました。
  - [Failure]：テンプレートは、選択された Autonomous アクセス ポイントから CAPWAP へのすべての移行に失敗しました。[View Migration Status] ページを使用して、失敗の詳細ステータスを確認できます。
  - [Partial Success]：テンプレートは、選択された Autonomous アクセス ポイントから CAPWAP へのサブセットの移行に失敗しました。[View Migration Status] ページを使用して、失敗の詳細ステータスを確認できます。

（注）　これらの状態では、[Name] リンクをクリックして、テンプレートを編集できます。

（注）　アクセス ポイントを Lightweight に変換すると、アクセス ポイントの前のステータスまたは設定は保持されません。

[Select a command] ドロップダウン リストから、次の機能を実行できます。

- [Add Template]：移行に関する必要な情報を提供できます。
- [Delete Templates]：現在のテンプレートを削除できます。

- [View Migration Report]：AP アドレス、移行ステータス（進行中または失敗）、タイムスタンプ、詳細なログへのリンクなどの情報を表示できます。
- [View Current Status]：現在の移行の進捗状況を表示できます（3 秒ごとに更新）。

（注）　すでに管理されている Autonomous アクセス ポイントを LWAPP へ移行する場合には、その位置とアンテナの情報も移行されます。情報を再入力する必要はありません。Prime Infrastructure では、移行後に自律アクセス ポイントは自動的に削除されます。

- [View Migration Analysis Summary]：アクセス ポイント変換に応じて、成功または失敗を一覧で示します。変換できるのは、すべての基準が成功であるアクセス ポイントだけです。

（注）　[Migration Analysis] オプションは、デフォルトでは、検出中に実行されません。検出中に移行分析を実行する場合、[Administration] > [Settings] > [CLI Session] の順に選択して、このオプションを有効にします。

（注）　Prime Infrastructure は、CAPWAP アクセス ポイントへの自律アクセス ポイントの移行もサポートしています。

現在の Autonomous AP 移行テンプレートの編集

現在の移行テンプレートを編集するには、次の手順を実行します。

ステップ 1　[Configure] > [Autonomous AP Migration Templates] を選択します。

ステップ 2　[Name] 列で移行テンプレートをクリックします。

ステップ 3　必要なパラメータを編集します。

- General
  - [Name]：移行テンプレートのユーザ定義名を示します。
  - [Description]：移行テンプレートを識別できるような簡単な説明を入力します。
- Upgrade Options
  - [DHCP Support]：クリックして、Dynamic Host Configuration Protocol サポートを有効にします。変換後にすべてのアクセス ポイントが DHCP サーバから IP を取得したことを確認します。
  - [Retain AP HostName]：クリックすると、このアクセス ポイントに対して同じホスト名を保持できます。

（注）　AP から CAPWAP に初めて移行する場合だけ、ホスト名が CAPWAP で維持されます。AP のアップグレードを複数回行っている場合、ホスト名が維持されない場合があります。Autonomous アクセス ポイントのホスト名が 32 文字を超えると、CAPWAP アクセス ポイントのホスト名は default に設定されます。

（注）　アクセス ポイントを 12.3(11)JA、12.3(11)JA1、12.3(11)JA2、12.3(11)JA3 Autonomous イメージから LWAPP にアップグレードする場合、変換されるアクセス ポイントは、スタティック IP アドレス、ネットマスク、ホスト名およびデフォルト ゲートウェイを維持しない場合があります。

- [Migrate over WANLink]：このオプションを有効にする場合、*env_vars* ファイルにリモート TFTP サーバ位置が保存されます。この情報は、AP にコピーされます。このオプションが選択されていない場合、Prime Infrastructure 内部 TFTP サーバを使用して、*env_vars* ファイルが AP にコピーされます。
- [DNS address]：DNS アドレスを入力します。
- [Domain Name]：ドメイン名を入力します。

- Controller Details

（注）　アクセス ポイントの許可情報（SSC）をこのコントローラ上で設定でき、変換されたアクセス ポイントが接続できることを確認してください。

- Controller IP
- AP Manager IP
- User Name
- Password

- TFTP Details
  - TFTP Server IP
  - File Path
  - File Name
- Schedule Details
  - Apply Template
  - [Notification]（任意）

ステップ 4　[Save] をクリックします。

移行分析概要の表示

移行分析概要を表示するには、次の手順を実行します。

（注）　移行分析概要は、[Tools] > [Migration Analysis] を選択して表示することもできます。

ステップ 1　[Configure] > [Autonomous AP Migration Templates] を選択します。

ステップ 2　[Select a Command] ドロップダウン リストから [View Migration Analysis Summary] を選択し、[Go] をクリックします。[Migration Analysis Summary] ページが表示されます。

Autonomous アクセス ポイントは、すべての基準が成功ステータスの場合だけ移行できます。赤の X マークは移行できないことを示し、緑のチェックマークは移行できることを示します。これらの列は次のものを表しています。

- [Privilege 15 Criteria] : Autonomous アクセス ポイントの検出の一部として指定された Telnet クレデンシャルは、特権 15 であることが必要です。
- [Software Version Criteria] : 変換は、12.3(11)JA、12.3(11)JA1、12.3(11)JA2 および 12.3(11)JA3 を除く Cisco IOS リリース 12.3(7)JA だけでサポートされます。
- [Role Criteria] : アソシエーション要求を送信するには、アクセス ポイントとコントローラの間の有線接続が必要です。そのため、次の Autonomous アクセス ポイント ロールが必要です。
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- [Radio Criteria] : デュアル無線アクセス ポイントの場合、1 つの無線の種類のみがサポートされている場合でも変換を実行できます。

移行テンプレートの追加と変更

移行テンプレートを追加する場合、[Configure] > [Autonomous AP Migration Templates] ページの [Select a command] ドロップダウン リストから [Add Template] を選択します。

既存テンプレートを変更するには、概要リストのテンプレート名をクリックします。

次の移行パラメータを入力または変更します。

General

- [Name] : この移行テンプレートのユーザ定義の名前。
- [Description] : 移行テンプレートを識別できるような簡単な説明。

Upgrade Options

- [DHCP Support] : 変換後にすべてのアクセス ポイントが DHCP サーバから IP を取得したことを確認します。
- [Retain AP HostName] : このアクセス ポイントに対して同じホスト名を保持できます。
- [Migrate over WANLink] : アクセス ポイントで実行される CLI コマンドのデフォルトのタイムアウトを延長します。
- DNS Address
- [Domain Name]

Controller Details

（注）　アクセス ポイントの許可情報（SSC）をこのコントローラ上で設定でき、変換されたアクセス ポイントが接続できることを確認してください。

- [Controller IP] : 新しく移行するアクセス ポイントに追加する WLAN コントローラの IP アドレスを入力します。
- [AP Manager IP] : アクセス ポイント マネージャ IP アドレスを入力することで、アクセス ポイントが接続するコントローラを指定します。

（注）　SSC 対応アクセス ポイントの場合、この IP アドレスは、コントローラ IP フィールドと同じにする必要があります。MIC 対応アクセス ポイントの場合、IP アドレスが一致する必要はありません。

- [User Name]：WLAN コントローラにログインするための有効なユーザ名を入力します。
- [Password]：WLAN コントローラへのログイン時に使用されるこのユーザ名に対する有効なパスワードを入力します。

TFTP Details

Prime Infrastructure は、インストールおよびセットアップ中に独自の TFTP および FTP サーバを提供します。

- [TFTP Server IP]：Prime Infrastructure サーバの IP アドレスを入力します。
- [File Path]：Prime Infrastructure 設定時に定義された TFTP ディレクトリを入力します。
- [File Name]：Prime Infrastructure 設定時に TFTP ディレクトリで定義された CAPWAP 変換ファイルを入力します（例：c1240-rcvk9w8-tar.123-11JX1.tar）。

Schedule Details

このグループ ボックスでは、移行テンプレートのスケジュール オプションを指定できます。

- [Apply Template]：移行のテンプレートを適用するときのオプションを選択します。
  - [Now]：このオプションを選択して、移行タスクをすぐに実行します。
  - [Schedule for later date/time]：移行を後でスケジューリングする場合、[Schedule] パラメータを入力します。テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。レポートは、この日付のこの時刻に実行を開始します。
- （任意）[Notification]：電子メールで通知を送信する受信者の電子メール アドレスを入力します。

（注）　電子メール通知を受信するには、[Administration] > [Settings] > [Mail Server Configuration] ページで Prime Infrastructure メール サーバを設定します。

- [Save] をクリックします。

テンプレートを Prime Infrastructure に追加すると、次の追加ボタンが表示されます。

- [Select APs]：このオプションを選択すると、変換のためのアクセス ポイントを選択する Prime Infrastructure の Autonomous アクセス ポイントの一覧が表示されます。変換できるのは、移行基準が*成功*であるアクセス ポイントだけです。
- [Select File]：変換用のアクセス ポイントの CSV 情報が表示されます。

移行テンプレートのコピー

移行テンプレートをコピーするには、次の手順を実行します。

ステップ 1　[Configure] > [Autonomous AP Migration Templates] を選択します。

ステップ 2　コピーするテンプレートのチェックボックスをオンにして、[Select a command] ドロップダウン リストから [Copy Template] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　現在のテンプレートのコピー先となる新しいテンプレートの名前を入力します。

移行テンプレートの削除

移行テンプレートを削除するには、次の手順を実行します。

ステップ 1　[Configure] > [Autonomous AP Migration Templates] を選択します。

ステップ 2　削除するテンプレートのチェックボックスをオンにして、[Select a command] ドロップダウン リストから [Delete Templates] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　[OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてテンプレートを削除せずにこのページを閉じます。

Cisco IOS アクセス ポイントの現在のステータスの表示

[Autonomous AP Migration Templates] ページの [Select a command] ドロップダウン リストから [View Current Status] を選択して、Cisco IOS アクセス ポイント移行のステータスを表示します。

次の情報が表示されます。

- [IP Address] : アクセス ポイントの IP アドレス。
- [Status] : 移行の現在のステータス。
- [Progress] : 移行の進捗状況の概要。

移行できないアクセス ポイントの無効化

変換できないことを示すラベルが付いている Autonomous アクセス ポイントは無効にすることができます。

FlexConnect の設定

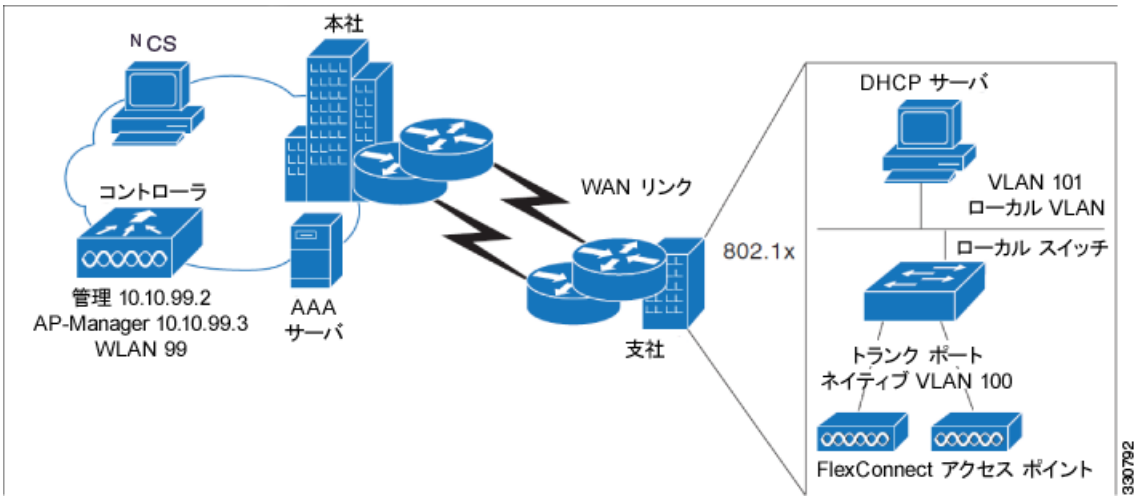
この章では、FlexConnect、およびこの機能をコントローラとアクセス ポイント上で設定する方法について説明します。ここで説明する内容は、次のとおりです。

FlexConnect について

FlexConnect は、ブランチ オフィスおよびリモート オフィスに導入されるソリューションです。これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスから Wide Area Network（WAN; ワイドエリア ネットワーク）経由で、支社またはリモート オフィスのアクセス ポイントを設定および制御できるようになります。ロケーションごとに導入できる FlexConnect のアクセス ポイント数は無制限です。FlexConnect アクセス ポイントは、クライアント データ トラフィックをローカルで切り替えて、コントローラへの接続が失われるとクライアント認証をローカルで実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

FlexConnect がサポートされているのは、1130AG、1240AG、1142 および 1252 アクセス ポイント、2000 および 4400 シリーズ コントローラ、Catalyst 3750G Integrated Wireless LAN Controller Switch、Cisco WiSM、Integrated Services Routers 用コントローラ ネットワーク モジュール、および Catalyst 3750G Integrated Wireless LAN Controller Switch 内のコントローラだけです。図 12-1 に一般的な FlexConnect の導入方法を示します。

図 12-1　FlexConnect の導入



ここでは、次の内容について説明します。

- 「FlexConnect 認証プロセス」（P.12-758）
- 「FlexConnect ガイドライン」（P.12-760）

FlexConnect 認証プロセス

FlexConnect アクセス ポイントは、ブート時にコントローラを検索します。コントローラが見つかると、そのコントローラに接続し、コントローラから最新のソフトウェアのイメージと設定情報をダウンロードし、無線を初期化します。スタンドアロン モードで使用するために、ダウンロードした設定を不揮発性メモリに保存します。

FlexConnect アクセス ポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- アクセス ポイントが IP アドレスを DHCP サーバから割り当てられている場合、通常の CAPWAP 検出プロセス（レイヤ 3 ブロードキャスト、無線プロビジョニング（OTAP）、DNS、または DHCP オプション 43）によりコントローラを検出します。

（注）　OTAP は、購入後初のブート時には動作しません。

- アクセス ポイントが静的 IP アドレスを割り当てられている場合、DHCP オプション 43 を除く CAPWAP 検出プロセスのメソッドのいずれかを使用してコントローラを検出できます。アクセス ポイントがレイヤ 3 ブロードキャストでも OTAP でもコントローラを検出できない場合は、DNS 解決を使用することを推奨します。DNS を使用すれば、固定 IP アドレスを持ち DNS サーバを認識しているアクセス ポイントは、最低 1 つのコントローラを見つけることができます。
- アクセス ポイントで CAPWAP 検出メカニズムを使用できないリモート ネットワークからコントローラを検出させる場合には、プライミングを使用できます。この方法を使用すると、アクセス ポイントの接続先のコントローラを（アクセス ポイントのコマンドライン インターフェイスにより）指定できます。

FlexConnect アクセス ポイントがコントローラに到達できるとき（*接続済みモード*と呼ばれます）、コントローラはクライアント認証を支援します。FlexConnect アクセス ポイントがコントローラにアクセスできないとき、アクセス ポイントはスタンドアロン モードに入り、独自にクライアントを認証します。

（注）　アクセス ポイント上の LED は、デバイスが異なる FlexConnect モードに入るときに変化します。LED パターンの情報については、アクセス ポイントのハードウェア インストール ガイドを参照してください。

クライアントが FlexConnect アクセス ポイントにアソシエートするとき、アクセス ポイントではすべての認証メッセージをコントローラに送信し、WLAN 設定に応じて、クライアント データ パケットをローカルにスイッチする（ローカル スイッチング）か、コントローラに送信（中央スイッチング）します。クライアント認証（オープン、共有、EAP、Web 認証、および NAC）とデータ パケットに関して、WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- **中央認証、中央スイッチング**：この状態では、コントローラがクライアント認証を処理し、すべてのクライアント データがコントローラにトンネル バックします。この状態は、接続済みモードの場合にだけ有効です。
- **中央認証、ローカル スイッチング**：この状態では、コントローラがクライアント認証を処理し、FlexConnect アクセス ポイントがデータ パケットをローカルにスイッチします。クライアントが認証に成功した後、コントローラは新しいペイロードとともにコンフィギュレーション コマンドを送信し、FlexConnect アクセス ポイントに対して、ローカルにデータ パケットのスイッチを始めるように指示します。このメッセージはクライアントごとに送信されます。この状態は接続モードにのみ適用されます。
- **ローカル認証、ローカル スイッチング**：この状態では、FlexConnect アクセス ポイントがクライアント認証を処理し、クライアント データ パケットをローカルにスイッチします。この状態はスタンドアロン モードおよび接続済みモードの場合に有効です。

  ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位（MTU）が 500 バイトを下回らない、最小帯域幅が 128 kbps のリモート オフィス設定の基準を維持できない場合に役立ちます。ローカル スイッチングでは、認証機能はアクセス ポイント自体に存在します。そのため、ローカル認証によって、ブランチ オフィスの遅延要件が軽減されます。

（注）　ローカル認証は、ローカル スイッチング モードの FlexConnect アクセス ポイントの WLAN 上のみで有効にできます。

  ローカル認証は、次のシナリオではサポートされません。

  - FlexConnect ローカル認証を有効にした WLAN では、ゲスト認証は実行できません。
  - RRM 情報は、FlexConnect ローカル認証を有効にした WLAN のコントローラでは使用不可です。
  - ローカル RADIUS はサポートされません。
  - クライアントがいったん認証されると、ローミングは WLC の後でのみサポートされ、グループ内の他の FlexConnect は、クライアント情報で更新されます。

- **認証ダウン、スイッチング ダウン**：この状態になると、WLAN は既存クライアントのアソシエートを解除し、ビーコン応答とプローブ応答の送信を停止します。この状態はスタンドアロン モードでのみ有効です。
- **認証ダウン、ローカル スイッチング**：WLAN は新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。この状態はスタンドアロン モードでのみ有効です。

FlexConnect アクセス ポイントがスタンドアロン モードに入ったときに、WLAN がオープン、共有、WPA-PSK、または WPA2-PSK 認証を行うように設定されている場合は、WLAN は「ローカル認証、ローカル スイッチング」状態に入り、引き続き新しいクライアントの認証を行います。その他の WLAN は、「認証ダウン、スイッチング ダウン」状態（WLAN が中央スイッチングに設定されている場合）または「認証ダウン、ローカル スイッチング」状態（WLAN がローカル スイッチングに設定されている場合）に入ります。

FlexConnect アクセス ポイントがスタンドアロン モードに入ると、中央スイッチング WLAN 上にあるすべてのクライアントのアソシエートが解除されます。802.1X または Web 認証 WLAN の場合、既存クライアントはアソシエートを解除されませんが、FlexConnect アクセス ポイントはアソシエートされたクライアントの数がゼロ（0）になると、ビーコンの送信を停止します。また、802.1X または Web 認証 WLAN にアソシエートしている新規クライアントへアソシエート解除のメッセージを送信します。802.1X 認証、NAC、および Web 認証（ゲスト アクセス）などのコントローラ依存アクティビティは無効になり、アクセス ポイントはコントローラに侵入検知システム（IDS）レポートを送信しません。さらに、ほとんどの無線リソース管理（RRM）機能（ネイバー探索、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバー リストの使用、不正の封じ込めおよび検出）は無効化されます。ただし、FlexConnect アクセス ポイントではスタンドアロン モードで動的周波数選択がサポートされています。

（注）　コントローラに Network Access Control（NAC）が設定されている場合、クライアントはアクセス ポイントが接続済みモードのときだけアソシエートできます。NAC が有効化されているときは、正常に動作しない VLAN（または隔離 VLAN）を作成してください。この VLAN に割り当てられたクライアントのデータ トラフィックがコントローラを経由するようにするためです。これは、WLAN がローカル スイッチングを行うように設定されている場合でも必要です。クライアントが隔離 VLAN に割り当てられると、そのクライアントのデータ パケットはすべて中央でスイッチングされます。

FlexConnect アクセス ポイントは、スタンドアロン モードに入った後も、クライアントの接続を維持します。ただし、アクセス ポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエート解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

FlexConnect ガイドライン

FlexConnect を使用する際は、次のガイドラインを考慮します。

- FlexConnect アクセス ポイントを導入するときは、固定 IP アドレスと DHCP アドレスのいずれも使用できます。DHCP の場合、DHCP サーバはローカルに使用可能であり、ブート時にアクセス ポイントの IP アドレスを提供できる必要があります。
- FlexConnect は、最小 500 バイトの最大伝送単位（MTU）の WAN リンクをサポートします。
- アクセス ポイントとコントローラの間のラウンドトリップ遅延が 300 ミリ秒（ms）を超えてはなりません。また、CAPWAP コントロール パケットは他のすべてのトラフィックよりも優先される必要があります。これを実現できない場合は、アクセス ポイントを設定してローカル認証を実行できます。ローカル認証およびローカル スイッチングを使用する FlexConnect ローカル認証の詳細については、「FlexConnect 認証プロセス」（P.12-758）を参照してください。
- コントローラはユニキャスト パケットまたはマルチキャスト パケットの形式でアクセス ポイントにマルチキャスト パケットを送信できます。FlexConnect モードでは、アクセス ポイントはマルチキャスト パケットをユニキャスト形式以外では受信しません。
- FlexConnect は CCKM 完全認証をサポートしますが、CCKM 高速ローミングをサポートしません。

- FlexConnect は 1 対 1 のネットワーク アドレス変換（NAT）設定をサポートします。また、真のマルチキャストを除くすべての機能に対してポート アドレス変換（PAT）もサポートします。NAT 境界を越えるマルチキャストもサポートされます（ユニキャスト オプションを使用して設定されている場合）。
- VPN、IPsec、L2TP、PPTP、Fortress 認証、および Cranite 認証は、これらのセキュリティ タイプがアクセス ポイントにおいてローカルでアクセスできれば、ローカル スイッチングのトラフィックに対してサポートされます。

FlexConnect の設定

FlexConnect を設定するには、この項の手順を記載順に実行します。ここでは、次の内容について説明します。

リモート サイトでのスイッチの設定

リモート サイトでスイッチを準備するには、次の手順を実行します。

ステップ 1　FlexConnect が有効になっているアクセス ポイントを、スイッチ上のトランクまたはアクセス ポートに接続します。

（注）　次に示す設定例では、FlexConnect アクセス ポイントはスイッチ上のトランク ポートに接続されます。

ステップ 2　次の設定例に従って、FlexConnect アクセス ポイントをサポートするようにスイッチを設定します。

この設定例では、FlexConnect アクセス ポイントは、トランク インターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。このアクセス ポイントは、このネイティブ VLAN 上での IP 接続を必要とします。リモート サイトのローカル サーバとリソースは、VLAN 101 上にあります。DHCP プールがスイッチの両 VLAN のローカル スイッチ内に作成されます。最初の DHCP プール（ネイティブ）は FlexConnect アクセス ポイントにより使用され、2 つ目の DHCP プール（ローカル スイッチング）は、クライアントがローカルでスイッチされる WLAN にアソシエートする場合、クライアントにより使用されます。設定例の太字のテキストは、これらの設定を示します。

（注）　この設定例のアドレスは、図示のみを目的としています。使用するアドレスは、アップストリーム ネットワークに適合している必要があります。

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
```

```
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

FlexConnect に対するコントローラの設定

この項では、FlexConnect に対するコントローラの設定手順について説明します。FlexConnect のコントローラの設定には、中央スイッチング VLAN とローカル スイッチング VLAN を作成する操作が含まれます。この手順では、次の 3 つの WLAN を例として使用します。

WLAN	セキュリティ	スイッチング	インターフェイス マッピング（VLAN）
employee	WPA1+WPA2	中央	management（中央でスイッチされる VLAN）
employee-local	WPA1+WPA2（PSK）	ローカル	101（ローカル スイッチング VLAN）
guest-central	Web 認証	中央	management（中央でスイッチされる VLAN）

中央スイッチングの WLAN を作成するには、次の手順を実行します。例では、これは最初の WLAN（employee）です。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　[IP Address] 列から目的のコントローラをクリックします。

ステップ 3　[WLANs] > [WLAN Configuration] を選択し、[WLAN Configuration] ページにアクセスします。

ステップ 4　[Select a command] ドロップダウン リストから [Add a WLAN] を選択し、[Go] をクリックします。

（注）　Cisco アクセス ポイントは、コントローラごとに最大 16 の WLAN をサポートします。ただし Cisco アクセス ポイントの中には、8 より大きい WLAN ID を持つ WLAN をサポートしないものがあります。この場合、WLAN を作成しようとすると、「Not all types of AP support WLAN ID greater than 8, do you wish to continue?」というメッセージが表示されます。[OK] をクリックすると、次に使用可能な WLAN ID を持つ WLAN が作成されます。ただし、8 より小さい WLAN ID を持つ WLAN を削除すると、削除した WLAN の WLAN ID が、次に作成される WLAN に適用されます。

ステップ 5　このコントローラにテンプレートを適用する場合には、ドロップダウン リストからテンプレート名を選択します。テンプレートの設定方法に応じて、フィールドが読み込まれます。新しい WLAN テンプレートを作成するには、[click here] リンクをクリックしてテンプレート作成ページにリダイレクトします（「WLAN テンプレートの設定」（P.11-620）を参照）。

ステップ 6　この WLAN の設定パラメータを変更します。この employee WLAN の例では、[Layer 2 Security] ドロップダウン リストから [WPA1+WPA2] を選択する必要があります。

ステップ 7　[General Policies] の下にある [Status] チェックボックスをオンにして、この WLAN を必ず有効にします。

（注）　NAC が有効で、これで使用するために隔離 VLAN が作成されている場合には、[General Policies] の下にある [Interface] ドロップダウン リストから必ずこれを選択します。また、[Allow AAA Override] チェックボックスをオンにして、コントローラが確実に隔離 VLAN 割り当てを検証するようにします。

ステップ 8　[Save] をクリックして変更をコミットします。

ステップ 9　ローカルにスイッチされる WLAN を作成する手順は次のとおりです。例では、これは 2 番めの WLAN（employee-local）です。

a. ステップ のサブステップに従って、新しい WLAN を作成します。例では、この WLAN の名前は「employee-local」です。

b. 元の [WLAN] ページで [WLAN ID] をクリックして、[WLANs edit] ページへ移動します。この WLAN の設定パラメータを変更します。この employee WLAN の例では、[Layer 2 Security] ドロップダウン リストから [WPA1+WPA2] を選択する必要があります。必ず [PSK authentication key management] を選択して、事前共有キーを入力します。

（注）　[Admin Status] チェックボックスをオンにして、この WLAN を必ず有効にします。また、[FlexConnect Local Switching] チェックボックスをオンにして、ローカル スイッチングを必ず有効にします。ローカル スイッチングを有効にすると、この WLAN をアドバタイズする FlexConnect アクセス ポイントはデータ パケットをローカルでスイッチできます（データ パケットをコントローラにトンネルしない）。

（注）　FlexConnect アクセス ポイントの場合、FlexConnect ローカル スイッチングに対して設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとしてアクセス ポイントで継承されます。これは SSID ごと、FlexConnect アクセス ポイントごとに簡単に変更できます。FlexConnect 以外のアクセス ポイントでは、すべてのトラフィックがトンネルを通じてコントローラに戻され、VLAN タギングは WLAN の各インターフェイス マッピングによって決定されます。

c. [Save] をクリックして変更をコミットします。

ステップ 10　ゲスト アクセスに使用される中央スイッチングの WLAN も作成する場合は、次の手順に従ってください。例では、これは 3 番めの WLAN（guest-central）です。中央サイトからの保護されていないゲスト トラフィックに対する企業データ ポリシーを施行できるように、ゲスト トラフィックをコントローラにトンネリングする必要のある場合があります。

a. ステップ のサブステップに従って、新しい WLAN を作成します。例では、この WLAN の名前は「guest-central」です。

b. [WLANs Edit] ページで、この WLAN の設定パラメータを変更します。employee WLAN の例では、[Security] タブの [Layer 2 Security] および [Layer 3 Security] ドロップダウン リストから [None] を選択し、[Web Policy] チェックボックスをオンにして、[Authentication] が選択されていることを確認します。

（注）　外部 Web サーバを使用する場合、事前認証アクセス コントロール リスト（ACL）をサーバの WLAN 上に設定してから、この ACL を WLAN の事前認証 ACL として選択する必要があります。

c. [Status] チェックボックスをオンにして、これを必ず有効にします。

d. [Save] をクリックして変更をコミットします。

e. ゲスト ユーザがこれにアクセスしたとき最初に表示されるログイン ページのコンテンツと外観をカスタマイズする場合は、「Web 認証テンプレートの設定」（P.11-667）の手順に従ってください。

f. この WLAN にローカル ユーザを追加するには、[Configure] > [Controller Template Launch Pad] を選択します。

g. 左側のサイドバーのメニューから、[Security] > [Local Net Users] を選択します。

h. [Local Net Users] ページが表示されたら、[Select a command] ドロップダウン リストから [Add Template] を選択して、[Go] をクリックします。

i. [Import from File] チェックボックスをオフにします。

j. ローカル ユーザのユーザ名とパスワードを入力します。

k. [Profile] ドロップダウン リストから、適切な SSID を選択します。

l. ゲスト ユーザ アカウントの説明を入力します。

m. [Save] をクリックします。

ステップ 11　FlexConnect に対して 2 つまたは 3 つのアクセス ポイントを設定する場合には、「FlexConnect のアクセス ポイントの設定」（P.12-764）を参照してください。

FlexConnect のアクセス ポイントの設定

この項では、FlexConnect のアクセス ポイントを設定する方法を説明します。

FlexConnect のアクセス ポイントを設定するには、次の手順を実行します。

ステップ 1　アクセス ポイントが物理的にネットワークに追加されていることを確認します。

ステップ 2　[Configure] > [Access Points] の順に選択します。

ステップ 3　[AP Name] リストでアクセス ポイントをクリックして、FlexConnect を設定するアクセス ポイントを選択します。[Access Point Detail] ページが表示されます。

[Inventory Information] グループ ボックスに表示される最後のフィールドは、このアクセス ポイントが FlexConnect に対して設定可能かどうかを示します。FlexConnect をサポートしているのは、1130AG および 1240AG アクセス ポイントだけです。

ステップ 4　[AP Mode] フィールドに *FlexConnect* が表示されることを確認します。そのように表示されない場合、ステップ 5 に進みます。FlexConnect がサポートされていると表示されている場合には、ステップ 9 に進みます。

ステップ 5　[Configure] > [AP Configuration Templates] > [Lightweight AP] または [Autonomous AP] を選択します。

ステップ 6　[AP Name] リストでアクセス ポイントをクリックして、FlexConnect を設定するアクセス ポイントを選択します。[Lightweight AP Template Detail] ページが表示されます。

ステップ 7　[FlexConnect Mode supported] チェックボックスをオンにします。この設定を有効にすると、すべてのプロファイル マッピングが表示できます。

（注）　モードを FlexConnect に変更するときに、アクセス ポイントがまだ FlexConnect モードでない場合、他のすべての FlexConnect パラメータはそのアクセス ポイントに適用されません。

ステップ 8　[VLAN Support] チェックボックスをオンにし、[Native VLAN ID] テキスト ボックスにリモート ネットワーク上のネイティブ VLAN の番号（100 など）を入力します。

（注）　デフォルトで、VLAN は FlexConnect アクセス ポイント上では有効化されていません。FlexConnect を有効にすると、アクセス ポイントは WLAN にアソシエートされた VLAN ID を継承します。この設定はアクセス ポイントで保存され、join response が成功した後に受信されます。デフォルトでは、ネイティブ VLAN は 1 です。VLAN が有効化されているドメインの FlexConnect アクセス ポイントごとに、ネイティブ VLAN を 1 つ設定する必要があります。そうしないと、アクセス ポイントはコントローラとのパケットの送受信ができません。クライアントが RADIUS サーバから VLAN を割り当てられている場合、その VLAN はローカル スイッチングの WLAN にアソシエートされます。

ステップ 9　[Apply/Schedule] タブをクリックして変更を保存します。

ステップ 10　[Locally Switched VLANs] セクションに、ローカル スイッチングの WLAN およびその VLAN ID が表示されます。[Edit] リンクをクリックして、クライアント IP アドレスを取得する VLAN の番号を変更できます。それによって、VLAN ID の変更を保存できるページにリダイレクトされます。

ステップ 11　[Save] をクリックして変更を保存します。

ステップ 12　リモート サイトで、FlexConnect に対して設定が必要なその他すべてのアクセス ポイントについて、この手順を繰り返します。

クライアント デバイスの WLAN への接続

「FlexConnect に対するコントローラの設定」（P.12-762）で作成した WLAN に接続するプロファイルをクライアント デバイスに作成する手順は次のとおりです。

例では、クライアント上で 3 つのプロファイルを作成します。

1. 「employee」WLAN に接続するには、WPA/WPA2 と PEAP-MSCHAPV2 認証を使用するクライアント プロファイルを作成します。クライアントが認証されると、コントローラの管理 VLAN から IP アドレスが取得されます。

2. 「employee-local」WLAN に接続するには、WPA/WPA2 認証を使用するクライアント プロファイルを作成します。クライアントが認証されると、ローカル スイッチの VLAN 101 から IP アドレスが取得されます。
3. 「guest-central」WLAN に接続するには、オープン認証を使用するプロファイルを作成します。クライアントが認証されると、アクセス ポイントへのネットワーク ローカル上の VLAN 101 から IP アドレスが取得されます。クライアントが接続されると、ローカル ユーザは任意の HTTP アドレスを Web ブラウザに入力します。Web 認証プロセスを完了するため、コントローラに自動的に誘導されます。Web ログイン ページが表示されたら、ユーザ名とパスワードを入力します。

クライアントのデータ トラフィックがローカル スイッチングか中央スイッチングかを確認するには、[Monitor] > [Devices] > [Clients] の順に選択します。

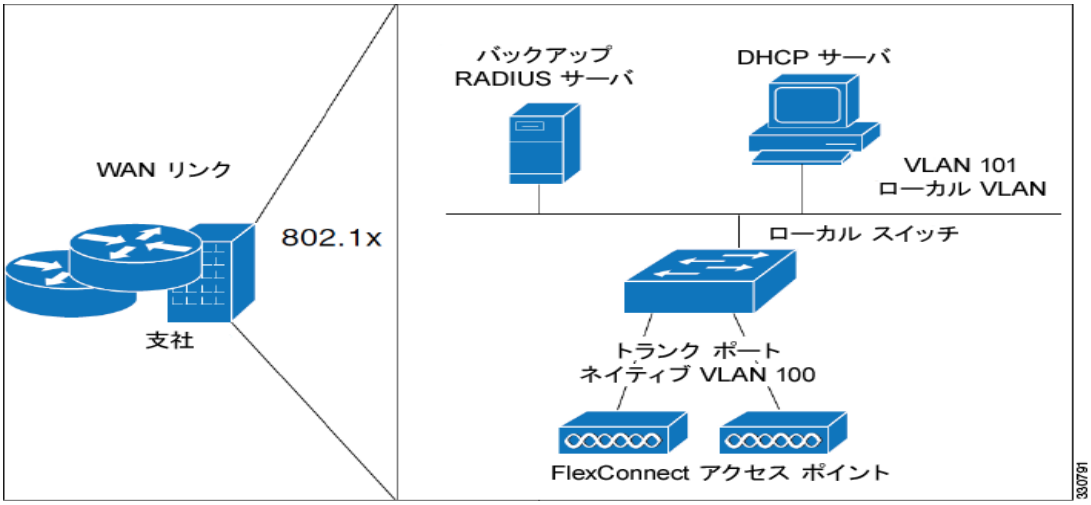
FlexConnect のアクセス ポイント グループ

FlexConnect を使用すると、ブランチ オフィスまたはリモート オフィスにあるアクセス ポイントを本社のオフィスからワイドエリア ネットワーク（WAN）リンクを使用して、各オフィスでコントローラを導入せずに、設定および制御できます。ロケーションごとに展開できる FlexConnect のアクセス ポイント数は無制限ですが、ブランチ オフィスは同じ設定を共有していることが多いため、フロアごとにアクセス ポイントを組織化してグループ化し、ビルディングごとに制限できます。

同じ設定でアクセス ポイント グループを作成することによって、個別にコントローラにアクセスするよりも CCKM 高速ローミングのような手順をより速く処理できます。たとえば、CCKM 高速ローミングを起動するには、FlexConnect アクセス ポイントがアソシエートできるすべてのクライアントの CCKM キャッシュを認識している必要があります。300 のアクセス ポイントと 1000 のクライアントに接続できるコントローラがある場合、1000 のクライアントすべてではなく FlexConnect グループの CCKM キャッシュを処理して送信する方が迅速で実用的です。特定の 1 つの FlexConnect グループでアクセス ポイントの少ないブランチ オフィスに焦点を絞ることができます。こうすることで、ブランチ オフィスのクライアントはこれらのいくつかのアクセス ポイント間にだけ接続し、ローミングできるようになります。確立されたグループがある場合、CCKM キャッシュやバックアップ RADIUS などの機能は、各アクセス ポイントで設定されるのではなく、FlexConnect グループ全体に対して設定されます。

グループ内のすべての FlexConnect アクセス ポイントは、同じ WLAN、バックアップ RADIUS サーバ、CCKM、およびローカル認証の設定情報を共有します。この機能は、リモート オフィス内や建物のフロア上に複数の FlexConnect アクセス ポイントがあり、すべてを一度に設定する場合に役立ちます。たとえば、FlexConnect グループに対してバックアップ RADIUS サーバを 1 つ設定しておけば、個々のアクセス ポイント上で同じサーバを設定する必要はありません。図 12-2 は、ブランチ オフィスにバックアップ RADIUS サーバを持つ、一般的な FlexConnect グループの導入を示しています。

図 12-2　FlexConnect グループの導入



ここでは、次の内容について説明します。

- 「FlexConnect グループおよびバックアップ RADIUS サーバ」（P.12-767）
- 「FlexConnect グループおよび CCKM」（P.12-767）
- 「FlexConnect グループおよびローカル認証」（P.12-768）
- 「FlexConnect グループの設定」（P.12-768）
- 「FlexConnect グループの監査」（P.12-770）

FlexConnect グループおよびバックアップ RADIUS サーバ

スタンドアロン モードの FlexConnect アクセス ポイントが完全な 802.1X 認証を実行して RADIUS サーバをバックアップできるようにコントローラを設定できます。プライマリ RADIUS サーバを設定することも、プライマリとセカンダリの両方の RADIUS サーバを設定することもできます。

FlexConnect グループおよび CCKM

CCKM 高速ローミングが FlexConnect アクセス ポイントで動作するためには、FlexConnect グループが必要です。CCKM 高速ローミングは、ワイヤレス クライアントを別のアクセス ポイントにローミングする際に簡単かつ安全にキー交換できるように、完全な EAP 認証が実行されたマスター キーの派生キーをキャッシュすることにより実現します。この機能により、クライアントをあるアクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM キャッシュ情報を取得する必要があります。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。たとえば、300 台のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対して CCKM キャッシュを送信することは現実的ではありません。少数のアクセス ポイントからなる FlexConnect グループを作成すれば（たとえば、同じリモート オフィス内の 4 つのアクセス ポイントのグループを作成）、クライアントはその 4 つのアクセス ポイント間でのみローミングします。CCKM キャッシュがその 4 つのアクセス ポイント間で配布されるのは、クライアントがそれらのアクセス ポイントの 1 つにアソシエートするときだけとなります。

（注）　FlexConnect アクセス ポイントと FlexConnect 以外のアクセス ポイント間の CCKM 高速ローミングはサポートされていません。

FlexConnect グループおよびローカル認証

スタンドアロン モードの FlexConnect アクセス ポイントが最大 20 人の静的に設定されたユーザに対して LEAP または EAP-FAST 認証を実行できるようにコントローラを設定できます。コントローラは、各 FlexConnect アクセス ポイントがコントローラに接続したときに、ユーザ名とパスワードの静的リストをそのアクセス ポイントに送信します。グループ内の各アクセス ポイントは、そのアクセス ポイントにアソシエートされたクライアントのみを認証します。

この機能は、Autonomous アクセス ポイント ネットワークから Lightweight FlexConnect アクセス ポイント ネットワークに移行する顧客で、かつ、より大きなユーザ データベースを保持する必要もなく、Autonomous アクセス ポイントで使用できる RADIUS サーバの機能と置き換える別のハードウェア デバイスを追加することもない顧客に最適です。

（注）　この機能は、FlexConnect バックアップ RADIUS サーバ機能と組み合わせて使用できます。FlexConnect グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect アクセス ポイントは常に、まずプライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。その後、セカンダリ バックアップ RADIUS サーバで試行し（プライマリに到達できない場合）、最後に FlexConnect アクセス ポイント自身で試行します（プライマリとセカンダリの両方に到達できない場合）。

FlexConnect グループの設定

FlexConnect グループを設定するには、次の手順を実行します。に従ってください。複数のコントローラに FlexConnect テンプレートを適用するには、「FlexConnect AP グループ テンプレートの設定」（P.11-645）のテンプレートの手順を参照してください。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　目的の IP アドレスをクリックして特定のコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[FlexConnect] > [FlexConnect AP Groups] の順に選択します。確立された FlexConnect AP グループが表示されます。

ステップ 4　[Group Name] 列に FlexConnect アクセス ポイント グループに割り当てられたグループ名が表示されます。別のグループを追加する場合は、[Select a command] ドロップダウン リストから [Add FlexConnect AP Group] を選択します。

または

既存のテンプレートを変更するには、[Template Name] 列のテンプレートをクリックします。[FlexConnect AP Groups Template] ページの [General] タブが表示されます。

（注）　グループ名を削除するには、削除するグループ名をクリックして、[Select a command] ドロップダウン リストから [Delete FlexConnect AP Group] を選択します。

[Template Name] フィールドに FlexConnect アクセス ポイント グループに割り当てられたグループ名が表示されます。

ステップ 5　各グループのプライマリ RADIUS 認証サーバを選択します。RADIUS 認証サーバがコントローラ上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。

（注）　Prime Infrastructure の FlexConnect RADIUS サーバ設定を適用する前に、コントローラ上で RADIUS サーバ設定を設定する必要があります。

ステップ 6　各グループのセカンダリ RADIUS 認証サーバを選択します。RADIUS 認証サーバがコントローラ上にない場合は、Prime Infrastructure で設定した RADIUS サーバは適用されません。

ステップ 7　グループにアクセス ポイントを追加するには、[FlexConnect AP] タブをクリックします。

ステップ 8　アクセス ポイントのイーサネット MAC アドレスは、同じコントローラ上の複数の FlexConnect グループに存在できません。複数のグループが同じコントローラに適用されている場合は、[Ethernet MAC] チェックボックスをオンにして、グループの 1 つのアクセス ポイントの選択を解除します。この変更を保存するか、コントローラに適用する必要があります。

ステップ 9　FlexConnect グループのローカル認証を有効にするには、[FlexConnect Configuration] タブをクリックします。[FlexConnect Configuration] タブが表示されます。

（注）　[General] タブで、[Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。

ステップ 10　この FlexConnect グループのローカル認証を有効にするには、[FlexConnect Local Authentication] チェックボックスをオンにします。デフォルト値はオフです。

（注）　この機能を使用しようとすると、ライセンスの必要な機能であることを知らせる警告メッセージが表示されます。

ステップ 11　FlexConnect アクセス ポイントが LEAP を使用してクライアントを認証できるようにするには、[LEAP] チェックボックスを選択します。それ以外の場合は、FlexConnect アクセス ポイントが EAP-FAST を使用してクライアントを認証できるようにするには、[EAP-FAST] チェックボックスを選択します。

ステップ 12　Protected Access Credential（PAC）をプロビジョニングする方法に応じて、次のいずれかを実行します。

- 手動の PAC プロビジョニングを使用するには、[EAP-FAST Key] テキスト ボックスに、PAC の暗号化と復号化に使用するキーを入力します。キーは 32 桁の 16 進数文字である必要があります。
- PAC プロビジョニング中に PAC のないクライアントに自動的に PAC を送信できるようにするには、[Auto Key Generation] チェックボックスをオンにします。

ステップ 13　[EAP-FAST Authority ID] テキスト ボックスに EAP-FAST サーバの認証局 ID を入力します。識別子は 32 桁の 16 進数文字である必要があります。

ステップ 14　[EAP-FAST Authority Info] テキスト ボックスに EAP-FAST サーバの認証局 ID に関する情報をテキスト形式で入力します。32 桁までの 16 進数文字を入力できます。

ステップ 15　[EAP-FAST Pac Timeout] テキスト ボックスの編集ボックスに PAC が表示され続ける秒数を入力することにより、PAC タイムアウト値を指定します。有効範囲は 2 ～ 4095 秒です。

（注）　個々のアクセス ポイントが FlexConnect グループに属していることを確認するには、[Users configured in the group] リンクをクリックします。[FlexConnect AP Group] ページが開き、グループの名前と、そのグループに属しているアクセス ポイントが表示されます。

FlexConnect グループの監査

FlexConnect 設定が Prime Infrastructure またはコントローラ上で時間とともに変化した場合は、設定を監査できます。変化は、後続の画面に表示できます。Prime Infrastructure またはコントローラを更新して、設定の同期を選択できます。

CHAPTER 13

アラームおよびイベント一覧

この章では、無線 LAN コントローラ、アクセス ポイント、およびロケーション アプライアンスが受信可能なイベントおよびアラーム通知について説明します。

イベントとは

*イベント*とは、ネットワーク内やその周辺である状態が発生すること、およびこれを検出することです。イベントは、特定の時点で発生する別個の問題です。イベントの例を次に示します。

- ポート ステータスの変化
- デバイスのリセット
- デバイスが管理ステーションから到達不能になる。

イベントは次のいずれかになります。

- ネットワークにおけるエラー、故障、異常事態など何らかの障害に伴うもの。たとえば、デバイスが到達不能になると、到達不能イベントがトリガーされます。
- 障害の解消に伴うもの。たとえば、デバイスの状態が到達不能から到達可能に変更されると、到達可能イベントがトリガーされます。

1 つ以上のイベントによって、異常状態またはアラームが生成されることがあります。アラームはクリアできますが、イベントは残ります。[Event Browser] を使用して、イベントのリストを表示できます。

[Events] ページにアクセスするには、[Monitor] > [Events] の順に選択します。

アラームとは

*アラーム*は、1 つ以上の関連イベントへの Prime Infrastructure 応答です。イベントの重大度（重大、やや重大、比較的重大でない、または警告）が高いと見なされた場合は、Prime Infrastructure はその状態が発生しなくなるまでアラームを発生させます。

1 つまたは複数のイベントで、発生するアラームが 1 つの場合もあります。アラームは、次の順序で作成されます。

1. ネットワークで障害が発生すると、通知がトリガーされます。
2. この通知に基づいてイベントが作成されます。
3. このイベントに対応するアクティブなアラームがないかどうかを確認した後で、アラームが作成されます。

アラームは、次の 2 つのタイプのイベントに関連付けられます。

- アクティブ イベント：クリアされていないイベント。アラームは、ネットワークで障害が解決されるまでこの状態のままです。
- 履歴イベント：クリアされたイベント。イベントは、ネットワークで障害が解決されると、その状態を履歴イベントに変更します。

アラームのクリア後は、アラームのライフ サイクルの終了を示します。クリアされたアラームは、プリセット期間内に同じ障害が再発生した場合に復活されることがあります。プリセット期間は、Prime Infrastructure で 5 分に設定されます。

[Alarms] ページにアクセスするには、[Monitor] > [Alarms] の順に選択します。

アラームおよびイベントの一覧については、『Cisco Prime Infrastructure のアラームおよびイベント（英語版）、（日本語版）』を参照してください。

イベントの作成、アラームおよびイベントの関連付け、アラーム ステータスの詳細については、『*Cisco Prime Infrastructure 1.2 User Guide*』を参照してください。

サポートされないトラップ

- BROADCAST_STORM_START: broadcastStormStartTrap
- FAN_FAILURE: fanFailureTrap
- POWER_SUPPLY_STATUS_CHANGE: powerSupplyStatusChangeTrap
- BROADCAST_STORM_END: broadcastStormEndTrap
- VLAN_REQUEST_FAILURE: vlanRequestFailureTrap
- VLAN_DELETE_LAST: vlanDeleteLastTrap
- VLAN_DEFAULT_CFG_FAILURE: vlanDefaultCfgFailureTrap
- VLAN_RESTORE_FAILURE_TRAP: vlanRestoreFailureTrap
- IPSEC_ESP_REPLAY_FAILURE: bsnIpsecEspReplayFailureTrap
- IPSEC_ESP_INVALID_SPI: bsnIpsecEspInvalidSpiTrap
- LRAD_UP: bsnAPUp
- LRAD_DOWN: bsnAPDown
- STP_NEWROOT: stpInstanceNewRootTrap
- STP_TOPOLOGY_CHANGE: stpInstanceTopologyChangeTrap
- BSN_DOT11_ESS_CREATED: bsnDot11EssCreated
- BSN_DOT11_ESS_DELETED BSNDOT11ESSDELETED
- LRADIF_RTS_THRESHOLD_CHANGED
- LRADIF_ED_THRESHOLD_CHANGED
- LRADIF_FRAGMENTATION_THRESHOLD_CHANGED
- LINK_FAILURE: linkFailureTrap

CHAPTER 14

レポート

Cisco Prime Infrastructure のレポート作成は、問題のトラブルシューティングにはもちろん、システムの監視とネットワーク状態の監視に必要です。複数のレポートを、即時でも定期的にでも実行して生成できます。レポートの種類ごとに、レポートの定義に役立つユーザ定義の条件がいくつか用意されています。レポートの形式には、概要、表、または組み合わせ（表とグラフ）レイアウトがあります。一度定義しておけば、今後の診断用に保存したり、定期的に実行してレポートを作成するようにスケジュールしたりできます。

レポートは CSV 形式または PDF 形式のいずれかで保存されます。後からダウンロードできるよう Prime Infrastructure 上のファイルに保存したり、または指定の電子メール アドレス宛に送信することもできます。

レポートには、次の種類があります。

- 現在。時間に依存しないデータのスナップ ショットを示します。
- 履歴。デバイスから定期的にデータを取得し、そのデータを Prime Infrastructure のデータベースに保存します。
- 傾向。集積データからレポートを生成します。ユーザが定義した間隔でデバイスから定期的にデータを収集できるほか、レポートの生成スケジュールを作成できます。

どのレポートも Prime Infrastructure を使用してエクスポートでき、表示したり、論理グループに分類したり、長期間の保管用にアーカイブしたりできます。

[Reports] メニューを使用すると、すべての Prime Infrastructure レポートに加えて、現在保存およびスケジュールされているレポートにもアクセスできます。

- [Report Launch Pad] : すべての Prime Infrastructure レポートへのポータルとなるページです。このページから、特定のタイプのレポートにアクセスでき、新しいレポートを作成できます。
- [Scheduled Run Results] : Prime Infrastructure で現在スケジュールされているすべての実行にアクセスでき、管理できます。オンデマンド エクスポートや、電子メールで送信されたレポートにアクセスして管理することもできます。
- [Saved Report Templates] : Prime Infrastructure で現在保存されているすべてのレポート テンプレートにアクセスして管理できます。

ここでは、次の内容について説明します。

- 「レポートの設定および管理」（P.14-774）
- 「スケジュールされた実行結果の管理」（P.14-776）
- 「保存されたレポート テンプレートの管理」（P.14-776）

レポートの設定および管理

レポート ラウンチ パッドでは、1 つのページからすべての Prime Infrastructure レポートにアクセスできます。このページから、新しいレポートの作成と保存、現在のレポートの表示、特定タイプのレポートのオープン、後で実行するレポートのスケジューリング、およびレポートの結果のカスタマイズを実行できます。

ヒント　レポート タイプの横のツール チップ上にマウス カーソルを合わせると、レポートの詳細が表示されます。

ここでは、次の内容について説明します。

新しいレポートの作成、スケジューリング、および実行

新しいレポートを作成して実行するには

ステップ 1　[Report] > [Report Launch Pad] の順に選択します。

レポートは、ページのメイン セクションおよび左側のサイドバーのメニューに、カテゴリ別にリストされます。レポートの各カテゴリのレポート タイプを表示するには、左側のサイド バーのメニューでカテゴリをクリックします。

ステップ 2　レポート ラウンチ パッドのメイン セクションで該当するレポートを見つけてください。

レポート タイプ用に現在保存されているレポート テンプレートを表示するには、[Report Launch Pad] 上のレポート名をクリックするか、[Report Launch Pad] ページの左側のナビゲーションにあるレポート タイプをクリックします。現在保存されているテンプレートがページのメイン セクションに一覧表示されます。

ステップ 3　レポートの右側にある [New] をクリックします。選択したレポートの [Report Details] ページが表示されます。

ステップ 4　[Report Details] ページで、表 D-1 の説明に従い各フィールドに入力します。[Report Details] に表示されるパラメータはレポート タイプによって異なります。

一部のレポートでは、レポートの結果をカスタマイズする必要があります。「レポート結果のカスタマイズ」（P.14-775）を参照してください。

ステップ 5　このレポートを後で実行する場合、または繰り返しレポートとして実行する場合、表 D-1 の「スケジュール」セクションの説明に従いスケジュール パラメータを入力します。スケジュール パラメータを使用すると、レポートを実行する日時と頻度を管理できます。

ステップ 6　すべてのレポート パラメータを設定したら、次のいずれかを選択します。

- [Run]：レポート設定を保存せずにレポートを実行する場合にクリックします。
- [Save]：レポートをすぐに実行せずにこのレポート設定を保存する場合にクリックします。スケジュール パラメータを入力すると、スケジュールされた日時にレポートが自動的に実行されます。
- [Run and Save]：クリックすると、このレポートの設定を保存し、ただちにレポートを実行します。
- [Save and Export]：クリックすると、レポートを保存、実行し、結果をファイルにエクスポートします。以下を要求するプロンプトが表示されます。

- エクスポートするレポートのファイル形式を選択します（CSV または PDF）。
- レポートの生成後に電子メールを送信するかどうかを選択します。このオプションを選択する場合、宛先メール アドレスと電子メールの件名を入力し、エクスポートされたファイルを添付ファイルとして電子メールに含めるかどうかを選択する必要があります。

終了したら、[OK] をクリックします。

- [Save and Email]：クリックすると、レポートを保存、実行して結果をファイルとしてエクスポートし、そのファイルを電子メールで送信します。以下を要求するプロンプトが表示されます。
  - エクスポートするレポートのファイル形式を選択します。
  - 宛先メール アドレスと電子メールの件名を入力します。

  終了したら、[OK] をクリックします。
- [Cancel]：このレポートを実行も保存もせずに前のページに戻る場合にクリックします。

特定のレポート タイプに対するレポートが保存されている場合は、レポート ラウンチ パッドから現在のレポートにアクセスできます。

（注）　生成されたレポートは、すべてのサブ ドメインに対してまとめて変更することも、更新することもできません。生成されたレポートは、対応するサブ ドメインを介して個別に開くことにより変更できます。すべてのレポートを更新する必要がある場合は、サブ ドメイン上に作成されたすべてのレポートを削除してから、変更を含めて、新規レポートの追加ワークフローを使用することにより、仮想ドメイン レポートを生成し直します。

レポート結果のカスタマイズ

多くのレポートでは、結果のカスタマイズが可能で、各種の情報を含めること、または除外することができます。作成するレポートでこれが許可されている場合、[Customize] ボタンが表示されます。このボタンをクリックすると、[Create Custom Report] ページにアクセスして、レポートの結果をカスタマイズできます。

レポート結果のカスタマイズは場合によって必要となります。例：Flexible NetFlow（FNF）拡張パラメータをトラフィック分析、アプリケーション、または音声ビデオ データ モニタリングの各テンプレートに追加すると、それらのパラメータは Prime Infrastructure モニタリング設定の一部になります。ただし、これにより、収集された FNF 拡張モニタリング データが、コア、アプリケーション応答時間（ART）、および RTP パフォーマンスに関するそれぞれの Conversations レポートに自動的に表示されるわけではありません。この FNF データがこれらの Conversations レポートに含まれるようにするには、[Create Custom Report] ページを使用して、これらの FNF パラメータを [Data fields to include] 列に追加する必要があります（表 D-2 を参照）。

レポート結果をカスタマイズするには

ステップ 1　[Report] > [Report Launch Pad] の順に選択します。

レポートは、ページのメイン セクションおよび左側のサイドバーのメニューに、カテゴリ別にリストされます。

ステップ 2　該当するレポートの [Report Title] リンクをクリックして、[Report Details] ページを開きます。

ステップ 3　[Customize] をクリックして [Create Custom Report] ページを開きます。

ステップ 4　表 D-2 の説明に従って、フィールドに入力します。

ステップ 5　[Apply] をクリックして変更を確定します。

（注）　[Create Custom Report] ページで行った変更は、[Report Details] ページで [Save] をクリックしないうちは保存されません。

スケジュールされた実行結果の管理

Prime Infrastructure で現在スケジュールされているすべての実行を表示するには、[Report] > [Scheduled Run Results] の順に選択します。

（注）　スケジュール設定されたレポート タスクは、タスクを実行する仮想ドメインの外部には表示されません。スケジュール設定されたレポート タスクの結果は、対応するドメインの [Scheduled Run Results] ページから参照できます。

（注）　スケジュールされた実行のリストは、レポート カテゴリ、レポート タイプ、タイム フレーム、およびレポート生成方法でソートできます。このページのフィールドの詳細については、表 D-3 を参照してください。

[Scheduled Run Results] ページには、次の情報が表示されます。

- [Report Title]：ユーザが割り当てたレポート名を示します。

  （注）　このレポートの詳細を表示するには、レポート タイトルをクリックします。

- [Report Type]：特定のレポート タイプを示します。
- [Status]：レポートが正常に実行されたかどうかを示します。
- [Message]：このレポートが保存されたかどうか、およびこのレポートのファイル名（保存されている場合）を示します。
- [Run Date/Time]：スケジュール設定されている、レポートの実行日時を示します。
- [History]：このレポートのスケジュールされたすべての実行とその詳細を表示するには、[History] アイコンをクリックします。
- [Download]：レポートの結果の .csv ファイルまたは .pdf ファイルを開くか保存するには、[Download] アイコンをクリックします。

保存されたレポート テンプレートの管理

[Saved Report Templates] ページでは、レポート テンプレートを作成すること、および保存されているレポート テンプレートを管理することができます。現在保存されているレポート テンプレートを有効化、無効化、削除、または実行することもできます。Prime Infrastructure でこのページを開くには、[Report] > [Saved Report Templates] の順に選択します。

（注）　保存されたレポート テンプレートのリストは、レポート カテゴリ、レポート タイプ、およびスケジュール設定のステータス（有効、無効、または期限切れ）によってソートできます。このページのフィールドの詳細については、表 D-4 を参照してください。

[Saved Report Templates] ページには、次の情報が表示されます。

- [Report Title]：ユーザが割り当てたレポート名を示します。

  （注）　このレポートの詳細を表示するには、レポート タイトルをクリックします。

- [Report Type]：特定のレポート タイプを示します。
- [Scheduled]：このレポートが有効か無効かを示します。
- [Run]：現在のレポートをすぐに実行するには、[Run] アイコンをクリックします。

[Show] ドロップダウン リストを使用すると、[Saved Report Templates] リストをカテゴリ、タイプ、およびスケジュール設定のステータスによってフィルタできます。保存されているレポート テンプレートのフィルタリングについては、表 D-4 を参照してください。

Prime Infrastructure のレポート

ここでは、Prime Infrastructure 固有のレポートについて説明します。内容は次のとおりです。

Autonomous AP レポート

Autonomous AP レポート カテゴリの横の [New] をクリックして、新規レポートを作成します。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。このページから、現在保存されているレポート テンプレートを有効、無効、削除、または実行できます。

表 14-1 に、Prime Infrastructure で生成できる各種 Autonomous AP レポートのリストと説明を示します。

表 14-1　Autonomous AP レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポートビュー	データフィールドのソート
Autonomous AP Memory and CPU Utilization	このレポートには、レポートの生成時に指定したフィルタリング基準に基づいて、Autonomous アクセス ポイントのメモリと CPU 使用率の傾向が表示されます。予期しない動作やネットワークのパフォーマンスの問題を識別するために役立つことがあります。	No	No	グラフ形式	No
Autonomous AP Summary	このレポートには、Autonomous AP の概要が表示されます。	Yes	No	表形式	No
Autonomous AP Tx Power and Channel	このレポートには、レポート生成時に使用したフィルタリング基準に基づき、デバイスのチャネル計画の割り当ておよび送信電力レベルの傾向が表示されます。予期しない動作やネットワークのパフォーマンスの問題を識別するために役立ちます。	No	Yes	グラフ形式	No
Autonomous AP Uptime	このレポートには、Autonomous AP の稼働時間が表示されます。	Yes	No	表形式	No
Autonomous AP Utilization	このレポートには、レポート生成時に使用したフィルタリング基準に基づき、Autonomous AP 無線の使用率の傾向が表示されます。このレポートは、現在のネットワークのパフォーマンスを識別し、今後のスケーラビリティの必要性に応じて容量を計画するうえで役立ちます。	No	No	グラフ形式	No
Busiest Autonomous APs	このレポートには、ワイヤレス ネットワーク上で総使用率（送信、受信、およびチャネルの使用率の合計）が最大の Autonomous AP が表示されます。	Yes	No	表形式	No

CleanAir レポート

レポートを新規作成するには、CleanAir レポート タイプの [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。

現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。
表 14-2 に、Prime Infrastructure で生成できる各種 CleanAir レポートのリストと説明を示します。

表 14-2　CleanAir レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Air Quality vs Time	このレポートには、ワイヤレス ネットワーク上のアクセス ポイントについて、電波品質の指標の一定期間にわたる分布が表示されます。	Yes	No	表形式	No
Security Risk Interferers	このレポートには、ワイヤレス ネットワークでのセキュリティ リスク干渉が表示されます。	Yes	No	表形式	No
Worst Air Quality APs	このレポートには、電波品質の指標が最小のアクセス ポイントが表示されます。	Yes	No	表形式	No
Worst Interferers	このレポートには、ワイヤレス ネットワークでの最悪の干渉が表示されます。	Yes	No	表形式	No

クライアント レポート

レポートを新規作成するには、クライアント レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

（注）　レポートに仮想ドメインを作成すると、作成後に仮想ドメインの統計収集が開始されます。したがって、ルートドメインの統計を取得する場合、以前の時間（仮想ドメインの作成よりも前の時間）に対する時間ごとの統計は取得されません。

表 14-3 に、Prime Infrastructure で生成できる各種クライアント レポートのリストと説明を示します。

表 14-3　クライアント レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Busiest Clients	このレポートには、スループット、使用率、およびその他の統計ごとに、ワイヤレス ネットワーク上の最もビジーなクライアントとビジーでないクライアントが表示されます。このレポートは、ロケーション、帯域、またはその他のパラメータによってソートできます。 （注）　Busiest Clients レポートには、Autonomous 型のクライアントは含まれ*ません*。	Yes	No	表形式	No
CCX Client Statistics	このレポートには、選択したレポートの実行オプションに応じて、Cisco Compatible Extensions v5 クライアントまたは Cisco Compatible Extensions v6 クライアントの 802.11 とセキュリティの統計が表示されます。	No	No	表形式	No

表 14-3　クライアント レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Client Count	この動向レポートには、ワイヤレス ネットワーク上のアクティブ クライアントの総数が表示されます。 Client Count レポートには、指定デバイス経由、指定の地域内、または特定の SSID か複数 SSID を介してネットワークに接続されたクライアント数についてのデータが表示されます。 （注）　Client Count レポートには、Autonomous 型の Cisco IOS アクセス ポイントに接続しているクライアントが含まれます。 （注）　ルート ドメインの下の 2 個のサブ仮想ドメインに対するクライアント数レポートを実行した場合、レポートされるデータは、この 2 個の仮想ドメインに割り当てられているコントローラが異なっていても、同一である場合があります。これは、このレポートは、システムのすべてのコントローラに対するデータを返すためです。単一仮想ドメインの個別レポートを取得するには、ルート ドメイン ユーザではなく、特定の仮想ドメイン ユーザとしてレポートを実行します。	No	No	グラフ形式	No
Client Session	このレポートには、特定の期間のクライアント セッション数が示されます。クライアント セッション数の履歴、統計、およびクライアントが指定された任意の期間にあるアクセス ポイントに接続されていた期間が表示されます。	Yes	No	表形式	No

表 14-3　クライアント レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Client Summary	Client Summary は、さまざまなクライアント統計を表示する詳細レポートです。 クライアント トラップを受信しない場合、Prime Infrastructure では、クライアント ステータス ポーリングを利用して、クライアント アソシエーションを検出します（このタスクの実行頻度はデフォルトでは 5 分ごと）。ただし、Prime Infrastructure では、クライアントが実際にアソシエートされた時間を正確に判別できません。Prime Infrastructure では、ポーリング時間にアソシエーションが開始されたと想定しますが、実際のアソシエーション時間よりも後のことがあります。したがって、平均クライアント スループットの計算結果は、特にクライアント セッションが短い場合、不正確なことがあります。 **（注）** Prime Infrastructure では、認証されているセッションのみをカウントします。DHCP または認証に失敗したユーザの場合、Prime Infrastructure では、対応するセッションがないことがあります。また、Prime Infrastructure は検出されたすべての AP アソシエーションをセッションと認識します。たとえば、クライアントが 2 個のアクセス ポイント間をローミングする場合、Prime Infrastructure では、2 個のアソシエーション セッションを持つことがあります。	Yes	Yes	各種	Yes
Client Traffic	このレポートには、ネットワーク上のワイヤレス クライアントによるトラフィックが表示されます。	No	No	グラフ形式	No
Client Traffic Stream Metrics	このレポートには、クライアントのトラフィック ストリーム メトリックが表示されます。次の中から選択できます。 • 特定のセットの SSID を持つすべてのクライアント • すべてのクライアント • 特定の単一クライアント **（注）** トラフィック ストリーム メトリックと無線のパフォーマンスのバックグラウンド タスクは、このレポートを生成する前に実行されている必要があります。	Yes	No	表形式[1]	No

表 14-3　クライアント レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Posture Status Count	この動向レポートには、ネットワーク上の失敗または成功したクライアント ポスチャ ステータス数が表示されます。	No	No	グラフ形式	No
Throughput	このレポートには、ネットワーク上のワイヤレス クライアントによる現行の帯域幅が表示されます。 （注）　Throughput レポートには、有線クライアントおよび Autonomous 型の Cisco IOS アクセス ポイントに接続するクライアントは含まれません。	No	No	表形式	No
Unique Client Summary	これは、さまざまな固有クライアントの統計情報を表示する詳細レポートです。1 日より短い間隔でレポートを実行する場合、Client Summary レポートの代わりにこのレポートを使用できます。 （注）　長時間にわたってこのレポートは実行しないでください。	No	Yes	表形式	No
Unique Clients	このレポートには、選択する時間、プロトコル、およびコントローラ フィルタ別に、すべての固有クライアントが表示されます。クライアントが固有かどうかは、クライアント デバイスの MAC アドレスによって判別されます。このクライアントは、このレポートのコントローラ別にソートされます。 （注）　Unique Client レポートは、指定された期間に接続を開始したか、指定された期間に接続を終了した、または指定された期間に接続された、任意のクライアントを対象としています。指定された期間は、レポートのスケジュール設定時に指定するレポート期間を示します。	Yes	No	表形式	No

1. [Subreport Client Summary] ビューは表形式にのみ対応しています。[Client Summary by Protocol] など、これ以外のサブレポートには、両方のレポート表示があり、表形式、グラフ式、または両方で表示するようにカスタマイズできます。

コンプライアンス レポート

Configuration Audit レポートには、Prime Infrastructure とコントローラの間の差異が表示されます。PCI DSS Compliance レポートには、PCI データ セキュリティ基準（Payment Card Industry Data Security Standard）の要件を基準とする無線 LAN セキュリティ コンポーネントの概要が示されます。カード所有者のデータを保存、処理または送信するすべての販売者およびサービス プロバイダーは PCI DSS に準拠する必要があります。PCI DSS 基準は、PCI Security Standards Council Web サイトで確認できます。

表 14-4 に、Prime Infrastructure で生成できる各種コンプライアンス レポートのリストと説明を示します。

表 14-4　コンプライアンス レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Configuration Audit	このレポートには、Prime Infrastructure とコントローラでの設定の差異が表示されます。[Administration] > [Settings] ページで監査モードを設定する必要があります。監査モードでは、テンプレートまたは保存した設定に基づいて監査を実行できます。このレポートには、設定の同期バックグラウンド タスクを使用して監査が最後に実行された時刻が表示されます。	Yes	No	表形式	No
PCI DSS Detailed	このレポートには、ワイヤレス ネットワークのセキュリティに関連する PCI データ セキュリティ基準（DSS）バージョン 2.0 の要件が詳細に表示されます。	Yes	No	表形式	No
PCI DSS Summary	このレポートには、ワイヤレス ネットワークのセキュリティに関連する PCI データ セキュリティ基準（DSS）バージョン 2.0 の要件の概要が表示されます。	No	No	グラフ形式	No

デバイス レポート

レポートを新規作成するには、デバイス レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-5 に、Prime Infrastructure で生成できる各種デバイス レポートのリストと説明を示します。

表 14-5　デバイス レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
AP Image Pre-download	このレポートには、スケジュールされたソフトウェアのダウンロード タスクのステータスが表示されます。	Yes			
AP Profile Status	このレポートには、アクセス ポイントの負荷、ノイズ、干渉、およびカバレッジ プロファイルのステータスが表示されます。	Yes	No	表形式	No

表 14-5　デバイス レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
AP Summary	このレポートには、SSID をブロードキャストしているアクセス ポイントの一覧が表示されます。このレポートでは、RF グループ名、モビリティ グループ名、アクセス ポイント グループ名、SSID、ロケーション、およびその他の統計によってデバイスをフィルタできます。 （注）　このレポートには、デフォルトでは、1 つ以上の SSID をブロードキャストしているアクセス ポイントの一覧が表示されます。デフォルトでは [All SSIDs] フィルタが選択されています。SSID をブロードキャストしていないアクセス ポイントは表示されません。 （注）　AP Summary レポートには、Autonomous アクセス ポイントは含まれていません。Autonomous アクセス ポイントについては、Autonomous AP Summary レポートを実行する必要があります。	Yes			
Busiest APs	このレポートには、ワイヤレス ネットワーク上で総使用率（送信、受信、およびチャネルの使用率）が最大のアクセス ポイントが表示されます。最初にレポートは、コントローラから Tx 使用率、Rx 使用率、およびチャネル使用率データを定期的に収集します。収集されたデータは集約テーブルに集約され、保存されます。次にレポートは、集約テーブルからデータを収集し、選択されたレポート作成期間に基づいて平均を計算します。	Yes	No	表形式	No
CPU Utilization	このレポートには、ネットワーク上の CPU 使用率スイッチ使用状況が表示されます。	No	No	グラフ形式	No
Classmap QOS Statistics	このレポートでは、ネットワーク内のクラスマップの Quality of Service（QoS）統計情報が表示されます。	Yes	No	表形式	Yes
Detailed Device Inventory	このレポートには、ネットワーク内のデバイスに関するインベントリ情報が表示されます。	Yes	Yes	表形式	No
Device Health	このレポートには、ネットワーク内のデバイスの状態の複合詳細が表示されます。	Yes	Yes	表形式	Yes
Dmvpn Reports	このレポートには、ネットワーク内のデバイスの DMVPN データが表示されます。	Yes	No	表形式	Yes
GET VPN Network Status	このレポートには、ネットワーク内のデバイスの VPN ステータスが表示されます。	Yes	No	表形式	Yes
Identity Capability	このレポートには、ネットワーク内のスイッチに関する識別機能の概要が表示されます。	No	No	各種	No

表 14-5　デバイス レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Interface Availability	このレポートには、ネットワーク内のデバイスのアベイラビリティの最も高いインターフェイスおよびアベイラビリティの最も低いインターフェイスが表示されます。	Yes	Yes	表形式	Yes
Interface Utilization	このレポートには、ネットワーク内のデバイス別に Rx/Tx 使用率の最も高いインターフェイスおよび Rx/Tx 使用率の最も低いインターフェイスが表示されます。	Yes	Yes	表形式	Yes
Inventory	このレポートでは、Prime Infrastructure によって管理されているコントローラ、アクセス ポイント、および MSE のインベントリ関連情報を生成できます。この情報には、ハードウェアの種類と分布、ソフトウェアの分布、CDP 情報、およびその他の統計が含まれます。 **（注）** モデル番号およびシリアル番号の値が Null つまり " になっている、アソシエーション解除されたアクセス ポイントは、AP インベントリ レポートから除外されます。	Yes	Yes	各種[1]	Yes
License by Device Type	このレポートには、ネットワーク内のデバイスで設定されている機能のライセンス情報が表示されます。	Yes	No	表形式	Yes
License by License Type	このレポートには、各ライセンス タイプのライセンス数が表示されます。	Yes	No	表形式	Yes
Memory Utilization	このレポートには、ネットワーク内のスイッチに関するメモリ使用率の概要が表示されます。	No	No	グラフ形式	No
Module Detail	このレポートには、ネットワーク内のデバイスの詳細モジュール情報が表示されます。	Yes	No	表形式	Yes
Non-Primary Controller APs	このレポートには、設定されているプライマリ コントローラに接続されていない、アクセス ポイントが表示されます。	Yes	No	表形式	Yes
Port Attribute	このレポートには、管理ステータス、動作ステータス、MAC アドレスなどのポート属性情報が表示されます。	Yes	No	表形式	Yes
Top AP by Client Count	このレポートには、ワイヤレス ネットワーク内のアクセス ポイントの、選択した期間における、アソシエートされているクライアントおよび認証されているクライアントの数が表示されます。	Yes	No	表形式	Yes
Uptime	このレポートには、アクセス ポイントの稼働時間、LWAPP の稼働時間、および LWAPP の接続時刻が表示されます。	Yes	No	表形式	No

表 14-5　デバイス レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Utilization	このレポートには、ワイヤレス ネットワーク上のコントローラ、AP、および MSE の使用率が表示されます。これらの統計（CPU 使用率、メモリ使用率、リンク使用率、無線使用率など）は、現在のネットワークのパフォーマンスを特定するために役立ち、将来の拡張の必要性に備える容量計画のために役立ちます。	No	No	グラフ形式	No
Vlan	このレポートには、ネットワーク内のスイッチの VLAN 情報が表示されます。	Yes	No	表形式	Yes

1. 複合インベントリ レポートに、AP、コントローラ、MSE、Autonomous AP、およびスイッチが出力されるようになりました。モデルまたはバージョン単位のレポートには、両方の表示があります。これらのビューは、モデル別のコントローラ数などの設定を使用してカスタマイズできます。Controller Inventory などの他のレポートは表形式にのみ対応しています。

ゲスト レポート

レポートを新規作成するには、ゲスト レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-6 に、Prime Infrastructure で生成できる各種ゲスト レポートのリストと説明を示します。

表 14-6　ゲスト レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Guest Accounts Status	このレポートには、ゲスト アカウントのステータスの変化が時系列順に表示されます。このレポートでは、アカウントを作成したゲスト ユーザによってゲスト アカウントがフィルタされます。ステータス変化の 1 つの例として、Scheduled から Active、Active から Expired という変化があります。	Yes	No	表形式	No
Guest Association	このレポートには、特定の期間にゲスト プロファイルや SSID にアソシエーションされるか、アソシエーション解除されたゲスト クライアントが表示されます。この期間はカスタマイズ可能です。	Yes	No	表形式	No
Guest Count	このレポートには、特定の期間にネットワークにログインしたゲスト クライアントの数がゲスト プロファイルや SSID ごとに表示されます。この期間はカスタマイズ可能です。	No	No	表形式	No

表 14-6　ゲスト レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Guest User Sessions	このレポートには、単一ゲスト ユーザの履歴のセッション データが表示されます。渡されたデータ量、ログインとログアウトの時刻、ゲスト IP アドレス、ゲスト MAC アドレスなどのセッション データは、デフォルトでは 1 ヵ月間使用できます。データ保持期間は、[Administration] > [Background Tasks] ページから設定できます。このレポートは、ソフトウェア バージョン 5.2 以降を実行しているコントローラにアソシエートされているゲスト ユーザについて生成できます。	Yes	No	表形式	No
NCS Guest Operations	このレポートには、単一またはすべてのゲストによって実行された、ゲスト ユーザ アカウントの作成、削除、更新などの、すべてのアクティビティが表示されます。ゲスト ユーザが Prime Infrastructure から削除された場合、このレポートには、削除アクティビティから 1 週間後までは、まだこの削除されたゲスト ユーザの実行したアクティビティが表示されます。	Yes	No	表形式	No

MSE 分析レポート

ここでは、Prime Infrastructure レポート ラウンチ パッドを使用して生成できる各種 MSE 分析レポートについて説明します。

新しい MSE 分析レポートを生成するには、MSE 分析レポート タイプの横の [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-7 に、Prime Infrastructure で生成できる各種 MSE 分析レポートのリストと説明を示します。

表 14-7　MSE 分析レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Client Location	このレポートには、MSE によって検出されたワイヤレス クライアントのロケーションの履歴が表示されます。	Yes	No	表形式	No
Client Location Density	このレポートには、MSE で検出されたワイヤレス クライアントとそれらの場所のリストが表示されます。複数の MSE を選択した場合は、選択したソート順序で、MSE ごとにこのリストはグループ化されます。	Yes	No	表形式	Yes

表 14-7　MSE 分析レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Device Count by Zone	このレポートでは、選択したゾーン内の MSE によって検出されたデバイスの数が示されます。	Yes	No	表形式	Yes
Device Dwell Time by Zone	このレポートは、MSE で検出されたデバイスのドウェル時間レポートを提供します。	Yes	No	表形式	Yes
Guest Location Density	このレポートには、フィルタリング基準に基づいて、MSE によって検出されたゲスト クライアントと、このクライアントのロケーションが表示されます。	Yes	No	表形式	No
Location Notifications by Zone	このレポートには、MSE によって生成されたロケーション通知が表示されます。	Yes	No	表形式	No
Mobile MAC Statistics	レポート ラウンチ パッドの [Mobile MAC Statistics] をクリックして [Mobile MAC Statistics Reports] ページを開きます。	No	Yes	表形式	No
Rogue AP Location Density	このレポートには、フィルタリング基準に基づいて、MSE によって検出された不正アクセス ポイントと、このアクセス ポイントのロケーションが表示されます。	Yes	No	表形式	No
Rogue Client Location Density	このレポートには、フィルタリング基準に基づいて、MSE によって検出された不正なクライアント アクセス ポイントと、このアクセス ポイントのロケーションが表示されます。	Yes	No	表形式	No
Service URI Statistics	レポート ラウンチ パッドの [Service URI Statistics] をクリックして [Service URI Statistics Reports] ページを開きます。	No	Yes	表形式	No
Tag Location	このレポートには、MSE によって検出されたタグのロケーションの履歴が表示されます。	Yes	No	表形式	No
Tag Location Density	このレポートには、フィルタリング基準に基づいて、MSE によって検出されたタグと、このタグのロケーションが表示されます。	Yes	No	表形式	No

メッシュ レポート

レポートを新規作成するには、メッシュ レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-8 に、Prime Infrastructure で生成できる各種メッシュ レポートのリストと説明を示します。

表 14-8　メッシュ レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Alternate Parent	このレポートには、メッシュ アクセス ポイントごとに、同じメッシュ グループが設定されている、代替できる親の数が表示されます。このレポートは、メッシュ パスでの障害を処理するアクセス ポイント機能の判別に使用できます。	Yes	No	表形式	No
Link Stats	このレポートには、親アクセス ポイント、リンク SNR、パケット エラー率、親の変更回数、ノードのホップ数、送信パケット総数、メッシュ パス、接続されたアクセス ポイント、メッシュ グループ、データ レート、チャネルなど、メッシュ リンクとメッシュ ノードの統計が表示されます。メッシュ リンクとメッシュ ノードの統計は、個別または組み合わせて実行できます。	Yes	No	表形式	No
Nodes	このレポートには、ホップ カウント、直接接続されている子の数、接続されているアクセス ポイントの数、メッシュ パスなど、各メッシュ アクセス ポイントのメッシュ ツリー情報が表示されます。	Yes	No	表形式	No
Packet Stats	このレポートには、送信されたパケットの合計数、1 分あたりの送信パケット数、パケット キュー平均、ドロップされたパケットの数、1 分あたりのドロップ パケット数、およびネイバー アクセス ポイントによる送信パケット エラー数が表示されます。データ タイプごとにレポート タイプを 1 つ選択できます。	No	No	グラフ形式	No
Stranded APs	このレポートには、孤立状態であると思われるアクセス ポイントが表示されます。これらのアクセス ポイントは、おそらく、いったんコントローラを接続してから、Prime Infrastructure によって管理されているコントローラに接続しなくなったか、Prime Infrastructure によって管理されているコントローラを接続したことがありません。	No	No	表形式	No
Worst Node Hops	このレポートには、指定したレポート期間での最低のノード ホップまたはバックホール SNR リンクが表示されます。この情報は、表形式とグラフ形式の両方で表示されます。レポート タイプには、最低ノード ホップ、すべてのネイバーの最低 SNR リンク、および親 / 子のみの最低 SNR リンクが含まれます。	Yes	Yes	各種	No

Network Summary

レポートを新規作成するには、Network Summary レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-9 に、Prime Infrastructure で生成できる各種 Network Summary レポートのリストと説明を示します。

表 14-9　Network Summary レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
802.11n Summary	このレポートには、指定した期間における、802.11n クライアントおよびクライアント帯域幅使用率のサマリーが表示されます。	No	Yes	グラフ形式	No
Preferred Calls	このレポートには、ワイヤレス ネットワークで行われた、優先コールを使用したアクセス ポイントが表示されます。	No	No	グラフ形式	No
Wireless Network Executive Summary	このレポートには、ワイヤレス ネットワークのクイック ビューが表示されます。	No	Yes	各種	No

パフォーマンス レポート

レポートを新規作成するには、Performance レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-10 に、Prime Infrastructure で生成できる各種パフォーマンス レポートのリストと説明を示します。

表 14-10　パフォーマンス レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
802.11 Counters	このレポートには、MAC レイヤでのアクセス ポイントのカウンタが表示されます。エラー フレーム、フラグメント数、RTS/CTS フレーム数、再試行フレームなどの統計情報は、フィルタリング基準に基づいて生成され、MAC 層のパフォーマンス（および問題）を解釈するために役立ちます。	Yes	No	両方	Yes
Application Summary	このレポートには、アプリケーション設定の詳細が表示されます。	No	Yes	表形式	Yes
Conversations	このレポートには、カンバセーションの詳細が表示されます。	Yes	Yes	表形式	Yes

表 14-10　パフォーマンス レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Coverage Hole	このレポートでは、ネットワークの潜在的なカバレッジ ホールの場所を識別し、特定のスポットで高頻度に発生するかどうかを識別します。このレポートは、RRM 設定を変更するためや、展開のまばらな領域をカバーするためにアクセス ポイントを追加する必要があるかどうかを判別するために役立ちます。アラーム テーブルに対して実行され、アラーム生成時間とクリア時間の両方（クリア済みの場合）、およびアラームの状態（アクティブまたはクリア済み）が表示されます。	Yes	No	表形式	No
End User Summary	このレポートには、クライアントあたりの平均 RTP パケット損失が表示されます。	No	Yes	表形式	Yes
Environmental Temperature	このレポートには、ネットワーク内のデバイスの環境温度データが表示されます。	Yes	Yes	表形式	Yes
Interface Errors and Discards	このレポートには、ネットワーク内のエラーおよび廃棄があるデバイスが表示されます。	Yes	No	表形式	Yes
Interface Summary	このレポートには、上位 N 個のアプリケーションの詳細が表示されます。	No	No	表形式	Yes
Network Utilization	このレポートには、ネットワーク上の全コントローラの集約されたポート使用率に基づくネットワーク全体の使用率が表示されます。これらの統計は、現在のネットワークのパフォーマンスを判断したり、将来のスケーラビリティの必要性に応じて容量の計画を作成したりするために役立つことがあります。 **（注）** 平均使用率（%）は、((Tx+Rx)/Bandwidth) で計算した、使用率のパーセントです。	Yes	Yes	両方	Yes
Site Summary	このレポートには、上位 N クライアント、下位 N クライアント、上位 N VLANS、および上位 N アプリケーションがサイト別に表示されます。	No	Yes	両方	Yes
Threshold Violation	このレポートには、ネットワークのしきい値違反イベント データが表示されます。	Yes	No	表形式	Yes
Traffic Stream Metrics	このレポートは、指定したクライアントの現在および過去の Quality of Service（QoS）を無線レベルで判断する場合に役立ちます。また、パケット損失率、平均キューイング遅延、遅延パケットの配布、ローミング遅延などのアップリンクおよびダウンリンク統計情報も表示されます。	Yes	Yes	両方	Yes

表 14-10　パフォーマンス レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Tx Power and Channel	このレポートには、レポート生成時に使用したフィルタリング基準に基づき、デバイスのチャネル計画の割り当ておよび送信電力レベルの傾向が表示されます。予期しない動作やネットワークのパフォーマンスの問題を識別するために役立ちます。	No	No	グラフ形式	No
Video Statistics	このレポートには、ネットワークのビデオ クライアント、ビデオ コール、ローミング ビデオ コール、拒否コール（ビデオごとの）によって使用される帯域幅の割合などの詳細情報が含まれており、ワイヤレス ネットワークの使用状況をビデオの観点から分析するのに役立ちます。このレポートから有益なデータを収集するために、コール アドミッション制御（CAC）がビデオ クライアントでサポートされていることを確認してください。	No	No	グラフ形式	No
VoIP Calls Graph	このレポートには、一定期間にわたるネットワーク上の VoIP コールの数と持続時間（無線ごと）などの詳細情報が含まれており、ワイヤレス ネットワークの使用状況を音声の観点から分析するために役立ちます。このレポートから有益なデータを収集するには、WLAN で VoIP スヌーピングが有効になっている必要があります。このレポートでは、グラフで情報が表示されます。	No	No	グラフ形式	No
VoIP Calls Table	このレポートには、一定期間にわたるネットワーク上の VoIP コールの数と持続時間（無線ごと）などの詳細情報が含まれており、ワイヤレス ネットワークの使用状況を音声の観点から分析するために役立ちます。このレポートから有益なデータを収集するには、WLAN で VoIP スヌーピングが有効になっている必要があります。このレポートでは、表形式で情報が表示されます。	No	No	表形式	No
Voice Statistics	このレポートには、ネットワークの音声クライアント、音声コール、ローミング コール、拒否コール（無線ごとの）によって使用される帯域幅の割合などの詳細情報が含まれており、ワイヤレス ネットワークの使用状況を音声の観点から分析するために役立ちます。このレポートから有用なデータを収集するためには、コール アドミッション制御（CAC）が音声クライアントでサポートされていることを確認してください。 **（注）** 音声統計レポートは、コール アドミッション制御（CAC）をサポートしており、CAC が有効にされているクライアントだけに適用されます。	No	No	グラフ形式	No

表 14-10　パフォーマンス レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Voice Video Summary	このレポートには、ボイスコール統計情報のサマリーが表示されます。	Yes	Yes	表形式	Yes
WAN Performance Analysis	このレポートには、WAN アプリケーションのトラフィック量の動向が表示されます。	No	Yes	グラフ形式	No
WAN Traffic Ananlysis Summary	このレポートには、WAN アプリケーションのトラフィックの詳細が表示されます。	No	Yes	表形式	Yes

Raw NetFlow

レポートを新規作成するには、Raw NetFlow レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-9 に、Prime Infrastructure で生成できる各種 Raw NetFlow レポートのリストと説明を示します。

表 14-11　Raw NetFlow レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Netflow V1	このレポートには、Netflow V1 のデータが表示されます。	No	No	グラフ形式	No
Netflow V5	このレポートには、Netflow V5 のデータが表示されます。	No	No	グラフ形式	No
Netflow V7	このレポートには、Netflow V7 のデータが表示されます。	No	No	グラフ形式	No

セキュリティ レポート

レポートを新規作成するには、セキュリティ レポート タイプに対応する [New] をクリックします。詳細については、「新しいレポートの作成、スケジューリング、および実行」（P.14-774）を参照してください。現在保存されているレポート テンプレートを表示するには、レポート タイプをクリックします。

表 14-12 に、Prime Infrastructure で生成できる各種セキュリティ レポートのリストと説明を示します。

表 14-12　セキュリティ レポート

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Adaptive wIPS Alarm	このレポートには、各アラーム タイプについて、選択した MSE、コントローラ、およびアクセス ポイント別の wIPS アラームが表示されます。	Yes	No	表形式	No
Adaptive wIPS Alarm Summary	このレポートには、ネットワーク上のすべての適応型ワイヤレス IPS アラームのサマリーが表示されます。	Yes	No	両方	No
Adaptive wIPS Top 10 APs	このレポートには、生成された適応型ワイヤレス IPS アラームの数について上位 10 個のアクセス ポイントが表示されます。	Yes	No	表形式	No
Adhoc Rogue Count Summary	このレポートには、すべてのアドホック不正アクセス ポイントの概略数が表示されます。	No	No	両方	No
Adhoc Rogues	このレポートには、最後に検出された時間に基づいて、ネットワーク アクセス ポイントによって検出されたすべてのアドホック不正デバイスの詳細が表示されます。 Prime Infrastructure では、トラップを使用するかポーリングによって、アドホック不正に関する更新をコントローラから受け取ります。最終検出時刻は、アドホック不正のトラップを受信するか、Prime Infrastructure の最後のポーリング サイクルでアドホック不正が検出されるたびに更新されます。 **（注）** このレポートには、clear severity の不正アクセス ポイント アラームが含まれます。	Yes	No	表形式	No
New Rogue AP Count Summary	このレポートには、すべての新規不正アクセス ポイントの概略数が表示されます。	No	No	両方	No
New Rogue APs	このレポートには、このレポート用に選択した時間帯に、ネットワーク上で初めて検出されたすべての新規の不正が表示されます。[Created Time] 列の値は、不正アクセス ポイントが最初に検出された時刻を示します。 **（注）** このレポートには、clear severity の不正アクセス ポイント アラームが含まれます。	No	No	グラフ形式	No
Rogue AP Count Summary	このレポートには、ネットワーク上の全不正アクセス ポイントの概略数が表示されます。	No	No	両方	No

表 14-12　セキュリティ レポート （続き）

レポート	説明	カスタマイズの可否	複数のサブレポート	レポート ビュー	データ フィールドのソート
Rogue AP Events	このレポートには、Prime Infrastructure で受信したすべての不正アクセス ポイント イベントが、イベントの時刻に基づいて表示されます。 Prime Infrastructure で受信したすべての不正関連のトラップは、Prime Infrastructure に不正イベントとして記録されます。新たに検出された不正アクセス ポイントがあると、Prime Infrastructure では、ポーリング データに基づいて、新規の不正アクセス ポイント イベントを作成します。Prime Infrastructure では、ユーザが Prime Infrastructure ユーザ インターフェイスを介して不正アクセス ポイントの状態および分類を変更した場合にも、イベントを作成します。 （注）　1 個の不正に対して、複数のイベントが存在することがあります。このレポートは、イベントのタイムスタンプに基づきます。	Yes	No	表形式	Yes
Rogue APs	Prime Infrastructure では、トラップを使用するかポーリングによって、不正に関する更新をコントローラから取得します。最終検出時刻は、不正のトラップを受信するか、Prime Infrastructure の最後のポーリング サイクルで不正が検出されるたびに更新されます。 このレポートには、不正アクセス ポイントの「最終検出時刻」および選択したフィルタリング基準に基づいて、ネットワークでアクセス ポイントによって検出されたすべての不正が表示されます。不正アクセス ポイントは、最終検出時刻によって配列されます。 （注）　このレポートには、clear severity の不正アクセス ポイント アラームが含まれます。	Yes	No	表形式	No
Security Alarm Trending Summary	このレポートには、一定期間にわたるセキュリティ アラームの傾向の概要が表示されます。	No	No	グラフ形式	No

CHAPTER 15

管理タスクの実行

管理機能では、タスクのスケジュール、アカウントの管理、およびローカル/外部の認証および許可の設定を実行できます。また、ロギング オプションの設定、メール サーバの設定、およびデータ保持期間の設定に関連するデータの管理も実行できます。Prime Infrastructure ライセンスの種類やライセンスのインストール方法についての情報を利用できます。

この章では、Cisco Prime Infrastructure の管理タスクについて説明します。ここで説明する内容は、次のとおりです。

バックグラウンド タスクの実行

Prime Infrastructure バックグラウンド タスクを使用して、データ収集タスクなどのバックグラウンド タスクをスケジュールおよびモニタできます。

ここでは、次の内容について説明します。

データ収集タスクなどのバックグラウンド タスクの詳細については、「データ収集タスク」（P.15-801）および「他のバックグラウンド タスク」（P.15-831）を参照してください。

バックグラウンド タスクについて

バックグラウンド タスクとは、表示可能なページなどのユーザ インターフェイスを使用せずにバックグラウンドで実行されるスケジュール プログラムです。Prime Infrastructure では、データの収集から設定のバックアップ取得まで、任意のタスクをバックグラウンド タスクとして実行できます。

（注）　複数のスケジュール タスクを表示するには、[Administration] > [Background Tasks] の順に選択します。[Background Tasks] ページが表示されます。

管理ステータスと動作ステータス、タスクの間隔、およびタスクが実行される時刻を表示できます。特定のタスクを実行するには、必要なタスクのチェックボックスをオンにして、[Select a command] ドロップダウン リストから [Execute Now] を選択します。タスクは、そのタスクに設定されている内容に基づいて実行されます。

タスクは、次の列とともに表に表示されます。

- チェックボックス：目的のタスクを選択するときにオンにします。選択されたタスクは、[Select a command] ドロップダウン リストから開始される操作の対象になります。このリストには、次の操作が含まれています。
  - [Execute Now]：チェックボックスがオンになっているすべてのデータ セットを実行します。
  - [Enable Collection]：スケジュールされた間隔でのデータ セットの実行を有効にします。
  - [Disable Collection]：スケジュールされた間隔でのデータ セットの実行を停止します。
- [Task]：設定ページへのリンクとして機能するタスク名。タスク名をクリックすると、該当のタスク設定ページに移動します。
- [Enabled]：タスクが有効か、無効かを示します。
- [Interval]：タスク実行の時間間隔。
- [Status]：タスクがアイドル状態か、無効か、または実行中かを示します。
- [Data Aggregation]（[Data Collections] のみ）：[Yes] に設定されている場合、データ セットは集約データです。
- [Non-Aggregation Data Retain Period (Days)]（[Data Collections] のみ）：非集約データが保持される日数。

（注）　Prime Infrastructure における集約データおよび非集約データの詳細については、「Prime Infrastructure の履歴データ」（P.15-860）を参照してください。

- [Last Execution Time]：タスクが実行された日付および時刻。
- [Last Execution Status]：実行されたタスクのステータス（成功、失敗、または部分的に成功）を示します。

このページでは、スケジュールされた Prime Infrastructure タスクのステータスを表示できます。スケジュールされたタスクは 2 種類に分けられます。詳細については、「データ収集タスク」（P.15-801）および「他のバックグラウンド タスク」（P.15-831）を参照してください。

データ収集タスクの実行

データ収集タスクは、レポート作成に役立つ情報を収集および整理するデータセット タスクです。

（注）　データの収集またはその他のバックグラウンド タスクに関連するすべてのタスクは、類似した方法で処理されます。

ステップ 1　[Administration] > [Background Tasks] の順に選択して、[Background Tasks] ページを表示します。このページは、次の情報を表示します。

- [Enabled]：タスクが有効になっているか、無効になっているか。
- [Interval]：タスク実行の時間間隔（分）。タスクのデータ収集設定ページで、間隔を設定できます。
- [Status]：タスクの現在の状態。
- [Data Aggregation]（[Data Collection Tasks] のみ）：[Yes] に設定されている場合、データ セットはデータを集約します。
- [Non-Aggregation Data Retain Period (Days)]（[Data Collection Tasks] のみ）：非集約データが保持される日数。タスクのデータ収集設定ページで、保持期間を設定できます。
- [Last Execution Time]：タスクが最後に実行された時刻および日付。
- [Last Execution Status]：最後のタスクが実行された後のステータス。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。

- タスクを有効にする。

  有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。有効化が完了すると、タスクは灰色から使用可能に変わります。

- タスクを無効にする。

  無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、タスクは灰色になります。

- タスクの詳細を表示する。

  特定のタスクを表示するには、[Data Collection Tasks] または [Other Background Tasks] 列の URL をクリックします。該当のタスクの詳細が表示されます。データの収集は、レポート作成に役立つ特定の種類の情報を収集および整理するデータセット タスクです。さまざまなデータ収集タスクの詳細については、「データ収集タスク」（P.15-801）を参照してください。

データ セットの設定ページにアクセスするには、[Data Collection] ページのデータ セットの名前を選択します。各データ セット設定ページには、データ セットの実行表が表示されます。表には次の列があります。

- 実行されたタスクの情報には、次の項目が含まれています。
  - [Last Execution Start Time]：データセット タスクの実行が開始された日付および時刻。
  - [End Time]：データセット タスクの実行が停止された日付および時刻。
  - [Elapsed Time (secs)]：タスクの実行に要した時間（秒）を示します。
  - [Result]：タスクの成功または失敗を示します。
  - [Additional Information]：特定のタスクに関するその他の情報を出力します。

各データ セット設定ページの [Collection Set Details] グループ ボックスには、次のパラメータおよび情報が含まれます。

- [Description]：データ セットの簡単な表示専用の説明を出力します。
- [Data Aggregation]：データ セットによって収集されたデータが集約されているかどうかを示します。
- [Used By Report(s)]：データ セットを使用するレポートの表示名。
  - [CleanAir Air Quality]：このデータ セットは、最低電波品質 AP（Worst Air Quality APs）レポートおよび電波品質対時間（Air Quality versus Time）レポート に使用されます。
  - [Interferers]：このデータ セットは最悪干渉源（Worst Interferers）レポート に使用されます。
- [Collection Status]：データ収集を有効にするには、[Enabled] チェックボックスをオンにします。

[Interval (min.)]：データ セット実行間隔を時間（分）で入力します。有効な値は 1 ～ 120 分です。

各データ セット設定ページの [Data Management] グループ ボックスには、次のパラメータが含まれます。

- [Non-Aggregation Data Retain Period (Days)]：データ セットによって収集された非集約データを保持する日数を入力します。有効な値は 1 ～ 31 日です。
- [Retain Aggregation Raw Data]：集約された生データの保持を有効にするには、[Enabled] チェックボックスをオンにします。

（注） [Aggregation Raw Data Retain Period] 設定は、ポーリングされた生データに適用されます。集約された傾向データの保持期間を設定するには、[Administration] > [Settings] の順に選択し、左側のサイドバー メニューから [Data Management] を選択します。

（注） 集約データおよび非集約データの詳細については、「コントローラの自動プロビジョニングの設定」（P.9-532）を参照してください。

（注） この例では、タスクとして Prime Infrastructure サーバのバックアップの実行が選択されています。各ページのフィールドに入力する情報は、選択したタスクによって異なります。

ステップ 3　[Enabled] チェックボックスをオンにします。

ステップ 4　[Report History Backup] チェックボックスをオンにします。

ステップ 5　[Max Backups to Keep] テキスト ボックスに、サーバ上に保存するバックアップ ファイルの最大数を入力します。

範囲：7 ～ 50

デフォルト：7

（注） Prime Infrastructure プラットフォームのディスク領域が不足しないようにするため、バックアップ ファイルの数がこのテキスト ボックスに入力した値を超えると、サーバによって古いバックアップ ファイルが自動的に削除されます。

ステップ 6　[Interval (Days)] テキスト ボックスに、バックアップの間隔を日数で入力します。たとえば、1 = 毎日のバックアップ、2 = 1 日おきのバックアップ、7 = 毎週のバックアップなどを入力します。

範囲：1 ～ 360

デフォルト：7

ステップ 7　[Time of Day] テキスト ボックスに、バックアップの開始時刻を入力します。次の形式で入力してください。*hh:mm AM/PM*（例：03:00 AM）AM/PM 表記が指定されていない場合、入力した時刻は常に AM になります。午後 5 時を指定する場合は、17:00 または 5:00 PM と入力します。保存後にページに再びアクセスすると、時刻は PM 指定されずに hh:mm（この場合は 17:00）として表示されます。

（注）　大きなデータベースのバックアップは、Prime Infrastructure サーバのパフォーマンスに影響を与えます。そのため、Prime Infrastructure サーバがアイドル状態にある時間帯（深夜など）にバックアップの実行をスケジューリングすることを推奨します。

ステップ 8　[Submit] をクリックして設定値を保存します。バックアップ ファイルは .zip ファイルとして ftp-install-dir/ftp-server/root/NCSBackup ディレクトリに保存されます。.zip ファイルの形式は次のとおりです。*dd-mmm-yy_ hh-mm-ss*.zip
（例：11-Nov-05_10-30-00.zip）。

データ収集タスク

表 15-1 に、Prime Infrastructure のさまざまなデータ収集タスクのリストと説明を示します。

表 15-1　データ収集タスク

タスク名	タスクのステータス	デフォルトのスケジュール	説明
AP Image Pre-Download Status	無効	15 分	このタスクは、コントローラ内の関連する AP のイメージ事前ダウンロード ステータスの確認に使用されます。アクセス ポイントのステータスを表示するには、コントローラにソフトウェアをダウンロードしている間に [Pre-download software to APs] チェックボックスをオンにする必要があります。
Autonomous AP CPU and Memory Utilization	有効	15 分	このタスクは、Autonomous AP のメモリおよび CPU 使用率に関する情報の収集に使用されます。
Autonomous AP Inventory	有効	180 分	このタスクは、Autonomous AP のインベントリ情報の収集に使用されます。
Autonomous AP Radio Performance	有効	15 分	このタスクは、Autonomous AP の無線パフォーマンス情報および無線のアップまたはダウン ステータスに関する情報の収集に使用されます。
Autonomous AP Tx Power and Channel Utilization	有効	30 分	このタスクは、Autonomous AP の無線パフォーマンスに関する情報の収集に使用されます。
CleanAir Air Quality	有効	15 分	このタスクは、CleanAir 電波品質に関する情報の収集に使用されます。
Client Statistics	有効	15 分	このタスクは、Autonomous および Lightweight クライアントの統計情報の取得に役立ちます。

表 15-1　データ収集タスク （続き）

タスク名	タスクのステータス	デフォルトのスケジュール	説明
Controller Performance	有効	30 分	このタスクは、コントローラのパフォーマンス情報の収集に使用されます。
Guest Sessions	有効	15 分	このタスクは、ゲスト セッションに関する情報の収集に使用されます。
Interferers	有効	15 分	このタスクは、干渉源に関する情報の収集に使用されます。
Media Stream Clients	有効	15 分	このタスクは、クライアントのメディア ストリームに関する情報の収集に使用されます。
Mesh link Performance	有効	10 分	このタスクは、メッシュ リンクのパフォーマンスに関する情報の収集に使用されます。
Mesh Link Status	有効	5 分	このタスクは、メッシュ リンクのステータスの収集に使用されます。
Mobility Service Performance	有効	15 分	このタスクは、モビリティ サービス エンジンのパフォーマンスに関する情報の収集に使用されます。
Radio Performance	有効	15 分	このタスクは、ワイヤレス無線の統計情報の収集に使用されます。
Rogue AP	有効	120 分	このタスクは、不正アクセス ポイントに関する情報の収集に使用されます。
Traffic Stream Metrics	有効	8 分	このタスクは、クライアントのトラフィック ストリーム メトリックの取得に役立ちます。
CCX Client Statistics	無効	60 分	このタスクは、CCX バージョン 5 およびバージョン 6 クライアントの Dot11 およびセキュリティ統計を収集するために使用されます。
Wired Switch Inventory	有効	毎日午前 0 時	このタスクは、有線スイッチのインベントリ情報の収集に使用されます。
Wireless Controller Inventory	無効	毎日午前 0 時	このタスクは、ワイヤレス コントローラのインベントリ情報の収集に使用されます。

その他のバックグラウンド タスクの実行

Prime Infrastructure 管理機能を使用して、その他のバックグラウンド タスクを実行することもできます。

（注）　Database Cleanup タスクは、実行、有効化、または無効化できません。このタスクは、誤って削除されないように、無効になっています。

ここでは、その他の Prime Infrastructure バックグラウンド タスクの手順について説明します。内容は次のとおりです。

- 「アプライアンスのステータスの表示」（P.15-803）
- 「Autonomous AP クライアントのステータスの表示」（P.15-804）

- 「Autonomous AP の動作ステータスの表示」（P.15-805）
- 「設定の同期の実行」（P.15-806）
- 「Lightweight クライアントのステータスの表示」（P.15-808）
- 「コントローラ設定バックアップ ステータスの表示」（P.15-809）
- 「コントローラの動作ステータスの表示」（P.15-810）
- 「データ クリーンアップ ステータスの表示」（P.15-811）
- 「デバイス データの収集の実行」（P.15-812）
- 「ゲスト アカウントの同期の実行」（P.15-813）
- 「アイデンティティ サービス エンジン ステータスの表示」（P.15-814）
- 「ライセンス ステータスの更新」（P.15-815）
- 「Lightweight AP の動作ステータス」（P.15-816）
- 「Lightweight AP クライアントのステータス」（P.15-817）
- 「ロケーション アプライアンスのバックアップの実行」（P.15-818）
- 「ロケーション アプライアンス ステータスの表示」（P.15-820）
- 「ロケーション アプライアンスの同期の実行」（P.15-821）
- 「Prime Infrastructure サーバのバックアップの実行」（P.15-822）
- 「OSS サーバのステータスの表示」（P.15-823）
- 「冗長性ステータスの表示」（P.15-824）
- 「スイッチの NMSP およびロケーション ステータスの表示」（P.15-825）
- 「スイッチの動作ステータスの表示」（P.15-825）
- 「サードパーティ アクセス ポイントの動作ステータスの表示」（P.15-826）
- 「サードパーティ コントローラの動作ステータスの表示」（P.15-827）
- 「wIPS アラームの同期の実行」（P.15-828）
- 「Wired Client Status」（P.15-829）

その他のバックグラウンド タスクの詳細については、「他のバックグラウンド タスク」（P.15-831）を参照してください。

アプライアンスのステータスの表示

アプライアンスのステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Appliance Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

[Appliance Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

または

- タスクを無効にする。

  [Appliance Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3　タスクを変更するには、[Background Tasks] 列の [Appliance Status] リンクをクリックします。[Task] > [Appliance Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Appliance Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - タスクの経過時間（秒）。
  - [Result]：成功またはエラー。
  - [Message]：このタスクに関するテキスト メッセージ。

ステップ 5　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Interval]：タスクの頻度（分）を示します。

ステップ 6　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

Autonomous AP クライアントのステータスの表示

[Autonomous AP Client Status] ページを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Autonomous AP Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Autonomous AP Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

[Autonomous AP Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3　タスクを変更するには、[Background Tasks] 列の [Autonomous AP Client Status] リンクをクリックします。[Task] > [Autonomous AP Client Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Autonomous AP Client Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - タスクの経過時間（秒）。
  - [Result]：成功またはエラー。
  - [Message]：このタスクに関するテキスト メッセージ。

ステップ 5　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Interval]：タスクの頻度（分）を示します。

ステップ 6　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

Autonomous AP の動作ステータスの表示

[Autonomous AP Operational Status] ページを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Autonomous AP Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Autonomous AP Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Autonomous AP Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3　タスクを変更するには、[Background Tasks] 列の [Autonomous AP Operational Status] リンクをクリックします。[Task] > [Autonomous AP Operational Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Appliance Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - タスクの経過時間（秒）。
  - [Result]：成功またはエラー。
  - [Message]：このタスクに関するテキスト メッセージ。

ステップ 5　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Interval]：タスクの頻度（分）を示します。

ステップ 6　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

設定の同期の実行

設定の同期を実行するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Configuration Sync] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Configuration Sync] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Configuration Sync] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3　タスクを変更するには、[Background Tasks] 列の [Configuration Sync] リンクをクリックします。[Task] > [Configuration Sync] ページが表示されます

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Configuration Sync] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。

- タスクの経過時間（秒）。
- [Result]：成功、警告、またはエラー。
- [Message]：このタスクに関するテキスト メッセージ。

（注）　[Result] が [Warning] で [Message] に [Failed] が表示された場合、デバイスは到達不能です。

ステップ 5　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Used By Report(s)]：これらのタスク結果を使用する Prime Infrastructure レポートを示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Network Audit]：チェックボックスをオンにすると、セカンダリ ネットワーク監査が有効になります。
- [Security Index Calculation]：チェックボックスをオンにすると、セキュリティ インデックスの計算が有効になります。セキュリティ インデックスは [Monitor] > [Security] ページから利用できます。
- [RRM Audit]：チェックボックスをオンにすると、RRM 監査が有効になります。

（注）　コントローラ監査では、デバイスの Prime Infrastructure データベース内の値の矛盾を検出します。

（注）　デバイスの SNMP 値を問い合わせるために、Prime Infrastructure では https://<Prime Infrastructure-IP>/webacs/manObjDiagQueryAction.do という URL を使用できます。

（注）　ネットワーク監査では、ネットワーク内のすべてのコントローラが監査され、RRM 監査およびセキュリティ監査も実行されます。これらのオプションは、[Administration] > [Background Tasks] > [Other Background Tasks] > [Configuration Sync] ページから選択できます。

- [Time of Day (hh:mm AM|PM)]：このタスクの実行時刻（AM または PM）を示します。

（注）　[Time of Day (hh:mm AM|PM)] は、次の形式で入力してください。hh:mm AM/PM（例：03:00 AM）AM/PM 表記が指定されていない場合、入力した時刻は常に AM になります。午後 5 時を指定する場合は、17:00 または 5:00 PM と入力します。保存後にページに再びアクセスすると、時刻は PM 指定されずに hh:mm（この場合は 17:00）として表示されます。

ステップ 6　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

Lightweight クライアントのステータスの表示

[Administration] > [Background Tasks] を選択し、次に [Lightweight Client Status] をクリックしてこのページにアクセスします。

このページでは、Lightweight クライアント ステータスのポーリング バックアップの履歴と現在のステータスを表示できます。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページからこのタスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する：実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする：有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする：無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Lightweight Client Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 3　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

コントローラ設定バックアップ ステータスの表示

[Administration] > [Background Tasks] を選択し、次に [Controller Configuration Backup] をクリックしてこのページにアクセスします。

このページでは、Cisco WLAN ソリューション設定バックアップの履歴と現在のステータスを表示できます。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページからこのタスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する：実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする：有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする：無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Controller Configuration Backup] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

（注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。
- Time of Day (hh:mm AM|PM)

（注）　[Time of Day (hh:mm AM|PM)] は、次の形式で入力してください。hh:mm AM/PM（例：03:00 AM）AM/PM 表記が指定されていない場合、入力した時刻は常に AM になります。午後 5 時を指定する場合は、17:00 または 5:00 PM と入力します。保存後にページに再びアクセスすると、時刻は PM 指定されずに hh:mm（この場合は 17:00）として表示されます。

- [TFTP Server, FTP Server, SFTP Server]：次のいずれかを選択します。
  - [TFTP Server]：[TFTP Server] を選択した場合は、ドロップダウン リストからサーバまたは [Default Server] を選択します。
  - [FTP Server]：[FTP Server] を選択した場合は、ドロップダウン リストからサーバまたは [Default Server] を選択し、FTP ユーザ名、FTP パスワード、および FTP ポート情報を各テキスト ボックスに入力します。
  - [SFTP Server]：[SFTP Server] を選択した場合は、ドロップダウン リストからサーバまたは [Default Server] を選択し、SFTP ユーザ名、SFTP パスワード、アップロード先ディレクトリ、および SFTP ポート情報を各テキスト ボックスに入力します。

（注）　[Default Server] オプションを使用するには、[Administration] > [Settings] > [Server Settings] で TFTP を有効にする必要があります。詳細については、「サーバ設定値の設定」（P.15-871）を参照してください。

（注）　Prime Infrastructure に FTP サーバまたは TFTP サーバを追加した場合のみ、[Server] ドロップダウン リストにサーバ名が設定されます。FTP サーバまたは TFTP サーバを追加するには、「TFTP、FTP、SFTP サーバの設定」（P.9-556）を参照してください。

ステップ 3　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

コントローラの動作ステータスの表示

デバイスのステータスでは、コントローラの到達可能性と WiSM ピア情報をポーリングします。

[Administration] > [Background Tasks] を選択し、次に [Controller Operational Status] をクリックしてこのページにアクセスします。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページから [Controller Operational Status] タスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する : 実行する [Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする : [Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする : [Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

[Controller Operational Status] タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列の [Controller Operational Status] バックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Controller Operational Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result] : 成功またはエラー。
  - [Message] : タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description] : 表示のみ。タスクの名前を表示します。
- [Enabled] : このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval] : タスクの頻度（分）を示します。

ステップ 3　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

データ クリーンアップ ステータスの表示

（注）　Database Cleanup タスクは、実行、有効化、または無効化できません。このタスクは、誤って削除されないように、無効になっています。

[Administration] > [Background Tasks] を選択し、次に [Database Cleanup] をクリックしてこのページにアクセスします。

このページでは、Cisco WLAN ソリューション データベース クリーンアップの履歴と現在のステータスを表示できます。

このタスクを変更するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Data Cleanup] ページに、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 3　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- Time of Day (hh:mm AM|PM)

（注）　[Time of Day (hh:mm AM|PM)] は、次の形式で入力してください。hh:mm AM/PM（例：03:00 AM）AM/PM 表記が指定されていない場合、入力した時刻は常に AM になります。午後 5 時を指定する場合は、17:00 または 5:00 PM と入力します。保存後にページに再びアクセスすると、時刻は PM 指定されずに hh:mm（この場合は 17:00）として表示されます。

ステップ 4　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

デバイス データの収集の実行

デバイス データの収集を実行するには、以下の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Device Data Collection] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Device Data Collection] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Device Data Collection] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列のタスクが灰色になります。

ステップ 3　タスクを変更するには、[Background Tasks] 列の [Device Data Collection] リンクをクリックします。[Task] > [Device Data Collector] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Device Data Collector] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - タスクの経過時間（秒）。
  - [Result]：成功またはエラー。
  - [Message]：このタスクに関するテキスト メッセージ。

ステップ 5　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：チェックボックスをオンにすると、このタスクが有効になります。
- [Controller IP address]：データの収集元のコントローラの IP アドレス。
- [CLI Commands]：指定されたコントローラで実行するコマンドライン インターフェイス コマンドをカンマで区切って入力します。
- [Clean Start]：データ収集の前にクリーン スタートを有効または無効にするには、このチェックボックスをオンまたはオフにします。
- [Repeat]：データ収集を実行する回数を入力します。
- [Interval]：データ収集を実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。

ステップ 6　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

ゲスト アカウントの同期の実行

[Administration] > [Background Tasks] を選択し、次に [Guest Accounts Sync] をクリックしてこのページにアクセスします。

このページでは、ゲスト アカウントの同期タスクの履歴と現在のステータスを表示できます。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページからこのタスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する：実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする：有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする：無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Guest Accounts Synchronization] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

（注） [Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。
- Time of Day (hh:mm AM|PM)

（注） [Time of Day (hh:mm AM|PM)] は、次の形式で入力してください。hh:mm AM/PM（例：03:00 AM）AM/PM 表記が指定されていない場合、入力した時刻は常に AM になります。午後 5 時を指定する場合は、17:00 または 5:00 PM と入力します。保存後にページに再びアクセスすると、時刻は PM 指定されずに hh:mm（この場合は 17:00）として表示されます。

ステップ 3　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

アイデンティティ サービス エンジン ステータスの表示

アイデンティティ サービス エンジンのステータスを更新するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Identity Services Engine Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Identity Services Engine Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Identity Services Engine Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　[Identity Services Engine Status] タスクを変更するには、[Background Tasks] 列の [Identity Services Engine Status] リンクをクリックします。[Identity Services Engine Status] ページが表示されます。

ステップ 4　[Task] 列の [Identity Services Engine Status] バックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[Identity Services Engine Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

ライセンス ステータスの更新

ライセンスのステータスを更新するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [License Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

[License Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

または

- タスクを無効にする。

  [License Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　コントローラ ライセンスのリセット タスクを変更するには、[Background Tasks] 列の [License Status] リンクをクリックします。[License Status] ページが表示されます。

このページは、最新のライセンスの再同期が実行されたときに表示されます。デフォルトでは、4 時間ごとに実行されます。このページから、このタスクを無効にするか、実行間隔を変更できます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[License Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

Lightweight AP の動作ステータス

Lightweight AP の動作ステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Lightweight AP Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

[Lightweight AP Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

または

- タスクを無効にする。

  [Lightweight AP Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　コントローラ ライセンスのリセット タスクを変更するには、[Background Tasks] 列の [Lightweight AP Operational Status] リンクをクリックします。[License Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[Lightweight AP Operational Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

Lightweight AP クライアントのステータス

Lightweight AP クライアントのステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Lightweight AP Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

[Lightweight AP Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

または

- タスクを無効にする。

  [Lightweight AP Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　コントローラ ライセンスのリセット タスクを変更するには、[Background Tasks] 列の [Lightweight AP Client Status] リンクをクリックします。[License Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[Lightweight AP Client Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

ロケーション アプライアンスのバックアップの実行

[Administration] > [Background Tasks] を選択し、次に [ロケーション アプライアンス Backup] をクリックしてこのページにアクセスします。

このページでは、モビリティ サービス エンジン データベースのバックアップをスケジュールできます。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページからこのタスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する：実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする：有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする：無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Mobility Service Backup] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Max backups to keep]：バックアップ サーバ上に保存するロケーション バックアップの最大数を入力します。
- [Interval (days)]：バックアップの頻度を入力します。
- [Time of the Day (hh:mm AM/PM)]：スケジュールされた日にバックアップを開始する時刻を入力します。

  （注）　[Time of Day (hh:mm AM|PM)] は、次の形式で入力してください。hh:mm AM/PM（例：03:00 AM）AM/PM 表記が指定されていない場合、入力した時刻は常に AM になります。午後 5 時を指定する場合は、17:00 または 5:00 PM と入力します。保存後にページに再びアクセスすると、時刻は PM 指定されずに hh:mm（この場合は 17:00）として表示されます。

- 完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

ロケーション アプライアンス ステータスの表示

[Administration] > [Background Tasks] を選択し、次に [ロケーション アプライアンス Status] をクリックしてこのページにアクセスします。

このページには、モビリティ サービス エンジンのステータスが表示されます。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページからこのタスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する：実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする：有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする：無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Mobility Service Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval (days)]：バックアップの頻度を入力します。

ステップ 3　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

ロケーション アプライアンスの同期の実行

[Administration] > [Background Tasks] を選択し、次に [ロケーション アプライアンス Synchronization] をクリックしてこのページにアクセスします。

このページでは、モビリティ サービス エンジン データベースを同期できます。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページからこのタスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する：実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする：有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする：無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Mobility Service Synchronization] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Out of Sync Alerts]：有効にすると、Prime Infrastructure に加えた変更がロケーション サーバに同期されていない場合に、マイナー アラームが生成されます。
- [Auto Synchronization]：この設定を使用して、ロケーション サーバの自動同期を有効にします。これにより、Prime Infrastructure に変更を加えたときに、ロケーション サーバはその変更を自動的に同期するようになります。
- [Interval (minutes)]：自動同期の間隔を指定します。

ステップ 3　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

Prime Infrastructure サーバのバックアップの実行

[Administration] > [Background Tasks] の順に選択し、次に [Prime Infrastructure Server Backup] をクリックしてこのページにアクセスします。

このページでは、Prime Infrastructure サーバのバックアップをスケジュールできます。

[Administration] > [Background Tasks] ページで、このタスクを実行、有効化、または無効化できます。[Administration] > [Background Tasks] ページからこのタスクを実行、有効化、または無効化するには、次の手順を実行します。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　実行、有効化、または無効化するバックグラウンド タスクのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストを使用して、次の作業のいずれかを実行します。

- すぐにタスクを実行する：実行するタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列のステータスが変わります。

  または

- タスクを有効にする：有効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。

  または

- タスクを無効にする：無効にするタスクのチェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。

タスクを変更するには、次の手順を実行します。

ステップ 1　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

[Prime Infrastructure Server Backup] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 2　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Report History Backup]：このチェックボックスをオンにすると、Prime Infrastructure によるレポート履歴のバックアップが有効になります。
- [Max Backups to Keep]：バックアップ サーバ上に保存する Prime Infrastructure サーバのバックアップの最大数を入力します。

- [Backup Repository]：既存のバックアップ リポジトリを選択するか、[Create] をクリックして新規バックアップ リポジトリを作成します。
- [Interval (days)]：1 ～ 360 の値を入力します。Prime Infrastructure サーバのデータは *n* 日ごとにバックアップされます。ここで、*n* はこのフィールドに指定された値です。
- [Time of the Day (hh:mm AM/PM)]：スケジュールされた日にバックアップを開始する時刻を入力します。

（注）　[Time of Day (hh:mm AM|PM)] は、次の形式で入力してください。hh:mm AM/PM（例：03:00 AM）AM/PM 表記が指定されていない場合、入力した時刻は常に AM になります。午後 5 時を指定する場合は、17:00 または 5:00 PM と入力します。保存後にページに再びアクセスすると、時刻は PM 指定されずに hh:mm（この場合は 17:00）として表示されます。

- 完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

OSS サーバのステータスの表示

OSS サーバのステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [OSS Server Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [OSS Server Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [OSS Server Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　コントローラ ライセンスのリセット タスクを変更するには、[Background Tasks] 列の [OSS Server Status] リンクをクリックします。[OSS Server Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[OSS Server Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）

- [Result]：成功またはエラー。
- [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

（注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

冗長性ステータスの表示

冗長性ステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Redundancy Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Redundancy Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Redundancy Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　[Redundancy Status] タスクを変更するには、[Background Tasks] 列の [Redundancy Status] リンクをクリックします。[Redundancy Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[Redundancy Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

（注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Save] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

スイッチの NMSP およびロケーション ステータスの表示

Cisco Prime Infrastructure 管理機能の [Switch NMSP and Location Status] オプションを使用して、スイッチの NMSP およびロケーション ステータスを表示できます。

スイッチの NMSP およびロケーション ステータスを表示するには、次の手順を実行します。

ステップ 1　[Prime Infrastructure] > [Administration] > [Background Tasks] の順に選択します。

ステップ 2　[Other Background Tasks] 表で、[Switch NMSP and Location Status] リンクをクリックします。

[Switch NMSP and Location Status] ページが表示されます。

[Switch NMSP and Location Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 3　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

（注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval (hours)]：バックアップの頻度を入力します。

ステップ 4　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

スイッチの動作ステータスの表示

スイッチの動作ステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Switch Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Switch Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Switch Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　[Switch Operational Status] タスクを変更するには、[Background Tasks] 列の [Switch Operational Status] リンクをクリックします。[Switch Operational Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[Switch Operational Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

サードパーティ アクセス ポイントの動作ステータスの表示

サードパーティ アクセス ポイントの動作ステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Third party Access Point Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Third party Access Point Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Third party Access Point Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　[Third party Access Point Operational Status] タスクを変更するには、[Background Tasks] 列の [Third party Access Point Operational Status] リンクをクリックします。[Third party Access Point Operational Status] ページが表示され、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 4　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（時間）を示します。

ステップ 5　完了したら、[Save] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

サードパーティ コントローラの動作ステータスの表示

サードパーティ コントローラの動作ステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

[Third Party Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

または

- タスクを有効にする。

  [Third Party Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Third Party Controller Operational Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　[Third Party Controller Operational Status] タスクを変更するには、[Background Tasks] 列の [Third Party Controller Operational Status] リンクをクリックします。[Third Party Controller Operational Status] ページが表示され、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 4　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（時間）を示します。

ステップ 5　完了したら、[Save] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

wIPS アラームの同期の実行

wIPS アラームの同期を実行するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [wIPS Alarm Sync] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

または

- タスクを有効にする。

  [wIPS Alarm Sync] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [wIPS Alarm Sync] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　[wIPS Alarm Sync] タスクを変更するには、[Background Tasks] 列の [wIPS Alarm Sync] リンクをクリックします。[wIPS Alarm Sync] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[wIPS Alarm Sync] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：タスクの頻度（日）を示します。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

Wired Client Status

有線クライアントのステータスを表示するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

ステップ 2　このページで、次のいずれかを実行します。

- すぐにタスクを実行する。

  [Wired Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Execute Now] を選択し、[Go] をクリックします。[Enabled] 列にステータス変更が表示されます。

  または

- タスクを有効にする。

  [Wired Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。[Enabled] 列のタスクが灰色から使用可能な状態に変わります。

  または

- タスクを無効にする。

  [Wired Client Status] チェックボックスをオンにします。[Select a command] ドロップダウン リストから、[Disable Task] を選択し、[Go] をクリックします。無効化が完了すると、[Enabled] 列でタスクが灰色から使用可能に変わります。

ステップ 3　[Wired Client Status] タスクを変更するには、[Background Tasks] 列の [Wired Client Status] リンクをクリックします。[Wired Client Status] ページが表示されます。

ステップ 4　[Task] 列のバックグラウンド タスクをクリックし、タスク詳細ページを開きます。

ステップ 5　[Wired Client Status] ページには、次の情報が表示されます。

- 最後の実行情報
  - 開始時刻および終了時刻。
  - 経過時間（秒）
  - [Result]：成功またはエラー。
  - [Message]：タスクの実行に関するテキスト メッセージ。

ステップ 6　[Edit Task] グループ ボックスで、次の項目を表示または編集します。

- [Description]：表示のみ。タスクの名前を表示します。
- [Enabled]：このチェックボックスをオンにすると、このタスクが有効になります。

  （注）　[Enabled] チェックボックスがオフの場合、タスクは指定された時刻には実行されません。

- [Interval]：有線クライアント ステータスのポーリングを実行する間隔を時間単位で入力します。有効な範囲は 1 ～ 8640 時間です。
- [Major Polling]：メジャー ポーリングを実行する 2 つの時間間隔を指定します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。

  有線クライアントの場合、Prime Infrastructure は定期的にマネージド スイッチをポーリングし、新たなクライアントや既存のクライアントへの変更を検出します。この検出を実行するために、Prime Infrastructure はインターフェイスの最後の変更時刻をキャッシュします。次のポーリング時に、インターフェイスの新たな変更時刻の値とキャッシュされた値をチェックして、インターフェイスに変更があったかどうかを判断します。ポーリングは変更があったインターフェイスのみを対象に実行されます。ポーリング間でインターフェイスに変更がなかった場合、そのインターフェイスへのポーリングは実行されません。ポーリングがメジャー ポーリングのスケジュールの間に実行される場合、インターフェイスへの変更有無に関係なく完全なポーリングが実行されます。メジャー ポーリングとマイナー ポーリングを実行する理由は、有線クライアントのすべてのインターフェイスに対してスイッチのポーリングを実行すると、Prime Infrastructure およびスイッチに対してコストがかかり、リソースを消費するためです。このため、メジャー ポーリングは 1 日 2 回のみ実行されます。

ステップ 7　完了したら、[Submit] をクリックしてタスクの変更内容を確定するか、[Cancel] をクリックして変更せずに [Administration] > [Background Tasks] ページに戻ります。

他のバックグラウンド タスク

表 15-2 に、Prime Infrastructure で使用できるその他のバックグラウンド タスクの説明を示します。

表 15-2　他のバックグラウンド タスク

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Appliance Status	5 分	このタスクは、アプライアンスのポーリングの詳細を表示するために使用されます。このタスクでは、[Administration] > [Appliance] > [Appliance Status] ページからアプライアンスのポーリングの詳細が読み込まれます。また、このバックグラウンド タスクでは、アプライアンスのパフォーマンス、障害検査機能などの情報が読み込まれます。	デフォルト：有効 [Interval]：有効な間隔（1 ～ 10080） 詳細については、「アプライアンスのステータスの表示」（P.15-803）を参照してください。
Autonomous AP Client Status	5 分	このタスクは、ネットワークからの Autonomous AP クライアントの検出に役立ちます。	デフォルト：有効 詳細については、「Autonomous AP クライアントのステータスの表示」（P.15-804）を参照してください。
Autonomous AP Operational Status	5 分	このタスクは、Autonomous AP の動作ステータスのポーリングを表示するために役立ちます。	デフォルト：有効 [Interval]：有効な間隔（1 ～ 10080） 詳細については、「Autonomous AP の動作ステータスの表示」（P.15-805）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Configuration Sync	毎日午前 4 時	このタスクは、設定の同期の表示に使用されます。	[Enable]：設定の同期を有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルト：有効 [Enable]：ネットワークの監査を有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルト：有効 [Enable]：セキュリティ インデックスの計算を有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルト：有効 [Enable]：RRM 監査を有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：設定の同期を実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 [Time of Day]：設定の同期を実行する時刻を入力します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。 詳細については、「設定の同期の実行」（P.15-806）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Controller Configuration Backup	毎日午後 10 時	このタスクは、コントローラ設定のバックアップ アクティビティの表示に使用されます。	[Enable]：コントローラ設定のバックアップを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、無効になっています。 [Interval]：設定の同期を実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 [Time of Day]：設定の同期を実行する時刻を入力します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。 [TFTP Server]：コントローラ設定のバックアップ先のサーバの IP アドレスを選択します。 詳細については、「コントローラ設定バックアップ ステータスの表示」（P.15-809）を参照してください。
Controller Operational Status	5 分	このタスクは、コントローラの動作ステータスのスケジュールおよび表示に使用されます。	[Enable]：コントローラ設定のバックアップを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：設定の同期を実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 詳細については、「コントローラの動作ステータスの表示」（P.15-810）を参照してください。
Data Cleanup	毎日午前 2 時	このタスクは、データのクリーンアップのスケジュールに使用されます	[Time of Day]：データのクリーンアップを実行する時刻を入力します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。デフォルトでは、有効になっています。 詳細については、「データ クリーンアップ ステータスの表示」（P.15-811）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Device Data Collector	30 分	このタスクは、指定されたコマンドライン インターフェイス コマンドに基づいたデータ収集を、設定された時間間隔でスケジュールするために使用されます。	[Enabled]：指定されたコントローラのデータ収集を有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、無効になっています。 [Controller IP address]：データの収集元のコントローラの IP アドレス。 [CLI Commands]：指定されたコントローラで実行する CLI コマンドをカンマで区切って入力します。 [Clean Start]：データ収集の前にクリーン スタートを有効または無効にするには、このチェックボックスをオンまたはオフにします。 [Repeat]：データ収集を実行する回数を入力します。 [Interval]：データ収集を実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 詳細については、「デバイス データの収集の実行」（P.15-812）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Guest Accounts Sync	毎日午前 1 時	このタスクは、ゲスト アカウントのポーリングおよび同期のスケジュールに使用されます。	[Enable]：ゲスト アカウントの同期を有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：ゲスト アカウントの同期を実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 [Time of Day]：ゲスト アカウントの同期を実行する時刻を入力します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。 詳細については、「ゲスト アカウントの同期の実行」（P.15-813）を参照してください。
Identity Services Engine Status	15 分	このタスクは、アイデンティティ サービス エンジンのポーリングのスケジュールに使用されます。	[Enable]：アイデンティティ サービス エンジンのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：アイデンティティ サービス エンジンのポーリングを実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 詳細については、「アイデンティティ サービス エンジン ステータスの表示」（P.15-814）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
License Status	4 時間	このタスクは、ライセンス ステータスのポーリングのスケジュールに使用されます。	[Enable]：ライセンス ステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：ライセンス ステータスのポーリングを実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 詳細については、「ライセンス ステータスの更新」（P.15-815）を参照してください。
Lightweight AP Operational Status	5 分。	このタスクは、Lightweight AP の動作ステータスのポーリングを表示するために役立ちます。	[Enable]：Lightweight AP の動作ステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：Lightweight AP の動作ステータスのポーリングを実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 詳細については、「Lightweight AP の動作ステータス」（P.15-816）を参照してください。
Lightweight Client Status	5 分。	このタスクは、ネットワークからの Lightweight AP クライアントの検出に役立ちます。	[Enable]：Lightweight クライアント ステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：Lightweight クライアント ステータスのポーリングを実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 詳細については、「Lightweight AP クライアントのステータス」（P.15-817）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Mobility Service Backup	7 日ごとに午前 1 時	このタスクは、モビリティ サービス バックアップのポーリングのスケジュールに使用されます。	[Enable]：モビリティ サービスのバックアップを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、無効になっています。 [Interval]：モビリティ サービスのバックアップを実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 [Time of Day]：モビリティ サービスのバックアップを実行する時刻を入力します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。 詳細については、「ロケーション アプライアンスのバックアップの実行」（P.15-818）を参照してください。
Mobility Service Status	5 分。	このタスクは、モビリティ サービス ステータスのポーリングのスケジュールに使用されます。	[Enable]：モビリティ サービス ステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：モビリティ サービス ステータスのポーリングを実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 詳細については、「ロケーション アプライアンス ステータスの表示」（P.15-820）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Mobility Service Synchronization	60 分	このタスクは、モビリティ サービスの同期のスケジュールに使用されます。	[Out of Sync Alerts]：同期外れアラートを有効にする場合は、このチェックボックスをオンにします。 [Smart Synchronization]：スマート同期を有効にする場合は、このチェックボックスをオンにします。デフォルトでは、有効になっています。 [Interval]：モビリティ サービスの同期を実行する間隔を分単位で入力します。有効な範囲は 1 ～ 10080 分です。 詳細については、「ロケーション アプライアンスの同期の実行」（P.15-821）を参照してください。
Prime Infrastructure Server Backup	7 日ごとに午前 1 時	このタスクは、Prime Infrastructure サーバのバックアップのスケジュールに使用されます。	[Enable]：Prime Infrastructure サーバのバックアップを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、無効になっています。 [Interval]：Prime Infrastructure サーバのバックアップを実行する間隔を日単位で入力します。有効な範囲は 1 ～ 360 日です。 [Time of Day]：Prime Infrastructure サーバのバックアップを実行する時刻を入力します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。 詳細については、「Prime Infrastructure サーバのバックアップの実行」（P.15-822）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
OSS Server Status	5 分。	このタスクは、OSS サーバ ステータスのポーリングのスケジュールに使用されます。	[Enable]：OSS サーバのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：OSS サーバのポーリングを実行する間隔を分単位で入力します。有効な範囲は 1 ～ 10080 分です。 詳細については、「OSS サーバのステータスの表示」（P.15-823）を参照してください。
Redundancy Status	60 分	このタスクは、プライマリおよびセカンダリ コントローラの冗長性ステータスを表示するために使用されます。	[Enable]：冗長性ステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、無効になっています。 [Interval]：冗長性ステータスのポーリングを実行する間隔を分単位で入力します。 詳細については、「冗長性ステータスの表示」（P.15-824）を参照してください。
Switch NMSP and Location Status	4 時間	このタスクは、スイッチの NMSP および都市ロケーションのポーリングのスケジュールに使用されます。	[Enable]：スイッチの NMSP および都市ロケーションのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：スイッチの NMSP および都市ロケーションのポーリングを実行する間隔を分単位で入力します。有効な範囲は 1 ～ 10080 分です。 詳細については、「スイッチの NMSP およびロケーション ステータスの表示」（P.15-825）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Switch Operational Status	5 分。完全なポーリングは 15 分です。	このタスクは、スイッチの動作ステータスのポーリングをスケジュールするために使用されます。	[Enable]：スイッチの NMSP および都市ロケーションのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。 [Interval]：スイッチの NMSP および都市ロケーションのポーリングを実行する間隔を分単位で入力します。有効な範囲は 1 ～ 10080 分です。 [Full operational status interval]：間隔を分単位で入力します。有効な範囲は 1 ～ 1440 分です。 詳細については、「スイッチの動作ステータスの表示」（P.15-825）を参照してください。
Third party Access Point Operational Status	3 時間	このタスクは、サードパーティ AP の動作ステータスのポーリングをスケジュールするために使用されます。	[Enable]：サードパーティ AP の動作ステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。 [Interval]：サードパーティ AP の動作ステータスのポーリングを実行する間隔を時間単位で入力します。有効な範囲は 3 ～ 4 時間です。 詳細については、「サードパーティ アクセス ポイントの動作ステータスの表示」（P.15-826）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
Third party Controller Operational Status	3 時間	このタスクは、サードパーティ コントローラの到達可能性ステータスのポーリングをスケジュールするために使用されます。	[Enable]：サードパーティ コントローラの到達可能性ステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。 [Interval]：サードパーティ コントローラの到達可能性ステータスのポーリングを実行する間隔を時間単位で入力します。有効な範囲は 3 ～ 4 時間です。 詳細については、「サードパーティ コントローラの動作ステータスの表示」（P.15-827）を参照してください。

表 15-2　他のバックグラウンド タスク （続き）

タスク名	デフォルトのスケジュール	説明	編集可能なオプション
wIPS Alarm Sync	120 分	このタスクは、wIPS アラームの同期のスケジュールに使用されます。	[Enable]：wIPS アラームの同期を有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：wIPS アラームの同期を実行する間隔を分単位で入力します。有効な範囲は 1 ～ 10080 分です。 詳細については、「wIPS アラームの同期の実行」（P.15-828）を参照してください。
Wired Client Status	2 時間	このタスクは、有線クライアントのステータスのポーリングをスケジュールするために使用されます。	[Enable]：有線クライアントのステータスのポーリングを有効または無効にするには、このチェックボックスをオンまたはオフにします。デフォルトでは、有効になっています。 [Interval]：有線クライアント ステータスのポーリングを実行する間隔を時間単位で入力します。有効な範囲は 1 ～ 8640 時間です。 [Major Polling]：メジャー ポーリングを実行する 2 つの時間間隔を指定します。有効な形式は、hh:mm AM|PM です。たとえば、12:49 AM と指定します。 詳細については、「Wired Client Status」（P.15-829）を参照してください。

仮想ドメインの設定

Prime Infrastructure 仮想ドメインは、一連の Prime Infrastructure デバイスおよび/またはマップで構成され、ユーザの表示をこれらの管理対象オブジェクトに関連する情報に制限します。

仮想ドメインを使用して、管理者はユーザが担当するデバイスおよびマップだけを表示できるようにすることができます。また、仮想ドメインのフィルタにより、ユーザはネットワークの割り当てられた部分*だけ*について、アラームを設定、表示およびレポートを生成できます。

（注）　仮想ドメインのマップ、コントローラ、アクセス ポイント、テンプレート、および設定グループという要素は分割できます。
仮想ドメインに分割できず、ルート パーティションからだけ使用できるのは、Google Earth マップ、自動プロビジョニング、およびモビリティ サービスです。

管理者は、許可した一連の仮想ドメインを各ユーザに指定します。ログインの際、ユーザについてこれらのドメインのうちアクティブとなるのは 1 つだけです。ユーザは、許可された別の仮想ドメインを [Virtual Domain] ドロップダウン リストから選択することで、現在の仮想ドメインを変更できます。仮想ドメインによって、すべてのレポート、アラーム、およびその他の機能がフィルタ処理されます。

Prime Infrastructure Release 1.0 以降では、ACS にタスク リストをエクスポートする際に、ACS に仮想ドメインを追加する必要があります。これには、デフォルトの ROOT-DOMAIN 仮想ドメインを使用できます。ACS に仮想ドメインを追加しない場合、ログインは許可されません。この仕様は、単一または複数のドメインに関係なく適用されます。

[Administration] > [Virtual Domain] ページを使用して、仮想ドメインを作成、編集、削除、インポート、またはエクスポートします。各仮想ドメインには、親仮想ドメインに含まれている要素のサブセットが含まれている場合があります。新しい仮想ドメインに追加のマップ、コントローラ、アクセス ポイント、およびスイッチを割り当てることができます。仮想ドメインの管理の詳細については、「仮想ドメインの管理」（P.15-848）を参照してください。

[Virtual Domain] ページには、次のボタンがあります。

- [New]：新しい仮想ドメインを作成します。詳細については、「仮想ドメインの新規作成」（P.15-847）を参照してください。
- [Delete]：選択した仮想ドメインを階層から削除します。
- [Import]：CSV ファイルをインポートします。
- [Export]：選択した仮想ドメインのカスタム属性を設定します。詳細については、「仮想ドメインの RADIUS 属性および TACACS+ 属性」（P.15-849）を参照してください。

ここでは、次の内容について説明します。

仮想ドメインの階層について

仮想ドメインは、階層構造で編成されています。既存の仮想ドメインのサブセットには、親仮想ドメインに含まれるネットワーク要素が含まれています。

（注）　デフォルトまたは「ROOT-DOMAIN」ドメインには、すべての仮想ドメインが含まれています。

ネットワーク要素は階層構造で管理されているため、レポート生成、検索、テンプレート、設定グループ、およびアラームなどの一部の機能およびコンポーネントが影響を受けます。

（注）　アクセス ポイントだけが割り当てられ、コントローラが割り当てられていない仮想ドメインを作成する場合、コントローラベースの機能のいくつかは選択できなくなります。たとえば、いくつかのオプションでは、コントローラからアクセス ポイントへドリルダウンする必要があります。コントローラは仮想ドメインにないため、関連付けられたレポートを生成できません。少数のコントローラのみでパーティションを作成し、[Configure] > [Access Points] を選択して、[AP Name] 列の各リンクをクリックすると、パーティションで指定されている限られた数のコントローラではなく、Prime Infrastructure によって割り当てられたプライマリ、セカンダリ、およびターシャリ コントローラの完全なリストが表示されます。

（注）　複数の仮想ドメインによってコントローラの設定が変更された場合、複雑な状況が発生する場合があります。これを回避するには、一度に 1 つの仮想ドメインから各コントローラを管理してください。

ここでは、パーティショニングの効果について説明します。内容は次のとおりです。

- 「レポート」（P.15-844）
- 「検索」（P.15-845）
- 「アラーム」（P.15-845）
- 「テンプレート」（P.15-845）
- 「設定グループ」（P.15-845）
- 「マップ」（P.15-845）
- 「アクセス ポイント」（P.15-846）
- 「コントローラ」（P.15-847）
- 「電子メール通知」（P.15-847）

レポート

レポートには、現在の仮想ドメインに割り当てられたコンポーネントだけが含まれています。たとえば、アクセス ポイントだけが割り当てられ、コントローラが割り当てられていない仮想ドメインを作成すると、コントローラのインベントリ レポートを生成したときに、一部のコントローラは表示されません。

アクセス ポイントだけが割り当てられ、コントローラが割り当てられていない仮想ドメインを作成する場合、コントローラベースの機能のいくつかは選択できなくなります。たとえば、いくつかのオプションでは、コントローラからアクセス ポイントへドリルダウンする必要があります。コントローラは仮想ドメインにないため、関連付けられたレポートを生成できません。

（注）　レポートは、現在の仮想ドメインにだけ表示されます。親仮想ドメインは、サブ仮想ドメインのレポートを表示できません。

Client Count などのクライアント レポートには、現在の仮想ドメインに属するクライアントだけが含まれます。

（注）　新しいクライアントが管理者によってこのパーティションに割り当てられていない場合、以前のレポートにはこれらの追加が反映されません。新しいレポートだけに新しいクライアントが反映されます。

検索

検索結果には、検索が実行される仮想ドメインに割り当てられたコンポーネントだけが含まれています。キャンパスが仮想ドメインに割り当てられていない場合、検索結果にフロア領域は表示されません。

（注）　保存された検索は、現在の仮想ドメインにだけ表示されます。親仮想ドメインは、これらの検索結果を表示できません。

（注）　Prime Infrastructure は、ネットワーク リストを分割しません。ネットワーク リストごとにコントローラを検索する場合、すべてのコントローラが返されます。

（注）　キャンパスが仮想ドメインに割り当てられていない場合、検索結果にフロア領域は表示されません。

アラーム

コンポーネントが仮想ドメインに追加された場合、そのコンポーネントの以前のアラームは、該当する仮想ドメインに表示されません。新しく生成されたアラームだけが表示されます。たとえば、新しいコントローラが仮想ドメインに追加されると、追加される前にそのコントローラに生成されたアラームは、現在の仮想ドメインには表示されません。

関連するコントローラまたはアクセス ポイントが仮想ドメインから削除された場合、同じ仮想ドメインのアラームは削除されません。

（注）　アラームの電子メールによる通知：ROOT-DOMAIN 仮想ドメインの場合のみ、ロケーション通知、ロケーション サーバ、および Prime Infrastructure 電子メール通知を有効にできます。

テンプレート

仮想ドメインでテンプレートを作成または検出する場合、そのテンプレートは、コントローラに適用されないかぎり、その仮想ドメインでだけ使用できます。テンプレートがコントローラに適用され、そのコントローラがサブ仮想ドメインに割り当てられる場合、テンプレートは新しい仮想ドメインのコントローラに適用されます。

（注）　サブ仮想ドメインを作成し、テンプレートを仮想ドメインの 2 つのネットワーク要素に適用すると、Prime Infrastructure はテンプレートが適用されたパーティションの数を不正に反映する場合があります。

設定グループ

仮想ドメインの設定グループは、親仮想ドメインでも表示できます。親仮想ドメインは、サブ（子）仮想ドメインの設定グループを変更できます。たとえば、親仮想ドメインは、サブ仮想ドメインのコントローラを追加または削除できます。

マップ

管理者が現在の仮想ドメインに割り当てたマップだけを表示できます。

- キャンパスが仮想ドメインに割り当てられた場合、そのキャンパスのすべてのビルディングが自動的に同じ仮想ドメインに割り当てられます。
- ビルディングが仮想ドメインに割り当てられると、そのビルディングに関連するすべてのフロアが自動的にビルディングに含まれます。
- フロアが割り当てられると、そのフロアに関連するすべてのアクセス ポイントが自動的にフロアに含まれます。

（注）　仮想ドメインにフロアだけが割り当てられる場合、マップベースの機能のいくつかが選択できなくなります。たとえば、いくつかのレポートおよび検索では、キャンパスからビルディング、フロアへドリルダウンする必要があります。キャンパスおよびビルディングは仮想ドメインにないため、これらの種類のレポートまたは検索を生成できません。

（注）　Prime Infrastructure に表示されるカバレッジ エリアは、キャンパスおよびビルディングにだけ適用されます。フロアだけの仮想ドメインの場合、Prime Infrastructure にカバレッジ エリアは表示されません。

（注）　フロアが直接仮想ドメインに割り当てられる場合、フロアが属しているビルディングがある仮想ドメインからそのフロアを削除できません。

（注）　キャンパスが仮想ドメインに割り当てられていない場合、検索結果にフロア領域は表示されません。

アクセス ポイント

コントローラまたはマップが仮想ドメインに割り当てられている場合、そのコントローラまたはマップに関連するアクセス ポイントも自動的に割り当てられます。アクセス ポイントを仮想ドメインに手動で（コントローラまたはマップとは別に）割り当てることができます。

（注）　コントローラを仮想ドメインから削除する場合、関連するすべてのアクセス ポイントも削除されます。アクセス ポイントが手動で割り当てられている場合、関連するコントローラが現在の仮想ドメインから削除されている場合でも、そのアクセス ポイントは割り当てられたままになります。

（注）　アクセス ポイントだけが割り当てられ、コントローラが割り当てられていない仮想ドメインを作成する場合、コントローラベースの機能のいくつかは選択できなくなります。たとえば、いくつかのオプションでは、コントローラからアクセス ポイントへドリルダウンする必要があります。コントローラは仮想ドメインにないため、関連付けられたレポートを生成できません。

（注）　手動で追加されたアクセス ポイントが仮想ドメインから削除されているにもかかわらず、同じ仮想ドメインに割り当てられているコントローラまたはマップに関連付けられている場合、そのアクセス ポイントは仮想ドメインで表示されたままになります。アクセス ポイントが削除されても、このアクセス ポイントに関連するアラームは削除されません。

（注）　マップを仮想ドメインから削除する場合、マップ上のアクセス ポイントを仮想ドメインから削除できます。

（注）　アクセス ポイントを後で別の場所に移動すると、（生成されたアラームなどの）いくつかのイベントが、元のパーティションの場所に残ったままになる場合があります。

（注）　不正アクセス ポイントのパーティションは、検出中のいずれかのアクセス ポイント（最新または最も強い RSSI 値を持つアクセス ポイント）と関連付けられます。検出中のアクセス ポイント情報がある場合、Prime Infrastructure は検出中のコントローラを使用します。
不正アクセス ポイントが異なるパーティションに存在する 2 つのコントローラによって検出された場合、不正アクセス ポイントのパーティションは随時変更される場合があります。

コントローラ

ネットワーク要素は階層構造で管理されているため、コントローラはパーティションによって影響を受ける場合があります。アクセス ポイントだけが割り当てられ、コントローラが割り当てられていない仮想ドメインを作成する場合、コントローラベースの機能のいくつかは選択できなくなります。たとえば、いくつかのオプションでは、コントローラからアクセス ポイントへドリルダウンする必要があります。コントローラは仮想ドメインにないため、関連付けられたレポートを生成できません。

少数のコントローラのみでパーティションを作成し、[Configure] > [Access Points] を選択して、[AP Name] 列の各リンクをクリックすると、パーティションで指定されている限られた数のコントローラではなく、Prime Infrastructure によって割り当てられたプライマリ、セカンダリ、およびターシャリ コントローラの完全なリストが表示されます。

（注）　複数の仮想ドメインによってコントローラの設定が変更された場合、複雑な状況が発生する場合があります。これを回避するには、一度に 1 つの仮想ドメインから各コントローラを管理してください。

電子メール通知

仮想ドメインごとに電子メール通知を設定できます。対象の仮想ドメインでアラームが発生した場合にだけ電子メールが送信されます。

仮想ドメインの新規作成

（注）　詳細については、「仮想ドメインの管理」（P.15-848）を参照してください。

新しい仮想ドメインを作成するには、次の手順を実行します。

ステップ 1　[Administration] > [Virtual Domains] を選択します。

ステップ 2　[Virtual Domain Hierarchy] 左サイドバー メニューで、サブ（子）仮想ドメインを追加する仮想ドメインを選択します。

（注）　選択した仮想ドメインが、新規作成するサブ仮想ドメインの親仮想ドメインとなります。

ステップ 3　[New] をクリックします。

[Virtual Domain Creation] ポップアップ ダイアログボックスが表示されます。

ステップ 4　テキスト ボックスに仮想ドメイン名を入力します。

ステップ 5　[Submit] をクリックすると仮想ドメインが作成され、[Cancel] をクリックすると変更せずにポップアップ ダイアログボックスが閉じます。

（注）　各仮想ドメインには、親仮想ドメインに含まれている要素のサブセットが含まれている場合があります。ユーザに仮想ドメインが割り当てられると、ユーザには親仮想ドメインに割り当てられるものと同じマップ、コントローラ、アクセス ポイントが表示される場合があります。

（注）　現在の仮想ドメイン名または説明を変更または更新するには、[Administration] > [Virtual Domains] を選択します。[Virtual Domain Hierarchy] 左サイドバー メニューで、編集する仮想ドメインを選択します。

仮想ドメインの管理

左サイドバー メニューの [Virtual Domain Hierarchy] で仮想ドメインを選択し、割り当てられたマップ、コントローラ、アクセス ポイント、およびスイッチを表示または編集します。[Summary] ページが表示されます。このページには、現在ログインしている仮想ドメインで使用可能なマップ、コントローラ、アクセス ポイント、およびスイッチを表示できるタブがあります。

（注）　すべてのマップ、コントローラ、およびアクセス ポイントはパーティション ツリーに含まれているため、このページの読み込みには数秒かかります。

[Maps] タブ、[Controllers] タブ、[Access Points] タブ、および [Switches] タブを使用して、この仮想ドメインに割り当てられているコンポーネントを追加または削除します。

サイト マップ、コントローラ、アクセス ポイント、または有線デバイスをこのドメインに割り当てるには、次の手順に従います。

ステップ 1　[Administration] > [Virtual Domains] を選択します。

ステップ 2　[Virtual Domain Hierarchy] 左サイドバー メニューから、仮想ドメイン階層を選択します。

（注）　すべてのマップ、コントローラ、およびアクセス ポイントはパーティション ツリーに含まれているため、読み込みには数分かかります。大量のコントローラおよびアクセス ポイントが存在するシステムの場合、この時間は増加します。

ステップ 3　該当する [Site Maps]、[Controller]、[Access Points]、または [Wired Devices] タブをクリックします。

ステップ 4　[Available]（[Site Maps]、[Controllers]、[Access Points]、または [Wired Devices]）列で、仮想ドメインに割り当てる新しいコンポーネントをクリックして強調表示します。

（注）　コンポーネントを [Selected]（[Site Maps]、[Controllers]、[Access Points]、または [Wired Devices]）に移動するには、[Add] をクリックします。仮想ドメインからコンポーネントを削除するには、[Selected]（[Site Maps]、[Controllers]、[Access Points]、または [Wired Devices]）列のコンポーネントをクリックして強調表示し、[Remove] をクリックします。コンポーネントが [Available] 列に戻ります。

（注）　ROOT-DOMAIN からスイッチ、コントローラ、または Autonomous AP を削除すると、そのデバイスは Prime Infrastructure から除去されます。デバイスが ROOT-DOMAIN に明示的にアソシエートされている場合、または現在の仮想ドメインの子ではない他の仮想ドメインに明示的にアソシエートされている場合、現在の仮想ドメインからデバイスを削除しても、そのデバイスはこの仮想ドメインからは除去されますが、Prime Infrastructure からは除去されません。

ステップ 5　[Submit] をクリックして、変更内容を確定します。

（注）　要素を仮想ドメインに割り当て変更を送信した後に、Prime Infrastructure がこれらの変更を処理するには、追加された要素の数に応じて、時間がかかる場合があります。

仮想ドメインの RADIUS 属性および TACACS+ 属性

[Virtual Domain Custom Attributes] ページを使用して、各仮想ドメインの適切なプロトコル固有のデータを指定することができます。[Virtual Domain Hierarchy] 左サイドバー メニューの [Export] ボタンを使用して、仮想ドメインの RADIUS 属性および TACACS+ 属性を事前に設定できます。これらの属性を ACS サーバにコピーして貼り付けることができます。これにより、該当する仮想ドメインだけを ACS サーバのページにコピーでき、ユーザはこれらの仮想ドメインだけにアクセスできるようになります。

設定済みの RADIUS 属性および TACACS+ 属性を ACS サーバに適用するには、次の手順を実行します。

ステップ 1　[Administration] > [Virtual Domains] を選択します。

ステップ 2　[Virtual Domain Hierarchy] 左サイドバー メニューで、RADIUS 属性および TACACS+ 属性を適用する仮想ドメインを選択します。

ステップ 3　[Export] をクリックします。

ステップ 4　（現在設定しているリストに応じて）[RADIUS Custom Attributes] リストまたは [TACACS+ Custom Attributes] リストのテキストを強調表示させ、ブラウザのメニューに移動し、[Edit] > [Copy] を選択します。

ステップ 5　ACS にログインします。

ステップ 6　[User Setup] または [Group Setup] に移動します。

（注）　ユーザ ベースで仮想ドメインを指定する場合、（たとえば、タスク、ロール、仮想ドメインなど）すべてのカスタム属性情報を [User] カスタム属性ページに追加していることを確認する必要があります。

ステップ 7　該当するユーザまたはグループの [Edit Settings] をクリックします。

ステップ 8　ブラウザの [Edit] > [Paste] の機能を使用して、RADIUS または TACACS+ のカスタム属性を該当するフィールドに入力します。

ステップ 9　チェックボックスをオンにして、これらの属性を有効にします。

ステップ 10　[Submit + Restart] をクリックします。

（注）　RADIUS 属性および TACACS+ 属性の ACS サーバへの追加の詳細は、「TACACS+ 用 ACS への Prime Infrastructure ユーザ グループの追加」（P.15-906）または「RADIUS 用 ACS への Prime Infrastructure ユーザ グループの追加」（P.15-907）を参照してください。

ユーザとしての仮想ドメインについて

ログインする際、管理者が割り当てたいずれかの仮想ドメインにアクセスできます。

ログイン時にアクティブにできる仮想ドメインは 1 つだけです。ページ上部の [Virtual Domain] ドロップダウン リストを使用して、現在の仮想ドメインを変更できます。割り当てられた仮想ドメインだけが、ドロップダウン リストに表示されます。

ドロップダウン リストから異なる仮想ドメインを選択すると、すべてのレポート、アラーム、およびその他の機能が、新しい仮想ドメインの条件によってフィルタ処理されます。

割り当てられた仮想ドメイン コンポーネントの表示

マップ、コントローラ、アクセス ポイント、スイッチなど、現在の仮想ドメインに割り当てられたすべてのコンポーネントを表示するには、[Administration] > [Virtual Domains] を選択します。[Summary] タブのリンクをクリックして、仮想ドメインに割り当てられたコンポーネントを表示します。

メニュー アクセスの制限

ROOT-DOMAIN でない仮想ドメインのユーザは、次の Prime Infrastructure メニューにはアクセスできません。

- [Monitor] > [RRM]
- [Configure] > [Auto Provisioning]
- [Configure] > [ACS View Servers]
- [Mobility] > [Mobility Services]
- [Mobility] > [Synchronize Servers]
- [Administration] > [Background Tasks]

- [Administration] > [Settings]
- [Administration] > [User Preferences]
- [Tools] > [Voice Audit]
- [Tools] > [Config Audit]

管理設定

設定には、Prime Infrastructure データ保持機能を管理するオプションが含まれています。ここでは、使用可能な一連のオプションについて説明します。内容は次のとおりです。

アラームとイベントの設定

この [Alarms and Events] ページでは、古いアラームを処理し、[Alarm Summary] ページに割り当て済みおよび承認済みのアラームを表示できます。

このページを開くには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Alarms and Events] を選択します。[Administration] > [System Settings] > [Alarms and Events] ページが表示されます。

ステップ 3　次の [Alarms and Events] のパラメータを追加または変更します。

- アラームとイベントのクリーンアップのオプション
  - [Delete active and cleared alarms after]: アクティブなアラームまたはクリアされたアラームが削除されるまでの日数を入力します。このオプションは、チェックボックスをオフにすることで無効にできます。
  - [Delete cleared security alarms after]：セキュリティ アラーム、不正 AP アラーム、およびアドホック不正アラームが削除されるまでの日数を入力します。
  - [Delete cleared non-security alarms after]：セキュリティ アラーム以外のアラームが削除されるまでの日数を入力します。セキュリティ アラーム以外のアラームには、[Security]、[Rogue AP]、または [Adhoc Rogue] カテゴリに属するアラーム以外のすべてのアラームが含まれます。
  - [Delete all events after]：すべてのイベントを削除するまでの日数を入力します。

（注）　データ クリーンアップ タスクは夜間に実行され、古いアラームが削除されます。データ クリーンアップ タスク以外に、Prime Infrastructure にはアラーム テーブル サイズを確認するための毎時タスクがあります。アラーム表のサイズが 300 K を超えると、タスクは 300 K 以内に収まるまで、クリアされたアラームのうち一番古いアラームを削除します。

（注）　クリアされたアラームを 7 日より多く保持する場合は、アラーム表のサイズが 300 K に達するまでに、[Delete cleared non-security alarms after] テキスト ボックスに 7 日より大きい値を指定します。

- Syslog クリーンアップのオプション
  - [Delete all syslogs after]：すべての Syslog を削除するまでの日数を入力します。
- Alarm Display Options

（注）　これらの設定は [Alarm Summary] ページのみに適用されます。任意のエンティティに対する Quick Search またはアラームでは、承認済みまたは割り当て済みの状態に関係なく、すべてのアラームが表示されます。

  - [Hide acknowledged alarms]：チェックボックスをオンにすると、承認済みのアラームは [Alarm Summary] ページに表示されません。このオプションは、デフォルトで有効です。

（注）　シビリティの変化に関係なく、承認済みのアラームに対して、電子メールは生成されません。

- [Hide assigned alarms]：チェックボックスをオンにすると、割り当て済みのアラームは [Alarm Summary] ページに表示されません。
- [Hide cleared alarms]：このチェックボックスをオンにすると、クリアされたアラームは [Alarm Summary] ページに表示されません。
- [Add controller name to alarm messages]：チェックボックスをオンにすると、アラーム メッセージにコントローラ名が追加されます。
- [Add NCS address to e-mail notifications]：このチェックボックスをオンにすると、電子メール通知に Prime Infrastructure アドレスが追加されます。

- アラームの電子メールのオプション
  - [Include alarm severity in the email subject line]：このチェックボックスをオンにすると、電子メールの件名にアラーム重大度が含まれるようになります。
  - [Include alarm Category in the email subject line]：このチェックボックスをオンにすると、電子メールの件名にアラームのカテゴリが含まれるようになります。
  - [Include prior alarm severity in the email subject line]：このチェックボックスをオンにすると、電子メールの件名に事前アラーム重大度が含まれるようになります。
  - [Include custom text in the email subject line]：このチェックボックスをオンにすると、電子メールの件名にカスタム テキストが追加されます。[Replace the e-mail subject line with custom text] チェックボックスをオンにして、電子メールの件名をカスタム テキストに置き換えることもできます。
  - [Include custom text in body of email]：チェックボックスをオンにすると、電子メールの本文にカスタム テキストが追加されます。
  - [Include alarm condition in body of email]：このチェックボックスをオンにすると、電子メールの本文にアラーム状態が含まれるようになります。
  - [Add link to Alarm detail page in body of email]：このチェックボックスをオンにすると、電子メールの本文に [Alarm detail] ページへのリンクが追加されます。
  - [Enable Secure Message Mode]：チェックボックスをオンにすると、セキュア メッセージ モードが有効になります。[Mask IP Address and Mask Controller Name] チェックボックスをオンにした場合、アラーム電子メールはセキュア モードで送信され、すべての IP アドレスとコントローラ名はマスクされます。
- アラームの他の設定
  - [Controller license count threshold]：必要なコントローラ ライセンスの最小数を入力します。コントローラ ライセンス数がこのしきい値未満の場合、アラームが生成されます。

ステップ 4　[Save] をクリックします。

監査の設定

[Administration] > [System Settings] > [Audit] ページでは、監査の種類と監査を実行するパラメータを決定できます。

- 監査モード：基本監査およびテンプレート ベースの監査のいずれかを選択します。

- 監査対象：すべてのパラメータの監査を実行するか、選択したパラメータでグローバル監査を実行するかを選択します。

監査モード

[Audit Mode] グループ ボックスでは、基本監査およびテンプレート ベースの監査のいずれかを選択できます。デフォルトでは、基本監査が選択されています。

- [Basic Audit] : Prime Infrastructure データベースの設定オブジェクトと現在の WLC デバイス値を照合して監査します。Prime Infrastructure 5.1.0.0 よりも前のバージョンでは、この監査モードのみが使用可能でした。

（注）　設定オブジェクトは、Prime Infrastructure データベースに保存されているデバイス構成を参照します。

- [Template-based Audit] : 適用されたテンプレート、設定グループのテンプレート（バックグラウンド監査に選択）、および設定の監査（該当するテンプレートが存在しない場合）を現在のコントローラ デバイスの値に対して監査します。

実行する監査の種類を指定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Audit] を選択します。[Audit] ページが表示されます。

ステップ 3　[Basic Audit] または [Template Based Audit] を選択します。基本監査では、Prime Infrastructure データベースの設定オブジェクトと現在のコントローラ設定が照合され監査されます。テンプレートベースの監査では、適用されたテンプレート、設定グループのテンプレート、および設定オブジェクト（該当するテンプレートが存在しない場合）を現在のコントローラの設定に対して監査します。

ステップ 4　すべてのパラメータの監査を実行するか、選択したパラメータの監査のみを実行するかを選択します。[Selected Parameters] オプション ボタンを選択した場合は、[Configure Audit Parameters] 設定ページにアクセスできます。（「監査パラメータの設定」（P.15-855）を参照してください）。[Select audit parameters URL] が表示されます。

選択した監査パラメータは、ネットワーク監査およびコントローラ監査で使用されます。

ステップ 5　[Save] をクリックします。

（注）　これらの設定は、コントローラの監査またはネットワークの監査が実行される場合に有効です。

監査対象

[Audit On] グループ ボックスでは、すべてのパラメータを監査するか、監査する特定のパラメータを選択できます。[Selected Parameters] オプション ボタンを選択すると、[Select Audit Parameters] 設定ページにアクセスできます。

選択した監査パラメータは、ネットワーク監査およびコントローラ監査で使用されます。

監査パラメータの設定

グローバル監査を実行する監査パラメータを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Audit] を選択します。

ステップ 3　[Selected Parameters] オプション ボタンを選択すると、[Select Audit Parameters] リンクが表示されます。

ステップ 4　[Save] をクリックします。

ステップ 5　[Administration] > [System Settings] > [Audit] > [Select Audit Parameters] ページで、[Select Audit Parameters] をクリックして監査の必須パラメータを選択します。

ステップ 6　各タブから、監査するパラメータを選択します。タブには、[System]、[WLAN]、[Security]、[Wireless]、[IPv6]、および [Selected Attributes] があります。

ステップ 7　必要なすべての監査パラメータを選択したら、[Submit] をクリックしてパラメータを確定するか、[Cancel] をクリックして監査パラメータを保存せずにページを閉じます。

[Submit] をクリックすると、選択された監査パラメータが [Selected Attributes] タブに表示されます。

現在のコントローラ監査レポートには、[Audit Status] 列からオブジェクトを選択し、[Configure] > [Controllers] ページからアクセスすることができます。

（注）　[Configure] > [Controllers] ページの [Select a command] ドロップダウン リストで [Audit Now] を選択するか、またはコントローラ監査レポートで [Audit Now] をクリックすると、コントローラを監査できます。「監査ステータスの表示（アクセス ポイント）」（P.9-497）を参照してください。

監査ログの消去の設定

[Administration] > [System Settings] > [Audit Log Purge Settings] ページで、Syslog を消去すること、および消去したログをゴミ箱またはリモート ディレクトリに送信することができます。

Syslog の消去設定を行うには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Audit] > [Log Purge Settings] の順に選択します。

ステップ 3　[Keep logs younger than days] テキスト ボックスに、日数を入力してログ消去設定を定義します。指定した日数より古いログは消去されます。

ステップ 4　消去したログをクリアするために、次のオプションのいずれかを選択します。

- [Send To Trash] : 消去したログはゴミ箱に送信されます。
- [Remote Directory] : 消去したログは [Remote Directory] テキスト ボックスに指定されたパスに送信されます。

ステップ 5　[Save] をクリックします。

クライアントの設定

次のクライアント プロセスを設定して、Prime Infrastructure のパフォーマンスおよび拡張性を向上させることができます。ここでは、次の内容について説明します。

- 「診断トラップの処理」（P.15-856）
- 「ホスト名の検索」（P.15-857）
- 「データ保存」（P.15-857）
- 「クライアント トラップおよび syslog」（P.15-857）
- 「自律クライアント トラップ」（P.15-858）

これらのクライアント設定への変更を確定するには、ページの下部にある [Save] をクリックします。

（注）　クライアント トラブルシューティングの詳細については、「[Client Troubleshooting] ダッシュレット」（P.10-562）を参照してください。

診断トラップの処理

[Settings] > [Client] ページでは、診断チャネル上で自動クライアント トラブルシューティングを有効にできます。

（注）　自動クライアント トラブルシューティングは、CCXV5 または CCXv6 クライアントでのみ利用できます。

この自動クライアント トラブルシューティングを有効にするには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Client] を選択します。[Client] ページが表示されます。

ステップ 3　[Automatically troubleshoot client on diagnostic channel] チェックボックスをオンにします。

（注）　このチェックボックスがオンの場合、Prime Infrastructure は診断アソシエーション トラップを処理します。このチェックボックスがオフの場合、Prime Infrastructure はトラップを発生させますが、自動トラブルシューティングは開始されません。

（注）　診断アソシエーション トラップの処理中に、Prime Infrastructure はクライアントに一連のテストを実行します。すべての完了タスクにおいて、クライアントは更新されます。自動トラブルシューティング レポートは dist/acs/win/webnms/logs に配置されます。テストが完了すると、ログの場所が [client details pages:V5 tab:Automated Troubleshooting Report] グループ ボックスに更新されます。[Export] ボタンでログをエクスポートできます。

ステップ 4　[Save] をクリックします。

ホスト名の検索

DNS ルックアップには、長時間かかることがあります。このため、クライアント ホスト名の DNS ルックアップを有効または無効にできます。デフォルトでは、無効に設定されています。

ホスト名の検索を有効にするには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Client] を選択します。

ステップ 3　[Lookup client host names from DNS server] チェックボックスをオンにします。

ステップ 4　ホスト名をキャッシュに保持する日数を入力します。

ステップ 5　[Save] をクリックします。

データ保存

クライアント アソシエーション履歴は、多くのデータベース領域およびディスク領域を使用する場合があります。これは、データベースのバックアップおよび復元機能において、問題となる場合があります。クライアント アソシエーション履歴の保持期間を設定して、この潜在的な問題を管理しやすくすることができます。

データ保持パラメータを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Client] を選択します。

ステップ 3　次のデータ保持パラメータを入力または編集します。

- [Dissociated Clients (days)] : Prime Infrastructure でデータを保持する日数を入力します。デフォルトは 7 日です。有効な範囲は 1 ～ 30 日です。
- [Client session history (days)] : Prime Infrastructure でデータを保持する日数を入力します。デフォルトは 32 日です。有効な範囲は 7 ～ 365 日です。

ステップ 4　[Save] をクリックします。

クライアントの検出

[Poll clients when client traps/syslogs received] チェックボックスをオンにした場合、Prime Infrastructure はクライアントにポーリングし、クライアントのセッションを迅速に特定します。ネットワークがビジー状態の場合は、クライアント トラップを受信したときのポーリングを無効にできます。このオプションは、デフォルトで無効です。

クライアント トラップおよび syslog

導入環境によっては、Prime Infrastructure は大量のクライアント アソシエーション トラップおよびディスアソシエーション トラップを受信する場合があります。これらのトラップをイベントとして保存すると、パフォーマンスがわずかに低下する可能性があります。このような場合、役立つ可能性のある他のイベントが想定よりも早く期限切れとなる場合があります。

Prime Infrastructure がクライアント アソシエーション トラップおよびディスアソシエーション トラップをイベントとして保存しないようにするには、[Save client association and disassociation traps as events] チェックボックスをオフにします。[Save] をクリックして、この設定の変更を確定します。このオプションは、デフォルトで無効です。

トラップおよび syslog の詳細については、「有線クライアントの検出のためのスイッチでのトラップと Syslog の有効化」（P.9-508）を参照してください。

自律クライアント トラップ

802.1x および 802.11 クライアント認証エラー トラップをイベントとして保存する場合は、[Save 802.1x and 802.11 client authentication fail traps as events] チェックボックスをオンにします。

[Interval Time] : エラー トラップをポーリングする間隔を秒単位で入力します。

CLI セッションのプロトコル設定

Autonomous アクセス ポイントやコントローラのコマンドライン インターフェイス テンプレートなどの多くの Prime Infrastructure 機能、および移行テンプレートでは、Autonomous アクセス ポイントまたはコントローラでコマンドライン インターフェイス コマンドを実行する必要があります。これらのコマンドライン インターフェイス コマンドは、Telnet または SSH セッションを確立して実行できます。CLI セッション ページでは、セッション プロトコルを選択できます。SSH がデフォルトです。

（注） コマンドライン インターフェイス テンプレートでは、質問に対して回答する操作（コマンドに対して「*Yes*」または「*No*」で回答する、*Enter* キーを*押して続行する*、など）は不要です。これは Prime Infrastructure によって自動的に実行されます。

CLI セッションのプロトコルを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[CLI Session] を選択します。

ステップ 3　デフォルトのコントローラ セッション プロトコルには、SSH が選択されています。Telnet を選択するには、該当のオプション ボタンを選択します。

ステップ 4　デフォルトの Autonomous アクセス ポイント セッション プロトコルには、SSH が選択されています。Telnet を選択するには、該当のオプション ボタンを選択します。

ステップ 5　デフォルトでは、[Run Autonomous AP Migration Analysis on discovery] オプション ボタンは [No] に設定されています。Autonomous AP を検出し、移行分析を実行する場合は、[Yes] を選択します。

ステップ 6　[Save] をクリックします。

設定の管理

[Administration] > [System Settings] > [Configuration] ページで、実行中の設定をバックアップおよびロールバックできます。

設定を管理するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Configuration] を選択します。[Configuration] ページが表示されます。

ステップ 3　次のパラメータを必要に応じて変更します。

- [Backup Running Configuration]：実行中の設定のバックアップを作成するには、このチェックボックスをオンにします。
- [Rollback Configuration]：前の設定に戻すには、このチェックボックスをオンにします。
- [Get show commands output from cache]：キャッシュから show コマンドの出力を取得するには、このチェックボックスをオンにします。デフォルトのキャッシュ タイムアウトは 60 秒です。コマンド出力がキャッシュに存在しない場合、出力はデバイスから取得され、キャッシュに追加されます。
- [Deploy Cli Thread pool count] :

ステップ 4　[Save] をクリックします。

コントローラのアップグレード設定

[Controller Upgrade Settings] ページでは、コントローラのアップグレード後に自動更新を実行することができます。自動更新を実行するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Controller Upgrade Settings] を選択します。

ステップ 3　[Auto refresh After Upgrade] チェックボックスをオンにすると、コントローラのイメージに変更があるたびに設定は自動的に復元されます。

ステップ 4　save config トラップを受信したときの Prime Infrastructure の動作を決定します。このチェックボックスをオンにすると、デバイスに存在して Prime Infrastructure には存在しない追加の設定を保持するか削除するかを選択できます。設定は、Prime Infrastructure によって管理されているすべてのコントローラに適用されます。

（注）　[Configure] > [Controllers] > [Properties] > [Settings] ページの [Auto Refresh on Save Config Trap] チェックボックスを選択した場合、この設定は上記のグローバル設定よりも優先されます。

（注）　自動更新の実行には最大 3 分かかります。

ステップ 5　[Save] をクリックします。

save config トラップを Prime Infrastructure が受信するたびに、このチェックボックスはオンになります。このチェックボックスをオンにすると、Prime Infrastructure の動作が決定されます。

このチェックボックスをオンにすると、ユーザはデバイスに存在して Prime Infrastructure には存在しない追加の設定を保持するか削除するかを選択できます。

この設定は、Prime Infrastructure によって管理されているすべてのコントローラに適用されます。[Controller] > [Properties] ページの save config トラップの処理に関する設定は、このグローバル設定よりも優先されます。

コントローラのイメージに変更がある場合、コントローラの設定は自動的に復元されます。

データ保存の設定

傾向データ、デバイス ヘルス データ、およびシステム ヘルス データの保存期間を、時間単位、日単位、および週単位で設定できます。パフォーマンス データの保存期間を、短期、中期、および長期単位で設定できます。

指定時刻に動作する計算およびネットワーク監査の計算で使用される集約データの保持期間を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Data Retention] を選択します。[Data Retention] ページが表示されます。

ステップ 3　データ（時間単位）を保存しておく日数を指定します。有効範囲は 1 ～ 31 です。デフォルトは、31 日です。

ステップ 4　データ（日単位）を保存しておく日数を指定します。有効な範囲は 7 ～ 365 です。デフォルトは、90 日です。

ステップ 5　データ（週単位）を保存しておく週数を指定します。有効な範囲は 2 ～ 108 です。デフォルトは 54 週間です。

ステップ 6　短期、中期、長期のパフォーマンス データを保存する日数を指定します。

ステップ 7　パージングの前に [Network Audit] バックグラウンド タスクで収集された監査データを保持する日数を指定します。上限は 365 日間で、最短のクリーンアップ間隔は 7 日間です。デフォルトは、90 日です。

（注）　インタラクティブ グラフ データを見やすくするには、デフォルト設定を可能な最大値に変更します。日単位の集積データは 90 日間、週単位の集積データは 54 週にします。これらの調整を補う RAM と CPU の容量を増やすために、適切な措置を執る必要もあります。

ステップ 8　[Save] をクリックします。

Prime Infrastructure の履歴データ

Prime Infrastructure の履歴データには、次の 2 種類があります。

- 集約履歴データ：一括して収集され、最小値、最大値、または平均値に集約された数値データ。クライアント数は、集約履歴データの 1 つの例です。

  [Administration] > [System Settings] > [Data Retention] ページを使用して、集約データの保持期間を定義します。集約タイプには、時単位、日単位、および週単位があります。

  これらの集約タイプの保持期間にはデフォルト値、最小値、最大値が定義されています（表 15-3 を参照）。

表 15-3　集約データの保持期間

集約データ	デフォルト	最小ハードウェア	最大
Hourly	31 日	1 日	31 日
Daily	90 日間	7 日間	365 日
Weekly	54 週間	2 週間	108 週間

- 非集約履歴データ：一括して収集（または集約）できない数値データ。クライアント アソシエーション履歴は、非集約履歴データの 1 つの例です。

  各データ収集タスクおよび他の設定における非集約保持期間を定義できます。

  たとえば、[Administration] > [System Settings] > [Client] でクライアント アソシエーション履歴の保持期間を定義します。デフォルトでは、保持期間は 31 日または 1,000,000 レコードです。この保持期間は 365 日まで増やすことができます。

データ重複除外の設定

[Data Deduplication] ページで、Prime Infrastructure から重複する情報を除去するための設定を行うことができます。

データ重複除外を設定するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Data Deduplication] を選択します。[Data Deduplication] ページが表示されます。

ステップ 3　[Enable Data Deduplication] チェックボックスをオンにして、Prime Infrastructure から重複する情報を除去します。

ステップ 4　[Save] をクリックします。

ゲスト アカウントの設定

[Guest Account Settings] ページでは、有効期限が切れたすべてのテンプレートをグローバルに削除できます。ゲスト アカウント設定を行うには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Guest Account Settings] を選択します。

ステップ 3　[Automatically remove expired guest accounts] チェックボックスをオンにすると、期限の切れたゲスト アカウントは保持されず、期限切れ状態に遷移します。期限切れ状態のアカウントは Prime Infrastructure から削除されます。

ステップ 4　デフォルトでは、Prime Infrastructure Lobby Ambassador は作成者に関係なく、すべてのゲスト アカウントにアクセスできます。[Search and List only guest accounts created by this lobby ambassador] チェックボックスをオンにした場合、Lobby Ambassador は本人が作成したゲスト アカウントのみにアクセスできます。

ステップ 5　[Save] をクリックします。

インベントリの設定

[Inventory] ページで、デバイスの syslog イベントが受信された場合に、Prime Infrastructure でインベントリを収集するかどうかを指定できます。

インベントリ設定を行うには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Inventory] を選択します。[Inventory] ページが表示されます。

ステップ 3　[Enable event based inventory collection] チェックボックスをオンにして、Prime Infrastructure がデバイスの syslog イベントを受信した場合にインベントリを収集できるようにします。

ステップ 4　[Save] をクリックします。

既知のイーサネット MAC アドレスの管理

[Known Ethernet MAC Address List] ページで、Prime Infrastructure に追加されたイーサネット MAC アドレスのリストを表示できます。このページでは、MAC アドレスを追加または削除することもできます。

MAC アドレスを追加するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Known Ethernet MAC Address List] を選択します。[Known Ethernet MAC Address List] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Entry] を選択し、[Go] をクリックします。

ステップ 4　[MAC Address] フィールドに、追加するイーサネット MAC アドレスを入力します。形式は、aa:bb:cc:dd:ee:ff です。

ステップ 5　[OK] をクリックします。MAC アドレスが [Known Ethernet MAC Address List] ページに表示されます。

（注）　[Known Ethernet MAC Address List] ページから MAC アドレスを削除することもできます。削除する MAC アドレスを選択し、[Select a Command] ドロップダウン リストから [Delete Entries] を選択します。[Go] をクリックします。選択した MAC アドレスがリストから削除されます。

ログイン ページの免責事項の設定

[Login Disclaimer] ページでは、ログイン ページの最上部に表示される免責事項を入力できます。この免責事項はすべてのユーザに対して表示されます。

ログイン ページの免責事項を入力する手順は、次のとおりです。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Login Disclaimer] を選択します。[Login Disclaimer] ページが表示されます。

ステップ 3　該当するテキスト ボックスに、ログイン ページに表示する免責事項を入力します。

ステップ 4　[Save] をクリックします。

メール サーバの設定

Prime Infrastructure レポート、アラーム通知などから電子メールを送信する際に使用するグローバル電子メール パラメータを設定できます。この [Mail Server] ページでは、電子メールのパラメータがすべて設定できます。[Mail Server] ページでは、プライマリ SMTP サーバおよびセカンダリ SMTP サーバのホストおよびポート、送信者の電子メール アドレス、および受信者の電子メール アドレスを設定できます。

（注）　SMTP 設定では電子メール アドレスに文字「=」または「+」は受け入れられません。

グローバル電子メール パラメータを設定するには、次の手順に従います。

（注）　グローバル電子メール パラメータを設定する前に、グローバル SMTP サーバを設定する必要があります。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Mail Server Configuration] を選択します。[Mail Server Configuration] ページが表示されます。

ステップ 3　プライマリ SMTP サーバのホスト名を入力します。

ステップ 4　SMTP サーバのユーザ名を入力します。

ステップ 5　SMTP サーバにログオンする際のパスワードを入力し、確定します。

（注）　ユーザ名およびパスワードは、両方ともオプションです。

ステップ 6　セカンダリ SMTP サーバに対してと同じ情報を提供します（セカンダリ メール サーバが使用できる場合のみ）。

ステップ 7　ページの [Sender And Receivers] 部分の [From] テキスト ボックスに *PI@<Prime Infrastructure server IP address>* が設定されます。これは別の送信者に変更可能です。

ステップ 8　[To] テキスト ボックスに、受信者の電子メール アドレスを入力します。指定した電子メール アドレスは、アラームやレポートなど、その他の機能エリアでデフォルト値として使用されます。複数の電子メール アドレスを追加する場合は、各アドレスをカンマで区切る必要があります。

（注）　ステップ 7 で受信者の電子メール アドレスに加えたグローバルな変更は、電子メール通知が設定されていた場合には無視されます。

プライマリ SMTP メール サーバを指定し、[From] アドレス テキスト ボックスに入力する必要があります。

入力した受信者リストにすべてのアラーム カテゴリを適用させる場合は、[Apply recipient list to all alarm categories] チェックボックスをオンにします。

ステップ 9　電子メールの件名に付加するテキストを入力します。

ステップ 10　[Configure e-mail notification for individual alarm categories] リンクをクリックすると、有効にするアラーム カテゴリおよびシビリティを指定できます。選択したカテゴリおよびシビリティに一致するアラームが発生すると、電子メール通知が送信されます。

（注）　アラーム カテゴリをクリックし、[Critical]、[Major]、[Minor]、または [Warning] を選択して、電子メール アドレスを入力することで、各アラームのシビリティを設定できます。

ステップ 11　[Test] ボタンをクリックして、設定したパラメータを使用したテスト メールを送信します。テスト操作の結果は同じページに表示されます。このテスト機能では「Prime Infrastructure test e-mail」という件名の電子メールが送信され、プライマリ メール サーバとセカンダリ メール サーバへの接続が確認されます。

満足なテスト結果が得られたら、[Save] をクリックします。

ヘルス データの自動収集の設定

[Monitoring Settings] ページで、デバイスとインターフェイスのヘルス データの自動収集を有効にすること、およびサーバ ヘルスに関するデータの重複除外を有効にすることができます。

ヘルス データの自動収集を設定するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Monitoring Settings] を選択します。[Monitoring Settings] ページが表示されます。

ステップ 3　[Auto monitoring] チェックボックスをオンにして、デバイスとインターフェイスのヘルス データの自動収集を有効にします。

ステップ 4　[Enable deduplication] チェックボックスをオンにして、サーバ ヘルスに関する重複データの自動除去を有効にします。

ステップ 5　[Save] をクリックします。

通知レシーバの設定

[Notification Receiver] ページには、ゲストのアクセスをサポートする現在の通知レシーバが表示されます。アラートおよびイベントは SNMPv2 通知として、設定された通知レシーバに送信されます。

このページで、現在の通知レシーバを表示するか、さらに通知レシーバを追加できます。

ここでは、次の内容について説明します。

- 「Prime Infrastructure への通知レシーバの追加」（P.15-865）
- 「通知レシーバの削除」（P.15-866）

[Notification Receiver] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Administration] > [Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Notification Receivers] を選択します。現在設定されているすべてのサーバがこのページに表示されます。サーバを追加する場合は、[Select a command] ドロップダウン リストから [Add Notification Receiver] を選択し、[Go] をクリックします。

Prime Infrastructure への通知レシーバの追加

現在の通知レシーバを表示するか、さらに通知レシーバを追加するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Notification Receivers] を選択します。現在設定されているすべてのサーバがこのページに表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Notification Receiver] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　サーバの IP アドレスと名前を入力します。

ステップ 6　[North Bound] または [Guest Access] のオプション ボタンを選択します。

デフォルトでは、[Notification Type] が自動的に UDP に設定されます。

ステップ 7　[Port Number] や [Community] などの UDP パラメータを入力します。

（注）　設定するレシーバは、設定されたポートと同じポートで UDP を待ち受ける必要があります。

ステップ 8　レシーバ タイプとして [North Bound] を選択した場合は、その条件とシビリティを指定します。

（注）　選択されたカテゴリのアラームのみが処理されます。

（注）　選択されたカテゴリと一致する、選択されたシビリティのアラームのみが処理されます。

ステップ 9　[Save] をクリックして、通知レシーバ情報を確定します。

（注）
- デフォルトでは、選択されたカテゴリに対する INFO レベルのイベントのみが処理されます。
- SNMPV2 トラップのみが North Bound 通知の対象となります。

通知レシーバの削除

通知レシーバを削除するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Notification Receivers] を選択します。現在設定されているすべてのサーバがこのページに表示されます。

ステップ 3　削除する通知レシーバのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから、[Remove Notification Receiver] をクリックします。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

次に、Prime Infrastructure からのイベント トラップを受信した North Bound SNMP レシーバの出力例を示します。

次の出力例は、Prime Infrastructure で生成されたログ ファイルです。このログ ファイルは、Prime Infrastructure サーバのログ ファイル ディレクトリ（/opt/CSCOlumos//webnms/logs）にあります。ログ出力は、アラームを North Bound SNMP レシーバで受信していない場合のトラブルシューティングに役立ちます。

```
06/04/10 08:30:58.559 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]Adding into queue
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrTotalNotifications2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrHandledInNotification2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][addNbAlarm]incrNonCongestedIn2
06/04/10 08:30:58.560 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][addNBAlert]Added into queue
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService$NbOrderQueue][getNbAlarm]incrHandledOutNotification2
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.services] :
[NBNotificationService][startNotifier]Processing the
alertNoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.561 INFO[com.cisco.ncslogger.notification] :
[NbAlertToNmsAlertCorrelator][formVarBindList]Generating the varbind list for NB
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.2.1.1.3.0 variable value: 10 days, 20:22:17.26
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.6.3.1.1.4.1.0 variable value:
1.3.6.1.4.1.9.9.199991.0.1
06/04/10 08:30:58.562 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.2 variable value:
07:da:05:18:0c:30:0d:09:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.3 variable value:
07:da:06:04:08:1e:3a:04:2d:07:00
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.4 variable value:
NoiseProfile_LradIf!00:17:df:a9:c8:30!0
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.5 variable value: 2
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.6 variable value: Radio
load threshold violation
06/04/10 08:30:58.563 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.7 variable value: 1
```

```
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.8 variable value:
172.19.29.112
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.9 variable value: AP
1250-LWAP-ANGN-170-CMR, Interface 802.11b/g/n
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.10 variable value:
Noise changed to acceptable level on '802.11b/g/n' interface of AP
'1250-LWAP-ANGN-170-CMR', connected to Controller '172.19.29.112'.
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.11 variable value: 1
06/04/10 08:30:58.564 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.12 variable value:
06/04/10 08:30:58.565 INFO[com.cisco.ncslogger.notification] :
[NBUtil][printVarBind]Variable OID: 1.3.6.1.4.1.9.9.199991.1.1.2.1.14 variable value:
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]OSS list
size with reachability status as up1
06/04/10 08:30:58.573 INFO[com.cisco.ncslogger.notification] : [NBUtil][sendTrap]Sending
UDP Notification for receiver:172.19.27.85 on port:162
```

MIB と Prime Infrastructure アラート/イベントのマッピング

表 15-4 に、Cisco-Prime Infrastructure-Notification-MIB と Prime Infrastructure アラート/イベントのマッピングの概要を示します。

表 15-4　Cisco-Prime Infrastructure-Notification-MIB と Prime Infrastructure アラート/イベントのマッピング

フィールド名およびオブジェクト ID	データ型	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationTimestamp	DateAndTime	createTime : NmsAlert eventTime : NmsEvent	アラーム/イベントの作成時刻。
cWNotificationUpdatedTimestamp	DateAndTime	modTime : NmsAlert	アラームの修正時刻。 イベントには修正時刻がありません。
cWNotificationKey	SnmpAdminString	objectId : NmsEvent entityString : NmsAlert	文字列形式の一意のアラーム/イベント ID。

表 15-4　Cisco-Prime Infrastructure-Notification-MIB と Prime Infrastructure アラート/イベントのマッピング （続き）

フィールド名およびオブジェクト ID	データ型	Prime Infrastructure イベント/アラート フィールド	説明
cwNotificationCategory	CWirelessNotificationCategory	該当なし	イベント/アラームのカテゴリを示し、有効値は次のとおりです。 unknown accessPoints adhocRogue clients controllers coverageHole interference contextAwareNotifications meshLinks mobilityService performance rogueAP rrm security wcs switch ncs
cWNotificationSubCategory	OCTET STRING	アラートの Type フィールドおよびイベントの eventType。	このオブジェクトは、アラートのサブカテゴリを表します。
cWNotificationServerAddress	InetAddress	該当なし	Prime Infrastructure の IP アドレス。

表 15-4　Cisco-Prime Infrastructure-Notification-MIB と Prime Infrastructure アラート/イベントのマッピング （続き）

フィールド名およびオブジェクト ID	データ型	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationManagedObjectAddressType	InetAddressType	該当なし	管理対象オブジェクトに到達可能なインターネット アドレスの種類。有効値： 0：不明 1：IPv4 2：IPv6 3：IPv4z 4：IPv6z 16：DNS Prime Infrastructure は IPv4 アドレスのみをサポートしているため、常に「1」に設定されます。
cWNotificationManagedObjectAddress	InetAddress	getNode() 値を使用（存在する場合）	getNode はイベントおよび一部のアラートに対して設定されます。ヌルでない場合は、このフィールドに使用されます。
cWNotificationSourceDisplayName	OCTET STRING	アラート/イベントの sourceDisplayName フィールド。	このオブジェクトは、通知の送信元の表示名を表します。
cWNotificationDescription	OCTET STRING	Text：NmsEvent Message：NmsAlert	アラームの説明を示す文字列。
cWNotificationSeverity	INTEGER	severity：NmsEvent、NmsAlert	アラート/イベントのシビリティ critical（1）、 major（2）、 minor（3）、 warning（4）、 clear（5）、 info（6）、 unknown（7）。

表 15-4　Cisco-Prime Infrastructure-Notification-MIB と Prime Infrastructure アラート/イベントのマッピング （続き）

フィールド名およびオブジェクト ID	データ型	Prime Infrastructure イベント/アラート フィールド	説明
cWNotificationSpecialAttributes	OCTET STRING	基本アラート/イベント クラス以外のすべてのアラート/イベントの属性。	このオブジェクトは、アラート専用の属性（APAssociated、APDisassociated、RogueAPAlert、CoverageHoleAlert など）を表します。文字列は CSV 形式で「プロパティ = 値」の組で表されます。
cWNotificationVirtualDomains	OCTET STRING	該当なし	アラームを発生させたオブジェクトの仮想ドメイン。このフィールドは現在のリリースでは設定されず、空の文字列が設定されます。

プロキシ設定

[Proxy Settings] ページで、Prime Infrastructure サーバとそのローカル認証サーバのプロキシを設定できます。

プロキシ設定を行うには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Proxy Settings] を選択します。[Proxy Settings] ページが表示されます。

ステップ 3　[Enable Proxy] チェックボックスをオンにして、Prime Infrastructure サーバのプロキシ設定を有効にします。

ステップ 4　[Proxy Server IP Host Name] フィールドに、Cisco.com に接続するためのプロキシ サーバの IP アドレスまたはホスト名を入力します。

ステップ 5　[Proxy Port Number] フィールドに、プロキシ サーバのポート番号を入力します。

ステップ 6　[Authentication Proxy] チェックボックスをオンにして、Prime Infrastructure のローカル認証サーバのプロキシ設定を有効にします。

ステップ 7　[Proxy User Name and Proxy Password] フィールドに、プロキシ サーバにログインするためのユーザ名とパスワードを入力します。

ステップ 8　[Save] をクリックします。

レポートの設定

スケジュールされたレポートが存在する場所とその日数を指定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Report] を選択します。[Report] ページが表示されます。

ステップ 3　ローカル PC にレポート データ ファイルを保存するためのパスを入力します。既存のデフォルト パスを編集できます。

ステップ 4　レポート データ ファイルを保持する日数を指定します。

ステップ 5　[Save] をクリックします。

不正 AP 設定

[Administration] > [System Settings] > [Rogue AP Settings] ページで、ネットワーク内の不正アクセス ポイントが接続している先のスイッチ ポートを Prime Infrastructure が自動的に追跡するように設定できます。

不正 AP 設定を行うには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Rogue AP Settings] を選択します。[Rogue AP Settings] ページが表示されます。

ステップ 3　[Enable Auto Switch Port Tracing] チェックボックスをオンにして、Prime Infrastructure が、不正アクセス ポイントが接続されているスイッチ ポートを自動的にトレースできるようにします。

ステップ 4　[Enable Auto Containment] チェックボックスをオンにします。

ステップ 5　[OK] をクリックします。

サーバ設定値の設定

TFTP、FTP、HTTP、または HTTPS を有効または無効にするには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Server Setting] を選択します。[Server Settings] ページが表示されます。

ステップ 3　インストール時に確立された FTP および TFTP ディレクトリまたは HTTP および HTTPS ポートを変更する場合は、変更するポート番号（または必要に応じてポート番号およびルート）を入力し、[Enable] または [Disable] をクリックします。

変更は再起動後に反映されます。

サーバ チューニングの設定

[Server Tuning] ページで、Prime Infrastructure サーバ再起動時にサーバ チューニングを有効にすることができます。サーバ チューニングにより、サーバがクライアントの要求を処理するために使用するリソースの数を制限することで、サーバのパフォーマンスを最適化できます。

サーバ チューニングを設定するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Server Tuning] を選択します。[Server Tuning] ページが表示されます。

ステップ 3　[Enable Server Tuning during restart] チェックボックスをオンにします。

ステップ 4　[Save] をクリックします。

アラームのシビリティの設定

新しく生成されるアラームの重大度を変更できます。

（注）　既存のアラームは変更されません。

新しく生成されるアラームのシビリティを変更するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Severity Configuration] を選択します。[Severity Configuration] ページが表示されます。

ステップ 3　重大度を変更するアラーム状態のチェックボックスをオンにします。

ステップ 4　[Configure Severity Level] ドロップダウン リストから、新しい重大度（[Critical]、[Major]、[Minor]、[Warning]、[Informational]、または [Reset to Default]）を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、変更を確定します。

SNMP クレデンシャルの設定

[SNMP Credentials] ページでは、クレデンシャルを指定して不正アクセス ポイントのトレースに使用できます。番号ベースのエントリを使用しても特定のエントリを確認できない場合は、このオプションを使用します。スイッチ クレデンシャルが Prime Infrastructure に追加されていない場合は、このページの SNMP クレデンシャルを使用してスイッチに接続できます。

SNMP クレデンシャルを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [SNMP Credentials] を選択します。[SNMP Credentials] ページが表示されます。

ステップ 3　現在の SNMP エントリの詳細を表示または編集するには、[Network Address] リンクをクリックします。詳細については、「現在の SNMP クレデンシャル詳細の表示」（P.15-873）を参照してください。

（注）　デフォルトのネットワーク アドレスは 0.0.0.0 であり、ネットワーク全体を示します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。0.0.0.0 は SNMP クレデンシャルのデフォルトであり、SNMP クレデンシャルが定義されていないときに使用されます。デフォルトのコミュニティ ストリングは、読み取りと書き込みの両方において *private* です。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 4　新しい SNMP エントリを追加するには、[Select a command] ドロップダウン リストから [Add SNMP Entries] を選択し、[Go] をクリックします。詳細については、「新しい SNMP クレデンシャル エントリの追加」（P.15-874）を参照してください。

現在の SNMP クレデンシャル詳細の表示

現在の SNMP クレデンシャルの詳細を表示または編集するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [SNMP Credentials] を選択します。

ステップ 3　[Network Address] リンクをクリックすると、[SNMP Credential Details] ページが開きます。[SNMP Credential Details] ページには、次の情報が表示されます。

General パラメータ

- [Add Format Type]：表示のみ。[Add Format Type] の詳細については、「新しい SNMP クレデンシャル エントリの追加」（P.15-874）を参照してください。
- Network Address
- Network Mask

[SNMP Parameters]：該当する SNMP パラメータのバージョンを選択します。SNMP クレデンシャルは、選択されている SNMP バージョンに応じて検証されます。

（注）　書き込みアクセスに対応する SNMP パラメータ（存在する場合）を入力します。表示専用のアクセス パラメータでは、スイッチが追加されますが、その設定を Prime Infrastructure では変更できません。デバイス接続テストでは、[Administration] > [Settings] > [SNMP Settings] で設定された SNMP リトライおよびタイムアウト パラメータが使用されます。

- [Retries]：スイッチの検出を試行する回数。
- [Timeout]：セッション タイムアウト値（秒）。この値により、クライアントの再認証が強制されるまでの最大時間が決定されます。
- [SNMP v1 Parameters or v2 Parameters]：選択した場合は、入力可能なテキスト ボックスに該当するコミュニティを入力します。
- [SNMP v3 Parameters]：選択した場合は、次のパラメータを設定します。

- Username
- Auth.Type
- Auth.Password
- Privacy Type
- Privacy Password

（注）　デフォルト コミュニティの SNMP v1 または v2 が設定されている場合、デフォルト コミュニティはよく知られているため、ネットワークが攻撃しやすくなります。デフォルトでないコミュニティの SNMP v1 または v2 はデフォルト コミュニティよりも安全性が高くなりますが、Auth および Privacy タイプおよびデフォルト ユーザなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 4　[OK] をクリックして変更を保存するか、[Cancel] をクリックして SNMP クレデンシャルの詳細を変更せずに [SNMP Credentials] ページに戻ります。

新しい SNMP クレデンシャル エントリの追加

新しい SNMP クレデンシャル エントリを追加するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [SNMP Credentials] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add SNMP Entries] を選択します。

ステップ 4　[Go] をクリックします。[SNMP Credentials] ページが開きます。

ステップ 5　次のいずれかを選択します。

手動で SNMP クレデンシャル情報を入力するには、[Add Format Type] ドロップダウン リストを [SNMP Credential Info] のままにします。複数のネットワーク アドレスを追加するには、各アドレスの間にカンマを使用します。ステップ 7 に進みます。

CSV ファイルのインポートにより複数のスイッチを追加する場合は、[Add Format Type] ドロップダウン リストから [File] を選択します。CSV ファイルを使用すると、独自のインポート ファイルを生成して必要に応じてデバイスを追加できます。ステップ 6 に進みます。

ステップ 6　[File] を選択した場合は、[Browse] をクリックしてインポートする CSV ファイルの場所を探します。ステップ 11 にスキップします。

CSV ファイルの最初の行は、含まれている列の説明に使用されます。IP アドレス列は必須です。

ファイル例：

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_passw
ord,snmpv3_privacy_type,snmpv3_privacy_password,network_mask
1.1.1.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,255.255.255.0
10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```

CSV ファイルには、次のフィールドを含めることができます。

- ip_address：IP アドレス
- snmp_version：SNMP バージョン

- network_mask：ネットワーク マスク
- snmp_community：SNMP V1/V2 コミュニティ
- snmpv3_user_name：SNMP V3 ユーザ名
- snmpv3_auth_type：SNMP V3 認証タイプ。None または HMAC-MD5 または HMAC-SHA を選択できます
- snmpv3_auth_password：SNMP V3 認証パスワード
- snmpv3_privacy_type：SNMP V3 プライバシー タイプ。None または DES または CFB-AES-128 を選択できます
- snmpv3_privacy_password：SNMP V3 プライバシー パスワード
- snmp_retries：SNMP リトライ
- snmp_timeout：SNMP タイムアウト

ステップ 7　[SNMP Credential Info] を選択した場合は、追加するスイッチの IP アドレスを入力します。複数のスイッチを追加するには、IP アドレスの文字列の間にカンマを使用します。

ステップ 8　[Retries] フィールドに、スイッチの検出を試行する回数を入力します。

ステップ 9　セッション タイムアウト値を秒単位で入力します。この値により、クライアントの再認証が強制されるまでの最大時間が決定されます。

ステップ 10　該当する SNMP パラメータのバージョンを選択します。SNMP クレデンシャルは、選択されている SNMP バージョンに応じて検証されます。

- [SNMP v1 Parameters or v2 Parameters] が選択されている場合は、入力可能なテキスト ボックスに該当するコミュニティを入力します。
- [SNMP v3 Parameters] が選択されている場合は、次のパラメータを設定します。
  - Username
  - Auth.Type
  - Auth.Password
  - Privacy Type
  - Privacy Password

（注）　デフォルト コミュニティの SNMP v1 または v2 が設定されている場合、デフォルト コミュニティはよく知られているため、ネットワークが攻撃しやすくなります。デフォルトでないコミュニティの SNMP v1 または v2 はデフォルト コミュニティよりも安全性が高くなりますが、Auth および Privacy タイプおよびデフォルト ユーザなしの SNMP v3 が最も安全な SNMP 接続です。

ステップ 11　[OK] をクリックします。

Prime Infrastructure がリストされている SNMP クレデンシャルを使用してスイッチにアクセスできる場合は、今後使用できるようにスイッチが追加され、[Configure] > [Ethernet Switches] ページに表示されます。

（注）　[Configure] > [Ethernet Switches] ページを使用して手動でスイッチを追加した場合、スイッチ ポートのトレースではこのページのクレデンシャルが使用され、[SNMP Credentials] ページにリストされているクレデンシャルは使用されません。手動で追加したスイッチ クレデンシャルが変更されている場合は、[Configure] > [Ethernet] ページからこれらのクレデンシャルを更新する必要があります。

SNMP 設定値の設定

[SNMP Settings] ページでは、Prime Infrastructure からグローバルな SNMP パラメータを設定できます。

（注）　このページで行うすべての変更は、Prime Infrastructure にグローバルに影響します。変更は、再起動をまたがって有効であり、バックアップと復元をまたがって有効です。

グローバルな SNMP 設定を行うには、次の手順に従ってください。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [SNMP Settings] を選択します。[SNMP Settings] ページが表示されます。

ステップ 3　[Trace Display Values] チェックボックスをオンにした場合は、SNMP を使用しているコントローラから取得したデータ値がメディエーション トレースレベル ログに表示されます。オフにした場合は、値は表示されません。

（注）　セキュリティ上の理由から、デフォルトではオフになっています。

ステップ 4　[Backoff Algorithm] の場合は、ドロップダウン リストから、[Exponential] または [Constant Timeout] を選択します。[Exponential]（デフォルト値）を選択した場合、SNMP の初回試行時には指定したタイムアウト値が使用され、2 回めからは、前回の試行時の 2 倍の待機時間が適用されます。[Constant Timeout] を選択した場合は、すべての SNMP 試行に対して同じ待機時間（指定したタイムアウト値）が適用されます。

（注）　ネットワークの信頼性が低く、再試行回数が多くなる可能性がある場合（衛星ネットワークなど）は、通常 [Constant Timeout] を使用します。再試行のたびにタイムアウト時間が倍加しないので、再試行回数が増えた場合でもそれほど時間がかかりません。

ステップ 5　到達可能性に関するパラメータを使用するかどうかを決定します。オンにした場合は、設定するグローバルな [Reachability Retries] および [Timeout] が Prime Infrastructure のデフォルトでは使用されます。オフにした場合は、Prime Infrastructure ではコントローラごと、または IOS アクセス ポイントごとに指定したタイムアウトと再試行が常に使用されます。デフォルトはオンです。

（注）　スイッチ ポート トレーシングの完了まで長時間かかる場合は、この設定を調整して小さくしてください。

ステップ 6　[Reachability Retries] フィールドに、デバイスの到達可能性を判断するためのグローバルな再試行回数を入力します。デフォルトの回数は 2 回です。このフィールドは、[Use Reachability Parameters] チェックボックスをオンにした場合だけ使用できます。

（注）　スイッチ ポート トレーシングの完了まで長時間かかる場合は、この設定を調整して小さくしてください。

ステップ 7　[Reachability Timeout] フィールドに、デバイスの到達可能性を判断するためのグローバルなタイムアウト値を入力します。デフォルトの回数は 2 回です。このフィールドは、[Use Reachability Parameters] チェックボックスをオンにした場合だけ使用できます。

ステップ 8　[Maximum VarBinds per PDU] フィールドに、要求 PDU または応答 PDU で使用する SNMP 変数バインドの最大数を入力します。デフォルトは 100 です。

（注）　ネットワークでの PDU フラグメンテーションに問題がある場合は、この数を 50 に減らすとフラグメンテーションが解消されます。

ステップ 9　表のフィールドあたりの最大行数は設定可能であり、デフォルト値は 50000 行です。設定した値は、Prime Infrastructure のバージョンをアップグレードしても保持されます。

ステップ 10　[Save] をクリックして、これらの設定を保存します。

サポート要求の設定

[Support Request Settings] ページで、一般的なサポートおよびテクニカル サポート情報を設定できます。

サポート要求を設定するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Support Request Settings] を選択します。[Support Request Settings] ページが表示されます。

ステップ 3　次のパラメータを設定します。

- 一般的なサポートの設定:
  - [Enable interactions directly from the server] : サーバからの直接的なサポート要求の対話を許可するには、このチェックボックスをオンにします。
  - [Sender E mail Address] : 送信者の電子メール アドレスを入力します。
  - [Interactions via client system only] : クライアント システムを通じてのみサポート要求に関する対話を許可する場合は、このチェックボックスをオンにします。
- テクニカル サポート プロバイダーの情報:
  - [Cisco] : テクニカル サポート プロバイダーがシスコの場合、このチェックボックスをオンにします。[Default Cisco.com Username] フィールドに、Cisco.com にログインするためのデフォルトのユーザ名を入力します。メール サーバ、Cisco サポート サーバ、およびフォーラム サーバへの接続をテストするには、[Test Connectivity] をクリックします。

– [Third-Party Support Provider] : テクニカル サポート プロバイダーがサードパーティの場合は、このチェックボックスをオンにします。電子メール アドレス、電子メールの件名行の形式、およびサードパーティまたはパートナー サポート プロバイダーの Web サイトの URL を入力します。

ステップ 4　[Save Settings] をクリックします。

スイッチ ポート トレーシングの設定

現在、Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、ネイバー リストにないフレームから検出された BSSID アドレスが記載されています。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。Prime Infrastructure では、コントローラから受信した情報をこの方法で収集します。ソフトウェア リリース 5.1 以降では、有線の不正アクセス ポイントのスイッチ ポートに関するスイッチ ポート トレーシングを組み込むことができるようになりました。この機能拡張により、検出された不正なアクセス ポイントに対応し、今後発生する攻撃を回避できます。トレース情報は不正アクセス ポイントの Prime Infrastructure ログだけで使用でき、不正クライアントのログには使用できません。

（注）　不正アクセス ポイントに接続した不正クライアントの情報を使用して、ネットワークで不正アクセス ポイントに接続したスイッチ ポートを追跡します。

（注）　危険性のない不正アクセス ポイントまたは削除された不正アクセス ポイントにトレーシングを設定しようとすると、警告メッセージが表示されます。

（注）　スイッチ ポート トレーシングで、v3 を使用してスイッチ ポートを正常にトレースするには、すべての OID を SNMP v3 のビューに含める必要があり、SNMP v3 グループ内の VLAN ごとに VLAN の内容を作成する必要があります。

（注）　スイッチ ポート トレーシングの設定については、「スイッチ ポート トレーシングの設定」（P.15-878）を参照してください。

[Switch Port Trace] ページでは、回線上で検出された不正アクセス ポイントに対するトレースを実行できます。

不正アクセス ポイントを適切にトレースして組み込むには、以下の情報を正しく指定する必要があります。

- レポート AP : 不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- AP CDP ネイバー : シード スイッチを判別するために、アクセス ポイント CDP ネイバー情報が必要です。

- スイッチの IP アドレスと SNMP のクレデンシャル：トレース対象のすべてのスイッチは管理 IP アドレスを持つ必要があり、SNMP 管理が有効にされている必要があります。個々のスイッチだけを追加するのではなく、ネットワーク アドレスをベースに項目を追加できます。正しい write コミュニティ ストリングを指定して、スイッチ ポートを有効または無効にする必要があります。トレーシングの場合は、read コミュニティ ストリングで十分です。
- スイッチ ポートの設定：トランキング スイッチ ポートを正しく設定する必要があります。スイッチ ポートのセキュリティはオフにする必要があります。
- シスコ イーサネット スイッチだけがサポートされています。
- スイッチ VLAN 設定を適切に行う必要があります。
- CDP プロトコルがすべてのスイッチ上で有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正アクセス ポイントとイーサネット スイッチの間に何らかのトラフィックが存在する必要があります。
- 不正アクセス ポイントは、最大ホップ カウントの制限内でスイッチに接続される必要があります。デフォルトのホップ カウントは 2、最大ホップ カウントは 10 です。
- SNMPv3 を選択している場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成します。

スイッチ ポート トレーシングのオプションを指定するには、次の手順に従ってください。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Switch Port Trace] を選択します。

ステップ 3　必要に応じて、以下の基本設定を行います。

- [MAC address +1/-1 search]：有効にするには、チェックボックスをオンにします。

  この検索では、無線 MAC アドレスに 1 加算するか 1 減算することによって不正アクセス ポイントの有線側の MAC アドレスを得る、慣習的な MAC アドレス +1/-1 方式を使用します。
- [Rogue client MAC address search]：有効にするには、チェックボックスをオンにします。

  不正クライアントが存在していると、検索可能な MAC アドレスのリストにクライアントの MAC アドレスが追加されます。
- [Vendor (OUI) search]：有効にするには、チェックボックスをオンにします。組織固有識別子である OUI、すなわち MAC アドレスの先頭 3 バイトで検索します。
- [Exclude switch trunk ports]: スイッチ ポートのトレースからスイッチ トランク ポートを除外する場合に、このチェックボックスをオンにします。

  （注）　特定の MAC アドレスについて複数ポートをトレースする場合は、精度を向上させるために、追加のチェックが実行されます。トランク ポートのチェック、ポート上にある AP でない CDP ネイバーのチェック、およびこの MAC アドレスがこのポート上の唯一のアドレスであるかどうかのチェックを含みます。
- [Exclude device list]：トレースから追加のデバイスを除外する場合に、このチェックボックスをオンにします。スイッチ ポート トレースから除外する各デバイスをデバイス リスト テキスト ボックスに入力します。各デバイス名はカンマで区切ります。
- [Max hop count]：このトレースに対するホップの最大数を入力します。ホップ カウントを大きくするほど、スイッチ ポート トレースの実行時間が長くなることに留意してください。

- [Exclude vendor list]: スイッチ ポート トレースから除外するすべてのベンダーをベンダー リスト テキスト ボックスに入力します。ベンダー名はカンマで区切ります。ベンダー リストでは、大文字と小文字が区別されません。

ステップ 4　必要に応じて、以下の拡張設定を行います。

- [TraceRogueAP task max thread] : スイッチ ポート トレーシングで、複数のスレッドを使用して不正アクセス ポイントをトレースします。このフィールドは、並列スレッドでトレースできる不正アクセス ポイントの最大数を示します。
- [TraceRogueAP max queue size] : スイッチ ポート トレーシングでは、キューを保持して、不正アクセス ポイントをトレースします。トレーシングする不正アクセス ポイントを選択すると、処理待ちのキューに入ります。このフィールドは、キューに保管できる項目の最大数を示します。
- [SwitchTask max thread] : スイッチ ポート トレーシングでは、複数のスレッドを使用して、スイッチ デバイスをクエリーします。このフィールドは、並列スレッドでクエリーできるスイッチ デバイスの最大数を示します。

（注）　これらのパラメータのデフォルト値は、通常の運用に適しています。これらのパラメータは、スイッチ ポート トレーシングと Prime Infrastructure のパフォーマンスに直接影響します。必要な場合を除き、これらのパラメータは変更しないことを推奨します。

- [Select CDP device capabilities] : 有効にするには、チェックボックスをオンにします。

（注）　Prime Infrastructure では、トレーシング中にネイバーを検出するために CDP を使用します。ネイバーが検証されると、Prime Infrastructure では、[CDP capabilities] フィールドを使用して、ネイバー デバイスが有効なスイッチであるかどうかを判別します。ネイバー デバイスが有効なスイッチでない場合は、トレースされません。

ステップ 5　行った変更を保存するには [Save] をクリックします。ページを元の設定に戻すには、[Reset] をクリックします。出荷時の初期状態に設定を戻すには、[Factory Reset] をクリックします。

スイッチ ポート トレーシングの確立

スイッチ ポート トレーシングを確立するには、次の手順に従ってください。

ステップ 1　Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。

ステップ 2　[Rogue APs and Adhoc Rogues] セクションで、不正要素の過去 1 時間以内、過去 24 時間以内、および合計のアクティブ数な指定する数値 URL をクリックします。

ステップ 3　[MAC Address] 列の URL をクリックして、スイッチ ポートを設定している不正アクセス ポイントを選択します。[Alarms] > [Rogue AP details] ページが開きます。

ステップ 4　[Select a command] ドロップダウン リストから、[Trace Switch Port] を選択します。[Trace Switch Port] ページが開き、Prime Infrastructure によってスイッチ ポート トレースが実行されます。

検索可能な MAC アドレスを 1 つ以上使用できる場合、Prime Infrastructure では CDP を使用して、検出中のアクセス ポイントから最大 2 ホップ離れて接続されているすべてのスイッチを検出します。各 CDP が検出したスイッチの MIB は、対象の MAC アドレスのいずれかが含まれているかどうかを確認するために検証されます。いずれかの MAC アドレスが見つかった場合、該当するポート番号が返され、不正スイッチ ポートとして報告されます。

スイッチの SNMP コミュニティについては、「スイッチの設定」（P.9-500）を参照してください。

[Switch Port Tracing Details] ダイアログボックスに関する追加情報については、「Switch Port Tracing Details」（P.15-881）を参照してください。

Switch Port Tracing Details

[Switch Port Tracing Details] ダイアログボックスでは、スイッチ ポートの有効化および無効化、スイッチ ポートのトレース、およびアクセス ポイント スイッチ トレースの詳細ステータスの表示を行うことができます。スイッチ ポート トレーシングの詳細については、以下のトピックを参照してください。

- スイッチ ポート トレーシングの設定：スイッチ ポート トレースの設定について説明します。
- スイッチの設定：SNMP スイッチの設定について説明します。
- SNMP クレデンシャルの設定：SNMP スイッチ クレデンシャルの設定について説明します。

[Switch Port tracing Details] ダイアログボックスで、次のいずれかを実行します。

- [Enable/Disable Switch Port(s)] をクリック：選択した任意のポートを有効または無効にします。
- [Trace Switch Port(s)] をクリック：別のスイッチ ポート トレースを実行します。
- [Show Detail Status] をクリック：このアクセス ポイントのスイッチ ポート トレースに関する詳細を表示します。
- [Close] をクリックします。

スイッチ ポート トレーシングのトラブルシューティング

スイッチ ポート トレーシング（SPT）は、ベストエフォート方式で動作します。SPT では、適切にトレースして不正 AP を組み込むために、以下の情報を必要とします。

- レポート アクセス ポイント：不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- アクセス ポイント CDP ネイバー：シード スイッチを判別するために、アクセス ポイント CDP ネイバー情報が必要です。
- スイッチの IP アドレスと SNMP のクレデンシャル
  - トレースする必要のあるすべてのスイッチは管理 IP アドレスを持つ必要があり、SNMP 管理が有効にされている必要があります。
  - SNMP クレデンシャルが新しく変更される場合は、個々のスイッチを Prime Infrastructure に追加するのではなく、ネットワーク アドレスに基づき追加できます。
  - この新しい SNMP クレデンシャル機能は、read と write の両方についてデフォルトのコミュニティ ストリングを「private」とするデフォルト エントリ 0.0.0.0 を持ちます。
  - スイッチ ポートを有効または無効にするには、正しい write コミュニティ ストリングを指定する必要があります。トレーシングの場合、通常、read コミュニティ ストリングで十分です。
- スイッチ ポートの設定
  - トランキングされているスイッチ ポートは、トランク ポートとして正しく設定されている必要があります。
  - スイッチ ポートのセキュリティはオフにする必要があります。
- シスコ イーサネット スイッチだけがサポートされています。

（注）　サポートされているスイッチは、3750、3560、3750E、3560E、および 2960 です。

- スイッチ VLAN 設定を適切に行う必要があります。
- すべてのスイッチについて CDP プロトコルが有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正アクセス ポイントとイーサネット スイッチの間に何らかのトラフィックが存在する必要があります。
- 不正アクセス ポイントは、最大ホップ カウントの制限内で、スイッチに接続される必要があります。デフォルト ホップは 2 です。最大ホップは 10 です。
- SNMPv3 を使用する場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成してください。

OUI の管理

Prime Infrastructure では、IEEE 組織固有識別子（OUI）データベースを使用してクライアント ベンダー名マッピングが識別されます。Prime Infrastructure では、ベンダー OUI マッピングは、vendorMacs.xml という名前の XML ファイルに保存されます。このファイルは、Prime Infrastructure のリリースごとに更新されます。OUI の更新により、以下を実行できます。

- 既存の OUI のベンダー表示名の変更。
- Prime Infrastructure への新しい OUI の追加。
- 新しいベンダー OUI マッピングによる vendorMacs.xml ファイルの更新、および Prime Infrastructure へのそのファイルのアップロード。

ここでは、次の内容について説明します。

- 「新しいベンダー OUI マッピングの追加」（P.15-882）
- 「更新されたベンダー OUI マッピング ファイルのアップロード」（P.15-883）

新しいベンダー OUI マッピングの追加

[User Defined OUI List] ページに、作成したベンダー OUI マッピングのリストが表示されます。このページで、新しいベンダー OUI マッピングの追加、OUI エントリの削除、および vendorMacs.xml ファイルに存在する OUI のベンダー名の更新を実行できます。

OUI を追加すると、Prime Infrastructure は vendorMacs.xml ファイルを調べて OUI があるかどうかを確認します。OUI がある場合、Prime Infrastructure は OUI のベンダー名を更新します。OUI がない場合、Prime Infrastructure はベンダー OUI マッピングに新しい OUI エントリを追加します。

新しいベンダー OUI マッピングを追加するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[User Defined OUI] を選択します。[User Defined OUI] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Add OUI Entries] を選択し、[Go] をクリックします。

ステップ 4　[OUI] フィールドに有効な OUI を入力します。形式は aa:bb:cc です。

ステップ 5　[Check] をクリックして、OUI がベンダー OUI マッピングに存在するかどうかを確認します。

ステップ 6　[Name] フィールドに、OUI のベンダーの表示名を入力します。

ステップ 7　[Change Vendor Name] チェックボックスをオンにして、OUI がベンダー OUI マッピングに存在する場合に、ベンダーの表示名を更新します。

ステップ 8　[OK] をクリックします。

更新されたベンダー OUI マッピング ファイルのアップロード

更新された vendorMacs.xml ファイルが cisco.com に定期的に掲示されます。このファイルをダウンロードし、同じファイル名の vendorMacs.xml を使用してローカル ディレクトリに保存できます。その後、このファイルを Prime Infrastructure にアップロードできます。Prime Infrastructure は、既存の vendorMacs.xml ファイルをアップロードされたファイルに置き換えて、ベンダー OUI マッピングを更新します。ただし、新しいベンダー OUI マッピングまたはユーザが行ったベンダー名の更新は上書きされません。

更新されたベンダー OUI マッピング ファイルをアップロードするには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Upload OUI] を選択します。[Upload OUI From File] ページが表示されます。

ステップ 3　Cisco.com からダウンロードした vendorMacs.xml ファイルを参照し、選択します。

ステップ 4　[OK] をクリックします。

Cable Modem Termination System（CMTS）の設定

CMTS は Cisco ユニバーサル ブロードバンド ルータ（uBR）で、Cisco MCxx ケーブル モデム カードを介してハイブリッド ファイバの同軸（HFC）ケーブル ネットワークとの通信を可能にします。Cisco MCxx ケーブル モデム カードを使用して HFC ネットワーク上のケーブル モデムをコミュニティ アンテナ テレビジョン（CATV）のヘッドエンド機能の Cisco uBR7200、uBR7100 または uBR10k に接続することができます。このモデムは Cisco uBR プロトコル制御情報（PCI）バスと DOCSIS HFC ネットワーク上の無線周波（RF）信号との間のインターフェイスを提供します。ケーブル モデムを管理するためにサービス プロバイダーが CMTS を使用し続けている間、Prime Infrastructure を使用して主要なケーブル モデムの健全性パラメータをモニタできます。

CMTS パラメータを設定するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバー メニューから [CMTS Configuration] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add CMTS] を選択し、[Go] をクリックします。

ステップ 4　[IP Address] には、CMTS の IP アドレスを入力します。

ステップ 5　次の SNMP 設定を行います。

- [Version]：SNMP バージョン番号で、v1 または v2c のいずれか。

- [Community]：このフィールドは、SNMP コミュニティ ストリングを示します。
- [Retries]：Prime Infrastructure が成功せずに停止するまでに許可される再試行回数。
- [Timeout]：SNMP タイムアウト値（秒単位）。

ステップ 6　マッピングするコントローラを選択します。

（注）　マップされたコントローラに関連付けられた Cisco Aironet 1552C および Cisco Aironet 1552CU アクセス ポイント モデルは CMTS によってモニタされます。Prime Infrastructure は、要求された AP のケーブル モデムの統計情報のためにこの CMTS に接続します。

ステップ 7　[Save] をクリックします。

関連トピック

- Cable Modem Termination System（CMTS）の設定

User Preferences の設定

[Administration] > [User Preferences] の順に選択して [User Preferences] ページを開きます。[User Preferences] ページでは、Prime Infrastructure の特定の表示オプションを制御できます。

（注）　root 以外のユーザが Prime Infrastructure にログインしてユーザ設定を変更しようとすると、「Permission Denied」メッセージが表示されます。これは正常な動作です。

リスト ページ

- [Items Per List]：コントローラ、アクセス ポイントなどの項目について、これらがリストされるページに表示される場合の項目の数を設定できます。[Items Per List Page] ドロップダウン リストから、表示する項目の数を選択してください。

マップ

- [Use Next Generation Maps]：次世代マップ機能を使用する場合は、このチェックボックスをオンにします。次世代マップ機能の詳細については、「マップについて」（P.6-153）を参照してください。

ユーザ アイドル タイムアウト

- [Logout idle user]：サーバによってセッションがキャンセルされるまでにユーザ セッションがアイドル状態になっていることを許容される時間（分）を設定するには、このチェックボックスをオンにします。
- [Logout idle user after]：サーバがアイドル ユーザを待機する最大分数を選択します。デフォルト値は 60 分です。最小値は 15 分です。最大値は 120 分です。

（注）　[Logout idle user] チェックボックスをオフにしてある場合、ユーザ セッションはタイムアウトしません。

アラーム

- [Refresh Map/Alarms page on new alarm] : 新しいアラームが生成されるたびにマップ ページおよびアラーム ページを更新する場合は、このチェックボックスをオンにします。
- [Refresh Alarm count in the Alarm Summary every]: ドロップダウン リストからアラーム概要の更新頻度（5 秒、15 秒、30 秒、1 分、2 分、または 5 分ごと）を選択します。
- [Display Alarm Category in Alarm Summary] ページ: 最小化した [Alarm Summary] に表示するアラーム カテゴリ（[Alarm Summary]、[Malicious AP]、[Unclassified AP]、[Coverage Holes]、[Security]、[Controllers]、[Access Points]、[Mobility Services]、[Mesh Links]、[Prime Infrastructure]、または [Performance]）を選択します。
- [Disable Alarm Acknowledge Warning Message] : アラームを承認するときは、問題が繰り返し起きてもアラームは繰り返し生成されないことを伝える警告が表示されます。機能を無効すれば、この警告は表示されなくなります。この警告メッセージが表示されないようにするには、このチェックボックスをオンにします。
- [Select alarms for Alarm Summary Toolbar] : [Alarm Summary] ツールバーに表示するアラームを選択するには、[Edit Alarm Categories] をクリックし、必要なアラーム カテゴリおよびサブカテゴリを選択します。

このページには、ユーザ固有の調整可能な設定が含まれています。

ユーザ固有の設定を変更するには、次の手順に従ってください。

ステップ 1　[Administration] > [User Preferences] の順に選択します。[User Preferences] ページが表示されます。

ステップ 2　[Items Per List Page] ドロップダウン リストを使用して、指定したリストのページ（アラーム、イベント、AP リストなど）に表示される項目の数を設定します。

ステップ 3　[Refresh home page] チェックボックスをオンにし、[Refresh home page every] ドロップダウン リストから時間間隔を選択することで、ホームページをリフレッシュする頻度を指定します。

ステップ 4　[Logout idle user] チェックボックスをオンにし、[Logout idle user after] テキスト ボックスに、サーバによってセッションがキャンセルされるまでのユーザ セッションのアイドル時間（分）を設定します。

ステップ 5　Prime Infrastructure で新しいアラームが発生したときにマップとアラームのページを自動的に更新する場合は、ページ上の [Alarms] 部分にある [Refresh Map/Alarms page on new alarm] チェックボックスをオンにします。

ステップ 6　[Refresh Alarm count in the Alarm Summary every] ドロップダウン リストからリセット頻度を指定する時間間隔を選択します。

ステップ 7　アラーム承認警告メッセージを表示しない場合は、[Disable Alarm Acknowledge Warning Message] チェックボックスをオンにします。

ステップ 8　[Edit Alarm Categories] をクリックして、[Alarm Summary] ページに表示するアラーム カテゴリを選択します。

ステップ 9　[Select Alarms] ページで、表示するデフォルト カテゴリをドロップダウン リストから選択し、アラーム ツールバーから表示するアラームのカテゴリとサブカテゴリを選択します。[Save] をクリックしてアラーム カテゴリ リストを保存します。選択したアラームのカテゴリおよびサブカテゴリが [User Preferences] ページに表示されます。

ステップ 10　[Save] をクリックして [User Preference] の設定を保存します。

アプライアンス詳細の表示

ここでは、アプライアンス詳細を示します。ここでは、次の内容について説明します。

アプライアンス ステータスの詳細の表示

アプライアンスのステータスを表示するには、次の手順を実行します。

ステップ 1　[Administration] > [Appliance] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Appliance Status] を選択します。次の情報を含む [Appliance Status] ページが表示されます。詳細については、表 15-5 を参照してください。

表 15-5　[Appliance Status] の詳細

フィールド	説明
Configure Details	
Host Name	マシンのホスト名。ユーザ マシンのホスト名が DNS にない場合、IP アドレスが表示されます。
Domain Name	サーバのドメイン名。
Default Gateway	属しているネットワーク環境のデフォルト ゲートウェイの IP アドレスです。
DNS Server(s)	DNS サーバの IP アドレスです。各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。
NTP Host(s)	NTP サーバの IP アドレスです。
Status Details	
Server Time	サーバのシステム時刻。
System Up Time	サーバが起動してからダウンタイムなしで稼働している時間の指標です。
Application Up Time	Prime Infrastructure が起動してからダウンタイムなしで稼働している時間の指標です。
Temperature Status	サーバの温度ステータス。
RAID Status	サーバの RAID ステータス。
Fan Status	サーバの冷却ファンのステータス。
Power Supply Status	サーバの電源装置のステータス。
CPU Utilization	サーバの CPU 使用率。
Memory Utilization	サーバのメモリ使用率。
Inventory Details	詳細インベントリ レポート。
UDI Details	
Product Identifier	製品 ID は、デバイスのタイプを識別します。
Serial Number	シリアル番号は、デバイスを一意に識別する 11 桁の番号です。
Version Identifier	VID は製品のバージョンです。製品が改訂されるたびに、VID は増分されます。

アプライアンス インターフェイスの詳細の表示

アプライアンス インターフェイスの詳細を表示するには、次の手順に従います。

ステップ 1　[Administration] > [Appliance] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Appliance Interface] を選択します。[Interfaces] ページが表示されます。

表 15-6　[Appliance Interface] の詳細

フィールド	説明
Interface Name	このインターフェイスのユーザ定義の名前。
MAC Address	インターフェイスの MAC アドレス。
IP Address	インターフェイスのローカル ネットワーク IP アドレス。
Netmask	範囲内の IP アドレスを持つマシンだけにインターネット サービスへのアクセスを許可するために定義された IP アドレスの範囲。
Type	スタティック（管理、ピア、AP-Manager、サービス ポート、および仮想インターフェイス）またはダイナミック（オペレータ定義インターフェイス）。

ステップ 3　インターフェイスがピア サーバまたは管理インターフェイスのどちらであるかを指定するには、設定する [Interface Type] をクリックします。

AAA の設定

ここでは、次の内容について説明します。

- 「Prime Infrastructure を使用した AAA の設定」（P.15-888）
- 「ACS 4.x の設定」（P.15-905）
- 「ACS 5.x の設定」（P.15-910）

Prime Infrastructure を使用した AAA の設定

[Administration] > [AAA] から、Prime Infrastructure 用に、認証、許可、アカウンティング（AAA）を設定できます。Prime Infrastructure AAA を設定する権限を持つユーザの名前は、*root* および SuperUser のみです。ローカル ユーザ アカウントに対するすべての変更は、ローカル モード用に設定した場合に有効です。RADIUS、TACACS+ などの外部認証を使用している場合、ユーザの変更は、リモート サーバ上で行う必要があります。

ここでは、次の内容について説明します。

- 「パスワードの変更」（P.15-889）
- 「ローカル パスワード ポリシーの設定」（P.15-890）
- 「AAA モードの設定」（P.15-889）
- 「ユーザの設定」（P.15-890）
- 「グループの設定」（P.15-895）

- 「アクティブなセッションの表示」（P.15-896）
- 「TACACS+ サーバの設定」（P.15-897）
- 「RADIUS サーバの設定」（P.15-899）
- 「SSO サーバの設定」（P.15-900）
- 「Cisco Identity Services Engine（ISE）を使用した RADIUS を介する AAA ユーザの認証」（P.15-901）

パスワードの変更

このページにアクセスするには、左側のサイドバーのメニューから、[Administration] > [AAA] > [Change Password] を選択します。

このページでは、現在ログインしているユーザのパスワードを変更できます。

- [User]：ログイン ユーザに適用されます。
- [Old Password]：現在のパスワードです。
- [New Password]：ASCII 文字を使用して新規パスワードを入力します。
- [Confirm password]：新しいパスワードを再度入力します。
- [Submit]：パスワードの変更を確定するには、[Submit] をクリックします。

AAA モードの設定

このページにアクセスするには、左側のサイドバーのメニューから、[Administration] > [AAA] > [AAA Mode] を選択します。

このページでは、全ユーザの認証モードを設定できます。

- AAA Mode Settings
  - [Local]：ローカル データベースと照合してユーザを認証します。
  - [RADIUS]：外部 RADIUS サーバと照合してユーザを認証します。
  - [TACACS+]：外部 TACACS+ サーバと照合してユーザを認証します。
  - [SSO]：シングル サインオン（SSO）サーバと照合してユーザを認証します。
- [Enable fallback to Local]：外部認証サーバが停止している場合に、ユーザをローカルで認証できます。このチェックボックスは、RADIUS、TACACS+、および SSO の場合のみ使用可能です。
  - ドロップダウン リストから [ONLY on no server response] または [on auth failure or no server response] を選択します。

「TACACS+ サーバの設定」（P.15-897）と「RADIUS サーバの設定」（P.15-899）も参照してください。

AAA Mode Settings

AAA モードを選択するには、次の手順を実行します。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [AAA Mode] を選択します。[AAA Mode Settings] ページが表示されます。

ステップ 3　使用する AAA モードを選択します。一度に 1 つしか選択できません。

ローカル ユーザ アカウントに関する変更は、ローカル モード（デフォルト）に設定されている場合しか反映されません。リモート認証を使用する場合は、リモート サーバ上でクレデンシャルが変更されます。リモート認証には RADIUS、TACACS+、および SSO の 3 種類があります。RADIUS では、異なるロケーション（米国東海岸と西海岸）に対して別々のクレデンシャルが必要となります。TACACS+ は、組み込みのフェールオーバー メカニズムを備えた効率的でセキュリティで保護された管理フレームワークです。SSO は、複数ユーザ、複数リポジトリ環境でユーザを認証および管理するため、および各種システムへのログインに使用される認証情報を保存および取得するために使用されます。

ステップ 4　外部の AAA サーバがダウンしたときに管理者にローカル データベースを使用させる場合は、[Enable Fallback to Local] チェックボックスをオンにします。

（注）　このチェックボックスは、AAA モードの種類として [*Local*] が選択されている場合には使用できません。

ステップ 5　[OK] をクリックします。

ローカル パスワード ポリシーの設定

このページにアクセスするには、左側のサイドバーのメニューから、[Administration] > [AAA] > [Local Password Policy] を選択します。このページでは、ローカル パスワード ポリシーを決定できます。

ローカル パスワードに対する以下のポリシーを有効または無効にすることができます。

- パスワードの最小長を設定します。デフォルトでは、8 に設定されています。
- ユーザ名やユーザ名の逆読みはパスワードにできません。
- cisco または ocsic（cisco の逆読み）という単語や、これと同じ内容を表す任意の特殊文字による置換は、パスワードにできません。
- public という単語は、ルート パスワードにできません。
- パスワード内で同じ文字を 4 回以上続けて繰り返すことはできません。
- パスワードには、大文字、小文字、数字、および特殊文字の中から 3 種類の文字を使用する必要があります。

[Save] をクリックして、ローカル パスワード ポリシーの変更を確定します。

ユーザの設定

この項では、Prime Infrastructure ユーザを設定する方法を説明します。完全なアクセス以外に、特定のユーザ グループに対して異なる権限の管理アクセスを付与できます。

このページにアクセスするには、左側のサイドバーのメニューから、[Administration] > [AAA] > [Users] を選択します。このページを使用すると、ユーザ詳細の表示、ユーザの作成、ユーザの削除、およびユーザ詳細の編集を行うことができます。

ここでは、次の内容について説明します。

- 「ユーザ詳細の表示」（P.15-891）
- 「現在のユーザの編集：パスワードおよび割り当てグループ」（P.15-891）

ユーザ詳細の表示

[Users] ページで Prime Infrastructure ユーザの詳細を表示できます。以下の情報は、[Administration] > [AAA] > [Users] ページにあります。

- Current User Names
- [Member Of]：ユーザが関連付けられているグループ。[Member Of] 列内の項目をクリックすると、このユーザの場合に許可されるタスクが表示されます。
- [Audit Trail]：現在の監査証跡を表示またはクリアするには、個別のユーザの [Audit Trail] アイコンをクリックします。「ユーザ操作の監査」（P.15-894）を参照してください。

（注） Prime Infrastructure では、いつでも最大 25 人の同時ユーザ ログインがサポートされます。

現在のユーザの編集：パスワードおよび割り当てグループ

現在のユーザ アカウント パスワードおよび割り当てグループを編集するには、次の手順に従ってください。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　[User Name] 列から具体的なユーザを選択します。

ステップ 4　（任意）必要に応じて、新しいパスワードを入力し、確定します。

ステップ 5　必要に応じて、[Groups Assigned to this User] チェックボックスの選択を変更します。

（注） ユーザが Lobby Ambassador、Monitor Lite、North Bound API、または User Assistant グループに属する場合、このユーザは他のグループに属すことはできません。

ステップ 6　[Submit] を選択して変更を確定するか、[Cancel] を選択して変更を有効にすることなくページを閉じます。

現在のユーザの編集：許可されるタスク

このユーザ アカウントの許可されるタスクを編集するには、次の手順に従ってください。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　[Member Of] 列から該当するグループを選択します。

ステップ 4　[List of Tasks Permitted] 列で該当するタスクを選択または選択解除して、タスクを許可または禁止します。

（注）　選択可能なタスクのリストは、グループのタイプによって異なります。

ステップ 5　[Submit] を選択して変更を確定するか、[Cancel] を選択して変更を有効にすることなくページを閉じます。

現在のユーザの編集：このユーザに割り当てられたグループ

このユーザに割り当てられたグループを編集するには、次の手順に従ってください。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　[User Name] 列から具体的なユーザを選択します。

ステップ 4　ユーザが割り当てられているグループのチェック ボックスをオンにします。

（注）　ユーザが Lobby Ambassador、Monitor Lite、North Bound API、または User Assistant グループに属する場合、このユーザは他のグループに属すことはできません。
Root は「root」ユーザにだけ割り当てでき、その割り当てを変更できません。

（注）　割り当てられたグループの詳細については、「新しいユーザの追加」（P.15-892）のステップ 7 を参照してください。

ステップ 5　[Submit] を選択して変更を確定するか、[Cancel] を選択して変更を有効にすることなくページを閉じます。

新しいユーザの追加

[Add User] ページを使用して、管理者はユーザ名、パスワード、ユーザに割り当てられるグループ、ユーザの仮想ドメインなど、新しいユーザ ログインを設定できます。仮想ドメインの割り当ての詳細については、「仮想ドメインの割り当て」（P.15-893）を参照してください。

（注）　仮想ドメインをユーザに割り当てることによって、ユーザはこれらの仮想ドメインに適切な情報に制限されます。

（注）　このページを開くには、SuperUsers ステータスである必要があります。

ユーザ名、パスワード、およびグループの追加

新規ユーザを追加する手順は、次のとおりです。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add User] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　新しいユーザ名を入力します。

ステップ 6　このアカウントのパスワードを入力して確定します。

ステップ 7　ユーザが割り当てられているグループのチェック ボックスをオンにします。

（注）　ユーザが Lobby Ambassador、Monitor Lite、North Bound API、または User Assistant グループに属する場合、このユーザは他のグループに属すことはできません。

- [Admin]：ユーザは Prime Infrastructure の動作をモニタおよび設定でき、Prime Infrastructure のユーザ アカウントとパスワードの管理を除くすべてのシステム管理タスクを実行できます。
- [Config Managers]：Prime Infrastructure の動作をモニタおよび設定できます。
- [Lobby Ambassador]：ゲストのアクセスで許可されるのは、ユーザ アカウントの設定と管理だけです。[Lobby Ambassador] を選択すると、[Lobby Ambassador Defaults] タブが表示されます。Lobby Ambassador アカウントの設定の詳細は、「Lobby Ambassador アカウントの管理」（P.7-258）を参照してください。
- [Monitor Lite]：アセットの位置をモニタできます。
- [North Bound API User]：Prime Infrastructure Web サービスの利用者だけで使用されるグループです。

（注）　North Bound API User には、仮想ドメインを割り当てられません。North Bound API グループを選択すると、[Virtual Domains] タブを使用できなくなります。

（注）　ROOT-DOMAIN にログインしている場合は、North Bound API User だけを追加できます。

- [Root]：このグループは「root」ユーザにだけ割り当てでき、その割り当てを変更できません。
- [Super Users]：Prime Infrastructure の動作をモニタおよび設定でき、Prime Infrastructure のユーザ アカウントとパスワードの管理を含むすべてのシステム管理タスクを実行できます。スーパーユーザのタスクは、変更できます。
- [System Monitoring]：Prime Infrastructure の動作をモニタできます。
- [User Assistant]：ローカル ネット ユーザの管理のみ実行できます。
- User Defined

仮想ドメインの割り当て

このユーザに仮想ドメインを割り当てるには、次の手順に従ってください。

ステップ 1　[Virtual Domains] タブを選択します。このページには、このユーザに割り当てられているか使用できるすべての仮想ドメインが表示されます。

（注）　[Virtual Domains] タブを使用して、管理者は仮想ドメインを各ユーザに割り当てることができます。仮想ドメインをユーザに割り当てることによって、ユーザはこれらの仮想ドメインに適切な情報に制限されます。

（注）　North Bound API User には、仮想ドメインを割り当てられません。North Bound API グループを選択すると、[Virtual Domains] タブを使用できなくなります。

ステップ 2　[Available Virtual Domains] リストで、このユーザに割り当てる仮想ドメインをクリックして強調表示します。

（注）　Shift キーまたは Ctrl キーを押したまま、複数の仮想ドメインを選択できます。

ステップ 3　[Add] をクリックします。仮想ドメインが [Available Virtual Domains] リストから [Selected Virtual Domains] リストに移動します。

仮想ドメインを [Selected Virtual Domains] リストから削除するには、[Selected Virtual Domains] リストのドメインをクリックして強調表示し、[Remove] をクリックします。仮想ドメインが [Selected Virtual Domains] リストから [Available Virtual Domains] リストに移動します。

ステップ 4　[Submit] を選択するか、[Cancel] を選択します。後者を選択した場合、現在のユーザは追加または編集されずにページが閉じられます。

ユーザ操作の監査

このアカウントの監査情報を表示またはクリアするには、次の手順に従ってください。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Users] を選択します。

ステップ 3　該当するアカウントの [Audit Trail] アイコンをクリックします。

（注）　このページを開くには、SuperUsers ステータスである必要があります。

このページでは、ユーザ操作の時系列のリストを表示できます。

- [User]：ユーザのログイン名。
- [Operation]：監査された操作の種類。
- [Time]：操作が監査された時刻。
- [Status]：成功または失敗。
- [Reason]：理由は障害だけに適用されます。
- [Configuration Changes]：設定が変更されている場合、このフィールドに [Details] リンクが表示されます。個々のユーザによる設定の変更の詳細を確認するには [Details] リンクをクリックします。Prime Infrastructure とコントローラ間の個別パラメータの値の変更が項目にリストされます。監査証跡の詳細については、「[Audit Trail Details] ページ」（P.7-251）を参照してください。

ステップ 4　監査証跡をクリアするには、該当する監査のチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Clear Audit Trail] を選択し、[Go] をクリックしてから [OK] をクリックして確定します。

グループの設定

このページには、現在の全グループのリストおよびこれに関連付けられたメンバが示されます。

- [Group Name]：このグループの許可されるタスクを表示または編集する具体的なグループをクリックします。選択可能なタスクは、グループのタイプによって異なります。詳細については、「現在のユーザの編集：許可されるタスク」（P.15-891）を参照してください。
- [Members]：ユーザを表示または編集するには、[Member] 列の下の具体的なユーザをクリックします。詳細については、「現在のユーザの編集：パスワードおよび割り当てグループ」（P.15-891）を参照してください。
- [Audit Trail]：このグループの監査を表示またはクリアするには [Audit Trail] アイコンをクリックします。詳細については、「ユーザ操作の監査」（P.15-894）を参照してください。
- [Export]：このグループと関連付けられたタスク リストをエクスポートする場合にクリックします。

[Groups] ページにアクセスするには、次の手順に従ってください。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [User Group] を選択します。

（注）　このページを開くには、SuperUsers ステータスである必要があります。

ユーザ グループ情報の表示または編集

定義されたグループ内でユーザによる実行の許可されている具体的なタスクを参照するか、タスクに変更を加えるには、次の手順に従ってください。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[User Groups] を選択します。

ステップ 3　[Group Name] 列内をクリックします。[Group Detail: *User Group*] ページが表示されます。

（注）　詳細事項を記載したページは、選択したグループに応じて異なります。

定義されたグループ内でユーザによる実行の許可されている具体的なタスクを参照できます。

ステップ 4　対応するユーザ グループの監査証跡情報を表示するには、[Audit Trail] をクリックします。監査証跡の詳細については、「[Audit Trail Details] ページ」（P.7-251）を参照してください。

ステップ 5　必要なすべての変更をタスクに加えます。

表 15-7　デフォルト ユーザ グループ

ユーザ グループ	説明
Admin	Prime Infrastructure 管理のためのグループ。
Config Managers	モニタリング タスクおよび設定タスク用のグループ。
Lobby Ambassador	ゲスト ユーザの管理だけを許可するグループ。このグループは編集不可能です。
Monitor Lite	アセットのモニタリングだけを許可するグループ。グループは編集不可能です。
North Bound API	North Bound API にアクセスできるグループ。グループは編集不可能です。
Root	ルート ユーザ用のグループ。グループは編集不可能です。
Super Users	すべての Prime Infrastructure タスクを許可するグループ。
System Monitoring	タスクだけのモニタリング用のグループ。
User Assistant	ローカル ネット ユーザの管理だけを許可するグループ。グループは編集不可能です。
User-Defined 1	ユーザ定義可能なグループ。
User-Defined 2	ユーザ定義可能なグループ。
User-Defined 3	ユーザ定義可能なグループ。
User-Defined 4	ユーザ定義可能なグループ。

ステップ 6　[Submit] をクリックします。

アクティブなセッションの表示

このページを開くには、左側のサイドバーのメニューから、[Administration] > [AAA] > [Active Sessions] を選択します。

このページには、現在ログインしているユーザのリストが表示されます。赤で表示されているユーザは、現在ログインしていることを表しています。

（注）　アクティブ セッションを参照するには、SuperUsers 権限を持つユーザ アカウントでログインする必要があります。

列見出しがハイパーリンクの場合、列見出しをクリックするとアクティブ セッションの一覧をその列の降順または昇順で並べ替えることができます。並べ替えの方向は、ハイパーリンクをクリックするたびに切り替わります。

[Active Sessions] ページの列は、次のとおりです。

- [Username] : ログインするユーザのユーザ ID。
- [IP/Host Name] : ブラウザが稼働しているマシンの IP アドレスまたはホスト名。ユーザ マシンのホスト名が DNS にない場合、IP アドレスが表示されます。
- [Login Time] : ユーザが Prime Infrastructure にログインした時刻。すべての時刻は、Prime Infrastructure サーバのマシンの時刻に基づいています。

- [Last Access Time] : ユーザのブラウザが Prime Infrastructure にアクセスした時刻。すべての時刻は、Prime Infrastructure サーバのマシンの時刻に基づいています。

（注）　この列に表示されている時刻は、通常、使用しているシステムの時刻より数秒遅れています。これは、[Alarm Status] パネルの更新によって、[Last Access Time] が頻繁に更新されるためです。ただし、ユーザが同じブラウザで Prime Infrastructure 以外の Web ページへ移動した場合、時刻のずれはさらに大きくなります。ブラウザに Prime Infrastructure Web ページが表示されていない場合、アラーム カウントは更新されません。

- [Login Method] : ログイン方式として次のいずれかを使用できます。
  - Local
  - RADIUS
  - TACACS+
- [User Groups] : ユーザが属しているグループのリスト。
- 監査証跡アイコン : そのユーザの監査証跡（以前のログイン時刻）を表示するページへのリンク。

TACACS+ サーバの設定

この項では、TACACS+ サーバの追加と削除の方法について説明します。TACACS+ サーバは、組み込みのフェールオーバー メカニズムを備えた効率的でセキュリティで保護された管理フレームワークを提供します。設定を変更するには、認証されている必要があります。

[TACACS+] ページには、TACACS+ サーバの IP アドレス、ポート、再送信レート、および認証の種類（パスワード認証プロトコル（PAP）またはチャレンジ ハンドシェイク認証プロトコル（CHAP））が表示されます。TACACS+ サーバは、それらの設定内容に基づいて試行されます。

（注）　TACACS+ サーバをアクティブにするには、「ACS 4.x の設定」（P.15-905）に記載されている方法で有効にする必要があります。

TACACS+ を設定するには、次の作業を行います。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[TACACS+] を選択します。[TACACS+] ページが表示されます。

ステップ 3　[TACACS+] ページには、TACACS+ サーバの IP アドレス、ポート、再送信レート、および認証の種類（パスワード認証プロトコル（PAP）またはチャレンジ ハンドシェイク認証プロトコル（CHAP））が表示されます。TACACS+ サーバは、それらの設定内容に基づいて試行されます。

（注）　TACACS+ サーバの試行順序を変更する必要がある場合は、関連のない TACACS+ サーバを削除し、目的の TACACS+ サーバを必要に応じた順序に再度追加します。

ステップ 4　右上隅のドロップダウン リストを使用して、TACACS+ サーバを追加または削除します。情報を変更する場合は、IP アドレスをクリックします。

ステップ 5　現在のサーバ アドレスとポートが表示されます。ドロップダウン リストを使用して、ASCII または HEX のいずれかの共有秘密形式を選択します。

ステップ 6　指定のサーバで使用する TACACS+ 共有秘密を入力します。

ステップ 7　[Confirm Shared Secret] テキスト ボックスに共有秘密をもう一度入力します。

ステップ 8　TACACS+ 認証要求がタイムアウトし、コントローラが再転送を試みるまでの時間を秒単位で指定します。

ステップ 9　再試行の回数を指定します。

ステップ 10　[Authentication Type] ドロップダウン リストで、PAP プロトコルまたは CHAP プロトコルを選択します。

ステップ 11　[Local Interface IP] ドロップダウン リストで、インターフェイスの IP アドレスを選択します。

このインターフェイス IP アドレスは、TACACS+ 用の ACS サーバで指定したアドレスと同じです。

ステップ 12　[Submit] をクリックします。

（注）　7.0.x リリースで作成した RADIUS サーバまたは TACACS サーバの IP アドレスおよびその他のクレデンシャルは、Prime Infrastructure 1.0 に移行されません。7.0.x から Prime Infrastructure 1.0 への移行の完了後に再度追加する必要があります。

（注）　ACS 5.x の設定の詳細については、「ACS 5.x の設定」（P.15-910）を参照してください。

Select a command

- [Add TACACS+ Server]：「TACACS+ サーバの追加」（P.15-898）を参照してください。
- [Delete TACACS+ Server]：削除する 1 台以上のサーバを選択し、このコマンドを選択してから [Go] をクリックすると、データベースからサーバが削除されます。

TACACS+ サーバの追加

このページにアクセスするには、左側のサイドバーのメニューから、[Administration] > [AAA] > [TACACS+] を選択します。[Select a command] ドロップダウン リストから [Add TACACS+ Server] を選択して、[Go] をクリックすると、このページが表示されます。

このページでは、新しい TACACS+ サーバを Prime Infrastructure に追加できます。

- [Server Address]：追加する TACACS+ サーバの IP アドレス。
- [Port]：コントローラ ポート。
- [Shared Secret Format]：[ASCII] または [Hex]。
- [Shared Secret]：TACACS+ サーバへのログイン時にパスワードとして機能する共有秘密。
- [Confirm Shared Secret]：TACACS+ サーバの共有秘密を再入力します。
- [Retransmit Timeout]：TACACS+ 認証要求の再送信タイムアウト値を指定します。
- [Retries]：認証要求で許可される再試行回数。1 ～ 9 の値を指定できます。
- [Authentication Type]：2 種類の認証プロトコルをサポートしています。パスワード認証プロトコル（PAP）およびチャレンジ ハンドシェイク認証プロトコル（CHAP）です。

コマンド ボタン

- Submit

- Cancel

（注）
- AAA モード設定を使用して TACACS+ サーバを有効にします。「AAA モードの設定」（P.15-889）を参照してください。
- Prime Infrastructure に 1 度に追加できるサーバは 3 台のみです。

RADIUS サーバの設定

この項では、RADIUS サーバの追加と削除の方法について説明します。設定を変更するには、RADIUS サーバを有効にし、RADIUS サーバ用のテンプレートを用意する必要があります。

RADIUS では、ネットワークにアクセスするユーザを認証できます。認証要求は、すべてのユーザ認証およびネットワーク アクセス情報を格納している RADIUS サーバに送信されます。パスワードは RADIUS を使用して暗号化されます。

設定された RADIUS サーバが停止している場合、ローカル認証へのフォールバック オプションが設定されていれば、Prime Infrastructure は、ローカルな認証と許可に戻ります。「AAA モードの設定」（P.15-889）を参照してください。

（注）　RADIUS サーバをアクティブにするには、「ACS 4.x の設定」（P.15-905）に記載されている方法で有効にする必要があります。

RADIUS サーバを設定するには、次の手順に従います。

ステップ 1　[Administration] > [AAA] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[RADIUS] を選択します。[RADIUS] ページが表示されます。

ステップ 3　[RADIUS] ページには、サーバ アドレス、認証ポート、再送信タイムアウト値、および設定する各 RADIUS サーバの認証の種類が表示されます。RADIUS サーバは、それらの設定内容に基づいて試行されます。

（注）　RADIUS サーバの試行順序を変更するには、関連のない RADIUS サーバを削除し、目的の RADIUS サーバを必要に応じた順序に再度追加します。

ステップ 4　右上隅のドロップダウン リストを使用して、RADIUS サーバを追加または削除します。情報を変更する場合は、IP アドレスをクリックします。

ステップ 5　現在の認証ポートが表示されます。ドロップダウン リストを使用して、ASCII または HEX のいずれかの共有秘密形式を選択します。

ステップ 6　指定のサーバで使用する RADIUS 共有秘密を入力します。

ステップ 7　[Confirm Shared Secret] テキスト ボックスに共有秘密をもう一度入力します。

ステップ 8　RADIUS 認証要求がタイムアウトし、コントローラが再転送を試みるまでの時間を秒単位で指定します。

ステップ 9　再試行の回数を指定します。

ステップ 10　[Authentication Type] ドロップダウン リストから、PAP プロトコルまたは CHAP プロトコルを選択します。

ステップ 11　[Local Interface IP] ドロップダウン リストで、インターフェイスの IP アドレスを選択します。

このインターフェイス IP アドレスは、RADIUS 用の ACS サーバで指定したアドレスと同じです。

ステップ 12　[Submit] をクリックします。

Select a command

- [Add RADIUS Server]：「RADIUS サーバの追加」（P.15-900）を参照してください。
- [Delete RADIUS Server]：削除する 1 台以上のサーバを選択し、このコマンドを選択してから [Go] をクリックすると、データベースからサーバが削除されます。

RADIUS サーバの追加

このページにアクセスするには、左側のサイドバーのメニューから、[Administration] > [AAA] > [RADIUS] を選択します。[Select a command] ドロップダウン リストから [Add RADIUS Server] を選択して、[Go] をクリックすると、このページが表示されます。

このページでは、新しい RADIUS サーバを Prime Infrastructure に追加できます。

- [Server Address]：追加する RADIUS サーバの IP アドレス。
- [Port]：コントローラ ポート。
- [Shared Secret Format]：[ASCII] または [Hex]。
- [Shared Secret]：RADIUS サーバへのログイン時にパスワードとして機能する共有秘密。
- [Confirm Shared Secret]：RADIUS サーバの共有秘密を再入力します。
- [Retransmit Timeout]：RADIUS 認証要求の再送信タイムアウト値を指定します。
- [Retries]：認証要求で許可される再試行回数。1 ～ 9 の値を指定できます。

コマンド ボタン

- Submit
- Cancel

（注）
- AAA モード設定を使用して RADIUS サーバを有効にします。「AAA モードの設定」（P.15-889）を参照してください。
- Prime Infrastructure に 1 度に追加できるサーバは 3 台のみです。

SSO サーバの設定

この項では、SSO サーバの追加と削除の方法について説明します。

Prime Infrastructure でシングル サインオン（SSO）認証を有効にできます。SSO により、資格情報を一度入力するだけで、SSO 対応の複数の Prime Infrastructure アプリケーションにナビゲートできます。SSO により、相互起動操作を簡単に実行することや、個別のアプリケーションからのコンテンツを含むダッシュレットを簡単に使用することができます。SSO を設定するには、管理者レベルの特権が必要です。

（注）　SSO を設定する前に、SSO が設定されたサーバが必要です。現在、SSO をサポートするサーバは Prime Central サーバのみです。Prime Central のすべての管理者を、Prime Infrastructure でも定義する必要があります。Prime Infrastructure での新規ユーザの追加の詳細については、「ユーザの設定」（P.15-890）を参照してください。

SSO サーバの追加

このページにアクセスするには、左側のサイドバーのメニューから、[Administration] > [AAA] > [SSO Servers] を選択します。[Select a command] ドロップダウン リストから [Add SSO Server] を選択し、[Go] をクリックすると、[Add SSO Servers] ページが表示されます。

このページでは、新しい SSO サーバを Prime Infrastructure に追加できます。

- [Server Address]：追加する SSO サーバの IP アドレス。
- [Port]：SSH ポート。デフォルト値は 8443 です。
- [Retries]：認証要求で許可される再試行回数。1 ～ 9 の値を指定できます。

コマンド ボタン

- Save
- Cancel

（注）　[Administration] > [AAA] > [SSO Servers] ページから SSO サーバを削除することもできます。削除する SSO サーバを選択し、[Select a Command] ドロップダウン リストから [Delete SSO Server(s)] を選択し、[Go] をクリックします。

Cisco Identity Services Engine（ISE）を使用した RADIUS を介する AAA ユーザの認証

ISE と Prime Infrastructure を統合できます。この項では、ISE を使用した RADIUS プロトコルによる Prime Infrastructure ユーザ認証について説明します。

（注）　ISE では、RADIUS サーバ認証だけがサポートされています。

ISE を使用し、RADIUS サーバを介して AAA を認証するには、以下のステップを実行します。

ステップ 1　Prime Infrastructure を AAA クライアントとして ISE に追加します。詳細については、「Prime Infrastructure を AAA クライアントとして ISE に追加」（P.15-902）を参照してください。

ステップ 2　ISE で新しいユーザ グループを作成します。詳細については、「ISE での新しいユーザ グループの作成」（P.15-902）を参照してください。

ステップ 3　ISE で新しいユーザを作成し、ISE で作成したユーザ グループにこのユーザを追加します。詳細については、「ISE で新しいユーザを作成してユーザ グループに追加する」（P.15-902）を参照してください。

ステップ 4　新しい許可プロファイルを作成します。詳細については、「ISE での新しい許可プロファイルの作成」（P.15-903）を参照してください。

ステップ 5　許可ポリシー規則を作成します。詳細については、「ISE での許可ポリシー規則の作成」（P.15-904）を参照してください。

ステップ 6　Prime Infrastructure で AAA を設定します。詳細については、「Prime Infrastructure での AAA の設定」（P.15-904）を参照してください。

Prime Infrastructure を AAA クライアントとして ISE に追加

Prime Infrastructure を AAA クライアントとして ISE に追加するには、次の手順に従います。

ステップ 1　ISE にログインします。

ステップ 2　[Administration] > [Network Devices] を選択します。

ステップ 3　左側のサイドバーのメニューから、[Network Devices] の横の矢印をクリックして、そのオプションを展開します。

展開されたリストには、すでに追加されているデバイスが表示されます。

ステップ 4　任意のデバイスをクリックすると、詳細が表示されます。

ステップ 5　左側のサイドバーのメニューから、 アイコンの横の矢印をクリックし、[Add new device] オプションを選択します。

ステップ 6　右側のペインで、追加するデバイスに関する以下の詳細を入力します。

- [Name]：デバイスの名前。
- [Description]：デバイスの説明。
- [IP Address]：Prime Infrastructure サーバの IP アドレス。たとえば、`209.165.200.225` と入力します。

ステップ 7　[Shared Secret] テキスト ボックスに共有秘密を入力します。

[Save] をクリックして、デバイスを追加します。

ISE での新しいユーザ グループの作成

ISE に新しいユーザ グループを作成できます。これは、異なる権限を持つ Prime Infrastructure ユーザの分類に役立ち、ユーザ グループに対して許可ポリシー規則を作成する場合も役立ちます。

ISE に新しいユーザ グループを作成するには、次の手順に従います。

ステップ 1　[ISE] > [Administration] > [Groups] を選択します。

ステップ 2　左側のサイドバーのメニューから [User Identity Groups] を選択します。

右側のペインに [User Identity Groups] ページが表示されます。

ステップ 3　[Add] をクリックします。

[Identity Group details] ページが表示されます。

ステップ 4　グループの名前と説明を入力します。

たとえば、ユーザ グループ *Prime Infrastructure-SystemMonitoring-Group* を作成します。

ステップ 5　[Save] をクリックします。

ISE で新しいユーザを作成してユーザ グループに追加する

ISE で新しいユーザを作成し、そのユーザをユーザ グループにマップできます。

ISE で新しいユーザを作成し、そのユーザをユーザ グループにマップするには、次の手順に従います。

ステップ 1　[ISE] > [Administration] > [Identity Management] > [Identities] を選択します。

ステップ 2　左側のサイドバーのメニューから [Identities] > [Users] の順に選択します。

右側のペインに [Network Access Users] ページが表示されます。

ステップ 3　[Add] をクリックします。

[Network Access User] ページが表示されます。

ステップ 4　ユーザのユーザ名とパスワードを入力し、パスワードを再度入力します。

たとえば、ユーザ *ncs-sysmon* を作成します。

ステップ 5　必要なユーザ グループを [User Group] ドロップダウン リストから選択して [Save] をクリックします。

新しいユーザが、必要なユーザ グループに追加されます。

（注）　Active Directory、LDAP などの外部ソースと ISE を統合することもできます。

ISE での新しい許可プロファイルの作成

ISE で許可プロファイルを作成できます。新しい許可プロファイルを作成するには、次の手順を実行します。

ステップ 1　[ISE] > [Policy] > [Policy Elements] > [Results] を選択します。

ステップ 2　左側のサイドバーのメニューから [Authorization] > [Authorization Profiles] の順に選択します。

右側のペインに [Standard Authorization Profiles] ページが表示されます。

ステップ 3　[Add] をクリックします。

詳細ページが表示されます。

ステップ 4　プロファイルの名前および説明を入力します。

たとえば、*Prime Infrastructure-SystemMonitor* という名前の許可プロファイルを作成します。

ステップ 5　[Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

ステップ 6　[Advanced Attribute Settings] グループ ボックスで、Prime Infrastructure ユーザ グループの RADIUS カスタム属性を次々に追加し、仮想ドメイン属性を末尾に付けます。

（注）　Prime Infrastructure で、ユーザ グループの RADIUS カスタム属性は、[Administration] > [AAA] > [User Groups] に配置されています。適切な権限のあるグループについて [Task List] をクリックします。

a. cisco - av - pair を選択し、Prime Infrastructure ユーザ グループの RADIUS カスタム属性をこのペアの横に貼り付けます。続けて追加します。

b. 各グループの最後の RADIUS カスタム属性の末尾に仮想ドメイン属性を追加します（RADIUS カスタム属性については、仮想ドメインの RADIUS 属性および TACACS+ 属性を参照してください）。

ステップ 7　許可プロファイルを保存します。

ISE での許可ポリシー規則の作成

許可ポリシー規則を作成するには、次の手順に従ってください。

ステップ 1　[ISE] > [Policy] > [Authorization] を選択します。

ステップ 2　[Authorization Policy] ページで、[Actions] ドロップダウン リストから [Insert New Rule Above] を選択します。

Prime Infrastructure ユーザのログインなどに使用する規則を作成します。

ステップ 3　[Rule Name] テキスト ボックスに規則の名前を入力します。

ステップ 4　[Identity Groups] ドロップダウン リストから必要な ID グループを選択します。

たとえば、[Prime Infrastructure-SystemMonitoring-Group] を選択します。

アイデンティティ ユーザ グループの作成の詳細については、「ISE での新しいユーザ グループの作成」（P.15-902）を参照してください。

ステップ 5　[Permissions] ドロップダウン リストから権限を選択します。権限は許可プロファイルです。

たとえば、[Prime Infrastructure-SystemMonitor authorization profile] を選択します。

許可プロファイルの作成の詳細については、「ISE での新しい許可プロファイルの作成」（P.15-903）を参照してください。

この例では、Prime Infrastructure System Monitoring Identity グループに属しているすべてのユーザに、システム モニタリング カスタム属性を定義した適切な許可ポリシーが適用されるように規則を定義しています。

ステップ 6　[Save] をクリックして許可規則を保存します。

（注）　[ISE] > [Monitor] > [Authentications] オプションを使用して、認証の成功および失敗をモニタすることもできます。

Prime Infrastructure での AAA の設定

Prime Infrastructure で AAA を設定するには、次の手順に従います。

ステップ 1　Prime Infrastructure に *root* としてログインします。

ステップ 2　[Prime Infrastructure] > [Administration] > [AAA] > [RADIUS Servers] の順に選択します。

ステップ 3　ISE の IP アドレスを使用して新しい RADIUS サーバを追加します。

たとえば、`209.165.200.230` と入力します。

ステップ 4　変更を保存するには、[Save] をクリックします。

ステップ 5　[ISE] > [Administration] > [AAA] > [AAA Mode Settings] を選択します。

[AAA Mode Settings] ページが表示されます。

ステップ 6　AAA モードとして [RADIUS] を選択します。

ステップ 7　[Save] をクリックします。

Prime Infrastructure 内で AAA モードに RADIUS が設定されます。

ステップ 8　Prime Infrastructure からログアウトします。

ステップ 9　ISE で定義されている AAA ユーザとして Prime Infrastructure に再ログインします。

たとえば、ユーザ *ncs-sysmon* としてログインします。

ISE でのユーザ作成の詳細については、「ISE で新しいユーザを作成してユーザ グループに追加する」（P.15-902）を参照してください。

ACS 4.x の設定

ここでは、Prime Infrastructure と連携するように ACS 4.x を設定するための手順を示します。

タスクを Cisco Secure ACS サーバへインポートするには、Prime Infrastructure を ACS サーバ（またはシスコ以外の ACS サーバ）に追加する必要があります。ここでは、次の内容について説明します。

TACACS+ サーバでの使用のために ACS サーバに Prime Infrastructure を追加

TACACS+ サーバに Prime Infrastructure を追加するには、次の手順に従います。

（注）　この項で示す手順と図は ACS バージョン 4.1 に関するものであり、バージョンやベンダーのタイプによって若干異なる場合があります。CiscoSecure ACS のマニュアルか、使用しているベンダー用のマニュアルを参照してください。

ステップ 1　ACS サーバの [Network Configuration] ページで [Add Entry] をクリックします。

ステップ 2　[AAA Client Hostname] テキスト ボックスに Prime Infrastructure のホスト名を入力します。

ステップ 3　[AAA Client IP Address] テキスト ボックスに Prime Infrastructure の IP アドレスを入力します。

ACS 用のインターフェイスが Prime Infrastructure で指定してあるインターフェイスと同じであり、到達可能であることを確認します。

ステップ 4　[Shared Secret] テキスト ボックスに、Prime Infrastructure サーバと ACS サーバの両方で設定する共有秘密を入力します。

ステップ 5　[Authenticate Using] ドロップダウン リストの [TACACS+] を選択します。

ステップ 6　[Submit + Apply] をクリックします。

ステップ 7　左側のサイドバーのメニューから [Interface Configuration] を選択します。

ステップ 8　[Interface Configuration] ページで [TACACS+ (Cisco IOS)] リンクをクリックします。

[TACACS+ (Cisco IOS) Interface Configuration] ページが表示されます。

ステップ 9　ページの [New Services] 部分の [Service] 列見出しに **NCS** を追加します。

ステップ 10　[Protocol] 列見出しに **HTTP** と入力します。

（注）　HTTP は大文字で入力してください。

ステップ 11　これらの項目の前にあるチェックボックスをオンにして、新しいサービスとプロトコルを有効にします。

ステップ 12　[Submit] をクリックします。

TACACS+ 用 ACS への Prime Infrastructure ユーザ グループの追加

TACACS+ サーバでの使用のために ACS サーバに Prime Infrastructure ユーザ グループを追加するには、次の手順に従います。

ステップ 1　Prime Infrastructure にログインします。

ステップ 2　[Administration] > [AAA] > [User Groups] を選択します。[User Groups] ページが表示されます。

ステップ 3　ACS に追加するユーザ グループの [Task List] リンクをクリックします。[Export Task List] ページが表示されます。

ステップ 4　[TACACS+ Custom Attributes] 内のテキストを強調表示し、ブラウザのメニューから [Edit] > [Copy] の順に選択します。

ステップ 5　ACS にログインします。

ステップ 6　[Group Setup] に移動します。[Group Setup] ページが表示されます。

ステップ 7　使用するグループを選択して [Edit Settings] をクリックします。[NCS HTTP] が TACACS+ 設定に表示されます。

ステップ 8　ブラウザの [Edit] > [Paste] を使用して、Prime Infrastructure からこのテキスト ボックスに TACACS+ カスタム属性を貼り付けます。

（注）　Prime Infrastructure をアップグレードする場合は、TACACS+ サーバまたは RADIUS サーバのすべての権限を再追加する必要があります。

ステップ 9　チェックボックスをオンにして、これらの属性を有効にします。

ステップ 10　[Submit + Restart] をクリックします。

これで ACS ユーザとこの ACS グループを結び付けられます。

（注）　Prime Infrastructure で TACACS+ を有効にする方法については、「TACACS+ サーバの設定」（P.15-897）を参照してください。ACS View サーバのクレデンシャルの設定については、「ACS View Server クレデンシャルの設定」（P.9-556）を参照してください。TACACS+ 用 ACS への Prime Infrastructure 仮想ドメインの追加については、「仮想ドメインの RADIUS 属性および TACACS+ 属性」（P.15-849）を参照してください。

（注）　Prime Infrastructure Release 1.0 以降では、ACS にタスク リストをエクスポートする際に、ACS に仮想ドメインを追加する必要があります。これには、デフォルトの ROOT-DOMAIN 仮想ドメインを使用できます。仮想ドメインの詳細については、「仮想ドメインの設定」（P.15-842）を参照してください。

RADIUS での使用のために ACS サーバに Prime Infrastructure を追加

RADIUS サーバでの使用のために ACS サーバに Prime Infrastructure を追加するには、次の手順に従います。シスコ以外の ACS サーバを使用する場合は、「RADIUS での使用のために Cisco ACS サーバ以外のサーバに Prime Infrastructure を追加」（P.15-908）を参照してください。

ステップ 1　ACS サーバで [Network Configuration] に移動します。

ステップ 2　[Add Entry] をクリックします。

ステップ 3　[AAA Client Hostname] テキスト ボックスに Prime Infrastructure のホスト名を入力します。

ステップ 4　[AAA Client IP Address] テキスト ボックスに Prime Infrastructure の IP アドレスを入力します。

（注）　ACS 用のインターフェイスが Prime Infrastructure で指定したインターフェイスと同じであり、到達可能であることを確認します。

ステップ 5　[Shared Secret] テキスト ボックスに、Prime Infrastructure サーバと ACS サーバの両方で設定する共有秘密を入力します。

ステップ 6　[Authenticate Using] ドロップダウン リストから [RADIUS (Cisco IOS/PIX 6.0)] を選択します。

ステップ 7　[Submit + Apply] をクリックします。

これで ACS ユーザとこの ACS グループを結び付けられます。

（注）　Prime Infrastructure で RADIUS を有効にする方法については、「RADIUS サーバの設定」（P.15-899）を参照してください。ACS View サーバのクレデンシャルの設定については、「ACS View Server クレデンシャルの設定」（P.9-556）を参照してください。

（注）　Prime Infrastructure Release 1.0 以降では、ACS にタスク リストをエクスポートする際に、ACS に仮想ドメインを追加する必要があります。これには、デフォルトの ROOT-DOMAIN 仮想ドメインを使用できます。仮想ドメインの詳細については、「仮想ドメインの設定」（P.15-842）を参照してください。

RADIUS 用 ACS への Prime Infrastructure ユーザ グループの追加

RADIUS サーバでの使用のために ACS サーバに Prime Infrastructure ユーザ グループを追加するには、次の手順に従います。

ステップ 1　Prime Infrastructure にログインします。

ステップ 2　[Administration] > [AAA] > [User Groups] を選択します。[All Groups] ページが表示されます。

ステップ 3　ACS に追加するユーザ グループの [Task List] リンクをクリックします。[Export Task List] ページが表示されます。

ステップ 4　[RADIUS Custom Attributes] 内のテキストを強調表示し、ブラウザのメニューから [Edit] > [Copy] の順に選択します。

（注）　Prime Infrastructure をアップグレードする場合は、TACACS+ サーバまたは RADIUS サーバのすべての権限を再追加する必要があります。

ステップ 5　ACS にログインします。

ステップ 6　[Group Setup] に移動します。[Group Setup] ページが表示されます。

ステップ 7　使用するグループを選択して [Edit Settings] をクリックします。Cisco IOS/PIX 6.x RADIUS Attributes 以下にある [009\001]cisco-av-pair を見つけます。

ステップ 8　ブラウザの [Edit] > [Paste] を使用して、Prime Infrastructure からこのテキスト ボックスに RADIUS カスタム属性を貼り付けます。

（注）　Prime Infrastructure をアップグレードする場合は、TACACS+ サーバまたは RADIUS サーバのすべての権限を再追加する必要があります。

ステップ 9　チェックボックスをオンにして、これらの属性を有効にします。

ステップ 10　[Submit + Restart] をクリックします。

これで ACS ユーザとこの ACS グループを結び付けられます。

（注）　Prime Infrastructure で RADIUS を有効にする方法については、「RADIUS サーバの設定」（P.15-899）を参照してください。ACS View サーバのクレデンシャルの設定については、「ACS View Server クレデンシャルの設定」（P.9-556）を参照してください。TACACS+ 用 ACS への Prime Infrastructure 仮想ドメインの追加については、「仮想ドメインの RADIUS 属性および TACACS+ 属性」（P.15-849）を参照してください。

（注）　Prime Infrastructure Release 1.0 以降では、ACS にタスク リストをエクスポートする際に、ACS に仮想ドメインを追加する必要があります。これには、デフォルトの ROOT-DOMAIN 仮想ドメインを使用できます。仮想ドメインの詳細については、「仮想ドメインの設定」（P.15-842）を参照してください。

RADIUS での使用のために Cisco ACS サーバ以外のサーバに Prime Infrastructure を追加

RADIUS サーバを使用して Prime Infrastructure にログインすると、ユーザ名とパスワードが検証された後、アクセス許可（Access=Accept）メッセージとともにユーザ グループと実行可能タスクのリストが AAA サーバから返送されます。ユーザ グループによっては多数のタスクが割り当てられているので、このアクセス許可（Access=Accept）メッセージは断片化されたパケットとして送られてきます。

各ユーザ グループに割り当てられているタスクは、C:\Program Files\Prime Infrastructure\webnms\webacs\WEB-INF\security\usergroup-map.xml ファイルで確認できます。これらのタスクはベンダー固有属性（VSA）として返送されるため、Prime Infrastructure では VSA を使用した許可情報（IETF RADIUS 属性番号 26）が必要となります。VSA には Prime Infrastructure RADIUS タスク リスト情報が含まれます。

VSA の内容は、次のとおりです。

- Type = 26（IETF VSA 番号）
- Vendor Id = 9（シスコ ベンダー ID）
- Vendor Type = 1（カスタム属性）
- Vendor Data = Prime Infrastructure タスク情報（Prime Infrastructure の例：task0 = ユーザとグループ）

Prime Infrastructure RADIUS タスク リストの各行はそれぞれの RADIUS VSA で送信する必要があります。

Admin ユーザ グループがログインしたときは、アクセス許可（Access=Accept）パケットのデータ部で出力が切り捨てられ、1 つのロールしか示されない場合があります。ロールに関連付けられているタスクは task0 から始まり、task1、task2... と続きます。表 15-8 は、「Access=Accept」パケットの各属性が何を意味しているかを示しています。

```
0000 06 6d 0e 59 07 3d 6a 24 02 47 07 35 d2 12 a4 eb .m.Y.=j$G.5...
0010 a2 5a fa 84 38 20 e4 e2 3a 3a bc e5 1a 20 00 00 .Z..8..::.. 
0020 00 09 01 1a 57 69 72 65 6c 65 73 73 2d 57 43 53 ....Prime Infrastructure
0030 3a 72 6f 6c 65 30 3d 41 64 6d 69 6e 1a 2b 00 00 :role0=Admin.+...
0040 00 09 01 25 57 69 72 65 6c 65 73 73 2d 57 43 53 ...%Prime Infrastructure
0050 3a 74 61 73 6b 30 3d 55 73 65 72 73 20 61 6e 64 :task0=Users and
0060 20 47 72 6f 75 70 73 1a 27 00 00 00 09 01 21 57 Groups.”....!W
0070 69 72 65 6c 65 73 73 2d 57 43 53 3a 74 61 73 6b Prime Infrastructure:task
0080 31 3d 41 75 64 69 74 20 54 72 61 69 6c 73 xx xx 1=Audit Trails.*
```

表 15-8　Access=Accept パケットの例

属性	説明
1a（10 進数の 26）	ベンダー属性
2b（10 進数の 43 バイト）	スキップして次の TLV へ到達する合計バイト数（task0 ではユーザとグループ）
4 バイト フィールド	ベンダー Cisco 09
01	Cisco AV ペア（Prime Infrastructure が読み取る TLV）
25（10 進数の 37 バイト）	長さ
HEX テキスト文字列	Prime Infrastructure:task0 = ユーザとグループ
	データ部が完全に処理される次の TLV。
255.255.255.255	TLV: RADIUS type 8（IP アドレス）
Type 35（0x19）	クラス（文字列）
Type 80（0x50）	メッセージ認証コード

トラブルシューティングを行う手順は、次のとおりです。

- RADIUS パケットが Access-Accept（アクセス許可）であるかどうかを確認します。
- Access-Accept パケットで、ユーザ グループのタスク名を確認します。

- RADIUS パケットのさまざまな長さのフィールドを確認します。

ACS 5.x の設定

ここでは、Prime Infrastructure と連携するように ACS 5.x を設定するための手順を示します。

ここでは、次の内容について説明します。

ネットワーク デバイスおよび AAA クライアントの作成

ネットワーク デバイスおよび AAA クライアントを作成するには、次の手順に従ってください。

ステップ 1　[Network Resources] > [Network Devices and AAA Clients] を選択します。

ステップ 2　IP アドレスを入力します。

グループの追加

グループを追加する手順は次のとおりです。

ステップ 1　[Users and Identity Stores] > [Identity Groups] を選択します。

ステップ 2　グループを作成します。

ユーザの追加

ユーザを追加する手順は次のとおりです。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Users] を選択します。

ステップ 2　ユーザを追加してから、このユーザにグループをマップします。

ポリシー要素または許可プロファイルの作成

ここでは、次の内容について説明します。

- 「TACACS 用ポリシー要素または許可プロファイルの作成」（P.15-911）

RADIUS 用ポリシー要素または許可プロファイルの作成

RADIUS 用ポリシー要素または許可プロファイルを作成するには、以下の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] を選択します。

ステップ 2　[Create] をクリックします。

ステップ 3　名前と説明を入力します。

ステップ 4　[RADIUS Attributes] タブをクリックします。

ステップ 5　RADIUS 属性を 1 つずつ追加します。

ステップ 6　[Submit] をクリックします。

TACACS 用ポリシー要素または許可プロファイルの作成

TACACS 用ポリシー要素または許可プロファイルを作成するには、以下の手順を実行します。

ステップ 1　[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] を選択します。

ステップ 2　[Create] をクリックします。

ステップ 3　名前と説明を入力します。

ステップ 4　[Custom Attributes] タブをクリックします。

ステップ 5　TACACS 属性を 1 つずつ追加します。

ステップ 6　[Submit] をクリックします。

（注）　サブメニューが Prime Infrastructure で表示されるようにするために、関連するメニュー アクセス タスクを追加する必要があります。たとえば、[Administration] メニューの下位のサブメニューを追加する場合、Prime Infrastructure で [Administration] メニューの下位のサブメニューを表示できるようにするために、最初に [Administration] メニュー アクセス タスクを追加する必要があります。

許可規則の作成

ここでは、RADIUS および TACACS 用に許可を設定する方法を説明します。

ここでは、次の内容について説明します。

- 「RADIUS 用のサービス セレクション規則の作成」（P.15-911）
- 「TACACS 用のサービス セレクション規則の作成」（P.15-912）

RADIUS 用のサービス セレクション規則の作成

RADIUS 用のサービス セレクション規則を作成するには、次のステップを実行します。

ステップ 1　[Access Policies] > [Access Services] > [Service Selection Rules] を選択します。

ステップ 2　[Create] をクリックします。

ステップ 3　プロトコルとして RADIUS を選択し、[Default Network Access] を選択します。

ステップ 4　[OK] をクリックします。

TACACS 用のサービス セレクション規則の作成

TACACS 用のサービス セレクション規則を作成するには、次の手順に従ってください。

ステップ 1　[Access Policies] > [Access Services] > [Service Selection Rules] を選択します。

ステップ 2　[Create] をクリックします。

ステップ 3　プロトコルとして TACACS を選択し、[Default Device Admin] を選択します。

ステップ 4　[OK] をクリックします。

アクセス サービスの設定

ここでは、RADIUS および TACACS 用にアクセス サービスを設定する方法を説明します。

ここでは、次の内容について説明します。

- 「RADIUS 用アクセス サービスの設定」（P.15-912）
- 「TACACS 用アクセス サービスの設定」（P.15-913）

RADIUS 用アクセス サービスの設定

RADIUS 用アクセス サービスを設定するには、次の手順を実行します。

ステップ 1　ACS 5.x サーバにログインし、[Access Policies] > [Access Services] > [Default Network Access] を選択します。

ステップ 2　[General] タブで、使用するポリシー構造を選択します。デフォルトでは、3 個の全ポリシー構造が選択されています。

ステップ 3　[Allowed Protocols] から使用するプロトコルを選択します。

（注）　アイデンティティおよびグループのマッピングのためにデフォルトを保持できます。

ステップ 4　RADIUS 用の許可規則を作成するには、[Access Policies] > [Access Services] > [Default Network Access] > [Authorization] の順に選択します。

ステップ 5　[Create] をクリックします。

ステップ 6　[Location] で、[All Locations] を選択します。または、ロケーションに基づいて規則を作成することもできます。

ステップ 7　[Group] で、前に作成したグループを選択します。

ステップ 8　[Device Type] で、[All Device Types] を選択します。または、デバイス タイプに基づいて規則を作成することもできます。

ステップ 9　[Authorization Profile] で、RADIUS 用に作成した許可プロファイルを選択します。

ステップ 10　[OK] をクリックします。

ステップ 11　[Save] をクリックします。

TACACS 用アクセス サービスの設定

TACACS 用アクセス サービスを設定するには、次の手順に従ってください。

ステップ 1　[Access Policies] > [Access Services] > [Default Device Admin] を選択します。

ステップ 2　[General] タブで、使用するポリシー構造を選択します。デフォルトでは、3 個すべてが選択されています。同様に、[Allowed Protocols] から使用するプロトコルを選択します。

（注）　アイデンティティおよびグループのマッピングのためにデフォルトを保持できます。

ステップ 3　TACACS 用の許可を作成するには、[Access Policies] > [Access Services] > [Default Device Admin] > [Authorization] を選択します。

ステップ 4　[Create] をクリックします。

ステップ 5　[Location] で、[All Locations] を選択します。または、ロケーションに基づいて規則を作成することもできます。

ステップ 6　[Group] で、前に作成したグループを選択します。

ステップ 7　[Device Type] で、[All Device Types] を選択します。または、デバイス タイプに基づいて規則を作成することもできます。

ステップ 8　[Shell Profile] で、TACACS 用に作成したシェル プロファイルを選択します。

ステップ 9　[OK] をクリックします。

ステップ 10　[Save] をクリックします。

ロギング オプションの設定

[Administration] > [Logging] の順に選択して、[Administer Logging Options] ページにアクセスします。コントローラの syslog 情報のロギングは、[Controller] > [Management] > [Syslog] ページで実行できます。ここでは、使用できるログ設定について説明します。内容は次のとおりです。

- 「一般的なロギング オプション」（P.15-914）
- 「SNMP ロギング オプション」（P.15-915）
- 「Syslog オプション」（P.15-916）

一般的なロギング オプション

電子メール ロギングを有効にするには、次の手順を実行します。設定内容が保存され、電子メール サーバで使用されます。

ステップ 1　[Administration] > [Logging] の順に選択します。[General Logging Options] ページが表示されます。

ステップ 2　左側のサイドバーのメニューから、[General Logging Options] を選択します。

ステップ 3　[Message level] ドロップダウン リストから [Trace]、[Information]、または [Error] を選択します。

ステップ 4　さまざまな管理モジュールを有効にするには、[Enable Log Module] グループ ボックス内のチェック ボックスをオンにします。

- [Message Level]：記録されるメッセージの最小レベルを選択します。[Error]、[Information]、または [Trace] が含まれます。
- [Enable Log Module]：以下の管理モジュールのロギングを有効化できます。
  - [Log Modules]：すべてのモジュールを選択する場合に、このチェックボックスをオンにします。
  - [SNMP]：Prime Infrastructure とコントローラの間の全 SNMP 通信のログをキャプチャします。
  - [AAA]：Prime Infrastructure の AAA 関連のログをキャプチャします。
  - [Admin]：管理ベースのログを含めます。このログには、管理コンソールを使用して実行されたすべての設定の変更が記録されます。
  - [Communication]：通信で使用されるプロトコルに関連するログを含みます。
  - [Config]：Prime Infrastructure から行うコントローラの設定をログに記録するために使用します。

    （注）　完全なコントローラ設定ログを取得するには、General ログ モジュールも有効にします。

    （注）　Prime Infrastructure がコントローラにログとして送信する設定値を取得するには、[Trace Display Values]（[Administration] > [Settings] > [SNMP Settings] > [Trace Display Value]）を有効にします。

  - [Database]：Prime Infrastructure で行う、データベース関連の重要な操作をデバッグするためのログを含みます。

    （注）　機能の中には、パフォーマンスを低下させないように、デバッグ中だけに使用を推奨するものがあります。たとえば、トレース モードおよび SNMP のメディエーションは大量のログ情報を生成するため、デバッグの際だけ有効にすることを推奨します。

  - [Faults]：イベントおよびアラート サブシステムによって使用されます。
  - [GUI]：UI 検証ログ全般を含みます。
  - [Inventory]：インベントリ関連のすべてログをキャプチャします。
  - [Monitor]：アラーム、Spectrum Intelligence、CCXV5、クライアントとタグ、クライアント無線測定、SSO、およびメッシュに使用します。

- [MSE] : MSE の追加または削除や、MSE 上のパラメータの変更など、MSE 関連の操作に使用します。NW 設計、コントローラなどの MSE 同期のロギングも有効になります。
- [Reports] : レポートの作成、保存、スケジューリング、および実行に関連するメッセージの記録に使用します。このモジュールは、スケジュールおよび保存されたレポートのリストも含みます。
- [System] : システム関連のすべてのログをキャプチャします。
- [Tools] : さまざまなプラグイン ツールに関連するログを含みます。
- [XMLMED] : MSE と Prime Infrastructure 間の通信のトレースを有効にする場合に使用します。

ステップ 5　[Log File Settings] 部分に以下の設定を入力します。これらの設定は、Prime Infrastructure の再起動後に有効になります。

- [Max.file size] : ログ ファイルごとに許可される最大 MB 数です。
- [Number of files] : 許可されるログ ファイルの最大数。
- [File prefix] : ログ ファイル プレフィックス。文字列「%g」を含めると、ファイルに連番を付けることができます。

ステップ 6　ローカル マシンにログ ファイルをダウンロードするには、[Download] をクリックします。

（注）　logs.zip のファイル名には、プレフィックスとしてホスト名と日時が付いているため、保管されたログ ファイルを簡単に識別できます。この .zip ファイルには、ログ ファイルについて記述した HTML ファイルが含まれます。

ステップ 7　ログ ファイルを送信する 1 つ以上の電子メール ID（複数の場合はカンマで区切る）を入力します。

（注）　ログ ファイルをメールで送信するには、電子メール サーバを設定しておく必要があります。

ステップ 8　[Submit] をクリックします。

SNMP ロギング オプション

SNMP の追跡を有効にする手順は、次のとおりです。設定内容が保存され、SNMP サーバで使用されます。

（注）　SNMP サーバは、SNMP ロギングのためにこれらの設定を使用する Prime Infrastructure サーバです。

（注）　WCS Release 7.x から Prime Infrastructure Release 1.1 にアップグレードする場合、[Administration] > [Logging Options] > [SNMP Logging Options] の下位の設定は保持されません。

ステップ 1　[Administration] > [Logging] の順に選択します。[Logging Options] ページが表示されます。

ステップ 2　左側のサイドバーのメニューから、[SNMP Logging Options] を選択します。

ステップ 3　コントローラと Prime Infrastructure 間での SNMP メッセージ（トラップも含む）の送信を有効にするために、[Enable SNMP Trace] チェックボックスをオンにします。

ステップ 4　SNMP メッセージ値を参照するために、[Display Values] チェックボックスをオンにします。

ステップ 5　SNMP トラップをトレースする 1 つ以上の IP アドレスを設定します。このテキスト ボックスには、最大 10 個の IP アドレスを追加できます。

ステップ 6　最大 SNMP ファイル サイズおよび SNMP ファイルの数を設定できます。

Syslog オプション

Syslog プロトコルは、単に、生成元のデバイスからコレクタにイベント メッセージを転送する目的で設計されています。システム情報およびアラート用の syslog メッセージがさまざまなデバイスによって生成されます。

（注）　WCS Release 7.x から Prime Infrastructure Release 1.1 にアップグレードする場合、[Administration] > [Logging Options] > [SysLog Logging Options] の下位の設定は保持されません。

Prime Infrastructure で Syslog を設定するには、次の手順に従います。

ステップ 1　[Administration] > [Logging] の順に選択します。[Logging Options] ページが表示されます。

ステップ 2　左側のサイドバーのメニューから、[Syslog Options] を選択します。

ステップ 3　システム ログの収集および処理を有効にするために、[Enable Syslog] チェックボックスをオンにします。

ステップ 4　メッセージの送信元であるインターフェイスの Syslog サーバ IP アドレスを設定します。

ステップ 5　[Syslog Facility] を選択します。syslog メッセージの送信用に、8 個のローカル用途のファシリティから任意に選択できます。このローカル用途のファシリティは予約されておらず、一般的な用途で使用可能です。

ロギング オプションを使用したトラブルシューティングの強化

ロギング ページでは、問題をデバッグするために Prime Infrastructure で収集するデータの量をカスタマイズできます。問題を簡単に再現できるよう、TAC への連絡に先立って次の手順を実行してください。以下の手順によって、トラブルシューティングのセッションが円滑になる可能性があります。

ステップ 1　[Administration] > [Logging] の順に選択します。

ステップ 2　[Message Level] ドロップダウン リストから [Trace] を選択します。

ステップ 3　各チェックボックスをオンにして、すべてのログ モジュールを有効にします。

ステップ 4　現在の問題を再現させます。

ステップ 5　[Logging Options] ページに戻ります。

ステップ 6　[Download Log File] セクションの [Download] をクリックします。

（注）　logs.zip のファイル名には、プレフィックスとしてホスト名と日時が付いているため、保管されたログ ファイルを簡単に識別できます。この .zip ファイルには、ログ ファイルについて記述した HTML ファイルが含まれます。

ステップ 7　ログを取得したら、[Message Level] ドロップダウン リストから [Information] を選択します。

（注）　[Message Level] を [*Trace*] のままにすると、長期間のうちにパフォーマンスに悪影響を与えるおそれがあります。

ハイ アベイラビリティの設定

障害時の運用の継続性を確保するために、Prime Infrastructure ではハイ アベイラビリティ フレームワーク（フェールオーバー フレームワーク）を使用できるようになりました。アクティブ（プライマリ）Prime Infrastructure で障害が発生した場合、セカンダリ Prime Infrastructure が障害が発生したプライマリ Prime Infrastructure の処理を引き継ぎ、サービスを引き続き提供します。フェールオーバーでは、障害が発生したプライマリ Prime Infrastructure のピアが、ローカル データベースとファイルを使用してセカンダリ Prime Infrastructure でアクティブ化され、セカンダリ Prime Infrastructure はフル機能の Prime Infrastructure を実行します。セカンダリ ホストがフェールオーバー モードの間、他のプライマリ Prime Infrastructure のデータベースおよびファイルのバックアップは、中断なしで続行されます。

HA 設定で電子メール アドレスを指定する場合、障害についての通知を受け取るには、メール サーバを設定して到達可能にする必要があります。

ハイ アベイラビリティの詳細については、以下の項を参照してください。

- 「ハイ アベイラビリティのガイドラインと制約事項」（P.15-918）
- 「フェールオーバー シナリオ」（P.15-919）
- 「フェールバック シナリオ」（P.15-919）
- 「バックグラウンド タスクの実行」（P.15-797）
- 「ハイ アベイラビリティのステータス」（P.15-920）
- 「プライマリ Prime Infrastructure でのハイ アベイラビリティの設定」（P.15-921）
- 「ハイ アベイラビリティの導入」（P.15-922）

ここでは、次の内容について説明します。

- 「ハイ アベイラビリティのガイドラインと制約事項」（P.15-918）
- 「フェールオーバー シナリオ」（P.15-919）
- 「フェールバック シナリオ」（P.15-919）
- 「ハイ アベイラビリティのステータス」（P.15-920）
- 「プライマリ Prime Infrastructure でのハイ アベイラビリティの設定」（P.15-921）
- 「ハイ アベイラビリティの導入」（P.15-922）
- 「新しいプライマリ Prime Infrastructure の追加」（P.15-923）
- 「プライマリ Prime Infrastructure の削除」（P.15-924）

ハイ アベイラビリティのガイドラインと制約事項

フェールオーバーを開始する前に、以下の前提条件および制限事項を検討する必要があります。

- Prime Infrastructure のスタンバイ インスタンスを実行する、プライマリ Prime Infrastructure と同一の追加のハードウェアを用意する必要があります。
- Prime Infrastructure は、物理と仮想の両方のアプライアンス導入モデル上でハイ アベイラビリティをサポートします。
- プライマリ Prime Infrastructure とバックアップ Prime Infrastructure の間には、信頼性の高い高速有線ネットワークが必要です。
- プライマリとセカンダリの Prime Infrastructure では、同じ Prime Infrastructure ソフトウェア リリースを実行する必要があります。
- プライマリ Prime Infrastructure でセカンダリ Prime Infrastructure とのハイ アベイラビリティを開始するには、セカンダリ Prime Infrastructure サービスのステータスが実行中であり、プライマリ Prime Infrastructure から到達可能である必要があります。したがって、最初にセカンダリ Prime Infrastructure をブートし、次にプライマリ Prime Infrastructure をブートして、ハイ アベイラビリティ登録を開始する必要があります。
- フェールオーバーは、一時的なものであると見なす必要があります。障害が発生したプライマリ Prime Infrastructure をできるだけ早く復旧して、フェールバックを再開する必要があります。障害が発生したプライマリ Prime Infrastructure の復旧に時間がかかるほど、セカンダリ Prime Infrastructure を共有する他の Prime Infrastructure をフェールオーバー サポートなしで稼働させる時間が長くなります。
- 最新のコントローラ ソフトウェアを使用する必要があります。
- プライマリとセカンダリのホストのサブネットは、同じでなくてもかまいません。これらのホストは地理的に分離できます。
- なんらかの原因でセカンダリ ホストが故障するとすべてのプライマリ インスタンスが影響を受けて、フェールオーバー サポートのないスタンドアロン モードで稼働します。
- プライマリとセカンダリの Prime Infrastructure が通信するポートを開く（ネットワーク ファイアウォール、アプリケーション ファイアウェイ、ゲートウェイなどでブロックしない）必要があります。tomcat ポートはインストール時に設定可能で、デフォルト ポートは 8082 です。1315 ～ 1319 までの固定データベース ポートを予約する必要があります。
- プライマリとセカンダリの Prime Infrastructure の間に適用するすべてのアクセス コントロール リストで、プライマリとセカンダリの Prime Infrastructure 間のトラフィックの通過を許可する必要があります。
- プライマリ Prime Infrastructure には十分な数のデバイス ライセンスが必要です。フェールオーバーが発生すると、セカンダリ Prime Infrastructure はプライマリ Prime Infrastructure のデバイス ライセンスを使用します。

ハイ アベイラビリティのための Prime Infrastructure 1.x の更新

- Prime Infrastructure Release 1.x では、セカンダリ Prime Infrastructure は 1 つのプライマリ Prime Infrastructure のみサポートできます。
- ハイ アベイラビリティを初めて有効にするときは、サーバの同期に多くの時間がかかります。この時間は、データベースのサイズによっては、30 分以上になります。

フェールオーバー シナリオ

フェールオーバーは、プライマリ Prime Infrastructure で障害が発生した場合に、セカンダリ Prime Infrastructure をアクティブにするプロセスです。フェールオーバーは、ハイ アベイラビリティ設定時に設定されたフェールオーバー タイプに基づき、手動で開始すること、または自動的に開始させることができます。ハイ アベイラビリティが手動モードに設定されている場合、障害を通知するために、登録されている電子メール アドレスに電子メールが送信されます。この電子メールには、障害のステータス、および [secondary Prime Infrastructure Health Monitor] ページへのリンクが含まれます。リンクを使用して、ヘルス モニタ UI を起動し、フェールオーバーを開始できます。

ハイ アベイラビリティが自動モードに設定されている場合、次のイベントが発生します。

（注）　1 台の物理セカンダリ Prime Infrastructure で、複数台のプライマリ デバイスをフェールオーバーできます。

1. セカンダリ Prime Infrastructure 上のヘルス モニタによってプライマリ Prime Infrastructure が機能していないことが確認されます（ハードウェアのクラッシュ、ネットワークのクラッシュなど）。
2. セカンダリ Prime Infrastructure インスタンスが即座に開始され（すでに配置されている設定を使用）、プライマリの対応するデータベースが使用されます。フェールオーバーが成功した後、クライアントは新しくアクティブ化された Prime Infrastructure（セカンダリ Prime Infrastructure）にアクセスする必要があります。セカンダリ Prime Infrastructure は、すべてのコントローラを更新して、セカンダリ Prime Infrastructure のアドレスをトラップの宛先として設定します。

   （注）　セカンダリ Prime Infrastructure への Web トラフィックのリダイレクトは、自動的には行われません。任意のインフラストラクチャ ツールを使用して、このリダイレクションを適切に設定する必要があります。

3. フェールオーバー操作の結果はヘルス モニタの UI にイベントとして示されます。または、クリティカル アラームが管理者および他の Prime Infrastructure インスタンスに送信されます。

（注）　NMS サーバにメモリ不足エラーがある場合、フェールオーバーは、HA 設定に基づいて手動または自動で開始されます。

フェールバック シナリオ

フェールバックは、プライマリ Prime Infrastructure を再びアクティブにするプロセスです。フェールバックは手動でのみ開始できます。https://<piip>:8082 を使用して、セカンダリ Prime Infrastructure の HealthMonitor UI にアクセスします。HealthMonitor UI 内で、認証キーを使用してログインし、フェールバック プロセスを開始します。

フェールバックが開始されると、次のイベントが発生します。

1. データベース情報およびファイルがプライマリ Prime infrastructure にコピーされます。プライマリ サーバのモードが「Primary Active」に変更され、セカンダリ サーバのモードが「Secondary Syncing」に変更されます。
2. セカンダリ Prime Infrastructure の、ヘルス モニタを除くすべてのプロセスがダウンします。これに対し、プライマリ Prime Infrastructure のすべてのプロセスが開始されます。
3. セカンダリ Prime Infrastructure が長時間アクティブ状態の場合、フェールバック操作には、フェールオーバー操作または登録操作よりも長い時間がかかります。

4. フェールバック プロセス中にプライマリ Prime Infrastructure がダウンすると、セカンダリ Prime Infrastructure へのフェールオーバーが開始されます。その後、OVA が新規インストールされたプライマリ Prime Infrastructure でフェールバックが実行されます。セカンダリ Prime Infrastructure が新しいプライマリ Prime Infrastructure に登録され、フェールバックが開始されます。

ハイ アベイラビリティのステータス

ハイ アベイラビリティの詳細を表示するには、次の手順に従います。

ステップ 1　[Administration] > [High Availability] を選択します。

ステップ 2　左側のサイドバーのメニューから [HA Status] を選択します。次の情報が表示されます。

- 現在のステータス
- 各イベントの時刻、状態、および説明

表 15-9 に、ハイ アベイラビリティの各種ステータスの詳細を示します。

表 15-9　ハイ アベイラビリティのステータス

HA ステータス	説明
HA not Configured	HA がまだ設定されていません。
Primary Alone	プライマリ Prime Infrastructure は孤立しており、セカンダリ Prime Infrastructure と同期していません。
HA Initializing	HA を初期化中です。
Primary Active	プライマリ Prime Infrastructure はセカンダリ Prime Infrastructure と問題なく同期しています。
Primary Lost Secondary	プライマリ Prime Infrastructure はセカンダリ Prime Infrastructure との接続を失っています。
Primary Failback	プライマリ Prime Infrastructure へのフェールバックが実行されています。
Primary Uncertain	プライマリ Prime Infrastructure はセカンダリ Prime Infrastructure の状態を認識できません。
Secondary Alone	セカンダリ Prime Infrastructure は孤立しており、プライマリ Prime Infrastructure と同期していません。
Secondary Syncing	セカンダリ Prime Infrastructure はプライマリ Prime Infrastructure と問題なく同期しています。
Secondary Active	プライマリ Prime Infrastructure 上で HA に障害が発生し、アプリケーションはセカンダリ Prime Infrastructure で実行されており、アクティブです。
Secondary Lost Primary	セカンダリ Prime Infrastructure はプライマリ Prime Infrastructure との接続を失っています。
Secondary Failover	セカンダリ Prime Infrastructure へのフェールオーバーが実行されています。

表 15-9　ハイ アベイラビリティのステータス （続き）

HA ステータス	説明
Secondary Post Failback	フェールバックが次のステップです。
Secondary Uncertain	セカンダリ Prime Infrastructure はプライマリ Prime Infrastructure の状態を認識できません。

プライマリ Prime Infrastructure でのハイ アベイラビリティの設定

プライマリ Prime Infrastructure でハイ アベイラビリティを設定するには、次の手順に従います。インストール時に Prime Infrastructure のロール（プライマリまたはセカンダリ）を指定する必要があります。

（注）
- ハイ アベイラビリティを設定する前に、メール サーバを設定する必要があります。メール サーバの設定手順については、「メール サーバの設定」（P.15-863）を参照してください。
- [HA Configuration] ページで電子メール アドレスを指定する場合は、メール サーバが設定されており、到達可能であることを確認してください。

（注）データベース トランザクション ログがデータベース パーティション ディスク領域の 1/3 に達した場合は、データベースを「スタンドアロン」モードに設定して、トランザクション ログが拡張されないようにします。ただし、その場合は、データベースの同期が次回発生したときに、完全な *netcopy* が必要です。

ステップ 1　[Administration] > [High Availability] を選択します。

ステップ 2　左側のサイドバーのメニューから、[HA Configuration] を選択します。[High Availability Configuration] ページが表示されます。

ハイ アベイラビリティの現在のステータスはページの上部に表示されます。ハイ アベイラビリティの各種ステータスの詳細については、表 15-9 を参照してください。

ステップ 3　セカンダリ Prime Infrastructure の IP アドレスまたはホスト名を入力します。

ステップ 4　セカンダリ Prime Infrastructure をインストールするときに指定した認証キーを入力します。

ステップ 5　[Administration] > [Settings] > [E-mail Server] で設定したデフォルトの管理者電子メール アドレスが自動的に入力されます。必要なすべての変更を実行できます。これらの電子メール アドレスに対するすべての変更は、[Administration] > [Settings] > [Mail Server] ページの [Secondary SMTP Server] セクションにも入力する必要があります。

（注）障害が通知されるようにハイ アベイラビリティを設定する場合は、電子メール アドレスを入力します。Prime Infrastructure は、電子メール サーバ設定をテストします。（メール サーバに接続できないことが原因で）このテストが失敗した場合、Prime Infrastructure は障害を通知できません。この場合でも、ハイ アベイラビリティ登録を開始できます。

ステップ 6　[Failover Type] ドロップダウン リストから、手動または自動を選択します。手動を選択した場合は、セカンダリ HealthMonitor グラフィカル ユーザ インターフェイスのボタンか、プライマリ Prime Infrastructure で障害が発生したときに管理者に送信される電子メールに指定されている URL を使用し

て、フェールオーバー操作をトリガーできます。自動を選択した場合は、プライマリ Prime Infrastructure で障害を検出した時点で、セカンダリ Prime Infrastructure がフェールオーバーを開始します。

ステップ 7　設定を保持してハイ アベイラビリティを有効にする場合は [Save] をクリックします。ハイ アベイラビリティおよびハイ アベイラビリティの設定を無効にする場合は [Remove] をクリックします。

（注）　[Remove] ボタンは、ハイ アベイラビリティがすでに設定されている場合だけ使用可能です。

この時点で、データベースを使用してセカンダリに到達可能であり、ヘルス モニタ間でファイルが同期されています。または、セカンダリに到達不能であり、セカンダリ インストールが実行されていないために、エラーが返されます。

ハイ アベイラビリティが有効になると、Prime Infrastructure グラフィカル ユーザ インターフェイス（[Administration] > [High Availability]）から以下の機能を実行できます。

- [Update]：更新機能は、レポート リポジトリのパス（[Administration] > [Settings] > [Report]）または FTP/TFTP のルート ディレクトリ（[Administration] > [Settings] > [Server Settings]）を変更する場合およびファイルを適切に同期する場合に使用します。
- [Delete]：セカンダリ Prime Infrastructure からプライマリ Prime Infrastructure を解放するには、この削除操作を使用します。

ハイ アベイラビリティの導入

既存の Prime Infrastructure インストールにハイ アベイラビリティを導入するには、次の手順に従います。

ステップ 1　セカンダリ Prime Infrastructure を実行するハードウェアを決定し、準備します。

ステップ 2　プライマリとセカンダリの Prime Infrastructure 間のネットワーク接続が機能しており、必要なすべてのポートが開いていることを確認します。

ステップ 3　プライマリにインストールされている Prime Infrastructure と同じバージョンの Prime Infrastructure をセカンダリにインストールします。

ステップ 4　プライマリ Prime Infrastructure とセカンダリ Prime Infrastructure を新しいバージョンにアップグレードします。

ステップ 5　プライマリ Prime Infrastructure を（プライマリとして）起動します。ヘルス モニタを含むすべてのプロセスが開始されます。

ステップ 6　「プライマリ Prime Infrastructure でのハイ アベイラビリティの設定」（P.15-921）で説明されているハイ アベイラビリティ パラメータを設定します。

ステップ 7　プライマリ Prime Infrastructure でハイ アベイラビリティをアクティブにします。プライマリ Prime Infrastructure は最初にそのデータベースをセカンダリ Prime Infrastructure にコピーし、次にセカンダリに接続します。次のファイルがプライマリ Prime Infrastructure からセカンダリ Prime Infrastructure にコピーされます。

- DB パスワード ファイル
- すべての自動プロビジョニング スタートアップ コンフィギュレーション ファイル
- すべてのドメイン マップ
- スケジュールされたレポート タスクによって生成されるすべての履歴レポート

ハイ アベイラビリティの導入完了です。https://<piip>:8082 を使用して HealthMonitor UI にアクセスします。HealthMonitor UI 内で、認証キーを使用してログインします。

認証キーは、Prime Infrastructure で、コマンド プロンプトを使用して変更できます。認証キーを変更するには、Prime Infrastructure インストール ディレクトリにパスを変更してから「bin」に変更し、**hmadmin - authkey** *key* と入力します。

ヘルス モニタの現在のステータスを表示するには、**hmadmin [-options] status** コマンドを入力します。ヘルス モニタの設定を削除するには、**hmadmin.sh remove** コマンドを入力します。

新しいプライマリ Prime Infrastructure の追加

新しいプライマリ Prime Infrastructure を既存の設定に追加するには、次の手順に従います。この新しいプライマリ Prime Infrastructure は、既存のセカンダリ Prime Infrastructure をフェールオーバー サーバとして使用します。

ステップ 1　新しいプライマリとセカンダリの間のネットワーク接続が機能しており、すべてのポートが開いていることを確認します。

ステップ 2　他のプライマリ Prime Infrastructure およびセカンダリ Prime Infrastructure にロードされているリリースと同じ Prime Infrastructure Release を新しいプライマリ Prime Infrastructure にロードする必要があります。

ステップ 3　Prime Infrastructure の正しいバージョンをプライマリ Prime Infrastructure にインストールします。

ステップ 4　新しいプライマリ Prime Infrastructure を起動します。ヘルス モニタを含むすべてのプロセスが開始されます。

（注）　新しいプライマリ Prime Infrastructure の IP アドレスおよびその他の設定が、古いプライマリ Prime Infrastructure の設定と同じであることを確認します。

ステップ 5　セカンダリ Prime Infrastructure のヘルス モニタ Web UI を起動します（[Administration] > [High Availability] > [HA Status] > [Launch Health Monitor]）。

または

https://<piip>:8082 を使用して HealthMonitor UI にアクセスします。HealthMonitor UI 内で、認証キーを使用してログインします。

ステップ 6　セカンダリ Prime Infrastructure の [Health Monitor Details] ページで、[Failback] をクリックします。データベースおよびその他の設定ファイルがセカンダリ Prime Infrastructure から新しいプライマリ Prime Infrastructure にコピーされます。既存のセカンダリ Prime Infrastructure への新しいプライマリ Prime Infrastructure の登録が開始されます。

ステップ 7　プライマリ Prime Infrastructure がセカンダリ Prime Infrastructure に接続した後、プライマリのヘルス モニタがセカンダリのヘルス モニタに接続します。これらのヘルス モニタは相互に確認応答し、モニタリングを開始します。

これで、ハイ アベイラビリティの導入完了です。

プライマリ Prime Infrastructure の削除

プライマリ Prime Infrastructure インスタンスをグループから除去するときは、セカンダリ Prime Infrastructure のピア データベース インスタンスを無効にし、このプライマリのヘルス モニタを削除する必要があります。（ハイ アベイラビリティからプライマリ Prime Infrastructure を削除するには、[High Availability configuration] ページの [Remove] ボタンを使用します）。セカンダリ Prime Infrastructure は、そのデータベース インスタンスを無効にし、アンインストールされたプライマリ Prime Infrastructure をそのヘルス モニタから削除します。

ライセンスの管理

ここでは、次の内容について説明します。

License Center

License Center では、Prime Infrastructure、ワイヤレス LAN コントローラ、および MSE のライセンスを管理できます。License Center は、[Prime Infrastructure Administration] メニューから使用できます。[License Center] ページを表示するには、[Administration] > [License Center] の順に選択します。

（注） License Center から Prime Infrastructure および MSE のライセンスを管理する場合には制限はありませんが、WLC ライセンスは表示のみ可能です。WLC ライセンスを管理するには、WLC または CLM を使用する必要があります。

ヒント Prime Infrastructure License Center の詳細については、Cisco.com でマルチメディア プレゼンテーションを参照してください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります 今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

ここでは、次の内容について説明します。

Prime Infrastructure ライセンス情報

[License Center] ページの [Prime Infrastructure Licenses] 部分に以下が表示されます。

- [Feature]：ライセンスの種類。これは Prime Infrastructure または DEMO です。
- [Device Limit]：ライセンスを持つアクセス ポイントとスイッチの総数。
- [Device Count]：現在ライセンスを使用しているアクセス ポイントおよびスイッチの数。

（注）　AP カウントには、関連付けられているアクセス ポイントと関連付けられていないアクセス ポイントの両方が含まれます。AP 制限値に近づいた場合は、関連付けられていない任意のアクセス ポイントを削除して、使用可能なライセンス容量を増やすことができます。デモ ライセンスの場合は、[If you do not have a Product Authorization Key (PAK), please click here for available licenses] リンクをクリックし、[Wireless Control System Trial License] を選択できます。

（注）　Autonomous アクセス ポイントは、ライセンスの合計デバイス数に含まれません。

（注）　有効な資格情報のある新規追加デバイスに対して、ライセンスの数が不十分の場合、これらのデバイスの収集ステータスは非管理対象ステートに変更されます。ライセンスを追加し、これらのデバイスを同期しても、収集ステータスは非管理対象ステートのままです。これらのデバイスをインベントリから削除し、Prime Infrastructure に再追加する必要があります。この後、収集ステータスは管理対象ステートに変更されます。

- [% Used]：Prime Infrastructure 全体でのライセンスを持つアクセス ポイントとスイッチのパーセンテージ。このパーセンテージが 75 % を上回ると、値は赤で表示されます。このレベルになると、関連付けられているアクセス ポイントと関連付けられていないアクセス ポイントの両方が AP カウントに含まれていることを示すメッセージも表示されます。
- [Type]：すべてのライセンスが永久の場合は [Permanent] です。いずれかのライセンスが評価（またはデモ）の場合は、期限切れまでの日数が最少の評価ライセンス上の残日数が表示されます。

（注）　Prime Infrastructure 用の新しいライセンスを取得するには、[Product License Registration] リンクに移動します。

（https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet）

そして、製品認証キー（PAK）とホスト名を入力します。

（注）　左側のサイドバーのメニューから [Summary] > [Prime Infrastructure] を選択すると、Prime Infrastructure ライセンス情報のみが表示されます。

次の URL の『*Cisco Wireless Control System Licensing and Ordering Guide*』を参照してください。
http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd804b4646.html#wp9000156。

正しい SKU の選択、SKU の注文、ソフトウェアのインストール、PAK 証明書の登録、およびサーバ上へのライセンス ファイルのインストールについて説明されています。

WLC コントローラ ライセンス情報

[License Center] ページの [Controller Licensing] 部分には、WPLUS ライセンスと Base ライセンスの両方に関して以下の情報が示されます。

- [Controller Count]：ライセンスを持つコントローラの現在の数。

（注）　5500 シリーズ コントローラだけがカウントに含まれています。Prime Infrastructure では、インベントリ ビューのみ提供されており、ライセンスの有効期限が近づくと警告が出されます。

（注）　この列の数をクリックする操作は、選択した機能でソートされている点を除いて、左側のサイドバーのメニューから、[Summary] > [Controller] を選択する操作と同じ機能を持ちます。このページには、アクティブ コントローラの概要が示されます。

- [AP Limit]：ライセンスを持つアクセス ポイントの総数。
- [Type]：次の 4 種類のライセンスがあります。

（注）　Permanent 以外のタイプのコントローラについては、期限切れまでの最少日数が表示されます。

  - [Permanent]：ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。
  - [Evaluation]：ライセンスはノードロックされておらず、一定期間だけ有効です。永久ライセンス、拡張ライセンス、および猶予期間ライセンスが存在しない場合だけ使用されます。評価ライセンスを使用する前に、エンド ユーザ ライセンス契約書（EULA）を受け入れる必要があります。このライセンスは、ノードロックされていませんが、ライセンスの使用状況はデバイスに記録されます。期限切れまでの日数が最少の評価ライセンス上の残日数が表示されます。
  - [Extension]：ライセンスはノードロックされており、定量の対象です。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。拡張ライセンスを使用するには、まず、インストール時に EULA を受け入れる必要があります。
  - [Grace Period]：ライセンスはノードロックされており、定量の対象です。これは、ライセンスをリホストするための許可チケットの一部として、シスコのライセンス ポータルによって発行されるライセンスです。これらのライセンスは、リホスト操作の一環としてデバイス上にインストールされます。リホスト操作の一環として EULA を受け入れる必要があります。

一方のコントローラでライセンスを取り消して別のコントローラにインストールする必要がある場合、これを*リホスト*と呼びます。コントローラの目的を変更するために、ライセンスのリホストが必要になる場合があります。ライセンスのリホストの詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』の第 4 章「メンテナンス操作の実行」を参照してください。

（注）　ライセンス ステータスは定期的に更新されます。更新を即座に開始するには、[Administration] > [Background Tasks] を選択し、Controller License Status タスクを実行します。

ネットワークにさまざまなライセンスを持つシスコ デバイスが含まれる場合、Cisco License Manager（CLM）を使用して、1 つのアプリケーションによるすべてのライセンスの管理を検討することを推奨します。CLM は、ネットワーク全体でシスコ ソフトウェアのライセンスを管理する、セキュアなクライアント/サーバ アプリケーションです。CLM ソフトウェアのダウンロードおよびユーザ ドキュメントへのアクセスは、次の URL で実行できます。http://www.cisco.com/go/clm。PAK 証明書は CLM またはライセンス ポータル（https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet）を使用して登録できます。

WLC コントローラ ライセンス サマリー

コントローラ ライセンスの詳細を参照するには、左側のサイドバーのメニューから、[Summary] > [Controller] を選択します。[License Center] ページが表示されます。コントローラ上で現在アクティブなすべてのライセンスが要約されます。

ライセンスを持つすべてのコントローラとその情報（下の箇条書きリスト）が表示されます。コントローラの結果の表示方法を変更する場合は、[Edit View] をクリックします。列を表示から除去するには、[Edit View] ページで、[License Status] を強調表示し、[Hide] をクリックします。

[Controller Summary] リストの上には、[Controller Name]、[Feature]、[Type]、または [Greater Than Percent Used] によってリストをフィルタできる一連のフィルタがあります。たとえば、50 を入力した場合、このリストには、50 % を超えるライセンスが使用されているすべての WLC が表示されます。

（注）　[Advanced Search] リンクを使用して、コントローラのリストをソートすることもできます。

- [Controller Name]：[Files] > [Controller Files] ページへのリンクがあります。
- [Controller IP]：コントローラの IP アドレス。
- [Model]：コントローラ モデル タイプ。
- [Feature]：ライセンスのタイプで、Base または WPLUS のいずれかです。Base ライセンスでは、標準のソフトウェア セットがサポートされ、WPLUS ライセンスではプレミアムの Wireless Plus（WPLUS）ソフトウェア セットがサポートされます。WPLUS ソフトウェア セットには、標準フィーチャ セットの他に、OfficeExtend アクセス ポイント、CAPWAP データ暗号化、およびエンタープライズ ワイヤレス メッシュのための追加機能が備わっています。
- [AP Limit]：アクセス ポイントでこのコントローラを接続できる最大容量。
- [AP Count]：現在ライセンスを使用しているアクセス ポイントの数。
- [% Used]：ライセンスを持つ使用中のアクセス ポイントのパーセンテージ。このパーセンテージが 75 % を超えている場合は、制限に近づいていることを示すためにバーが赤で表示されます。
- [Type]：次の 3 種類のライセンスがあります。

  （注）　Permanent 以外のタイプのコントローラについては、期限切れまでの最少日数が表示されます。

  - [Permanent]：ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。
  - [Evaluation]：ライセンスはノードロックされておらず、一定期間だけ有効です。永久ライセンス、拡張ライセンス、および猶予期間ライセンスが存在しない場合だけ使用されます。評価ライセンスを使用する前に、エンド ユーザ ライセンス契約書（EULA）を受け入れる必要があります。このライセンスは、ノードロックされていませんが、ライセンスの使用状況はデバイスに記録されます。期限切れまでの日数が最少の評価ライセンス上の残日数が表示されます。
  - [Extension]：ライセンスはノードロックされており、定量の対象です。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。拡張ライセンスを使用するには、まず、インストール時に EULA を受け入れる必要があります。

（注）　ライセンスが期限切れであると表示されたときに、コントローラの機能は停止されません。期限切れのライセンスを持つコントローラは、リブートして初めて非アクティブになります。

- [Status]：[In Use]、[Not in Use]、[Inactive]、または [EULA Not Accepted]。
  - [Inactive]：このライセンス レベルは使用中ですが、このライセンスは使用中ではありません。
  - [Not In Use]：このライセンス レベルは使用中でなく、このライセンスは現在認識されていません。
  - [Expired In Use]：このライセンスは使用中ですが期限切れであり、次回のリブートで使用されなくなります。
  - [Expired Not In Use]：ライセンスは期限切れであり、もう使用できません。
  - [Count Consumed]：この ap-count ライセンスは使用中です。

モビリティ サービス エンジン（MSE）のライセンス情報

ライセンスには次の 3 種類があります。

- [Permanent]：ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。
- [Evaluation]：ライセンスはノードロックされておらず、一定期間だけ有効です。永久ライセンス、拡張ライセンス、および猶予期間ライセンスが存在しない場合だけ使用されます。評価ライセンスを使用する前に、エンド ユーザ ライセンス契約書（EULA）を受け入れる必要があります。このライセンスは、ノードロックされていませんが、ライセンスの使用状況はデバイスに記録されます。期限切れまでの日数が最少の評価ライセンス上の残日数が表示されます。
- [Extension]：ライセンスはノードロックされており、定量の対象です。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。拡張ライセンスを使用するには、まず、インストール時に EULA を受け入れる必要があります。

[License Center] ページの [MSE Licenses] 部分には、各サービスの情報が示されます。（表 15-10 を参照）。

表 15-10　MSE ライセンス情報

フィールド	説明
CAS Elements	
Permanent Limit	永久ライセンスを持つ CAS 要素の総数。
Evaluation Limit	評価ライセンスを持つ CAS 要素の総数。
Count	MSE 全体での現在ライセンスを持つ CAS 要素の数。
% Used	MSE 全体でのライセンスを持つ CAS 要素のパーセンテージ。
wIPS Monitor Mode APs	
Permanent Limit	永久ライセンスを持つワイヤレス IPS モニタ モード AP の総数。
Evaluation Limit	評価ライセンスを持つワイヤレス IPS モニタ モード AP の総数。
Count	MSE 全体での現在ライセンスを持つワイヤレス IPS モニタ モード AP の数。
% Used	MSE 全体でのライセンスを持つワイヤレス IPS モニタ モード AP のパーセンテージ。
[wIPS Monitor Mode Aps] または [wIPS Local Mode Aps] の下のアクティブ リンクをクリックすると、ライセンスを持つアクセス ポイントのリストが表示されます。ライセンスを持つクライアントおよびタグのリストにはアクセスできません。	
wIPS Local Mode APs	
Permanent Limit	永久ライセンスを持つワイヤレス IPS ローカル モード AP の総数。
Evaluation Limit	評価ライセンスを持つワイヤレス IPS ローカル モード AP の総数。
Count	MSE 全体での現在ライセンスを持つワイヤレス IPS ローカル モード AP の数。
% Used	MSE 全体でのライセンスを持つワイヤレス IPS ローカル モード AP のパーセンテージ。
[wIPS Monitor Mode APs] または [wIPS Local Mode APs] の下のアクティブ リンクをクリックすると、ライセンスを持つアクセス ポイントのリストが表示されます。ライセンスを持つクライアントおよびタグのリストにはアクセスできません。	

（注）
- ライセンスを削除すると、新しいライセンス制限をロードするためにモビリティ サービス エンジンが自動的に再起動されます。
- パートナー タグ エンジンが起動されている場合、MSE ライセンス情報にはタグ ライセンス上の情報も構成されています。

MSE ライセンスの詳細については、「MSE ライセンスの概要」（P.16-1034）を参照してください。

モビリティ サービス エンジン（MSE）ライセンスの概要

MSE ライセンスの詳細を参照するには、左側のサイドバーのメニューから、[Summary] > [MSE] を選択します。[License Center] ページが表示されます。

ライセンスを持つすべての MSE が以下の列にリストされます。

- [MSE Name]：MSE ライセンス ファイル リスト ページのリンクがあります。

（注）　[MSE Name/UDI] の左方のアイコンは、モビリティ サービス エンジンがローエンドなのかハイエンドなのかを示します。
ハイエンド モビリティ サービス エンジン（3350）は、メモリ容量が大きく、18,000 台までのクライアントとタグを追跡できます。ローエンド モビリティ サービス エンジン（3310）では、2000 台までのクライアントとタグを追跡できます。

- [Type]：MSE のタイプを指定します。

（注）　[wIPS Monitor Mode APs] または [wIPS Local Mode APs] の下のアクティブ リンクをクリックすると、ライセンスを持つアクセス ポイントのリストが表示されます。ライセンスを持つクライアントまたはタグのリストにはアクセスできません。

- [Limit]：MSE 全体でのライセンスを持つクライアント要素の総数が表示されます。
- [Count]：MSE 全体での現在ライセンスを持つクライアント要素の数が表示されます。
- [Unlicensed Count]：ライセンスを持たないクライアント要素の数が表示されます。

（注）　wIPS サービスでは、このライセンスを持たないアクセス ポイントから生成されたアラームを処理しません。

- [% Used]：MSE 全体での使用中クライアントのパーセンテージが表示されます。
- [License Type]：次の 3 種類のライセンスがあります。
  - [Permanent]：ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。
  - [Evaluation]：ライセンスはノードロックされておらず、一定期間だけ有効です。永久ライセンス、拡張ライセンス、および猶予期間ライセンスが存在しない場合だけ使用されます。評価ライセンスを使用する前に、エンド ユーザ ライセンス契約書（EULA）を受け入れる必要があります。このライセンスは、ノードロックされていませんが、ライセンスの使用状況はデバイスに記録されます。期限切れまでの日数が最少の評価ライセンス上の残日数が表示されます。
  - [Extension]：ライセンスはノードロックされており、定量の対象です。これは、シスコのライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。拡張ライセンスを使用するには、まず、インストール時に EULA を受け入れる必要があります。
- Status
  - [Active]：ライセンスはインストールされており、機能によって使用中です。
  - [Inactive]：ライセンスはインストールされていますが、機能によって使用されていません。

- [Expired]：ライセンスは期限切れです。
- [Corrupted]：ライセンスは破損しています。

MSE ライセンスの詳細については、「MSE ライセンスの概要」（P.16-1034）を参照してください。

Prime Infrastructure ライセンスの管理

左側のサイドバーのメニューから [Files] > [Prime Infrastructure Files] の順に選択すると、Prime Infrastructure ライセンスを管理できます。このページは、次の情報を表示します。

- Product Activation Key（PAK）
- 機能
- アクセス ポイントの上限
- タイプ

ここでは、次の内容について説明します。

- 「新しい Prime Infrastructure ライセンス ファイルの追加」（P.15-931）
- 「Prime Infrastructure ライセンス ファイルの削除」（P.15-931）

新しい Prime Infrastructure ライセンス ファイルの追加

新しい Prime Infrastructure ライセンス ファイルを追加するには、次の手順を実行します。

ステップ 1　[License Center] > [Files] > [Prime Infrastructure Files] ページで [Add] をクリックします。

ステップ 2　[Add a License File] ダイアログボックスで、該当するライセンス ファイルを入力するか、ブラウズして選択します。

ステップ 3　[License File] テキスト ボックスに表示されたら、[Upload] をクリックします。

Prime Infrastructure ライセンス ファイルの削除

Prime Infrastructure ライセンス ファイルを削除するには、次の手順に従います。

ステップ 1　[License Center] > [Files] > [Prime Infrastructure Files] ページで、削除する Prime Infrastructure ライセンス ファイルのチェックボックスをオンにします。

ステップ 2　[Delete] をクリックします。

ステップ 3　[OK] をクリックして、削除を実行します。

コントローラ ライセンスのモニタリング

左側のサイドバーのメニューから [Files] > [Controller Files] を選択するとコントローラ ライセンスをモニタできます。

（注）　Prime Infrastructure は、コントローラ ライセンスを直接管理するのではなく、単にこのライセンスをモニタします。このライセンスは、コマンドライン インターフェイス、Web UI、または Cisco License Manager（CLM）を使用して管理できます。

このページには、次のパラメータが表示されます。

- Controller Name
- [Controller IP]：コントローラの IP アドレス。
- [Feature]：ライセンス機能には、wplus-ap-count、wplus、base-ap-count、および base が含まれます。

  インストールされているすべての物理ライセンスについて、コントローラに機能レベル ライセンスと ap-count ライセンスの 2 個のライセンス ファイルが表示されます。たとえば、コントローラに「WPlus 500」ライセンスをインストールすると、「wplus」機能および「wplus-ap-count」機能が表示されます。組み合わせによって機能レベル（WPlus または Base）および AP カウントを有効にするために、常時、このうち 2 個の機能がアクティブになっています。

  （注）　WPlus と Base の両方のライセンスを保持できますが、特定の時期にアクティブにできるのは 1 つだけです。

- [AP Limit]：アクセス ポイントでこのコントローラを接続できる最大容量。
- [EULA status]：[Accepted] または [Not Accepted] のいずれかで、エンド ユーザ ライセンス契約書のステータスが表示されます。
- [Comments]：ライセンスをインストールするときにユーザが入力したコメント。
- [Type]：次の 4 種類のライセンスがあります。
  - [Permanent]：ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコ ライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。
  - [Evaluation]：ライセンスはノードロックされておらず、一定期間だけ有効です。永久ライセンス、拡張ライセンス、および猶予期間ライセンスが存在しない場合だけ使用されます。評価ライセンスを使用する前に、エンド ユーザ ライセンス契約書（EULA）を受け入れる必要があります。このライセンスは、ノードロックされていませんが、ライセンスの使用状況はデバイスに記録されます。アクティブ ライセンスの残日数が最少の評価ライセンスについて、残日数が表示されます。
  - [Extension]：ライセンスはノードロックされており、定量の対象です。これは、シスコ ライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。拡張ライセンスを使用するには、まず、インストール時に EULA を受け入れる必要があります。
  - [Grace Period]：ライセンスはノードロックされており、定量の対象です。これは、ライセンスをリホストするための許可チケットの一部として、シスコ ライセンス ポータルによって発行されるライセンスです。これらのライセンスは、リホスト操作の一環としてデバイス上にインストールされます。リホスト操作の一環として EULA を受け入れる必要があります。

  （注）　Permanent 以外のタイプでは、ライセンスが期限切れになるまでの残日数が表示されます。現在使用中でないライセンスは、「In Use」にならないうちは、カウントを減算されません。

- Status
  - [In Use]：このライセンス レベルおよびライセンスは使用中です。
  - [Inactive]：このライセンス レベルは使用中ですが、このライセンスは使用中ではありません。
  - [Not In Use]：このライセンス レベルは使用中でなく、このライセンスは現在認識されていません。
  - [Expired In Use]：このライセンスは使用中ですが期限切れであり、次回のリブートで使用されなくなります。
  - [Expired Not In Use]：ライセンスは期限切れであり、もう使用できません。
  - [Count Consumed]：この ap-count ライセンスは使用中です。

（注）　ライセンス ファイルのリストをフィルタする必要がある場合は、コントローラ名、機能、またはタイプを入力して [Go] をクリックします。

モビリティ サービス エンジン（MSE）ライセンスの管理

左側のサイドバーのメニューから [Files] > [MSE Files] を選択するとモビリティ サービス エンジン ライセンスを管理できます。

ここでは、次の内容について説明します。

- 「製品認証キーの登録」（P.15-934）
- 「クライアント ライセンス ファイルおよびワイヤレス IPS ライセンス ファイルのインストール」（P.15-935）
- 「モビリティ サービス エンジンのライセンス ファイルの削除」（P.15-936）

このページには、見つかったモビリティ サービス エンジン ライセンスが表示されます。以下の情報が含まれます。

（注）　タグ ライセンスは、該当のベンダー アプリケーションを使用して追加および管理されるため、タグ ライセンスはこのページに表示されません。詳細については、次の URL を参照してください。
http://support.aeroscout.com。
評価（デモ）ライセンスも表示されません。

パートナー エンジンを使用してタグが追跡される場合、タグ ライセンスをインストールするには、*AeroScout System Manager* を使用します。その他の場合、タグは CAS 要素ライセンスとまとめてカウントされます。

- [MSE License File]：MSE ライセンスを示します。
- [MSE]：MSE 名を示します。
- [Type]：モビリティ サービス エンジンのタイプ（クライアント要素、ワイヤレス IPS ローカル モード、またはワイヤレス IPS モニタ モード アクセス ポイント）を示します。
- [Limit]：モビリティ サービス エンジン全体でのライセンスを持つクライアント要素またはワイヤレス IPS モニタ モード アクセス ポイントの総数が表示されます。
- [License Type]：このページに表示されるライセンスの種類は永久ライセンスだけです。

– [Permanent]：ライセンスはノードロックされており、使用期間は関連付けられていません。これは、シスコ ライセンス ポータルによって発行されるライセンスであり、デバイス上の管理インターフェイスを使用してインストールする必要があります。これらのライセンスをインストールすれば、さまざまなバージョンをまたがって必要な権限を得られます。

製品認証キーの登録

クライアント、wIPS、またはタグのライセンスをシスコに注文すると、製品認証キー（PAK）が配布されます。モビリティ サービス エンジン上にインストールするライセンス ファイルを受け取るには、PAK を登録する必要があります。PAK の登録に成功すると、ライセンス ファイルが電子メールで送信されます。

クライアントおよびワイヤレス IPS の PAK は、シスコに登録します。

（注）　タグ PAK は AeroScout に登録されます。タグ PAK を登録するには、AeroScout Web サイトにアクセスします。

インストールするライセンス ファイルを入手するために製品認証キー（PAK）を登録するには、次の手順に従います。

ステップ 1　ブラウザ ページを開き、www.cisco.com/go/license に移動します。

（注）　このサイトへは、Prime Infrastructure の [License Center] ページにある [Product License Registration] リンクをクリックすることでもアクセスできます。

ステップ 2　PAK を入力し、[SUBMIT] をクリックします。

ステップ 3　ライセンスの購入内容を確認します。正しい場合は [Continue] をクリックします。ライセンス入力ページが表示されます。

（注）　ライセンスが正しくない場合は、[TAC Service Request Tool] リンクをクリックして問題をレポートしてください。

ステップ 4　[Designate Licensee] ページで、[host ID] テキスト ボックスにモビリティ サービス エンジンの UDI を入力します。これは、ライセンスがインストールされているモビリティ サービス エンジンです。

（注）　モビリティ サービス エンジンの UDI 情報は、[Services] > [Mobility Services Engine] > [*Device Name*] > [*System*] にある [General Properties] グループ ボックスに表示されます。

ステップ 5　[Agreement] チェックボックスをオンにします。[Agreement] チェックボックスの下に登録者情報が表示されます。

必要に応じて情報を変更します。

（注）　登録者およびエンド ユーザの電話番号に、文字が含まれていないことを確認します。たとえば 408.555.1212 や 408-555-1212 ではなく 408 555 1212 と入力します。

ステップ 6　登録者とエンド ユーザが異なる場合は、登録者情報の下の [Licensee (End-User)] チェックボックスをオンにしてエンド ユーザ情報を入力します。

ステップ 7　[Continue] をクリックします。入力したデータの概要が表示されます。

ステップ 8　[Finish and Submit] ページで登録者とエンド ユーザのデータを確認します。必要な場合は [Edit Details] をクリックして情報を訂正します。

ステップ 9　[Submit] をクリックします。確認用のページが表示されます。

クライアント ライセンス ファイルおよびワイヤレス IPS ライセンス ファイルのインストール

Prime Infrastructure から CAS 要素ライセンスおよび wIPS ライセンスをインストールできます。

（注）　タグ ライセンスをインストールするには、*AeroScout System Manager* を使用します。追加情報については、次の URL を参照してください。
http://support.aeroscout.com。

PAK の登録後にクライアント ライセンスまたは wIPS ライセンスを Prime Infrastructure に追加するには、次の手順に従います。

ステップ 1　[Administration] > [License Center] を選択します。

ステップ 2　左側のサイドバーのメニューから [Files] > [MSE Files] の順に選択します。

ステップ 3　[License Center] > [Files] > [MSE Files] ページで [Add] をクリックして [Add a License File] ダイアログボックスを開きます。

ステップ 4　[MSE Name] ドロップダウン リストから、ライセンス ファイルを追加するモビリティ サービス エンジンを選択します。

（注）　選択されているモビリティ サービス エンジンの UDI が、PAK 登録時に入力したものと一致していることを確認します。

ステップ 5　[License File] テキスト ボックスにライセンス ファイルを入力するか、該当するライセンス ファイルをブラウズして選択します。

ステップ 6　[License File] テキスト ボックスに表示されたら、[Upload] をクリックします。新しく追加されたライセンスがモビリティ サービス エンジン ライセンス ファイル リストに表示されます。

（注）　クライアント ライセンスまたはタグ ライセンスをインストールすると、Context-Aware Service（CAS）が再起動されます。ワイヤレス IPS ライセンスをインストールすると、ワイヤレス IPS サービスが再起動されます。

（注）　別のライセンスの追加または削除を試行するには、その前にサービスが開始されている必要があります。

モビリティ サービス エンジンのライセンス ファイルの削除

モビリティ サービス エンジン ライセンス ファイルを削除するには、次の手順に従ってください。

ステップ 1　[License Center] > [Files] > [MSE Files] ページで、削除するモビリティ サービス エンジン ライセンス ファイルのチェックボックスをオンにします。

ステップ 2　[Delete] をクリックします。

ステップ 3　[OK] をクリックして、削除を実行します。

Prime Infrastructure サービス

この章の内容は、次のとおりです。

モビリティ サービス

この項では、Cisco Prime Infrastructure がサポートする CAS、wIPS、および分析サービスについて簡単に説明し、すべてのサービスに共通するモビリティ手順を示します。

CAS

Context-Aware Service（CAS）ソフトウェアにより、シスコ アクセス ポイントから状況依存情報（ロケーション、温度、可用性など）を取得することで、モビリティ サービス エンジンは数千のモバイル アセットとクライアントを同時に追跡できます。

（注） アクセス ポイントからタグおよびクライアントに関する状況依存情報を取得するには、シスコからライセンスを購入する必要があります。タグとクライアントのライセンスはそれぞれ個別に提供されます。タグおよびクライアントのラインセンスの詳細については、次の URL にある『*Cisco 3350 Mobility Services Engine Release Note*』を参照してください。

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

wIPS

Cisco Adaptive Wireless IPS（wIPS）は、無線の脅威の検出およびパフォーマンスの管理のための高度な手法です。wIPS では、ネットワーク トラフィック分析、ネットワーク デバイス / トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。

（注）　非ルート パーティション ユーザに対しては wIPS 機能はサポートされていません。

モバイル コンシェルジュ

モバイル コンシェルジュ サービスにより、場所所有者とサービス プロバイダーは WLAN をモニタできます。モバイル コンシェルジュ サービスは、スマート フォンを使用している顧客に固有のストア内エクスペリエンスを提供します。

モバイル コンシェルジュ サービスは、ネットワーク接続を確立するための一連のポリシーを使用して設定されたワイヤレス スマート フォンを使用します。モバイル コンシェルジュ サービスにより、使用可能なネットワーク ベースのサービスをスマート フォンで簡単に検出できます。ストアの Wi-Fi ネットワークに接続した後、ストアのワイヤレス ゲスト ネットワークに参加して、電子クーポン、プロモーション オファー、顧客ロイヤルティ データ、製品提案、ショッピング リストの編成機能など、さまざまなサービスにアクセスしたり、ショッピング設定に基づいて固有のデジタル署名を受け取ることができます。

ロケーション分析サービス

ロケーション分析サービスは、特定のネットワーク上のワイヤレス デバイスのロケーション情報を分析します。ロケーション分析サービスは、Cisco Mobility Services Engine（MSE）が提供するデータを使用して、WLAN（無線 LAN）内の Wi-Fi デバイスのロケーションを計算します。

ネットワーク内でワイヤレス デバイスが有効化されている場合、そのワイヤレス デバイスはプローブ要求パケットを送信して、その近隣のワイヤレス ネットワークを識別します。クライアント デバイスは、WLAN 内のアクセス ポイントに接続した後でも、よりよい QoS のその他のアクセス ポイントを識別するために、プローブ要求パケットを引き続き送信します。アクセス ポイントは、各種のワイヤレス デバイスからこれらの要求と関連する RSSI を収集し、それらをワイヤレス LAN コントローラ（WLC）に送信します。コントローラは、この情報を MSE に送信します。

各種 AP から収集された基本データを分析すると、建物内で Wi-Fi デバイスを使用しているユーザの移動および行動パターンについて情報や知識を得ることができます。たとえば建物では、空港、ショッピング モール、街の中心などがあります。ロケーション分析サービスは、空港局や建物の所有者が自分の建物内の通行人または顧客の動向を認識できます。これは、これらの所有者が建物内の標示を改善したり、使用率の低い場所に変更を加えたりするのに役立ちます。

モバイル ビルボード サービス

モバイル ビルボードは、企業の管理者がゲストへの付加価値サービスを作成できるソリューションです。モバイル ビルボードでは企業が Wi-Fi を戦略的に売上を生成するツールとすることが可能で、企業内での顧客の行動に関するデータを収集しビジネスに役立つ分析情報を提供します。モバイル ビルボードの支援により、企業はインターネットを閲覧しているデバイスに小さな Web バナーを配置できます。

バーゲンやパンフレットに加えて、モバイル ビルボードは施設内の顧客の行動に関する情報を企業が収集しやすくします。モバイル ビルボードはさまざまなロケーション ベースのサービスおよびコンテキスト認識型メッセージングを可能にするモバイル コンシェルジュの主要コンポーネントです。付加価値サービスやメッセージを提供するには、モバイル ビルボードは HTTP トラフィック フローに依存します。

Web バナーを導入する目的は次のとおりです。

- ショップの提案をライブで提供することで顧客との対話を提供。
- 他社の広告のプラットフォームとしてのネットワークの Web バナーの使用。

次は異なるモバイル ビルボードのコンポーネントです:

- ビルボード プラットフォーム：キャンペーン、メッセージ、サービス、アカウント、関心のあるポイント、およびその他のサービスを管理するため Web ポータルを介してアクセス可能な管理コンソール。
- ビルボード署名挿入コンポーネント：HTTP トラフィックを代行受信し、ビルボードのエンドポイントの署名を挿入する機能。
- モバイル サービス エンジン：ビルボードのエンドポイントのリアルタイムなロケーション関連情報。

HTTP プロキシ サービス

ワイヤレス LAN コントローラ（WLC）UI はコントローラ側の HTTP プロキシ サービスを有効にし制御します。Prime Infrastructure UI は、Mobility Services Engine で HTTP プロキシを有効にし制御します。HTTP プロキシはトラフィック フロー テーブルを Network Based Application Recognition（NBAR）から分割します。

HTTP プロキシ サービスの主要なコンポーネントは次のとおりです。

- ビルボード プラットフォーム：管理者がキャンペーン、メッセージ、サービス、アカウント、および関心のあるポイントなどのさまざまなメッセージ オブジェクトを管理する管理コンソールが含まれます。また、特定のエンドポイントに対する場所およびコンテキスト認識型サービスおよびメッセージを提供するランタイム エンジンがあります。
- ビルボード署名挿入コンポーネント：ブラウズ中に HTTP 応答に追加され単純なスクリプトです。これは次のいずれかで実現できます。
  - リモート HTTP プロキシのあるワイヤレス コントローラ
  - クラウド コネクタとして HTTP プロキシのある ISR
- 署名：必須パラメータとしてエンドポイントの IP アドレスまたは MAC アドレスが含まれます。名前と値のペアとし他のパラメータを追加できます。
- モバイル サービス エンジン：モバイル ビルボードのエンドポイントのリアルタイムなロケーション関連情報を提供します。エンドポイントは、エンド ユーザにとって意味がありコンテキスト / ロケーション連動サービスおよびメッセージを有効にする主要因です。

ここでは、次の内容について説明します。

Cisco Context-Aware Mobility ソリューション

CAM ソリューションの基盤は CUWN のコントローラ ベースのアーキテクチャです。CUWN には、次の主要コンポーネントが含まれます。

Cisco Prime Infrastructure

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

WLAN コントローラ

WLAN コントローラは、高い拡張性と柔軟性を備えたプラットフォームで、中大規模企業やキャンパス環境でのミッションクリティカルなワイヤレス通信のためのシステム全体のサービスを実現します。802.11n のパフォーマンスと最大限の拡張性を重点に設計された WLAN コントローラは、5000 アクセス ポイントから 250 アクセス ポイントまでを同時に管理する能力により強化された稼働時間、信頼性

の高いストリーミング ビデオや有料レベルの音声品質を可能にする優れたパフォーマンス、そして要求が非常に高い環境での安定したモビリティ経験を実現する進んだディザスタ リカバリ性能を備えています。

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

- Cisco 2700 シリーズ ロケーション アプライアンス
- Cisco 2000 シリーズ ワイヤレス LAN コントローラ
- Cisco 2100 シリーズ ワイヤレス LAN コントローラ
- Cisco 2500 シリーズ ワイヤレス コントローラ
- Cisco 4400 シリーズ ワイヤレス LAN コントローラ
- Cisco 5500 シリーズ ワイヤレス コントローラ
- Catalyst 3750G ワイヤレス LAN コントローラ スイッチ
- Cisco Catalyst 6500 シリーズ スイッチ用 Cisco Wireless Services Module（WiSM）
- Cisco Catalyst 6500 シリーズ スイッチ用 Cisco Wireless Services Module 2（WiSM2）
- ISR G2 ルータ用 Cisco ワイヤレス コントローラ on SRE
- Cisco Flex 7500 シリーズ ワイヤレス コントローラ
- Cisco Integrated Services Router 用 Cisco WLAN コントローラ ネットワーク モジュール

アクセス ポイント

次のアクセス ポイントがサポートされています。

- Cisco Aironet 801、802、1000、1040、1100、1130、1140、1200、1230、1240、1250、1260、1310、1500、1524、1552、1600i、1600e、2600i、2600e、3500i、3500e、3500p、3600i、および 3600e シリーズ Lightweight アクセス ポイント。
- Cisco Aironet 1040、1100、1130、1141、1142、1200、1240、1250、1260、2600i、および 2600e 自律アクセス ポイント。
- Cisco 600 シリーズ OfficeExtend アクセス ポイント。
- Lightweight アクセス ポイント プロトコル（LWAPP）または Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルが動作している Cisco Aironet アクセス ポイント。

Cisco 3300 シリーズ モビリティ サービス エンジン

Cisco 3300 シリーズ モビリティ サービス エンジンは、CAM ソリューションのコンポーネントである CAS で動作します。モビリティ サービス エンジンには 2 種類のモデルがあります。

- Cisco 3300 Mobility Services Engine
- Cisco 3355 モビリティ サービス エンジン

サービスへのアクセス

MSE インストール ガイドは次の URL からご利用いただけます。

MSE 3355 インストール ガイド：

http://www.cisco.com/en/US/docs/wireless/mse/3355/user/guide/mse_qsgmain.html

MSE サービスの共存

MSE 6.0 以上では、複数のサービス（Context Aware サービスおよび wIPS）を同時に実行できます。6.0 よりも前のバージョンでは、モビリティ サービス エンジンでは一度に 1 つのアクティブ サービスだけがサポートされていました。

複数サービスを共存させる場合には、以下の点を考慮してください。

- サービスの共存は、ライセンス執行の影響を受けることがあります。ライセンスが有効期限内である限り、複数サービスを有効にできます。

（注）　サービスごとに制限事項が異なります。たとえばローエンド モビリティ サービス エンジン（MSE-3310）は合計 2,000 の CAS 要素を追跡し、ハイエンド モビリティ サービス エンジン（MSE-3355）は合計 25,000 の CAS 要素を追跡します。
ローエンド モビリティ サービス エンジンで追跡可能な wIPS 要素の最大数は 2000、ハイエンド モビリティ サービス エンジンで追跡可能な wIPS 要素の最大数は 3000 です。

（注）　CAS ライセンスは、現在はベース ロケーション ライセンスと呼びます。

- 有効期限切れの評価ライセンスがあると、サービスが起動できません。
- Base ロケーション ライセンスを追加または削除すると、モビリティ サービス エンジンのすべてのサービス（wIPS を含む）が再起動されます。wIPS ライセンスを追加または削除しても CAS には影響しません。wIPS が再起動するだけです。
- 最大数の要素の永久ライセンスが適用されている場合でも、その他のサービスを評価モードで有効にできます。

  サービスの 1 つが最大数のライセンスで実行可能になっている場合は常に、別のサービスを並行して実行することはできません。これは、両方のサービスに同時に対応できる十分なキャパシティが MSE にないためです。たとえば、MSE-3310 に 2000 要素の wIPS ライセンスをインストールしている場合、CAS を同時に実行することはできません。ただし、評価ライセンスはこの制限の対象外です。

（注）　[Services] タブの [Mobility Services Engines]、[Synchronize Services]、[Synchronization History]、[High Availability]、[Context-Aware Notifications]、および [Mobile Concierge Services] ページは、リリース 7.3 の root 仮想ドメインでのみ使用できます。

現在のモビリティ サービスの表示

現在のモビリティ サービスのリストを表示するには、[Services] > [Mobility Services Engines] の順に選択します。

[Mobility Services Engines] ページに、各デバイスに関する次の情報と機能が表示されます。

- [Device Name]：モビリティ サービス エンジンのユーザ割り当て名。モビリティ サービス エンジンの詳細を表示、管理するには、デバイス名をクリックします。詳細については、「モビリティ サービス エンジンのシステム プロパティの管理」（P.16-966）を参照してください。

- [Device Type]：モビリティ サービス エンジンのタイプを示します（例：Cisco 3310 Mobility Services Engine）。デバイスが仮想アプライアンスであるかどうかを示します。
- [IP Address]：モビリティ サービス エンジンの IP アドレスを示します。
- [Version]：モビリティ サービス エンジンのバージョン番号を示します。
- [Reachability Status]：モビリティ サービス エンジンが到達可能であるかどうかを示します。
- [Secondary Server]：セカンダリ サーバがインストールされているかどうかを示します。
- Mobility Service:
  - [Name]：モビリティ サービスの名前を示します。
  - [Admin Status]：モビリティ サービスが有効または無効のいずれであるかを示します。
  - [Service Status]：モビリティ サービスが現在実行中であるかどうかを示します。
- [Select a command] ドロップダウン リスト：
  - [Add Location Server]
  - [Add Mobility Services Engine]：Context-Aware サービス、Cisco Adaptive Wireless IPS（wIPS）サービス、モバイル コンシェルジュ サービス、およびロケーション分析サービスが含まれます。
  - Delete Service
  - Synchronize Service
  - Synchronization History
  - Edit Configuration

（注） Prime Infrastructure のロケーション機能およびモビリティ サービス機能では、パーティショニングはサポートされていません。

モビリティ サービス エンジンの追加

[Mobility Service] ページの [Add Mobility Services Engine] ダイアログボックスを使用して MSE を追加できます。このダイアログボックスでは、ライセンス ファイルと追跡パラメータを追加し、マップを MSE に割り当てることができます。設定のために既存の MSE でウィザードを起動する場合、[Add MSE] オプションの代わりに [Edit MSE Details] として表示されます。

ヒント Cisco Adaptive wIPS 機能の詳細については、Cisco.com でマルチメディア プレゼンテーションを参照してください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールがあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

（注） Prime Infrastructure Release 1.0 は、MSE 3355 を適切に認識してサポートします。

（注） [Services] > [Mobility Services Engine] ページは、root 仮想ドメインでのみ使用可能です。

Prime Infrastructure にモビリティ サービス エンジンを追加するには、Prime Infrastructure にログインし、次の手順に従います。

ステップ 1　追加するモビリティ サービス エンジンに対して Prime Infrastructure から ping を実行できることを確認します。

ステップ 2　[Services] > [Mobility Services Engines] の順に選択し、[Mobility Services] ページを表示します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Mobility Services Engine] を選択し、[Go] をクリックします。

[Add Mobility Services Engine] ページが表示されます。

ステップ 4　次の情報を入力します。

- [Device Name]：モビリティ サービス エンジンのユーザ割り当て名。
- [IP Address]：モビリティ サービス エンジンの IP アドレス。

（注）　有効な IP アドレスが入力された場合にだけ、モビリティ サービス エンジンが追加されます。デバイス名は、複数のモビリティ サービス エンジンと複数の Prime Infrastructure を使用している場合にデバイスを区別するのに役立ちますが、モビリティ サービス エンジンを検証するときには考慮されません。

- [Contact Name]（任意）：モビリティ サービス エンジン管理者。
- [Username]：デフォルトのユーザ名は admin です。これは、MSE に対して設定されている Prime Infrastructure 通信ユーザ名です。
- [Password]：デフォルトのパスワードは admin です。これは、MSE に対して設定されている Prime Infrastructure 通信パスワードです。

（注）　自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、変更後の値をここに入力してください。デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

- [HTTP]：有効に設定されている場合、Prime Infrastructure とモビリティ サービス エンジン間の通信に HTTP が使用されます。デフォルトでは、Prime Infrastructure は MSE との通信に HTTPS を使用します。

（注）　モビリティ サービス エンジンとの HTTP 通信を実行するには、モビリティ サービス エンジンで HTTP が明示的に有効化されている必要があります。

- モビリティ サービス エンジンからすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。

  このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 5　[Next] をクリックします。Prime Infrastructure により、選択されている要素と MSE が自動的に同期されます。

同期完了後、[MSE License Summary] ページが表示されます。[MSE License Summary] ページから、ライセンスのインストール、ライセンスの追加、ライセンスの削除、アクティベーション ライセンスのインストール、サービス ライセンスのインストールを実行します。

MSE のサービスの設定

ステップ 6　モビリティ サービス エンジン上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスは、Context-Aware サービス、wIPS、モバイル コンシェルジュ サービス、ロケーション分析サービス、モバイル ビルボード サービス、および HTTP プロキシ サービスなどです。

MSE 追跡パラメータおよび履歴パラメータの設定

ステップ 7　モビリティ サービス エンジンでサービスを有効にすると、[Select Tracking & History Parameters] ページが表示されます。

（注）　追跡パラメータの設定を省略すると、デフォルト値が選択されます。

ステップ 8　追跡するクライアントを選択するには、対応する [Tracking] チェックボックスをオンにします。追跡パラメータを以下に示します。

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

ステップ 9　デバイスの履歴トラッキングを有効にするには、対応するデバイスのチェックボックスをオンにします。履歴パラメータを以下に示します。

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

ステップ 10　[Next] をクリックして MSE にマップを割り当てます。

MSE へのマップの割り当て

（注）　[Assigning Maps] ページは、MSE で有効にするサービスの 1 つとして CAS を選択する場合にだけ使用可能です。

ステップ 11　MSE 追跡パラメータおよび履歴パラメータを設定すると、[Assigning Maps] ページが表示されます。

[Assign Maps] ページには以下の情報が表示されます。

- 名前
- タイプ（ビルディング、フロア、キャンパス）
- ステータス

ステップ 12　必要なマップ タイプを確認するには、ページで使用可能な [Filter] オプションから [All]、[Campus]、[Building]、[Floor Area]、または [Outdoor Area] を選択します。

ステップ 13　マップを同期するには、[Name] チェックボックスをオンにし、[Synchronize] をクリックします。

ネットワーク設計の同期が完了すると、特定のネットワーク設計で AP が割り当てられている適切なコントローラが MSE と自動的に同期されます。

ステップ 14　[Next] をクリックして、モバイル アプリケーションの有効化を設定します。

モバイル アプリケーションの有効化

この統合を有効にすると、MSE はフロア マップおよびワイヤレス クライアントの位置通知を Meridian に送信できます。Meridian は、この情報を使用して、ロケーション ベースのサービスをユーザに提供します。このとき、ユーザは、ネットワークに接続し、MSE に直接アクセスする必要はありません。Meridian を有効にした後、アカウントをアクティブにする方法、および組織内の他のユーザとアクセスを共有する方法についての指示を含む電子メールを受信します。Meridian モバイル アプリケーションまたは Android および iOS 向けのモバイル SDK を使用した独自のアプリケーションのいずれかを介してビジターにロケーション サービスを提供するために Meridians プラットフォームを使用できます。MSE から Meridian への各ワイヤレス クライアント位置通知またはゾーン通知のデータ帯域幅は最大 1 MB/ 秒です。詳細については、http://www.meridianapps.com/mse を参照してください。

ステップ 15　MSE にマップを割り当てると、[Mobile App Enablement] ページが表示されます。

ステップ 16　[Enable Mobile App Integration] チェックボックスを選択してモバイル アプリケーション統合を有効にします。このアイコンをクリックして [Mobile App Enablement Help] ページを開くことができます。

ステップ 17　[Location Name] テキスト ボックスにロケーションの名前を入力します。ここに入力する名前が Meridian アプリケーションで表示されるため、各自のデバイスでロケーション サービスをテストできます。

ステップ 18　Meridian オンライン エディタおよび SDK にアクセスするために、[E-mail Address] テキスト ボックスに電子メール アドレスを入力します。Meridian は、これらのアドレスに、アカウントへのアクセス方法、および組織内の他のユーザとのアカウント共有方法についての指示を含む電子メールを送信します。

ステップ 19　[Street Address] テキスト ボックスに、ロケーションの住所を入力します。

ステップ 20　[Phone Number] テキスト ボックスに、Meridian からの連絡用の電話番号を入力します。

ステップ 21　[Advanced] ペインを開くには、[Advanced] をクリックします。

ステップ 22　ワイヤレス クライアントが選択したゾーンに入った場合に MSE でリアルタイム通知を Meridian に送信する場合は、[Enable Zone Notifications for zones] チェックボックスをオンにし、ドロップダウン リストからフロアおよびゾーンを選択します。

[Enable zone notifications for zones] ドロップダウン リストには、Prime Infrastructure に追加され、MSE と同期しているすべてのフロアおよびゾーンが表示されます。

ステップ 23　ゾーンとフロアを選択した後、[OK] をクリックします。

ステップ 24　[Save] をクリックします。

ステップ 25　[Done] をクリックして MSE 設定を保存します。

MSE ライセンス ファイルの削除

MSE ライセンス ファイルを削除するには、次の手順に従います。

（注）　[Services] > [Mobility Services Engine] ページは、リリース 7.3 の root 仮想ドメインでのみ使用可能です。

ステップ 1　[Services] > [Mobility Service Engine] の順に選択します。

[Mobility Services] ページが表示されます。

ステップ 2　削除するモビリティ サービス エンジン ライセンスを選択するため、対応する [Device Name] チェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Edit Configuration] を選択します。

[Edit Mobility Services Engine] ダイアログボックスが表示されます。

ステップ 4　[Edit Mobility Services Engine] ダイアログボックスの [Next] をクリックします。

[MSE License Summary] ページが表示されます。

ステップ 5　[MSE License Summary] ページで削除する MSE ライセンス ファイルを選択します。

ステップ 6　[Remove License] をクリックします。

ステップ 7　[OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてライセンスを削除せずにこのページを閉じます。

ステップ 8　[Next] をクリックしてモビリティ サービス エンジン上でサービスを有効にします。

Prime Infrastructure からのモビリティ サービス エンジンの削除

Prime Infrastructure データベースからモビリティ サービス エンジンを削除するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engine] の順に選択します。

[Mobility Services] ページが表示されます。

ステップ 2　削除するモビリティ サービス エンジンを選択するため、対応する [Device Name] チェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Delete Service(s)] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　選択したモビリティ サービス エンジンを Prime Infrastructure データベースから削除することを確定するには、[OK] をクリックします。

ステップ 6　削除を中止するには、[Cancel] をクリックします。

製品認証キーの登録

CAS 要素、wIPS、またはタグのライセンスをシスコに発注すると、製品認証キー（PAK）が配布されます。モビリティ サービス エンジン上にインストールするライセンス ファイルを受け取るには、PAK を登録する必要があります。PAK の登録に成功すると、ライセンス ファイルが電子メールで送信されます。

（注）　PAK がない場合は販売注文番号を使用して PAK を取得できます。詳細については、「PAK の取得」（P.16-948）を参照してください。

PAK を登録し、インストールするライセンス ファイルを入手するには、次の手順に従います。

ステップ 1　Web ブラウザで、https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet にアクセスします。

ステップ 2　PAK を入力し、[SUBMIT] をクリックします。

ステップ 3　ライセンスの購入内容を確認します。正しい場合は [Continue] をクリックします。ライセンス入力ページが表示されます。

（注）　ライセンスが正しくない場合は、[TAC Service Request Tool] URL をクリックして問題をレポートしてください。

ステップ 4　[Designate Licensee] ページで、[Host ID] テキスト ボックスに Mobility Services Engine の UDI を入力します。これは、ライセンスがインストールされているモビリティ サービス エンジンです。

（注）　モビリティ サービス エンジンの UDI 情報は、[Services] > [Mobility Services Engine] > [*Device Name*] > [*System*] の [General Properties] ダッシュレットに表示されます。

ステップ 5　[Agreement] チェックボックスをオンにします。[Agreement] チェックボックスの下に登録者情報が表示されます。

必要に応じて情報を変更します。

（注）　登録者およびエンド ユーザの電話番号に、文字が含まれていないことを確認します。たとえば 408.555.1212 や 408-555-1212 ではなく 408 555 1212 と入力します。

ステップ 6　登録者とエンド ユーザが異なる場合は、登録者情報の下の [Licensee (End-User)] チェックボックスをオンにしてエンド ユーザ情報を入力します。

ステップ 7　[Continue] をクリックします。入力したデータの概要が表示されます。

ステップ 8　[Finish and Submit] ページで、登録者データとエンド ユーザ データを確認します。情報を訂正する必要がある場合は [Edit Details] をクリックします。

ステップ 9　[Submit] をクリックします。確認用のページが表示されます。

PAK の取得

PAK がない場合は販売注文番号を使用して PAK を取得できます。

ステップ 1　次の URL にある Sales Order Status Tool にアクセスします。
http://tools.cisco.com/qtc/status/tool/action/LoadOrderQueryScreen

ステップ 2　ログイン後に [Type of Query] ドロップダウン リストから [Sales Order (SO)] を選択します。

ステップ 3　[Value] テキストボックスに販売注文書番号を入力します。

（注）　この問い合わせでは、[Date Submitted] のフィールドの入力は必要ありません。

ステップ 4　[Show Serial Number] チェックボックスをオンにします。

ステップ 5　[Orders] オプション ボタンがまだ選択されていない場合は、このボタンを選択します。

ステップ 6　[Deliver through] ドロップダウン リストから [Screen] を選択します。

ステップ 7　[Search] をクリックします。モビリティ サービス エンジンの発注に関する詳細情報が表示されます。

ステップ 8　テーブルで [Line 1.1] をクリックします。

ステップ 9　[Product] 列（2 行め）に、ライセンスを取得するために登録する PAK 番号（3201J で始まる番号）をコピーします。

デバイスおよび wIPS ライセンス ファイルのインストール

Prime Infrastructure からデバイス ライセンスと wIPS ライセンスをインストールできます。

（注）　リリース 7.2 以降からリリース 7.5 にアップグレードした場合にタグのライセンスが検出されると、AeroScout ライセンスとエンジンの削除に関する警告メッセージが表示されます。承諾すると、すべてのパートナー エンジンのサブ サービスが削除され、その後 Cisco タグ エンジン サブ サービスがデフォルトで有効になります。パートナー エンジンの排除を承諾しない場合、インストールが続行さえます。タグのライセンスが検出されない場合、インストールはそのまま進行します。

PAK の登録後にクライアント ライセンスまたは wIPS ライセンスを Prime Infrastructure に追加するには、次の手順に従います。

（注）　[Administration] > [Licensing] ページは、リリース 7.3 の root 仮想ドメインでのみ使用可能です。

ステップ 1　[Administration] > [Licensing] の順に選択します。

ステップ 2　[Files] > [MSE] の順に選択します。

ステップ 3　[Add] をクリックします。[Add a License File] ダイアログが表示されます。

ステップ 4　[MSE Name] ドロップダウン リストから該当する MSE 名を選択します。

（注）　選択されているモビリティ サービス エンジンの UDI が、PAK 登録時に入力したものと一致していることを確認します。

ステップ 5　[Choose File] をクリックし、ライセンス ファイルを参照して選択します。

ステップ 6　[Upload] をクリックします。新たに追加されたライセンスが MSE ライセンス ファイル リストに表示されます。

ロケーション サーバの追加

ロケーション サーバを追加するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから [Add Location Server] を選択します。

ステップ 3　[Go] をクリックします。

ステップ 4　次の情報を入力します。

- デバイス名
- IP アドレス
- 連絡先名
- ユーザ名
- パスワード
- ポート
- HTTPS：有効に設定されている場合、Prime Infrastructure とロケーション サーバ間の通信には HTTPS が使用されます。

ステップ 5　モビリティ サービス エンジンからすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。

このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 6　[Save] をクリックします。

（注）　ロケーション サーバを追加したら、ロケーション サーバを Prime Infrastructure と同期する必要があります。詳細については、「サービスの同期化」（P.16-950）を参照してください。

（注）　Prime Infrastructure のロケーション機能およびモビリティ サービス機能では、パーティショニングはサポートされていません。

サービスの同期化

ここでは、Cisco ワイヤレス LAN コントローラおよび Prime Infrastructure をモビリティ サービス エンジンに同期させる方法について説明します。内容は次のとおりです。

（注）　[Services] タブの [Synchronize Services] ページは、リリース 7.3 の root 仮想ドメインでのみ使用可能です。

モビリティ サービス エンジンの同期

ここでは、Prime Infrastructure とモビリティ サービス エンジンを手動で同期する方法、および自動的に同期する方法について説明します。

モビリティ サービス エンジンを Prime Infrastructure に追加した後、ネットワーク設計（キャンパス、ビルディング、フロア、および屋外マップ）、イベント グループ、コントローラ情報（名前と IP アドレス）、または有線スイッチとモビリティ サービス エンジンを同期させることができます。

（注）　同期を実行する前に、コントローラ、Prime Infrastructure、およびモビリティ サービス エンジン間のソフトウェアの互換性を確認してください。URL http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html で、モビリティ サービス エンジンの最新リリース ノートを参照してください。

（注）　モビリティ サービス エンジン、Prime Infrastructure、およびコントローラ間の通信では協定世界時（UTC）が使用されます。各システムで NTP を設定すると、デバイスに UTC 時刻が提供されます。モビリティ サービス エンジンとその関連コントローラは、同一 NTP サーバと同一 Prime Infrastructure サーバにマップする必要があります。NTP サーバは、コントローラ、Prime Infrastructure、およびモビリティ サービス エンジン間で時刻を自動的に同期させるために必要です。

Prime Infrastructure とモビリティ サービス エンジンの同期

ここでは、Prime Infrastructure とモビリティ サービス エンジンを手動でスマートに同期させる方法について説明します。

Prime Infrastructure にモビリティ サービス エンジンを追加したら、ネットワーク設計（キャンパス、ビルディング、フロア、および屋外マップ）、コントローラ（名前と IP アドレス）、特定の Catalyst 3000 シリーズおよび 4000 シリーズ スイッチ、およびイベント グループをモビリティ サービス エンジンと同期できます。

- ネットワーク設計：施設全体でのアクセス ポイントの物理的配置の論理マッピング。1 つのネットワーク設計は、1 つのキャンパス、そのキャンパスを構成するビルディング、および各ビルディングを構成するフロアという階層構造で構成されます。
- コントローラ：モビリティ サービス エンジンに関連付けられている選択されたコントローラ。モビリティ サービス エンジンと定期的にロケーション情報を交換します。定期的な同期により、正確なロケーション情報を維持できます。
- イベント グループ：イベントを生成するトリガーを定義する事前定義イベントのグループ。定期的な同期により、最新の定義イベントが追跡されます。
- 有線スイッチ：ネットワーク上の有線クライアントへのインターフェイスを提供する有線 Catalyst スイッチ。定期的な同期によって、ネットワーク上の有線クライアントのロケーションが正確に追跡されます。

  - モビリティ サービス エンジンは、Catalyst スタッカブル スイッチ（3750、3750-E、3560、2960、IE-3000 スイッチ）、スイッチ ブレード（3110、3120、3130、3040、3030、3020）、およびスイッチ ポートと同期できます。
  - Mobility Services Engine は、Catalyst 4000 シリーズ スイッチ WS-C4948、WS-C4948-10GE、ME-4924-10GE、WS-4928-10GE、WS-C4900M、WS-X4515、WS-X4516、WS-X4013+、WS-X4013+TS、WS-X4516-10GE、WS-X4013+10GE、WS-X45-SUP6-E、および WS-X45-SUP6-LE とも同期できます。
- サードパーティ要素：要素を MSE と同期する場合、サードパーティ アプリケーションにより MSE にイベント グループが作成されていることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。
- サービス アドバタイズメント：モバイル コンシェルジュ サービスは、モバイル デバイスにサービス アドバタイズメントを提供します。これにより、MSE と同期されたサービス アドバタイズメントが示されます。

（注） 同期を実行する前に、コントローラ、Prime Infrastructure、およびモビリティ サービス エンジン間のソフトウェアの互換性を確認してください。URL http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html で、モビリティ サービス エンジンの最新リリース ノートを参照してください。

（注） モビリティ サービス エンジン、Prime Infrastructure、およびコントローラ間の通信では協定世界時（UTC）が使用されます。各システムで NTP を設定すると、デバイスに UTC 時刻が提供されます。モビリティ サービス エンジンとその関連コントローラは、同一 NTP サーバと同一 Prime Infrastructure サーバにマップする必要があります。NTP サーバは、コントローラ、Prime Infrastructure、およびモビリティ サービス エンジン間で時刻を自動的に同期させるために必要です。

Prime Infrastructure ネットワーク設計、コントローラ、有線スイッチ、またはイベント グループの同期

Prime Infrastructure ネットワーク設計、コントローラ、有線スイッチ、またはイベント グループをモビリティ サービス エンジンと同期させるには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、適当なメニュー オプション（[Network Designs]、[Controllers]、[Event Groups]、[Wired Switches]、[Third Party Elements]、または [Service Advertisements]）を選択します。

ステップ 3　モビリティ サービス エンジンにネットワーク設計を割り当てるには、左側のサイドバー メニューから [Network Designs] を選択します。

ステップ 4　対応する [Name] チェックボックスをオンにして、モビリティ サービス エンジンと同期させるすべてのマップを選択します。

（注） 6.0 では、モビリティ サービス エンジンに割り当てることができる最も詳細なレベルはキャンパス レベルです。7.0 以降では、このオプションはフロア レベルまで拡大されました。たとえば、floor1 を MSE 1 に、floor2 を MSE 2 に、floor3 を MSE 3 に割り当てることを選択できます。

ステップ 5　[Change MSE Assignment] をクリックします。

ステップ 6　マップと同期するモビリティ サービス エンジンを選択します。

（注）　ネットワーク設計には、キャンパス内のフロアや、複数のビルディングが含まれている大規模キャンパス（各ビルディングが異なるモビリティ サービス エンジンによりモニタされる）などがあります。このため、単一ネットワーク設計を複数のモビリティ サービス エンジンに割り当てる必要があります。

ステップ 7　[MSE Assignment] ダイアログボックスで次のいずれかをクリックします。

- [Save] : モビリティ サービス エンジン割り当てを保存します。次のメッセージが [Network Designs] ページの [Messages] 列に黄色の矢印アイコンとともに表示されます。

  「To be assigned - Please synchronize.」

- [Cancel] : Mobility Services Engine 割り当ての変更内容を取り消し、[Network Designs] ページに戻ります。

また、[Reset] をクリックすると、モビリティ サービス エンジンの割り当てが取り消されます。

（注）　ネットワーク設計には、キャンパス内のフロアや、複数のビルディングが含まれている大規模キャンパス（各ビルディングが異なるモビリティ サービス エンジンによりモニタされる）などがあります。このため、単一ネットワーク設計を複数のモビリティ サービス エンジンに割り当てる必要がある場合があります。

（注）　ネットワーク設計割り当てでは、同期対象のコントローラが自動的に選択されます。

ステップ 8　[Synchronize] をクリックし、モビリティ サービス エンジン データベースを更新します。

項目が同期されると、[Sync] に緑色の 2 つの矢印のアイコンが表示されます。

有線スイッチまたはイベント グループをモビリティ サービス エンジンに割り当てるときにも同じ手順を使用できます。モビリティ サービス エンジンへのコントローラの割り当ての詳細については、「コントローラとモビリティ サービス エンジンの同期」（P.16-953）を参照してください。

コントローラとモビリティ サービス エンジンの同期

サービス単位（CAS または wIPS）で MSE を任意のワイヤレス コントローラに割り当てることができます。

MSE サービスをワイヤレス コントローラに割り当てるには、次の手順に従います。

ステップ 1　同期ページで [Controllers] を選択します。

ステップ 2　モビリティ サービス エンジンに割り当てるコントローラを選択します。

ステップ 3　[Change MSE Assignment] をクリックします。

ステップ 4　コントローラと同期する必要があるモビリティ サービス エンジンを選択します。

ステップ 5　ダイアログボックスで次のいずれかをクリックします。

- [Save] : モビリティ サービス エンジン割り当て を保存します。[Controllers] ページの [Messages] 列に次のメッセージが表示されます。

  To be assigned - Please synchronize.

- [Cancel]：モビリティ サービス エンジン割り当ての変更内容を取り消し、[Controllers] ページに戻ります。

  また、[Reset] をクリックして黄色ボタンの割り当てを取り消すこともできます。

ステップ 6　[Synchronize] をクリックし、同期プロセスを実行します。

ステップ 7　モビリティ サービス エンジンが、選択されているサービスの各コントローラだけと通信していることを確認します。これは、ステータス ページの [NMSP status] リンクをクリックして確認できます。

（注）　コントローラの同期後、関連付けられているコントローラでタイムゾーンが設定されていることを確認します。詳細については、「コントローラのタイムゾーンの設定と確認」（P.16-955）を参照してください。

（注）　モビリティ サービス エンジンと同期するコントローラの名前は固有でなければなりません。同じ名前のコントローラが 2 つある場合は 1 つのコントローラだけが同期されます。

モビリティ サービス エンジンからネットワーク設計、コントローラ、有線スイッチ、またはイベント グループの割り当てを解除するには、次の手順に従います。

ステップ 1　該当するタブで 1 つ以上の要素をクリックし、[Change MSE Assignment] をクリックします。[Choose Mobility Services Engine] ダイアログボックスが表示されます。

ステップ 2　モビリティ サービス エンジンに要素を関連付けない場合は、[Mobility Services Engine] チェックボックスをオフにします。

ステップ 3　[Save] をクリックし、割り当ての変更内容を保存します。

ステップ 4　[Synchronize] をクリックします。[Sync Status] 列に 2 つの矢印のアイコンが表示されます。

サードパーティ要素の操作

要素を MSE と同期する場合、MSE にサードパーティ アプリケーションによって作成されたイベント グループがあることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。

要素を削除またはサード パーティ要素としてマークするには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

[Network Design] ページが表示されます。

[Network Design] ページで、左側のサイドバーのメニューから [Third Party Elements] を選択します。

[Third Party Elements] ページが表示されます。

ステップ 2　1 つ以上の要素を選択します。

ステップ 3　次のいずれかのボタンをクリックします。

- [Delete Event Groups]：選択されているイベント グループを削除します。

- [Mark as 3rd Party Event Group(s)]:選択されているイベント グループをサードパーティ イベント グループとしてマークします。

コントローラのタイムゾーンの設定と確認

リリース 4.2 以上のコントローラでは、モビリティ サービス エンジン（リリース 5.1 以上）がネットワークにインストールされている場合、2 つのシステム間で同期が適切に実行されるようにするため、コントローラでタイムゾーンを設定する必要があります。

コントローラのタイムゾーン システム時刻を設定する際の基準として、グリニッジ標準時（GMT）が使用されます。

コントローラの初期システム セットアップ時にタイムゾーンを自動的に設定するか、またはすでにネットワークに導入されているコントローラで手動でタイムゾーンを設定することができます。

ネットワークの既存のコントローラ上で CLI を使用して時刻とタイムゾーンを手動で設定するには、次の手順に従います。

ステップ 1　コントローラ上で現在の現地時間を GMT で設定するため、次のコマンドを入力します。

```
(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end
```

（注）　時刻を設定するときは、現在の現地時間を GMT で表した時間を 00:00 ～ 24:00 の範囲内の値として入力します。たとえば、米国の太平洋標準時（PST）で 8 AM の場合、PST タイムゾーンは GMT よりも 8 時間遅れているため、16:00（4 PM PST）と入力します。

ステップ 2　次のコマンドを入力し、現在の現地時間が GMT で表した時間として設定されていることを確認します。

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 16:00:02 2007
Timezone delta........................... 0:0
```

ステップ 3　次のコマンドを入力し、システムの現地時間のタイムゾーンを設定します。

（注）　タイムゾーンを設定するときは、GMT を基準とした現地時間の時間帯との時差を +/- を付けて入力します。たとえば米国（US）の太平洋標準時（PST）は、GMT（UTC）時間よりも 8 時間遅れています。したがって、-8 と入力します。

```
(Cisco Controller) >config time timezone -8
(Cisco Controller) >config end
```

ステップ 4　次のコマンドを入力し、コントローラで、GMT ではなく現地のタイムゾーンに基づいて現在の現地時間が表示されることを確認します。

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 08:00:26 2007
Timezone delta........................... -8:0
```

（注）　**show time** コマンドの time zone delta パラメータは、現地のタイムゾーンと GMT の時差（8 時間）を示します。設定前のこのパラメータの設定値は 0.0 です。

モビリティ サービス エンジン データベースのスマート同期の設定

Prime Infrastructure とモビリティ サービス エンジン データベースの手動同期では、ただちに同期が実行されます。ただし、将来のデプロイメントの変更（マップやアクセス ポイントの位置の変更など）が原因で、同期を再実行するまでは、ロケーションの計算やアセットの追跡が正しく行われないことがあります。

同期していない状態が発生しないようにするため、Prime Infrastructure を使用して同期を実行します。このポリシーにより、Prime Infrastructure とモビリティ サービス エンジン データベース間の同期が定期的に実行され、関連アラームがすべてクリアされます。

1 つ以上の同期コンポーネントに対する変更は、モビリティ サービス エンジンと自動的に同期されます。たとえば、アクセス ポイントが設置されているフロアを特定のモビリティ サービス エンジンと同期し、その後 1 つのアクセス ポイントが同じフロアの新しいロケーション、または別のフロア（モビリティ サービス エンジンと同期されるフロア）に移動すると、アクセス ポイントの変更後のロケーションが自動的に伝達されます。

Prime Infrastructure と MSE が同期されるようにするため、バックグラウンドでスマート同期が実行されます。

スマート同期を設定するには、次の手順に従います。

ステップ 1　[Administration] > [Background Tasks] の順に選択します。

[Background Tasks summary] ページが表示されます。

ステップ 2　[Mobility Service Synchronization] チェックボックスをオンにします。

ステップ 3　[Mobility Services Synchronization] ページが表示されます。

ステップ 4　モビリティ サービス エンジンが同期外れアラートを送信するように設定するには、[Out of Sync Alerts] グループ ボックスの [Enabled] チェックボックスをオンにします。

ステップ 5　スマート同期を有効にするには、[Smart Synchronization] の [Enabled] チェックボックスをオンにします。

（注）　スマート同期は、モビリティ サービス エンジンに割り当てられていない要素（ネットワーク設計、コントローラ、またはイベント グループ）には適用されません。ただし、これらの未割り当て要素に関する out-of-sync アラームは生成されます。スマート同期をこれらの要素に適用するには、これらの要素をモビリティ サービス エンジンに手動で割り当てる必要があります。

（注）　Prime Infrastructure にモビリティ サービス エンジンが追加されると、Prime Infrastructure のデータは常に、モビリティ サービス エンジンと同期するプライマリ コピーとして扱われます。モビリティ サービス エンジンに含まれているが、Prime Infrastructure には含まれていない同期対象のネットワーク設計、コントローラ、イベント グループ、および有線スイッチはすべて、モビリティ サービス エンジンから自動的に削除されます。

ステップ 6　スマート同期の実行間隔を分数単位で入力します。

デフォルトでは、スマート同期は無効化されています。

ステップ 7　[Submit] をクリックします。

スマート コントローラの割り当てと選択のシナリオの詳細については、「スマート コントローラの割り当てと選択のシナリオ」（P.16-957）を参照してください。

スマート コントローラの割り当てと選択のシナリオ

シナリオ 1

[Synchronization] ページの [Network Designs] セクションで、コントローラからのアクセス ポイントが 1 つ以上存在するフロアをモビリティ サービス エンジンと同期することを選択した場合、アクセス ポイントに接続しているコントローラが、CAS サービスのモビリティ サービス エンジンへの割り当て対象として自動的に選択されます。

シナリオ 2

コントローラからの 1 つ以上のアクセス ポイントが、モビリティ サービス エンジンと同期されるフロアに配置されている場合、アクセス ポイントに接続するコントローラは、CAS サービスの同じモビリティ サービス エンジンに自動的に割り当てられます。

シナリオ 3

アクセス ポイントがフロアに追加され、モビリティ サービス エンジンに割り当てられます。このアクセス ポイントをコントローラ A からコントローラ B に移動すると、コントローラ B がモビリティ サービス エンジンと自動的に同期されます。

シナリオ 4

モビリティ サービス エンジンと同期するフロアに配置されているすべてのアクセス ポイントが削除されると、そのコントローラがモビリティ サービス エンジン割り当てから削除されるか、または同期されなくなります。

Out-of-Sync アラーム

Out-of-Sync アラームは、シビリティが Minor（黄色）のアラームであり、次の条件に対して出されます。

- Prime Infrastructure で要素が変更された（自動同期ポリシーによりこれらの要素がプッシュされます）。
- モビリティ サービス エンジンで要素が変更された。
- コントローラ以外の要素がモビリティ サービス エンジン データベースに存在するが、Prime Infrastructure に存在しない。
- 要素がモビリティ サービス エンジンに割り当てられていない（自動同期ポリシーは適用されません）。

Out-of-Sync アラームは、次の条件が発生するとクリアされます。

- モビリティ サービス エンジンが削除される

（注） モビリティ サービス エンジンを削除すると、そのシステムの Out-of-Sync アラームも削除されます。また、使用可能な最後のモビリティ サービス エンジンを削除すると、「どのサーバにも割り当てられていない要素」のアラームも削除されます。

- 要素が手動または自動で同期される
- ユーザがアラームを手動でクリアする（ただしスケジュールされているタスクが次回実行されるときに、アラームが再び表示される可能性があります）

（注）　デフォルトでは、Out-of-Sync アラームは有効に設定されています。Prime Infrastructure でアラームを無効にするには、[Administration] > [Scheduled Tasks] の順に選択し、[Mobility Service Synchronization] をクリックします。[Auto Synchronization] チェックボックスをオフにし、[Submit] をクリックします。

モビリティ サービス エンジンの同期ステータスの表示

Prime Infrastructure で Synchronize Servers コマンドを使用して、ネットワーク設計、コントローラ、およびイベント グループとモビリティ サービス エンジンとの同期のステータスを表示できます。

同期ステータスを表示するには、次の手順に従います。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Network Designs]、[Controllers]、[Event Groups]、[Wired Switches]、[Third Party Elements]、または [Service Advertisements] を選択します。

要素ごとに、[Sync. Status] 列に、同期状態が表示されます。緑色の 2 つの矢印のアイコンは、対応する要素が指定サーバ（モビリティ サービス エンジンなど）と同期されていることを示します。灰色の 2 つの矢印と赤い円のアイコンは、対応する項目が指定のサーバと同期していないことを示します。

（注）　緑色の 2 つの矢印のアイコンは、コントローラの NMSP 接続状態は示しません。

[Monitor] > [Maps] > [System Campus] > *ビルディング*> *フロア*を選択して、同期ステータスを表示することもできます。

この*ビルディング*はキャンパス内のビルディング、*フロア*はキャンパス ビルディング内の特定のフロアです。

左側のサイドバーのメニューの [MSE Assignment] オプションに、フロアが現在割り当てられているモビリティ サービス エンジンが表示されます。このページからモビリティ サービス エンジン割り当てを変更できます。

同期履歴の表示

モビリティ サービス エンジンの過去 30 日間の同期履歴を表示できます。アラームが自動的にクリアされるため、これは特に自動同期が有効な場合に便利です。[Synchronization History] には、クリアされたアラームの要約が表示されます。

（注）　[Services] タブの [Synchronization History] ページは、リリース 7.3 の root 仮想ドメインでのみ使用可能です。

同期履歴を表示するには、[Services] > [Synchronization History] の順に選択し、列ヘッダーをクリックしてエントリをソートします。

通知統計情報の表示

特定のモビリティ サービス エンジンの通知統計情報を表示できます。特定のモビリティ サービス エンジンの通知統計情報を表示するには、次の手順に従います。

[Services] > [Mobility Services] > [*MSE-name*] > [Context Aware Service] > [Notification Statistics] の順に選択します。

MSE-name は、モビリティ サービス エンジンの名前です。

表 16-1 で、[Notification statistics] ページのフィールドについて説明します。

表 16-1　[Notification Statistics] のフィールド

フィールド	説明
Summary	
Destinations	宛先の名前。
Total	宛先の合計数。
Unreachable	到達不能宛先の数。
Notification Statistics Summary	
Destination Address	通知送信先の宛先アドレス。
Destination Port	通知送信先の宛先ポート。
Destination Type	宛先のタイプ。例：SOAP_XML
Destination Status	トラック定義のステータス。トラック通知ステータスは [Enabled] または [Disabled] のいずれかです。
Last Sent	最終通知が宛先デバイスに送信された日時。
Last Failed	通知が失敗した日時。
Track Definition (Status)	トラック定義情報。
Total Count	宛先に送信された通知の合計数。宛先デバイスの通知統計詳細情報を表示するには、カウント リンクをクリックします。

ハイ アベイラビリティの設定

モビリティ サービス エンジンは、複数のモビリティ アプリケーションをホストするプラットフォームです。アクティブな各 MSE は別の非アクティブ インスタンスによりバックアップされます。アクティブな MSE はプライマリ MSE、非アクティブな MSE はセカンダリ MSE と呼ばれます。

ハイ アベイラビリティ システムの主要なコンポーネントは、ヘルス モニタです。ヘルス モニタは、ハイ アベイラビリティ セットアップを設定、管理、モニタします。プライマリ MSE とセカンダリ MSE の間でハートビートが維持されます。ヘルス モニタは、データベースのセットアップ、ファイルのレプリケーション、アプリケーションのモニタリングを行います。プライマリ MSE で障害が発生し、セカンダリ MSE に切り替わると、プライマリ MSE の仮想アドレスが透過的に切り替わります。

ここでは、ハイ アベイラビリティ アーキテクチャの概要について説明します。

- アクティブな各プライマリ MSE は別の非アクティブ インスタンスによりバックアップされます。セカンダリ MSE の目的は、プライマリ MSE のアベイラビリティと状態をモニタすることです。セカンダリ MSE は、フェールオーバー手順の開始後にアクティブになります。
- フェールオーバー手順は手動または自動です。
- 1 つのセカンダリ MSE では 2 つのプライマリ MSE をサポートできます。
- 登録されているプライマリ MSE ごとに 1 つのソフトウェアおよびデータベース インスタンスが存在します。

（注）　[Services] タブの [high availability] は、リリース 7.3 の root 仮想ドメインでのみ使用可能です。

この項の内容は次のとおりです。

組み合わせ表

表 16-2 は組み合わせ表情報です。

表 16-2　組み合わせ表

	セカンダリ サーバ タイプ						
プライマリ サーバ タイプ		3310	3355	VA-2	VA-3	VA-4	VA-5
	3310	Y	Y	N	N	N	N
	3355	N	Y	N	N	N	N
	VA-2	N	N	Y	Y	Y	Y
	VA-3	N	N	N	Y	Y	Y
	VA-4	N	N	N	N	Y	Y
	VA-5	N	N	N	N	N	Y

ハイ アベイラビリティのガイドラインと制約事項

- ヘルス モニタ IP と仮想 IP の両方に Cisco Prime Infrastructure からアクセスできるようにする必要があります。

- ヘルス モニタ IP と仮想 IP は常に異なる IP でなければなりません。ヘルス モニタと仮想インターフェイスは、同じインターフェイス上にあっても別のインターフェイス上にあってもかまいません。
- 手動フェールオーバーと自動フェールオーバーのいずれかを使用できます。フェールオーバーは、一時的なものであると見なす必要があります。故障した MSE をできるだけ早く復旧して、フェールバックを再開する必要があります。故障した MSE の復旧に時間がかかるほど、セカンダリ MSE を共有する他の MSE をフェールオーバー サポートなしで稼働する時間が長くなります。
- 手動フェールバックと自動フェールバックのいずれかを使用できます。
- プライマリ MSE とセカンダリ MSE は、同じソフトウェア バージョンを実行する必要があります。
- WAN 上のハイ アベイラビリティはサポートされません。
- LAN 上のハイ アベイラビリティは、プライマリ MSE とセカンダリ MSE の両方が同じサブネット内にある場合に限りサポートされます。
- プライマリとセカンダリの MSE が通信するポートを開ける（ネットワーク ファイアウォール、アプリケーション ファイアウェイ、ゲートウェイなどでブロックしない）必要があります。

ハイ アベイラビリティのフェールオーバー シナリオ

プライマリ MSE で障害が検出されると、次のイベントが発生します。

（注）　1 つのセカンダリ MSE が複数のプライマリ MSE をバックアップできます。

- セカンダリ MSE のヘルス モニタにより、プライマリ MSE が機能していないこと（ハードウェア障害、ネットワーク障害など）が確認されます。
- 自動フェールオーバーが有効に設定されている場合、セカンダリ MSE がただちに起動し、プライマリ MSE の該当するデータベースを使用します。自動フェールオーバーが無効にされている場合は、フェールオーバーを手動で開始するかどうかを確認する電子メールが管理者に送信されます。
- 手動フェールオーバーが設定されていると、電子メールが MSE アラーム用に設定されている場合にのみ電子メールが送信されます。手動フェールオーバーが設定されていて、呼び出されない場合、フェールバックの必要はありません。
- フェールバックが呼び出され、プライマリ MSE がすべての操作を実行するようになります。
- フェールオーバー操作の結果はヘルス モニタ UI でイベントとして示され、クリティカル アラームが管理者に送信されます。

フェールバック

セカンダリ MSE がすでにプライマリ MSE をフェールオーバーしている場合、プライマリ MSE が通常の状態に戻ると、フェールバックを呼び出すことができます。

フェールバックが発生するのは、セカンダリ MSE がプライマリ インスタンスに対して次のいずれかの状態である場合だけです。

- セカンダリ MSE が実際にプライマリ MSE をフェールオーバーしている。
- 手動でのフェールオーバーが設定されているが、管理者が呼び出さなかった。
- プライマリ MSE で障害が発生したが、エラーが検出されたか、またはセカンダリ MSE が別のプライマリ MSE をフェールオーバーしていることが原因で、セカンダリ MSE が引き継ぐことができない。
- フェールバックは、障害が発生したプライマリ MSE を管理者が起動する場合にだけ行われます。

HA ライセンス

MSE HA システムをセットアップする場合、別途ライセンスは必要ありません。仮想アプライアンス セカンダリにはアクティベーション ライセンスは必要ありません。

MSE でのハイ アベイラビリティの設定

MSE でハイ アベイラビリティを設定するには、次の 2 つの操作を行う必要があります。

- MSE ソフトウェアのインストール中に、コマンドライン クライアントを使用して特定の設定を行う必要があります。
- Prime Infrastructure UI からプライマリ MSE とセカンダリ MSE を組み合わせます。

（注） ハイ アベイラビリティ サポートを使用しない場合、および古いリリースからのアップグレードを実行している場合は、引き続き MSE の古い IP アドレスを使用してください。ハイ アベイラビリティをセットアップするには、ヘルス モニタの IP アドレスを設定する必要があります。したがって、ヘルス モニタが仮想 IP アドレスになります。

（注） デフォルトでは、すべての MSE がプライマリとして設定されます。

プライマリ MSE でハイ アベイラビリティを設定するには、次の手順に従います。

ステップ 1　プライマリとセカンダリの間のネットワーク接続が機能しており、すべての必要なポートが開いていることを確認します。

ステップ 2　正しいバージョンの MSE をプライマリ MSE 上にインストールします。

ステップ 3　他のプライマリ MSE 上およびセカンダリ MSE 上でロードされているリリース バージョンと同じ MSE リリース バージョンが、新しいプライマリ MSE 上にもロードされていることを確認します。

ステップ 4　プライマリ MSE で次のコマンドを入力します。

```
/opt/mse/setup/setup.sh
----------------------------------------------------------------
Welcome to the appliance setup.
Please enter the requested information.  At any prompt,
enter ^ to go back to the previous prompt. You may exit at
any time by typing <Ctrl+C>.
You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.
Changes made will only be applied to the system once all the
information is entered and verified.
----------------------------------------------------------------
```

ステップ 5　ホスト名を設定します。

```
Current hostname=[mse]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

ホスト名は、ネットワーク上のデバイスを識別できる一意の名前にしてください。ホスト名は、文字で開始し、文字または数字で終了し、文字、数字、およびダッシュだけを含みます。

ステップ 6　ドメイン名を設定します。

デバイスが属するネットワーク ドメインのドメイン名を入力します。ドメイン名は、文字で開始し、*.com* などの有効なドメイン名サフィックスで終了します。ドメイン名には、文字、数字、ダッシュ、ピリオドを使用できます。

```
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 7　HA ロールを設定します。

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary):
Select role [1 for Primary, 2 for Secondary] [1]: 1
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:eth0
----------------------------------------------------------------------
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
----------------------------------------------------------------------
```

ステップ 8　イーサネット インターフェイス パラメータを設定します。

```
Select direct connect interface [eth0/eth1/none] [none]: eth0
Enter a Virtual IP address for first this primary MSE server:
Enter Virtual IP address [172.31.255.255]:
Enter the network mask for IP address 172.31.255.255.
Enter network mask [255.255.255.0]:
Current IP address=[172.31.255.255]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[172.31.255.256
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 9　「eth1」インターフェイス パラメータの入力を求められた場合、Skip と入力して次の手順に進みます。2 つめの NIC は操作に必要ではありません。

```
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

セカンダリ MSE を設定するには、ステップ 10 ～ステップ 13 に従います。

ステップ 10　セカンダリ MSE のホスト名を設定します。

```
Current hostname=[]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 11　ドメイン名を設定します。

```
Current domain=
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 12　HA ロールを設定します。

```
Current role=[Primary]
```

```
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 2
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:[eth0/eth1]
------------------------------------------------------------------
Direct connect configuration facilitates use of a direct cable connection between the
primary and secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure
detection times.
Please choose a network interface that you wish to use for direct connect. You should
appropriately configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
------------------------------------------------------------------
```

ステップ 13　イーサネット インターフェイス パラメータを設定します。

```
Select direct connect interface [eth0/eth1/none] [none]: eth1
Enter a Virtual IP address for first this primary MSE server
Enter Virtual IP address [172.19.35.61]:
Enter the network mask for IP address 172.19.35.61:
Enter network mask [255.255.254.0]:
Current IP address=[172.19.35.127]
Current eth0 netmask=[255.255.254.0]
Current gateway address=[172.19.34.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 14　プライマリ MSE とセカンダリ MSE の両方を設定したら、Prime Infrastructure UI を使用してプライマリ MSE とセカンダリ MSE の組み合わせを設定する必要があります。

ステップ 15　プライマリ MSE が適切に追加されたら、[Services] > [High Availability] の順に選択するか、または [Services] > [Mobility Services Engine] ページを選択してこのページでプライマリ MSE デバイスをクリックし、左側のサイドバーのメニューから [HA Configuration] > [Service High Availability] の順に選択します。

[HA Configuration] ページが表示されます。

ステップ 16　プライマリ MSE とペアにするセカンダリ デバイスの名前を入力します。

ステップ 17　セカンダリ IP アドレス（セカンダリ MSE のヘルス モニタ IP アドレス）を入力します。

ステップ 18　セカンダリのパスワードを入力します。これは、MSE 上で設定されている Prime Infrastructure 通信パスワードです。

ステップ 19　フェールオーバー タイプを指定します。[Failover Type] ドロップダウン リストから [Manual] または [Automatic] を選択できます。10 秒後にシステムがフェールオーバーします。セカンダリ サーバは、プライマリ サーバからの次のハートビートを最大 10 秒間待機します。10 秒以内にハートビートを受信しないと、失敗が宣言されます。

ステップ 20　[Failback Type] ドロップダウン リストから [Manual] または [Automatic] を選択して、フェールバック タイプを指定します。

ステップ 21　[Long Failover Wait] に秒単位で値を指定します。

10 秒後にシステムがフェールオーバーします。最大フェールオーバー待機時間は 2 秒です。

ステップ 22　[Save] をクリックします。

ペアリングと同期が自動的に行われます。

ステップ 23　プライマリ MSE からハートビートを受信しているかどうかを確認するには、[Services] > [Mobility Services Engine] の順に選択するか、[Device Name] をクリックして設定されているパラメータを表示します。

ステップ 24　左側のサイドバーのメニューから [HA Configuration] > [Service High Availability] の順に選択します。

プライマリ MSE からハートビートを受信しているかどうかを確認します。

ハイ アベイラビリティについて設定されているパラメータの表示

ハイ アベイラビリティについて設定されているパラメータを表示するには、次の手順に従います。

ステップ 1　[Services] > [High Availability] の順に選択します。

ステップ 2　[Device Name] をクリックして、設定されているパラメータを表示します。

[HA Configuration] ページが表示されます。

ステップ 3　左側のサイドバー メニューから [Services High Availability] > [HA Configuration] の順に選択します。[HA Configuration] ページには次の情報が表示されます。

- Primary Health Monitor IP
- Secondary Device Name
- Secondary IP Address
- Secondary Password
- Failover Type
- Failback Type
- Long Failover Wait

ハイ アベイラビリティ ステータスの表示

ハイ アベイラビリティ ステータスを表示するには、次の手順に従います。

ステップ 1　[Services] > [High Availability] の順に選択します。

ステップ 2　[Device Name] をクリックして、該当するステータスを表示します。

[HA Configuration] ページが表示されます。

ステップ 3　左側のサイドバー メニューから [Services High Availability] > [HA Status] の順に選択します。[HA Configuration] ページには次の情報が表示されます。

- Current high Availability Status
  - [Status] : プライマリ MSE インスタンスとセカンダリ MSE インスタンスが正しく同期されているかどうかを示します。
  - [Heartbeats] : プライマリ MSE からハートビートを受信しているかどうかを示します
  - [Data Replication] : プライマリ データベースとセカンダリ データベース間でデータ レプリケーションが実行されているかどうかを示します。

  - [Mean Heartbeat Response Time]：プライマリ MSE インスタンスとセカンダリ MSE インスタンス間での平均ハートビート応答時間を示します。
- [Event Log]：MSE により生成されるすべてのイベントを表示します。最新 20 イベントが表示されます。

モビリティ サービス エンジンのシステム プロパティの管理

Prime Infrastructure を使用して、モビリティ サービス エンジンのシステム プロパティを管理できます。この項では、モビリティ サービス エンジンの各種システム プロパティについて説明します。内容は次のとおりです。

モビリティ サービス エンジンの一般プロパティの編集

Prime Infrastructure を使用して、Prime Infrastructure データベースに登録されているモビリティ サービス エンジンの一般プロパティを編集できます。一般プロパティには、連絡担当者名、ユーザ名、パスワード、HTTP などがあります。

モビリティ サービス エンジンの一般プロパティを編集するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択し、[Mobility Services] ページを表示します。

ステップ 2　編集するモビリティ サービス エンジンの名前をクリックします。[General Properties] ページが表示されます（[General] タブと [Performance] タブがあります）。

[General] タブには次の読み取り専用サーバ情報が表示されます。

- デバイス名
- デバイス タイプ
- デバイス UDI

（注）　ライセンスでは、デバイス UDI ストリングは二重引用符で囲まれています（ストリングの末尾にスペースがある場合はスペースも含まれます）。コピー ペースト機能を使用して二重引用符を除外します。

- バージョン

- 開始時刻
- IP アドレス

ステップ 3　[General Properties] ページで以下のサーバ詳細情報を必要に応じて変更します。

- [Contact Name] : モビリティ サービスの連絡先の名前を入力します。
- [Username] : モビリティ サービスを管理する Prime Infrastructure サーバのログイン ユーザ名を入力します。
- [Password] : モビリティ サービスを管理する Prime Infrastructure サーバのログイン パスワードを入力します。
- [HTTP] : HTTP を有効にするには、[HTTP enable] チェックボックスをオンにします。

（注）　デフォルト以外のポートを使用しているか、または HTTPS がオンになっている場合、コマンドを使用して正しい情報を受け渡す必要があります。たとえば *getserverinfo* に *-port <<port>> -protocol <<HTTP/HTTPS>>* を指定する必要があります。同様にサーバを停止するには、*stoplocserver - port <<port>> -protocol <HTTP/HTTPS>>* を使用します。

- [Legacy Port] : 8001
- [Legacy HTTPS] : レガシー HTTPS を有効にするには、このチェックボックスをオンにします。
- [Delete synchronized service assignments and enable synchronization] : モビリティ サービス エンジンからすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。このオプションが表示されるのは、モビリティ サービス エンジンを追加するときに [Delete synchronized service assignments] チェックボックスをオフにした場合のみです。

（注）　Prime Infrastructure は、モビリティ サービス エンジンとの通信に HTTPS を常に使用します。

（注）　リリース 6.0 の MSE で使用される TCP ポートは、tcp 22（MSE SSH ポート）、tcp 80（MSE HTTP ポート）、tcp 443（MSE HTTPS ポート）、tcp 1411（AeroScout）、tcp 1999（AeroScout 内部ポート）、tcp 4096（AeroScout 通知ポート）、tcp 5900X（AeroScout）（X は 1 ～ 10）、tcp 8001（レガシー ポート）です。ロケーション API に使用されます。

（注）　リリース 6.0 の MSE で使用される UDP ポートは、udp 123（NTPD ポート、NTP 設定の後に開きます）、udp 162（AeroScout SNMP）、udp/tcp 4000X（AeroScout プロキシ、X は 1 ～ 5）、udp 12091（AeroScout デバイス）（TDOA Wi-Fi レシーバ、チョークポイント）、udp 12092（AeroScout デバイス）（TDOA Wi-Fi レシーバ、チョークポイント）、udp 32768（ロケーション内部ポート）、udp 32769（AeroScout 内部ポート）、udp 37008（AeroScout 内部ポート）です。

ステップ 4　[Mobility Services] ダイアログボックスで [Admin Status] チェックボックスをオンにし、該当する Context Aware Service または wIPS を有効にします。

[Context Aware Service] を選択する場合は、ロケーション計算を実行するロケーション エンジンを選択する必要があります。

次のいずれかを選択します。

- **Cisco Tag Engine**

または

- **Partner Tag Engine**

（注）　MSE 6.0 では、複数のサービス（CAS と wIPS）を同時に有効にできます。6.0 よりも前のバージョンでは、Mobility Services Engine では一度に 1 つのアクティブ サービスだけがサポートされていました。

[Mobility Services] ダイアログボックスには次の情報が表示されます。

- サービス名
- サービス バージョン
- サービス ステータス
- ライセンス タイプ

（注）　モビリティ サービス エンジンのライセンスの詳細については、[Click here] リンクを使用してください。

ステップ 5　[Save] をクリックして Prime Infrastructure とモビリティ サービス エンジン データベースを更新します。

（注）　モビリティ サービス エンジンのライセンスの詳細については、[Click here] リンクを使用してください。

ステップ 6　[Performance] タブをクリックし、CPU とメモリの使用率のグラフを表示します。

モビリティ サービス エンジンの NMSP パラメータの編集

ネットワーク モビリティ サービス プロトコル（NMSP）は、モビリティ サービスとコントローラ間の通信を管理します。モバイル サービスとコントローラの間でのテレメトリ、緊急事態、RSSI の値の転送はこのプロトコルにより管理されます。

（注）
- リリース 3.0 ～ 7.0.105.0 でインストールされたモビリティ サービスでは、NMSP パラメータがサポートされています。7.0.105.0 より後のリリースではサポートされていません。
- NMSP は、リリース 3.0 で導入された LOCP の条件に置き換わるものです。
- テレメトリおよび緊急事態情報は、コントローラおよびリリース 4.1 ソフトウェアをインストールした Prime Infrastructure、リリース 3.0 以上のソフトウェアを実行するモビリティ サービス エンジンでのみ表示されます。
- コントローラとモビリティ サービスとの通信には、TCP ポート 16113 が使用されます。コントローラとモビリティ サービスの間にファイアウォールがある場合は、NMSP を機能させるにはこのポートが開いている（ブロックされていない）ことが必要です。

Prime Infrastructure の [NMSP Parameters] ダイアログボックスでは、エコー間隔、ネイバー デッド間隔、応答期間、再送信期間などの NMSP パラメータを変更できます。

NMSP パラメータを設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　プロパティを編集するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから [System] > [NMSP Parameters] の順に選択します。

ステップ 4　必要に応じて、NMSP パラメータを変更します。

（注）　ネットワークの応答が遅くなっている場合や大幅な遅延が発生している場合を除き、デフォルトのパラメータ値を変更しないでおくことを推奨します。

NMSP パラメータには、次のものがあります。

- [Echo Interval]：モビリティ サービスからコントローラにエコー要求を送信する頻度を定義します。デフォルト値は 15 秒です。有効値の範囲は 1 ～ 120 秒です。

  （注）　ネットワークの応答が遅くなっている場合は、[Echo Interval]、[Neighbor Dead Interval]、[Response Timeout] の値を大きくし、エコー確認の失敗回数を制限できます。

- [Neighbor Dead Interval]：モビリティ サービス エンジンがネイバー デッドを宣言するまでに、コントローラから正常なエコー応答の受信を待機する時間（秒数）です。この時間は、エコー要求が送信された時点から始まります。

  デフォルト値は 30 秒です。有効値の範囲は 1 ～ 240 秒です。

  （注）　この値はエコー間隔値の 2 倍以上でなければなりません。

- [Response Timeout]：モビリティ サービスが、保留要求をタイムアウトと見なすまでに待機する時間を示します。デフォルト値は 1 秒です。最小値は 1 です。最大値はありません。
- [Retransmit Interval]：モビリティ サービスが、応答タイムアウトの通知を受け取ってから要求再送信を開始するまで待機する時間です。デフォルト設定は 3 秒です。有効値の範囲は 1 ～ 120 秒です。
- [Maximum Retransmits]：要求に対する応答がない場合に実行される再送信の最大回数を定義します。デフォルト設定は 5 です。有効な最小値は 0 です。最大値はありません。

ステップ 5　[Save] をクリックして Prime Infrastructure とモビリティ サービス エンジン データベースを更新します。

モビリティ サービス エンジンのアクティブ セッションの詳細の表示

Prime Infrastructure の [Active Sessions] ダイアログボックスでは、モビリティ サービス エンジンのアクティブなユーザ セッションを表示できます。

アクティブなユーザ セッションを表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　モビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Active Sessions] の順に選択します。

Prime Infrastructure により、アクティブなモビリティ サービス セッションのリストが表示されます。Prime Infrastructure は各セッションに関する次の情報を表示します。

- セッション ID
- モビリティ サービス アクセス元の IP アドレス
- 接続ユーザのユーザ名
- セッションが開始された日時
- モビリティ サービスが最後にアクセスされた日時
- 最終アクセス以降セッションがアイドルになっていた期間

モビリティ サービス エンジンのトラップ宛先の表示と追加

Prime Infrastructure の [Trap Destinations] ダイアログボックスでは、モビリティ サービス エンジンにより生成される SNMP トラップを受信する Prime Infrastructure または Cisco Security Monitoring, Analysis, and Response System（CS-MARS）ネットワーク管理プラットフォームを指定できます。

モビリティ サービス エンジンのトラップ宛先を表示または管理するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　モビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Trap Destinations] の順に選択します。

Prime Infrastructure は現在のトラップ宛先のリストを表示します。これには、次の情報が含まれます。

- IP アドレス
- ポート番号
- コミュニティ
- 宛先タイプ
- SNMP バージョン

[Select a command] ドロップダウン リストを使用してトラップ宛先を追加または削除します。

トラップ宛先を追加するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　モビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Trap Destinations] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Trap Destination] を選択します。

[New Trap Destination] ページが表示されます。

ステップ 5　次の詳細情報を入力します（表 16-3 を参照）。

表 16-3　[Add Trap Destination] ページ

フィールド	説明
IP Address	トラップ宛先の IP アドレス。
Port Number	トラップ宛先のポート番号。デフォルト ポート番号は、162 です。
Destination Type	このフィールドは編集できず、値 [Other] が表示されます。
SNMP Version	[v2c] または [v3] を選択します
SNMP バージョンとして v3 を選択した場合にだけ表示されるフィールドを以下に示します。	
User Name	SNMP バージョン 3 のユーザ名。
Security Name	SNMP バージョン 3 のセキュリティ名。
Authentication Type	次のいずれかを選択します。 HMAC-MD5 HMAC-SHA
Authentication Password	SNMP バージョン 3 の認証パスワード。
Privacy Type	次のいずれかを選択します。 CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	SNMP バージョン 3 のプライバシー パスワード。

ステップ 6　[Save] をクリックして変更内容を保存するか、または [Cancel] をクリックして変更内容を取り消します。

モビリティ サービス エンジンの詳細パラメータの編集

Prime Infrastructure [Advanced Parameters] ダイアログ ボックスでは、イベントを保持する日数、セッション タイムアウト値、および不明データのクリーンアップ間隔を設定すること、および詳細デバッグを有効または無効にすることができます。

（注）　Prime Infrastructure を使用してモビリティ サービス エンジンのトラブルシューティング パラメータを変更できます。

モビリティ サービス エンジンの詳細パラメータを編集するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Advanced Parameters] の順に選択します。

ステップ 4　必要に応じて詳細パラメータを確認または変更します。

- General Information
- Advanced Parameters

注意　詳細デバッグを実行するとモビリティ サービスの処理速度が低下するため、詳細デバッグは Cisco TAC 担当者の指示がある場合に限り有効にしてください。

  - [Number of Days to keep Events]：ログを維持する日数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。
  - [Session Timeout]：セッションがタイムアウトになるまでの分数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。現時点では、このオプションは淡色表示されます。
- Cisco UDI
  - [Product Identifier (PID)]：モビリティ サービス エンジンの製品 ID。
  - [Version Identifier (VID)]：モビリティ サービス エンジンのバージョン番号。
  - [Serial Number (SN)]：モビリティ サービス エンジンのシリアル番号。
- Advanced Commands
  - [Reboot Hardware]：モビリティ サービス ハードウェアをリブートする場合にクリックします。詳細については、「モビリティ サービス エンジン ハードウェアのリブート」（P.16-972）を参照してください。
  - [Shutdown Hardware]：モビリティ サービス ハードウェアをオフにする場合にクリックします。詳細については、「Mobility Services Engine ハードウェアのシャットダウン」（P.16-973）を参照してください。
  - [Clear Database]：モビリティ サービス データベースをクリアする場合にクリックします。詳細については、「モビリティ サービス エンジン データベースのクリア」（P.16-973）を参照してください。Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除するには、[Retain current service assignments in the Prime Infrastructure] チェックボックスをオフにします。[Services] > [Synchronize Services] ページからリソースを再割り当てする必要があります。このオプションは、デフォルトで選択されます。

ステップ 5　[Save] をクリックして Prime Infrastructure とモビリティ サービス エンジン データベースを更新します。

モビリティ サービス エンジン ハードウェアのリブート

モビリティ サービス エンジンを再起動する必要がある場合は、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　リブートするモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] をクリックします。

ステップ 4　[Advanced Parameters] をクリックします。

ステップ 5　[Advanced Commands] ダイアログボックスで [Reboot Hardware] をクリックします。

ステップ 6　[OK] をクリックし、モビリティ サービス エンジン ハードウェアをリブートすることを確定します。

リブート プロセスには数分間かかることがあります。

Mobility Services Engine ハードウェアのシャットダウン

モビリティ サービス エンジンをシャットダウンする必要がある場合は、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。
ステップ 2　シャットダウンするモビリティ サービス エンジンの名前をクリックします。
ステップ 3　[System] をクリックします。
ステップ 4　[Advanced Parameters] をクリックします。
ステップ 5　[Advanced Commands] ダイアログボックスで [Shutdown Hardware] をクリックします。
ステップ 6　[OK] をクリックし、モビリティ サービス エンジンをシャットダウンすることを確定します。

モビリティ サービス エンジン データベースのクリア

モビリティ サービス エンジン設定をクリアし、出荷時の初期状態に戻すには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。
ステップ 2　設定するモビリティ サービス エンジンの名前をクリックします。
ステップ 3　[System] をクリックします。
ステップ 4　[Advanced Parameters] をクリックします。
ステップ 5　Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除するには、[Advanced Commands] ダイアログボックスの [Retain current service assignments in the Prime Infrastructure] チェックボックスをオフにします。

[Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。デフォルトでは、このオプションが選択されています。

ステップ 6　[Advanced Commands] ダイアログボックスで [Clear Database] をクリックします。
ステップ 7　[OK] をクリックし、モビリティ サービス エンジン データベースをクリアします。

ログの操作

この項では、ロギング オプションの設定方法と、ログ ファイルのダウンロード方法を説明します。内容は次のとおりです。

- 「ロギング オプションの設定」（P.16-973）
- 「モビリティ サービス エンジン ログ ファイルのダウンロード」（P.16-975）

ロギング オプションの設定

Prime Infrastructure を使用して、ログに記録するメッセージのタイプとログ レベルを指定できます。

ロギング オプションを設定するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　設定するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[System] > [Logs] を選択します。選択されているモビリティ サービス エンジンの詳細パラメータが表示されます。

ステップ 4　[Logging Level] ドロップダウン リストから適切なオプションを選択します。

ロギング オプションは、[Off]、[Error]、[Information]、および [Trace] の 4 つです。

ログ レベルを [Error] またはこれよりも前のレベルに設定した場合、ログ レコードはすべて、新しいエラー ログ ファイル locserver-error-%u-%g.log に記録されます。これは、ロケーション サーバの locserver-%u-%g.log ログ ファイルとともに維持される追加のログ ファイルです。このエラー ログ ファイルには、[Error] レベルのログとそのコンテキスト情報が記録されます。コンテキスト情報には、当該エラーよりも前の 25 ログ レコードが含まれています。最大 10 のエラー ログ ファイルを維持できます。各ログ ファイルの最大許容サイズは 10 MB です。

注意　[Error] と [Trace] は、Cisco TAC 担当者の指示がある場合にのみ使用してください。

ステップ 5　イベントのロギングを開始する各要素の横の [Enabled] チェックボックスをオンにします。

ステップ 6　[Advanced Parameters] ダイアログボックスの [Enable] チェックボックスをオンにし、詳細デバッグを有効にします。デフォルトでは、このオプションは無効になっています。

ステップ 7　サーバからログ ファイルをダウンロードするには、[Download Logs] をクリックします。詳細については、「モビリティ サービス エンジン ログ ファイルのダウンロード」（P.16-975）を参照してください。

ステップ 8　[Log File] グループ ボックスに、以下の情報を入力します。

- モビリティ サービス エンジンで維持するログ ファイルの数。モビリティ サービス エンジンで維持できるログ ファイルの数は 5 ～ 20 です。
- 最大ログ ファイル サイズ（MB 単位）。ログ ファイルのサイズは 10 ～ 50 MB です。

ステップ 9　[MAC Address Based Logging] グループ ボックスで、次の手順を実行します。

- [Enable] チェックボックスをオンにし、MAC アドレス ロギングを有効にします。デフォルトでは、このオプションは無効になっています。
- ロギングを有効にする 1 つ以上の MAC アドレスを追加します。また、以前に追加した MAC アドレスを削除できます。削除するには、リストから MAC アドレスを選択して [Remove] をクリックします。

MAC アドレスに基づくロギングの詳細については、「MAC アドレスに基づくロギング」（P.16-974）を参照してください。

ステップ 10　[Save] をクリックして変更を適用します。

MAC アドレスに基づくロギング

この機能では、指定されている MAC アドレスのエンティティ固有のログ ファイルを作成できます。ログ ファイルは次に示すパスの locserver ディレクトリ内に作成されます。

/opt/mse/logs/locserver

一度に最大で 5 つの MAC アドレスをログに記録できます。MAC アドレス aa:bb:cc:dd:ee:ff のログ ファイルの形式は macaddress-debug-aa-bb-cc-dd-ee-ff.log です。

1 つの MAC アドレスに対して最大で 2 つのログ ファイルを作成できます。2 つのログ ファイルのうち、1 つがメインのログファイルであり、もう 1 つがバックアップまたはロールオーバー ログ ファイルです。

MAC ログ ファイルの最小サイズは 10 MB です。最大許容サイズは、MAC アドレスあたり 20 MB です。MAC ログ ファイルの未更新時間が 24 を超えると、この MAC ログ ファイルはプルーニングされます。

モビリティ サービス エンジン ログ ファイルのダウンロード

モビリティ サービス エンジン ログ ファイルを解析する必要がある場合は、Prime Infrastructure を使用してログ ファイルをシステムにダウンロードできます。Prime Infrastructure ではログ ファイルを含む .zip ファイルがダウンロードされます。

ログ ファイルが含まれている .zip ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　ステータスを表示するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[Logs] を選択します。

ステップ 4　[Download Logs] をクリックします。

ステップ 5　[File Download] ダイアログボックスの指示に従い、ファイルを開くかまたは .zip ファイルをシステムに保存します。

モビリティ サービス エンジンのユーザ アカウントおよびグループ アカウントの管理

この項では、モビリティ サービス エンジンでユーザとグループを設定および管理する方法を説明します。

この項では、モビリティ サービス エンジンのユーザの追加、削除、編集方法を説明します。内容は次のとおりです。

- 「モビリティ サービス エンジンのユーザの追加」（P.16-976）
- 「ユーザの削除」（P.16-976）
- 「ユーザ プロパティの編集」（P.16-976）

（注）　各ユーザのアクティブ セッションの表示については、「モビリティ サービス エンジンのアクティブ セッションの詳細の表示」（P.16-969）を参照してください。

- グループ アカウントの管理：この項では、モビリティ サービス エンジンのユーザ グループの追加、削除、編集方法を説明します。内容は次のとおりです。
  - 「ユーザ グループの追加」（P.16-977）
  - 「ユーザ グループの削除」（P.16-977）
  - 「グループ ユーザ権限の編集」（P.16-978）

モビリティ サービス エンジンのユーザの追加

モビリティ サービス エンジンにユーザを追加するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。
ステップ 2　編集するモビリティ サービス エンジンのデバイス名をクリックします。
ステップ 3　左側のサイドバー メニューから [Systems] > [Accounts] > [Users] の順に選択します。
ステップ 4　[Select a command] ドロップダウン リストから、[Add User] を選択します。
ステップ 5　[Go] をクリックします。
ステップ 6　[Username] テキストボックスにユーザ名を入力します。
ステップ 7　[Password] テキストボックスにパスワードを入力します。
ステップ 8　[Group Name] テキストボックスにユーザが属するグループの名前を入力します。
ステップ 9　[Permission] ドロップダウン リストから権限レベルを選択します。

選択できる権限レベルには、[Read Access]、[Write Access]、および [Full Access]（Prime Infrastructure がモビリティ サービス エンジンにアクセスするために必要な権限）の 3 つがあります。

注意　グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限が付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジンを設定できなくなります。

ステップ 10　[Save] をクリックして新規ユーザをモビリティ サービス エンジンに追加します。

ユーザの削除

モビリティ サービス エンジンからユーザを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services] の順に選択します。
ステップ 2　編集するモビリティ サービス エンジンのデバイス名をクリックします。
ステップ 3　左側のサイドバー メニューから [Systems] > [Accounts] > [Users] の順に選択します。
ステップ 4　削除するユーザのチェックボックスをオンにします。
ステップ 5　[Select a command] ドロップダウン リストから [Delete User] を選択します。
ステップ 6　[Go] をクリックします。
ステップ 7　[OK] をクリックして、選択したユーザを削除することを確定します。

ユーザ プロパティの編集

ユーザ プロパティを変更するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。
ステップ 2　編集するモビリティ サービス エンジンのデバイス名をクリックします。
ステップ 3　左側のサイドバー メニューから [Systems] > [Accounts] > [Users] の順に選択します。

ステップ 4　編集するユーザのユーザ名をクリックします。

ステップ 5　[Password]、[Group Name]、および [Permission] テキストボックスで必要な変更を行います。

ステップ 6　[Save] をクリックして変更を適用します。

ユーザ グループの追加

モビリティ サービス エンジンにユーザ グループを追加するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　編集するモビリティ サービス エンジンのデバイス名をクリックします。

ステップ 3　左側のサイドバー メニューから [Systems] > [Accounts] > [Groups] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add Group] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[Group Name] テキストボックスにグループ名を入力します。

ステップ 7　[Permission] ドロップダウン リストから権限レベルを選択します。

次の 3 つの権限レベルのいずれかを選択できます。

- **Read Access**
- **Write Access**
- **Full Access**（Prime Infrastructure がモビリティ サービス エンジンにアクセスするために必要な権限）

ステップ 8　[Save] をクリックして新規グループをモビリティ サービス エンジンに追加します。

注意　グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフルアクセス権限を付与し、読み取りアクセス権限が付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジン設定を変更できなくなります。

ユーザ グループの削除

モビリティ サービス エンジンからユーザ グループを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　編集するモビリティ サービス エンジンのデバイス名をクリックします。

ステップ 3　左側のサイドバー メニューから [Systems] > [Accounts] > [Groups] の順に選択します。

ステップ 4　削除するグループのチェックボックスをオンにします。

ステップ 5　[Select a command] ドロップダウン リストから [Delete Group] を選択します。

ステップ 6　[Go] をクリックします。

ステップ 7　[OK] をクリックして、選択したユーザを削除することを確定します。

グループ ユーザ権限の編集

ユーザ グループの権限を変更するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　編集するモビリティ サービス エンジンのデバイス名をクリックします。

ステップ 3　左側のサイドバー メニューから [Systems] > [Accounts] > [Groups] の順に選択します。

ステップ 4　編集するグループのグループ名をクリックします。

ステップ 5　[Permission] ドロップダウン リストから権限レベルを選択します。

ステップ 6　[Save] をクリックして変更を適用します。

注意　グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限のみ付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジンを設定できなくなります。

モビリティ サービス エンジンのステータス情報のモニタリング

[System] > [Status] ページでは、サーバ イベント、Prime Infrastructure アラームとイベント、およびモビリティ サービス エンジンの NMSP 接続ステータスをモニタできます。

この項では詳細情報を説明します。内容は次のとおりです。

- 「モビリティ サービス エンジンのサーバ イベントの表示」（P.16-978）
- 「モビリティ サービス エンジンの Prime Infrastructure アラームの表示」（P.16-979）
- 「モビリティ サービス エンジンの Prime Infrastructure イベントの表示」（P.16-979）
- 「モビリティ サービス エンジンの NMSP 接続ステータスの表示」（P.16-979）

モビリティ サービス エンジンのサーバ イベントの表示

サーバ イベントのリストを表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　該当するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[System] > [Status] > [Server Events] の順に選択します。

[Status] > [Server Events] ページに、次の情報が表示されます。

- [Timestamp]：サーバ イベントの時刻。
- [Severity]：サーバ イベントのシビリティ。
- [Event]：イベントの詳細な説明。
- [Facility]：イベントが発生した機能。

モビリティ サービス エンジンの監査ログの表示

モビリティ サービス エンジンで使用可能な [Audit Logs] オプションを使用して、ユーザが実行した操作の監査ログを表示できます。監査ログを表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　該当するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[System] > [Status] > [Audit Logs] の順に選択します。

[Status] > [Audit Logs] ページに、次の情報が表示されます。

- [Username]：監査ログを生成したユーザのユーザ名。
- [Operation]：ユーザが実行した操作。
- [Operation Status]：操作のステータス。これは [SUCCESSFUL] または [FAILED] です。
- [Invocation Time]：示されている操作について監査ログが記録された日時。

-

モビリティ サービス エンジンの Prime Infrastructure アラームの表示

Prime Infrastructure アラームのリストを表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　該当するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[System] > [Status] > [Prime Infrastructure Alarms] の順に選択します。詳細については、「アラームのモニタリング」（P.5-127）を参照してください。

モビリティ サービス エンジンの Prime Infrastructure イベントの表示

Prime Infrastructure イベントのリストを表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　該当するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[System] > [Status] > [Prime Infrastructure Events] の順に選択します。詳細については、「イベントのモニタリング」（P.5-143）を参照してください。

モビリティ サービス エンジンの NMSP 接続ステータスの表示

[NMSP Connection Status] ページでは、モビリティ サービス エンジンと、このモビリティ サービス エンジンが割り当てられているシスコ コントローラ間の NMSP 接続を確認できます。

（注）　ネットワーク モビリティ サービス プロトコル（NMSP）は、モビリティ サービスとコントローラ間の通信を管理するプロトコルです。

コントローラとモビリティ サービス エンジンの間の NMSP 接続を確認するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　該当するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[System] > [Status] > [NMSP Connection Status] の順に選択します。

[NMSP Connection Status] ページに、次の情報が表示されます。

- [Summary]：[Summary] セクションには、各デバイス タイプ、接続の合計数、非アクティブな接続の数が表示されます。
- [NMSP Connection Status]：このグループ ボックスには以下が表示されます。
  - [IP address]：デバイスの IP アドレスをクリックすると、そのデバイスの NMSP 接続ステータスの詳細が表示されます。追加情報については、「NMSP サーバの接続ステータスの詳細の表示」（P.16-980）を参照してください。
  - [Target Type]：NMSP 接続の接続先デバイスを示します。
  - [Version]：デバイスの現在のソフトウェア バージョンを示します。
  - [NMSP Status]：接続がアクティブまたは非アクティブのいずれであるかを示します。
  - [Echo Request Count]：送信されたエコー要求の数を示します。
  - [Echo Response Count]：受信したエコー応答の数を示します。
  - [Last Message Received]：最新メッセージの受信日時を示します。

ステップ 4　[NMSP Status] が [ACTIVE] であることを確認します。

- アクティブである場合は、有線スイッチ、コントローラ、および有線クライアントの詳細情報を表示できます。
- アクティブではない場合、Prime Infrastructure デバイスとモビリティ サービス エンジンを再同期します。

（注）　非アクティブな接続に対して NMSP トラブルシューティング ツールを実行できます。

NMSP サーバの接続ステータスの詳細の表示

NMSP の接続ステータスの詳細を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　該当するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[System] > [Status] > [NMSP Connection Status] の順に選択します。

ステップ 4　デバイスの IP アドレスをクリックします。[NMSP Connection Status Details] ページが開きます。[Details] ページには次の情報が表示されます。

- Summary

  - IP Address
  - [Version]：デバイスの現在のソフトウェア バージョン。
  - [Target Type]：NMSP 接続の接続先デバイス。
  - [NMSP Status]：接続がアクティブまたは非アクティブのいずれであるかを示します。
  - [Echo Request Count]：送信されたエコー要求の数。
  - [Echo Response Count]：受信したエコー応答の数。
  - [Last Activity Time]：デバイスとモビリティ サービス エンジン間での最終メッセージ アクティビティの日時。
  - [Last Echo Request Message Received At]：最新のエコー要求を受信した日時。
  - [Last Echo Response Message Received At]：最新のエコー応答を受信した日時。
  - [Model]：デバイスのモデル。
  - [MAC Address]：デバイスの MAC アドレス（該当する場合）。
  - [Capable NMSP Services]：このデバイスの NMSP 対応サービス（ATTACHMENT、LOCATION など）。
- [Subscribed Services]：サブスクライブしている各 NMSP サービスのサブサービスを示します。たとえば、MOBILE_STATION_ATTACHMENT は ATTACHMENT のサブサービスです。
- Messages
  - [Message Type]：メッセージ タイプには、ATTACHMENT_NOTIFICATION、ATTACHMENT_REQUEST、ATTACHMENT_RESPONSE、CAPABILITY_NOTIFICATION、ECHO_REQUEST、ECHO_RESPONSE、LOCATION_NOTIFICATION、LOCATION_REQUEST、SERVICE_SUBSCRIBE_REQUEST、SERVICE_SUBSCRIBE_RESPONSE などがあります。
  - [In/Out]：メッセージが着信メッセージと発信メッセージのいずれであるかを示します。
  - [Count]：着信メッセージまたは発信メッセージの数を示します。
  - [Last Activity Time]：最新のアクティビティまたはメッセージの日時。
  - [Bytes]：メッセージのサイズ（バイト単位）。

モビリティ サービスのメンテナンス管理

この項では、次のトピックを扱います。

モビリティ サービス バックアップ パラメータの表示または編集

モビリティ サービス バックアップ パラメータを表示または編集するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[Maintenance] > [Backup] の順に選択します。

- [Backups located at] : バックアップ ファイルの場所を示します。
- [Enter a name for the Backup] : バックアップ ファイル名を入力または編集します。
- [Timeout (in secs)] : ファイル バックアップ試行操作がタイムアウトになるまでの時間（秒単位）を示します。

モビリティ サービス エンジンの履歴データのバックアップ

Prime Infrastructure には、モビリティ サービス エンジンのデータをバックアップするための機能があります。

モビリティ サービス エンジン データをバックアップするには、次の手順に従います。

ステップ 1　Prime Infrastructure UI で、[Services] > [Mobility Services] の順に選択します。

ステップ 2　バックアップするモビリティ サービス エンジンの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[Maintenance] > [Backup] の順に選択します。

ステップ 4　バックアップの名前を入力します。

ステップ 5　バックアップがタイムアウトになるまでの時間（秒単位）を入力します。

ステップ 6　[Submit] をクリックし、Prime Infrastructure が実行されているサーバのハード ドライブに履歴データをバックアップします。

バックアップ処理中に、このページでバックアップのステータスを確認できます。バックアップ処理中に、このページには 3 つの項目が表示されます。（1）[Last Status] フィールドには、バックアップのステータスを示すメッセージが表示され、（2）[Progress] フィールドには、バックアップの完了率が表示され、（3）[Started at] フィールドには、バックアップの開始日時が示されます。

（注）　他の Prime Infrastructure ページで他のモビリティ サービス エンジン操作を実行しながら、バックアップ プロセスをバックグラウンドで実行できます。

（注）　バックアップは、Prime Infrastructure インストール時に指定した FTP ディレクトリに保管されます。ただし、Prime Infrastructure のインストールでは、FTP ディレクトリは指定されません。場合によっては、FTP ルートのフル パスを指定する必要があります。

モビリティ サービス エンジンの履歴データの復元

ファイルをモビリティ サービス エンジンに復元するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[Maintenance] > [Restore] の順に選択します。

ステップ 4　ドロップダウン リストから、復元するファイルを選択します。

ステップ 5　モビリティ サービス エンジンからすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。

このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 6　[Submit] をクリックして復元プロセスを開始します。

ステップ 7　[OK] をクリックし、Prime Infrastructure サーバのハード ドライブからデータを復元することを確定します。

復元が完了すると、Prime Infrastructure にそのことを示すメッセージが表示されます。

（注）　他の Prime Infrastructure ページで他のモビリティ サービス エンジン操作を実行しながら、復元プロセスをバックグラウンドで実行できます。

Prime Infrastructure を使用したモビリティ サービス エンジンへのソフトウェアのダウンロード

Prime Infrastructure を使用してソフトウェアをモビリティ サービス エンジンにダウンロードするには、次の手順に従います。

ステップ 1　アプリケーション コードのダウンロードに使用する Prime Infrastructure または外部 FTP サーバから、ロケーション アプライアンスに対して ping を実行できることを確認します。

ステップ 2　[Services] > [Mobility Services] の順に選択します。

ステップ 3　ソフトウェアをダウンロードするモビリティ サービス エンジンの名前をクリックします。

ステップ 4　左側のサイドバーのメニューから、[Maintenance] を選択します。

ステップ 5　[Download Software] をクリックします。

ソフトウェアをダウンロードするには、次のいずれかを実行します。

- Prime Infrastructure ディレクトリにリストされているソフトウェアをダウンロードするには、[Select from uploaded images to transfer into the Server] チェックボックスをオンにします。次に、ドロップダウン リストからバイナリ イメージを選択します。

  Prime Infrastructure で、ドロップダウン リストにリストされているバイナリ イメージが、Prime Infrastructure のインストール時に指定した FTP サーバ ディレクトリにダウンロードされます。

  Prime Infrastructure のインストールでは、FTP ディレクトリは指定されません。場合によっては、FTP ルートのフル パスを指定する必要があります。

- ローカルまたはネットワーク経由で使用可能なダウンロード済みソフトウェアを使用するには、[Browse a new software image to transfer into the Server] チェックボックスをオンにし、[Browse] をクリックします。ファイルを見つけ、[Open] をクリックします。

ステップ 6　ソフトウェア ダウンロードがタイムアウトになるまでの時間（秒単位、1 ～ 1800）を入力します。

ステップ 7　[Download] をクリックし、ソフトウェアをモビリティ サービス エンジンの /opt/installers ディレクトリにダウンロードします。

モビリティ サービス エンジンのパートナー システムの設定

[System] > [Partner Systems] ページで、MSE-Qualcomm PDS の設定を実行できます。この設定の目的は、モバイル デバイスのナビゲーション機能を向上させることです。パートナー検出サーバ（PDS）は、MSE によって提供されるフロア プランと AP データを使用して暗号化されたサポート データを生成します。PDS は Qualcomm スマート フォンで使用される最適化された形式にこの情報を変換します。

この項では詳細情報を説明します。内容は次のとおりです。

Qualcomm PDS の設定

Qualcomm PDS の設定を実行するには、次の手順に従ってください。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　モビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバーのメニューから、[System] > [Partner Systems] の順に選択します。

[Qualcomm PDS Configuration for MSE] ページが表示されます。

ステップ 4　MSE-qualcomm コミュニケーションを有効にする場合は、[Enable Qualcomm] チェックボックスをオンにします。

ステップ 5　[Qualcomm PDS Endpoint] テキスト ボックスに、Qualcomm PDS サーバの URL を入力します。これは、データ サポートをフェッチできる PDS の URL です。デフォルトの URL は http://207.114.133.174:8000/AssistanceDataMgr/AssistanceDataMgrSOAP?wsdl です。

ステップ 6　[MSE URL to request assistance data] テキスト ボックスに MSE URL を入力します。これは、場所においてデバイスがアクセスできる MSE の URL です。

ステップ 7　[Cisco Mobile Concierge SSID] テキスト ボックスに、モバイル クライアントを接続させる先のモバイル コンシェルジュ SSID 情報を入力します。Qualcomm のスマート フォンがこの SSID を関連付けられ、MSE と通信します。

ステップ 8　[Venue Description] テキスト ボックスに場所の説明を入力します。

ステップ 9　[Refresh time period for assistance data on MSE] テキスト ボックスに、MSE のサポート データの更新間隔を入力します。

ステップ 10　[Refresh time period for assistance data on mobile clients] テキスト ボックスに、モバイル クライアントのサポート データの更新間隔を入力します。

ステップ 11　メッセージ/サポート データを Qualcomm PDS サーバに送信し、モバイル クライアントが著作権で保護される必要がある場合は、**[Include Copyright Information]** チェックボックスを選択します。

ステップ 12　[Copyright Owner] テキスト ボックスに、含める必要のある著作権者の情報を入力します。

ステップ 13　[Copyright Year] テキスト ボックスに、含める必要のある著作権年を入力します。

ステップ 14　設定を保存する場合は [Save] を、元に戻る場合は [Cancel] をクリックします。

MSE-Qualcomm 設定

MSE-Qualcomm の設定には、次の手順が含まれます。

- CAD ファイルからの Map Extraction Tool（MET）の出力の生成
- Prime Infrastructure への MET 出力の入力
- GPS マーカーの追加
- フロアを MSE に同期
- Qualcomm QUIPS/PDS および著作権情報の提示
- MSE での Qualcomm PDS サーバに対する F2 インターフェイス要求の実行

CAD ファイルからの Map Extraction Tool（MET）の出力の生成

Qualcomm の MET は、マップ ファイル（DXF ファイル）から各種レイヤをカスタマイズおよび選択し、以下を含む zip ファイルを生成するアプリケーションです。

- Prime Infrastructure でフロア マップとして使用されるイメージ ファイル（.PNG 形式）。
- メートル単位でのフロア面積（水平および垂直）を含む Span.xml ファイル。
- 壁、扉、関心のあるポイントなどに関連する幾何機能情報を含む Qualcomm 固有のマップ XML ファイル。

（注） MET アプリケーションは Prime Infrastructure および MSE には依存せず、ホスト マシンに常駐させることができます。MET の出力だけが Prime Infrastructure でマップ関連の入力情報として使用されます。

CAD ファイルから Map Extraction Tool の出力を生成するには、次の手順に従ってください。

ステップ 1　[MET Tool] フォルダ内の ReadMe.txt ファイルにある手順に従って、Qualcomm MET ツールを起動します。

ステップ 2　Map Extraction Tool に DXF ファイルを入力します。

ステップ 3　左側のサイド バーのメニューから必要な階層を選択します。

ステップ 4　Map Extraction Tool のユーザ インターフェイスで目的の場所に Map Extraction Tool の出力を保存します。

Cisco Adaptive wIPS サービス パラメータの管理

[wIPS Service] ページでは、wIPS サービス管理設定を表示、管理できます。

（注） 非ルート パーティション ユーザに対しては Cisco Adaptive wIPS 機能はサポートされていません。

wIPS サービス管理設定の管理

wIPS サービス管理設定を表示または管理するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　該当するモビリティ サービス エンジンのデバイス名を選択します。

ステップ 3　左側のサイドバー メニューから [wIPS Service] を選択します。

ステップ 4　次のパラメータを表示または編集します。

- [Log level]：ドロップダウン リストから適切なログ レベルを選択します。ログ レベルには、debug、error、important event、major debug、none、および warning があります。
- [Forensic size limit (GB)]：フォレンジック ファイルの最大許容サイズを入力します。
- [Alarm ageout (hours)]：各アラームの有効期間を時間単位で入力します。
- [Device ageout (days)]：デバイスによるアラーム送信の有効期間を日単位で入力します。

ステップ 5　[Save] をクリックして変更を確定するか、または [Cancel] をクリックして変更を適用せずにページを閉じます。

Context-Aware Service ソフトウェアのパラメータの管理

Context-Aware Service（CAS）ソフトウェアにより、シスコ アクセス ポイントからクライアントまたはタグに関する状況依存情報（ロケーション、温度、可用性など）を取得することで、Mobility Services Engine は数千のモバイル アセットとクライアントを同時に追跡できます。

CAS は、受信した状況依存情報を処理する際に 2 つのエンジンを使用します。*Context-Aware Engine for Clients* は Wi-Fi クライアントから受信したデータを処理し、*Context-Aware Engine for Tags* は Wi-Fi タグから受信したデータを処理します。これらのエンジンは、業務上のニーズに応じて一括でまとめて導入するか、または個別に導入することができます。

（注）　モビリティ サービス エンジンは Cisco CX 以外のタグの追跡とマッピングは行いません。

（注）　CAS は、以前は Cisco ロケーションベース サービスと呼ばれていました。

追跡対象のクライアントまたはタグの数とタイプに関する Context-Aware サービス ソフトウェアのプロパティと、クライアントまたはタグのロケーションを計算するかどうかの設定を変更できます。

クライアントとタグのロケーション計算（受信信号強度インジケータ（RSSI）測定など）に影響するパラメータも変更できます。

状況依存情報の表示

Prime Infrastructure を使用して状況依存情報を表示する前に、コマンドライン インターフェイス（CLI）コンソール セッションを使用してモビリティ サービス エンジンの初期設定を行う必要があります。『*Cisco 3355 Mobility Services Engine Getting Started Guide*』および『*Cisco 3100 Mobility Services Engine Getting Started Guide*』を参照してください。これらのマニュアルは http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html にあります。

モビリティ サービス エンジンのインストールと初期設定が完了したら、モビリティ サービス エンジンは複数の Cisco ワイヤレス LAN コントローラと通信し、オペレータにより定義された状況依存情報を収集できます。次に、関連付けられている Prime Infrastructure を使用して各モビリティ サービス エンジンと通信し、選択されたデータを転送および表示できます。

クライアント、不正アクセス ポイント、不正クライアント、モバイル ステーション、干渉、およびアクティブ RFID アセット タグに関するデータを収集するようにモビリティ サービス エンジンを設定できます。

クライアントおよびタグのライセンス

（注）　パートナー エンジンのライセンスは、リリース 7.5 から削除されます。

アクセス ポイントからタグおよびクライアントに関する状況依存情報を取得するには、シスコからライセンスを購入する必要があります。

- タグとクライアントのライセンスはそれぞれ個別に提供されます。
- クライアント ライセンスには、不正クライアント、不正アクセス ポイント、および干渉（有効に設定されている場合）の追跡機能も含まれています。
- タグとクライアントのライセンスは、さまざまな数量（1,000 ～ 12,000 ユニット）で提供されます。

（注）　リリース 7.2 以降のリリースから 7.5 にアップグレードする場合は、AeroScout ライセンスとエンジンがなくなることに関する警告メッセージが表示されます。

（注）　次の URL にある『*Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 6.0*』を参照してください。
http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Context-Aware パラメータに関する追加情報については、次のトピックを参照してください。

- 「Context-Aware Service の一般パラメータ」（P.16-987）
- 「Context-Aware Service の管理パラメータ」（P.16-988）
- 「Context Aware Service の詳細パラメータ」（P.16-1006）

Context-Aware Service の一般パラメータ

[Context Aware Service] > [General] ページにアクセスするには、左側のサイドバーのメニューから [Services] > [Mobility Services] > [General] の順に選択します。このページには、次の情報が表示されます。

- 追跡対象クライアントの数
- トレース対象タグの数
- 追跡対象不正クライアント/アクセス ポイントの数
- 追跡対象干渉の数
- 追跡対象有線クライアントの数
- 追跡対象要素の合計数の制限
- 追跡対象タグ数の制限
- モビリティ サービス エンジン クライアントおよびタグの数を示すインタラクティブ グラフ

Context-Aware Service の管理パラメータ

ここでは、次の内容について説明します。

モビリティ サービスの追跡パラメータの変更

モビリティ サービス エンジンでは、最大 25,000 クライアントまたは 25,000 タグを追跡できます（適切なライセンスを購入している場合）。追跡中の要素のロケーションに関する更新情報は、Cisco ワイヤレス LAN コントローラからモビリティ サービス エンジンに送信されます。

このうち、コントローラから追跡対象として指定したデバイスだけを、Prime Infrastructure マップ、クエリー、およびレポートで表示できます。追跡対象外の要素のイベントとアラームは一切収集されず、クライアントまたはタグの 25,000 個の要素上限にはカウントされません。

Prime Infrastructure を使用して次の追跡パラメータを変更できます。

- アクティブに追跡する要素ロケーション（クライアント ステーション、アクティブなアセット タグ、干渉、有線クライアント、不正クライアント、不正アクセス ポイント）の有効化および無効化。
  - 有線クライアント ロケーションの追跡により、データセンターのサーバはネットワーク上の有線クライアントを容易に検出できるようになります。サーバにはネットワーク上の有線スイッチ ポートが関連付けられています。
- 追跡対象とする特定要素の個数上限を設定します。

  たとえば、12,000 の追跡対象ユニットのクライアント ライセンスで、追跡できるクライアント ステーションの数の上限として 8,000 を設定できます（この場合残りの 4,000 ユニット分は、不正クライアントと不正アクセス ポイントの追跡に使用できます）。特定の要素の追跡上限に達すると、追跡されていない要素の合計数が [Tracking Parameters] ページに表示されます。
- アドホックの不正クライアントと不正アクセス ポイントの追跡解除とレポート解除。

モビリティ サービス エンジンの追跡パラメータを設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] を選択し、[Mobility Services] ページを開きます。

ステップ 2　プロパティを編集するモビリティ サービス エンジンの名前をクリックします。[General Properties] ページが表示されます。

ステップ 3　[Administration] サブヘッダーから [Context-Aware Software] > [Tracking Parameters] の順に選択して設定オプションを表示します。

ステップ 4　次に示す追跡パラメータを必要に応じて変更します（表 16-4 を参照）。

表 16-4　Tracking Parameters

フィールド	設定オプション
Tracking Parameters	
Wired Clients	1. モビリティ サービス エンジンによるクライアント ステーションの追跡を有効にするには、[Enable] チェックボックスをオンにします。 7.0 では、クライアント ライセンスはすべてのネットワーク ロケーション サービス要素を対象としており、有線クライアント、ワイヤレス クライアント、不正クライアント、不正アクセス ポイント、および干渉の間で共有されます。 有線クライアント数の上限は、モビリティ サービス エンジン 7.0 および Prime Infrastructure 1.0 からサポートされています。つまり、有線クライアントの数を一定数（例：500）に制限できます。この上限を設定することで、ライセンスで許可されているデバイスの数が有線クライアントによって使い切ることがなく、一部のライセンスが他のデバイスに対して使用可能になります。 **注意** モビリティ サービス エンジンを 6.0 から 7.0 にアップグレードすると、ワイヤレス クライアントまたは不正クライアント/アクセス ポイントの上限が設定されている場合、この上限はリセットされます。これは、7.0 では有線クライアントの上限が変更されているためです。 **（注）** [Active Value]（表示のみ）：現在追跡されている有線クライアント ステーションの数を示します。 **（注）** [Not Tracked]（表示のみ）：上限を超えている有線クライアント ステーションの数を示します。
Wireless Clients	1. モビリティ サービス エンジンによるクライアント ステーションの追跡を有効にするには、[Enable] チェックボックスをオンにします。 2. 追跡対象クライアント ステーションの数の上限を設定するには、[Enable Limiting] チェックボックスをオンにします。 3. 上限が有効になっている場合は、上限値を入力します。入力できる上限値は、25,000（モビリティ サービス エンジンで追跡できるクライアントの最大数）までの正の値です。 **（注）** 追跡対象クライアントの実際の数は、購入ライセンスによって決まります。 **（注）** [Active Value]（表示のみ）：現在追跡されているクライアント ステーションの数を示します。 **（注）** [Not Tracked]（表示のみ）：上限を超えているクライアント ステーションの数を示します。

表 16-4　Tracking Parameters （続き）

フィールド	設定オプション
Rogue Access Points	1. モビリティ サービス エンジンによる不正クライアントおよび不正アクセス ポイントの追跡を有効にするには、[Enable] チェックボックスをオンにします。 2. 追跡する不正クライアントおよび不正アクセス タグ ステーションの数を設定するには、[Enable Limiting] チェックボックスをオンにします。 3. 上限が有効になっている場合は、上限値を入力します。入力できる上限値は、25,000（モビリティ サービス エンジンで追跡できる不正クライアントおよび不正アクセス ポイントの最大数）までの正の値です。 （注） 追跡対象不正クライアント/アクセス ポイントの実際の数は、購入したクライアント ライセンスによって決まります。クライアント、不正クライアント、および不正アクセス ポイントには同一ライセンスが適用されるため、不正クライアントと不正アクセス ポイントの追跡のために割り当て可能な数量を決定する際には、追跡されているクライアントの数を考慮する必要があります。 （注） [Active Value]（表示のみ）：現在追跡している不正クライアントと不正アクセス ポイントの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えた不正クライアントと不正アクセス ポイントの数を示します。
Exclude Ad-Hoc Rogues	ネットワーク内のアドホックの不正クライアント/アクセス ポイントの追跡と報告を無効にするには、このチェックボックスをオンにします。このように設定すると、Prime Infrastructure マップにアドホック不正クライアント/アクセス ポイントが表示されず、イベントとアラームが報告されません。
Rogue Clients	1. モビリティ サービス エンジンによる不正クライアントの追跡を有効にするには、[Enable] チェックボックスをオンにします。 2. 追跡対象不正クライアントの数の上限を設定するには、[Enable Limiting] チェックボックスをオンにします。 3. 上限が有効になっている場合は、上限値を入力します。入力できる上限値は、25,000（モビリティ サービス エンジンで追跡できる不正クライアントの最大数）までの正の値です。 （注） 追跡対象不正クライアント/アクセス ポイントの実際の数は、購入したクライアント ライセンスによって決まります。クライアント、不正クライアント、および不正アクセス ポイントには同一ライセンスが適用されるため、不正クライアントと不正アクセス ポイントの追跡のために割り当て可能な数量を決定する際には、追跡されているクライアントの数を考慮する必要があります。 （注） [Active Value]（表示のみ）：追跡されている不正クライアントの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えている不正クライアントの数を示します。

表 16-4　Tracking Parameters （続き）

フィールド	設定オプション
Interferers	1. モビリティ サービス エンジンによる干渉の追跡を有効にするには、[Enable] チェックボックスをオンにします。 7.0 では、クライアント ライセンスはすべてのネットワーク ロケーション サービス要素を対象としており、有線クライアント、ワイヤレス クライアント、不正クライアント、不正アクセス ポイント、および干渉の間で共有されます。 （注）　[Active Value]（表示のみ）：現在追跡されている干渉の数を示します。 （注）　[Not Tracked]（表示のみ）：上限を超えている干渉の数を示します。
Asset Tracking Elements	
Active RFID Tags	1. モビリティ サービス エンジンによるアクティブ RFID タグの追跡を有効にするには、[Enable] チェックボックスをオンにします。 （注）　追跡対象のアクティブ RFID タグの実際の数は、購入ライセンスによって決まります。 （注）　[Active Value]（表示のみ）：現在追跡されているアクティブ RFID タグの数を示します。これは、選択されたタグ エンジンによって異なります。 （注）　[Not Tracked]（表示のみ）：上限を超えているアクティブ RFID タグの数を示します。
SNMP Parameters（7.0.105.0 以降のモビリティ サービスには適用されません）。	
SNMP Retry Count	ポーリング サイクルの再試行回数を入力します。デフォルト値は 3 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能）
SNMP Timeout	ポーリング サイクルがタイムアウトになるまでの時間を秒数で入力します。デフォルト値は 5 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能）
SNMP Polling Interval	
Client Stations	クライアント ステーションのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。デフォルト値は 300 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能）
Active RFID Tags	アクティブ RFID タグのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。有効値は 1 ～ 99999 です。 （注）　モビリティ サービスがコントローラからアセット タグ データを収集する前に、コントローラで CLI コマンド **config rfid status enable** を使用して、アクティブ RFID タグの検出を有効にする必要があります。
Rogue Clients and Access Points	不正アクセス ポイントのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。デフォルト値は 600 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能）。
Statistics	モビリティ サービスの統計ポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。デフォルト値は 900 です。有効値は 1 ～ 99999 です。（リリース 4.1 以前のコントローラでのみ設定可能）。

ステップ 5　[Save] をクリックし、モビリティ サービス エンジン データベースに新しい設定を保存します。

モビリティ サービスのフィルタリング パラメータ

Prime Infrastructure では、以下の項目をフィルタリングすることで、ロケーションが追跡されるアセット タグ、有線クライアント、不正クライアント、干渉、およびアクセス ポイントの数を制限できます。

- MAC アドレス

  特定の MAC アドレスを入力し、ロケーション追跡での許可または不許可を設定できます。許可または不許可にする MAC アドレスを記述したファイルをインポートできます。

  MAC アドレスの入力形式は xx:xx:xx:xx:xx:xx です。MAC アドレスのファイルをインポートする場合、ファイルは次の形式に従っている必要があります。

  - 各 MAC アドレスを 1 行ずつ記述する必要があります。
  - 最初に許可 MAC アドレスを最初にリストする必要があります。この際、許可 MAC アドレスの前に「[Allowed]」行項目を記述します。[Disallowed] の後に不許可 MAC アドレスをリストする必要があります。
  - ワイルドカードを使用して MAC アドレスの範囲を指定できます。たとえば、以下の [Allowed] リストの 1 番めのエントリ「00:11:22:33:*」はワイルドカードです。

（注）　許可 MAC アドレスの形式は、[Filtering Parameters] 設定ページに表示されます。詳細については、表 16-5 を参照してください。

ファイルの記述例：

```
[Allowed]
00:11:22:33:*
22:cd:34:ae:56:45
02:23:23:34:*
[Disallowed]
00:10:*
ae:bc:de:ea:45:23
```

- プローブ クライアント

  プローブ クライアントとは、別のコントローラに関連付けられているが、プロービング アクティビティによって別のコントローラから認識され、そのプライマリ コントローラとともに「プローブ済み」コントローラによって要素としてカウントされるクライアントです。

フィルタリング パラメータの変更

モビリティ サービス エンジンのフィルタリング パラメータを設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。[Mobility Services] ページが表示されます。

ステップ 2　プロパティを編集するモビリティ サービス エンジンの名前をクリックします。[General Properties] ページが表示されます。

ステップ 3　[Context-Aware Software] メニューの [Administration] サブヘッダーから [Filtering Parameters] を選択します。設定オプションが表示されます。

ステップ 4　次に示すフィルタリング パラメータを必要に応じて変更します（表 16-5 を参照）。

表 16-5　Filtering Parameters

フィールド	設定オプション
Advanced Filtering Params	
Duty Cycle Cutoff Interferers	指定した制限を満たすデューティ サイクルのある干渉のみ追跡され、Base ロケーション ライセンスに対してカウントされるように、干渉のデューティ サイクルのカットオフ値を入力します。 [Duty Cycle Cutoff Interferers] のデフォルト値は 0% で、設定可能な範囲は 0% ～ 100% です。 ロケーション ライセンスをより適切に使用するために、干渉のデューティ サイクルに基づいて干渉のフィルタを指定することもできます。
MAC Filtering Params	

表 16-5　Filtering Parameters （続き）

フィールド	設定オプション
Exclude Probing Clients	プローブ クライアントのロケーション計算を実行しないようにするには、このチェックボックスをオンにします。
Enable Location MAC Filtering	1. MAC アドレスによる特定要素の MAC フィルタリングを有効にするには、このチェックボックスをオンにします。 2. MAC アドレスのファイルをインポートするには（[Upload a file for Location MAC Filtering] フィールド）、ファイル名を検索して選択し、[Save] をクリックしてファイルをロードします。インポートされた MAC アドレスのリストは、ファイルでの指定に基づいて [Allowed List] と [Disallowed List] に自動的に読み込まれます。 （注）　許可 MAC アドレスの形式を表示するには、[Upload a file for Location MAC Filtering] フィールドの横にある赤色の疑問符をクリックします。 3. 個々の MAC アドレスを追加するには、MAC アドレス（形式 : xx:xx:xx:xx:xx:xx）を入力して [Allow] または [Disallow] をクリックします。該当する列にアドレスが表示されます。 （注）　[Allow] 列と [Disallow] 列の間でアドレスを移動するには、MAC アドレス項目を選択し、該当する列にあるボタンをクリックします。 （注）　複数のアドレスを移動するには、1 番めの MAC アドレスをクリックし、Ctrl キーを押しながら [Enter] をクリックして他の MAC アドレスを選択します。追加先の列に基づいて [Allow] または [Disallow] をクリックします。 （注）　MAC アドレスが [Allow] 列と [Disallow] 列のいずれにもリストされていない場合、デフォルトでは [Blocked MACs] 列に表示されます。[Unblock] をクリックすると、MAC アドレスは自動的に [Allow] 列に移動します。[Disallow] 列に移動するには、[Allow] 列にある [Disallow] をクリックします。

ステップ 5　[Save] をクリックし、モビリティ サービス エンジン データベースに新しい設定を保存します。

モビリティ サービスの履歴パラメータの変更

Prime Infrastructure を使用して、クライアント ステーション、不正クライアント、およびアセット タグに関する履歴の保存（アーカイブ）期間を指定できます。履歴は、モビリティ サービスに関連付けられているコントローラから受信します。

また、ハード ドライブに保存するデータの量を削減するため、履歴ファイルから重複データを定期的に削除（プルーニング）するようにモビリティ サービスをプログラミングできます。

モビリティ サービス エンジンの履歴設定を設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバー メニューから [Context Aware Service] > [History Parameters] の順に選択します。

ステップ 4　次に示す履歴パラメータを必要に応じて変更します（表 16-6 を参照）。

表 16-6　History Parameters

フィールド	説明
Archive for	ロケーション アプライアンスで有効な各カテゴリの履歴を維持する日数を入力します。デフォルト値は 30 です。有効値は 1 ～ 99999 です。
Prune data starting at	ロケーション アプライアンスがデータ プルーニングを開始する時刻（時間と分）を入力します（時間は 0 ～ 23、分は 1 ～ 59）。 データ プルーニングを再び開始するまでの間隔を入力します（0 ～ 99900000、0 はプルーニングを実行しないことを意味します）。デフォルトの開始時刻は 23 時間 50 分、デフォルトの間隔は 1440 分です。
Enable History Logging of Location Transitions for	ロケーション遷移の履歴ロギングを有効にするには、次に示す項目を 1 つ以上選択します。 • Client Stations • Wired Stations • Asset Tags • Rogue Clients • Rogue Access Points • Interferers （注）　モビリティ サービスがコントローラからアセット タグ データを収集する前に、CLI コマンド **config rfid status enable** を使用して、RFID タグの検出を有効にする必要があります。

ステップ 5　[Save] をクリックし、選択した内容を ロケーション アプライアンス データベースに保存します。

モビリティ サービスのロケーション表示の有効化

モビリティ サービス エンジンでロケーション表示を有効にすると、シスコのデフォルト設定（キャンパス、ビルディング、フロア、XY 座標）以外の拡張都市ロケーション情報（市町村、州、郵便番号、国）および GEO ロケーション情報（経度、緯度）を表示できます。ワイヤレス クライアントと有線クライアントは、ロケーションベースのサービスとアプリケーションで使用するためにオンデマンド ベースでこの情報を要求できます。

また、拡張ロケーション情報（有線クライアントの MAC アドレス、有線クライアントが接続している有線スイッチのスロットおよびポートなど）をインポートできます。

新しいキャンパス、ビルディング、フロア、または屋外領域が後で追加または設定されるときに、ロケーション表示を設定できます。

有効にすると、Mobility Services Engine はロケーションを要求する Cisco CX v5 クライアントに対してそのロケーションを提供できます。

（注） この機能を有効にする前に、モビリティ サービス エンジンを同期してください。

モビリティ サービス エンジンでロケーション表示を有効化および設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] > [*Device Name*] の順に選択します。キャンパス、ビルディング、またはフロアが割り当てられているモビリティ サービス エンジンを選択します。

ステップ 2　左側のサイドバー メニューから、[Context Aware Services] > [Administration] > [Presence Parameters] の順に選択します。

ステップ 3　[Service Type On Demand] チェックボックスをオンにし、Cisco CX クライアント v5 のロケーション表示を有効にします。

ステップ 4　[Location Resolution] ドロップダウン リストで、次のいずれかを選択します。

a. [Building] が選択されている場合、モビリティ サービス エンジンは要求クライアントに対し、そのクライアントのロケーションをビルディングで示します。

- たとえば、Building A に配置されているクライアントがそのロケーションを要求している場合、モビリティ サービス エンジンはクライアント アドレスとして Building A を返します。

b. [AP] が選択されている場合、モビリティ サービス エンジンは要求クライアントに対し、そのクライアントのロケーションを、関連付けられているアクセス ポイントで示します。アクセス ポイントの MAC アドレスが表示されます。

- たとえば、MAC アドレス 3034:00hh:0adg のアクセス ポイントに関連付けられているクライアントがそのロケーションを要求している場合、モビリティ サービス エンジンはクライアントにアドレス 3034:00hh:0adg を返します。

c. [X,Y] が選択されている場合、モビリティ サービス エンジンは要求クライアントに対し、そのクライアントのロケーションを XY 座標で示します。

- たとえば、(50, 200) に位置しているクライアントがそのロケーションを要求している場合、モビリティ サービス エンジンはクライアントにアドレス 50, 200 を返します。

ステップ 5　必要なロケーション形式のチェックボックスをオンにします。

a. [Cisco] チェックボックスをオンにすると、ロケーションがキャンパス、ビルディング、フロア、および XY 座標で示されます（デフォルト）。

b. [Civic] チェックボックスをオンにすると、キャンパス、ビルディング、フロア、または屋外領域の名前とアドレス（通り、市、州、郵便番号、国）が示されます。

（注）　複数の Civic リストが記述されたファイルのインポートの詳細については、「モビリティ サービスの都市情報のインポート」（P.16-998）を参照してください。

c. [GEO] チェックボックスをオンにすると、緯度と経度による座標が示されます。

ステップ 6　デフォルトでは、[Location Response Encoding] の [Text] チェックボックスがオンになっています。これは、クライアントが受信する情報の形式を示しています。この設定を変更する必要はありません。

ステップ 7　受信側クライアントが受信した情報を別の相手へ再送信できるようにするには、[Retransmission Rule] の [Enable] チェックボックスをオンにします。

ステップ 8　[Retention Expiration] 値を分単位で入力します。これにより、クライアントで格納される受信情報が上書きされるまでの時間を決定します。デフォルト値は 24 時間（1440 分）です。

ステップ 9　[Save] をクリックします。

モビリティ サービスのアセット情報のインポート

Prime Infrastructure を使用してモビリティ サービス エンジンのアセット、チェックポイント、および TDOA レシーバ情報をインポートするには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　アセット情報のインポート先モビリティ サービス エンジンの名前をクリックします。

ステップ 3　[Context Aware Service] > [Administration] > [Import Asset Information] の順に選択します。

ステップ 4　テキスト ファイル名を入力するか、ファイル名を参照して選択します。

インポート ファイルの情報を次の形式で指定します。

- タグ形式：# タグ、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名
- ステーション形式：# ステーション、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名

ステップ 5　インポート ファイル名が [Browse] テキストボックスに表示されたら、[Import] をクリックします。

モビリティ サービスのアセット情報のエクスポート

Prime Infrastructure を使用してアセット、チェックポイント、および TDOA レシーバ情報をモビリティ サービス エンジンからファイルにエクスポートするには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　アセット情報のエクスポート元モビリティ サービス エンジンの名前をクリックします。

ステップ 3　[Context Aware Service] > [Administration] > [Export Asset Information] の順に選択します。

エクスポート ファイルの情報を次の形式で指定します。

- タグ形式：# タグ、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名
- ステーション形式：# ステーション、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名

ステップ 4　[Export] をクリックします。

[Open]（画面に表示）、[Save]（外部 PC またはサーバに保存）、または [Cancel]（要求を取り消す）をクリックします。

（注）　[Save] を選択すると、アセット ファイルの保存先とアセット ファイル名を選択するよう求められます。デフォルトのファイル名は assets.out です。ダウンロードが完了したら、ダイアログボックスの [Close] をクリックします。

モビリティ サービスの都市情報のインポート

Prime Infrastructure を使用してモビリティ サービスの都市情報をインポートするには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　インポートするアセット情報のモビリティ サービス エンジンの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[Context Aware Software] を選択します。

ステップ 4　左側のサイドバー メニューの [Administration] から、[Import Civic Information] を選択します。

ステップ 5　テキスト ファイル名を入力するか、ファイル名を参照して選択します。

インポート ファイルの情報は、次のいずれかの形式でなければなりません。

スイッチ IP アドレス、スロット番号、ポート番号、拡張親都市アドレス、X、Y、フロア ID、ビルディング ID、ネットワーク設計 ID、ELIN:"ELIN"、PIDF-Lo-Tag:"Civic Address Element Value"

（注）　各エントリをそれぞれ個別の行に指定する必要があります。

ステップ 6　[Import] をクリックします。

Context Aware Service の Wired パラメータ

この項では、[Context Aware Service] > [Wired] ドロップダウン リストのパラメータについて説明します。内容は次のとおりです。

- 「有線スイッチのモニタリング」（P.16-998）
- 「有線スイッチの詳細」（P.16-999）
- 「有線クライアントのモニタリング」（P.16-1000）
- 「有線クライアントの詳細」（P.16-1001）

有線スイッチのモニタリング

有線スイッチの詳細情報（IP アドレス、MAC アドレス、シリアル番号、ソフトウェア バージョン、ELIN）と、有線スイッチのポート、有線クライアント（カウントとステータス）、および都市情報の詳細を確認できます。

イーサネット スイッチとモビリティ サービス エンジンが同期されると（[Services] > [Synchronize Services] > [Switches]）、Prime Infrastructure を介して有線スイッチ データがモビリティ サービス エンジンにダウンロードされます。ロケーション対応スイッチとモビリティ サービス エンジンは、NMSP 経由で通信します。Prime Infrastructure とモビリティ サービス エンジンは XML 経由で通信します。

有線スイッチの詳細を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　[Mobility Services] ページで、該当する有線ロケーション スイッチのデバイス名リンクをクリックします。

ステップ 3　[Context Aware Service] > [Wired] > [Wired Switches] の順に選択します。モビリティ サービス エンジンと同期された有線スイッチの概要が表示されます。

ステップ 4　スイッチとそのポート、有線クライアント（カウントおよびステータス）、および都市情報の詳細については、「有線スイッチの詳細」（P.16-999）を参照してください。

有線スイッチの詳細

有線スイッチの詳細を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　[Mobility Services] ページで、該当するモビリティ サービス エンジンのデバイス名リンクをクリックします。

ステップ 3　[Context Aware Service] > [Wired] > [Wired Switches] の順に選択します。モビリティ サービス エンジンと同期された有線スイッチの概要が表示されます。

ステップ 4　該当する有線スイッチの IP アドレス リンクをクリックします。[Wired Switch Details] ページが表示されます。

[Wired Switch Details] ページには、[Switch Information]、[Switch Ports]、[Civic]、および [Advanced] の 4 つのタブがあります。

（注）　スイッチから都市情報をエクスポートするには、[Select a command] ドロップダウン リストからそのオプションを選択します。このオプションは、[Wired Switches] ページの 4 つのダッシュレットすべてで使用可能です。

[Wired Switch Details] のタブには次の情報が表示されます。

- [Switch Information]：スイッチに接続している有線クライアントの合計数の要約とクライアントの状態（接続、未接続、不明）が表示されます。
  - [Connected clients]：有線スイッチに接続しているクライアント。
  - [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
  - [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、クライアントは不明としてマークされます。

（注）　有線クライアントの詳細情報を表示するには、クライアント カウント リンク（合計クライアント数、接続、未接続、不明）のいずれかをクリックします。詳細については、「有線クライアントのモニタリング」（P.16-1000）を参照してください。

- [Switch Ports]：スイッチのポートの詳細なリストを表示します。

（注）　ポート IP アドレス、スロット番号、モジュール番号、ポート タイプ、ポート番号のリストの順序（昇順、降順）を変更できます。変更するには、該当する列見出しをクリックします。

- [Civic]：有線スイッチの都市情報の詳細なリストを表示します。
- [Advanced]：有線スイッチの追加都市情報の詳細なリストを表示します。

有線クライアントのモニタリング

有線クライアントの詳細情報（MAC アドレス、IP アドレス、ユーザ名、シリアル番号、UDI、モデル番号、ソフトウェア バージョン、VLAN ID）、ポートの関連付け、都市情報を表示できます。

スイッチとモビリティ サービス エンジンが同期されると（[Services] > [Synchronize Services] > [Switches]）、Prime Infrastructure を介して有線クライアント データがモビリティ サービス エンジンにダウンロードされます。

Prime Infrastructure とモビリティ サービス エンジンは XML 経由で通信します。

有線クライアントの詳細は、有線スイッチのページ（[Context Aware Service] > [Wired] > [Wired Switches]）または有線クライアントのページ（[Context Aware Service] > [Wired] > [Wired Clients]）に表示されます。

- IP アドレス、MAC アドレス、VLAN ID、シリアル番号、またはユーザ名が判明している場合は、有線クライアントのページの検索フィールドを使用できます。
- 特定のスイッチに関連する有線クライアントを調べるには、有線スイッチのページでその情報を確認できます。詳細については、「有線スイッチのモニタリング」（P.16-998）を参照してください。

有線クライアントの詳細を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。[Mobility Services] ページが表示されます。

ステップ 2　該当する有線ロケーション スイッチのデバイス名リンクをクリックします。

ステップ 3　[Context Aware Service] > [Wired] > [Wired Clients] の順に選択します。

[Wired Clients] 要約ページでは、クライアントがスイッチ別にグループ化されています。

クライアント ステータスは接続、未接続、不明として示されます。

- [Connected clients]：有線スイッチに接続しているアクティブなクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、不明としてマークされたクライアント。NMSP 接続の詳細については、「モビリティ サービス エンジンの NMSP 接続ステータスの表示」（P.16-979）を参照してください。

有線クライアントの MAC アドレスが判明している場合は、そのリンクをクリックしてクライアントの詳細ページを表示するか、または検索フィールドを使用することができます。有線クライアントの詳細については、「有線クライアントの詳細」（P.16-1001）を参照してください。

- 有線クライアントを IP アドレス、ユーザ名、または VLAN ID で検索することもできます。

スイッチの IP アドレスをクリックすると、スイッチの詳細ページが表示されます。詳細については、「有線スイッチのモニタリング」（P.16-998）を参照してください。

ステップ 4　該当するクライアントの MAC アドレスをクリックして、有線クライアントの詳細を表示します。有線クライアントの詳細については、「有線クライアントの詳細」（P.16-1001）を参照してください。

有線クライアントの詳細

有線クライアントの詳細を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　[Mobility Services] ページで、該当するモビリティ サービス エンジンのデバイス名リンクをクリックします。

ステップ 3　[Context Aware Service] > [Wired] > [Wired Clients] の順に選択します。モビリティ サービス エンジンと同期された有線クライアントの概要が表示されます。

ステップ 4　該当する有線クライアントの MAC アドレス リンクをクリックします。[Wired Client Details] ページが表示されます。

[Wired Client Details] ページには、[Device Information]、[Port Association]、[Civic Address]、および [Advanced] の 4 つのタブがあります。

[Wired Switch Details] のタブには次の情報が表示されます。

- [Device Information] : MAC アドレス、IP アドレス、ユーザ名、シリアル番号、モデル番号、UDI、ソフトウェア バージョン、VLAN ID、および VLAN 名が表示されます。
- [Port Association] : 有線クライアントが終端するスイッチ ポート、スロット、またはモジュールの物理的なロケーション、クライアントのステータス（接続、未接続、不明）、およびスイッチ IP アドレスが表示されます。
- [Civic Address] : 都市アドレス情報が表示されます。
- [Advanced] : 有線クライアントの拡張物理アドレス詳細情報が表示されます（該当する場合）。

（注）　クライアントは、クライアントが終端するポートに対して設定されている都市アドレス情報と拡張ロケーション情報を使用します。ポート（ポート、スロット、モジュール）に対して都市情報と拡張情報が定義されていない場合、ロケーション データは表示されません。

干渉のモニタリング

[Monitor] > [Interferers] ページでは、CleanAir 対応アクセス ポイントにより検出された干渉デバイスをモニタできます。

この項では、CleanAir 対応アクセス ポイントにより検出される干渉について説明します。デフォルトでは、「[Monitor] > [Interferers] > [AP Detected Interferers]」（P.16-1002）ページが表示されます。

ここでは、次の内容について説明します。

[Monitor] > [Interferers] > [AP Detected Interferers]

ワイヤレス ネットワーク上の CleanAir 対応アクセス ポイントにより検出されたすべての干渉デバイスを表示するには、[Monitor] > [Interferers] の順に選択します。このページには干渉デバイスの概要が表示されます。表示される概要には、次のデフォルト情報が含まれています。

- [Interferer ID]：干渉の固有識別子。干渉源の詳細を参照するには、このリンクをクリックします。
- [Type]：干渉源のカテゴリを示します。デバイスのタイプの詳細を参照するには、ここをクリックします。表示されるダイアログボックスに、詳細が示されます。次のカテゴリがあります。
  - [Bluetooth link]：Bluetooth リンク（802.11b/g/n のみ）
  - [Microwave Owen]：電子レンジ（802.11b/g/n のみ）
  - [802.11 FH]：802.11 周波数ホッピング デバイス（802.11b/g/n のみ）
  - [Bluetooth Discovery]：Bluetooth 検出（802.11b/g/n のみ）
  - [TDD Transmitter]：時分割複信（TDD）トランスミッタ
  - [Jammer]：電波妨害デバイス
  - [Continuous Transmitter]：連続トランスミッタ
  - [DECT-like Phone]：Digital Enhanced Cordless Communication（DECT）対応電話
  - [Video]：ビデオ カメラ
  - [802.15.4]：802.15.4 デバイス（802.11b/g/n のみ）
  - [WiFi Inverted]：スペクトル反転 Wi-Fi 信号を使用するデバイス
  - [WiFi Invalid]：非標準の Wi-Fi チャネルを使用するデバイス
  - [SuperAG]：802.11 SuperAG デバイス
  - [Canopy]：Motorola Canopy デバイス
  - [Radar]：レーダー デバイス（802.11a/n のみ）
  - [XBox]：Microsoft Xbox（802.11b/g/n のみ）
  - [WiMAX Mobile]：WiMAX モバイル デバイス（802.11a/n のみ）
  - [WiMAX Fixed]：WiMAX 固定デバイス（802.11a/n のみ）
  - TDD Exalt
  - Motorola Canopy
- [Status]：干渉デバイスのステータスを示します。
  - [Active]：干渉が現在 CleanAir 対応アクセス ポイントにより検出されていることを示します。
  - [Inactive]：干渉が CleanAir 対応アクセス ポイントにより検出されないか、または CleanAir 対応アクセス ポイントが、干渉デバイスを Prime Infrastructure から到達可能ではないと見なしたことを示します。
- [Severity]：干渉デバイスの重大度ランクを示します。
- [Affected Band]：このデバイスが干渉している帯域を表示します。
- [Affected Channels]：影響を受けるチャネルを表示します。
- [Duty Cycle (%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- [Discovered]：検出された時刻を表示します。
- [Last Updated]：干渉源が最後に検出された時刻。
- [Floor]：干渉デバイスが存在していたロケーション。

（注）　干渉デバイスは、[Tracking Parameters] ページで干渉デバイスを追跡するオプションが有効な場合にだけ表示されます。このオプションは、デフォルトで無効です。追跡パラメータの詳細については、「モビリティ サービスの追跡パラメータの変更」（P.16-988）を参照してください。

[Monitor] > [Interferers] > [AP Detected Interferers] > [Interferer Details]

[Monitor] > [Interferers] > [*Interferer ID*] の順に選択し、このページを表示します。このページでは、アクセス ポイントにより検出された干渉デバイスの詳細情報が表示されます。このページには、干渉デバイスに関する次の詳細情報が表示されます。

- [Interferer Properties]
  - [Type]：AP により検出された干渉デバイスのタイプが表示されます。
- [Status]：干渉デバイスのステータス。干渉デバイスのステータスを示します。
  - [Active]：干渉が現在 CleanAir 対応アクセス ポイントにより検出されていることを示します。
  - [Inactive]：干渉が CleanAir 対応アクセス ポイントにより検出されないか、または CleanAir 対応アクセス ポイントが、干渉デバイスを Prime Infrastructure から到達可能ではないと見なしたことを示します。
  - [Severity]：干渉デバイスの重大度ランクを示します。
  - [Duty Cycle (%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
  - [Affected Band]：このデバイスが干渉している帯域を表示します。
  - [Affected Channels]：影響を受けるチャネルを表示します。
  - [Discovered]：検出された時刻を表示します。
  - [Last Updated]：干渉源が最後に検出された時刻。
- Location
  - [Floor]：この干渉デバイスが検出されたロケーション。
  - [Last Located At]：干渉デバイスが最後に検出された時刻。
  - [On MSE]：この干渉デバイスが検出されたモビリティ サーバ エンジン。
- Clustering Information
  - [Clustered By]：次の情報を表示します。

    コントローラの IP アドレス（コントローラによりクラスタ化されている場合）。

    モビリティ サービス エンジンの IP アドレス（モビリティ サービス エンジンによりクラスタ化されている場合）。
  - [Detecting APs]：干渉デバイスを検出したアクセス ポイントの詳細情報を表示します。詳細情報には、[Access Point Name (Mac)]、[Severity]、および [Duty Cycle(%)] などが含まれます。

（注）　検出アクセス ポイントの情報は、アクティブ デバイスでのみ使用可能です。ただし一部のアクティブ デバイスでは、この情報が使用可能ではないことがあります。これは、これらの干渉デバイスが非アクティブとしてマークされる過程にあり、[Monitor] > [Interferers] ページを次回更新すると、これらのデバイスは非アクティブとして示されるためです。

- [Details]：干渉タイプに関する短い説明を表示します。

Select a command

[Select a command] ドロップダウン リストでは、アクセス ポイントにより検出された干渉デバイスのロケーション履歴が表示されます。詳細については、「[Monitor] > [Interferers] > [AP Detected Interferer Details] > [Interference Device ID] > [Location History]」（P.16-1004）を参照してください。

[Monitor] > [Interferers] > [AP Detected Interferer Details] > [Interference Device ID] > [Location History]

このページを表示するには、[Monitor] > [Interferers] > [Interference Device ID] の順に選択し、[Select a command] ドロップダウン リストから [Location History] を選択し、[Go] をクリックします。

- [Interferer Information]：干渉デバイスに関する基本情報を表示します。
  - [Data Collected At]：データが収集された時点のタイムスタンプ。
  - [Type]：干渉デバイスのタイプ。
  - [Severity]：干渉デバイスの重大度インデックス。
  - [Duty Cycle]：干渉デバイスのデューティ サイクル（パーセンテージ）。
  - [Affected Channels]：影響を受けるチャネルのカンマ区切りリスト。
- [Interferer Location History]：干渉デバイスのロケーション履歴を表示します。
  - Time Stamp
  - Floor
- Clustering Information
  - Clustered By
- Detecting APs
  - [AP Name]：干渉デバイスを検出したアクセス ポイント。
  - [Severity]：干渉デバイスの重大度インデックス。
  - [Duty Cycle(%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- Location
  - [Location Calculated At]：この情報が生成された時点のタイムスタンプを表示します。
  - [Floor]：干渉デバイスのロケーション情報を表示します。
  - 干渉デバイスのロケーションがマップにグラフィカルに表示されます。イメージを拡大表示するには [Enlarge] リンクをクリックします。

[Monitor] > [Interferers] > [Edit View]

[Edit View] ページでは、[AP Detected Interferers Summary] ページの列を追加、削除、並び替えできます。また、干渉を検索できます。デフォルトでは、アクティブな状態でありシビリティが 5 以上の干渉が [AP Detected Interferers] ページに表示されます。検索条件の編集の詳細については、「[Monitor] > [Interferers] > [Edit View] > [Edit Search]」（P.16-1005）を参照してください。

[AP Detected Interferers] ページの列を編集するには、次の手順に従います。

ステップ 1　[Monitor] > [Interferers] の順に選択します。[AP Detected Interferers] ページが表示されます。このページには、CleanAir 対応アクセス ポイントにより検出された干渉源の詳細が表示されます。

ステップ 2　[AP Detected Interferers] ページの [Edit View] リンクをクリックします。

ステップ 3　アクセス ポイント表に新しい列を追加するには、左側の領域で、列見出しをクリックして選択します。[Show] をクリックして、選択した列見出しを右側の領域へ移動します。右側の領域にあるすべての項目が表に表示されます。

ステップ 4　アクセス ポイント表から列を削除するには、右側の領域で、削除する列見出しをクリックして選択します。[Hide] をクリックして、選択した列見出しを左側の領域へ移動します。左側の領域にある項目はすべて、表に表示されません。

ステップ 5　[Up] ボタンと [Down] ボタンを使用して、表内での情報の並び順を指定します。目的の列見出しを選択し、[Up] または [Down] をクリックして、現在のリスト内での位置を変更します。

ステップ 6　デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7　[Submit] をクリックして、変更内容を確定します。

[Monitor] > [Interferers] > [Edit View] > [Edit Search]

特定の条件に基づいて干渉を検索できます。デフォルトでは、アクティブな状態でありシビリティが 5 以上の干渉が [AP Detected Interferers] ページに表示されます。干渉の検索をカスタマイズするには、[Edit Search] オプションを使用します。

検索条件を編集するには、次の手順に従います。

ステップ 1　[Monitor] > [Interferers] の順に選択します。[AP Detected Interferers] ページが表示されます。

ステップ 2　[Edit Search] をクリックし、適切な条件を選択します。このオプションでは、以下の検索条件を指定できます。

- [Search Category]：干渉の検索では、検索カテゴリは [Interferers] です。
- [Detected By]：ドロップダウン リストから [Access Points] または [Spectrum Experts] を選択します。
- [Search By]：リストから次のいずれかのオプションを選択します。
  - **All Interferers**
  - **Interferer ID**
  - **Interferer Type**
  - **Severity**
  - **Duty Cycle**
  - **Location**
- [Severity greater than]：テキスト ボックスにシビリティ レベルを入力します。
- [Detected within the last]：リストから、次のオプションのいずれかを選択します。
  - **5 Minutes**
  - **15 Minutes**
  - **30 Minutes**
  - **1 Hour**
  - **3 Hours**
  - **6 Hours**
  - **12 Hours**
  - **24 Hours**
  - **All History**
- [Interferer status]：リストから、次のいずれかのオプションを選択します。
  - **Active**

  - **Inactive**
  - **All**
- [Restrict By Radio Band/Channels]：検索で特定の無線周波数またはチャネルを制限するには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフです。このチェックボックスをオンにするとリストが表示されます。このリストには、[2.4-GHz]、[5-GHz]、および [Individual Channel] オプションが表示されます。[Individual Channel] を選択すると、[Affected Channels] テキスト ボックスが表示されます。チャネルを指定し、[Match All] または [Match Any] オプション ボタンを選択します。

ステップ 3　検索結果として表示するページあたりの項目数を選択します。

ステップ 4　検索条件を保存する場合は [Save Search] チェックボックスをオンにします。

ステップ 5　検索条件の指定が完了したら、[Go] をクリックして検索結果を表示します。

Context Aware Service の詳細パラメータ

ここでは、次の内容について説明します。

- 「ノースバウンド通知の変更」（P.16-1006）
- 「モビリティ サービスのロケーション パラメータの変更」（P.16-1008）
- 「モビリティ サービスの通知パラメータの変更」（P.16-1010）

ノースバウンド通知の変更

ノースバウンド通知により、モビリティ サービス エンジンがサードパーティ アプリケーションに送信するタグ通知が定義されます。

ノースバウンド パラメータを設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engines] の順に選択します。

ステップ 2　設定するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[Context Aware Service] > [Advanced] > [Notification Parameters] の順に選択して設定オプションを表示します。

ステップ 4　[Enable Northbound Notifications] チェックボックスをオンにし、この機能を有効にします。

ステップ 5　通知をサードパーティアプリケーションに送信するため（ノースバウンド）、[Notification Contents] チェックボックスをオンにします。

ステップ 6　次の [Notification Contents] チェックボックスを 1 つ以上オンにします。

- **Chokepoints**
- **Telemetry**
- **Emergency**
- **Battery Level**
- **Vendor Data**
- **Location**

ステップ 7　[Notification Triggers] チェックボックスをオンにします。

ステップ 8　次の [Notification Triggers] チェックボックスを 1 つ以上オンにします。

- **Chokepoints**
- **Telemetry**
- **Emergency**
- **Battery Level**
- **Vendor Data**
- **Location Recalculation**

ステップ 9　ノースバウンド通知を受信するシステムの IP アドレスまたはホスト名およびポートを入力します。

ステップ 10　ドロップダウン リストからトランスポート タイプを選択します。

ステップ 11　宛先システムに安全にアクセスするために HTTPS プロトコルを使用する場合は、[HTTPS] チェックボックスをオンにします。

ステップ 12　通知パラメータの設定を変更するには、このページの [Advanced] タブの該当するテキスト ボックスに新しい値を入力します。表 16-7 を参照してください。

表 16-7　ユーザが設定可能な条件付き通知とノースバウンド通知のフィールド

フィールド	設定オプション
Rate Limit	モビリティ サービス エンジンが通知を生成するレートをミリ秒単位で入力します。値 0（デフォルト）を指定すると、モビリティ サービス エンジンは可能な限り迅速に通知を生成します（ノースバウンド通知のみ）。
Queue Limit	通知送信のイベント キュー制限を入力します。モビリティ サービス エンジンは、この制限を超過するイベントをすべてドロップします。デフォルト値：Cisco 3350（30000）、Cisco 3315（5,000）、および Cisco 2710（10,000）。
Retry Count	リフレッシュ時間の終わりまでにイベント通知を生成する回数を入力します。このパラメータは非同期トランスポート タイプの場合にだけ使用されます。非同期トランスポート タイプでは通知受信が確認されないため、通知が送信中に失われる可能性があります。デフォルト値は、1 です **（注）**　モビリティ サービス エンジン データベースにイベントが保存されません。
Refresh Time	通知を再送信するまで待機する必要がある時間を分単位で入力します。たとえば、In Coverage Area 通知の対象としてデバイスが設定されており、このデバイスがカバレッジ エリア内で頻繁に検出されるとします。この通知は、リフレッシュ時間ごとに 1 回送信されます。デフォルト値は 0 分です。
Drop Oldest Entry on Queue Overflow	(読み取り専用)。起動時以降にキューからドロップされたイベント通知の数。
Serialize Events per Mac address per Destination	同じ MAC アドレスの連続するイベントを、連続して 1 つの宛先に送信するには、このオプションを選択します。

ステップ 13　[Save] をクリックします。

モビリティ サービスのロケーション パラメータの変更

Prime Infrastructure を使用して、モビリティ サービスでその計算時間を保持するかどうか、およびモビリティ サービスでその受信信号強度インジケータ（RSSI）の累積測定時間を削除するまでの期間を指定できます。要素のロケーション移動を管理するため、さまざまなスムージング レートを適用できます。

ロケーション パラメータを設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3　左側のサイドバー メニューから、[Context Aware Service] > [Location Parameters] の順に選択します。

ステップ 4　次に示すロケーション パラメータを必要に応じて変更します（表 16-8 を参照）。

表 16-8　Location Parameters

フィールド	説明
General	
Enable Calculation Time	ロケーション計算に要する時間の計算を有効にするには、このチェックボックスをオンにします。 **注意**　このフィールドを有効にすると、ロケーション計算にかかる時間が全体的に長くなるため、シスコ TAC 担当員の指示がある場合にだけ有効にしてください。
Enable OW Location	ロケーション計算の一部として外壁（OW）計算を有効にするには、このチェックボックスをオンにします。 **（注）**　ロケーション サーバではこの OW ロケーション パラメータは無視されます。
Relative discard RSSI time	最新の RSSI サンプルから、RSSI 測定が古いものと見なされ廃棄されるまでの経過時間を分単位で入力します。デフォルト値は 3 です。有効値の範囲は 0 ～ 99999 です。3 未満の値を指定することは推奨されません。
Absolute discard RSSI time	最新のサンプルに関係なく、RSSI 測定が古いものと見なされ廃棄されるまでの経過時間を分単位で入力します。デフォルト値は 60 です。有効値の範囲は 0 ～ 99999 です。60 未満の値を指定することは推奨されません。

表 16-8　Location Parameters （続き）

フィールド	説明
RSSI Cutoff	1 mW（dBm）に基づく RSSI の遮断の値をデシベル（dBs）単位で入力します。この値に達するまでは、モビリティ サービス エンジンは常にアクセス ポイント測定を使用します。デフォルト値は -75 です。 （注）　RSSI の遮断値よりも前に 3 つ以上の測定が使用可能な場合、モビリティ サービスでは計算には最も強力な 3 つ（またはこれ以上）の測定が使用され、それ以外の弱い値はすべて破棄されます。ただし、RSSI の遮断値以降の弱い測定のみが使用可能な場合は、これらの値が計算に使用されます。 注意　変更は、シスコ TAC 担当者の指示がある場合にだけ行ってください。この値を変更すると、ロケーション計算の精度が低下する可能性があります。
Enable Location Filtering	有効にすると、クライアント ロケーション計算にだけロケーション フィルタが適用されます。 ロケーション フィルタを有効にすると、現行ロケーションの推定に以前のロケーション推定値を使用できるようになります。これにより、ステーショナリ クライアントのロケーション ジッターが低下し、モバイル クライアントの追跡機能が向上します。
Chokepoint Usage	ロケーションの判別時にチョークポイント プロキシミティを使用可能にするには、このチェックボックスをオンにします。チョークポイント プロキシミティを報告できるシスコ互換タグに適用されます。
Use Chokepoints for Interfloor conflicts	フロア間競合で正しいフロアを判別するときにチョークポイントを使用できるようにします。 [Never]、[Always]、または [Floor Ambiguity] を選択します。
Chokepoint Out of Range Timeout	シスコ互換タグ エンジンがチョークポイント プロキシミティ範囲を離れた後のタイムアウト（秒単位）です。タイムアウトになると、RSSI 情報がロケーションの判別に再び使用されるようになります。
Absent Data Cleanup Interval	非アクティブ要素をデータベースから削除する操作の間隔（分単位）を入力します。

表 16-8　Location Parameters （続き）

フィールド	説明
Use Default Heatmaps for Non Cisco Antennas	ロケーション計算中にシスコ以外のアンテナにデフォルトのヒートマップを使用可能にするには、このチェックボックスをオンにします。このオプションは、デフォルトで無効です。
Movement Detection	
Individual RSSI change threshold	このフィールドには、個別 RSSI 移動再計算トリガーしきい値を指定します。 0 ～ 127 dBm の範囲内のしきい値を入力します Cisco TAC の指示がない場合は変更しないでください。
Aggregated RSSI change threshold	このフィールドには、集約 RSSI 移動再計算トリガーしきい値を指定します。 0 ～ 127 dBm の範囲内のしきい値を入力します この値は、Cisco TAC の指示がない場合は変更しないでください。
Many new RSSI change percentage threshold	このフィールドには、複数の新規 RSSI 移動再計算トリガーしきい値（パーセンテージ）を指定します。 この値は、Cisco TAC の指示がない場合は変更しないでください。
Many missing RSSI percentage threshold	このフィールドには、複数の欠落 RSSI 移動再計算トリガーしきい値（パーセンテージ）を指定します。 この値は、Cisco TAC の指示がない場合は変更しないでください。

ステップ 5　[Save] をクリックし、選択内容を Prime Infrastructure およびモビリティ サービスのデータベースに保存します。

モビリティ サービスの通知パラメータの変更

Prime Infrastructure を使用して、モビリティ サービス エンジンのイベント通知パラメータを設定できます。これらのパラメータは、モビリティ サービス エンジンによる通知の生成または再送信の頻度などの項目を定義します。

（注）　通知パラメータを変更するのは、モビリティ サービス エンジンが大量の通知を送信する場合、または通知を受信しない場合だけにしてください。

タグのノースバウンド通知をサードパーティ アプリケーションに転送できるようにも設定できます。

モビリティ サービス エンジンが送信するノースバウンド通知の形式は、次の URL のシスコ開発者向けサポート ポータルで参照できます。

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

通知パラメータを設定するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services] の順に選択します。

ステップ 2　設定するモビリティ サービス エンジンの名前をクリックします。

ステップ 3　[Context Aware Software] メニューの [Advanced] サブヘッダーから [Notification Parameters] を選択します。設定オプションが表示されます。

ステップ 4　[Enable Northbound Notifications] チェックボックスをオンにし、この機能を有効にします。

ステップ 5　通知をサードパーティアプリケーションに送信するため（ノースバウンド）、[Notification Contents] チェックボックスをオンにします。

ステップ 6　次の Notification コンテンツ オプションを 1 つ以上選択します。

- **Chokepoints**
- **Telemetry**
- **Emergency**
- **Battery Level**
- **Vendor Data**
- **Location**

ステップ 7　[Notification Triggers] チェックボックスをオンにします。

ステップ 8　次の [Notification trigger] オプションを 1 つ以上選択します。

- **Chokepoints**
- **Telemetry**
- **Emergency**
- **Battery Level**
- **Vendor Data**
- **Location Recalculation**

ステップ 9　ノースバウンド通知を受信するシステムの IP アドレスとポートを入力します。

ステップ 10　ドロップダウン リストからトランスポート タイプを選択します。

ステップ 11　宛先システムに安全にアクセスするために HTTPS プロトコルを使用する場合は、[HTTPS] を選択します。

ステップ 12　通知パラメータの設定を変更するには、このページの [Advanced] タブの該当するテキスト ボックスに新しい値を入力します。表 16-9 に、各パラメータについての説明を示します。

表 16-9　ユーザ設定の機密およびノースバウンド通知パラメータ

フィールド	設定オプション
Rate Limit	モビリティ サービス エンジンが通知を生成するレートをミリ秒単位で入力します。値 0（デフォルト）を指定すると、モビリティ サービス エンジンは可能な限り迅速に通知を生成します（ノースバウンド通知のみ）。
Queue Limit	通知送信のイベント キュー制限を入力します。モビリティ サービス エンジンは、この制限よりも前のイベントをすべてドロップします。デフォルト値：Cisco 3350（30000）、Cisco 3310（5,000）、および Cisco 2710（10,000）。

表 16-9　ユーザ設定の機密およびノースバウンド通知パラメータ　（続き）

フィールド	設定オプション
Retry Count	リフレッシュ時間の終わりまでにイベント通知を生成する回数を入力します。このフィールドは非同期トランスポート タイプの場合にだけ使用されます。非同期トランスポート タイプでは通知受信が確認されないため、通知が送信中に失われる可能性があります。デフォルト値は 1 です。 （注）　モビリティ サービス エンジン データベースにイベントが保存されません。
Refresh Time	通知を再送信するまで待機する必要がある時間を分単位で入力します。たとえば In Coverage Area 通知の対象としてデバイスが設定されており、このデバイスがカバレッジ エリア内で頻繁に検出されるとします。この通知は、リフレッシュ時間ごとに 1 回送信されます。
Drop Oldest Entry on Queue Overflow	（読み取り専用）。起動時以降にキューからドロップされたイベント通知の数。
Serialize Events per Mac address per Destination	同じ MAC アドレスの連続するイベントを、連続して 1 つの宛先に送信するには、このオプションを選択します。

ステップ 13　[Save] をクリックします。

モビリティ サービスの通知情報の表示

[Services] > [Context Aware Notifications] ページでは、イベントを定義できます。ここでは、次の内容について説明します。

- 「モビリティ サービスの通知概要の表示」（P.16-1012）
- 「モビリティ サービスの通知定義の表示および管理」（P.16-1013）
- 通知統計情報の表示

モビリティ サービスの通知概要の表示

通知の概要を表示するには、[Services] > [Context Aware Notifications] > [Notification Summary] の順に選択します。

モビリティ サービスはイベント通知を送信しますが、通知を保存しません（ファイア アンド フォーゲット）。ただし、通知イベントの宛先が Prime Infrastructure の場合、Prime Infrastructure は受信した通知を保存し、次に示す 7 つのカテゴリに分類します。

- [Absence (Missing)]：モビリティ サービス エンジンが、指定された時間内に WLAN 上のアセットを認識できない場合に生成されます。
- [Location Change Events]：クライアント ステーション、アセット タグ、不正クライアント、および不正アクセス ポイントが前のロケーションから移動した場合に生成されます。
- [Chokepoint Notifications]：チョークポイントによってタグが確認（スティミュレート）されたときに生成されます。この情報は、CCX v.1 準拠のタグについてのみ、報告および表示されます。
- [Battery Level]：追跡対象のアセット タグが指定した電池残量になったときに生成されます。
- [In/Out Area]：アセットが指定エリア内外に移動したときに生成されます。

（注）　Prime Infrastructure の [Maps] セクション（[Monitor] > [Maps]）で Containment 領域（キャンパス、ビルディング、またはフロア）を定義します。カバレッジ エリアを定義するには、Map Editor を使用します。

- [Movement from Marker]：マップ上に定義する指定マーカーから指定の距離を超えてアセットが移動したときに生成されます。
- [Emergency]：タグのパニック ボタンが生成されたか、タグが削除、改ざん、非アクティブになった、または不明な状態が報告されたときに、CCX v.1 準拠のアセット タグについて生成されます。この情報は、CCX v.1 準拠のタグについてのみ、報告および表示されます。

概要の詳細には、次の情報が含まれます。

- All Notifications
- Client Stations
- Asset Tags
- Rogue Clients
- Rogue Access Points

（注）　各通知の詳細を表示するには、[Last Hour]、[Last 24 Hours]、または [Total Active] 列の数値をクリックし、該当する通知の詳細ページを開きます。

クリアされた通知

モビリティ サービスでは、次のいずれかの状況でイベント条件をクリアしたときに、イベント通知を送信します。

- [Missing (Absence)]：要素が再び表示される。
- [In/Out Area (Containment)]：要素が封じ込むエリア内に戻るか、このエリアから外に出る。
- [Distance]：要素がマーカーから指定された距離以内に戻る。
- [Location Changes]：クリアの状態はこの条件には適用されません。
- [Battery Level]：普通の電池残量で動作しているタグが再検出される。
- Emergency
- Chokepoint

（注）　Prime Infrastructure の [Notifications Summary] ページには、クリアされたイベント条件の通知を受信したかどうかが反映されます。

モビリティ サービスの通知定義の表示および管理

通知の定義を表示するには、[Services] > [Context Aware Notifications] > [Notification Definition] の順に選択します。このページのグループにイベント グループおよびイベント定義を追加できます。どのグループも、イベント通知を編成するのに役立ちます。イベント定義は、特定のグループに属さなければなりません。

イベント グループおよびイベント定義の追加の詳細については、「イベント グループの追加」（P.16-1016）および「イベント定義の追加」（P.16-1019）を参照してください。

イベント グループおよびイベント定義を追加した後でのみ、[Notification Definition] ページに次のパラメータが表示されます。

表 16-10 に、[Notification Definition] ページのフィールドのリストおよび説明を示します。

表 16-10　[Notification Definition] ページ

フィールド	説明
Group Name	イベント定義を追加する先のグループの名前。
Event Definitions	イベント グループの既存のイベント定義。
Created On	イベント グループの作成日。

通知統計情報の表示

特定のモビリティ サービス エンジンの通知統計情報を表示できます。特定のモビリティ サービス エンジンの通知統計情報を表示するには、[Services] > [Mobility Services] > [*MSE-name*] > [Context Aware Service] > [Notification Statistics] を選択します。

MSE-name は、モビリティ サービス エンジンの名前です。

表 16-11 に、[Notification statistics] ページのフィールドをリストして説明します。

表 16-11　[Notification Statistics] のフィールド

フィールド	説明
Summary	
Destinations	
Total	宛先の合計数。
Unreachable	到達不能な宛先の数。
Notification Statistics Summary	
Track Definition Status	トラック定義のステータス。トラック通知ステータスは [Enabled] または [Disabled] のいずれかです。
Track Definition	トラック定義は、Northbound または CAS イベント通知です。
Destination IP Address	通知送信先の宛先 IP アドレス。
Destination Port	通知送信先の宛先ポート。
Destination Type	宛先のタイプ。たとえば、SOAP_XML です
Destination Status	宛先デバイスのステータス。ステータスは [Up] または [Down] です。
Last Sent	最終通知が宛先デバイスに送信された日時。
Last Failed	通知に失敗した日時。
Total Count	宛先に送信された通知の合計数。宛先デバイスの通知統計詳細情報を表示するには、カウント リンクをクリックします。

モバイル コンシェルジュ サービスのパラメータ

ここでは、次の内容について説明します。

設定済みサービス アドバタイズメントの表示

設定済みのサービス アドバタイズメントを表示するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engine] の順に選択します。

ステップ 2　[Device Name] をクリックして、そのプロパティを表示します。

[General Properties] ページが表示されます。

ステップ 3　左側のサイドバーのメニューから、[Mobile Concierge Service] > [Advertisements] の順に選択します。

[Mobile Concierge Service] ページに次の情報が表示されます。

- [Icon]：サービス プロバイダーに関連付けられたアイコンを表示します。
- [Provide Name]：サービス プロバイダー名を表示します。
- [Venue Name]：場所の名前を表示します。
- Advertisements
  - [Friendly Name]：ヘッドセットに表示されるわかりやすい名前。
  - [Advertisement Type]：ヘッドセットに表示されるアドバタイズメントのタイプ。

モバイル コンシェルジュ サービスの統計情報の表示

モバイル コンシェルジュ サービスの統計情報を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engine] の順に選択します。

ステップ 2　[Device Name] をクリックして、そのプロパティを表示します。

[General Properties] ページが表示されます。

ステップ 3　左側のサイドバーのメニューから、[Mobile Concierge service] > [Statistics] の順に選択します。

[Mobile Concierge Service] ページに次の情報が表示されます。

- [Top 5 Active Mobile MAC addresses] : 特定の場所で最もアクティブなモバイルについての情報を表示します。
- [Top 5 Service URIs]：特定の場所またはプロバイダー上でサービスの使用量についての情報を表示します。

イベント グループについて

イベントをより効率的に管理するために、Prime Infrastructure を使用してイベント グループを作成できます。イベント グループを使用すると、イベント定義を編成しやすくなります。

ここでは、次の内容について説明します。

イベント グループの追加

イベント グループを追加するには、次の手順を実行します。

ステップ 1　[Services] > [Context Aware Notifications] を選択します。

ステップ 2　左側のサイドバーのメニューから [Notification Definitions] を選択します。

ステップ 3　[Select a command] ドロップダウン リストから、[Add Event Group] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　[Group Name] テキストボックスにグループ名を入力します。

ステップ 6　[Save] をクリックします。

[Event Settings] ページに新しいイベント グループが表示されます。

イベント グループの削除

イベント グループを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Context Aware Notifications] を選択します。

ステップ 2　左側のサイドバーのメニューから [Notification Definitions] を選択します。

ステップ 3　削除するイベント グループのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから、[Delete Event Group(s)] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

ステップ 7　[Save] をクリックします。

イベント定義の使用

イベント定義には、イベントを発生させた条件、イベントが適用されるアセット、イベント通知の宛先に関する情報が含まれます。この項では、イベント定義の追加、削除、およびテストの方法について説明します。

（注）　Prime Infrastructure では、グループ単位に定義を追加できます。新しいイベント定義はいずれも、特定のグループに属さなければなりません。

イベント定義を追加するには、次の手順を実行します。

ステップ 1　[Services] > [Context Aware Notifications] を選択します。

ステップ 2　左側のサイドバーのメニューから、[Notification Definitions] を選択します。

ステップ 3　イベントを追加するグループの名前をクリックします。選択したイベント グループのイベント定義の概要ページが表示されます。

ステップ 4　[Select a command] ドロップダウン リストから、[Add Event Definition] を選択します。

ステップ 5　[Go] をクリックします。

ステップ 6　[Event Definition Name] テキスト ボックスにイベント定義の名前を入力します。

（注）　イベント定義名は、イベント グループ内で一意である必要があります。

ステップ 7　[Save] をクリックします。

ステップ 8　[General] タブで、次のパラメータを管理します。

- [Admin Status] : [Enabled] チェックボックスをオンにして、イベントの生成を有効にします（デフォルトは無効）。
- [Priority] : ドロップダウン リストから数値を選択して、イベントの優先順位を設定します。ゼロは、最も高くなります。

  （注）　優先順位の高いイベント定義は、優先順位の低いイベント定義よりも先に処理されます。

- [Activate] : 継続してイベントをレポートするには [All the Time] チェックボックスを選択します。アクティベーションを特定の日時に指定するには、[All the Time] チェックボックスをオフにし、適用する日付および開始時刻と終了時刻を選択します。[Save] をクリックします。

ステップ 9　[Conditions] タブで、1 つ以上の条件を追加します。条件ごとに、イベント通知を生成するためのルールを指定します。条件を追加するには、次の手順を実行します。

a.　[Add] をクリックして、[Add/Edit Condition] ページを開きます。

b.　[Condition Type] ドロップダウン リストから条件タイプを選択し、それに関連付ける [Trigger If] パラメータを設定します（表 16-12 を参照）。

表 16-12　[Condition Type]/[Trigger If] パラメータ

Condition Type	Trigger If
Missing	[Missing for Time (mins)]：不明なアセット イベントが生成されてから経過した時間（分）を入力します。 たとえば、このテキスト ボックスに 10 と入力した場合、モビリティ サービス エンジンは、10 分経過してもアセットが見つからないときに、不明なアセット イベントを生成します。
In/Out	[Inside of] または [Outside of]：[Select Area] をクリックし、[Select] ページからエリア パラメータを選択します。[Select] をクリックします。モニタするエリアは、キャンパス全体、キャンパス内のビルディング、ビルディング内のフロア、またはカバレッジ エリアになります（Map Editor を使用してカバレッジ エリアを定義できます）。
Distance	[In the distance of *x* (feet) from Marker] テキスト ボックス：モニタ対象アセットが指定マーカーから指定の距離を超えて移動したときに、イベント通知を生成する距離（フィート単位）を入力します。[Select Marker] をクリックし、[Select] ページでマーカー パラメータを選択します。[Select] をクリックします。
Battery Level	[Battery Level Is]：Low（低）、Medium（中）、Normal（普通）。イベントを生成する適切な電池残量を選択します。
Location Change	アセットの位置が変わったときにイベントが生成されます。
Emergency	[Any]、[Panic Button]、[Tampered]、または [Detached] チェックボックスを選択します。
Chokepoint	[In the range of Chokepoints]：[Select Chokepoint] チェックボックスをオンにし、[Select] ページでチョークポイント パラメータを選択します。[Select] をクリックします。

c. [Apply To] ドロップダウン リストから、生成条件を満たした場合にイベントを生成するアセットのタイプ（[Any]、[Clients]、[Tags]、[Rogue APs]、[Rogue Clients]、または [Interferers]）を選択します。

（注） Emergency イベントおよび Chokepoint イベントは、タグ（CCXv.1 準拠）だけに適用できます。

d. [Match By] ドロップダウン リストから、一致基準（[MAC Address]、[Asset Name]、[Asset Group]、または [Asset Category]）、演算子（[Equals] または [Like]）を選択し、選択した [Match By] 要素に適切なテキストを入力します。

e. [Add] をクリックします。

ステップ 10　[Destination and Transport] タブで、次の手順を実行して、イベント通知を受信する 1 つ以上の宛先を追加し、転送設定を行います。

a. [Add] をクリックして、[Add/Edit Destination and Transport] ページを開きます。

b. 1 つ以上の新しい宛先を追加するには、[Add New] をクリックし、該当する IP アドレスを入力して [OK] をクリックします。

（注） 受信者のシステムのイベント リスナーが通知を処理するように動作している必要があります。デフォルトでは、イベント定義を作成すると、Prime Infrastructure によりその IP アドレスが宛先として追加されます。

c. 通知を受信する宛先を選択するには、右側のボックスで 1 つ以上の IP アドレスをクリックして強調表示させ、[Select] をクリックして、左側のボックスに IP アドレスを追加します。

d. [Message Format field] ドロップダウン リストから、[XML] または [Plain Text] を選択します。

（注） Prime Infrastructure を宛先として選択する場合は、XML 形式を選択する必要があります。

e. [Transport Type] ドロップダウン リストから次のいずれかの転送タイプを選択します。

- [SOAP] : Simple Object Access Protocol。通知は、SOAP を使用して、HTTP/HTTPS を介して送信され、宛先の Web サービスによって処理されます。

  HTTPS を介して通知を送信するかどうかを、対応するチェックボックスをオンにして指定します。[Port Number] テキスト ボックスに宛先のポート番号を入力します。
- [Mail] : 電子メールで通知を送信するには、このオプションを使用します。

  [Mail Type] ドロップダウン リストから、メールを送信するためのプロトコルを選択します。必要に応じて、ユーザ名とパスワード（認証が有効な場合）、送信者の名前、件名行に追加するプレフィックス、受信者の電子メール アドレス、およびポート番号を入力します。
- [SNMP] : Simple Network Management Protocol（簡易ネットワーク管理プロトコル）。このオプションを使用すると、SNMP 対応デバイスに通知を送信します。

  SNMP バージョン v2c を選択した場合は、[SNMP Community] テキスト ボックスに SNMP コミュニティ ストリングを、[Port Number] テキスト ボックスに該当するポート番号を入力するように指示されます。

  SNMP バージョン v3 を選択した場合は、ユーザ名、セキュリティ名を入力し、ドロップダウン リストから認証タイプを選択して認証パスワードを入力し、ドロップダウン リストからプライバシー タイプを選択してプライバシー パスワードを入力するように指示されます。
- [SysLog] : イベント通知の受信者である宛先システム上のシステム ログを指定します。
- [Priority] テキスト ボックスに通知の優先順位を入力し、ファシリティの名前、および宛先システムのポート番号を入力します。

f. [Add] をクリックします。

ステップ 11　イベント グループに新しいイベント定義がリストされたことを確認します（[Context Aware Service] > [Notifications] > [Event] > [Settings] > [Event Group Name]）。

イベント定義の追加

イベント定義には、イベントを発生させた条件、イベントが適用されるアセット、イベント通知の宛先に関する情報が含まれます。

Prime Infrastructure では、グループごとに定義を追加できます。イベント定義は、特定のグループに属さなれければなりません。イベント定義の削除またはテストの詳細については、『*Cisco Content-Aware Software Configuration Guide*』を参照してください。

イベント定義を追加するには、次の手順を実行します。

ステップ 1　[Services] > [Context Aware Notifications] を選択します。

ステップ 2　左側のサイドバーのメニューから [Notification Definitions] を選択します。

ステップ 3　イベントに追加するグループの名前をクリックします。選択したイベント グループのイベント定義の概要ページが表示されます。

ステップ 4　[Select a command] ドロップダウン リストから、[Add Event Definition] を選択し、[Go] をクリックします。

ステップ 5　[Conditions] タブで、1 つ以上の条件を追加します。追加する条件ごとに、イベント通知を生成するためのルールを指定します。

ヒント　たとえば、病院で心臓モニタによる経過観察を行う場合、心臓モニタを見失ってから 1 時間経過したとき、心臓モニタがその割り当てられたフロアから移動したとき、心臓モニタがフロア内の特定のカバレッジ エリアに入ったときなどにイベント通知を生成するルールを追加します。

条件を追加するには、次の手順を実行します。

a. [Add] をクリックして、このイベントを生成する条件を追加します。

b. [Add/Edit Condition] ダイアログ ボックスで、次の手順を実行します。

1. [Condition Type] ドロップダウン リストから条件タイプを選択します。

[Condition Type] ドロップダウン リストから [Missing] を選択した場合は、不明なアセット イベントが生成されてから経過した時間（分）を入力します。たとえば、このテキスト ボックスに 10 と入力した場合、モビリティ サービス エンジンは、10 分経過してもアセットが見つからないときに、不明なアセット イベントを生成します。手順 c に進みます。

[Condition Type] ドロップダウン リストから [In/Out] を選択した場合は、[Inside of] または [Outside of] を選択してから [Select Area] を選択し、アセットが出入りする対象エリアを選択します。[Select] ダイアログボックスで、モニタするエリアを選択し [Select] をクリックします。モニタするエリアは、キャンパス全体、キャンパス内のビルディング、ビルディング内のフロア、またはカバレッジ エリアになります（Map Editor を使用してカバレッジ エリアを定義できます）。たとえば、ビルディング内のフロア部分をモニタするには、[Campus] ドロップダウン リストからキャンパスを、[Building] ドロップダウン リストからビルディングを、[Floor Area] ドロップダウン リストからモニタするエリアを選択します。次に、[Select] をクリックします。手順 c に進みます。

[Condition Type] ドロップダウン リストから [Distance] を選択した場合は、モニタ対象アセットが指定マーカーから指定の距離を超えて移動した場合にイベント通知を生成する距離（フィート単位）を入力し、[Select Marker] をクリックします。[Select] ダイアログボックスで、キャンパス、ビルディング、フロア、およびマーカーを、対応するドロップダウン リストから選択し、[Select] をクリックします。たとえば、マーカーをフロア図面に追加し、トリガーに距離を設定する場合などです。テキスト ボックスに 60 フィートと設定した場合、モニタ対象アセットがマーカーから 60 フィートを超えて離れたときにイベント通知が生成されます。手順 c に進みます。

（注）　Map Editor を使用して、マーカーおよびカバレッジ エリアを作成できます。マーカー名を作成する場合は、システム全体で一意になるようにします。

[Condition Type] ドロップダウン リストから [Battery Level] を選択した場合は、イベントを生成する電池残量（低、中、普通）の横にあるチェックボックスをオンにします。手順 c に進みます。

[Condition Type] ドロップダウン リストから [Location Change] を選択した場合は、手順 c に進みます。

[Condition Type] ドロップダウン リストから [Emergency] を選択した場合は、イベントを生成する緊急事態（すべて、パニック ボタン、改ざん、削除）の横にあるボタンをクリックします。手順 c に進みます。

[Condition Type] ドロップダウン リストから [Chokepoint] を選択した場合は、手順 c に進みます。生成条件は 1 つだけあり、デフォルトで表示されます。設定は必要ありません。

c. [Apply To] ドロップダウン リストから、生成条件を満たした場合にイベントを生成するアセットのタイプ（[Any]、[Clients]、[Tags]、[Rogue APs]、[Rogue Clients]、または [Interferers]）を選択します。

（注） [Apply to] ドロップダウン リストから [any] オプションを選択した場合は、タグ、クライアント、不正アクセス ポイント、および不正クライアントのすべてに電池の条件が適用されます。

（注） Emergency イベントおよび Chokepoint イベントは、Cisco Compatible Extensions のタグのバージョン 1（以降）だけに適用されます。

d. [Match By] ドロップダウン リストから一致基準（[MAC Address]、[Asset Name]、[Asset Group]、または [Asset Category]）を、ドロップダウン リストから演算子（[Equals] または [Like]）を選択し、選択した [Match By] 要素に適切なテキストを入力します。

次に、指定可能なアセットの一致基準の例をいくつか示します。

- [Match By] ドロップダウン リストから [MAC Address] を選択し、[Operator] ドロップダウン リストから [Equals] を選択して、MAC アドレス（たとえば、12:12:12:12:12:12）を入力した場合、MAC アドレスが 12:12:12:12:12:12（完全一致）の要素にイベント条件が提供されます。
- [Match By] ドロップダウン リストから [MAC Address] を選択し、[Operator] ドロップダウン リストから [Like] を選択して、**12:12** を入力した場合、MAC アドレスが 12:12 で始まる要素にイベント条件が適用されます。

e. [Add] をクリックして、定義済みの条件を追加します。

（注） チョークポイントを定義している場合は、条件を追加した後にチョークポイントを選択する必要があります。

チョークポイントを選択するには、次の手順を実行します。

1. [Select Chokepoint] をクリックします。入力ページが表示されます。
2. [Campus]、[Building]、および [Floor] を該当するドロップダウン リストから選択します。
3. 表示されるメニューから [Chokepoint] を選択します。

[Add/Edit Condition] ページに戻ると、[Select Checkpoint] ボタンの横にあるテキスト領域にチョークポイントのロケーション パス（[Campus] > [Building] > [Floor]）が自動的に読み込まれます。

ステップ 6　[Destination and Transport] タブで、次の手順を実行して、イベント通知を受信する 1 つ以上の宛先を追加し、転送設定を行います。

a. 新しい宛先を追加する場合は、[Add] をクリックします。[Add/Edit Destination configuration] ページが表示されます。

b. [Add New] をクリックします。

c. イベント通知を受信するシステムの IP アドレスを入力し、[OK] をクリックします。

受信者のシステムのイベント リスナーが通知を処理するように動作している必要があります。デフォルトでは、イベント定義を作成すると、Prime Infrastructure によりその IP アドレスが宛先として追加されます。

d. イベント通知を送信する宛先を選択する場合は、右側のボックスで 1 つ以上の IP アドレスを強調表示し、[Select] をクリックして左側のボックスに IP アドレスを追加します。

e. [XML] または [Plain Text] を選択して、メッセージ形式を指定します。

f. [Transport Type] ドロップダウン リストから次のいずれかの転送タイプを選択します。

- [SOAP]：イベント通知を送信するための転送タイプとして、簡易 XML プロトコルである Simple Object Access Protocol を指定します。通知は、SOAP を使用して、HTTP/HTTPS を介して送信され、宛先の Web サービスによって処理されます。

  [SOAP] を選択した場合は、HTTPS を介して通知を送信するかどうかを、対応するチェックボックスをオンにして指定します。選択しない場合は HTTP が使用されます。また、[Port Number] テキスト ボックスに宛先のポート番号を入力します。

- [Mail]：電子メールで通知を送信するには、このオプションを使用します。

  [Mail] を選択した場合は、[Mail Type] ドロップダウン リストから電子メールを送信するためのプロトコルを選択する必要があります。必要に応じて、ユーザ名とパスワード（認証が有効な場合）、送信者の名前、件名行に追加するプレフィックス、受信者の電子メール アドレス、およびポート番号を入力する必要もあります。

- [SNMP]：SNMP 対応デバイスに通知を送信するために使用され、ネットワークのモニタリングに広く使用されている技術である Simple Network Management Protocol を使用します。

  [SNMP] を選択した場合は、[SNMP Community] テキスト ボックスに SNMP コミュニティ ストリングを、[Port Number] テキスト ボックスに通知の送信先のポート番号を入力します。

- [SysLog]：イベント通知の受信者である宛先システム上のシステム ログを指定します。

  [SysLog] を選択した場合は、[Priority] テキスト ボックスに通知の優先順位を、[Facility] テキスト ボックスにファシリティの名前を、[Port Number] テキスト ボックスに宛先システムのポート番号を入力します。

g. HTTPS を有効にするには、その横にある [Enable] チェックボックスをオンにします。

ポート番号が自動的に読み込まれます。

h. [Save] をクリックします。

ステップ 7　[General] タブで、次の手順を実行します。

a. [Admin Status] の [Enabled] チェックボックスをオンにして、イベントの生成を有効にします（デフォルトは無効）。

b. [Priority] ドロップダウン リストから数値を選択して、イベントの優先順位を設定します。ゼロが最も高い優先順位です。

（注）　優先順位の高いイベント通知は、優先順位の低いイベント定義よりも先に処理されます。

c. イベント通知の送信頻度を選択するには、次の手順を実行します。

1. イベントを継続的に報告する場合は、[All the Time] チェックボックスをオンにします。手順 g に進みます。
2. イベント通知を送信する曜日と時刻を選択する場合は、[All the Time] チェックボックスをオフにします。曜日と時刻のフィールドが表示され、選択できるようになります。手順 d に進みます。

d. イベント通知を送信する各日の横にあるチェックボックスをオンにします。

e. [Apply From] 見出しから適切な時、分、AM/PM のオプションを選択して、イベント通知を開始する時刻を選択します。

f. [Apply Until] 見出しから適切な時、分、AM/PM のオプションを選択して、イベント通知を終了する時刻を選択します。

g. [Save] をクリックします。

ステップ 8　イベント グループに新しいイベント通知がリストされたことを確認します（[Mobility] > [Notifications] > [Settings] > [Event Group Name]）。

イベント定義の削除

Prime Infrastructure から 1 つ以上のイベント定義を削除するには、次の手順に従います。

ステップ 1　[Services] > [Context Aware Notifications] を選択します。

ステップ 2　左側のサイドバーのメニューから、[Settings] を選択します。

ステップ 3　イベント定義を削除するグループの名前をクリックします。

ステップ 4　削除するイベント定義を、対応するチェックボックスをオンにして選択します。

ステップ 5　[Select a command] ドロップダウン リストから、[Delete Event Definition(s)] を選択します。

ステップ 6　[Go] をクリックします。

ステップ 7　[OK] をクリックして、選択したイベント定義を削除することを確認します。

MSE でのクライアントのサポート

Prime Infrastructure の Advanced Search 機能を使用して、特定のカテゴリおよびフィルタに基づいて、クライアント リストを絞り込むことができます。[Show] ドロップダウン リストを使用して、現在のリストをフィルタリングすることもできます。

ここでは、次の内容について説明します。

- 「IPv6 アドレスによる MSE 上の Prime Infrastructure のワイヤレス クライアントの検索」（P.16-1024）
- 「MSE で検出されたクライアントの表示」（P.16-1025）

IPv6 アドレスによる MSE 上の Prime Infrastructure のワイヤレス クライアントの検索

（注）　このリリースでは、ワイヤレス クライアントだけが IPv6 アドレスを使用します。

Prime Infrastructure の Advanced Search 機能を使用して、MSE の配置されたクライアントを検索するには、次の手順に従います。

ステップ 1　[Advanced Search] をクリックします。

ステップ 2　[New Search] ダイアログで、[Search Category] ドロップダウン リストから検索カテゴリとして [Clients] を選択します。

ステップ 3　[Media Type] ドロップダウン リストから、[Wireless Clients] を選択します。

（注）　メディア タイプとして [Wireless Clients] を選択した場合だけ、[Wireless Type] ドロップダウン リストが表示されます。

ステップ 4　[Wireless Type] ドロップダウン リストから、[All]、[Lightweight]、または [Autonomous Clients] のうちいずれかのタイプを選択します。

ステップ 5　[Search By] ドロップダウン リストから、[IP Address] を選択します。

（注）　IP アドレスによるクライアントの検索は、IP アドレス全体または一部を対象にできます。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

ステップ 6　[Clients Detected By] ドロップダウン リストから、クライアント検出の実行を MSE として選択します。

これは、コントローラと直接通信することで、MSE の Context-Aware Service で検索したクライアントが表示されます。

ステップ 7　[Last detected within] ドロップダウン リストから、クライアントが検出された時間帯を選択します。

ステップ 8　[Client IP Address] テキスト ボックスにクライアント IP アドレスを入力します。IPv6 アドレスの一部または全体を入力できます。

（注）　IPv4 アドレスを使用して、MSE 上で Prime Infrastructure のクライアントを検索している場合は、[Client IP address] テキスト ボックスに IPv4 アドレスを入力します。

ステップ 9　[Client States] ドロップダウン リストから、クライアントの状態を選択します。ワイヤレス クライアントに指定できる値は、[All States]、[Idle]、[Authenticated]、[Associated]、[Probing]、または [Excused] です。 有線クライアントに指定できる値は、[All States]、[Authenticated]、および [Associated] です。

ステップ 10　[Posture Status] ドロップダウン リストからポスチャ ステータスを選択すると、デバイスがクリーンであるかどうかを判別します。指定できる値は、[All]、[unknown]、[Passed]、および [Failed] です。

ステップ 11　[CCX Compatible] チェックボックスをオンにすると、Cisco Client Extensions と互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、[V2]、[V3]、[V4]、[V5]、および [V6] です。

ステップ 12　[E2E Compatible] チェックボックスをオンにして、エンドツーエンドの互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、および [V2] です。

ステップ 13　[NAC State] チェックボックスをオンにすると、特定のネットワーク アドミッション コントロール（NAC）の状態で特定されるクライアントを検索します。指定可能な値は、[Quarantine]、[Access]、[Invalid]、および [Not Applicable] です。

ステップ 14　[Include Disassociated] チェックボックスをオンにすると、ネットワーク上には存在しなくなったが、Prime Infrastructure には履歴レコードが残っているクライアントが含まれます。

ステップ 15　[Items per page] ドロップダウン リストから、検索結果ページに表示するレコードの数を選択します。

ステップ 16　[Save Search] チェックボックスをオンにして、選択した検索オプションを保存します。

ステップ 17　[Go] をクリックします。

[Clients and Users] ページに、MSE で検出されたすべてのクライアントが表示されます。

MSE で検出されたクライアントの表示

MSE で検出されたすべてのクライアントを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。

[Client and Users] ページが表示されます。

[Clients and Users] テーブルにはデフォルトでいくつかの列が表示されます。使用可能な列を追加して表示する場合は、⚙ をクリックし、[Columns] をクリックします。使用可能な列が表示されます。[Clients and Users] 表に表示する列をクリックします。列内の任意の場所をクリックすると、その列が選択され、クライアントの詳細が表示されます。

ステップ 2　[Show] ドロップダウン リストから [Clients detected by MSE] を選択して、現在のリストをフィルタリングし、MSE で検出されたクライアントをすべて選択します。

有線およびワイヤレスを含め、MSE で検出されたすべてのクライアントが表示されます。

[Clients Detected by MSE] 表では、次のさまざまなパラメータを使用できます。

- [MAC Address] : クライアント MAC アドレス。
- [IP Address] : クライアント IP アドレス。

  [IP Address] 列に表示される IP アドレスは、定義済みの優先順位によって決まります。使用可能な最初の IP アドレスが次の順番で [IP address] テキスト ボックスに表示されます。

  – IPv4 アドレス

  （注）　このリリースでは、ワイヤレス クライアントだけが IPv6 アドレスを使用します。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

  – IPv6 グローバル固有アドレス。このタイプのアドレスが複数ある場合は、クライアントが受信した最新の IPv6 アドレスが表示されます。ユーザがグローバル IPv6 アドレスを 2 つ持っていても、どちらかが期限切れになっている古いルータ アドバタイズメントによって取得したアドレスである場合があるためです。

  – IPv6 ローカル固有アドレス。IPv6 ローカル固有アドレスが複数ある場合は、最新のアドレスが表示されます。

  – IPv6 リンク ローカル アドレス。IPv6 クライアントには少なくとも 1 個のリンク ローカル アドレスが常にあります。

  次のようなさまざまな IPv6 アドレス タイプがあります。

  - リンクローカル ユニキャスト：リンクローカル アドレスは、自動アドレス設定、ネイバー探索、ルータが存在しないときなどのために、単一リンクでのアドレス指定に使用するように設計されています。
  - サイトローカル ユニキャスト：サイトローカル アドレスは、グローバル プレフィックスには必要のない、サイト内部でのアドレス指定に使用するように設計されています。
  - 集約可能グローバル ユニキャスト：集約可能グローバル ユニキャスト アドレスは、グローバル ネットワーク内でクライアントを一意に特定します。パブリック IPv4 アドレスと同等です。クライアントは複数の集約可能グローバル ユニキャスト アドレスを持つことができます。
- [IP Type]：IP アドレス タイプは IPv4 および IPv6 です。
  - グローバル固有
  - 固有ローカル
  - リンク ローカル
- [User Name]：802.1x 認証に基づいたユーザ名。ユーザ名を使用しないで接続されたクライアントの場合は [Unknown] と表示されます。
- [Type]：クライアント タイプを示します。
  -  Lightweight クライアントを示します
  -  有線クライアントを示します
  -  自立クライアントを示します
- [Vendor]：OUI から導き出されたデバイス ベンダー。
- [Device Name]：ネットワーク認証デバイス名。たとえば、WLC、スイッチなどです。
- [Location]：接続しているデバイスのマップ位置。
- [VLAN]：このクライアントのアクセス VLAN ID を示します。
- [Status]：現在のクライアントのステータス。
  - [Idle]：正常の動作。クライアントのアソシエーション要求は拒否されていません。
  - [Auth Pending]：AAA トランザクションを実行しています。
  - [Authenticated]：802.11 認証が完了しています。
  - [Associated]：802.11 アソシエーションが完了しています。これは、現在クライアントがネットワークに接続されていることを示すために有線クライアントでも使用されます。
  - [Disassociated]：802.11 ディスアソシエーションが完了しています。これは、現在クライアントがネットワーク上に存在しないことを示すために有線クライアントでも使用されます。
  - [To Be Deleted]：ディスアソシエーション後にクライアントが削除されます。
  - [Excluded]：セキュリティの脅威と見なされたため、システムによって自動的に無効化されています。
- [Interface]：クライアントが接続するコントローラ インターフェイス（ワイヤレス）またはスイッチ インターフェイス（有線）。
- Protocol
  - [802.11]：ワイヤレス
  - [802.3]：有線
- [Association Time]：最後のアソシエーションの開始時間（ワイヤレス クライアントの場合）。有線クライアントの場合、これは、クライアントがスイッチ ポートに接続した時間です。クライアントがアソシエートされているが、ネットワーク上で問題がある場合は空欄になります。
- [CCX]：Lightweight ワイヤレスのみ。

ステップ 3　[Client and User] ページの MAC アドレスの横にあるオプション ボタンを選択して、アソシエートされたクライアント情報を表示します。次の各クライアント パラメータが表示されます。

- クライアント属性

（注）　クライアントの統計には、クライアント詳細情報の後に統計情報が表示されます。

- 「クライアント統計情報」（P.16-1029）
- 「クライアント IPv6 アドレス」（P.16-1029）
- 「クライアント アソシエーション履歴」（P.16-1029）
- 「Event」（P.16-1030）
- 「Map」（P.16-1030）

クライアント属性

[Clients and Users] リストからクライアントを選択すると、次のクライアント詳細情報が表示されます。クライアントは、MAC アドレスを使用して特定されます。

次の詳細情報が表示されます。

- 全般：次の情報がリストされます。
  - ユーザ名
  - IP アドレス
  - MAC アドレス
  - ベンダー
  - エンドポイント タイプ
  - クライアント タイプ
  - メディア タイプ
  - モビリティ ロール
  - ホスト名
  - E2E
  - 電力節約
  - CCX
  - ファンデーション サービス
  - 管理サービス
  - 音声サービス
  - ロケーション サービス

（注）　ユーザ名の横にある アイコンをクリックすると、ユーザの関連するユーザにアクセスします。

- セッション：次のクライアント セッション情報をリストします。
  - コントローラ名
  - AP 名

  - AP IP アドレス
  - AP タイプ
  - AP ベース無線 MAC
  - アンカー アドレス
  - 802.11 ステート
  - アソシエーション ID
  - ポート
  - インターフェイス
  - SSID
  - プロファイル名
  - プロトコル
  - VLAN ID
  - AP モード
- セキュリティ（ワイヤレス クライアントおよびアイデンティティ有線クライアントのみ）：次のセキュリティ情報をリストします。
  - セキュリティ ポリシー タイプ
  - EAP タイプ
  - ネットワーク上
  - 802.11 認証
  - 暗号化方式
  - SNMP NAC の状態
  - RADIUS NAC の状態
  - AAA Override ACL 名
  - AAA Override ACL の適用された状態
  - リダイレクト URL
  - ACL 名
  - ACL の適用された状態
  - FlexConnect ローカル認証
  - Policy Manager ステート
  - 認証 ISE
  - 許可プロファイル名
  - ポスチャ ステータス
  - TrustSec セキュリティ グループ
  - Windows AD ドメイン

（注）　アイデンティティ クライアントは、認証タイプが 802.1x、MAC 認証バイパス、または Web 認証のクライアントです。アイデンティティ クライアント以外の認証タイプは N/A です。

（注）　クライアント属性の下に表示されるデータは、アイデンティティ クライアントかそうでないかによって異なります。アイデンティティ クライアントの場合は、認証ステータス、監査セッション ID などのセキュリティ情報を確認できます。

- 統計情報（ワイヤレスのみ）
- トラフィック：クライアントのトラフィック情報を表示します。
- ワイヤレス クライアントの場合、クライアントのトラフィック情報はコントローラから取得します。有線クライアントの場合、クライアントのトラフィック情報は ISE から取得するため、スイッチ上でアカウンティング情報およびその他に必要な機能を有効にする必要があります。

クライアント統計情報

[Statistics] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- クライアント AP アソシエーション履歴
- クライアント RSSI 履歴（dBm）: クライアントがアソシエートされたアクセス ポイントで検出された RSSI（受信信号強度インジケータ）の履歴。
- クライアント SNR 履歴 : クライアントがアソシエートされたアクセス ポイントで検出された SNR（クライアント RF セッションの信号対雑音比）の履歴。
- 送受信バイト（Kbps）: アソシエートされたアクセス ポイントで送受信したバイト数。
- 送受信パケット（毎秒）: アソシエートされたアクセス ポイントで送受信したパケット数。

（注）　グラフ上にマウス カーソルを合わせると、その他の統計情報が表示されます。

クライアント IPv6 アドレス

[IPv6 address] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- IP アドレス：クライアント IPv6 アドレスを表示します。
- スコープ：3 種類のスコープがあります。スコープには、グローバル固有、ローカル固有、およびリンク ローカルがあります。
- アドレス タイプ：アドレス タイプを表示します。
- 検出時間：IP が検出された時間です。

クライアント アソシエーション履歴

[Association History] ダッシュレットには、選択したクライアントの過去 10 件のアソシエーション時間に関する情報が表示されます。この情報は、クライアントのトラブルシューティングの際に役立ちます。

[Association History] ダッシュレットには、次の情報が含まれます。

- アソシエーション時間
- 持続時間
- ユーザ名
- IP アドレス
- IP アドレス タイプ
- AP 名

- コントローラ名
- SSID

Event

[Client Details] ページの [Event group] ボックスには、イベント タイプやイベントの日時など、このクライアントのすべてのイベントが表示されます。

- イベント タイプ
- イベント時間
- 説明

Map

[View Location History] をクリックすると、有線クライアントおよびワイヤレス クライアントのロケーション履歴の詳細が表示されます。

有線クライアントおよびワイヤレス クライアントのロケーションの詳細を表示できます。

有線クライアントまたはワイヤレス クライアントの次のロケーション履歴情報が表示されます。

- タイムスタンプ
- ステート
- ポート タイプ
- スロット
- モジュール
- ポート
- ユーザ名
- IP アドレス
- スイッチ IP
- サーバ名
- マップ位置の都市ロケーション

5.0 から 6.0 または 7.0 へのアップグレード

注意　リリース 6.0 以降のリリースにアップグレードする場合、サポートされるクライアント、タグ、およびアクセス ポイント（wIPS）の数は、クライアントが 100 個、タグが 100 個、アクセス ポイントが 20 個にリセットされます。この上限を超える追跡はすべて消失します。この制限は、標準の 120 日間の評価ライセンスに相当します。

注意　モビリティ サービス エンジンを 6.0 から 7.0 にアップグレードすると、ワイヤレス クライアントまたは不正クライアント/アクセス ポイントの上限が設定されている場合、この上限はリセットされます。これは、7.0 では有線クライアントの上限が変更されているためです。

注意　リリース 5.1 または 6.0 から 7.0 にアップグレードする前に、モビリティ サービス エンジン データベースをバックアップして、クライアント、タグ、およびアクセス ポイントの設定を保持します。ソフトウェア アップグレードの後、データベースを復元できます。

（注）　リリース 5.1 ではライセンスに対応していませんでした。120 日間の評価ライセンスの制限を超えて、クライアントとタグの位置（CA）またはアクセス ポイント（wIPS）を追跡するには、ライセンスを注文して登録のうえ、インストールする必要があります。

リリース 7.0 にアップグレードするには、次の手順に従います。

ステップ 1　製品認証キー（PAK）を登録します。

（注）　PAK はライセンス注文時に受け取ります。PAK を紛失した場合は、モビリティ サービス エンジンの販売注文番号または UDI 番号を使用して登録できます。

- クライアントおよび wIPS のライセンスは次のサイトで登録します。
  www.cisco.com/go/license

ステップ 2　モビリティ サービス エンジンのデータベースをバックアップします。

a. [Services] > [Mobility Services] の順に選択します。

b. バックアップを行うモビリティ サービス エンジンの名前をクリックします。

c. [System] > [Maintenance] の順に選択します。

d. [Backup] をクリックします。

e. バックアップ ファイルの名前を入力します。

f. [Submit] をクリックし、Prime Infrastructure が実行されているサーバのハード ドライブに履歴データをバックアップします。

ステップ 3　リリース 7.0 をダウンロードします。

a. [Services] > [Mobility Services] の順に選択します。

b. ソフトウェアをダウンロードする先のモビリティ サービス エンジンの名前をクリックします。

c. 左側のサイドバーのメニューから、[System] > [Maintenance] > [Download Software] の順に選択します。

d. ソフトウェアをダウンロードするには、次のいずれかを実行します。

- Prime Infrastructure ディレクトリにリストされているソフトウェアをダウンロードするには、[Select from uploaded images to transfer into the Server] オプション ボタンを選択します。ドロップダウン リストからバイナリ イメージを選択します。

  Prime Infrastructure のインストール時に指定した FTP サーバ ディレクトリにバイナリ イメージがダウンロードされます。

- ローカルまたはネットワーク経由で使用可能なダウンロード済みソフトウェアを使用するには、[Browse a new software image to transfer into the Server] オプション ボタンを選択し、[Choose File] をクリックします。ファイルを見つけ、[Open] をクリックします。

e. [Download] をクリックし、ソフトウェアをモビリティ サービス エンジンの /opt/installers ディレクトリにダウンロードします。

ステップ 4　MSE CLI を使用してリリース 7.0 をインストールします。

a. 既存のソフトウェアを上書きするには、次を入力してください。

```
/etc/init.d/msed stop
cd opt/installers
./<mse software file name>
```

b. 新規インストールを実行するには、次を入力します。

```
/etc/init.d/msed stop
cd /opt/mes/uninstall
```

./uninstall（ディレクトリでこれを一度入力します）

（古いデータベースを維持するには、プロンプトで指示されたときに **no** と入力します）

```
cd /opt/installers
./<mse software file name>
```

ステップ 5　モビリティ サービス エンジン データベースを復元します（ステップ 4 の b. の場合）。

a. [Services] > [Mobility Services] の順に選択します。

b. ソフトウェアをアップグレードしたモビリティ サービス エンジンの名前をクリックします。

c. 左側のサイドバーのメニューから [Maintenance] > [Restore] の順に選択します。

d. ドロップダウン リストから、復元するファイルの名前を選択します。[Submit] をクリックします。

ステップ 6　ライセンスをインストールします。

詳細については、次の URL で『*ContextAware Services Configuration Guide Release 7.0*』の第 2 章を参照してください。

http://www.cisco.com/en/US/products/ps9806/products_installation_and_configuration_guides_list.html

MSE アラーム詳細の表示

[Monitor] > [Alarms] ページで、[Failure Source] 列の下にある MSE 項目をクリックし、特定の MSE のアラーム詳細にアクセスします。

別の方法として、[Services] > [Mobility Services] > [*MSE Name*] > [System] > [Status] > [Prime Infrastructure Alarms] ページにアクセスし、[Failure Source] 列の下にある特定の MSE 項目をクリックして、特定の MSE のアラーム詳細にアクセスできます。

図 16-1 に、MSE の Prime Infrastructure アラームを示します。

図 16-1　MSE アラーム

表 16-13 では、MSE の [Alarm Detail] ページの各種フィールドについて説明します。

表 16-13　General パラメータ

フィールド	説明
Failure Source	アラームを生成した MSE。
Owner	このアラームの担当者の名前または空欄。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。
Category	アラームのカテゴリ。アラーム カテゴリは、MSE のモビリティ サービスです。
Created	アラームが作成された日時（月、日、年、時、分、秒、AM/PM）。
Modified	最後にアラームが修正された日時（月、日、年、時、分、秒、AM または PM）。
Generated By	このフィールドは MSE と表示されます。
Severity	セキュリティのレベル：Critical（重大）、Major（やや重大）、Minor（比較的重大でない）、Warning（警告）、Clear（クリア）、Info（通知）が色分けして表示されます。
Previous Severity	Critical（重大）、Major（やや重大）、Minor（比較的重大でない）、Warning（警告）、Clear（クリア）、Info（通知）が 色分けして表示されます。

（注）　全般情報は、アラームのタイプによって異なる場合があります。たとえば、アラーム詳細の中に、ロケーションおよびスイッチ ポート トレーシング情報を含む場合もあります。

- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。注釈は [Annotations] 表示ページに表示されます。
- [Messages]：アラームに関する情報が表示されます。
- [Audit Report]：クリックして、設定監査アラームの詳細を表示します。このレポートは、設定監査アラームにだけ使用できます。

  監査の矛盾が設定グループに施行されると、設定監査アラームが生成されます。

（注）　施行が失敗すると、設定グループに重大なアラームが生成されます。施行が成功すると、設定グループに比較的重大でないアラームが生成されます。

アラームには監査レポートへのリンクがあり、各コントローラの矛盾のリストを表示できます。

- [Event History]：[MSE Alarm Events] ページを開き、このアラームのイベントを表示します。アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

Select a command

[Select a command] ドロップダウン リストからは、次の機能にアクセスできます。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。アラームがどのアクセス ポイントでも検出されなくなったことを示します。

（注）　重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。

- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge]：すでに認知しているアラームの認知を解除できます。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Event History]：[Monitor] > [Events] ページに移動し、このアラームのイベントを表示します。

MSE ライセンスの概要

MSE には、次のような関連サービス エンジンとアプリケーション プロセスとともに、ネットワーク トポロジ、NMSP などの設計、ネットワーク リポジトリに関連する複数の製品機能が付属しています。

- Context-Aware サービス
- ワイヤレス侵入防御システム（wIPS）

MSE とそのサービスをスムーズに管理できるように、各種ライセンスが提供されています。

（注）　MSE とその関連サービスを使用するには、Cisco Prime Infrastructure ライセンスが必要です。

ここでは、次の内容について説明します。

- 「MSE ライセンスの構成マトリクス」（P.16-1035）

- 「MSE のライセンス ファイルのサンプル」（P.16-1035）
- 「MSE ライセンスの取り消しと再使用」（P.16-1036）

MSE ライセンスの構成マトリクス

表 16-14 に、MSE、ロケーション サービス、SCM、wIPS および MIR について、ハイエンド、ローエンド、および評価ライセンス間でのライセンスの区別をリストします。

表 16-14　MSE ライセンスの構成マトリクス

	ハイエンド	ローエンド	評価
MSE プラットフォーム	Cisco 3350 および 3355 モビリティ サービス エンジンなどのハイエンド アプライアンスおよびインフラストラクチャ プラットフォーム。	Cisco 3310 モビリティ サービス エンジンなどのローエンド アプライアンスおよびインフラストラクチャ プラットフォーム。	—
Context-Aware サービス	25,000 タグ	2000 タグ	120 日間有効、100 タグおよび 100 要素。
	25,000 要素	2000 要素	
wIPS	3000 アクセス ポイント	2000 アクセス ポイント	120 日間有効、20 アクセス ポイント。

MSE のライセンス ファイルのサンプル

次に、MSE ライセンス ファイルのサンプルを示します。

```
FEATURE MSE cisco 1.0 permanent uncounted \
    VENDOR_STRING=UDI=udi,COUNT=1 \
    HOST ID=ANY \
    NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \
    <PAK>dummyPak</PAK>" \
    SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
    45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
    1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

このサンプル ファイルには、ライセンス エントリが 5 つあります。どのライセンス エントリでも最初の行の先頭の語は、どのタイプのライセンスであるかを示します。これは、Feature または Increment ライセンスのいずれかになります。Feature（機能）ライセンスは、ライセンス付与する唯一の固定アイテムです。MSE で実行しているサービス エンジンは複数ある場合があります。Increment（増分）ライセンスは、追加型のライセンスです。MSE では、個々のサービス エンジンが Increment ライセンスとして扱われます。

最初の行の 2 番めの語は、ライセンス付与する特定のコンポーネントを定義します。たとえば、MSE、LOCATION_TAG などです。3 番めの語はライセンスのベンダーを示します。たとえば、Cisco などです。4 番めの語はライセンスのバージョンを示します。たとえば、1.0 などです。5 番めの語は有効期限を示します。これは、期限のないライセンスの場合は permanent、それ以外の場合は dd-mm-yyyy の形式の日付になります。最後の語は、このライセンスをカウントするかどうかを定義します。

MSE ライセンスの取り消しと再使用

MSE アプリケーション ライセンスをあるシステムから取り消し、別のシステムで再使用できます。ライセンスを取り消すと、ライセンス ファイルはシステムから削除されます。ライセンスを別のシステムで再使用する場合は、ライセンスをリホストする必要があります。

別のシステムでアップグレード SKU を使用してライセンスを再使用する場合は、対応する Base ライセンス SKU を、アップグレード SKU を再使用するシステムにインストールする必要があります。対応する Base ライセンス SKU がシステムから削除された場合、そのシステムではアップグレード ライセンス SKU を再使用できません。

ライセンスを取り消すと、ライセンスに対して変更を反映するため、MSE により個別のサービス エンジンが再起動されます。次に、サービス エンジンは、起動時に MSE から更新された容量を受け取ります。

MSE 仮想アプライアンスの配置

MSE は、仮想アプライアンスとしても提供されます。MSE 仮想アプライアンス ソフトウェアは、Open Virtualization Archive（OVA）ファイルとして配布されます。

（注） VMware 環境のセットアップの詳細については、VMware cSphere 4.0 のドキュメントを参照してください。

（注） 物理アプライアンスの詳細については、『*Cisco Prime Infrastructure Getting Started Guide, Release 1.0*』を参照してください。

物理アプライアンスに MSE を配置する場合、ライセンス インストール プロセスは Cisco UDI（Unique Device Identifier）に基づきます。Prime Infrastructure UI で [Administration] > [License Center] の順に選択して、ライセンスを追加します。仮想アプライアンスに MSE を配置する場合、ライセンスのインストールは、UDI ではなく、VUDI（Virtual Unique Device Identifier）を使用して実行されます。

（注） MSE は、このリリース以降の仮想アプライアンスとして使用できます。仮想アプライアンスは、他のサービスのライセンスをインストールする前に、最初にアクティブにする必要があります。

仮想アプライアンスの場合は、アクティベーション ライセンスが必要です。アクティベーション ライセンスがない場合、MSE は、ホスト上にライセンスが存在する場合でも、評価モードで開始され、アクティベーション ライセンスがインストールされていない場合は永久ライセンスを拒否します。仮想アプライアンスを Prime Infrastructure に追加する場合、Prime Infrastructure では、アクティベーション ライセンスが MSE に追加されない限り、MSE を同期できません。

（注） 仮想ライセンスは物理アプライアンスでは使用できません。

MSE を初めてインストールする場合は [Services] > [Mobility Services Engine] > [Add Mobility Services Engine] ページを使用して、仮想アプライアンス ライセンスを追加および削除できます。または、[Administration] > [License Center] ページを使用してライセンスを追加または削除できます。

モビリティ サービス エンジン ウィザードを使用したライセンスの追加およびライセンスの削除については、「License Center を使用したライセンス ファイルの MSE への追加」（P.16-1037）および「MSE ライセンス ファイルの削除」（P.16-946）を参照してください。

ここでは、次の内容について説明します。

License Center を使用したライセンス ファイルの MSE への追加

ライセンスを追加するには、次の手順を実行します。

ステップ 1　MSE 仮想アプライアンスをインストールします。

ステップ 2　「モビリティ サービス エンジンの追加」（P.16-943）を使用して Prime Infrastructure に MSE を追加します。

ステップ 3　Prime Infrastructure UI で [Administration] > [License Center] の順に選択して、[License Center] ページにアクセスします。

ステップ 4　左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

ステップ 5　[Add] をクリックして、ライセンスを追加します。

[Add A License File] メニューが表示されます。

ステップ 6　MSE を選択し、アクティベーション ライセンス ファイルを参照します。

ステップ 7　[Submit] をクリックします。

送信したら、ライセンスがアクティブになり、[License Center] ページにライセンス情報が表示されます。

License Center を使用した MSE ライセンス情報の表示

License Center では、Prime Infrastructure、ワイヤレス LAN コントローラ、および MSE のライセンスを管理できます。ライセンス情報を表示するには、次の手順を実行します。

ステップ 1　[Administration] > [License Center] を選択して、[License Center] ページにアクセスします。

ステップ 2　左側のサイドバーのメニューから、[Summary] > [MSE] を選択して、概要ページを表示します。

[MSE Summary] ページに次の情報が表示されます。表 16-15 を参照してください。

表 16-15　General パラメータ

フィールド	説明
MSE Name	MSE ライセンス ファイルのリスト ページへのリンクを提供します。
Service	使用するサービスのタイプ（CAS または wIPS）。
Platform Limit	プラットフォームの制限。

表 16-15　General パラメータ （続き）

フィールド	説明
Type	MSE のタイプを指定します。
Installed Limit	MSE 上でライセンス付与されたクライアント要素の合計数を表示します。
License Type	3 つの異なるタイプのライセンス。永久、評価、および拡張があります。
Count	MSE 上で現在ライセンス付与されている CAS または wIPS の要素数。
Unlicensed Count	ライセンス付与されていないクライアント要素の数を表示します。
%Used	MSE 上でライセンス付与されている CAS または wIPS の要素の割合。

License Center を使用したライセンス ファイルの削除

ライセンスを削除するには、次の手順を実行します。

ステップ 1　MSE 仮想アプライアンスをインストールします。

ステップ 2　ウィザードを使用して Prime Infrastructure に MSE を追加します。

ステップ 3　Prime Infrastructure UI で [Administration] > [License Center] の順に選択して、[License Center] ページにアクセスします。

ステップ 4　左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

ステップ 5　オプション ボタンを選択して、削除する MSE ライセンス ファイルを選択し、[Remove] をクリックします。

ステップ 6　[OK] をクリックして、削除を実行します。

自動スイッチ ポート トレーシングおよび不正 AP の自動封じ込め

現在、Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、ネイバー リストにないフレームから検出された BSSID アドレスが記載されています。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方法を使用した場合、Prime Infrastructure では、そのまま、コントローラから受信した情報を収集します。一方、ソフトウェア リリース 5.1 から、有線の不正アクセス ポイントのスイッチ ポートに関するスイッチ ポート トレーシングを組み込むことができます。

自動 SPT と封じ込めは、リリース 7.3 で導入されました。自動 SPT は、大規模なワイヤレス ネットワークにより適しています。不正 AP が Prime Infrastructure に報告されると、自動 SPT が自動的に起動します。自動 SPT は、不正 AP の有線ロケーション アソシエーションに基づく高速スキャンを提供することで、手動 SPT 機能を補完します。トレースを実行し、回線上で検出された不正アクセス ポイントを封じ込められるようにするために、Prime Infrastructure UI を使用して、自動 SPT および自動封じ込めの基準を設定できます。

不正 AP を自動的に封じ込める必要があることを複数のコントローラが報告した場合、Prime Infrastructure は最も強い RSSI を報告したコントローラを検出し、そのコントローラに封じ込め要求を送信します。

Prime Infrastructure での自動スイッチ ポート トレーシング基準の設定

Prime Infrastructure で自動スイッチ ポート トレーシングを設定するには、次の手順に従います。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Rogue AP Settings] を選択します。[Rogue AP Settings] ページが表示されます。

ステップ 3　[Enable Auto Switch Port Tracing] チェックボックスをオンにして、Prime Infrastructure が、不正アクセス ポイントが接続されているスイッチ ポートを自動的にトレースできるようにします。次のパラメータを設定できます。

- [Repeat Search After]：分単位の時間を入力します。この時間が経過した後、Prime Infrastructure は不正 AP の検索を自動的に繰り返します。デフォルトでは、Prime Infrastructure は 120 分おきに不正 AP の検索を繰り返します。
- [Allow Trace For Found On Wire Rogue AP]：有線の不正 AP をトレースする自動 SPT を有効にするには、このチェックボックスをオンにします。
- [Critical]：アラーム重大度を critical に設定するには、このチェックボックスをオンにします。
- [Major]：アラーム重大度を major に設定するには、このチェックボックスをオンにします。
- [Minor]：アラーム重大度を minor に設定するには、このチェックボックスをオンにします。

ステップ 4　[OK] をクリックします。

Prime Infrastructure での自動封じ込めの設定

Prime Infrastructure で自動封じ込めを設定するには、次の手順に従います。

ステップ 1　[Administration] > [Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Rogue AP Settings] を選択します。[Rogue AP Settings] ページが表示されます。

ステップ 3　[Enable Auto Containment] チェックボックスをオンにして、Prime Infrastructure が不正 AP を受信した場合に自動封じ込めをトリガーできるようにします。次のパラメータを設定できます。

- [Exclude Rogue APs Found On Wire By Switch Port Tracing]：自動 SPT を通じて有線ネットワークで検出された AP を自動的に除外するには、このチェックボックスをオンにします。
- [Critical]：アラーム重大度を critical に設定するには、このチェックボックスをオンにします。
- [Major]：アラーム重大度を major に設定するには、このチェックボックスをオンにします。
- [Containment Level]：自動封じ込めレベルを有効にするには、このチェックボックスをオンにします。これは、不正 AP の封じ込めレベルを示します。
  - [1 AP Containment]：不正アクセス ポイントを 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。これを選択すると、不正な機器の近辺にある 1 つのアクセス ポイントが、不正な機器にアソシエートされているクライアント デバイスに、認証解除とアソシエート解除のメッセージを送信します。

- [2 AP Containment] : 不正アクセス ポイントを 2 つの Cisco Lightweight アクセス ポイントで封じ込めます。不正な機器の近辺にある 2 つのアクセス ポイントが、不正クライアントに、認証解除とアソシエート解除のメッセージを送信します。
- [3AP Containment] : 不正アクセス ポイントを 3 つの Cisco Lightweight アクセス ポイントで封じ込めます。
- [4AP Containment] : 不正アクセス ポイントを 4 つの Cisco Lightweight アクセス ポイントで封じ込めます （最大封じ込めレベル）。

（注） 不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。

注意 不正アクセス ポイントの封じ込めは法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

ステップ 4　[OK] をクリックします。

Context Aware ダッシュボードからのロケーション アシストされるクライアントのトラブルシューティング

Prime Infrastructure ホームページの [Context Aware] タブを使用して、クライアントのトラブルシューティングを実行できます。

MAC アドレス、ユーザ名、または IP アドレスを検索条件として指定し、[Troubleshoot] をクリックします。

（注） ユーザ名、IP アドレス、および部分的な MAC アドレスベースのトラブルシューティングは、バージョン 7.0.200.0 以降の MSE でのみサポートされます。

[Troubleshoot Client] ページが表示されます。

[Context Aware History] タブで Context Aware 履歴レポートを表示できます。

このレポートを MSE 名に基づいてフィルタリングできます。さらにタイムゾーン、状態、またはすべてに基づいて、レポートをフィルタリングできます。状態は、アソシエート済みまたはディスアソシエート済みのいずれかです。

タイムゾーンを選択した場合は、次のいずれかを選択できます。

- **日付と時刻**

または

- ドロップダウン リストの次のいずれかの値 :
  - **Last 1 Hour**
  - **Last 6 Hours**
  - **Last 1 Day**
  - **Last 2 Days**

- **Last 3 Days**
- **Last 4 Days**
- **Last 5 Days**
- **Last 6 Days**
- **Last 7 Days**
- **Last 2 Weeks**
- **Last 4 Weeks**

別の方法として、[Generate Report] リンクを使用して、クライアント ロケーション履歴レポートを生成できます。また、レポート ページにあるアイコンを使用して、CSV または PDF 形式にエクスポートすることや、レポートを電子メールで送信することができます。

MSE 分析レポート

レポート ラウンチ パッドを使用して複数の MSE 分析レポートを生成できます。

マップのモニタリング

マップでは、キャンパス、ビルディング、屋外領域、およびフロア上のすべての管理対象システムの概要を表示できます。マップの詳細については、「マップについて」（P.6-153）を参照してください。

モバイル コンシェルジュ サービス

モバイル コンシェルジュ サービスにより、場所所有者とサービス プロバイダーは WLAN をモニタできます。モバイル コンシェルジュ サービスは、スマート フォンを使用している顧客に固有のストア内エクスペリエンスを提供します。

モバイル コンシェルジュ サービスは、ネットワーク接続を確立するための一連のポリシーを使用して設定されたワイヤレス スマート フォンを使用します。モバイル コンシェルジュ サービスにより、使用可能なネットワーク ベースのサービスをスマート フォンで簡単に検出できます。ストアの Wi-Fi ネットワークに接続した後、ストアのワイヤレス ゲスト ネットワークに参加して、電子クーポン、プロモーション オファー、顧客ロイヤルティ データ、製品提案、ショッピング リストの編成機能など、さまざまなサービスにアクセスしたり、ショッピング設定に基づいて固有のデジタル署名を受け取ることができます。

ここでは、次の内容について説明します。

- 「設定済みサービス アドバタイズメントの表示」（P.16-1047）
- 「モバイル コンシェルジュ ライセンス情報の [MSE Summary] ページの表示」（P.16-1048）
- 「サービス アドバタイズメントの同期ステータスの表示」（P.16-1048）
- 「License Center を使用したモバイル コンシェルジュ サービス ライセンスの追加」（P.16-1048）
- 「モバイル コンシェルジュ レポート」（P.16-1048）

モバイル コンシェルジュのライセンス

モバイル コンシェルジュ サービスは、有効な拡張ロケーション ライセンス（Base ロケーション ライセンス、モバイル コンシェルジュ、および Analytics ライセンス）がある場合にのみ有効にすることができます。評価ライセンスは 120 日間有効です。永久ライセンスは、MSE プラットフォームとサポートされるサービス アドバタイズメントの数に基づきます。

場所の定義

場所を定義するには、次の手順に従います。

ステップ 1　[Services] > [Mobile Concierge] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Mobile Concierge Services] > [Venues] の順に選択します。

[Venues] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Define New Venue] を選択し、[Go] をクリックします。

[Venue Wizard] ページが表示されます。

ステップ 4　[Venue Name] テキスト ボックスに場所の名前を入力し、[Next] をクリックします。

ステップ 5　[Floor/Outdoor Association] グループ ボックスで、以下を設定できます。

- [Area Type] ドロップダウン リストから、サービス アドバタイズメントを表示するエリア タイプを選択します。指定できる値は、[Floor Area] および [Outdoor Area] です。

（注）　エリア タイプとして [Floor Area] を選択した場合に限り、[Building, Floor Area, and Coverage Area] ドロップダウン リストが表示されます。

- [Campus] ドロップダウン リストから、サービス アドバタイズメントを表示させるキャンパス名を選択します。
- [Building] ドロップダウン リストから、アドバタイズメントを表示させるビルディング名を選択します。
- [Floor] ドロップダウン リストから、フロア タイプを選択します。
- [Coverage Area] ドロップダウン リストから、フロア内のカバレッジ領域を選択します。
- [Outdoor Area] ドロップダウン リストから、サービス アドバタイズメントを表示する屋外領域を選択します。このフィールドは、エリア タイプとして [Outdoor Area] を選択した場合にのみ表示されます。

ステップ 6　[Next] をクリックします。[Audio] グループ ボックスが表示されます。

ステップ 7　[Audio] グループ ボックスで [Choose File] をクリックして、オーディオ通知を再生するためのオーディオ ファイルを参照して選択します。

ステップ 8　[Next] をクリックします。[Icons] グループ ボックスが表示されます。

ステップ 9　[Icons] グループ ボックスで [Choose File] をクリックして、クライアント無線端末に表示するアイコンを参照して選択します。

ステップ 10　[Next] をクリックします。[Venue Apps] グループ ボックスが表示されます。

ステップ 11　[Venue Apps] グループ ボックスで [Web App] ドロップダウン リストから、サービス アドバタイズメントを表示する場所アプリケーションを選択します。

ステップ 12　[Next] をクリックします。[Additional Venue Information] グループ ボックスが表示されます。

ステップ 13　[Additional Information] グループ ボックスで、場所でモバイル アプリケーションに提供する追加情報を指定できます。次の設定を行えます。

- [Location Detail] テキスト ボックスに場所の詳細情報を入力します。ここでは、場所のストア アドレス、郵便番号、住所などの詳細を指定します。
- [Latitude and Longitude] テキスト ボックスに、場所の GPS 緯度および経度を入力します。これにより、アプリケーションは場所を正確に特定できます。
- [Additional Information] テキスト ボックスに、場所でモバイル アプリケーションに提供する追加情報を入力します。

ステップ 14　[Save] をクリックします。この情報は MSE に適用され、自動的に同期されます。

場所の削除

場所を削除するには、次の手順に従います。

ステップ 1　[Services] > [Mobile Concierge] の順に選択します。

[Venues] ページが表示されます。

ステップ 2　削除する場所のチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Delete Venue] を選択し、[Go] をクリックします。

ステップ 4　[OK] をクリックして、削除を実行します。

ポリシーを使用したプロバイダーの定義

ステップ 1　[Service] > [Mobile Concierge] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Mobile Concierge Services] > [Providers] の順に選択します。

[Providers] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Define New Provider] を選択し、[Go] をクリックします。

[Provider Wizard] ページが表示されます。

ステップ 4　[Provider Name] テキスト ボックスにプロバイダーの名前を入力します。

ステップ 5　[Next] をクリックします。[Icons] グループ ボックスが表示されます。

ステップ 6　[Icons] グループ ボックスで [Choose File] をクリックして、クライアント無線端末に表示するアイコンを参照して選択します。

ステップ 7　[Next] をクリックします。[Local Services] グループ ボックスが表示されます。

ステップ 8　[Local Services] グループ ボックスで、次の手順を実行します。

- [Local Service # name] の左側にある青色の逆三角形アイコンをクリックして [Local Service] を展開し、以下を設定します。
  - [Service Type] ドロップダウン リストからサービス タイプを選択します。選択可能なオプションは、[Directory Info]、[Sign Up]、[Discount Coupon]、[Network Help]、および [Other] です。
  - [Display Name] テキスト ボックスに表示名を入力します。
  - [Description] テキスト ボックスに説明を入力します。
  - ドロップダウン リストからサービス URI を選択します。
  - [Recommended Apps]：場所用の推奨アプリケーション

ステップ 9　[Save] をクリックします。

サービス プロバイダーの削除

サービス プロバイダーを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Mobile Concierge] の順に選択します。

[Venues] ページが表示されます。

ステップ 2　左側のサイドバーのメニューから [Mobile Concierge Services] > [Providers] の順に選択します。

[Providers] ページが表示されます。

ステップ 3　削除するプロバイダーのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから、[Delete Provider] を選択し、[Go] をクリックします。

[OK] をクリックして、削除を実行します。

新しいポリシーの定義

ポリシーを定義するには、次の手順に従います。

ステップ 1　[Services] > [Mobile Concierge] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Mobile Concierge Services] > [Policies] の順に選択します。

[Policies] ページが表示されます。

ステップ 3　[Select a command] ドロップダウン リストから、[Define New Policy] を選択し、[Go] をクリックします。

[Policy Wizard] ページが表示されます。

ステップ 4　[Venue] ドロップダウン リストから、ポリシーを適用する場所を選択します。

ステップ 5　[Next] をクリックします。[Provider] グループ ボックスが表示されます。

ステップ 6　[Provider] ドロップダウン リストからプロバイダーを選択します。

ステップ 7　[Next] をクリックします。[SSID] グループ ボックスが表示されます。

ステップ 8　[SSID] ドロップダウン リストから、サービス アドバタイズメントをブロードキャストする SSID を選択し、[OK] をクリックします。複数の SSID を選択できます。

ステップ 9　[Next] をクリックします。[Display Rule] グループ ボックスが表示されます。

ステップ 10　[Display Rule] グループ ボックスで、次の操作を実行できます。

- [Display Rule] オプション ボタンをオンにします。[Display everywhere] または [Display near selected APs] オプション ボタンのいずれかを選択できます。デフォルトでは、[Display everywhere] が選択されています。

[Display everywhere] を選択した場合、これらの SSID を提供するすべてのモバイル コンシェルジュ対応コントローラが検索され、それらのコントローラが MSE に割り当てられます。

[Display near selected APs] を選択した場合、次のパラメータを設定できます。

- [AP] : アドバタイズメントをブロードキャストする AP を選択します。
- [Radio] : アドバタイズメントをブロードキャストする無線周波数を選択します。選択した無線帯域の近くにモバイルデバイスがある場合、サービス アドバタイズメントが表示されます。指定できる値は 2.4 GHz または 5 GHz です。
  - [min RSSI] : ユーザ インターフェイスにサービス アドバタイズメントを表示する RSSI の値を入力します。

ステップ 11　[Finish] をクリックします。

新しいポリシーの削除

新しいポリシーを削除するには、次の手順に従ってください :

ステップ 1　[Services] > [Mobile Concierge] の順に選択します。

[Venues] ページが表示されます。

ステップ 2　左側のサイドバーのメニューから [Mobile Concierge Services] > [Policies] の順に選択します。

[Policies] ページが表示されます。

ステップ 3　削除するポリシーのチェックボックスをオンにします。

ステップ 4　[Select a command] ドロップダウン リストから、[Delete Policy] を選択し、[Go] をクリックします。

[OK] をクリックして、削除を実行します。

フロア マップへのサービス アドバタイズメントの追加

フロア マップ内のカバレッジ領域にサービス アドバタイズメントを追加するには、次の手順に従います。

ステップ 1　[Monitor] > [Site Maps] を選択します。

[Site Maps] ページが表示されます。

ステップ 2　リストから該当するフロア ロケーション リンクを選択します。

マップが表示され、インストールされているすべてのアクセス ポイント、クライアント、およびタグの配置とそれらの相対的な信号強度が表示されます。

ステップ 3　フロア マップ ページで [Services] アイコンをクリックします。

サービス アドバタイズメントをその特定の場所にアソシエートするための [Venue] ダイアログボックスが表示されます。

ステップ 4　[Show/Associate Services] リンクをクリックして [Add/Edit Mobile Concierge Service Services] ページを開きます。

使用可能なすべてのサービス アドバタイズメントのリストが表示されます。これらを選択して、サービス アドバタイズメントをアソシエートできます。

ステップ 5　サービス アドバタイズメントをアソシエートするために、次の操作を実行できます。

- [Filter By] ドロップダウン リストからプロバイダー名またはフレンドリ名を選択して、これらの名前に基づいてフィルタリングすることでアドバタイズメントを選択します。

  または

- [Associate] チェックボックスをオンにして、特定のサービス アドバタイズメントをアソシエートします。

ステップ 6　[OK] をクリックします。

フロア マップからのサービス アドバタイズメントの作成

フロア マップからサービス アドバタイズメントを作成するには、次の手順に従います。

ステップ 1　[Monitor] > [Site Maps] を選択します。

[Site Maps] ページが表示されます。

ステップ 2　リストから該当するフロア ロケーション リンクを選択します。

マップが表示され、インストールされているすべてのアクセス ポイント、クライアント、およびタグの配置とそれらの相対的な信号強度が表示されます。

ステップ 3　フロア マップ ページで [Services] アイコンをクリックします。

サービス アドバタイズメントをその特定の場所にアソシエートするための [Venue] ダイアログボックスが表示されます。

ステップ 4　[Show/Associate Services] リンクをクリックして [Add/Edit Mobile Concierge Services] を開きます。

使用可能なすべてのサービス アドバタイズメントのリストが表示されます。これらを選択して、サービス アドバタイズメントをアソシエートできます。

ステップ 5　サービス アドバタイズメントを作成するには、[Create Mobile Concierge Service] をクリックします。

[Service] > [Mobile Concierge] > [Add Service Advertisements] ページにリダイレクトされます。

ステップ 6　「フロア マップへのサービス アドバタイズメントの追加」（P.16-1045）の手順に従い、提供するサービス アドバタイズメントを作成します。

設定済みサービス アドバタイズメントの表示

設定済みのサービス アドバタイズメントを表示するには、次の手順を実行します。

ステップ 1　[Services] > [Mobility Services Engine] の順に選択します。

ステップ 2　[Device Name] をクリックして、そのプロパティを表示します。

[General Properties] ページが表示されます。

ステップ 3　左側のサイドバーのメニューから、[Mobile Concierge Service] > [Advertisements] の順に選択します。

[Mobile Concierge Service] ページに次の情報が表示されます。

- [Icon]：サービス プロバイダーに関連付けられたアイコンを表示します。
- [Provide Name]：サービス プロバイダー名を表示します。
- [Venue Name]：場所の名前を表示します。
- Advertisements
  - [Friendly Name]：ヘッドセットに表示されるわかりやすい名前。
  - [Advertisement Type]：ヘッドセットに表示されるアドバタイズメントのタイプ。

モバイル コンシェルジュ サービスの統計情報の表示

モバイル コンシェルジュ サービスの統計情報を表示するには、次の手順に従います。

ステップ 1　[Services] > [Mobility Services Engine] の順に選択します。

ステップ 2　[Device Name] をクリックして、そのプロパティを表示します。

[General Properties] ページが表示されます。

ステップ 3　左側のサイドバーのメニューから、[Mobile Concierge service] > [Statistics] の順に選択します。

[Mobile Concierge Service] ページに次の情報が表示されます。

- [Top 5 Active Mobile MAC addresses]：特定の場所で最もアクティブなモバイルについての情報を表示します。
- [Top 5 Service URIs]：特定の場所またはプロバイダー上でサービスの使用量についての情報を表示します。

モバイル コンシェルジュ ライセンス情報の [MSE Summary] ページの表示

MSE ライセンスの詳細については、「モビリティ サービス エンジン（MSE）ライセンスの管理」（P.15-933）を参照してください。

サービス アドバタイズメントの同期ステータスの表示

サービス アドバタイズメントの同期ステータスを表示するには、次の手順を実行します。

ステップ 1　[Services] > [Synchronize Services] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Service Advertisements] を選択します。

[Service Advertisements] ページに次の情報が表示されます。

- [Provider Name]：サービス プロバイダーの名前を表示します。
- [Service]：特定のアドバタイズメントが使用しているサービスのタイプを表示します。
- [MSE]：サービス アドバタイズメントが MSE と同期しているかどうかを表示します。
- [Sync Status]：同期ステータスを表示します。緑の 2 つの矢印アイコンは、その対応する要素が、MSE などの指定されたサーバと同期していることを示します。灰色の 2 つの矢印と赤い円のアイコンは、対応する項目が指定のサーバと同期していないことを示します。
- [Message]：アドバタイズメントの同期の失敗に関連するメッセージがあれば表示します。

License Center を使用したモバイル コンシェルジュ サービス ライセンスの追加

License Center を使用してモバイル コンシェルジュ サービス ライセンスを追加するには、次の手順に従います。

ステップ 1　[Administration] > [Licenses] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

[License Center] ページが表示されます。

ステップ 3　[Add] をクリックして、ライセンス ファイルを選択します。

ステップ 4　[OK] をクリックしてライセンスを追加します。

モバイル コンシェルジュ サービス ライセンスが追加されます。

モバイル コンシェルジュ レポート

2 種類のモバイル コンシェルジュ レポートを生成できます。

- サービス URI 統計情報：このレポートでは、場所、プロバイダー、モバイル Mac などのフィルタに基づいて、使用した上位サービスについての情報を取得できます。このレポートでは、特定の場所でのサービスの使用量についての追加情報も取得できます。
- モバイル MAC 統計情報：このレポートでは、場所などのフィルタに基づいて、最もアクティブなクライアントについての情報を取得できます。このレポートでは、特定の場所で最もアクティブなモバイルについての追加情報も取得できます。

Identity Services

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

Prime Infrastructure は、ネットワーク上の有線クライアントとワイヤレス クライアントの両方を管理します。クライアントの認証に Cisco ISE を RADIUS サーバとして使用する場合、Prime Infrastructure は ISE からこれらのクライアントに関する詳細情報を収集し、単一のコンソールで表示するために関連するすべてのクライアント情報が Prime Infrastructure に提供されます。

（注）　Prime Infrastructure は REST API を使用して ISE と通信します。Cisco ISE API の詳細については、http://www.cisco.com/en/US/docs/security/ise/1.0/api_ref_guide/ise10_api_ref_guide_ch1.html を参照してください。

（注）　有線クライアントのアカウンティング データは、15 分ごとに ISE から収集されます。ISE のステータスを得るため、Prime Infrastructure に追加されたすべての ISE を 15 分ごとにポーリングし、ステータスを更新するバックグラウンド ISE ステータス タスクがあります。

Prime Infrastructure の ISE 統合は次の機能を提供します。

- ISE に対する定期的なポーリング。クライアント リスト、ダッシュボード グラフ、およびレポートに必要なクライアント統計情報やその他の属性を収集します。
- ISE へのオンデマンド クエリー。許可プロファイル、ポスチャ、エンドポイント タイプ（プロファイラ）などの追加のクライアント詳細を取得します。
- 自動シングル サインオンによる ISE ユーザ インターフェイスの相互起動。

ISE の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.0*』（URL：http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html）を参照してください。

ここでは、次の内容について説明します。

- 「アイデンティティ サービスの表示」（P.16-1049）
- 「アイデンティティ サービス エンジンの追加」（P.16-1050）
- 「アイデンティティ サービス エンジンの削除」（P.16-1050）

アイデンティティ サービスの表示

Prime Infrastructure に追加されているアイデンティティ サービス エンジンを確認するには、[Services] > [Identity Services] の順に選択します。次のパラメータが表示されます。

- [Server Address] : ISE の IP アドレス。
- [Port] : サーバの HTTPS ポート番号。
- [Retries] : 再試行回数を示します。
- [Version] : ISE のバージョンを示します。
- [Status] : 到達可能性ステータス、つまり、Reachable（到達可能）か Unreachable（到達不能）かを示します。
- [Role] : ノードがプライマリ ノード、スタンドアロン ノード、またはスタンバイ ノードのいずれであるかを示します。

アイデンティティ サービス エンジンの追加

（注）　最大 2 つの ISE を Prime Infrastructure に追加できます。2 つの ISE を追加すると、1 つはプライマリで、他方はスタンバイになります。スタンドアロン ノードを追加している場合は、スタンドアロン ノードを 1 つだけ追加でき、2 つ目のノードは追加できません。

アイデンティティ サービス エンジンを追加するには、次の手順を実行します。

ステップ 1　[Services] > [Identity Services] を選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[Add Identity Services Engine] を選択します。

ステップ 3　[Server Address] テキスト ボックスに、サーバの IP アドレスを入力します。

ステップ 4　[Port] テキスト ボックスに、サーバのポート番号を入力します。デフォルトは 443 です。

ステップ 5　[Username] テキスト ボックスに、ユーザ名を入力します。

ステップ 6　[Password] テキスト ボックスに、パスワードを入力します。

ステップ 7　[Confirm Password] テキスト ボックスにパスワードを再入力します。

（注）　資格情報として、スーパーユーザの資格情報が必要です。それ以外の場合、ISE の統合は機能しません。

ステップ 8　[HTTP Connection Timeout] テキスト ボックスで、プロセスがタイムアウトになるまでの許容時間（秒単位）を入力します。デフォルトは 30 秒です。

ステップ 9　[Save] をクリックします。

アイデンティティ サービス エンジンの削除

アイデンティティ サービス エンジンを削除するには、次の手順を実行します。

ステップ 1　[Services] > [Identity Services] を選択します。

ステップ 2　削除するアイデンティティ サービス エンジンのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから、[Delete Identity Services Engine(s)] を選択します。

ステップ 4　[OK] をクリックして、削除を実行します。

Tools

[Tools] メニューでは、Cisco Prime Infrastructure の Voice Audit、Location Accuracy Tool、Configuration Audit Summary、および Migration Analysis 機能にアクセスできます。この章の内容は、次のとおりです。

Voice Audit の実行

Prime Infrastructure には、コントローラの設定を確認し、導入ガイドラインからの逸脱を Audit Violation として強調表示するための、音声監査メカニズムが用意されています。

Voice Audit 機能にアクセスするには、[Tools] > [Voice Audit] の順に選択します。[Voice Audit Report] ページが表示されます。

このページには、[Controllers]、[Rules]、[Reports] の 3 つのタブがあります。

- [Controllers] タブでは、音声監査を実行するコントローラを選択できます。
- [Rules] タブでは、この音声監査の該当する VoWLAN SSID と該当するルールを指示できます。
- [Report] タブでは、音声監査の概要とレポート結果が表示されます。

Voice Audit 機能にアクセスするには、[Tools] > [Voice Audit] の順に選択します。

ここでは、次の内容について説明します。

コントローラに対する音声監査の実行

[Controllers] タブでは、音声監査を実行するコントローラを選択できます。

（注）　1 回の操作で、最大 50 台のコントローラで音声監査を実行できます。

音声監査用のコントローラを選択するには、次の手順を実行します。

ステップ 1　[Tools] > [Voice Audit] の順に選択します。

ステップ 2　[Controllers] タブをクリックします。

ステップ 3　[Run audit on] ドロップダウン リストから、[All Controllers] 、[A Floor Area]、または [A Single Controller] を選択します。

- [All Controllers]：追加のコントローラ情報は不要です。
- [A Floor Area]：ドロップダウン リストから、該当するキャンパス、ビルディング、フロア、およびコントローラを選択します。
- [A Single Controller]：該当するコントローラをドロップダウン リストから選択します。

ステップ 4　音声監査のルールを決定するには、[Rules] タブをクリックします。詳細については、「音声監査ルールの選択」（P.17-1054）を参照してください。

音声監査ルールの選択

[Rules] タブでは、この音声監査の該当する VoWLAN SSID と該当するルールを指示できます。

音声監査用のルールを指定するには、次の手順を実行します。

ステップ 1　[Tools] > [Voice Audit] ページで、[Rules] タブをクリックします。

ステップ 2　該当する VoWLAN SSID を [VoWLAN SSID] テキスト ボックスに入力します。

ステップ 3　[Rules List] から、この音声監査用の該当するルールのチェックボックスをオンにします（表 17-1 を参照）。

（注）　赤い円は無効なルールを示します（データが不十分なため）。緑の円は有効なルールを示します。

表 17-1　音声監査のルール リスト

ルール	ルールの詳細
VoWLAN SSID	説明：VoWLAN SSID が存在するかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
CAC: 7920	説明：7920 AP CAC が VoWLAN で有効になっているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
CAC: 7920 Clients	説明：7920 クライアント CAC が VoWLAN で無効になっているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。

表 17-1　音声監査のルール リスト （続き）

ルール	ルールの詳細
DHCP Assignment	説明：DHCP の割り当てが VoWLAN で無効になっているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
MFP Client	説明：VoWLAN で MFP クライアント保護が [Required] に設定されていないかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
Platinum QoS	説明：VoWLAN で QoS が Platinum（Voice）に設定されているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
Non Platinum QoS	説明：非 VoWLAN で QoS が Platinum に設定されていないことを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
WMM	説明：WMM が VoWLAN で有効になっているかどうかを確認します。 ルール データ：ドロップダウン リストから [Allowed] または [Required] を選択します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
CCKM	説明：CCKM が VoWLAN で有効になっているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
CCKM With No AES- for 792x phones	説明：VoWLAN 向け Cisco Centralized Key Management（CCKM）を使用して AES 暗号化が有効になっていないことを確認します。このルールは、792x 電話機専用です。 ルールの有効性：ユーザ定義の VoWLAN SSID。
TSM	説明：Traffic Stream Metrics（TSM）が有効になっていることを確認します。 ルール データ：[802.11a/n TSM] と [802.11b/g/n TSM] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。
DFS	説明：Channel Announcement と Channel Quite Mode の両方で、動的周波数選択（DFS）が有効になっているかどうかを確認します。
ACM	説明：アドミッション制御が有効になっているかどうかを確認します。 ルール データ：[802.11a/n ACM] と [802.11b/g/n ACM] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。

表 17-1　音声監査のルール リスト （続き）

ルール	ルールの詳細
DTPC	説明：動的送信電力制御が有効になっているかどうかを確認します。 ルール データ：[802.11a/n DTPC] と [802.11b/g/n DTPC] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。
Expedited Bandwidth	説明：緊急帯域幅が有効になっているかどうかを確認します。 ルール データ：[802.11a/n Expedited Bandwidth] と [802.11b/g/n Expedited Bandwidth] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。
Load Based CAC	説明：負荷ベースのアドミッション制御（CAC）が有効になっているかどうかを確認します。 ルール データ:[802.11a/n Load Based CAC] と [802.11b/g/n Load Based CAC (LBCAC)] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。
CAC: Max Bandwidth	説明：コール アドミッション制御の最大 RF 帯域幅が適切に設定されているかどうかを確認します。 ルール データ：テキスト ボックスに、802.11a/n と 802.11b/g/n の最大許容帯域幅のパーセンテージを入力します。 ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 0 ～ 100 % です。
CAC: Reserved Roaming Bandwidth	説明：コール アドミッション制御の予約済みローミング帯域幅が適切に設定されているかどうかを確認します。 ルール データ：テキスト ボックスに、802.11a/n と 802.11b/g/n の最大予約済みローミング帯域幅のパーセンテージを入力します。 ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 0 ～ 100 % です。
Pico Cell mode	説明：ピコ セル モードが無効になっているどうかを確認します。 ルール データ：[802.11a/n Pico Cell mode] と [802.11b/g/n Pico Cell mode] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。

表 17-1　音声監査のルール リスト （続き）

ルール	ルールの詳細
Beacon Period	説明：ビーコン周期が適切に設定されているかどうかを確認します。 ルール データ：テキスト ボックスに、11a/n および 11b/g/n のビーコン周期（ミリ秒単位）を入力します。 ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 20 ～ 1000 です。帯域を検査しない場合は、0 を入力するか、空のままにします。
Short Preamble	説明：短いプリアンブルが 11b/g で有効かどうかを確認します。
Fragmentation Threshold	説明：フラグメンテーションしきい値が適切に設定されているかどうかを確認します。 ルール データ：テキスト ボックスに、11a/n と 11b/g/n のフラグメンテーションしきい値（バイト単位）を入力します。 ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 256 ～ 2346 です。帯域を検査しない場合は、0 を入力するか、空のままにします。
Data Rate	説明：データ レートが適切に設定されているかどうかを確認します。 11b/g のデータ レート設定：各 Mbps カテゴリで、[Disabled] 、[Supported] 、または [Mandatory] を選択します。 11a のデータ レート設定：各 Mbps カテゴリで、[Disabled] 、[Supported] 、または [Mandatory] を選択します。
Aggressive Load Balancing	説明：アグレッシブ ロード バランシングが無効になっているかどうかを確認します。
QoS Profile	説明：QoS プロファイルがデフォルト値から変更されていないかどうかを確認します。
EAP Request Timeout	説明：EAP 要求タイムアウトが適切に設定されているかどうかを確認します。 ルール データ：EAP 要求タイムアウトの時間制限（秒単位）を入力します。 ルールの有効性：データを空白のままにしたりゼロを設定したりできません。有効な範囲は 1 ～ 120 です。
ARP Unicast	説明：ARP ユニキャストが無効になっているどうかを確認します。

（注）　値をデフォルト設定にリセットするには [Reset] をクリックします。

ステップ 4　この音声監査でルールが設定されている場合、[Save] をクリックして現在の設定を保存するか、[Save and Run] をクリックし設定を保存してレポートを実行します。

ステップ 5　レポート結果を表示するには [Report] タブをクリックします。詳細については、「音声監査レポートの詳細」（P.17-1058）を参照してください。

音声監査レポートの詳細

音声監査の詳細では、次の情報が表示されます。

- [Audit Status]：監査が完了しているかどうかを示します。
- [Start Time and End Times]：音声監査が開始および終了した時刻を示します。
- [# Total Devices]：音声監査に関係するデバイスの数を示します。
- [# Completed Devices]：ツールが監査を試みたデバイスの数を示します。

（注）　コントローラが到達不能な場合、そのコントローラの監査がスキップされます。そのコントローラに対してはルール チェックが実行されません。

- [# Rules]：音声監査で選択されたルールの数を示します。

音声監査レポートの結果

音声監査レポートの結果には、次の情報が含まれています。

- [IP Address]：音声監査に関係するコントローラの IP アドレスを示します。
- [Rule]：このコントローラに適用されたルールを示します。
- [Result]：適用されたルールの結果（[Skipped]、[Violation]、[Unreachable]）を示します。

（注）　現在の設定とルール値に不一致が存在しない場合、そのルールの結果は表示されません。

- [Details]：ルールの結果の説明を定義します。

（注）　適用されたルールの結果が [Violation] である場合、[Details] リンクをクリックすると、名前、デバイス値、ルール値などの詳細が表示されます。リンクにマウス カーソルを合わせると詳細が表示されます。

- [Time]：音声監査のタイムスタンプが表示されます。

音声診断の実行

音声診断ツールでは、リアルタイムでボイスコールを診断するインタラクティブ ツールです。このツールは、クライアントのコール制御関連のエラー、ローミング履歴、および関連 AP で許可および拒否されたアクティブ コールの合計数をレポートします。このツールを使用して、音声診断を開始または停止できます。

音声診断テストは複数のコントローラに対してプロビジョニングされます。つまり、ローミング時に AP が複数のコントローラにアソシエートされた場合、音声診断テストにより、アソシエートされたすべてのコントローラがテストされます。Prime Infrastructure は、AP が上下 3 フロアに配置されたコントローラのテストをサポートしています。たとえば、Prime Infrastructure マップにフロア 1 ～ 4 があり、すべての AP がコントローラ（wlc1、wlc2、wlc3、wlc4）にアソシエートされており、Prime

Infrastructure マップに配置されているとします。ここで、クライアントが 1 階にある wlc1 の AP にアソシエートされ、音声診断テストがこのクライアントに対して開始された場合、テストは wlc2 から wlc3 にもプロビジョニングされます。これは、ローミングのために実行されます

[Voice diagnostic] ページには、以前に実行されたテストがリストされます（ある場合）。[Voice diagnostic] ページには、次の詳細情報が表示されます。

- [Test Name]：テストの名前。
- [First Client]：テスト対象の 1 番めの電話機の Mac アドレス。
- [Second Client]：テスト対象の 2 番めの電話機の Mac アドレス。
- [Start Time]：テストが開始された時刻。
- [Remaining Time]：テストの残り時間。
- [State]：テストの状態。これは、4 つの状態（[Running]、[Completed]、[Stopped]、または [Aborted]）のいずれかです。
- [Problem]：テストのステータス。赤はテストで問題が検出されたことを示します。緑は通話中に問題が検出されなかった音声診断テストを示します。

ドロップダウン リストの [Select a command] から、新しいテストを開始すること、既存のテスト結果を表示することや、テストを削除することができます。

テストの詳細を表示するには、[Test Name] リンクをクリックします。[test detail] ページには、次の詳細情報が表示されます。

- [Test Name]：テストの名前。
- [State]：テストの状態。これは、4 つの状態（[Running]、[Completed]、[Stopped]、または [Aborted]）のいずれかです。
- [Problem]：テストのステータス。赤はテストで問題が検出されたことを示します。緑は音声診断テストが問題なく成功したことを示します。
- [Duration]：テストが実行された期間。期間は、10、20、30、40、50、または 60 分です。デフォルトの選択は 10 分です。
- [Starting Time]：テストが開始された時刻。
- [Remaining/Stopped Time]：テストの残り時間。
- [First Client Details]：クライアントの MAC アドレス、クライアントに対してプロビジョニングされたすべてのコントローラなど、1 番めのクライアントの詳細が表示されます。コントローラが到達不能の場合は、プロビジョニングが失敗したコントローラもリストされます。
- [Second Client Details]：クライアントの MAC アドレス、クライアントに対してプロビジョニングされたすべてのコントローラなど、2 番めのクライアント（ある場合）の詳細が表示されます。コントローラが到達不能の場合は、プロビジョニングが失敗したコントローラもリストされます。

（注） このツールは、ローミングをサポートするために、同じビルディング内のコントローラを、クライアントのアソシエート AP ビルディングのコントローラとして認識し、すべてのコントローラの監視リストに追加します。このツールは、コントローラを設定するために、クライアントの現在のアソシエーション AP の場所から上下 5 階のコントローラを検索します。コントローラの監視リストには、エントリは 10 分間設定されます。10 分後に、コントローラは監視リストからエントリを削除します。

音声診断テストの開始

音声診断テストを開始するには、次の手順に従います。

ステップ 1　[Tools] > [Voice Diagnostics] の順にクリックします。

ステップ 2　[Select a command] ドロップダウン リストから、新しいテストを選択し、[GO] をクリックします。設定ページが表示されます。

このページで、ボイスコール診断の目的で最大 2 つのクライアントを設定できます。両方のクライアントを同じコールで診断すること、または別のコールで診断することができます。

ステップ 3　テスト名およびボイスコールを監視する期間を入力します。音声診断テストは 10、20、30、40、50、または 60 分間実行できます。Prime Infrastructure では 10 分間がデフォルトで選択されます。

ステップ 4　音声診断テストの対象デバイスの MAC アドレスを入力します。

ステップ 5　デバイス タイプを選択します。これは、Cisco ベースの電話機かカスタム電話機です。カスタム電話機の場合、そのカスタム電話機の RSSI 範囲を入力する必要があります。Cisco 電話機の場合、RSSI 範囲は事前に選択されています。

ステップ 6　[StartTest] をクリックしてテストを開始するか、テストが完了した場合はテストを再開できます。

（注）　テストが完了していない場合、状態は [Running] で、テストが完了すると状態は [Completed] になります。テストを途中で停止するには、[Stop] をクリックでき、状態は停止になります。

音声診断テスト レポートの表示

テスト レポートは表形式のデータを使用して表示されます。4 つの主要タブがあります。ここでは、次の内容について説明します。

- 「[Summary] タブ」（P.17-1060）
- 「[Charts] タブ」（P.17-1061）
- 「[Roam History] タブ」（P.17-1061）
- 「[Events] タブ」（P.17-1062）

[Summary] タブ

このタブは 3 つの領域に分割されており、上部の領域にはテストとクライアントの詳細が表示され、中間の領域には問題が表示され、下部の領域には対応するログ メッセージが表示されます。

Test and Client Details

[Test Status] に、テストの名前、1 番めのクライアントの MAC アドレス、2 番めのクライアントの MAC アドレス、デバイス タイプ、テスト ステータス、開始時刻、残り時間、テスト期間などのテスト詳細が表示されます。テストが停止または完了した場合、テストを再開します。実行中のテストを停止するために、[Stop] ボタンが用意されています。ステータスおよびクライアントの詳細を更新するには、[Refresh Status Tab] ボタンおよび [Refresh Client Tab] ボタンを使用します。クライアント ユーザ名、IP アドレス、MAC アドレス、ベンダー、CCX バージョンは、802.11 ステート、プロトコル、SSID、プロファイル名、AP 詳細などのクライアント詳細が表示されます。クライアントの MAC アドレスをクリックすると、クライアントの詳細を表示できます。

Problems

[Problems] ペインは [test and client status details] ペインの下に表示されます。このペインには、現在の診断に関連するすべての問題が表示されます。このペインは 5 秒ごとに個別に更新されます。ページ全体を更新する必要はありません。ペインのいずれかの列をクリックすることで、このペインの情報をソートできます。[Problems] ペインのいずれかの行をクリックすると、ポップアップ ダイアログボックスが表示され、そこに問題の詳しい説明と推奨措置が表示されます。

（注）　コントローラ間ローミング障害の一部のケースでは、[From AP] 情報の MAC アドレスが不正確で、「00:00:00:00:00:00」と表示される場合があります。

Logs

[Logs] ペインは、[Problems] ペインの下に表示されます。このペインには、この診断時にコントローラと WCS 間で交換されたすべてのメッセージが表示されます。ペインのいずれかの列をクリックすることで、このペインの情報をソートできます。このペインは、ページ全体を更新しなくても、5 秒ごとに個別に更新されます。

[Charts] タブ

このタブには、各クライアントのアップリンクおよびダウンリンク トラフィックのグラフが表示されます。グラフは、10 秒ごとに更新されます。

[Client Uplink and DownLink TSM] グラフとローミング

[Client Uplink Traffic Stream Metric (TSM)] グラフには、CCX V4 以上をサポートするクライアントが表示されます。TSM のデータは 10 秒ごとにプロットされます。TSM グラフには、一連のメトリックが表示されます。これらのメトリックは、グラフの [Select Series] ボタンを使用して有効または無効にできます。

[Client Uplink and DownLink QoS] グラフ

各インターバルで、QoS が計算され、グラフに表示されます。[Client Uplink QoS] グラフが表示されます。この円グラフでは、QoS グラフの合計数と 3 つのカテゴリにおけるその分布が示されます。これらのカテゴリは、通常、ボイスコールの品質を示します。

Average Uplink and Downlink AC Queue

[AC Queue] には、パケットのタイプおよび 1 つのシリーズのパケットの数が表示されます。[Select Series] ボタンを使用して、シリーズを有効または無効にできます。

[Roam History] タブ

このタブでは、[Roaming] テーブルにローミング履歴情報が表示されます。この [Roaming] テーブルには、成功および失敗したローミングの履歴が表示されます。[Roaming] テーブルは次の情報を提供します。

- クライアントのローミングが実行された時刻
- クライアントの移動元の AP の名前
- クライアントの移動元の無線のタイプ

- クライアントの移動元のコントローラの IP アドレス
- クライアントの移動先の AP の名前
- クライアントの移動先のコントローラの IP アドレス
- クライアントの移動先の無線のタイプ
- ローミングの結果（成功または失敗）
- ローミングが失敗した場合は、失敗した原因

[Events] タブ

[Event] タブには、ボイスコール中のクライアントと AP に関連するイベント履歴がリスト形式で表示されます。直近 10 のイベントが表示されます。2 つのイベント テーブル（[Client Events] および [AP Events]）を使用できます。[Client Events] テーブルには、ボイスコール中のクライアント固有イベントが表示され、[AP Event] テーブルには、AP 固有イベントが表示されます。

イベントの詳細については、「イベントのモニタリング」セクションを参照してください。

Location Accuracy Tool の設定

Location Accuracy Tool を使用すると、不正でないクライアント、不正クライアント、干渉源、およびアセット タグの位置精度を分析できます。

位置精度を確認することによって、既存のアクセス ポイントの導入が、少なくとも 90 % の確率で、10 m 以内にある要素の真の位置を推定できることを確認できます。

Location Accuracy Tool では、次のいずれかのテストを実行できます。

位置精度をテストするには、次の 2 つの方法があります。

- **スケジュール設定された精度テスト**：クライアント、タグ、干渉源がすでに展開されており、無線 LAN インフラストラクチャにすでにアソシエートされている場合に使用します。クライアント、タグ、干渉源がすでに事前に配置されている場合は、テストが定期的なスケジュールに基づいて実行できるように、スケジュール設定されたテストを設定して保存できます。
- **オン デマンド精度テスト**：要素はアソシエートされているが、事前に配置されていない場合に使用します。オンデマンド テストを使用すると、多数のさまざまな位置のクライアント、タグ、および干渉源の位置精度をテストできます。通常は、少数のクライアント、タグ、干渉源の位置精度をテストするために使用します。

両方のテストとも、1 つのページで設定および実行されます。

ここでは、次の内容について説明します。

Location Accuracy Tool の有効化

（注）　スケジュール設定済みおよびオンデマンドの位置精度ツールのテスト機能を使用するには、Prime Infrastructure で [Advanced Debug] オプションを有効にする必要があります。[Advanced Debug] オプションが有効になっていない場合、Location Accuracy Tool は [Tools] メニューに選択肢として表示されません。

Prime Infrastructure で詳細デバッグ オプションを有効にするには、次の手順に従います。

ステップ 1　Prime Infrastructure で、[Monitor] > [Maps] をクリックします。

ステップ 2　[Select a command] ドロップダウン リストから [Properties] を選択し、[Go] をクリックします。

ステップ 3　表示されるページで [Enabled] チェックボックスをオンにし、Advanced Debug モードを有効にします。[OK] をクリックします。

（注）　Advanced Debug がすでに有効になっている場合は、さらに操作を行う必要はありません。[Cancel] をクリックします。

これで、Location Accuracy Tool を使用して、モビリティ サービス エンジンに対して位置精度テストを実行できるようになります。

「スケジュール設定された精度テストを使用した現在の位置の検証」（P.17-1064）または「オンデマンド精度テストを使用した位置精度のテスト」（P.17-1066）に進みます。

現在スケジュール設定されている精度テストの表示

現在スケジュール設定されている位置精度テストを表示するには、次の手順を実行します。

ステップ 1　[Tools] > [Location Accuracy Tool] の順に選択します。

ステップ 2　[Accuracy Tests] ページに、現在スケジュール設定されているすべての精度テストが表示されます。このページには、次の情報が表示されます。

- テスト名：名前をクリックすると、この精度テストに関する詳細が表示されます。
- テストの種類
- フロア領域または屋外領域：このテストの位置が表示されます。
- ステータス
- 精度 %
- 平均エラー数（m）

新しいスケジュール設定された精度テストまたはオンデマンドの精度テストの作成、最後の実行のログのダウンロード、すべてのログのダウンロード、現在の精度テストの削除を行うには、[Select a command] ドロップダウン リストを使用します。

（注）
- [Accuracy Tests] 概要ページから精度テストのログをダウンロードできます。これを行うには、精度テストを選択し、[Select a command] ドロップダウン リストから、[Download Logs] または [Download Logs for Last Run] を選択します。[Go] をクリックします。
- [Download Logs] オプションは、選択したテストのすべての精度テストのログをダウンロードします。
- [Download Logs for Last Run] オプションは、選択したテストの最新のテスト実行のログのみをダウンロードします。

精度テストの詳細の表示

現在の精度テストに関する詳細を表示するには、次の手順を実行します。

ステップ 1　[Tools] > [Location Accuracy Tool] の順に選択します。

ステップ 2　詳細にアクセスする精度テストの名前をクリックします。

[Accuracy Test Details] ページで、テスト ポイントの配置や精度テストの削除を行うことができます。

ステップ 3　[Accuracy Test] 概要ページに戻るには、[Cancel] をクリックします。

スケジュール設定された精度テストを使用した現在の位置の検証

スケジュール設定された精度テストを設定するには、次の手順を実行します。

ステップ 1　[Tools] > [Location Accuracy Tool] の順に選択します。

ステップ 2　[Select a Command] ドロップダウン リストから [New Scheduled Accuracy Test] を選択します。

ステップ 3　テスト名を入力します。

ステップ 4　ドロップダウン リストから [Area Type] を選択します。

ステップ 5　キャンパスは、デフォルトでルート領域として設定されています。この設定を変更する必要はありません。

ステップ 6　ドロップダウン リストからビルディングを選択します。

ステップ 7　ドロップダウン リストからフロアを選択します。

ステップ 8　日、時、分を入力して、テストの開始時間および終了時間を選択します。時間は、24 時間表記で入力します。

（注）　テスト開始時間を入力する場合には、マップ上にテストポイントを配置するためにテスト開始前に十分な時間があることを確認します。

ステップ 9　テスト結果は [Accuracy Tests] > [Results] ページに表示されます。レポートは PDF 形式で示されます。

（注）　[Email] オプションを選択する場合は、目的の電子メール アドレスに対して SMTP メール サーバを定義しておく必要があります。[Administrator] > [Settings] > [Mail Server] の順に選択して、適切な情報を入力します。

ステップ 10　[Position Testpoints] をクリックします。フロア上のすべてのクライアント、タグ、および干渉源が、MAC アドレスとともにフロア マップに表示されます。

ステップ 11　位置精度を確認する各クライアント、タグ、および干渉源の隣のチェックボックスをオンにします。

[MAC Address] チェックボックスをオンにすると、2 つのアイコンがマップに表示されます。一方のアイコンは実際の位置を表し、もう一方のアイコンは報告された位置を表しています。

（注）　一覧表示されないクライアント、タグ、または干渉源の MAC アドレスを入力するには、[Add New MAC] チェックボックスをオンにして MAC アドレスを入力し、[Go] をクリックします。その要素のアイコンがマップに表示されます。新しく追加された要素が別のフロアのロケーション サーバ上にある場合は、左端の隅（0, 0 の位置）にアイコンが表示されます。

ステップ 12　要素の実際の位置が報告された位置と同じではない場合、その要素の実際の位置アイコンをマップ上の正しい位置にドラッグします。実際の位置のアイコンだけをドラッグできます。

ステップ 13　すべての要素が配置されたら [Save] をクリックします。精度テストが成功したことを確認するダイアログ ボックスが表示されます。

ステップ 14　[OK] をクリックして、確認ダイアログボックスを閉じます。[Accuracy Tests] 概要ページに戻ります。

（注）　テストの実行直前は、精度テスト ステータスは [Scheduled] と表示されます。テストが処理中の場合は [Running] ステータスが表示され、テストが完了した場合は [Idle] ステータスが表示されます。テストが正常に終了しないと [Failure] ステータスが表示されます。

ステップ 15　位置精度テストの結果を表示するには、テスト名をクリックして表示されるページの [Results] タブをクリックします。

ステップ 16　[Results] ページで、[Saved Report] 見出しの下の [Download] リンクをクリックしてレポートを表示します。

Scheduled Location Accuracy Report に表示される情報は、次のとおりです。

- さまざまなエラー範囲内の要素の割合を説明する概要の位置精度レポート。
- エラー距離ヒストグラム。
- 累積エラー分布グラフ。
- エラー距離経時グラフ。
- ロケーション精度がテストされた各 MAC アドレスの概要（実際のロケーションとエラー距離の記載付き）、および各 MAC の空間精度（実際のロケーション対計算されたロケーション）と経時的エラー距離を示すマップの概要が表示されます。

オンデマンド精度テストを使用した位置精度のテスト

オンデマンド精度テストは、要素がアソシエートされているが、事前に配置されていない場合に実行します。オンデマンド テストを使用すると、多数のさまざまな位置のクライアント、タグ、および干渉源の位置精度をテストできます。通常は、少数のクライアント、タグ、干渉源の位置精度をテストするために使用します。

オンデマンド精度テストを実行するには、次の手順に従います。

ステップ 1　[Tools] > [Location Accuracy Tool] の順に選択します。

ステップ 2　[Select a command] ドロップダウン リストから、[New On demand Accuracy Test] を選択します。

ステップ 3　テスト名を入力します。

ステップ 4　ドロップダウン リストから [Area Type] を選択します。

ステップ 5　キャンパスは、デフォルトでルート領域として設定されています。この設定を変更する必要はありません。

ステップ 6　ドロップダウン リストからビルディングを選択します。

ステップ 7　ドロップダウン リストからフロアを選択します。

ステップ 8　テスト結果の宛先を選択します。テスト結果は [Accuracy Tests] > [Results] ページに表示されます。レポートは PDF 形式で示されます。

ステップ 9　[Position Testpoints] をクリックします。座標（0,0）に赤色の十字線が付いたフロア マップが表示されます。

ステップ 10　特定の位置の位置精度と RSSI をテストするには、左側のドロップダウン リストからクライアント、タグ、または干渉源を選択します。選択したオプション（クライアント、タグ、干渉源のいずれか）のすべての MAC アドレスのリストが、オプションの右側のドロップダウン リストに表示されます。

ステップ 11　ドロップダウン リストから MAC アドレスを選択し、赤色の十字線をマップ位置に移動して、マウスをクリックして配置します。

ステップ 12　[Zoom percentage] ドロップダウン リストから、マップのズーム パーセンテージを選択します。

[X] および [Y] テキスト ボックスには、マップ内の赤色の十字線の位置に基づいて座標が入力されます。

ステップ 13　[Start] をクリックして、精度データの収集を開始します。

ステップ 14　[Stop] をクリックして収集を終了します。[Stop] をクリックする前に少なくとも 2 分間テストを実行してください。

ステップ 15　マップ上にプロットする各テスト ポイントについてステップ 11 ～ステップ 14 を繰り返します。

ステップ 16　テストポイントのマッピングが終了したら、[Analyze Results] をクリックします。

ステップ 17　表示されるページで [Results] タブをクリックします。

[On-demand Accuracy Report] に表示される概要は、次のとおりです。

- さまざまなエラー範囲内の要素の割合を説明する概要の位置精度レポート。
- エラー距離ヒストグラム
- 累積エラー分散グラフ

監査サマリーの設定

[Tools] > [Config Audit] の順に選択して、[Config Audit Summary] ページを表示します。

このページには、次の概要が表示されます。

- [Total Enforced Config Groups] : バックグラウンド監査用に設定され適用が有効になっている、設定グループのテンプレートの数を示します。

  リンクを起動すると、[Enforce Configuration] が有効な設定グループを示す [Config Group] ページが表示されます。

- [Total Mismatched Controllers] : 一致しないコントローラの数を示します。一致しないコントローラは、最近の監査時に Prime Infrastructure とコントローラに間に設定の相違が見つかったことを示します。

  リンクをクリックすると、[Mismatched audit status] 列でソートされたコントローラ リストが表示されます。[Audit Status] 列の項目をクリックすると、このコントローラの監査レポートが表示されます。

- [Total Config Audit Alarms] : 設定グループに監査の矛盾が施行された場合に生成されたアラーム数を示します。

  リンクをクリックすると、すべての設定監査アラームの詳細が表示されます。

  （注）　施行が失敗すると、設定グループに重大なアラームが生成されます。施行が成功すると、設定グループに比較的重大でないアラームが生成されます。アラームには監査レポートへのリンクがあり、各コントローラの矛盾のリストを表示できます。

- [Most recent 5 config audit alarms] : 監査アラームのオブジェクト名、イベントのタイプ、日付と時刻など、最近の設定監査のアラームを示します。

[View All] をクリックすると該当する [Alarm] ページが開き、すべての設定監査アラームが表示されます。

移行分析の設定

[Migration Analysis Summary] ページを表示するには、[Tools] > [Migration Analysis] の順に選択します。

（注）　また、[Configure] > [Autonomous AP] > [Migration Templates] の順に選択し、[Select a command] ドロップダウン リストから [View Migration Analysis Summary] を選択することでも、移行分析の概要にアクセスできます。

Autonomous アクセス ポイントは、すべての基準のステータスが合格の場合のみ移行対象になります。赤い X は適格でないことを示し、緑のチェック マークは適格であることを示します。これらの列は次のものを表しています。

- [Privilege 15 Criteria] : Autonomous アクセス ポイントの検出の一部として指定された Telnet クレデンシャルは、特権 15 であることが必要です。
- [Software Version] : 12.3(7)JA リリースからの変換のみがサポートされています。ただし、12.3(11)JA、12.3(11)JA1、12.3(11)JA2、および 12.3(11)JA3 を除きます。

- [Role Criteria] : アソシエーション要求を送信するには、アクセス ポイントとコントローラの間の有線接続が必要です。そのため、次の Autonomous アクセス ポイント ロールが必要です。
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only

[Radio Criteria] : デュアル無線アクセス ポイントの場合、1 つの無線の種類のみがサポートされている場合でも変換を実行できます。

ここでは、次の内容について説明します。

- 「Autonomous アクセス ポイントのアップグレード」（P.17-1068）
- 「ファームウェア アップグレード レポートの表示」（P.17-1069）
- 「ロール変更レポートの表示」（P.17-1069）

Autonomous アクセス ポイントのアップグレード

Autonomous アクセス ポイントは、手動または自動でアップグレードできます。[Migration Analysis] ページで、ソフトウェア バージョンが [failed] と表示されたアクセス ポイントを選択し、[Select a command] ドロップダウン リストから [Upgrade Firmware (Manual or Automatic)] を選択します。このプロセスにより、Cisco IOS アクセス ポイントの自律ファームウェア イメージがサポートされているバージョンにアップグレードされます。

Prime Infrastructure は Telnet ベースの接続を使用してアクセス ポイントのファームウェアをアップグレードします。自動オプションを選択した場合、Prime Infrastructure にあるデフォルト イメージとともに内部 TFTP サーバが使用されます。デバイスの種類ごとのデフォルト イメージは次のとおりです。

- ap801-k9w7-tar.124-10b.JA3.tar
- ap802-k9w7-tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

手動オプションを選択した場合、TFTP サーバ IP、ファイル パス、ファイル パス名を含む追加のページが表示されます。最終的なページは [Report] ページです。

ルート モードへのステーション ロールの変更

アソシエーション要求を送信するには、アクセス ポイントとコントローラの間の有線接続が必要であるため、Autonomous アクセス ポイントに適切なロールを割り当てる必要があります。ロールが不適格として表示される場合は、[Select a command] ドロップダウン リストから [Change Station Role to Root Mode] を選択してモードを変更します。

移行分析の実行

[Migration Analysis Summary] ページの [Select a command] ドロップダウン リストから [Run Migration Analysis] を選択します。得られた移行分析の概要には、さまざまな条件の現在のステータスが表示されます。アクセス ポイントが検出されると、最初に移行分析が自動的に実行されます。

移行分析レポートの表示

[Migration Analysis Summary] ページの [Select a command] ドロップダウン リストから [View Migration Analysis Report] を選択してレポートを生成できます。レポートには次の情報が含まれます。

- アクセス ポイントのアドレス
- ステータス
- タイムスタンプ
- アクセス ポイントのログ

ファームウェア アップグレード レポートの表示

選択したアクセス ポイントのアップグレード ステータスの現在のレポートを表示するには、[Select a command] ドロップダウン リストから [View Firmware Upgrade Report] を選択します。

次の情報が表示されます。

- [AP Address]：アクセス ポイントの IP アドレス。
- [Status]：ファームウェア アップグレードの現在のステータス。
- [TimeStamp]：アップグレードの日時。
- AP Logs

[Migration Analysis Summary] ページに戻るには [OK] をクリックします。

詳細については、「Autonomous アクセス ポイントのアップグレード」（P.17-1068）を参照してください。

ロール変更レポートの表示

アソシエーション要求を送信するには、アクセス ポイントとコントローラの間の有線接続が必要であるため、Autonomous アクセス ポイントに適切なロールを割り当てる必要があります。

これらのロール変更のレポートを表示するには、[Select a command] ドロップダウン リストから [View Role Change Report] を選択します。次の情報が表示されます。

- [AP Address]：アクセス ポイントの IP アドレス。
- [Status]：ロール変更の現在のステータス。
- [TimeStamp]：アップグレードの日時。
- AP Logs

[Migration Analysis Summary] ページに戻るには [OK] をクリックします。

TAC ケース添付ファイルの設定

（注）　TAC ケース添付ファイルを設定する前に、有効なメール サーバを設定する必要があります。

TAC Case Attachment ツールを使用すると、該当するすべてのコントローラ TAC ケース情報を一度に簡単に添付できます。このツールには次の 2 つのオプションがあります。

- [Send] : attach@cisco.com に電子メールを送信します。
- [Download] : ローカル コンピュータに情報をダウンロードします。データを attach@cisco.com に電子メールで手動送信する必要があります。このオプションは、Prime Infrastructure サーバと Cisco の間に電子メール接続がない場合、または情報が大きすぎて電子メールに添付できない場合に便利です。

このツールでは、次の情報が送信されます。

- [Network Information] : デバイス インベントリの詳細とクライアントの種類が送信されます。
- [Controller Information] : 実行コンフィギュレーションの詳細、テクニカル サポート、メッセージ ログ、トラップ ログ、コントローラ クラッシュ ファイルが送信されます。
- [Access Point Information] : クラッシュ ファイルと無線コアダンプが送信されます。

情報を [Send] または [Download] するには、次の内容を入力する必要があります。

- 有効な TAC ケース番号を入力します。
- コントローラまたは AP 情報を送信する場合は、コントローラを選択します。

（注）　[additional comments] テキスト ボックスを使用して追加情報を送信することもできます。情報を送信した後、Case ツールの [attachment] セクションを参照することで、データが Cisco に到着したかどうかを確認できます。

（注）　このツールでは、コントローラまたはアクセス ポイントの情報を収集およびアップロードするために、コントローラに対する読み書きアクセス権が必要です。

CHAPTER 18

wIPS ポリシー アラーム リファレンス

セキュリティ IDS/IPS の概要

企業環境に WLAN を追加すると、ネットワーク セキュリティに対する新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無許可のユーザに公開する可能性があります。個人の使用のために従業員によって設置された不正アクセス ポイントは通常、企業のセキュリティ ポリシーに準拠していません。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正アクセス ポイントの脅威以外にも、アクセス ポイントの設定ミスや未設定、DoS（サービス拒否）攻撃といったさまざまなワイヤレス セキュリティ リスクや侵入の可能性が存在します。

Cisco Adaptive Wireless IPS は適切なセキュリティ設定を検証し、侵入攻撃の可能性を検出することで、セキュリティの脅威への対処を支援します。Cisco Adaptive Wireless IPS は、包括的なセキュリティ モニタリング テクノロジー スイートを使用して、次のカテゴリ内の 100 件を超えるさまざまな脅威状況をユーザに警告します。

- ユーザ認証とトラフィック暗号化
- 不正デバイスとアドホック モード デバイス
- 設定の脆弱性
- 侵入検知（セキュリティ突破）
- 侵入検知（DoS 攻撃）

Cisco Adaptive Wireless IPS の機能を最大限に活用するために、セキュリティ導入ポリシーに最も適したものになるようにセキュリティ アラームをカスタマイズできます。たとえば WLAN の導入時に特定ベンダーのアクセス ポイントを導入する場合、そのアクセス ポイントまたはセンサーによって別のベンダーのアクセス ポイントが検出されると不正アクセス ポイント アラームを生成するように製品をカスタマイズできます。

（注） wIPS ローカル モードまたは FlexConnect モード アクセス ポイントではすべてのセキュリティ アラームがサポートされているわけではありません。虫眼鏡のアイコン が付いているアラームは、wIPS ローカル モードまたは FlexConnect モード アクセス ポイントではサポートされていません。

各種 WLAN 環境に対応して事前に設定されているプロファイル

インストール中に、実装されている WLAN ネットワークに基づいて適切なプロファイルをユーザが選択できます。

Cisco Adaptive Wireless IPS は次の個別のプロファイルを提供します。

- Enterprise best practice

- Enterprise rogue detection only
- Financial（Gramm-Leach-Bliley 法に準拠）
- HealthCare（Health Insurance Portability and Accountability 法に準拠）
- Hotspot implementing 802.1x security
- Hotspot implementing NO security
- Tradeshow environment
- Warehouse/manufacturing environment
- Government/Military（8100.2 指令に準拠）
- Retail environment

管理者が適切なプロファイルを選択すると、Cisco Adaptive Wireless IPS によりその WLAN 環境に該当するポリシー プロファイルのアラームが有効または無効にされます。たとえば医療機関の場合、[Helthcare] プロファイルを選択すると HIPAA 準拠のために必要なすべてのアラームが有効になります。管理者はインストール後にアラームを有効または無効にしたり、プリファレンスごとにしきい値を変更したりできます。

Cisco Adaptive Wireless IPS システムは IDS（侵入検知システム）かつ IPS（侵入防御システム）でもあります。

ヒント　Cisco Adaptive wIPS 機能の詳細については、Cisco.com にアクセスして、マルチメディア プレゼンテーションをご覧ください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールがあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

Cisco Adaptive Wireless IPS のポリシーは、「wIPS：DoS（サービス拒否）攻撃」と「wIPS：セキュリティ突破」という 2 つのサブカテゴリに分類されます。

ここでは、次の内容について説明します。

- 「侵入検知：DoS 攻撃」（P.18-1072）
- 「侵入検知：セキュリティ突破」（P.18-1095）

侵入検知：DoS 攻撃

ワイヤレス DoS（サービス拒否）攻撃は、レイヤ 1 またはレイヤ 2 における WLAN のさまざまな脆弱性を悪用してワイヤレス サービスを妨害することを狙いとしています。DoS 攻撃は、物理的な RF 環境、アクセス ポイント、クライアント ステーション、またはバックエンド認証 RADIUS サーバをターゲットとする可能性があります。たとえばオフィスがある建物の外部から、高出力指向性アンテナを使った遠隔 RF 電波妨害攻撃が行われることがあります。侵入者が使用する攻撃ツールは、スプーフされた 802.11 管理フレームやスプーフされた 802.1x 認証フレームなどのハッキング技法、または単に総当たりのパケット フラッディング方法を利用します。

このような攻撃の中には、ワイヤレスの特性とワイヤレス プロトコル標準を対象にするものがあります。シスコは、このような攻撃の多くを未然に防ぐため、802.11i のベースとなる管理フレーム保護を開発しました。(MFP の詳細については、Cisco Prime Infrastructure オンライン ヘルプを参照してください)。Cisco Adaptive Wireless IPS は、攻撃シグニチャの照合が行われる早期検知システムによってこのソリューションに寄与しています。Cisco Adaptive Wireless IPS の DoS 検出機能は WLAN レイヤ 1（物理層）とレイヤ 2（データ リンク層、802.11、802.1x）を対象にしています。強力な WLAN 認証および暗号化メカニズムが採用されている場合、上位層（IP 層以上）への DoS 攻撃が困難になりま

す。wIPS サーバでは強力な認証および暗号化ポリシーを検証することで、WLAN 防衛が強化されます。また Cisco Adaptive Wireless IPS の DoS 攻撃とセキュリティ突破に対する侵入検知機能は、ワイヤレス攻撃の可能性を常時モニタします。

この項では、DoS 攻撃のサブカテゴリについて説明します。この項は次のトピックで構成されています。

- 「アクセス ポイントに対する DoS 攻撃」（P.18-1073）
- 「インフラストラクチャに対する DoS 攻撃」（P.18-1079）
- 「クライアント ステーションに対する DoS 攻撃」（P.18-1084）

アクセス ポイントに対する DoS 攻撃

アクセス ポイントに対する DoS 攻撃は主に次の事項を前提として実行されます。

- アクセス ポイントのリソースが限られている。（クライアントごとのアソシエーション ステート テーブルなど）。
- WLAN 管理フレームおよび認証プロトコル 802.11 と 802.1x に暗号化メカニズムがない。

ワイヤレス侵入者は、スプーフした MAC アドレスを使って多数のワイヤレス クライアントをエミュレートし、アクセス ポイントのリソース（最も重要なものとしてクライアント アソシエーション テーブル）を枯渇させます。エミュレートされた各クライアントはターゲット アクセス ポイントとのアソシエートと認証を試行しますが、プロトコル トランザクションは未完了のままになります。アクセス ポイント リソースとクライアント アソシエーション テーブルがこのようなエミュレートされたクライアントとその未完了認証ステートでいっぱいになるため、攻撃を受けたアクセス ポイントは正規のクライアントに対処できなくなります。このようにして DoS 攻撃が成立します。

Cisco Adaptive Wireless IPS はクライアント認証プロセスを追跡し、アクセス ポイントに対する DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、攻撃検知および統計的シグニチャ照合プロセスが開始されます。DoS 攻撃が検出されると wIPS アラームが発行されます。このアラームには、標準のアラーム詳細記述とターゲット デバイス情報が含まれます。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。

この項では、アクセス ポイントに対する DoS 攻撃について説明します。この項は次のトピックで構成されています。

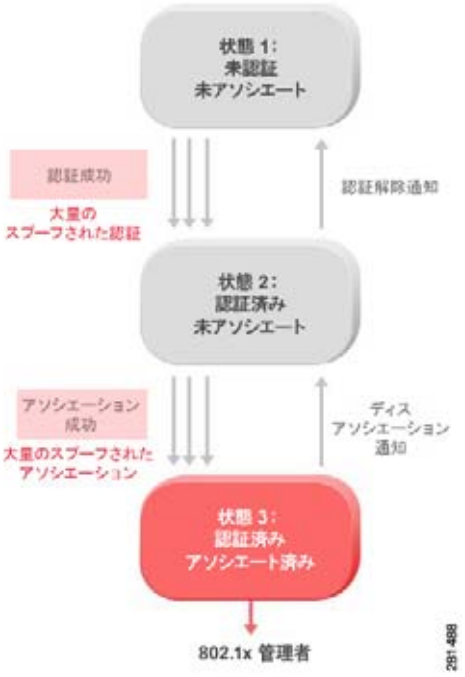
- 「DoS 攻撃：アソシエーション フラッド」（P.18-1074）
- 「DoS 攻撃：アソシエーション テーブル オーバーフロー」（P.18-1075）
- 「DoS 攻撃：認証フラッディング」（P.18-1075）
- 「DoS 攻撃：EAPOL-Start 攻撃」（P.18-1076）
- 「DoS 攻撃：PS ポール フラッディング」（P.18-1077）
- 「DoS 攻撃：未認証アソシエーション」（P.18-1078）

DoS 攻撃：アソシエーション フラッド

アラームの説明と考えられる原因

この DoS 攻撃は、アクセス ポイントに大量のスプーフされたクライアント アソシエーションを送り付け、アクセス ポイント リソース（特にクライアント アクセス テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、この認証が使用されることはほとんどありません。別の方法として、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）が使用されることがあります。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントをエミュレートし、多数のクライアントを状態 3 にしてターゲット アクセス ポイント クライアント アソシエーション テーブルのフラッディングを発生させます。クライアント アソシエーション テーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃が成立します（図 18-1 を参照）。

図 18-1　　DoS 攻撃：アソシエーション フラッディング



wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するために、クライアントのアソシエートが正常に完了した後で、スプーフされた MAC アドレスを検出し、802.1x アクションとデータ通信を追跡します。Cisco Adaptive Wireless IPS によりこの攻撃が報告されたら、このアクセス ポイントにログオンし、アソシエーション テーブルでクライアント アソシエーションの数を検査します。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。

DoS 攻撃：アソシエーション テーブル オーバーフロー

アラームの説明と考えられる原因

ワイヤレス侵入者は、スプーフした MAC アドレスを使って多数のワイヤレス クライアントを偽装し、アクセス ポイントのリソース（最も重要なのものとしてクライアント アソシエーション テーブル）を枯渇させます。それぞれの偽装クライアントがターゲット アクセス ポイントとのアソシエートと認証を試行します。通常、802.11 認証は完了します。これは、ほとんどのデプロイメントでは 802.11 オープン システム認証（Null 認証プロセス）が採用されているためです。このような偽装クライアントとのアソシエートの後に認証プロセスが実行されます。ただし偽装クライアントは 802.1x や VPN のような高度な認証は行わないため、プロトコル トランザクションが未完了状態になります。この時点で、攻撃を受けたアクセス ポイントでは各偽装クライアントのステートがクライアント アソシエーション テーブルに維持されます。アクセス ポイント リソースとクライアント アソシエーション テーブルがこのような偽装クライアントとそのステート情報でいっぱいになるため、攻撃を受けたアクセス ポイントは正規のクライアントに対処できなくなります。このようにして DoS 攻撃が成立します。

wIPS による解決

Cisco Adaptive Wireless IPS はクライアント認証プロセスを追跡し、アクセス ポイントに対する DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、Cisco Adaptive Wireless IPS 攻撃検知および統計的シグニチャ照合プロセスが開始されます。

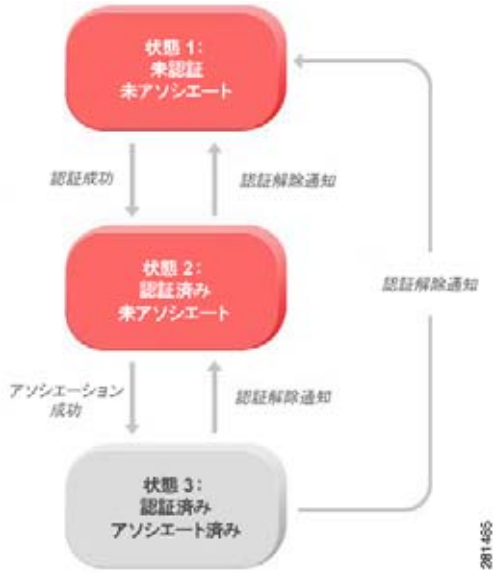
DoS 攻撃：認証フラッディング

攻撃ツール：Void11

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に準拠してこのようなステート マシンを実装しています。（図 18-2 を参照）。アクセス ポイントでは各クライアントのステートがアクセス ポイント クライアント テーブル（アソシエーション テーブル）に記録されます。この記録されるステートのサイズは制限されています。この制限は、ハードコーディングされた数値または物理メモリ制約に基づく数値のいずれかです。

図 18-2　クライアント ステート マシン



この DoS 攻撃は、多数のクライアント ステーションを偽装して（MAC アドレス スプーフィング）アクセス ポイントに認証要求を送信し、アクセス ポイント クライアント ステート テーブル（アソシエーション テーブル）のフラッディングを引き起こします。ターゲット アクセス ポイントでは、個々の認証要求を受け取るたびにアソシエーション テーブルに状態 1 のクライアント項目が作成されます。オープン システム認証が使用されているアクセス ポイントは、*認証成功* フレームを戻し、クライアントを状態 2 にします。共有キー認証が使用されているアクセス ポイントは、攻撃者が偽装しているクライアントに*認証チャレンジ*を送信します。この場合攻撃者から応答はありません。この場合アクセス ポイントはクライアントを状態 1 のままにします。いずれの場合でも、アクセス ポイントに状態 1 または状態 2 のクライアントが多数あり、アクセス ポイント アソシエーション テーブルがいっぱいになります。テーブルが上限に達すると、正規のクライアントがこのアクセス ポイントに対して認証およびアソシエートできなくなります。これにより DoS 攻撃が成立します。

wIPS による解決

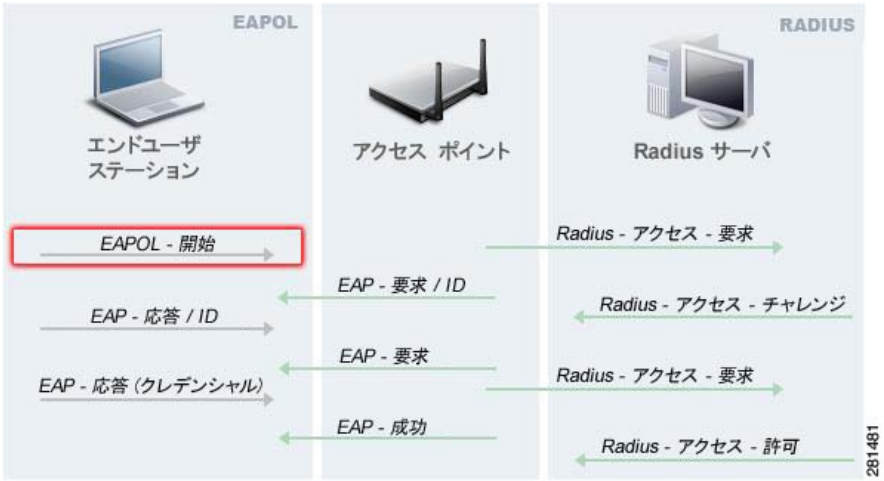
Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ アナリストはそのアクセス ポイントにログオンして現在のアソシエーション テーブルのステータスを確認できます。

DoS 攻撃：EAPOL-Start 攻撃

アラームの説明と考えられる原因

IEEE 802.1x 標準は、EAP over LAN（EAPOL）を使用して認証プロトコルを定義します。802.1x プロトコルは、クライアント ステーションから送信された EAPOL-Start フレームで認証トランザクションを開始します。アクセス ポイントは EAPOL-start フレームに対し EAP ID 要求および内部リソース割り当てによって応答します（図 18-3 を参照）。

図 18-3　EAPOL-Start プロトコルと EAPOL-Start 攻撃



攻撃者は、アクセス ポイントに EAPOL-start フレームを大量に送り付け、アクセス ポイント内部リソースを枯渇させることでアクセス ポイントを妨害しようとします。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、802.1x 認証ステート遷移および特定の攻撃シグニチャを追跡します。

DoS 攻撃：PS ポール フラッディング

アラームの説明と考えられる原因

電源管理は、おそらくワイヤレス LAN デバイスにおいて最も重要な機能の 1 つです。電源管理は、ステーションを長期にわたり省電力モードで維持し、アクセス ポイントから特定の間隔でのみデータを受信するようにすることで、電力を節約します。

ワイヤレス クライアントはアクセス ポイントに対し、スリープ モード（省電力モード）にある期間を通知する必要があります。この期間が終わるとクライアントは再起動し、待機データ フレームがあるかどうかを確認します。アクセス ポイントとのハンドシェイクが完了すると、データ フレームを受信します。アクセス ポイントからのビーコンには、クライアントが再起動してマルチキャスト トラフィックを受け入れる必要がある時点でクライアントにその旨を通知する Delivery Traffic Indication Map（DTIM）も含まれています。

アクセス ポイントは引き続き、スリープ中のワイヤレス クライアントのためにデータ フレームをバッファします。アクセス ポイントは Traffic Indication Map（TIM）を使用してワイヤレス クライアントに対しアクセス ポイントにデータがバッファされていることを通知します。マルチキャスト フレームは、DTIM を通知するビーコンの後に送信されます。

クライアントは、PS-Poll フレームを使用してアクセス ポイントへバッファ フレームを配信することを要求します。すべての PS-Poll フレームに対し、アクセス ポイントはデータ フレームで応答します。ワイヤレス クライアントのためにバッファされているフレームが多数ある場合、アクセス ポイントはフレーム応答のデータ ビットを設定します。その後、クライアントは次のデータ フレームを取得するために別の PS-Poll フレームを送信します。この処理は、バッファされたデータをすべて受信するまで行われます。

ハッカーがワイヤレス クライアントの MAC アドレスをスプーフし、大量の PS-Poll フレームを送信することがあります。この場合アクセス ポイントはバッファ データ フレームをワイヤレス クライアントに送信します。実際には、クライアントは省電力モードになっておりデータ フレームを受信しないことがあります。

wIPS による解決

Cisco Adaptive Wireless IPS は、ワイヤレス クライアントが正規のデータを失う可能性があるこの DoS 攻撃を検出できます。デバイスを特定し、ワイヤレス環境から削除します。

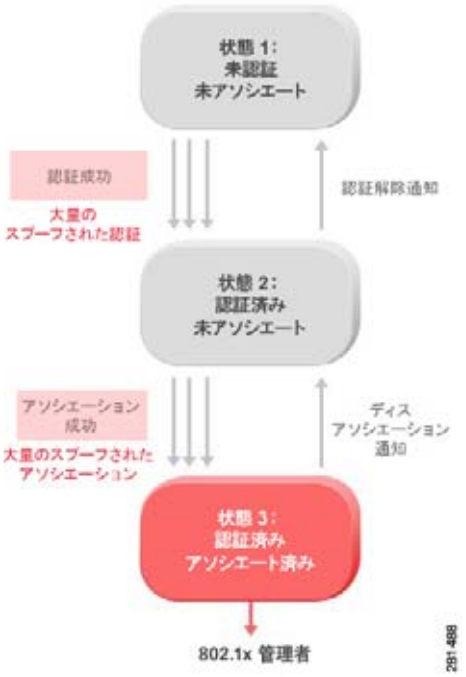
また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。

DoS 攻撃：未認証アソシエーション

アラームの説明と考えられる原因

この DoS 攻撃では、アクセス ポイントに大量のスプーフされたクライアント アソシエーションを送り付け、アクセス ポイント リソース（特にクライアント アソシエーション テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、この認証が使用されることはほとんどありません。別の方法として、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）が使用されることがあります。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントを偽装し、多数のクライアントを状態 3 にしてターゲット アクセス ポイント クライアント アソシエーション テーブルのフラッディングを発生させます。クライアント アソシエーション テーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃の原因となります（図 18-4 を参照）。

図 18-4　DoS 攻撃：未認証アソシエーション



wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するために、クライアントのアソシエートが正常に完了した後で 802.1x アクションとデータ通信を追跡し、スプーフされた MAC アドレスを検出します。Cisco Adaptive Wireless IPS によりこの攻撃が報告されたら、このアクセス ポイントにログオンし、アソシエーション テーブルでクライアント アソシエーションの数を検査します。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。

インフラストラクチャに対する DoS 攻撃

アクセス ポイントやクライアント ステーションに対する攻撃の他に、ワイヤレス侵入者は RF スペクトラムまたはバックエンド認証 RADIUS サーバをターゲットにして DoS 攻撃を行うことがあります。遠隔から高出力アンテナを使って RF ノイズを発生させることで、RF スペクトラムを容易に妨害できます。DDoS（分散型サービス拒否）攻撃で複数のワイヤレス攻撃者がバックエンド RADIUS サーバに対して認証要求を送り付けると、この RADIUS サーバが過負荷になります。この攻撃を行う上で、認証が成功する必要はありません。

この項では、インフラストラクチャに対する DoS 攻撃について説明します。この項は次のトピックで構成されています。

- 「DoS 攻撃：CTS フラッディング」（P.18-1080）
- 「DoS 攻撃：クイーンズランド工科大学により検出された脆弱性」（P.18-1080）
- 「DoS 攻撃：RF 電波妨害」（P.18-1081）
- 「DoS 攻撃：RTS フラッディング」（P.18-1082）
- 「DoS 攻撃：仮想キャリア攻撃」（P.18-1083）

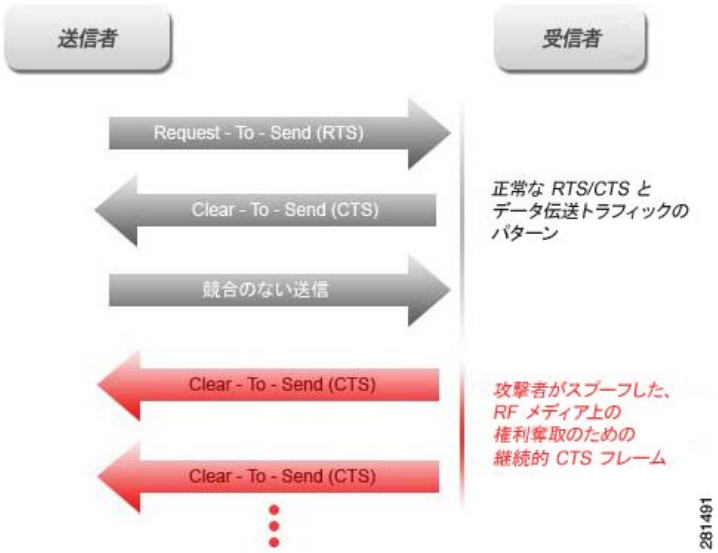
DoS 攻撃：CTS フラッディング

攻撃ツール：CTS Jack

アラームの説明と考えられる原因

IEEE 802.11 標準には、ステーションによる RF 媒体へのアクセスを制御する RTS/CTS（Request-To-Send/Clear-To-Send）機能がオプションとして含まれています。送信準備が整ったワイヤレス デバイスは、指定された期間にわたって RF 媒体への送信権限を獲得するため、RTS フレームを送信します。レシーバは同じ期間の CTS フレームを送信して RF 媒体への権限をトランスミッタに付与します。CTS フレームを監視するワイヤレス デバイスはすべて、競合がない状態で送信できるようにトランスミッタに対してこの媒体を生成します（図 18-5 を参照）。

図 18-5　CTS DoS 攻撃と標準 RTS/CTS 機能の比較



ワイヤレス DoS 攻撃を行うハッカーが、CTS フレームに付与された特権を悪用して RF 媒体を送信用に予約することがあります。攻撃者はバックツーバック CTS フレームを送信することで、攻撃者が CTS フレームの送信をやめるまで RF 媒体を共有する他のワイヤレス デバイスが送信を行わないようにできます。

wIPS による解決

Cisco Adaptive Wireless IPS は DoS 攻撃のための CTS フレームの不正使用を検出します。

DoS 攻撃：クイーンズランド工科大学により検出された脆弱性

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02.

アラームの説明と考えられる原因

802.11 WLAN デバイスは、基本アクセス メカニズムとしてキャリア検知多重アクセス/衝突回避（CSMA/CA）を採用しています。このメカニズムでは、WLAN デバイスが送信開始前に媒体を待機し、すでに実行中の送信を検出するとバックオフします。衝突回避では、媒体が送信可能になる前の時点で物理検知メカニズムと Network Allocation Vector（NAV）を含む仮想検知メカニズムが組み合わせられます。DSSS プロトコルのクリア チャネル アセスメント（CCA）は、WLAN チャネルがクリアであり 802.11b デバイスがこのチャネルを介して送信できるかどうかを判断します。

802.11b プロトコル標準に DoS 無線周波数電波妨害攻撃を可能にする脆弱性があることが、オーストラリアのブリスベンにあるクイーンズランド工科大学 Information Security Research Centre 所属の Mark Looi、Christian Wullems、Kevin Tham、および Jason Smith により明らかになりました。

この攻撃では特に CCA 機能が攻撃を受けます。AusCERT の勧告では「この脆弱性に対する攻撃では、物理層の CCA 機能が悪用され、攻撃中に範囲内のすべての WLAN ノード（クライアントとアクセス ポイントの両方）によるデータ送信が遅延します。攻撃を受けたデバイスは、チャネルが使用中であるかのように動作し、ワイヤレス ネットワーク経由でのデータ送信が妨害されます。」と述べられています。

この DoS 攻撃は、IEEE 802.11、802.11b、および低速（20 Mbps 以下）802.11g ワイヤレス デバイスを含む DSSS WLAN デバイスに影響します。IEEE 802.11a（OFDM を使用）、高速（OFDM 使用で 20 Mbps を上回る速度）802.11g ワイヤレス デバイスはこの攻撃の影響を受けません。FHSS を使用するデバイスは影響を受けません。

攻撃者は WLAN カードを装着したラップトップや PDA を使い、SOHO WLAN と企業 WLAN に対してこの攻撃を行うことができます。この DoS 攻撃に対する唯一の回避策は、802.11a プロトコルに切り替えることです。

この DoS 攻撃の詳細については、以下を参照してください。

- www.isrc.qut.edu.au
- www.isrc.qut.edu.au/wireless
- http://www.auscert.org.au/render.html?it=4091
- http://www.kb.cert.org/vuls/id/106678

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出すると、アラームを発行します。当該デバイスを特定し、ワイヤレス環境から削除します。

DoS 攻撃：RF 電波妨害

アラームの説明と考えられる原因

WLAN の信頼性と効率は、無線周波数（RF）媒体の品質に基づきます。各 RF は RF ノイズの影響を受けます。攻撃者はこの WLAN の脆弱性を利用して 2 種類の DoS 攻撃を行う可能性があります。

- WLAN サービスの妨害：無免許の 2.4 GHz スペクトラムでは、攻撃が意図的ではないことがあります。コードレス電話、Bluetooth デバイス、電子レンジ、ワイヤレス監視ビデオ カメラ、ベビーモニタなどはすべて RF エネルギーを放出し、WLAN サービスを妨害する可能性があります。悪意のある攻撃では、高出力指向性アンテナを使い 2.4 GHz または 5 GHz スペクトラムで RF 出力を操作し、遠隔から攻撃の影響を増幅させることができます。自由空間と建物内での減衰により、建物から 300 フィート離れた位置にある 1-kW 電波妨害デバイスは、オフィス エリアへ 50 ～ 100

フィートの電波妨害が可能です。同じ 1-kW 電波妨害デバイスを建物の中に配置すると、オフィス エリアへ 180 フィートの電波妨害が可能です。攻撃中は、ターゲット エリア内の WLAN デバイスはワイヤレス サービスを利用できません。

- 物理的な損傷を受けた AP ハードウェア：攻撃者は指向性高利得アンテナを備えた高出力トランスミッタをアクセス ポイントから 30 ヤード離れた位置で使い、アクセス ポイント内の電子部品に損害を与え、アクセス ポイントを永久に使用不能にするのに十分な RF 出力を発生できます。このような高エネルギー RF（HERF）ガンは効果的であり、安価で製作できます。

wIPS による解決

Cisco Adaptive Wireless IPS は、RF 電波妨害攻撃の可能性のある特定しきい値を超える連続 RF ノイズを検出します。

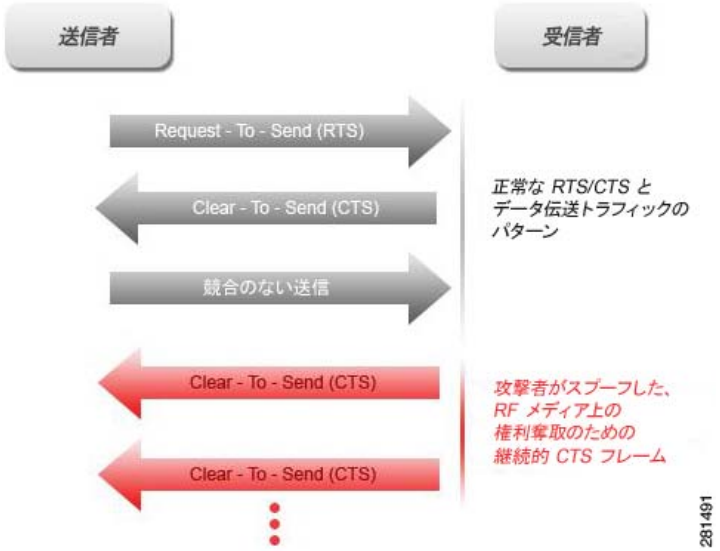
Cisco Spectrum Intelligence にも、802.11 非準拠電波妨害デバイスを検出する機能があります。Cisco Spectrum Intelligence の詳細については、『*Cisco Wireless Control System Configuration Guide*』を参照してください。

DoS 攻撃：RTS フラッディング

アラームの説明と考えられる原因

IEEE 802.11 標準には、ステーションによる RF 媒体へのアクセスを制御する RTS/CTS（Request-To-Send/Clear-To-Send）機能がオプションとして含まれています。送信準備が整ったワイヤレス デバイスは、指定された期間にわたって RF 媒体への送信権限を獲得するため、RTS フレームを送信します。レシーバは同じ期間の CTS フレームを送信して RF 媒体への権限をトランスミッタに付与します。CTS フレームを監視するワイヤレス デバイスはすべて、競合がない状態で送信できるようにトランスミッタに対してこの RF 媒体を生成します。図 18-6 を参照してください。

図 18-6　標準 RTS/CTS メカニズムと 侵入者によるインジェクション RTS DoS 攻撃



ワイヤレス DoS 攻撃を行うハッカーが、CTS フレームに付与された特権を悪用して RF 媒体を送信用に予約することがあります。攻撃者は大きな送信期間フィールドを含むバックツーバック RTS フレームを送信して無線媒体を予約し、RF 媒体を共有する他のワイヤレス デバイスが送信を行わないようにします。

wIPS による解決

Cisco Adaptive Wireless IPS は DoS 攻撃のための RTS フレームの不正使用を検出します。

DoS 攻撃：仮想キャリア攻撃

アラームの説明と考えられる原因

仮想キャリア検知攻撃を実行するには、ランダムな持続時間値を定期的に送信できるように 802.11 MAC 層実装を改ざんします。この攻撃は ACK、データ、RTS、および CTS フレームに対し、大きな持続時間値を使用して実行されます。これにより攻撃者は正規ユーザに対しチャネルへのアクセスを妨害できます。

通常の状況では、ACK フレームに大きな持続時間値が含まれているのは、ACK がフラグメンテーション パケット シーケンスの一部である場合だけです。データ フレームに大きな持続時間値が含まれているのは、そのデータ フレームがフラグメンテーション パケット交換の一部である場合だけです。

この攻撃への対処の 1 つとして、ノードにより受け入れられる持続時間値を制限する方法があります。この制限を超える大きな持続時間値が含まれているパケットはすべて、最大許容値になるように切り捨てられます。ロー キャップ値とハイ キャップ値が使用されます。ロー キャップの値は、ACK フレームの送信に必要な時間にフレームのメディア アクセス バックオフを加算した値です。ロー キャップが使用されるのは、監視対象パケットの後に送信可能なパケットが ACK または CTS のみである場合です。これには RTS フレームとすべての管理フレーム（アソシエーションなど）が含まれます。ハイ キャップが使用されるのは、監視対象フレームの後にデータ パケットが送信可能である場合です。この場合の制限には、最大データ フレームの送信に必要な時間とそのフレームのメディア アクセス バッ

クオフが含まれている必要があります。ハイ キャップを使用する必要があるのは、ACK 監視時（ACK が MAC レベルのフラグメンテーション パケットの一部である可能性があるため）と CTS 監視時です。

RTS フレーム受信するステーションはデータ フレームも受信します。IEEE 802.11 標準では、後続の CTS フレームとデータ フレームの正確な時間が指定されています。次のデータ フレームが受信されるかまたは受信されない時点まで、RTS の持続時間値が順守されます。監視対象 CTS が非請求であるか、または監視ノードが隠れ端末です。この CTS が有効な範囲内のステーション宛てである場合、有効なステーションは持続時間がゼロの Null ファンクション フレームを送信することでこれを無効にできます。この CTS が範囲外のステーション宛てである場合、防御策の 1 つとして、暗号を使用して署名された前の RTS のコピーを含む認証済み CTS フレームを導入する方法があります。この方法では、オーバーヘッドまたはフィジビリティの問題が発生する可能性があります。

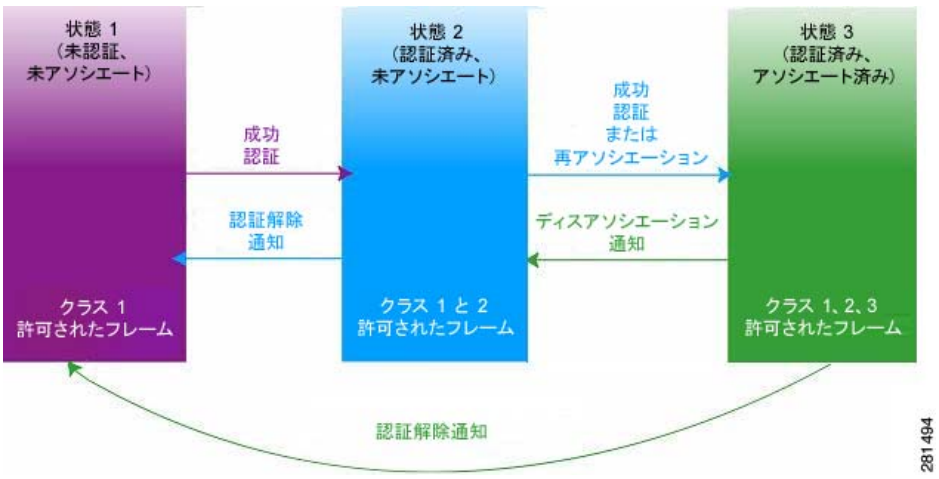
wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出します。デバイスを特定し、適切な手順でワイヤレス環境からそのデバイスを削除します。

クライアント ステーションに対する DoS 攻撃

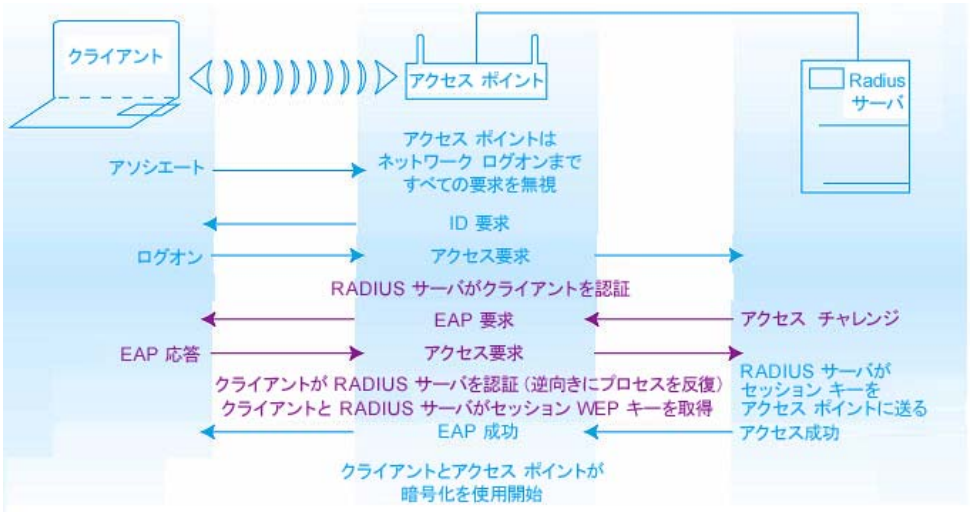
ワイヤレス クライアント ステーションに対する DoS（サービス拒絶）攻撃は通常、802.11 管理フレームと 802.1x 認証プロトコルには暗号化メカニズムがないためにスプーフィング可能であるという事実に基づいて実施されます。たとえばワイヤレス侵入者はアクセス ポイントからクライアント ステーションへの 802.11 アソシエート解除フレームまたは認証解除フレームを継続的にスプーフすることで、クライアント ステーションへのサービスを妨害できます。IEEE 標準で指定されている 802.11 アソシエーション ステート マシンを図 18-7 に示します。この図では、アソシエートされているステーションに対し、さまざまなタイプのスプーフィング フレームによって認証済みステートおよびアソシエート済みステートを偽装する方法を示します。

図 18-7　802.11 アソシエーションおよび認証ステート マシン



802.11 認証およびアソシエーション ステート攻撃の他に、802.1x 認証でも同様の攻撃シナリオがあります。たとえば 802.1x EAP-Failure メッセージまたは EAP-logoff メッセージは暗号化されていないため、これらのメッセージをスプーフして 802.1x 認証済みステートを妨害し、ワイヤレス サービスを妨害できます。802.1x 認証およびキー交換ステートの変化については、図 18-8 を参照してください。

図 18-8　802.1x ユーザ認証プロセス



Cisco Adaptive Wireless IPS はクライアント認証プロセスを追跡し、DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、攻撃検知および統計的シグニチャ照合プロセスが開始されます。DoS 攻撃が検出されると wIPS アラームが発行されます。このアラームには、標準のアラーム詳細記述とターゲット デバイス情報が含まれます。

この項では、クライアント ステーションに対する DoS 攻撃について説明します。この項は次のトピックで構成されています。

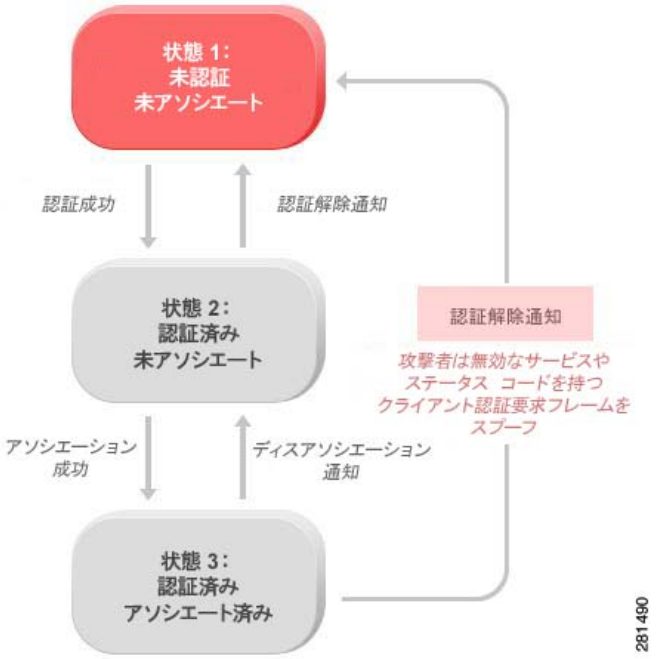
- 「DoS 攻撃：認証失敗攻撃」（P.18-1085）
- 「DoS 攻撃：ブロック ACK」（P.18-1086）
- 「DoS 攻撃：認証解除ブロードキャスト フラッディング」（P.18-1087）
- 「DoS 攻撃：認証解除フラッディング」（P.18-1088）
- 「DoS 攻撃：アソシエート解除ブロードキャスト フラッディング」（P.18-1089）
- 「DoS 攻撃：アソシエート解除フラッディング」（P.18-1090）
- 「DoS 攻撃：EAPOL-Logoff 攻撃」（P.18-1092）
- 「DoS 攻撃：FATA Jack ツール」（P.18-1092）
- 「DoS 攻撃：不完全な EAP-Failure」（P.18-1094）
- 「DoS 攻撃：不完全な EAP-Success」（P.18-1094）

DoS 攻撃：認証失敗攻撃

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは IEEE 標準に基づいてこのクライアント ステート マシンを実装します（図 18-9 を参照）。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信プロセスに参加できません。IEEE 802.11 ではオープン システム認証と共有キー認証という 2 種類の認証サービスが定義されています。ワイヤレス クライアントはいずれかの認証プロセスによってアクセス ポイントにアソシエートされます。

図 18-9　クライアント ステート マシン



DoS（サービス拒否）攻撃では、状態 3 のアソシエートされているクライアントからアクセス ポイントへ送信される無効な認証要求フレームが（不正な認証サービスおよびステータス コードで）スプーフされます。アクセス ポイントは無効な認証要求を受信するとクライアントを状態 1 に更新しますが、これによりクライアント ワイヤレス サービスが切断されます。

wIPS による解決

Cisco Adaptive Wireless IPS は、この DoS 攻撃を検出するためスプーフィング MAC アドレスと認証失敗をモニタします。このアラームは侵入が試みられたことを示すこともあります。アクセス ポイントとの認証段階でワイヤレス クライアントの失敗回数が多すぎると、サーバは侵入者がセキュリティを侵害しようとしている可能性を示すため、このアラームを生成します。

（注）　このアラームは、IEEE 802.11 の認証方式（オープン システムと共有キーなど）を対象にしています。EAP および 802.1x ベースの認証は、他のアラームによってモニタされます。

DoS 攻撃：ブロック ACK

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者は 802.11n AP を妨害し、特定の有効な企業クライアントからフレームを受信できないようにします。802.11n 規格の導入に伴い、クライアントがフレームの大きなブロックをセグメントに分割することなく、同時に送信することができるトランザクション メカニズムが導入されました。この交換を開始するために、クライアントは、送信ブロックのサイズを AP に知らせるシーケンス番号が含まれている Add Block Acknowledgement（ADDBA）を AP に送信します。AP は指定されているシーケンス内のすべてのフレームを受け入れ（範囲外のフレームはすべてドロップし）、トランザクションが完了したら BlockACK メッセージをクライアントに送信します。

攻撃者はこのプロセスを悪用するために、有効なクライアント MAC アドレスをスプーフしている間に無効な ADDBA フレームを送信できます。このプロセスにより、AP は無効なフレーム範囲の終わりに達するまで、クライアントから送信される有効なトラフィックを無視します。

wIPS による解決

wIPS サーバはスプーフされたクライアント情報の署名を確認するため ADDBA トランザクションをモニタします。攻撃者がブロック ACK 攻撃を開始しようとしていることが検出されると、アラームが生成されます。危険性のあるデバイスを特定し、特定したら早急にワイヤレス環境からそのデバイスを削除することを推奨します。

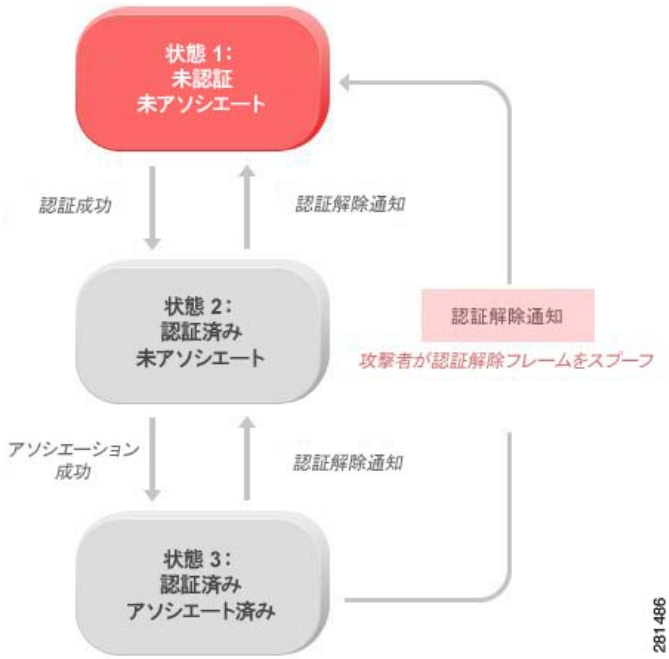
DoS 攻撃：認証解除ブロードキャスト フラッディング

攻撃ツール：WLAN Jack、Void11、Hunter Killer

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 18-10 を参照）。

図 18-10　クライアント ステート マシンと認証解除ブロードキャスト攻撃



この DoS 攻撃は、アクセス ポイントからブロードキャスト アドレスへの認証解除フレームをスプーフして、アクセス ポイントのすべてのクライアントを状態 1（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃は複数クライアントに対してワイヤレス サービスを

妨害する点で非常に効果的であり即効性があります。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフされた認証解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ アナリストはこのアクセス ポイントにログオンして現在のアソシエーション テーブルのステータスを確認できます。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』を参照してください。

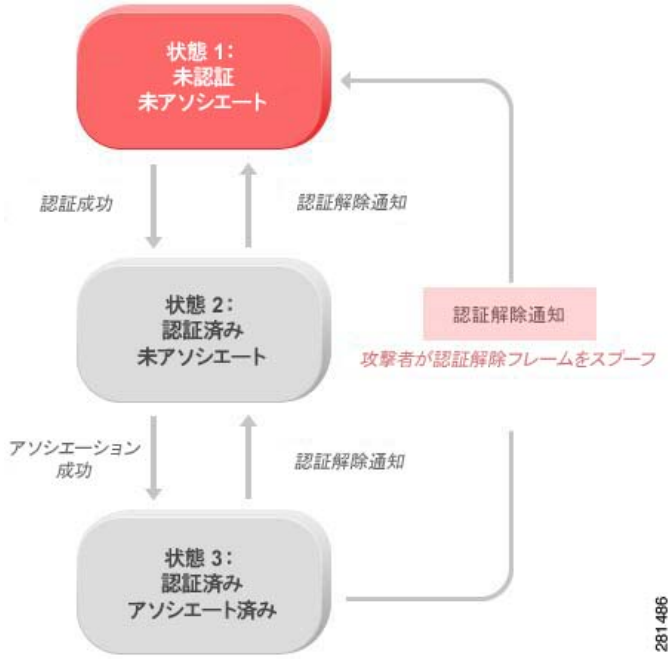
DoS 攻撃：認証解除フラッディング

攻撃ツール：WLAN Jack、Void11

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 18-11 を参照）。

図 18-11　クライアント ステート マシンと認証解除フラッディング攻撃



この DoS 攻撃では、アクセス ポイントからクライアント ユニキャスト アドレスへの認証解除フレームをスプーフしてアクセス ポイント クライアントを状態 1（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃はクライアントに対するワイヤレス サービスを妨害する点で非常に効果的かつ即効性があります。通常、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返し認証解除フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフされた認証解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントとクライアントが特定されます。WLAN セキュリティ オフィサはアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』を参照してください。

DoS 攻撃：アソシエート解除ブロードキャスト フラッディング

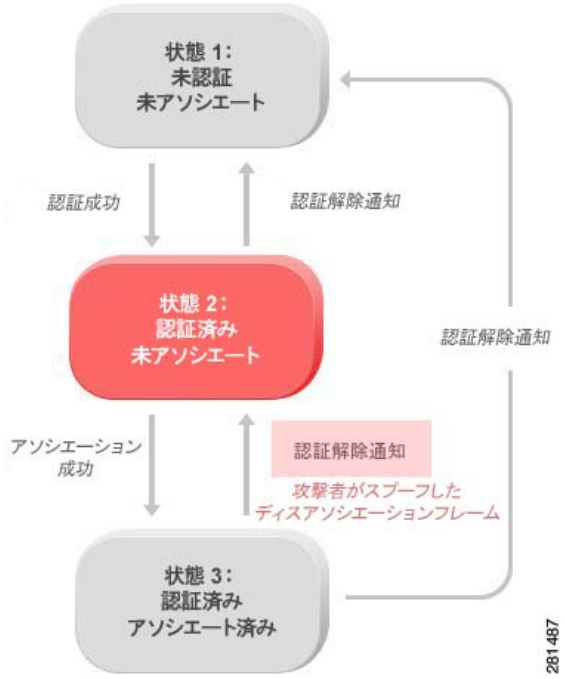
攻撃ツール：ESSID Jack

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアント ステー

ションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 18-12 を参照）。

図 18-12　クライアント ステート マシンとアソシエート解除ブロードキャスト攻撃



この DoS 攻撃では、アクセス ポイントからブロードキャスト アドレス（すべてのクライアント）へのアソシエート解除フレームをスプーフしてアクセス ポイント クライアントを状態 2（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃は複数クライアントに対してワイヤレス サービスを妨害する点で効果的かつ即効性があります。通常、クライアント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフされたアソシエート解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ オフィサはアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』を参照してください。

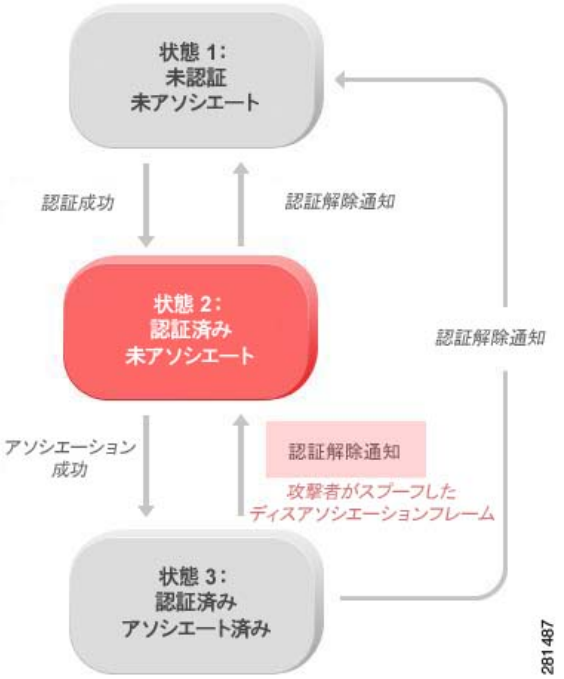
DoS 攻撃：アソシエート解除フラッディング

攻撃ツール：ESSID Jack

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアントは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアントは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません（図 18-13 を参照）。

図 18-13　クライアント ステート マシンとアソシエート解除フラッディング攻撃



この DoS 攻撃では、アクセス ポイントからクライアントへのディスアソシエーション フレームをスプーフしてアクセス ポイントを状態 2（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃はこのクライアントに対してワイヤレス サービスを妨害する点で効果的かつ即効性があります。通常、クライアント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、クライアントを使用不能な状態にします。

wIPS による解決

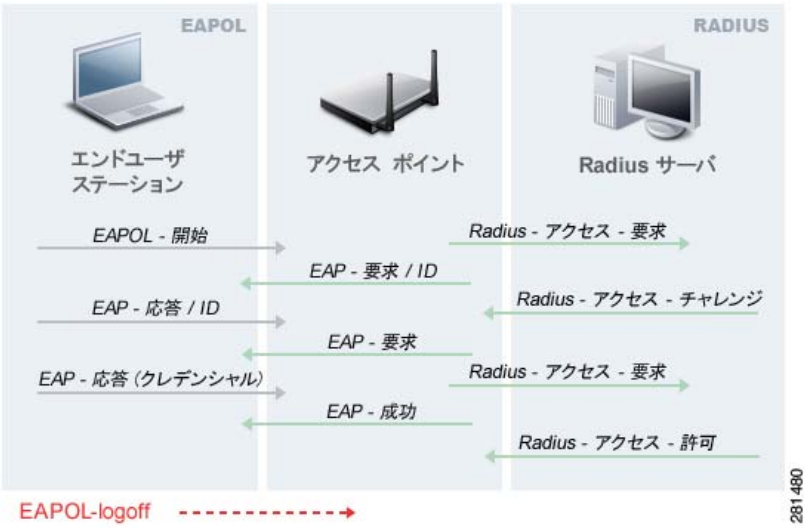
Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフされたアソシエート解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ オフィサはアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

DoS 攻撃：EAPOL-Logoff 攻撃

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol (EAP) over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-start フレームで開始します。認証セッションの終了時にクライアント ステーションがログオフするときに、クライアント ステーションは 802.1x EAPOL-logoff フレームを送信し、アクセス ポイントとのセッションを終了します（図 18-14 を参照）。

図 18-14　EAPOL-Logoff プロトコルと EAPOL-Logoff 攻撃



EAPOL-logoff フレームは認証されないため、攻撃者はこのフレームをスプーフし、ユーザをアクセス ポイントからログオフさせることができます。これにより DoS 攻撃が成立します。クライアントがアクセス ポイントからログオフしたことは、クライアントが WLAN 経由で通信を試行するまでは明らかではありません。通常この妨害が検出されると、クライアントはワイヤレス接続を回復するため自動的にアソシエートと認証を再実行します。攻撃者はスプーフィング EAPOL-logoff フレームを継続的に送信することで、この攻撃の効果を維持できます。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、802.1x 認証ステートを追跡します。アラームが生成されると、攻撃を受けたクライアントとアクセス ポイントが特定されます。WLAN セキュリティ オフィサはこのアクセス ポイントにログオンして現在のアソシエーション テーブルのステータスを確認できます。

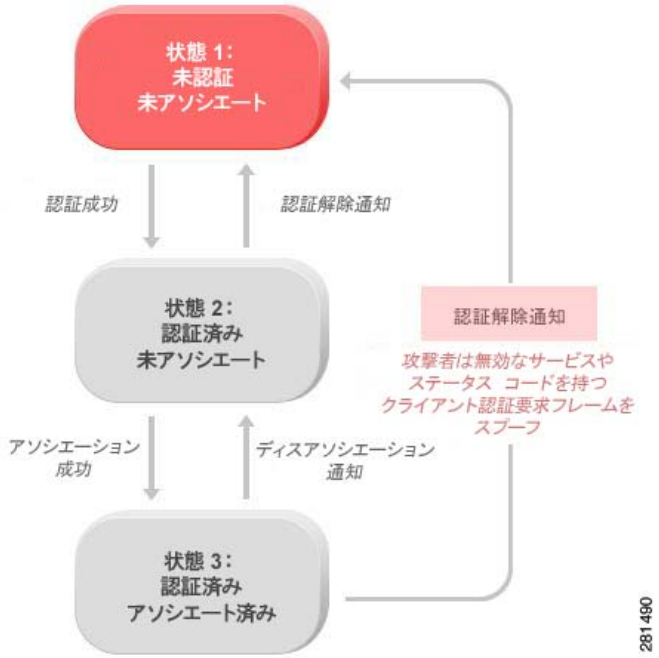
DoS 攻撃：FATA Jack ツール

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは IEEE 標準に基づいてこのステート マシンを実装します。適切にアソシエートされたクライアント ステー

ションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信プロセスに参加できません。IEEE 802.11 ではオープン システムと共有キーという 2 種類の認証サービスが定義されています。ワイヤレス クライアントはいずれかの認証プロセスによってアクセス ポイントにアソシエートされます（図 18-15 を参照）。

図 18-15　クライアント ステート マシンと DoS 攻撃



この DoS 攻撃では、状態 3 のアソシエートされているクライアントからアクセス ポイントへ送信される無効な認証要求フレームが（不正な認証サービスおよびステータス コードで）スプーフされます。アクセス ポイントは無効な認証要求を受信するとクライアントを状態 1 に更新しますが、これによりクライアント ワイヤレス サービスが切断されます。

FATA-jack は、同様の攻撃を実行するために最もよく使用されるツールの 1 つです。これは WLAN-jack を改変したツールであり、認証失敗パケットと、前回の認証失敗の理由コードをワイヤレス ステーションに送信します。これは、アクセス ポイントの MAC アドレスをスプーフィングした後に行われます。FATA-jack は最もアクティブな接続を閉じるため、時には、ユーザは通常の処理を続行するためにステーションをリブートする必要があります。

wIPS による解決

Cisco Adaptive Wireless IPS は、FATA-jack の利用を検出するためスプーフィング MAC アドレスと認証失敗をモニタします。このアラームは侵入が試みられたことを示すこともあります。アクセス ポイントとの認証段階でワイヤレス クライアントの失敗回数が多すぎると、Cisco Adaptive Wireless IPS はセキュリティを侵害しようとする侵入者の可能性を示すため、このアラームを生成します。

（注） このアラームは 802.11 認証方式（オープン システム、共有キーなど）を監視の対象とします。EAP および 802.1x ベースの認証は、他のアラームによってモニタされます。

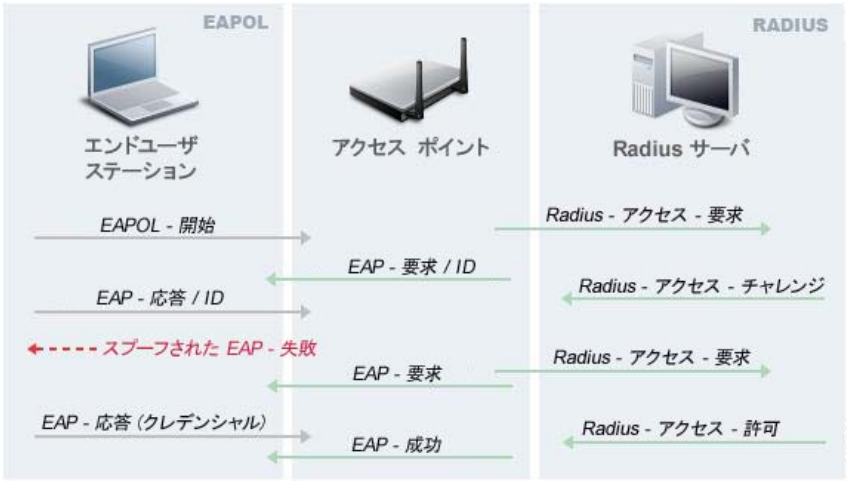
また、Cisco 管理フレーム保護は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。

DoS 攻撃：不完全な EAP-Failure

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-Start フレームで開始します。バックエンド RADIUS サーバとの 802.1x 認証パケット交換が完了すると、アクセス ポイントからクライアントに対し、認証の成功を示す EAP-success または失敗を示す EAP-failure が送信されます（図 18-16 を参照）。

図 18-16　EAP-Failure プロトコルと不完全な EAP-Failure 攻撃



IEEE 802.1X 仕様では、必要な相互認証が完了していない場合にクライアントによるインターフェイスの表示が禁止されています。これにより、適切に実装された 802.1x クライアント ステーションが、不完全な EAP-success パケットを送信する疑似アクセス ポイントにだまされることを回避できます。

攻撃者はアクセス ポイントからクライアントへの不完全な EAP-failure フレームを継続的にスプーフしてクライアントの認証ステートを妨害し、クライアント インターフェイスが表示されないようにします。

wIPS による解決

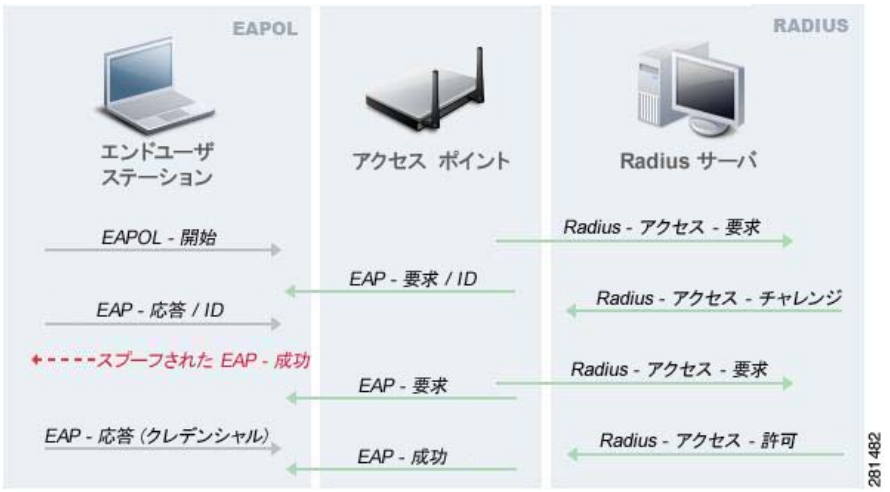
Cisco Adaptive Wireless IPS は、スプーフされた不完全な EAP-failure フレームと各クライアント ステーションおよびアクセス ポイントの 802.1x 認証ステートを追跡することで、この DoS 攻撃を検出します。デバイスを特定してワイヤレス環境から削除します。

DoS 攻撃：不完全な EAP-Success

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-start フレームで開始します。バックエンド RADIUS サーバとの 802.1x 認証パケット交換が完了すると、アクセス ポイントからクライアントに対し、認証が正常に完了したことを示す EAP-success フレームが送信されます（図 18-17 を参照）。

図 18-17　EAP-Success プロトコルと EAP-Success 攻撃



IEEE 802.1X 仕様では、必要な相互認証が完了していない場合にクライアントによるインターフェイスの表示が禁止されています。これにより、適切に実装された 802.1x クライアント ステーションが、不完全な EAP-success パケットを送信して相互認証プロセスを迂回する疑似アクセス ポイントにだまされることを回避できます。

攻撃者はアクセス ポイントからクライアントへの不完全な EAP-success フレームを継続的にスプーフして認証ステートを妨害し、クライアント インターフェイスが表示されないようにします。

wIPS による解決

Cisco Adaptive Wireless IPS は、スプーフされた不完全な EAP-success フレームと各クライアント ステーションおよびアクセス ポイントの 802.1x 認証ステートを追跡することで、この DoS 攻撃を検出します。デバイスを特定してワイヤレス環境から削除します。

侵入検知：セキュリティ突破

ワイヤレス侵入の 1 つに、WLAN 認証メカニズムを突破し、有線ネットワークまたはワイヤレス デバイスへのアクセスを獲得するものがあります。認証方式への辞書攻撃は、アクセス ポイントに対する一般的な攻撃の 1 つです。侵入者は、アクセス ポイントとのアソシエーション プロセス中にワイヤレス クライアント ステーションを攻撃することもあります。たとえば何も知らないワイヤレス クライアントに対する疑似アクセス ポイント攻撃により、そのクライアントが疑似アクセス ポイントにアソシエートすることがあります。この攻撃によって、侵入者はワイヤレス ステーションへのネットワーク アクセスを取得して、ファイル システムをハッキングできる可能性があります。その後、侵入者はそのステーションを使用して企業の有線ネットワークにアクセスできます。

セキュリティに対するこのような脅威は、相互認証と強力な暗号化手法を使用することで防止できます。Cisco Adaptive Wireless IPS は弱いセキュリティ構成と侵入攻撃の試みを検出します。Cisco Adaptive Wireless IPS は最良のセキュリティ ポリシー実装を検証し、侵入の試みを検出することで強力なワイヤレス セキュリティ保護を実現します。このような脆弱性や攻撃の試みが検出されると、Cisco Adaptive Wireless IPS はこのような侵入の試みを管理者に通知するアラームを生成します。

この項では、セキュリティ突破攻撃について説明します。この項は次のトピックで構成されています。

- 「Airsnarf 攻撃」（P.18-1096）

- 「ChopChop 攻撃」（P.18-1098）
- 「WLAN パフォーマンス異常によるゼロデイ攻撃」（P.18-1099）
- 「WLAN のセキュリティ異常によるゼロデイ攻撃」（P.18-1101）
- 「デバイスのパフォーマンス異常によるゼロデイ攻撃」（P.18-1102）
- 「デバイスのセキュリティ異常によるゼロデイ攻撃」（P.18-1103）
- 「AP のデバイス プローブ」（P.18-1105）
- 「EAP メソッドへの辞書攻撃」（P.18-1106）
- 「802.1x 認証に対する EAP 攻撃」（P.18-1107）
- 「疑似アクセス ポイントの検出」（P.18-1107）
- 「偽の DHCP サーバの検出」（P.18-1108）
- 「高速 WEP クラック ツールの検出」（P.18-1109）
- 「フラグメンテーション攻撃」（P.18-1110）
- 「Hot-Spotter ツール検出」（P.18-1111）
- 「不正 802.11 パケットの検出」（P.18-1113）
- 「中間者攻撃」（P.18-1113）
- 「モニタ対象デバイスの検出」（P.18-1114）
- 「NetStumbler の検出」（P.18-1115）
- 「NetStumbler 犠牲者の検出」（P.18-1116）
- 「Publicly Secure Packet Forwarding（PSPF）違反の検出」（P.18-1117）
- 「ASLEAP ツール検出」（P.18-1118）
- 「ハニーポット AP の検出」（P.18-1120）
- 「ソフト AP またはホスト AP の検出」（P.18-1120）
- 「スプーフされた MAC アドレスの検出」（P.18-1121）
- 「疑わしい営業時間外のトラフィックの検出」（P.18-1121）
- 「ベンダー リストによる未承認アソシエーション」（P.18-1122）
- 「未承認アソシエーションの検出」（P.18-1123）
- 「Wellenreiter の検出」（P.18-1123）

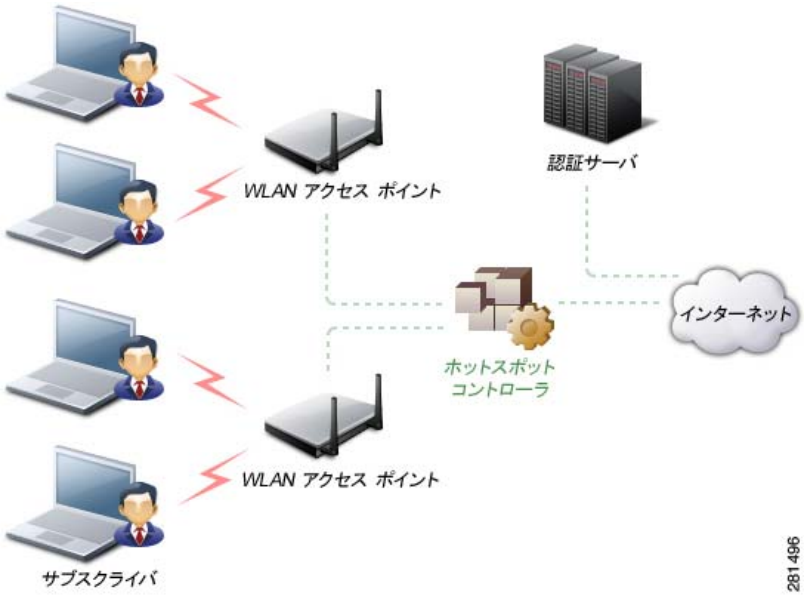
Airsnarf 攻撃

アラームの説明と考えられる原因

ホットスポットとは、Wi-Fi ネットワーク アクセスが一般向けに開放されている場所を指します。ホットスポットは空港、ホテル、喫茶店をはじめ、ビジネスマンが集まることが多い場所にあります。ホットスポットは出張旅行者にとって最も重要なネットワーク アクセス サービスです。

ワイヤレス対応ラップトップや携帯機器から正規のアクセス ポイントに接続してサービスを利用できます。ほとんどのホットスポットでは、ユーザがアクセス ポイントに接続するときには、ログイン用の Web ページを開く操作以外の高度な認証メカニズムは不要です。ログインできるかどうかの条件は、利用者が利用料金を支払っているかどうかだけです。ワイヤレス ホットスポット環境では誰も信用すべきではありません。現在のセキュリティ上の懸念から、一部の WLAN ホットスポット ベンダーはユーザ ID の検証に 802.1x 以上の認証メカニズムを採用しています（図 18-18 を参照）。

図 18-18　WLAN ホットスポット ネットワークの基本コンポーネント



ホットスポット ネットワークの 4 つの基本コンポーネントを次に示します。

- ホットスポット利用ユーザ：ワイヤレス対応のラップトップまたは携帯機器を所持し、ホットスポット ネットワークにアクセスするための有効なログイン情報を持つユーザ。
- WLAN アクセス ポイント：ホットスポット実装に応じて、SOHO ゲートウェイまたはエンタープライズ レベル アクセス ポイントのいずれかです。
- ホットスポット コントローラ：ユーザ認証、課金情報の収集、利用時間の追跡、機能のフィルタリングなどを実行します。これは独立したマシンであるか、またはアクセス ポイント自体に組み込まれています。
- 認証サーバ：利用ユーザのログイン資格情報が保管されています。ほとんどのホットスポット コントローラは、認証サーバを使用して利用ユーザの資格情報を検証します。

Airsnarf は、ハッカーがパブリック ワイヤレス ホットスポットからユーザ名とパスワードのクレデンシャルをどのように盗むことができるかを示すワイヤレス アクセス ポイント セットアップ ユーティリティです。

Airsnarf はシェル スクリプト ベースのツールであり、ユーザがログイン情報を入力するキャプティブ ポータルとホットスポットを作成します。ローカル ネットワーク情報、ゲートウェイ IP アドレス、SSID などの重要な値は airsnarf 設定ファイル内で設定できます。このツールは最初に、インターネットに接続されている許可済みのアクセス ポイントからホットスポット ワイヤレス クライアントをディスアソシエーションする非常に強力な信号をブロードキャストします。ワイヤレス クライアントは、何らかの不明な問題が原因でインターネットから一時的に切断されていると仮定して再度ログインしようとします。Airsnarf アクセス ポイントにアソシエートするワイヤレス クライアントが、ホットスポット オペレータにより導入された正規のアクセス ポイントではなく不正な Airsnarf アクセス ポイントから、IP アドレス、DNS アドレス、ゲートウェイ IP アドレスを受信します。Web ページからユーザ名とパスワードの入力が求められ、不正な Airsnarf アクセス ポイントによって DNS クエリが解決されます。ハッカーは入力されたユーザ名とパスワードを収集します。

そのユーザ名とパスワードは、ユーザに悪用を気づかれることなく、国内にある同じプロバイダーの他のホットスポット ロケーションで使用することができます。影響が小さくなる唯一のケースは、ホットスポット ユーザが利用時間課金制で接続している場合です。

Airsnarf ツールは、Airsnarf アクセス ポイントに知らないうちに接続しているラップトップ クライアントにも侵入する可能性があります。AirSnarf ツールは次のサイトで公開されており、ハッカーもダウンロードできます。

http://airsnarf.shmoo.com/

wIPS による解決

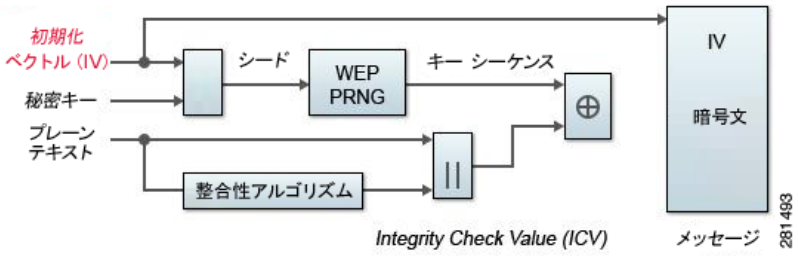
Cisco Adaptive Wireless IPS は AirSnarf ツールを実行しているワイヤレス デバイスを検出します。AirSnarf ツールを WLAN 環境から削除するために管理者が適切な措置をとる必要があります。

ChopChop 攻撃

アラームの説明と考えられる原因

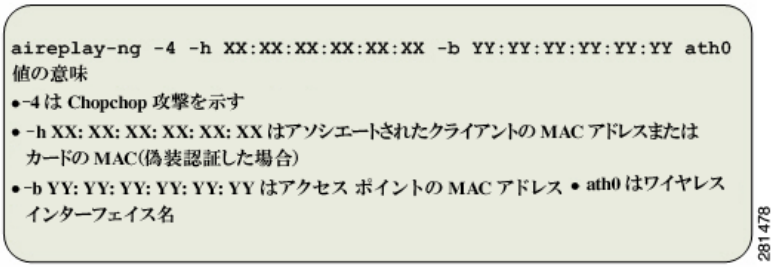
暗号化に静的 WEP キーを使用する WLAN デバイスは、さまざまな WEP クラッキング攻撃の対象となるリスクがあることはよく知られています（図 18-19 を参照）。詳しくは、『*Weaknesses in the Key Scheduling Algorithm of RC4 - I*』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照してください。

図 18-19　　WEP 暗号化プロセスのブロック図



クラックされた WEP 秘密キーでは送信データは暗号化保護されず、データ プライバシーが侵害されます。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーであり、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。chopchop ツールは Korek により Linux オペレーティング システム向けに開発されたツールで、WEP の脆弱性を悪用して WEP データ パケットの暗号化を解除します。ただし chopchop ツールはプレーンテキストのみを公開します（図 18-20 を参照）。攻撃者は初期フェーズ中に以前にインジェクトされたパケットのパケット キャプチャ ファイルを使用し、改ざんしたパケットを攻撃対象ネットワークに再送信してパケットの暗号化を解除します。攻撃が完了すると、chopchop ツールは暗号化されていないパケット キャプチャ ファイルと、暗号化解除プロセスで判別された PRGA（Pseudo Random Generation Algorithm）情報を使用したもう 1 つのファイルを作成します。次に PGRA はプレーンテキストを取得するために暗号文と XOR されます。

図 18-20　Chopchop 攻撃実行コマンド



60 バイト未満のデータ パケットをドロップするアクセス ポイントは、この攻撃に対して脆弱ではありません。アクセス ポイントが 42 バイト未満のパケットをドロップする場合、aireplay はヘッダーが予測可能な限り、残りの欠落データを推測しようとします。IP パケットがキャプチャされると、ヘッダーの欠落部分を推測した後でヘッダーのチェックサムが正しいかどうかを検査します。攻撃者は 1 つ以上の WEP データ パケットを必要とします。chopchop 攻撃は動的 WEP 設定にも有効です。Cisco Adaptive Wireless IPS は chopchop ツールを使用した攻撃の可能性を検出できます。

wIPS による解決

Cisco Adaptive Wireless IPS は、chopchop の可能性がある攻撃が進行している場合にアラートを出します。企業環境では WEP を使用しないでください。ネットワーク内でセキュリティ ホールが発生しないように適切な手段を講じ、よりセキュアな IEEE 802.11i 標準を使用するようにワイヤレス ネットワーク インフラストラクチャとデバイスをアップグレードしてください。

WLAN パフォーマンス異常によるゼロデイ攻撃

アラームの説明と考えられる原因

WLAN のパフォーマンス効率は、常に RF 環境の変動とクライアント デバイスの移動の影響を受けます。注意深くモニタされ、適切に調整されている WLAN システムでは、適切に管理されていない WLAN システムよりも高いスループットを実現できます。Cisco Unified Wireless Network に内蔵されている無線リソース管理（RRM）機能は、RF 環境をモニタし、この環境で検出されるパフォーマンスの問題を動的に修正します。さらなるパフォーマンス異常のモニタリングは、Wireless IPS システムを使用して行うことができます。RRM の詳細については、Cisco Prime Infrastructure オンライン ヘルプを参照してください。

Cisco Adaptive Wireless IPS は、WLAN を継続的にモニタし、ワイヤレス管理者に対して問題を警告する早期兆候を通知することで、WLAN のパフォーマンスと効率を維持します。パフォーマンスが低下すると生成されるパフォーマンス アラームは、次のカテゴリに分類されます。

- RF 管理：Cisco Adaptive Wireless IPS は物理 RF 環境をモニタします。この RF 環境は動的であり、WLAN パフォーマンスの問題の発生源となることがよくあります。RF 環境のモニタリング中に、サーバは以下の WLAN の基本情報を明らかにし、問題を報告します。
  - チャネルの干渉とチャネルの割り当ての問題
  - チャネル ノイズと非 802.11 信号
  - WLAN RF サービス対象エリア
  - 典型的な RF 隠れノードの問題

- 問題のあるトラフィック パターン：RF マルチパスの問題をはじめとする多くの WLAN パフォーマンス問題は、MAC 層プロトコル トランザクションと統計に表れます。Cisco Adaptive Wireless IPS はワイヤレス トラフィックを追跡、分析することで、パフォーマンスの非効率性と低下を早期に検出できます。多くの場合、Cisco Adaptive Wireless IPS は検出されたパフォーマンスの問題の原因を判別し、対策を提案できます。Cisco Adaptive Wireless IPS が追跡する MAC 層プロトコルの特性には次のものがあります。
  - フレーム CRC エラー
  - フレーム再送信
  - フレーム速度（1、2、5.5、11、... Mbps）の使用と分布
  - レイヤ 2 フレーム フラグメンテーション
  - アクセス ポイントとステーションのアソシエート / 再アソシエート / アソシエート解除の関係
  - ローミング ハンドオフ
- チャネルまたはデバイスのオーバーロード：Cisco Adaptive Wireless IPS は、負荷をモニタおよび追跡して、チャネル帯域幅の制限と WLAN デバイスのリソース容量の両方でスムーズな運用ができるようにします。プロビジョニングの不足や過剰な増加のために、WLAN のパフォーマンスが十分でない場合、Cisco Adaptive Wireless IPS はアラームを生成して、詳細な情報を提供します。RF には、同僚が隣接チャネルに新しい WLAN デバイスを取り付けた場合でも、WLAN チャネルの使用率が大幅に増加する可能性のある境界はありません。Cisco Adaptive Wireless IPS は適切な帯域幅とリソースのプロビジョニングを実現するため、WLAN をモニタします。
- 導入および運用時のエラー：Cisco Adaptive Wireless IPS は電波をスキャンして設定エラーと運用エラーを確認します。次に示す領域は継続的にモニタされます。
  - 同一 SSID を使用するアクセス ポイント間の矛盾する設定
  - ベスト プラクティスの原則に違反する設定
  - クライアントおよびアクセス ポイントの設定の不一致が原因で発生する接続の問題
  - WLAN インフラストラクチャのデバイスのダウンまたはリセット
  - WLAN デバイス実装の欠陥
- IEEE 802.11e および VoWLAN の問題：IEEE 802.11e 標準では、既存の 802.11 a/b/g ワイヤレス標準に加えて QoS（Quality of Service）機能とマルチメディア サポートが導入されました。これらの標準との完全な下位互換性を維持しながら、付加機能が追加されました。QoS 機能は、音声ビデオ アプリケーションで重要です。ワイヤレス LAN では帯域幅が制限されており、従来の有線イーサネットと比較するとオーバーヘッドが高くなっています。RTS/CTS メカニズム、パケット フラグメンテーション、パケット再送信、確認、コリジョンなど、さまざまな理由でスループットが低下します。

wIPS による解決

Cisco Adaptive Wireless IPS は、ワイヤレス ネットワーク上の多数のデバイスにおける 1 つのパフォーマンス侵害ポリシー違反を検出します。指定の期間内に特定のポリシーに違反しているデバイス数が検出されたか、またはアラームのしきい値設定に指定されているデバイス数のパーセンテージが突然増加しています。パフォーマンス侵害違反によっては、詳しい分析のためにデバイスをモニタおよび特定することを推奨します。

次に例を示します。

- 多数のデバイスによって「ステーションにより過負荷状態になったアクセス ポイント」アラームが生成される場合、ハッカーが数千のステーションを生成し、これらのステーションを企業アクセス ポイントに強制的にアソシエートしている可能性があります。この状況が発生すると、正規の企業クライアントがアクセス ポイントに接続できなくなります。

- ワイヤレス デバイスで*フレーム再試行が過剰に行われる*場合、ノイズ、干渉、パケット コリジョン、マルチパス、隠れノードの問題などが発生している可能性があります。

WLAN のセキュリティ異常によるゼロデイ攻撃

アラームの説明と考えられる原因

企業環境に WLAN を追加すると、ネットワーク セキュリティに対するまったく新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無許可のユーザに公開する可能性があります。個人の使用のために従業員によって設置された不正アクセス ポイントは通常、企業のセキュリティ ポリシーに準拠していません。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正なアクセス ポイントの他にも、ワイヤレス ネットワークのセキュリティを侵害するワイヤレス セキュリティの脆弱性（アクセス ポイントの設定ミス、未設定のアクセス ポイントなど）があります。さまざまなソースから企業ネットワークに対して DoS（サービス拒否）攻撃が行われることもあります。

Prime Infrastructure は、ワイヤレス インフラストラクチャ内でセキュリティの脆弱性を自動的に評価する機能を提供します。この機能は、セキュリティの脆弱性または設定ミスを事前に報告します。さらに詳細な評価が Wireless IPS システムから無線で行われることがあります。Cisco Adaptive Wireless IPS は、包括的なセキュリティ モニタリング テクノロジー スイートを使用して、次のカテゴリ内の 100 件を超えるさまざまな脅威状況をユーザに警告します。

- ユーザ認証とトラフィック暗号化（静的 WEP 暗号化、VPN、Fortress、Cranite、802.11i、802.1x）：このカテゴリ（認証と暗号化）の一般的なセキュリティ違反には、設定ミス、古いソフトウェア / ファームウェア、最適ではない企業セキュリティ ポリシーの選択などがあります。
- 不正デバイス、モニタ対象デバイス、アドホック モード デバイス：企業ネットワーク（ワイヤレスおよび有線）の整合性を保護するため、不正デバイスを検出し、即時に削除する必要があります。
- 設定の脆弱性：セキュアな WLAN においては強力な導入ポリシーを実装することが重要です。ただしポリシーを適用するには、設定ミスや装置ベンダーの実装エラーにより引き起こされる違反を定期的なモニタによって捕捉する必要があります。ラップトップに Wi-Fi 機能が内蔵される傾向が高まっていることから、WLAN 設定の複雑さは、アクセス ポイントからユーザ ラップトップに拡大しています。WLAN デバイス設定管理製品を利用すると設定プロセスが容易になりますが、内蔵 Wi-Fi 機能が未使用、未設定の状態のラップトップでは特に検証を行う必要があります。
- セキュリティ突破に関する侵入検知：このワイヤレス侵入には、WLAN 認証メカニズムの突破による有線ネットワークまたはワイヤレス デバイスへのアクセスの獲得が含まれます。認証方式への辞書攻撃は、アクセス ポイントに対する非常に一般的な攻撃の 1 つです。侵入者は、アクセス ポイントとのアソシエーション プロセス中にワイヤレス クライアント ステーションを攻撃することもあります。たとえば何も知らないワイヤレス クライアントに対する疑似 AP 攻撃により、そのクライアントが疑似アクセス ポイントにアソシエートすることがあります。この攻撃によって、侵入者はワイヤレス ステーションへのネットワーク アクセスを取得して、ファイル システムをハッキングできる可能性があります。その後、侵入者はそのステーションを使用して企業の有線ネットワークにアクセスできます。
- DoS 攻撃の侵入検知：ワイヤレス DoS（サービス拒否）攻撃は、レイヤ 1 またはレイヤ 2 における WLAN のさまざまな脆弱性を悪用してワイヤレス サービスを妨害することを狙いとしています。DoS 攻撃は、物理的な RF 環境、アクセス ポイント、クライアント ステーション、またはバックエンド認証 RADIUS サーバをターゲットとする可能性があります。たとえば、オフィスがある建物の外部から、高出力指向性アンテナを使用した遠隔 RF 電波妨害攻撃が行われることがあります。侵入者が使用する攻撃ツールは、スプーフされた 802.11 管理フレームやスプーフされた 802.1x 認証フレームなどのハッキング技法、または単に総当たりのパケット フラッディング方法を利用します。

wIPS による解決

Cisco Adaptive Wireless IPS は、ワイヤレス ネットワーク上の多数のデバイスにおける 1 つのセキュリティ IDS/IPS ポリシー違反を検出します。指定の期間内に特定のポリシーに違反しているデバイス数が検出されたか、またはアラームのしきい値設定に指定されているデバイス数のパーセンテージが突然増加しています。セキュリティ IDS/IPS 違反によっては、詳しい分析のためにデバイスをモニタおよび特定し、デバイスがエンタープライズ ワイヤレス ネットワークを何らかの形（攻撃または脆弱性）で侵害していないかどうかを確認することを推奨します。不正デバイスの数が増加している場合は、ネットワークに対して攻撃が行われている可能性があります。WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、デバイスを検出する不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースします。

暗号化が無効な状態でクライアント デバイスの数が突然増加した場合は、企業セキュリティ ポリシーを再確認し、ポリシー ルールに基づいてユーザが最高レベルの暗号化と認証を強制的に使用するようにする必要があります。

デバイスのパフォーマンス異常によるゼロデイ攻撃

アラームの説明と考えられる原因

WLAN のパフォーマンス効率は、常に RF 環境の変動とクライアント デバイスの移動の影響を受けます。注意深くモニタされ、適切に調整されている WLAN システムでは、適切に管理されていない WLAN システムよりも高いスループットを実現できます。Cisco Unified Wireless Network に内蔵されている無線リソース管理機能は、RF 環境をモニタし、この環境で検出されるパフォーマンスの問題を動的に修正します。さらなるパフォーマンス異常のモニタリングは、Wireless IPS システムを使用して行うことができます。RRM の詳細については、Cisco Prime Infrastructure オンライン ヘルプを参照してください。

Cisco Adaptive Wireless IPS は、WLAN を継続的にモニタし、ワイヤレス管理者に対して問題を警告する早期兆候を通知することで、WLAN のパフォーマンスと効率を維持します。パフォーマンスが低下すると生成されるパフォーマンス アラームは、次のカテゴリに分類されます。

- RF 管理：Cisco Adaptive Wireless IPS は物理 RF 環境をモニタします。この RF 環境は動的であり、WLAN パフォーマンスの問題の発生源となることがよくあります。RF 環境のモニタリング中に、サーバは以下の WLAN の基本情報を明らかにし、問題を報告します。
  - チャネルの干渉とチャネルの割り当ての問題
  - チャネル ノイズと非 802.11 信号
  - WLAN RF サービス対象エリア
  - 典型的な RF 隠れノードの問題
- 問題のあるトラフィック パターン：RF マルチパスの問題をはじめとする多くの WLAN パフォーマンス問題は、MAC 層プロトコル トランザクションと統計に表れます。Cisco Adaptive Wireless IPS はワイヤレス トラフィックを追跡、分析することで、パフォーマンスの非効率性と低下を早期に検出できます。多くの場合、Cisco Adaptive Wireless IPS は検出されたパフォーマンスの問題の原因を判別し、対策を提案できます。Cisco Adaptive Wireless IPS が追跡する MAC 層プロトコルの特性には次のものがあります。
  - フレーム CRC エラー
  - フレーム再送信
  - フレーム速度（1、2、5.5、11、... Mbps）の使用と分布
  - レイヤ 2 フレーム フラグメンテーション
  - アクセス ポイントとステーションのアソシエート / 再アソシエート / アソシエート解除の関係

  - ローミング ハンドオフ

- チャネルまたはデバイスのオーバーロード：Cisco Adaptive Wireless IPS は、負荷をモニタおよび追跡して、チャネル帯域幅の制限と WLAN デバイスのリソース容量の両方でスムーズな運用ができるようにします。プロビジョニングの不足や過剰な増加のために、WLAN のパフォーマンスが十分でない場合、Cisco Adaptive Wireless IPS はアラームを生成して、詳細な情報を提供します。RF には、同僚が隣接チャネルに新しい WLAN デバイスを取り付けた場合でも、WLAN チャネルの使用率が大幅に増加する可能性のある境界はありません。Cisco Adaptive Wireless IPS は適切な帯域幅とリソースのプロビジョニングを実現するため、WLAN をモニタします。
- 導入および運用時のエラー：Cisco Adaptive Wireless IPS は電波をスキャンして設定エラーと運用エラーを確認します。次に示す領域は継続的にモニタされます。
  - 同一 SSID を使用するアクセス ポイント間の矛盾する設定
  - ベスト プラクティスの原則に違反する設定
  - クライアントおよびアクセス ポイントの設定の不一致が原因で発生する接続の問題
  - WLAN インフラストラクチャのデバイスのダウンまたはリセット
  - WLAN デバイス実装の欠陥
- IEEE 802.11e および VoWLAN の問題：IEEE 802.11e 標準では、既存の 802.11 a/b/g ワイヤレス標準に加えて QoS（Quality of Service）機能とマルチメディア サポートが導入されました。これらの標準との完全な下位互換性を維持しながら、付加機能が追加されました。QoS 機能は、音声ビデオ アプリケーションで重要です。ワイヤレス LAN では帯域幅が制限されており、従来の有線イーサネットと比較するとオーバーヘッドが高くなっています。RTS/CTS メカニズム、パケット フラグメンテーション、パケット再送信、確認、コリジョンなど、さまざまな理由でスループットが低下します。

Cisco Adaptive Wireless IPS の機能を最大限に活用するために、WLAN 導入仕様に最も適したものになるようにパフォーマンス アラームをカスタマイズできます。たとえば、すべてのユーザが速度 5.5 Mbps と 11 Mbps のみを使用するように設計されている WLAN では、「低速 tx 速度超過」パフォーマンス アラームのしきい値をカスタマイズしてその条件を反映します。

wIPS による解決

Cisco Adaptive Wireless IPS は、多数のパフォーマンス侵害ポリシーに違反するデバイスを検出します。指定の期間内にこのデバイスで多数のパフォーマンス侵害違反が発生したか、またはさまざまなアラームのしきい値設定に指定されている突然のパーセンテージ上昇が発生しています。このデバイスが原因でネットワーク全体のパフォーマンスに問題が発生している場合は、詳しい分析のためにデバイスをモニタおよび特定することを推奨します。

たとえば、「ステーションにより過負荷状態になったアクセス ポイント」アラームと「使用状況により過負荷状態になったアクセス ポイント」アラームで設定されているアクセス ポイント数の増加を引き起こしたデバイスがある場合、アクセス ポイントがステーションを処理できない可能性があります。管理者はアクセス ポイントの再導入を再び検討する必要があります。

デバイスのセキュリティ異常によるゼロデイ攻撃

アラームの説明と考えられる原因

企業環境に WLAN を追加すると、ネットワーク セキュリティに対する新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無許可のユーザに公開する可能性があります。個人の使用のために従業員によって設置された不正アクセス ポイントは通常、企業のセキュリティ ポリシーに準拠していません。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正なアクセス ポイントの他にも、ワイヤレ

ス ネットワークのセキュリティを侵害するワイヤレス セキュリティの脆弱性（アクセス ポイントの設定ミス、未設定のアクセス ポイントなど）があります。さまざまなソースから企業ネットワークに対して DoS 攻撃が行われることもあります。

Prime Infrastructure は、ワイヤレス インフラストラクチャ内でセキュリティの脆弱性を自動的に評価する機能を提供します。この機能は、セキュリティの脆弱性または設定ミスを事前に報告します。さらに詳細な評価が Wireless IPS システムから無線で行われることがあります。Cisco Adaptive Wireless IPS は、包括的なセキュリティ モニタリング テクノロジー スイートを使用して、次のカテゴリ内の 100 件を超えるさまざまな脅威状況をユーザに警告します。

- ユーザ認証とトラフィック暗号化（静的 WEP 暗号化、VPN、Fortress、Cranite、802.11i、802.1x）：このカテゴリ（認証と暗号化）の一般的なセキュリティ違反には、設定ミス、古いソフトウェア/ファームウェア、最適ではない企業セキュリティ ポリシーの選択などがあります。
- 不正デバイス、モニタ対象デバイス、アドホック モード デバイス：企業ネットワーク（ワイヤレスおよび有線）の整合性を保護するため、不正デバイスを検出し、即時に削除する必要があります。
- 設定の脆弱性：セキュアな WLAN においては強力な導入ポリシーを実装することが重要です。ただしポリシーを適用するには、設定ミスや装置ベンダーの実装エラーにより引き起こされる違反を定期的なモニタによって捕捉する必要があります。ラップトップに Wi-Fi 機能が内蔵される傾向が高まっていることから、WLAN 設定の複雑さは、アクセス ポイントからユーザ ラップトップに拡大しています。WLAN デバイス設定管理製品を利用すると設定プロセスが容易になりますが、内蔵 Wi-Fi 機能が未使用、未設定の状態のラップトップでは特に検証を行う必要があります。
- セキュリティ突破に関する侵入検知：このワイヤレス侵入には、WLAN 認証メカニズムの突破による有線ネットワークまたはワイヤレス デバイスへのアクセスの獲得が含まれます。認証方式への辞書攻撃は、アクセス ポイントに対する非常に一般的な攻撃の 1 つです。侵入者は、アクセス ポイントとのアソシエーション プロセス中にワイヤレス クライアント ステーションを攻撃することもあります。たとえば何も知らないワイヤレス クライアントに対する疑似 AP 攻撃により、そのクライアントが疑似アクセス ポイントにアソシエートすることがあります。この攻撃によって、侵入者はワイヤレス ステーションへのネットワーク アクセスを取得して、ファイル システムをハッキングできる可能性があります。その後、侵入者はそのステーションを使用して企業の有線ネットワークにアクセスできます。
- DoS 攻撃の侵入検知：ワイヤレス DoS（サービス拒否）攻撃は、レイヤ 1 またはレイヤ 2 における WLAN のさまざまな脆弱性を悪用してワイヤレス サービスを妨害することを狙いとしています。DoS 攻撃は、物理的な RF 環境、アクセス ポイント、クライアント ステーション、またはバックエンド認証 RADIUS サーバをターゲットとする可能性があります。たとえば、オフィスがある建物の外部から、高出力指向性アンテナを使用した遠隔 RF 電波妨害攻撃が行われることがあります。侵入者が使用する攻撃ツールは、スプーフされた 802.11 管理フレームやスプーフされた 802.1x 認証フレームなどのハッキング技法、または単に総当たりのパケット フラッディング方法を利用します。

wIPS による解決

Cisco Adaptive Wireless IPS は、多数のセキュリティ IDS/IPS ポリシーに違反するデバイスを検出します。指定の期間内にこのデバイスで多数のセキュリティ IDS/IPS 違反が発生したか、またはさまざまなアラームのしきい値設定に指定されている突然のパーセンテージ上昇が発生しています。詳しい分析のためにデバイスをモニタおよび特定し、デバイスがエンタープライズ ワイヤレス ネットワークを何らかの形（攻撃または脆弱性）で侵害していないかどうかを確認することを推奨します。不正デバイスの場合、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、デバイスを検出する不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースします。

AP のデバイス プローブ

よく使用されるスキャン ツールには、NetStumbler（新しいバージョン）、MiniStumbler（新しいバージョン）、MACStumbler、WaveStumbler、PrismStumbler、dStumbler、iStumbler、Aerosol、Boingo Scans、WiNc、AP Hopper、NetChaser、Microsoft Windows XP scan などがあります。

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は WLAN をプローブし、アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を試行するワイヤレス デバイスを検出します。

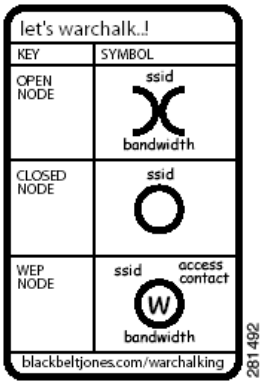
このようなデバイスは、次のいずれかでセキュリティの脅威となる可能性があります。

- ウォードライビング、WiLDing（ワイヤレス LAN 検出）、ウォーチョーキング、ウォーサイクルイング、ウォーライトレイリング、ウォーブッシング、ウォーフライング。
- 危険な無差別アソシエーションを試行する正規ワイヤレス クライアント。

ウォードライビング、ウォーチョーキング、ウォーウォーキング、ウォーフライングでは次のような行動が行われます。

- ウォードライビング：ワイヤレス ハッカーがウォードライビング ツールを使ってアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティなどの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します。
- ウォーチョーキング：ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に共通シンボルを使って WLAN 設定をマーキングします（図 18-21）。

図 18-21　　ウォーチョーキングで使用される共通シンボル



- ウォーウォーキング：ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。
- ウォーフライング：ウォーフライングは、ワイヤレス ネットワークを上空から探します。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

危険なアソシエートを試行する正規ワイヤレス クライアント

このアラームでのもう 1 つのセキュリティの脅威は、より深刻な損害をもたらす可能性があります。これらのアラームの一部は、使用可能なアクセス ポイント（ネイバー アクセス ポイントやより深刻な損害をもたらす不正なアクセス ポイントを含む）にアソシエートしようとしている WLAN 上の正規の許

可ワイヤレス クライアントによって発生することがあります。このセキュリティの脅威は、Wi-Fi カード内蔵 Microsoft Windows XP ラップトップや、Boingo クライアント ユーティリティまたは WiNc クライアント ユーティリティなどのワイヤレス接続ツールを使用するラップトップに起因することがあります。このクライアント ステーションへのアソシエートが完了すると侵入者がこのクライアント ステーションにアクセスできるようになり、これが原因で重大なセキュリティ侵害が発生する可能性があります。さらにクライアント ステーションが意図しないアクセス ポイントと企業内の有線 LAN を接続するブリッジとなることがあります。一般にラップトップには Wi-Fi カードが内蔵されており、またこのようなラップトップは企業内 WLAN ネットワークに物理的に接続しています。Windows ラップトップで Windows ブリッジ サービスが有効になっている場合は有線ネットワークが外部に公開されます。セキュリティ保護のため、すべてのクライアント ステーションに固有の SSID を設定し、意図しないアクセス ポイントからのアソシエートを防止します。また、802.1x やさまざまな EAP 方式などの相互認証を検討してください。

Cisco Adaptive Wireless IPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。ハッカーが最新バージョンの NetStumbler ツールを使っている場合、「アクセス ポイントをプローブするデバイス」アラームが生成されます。古いバージョンの場合、「NetStumbler の検出」アラームが生成されます。

NetStumbler は、ウォードライビングとウォーチョーキングに最も広く使用されているツールです。NetStumbler Web サイト（http://www.netstumbler.com/）は、ウォーウォーカーが重たいラップトップを持ち歩かずにすむように、Pocket PC ハードウェアで使用できる MiniStumbler ソフトウェアを提供します。Windows 2000、Windows XP およびこれ以降のオペレーティング システムが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピングセンターや小売店舗を徘徊します。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS で、ビーコンで SSID をブロードキャスト（アナウンス）しているアクセス ポイントを確認してください。

EAP メソッドへの辞書攻撃

アラームの説明と考えられる原因

EEE 802.1x は、ワイヤレス LAN および有線 LAN の認証の EAP フレームワークを規定しています。EAP フレームワークにより、柔軟な認証プロトコルを実装できます。一部の 802.1x または WPA 実装では LEAP、MD5、OTP（ワンタイム パスワード）、TLS、TTLS などの認証プロトコルが使用されています。このような認証プロトコルの一部で使用されるユーザ名とパスワードのメカニズムでは、ユーザ名が暗号化されずに送信され、認証チャレンジへの応答にパスワードが使用されます。

ほとんどのパスワード ベースの認証アルゴリズムは、辞書攻撃の影響を受けます。辞書攻撃では攻撃者が暗号化されていない 802.1x ID プロトコル交換からユーザ名を獲得します。その後攻撃者は一般的なパスワードの辞書のすべての単語またはパスワードの組み合わせからユーザ パスワードを推測してネットワーク アクセスを獲得しようとします。辞書攻撃は、パスワードに一般的な単語、名前、またはこの両方の組み合わせとわずかな変更（末尾の 1 桁または 2 桁の番号など）が使用されることに依存しています。

辞書攻撃がオンラインでアクティブに行われる場合、攻撃者はあらゆるパスワードの組み合わせを繰り返し試行します。オンライン辞書攻撃を防止するには、認証サーバ（RADIUS サーバ）で使用可能なロックアウト メカニズムを利用し、無効なログインが特定の回数を超えた後にユーザをロックアウトします。辞書攻撃はオフラインで行われることもあります。この場合、攻撃者は正常に完了した認証チャレンジ プロトコル交換をキャプチャし、チャレンジ応答に対してあらゆるパスワードの組み合わ

せを突き合わせます。オンライン攻撃とは異なり、オフライン アタックは容易に検出されません。強力なパスワード ポリシーを採用し、定期的にユーザ パスワードの有効期限が切れるように設定することで、オフライン攻撃ツールによる攻撃の成功率を大幅に削減します。

wIPS による解決

Cisco Adaptive Wireless IPS はオンライン辞書攻撃を検出するため、802.1x 認証プロトコル交換とユーザ ID の利用状況を追跡します。辞書攻撃が検出されると、ユーザ名と攻撃ステーションの MAC アドレスがアラーム メッセージに示されます。

Cisco Adaptive Wireless IPS は、ユーザ名とパスワードに基づく認証方式から、シスコをはじめとする多くのベンダーによりサポートされている暗号化トンネルに基づく認証方式（PEAP や EAP-FAST など）に切り替えるように指示します。

802.1x 認証に対する EAP 攻撃

アラームの説明と考えられる原因

IEEE 802.1x は、ワイヤレス LAN および有線 LAN の認証の拡張認証プロトコル（EAP）フレームワークを定義します。EAP フレームワークにより、柔軟な認証プロトコルを実装できます。一部の 802.1x または WPA 実装では LEAP、MD5、OTP（ワンタイム パスワード）、TLS、TTLS、EAP-FAST などの認証プロトコルが使用されています。このような認証プロトコルの一部で使用されるユーザ名とパスワードのメカニズムでは、ユーザ名が暗号化されずに送信され、認証チャレンジへの応答にパスワードが使用されます。

ほとんどのパスワード ベースの認証アルゴリズムは、辞書攻撃の影響を受けます。辞書攻撃では攻撃者が暗号化されていない 802.1x ID プロトコル交換からユーザ名を獲得します。その後攻撃者は一般的なパスワードの辞書のすべての単語またはパスワードの組み合わせからユーザ パスワードを推測してネットワーク アクセスを獲得しようとします。辞書攻撃は、パスワードに一般的な単語、名前、またはこの両方の組み合わせと一部の変更（末尾の 1 桁または 2 桁の番号など）がよく使用されることに依存しています。

正規の 802.1x ユーザ ID とパスワードの組み合わせ（または有効な証明書）を使用する侵入者は、正確な EAP タイプを理解していなくても 802.1x 認証プロセスを突破できます。侵入者はさまざまな EAP（TLS、TTLS、LEAP、EAP-FAST、PEAP など）を使ってネットワークへのログオンを試みます。攻撃者がネットワークへの認証を試す EAP の種類が限られていることから、これは試行錯誤による攻撃です。

wIPS による解決

Cisco Adaptive Wireless IPS は、攻撃者がさまざまな 802.1x 認証タイプを使ってネットワークへアクセスしようとする試みを検出します。適切な手順に従ってデバイスを特定し、ワイヤレス環境から削除してください。

疑似アクセス ポイントの検出

アラームの説明と考えられる原因

疑似 AP ツールは、NetStumbler、Wellenreiter、MiniStumbler、Kismet などを使うウォードライバを混乱させるおとりとして動作して WLAN を保護します。このツールは数千もの偽の 802.11b アクセス ポイントを模倣してビーコン フレームを生成します。ウォードライバは大量のアクセス ポイントを検出すると、ユーザが実際に導入している実際のアクセス ポイントを特定できません。このツールは

ウォードライバを阻止するには非常に有効ですが、帯域幅消費、正規クライアント ステーションの誤誘導、WLAN 管理ツールとの干渉といったデメリットがあります。WLAN 内で疑似 AP ツールを実行することは推奨しません。

wIPS による解決

管理者は疑似 AP ツールを実行するデバイスを特定してワイヤレス環境から削除する必要があります。

偽の DHCP サーバの検出

アラームの説明と考えられる原因

ネットワーク上のデバイスへの動的 IP アドレスの割り当てにはダイナミック ホスト コンフィギュレーション プロトコル（DHCP）が使用されます。

DHCP アドレス割り当ては次のように行われます。

ステップ 1　クライアント NIC から、DHCP サーバの IP アドレスが必要であることを示す DHCP 検出パケットが送信されます。

ステップ 2　サーバは IP アドレスを含む DHCP オファー パケットを送信します。

ステップ 3　クライアント NIC が DHCP 要求を送信します。この要求は DHCP サーバに対し、サーバ オファーにより送信された IP アドレスをクライアントに割り当てることを求めます。

ステップ 4　サーバは、NIC から特定の IP アドレスに対する要求が送信されたことを確認する DHCP ACK を戻します。

ステップ 5　クライアント インターフェイスが、DHCP サーバから最初に提供された IP アドレスを割り当てるかまたはバインドします。

DHCP サーバとして専用マシンを使用、企業内有線ネットワークに接続してください。また、DHCP サーバとしてワイヤレスゲートウェイおよび有線ゲートウェイを使用することもできます。その他のワイヤレス デバイスでは、DHCP サービスが無害な状態で実行される場合と、WLAN IP サービスを妨害する目的で悪意を持って実行される場合があります。ワイヤレス クライアントにはサーバを認証する機能がないため、DHCP サーバの IP アドレスを要求するワイヤレス クライアントは、このような疑似 DHCP サーバに接続してこの疑似サーバの IP アドレスを取得する可能性があります。このような疑似 DHCP サーバはクライアントに対して機能しないネットワーク設定が提供するか、またはすべてのクライアント トラフィックを疑似サーバ経由にすることがあります。これで、ハッカーはクライアントから送信されるすべてのパケットを盗聴できます。ハッカーは不正な DNS サーバを利用して偽の Web ページ ログインにユーザを誘導し、ユーザ名とパスワードの資格情報を取得しようとします。DoS 攻撃のために機能しないルーティング不可能な IP アドレスを提供することもあります。通常、このような攻撃は暗号化されていない WLAN（ホットスポットやトレードショー ネットワークなど）が対象となります。

wIPS による解決

Cisco Adaptive Wireless IPS は、DHCP サービスを実行し、気づいていないユーザに IP アドレスを提供するワイヤレス STA を検出します。

クライアントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、デバイスを検出します。

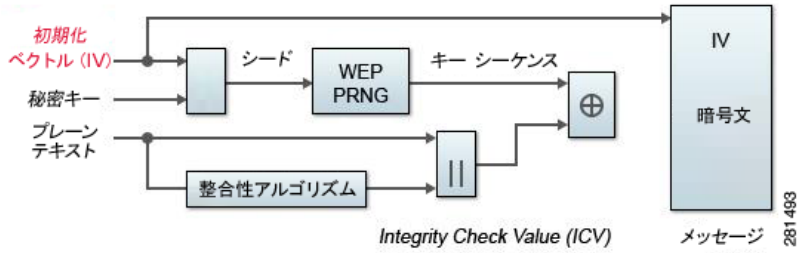
高速 WEP クラック ツールの検出

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは WEP キー クラッキング攻撃に対して脆弱であることがよく知られています（『*Weaknesses in the Key Scheduling Algorithm of RC4 - I*』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照）。

攻撃者によって WEP 秘密キーがクラックされると、暗号化による保護がなくなり、結果としてデータ プライバシーが侵害されます（図 18-22 を参照）。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーで構成され、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。送信ステーションが決定する IV を頻繁に再利用したり、連続するフレームで再利用したりできるので、ワイヤレス侵入者がこの秘密キーを復元できる可能性が高まります。

図 18-22　　WEP 暗号化のブロック図



WEP キーに対する攻撃で最も重要な点は、キーのサイズです。十分な固有 IV の数は、64 ビット WEP キーで約 15 万、128 ビット WEP キーで約 50 万から 100 万です。トラフィックが不十分な場合に、ハッカーはこのような攻撃を行うために十分なトラフィックを生成する手法を編み出しています。これは、arp-request パケットに基づくリプレイ アタックと呼ばれます。このようなパケットの長さは一定であるため、容易に検出できます。1 つの正規 arp-request パケットをキャプチャして繰り返し再送信すると、他のホストは暗号化された応答で対応し、新しい（そして弱い場合もある）IV を提供します。

wIPS による解決

Cisco Adaptive Wireless IPS は弱い WEP 実装について警告し、IV 使用の問題を訂正するためのデバイス ファームウェア アップグレードがデバイス ベンダーからリリースされている場合はこのアップグレードを推奨します。企業 WLAN ネットワークで TKIP（Temporal Key Integrity Protocol）暗号化メカニズムを使用して WEP の脆弱性を保護することが理想的です。TKIP はほとんどのエンタープライズ レベル ワイヤレス装置でサポートされています。TKIP 対応デバイスはこのような WEP キー攻撃の対象となりません。

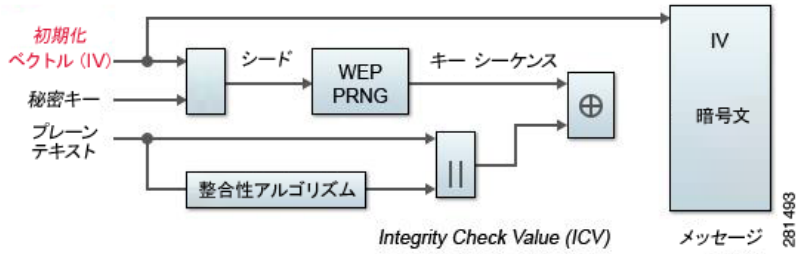
Prime Infrastructure からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、弱い暗号化または認証を使用するように設定されているアクセス ポイントを事前予防的に報告します。自動セキュリティ脆弱性スキャン機能の詳細については、Cisco Prime Infrastructure オンライン ヘルプを参照してください。

フラグメンテーション攻撃

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは、さまざまな WEP クラッキング攻撃の対象となるリスクがあることはよく知られています（図 18-23 を参照）。詳しくは、『*Weaknesses in the Key Scheduling Algorithm of RC4 - I*』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照してください。

図 18-23　　WEP 暗号化プロセスのブロック図



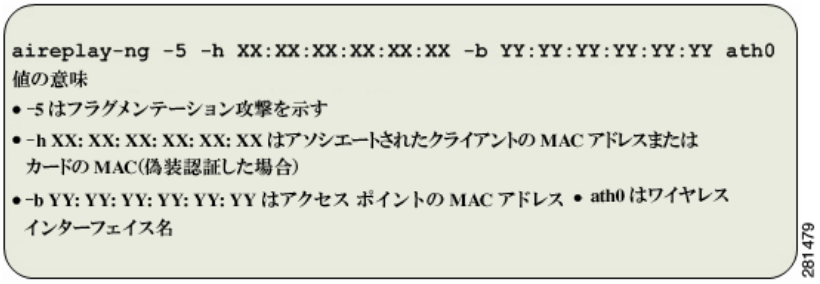
クラックされた WEP 秘密キーでは送信データは暗号化保護されず、データ プライバシーが侵害されます。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーであり、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。

http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation によれば、aircrack プログラムはパケットからわずかな量のキー関連情報を収集し、ARP パケットまたは LLC パケット（あるいはこの両方）を判明している情報と共にアクセス ポイントに送信します。パケットがアクセス ポイントから正常にエコーバックされると、戻されるパケットからより多くのキー関連情報を取得できます。PRGA の 1500 バイト（場合によっては 1500 バイト未満）分を取得するまで、このサイクルが繰り返されます。

この攻撃では WEP キー自体は復元されず、PRGA が取得されるだけです。「packetforge-ng」によってさまざまなインジェクション攻撃に使用できるパケットを生成するときにこの PRGA を使用できます。

Cisco Adaptive Wireless IPS は、Wi-FI ネットワークに対して進行中のフラグメンテーション攻撃を検出します（図 18-24 を参照）。

図 18-24　フラグメンテーション攻撃を実行するコマンド



wIPS による解決

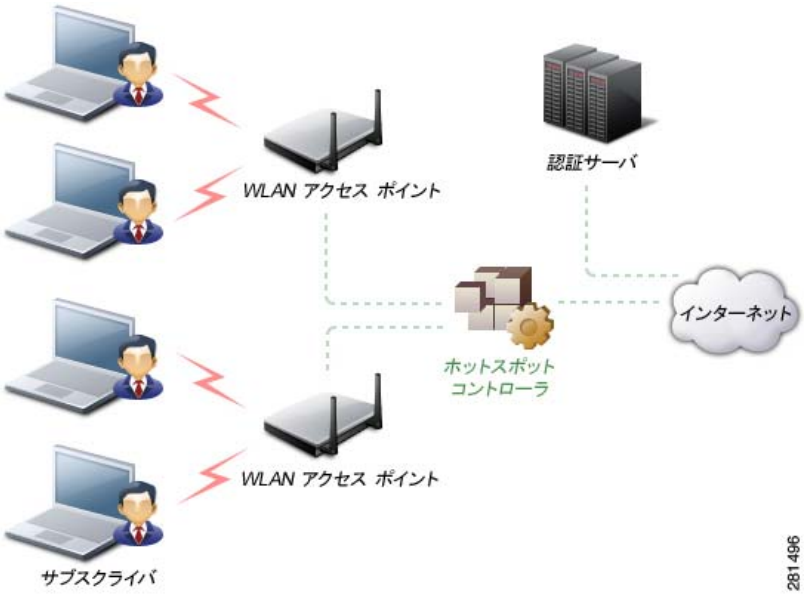
Cisco Adaptive Wireless IPS は、進行中のフラグメンテーション攻撃の可能性を検出すると警告を出します。また、企業環境で WEP を使用せず、ネットワークのセキュリティ ホールを回避するための処置を講じ、ワイヤレス ネットワーク インフラストラクチャとデバイスをアップグレードしてより安全な IEEE 802.11i 標準を使用することを推奨します。

Hot-Spotter ツール検出

アラームの説明と考えられる原因

ホットスポットとは、Wi-Fi ネットワーク アクセスが一般向けに開放されている場所を指します。ホットスポットは空港、ホテル、喫茶店をはじめ、ビジネスマンが集まることが多い場所にあります。現在、ホットスポットは出張旅行者にとっては最も重要なネットワーク アクセス サービスです。正規のアクセス ポイントに接続してサービスを利用するには、ワイヤレス対応ラップトップまたは携帯機器が必要です。ほとんどのホットスポットでは、ユーザがアクセス ポイントに接続するときには、ログイン用の Web ページを開く操作以外の高度な認証メカニズムは不要です。ログインできるかどうかの条件は、利用者が利用料金を支払っているかどうかだけです。ワイヤレス ホットスポット環境では誰も信用すべきではありません。現在のセキュリティ上の懸念から、一部の WLAN ホットスポット ベンダーはユーザ ID の検証に 802.1x 以上の認証メカニズムを採用しています（図 18-25 を参照）。

図 18-25　WLAN ホットスポット ネットワークの基本コンポーネント



ホットスポット ネットワークの 4 つの基本コンポーネントを次に示します。

- ホットスポット利用ユーザ：ワイヤレス対応のラップトップまたは携帯機器を所持し、ホットスポット ネットワークにアクセスするための有効なログイン情報を持つユーザ。
- WLAN アクセス ポイント：ホットスポット実装に応じて、SOHO ゲートウェイまたはエンタープライズ レベル アクセス ポイントのいずれかです。
- ホットスポット コントローラ：ユーザ認証、課金情報の収集、利用時間の追跡、機能のフィルタリングなどを実行します。これは独立したマシンであるか、またはアクセス ポイント自体に組み込まれています。
- 認証サーバ：利用ユーザのログイン資格情報が保管されています。ほとんどの場合、ホットスポット コントローラは認証サーバを使用して利用ユーザの資格情報を検証します。

「Hotspotter」は、採用されている暗号メカニズムに依存せずに、ワイヤレス クライアントに対する侵入操作を自動化します。攻撃者は Hotspotter ツールを使用してワイヤレス ネットワークでプローブ要求フレームを受動的にモニタし、Windows XP クライアント ネットワークの SSID を特定します。

攻撃者は優先ネットワーク情報を獲得した後に、提供されるよく使用されるホットスポット ネットワーク名のリストに対してネットワーク名（SSID）を照合します。一致するネットワーク名が見つかると、Hotspotter クライアントがアクセス ポイントとして動作します。クライアントはこの状況を知らずにこの疑似アクセス ポイントを認証してアソシエートします。

クライアントがアソシエートされたら、DHCP デーモンやその他のスキャンを新たなターゲットに対して実行するコマンド（スクリプトなど）を実行するように Hotspotter ツールを設定できます。

異なる環境（ホームとオフィスなど）で稼働しているが、Windows XP ワイヤレス接続設定で同じホットスポット SSID を使用するように設定されているクライアントも、この攻撃の影響を受けます。クライアントはその SSID を使用してプローブ要求を送信するため、ツールに対して脆弱になります。

wIPS による解決

Cisco Adaptive Wireless IPS により不正なアクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、または不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

不正 802.11 パケットの検出

アラームの説明と考えられる原因

不正なパケット（不正な非標準 802.11 フレーム）を使用するハッカーは、ワイヤレス デバイスを予期しない方法で動作させることができます。一部のベンダーのワイヤレス NIC のファームウェアは、不正なパケットによってクラッシュすることがあります。

このような脆弱性の例として、NULL プローブ応答フレーム（プローブ応答フレームの SSID が Null）や管理フレームの過大サイズの情報要素などがあります。このような不正なフレームがブロードキャストされると、複数のワイヤレス クライアントがクラッシュすることがあります。

wIPS による解決

Cisco Adaptive Wireless IPS は、一部の NIC のロックアップとクラッシュを引き起こす可能性がある不正なパケットを検出できます。また、攻撃を受けている間にブルースクリーンやロックアップの問題が発生するワイヤレス クライアントでは、WLAN NIC ドライバまたはファームウェアのアップグレードを検討する必要があります。

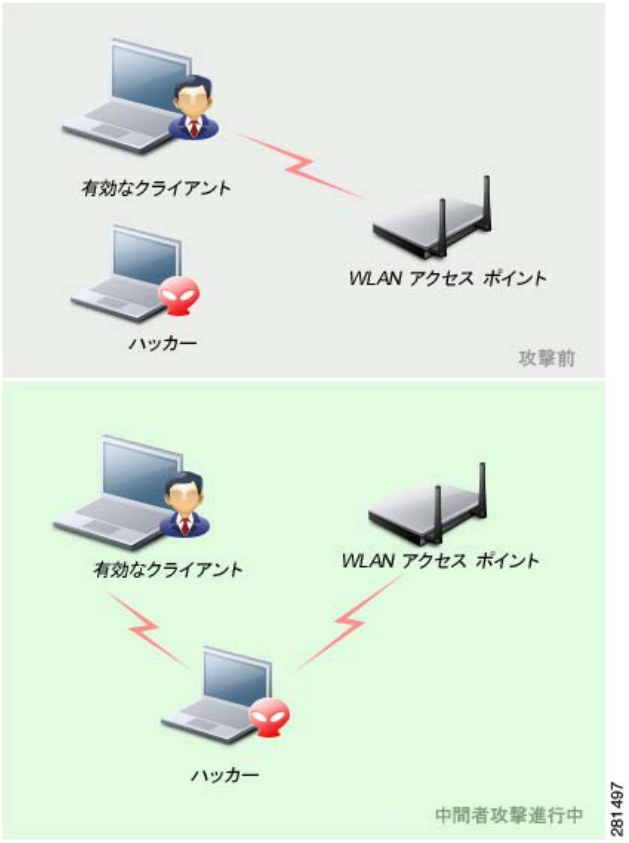
Cisco Adaptive Wireless IPS によりクライアントが特定、報告されると、WLAN 管理者はデバイス ロケータを使用してそのクライアントを見つけることができます。

中間者攻撃

アラームの説明と考えられる原因

中間者（MITM）攻撃は、最も一般的な 802.11 攻撃の 1 つであり、企業の機密情報や個人情報がハッカーに漏れる可能性があります。MITM 攻撃ではハッカーは 802.11 ワイヤレス アナライザを使用し、WLAN 上で送信される 802.11 フレームをモニタします（図 18-26 を参照）。ハッカーはアソシエーション フェーズでワイヤレス フレームをキャプチャし、ワイヤレス クライアント カードとアクセス ポイントの IP アドレスと MAC アドレスの情報、クライアントのアソシエーション ID、ワイヤレス ネットワークの SSID を取得します。

図 18-26　中間者攻撃



一般的な MITM 攻撃では、ハッカーがスプーフされたディスアソシエーション フレームまたは認証解除フレームを送信します。ハッカー ステーションがクライアントの MAC アドレスをスプーフし、アクセス ポイントとのアソシエートを継続します。同時にハッカーはスプーフされたアクセス ポイントを別のチャネルにセットアップし、クライアントとのアソシエーションを維持します。有効なクライアントとアクセス ポイント間のトラフィックはすべてのこのハッカー ステーションを経由します。

最もよく使用される MITM 攻撃ツールの 1 つに Monkey-Jack があります。

wIPS による解決

Cisco Adaptive Wireless IPS は、ハッカーによる MITM 攻撃を阻止するために強力な暗号化および認証メカニズムを使用することを推奨します。このような攻撃を回避する方法の 1 つに、MAC アドレス除外リストを使用し RF チャネル環境をモニタして、MAC アドレスのスプーフを防止する方法があります。

また、Cisco 管理フレーム保護（MFP）は MITM 攻撃に対して完全な予防的保護を提供します。

モニタ対象デバイスの検出

アラームの説明と考えられる原因

場合によっては、アクセス ポイントと STA のアクティビティを継続的にモニタする必要があります。

- 企業の有線ネットワークへのハッキングを試みる悪意のある侵入者をモニタする必要があります。アクセス ポイントと STA を追跡し、不正関連の問題や侵入の問題が繰り返し発生することを防ぐことが重要です。

- 企業のワイヤレス機器を紛失した場合は紛失した機器を見つける必要があります。
- 以前にセキュリティ違反が発生した脆弱なデバイスをモニタする必要があります。
- すべてのワイヤレス装置を返却していない可能性がある元従業員が使用していたデバイスをモニタする必要があります。

次回アクセス ポイントまたは STA が RF 環境に現れた場合にワイヤレス管理者に対して警告できるように、これらのノードはモニタ リストに追加されます。

wIPS による解決

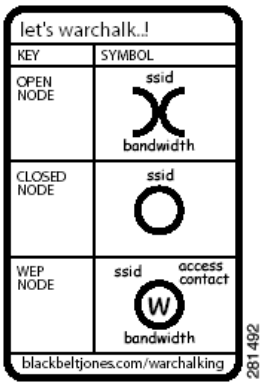
ワイヤレス管理者は、Cisco Adaptive Wireless IPS でアクセス ポイントまたは STA をモニタ対象デバイスとして指定し、これらをモニタ リストに追加します。

NetStumbler の検出

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します（図 18-27 を参照）。ハッカーが新しいバージョンの NetStumbler ツールを使っている場合、「*アクセス ポイントをプローブするデバイス*」アラームが生成されます。古いバージョンの場合、Cisco Adaptive Wireless IPS は「*NetStumbler の検出*」アラームを生成します。

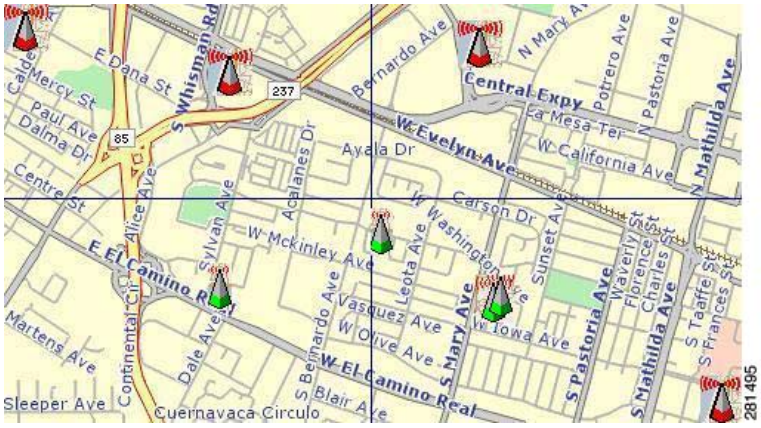
図 18-27　　ウォーチョーキングで使用される共通シンボル



NetStumbler は、ウォードライビングとウォーチョーキングに最も広く使用されているツールです。ワイヤレス ハッカーがウォードライビング ツールを使ってアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティなどの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。NetStumbler Web サイト（http://www.netstumbler.com/）は、ウォーウォーカーが重たいラップトップを持ち歩かずにすむように、Pocket PC ハードウェアで使用できる MiniStumbler ソフトウェアを提供します。このツールは Windows 2000、Windows XP、およびこれ以降のバージョンが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力ア

ンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています（図 18-28 を参照）。

図 18-28　投稿された 802.11 アクセス ポイントの場所



wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

Prime Infrastructure からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、SSID をブロードキャストするように設定されているアクセス ポイントをすべて報告します。自動セキュリティ脆弱性スキャン機能の詳細については、Cisco Prime Infrastructure オンライン ヘルプを参照してください。

NetStumbler 犠牲者の検出

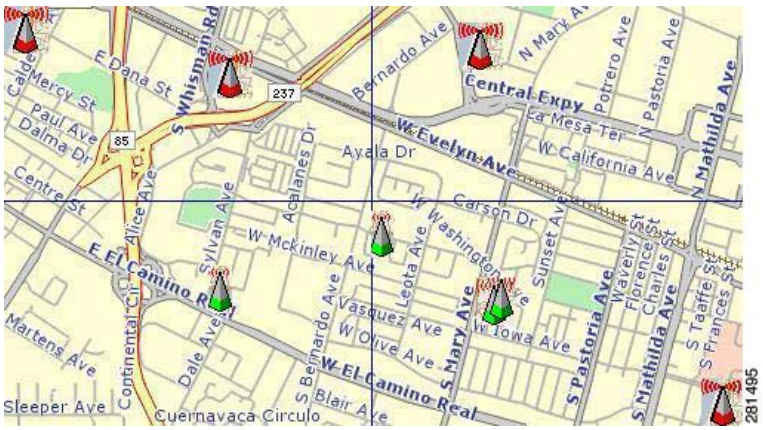
アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。ハッカーが新しいバージョンの NetStumbler ツールを使っている場合、「アクセス ポイントをプローブするデバイス」アラームが生成されます。古いバージョンの場合、Cisco Adaptive Wireless IPS は「NetStumbler の検出」アラームを生成します。

NetStumbler は、ウォードライビング、ウォーウォーキング、ウォーチョーキングに最も広く使用されているツールです。ワイヤレス ハッカーがウォードライビング ツールを使ってアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティなどの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、不正処理をハッカーが車ではなく徒歩で行います。NetStumbler Web サイト（http://www.netstumbler.com/）は、ウォーウォーカーが重たいラップトップを持ち歩かずにすむように、Pocket PC ハードウェアで使用できる MiniStumbler ソフトウェアを提供します。このツールは Windows 2000、Windows XP、およびこれ以降のバージョンが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピング センターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークの

スニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています（図 18-29 を参照）。

図 18-29　投稿された 802.11 アクセス ポイントの場所



Cisco Adaptive Wireless IPS は、NetStumbler を実行するステーションが企業アクセス ポイントにアソシエートされていることを検出すると、ユーザに対して警告を出します。

wIPS による解決

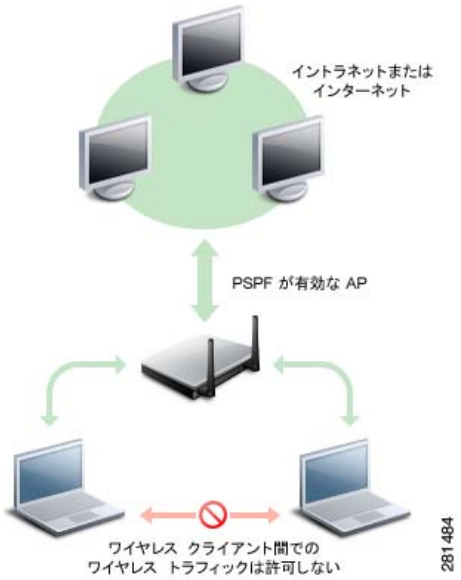
アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

Publicly Secure Packet Forwarding（PSPF）違反の検出

アラームの説明と考えられる原因

PSPF はワイヤレス クライアント同士の通信を無効にする機能であり、WLAN アクセス ポイントに実装されています。PSPF が有効になっている場合、ワイヤレス ネットワーク上のクライアント デバイス同士は通信できません（図 18-30 を参照）。

図 18-30　PSPF



ほとんどの WLAN 環境では、ワイヤレス クライアントは有線ネットワーク上の Web サーバなどのデバイスとだけ通信します。PSPF を有効にすると、ワイヤレス クライアントをワイヤレス侵入者によるハッキングから保護できます。PSPF は特に、空港、ホテル、喫茶店、大学構内など、認証がなく誰もがアクセス ポイントにアソシエートできるワイヤレス パブリック ネットワーク（ホットスポット）でワイヤレス クライアントを保護する場合に効果的です。PSPF 機能により、クライアント デバイスが誤ってワイヤレス ネットワーク上の他のクライアント デバイスとファイルを共有することが防止されます。

wIPS による解決

Cisco Adaptive Wireless IPS は PSPF 違反を検出します。ワイヤレス クライアントが別のワイヤレス クライアントと通信しようとすると、Cisco Adaptive Wireless IPS は侵入攻撃の可能性に関するアラームを生成します。WLAN にワイヤレス プリンタまたは VoWLAN アプリケーションを導入している場合、このようなアプリケーションはクライアント間ワイヤレス通信を利用するため、このアラームは適用されません。

ASLEAP ツール検出

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは、WEP キー クラッキング攻撃に対して脆弱です（詳細については『*Weaknesses in the Key Scheduling Algorithm of RC4-I*』（Scott Fluhrer、Itsik Mantin、Adi Shamir 著）を参照）。

シスコは、既存の 802.1x フレームワークを利用して WEP キー攻撃を回避する LEAP（Lightweight Extensible Authentication Protocol）を導入しました。Cisco LEAP ソリューションには、セッションごとまたはユーザ キーに基づいて動的な相互認証と設定可能な WEP セッション キー タイムアウトが含まれています。LEAP ソリューションは安定したセキュリティ ソリューションとして見なされており、容易に設定できます。

LEAP を実行するワイヤレス LAN ネットワークを侵害するためオフライン辞書攻撃で LEAP パスワードを解読するハッキング ツールがあります。このツールは LEAP を採用している WLAN ネットワークを検出すると、ユーザを認証解除します。これによりユーザは再接続しなければならないため、ユーザ名とパスワードのクレデンシャルを入力します。ハッカーはネットワークへ再アクセスする正規ユーザのパケットをキャプチャします。その後攻撃者はトラフィックをオフラインで解析し、辞書の値をテストしてパスワードを推測できます。

ASLEAP ツールの主な機能を以下に示します。

- libpcap を使用して RFMON モードでワイヤレス インターフェイスからリアルタイムに読み取る。
- 1 つのチャネルをモニタするか、またはチャネル ホッピングを実行して LEAP を実行しているターゲット ネットワークを探す。
- LEAP ネットワークのユーザをアクティブに認証解除し、ユーザに再認証を実行させる。これにより LEAP パスワードを迅速にキャプチャできます。
- LEAP を実行していないユーザではなく、まだ確認されていないユーザのみを認証解除する。
- 保存されている libpcap ファイルを読み取る。
- ダイナミック データベース テーブルと索引を使用して大きなファイルを迅速に検索できるようにする。これにより、フラット ファイルの検索とは対照的に、最悪検索時間が .0015 % 短くなります。
- LEAP 交換情報のみを libpcap ファイルに書き込む。

これは、ディスク スペースが少ないデバイス（iPaq など）で LEAP クレデンシャルをキャプチャするときに使用できます。キャプチャされた LEAP クレデンシャルは、辞書攻撃を実行するためにそのデバイスよりもストレージ リソースが多いシステムの libpcap ファイルに保存されます。

このツールのソースと Win32 バイナリ ディストリビューションは http://asleap.sourceforge.net から入手できます。

シスコは、辞書攻撃を阻止する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）プロトコルを開発しました。EAP-FAST は中間者攻撃、辞書攻撃、パケットおよび認証偽造攻撃を阻止します。EAP-FAST では、クライアントとサーバ間に PAC（Protected Access Credential）を使用して相互認証するトンネルが作成されます。トンネル確立プロセスが完了したら、クライアントはユーザ名とパスワードのクレデンシャルを使用して認証されます。

EAP-FAST の特長を以下に示します。

- 独自のプロトコルではない。
- IEEE 802.11i 標準に準拠している。
- TKIP と WPA に対応している。
- 証明書を使用しないため複雑な PKI インフラストラクチャを回避する。
- PC および Pocket PC の複数のオペレーティング システムに対応している。

wIPS による解決

Cisco Adaptive Wireless IPS は ASLEAP ツールの認証解除シグニチャを検出します。シグニチャを検出すると、サーバはワイヤレス管理者に警告します。攻撃を受けたステーションのユーザはパスワードをリセットする必要があります。最良の ASLEAP ツール対処策は、企業 WLAN 環境で LEAP を EAP-FAST に置き換える方法です。

Prime Infrastructure からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、弱い暗号化または認証を使用するように設定されているアクセス ポイントを事前予防的に報告します。自動セキュリティ脆弱性スキャン機能の詳細については、Cisco Prime Infrastructure オンライン ヘルプを参照してください。

ハニーポット AP の検出

アラームの説明と考えられる原因

企業環境に WLAN を追加すると、ネットワーク セキュリティに対するまったく新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無許可のユーザに公開する可能性があります。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正アクセス ポイントの脅威以外にも、アクセス ポイントの設定ミスや未設定、DoS（サービス拒否）攻撃といったさまざまなワイヤレス セキュリティ リスクや侵入の可能性が存在します。

企業のワイヤレス ネットワークを対象とする最も効果的な攻撃の 1 つに、「ハニー ポット」アクセス ポイントを使用した攻撃があります。攻撃者は NetStumbler、Wellenreiter、MiniStumbler などのツールを使い、企業アクセス ポイントの SSID を検出します。次に建物の外（可能な場合は同じ建物の中）にアクセス ポイントをセットアップし、検出した企業 SSID をブロードキャストします。何も知らないクライアントが、信号強度が高いこの「ハニー ポット」アクセス ポイントに接続します。アソシエートが完了すると、トラフィックが「ハニー ポット」アクセス ポイントを経由するため、攻撃者はクライアント ステーションに対して攻撃を実行します。

wIPS による解決

Cisco Adaptive Wireless IPS により「ハニー ポット」アクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、または不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

ソフト AP またはホスト AP の検出

ホスト AP ツール：Cqure AP

アラームの説明と考えられる原因

ホストベースのアクセス ポイント（ワイヤレス アクセス スポットとして機能するデスクトップまたはラップトップ コンピュータ）は、企業のセキュリティに対する 2 つの脅威をもたらします。1 つ目の脅威は、ホストベース アクセス ポイントは一般に企業ワイヤレス インフラストラクチャに組み込まれておらず、企業のセキュリティ ポリシーに準拠しない不正なデバイスとなる可能性があることです。2 つ目の脅威は、ホストベースのアクセス ポイントは、ワイヤレス攻撃者によりさまざまな既知の攻撃（中間者攻撃、ハニーポット アクセス ポイント攻撃、アクセス ポイント偽装攻撃、DoS（サービス拒否）攻撃など）を実行するための便利なプラットフォームとして使用される点です。デスクトップまたはラップトップをアクセス ポイントとして設定するソフトウェア ツールはインターネットから簡単にダウンロードできるため、ホストベースのアクセス ポイントは単なる理論上の脅威の域を超えています。

一部のラップトップは、ホスト AP ソフトウェアがプリロードおよびアクティブにされた状態で出荷されます。このようなラップトップが企業ワイヤレス ネットワークに接続すると、ワイヤレス ネットワークがハッカーからの攻撃の危険性にさらされることになります。

wIPS による解決

Cisco Adaptive Wireless IPS はこれまで、ソフト アクセス ポイントを不正アクセス ポイントおよび侵入試行の可能性として検出していました。Cisco Adaptive Wireless IPS によりソフト アクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、または不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

スプーフされた MAC アドレスの検出

スプーフィング ツールの一例：SMAC、macchanger、SirMACsAlot。

アラームの説明と考えられる原因

ワイヤレス攻撃者は、入手可能なさまざまな攻撃ツールを使ってワイヤレス ネットワークを妨害します。このようなツールの多くは、インターネットから無料でダウンロードできます。ほとんどのツールはスプーフされた MAC アドレスを利用します。スプーフされた MAC アドレスは、許可されたワイヤレス アクセス ポイントまたは許可されたクライアントとして動作します。攻撃者はこのようなツールを使ってさまざまな DoS（サービス拒否）攻撃を実行し、アクセス制御メカニズムを迂回し、ワイヤレス クライアントにサービスを不正にアドバタイズします。

wIPS による解決

Cisco Adaptive Wireless IPS はスプーフされた MAC アドレスを検出するため、IEEE 許可 OUI（ベンダー ID）と 802.11 フレーム シーケンス番号シグニチャを追跡します。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』を参照してください。

疑わしい営業時間外のトラフィックの検出

アラームの説明と考えられる原因

ワイヤレス セキュリティ突破試行を検出する方法の 1 つに、ワイヤレス トラフィックが発生することにはなっていない時間とワイヤレス利用状況を照合する方法があります。wIPS サーバはこのアラームで設定された営業時間を基準にしてトラフィック パターンをモニタし、異常が検出されるとアラートを生成します。営業時間外に wIPS サーバにより追跡される疑わしいワイヤレス利用には、次のものがあります。

- セキュリティ侵害を示す可能性があるオフィス WLAN への認証要求またはアソシエート要求を発行するクライアント ステーション。
- ワイヤレス ネットワーク上での疑わしいダウンロードまたはアップロードを示す可能性があるワイヤレス データ トラフィック。

wIPS による解決

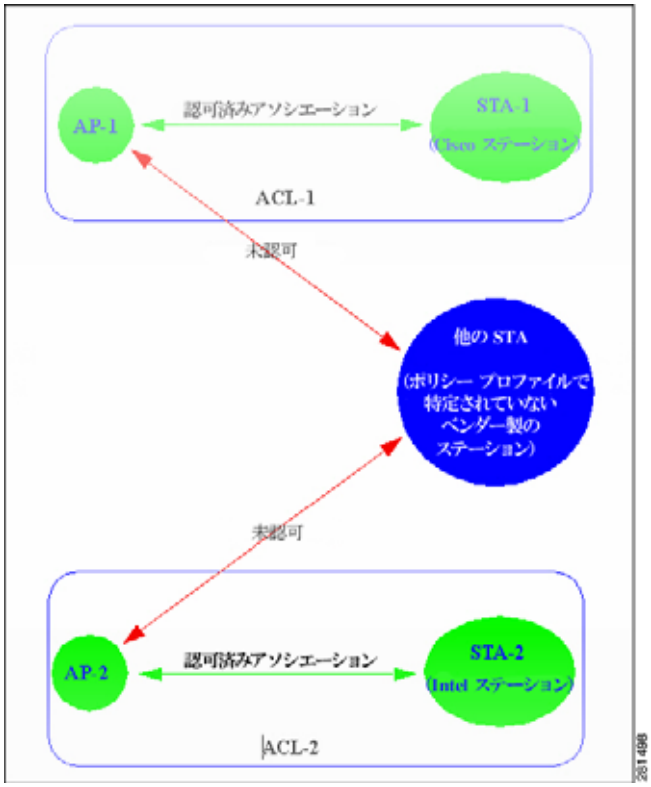
wIPS をグローバルに導入する場合、設定可能な営業時間範囲は現地時間で定義されます。管理を容易にするため、アクセス ポイントまたはセンサーを特定の時間帯に基づいて設定できます。オフィスと製造現場が混在する WLAN では、オフィスの WLAN SSID にオフィスの営業時間を定義し、製造現場の WLAN SSID に別の営業時間を定義できます。アラームが生成されたら、管理者は疑わしいトラフィックに関与するデバイスを特定してワイヤレス環境から削除してください。

ベンダー リストによる未承認アソシエーション

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS では、ネットワーク管理者がベンダー情報をポリシー プロファイルに組み込むことができます。これにより、WLAN 上にある承認ベンダー以外のステーションを検出できます。このようなポリシー プロファイルを作成すると、未承認ベンダーによりステーションとアクセス ポイントがアソシエートされると常にアラームが生成されます（図 18-31 を参照）。

図 18-31　ステーション ベンダーによりフィルタリングされる未承認アクセス ポイントとステーションのアソシエーション



この図の ACL-1 のアクセス ポイントはシスコ製のステーションとだけアソシエート可能であり、ACL-2 のアクセス ポイントは Intel 製のステーションとだけアソシエート可能です。この情報は wIPS システム ポリシー プロファイルに入力されます。アクセス ポイントとシスコおよび Intel 以外のベンダーのステーションとのアソシエーションはすべて承認されず、アラームが生成されます。

企業 WLAN 環境では、不正なステーションが原因でセキュリティの問題が発生し、ネットワーク パフォーマンスが低下します。このような不正なステーションは空間を占有し、ネットワーク帯域幅をめぐって競合します。アクセス ポイントが対応できるステーションの数が限られているため、アクセス ポイントは対応するステーションの数が上限に達すると、ステーションからのアソシエート要求を拒否します。多数の不正なステーションに対応しており、これ以上のステーションに対応できないアクセス ポイントは、ネットワークにアクセスする正規のステーションを拒否します。不正なステーションによってよく引き起こされる問題には、接続の問題やパフォーマンス低下があります。

wIPS による解決

Cisco Adaptive Wireless IPS は、アクセス ポイントとステーション間で非準拠ステーションが関与する未承認アソシエーションについて、このアラームを使用してネットワーク管理者に警告します。このアラームが生成されたら、未承認ステーションを特定し、この問題を解決するための措置をとる必要があります。この措置の 1 つに、不正の封じ込め処理を使用してブロックする方法があります。

未承認アソシエーションの検出

アラームの説明と考えられる原因

通常、企業ネットワーク環境では従業員が導入した不正なアクセス ポイントはネットワーク標準導入プラクティスに従っておらず、ネットワークの整合性を侵害します。このような不正なアクセス ポイントはネットワーク セキュリティの抜け穴であり、侵入者はこのアクセス ポイントからが企業の有線ネットワークに容易にハッキングできるようになります。多くのワイヤレス ネットワーク管理者が抱える主な課題の 1 つに、ACL に登録されているステーションと不正なアクセス ポイントの間の未承認アソシエーションがあります。ステーションと不正なアクセス ポイントの間でデータが転送されるため、ハッカーが機密情報を盗み出すことが可能になります。

不正なステーションはセキュリティの問題を引き起こし、ネットワーク パフォーマンスを低下させます。このような不正なステーションは空間を占有し、ネットワーク帯域幅をめぐって競合します。アクセス ポイントが対応できるステーションの数が限られているため、アクセス ポイントは対応するステーションの数が上限に達すると、ステーションからのアソシエート要求を拒否します。多数の不正なステーションに対応しており、これ以上のステーションに対応できないアクセス ポイントは、ネットワークにアクセスする正規のステーションを拒否します。不正なステーションによってよく引き起こされる問題には、接続の妨害やパフォーマンス低下があります。

wIPS による解決

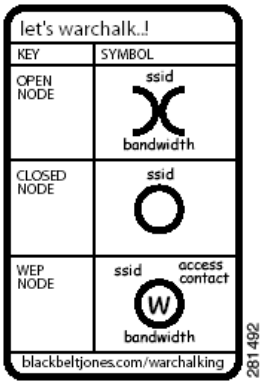
アクセス ポイントとステーション間の未承認アソシエーションがネットワーク上で検出されると、Cisco Adaptive Wireless IPS はネットワーク管理者に対してこのアラームで通知します。このアラームが生成されたら、不正なデバイスまたは許可されていないデバイスを特定し、報告された問題を解決するための措置をとる必要があります。

Wellenreiter の検出

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、Wellenreiter ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します（図 18-32 を参照）。

図 18-32　ウォーチョーキングで使用される共通シンボル



Wellenreiter は、ウォードライビングとウォーチョーキングによく利用されるツールです。ワイヤレス ハッカーがウォードライビング ツールを使ってアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティなどの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。ウォーウォーカーは、Wellenreiter や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています（図 18-33 を参照）。

図 18-33　投稿された 802.11 アクセス ポイントの場所

このツールは、Prism2、Lucent、および Cisco ベースのカードに対応しています。このツールは SSID と WEP 機能をブロードキャストしているインフラストラクチャとアドホック ネットワークを検出し、ベンダー情報を自動的に提供することができます。また、ethereal/tcpdump 互換ダンプ ファイルとアプリケーション savefile を作成します。GPS にも対応しています。ユーザは http://www.wellenreiter.net/index.html からこのツールをダウンロードできます。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

Prime Infrastructure からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、SSID をブロードキャストするように設定されているアクセス ポイントをすべて報告します。自動セキュリティ脆弱性スキャン機能の詳細については、Prime Infrastructure オンライン ヘルプを参照してください。

-

トラブルシューティングおよびベスト プラクティス

この付録では、特定の機能を実装する際に必要となる可能性のあるその他のトラブルシューティングとベスト プラクティスを示し、説明します。

この付録の内容は、次のとおりです。

Cisco Compatible Extensions バージョン 5 クライアント デバイスのトラブルシューティング

Cisco Compatible Extension クライアントとの通信の問題をトラブルシューティングするために、診断チャネルとクライアント レポーティングの 2 つの機能が設計されています。

（注） これらの機能は、Cisco Compatible Extensions バージョン 5 クライアント デバイスだけでサポートされています。Cisco Compatible Extensions バージョン 5 クライアント デバイス以外での使用、および以前のバージョンが稼働しているクライアントでの使用はサポートされていません。

診断チャネル

診断チャネル機能により、WLAN とのクライアント通信に関する問題のトラブルシューティングが可能になります。困難を抱えたクライアントによって起動する場合も診断チャネルは WLAN です。したがって、クライアントのパスに置かれた通信への障害物が最も少なく、最も堅牢な通信方法が提供されるように設定されます。クライアントが経験した通信の困難の原因を特定する試行において、定義済みの一連のテストをクライアントとアクセス ポイントに受けさせることができます。

（注）　コントローラごとに 1 つの WLAN しか診断チャネルを有効にできず、この WLAN のセキュリティはすべて無効となります。

診断チャネルの設定

診断チャネルを設定する手順は、次のとおりです。

ステップ 1　[Configure] > [Controllers] の順に選択します。

ステップ 2　IP アドレスをクリックして、特定のコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、[WLANs] > [WLAN Configuration] の順に選択します。

ステップ 4　[Select a command] ドロップダウン リストから [Add a WLAN] を選択して新しいプロファイルを作成するか、既存のプロファイル名をクリックします。

（注）　診断テストを実行するための新しい WLAN を作成することを推奨します。

ステップ 5　[WLANs] ページが表示されたら、[Advanced] タブをクリックします。

ステップ 6　この WLAN 上で診断チャネルでのトラブルシューティングを有効にする場合は、[Diagnostic Channel] チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします（デフォルト値）。

ステップ 7　[Save] をクリックして変更をコミットします。

WLAN 上の Web 認証セキュリティ

この項では、WLAN に Web 認証セキュリティを実装する場合に役立つトラブルシューティングとベスト プラクティスの手順を説明します。

Web 認証は、WLAN 上のユーザへの Web ベースの認証を可能にするレイヤ 3 のセキュリティ機能です。主にゲスト ネットワークのシナリオで使用されますが、これに限定されるわけではありません。

WLAN が Web 認証セキュリティで設定されると、レイヤ 2 認証（静的 WEP、WPA+PSK、MAC フィルタリングなど）の通過後にログイン ページにリダイレクトされます。ログイン ページは、ローカル デバイスまたは外部 Web サーバに格納され、ロゴ、タイトルなどのカスタマイズが許可されるように変更できます。

WLAN が Web 認証 WLAN で設定された後は、要求された Web サイトに、無線クライアントによって HTTP *get* request が送信されます。コントローラ ファイアウォールによって、指定された URL の DNS 名前解決が許可されます。名前解決後に、コントローラが無線クライアントからの HTTP パケッ

トに割り込んで、ログイン ページにリダイレクトします。クレデンシャルがログイン ページに入力および送信されると、ローカル データベースに対して認証されます。ユーザがローカル データベースで検出されない場合、設定された RADIUS サーバに接触します。

（注）　クライアントと認証エージェント間には、PAP および CHAP 認証が使用されます。RADIUS サーバがこれらのプロトコルをいずれもサポートしていて、Web 認証が許されていることを確認してください。

認証が成功すると、トラフィックを通過させることができます。認証の試行が 3 回失敗すると、クライアントは除外されます。除外されたクライアントは、除外タイムアウト制限を超えるまでアソシエートできません。除外タイムアウト制限は、アグレッシブ ロード バランシングで設定されます。アグレッシブ ロード バランシングは、モバイル クライアントとアソシエートされたアクセス ポイントの間で負荷をアクティブに分散させます。

Web 認証 WLAN は、事前認証の Access Control List（ACL;アクセス コントロール リスト）が設定されることもあります。この ACL は通常の ACL 同様に設定されますが、クライアントが認証に先立って必要とするリソースへのアクセスを許可します。管理者は、インターフェイス セクションを使用して認証後に ACL をクライアントに適用する必要があります。

Web 認証 WLAN は、セッションのタイムアウト値も設定できます。この値によって、クライアントが再度デバイスの認証を行うのに必要な時間が定義されます。値が 0 に設定される場合、これは無限を意味するので、クライアントはログアウト オプションが使用されるまで再度認証されることはありません。http://<VirtualIP>/logout.html でログアウト URL にアクセスできます。

（注）　ログアウト ページを表示するには、クライアント上のポップアップ ブロッカーをすべてオフにします。

Web 認証は、レイヤ 3 セキュリティ下の異なるモードに設定することができます。最も一般的に使用される Web 認証のモードは、次のとおりです。

- Internal Web：http://<virtual IP /DNS name >/login.html を使用した、内部ページへのリダイレクション。カスタマイズ可能です。
- External Web：外部 URL へのリダイレクション。

debug コマンド

次のデバッグ コマンドが使用できます。

```
debug client <client-mac-address>
debug pm ssh-tcp enable
debug pm ssh-appgw enable
debug pm rules enable
debug pm config enable

show client detail <client-mac-address>
debug pem event enable
```

デバッグ戦略

ゲスト トンネリングなしで WLAN に設定された Web 認証に対して、次の戦略を使用します。

ステップ 1　無線 MAC アドレスを使用し書き込むモバイル クライアントを特定します。MS Windows ベースのすべてのシステムでコマンド **prompt > ipconfig /all** を使用します。

ステップ 2　モバイル クライアントの無線を無効にします。

ステップ 3　高速（115200）用シリアル コンソール セットまたはコントローラの管理ポートへの SSH セッション経由で次のデバッグ コマンドを入力にします。

```
debug client <client-mac-address>
debug pm ssh-tcp enable
debug pm ssh-appgw enable
debug pm rules enable
debug pm config enable

show client detail <client-mac-address>

debug pem event enable
debug pem state enable
```

ステップ 4　無線を有効にし、クライアントをアソシエートさせます。クライアントがアソシエートされてから、**show client detail** *client-mac-address* コマンドを入力します。

```
$Router1> show client detail 00:0b:85:09:96:10
Client Username ..............................  N/A
AP MAC Address................................  00:0b:85:09:96:10
Client State..................................  Associated
Wireless LAN Id...............................  1
BSSID.........................................  00:0b:85:09:96:1f
Channel.......................................  11
IP Address....................................  10.50.234.3
Association Id................................  1
Authentication Algorithm......................  Open System
Reason Code...................................  0
Status Code...................................  0
Session Timeout...............................  0
Client CCX version............................  3
Mirroring.....................................  Disabled
QoS Level.....................................  Silver
Diff Serv Code Point (DSCP)...................  disabled
802.1P Priority Tag...........................  disabled
WMM Support...................................  Disabled
Mobility State................................  Local
Internal Mobility State.......................  apfMsMmInitial
Mobility Move Count...........................  0
--More-- or (q)uit
Security Policy Completed.....................  No
Policy Manager State..........................  WEBAUTH_REQD ========**
Policy Manager Rule Created...................  Yes
NPU Fast Fast Notified........................  Yes
Last Policy Manager State.....................  WEBAUTH_REQD
Client Entry Create Time......................  67733 seconds
Policy Type...................................  N/A
Encryption Cipher.............................  None
Management Frame Protection...................  No
EAP Type......................................  Unknown
Interface.....................................  management
VLAN..........................................  0
Client Capabilities:
      CF Pollable.............................  Not implemented
      CF Poll Request.........................  Not implemented
      Short Preamble..........................  Implemented
      PBCC....................................  Not implemented
      Channel Agility.........................  Not implemented
```

```
      Listen Interval..... 0
Client Statistics:
      Number of Bytes Received..... 188595
      Number of Bytes Sent..... 19229
      Number of Packets Received..... 3074
--More-- or (q)uit
      Number of Packets Sent..... 76
      Number of Policy Errors..... 0
      Radio Signal Strength Indicator..... -41 dBm
      Signal to Noise Ratio..... 59 dB
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      ap:09:96:10(slot 1) .....
antenna0: 48 seconds ago -45 dBm..... antenna1: 123 seconds ago -128 dBm
```

ステップ 5　クライアントの PEM 状態が WEBAUTH_REQD であることを確認します。クライアントのブラウザ ページを開いて、次のメッセージを探します。

```
Wed Mar  7 17:59:15 2007: ************* sshpmAddWebRedirectRules: POLICY SEMAPHORE LOCKED
*************
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: mobile station addr is 10.50.234.3
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: RuleID for ms 10.50.234.3 is 44
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: using HTTP-S for web auth (addr:
10.50.234.15).
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: inbound local http rule created for ms
10.50.234.3 local 1.1.1.1.
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: inbound http redirect rule created.
Wed Mar  7 17:59:15 2007: sshpmRuleIndexInsert: adding rule for RuleID 44
Wed Mar  7 17:59:15 2007: sshpmRuleIndexInsert: computed raw hash index 02ad3271 for rule
id 0000002c
Wed Mar  7 17:59:15 2007: sshpmRuleIndexInsert: computed adjusted index 00000c32 for rule
id 0000002c
Wed Mar  7 17:59:15 2007: sshpmAddWebRedirectRules: committing rules for ms 10.50.234.3
Wed Mar  7 17:59:15 2007: ************* sshpmPolicyCommitCallback: POLICY SEMAPHORE
UNLOCKED - [unconditionally] ************
Wed Mar  7 17:59:15 2007: sshpmPolicyCommitCallback: called; ContextPtr: 0x2c; Success: 1
Wed Mar  7 17:59:15 2007: ************* sshpmPolicyCommitCallback: POLICY SEMAPHORE
UNLOCKED - [unconditionally] ************
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1234/ssh_pm_appgw_request: New application
gateway request for `alg-http@ssh.com': 10.50.234.3.1153 > 10.50.234.1.80 (nat:
10.50.234.1.80) tcp ft=0x00000000 tt=0x00000000
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1239/ssh_pm_appgw_request: Packet
attributes: trigger_rule=0x4ecb, tunnel_id=0x0, trd_index=0xdfffffff,
prev_trd_index=0xdfffffff
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:1240/ssh_pm_appgw_request: Packet:
Wed Mar  7 18:02:32 2007: 00000000: 4500 0030 0308 4000 8006 0f57 0a32 ea03
E..0..@....W.2..
Wed Mar  7 18:02:32 2007: 00000010: 0a32 ea01 0481 0050 2f42 e3a4 0000 0000
.2.....P/B......
Wed Mar  7 18:02:32 2007: 00000020: 7002 4000 42fe 0000 0204 05b4 0101 0402
p.@.B...........
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:403/ssh_pm_st_appgw_start: Calling
redirection callback
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:155/ssh_appgw_redirect: Application
gateway redirect: 10.50.234.1.80 -> 10.50.234.1.80
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:445/ssh_pm_st_appgw_mappings:
Creating application gateway mappings: 10.50.234.3.1153 > 10.50.234.1.80 (10.50.234.1.80)
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:102/ssh_pm_appgw_mappings_cb: appgw
connection cached: init flow_index=5967 resp flow_index=5964 event_cnt=718
```

```
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:493/ssh_pm_st_appgw_mappings_done:
NAT on initiator side
Wed Mar  7 18:02:32 2007:
SshPmStAppgw/pm_st_appgw.c:583/ssh_pm_st_appgw_tcp_responder_stream_done:
ssh_pm_st_appgw_tcp_responder_stream_done: conn->context.responder_stream=0x0
Wed Mar  7 18:02:32 2007:
SshPmStAppgw/pm_st_appgw.c:624/ssh_pm_st_appgw_tcp_responder_stream_done: Opening
initiator stream 10.50.234.1:61611 > 10.76.108.121:2024
Wed Mar  7 18:02:32 2007: SshPmStAppgw/pm_st_appgw.c:154/ssh_pm_appgw_i_flow_enabled:
Initiator flow mode has now been set.
Wed Mar  7 18:02:32 2007: SshPmAppgw/pm_appgw.c:507/ssh_appgw_tcp_listener_callback: New
initiator stream: src=10.50.234.1:61611, dst=10.76.108.121:2024
Wed Mar  7 18:02:32 2007:
SshPmStAppgw/pm_st_appgw.c:646/ssh_pm_st_appgw_tcp_open_initiator_stream: Initiator stream
opened
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:531/ssh_appgw_http_conn_cb: New TCP
HTTP connection 10.50.234.3.1153 > 10.50.234.1.80
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:535/ssh_appgw_http_conn_cb: Responder
sees initiator as `10.50.234.15.1153'
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:539/ssh_appgw_http_conn_cb: Initiator
sees responder as `10.50.234.1.80'
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (r) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:132/ssh_appgw_http_st_wait_input:
appgw_http.c.132: io->src is NULL
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:32 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (r) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:32 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:36 2007: SshAppgwHttp/appgw_http.c:132/ssh_appgw_http_st_wait_input:
appgw_http.c.132: io->src is NULL
Wed Mar  7 18:02:36 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
283 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 283
bytes:
Wed Mar  7 18:02:41 2007: 00000000: 4745 5420 2f20 4854 5450 2f31 2e31 0d0a  GET /
HTTP/1.1..
Wed Mar  7 18:02:41 2007: 00000010: 4163 6365 7074 3a20 696d 6167 652f 6769  Accept:
image/gi
Wed Mar  7 18:02:41 2007: 00000020: 662c 2069 6d61 6765 2f78 2d78 6269 746d  f,
image/x-xbitm
```

```
Wed Mar  7 18:02:41 2007: 00000030: 6170 2c20 696d 6167 652f 6a70 6567 2c20  ap,
image/jpeg,
Wed Mar  7 18:02:41 2007: 00000040: 696d 6167 652f 706a 7065 672c 2061 7070  image/pjpeg,
app
Wed Mar  7 18:02:41 2007: 00000050: 6c69 6361 7469 6f6e 2f78 2d73 686f 636b
lication/x-shock
Wed Mar  7 18:02:41 2007: 00000060: 7761 7665 2d66 6c61 7368 2c20 2a2f 2a0d  wave-flash,
*/*.
Wed Mar  7 18:02:41 2007: 00000070: 0a41 6363 6570 742d 4c61 6e67 7561 6765
.Accept-Language
Wed Mar  7 18:02:41 2007: 00000080: 3a20 656e 2d75 730d 0a41 6363 6570 742d  :
en-us..Accept-
Wed Mar  7 18:02:41 2007: 00000090: 456e 636f 6469 6e67 3a20 677a 6970 2c20  Encoding:
gzip,
Wed Mar  7 18:02:41 2007: 000000a0: 6465 666c 6174 650d 0a55 7365 722d 4167
deflate..User-Ag
Wed Mar  7 18:02:41 2007: 000000b0: 656e 743a 204d 6f7a 696c 6c61 2f34 2e30  ent:
Mozilla/4.0
Wed Mar  7 18:02:41 2007: 000000c0: 2028 636f 6d70 6174 6962 6c65 3b20 4d53   (compatible;
MS
Wed Mar  7 18:02:41 2007: 000000d0: 4945 2036 2e30 3b20 5769 6e64 6f77 7320  IE 6.0;
Windows
Wed Mar  7 18:02:41 2007: 000000e0: 4e54 2035 2e31 3b20 5356 3129 0d0a 486f  NT 5.1;
SV1)..Ho
Wed Mar  7 18:02:41 2007: 000000f0: 7374 3a20 3130 2e35 302e 3233 342e 310d  st:
10.50.234.1.
Wed Mar  7 18:02:41 2007: 00000100: 0a43 6f6e 6e65 6374 696f 6e3a 204b 6565  .Connection:
Kee
Wed Mar  7 18:02:41 2007: 00000110: 702d 416c 6976 650d 0a0d 0a              p-Alive....
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:985/ssh_appgw_parse_request_line: parsing request
line GET / HTTP/1.1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1018/ssh_appgw_parse_request_line: internal http
version 3
Wed Mar  7 18:02:41 2007: SshAppgwHttpState/appgw_http_state.c:1155/ssh_appgw_add_method:
caching method 2 for reply 0
Wed Mar  7 18:02:41 2007: SshAppgwHttpState/appgw_http_state.c:1604/ssh_appgw_check_msg:
examining request using service id 34
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:594/ssh_appgw_http_get_dst_host: destination host:
10.50.234.1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1474/ssh_appgw_inject_reply: injecting 404 reply as
msg 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:284/ssh_appgw_http_st_write_data:
entering state st_write_data
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 1
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:136/ssh_appgw_http_st_wait_input: read
-1 bytes (offset 0 data 0)
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (r) reading_hdr 1 nmsgs 0
Wed Mar  7 18:02:41 2007:
SshAppgwHttpState/appgw_http_state.c:1851/ssh_appgw_http_is_inject: next inject is msg# 0
current msg# 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:207/ssh_appgw_http_st_inject: entering
state st_inject (r): msgs 0
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:259/ssh_appgw_http_st_inject: closing
connection after inject
Wed Mar  7 18:02:41 2007: SshAppgwHttp/appgw_http.c:400/ssh_appgw_http_st_terminate:
entering state st_terminate (r): teardown 0 terminate i: 1 r: 1
```

```
Wed Mar  7 18:02:45 2007: SshAppgwHttp/appgw_http.c:99/ssh_appgw_http_st_wait_input:
entering state st_wait_input: (i) reading_hdr 1 nmsgs 1
Wed Mar  7 18:02:45 2007:
SshAppgwHttpState/appgw_http_state.c:2077/ssh_appgw_http_handle_state: handling: 0 bytes:
Wed Mar  7 18:02:45 2007: SshAppgwHttp/appgw_http.c:400/ssh_appgw_http_st_terminate:
entering state st_terminate (i): teardown 0 terminate i: 1 r: 1
Wed Mar  7 18:02:45 2007:
SshAppgwHttp/appgw_http.c:732/ssh_appgw_http_connection_terminate: service HTTP-REDIR: TCP
HTTP connection 10.50.234.3.1153 > 10.50.234.1.80 terminated
Wed Mar  7 18:02:45 2007: SshPmStAppgw/pm_st_appgw.c:1094/ssh_pm_st_appgw_terminate:
terminating appgw instance
```

ステップ 6　HTTP GET メッセージが表示されない場合、HTTP パケットがコントローラに到達していません。クライアントがリダイレクションを完了してから、ログインを入力して送信します。

ステップ 7　NPUdevshell hapiMmcDebugScbInfoShow へのクライアントのエントリ（「クライアント MAC アドレス」）を確認します。PEM 状態が WEBAUTH_REQD to RUN から動かない場合、クレデンシャルの問題が存在します。ローカルまたは RADIUS データベース内（設定場所にかかわらず）のクレデンシャルを確認します。

ステップ 8　クライアントに RUN 状態が表示される場合、クライアントからゲートウェイへの確認を行い、トラフィックが通過中かどうか確認します。

RF ヒートマップ分析

シナリオ：アクセス ポイントの矛盾したヒート マップが一部表示されます。アクセス ポイントの一部が、強いヒート マップを示し、他の部分が弱いヒート マップを示します。

分析：これは、一部の隣接アクセス ポイントの RSSI 値を取得し、その他の隣接アクセス ポイントの RSSI 値を取得していない場合に発生することがあります。厚い壁や有線ハウジングがあることが原因で、ヒート マップが正しくなくなる可能性があるため、一方の RSSI 値のみを使用してヒート マップを予測することは推奨されません。

シナリオ：動的ヒート マップを正しく表示できません。

分析：動的ヒート マップを正しく表示できない場合は、次の点を確認します。

- コントローラと Prime Infrastructure の両方でネイバー AP RSSI 値が同じかどうかを確認します。
- 最新の動的ヒート マップ データにヒート マップが更新されるまで、20 分待ちます。
- AP の位置を確認します。

ベスト プラクティス

クライアントがログイン ページにリダイレクトされず、ネットワーク内の DNS 解決を避ける必要がある場合は、**http://***controller-mgmt-ip* と入力します。リダイレクションが発生する場合、問題はネットワーク関連ではありません。

config network web-auth-port *Port* を入力して、コントローラに標準の HTTP ポート (80) 以外のポートを定義します。コントローラは、ポートが割り込みに設定されていても、セキュア HTTP または HTTPS (443) に割り込みません。

RAID カード設定のトラブルシューティング

シナリオ：

偶発的な停電が原因で、NVRAM（不揮発性 RAM）に保存されていた RAID カード設定に関する情報が破損または消去されました。設定情報が失われると、RAID カードは通常モードで起動できません。ただし、RAID カードはハード ドライブに設定情報をバックアップします。RAID カードは、ハード ドライブに保存されているバックアップ設定を認識しましたが、手作業なしでは、その設定情報をデフォルト設定としてをロードしません。

分析：

システムが起動しようとすると、RAID ファームウェアにより、以前の設定に関する情報が失われ、設定ユーティリティをロードするために C キーを押す必要があることを示すエラー メッセージが返されます。エラー メッセージはシリアル コンソールに表示され、入力なしでは起動は進行しません。

次の手順を実行する必要があります。

ステップ 1　シリアル コンソールで、C キーを押して RAID 管理ツールをロードします。RAID ファームウェアにより、外部設定を使用できることが示されます。外部設定はハード ドライブにバックアップされた RAID カード設定です。ただし、RAID ファームウェアはこの設定情報を自動的にロードしません。

ステップ 2　RAID 管理ツールで、次のコマンドを入力します。

-CfgForeign -Import -a0

ステップ 3　サーバをリブートします。

暗号化アクセス用 Cisco.com アカウントの申請

暗号化イメージをダウンロードするには、暗号化アクセス用の Cisco.com アカウントが必要です。

暗号化アクセスを申請する手順は、次のとおりです。

ステップ 1　Cisco.com アカウントを持っている場合は、ステップ 2 に進みます。Cisco.com アカウントを持っていない場合は、次の URL で登録してください。http://tools.cisco.com/RPF/register/register.do

ステップ 2　次の URL にアクセスします。http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y

[Enter Network Password] ダイアログボックスが表示されます。

ステップ 3　Cisco.com アカウントでログインします。

[Encryption Software Export Distribution Authorization] ページが表示されます。

ステップ 4　リストボックスでソフトウェアを選択して [Submit] をクリックします。

[Encryption Software Export Distribution Authorization] ページが表示されます。

ステップ 5　Encryption Software Export Distribution Authorization Form を検討し、各項目に入力し、[Submit] をクリックします。

「Cisco Encryption Software: Crypto Access Granted」というメッセージが表示されます。

（注）　申請の処理には約 4 時間かかります。この資格付与の処理が完了するまで、ソフトウェアのダウンロードはできません。これに関する通知は送信されません。

ディスクのクリーンアップの実行

Prime Infrastructure のディスク領域が不足していると、アラームがシステムで発生します。また、次のエラーがポップアップ ダイアログボックスに表示されます。

```
The system is running low on diskspace, please refer to online help to perform
disk cleanup.
```

この問題を解決するには、次の CLI コマンドを使用します。

ncs cleanup

このコマンドを使用すると、ディスク領域を解放し、再利用できます。

また、システム ディスクの使用量をモニタすることもできます。詳細については、「システム ディスクの使用量の検査」（P.A-10）を参照してください。

Prime Infrastructure のネットワーク データの収集と保存の管理について詳しくは、次の URL を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/user/guide/ManageData.html

システム ディスクの使用量の検査

[Administration] > [Appliance] ページの [Appliance Status] タブを使用して、システム ディスク領域使用率の合計をすぐに確認できます。

[Administration] > [Appliance] > [Appliance Status] の順に選択します。

[Disk Usage] に、現在のストレージ割り当て、および Prime Infrastructure が使用する各メイン ディスク ボリュームの使用率が表示されます。

Prime Infrastructure のパスワードで使用できない特殊文字

パスワードには、「cisco」、「ocsic」、「admin」、または「nimda」は使用できません。また、これらの単語は、大文字と小文字を変えたり、「i」を「1」、「|」、「!」、「o」を「0」、または「s」を「$」に変えても使用できません。

$、'、\、%、&、(、)、;、"、<、>、,、?、| などの特殊文字は、FTP パスワードの一部として使用できません。@、#、^、*、~、_、-、+、=、{、}、[、]、:、.、および / などの特殊文字をパスワードには使用できます。特殊文字「!」（感嘆符）は、パスワード ポリシーが無効の場合に動作します。

Cisco Prime Infrastructure サーバの強化

この付録では、Prime Infrastructure サーバの強化に関するチェックリストについて説明します。理想的には、サーバの強化の目的は、他の形式の保護を使用せずにサーバをインターネットに公開しておくことです。ここでは、公開する一部のサービスおよびプロセスが正常に機能することが求められる、Prime Infrastructure の強化について説明します。これは Prime Infrastructure のベスト プラクティスとして考えてください。Prime Infrastructure の強化には、不要なサービスの無効化、レジストリ キー エントリの削除と変更、ならびにファイル、サービスおよびエンド ポイントに対する適切な制限的権限の適用などが含まれます。

この付録の内容は、次のとおりです。

Prime Infrastructure のパスワード処理

[Administration] > [AAA] > [Local Password Policy] ページで [Local Password Policy] パラメータを設定して追加の認証を設定できます。設定を有効にするには、チェックボックスをオンにします。

追加の認証では、次の設定が追加されます。

- パスワードの最小長が設定できます。
- ユーザ名またはユーザ名を逆にしたものをパスワードの一部として使用できるかどうかを設定できます。
- パスワードに、「cisco」、「ocsic」またはその中に大文字を使用した異形や、「i」の代わりに「1」、「|」、または「!」、「o」の代わりに「0」、「s」の代わりに「$」を使用したものを含められるかどうかを設定できます。
- ルート パスワードに **public** という語を使用できるかどうかを設定できます。
- パスワード内に 1 つの文字を 3 回よりも多く連続して繰り返せるかどうかを設定できます。
- パスワードに、大文字、小文字、数字、特殊文字の中から 3 種類の文字を含める必要があるかどうかを設定できます。

SSL 認証の設定

Secure Sockets Layer（SSL）認証は、Web サーバとブラウザ間のセキュアなトランザクションを保証するために使用されます。DoD 証明書をインストールすると、Web ブラウザでアイデンティティを信頼し、米国国防総省（DoD）によって認証されたセキュアな通信を提供できるようになります。

これらの証明書は、サーバまたは Web サイトのアイデンティティを確認するため、また SSL で使用する暗号キーを生成するために使用されます。この暗号化により、サーバとクライアント間で受け渡される情報が保護されます。

ここでは、次の内容について説明します。

SSL クライアント認証の設定

DoD 証明書を使用して SSL クライアント証明書の認証を設定するには、次の手順に従います。

（注）　前提条件として、SSL 証明書を作成するには、Keytool が必要です（JDK で使用可能）。KeyTool は、キーストアおよび証明書を管理するために使用するコマンドライン ツールです。

ステップ 1　次のコマンドを使用して、SSL クライアント証明書を作成します。

```
% keytool -genkey -keystore nmsclientkeystore -storetype pkcs12 -keyalg RSA -keysize 2048
-alias nmsclient -dname "CN=nmsclient, OU=WNBU, O=Cisco, L=San Jose, ST=CA, C=US"
-storepass nmskeystore
```

（注）　キー アルゴリズムに RSA、キー サイズに 1024 または 2048 を指定します。

ステップ 2　次のコマンドを使用して、証明書署名要求（CSR）を生成します。

```
% keytool -certreq -keyalg RSA -keysize 2048  -alias nmsclient -keystore nmsclientkeystore
-storetype pkcs12 -file <csrfilename>
```

（注）　キー アルゴリズムに RSA、キー サイズに 1024 または 2048 を指定し、証明書ファイル名を指定します。

ステップ 3　生成された CSR ファイルを DoD に送信します。DoD によって対応する署名証明書が発行されます。

（注）　CSR 応答は、dod.p7b ファイルによって行われます。また、ユーザはルート CA 証明書も受信します。

（注）　PKCS7 符号化された証明書を必ず取得するようにします。認証局では、PKCS7 符号化された証明書の取得のオプションを提供しています。

ステップ 4　次のコマンドを使用して、キーストアに CSR 応答をインポートします。

```
% keytool -import dod.p7b -keystore nmsclientkeystore -storetype pkcs12
-storepass nmskeystore
```

ステップ 5　受信したルート CA 証明書の形式が base 64 符号化であることを確認します。base 64 符号化でない場合、OpenSSL コマンドを使用して base 64 符号化形式に変換します。

```
% openssl x509 -in rootCA.cer -inform DER -outform PEM -outfile rootCA.crt
% openssl x509 -in DoD-sub.cer -inform DER -outform PEM -outfile rootCA.crt
```

（注）　受信したルート CA 証明書と下位の証明書の両方を変換します。

ルート CA 証明書と下位の証明書の両方を受信した場合は、次のコマンドを使用してこれらをバンドルする必要があります。

```
% cat DoD-sub.crt > ca-bundle.crt
% cat DoD-rootCA.crt >> ca-bundle.crt
```

ステップ 6　証明書を使用して SSL クライアント認証を設定するには、<NCS_Home>/webnms/apache/ssl/backup/ フォルダにある、**ssl.conf** ファイル内の Apache の SSL クライアント認証を有効にする必要があります。

```
SSLCACertificationPath conf/ssl.crt
SSLCACertificationFile conf/ssl.crt/ca-bundle.crt
SSLVerifyClient  require
SSLVerifyDepth 2
```

（注）　SSLVerifyDepth は、証明書チェーンのレベルにより異なります。ルート CA 証明書を 1 つだけ保持する場合は、これを 1 に設定する必要があります。証明書チェーンを保持する場合（ルート CA および下位 CA）、これを 2 に設定する必要があります。

ステップ 7　Prime Infrastructure に DoD ルート CA 証明書をインストールします。

ステップ 8　ブラウザに nmsclientkeystore をインポートします。

SSL サーバ認証の設定

DoD 証明書を使用して SSL サーバ証明書を設定するには、次の手順に従います。

ステップ 1　証明書署名要求（CSR）を生成します。

```
% keyadmin -newdn  genkey <csrfilename>
```

ステップ 2　生成された CSR ファイルを DoD に送信します。DoD によって対応する署名証明書が発行されます。

（注）　CSR 応答は、dod.p7b ファイルによって行われます。また、ユーザはルート CA 証明書も受信します。

（注）　PKCS7 符号化された証明書を必ず取得するようにします。認証局では、PKCS7 符号化された証明書の取得のオプションを提供しています。

ステップ 3　KeyTool で次のコマンドを使用して、署名証明書をインポートします。

```
% keyadmin -importsignedcert <dod.p7>
```

（注）　Prime Infrastructure は /opt/CSCOncs/httpd/conf/ssl.crt で自己署名証明書を保存します。インポートした証明書 / キーは /opt/CSCOncs/migrate/restore で保存されます。

Cisco Prime Infrastructure でのサードパーティ証明書の証明書署名要求（CSR）の生成

この付録では、Cisco Prime Infrastructure を使用してサードパーティの証明書を取得するために証明書署名要求（CSR）を生成する方法および Cisco Prime Infrastructure に証明書をインポートする方法について説明します。ここで説明する内容は、次のとおりです。

前提条件

この設定を行う前に、以下の要件を満たしていることを確認してください。

- 基本動作に対応するための Prime Infrastructure のインストールおよび設定方法の知識
- 自己署名およびデジタル証明書、公開キー インフラストラクチャ（PKI）に関連するその他のセキュリティ メカニズムの知識

使用されるコンポーネント

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

サポートされているハードウェアの詳細情報については、次の URL にある Prime Infrastructure のリリース ノートを参照してください。

http://www.cisco.com/en/US/products/ps12239/prod_release_notes_list.html

証明書署名要求（CSR）

証明書は、サーバ、企業などのエンティティを識別し、公開キーとそのアイデンティティを関連付けるために使用する電子ドキュメントです。

自己署名証明書は、その作成者自身によって署名されたアイデンティティ証明書です。つまり、証明書を作成した人もその正当性を認めています。

証明書は、自己署名により、または認証局（CA）からデジタル署名により証明されます。

CA は、アイデンティティを確認し、証明書を発行するエンティティです。CA によって発行された証明書により、その証明書を識別するエンティティ名（サーバ名またはデバイス名など）に特定の公開キーがバインドされます。証明書で認証する公開キーだけが、証明書で識別するエンティティが所有する対応した秘密キーと連動します。証明書により、偽装のための疑似公開キーの使用を防ぐことができます。

CSR は、デジタル ID 証明書を申請するために申請者が CA に送信するメッセージです。CSR を作成する前に、申請者は、最初に秘密キーを守るキー ペアを生成します。CSR には、申請者を識別する情報（X.509 証明書の場合はディレクトリ名など）、および申請者が選択した公開キーが含まれます。対応する秘密キーは CSR に含まれていませんが、要求全体に対するデジタル署名を行うために使用されます。

CSR には、認証局が要求するアイデンティティに対する他のクレデンシャルや証明情報を添付することができます。認証局は申請者と連絡を取ってさらに情報を求めることもできます。概して、Entrust や VeriSign など、サードパーティの CA 企業は、会社がデジタル証明書を作成する前に CSR を要求します。

CSR の生成は、外部証明書をインストールするデバイスに依存しません。したがって、CSR と秘密キー ファイルは、CSR の生成をサポートする任意のマシンで個々に生成できます。この場合、CSR の生成は、スイッチまたはアプライアンスにも依存しません。

表 C-1 に、CSR を生成、インポート、表示、および削除するコマンドのリストを示します。

表 C-1　CSR コマンド

コマンド	説明
ncs key genkey	サードパーティ証明書を生成します。
ncs key importcacert	Prime Infrastructure の信頼ストアに CA 証明書をインポートします。
ncs key importsignedcert	Prime Infrastructure に RSA キーおよび署名付き証明書をインポートします。
ncs key listcacerts	Prime Infrastructure 信頼ストアにあるすべての CA 証明書を一覧表示します。
ncs key deletecacert	Prime Infrastructure 信頼ストアにあるすべての CA 証明書を削除します。

上記の表に記載されているコマンドの詳細情報については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.2/command/reference/cli12_appendix_011.html

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

レポートのフィールド リファレンス

このセクションでは、Prime Infrastructure のレポート内のページのフィールドについて説明します。内容は次のとおりです。

レポート ラウンチ パッド

次の表で、[Report] > [Report Launch Pad] > [Report Type] > [New] ページのフィールドについて説明します。

- 表 D-1：設定およびスケジュール
- 表 D-2：カスタム レポートの作成

[Report Launch Pad] > [Report Type] > [New]

表 D-1 で、[Report] > [Report Launch Pad] > [Report Type] > [New] ページのフィールドについて説明します。

表 D-1　[Report Launch Pad] > [Report Type] > [New Field Descriptions]

フィールド	説明
Settings	
Create reports in current and each sub Virtual Domains	現在の仮想ドメインだけでなく、各サブ仮想ドメインでもレポートを作成する場合、このチェックボックスをオンにします。仮想ドメインの名前、電子メール アドレス、タイム ゾーンなど仮想ドメインに関する詳細を表示するには、[View applied Virtual Domains] リンクをクリックします。 **（注）** このチェックボックスをオンにしており、レポートがスケジュールされていない場合、レポート テンプレートは作成されてすべてのサブドメインに保存されますが、レポートは実行されません。一方、[Create reports in current and sub Virtual Domains] チェックボックスをオンにし、レポートをスケジュールした場合、レポートはすべてのサブドメインにスケジュールされ、スケジュールされた時間に実行されます。 **（注）** このチェックボックスをオンにした場合は、レポートの保存のみが可能であるため、実行、実行して保存、保存してエクスポート、保存して電子メール送信など、他のオプションは、いずれもレポート詳細ページに表示されません。つまり、レポートは、サブドメインでだけ、作成と実行のスケジューリングが可能です。 **（注）** レポートの作成時間はシステムごとに異なるため、レポートの作成とレポートの実行の間には十分な時間間隔（30 分以上）が必要です。
Report Title	レポート名を入力します。 **（注）** [Create reports in current and each sub Virtual Domains] チェックボックスをオンにした場合、このレポート タイトルの末尾に *_VirtualDomainName* が付加されます。この *VirtualDomainName* は、レポートが生成された仮想ドメインの名前です。
Report By	ドロップダウン リストから適切な [Report By] カテゴリを選択します。カテゴリはレポートごとに異なります。 **（注）** インベントリ レポートでは、動作していない AP を表示するために [Report Type] ドロップダウン リストで [Dead Radios] オプションを選択できます。つまり、管理状態が「Up」であり動作ステータスが「Down」の AP です。
Report Criteria	このフィールドでは、事前に選択した [Report By] に応じて、結果をソートできます。[Edit] をクリックして [Filter Criteria] ページを開き、必要なフィルタ基準を選択します。

表 D-1　[Report Launch Pad] > [Report Type] > [New Field Descriptions] （続き）

フィールド	説明
Connection Protocol	次の接続プロトコルのいずれかを選択します。 • **All Clients** • **All Wired (802.3)** • **All Wireless (802.11)** • **All 11u Capable Clients** • **802.11a/n/ac** • **802.11b/g/n** • **802.11a** • **802.11b** • **802.11g** • **802.11ac** • **802.11n (5 GHz)** • **802.11n (2.4 GHz)**
SSID	すべての SSID がデフォルト値です。
Reporting Period	[Select a time period] オプション ボタンを選択して、ドロップダウン リストから期間を選択します。 または [From] オプション ボタンを選択して、開始日時と終了日時を入力します。テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして日付を選択できます。ドロップダウン リストから時間と分を選択します。
Show	レポートに表示するレコード数を入力します。 **（注）** 5 ～ 1000 までの数値を入力するか、テキスト ボックスをブランクのままにするとすべてのレコードが表示されます。
Schedule	
Scheduling	設定したスケジュールに従ってレポートを実行するには、[Enable] チェックボックスをオンにします。
Export Format	レポート実行後にレポート結果をエクスポートする形式として [CSV] または [PDF] を選択します。 **（注）** CSV ファイルおよび PDF ファイルのデフォルトの場所は、次のとおりです。 /ncs-ftp/reports/Inventory/*ReportTitleName_yyyymmdd_HHMMSS.csv* /ncs-ftp/reports/Inventory/*ReportTitleName_yyyymmdd_HHMMSS.pdf*

表 D-1　[Report Launch Pad] > [Report Type] > [New Field Descriptions]（続き）

フィールド	説明
Destination	宛先タイプ（ファイルまたは電子メール）を選択します。該当するファイルの場所または電子メール アドレスを入力します。 （注）　[Create reports in current and each sub Virtual Domains] チェックボックスをオンにすると、[Email] オプション ボタンではなく、[Email to default Contact in each Virtual Domain] オプション ボタンが表示されます。[View Contacts] リンクをクリックすると、各仮想ドメインの電子メール ID を表示できます。 （注）　電子メール用のメール サーバ セットアップを設定するには、[Administration] > [Settings] を選択し、左側のサイドバーのメニューの [Mail Server] を選択して [Mail Server Configuration] ページを開きます。SMTP およびその他の必要な情報を入力します。 （注）　サブ仮想ドメインの電子メール アドレスが指定されていない場合は、現在の仮想ドメインの電子メール アドレスが指定されていれば、この現在の仮想ドメインのアドレスが使用されます。
Start Date/Time	表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。このデータに対するレポートの実行が、この日時に開始されます。 （注）　ここで指定する時間は、Prime Infrastructure サーバの時間であり、ブラウザの現地時間ではありません。 （注）　[Create reports in current and each sub Virtual Domains] チェックボックスをオンにした場合は、[Use Virtual Domain time zone] チェックボックスが表示されます。仮想ドメインのタイム ゾーンをタイム ゾーンとして使用する場合は、このチェックボックスをオンにします。さまざまな仮想ドメインのタイム ゾーンを表示するには、[View time zones] リンクをクリックします。
Recurrence	次のオプションからレポート実行の頻度を選択します。 • [No Recurrence]：レポートは 1 度だけ実行されます（[Start Date/Time] で示した時間に実行）。 • [Hourly]：レポートは、[Entry] テキスト ボックスに入力する時間数で示す間隔で実行されます。 • [Daily]：レポートは、[Every] テキスト ボックスに入力する日数で示す間隔で実行されます。 • [Weekly]：レポートは、[Every] テキスト ボックスに入力する週数およびチェックボックスをオンにした曜日に実行されます。 • [Monthly]：レポートは、[Every] テキスト ボックスに入力する月数で示す間隔で実行されます。

[Report Launch Pad] > [Report Type] > [New] > [Customize]

表 D-2 で、[Report] > [Report Launch Pad] > [Report Type] > [New] > [Customize] ページのフィールドについて説明します。

表 D-2　[Report Launch Pad] > [Report Type] > [New] > [Customize Field Descriptions]

フィールド	説明
Custom Report Name	ドロップダウン リストからカスタマイズするレポートを選択します。 （注）　[Available data fields] 列と [Data fields to include] 列の見出しの選択項目は、選択したレポートにより異なる場合があります。
Report View	レポートの表示形式（表形式、グラフ形式、または結合形式（両方））を指定します。 （注）　このオプションは、一部のレポートでは使用できません。
Available data fields/Data fields to include	[Add >] ボタンおよび [< Remove] ボタンを使用して、[Available data fields] 列と [Data fields to include] 列の間で強調表示したフィールドを移動します。 （注）　[Data fields to include] 列に青色のフォントで表示されるフィールドは、[Custom Report Name] フィールドで選択したレポートの必須フィールドです。
[Change order] ボタン	[Move Up] ボタンおよび [Move Down] ボタンを使用して、結果テーブル内の列の順序を決定します。[Selected Columns] リストで上方の列見出しが、結果表の左方に表示されます。
Data field sorting	ソート設定を指定します（[Ascending] または [Descending]）。レポート データのソート方法を指定します。 • ソート順序を指定できる 4 つのデータ フィールドを選択できます。[Sort by and Then by] ドロップダウン リストを使用して、ソート用の各データ フィールドを選択します。 • 各ソート対象データ フィールドについて、昇順でソートするか降順でソートするかを選択します。 （注）　表形式のレポートのみソートできます（グラフおよび複合形式は不可）。ソートできるフィールドのみが [Data field sorting] ドロップダウン リストに表示されます。 （注）　[Create Custom Report] ページに表示される [Sortable fields] には、[Data fields to include] ペインにあるデータ フィールドだけでなく、ソート可能なすべてのフィールドがリストされます。レポートは、対応する列がレポートに表示されない場合でも、選択したデータ フィールドに基づいてソートされます。

Scheduled Run Results

表 D-3 で、[Report] > [Scheduled Run Results] ページのフィールドについて説明します。

表 D-3　[Scheduled Run Results] のフィールドの説明

フィールド	説明
Report Category	ドロップダウン リストから適切なレポート カテゴリを選択するか、[All] を選択します。
Report Type	ドロップダウン リストから適切なレポート タイプを選択するか、[All] を選択します。レポート タイプの選択項目は、選択したレポート カテゴリに応じて変わります。
From/To	レポートの開始日（[From]）と終了日（[To]）をテキスト ボックスに入力するか、カレンダー アイコンをクリックして開始日と終了日を選択します。
Report Generation Method	次のオプションからいずれかのレポート生成方式を選択します。 • Scheduled • On-demand Export • On-demand Email

Saved Report Templates

表 D-4 で、[Report] > [Saved Report Templates] ページのフィールドについて説明します。

表 D-4　[Saved Report Templates] のフィールドの説明

フィールド	説明
Report Category	ドロップダウン リストから適切なレポート カテゴリを選択するか、[All] を選択します。
Report Type	ドロップダウン リストから適切なレポート タイプを選択するか、[All] を選択します。レポート タイプの選択項目は、選択したレポート カテゴリに応じて変わります。
Scheduled	[All]、[Enabled]、[Disabled]、または [Expired] を選択して、スケジュールされたステータスによって [Saved Report Templates] リストをフィルタします。

レポート結果

ここでは、[Report] > [Report Launch Pad] > [Report Type] > [New] > [Customize] > [Create Custom Report] ページでのレポートのカスタマイズ方法に基づき、各種レポート タイプで表示される結果について説明します。ここでは、次の内容について説明します。

- 「クライアント レポート」（P.D-6）
- 「デバイス レポート」（P.D-11）

クライアント レポート

次の表で、各種クライアント レポートの結果に表示されるフィールドについて説明します。

- 表 D-5：Busiest Clients レポートの結果
- 表 D-6：Client Sessions レポートの結果
- 表 D-7：Client Traffic Stream Metrics レポートの結果
- 表 D-8：Unique Client レポートの結果
- 表 D-9：CCX Client Statistics レポートの結果

Busiest Clients レポートの結果

表 D-5 で、Busiest Clients レポート生成時に表示される可能性のある結果について説明します。

表 D-5　Busiest Clients レポート結果のフィールドの説明

フィールド	説明
Client MAC Address	クライアントの MAC アドレス。
IP Address	クライアントの IP アドレス。このフィールドには、IPv6 クライアントの場合は IPv6 アドレス、IPv4 およびデュアル スタック クライアントの場合は IPv4 アドレスが表示されます。
Protocol	802.11a/n または 802.11b/g/n。
Throughput	Mbps または kbps。 **（注）**　スループットが 0.1 kbps 未満の場合は、「<0.1 kbps」が表示されます。

表 D-5　Busiest Clients レポート結果のフィールドの説明 （続き）

フィールド	説明
Global Unique	IPv6 アドレスの集約グローバル ユニキャスト アドレス。このフィールドには、クライアントにグローバル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
Local Unique	IPv6 アドレスのローカル ユニキャスト アドレス。このフィールドには、クライアントにローカル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
Link Local	IPv6 アドレスのリンクローカル ユニキャスト アドレス。このフィールドには、クライアントにリンクローカル IPv6 アドレスが割り当てられている場合のみ値が入力されます。
On Device	クライアントが配置されているデバイス。
Bytes sent (MB)	送受信されたバイト数（MB）。
Bytes received (MB)	（注）　この値が 1,000,000,000 を超える場合は、値の末尾に G が追加されます（例：3.45 G）。この値が 1,000,000 を超え、1,000,000,000 未満の場合は、値の末尾に M が追加されます（例：456.8 M）。
Packets sent	送受信されたパケット数（MB）。
Packets received	（注）　この値が 1,000,000,000 を超える場合は、値の末尾に G が追加されます（例：3.45 G）。この値が 1,000,000 を超え、1,000,000,000 未満の場合は、値の末尾に M が追加されます（例：456.8 M）。

Client Sessions レポートの結果

表 D-6 で、Client Sessions レポート生成時に表示される可能性のある結果について説明します。

表 D-6　Client Sessions レポート結果のフィールドの説明

フィールド	説明
Client Username	このクライアントのユーザ名。
IP Address	このクライアントの IP アドレス。
MAC Address	このクライアントの MAC アドレス。
Association Time	このクライアントがアソシエートされた日時。
Access Point Name	このクライアントが割り当てられたアクセス ポイントの名前。
Map Location	クライアントがあるビルディング、フロア領域、または屋外領域（該当する場合）。
SSID	このクライアントがアソシエートされた SSID。
Profile	このクライアントがアソシエートされたプロファイルの名前。
VLAN ID	VLAN ID。範囲は 1 ～ 4096 です。
Protocol	802.11a、802.11b、802.11g、802.11n_5GHz、または 802.11b_2.4GHz。
Policy Type	このクライアント セッションのセキュリティ ポリシーのタイプ。
Host Name	このクライアントが配置されているマシンの DNS ホスト名。 Prime Infrastructure は、DNS ルックアップを実行して、クライアント IP アドレスからホスト名を解決します。IP アドレスとホスト名のマッピングが、DNS サーバで定義されている必要があります。デフォルトでは、ホスト名のルックアップは無効です。ホスト名のルックアップを有効にするには、[Administration] > [Settings] > [Clients] を使用します。
Global Unique	IPv6 アドレスの集約グローバル ユニキャスト アドレス。このフィールドには、クライアントにグローバル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。

表 D-6　Client Sessions レポート結果のフィールドの説明 （続き）

フィールド	説明
Local Unique	IPv6 アドレスのローカル ユニキャスト アドレス。このフィールドには、クライアントにローカル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
Link Local	IPv6 アドレスのリンクローカル ユニキャスト アドレス。このフィールドには、クライアントにリンクローカル IPv6 アドレスが割り当てられている場合のみ値が入力されます。
CCX	Cisco Client Extension のバージョン番号。
AP MAC Address	アクセス ポイントの MAC アドレス。
AP IP Address	アクセス ポイントの IP アドレス。
AP Radio	アクセス ポイントの無線タイプ。
Device IP Address	このクライアントがアソシエートされたデバイスの IP アドレス。
Device Port	このクライアントがアソシエートされたデバイスのポート番号。
Anchor Controller	モビリティ クライアントのアンカーまたは外部コントローラの IP アドレス（該当する場合）。
Association ID	このクライアント セッションで使用されたアソシエーション ID。
Disassociation Time	このクライアントのアソシエーションが解除された日時。
Authentication	このクライアントの認証方式。
Encryption Cypher	このクライアント セッションで使用された暗号化。
EAP Type	このクライアント セッションで使用された EAP タイプ。
Authentication Algorithm	このクライアント セッションで使用された EAP タイプ。
Web Security	このクライアント セッションで使用された Web セキュリティ。
Tx and Rx (bytes)	クライアント セッション中に送信または受信されたおおよそのバイト数。
SNR	このクライアント セッションの信号対雑音比。
RSSI	受信信号強度インジケータ（dBm）。
Status	[Associated] または [disassociated]。
Reason	アソシエーション解除の理由。
E2E	バージョン番号または [Not Supported]。

Client Traffic Stream Metrics レポートの結果

表 D-7 で、Client Traffic Stream Metrics レポート生成時に表示される可能性のある結果について説明します。

表 D-7　Client Traffic Stream Metrics レポート結果のフィールドの説明

フィールド	説明
Time	アクセス ポイントから統計情報が収集された時刻。
Client MAC	クライアントの MAC アドレス。これには、過去 90 秒の間隔中に評価されたクライアントのリストが表示されます。クライアントとしては、VoIP 電話、ラップトップ、PDA などがあり、測定値を収集しているアクセス ポイントに接続されたすべてのクライアントを示します。

表 D-7　Client Traffic Stream Metrics レポート結果のフィールドの説明 （続き）

フィールド	説明
QoS	WLAN に影響を与える可能性のある QoS 値（パケット遅延、パケット ジッタ、パケット損失、ローミング時間）がモニタされます。アクセス ポイントおよびクライアントでメトリックを測定し、アクセス ポイントで計測結果を収集してこれらをコントローラに送信します。アクセス ポイントでは、90 秒ごとにコントローラのトラフィック ストリーム メトリック情報を更新し、クライアントごとに 10 分間分のデータが WLC に格納されます。Prime Infrastructure は、過去 7 日間のこのデータをポーリングして保存します。
AP Name	このクライアントがアソシエートされたアクセス ポイントの名前。
Radio Type	アクセス ポイントの無線タイプ。
Avg Queuing Delay (ms) (Downlink)	ダウンリンクの平均キューイング遅延（ミリ秒単位）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
Avg Queuing Delay (ms) (Uplink)	アップリンクの平均キューイング遅延（ミリ秒単位）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
% PLR (Downlink)	90 秒の間隔中にダウンリンク（アクセス ポイントからクライアントへ向かう方向）で失われたパケットの割合。
% PLR (Uplink)	90 秒の間隔中にアップリンク（クライアントからアクセス ポイントへ向かう方向）で失われたパケットの割合。
% Packets > 40ms Queuing Delay (Uplink)	40 ms を超えるキューイング遅延パケットのパーセンテージ。
% Packets 20ms-40ms Queuing Delay (Uplink)	20ms ～ 40 ms のキューイング遅延パケットのパーセンテージ。
Roaming Delay	ローミング遅延（ミリ秒単位）。クライアントによって測定されるローミング遅延は、古いアクセス ポイントから最後のパケットを受信した時点から、ローミングが正常に行われた後で新しいアクセス ポイントから最初のパケットを受信した時点まで測定されます。

Unique Client レポートの結果

表 D-8 で、Unique Client レポート生成時に表示される可能性のある結果について説明します。

表 D-8　Unique Client レポート結果のフィールドの説明

フィールド	説明
First/Last Seen	固有クライアントが最初に検出された日時および最後に検出された日時。
User	クライアントのユーザ名。
Vendor	ベンダー名または [unknown]。
Client IP Address	クライアントの IP アドレス。
Client MAC Address	クライアントの MAC アドレス。
AP Name	このクライアントがアソシエートされたアクセス ポイントの名前。
Controller	クライアントがアソシエートされたコントローラ。
Port	このクライアントがアソシエートされたデバイスのポート番号。
802.11	[Associated]、[Disassociated]、または [Idle]。

表 D-8　Unique Client レポート結果のフィールドの説明 （続き）

フィールド	説明
SSID	このクライアントがアソシエートされた SSID。 （注）　クライアントがプロービングを行っている場合は、[SSID] フィールドに「N/A」が表示されます。
Authenticated	クライアントが認証されているかどうかを示します（[Yes] または [No]）。
Protocol	802.11a、802.11b、802.11g、802.11n_5GHz、または 802.11b_2.4GHz。
VLAN ID	VLAN ID。範囲は 1 ～ 4096 です。
CCX	CCX（Cisco Client Extensions）がサポートされているかどうかを示します。
E2E	E2E（エンドツーエンド）がサポートされているかどうかを示します。

CCX Client Statistics レポートの結果

表 D-9 で、CCX Client Statistics レポート生成時に表示される可能性のある結果について説明します。

表 D-9　CCX Client Statistics レポート結果のフィールドの説明

フィールド	説明
Client MAC Address	クライアントの MAC アドレス。
Transmitted Fragment Count	このカウンタは、正常に受信した MPDU データまたは管理タイプごとに増分されます。
Multicast Transmitted Frame Count	このカウンタは、正常に送信された MAC Service Data Unit（MSDU）の宛先 MAC アドレス中でマルチキャスト ビットが設定されている場合にのみ減少します。Extended Service Set（ESS）でステーション（STA）として動作している場合、これらのフレームはアクセス ポイントに送信されます。これは、アソシエートされたすべての MAC Protocol Data Unit（MPDU）に対する確認応答を受信したことを示します。
Failed Count	このカウンタは、MSDU の送信が失敗した場合に、増分されます。
Retry Count	このカウンタは、1 回以上の再送信の後で MSDU が正常に送信された場合に増分されます。
Multicast Retry Count	このカウンタは、複数回の再送信の後で MSDU が正常に送信された場合に増分されます。
Frame Duplicate Count	このカウンタは、Sequence Control フィールドで重複が示されているフレームを受信した場合に増分されます。
RTS Success Count	このカウンタは、RTS（ready-to-send）への応答として CTS（clear-to-send）を受信した場合に増分されます。
RTS Fail Count	このカウンタは、ready-to-send への応答として clear-to-send を受信しない場合に増分されます。
ACK Fail Count	このカウンタは、正常な ACK を受信しなかった場合に増分されます。
Received Fragment Count	長さが 64 オクテット（フレーミング ビットは除外するが、FCS オクテットは含む）未満の受信済みパケットの総数。
Multicast Received Frame Count	このカウンタは、宛先 MAC アドレスにマルチキャスト ビットが設定された MSDU を受信したときに増分されます。
FCS Error Count	このカウンタは、受信した MPDU でフレーム チェック シーケンス エラーが検出されると増分されます。
Transmitted Frame Count	このカウンタは、MSDU を正常に送信するたびに増分されます。

デバイス レポート

次の表で、各種デバイス レポートの結果に表示されるフィールドについて説明します。

- 表 D-10：AP Image Predownload レポートの結果
- 表 D-11：AP Profile Status レポートの結果
- 表 D-12：Busiest APs レポートの結果

AP Image Predownload レポートの結果

表 D-10 で、AP Image Predownload レポート生成時に表示される可能性のある結果について説明します。

表 D-10　AP Image Predownload レポート結果のフィールドの説明

フィールド	説明
AP Name	アクセス ポイントの名前。
Primary Image	AP にある現在のプライマリ イメージ。
Backup Image	AP にある現在のバックアップ イメージ。
Predownload Version	事前ダウンロード プロセスの一部として現在コントローラから AP にダウンロードされているイメージのバージョン。
Predownload Status	事前ダウンロード プロセスの一部であるイメージ ダウンロードの現在のステータス。
MAC Address	AP の MAC アドレス。
Controller IP Address	アクセス ポイントがアソシエートされたコントローラの IP アドレス。
Upgrade Role	アップグレード ロールの現在のステータス。これは次のいずれかになります。 • Master Central • Master Local • Slave Central • Slave Local • Unknown

AP Profile Status レポートの結果

表 D-11 で、AP Profile Status レポート生成時に表示される可能性のある結果について説明します。

表 D-11　AP Profile Status レポート結果のフィールドの説明

フィールド	説明
Time	AP プロファイル ステータスの収集日時。
AP Name	アクセス ポイントの名前。
AP MAC Address	アクセス ポイントの MAC アドレス。
Radio Type	802.11a/n または 802.11b/g/n。
Load	[Pass] または [Fail]。負荷レベルがしきい値レベルを超えているかどうかを示します。
Noise	[Pass] または [Fail]。ノイズ レベルがしきい値レベルを超えているかどうかを示します。
Interference	[Pass] または [Fail]。干渉レベルがしきい値レベルを超えているかどうかを示します。

表 D-11　AP Profile Status レポート結果のフィールドの説明 （続き）

フィールド	説明
Coverage	[Pass] または [Fail]。カバレッジ レベルがしきい値レベルを超えているかどうかを示します。
Controller Name	アクセス ポイントがアソシエートされたコントローラの名前。
Controller IP Address	アクセス ポイントがアソシエートされたコントローラの IP アドレス。

Busiest APs レポートの結果

表 D-12 で、Busiest APs レポート生成時に表示される可能性のある結果について説明します。

表 D-12　Busiest APs レポート結果のフィールドの説明

フィールド	説明
AP Name	アクセス ポイントの名前。
Radio Type	802.11a/n または 802.11b/g/n。
Rx Utilization (%)	アクセス ポイント レシーバがパケットの処理でビジーな時間の割合。これは、0 ～ 1 までの負荷を表す 0 ～ 100 までの数値です。
Tx Utilization (%)	アクセス ポイント トランスミッタがパケットの処理でビジーな時間の割合。これは、0 ～ 1 までの負荷を表す 0 ～ 100 までの数値です。
Channel Utilization (%)	アクセス ポイント チャネルがパケットの処理でビジーな時間の割合。これは、0 ～ 1 までの負荷を表す 0 ～ 100 までの数値です。
Controller Name	アクセス ポイントがアソシエートされたコントローラの名前。
Controller IP Address	アクセス ポイントがアソシエートされたコントローラの IP アドレス。
Map Location	アクセス ポイントがあるビルディング、フロア領域、または屋外領域（該当する場合）。

数字

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

の

は

ひ

ふ

へ

ほ

ま

み

む

め

も

ゆ

り

る

れ

ろ

わ

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/