Wi-Fi ロケーションベース サービス 4.1 デザイン ガイド

Wi-Fi Location-Based Services 4.1 Design Guide

2008 年 5 月 20 日

Text Part Number: OL-11612-01-J

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

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されているデザイン、仕様、表現、情報、および推奨事項（総称して「デザイン」）は、障害も含めて本マニュアル作成時点のものです。シスコシステムズおよびそのサプライヤは、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、一切の保証の責任を負わないものとします。いかなる場合においても、シスコシステムズおよびそのサプライヤは、このデザインの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはそのサプライヤに知らされていても、それらに対する責任を一切負わないものとします。

デザインは予告なしに変更されることがあります。このマニュアルに記載されているデザインの使用は、すべてユーザ側の責任になります。これらのデザインは、シスコシステムズ、そのサプライヤ、パートナーの技術的な助言や他の専門的な助言に相当するものではありません。ユーザは、デザインを実装する前に技術アドバイザーに相談してください。シスコによるテストの対象外となった要因によって、結果が異なることがあります。

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Wi-Fi ロケーションベース サービス 4.1 デザイン ガイド
© 2008 Cisco Systems, Inc.
All rights reserved.

Copyright © 2009, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

CHAPTER 1 **概要** 1-1

はじめに 1-1

このガイドについて 1-2

このガイドの対象 1-2

目的 1-2

追加参考文献 1-3

ハードウェアおよびソフトウェア コンポーネント 1-3

CHAPTER 2 **ロケーション トラッキング アプローチ** 2-1

基点のセル 2-2

距離に基づく（ラテレーション）技法 2-3

到達時間 2-3

到達時間差（TDoA） 2-5

受信信号強度（RSS） 2-7

角度ベース（アンギュレーション）技法 2-9

到達角度（AoA） 2-9

ロケーションのパターン作成（パターン認識）技法 2-10

調整フェーズ 2-11

運用フェーズ 2-12

CHAPTER 3 **Cisco ロケーションベース サービスのアーキテクチャ** 3-1

RF フィンガープリント 3-1

ロケーション認識 Cisco UWN アーキテクチャ 3-4

Location Appliance の役割 3-7

Location Appliance を使用しないロケーション トラッキング 3-9

確度と精度 3-12

クライアント、資産、不正なデバイスの追跡 3-13

クライアント プローブ 3-14

Cisco Compatible Extensions ロケーション測定 3-15

WLAN クライアント 3-19

802.11 アクティブ RFID タグ 3-23

不正アクセス ポイント 3-30

不正クライアント 3-32
ワークグループ ブリッジ 3-35
Cisco Location Control Protocol（LOCP） 3-36
LOCP を使用する資産タグ テレメトリ 3-38
LOCP を使用する資産タグ通知 3-41

CHAPTER 4 インストールおよび構成 4-1
Location Appliance のインストールと構成 4-1
ロケーション トラッキング用の Cisco WCS の設定 4-1
Location Appliance 履歴パラメータの設定 4-2
履歴アーカイブ期間 4-2
履歴データベースの消去 4-3
Location Appliance 詳細パラメータの設定 4-3
不明データのクリーンアップ間隔 4-3
メモリ情報 4-5
詳細コマンド 4-5
Location Appliance ロケーション パラメータの設定 4-7
計算回数の有効化 4-7
外壁（OW）ロケーションの有効化 4-7
RSSI 破棄時間 4-7
RSSI の遮断 4-8
Location Appliance 通知パラメータの設定 4-8
Queue Limit 4-8
Retry Count 4-9
Refresh Time 4-9
Notifications Dropped 4-9
Location Appliance LOCP パラメータの設定 4-10
Location Appliance の二重イーサネット運用 4-10
Location Appliance のデフォルト パスワードの変更 4-10
"root" ユーザ Linux システム パスワードの変更 4-10
"admin" Location Server Application パスワードの変更 4-11
Location Appliance の時間同期 4-13
Location Appliance の停止 4-14

CHAPTER 5 ベスト プラクティス：ロケーション認識 WLAN 設計の考慮事項 5-1
信号レベルの最小しきい値 5-2
アクセス ポイントの配置 5-5
アクセス ポイントの間隔 5-12

ロケーション準備の確認 5-18
ロケーション、音声、データの共存 5-20
ロケーション表示ジッタの回避 5-31
複数 Location Appliance の設計 5-32
シングル管理ドメイン（マルチ ロケーション ドメイン） 5-36
マルチ管理ドメイン（マルチ ロケーション ドメイン） 5-40
アンテナに関する考慮事項 5-44
サードパーティ製のアンテナ 5-44
アンテナの方向とアクセス ポイントの配置 5-46
調整 5-48
調整の有効性 5-55
調整を成功させるためのヒント 5-56
データ収集 5-56
典型的な条件下での調整 5-57
推奨される調整クライアントとテクニック 5-58
一様でない環境での調整 5-62
ロケーション品質の検査 5-63
テスト ポイントを使用した確度の確認 5-67

CHAPTER 6 **RFID タグの考慮事項** 6-1
RFID タグ テクノロジー 6-1
パッシブ RFID タグ 6-2
セミパッシブ RFID タグ 6-5
アクティブ RFID タグ 6-6
アクティブ RFID タグのビーコン送信 6-7
802.11 アクティブ RFID タグ 6-7
マルチモード RFID タグ 6-8
チョークポイント トリガー 6-9
Cisco UWN での Wi-Fi RFID タグの使用 6-15
互換性のある RFID タグ 6-15
802.11g 環境での 802.11b タグの使用 6-16
資産タグ トラッキングの有効化 6-17
資産タグ RF データ タイムアウトの有効化 6-17
資産タグ ポーリングの有効化 6-18
資産タグ表示の有効化 6-19
資産タグの設定 6-20
タグ テレメトリおよび通知に関する考慮事項 6-26
タグ テレメトリの展開 6-27
タグ高優先順位通知の展開 6-29

タグのテレメトリおよび通知の設定 6-31
チョークポイントに関する考慮事項 6-31
チョークポイント トリガーの設定 6-31
Cisco UWN へのチョークポイント トリガーの定義 6-33
チョークポイント トリガーのトラフィックに関する考慮事項 6-34

CHAPTER 7 注意事項 7-1
CSCse14724：モニター モード AP でのロケーション確度の低下 7-1
CSCsh88795：CCX S36 ビーコン測定要求のデュアル バンド サポート 7-1
CSCsi95122：WCS がロケーション通知のためのノースバウンド電子メールを送信しない 7-2

APPENDIX A Maxima 使用による概算ルートの算出 A-1

APPENDIX B WLAN コントローラでの資産タグ検出の確認 B-1
資産タグの検出 B-1
資産タグが検出されない場合 B-6
資産タグのテレメトリおよびイベントの確認 B-8

CHAPTER 1

概要

はじめに

この 10 年で、802.11 無線は、主に垂直産業の生産性を改善するための技術から社会全体に普及する技術として著しく進化しました。Wi-Fi ネットワークが広範に受け入れられたことがこの飛躍的な採用につながり、導入はオフィスや配信センターから家庭へ、そして無線大都市圏へと拡大しています。この幅広い導入によって急速に成熟し、必要十分な需要に達したため、無線インフラストラクチャのコストは大幅に低下し、高品質の機器を低コストで入手できるようになりました。

Wi-Fi 採用率が急速に上昇し、高品質インフラストラクチャを妥当なコストで利用できるようになったことが、Wi-Fi ロケーションベース サービス関連の活動が高まった大きな要因です。ロケーション受信装置と RFID タグ リーダーという専用の独立したインフラストラクチャを必要とするソリューションと混同しないよう注意してください。Wi-Fi ロケーション予測技法の研究開発は、基本的に IEEE 802.11 インフラストラクチャに基づく屋内 RF ロケーション トラッキング システムの登場を促しました。消費者および流通サプライ チェーンでの激しい RFID システム導入競争と相まって、かつては一般市場で一過性の興味の対象でしかなかったロケーションベース サービスが、Wi-Fi 無線に*絶対に必要*な 802.11 に基づく アプリケーションとしての地位を占めるまでになりました。

その理由を理解するのは難しいことではありません。企業の無線 LAN にロケーション トラッキング機能を統合すれば、ビジネス資産としての価値がさらに高まります。今日のペースの速い競争の激しい市場では特に重要です。他社より優位に立っていた企業が、必要な資産を持っていないためではなく、それらの資産の場所を特定し、急速に変化するビジネス環境に対応してすばやく再配置できないために競争から脱落することもありえます。企業のネットワーク管理者、セキュリティ担当者、ユーザ、資産所有者および他の関係者は、彼らが置かれた環境で次の主要な問題の解決に役立つロケーションベース サービスに大きな関心を寄せています。

- 重要な資産や主要スタッフの所在を迅速かつ効率的に確認する必要性。
- 資産と人員の効率的な割り当てにより、生産性を向上する。
- 資産の無断持ち出しを防止し、損失を削減する。
- サービスに影響を与える重要な資産の所在をすばやく確認し、顧客満足度を高める。
- WLAN の計画能力と調整能力を高める。
- セキュリティ ポリシーに基づいて Wi-Fi デバイスのロケーションを調整する。
- 不正デバイスのロケーションを特定する。
- 環境内の主要資産のヘルスとステータスを監視し、変化がある場合、迅速に通知を受け取る。
- 資産の不正な追加または削除が発生した場合、迅速に通知を受け取る。

このガイドでは、ロケーション認識 Cisco Unified Wireless Network（UWN）について説明します。主に、屋内のロケーションベース サービス設計時の考慮事項と展開の選択について説明します。このガイドを通して、関連する既存マニュアルがある場合は、参照先を示します。また、次のトピックを扱う資料も多数参照できます。

- ラテレーション、アンギュレーション、およびパターン認識アプローチを含む位置決めテクノロジーの基本
- Cisco RF フィンガープリントの動作および他のアプローチとの比較
- ロケーション認識 Cisco UWN のアーキテクチャ
- 音声、データ、ロケーションベース サービスの共存を含む設計上の考慮事項
- 適切な設置および構成に関するヒント

このガイドについて

このガイドの対象

このガイドは、Cisco Wireless Location Appliance、Cisco Wireless Control System（WCS）、および Cisco Unified Wireless Network（UWN）の他のコンポーネントを含む、屋内の Cisco Wireless LAN（WLAN）ソリューションの設計および展開に関心のあるユーザを対象としています。

目的

このガイドの目的は次のとおりです。

- ロケーションベース サービスに馴染みのない読者に、ロケーション トラッキングおよび位置決めシステムの技術面の基礎について説明する。第 2 章「ロケーション トラッキング アプローチ」では、基点のセル、到達時間、到達時間差、到達角度、パターン認識など、位置決めシステム技法の背景情報について詳しく説明します。
- ロケーション認識 Cisco UWN の中心テクノロジーである RF フィンガープリントを定義し、説明する。第 3 章「Cisco ロケーションベース サービスのアーキテクチャ」では、RF フィンガープリントと、第 2 章「ロケーション トラッキング アプローチ」で説明されている他のアプローチの類似点と違い、RF フィンガープリントでコスト効率の優れた屋内 Wi-Fi ロケーション トラッキング ソリューションを展開する方法について説明します。この知識は、ロケーション認識 Cisco Unified Wireless Network を他の屋内ロケーション トラッキング アプローチと比較する場合に有益です。
- LWAPP 対応アクセス ポイント、サードパーティ製チョークポイント トリガー、WLAN コントローラ、WCS、Location Appliance で構成されるロケーション認識 Cisco UWN の設置および構成に必要な手順を検討する。
- 適切な設置および高度なパラメータの理解に役立つ情報を提供する（第 4 章「インストールおよび構成」を参照してください）。
- ロケーション認識無線 LAN の設計および展開で従う必要のあるベスト プラクティスについて説明する。第 5 章「ベスト プラクティス：ロケーション認識 WLAN 設計の考慮事項」では、アクセス ポイントの配置と分離、複数の Location Appliance 設計、およびアンテナに関する考慮事項から調整や厳しいロケーション環境まで、さまざまなトピックについて説明します。ここで説明する情報はすべて、設計者がロケーション認識設計を最適化し、ロケーション忠実度を改善するのに役立ちます。

- RFID タグ テクノロジーに精通していない読者に、さまざまなタイプのタグとロケーション認識 Cisco UWN の関連に関する基礎知識を提供する。第 6 章「RFID タグの考慮事項」では、RFID 資産タグの詳細と、これらの製品の機能について説明します。この章では、RFID タグ使用時の Cisco WLAN コントローラ、WCS、および Location Appliance の適切な構成に重点を置いて説明します。

追加参考文献

読者は、次のマニュアルに精通していることを前提とします。

- Cisco Wireless Location Appliance リリース 3.0 マニュアル
  http://www.cisco.com/en/US/products/ps6386/tsd_products_support_series_home.html
- Cisco Wireless Control System リリース 4.1 マニュアル
  http://www.cisco.com/en/US/products/ps6305/tsd_products_support_series_home.html
- Cisco 4400 シリーズ WLAN Controller リリース 4.1 マニュアル
  http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html
- Cisco 2100 シリーズ WLAN Controller リリース 4.1 マニュアル
  http://www.cisco.com/en/US/products/ps7206/tsd_products_support_series_home.html
- Cisco Catalyst 3750 シリーズ Integrated Wireless LAN Controller マニュアル
  http://www.cisco.com/en/US/products/ps6915/
- Cisco Wireless LAN Controller モジュール マニュアル
  http://www.cisco.com/en/US/products/ps6730/tsd_products_support_model_home.html
- Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）マニュアル
  http://www.cisco.com/en/US/products/ps6526/tsd_products_support_model_home.html

（注） 名称は異なりますが、このガイドで Cisco Unified Wireless Network（UWN）ソフトウェア リリース 4.1 について説明している場合、通常 Cisco Location Appliance ソフトウェア リリース 3.0 も含まれています。

Cisco と InnerWireless の統合ソリューションで InnerWireless（旧 PanGo）Vision Locator ロケーション クライアントを使用する際の設計上の考慮事項は、次の文書を参照してください。

- 『*Design Considerations for Cisco – PanGo Asset Tracking*』
- http://www.cisco.com/univercd/cc/td/doc/solution/pangoex.pdf

Voice over WLAN（VoWLAN）ハンドセットとそれをサポートするインフラストラクチャをロケーションベース サービスとともに展開する際の設計の参考文献として、次のガイドをお勧めします。

- 『*Voice over Wireless LAN 4.1 Design Guide*』
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

ハードウェアおよびソフトウェア コンポーネント

表 1-1 は、このガイドの執筆時点で使用したハードウェアとソフトウェアのリストです。

（注）　サポートされている他のハードウェアおよびソフトウェアについては、http://www.cisco.com/en/US/products/ps6386/index.html の情報を参照してください。

表 1-1　テストされたハードウェアおよびソフトウェア

Location Appliance	
AIR-LOC2700-L-K9[1]	Location Appliance 2700 シリーズ。ソフトウェア リリース 3.0.42.0
Wireless Control System（WCS）	
WCS-STANDARD-K9-4.1.91.0.exe	Windows 2003 Server 用 Wireless Control System リリース 4.1.91.0[2]
WLAN コントローラ	
AIR-WLC4402-12-K9	4400 Series WLAN Controller。リリース 4.1.185.0
AIR-WLC2106-K9	2106 Series WLAN Controller。リリース 4.1.185.0
アクセス ポイント	
AIR-LAP1242AG-A-K9	802.11ag LWAPP AP North American。バージョン 12.3(11)JX
外部アンテナ	
AIR-ANT4941	2.4 GHz、2.2 dBi ダイポール
AIR-ANT5135D-R	5 GHz、3.5 dBi ダイポール

1. Cisco Wireless Location Appliance 2710（AIR-LOC2710-L-K9）は、2700（AIR-LOC2700-L-K9）の後継モデルです。2700 と 2710 に機能上の違いはありません。どちらのモデルも同じ機能をサポートします。

2. ロケーションベース サービスのサポートおよびサポートされるアクセス ポイントの総数に対応するライセンスが必要です。

表 1-2　その他のハードウェアおよびソフトウェア コンポーネント

AeroScout Ltd.	**System Manager**	**バージョン 3.2.20.1**
	Network Exciter Manager（ANEM）	バージョン 1.2
	EX-3100 Exciter Manager	1.0.20
	Exciter EX-2000	DSP 216、SB 50008、HW v2
	Exciter EX-3100	310.01
	Exciter EX-3200	DSP 30007、SB 60007、HW v2
	ADP-030 電源	該当しない
	ADP-040 電源	該当しない
	Tag Manager	3.0.4
	Tag Activator BWH1000-02-TA	DSP 22059、FPGA 5201、SB 175、CPLD 5107

表 1-2　その他のハードウェアおよびソフトウェア コンポーネント

	BWH-3000CT T2 RFID タグ	4.33
	EDK-200 T2 テレメトリ タグ	4.33
	ExciterConfig.exe	1.3.1

CHAPTER 2

ロケーション トラッキング アプローチ

ロケーション トラッキングと位置決めシステムは、モバイル デバイスのロケーション（*ローカリゼーション*）の特定に使用される測定技法によって分類できます。これらのアプローチには、監視下のターゲット環境におけるモバイル デバイスの位置の検知と測定に使用される特定の技法に違いがあります。一般的に、*Real Time Location System*（*RTLS; リアルタイム位置情報システム*）は、次の項目に基づいて位置を決定する 4 つの基本カテゴリに分類できます。

- 基点のセル（*最も近いセル*）
- 距離（*ラテレーション*）
- 角度（*アンギュレーション*）
- ロケーションのパターン作成（*パターン認識*）

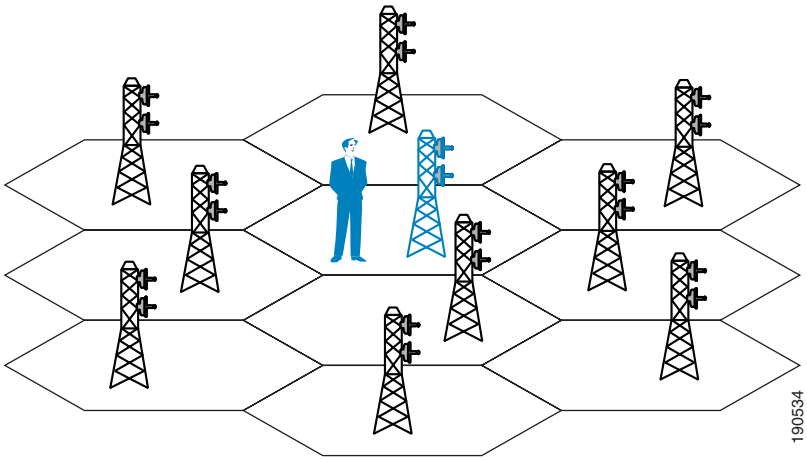
RTLS の設計者は、これらの技法から 1 つ以上を選択して実装できます。これは、伝播特性が大きく異なる複数の環境においてパフォーマンスを最適化しようとするいくつかのアプローチに見ることができます。このアプローチは人気が高く、上述の技法を少なくとも 2 つ組み合わせて位置を検知し、測定する RTLS を網羅した 5 番目のカテゴリを支持する意見もよく耳にします。

基盤となる位置決定テクノロジーの種類に関係なく、RTLS の「リアルタイム性」は、最新のタイムスタンプ、信号強度の読み取り、または受信角度の測定がリアルタイムであることにすぎません。プローブ応答のタイミング、タグ転送、およびロケーション サーバのポーリング間隔は、実際のデバイスの位置と、各報告間隔において観測される報告されたデバイスの位置の間に不一致を招く可能性があります。

基点のセル

RF の「セル」に基づくシステムでおよその位置を推測する最も単純なメカニズムの 1 つは、図 2-1 に示す基点のセル（Wi-Fi 802.11 システムでは「関連付けされたアクセス ポイント」）という概念です。

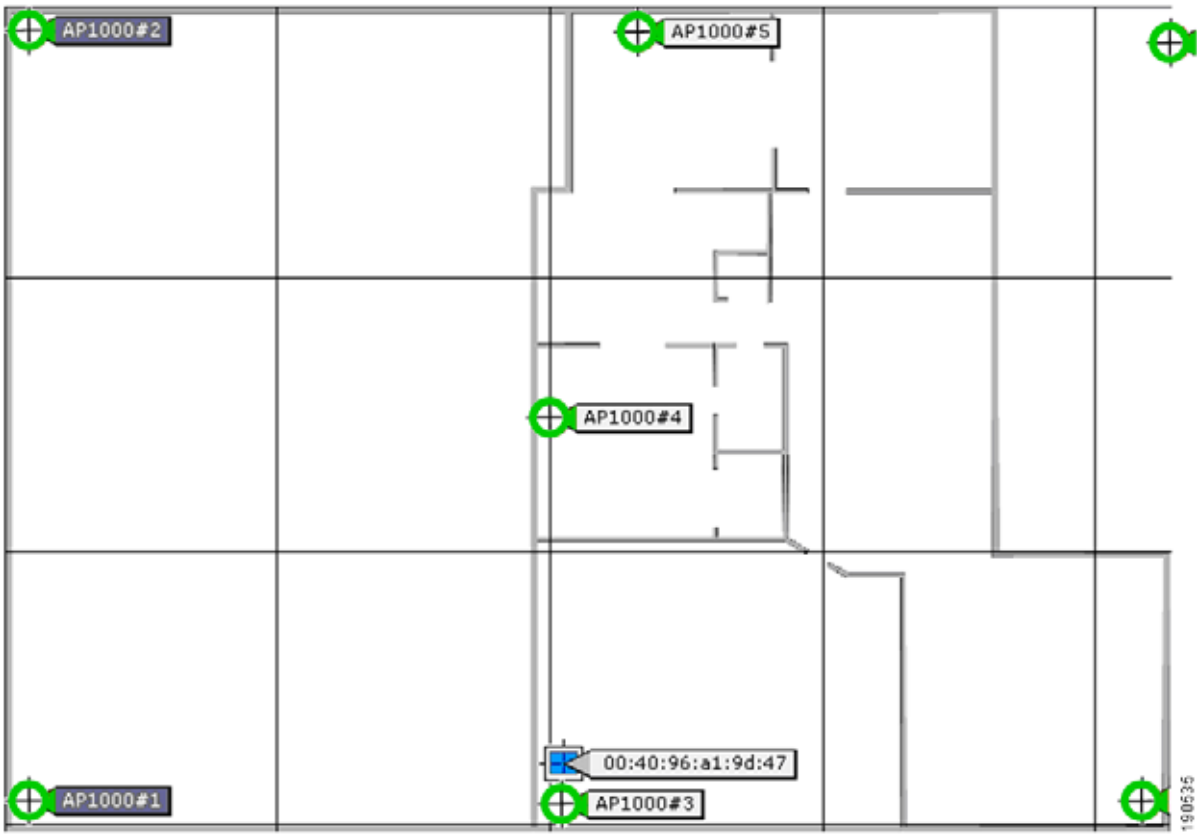
図 2-1　　基点のセル



最も単純な形の場合、この技法では、モバイル デバイスが登録されている（または登録された）セルを超えた場合、その位置を明示的に解決しようとはしません。この技法を 802.11 システムに適用すると、モバイル デバイスが関連付けられたセルが追跡されます。この技法の主な利点は、実装のしやすさです。基点のセルでは、複雑なアルゴリズムを実装する必要がなく、位置決めのパフォーマンスが非常に高速です。ほとんどすべてのセルベースの WLAN と他のセルラーベースの RF システムは、簡単にコスト効果の高い方法で、基点のセルによる位置決め機能を提供するように改造できます。ただし、純粋な基点のセルによる位置決めアプローチの重大な欠点は、精度が粗いことです。さまざまな理由から、モバイル デバイスは、近くに他にもセルがあるにもかかわらず、物理的に遠いセルと関連付けられることがあります。この精度の粗さは、フロア間でセルが重なることが多い高層構造でモバイル デバイスの実際の位置を解決しようとする場合に特に問題となります。

一般に、モバイル デバイスを含む可能性が最も高いセルの領域かを高い精度で特定するには、セル内のロケーションを解決する追加の方法が必要です。これには、手動の方法（人間がデバイスのセル全体を検索する）またはコンピュータ支援の方法があります。受信セルがモバイル デバイスの *Received Signal Strength Indication（RSSI; 受信信号強度表示）*を提供する場合、*最高の信号強度*を使用する技法により、基点のセルのロケーション精度を改善できます。このアプローチでは、モバイル デバイスのローカリゼーションは、モバイル デバイスを最高の信号強度で検出したセルに基づいて実行されます。これを図 2-2 に示します。青い四角形のクライアント デバイス アイコンが、最高の信号強度でデバイスを検出した最も近いセルに置かれています。

図 2-2　最高の信号強度技法



この技法を使用すると、純粋な基点のセルの場合より、本当に「最も近いセル」が選択される確率が高くなります。基本となるビジネス アプリケーションの精度要件によっては、モバイル クライアントの一時的な位置を探すには、最高の信号強度技法を使用したパフォーマンスで十分な場合があります。たとえば、基幹業務に関わらない状況で、間違った場所に置かれたクライアント デバイスを見つける必要がある場合だけロケーションベース サービスを使用したいユーザには、最高の信号強度アプローチを使用したソリューションが提供する価格とパフォーマンスの組み合わせで十分です。しかし、より精密なロケーションを必要とするユーザの場合、最高の信号強度技法は、セル全体をカバーする方法と比較すると、高い精度でモバイル デバイスのロケーションを突き止めることができず、それが重大な制約となることがあります。このようなユーザには、分解能と精度の高いラテレーション、アンギュレーション、ロケーションのパターン作成を使用したアプローチが適しています。これらの技法については後述します。

距離に基づく（ラテレーション）技法

到達時間

*到達時間（ToA）*システムは、モバイル デバイスから送信された信号から複数の受信センサーへの到達時間の正確な測定値に基づきます。信号は既知の速度（ほぼ光速（*c*）またはマイクロ秒あたり ～300 メートル）で伝わるので、モバイル デバイスと各受信センサーの距離は、これらの間を伝わる経過伝播時間から判断できます。ToA 技法では、非常に正確な伝送開始時間が必要です。また、すべての受信センサーとモバイル デバイスが正確な時間ソースと精密に同期している必要があります。

伝播速度と測定時間の両方がわかっている場合、次の式でモバイル デバイスと受信センサーの距離（*D*）を計算できます。

$D = c\ (t)$

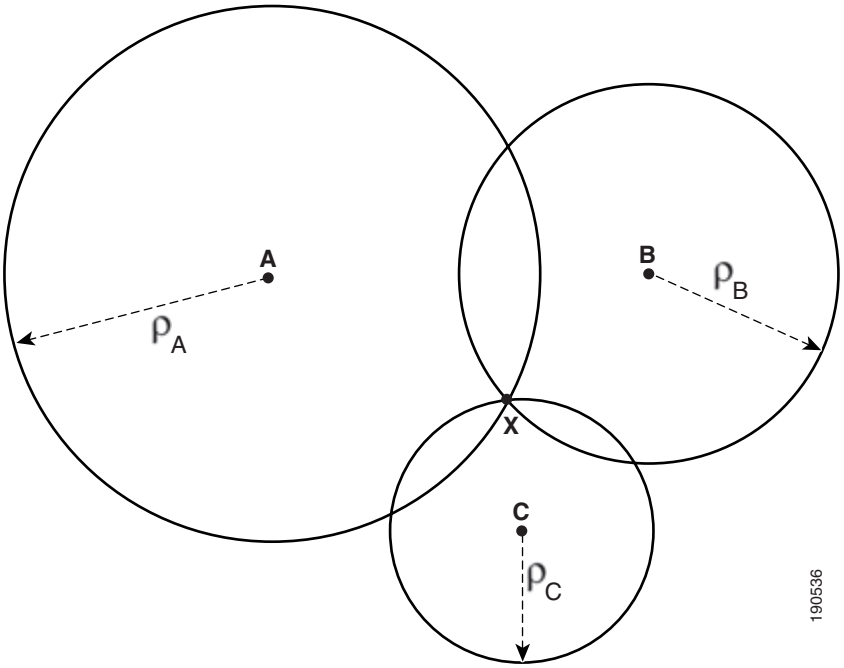
定義：

- *D* = 距離（メートル）
- *c* = マイクロ秒あたり ～ 300 メートルの伝播速度
- *t* = 時間（マイクロ秒）

モバイル デバイスが存在する可能性の高いロケーションの領域を、受信センサーを中心に距離を半径とする円で表せます。2 つのセンサーからの ToA 情報は、モバイル デバイスの位置を 2 つの同等に可能性の高いポイントに解決します。ToA *三角ラテレーション*では、3 つのセンサーを使用して、より高い鮮度でモバイル デバイスのロケーションを解決できます。

図 2-3 は、ToA 三角ラテレーションの概念を示しています。ステーション X から送信されたメッセージが受信センサー A、B、および C に到達するまでの所要時間は、t_A、t_B、t_C として正確に測定されます。伝播速度（*c*）がわかっている場合、3 つの各受信センサーからのモバイル デバイスの距離は、それぞれ D_A、D_B、D_C として計算できます。計算された各距離値は、それぞれの受信センサーを囲む円の作成に使用されます。各レシーバそれぞれの観点から、ステーション X は、この図に沿ったある場所に置かれていると考えられます。図 2-3 に示すように、3 つの円の交差がステーション X のロケーションとなります。3 つのリモート センサーを使用して三角ラテレーションを実行しても、モバイル デバイス ステーション X のロケーションに複数の解が考えられる場合があります。このような場合は、4 つ以上のセンサーを展開して、ToA *マルチラテレーション*を実行します。

図 2-3　　到達時間（ToA）



ToA 技法では、2 次元だけでなく 3 次元でロケーションを解決できます。3D の解決は、円モデルではなく球モデルを作成して実行できます。

ToA アプローチの欠点は、すべてのステーション、特にモバイル デバイスの時間を正確に同期しなければならないことです（802.11 クライアント デバイス実装にとっては厳しい課題となります）。伝播速度が高速の場合、時間同期の非常に小さなずれが、ロケーション精度の大きな誤差につながることがあ

ります。たとえば、100 ナノ秒の小さな時間測定誤差が、30 メートルのローカライゼーション誤差につながる可能性があります。一般に、ToA ベースの位置決めソリューションは、大量のマルチパス干渉、つまりノイズが存在する可能性がある環境では課題があります。

Global Positioning System（GPS）は、電波時計によって正確なタイミングが提供される、広く知られた ToA システムの一例です。

到達時間差（TDoA）

*到達時差（TDoA）*技法では、*絶対*時間測定ではなく、各受信センサーで「相対」時間測定を使用します。このため、TDoA では、タイムスタンプを解決し、ロケーションを特定するために、送信点（モバイル デバイス）で同期された時間ソースを使用する必要はありません。TDoA では、開始時間が不明の伝送がさまざまな受信センサーで受信されます。時間の同期が必要なのはレシーバだけです。

TDoA の実装は、*双曲線ラテレーション*として知られる数学的概念に基づいています。このアプローチでは、時間が同期された受信装置が少なくとも 3 台必要です。図 2-4 では、ステーション X がメッセージを送信したときに、このメッセージが時間 T_A に受信センサー A に、時間 T_B に受信ステーション B に到達すると仮定します。このメッセージの到達時間の差は、次のように、センサー B と A のロケーション間で正の定数 k として計算されます。

$$TDoA_{B\text{-}A} = | T_B - T_A | = k$$

$TDoA_{B\text{-}A}$ の値を使用して、受信センサー A と B 両方のロケーションを焦点とする双曲線を作成できます。この双曲線は、x-y 平面にあるすべての点の位置を表し、2 つの焦点からのそれぞれの距離の差は、$k(c)$ メートルと等しくなります。数学的には、次のように、モバイル デバイス X が存在する可能性のあるすべてのロケーションを表します。

$$| D_{XB} - D_{XA} | = k(c)$$

モバイル ステーション X が存在する可能性のあるロケーションは、この双曲線に沿った点で表せます。ステーション X のロケーションをさらに正確に解決するには、ロケーション C にある 3 番目の受信センサーを使用して、センサー C と A 間のメッセージの到達時間差を計算します。

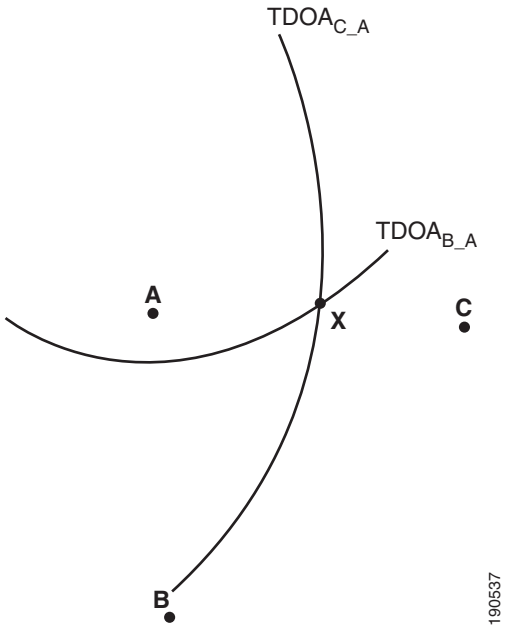
$$TDoA_{C\text{-}A} = | T_C - T_A | = k_1$$

定数 k_1 がわかると、x-y 平面にあるすべての点の場所を表す 2 番目の双極線を描けます。2 つの焦点（2 つの受信センサー A と C）からの距離の差は、$k_1(c)$ と等しくなります。数学的には、次のように、モバイル デバイス X が存在する可能性のあるすべてのロケーションを表すと考えることができます。

$$| D_{XC} - D_{XA} | = k_1(c)$$

図 2-4 は、2 つの双曲線 $TDoA_{C-A}$ と $TDoA_{B-A}$ の交差を使用して、ステーション X の位置を解決する方法を示しています。

図 2-4　　到達時間差（TDoA）



4 番目の受信センサーと 3 番目の双曲線を追加して、TDoA *双曲線マルチラテレーション*の精度を改善できます。これは、TDoA 双曲線三角ラテレーションの使用時に複数の解がある場合に必要になることがあります。

近年、TDoA システムの設計者は、TDoA レシーバの厳格な時間同期要件を回避することを目的としたローカル クロック オシレータ ドリフトに対応する方法を導き出しました。たとえば、基準クロック ソースに基づいて時間調整を定期的に計算できます。その後、これらのクロック調整を使用して、システムの他の場所の基準クロックからのオフセット用に訂正できます。パケット送信が可能な TDoA レシーバの場合（802.11 WLAN アクセス ポイントに組み込み可能な TDoA レシーバなど）、レシーバ間での「タイミング」パケットの定期交換という革新的なアプローチもあります。このアプローチでは、各レシーバと「基準レシーバ」間の時間オフセットを量子化し、それによって得られる時間調整をシステム内で適用できます。

今日使用されている TDoA システムとしてよく知られているのが、空港の測距システムです。携帯電話の世界では、TDoA は Enhanced Observed Time Difference（E-OTD）とも呼ばれ、この用途で、農村地域で約 60 メートル、RF の多い都市部で 200 メートルの屋外精度を提供します。

ToA と TDoA には、いくつかの類似点があります。どちらも、大規模な屋外位置決めシステムに非常に適していることが実証されています。さらに、円形劇場やスタジアムなどの半屋外環境や、自動車レンタルおよび新車駐車場、通関手続地などの限定的な屋外環境でも、ToA および TDoA システムは優れた結果が得られています。屋内では、TDoA システムは、全体的に障害が少なく、天井が高く、ビルの設備機器と天井の空間が広い、比較的開放的な大型ビルで最高のパフォーマンスを示します。TDoA および ToA ベースのシステムは、これらの開かれた広々とした環境で、最高の効率とパフォーマンスで動作します。

受信信号強度（RSS）

ここまでは、経過時間を使用して距離を測定する 2 つのラテレーション技法（ToA と TDoA）について説明してきました。ラテレーションは、時間の代わりに受信信号強度（RSS）を使用して行うこともできます。このアプローチでは、RSS は、モバイル デバイスまたは受信センサーのどちらかで測定します。トランスミッタ電力、ケーブル損失、アンテナ ゲイン、および適切なパス損失モデルを使用して、2 つのステーション間の距離を解決できます。

次に、屋内電波で使用される一般的なパス損失モデルの例を示します。

$$PL = PL_{1Meter} + 10\log(d^n) + s$$

定義：

- *PL* は、受信側と送信側間で発生した総*パス損失*（dB）です。この値は通常 0 以上です。
- PL_{1Meter} は、レシーバとトランスミッタの距離が 1 メートルの場合の希望周波数の*基準パス損失*（dB）です。ゼロ以上の値として指定する必要があります。
- *d* は、トランスミッタとレシーバの*距離*（メートル）です。
- *n* は、環境の*パス損失指数*です。
- *s* は、環境に存在する*シャドウ フェーディング*の度合いと関連付けられた標準偏差（dB）を表します。ゼロ以上の値として指定する必要があります。

パス損失（*PL*）は、送信側のアンテナの表面で測定された送信信号レベルと、受信側のアンテナの表面で測定された受信信号レベルの差です。パス損失は、アンテナ ゲインやケーブル損失を考慮しません。パス損失は、自由空間伝播、リフレクション、回折、散乱の影響による、環境での信号減衰レベルを表します。

パス損失指数（*n*）は、パス損失が距離とともに増加する比率を示します。パス損失指数の値は、周波数と環境によって異なり、環境に存在する障害（「ノイズ」）レベルに大きく依存します。一般的なパス損失指数の値は、開放的な自由空間の 2 から、障害が存在する環境の 2 超まで幅があります。屋内オフィス環境の標準的なパス損失指数は 3.5、密集した商業または工業地域では 3.7 ～ 4.0、住宅過密地域は 4.5 程度になります。

シャドウ フェーディング（*s*）の標準偏差は、上述のパス損失の方程式では考慮されなかったソースからの信号強度の変動の測定値を表します（「ノイズ」とも呼ばれます）。これには、存在する障害物の数、ロケーションのレシーバのアンテナとクライアント デバイスのアンテナの向きの違い、マルチパスによるリフレクションなどを原因とする減衰などの要因が含まれます。ダイバーシティ アンテナを実装すると、シャドウ フェーディングによる受信信号の変動が低減されます。この理由から、通常ダイバーシティ アンテナが推奨されています。ダイバーシティ アンテナを使用する多くの屋内設置では、一般に、シャドウ フェーディングの標準偏差は 3 ～ 7 dB です。

送信電力、パス損失、アンテナ ゲイン、ケーブル損失の数値がわかっている場合に、一般的に受け入れられているレシーバの信号強度の計算方法は次のとおりです。

$$RX_{PWR} = TX_{PWR} - Loss_{TX} + Gain_{TX} - PL + Gain_{RX} - Loss_{RX}$$

パス損失の方程式を上の方程式に直接置き換えることができます。これで、次のように距離 *d* を解決できます。

$$d = 10^{\frac{TX_{PWR} - RX_{PWR} - Loss_{TX} + Gain_{TX} - PL_{1meter} + s + Gain_{RX} - Loss_{RX}}{10n}}$$

上の方程式の用語の意味は次のとおりです。

- Rx_{PWR} は、検出された受信信号強度（dB）です。
- Tx_{PWR} は、トランスミッタ電力（dB）です。

- $Loss_{TX}$ は、送信側のケーブルおよびコネクタの損失の合計（dB）です。
- $Gain_{TX}$ は、送信側のアンテナ ゲイン（dBi）です。
- $Loss_{RX}$ は、受信側のケーブルおよびコネクタの損失の合計（dB）です。
- $Gain_{RX}$ は、送信側のアンテナ ゲイン（dBi）です。

これらすべての値は、正の値として指定します。

レシーバとモバイル デバイスの距離を解決すると、*d* を半径として、レシーバの場所の周囲に円形の領域を描けます。モバイル デバイスのロケーションは、この円形図上のある場所に存在すると考えられます。他の技法と同様、他のセルにある他のレシーバからの入力（この場合、信号強度情報または RSSI）を使用して、RSS *三角ラテレーション*または RSS *マルチラテレーション*を実行すると、ロケーションの精度が向上します。

位置の特定に使用される信号強度情報は、次の 2 つのソースのどちらかから取得できます。

- モバイル デバイスの通信を受け取った受信信号強度を報告するネットワーク インフラストラクチャ（ネットワーク側）
- ネットワークからの通信を受け取った信号強度を報告するモバイル デバイス（クライアント側）

802.11 WLAN では、RSSI が報告される精度は、通常無線ベンダーごとに異なります。実際、さまざまなシリコン メーカーが製造する 802.11 クライアント デバイスは、一貫性のないメトリックを使用して受信信号強度を報告している可能性があります。このため、ロケーション トラッキング性能が低下したり一貫性に欠けたりします。「ネットワーク側」の RSSI 測定を利用したロケーション トラッキング ソリューションでは、RSSI のすべての測定がモバイル デバイスではなくネットワーク インフラストラクチャで実行されるので、さまざまなメーカーのモバイル デバイスをサポートする場合に、この潜在的な問題を回避できます。これは、ネットワーク インフラストラクチャとエンド ユーザのクライアント モバイル デバイスの一貫性を詳細に制御できる単純なアプローチとして RSS ラテレーション ソリューションのベンダーで最も多く採用されています。

「クライアント側」の RSSI 測定に基づくロケーション トラッキング ソリューションの場合は、追加手順を実行して、一貫性のないモバイル デバイス ハードウェアによりロケーションが不正確になるのを回避する必要があります。すべてのモバイル デバイスが同じハードウェア ベンダーから提供されると仮定するのは非現実的なので、想定される「基準モデル」に沿って変動を「均等化」する方法が必要です。たとえば、ある位置決めシステムでは、報告される RSSI を、1 dBm につき 254 の増分で、-127dBm ～ +127dBm と想定しているとします。システムの一部のモバイル デバイスしか、この想定値をサポートできない場合（システムの他のデバイスは、3dBm につき 74 の増分で、-111dBm ～ +111 dBm の RSSI しか報告できない）、数学的な補償が必要です。

一般に、そのような均等化を提供する責任は、ロケーション ソリューションの提供者にあります。そのような調整は、各モバイル デバイスにインストールされる専用クライアント ソフトウェアを通して行い、すべてのモバイル デバイスをほぼ等しい一貫性で特定できるようにするのが一般的です。

今日、RSS ラテレーションを使用した実装は、モバイル デバイスまたはネットワーク インフラストラクチャのロケーションで専用ハードウェアを必要しないことから、コスト上利点があります。このため、コストパフォーマンスの観点から、信号強度に基づくラテレーション技法は、ラテレーションベースの統合型位置決めソリューションを提供しようとしている 802.11 ベースの WLAN システム設計者にとって非常に魅力的です。しかし、「純粋な」RSS ラテレーションの既知の欠点は、環境内の異方性条件によって発生する伝播の変則性が、精度を著しく低下させることです。これは、一部には、現実にセルの伝播が理想的なパス損失モデルに基づく純粋な円形パターンとかけ離れていることが原因です。「教科書的」には、理論上最も純粋な形の RSS ラテレーション モデルでは、実際のサイト内で見られる変動は測定も考慮もされず、通常よく知られたパス損失値とシャドウ フェーディング値を前提としています。

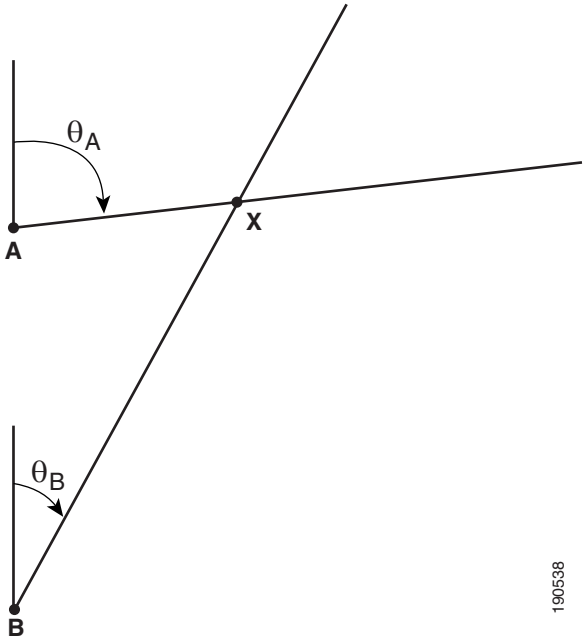
環境の減衰やマルチパスを考慮した追加手順を行わない純粋な RSS ベースのラテレーション技法では、非常に制御された状況を除いて、許容可能な結果は得られません。この制御された状況には、モバイル デバイスと受信センサー間に常に確立した明確な見通し線があり、自由空間パス損失やマルチパスからの微少な影響以外にほとんど減衰がない状況が含まれます。

角度ベース（アンギュレーション）技法

到達角度（AoA）

*到達角度（AoA）*技法は*到達方向（DoA）*と呼ばれることもあり、信号が受信センサーに到達する*入射角度*を測定して、モバイル ステーションの位置を確定します。その後、幾何学的な関係を使用して、図 2-5 に示すように、各受信センサーへの放射状の直線によって形成される 2 つの方位線（LoB）の交差からロケーションを推定できます。2 次元平面では、ロケーションの推定には、少なくとも 2 つの受信センサーが必要ですが、少なくとも 3 つ以上の受信センサー（*三角測量*）によって精度が向上します。

図 2-5　　到達角度（AoA）



最も純粋な形では（モバイル デバイス X と受信センサー A および B 間の見通し線が明確）、受信センサーに展開された機動的な指向性アンテナが、信号強度の最も高いポイントに調整されます。指向性アンテナの位置を直接使用して、LoB を特定し、入射 θ_A と θ_B の角度を測定します。

AoA の実践的な商用および軍事的な実装では、複数の要素アンテナ配列を使用して、受信信号をサンプリングすることで、複雑でメンテナンス頻度の高い機械アンテナ システムの必要性を排除しています。配列または各配列の部分間で電子交換を実行できます。また、バックグラウンド コンピューティング システムで処理される数学的な計算を使用して、入射角度が抽出されます。この技法では、実際に、各要素での受信位相の差を測定することで、配列の要素間の TDoA を計算します。適切に構築された配列では、要素ごとの到達時間はわずかながら異なり、位相に差があります。この技法は、「リバース ビーム形成」と呼ばれることもあり、各要素で信号の到達時間を直接測定し、配列要素間の TDoA を計算し、この情報を AoA 測定値に変換します。このようなことが可能なのは、ビーム形成では、各要素からの信号が時間遅延し（位相偏移）、アンテナ配列のゲインを「導く」からです。

AoA の実装としては、108.1 ～ 117.95 MHz の航空機のナビゲーションに使用される VHF Omnidirectional Range（VOR：超短波全方向式無線）システムが有名です。米国その他の地域周辺の VOR ビーコンは、複数の VHF 「ラジアル」を送ります。各ラジアルは異なる入射角度で発せられま

す。航空機の VOR レシーバは、VOR ビーコンに近づく際、ビーコンに対する入射角度により、飛行機が置かれているラジアルを決定できます。少なくとも 2 つの VOR ビーコンを使用することで、航空機のナビゲータは、オンボードの AoA レンジング装置を使って、アンギュレーション（3 つの VOR ビーコンを使う場合は三角アンギュレーション）を実行し、航空機の位置を正確に特定できます。

AoA 技法は、携帯電話産業でも、ユーザへのロケーション トラッキング サービスの提供に早期から適用されてきました。これは、主にセル システムに、緊急（911）通話をするユーザのロケーションを報告させるよう求めた法律に準拠することを目的としていました。複数のタワー サイトが、携帯ユーザの信号の AoA を計算し、この情報を使用して、三角アンギュレーションを実行します。この情報は、ユーザのロケーションを計算して AoA データを緯度と経度の座標に変換する交換プロセッサに中継されます。その後、情報は、緊急要員派遣システムに提供されます。

AoA がこれまでに説明した他の一部の技法と共有する欠点は、マルチパス干渉を受けやすいことです。前述のとおり、AoA は、見通し線が明確な場合はうまく機能しますが、周囲の物体によって信号が反射すると精度が低下します。残念ながら、密集した都市部では、複数のベース ステーションへの見通し線が存在することはまれなので、AoA はほとんど使用できません。

ロケーションのパターン作成（パターン認識）技法

*ロケーションのパターン作成*とは、特定環境での無線信号の動作パターンをサンプリングおよび記録する技法を指します。技術的に、ロケーションのパターン作成ソリューションでは、モバイル デバイスと受信センサーのどちらでも専用のハードウェアを必要としません（ただし、少なくとも 1 つのよく知られたロケーション パターン認識に基づく RTLS では、各クライアント デバイスに、「クライアント側」からそのロケーション位置決めサーバに RSSI を報告できるようにする専用の RFID タグとソフトウェアが必要です）。ロケーションのパターン作成は、すべてソフトウェアで実装でき、アンギュレーションや純粋に時間に基づくラテレーション システムと比較すると、複雑さとコストを大幅に低減できます。

ロケーションのパターン作成技法は、基本的に次のことを前提としています。

- 各デバイスのロケーション候補は、明確な固有の RF 「シグニチャ」をもつ。この仮説が現実に近いほど、ロケーションのパターン作成ソリューションのパフォーマンスは向上します。
- 各フロアまたはサブセクションは、独自の信号電波特性をもつ。同一の装置を配置しても、パターン認識 RTLS ソリューションの観点では、真に同じ特性をもつフロア、ビル、キャンパスはありません。

通常、ほとんどの商用ロケーション パターン作成ソリューションは、そのようなシグニチャのベースを受信信号強度（RSSI）にしていますが、パターン認識は、ToA、AoA、TDoA ベースの RF シグニチャを含めるように拡張できます。パターン作成に基づく位置決めシステムの展開は、通常 2 つのフェーズに分けられます。

- 調整フェーズ
- 運用フェーズ

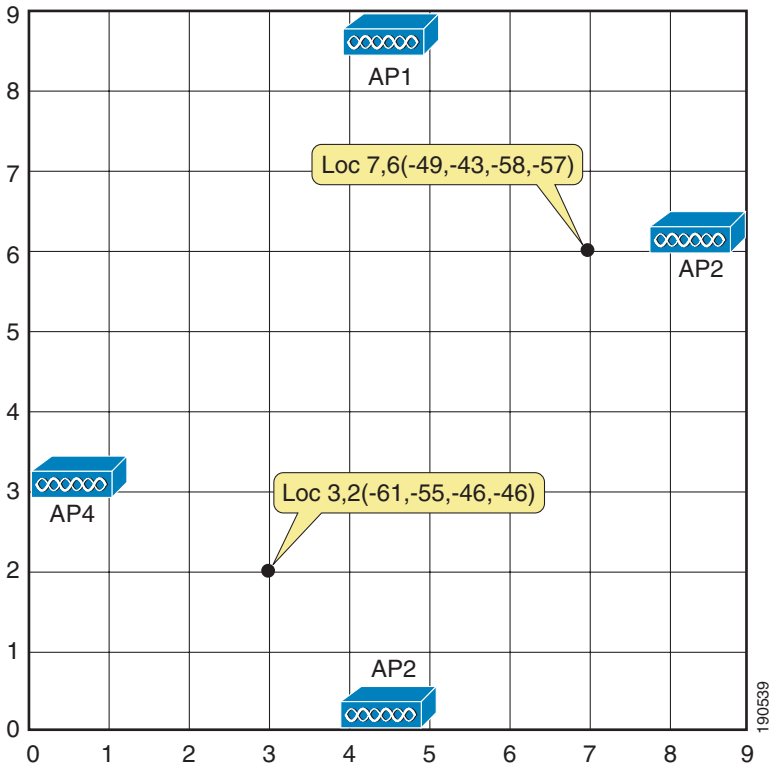
運用フェーズ中、ロケーションのパターン作成に基づくソリューションは、追跡対象のデバイスの報告された RF シグニチャを、調整フェーズ中に蓄積された RF シグニチャのデータベースと「照合」する能力に依存します。記録された RF シグニチャのデータベースは、サイトの代表的な運用期間中に蓄積されるので、調整フェーズ中の壁や他の物体からの減衰などの変動が直接考慮されます。

調整フェーズ

調整フェーズ中、データは、モバイル デバイスを持ってターゲット環境を歩き回ることで蓄積され、複数の受信センサー（802.11 WLAN の場合はアクセス ポイント）でモバイル デバイスの信号強度をサンプリングできます（ロケーションのパターン作成の「ネットワーク側」実装を指します）。

調整する地域のグラフィカル表現に、オペレータがサンプル データを取得する場所を正確に決定する指針となる一式のグリッド ポイントまたは記号が重ねられます。各サンプル ロケーションで、調整デバイスに関連付けられた RSS 値の配列（または*ロケーション ベクトル*）が、*無線マップ*または*トレーニング セット*と呼ばれるデータベースに記録されます。このサンプル ロケーションのベクトルのサイズは、モバイル デバイスを検出できる受信ステーション数によって決まります。図 2-6 は、このアプローチを簡略化したものです。2 つのサンプル ポイントと、それぞれのロケーション ベクトルが、検出されたクライアント RSSI からどのように形成されるかを示しています。

図 2-6　　ロケーションのパターン作成の調整



フェーディングや他の現象により、特定のロケーションで観測されたモバイル デバイスの信号強度は静的ではなく、時間をかけて変化すると考えられます。そのため、調整フェーズのソフトウェアは、通常、実際のサンプリング プロセス中、モバイル デバイスについて多くの信号強度サンプルを記録します。技法によっては、1 つ以上の創造的なアプローチを通して、記録された実際のベクトル配列要素でこの変動を説明できます。よく使用される、実装が簡単な方法は、特定のレシーバに関連付けられた配列要素を、報告されたサンプル座標についてその受信センサーが計測した、そのモバイル デバイスの全測定値の*平均信号強度*として表す方法です。ロケーション ベクトルは、次の方程式に示すように、*平均信号強度要素*のベクトル配列となります。x と y は報告されたサンプル座標を、r は報告された RSSI を表します。

$$(x,y) = (\overline{r}_{AP1}, \overline{r}_{AP2}, \overline{r}_{AP3}, \overline{r}_{AP4})$$

運用フェーズ

運用フェーズでは、受信センサーのグループが、追跡対象のモバイル デバイスに関する信号強度測定値を提供し（ネットワーク側報告の実装）、その情報をロケーション トラッキング サーバに転送します。ロケーション サーバは、複雑な位置決めアルゴリズムと無線マップ データベースを使用して、モバイル デバイスのロケーションを推定します。その後、サーバは、位置決め情報を要求するロケーション クライアント アプリケーションに推定されたロケーションを報告します。

ロケーションのパターン作成による位置決めアルゴリズムは、3 つの基本グループに分類できます。

- *決定論的アルゴリズム*は、検出された RSSI ロケーション ベクトルとさまざまな調整サンプル ポイントのロケーション ベクトル間の*最小統計信号距離*を検索します。これは、デバイスの実際のロケーションと調整サンプルとして記録されたロケーション間の最小物理距離と等しくない場合があります。デバイスと検出されたロケーション ベクトル間の最小統計信号距離をもつサンプル ポイントは、一般に、調整データベースに含まれる最適な未加工ロケーション推定値と見なされます。決定論的アルゴリズムの例としては、ユークリッド、マンハッタン、またはマハラノビス距離の計算に基づくものがあります。
- *確率的アルゴリズム*は、確率推論を使用して、特定のロケーション ベクトル配列が検出されている場合に、そのロケーションの可能性を決定します。調整データベースそのものは、アルゴリズムにより、特定のロケーションの可能性を決定するための*推測的*条件確率分布と見なされます。そのようなアプローチには、*ベイズ確率*推定を使用するアプローチも含まれます。
- 他の技法は、決定論的アプローチおよび確率論的アプローチの範囲を超えています。そのようなアプローチの 1 つは、ロケーションのパターン作成は複雑すぎて数学的に分析できないため、分類に非線形分別関数（*ニューラル ネットワーク*）を適用する必要があるという前提に基づいています。*サポート ベクトル モデリング*または *SVM* として知られる技法は、リスクの最小化に基づき、統計、機械学習、ニューラル ネットワークの原則を組み合わせています。

そのようなロケーションのパターン作成アルゴリズムの動作をよく理解するために、決定論的アルゴリズム（ここではユークリッド距離）を使用する例を見てみましょう。前述のとおり、決定論的アルゴリズムは最小統計信号距離を計算しますが、その値は、デバイスの実際のロケーションと調整サンプルの記録されたロケーション間の最小物理距離と等しくない場合があります。

たとえば、2 つのアクセス ポイント X と Y、およびモバイル デバイス Z があるとします。アクセス ポイント X は、x_1 という RSS サンプルでモバイル デバイス Z を報告します。ほとんど同時に、アクセス ポイント Y は、y_1 という RSS サンプルでモバイル デバイス Z を報告します。これら 2 つの RSS レポートは、ロケーション ベクトル (x_1,y_1) として表せます。調整フェーズ中、$F(x_2,y_2)$ という形式のロケーション ベクトルの大きな母集団が、ロケーション サーバの調整データベースに挿入されます。*F* は記録されたロケーションの物理座標を表します。

ロケーション サーバは、現在報告されているロケーション ベクトル (x_1,y_1) と調整無線マップの各ロケーション ベクトル間のユークリッド距離 *d* を計算できます。

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

モバイル デバイスの報告されたロケーション ベクトルとのユークリッド距離が最小となるデータベースのロケーション ベクトルに関連付けられている物理座標 *F* が、通常、モバイル デバイスの正しい推定位置と見なされます。

RSS ラテレーション ソリューションと同様、ロケーションのパターン作成を使用するリアルタイム ロケーション システムでは、ベンダーは既存の無線インフラストラクチャを利用できます。これは、実装によって異なりますが、AoA、ToA、TDoA アプローチより有利です。ロケーションのパターン作成ソリューションは、少なくとも 3 つのレシーバを常時モバイル デバイスの範囲に配置することで、屋内環境で非常に優れたパフォーマンスを発揮します。モバイル デバイスの範囲に 6 ～ 10 台のレシーバを配置すると、精度とパフォーマンスが向上します（多くの場合 5 メートルを超す精度で）。

ロケーションのパターン作成アプリケーションは、ロケーション ベクトルごとに、位置決めアプリケーションが個々のロケーションを即座に判別できる十分な配列エントリがある場合、適切に動作します。ただし、この要件は、好ましくない展開特性に寄与することもあります。ロケーションのパターン作成では、高いパフォーマンス レベルを達成するには、通常多くのレシーバ（802.11 の場合はアクセス ポイント）が必要なだけでなく、それらを緊密に配置する必要があります。クライアントがどのような場所にでも移動する可能性のある大きな領域では、調整時間が長くなることがあります。この理由から、一部の商用のロケーション パターン作成では、ターゲットのロケーション環境を、クライアントが移動する可能性がある領域、クライアントが移動する可能性はあるが、確率が低い領域、およびクライアントのロケーションの特定が不可能な領域（壁が厚いトンネル内、屋内アトリウムの開放スペースなど）にセグメント化できます。調整の量とこれら 2 つのクラスの領域に配分される計算リソースは、クライアントがその場所に置かれる相対確率に従って、位置決めアプリケーションにより調整されます。

パターン認識位置決めエンジンが使用する無線マップまたは調整データベースは、それが作成された領域固有になる傾向があり、再使用されることはほとんどありません。構造やレイアウトが同一のように見えても、2 つの領域が同じ調整データ セットを生成する可能性はほとんどありません。このため、ロケーションのパターン作成ソリューションを使用して、高層オフィス ビルの複数フロアに同じ調整データ セットを使用するのは不可能です。同じように見えても、各フロアの同じ位置で収集されたロケーション ベクトルが同じである確率は有意に低いからです。

一般に、他のすべての変数が等しい場合、ロケーションのパターン作成の精度は、調整直後に頂点に達します。そのとき、情報は最新で、環境内の状態を示します。時間が進み、RF 伝播に影響する変化が発生すると、環境の変化のレベルに従って、精度は低下する可能性があります。たとえば、大規模なクロスドッキング施設など動きの激しい物流エリアでは、30 日間で 20% の精度の低下が予測されます。調整データ マップは時間とともに精度が低下するので、高度な一貫した精度が必要な場合、ロケーションのパターン作成ソリューションでは、定期的な再検証と、可能な場合は再調整が必要です。たとえば、調整データの精度を四半期ごとに再検証したり、半年に 1 度再調整したりするのは妥当とはいえません。

CHAPTER 3

Cisco ロケーションベース サービスのアーキテクチャ

この章では、Cisco Location-Based Services（LBS; ロケーションベースのサービス）アーキテクチャについて説明します。この章の内容は、次のとおりです。

- 「RF フィンガープリント」（P.3-1）
- 「ロケーション認識 Cisco UWN アーキテクチャ」（P.3-4）
- 「Location Appliance の役割」（P.3-7）
- 「確度と精度」（P.3-12）
- 「クライアント、資産、不正なデバイスの追跡」（P.3-13）
- 「Cisco Location Control Protocol（LOCP）」（P.3-36）

RF フィンガープリント

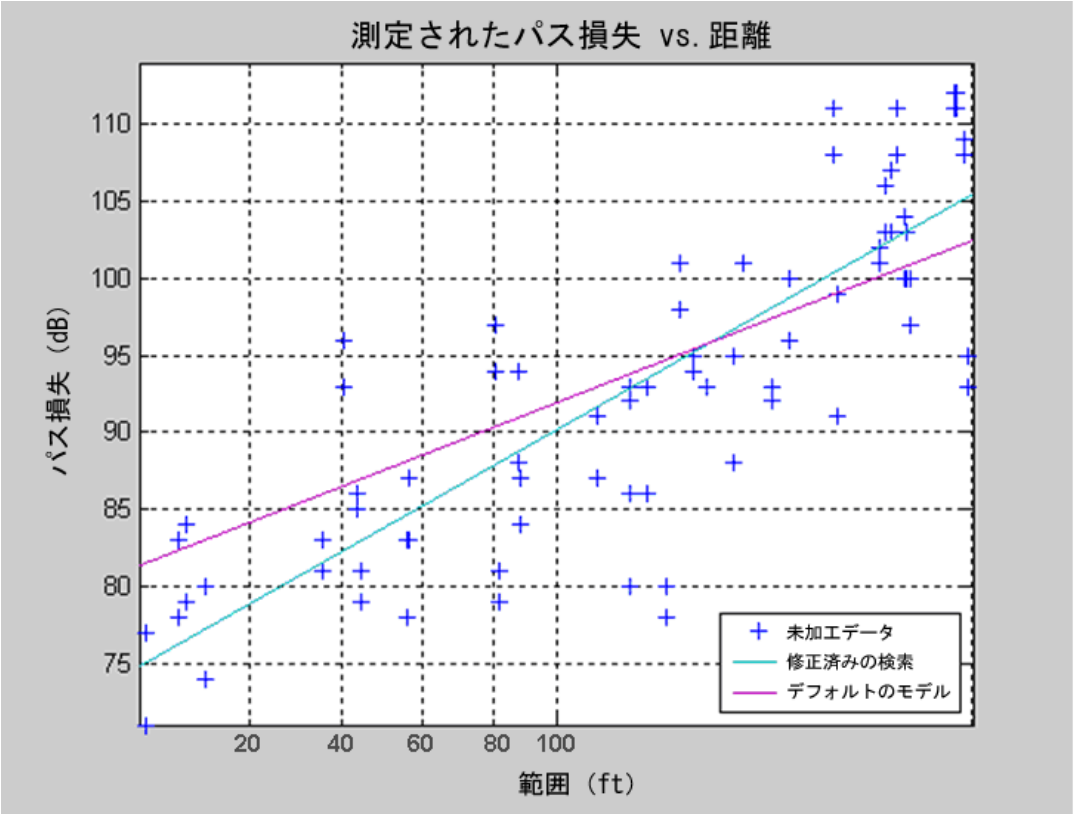
Cisco *RF フィンガープリント*は、従来の信号強度ラテレーション技法の確度や精度を大幅に向上させる、革新的で新しいアプローチです。Cisco RF フィンガープリントでは、以前、ロケーション パターン作成ソリューションでのみ使用可能であった、カスタマイズされた調整機能と屋内パフォーマンスによって、Received Signal Strength Indication（RSSI; 受信信号強度表示）ベースのラテレーション アプローチが簡略化されます。RF フィンガープリントは、対象環境または類似環境で直接収集されたデータから開発した RF 伝播モデルを使用して、RSS ラテレーションを大幅に向上させます。RF フィンガープリントには、ロケーションのパターン作成方法と同様の（ただし、より高速な）方法で RF モデルを特定の環境に調整する機能が備わっています。

あらかじめパッケージ化された伝播モデルを使用するほかに、RF フィンガープリントは、オンサイトのデータ収集に基づいたカスタマイズ モデルを開発する機能を提供します。このプロセスでは、2.4 GHz および 5 GHz のパス損失モデルの導出時に、実際の環境での全体的な減衰特性を考慮に入れることができます。各調整グリッド位置で、調整クライアントの物理的ロケーション座標（調整オペレータにより提供される）は、3 箇所以上の LWAPP 対応アクセス ポイントからのクライアント RSSI とともに記録されます。

調整フェーズの間に蓄積されたデータは、統計的処理が行われて、調整された後、各アクセス ポイント周辺の追跡対象デバイス RSSI の予測に使用する RF 伝播モデルの構築に使用されます。ここで、環境内に存在する特定の伝播異常をよりうまく反映するように、サンプル調整データからパス損失指数、シャドウ フェーディングの標準偏差、PL_{1meter} 値が計算されます。このプロセスはいくつかの演算サイクルからなり、前述したパラメータが帯域ごとに計算されます。図 3-1 に示すように、Minimum Mean Square Error（MMSE; 最小平均 2 乗誤差）推算方法がパラメータの*初期*値の取得に使用されます。ここで、パス損失指数は最適検索の適用可能 MMSE の線（つまり、デフォルトまたは修正済みの検索）の傾斜により表されます。ただし、RF フィンガープリント アプローチでは、ロケーション パス

の損失モデルの選択が MMSE で終わるわけではありません。ロケーション確度に関して、MMSE はむしろ、最終パス損失モデル最適化の最終目的である、帯域ごとの最終パラメータ選択の開始点としてのみ使用されます。RF フィンガープリントでは、十分なカバレッジ マッピングを提供するだけの RF 伝達モデルの副産物である、高いロケーション パフォーマンスに依存しません。

図 3-1　　MMSE 予測



RF フィンガープリントの運用フェーズの間にモバイル クライアントを検出するには、あらかじめパッケージ化された RF モデルまたは調整フェーズ時に作成されたカスタマイズ モデルのいずれかを使用して RSS マルチラテレーションを実行します。このプロセスにより、追跡対象デバイスの現在の場所を最も正確に表すことのできるデータ ポイント座標が生成されます。調整データの分布を統計分析することによって収集された追加情報が使用され、場所の確度と精度がさらに向上します。

Cisco RF フィンガープリントでは、従来のアプローチ以外に、次のいくつかの重要な利点があります。

- 既存の LWAPP 対応 Cisco Unified Networking コンポーネントの使用 : 他のソリューションとは異なり、RF フィンガープリント機能搭載のロケーション認識 Cisco UWN は、結合されたインフラストラクチャを使用した音声およびデータ サービスとともに Wi-Fi ベースの RTLS を提供します。Cisco Location Appliance は、ロケーションと統計情報の履歴をサポートし、アプライアンスごとに最大 2,500 台のデバイスを同時に追跡する、集中化された測位エンジンとして機能します。必要な場合、オプションのチョークポイント トリガーをソリューションに追加して、存在検出、プロキシミティ検出を行うことができるため、選択したハードウェアに応じて 25 フィートから 1 フィート未満の範囲内で資産タグの詳細検出が可能になります。
- 専用のクライアント ハードウェアまたはソフトウェアの開発が不要 : RF フィンガープリント機能搭載のロケーション認識 Cisco UWN は、ネットワーク側のロケーション モデルを使用します。このため、Cisco RF フィンガープリントでは、*各クライアントに専用のクライアント トラッキング ソフトウェアやロケーション対応無線 ドライバをロードすることなく*、多種多様な業界標準 Wi-Fi

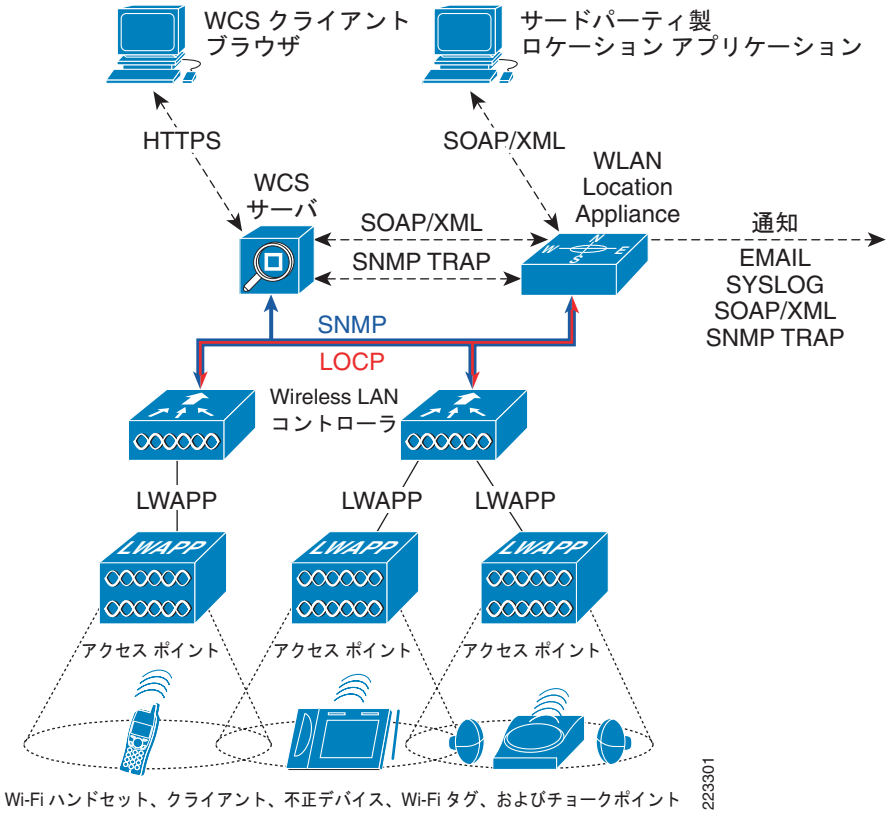
クライアント（一般的な Windows ベースのオペレーティング システムに限らず）ロケーション トラッキングを実現できます。これには、Cisco 7920 や 7921G などの一般的な VoIP 端末や、専用のアドオン ロケーション トラッキング クライアント ソフトウェアを入手できないデバイスが含まれます。

- 一般的な Wi-Fi アクティブ RFID 資産タグのサポート：ロケーション認識 Cisco UWN では RF フィンガープリントがネットワーク側のモデルとして実装されるため、RFID 資産タグ内に常駐する専用ソフトウェアには、ローカライズするための依存関係はありません。これによりロケーション認識 Cisco UWN は、AeroScout、PanGo Networks、WhereNet、G2 Microsystems、などの他の一般的なベンダーからのアクティブ RFID 資産タグと相互運用できます。Cisco Compatible Extensions Wi-Fi Tag 仕様をサポートする資産タグは、ソフトウェア リリース 4.1 で導入された拡張機能（タグ テレメトリおよびチョークポイント情報を Cisco UWN に渡すなど）を利用できます。Cisco は、Cisco Technology Development Partners（CTDP）でこの仕様を使用可能にし、仕様に準拠する相互運用可能なアクティブ RFID タグ ハードウェアの開発を促進します。
- 確度と精度の向上：Cisco RF フィンガープリントでは、純粋な三角測量技法や RSS ラテレーション技法のみを採用したソリューションよりも大幅にパフォーマンスが向上します。通常、これらの技法は、環境内の減衰の影響を考慮しないため、パフォーマンスの低下に左右されやすくなります。Cisco RF フィンガープリント テクノロジーの利点は、これらの従来のアプローチではできなかったことが開始点となります。Cisco RF フィンガープリントは、特に問題の環境に関係する場合に、まず RF 伝播をよりよく理解することから開始します。ロケーションのパターン作成の調整フェーズを除き、これまで説明してきた従来のラテレーション技法とアンギュレーション技法のどちらも、このように環境を直接考慮することはありません。RF フィンガープリントは、さらに進んで、収集された調整データのセットに統計分析技法を適用します。このことにより、Cisco Location Appliance は、非論理的なデータや異常なデータを排除し、精度を一層高めて、モバイル クライアントのロケーション予測をさらに洗練させることができます。これらの作業の結果、従来のソリューションに比べて、確度が高くなるだけでなく、精度が大幅に向上します。
- 調整作業の軽減：Cisco RF フィンガープリント テクノロジーは、屋内のロケーション パターン作成ソリューションにおいて重要な利点がありますが、システム調整に必要な作業も大幅に削減されます。両方のソリューションはオンサイト調整をサポートしていますが、Cisco RF フィンガープリント アプローチの方が、再調整の回数が少なくてすむため、ロケーション パターン作成ソリューションよりもアクセス ポイント間の距離を広げることができます。また、Cisco RF フィンガープリントは、同種の環境間で RF モデルを共有することができ、一般的な屋内オフィス環境での迅速な展開を促進するあらかじめパッケージ化された調整モデルをいくつか組み込むことができます。

ロケーション認識 Cisco UWN アーキテクチャ

ロケーション認識 Cisco Unified Wireless Network の全体的なアーキテクチャを図 3-2 に示します。

図 3-2　ロケーション認識 Cisco UWN アーキテクチャ



アクセス ポイントは WLAN クライアント、資産タグ、不正アクセス ポイント、または不正クライアントから検出した信号強度に関する情報を WLAN コントローラに転送します。アクセス ポイントの通常動作では、規制区域のためのチャネル セット内でチャネルの停止と他のチャネルのスキャンを周期的に繰り返しながら、プライマリ操作チャネル上でのこの情報の収集活動に集中します。収集された信号強度情報は、アクセス ポイントが現在登録されている WLAN コントローラに転送され、そこで情報が集約されます。Location Appliance は、SNMP を使用して各コントローラをポーリングし、追跡対象の各デバイス カテゴリの最新の信号強度情報を取得します。ロケーション トラッキング システムが Location Appliance なしで展開されている場合、WCS は、この情報を各コントローラから直接取得します。

このプロセスのフロー チャートを図 3-3 に示します。ここでは、レイヤ 2 マルチキャストを介して通信するアクティブ RFID 資産タグの信号強度とタグ ペイロード情報を示します。

図 3-3　　資産タグ RSSI データの情報フロー

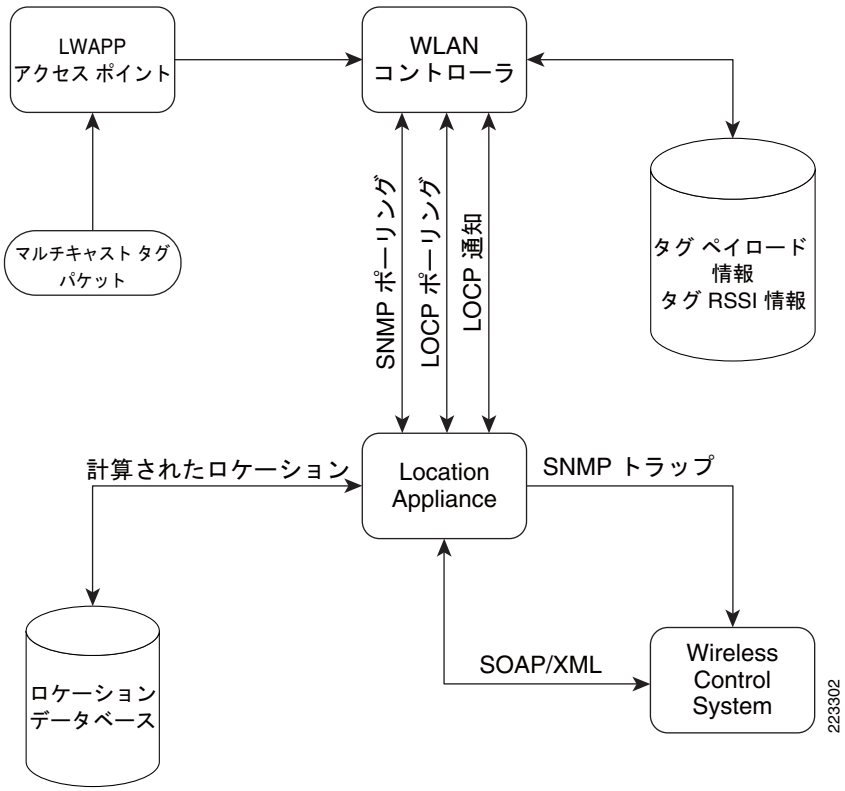


図 3-3 は以下のイベントの要約です。

ステップ 1　各タグの送信間隔で、資産タグは設定済みの各チャネル上でマルチキャスト フレームを送信します。

ステップ 2　少なくとも 3 箇所のアクセス ポイントで、資産タグの伝送を検出します。検出されると、検出中のアクセス ポイントが登録されている WLAN コントローラ（WLC）に転送されます。

ステップ 3　WLC は、資産タグ MAC アドレスでインデックス化された内部タグ情報テーブル内の資産タグに関連付けられている情報ペイロードを格納します。この情報ペイロードには、バッテリ ステータスやタグまたは資産テレメトリなどの情報が含まれています。

ステップ 4　この WLC に登録されているアクセス ポイントによってネットワーク内で検出されたタグの場合、WLC は、次の資産タグ情報を内部 RSSI テーブル内に配置します。

a.　タグの MAC アドレス

b.　AP の MAC アドレス

c.　AP インターフェイス

d.　RSSI 測定

ステップ 5　Location Appliance は SNMP を使用して、WLC でタグ RSSI テーブルの内容を定期的にポーリングします。

ステップ 6　Cisco UWN ソフトウェア リリース 4.1 の使用を開始する場合、Cisco Location Control Protocol（LOCP）を使用して、WLC でタグ情報テーブルの内容をポーリングします。

ステップ 7　Location Appliance は、RSSI 情報を使用して資産タグの位置を計算し、ロケーション情報をデータベースに格納します。

ステップ 8　Location Appliance は、すべてのノースバウンド通知（SNMP トラップ、電子メール、更新された資産タグの位置に基づいた syslog または SOAP/XML メッセージなど）を送信します。

ステップ 9　ロケーション エンド ユーザは WCS（またはサード パーティのロケーション クライアント）を使用して、フロア マップまたは検索条件に基づいてロケーション情報を要求します。ロケーション情報の要求は、SOAP/XML オンライン クエリーを介して Location Appliance に対してロケーションから行われます。

ロケーション認識 Cisco UWN ソフトウェア リリース 4.1 から、LOCP では、WLAN コントローラから Location Appliance に対して高優先順位のメッセージを非同期的に送信できるようになりました。このカテゴリに含まれるのは、タグのコール ボタン アラート、チョークポイント プロキシミティ、およびベンダー固有のタグ ペイロードなどの高優先順位のタグ イベントです。

WCS と Location Appliance は、「*同期化*」と呼ばれるプロセス時に（調整マップやネットワーク設計などの）情報を交換します。このプロセス時、最新の情報を処理するパートナーによってもう一方のパートナーが更新されます。同期化は、オンデマンドでまたはスケジュール済みタスクとして実行され、そのタイミングは、Cisco Wireless Control System（WCS）メイン メニュー バーの [Administration] > [Scheduled Tasks] メイン メニュー オプションで決定されます。

ロケーション情報は、Cisco Wireless Location Appliance とともに*ロケーション クライアント*アプリケーションを使用すると、エンド ユーザに表示されます。通常、この役割は Cisco WCS が果たします。これについてはこのマニュアルの後の項で説明します。ロケーション クライアントとして、Cisco WCS は、クライアントの現在および過去の位置、資産タグ、不正アクセス ポイント、および不正クライアントに関する多数の情報を表示できます。

（注）　WCS と Cisco Wireless Location Appliance のバージョン間の互換性については、次の URL にある『*Release Notes for Cisco Wireless Location Appliance Release 3.0*』を参照してください。
http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html

ロケーション クライアントの機能は WCS に限定されません。Cisco Location Appliance Application Programming Interface（API）に準拠して作成されたサードパーティ製アプリケーションも、Wireless Location Appliance のロケーション クライアントとしての役割を果たします（図 3-2 を参照）。WCS で使用可能な Location Appliance に含まれているものと同じ情報（資産タグから受信したベンダー固有の情報も含む）を、Location Appliance API を介してサードパーティ製ロケーション クライアントも使用できるようになります。

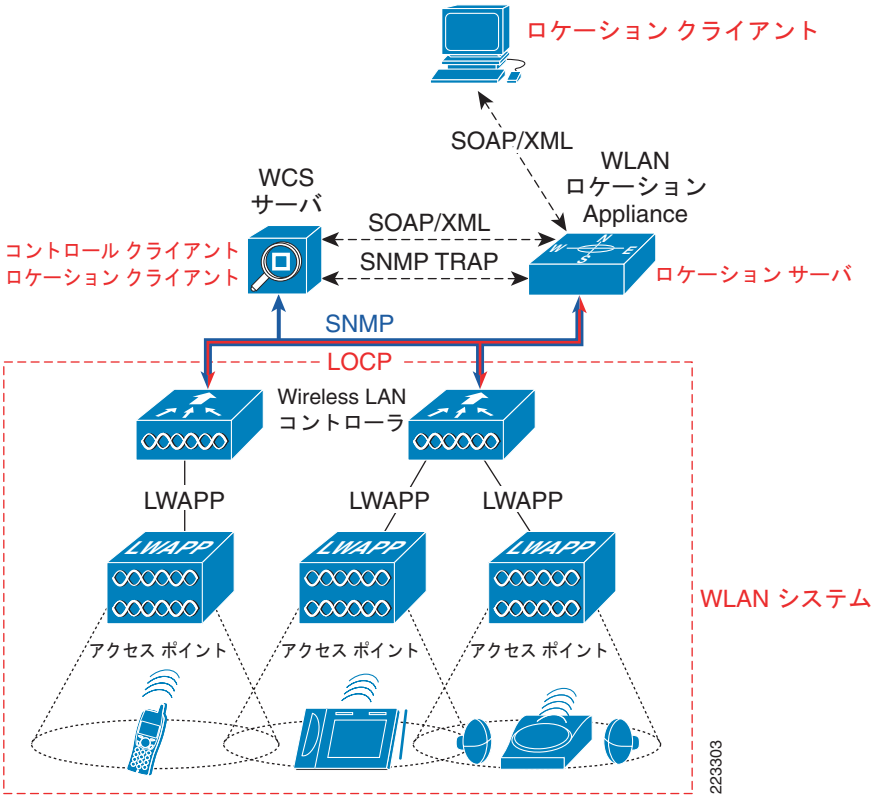
サードパーティ製のロケーション クライアントは、WCS と同様の方法でネットワーク設計を Location Appliance と同期できます。この場合、Location Appliance は、ネットワーク設計とマップ イメージについて最新の情報を使用してロケーション クライアントを更新します。WCS について、同期はオンデマンド、またはスケジュールに基づいて行われます。同期のタイミングは通常、ロケーション クライアント内に含まれる設定パラメータによって決定されます。

Cisco Location Appliance も、電子メール（SMTP）、syslog、SNMP トラップ、または SOAP/XML プロトコルを介して外部システムにノースバウンド通知を発行できます。これらのノースバウンド通知の発行は、1 つ以上のさまざまなイベントの発生に依存します。詳細については、このマニュアルの後の項で説明します。

Location Appliance の役割

ロケーション認識 Cisco UWN は、図 3-4 に示すように、4 つの基本コンポーネント グループに分類できます。

図 3-4　ロケーション認識 Cisco UWN のコンポーネント



- *ロケーション クライアント*：ロケーション クライアントの主要な役割は、ロケーション サーバに保存されたロケーションおよび資産情報へのインターフェイスとして機能することです。1 台以上のロケーション クライアントは要求に応じて情報を受信します（「pull」モード）。または、事前定義済みの条件に従い、ロケーション サーバからの定期的な情報送信を待機するリスニングの役割を果たします（「push」モード）。
- *WCS*：WCS は Location Appliance に対するデフォルト ロケーション クライアントとして機能し、ほとんどの IT セントリックの、およびネットワーク監視の要件を満たすことのできるロケーション表示機能を提供します。Location Appliance API から提供された柔軟性により、サードパーティ製ロケーション クライアントが、WCS を補完する形で UWN に常駐することができます。これらのサードパーティ製品は、資産管理に焦点を絞り、RFID、ローカリゼーションおよびネットワーク管理にはあまり重点を置かない、ビジネスに焦点を当てた UI を提供します。
- *コントロール クライアント*：コントロール クライアントは、ロケーション サーバの管理ができ、ロケーション サーバ上のすべてのロケーション データおよび設定データの読み取りおよび書き込みができます。ロケーション認識 Cisco UWN では、コントロール クライアントの役割は Cisco WCS によって実行されます。コントロール クライアントの主要な機能は、物理環境についての情報（ネットワーク設計、フロア マップ、調整モデル、アクセス ポイントのロケーションなど）および監視すべきネットワーク要素をサーバに入力することです。コントロール クライアントは、ネットワークに展開されている 1 台以上のロケーション サーバに対する管理機能も持っています。

- *ロケーション サーバ*: ロケーション サーバはネットワークまたはネットワークの一部（*ロケーション ドメイン*）向けの一般的なロケーション サービスを提供し、クライアント ロケーションを予測するアルゴリズムの実行を主に担当します。ロケーション サーバは、ロケーション履歴情報も保管します。ロケーション サーバは、複数のロケーションまたはコントロール クライアントと通信を行うことができます。ロケーション認識 Cisco UWN では、Cisco Wireless Location Appliance がロケーション サーバの役割を果たします。Cisco Location Appliance も、電子メール（SMTP）、syslog、SNMP トラップ、または SOAP/XML プロトコルを介して外部システムに通知を発行できます。
- *無線 LAN システム*：無線 LAN システムは次のもので構成されています。
  - WLAN コントローラ内に含まれる組み込みソフトウェア。ステーション / タグ / 不正検出、デバイスの トラッキングおよび統計情報に関する情報への集約ポイントとして機能します。
  - モバイル デバイス（タグ、モバイル ステーション、不正クライアント、および不正アクセス ポイント）。無線ネットワークおよびロケーション認識 Cisco UWN が監視するロケーションとやりとりします。
  - オプションのインフラストラクチャ コンポーネント（チョークポイント トリガーなど）。アクティブ RFID タグから利用可能な機能を拡張し、これらの資産タグのローカリゼーションでの精度を高めます。

コンソール セッションを介して直接 Location Appliance にアクセスすることは可能ですが、すべてのエンドユーザの Location Appliance との対話は、通常、WCS またはサードパーティ製のロケーション クライアント アプリケーションを介して行われます。

Cisco Location Appliance を Cisco Unified Wireless Network アーキテクチャに統合すると、すぐに Cisco UWN のベースライン機能に加えて、ロケーションの改良が可能になります。たとえば、次のものがあります。

- *スケーラビリティ*：Cisco Location Appliance を追加すると、ロケーション認識 Cisco UWN でスケーラビリティが著しく増加し、オンデマンド トラッキングできるデバイス（WLAN クライアント、RFID タグ、不正アクセス ポイント、および不正クライアント）の台数が、1 台から最大 2,500 台まで増加します。企業内で 2,500 台を超えるデバイスをトラッキングする必要のある状況に対処するには[1]、追加の Location Appliance を展開できます。特定のコントローラを各アプライアンスに割り当てることによって、設計を分割できます。各アプライアンスは、最大 2,500 台のデバイスに対して、ロケーション ドメイン内のコントローラおよびアクセス ポイントのトラッキングを行います。また、共通 WCS によって管理されます。
- *チョークポイント ロケーション*：ソフトウェア リリース 4.1 または後続リリースでの Cisco Location Appliance の追加により、AeroScout や WhereNet などの Cisco テクノロジー パートナーからのオプションのチョークポイント トリガーが使用できるようになります。これらのデバイスは 1 フィート未満から 12 フィートを超える範囲で、精度の高い資産タグのロケーションをサポートします。
- *履歴および統計情報*：Location Appliance は、ロケーションと統計の履歴情報を記録および管理します。これらの情報は、WCS を介して表示できます。
- *ロケーション通知*：Cisco Location Appliance は、電子メール（SMTP）、syslog、SNMP トラップ、および SOAP/XML を介してロケーションベースのイベント通知を特定の宛先に直接送信できます。クライアントまたは資産が次の条件に合致したときに、これらの通知をトリガーできます。
  - ロケーションが変化する
  - 事前に決定されたマーカー位置から設定距離を逸脱する
  - 行方不明になる、またはカバレッジ領域に入る / 離れる
  - バッテリ レベルが変わる

1. 追跡対象デバイスがロケーション ドメイン間をローミングすると、集約された追跡対象デバイスのキャパシティは減少します。

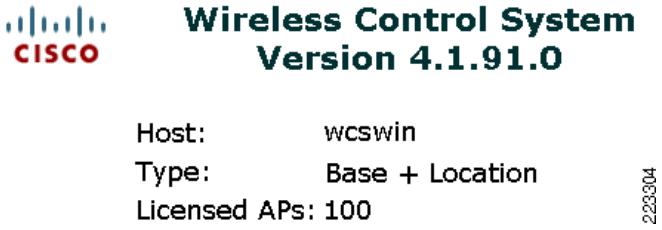
  - チョークポイント トリガーの「スティミュレーション ゾーン」に入る
  - 以下の 1 つ以上のプライオリティの条件に該当する
    - タグのボタン呼び出しの抑制
    - タグの資産からの剥離
    - 内部改ざんの試み
- SOAP/XML Location Appliance Application Programming Interface（API）: Location Appliance API によって、顧客とパートナーは、Cisco Wireless Location Appliance と対話するロケーションベース プログラムを作成できます。リアルタイムのロケーションベースのデータ取得、テレメトリでのデバイス管理、ワークフローの自動化、拡張された WLAN セキュリティ、ユーザまたはデバイスの追跡を含む、革新的な独自のアプリケーションをサポートするために、これらのプログラムを開発できます。API は、SOAP/XML インターフェイスを使用して、Cisco Wireless Location Appliance 設定データベースからのデータを挿入、取得、更新、削除するためのメカニズムを提供します。開発者は、Cisco Wireless Location Appliance プロビジョニング サービスにアクセスして、XML 形式でデータを交換できます。Location Appliance API は、ソリューション開発を促進するためのツールと共に、シスコ開発コミュニティで入手できます。Cisco Developer Services Program （サブスクリプションベースのサービス）を介して統合サービスを利用できます。

（注） Cisco Developer Service Program についての詳細は、次の URL にある Cisco Developer Support Web サイト を参照してください。
http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

Location Appliance を使用しないロケーション トラッキング

Cisco UWN の任意の RF フィンガープリントベースのロケーション トラッキング機能にアクセスするために、または Cisco Wireless Location Appliance を設定するためにも、Cisco WCS はロケーションで使用するために適切なライセンスが付与されている必要があります。ロケーション ライセンス版の WCS が使用されている場合（WCS メイン メニュー バーのオプション [Help] > [About the Software]、図 3-5）、チョークポイントベース以外のロケーションの特定に RF フィンガープリントが使用されます。ロケーション ライセンス版の WCS で Location Appliance が使用されていない場合、追跡対象デバイスのロケーションの特定に引き続き RF フィンガープリントが使用されます。ただし、オンデマンドのみ、および一度に 1 台の追跡対象デバイスに限られます。

図 3-5　ロケーション ライセンス版の WCS



Location Appliance を使用せずに、ロケーション ライセンス版の WCS を使用した場合、次の機能が使用できなくなります。

- Cisco Wireless Location Appliance を設定する機能
- ロケーション データの履歴の蓄積、再生
- タグ テレメトリおよび高優先順位通知

- チョークポイント ロケーション
- SOAP/XML API を介して外部のサードパーティ製アプリケーションとやりとりする機能
- フロア マップ上にある複数のデバイスの同時トラッキング ロケーション トラッキング サービスは、オンデマンド サービスとしてのみ、また一度に 1 台のデバイスでのみ、使用できます。図 3-6 に、1 台の WLAN クライアントに対するオンデマンド ローカリゼーションの使用を示します。このようにオンデマンド ローカリゼーションを使用する場合、デバイス アイコンの周囲の色は、アイコンの配置に関連付けられたロケーション エラーの度合いを示していることに注意してください。アイコンの周囲の濃いめの色は、信頼性が高い領域を表します（デバイスが、アイコンが配置されている、またはこの領域内にあるという確率が高くなります）。薄めの色は、信頼性が低い領域を表します（デバイスが、これらの領域内に物理的に配置されているという確率が低くなります）。

図 3-6　ロケーション ライセンスを持つ WCS を使用するオンデマンド WLAN クライアント ローカリゼーション

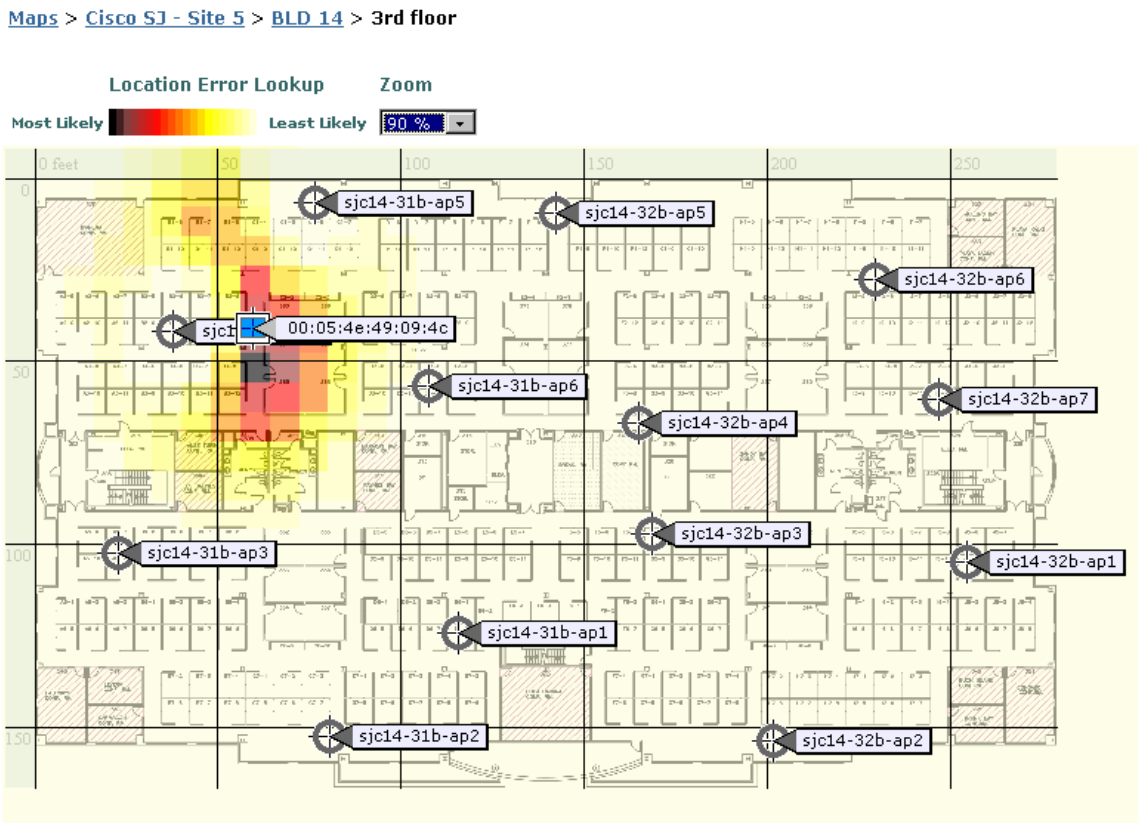
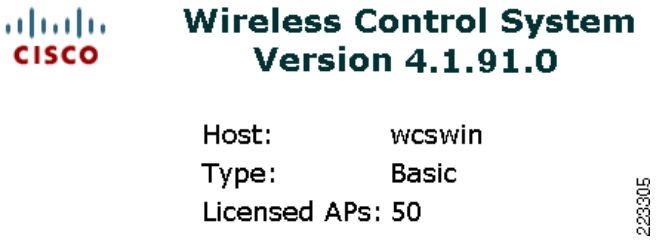


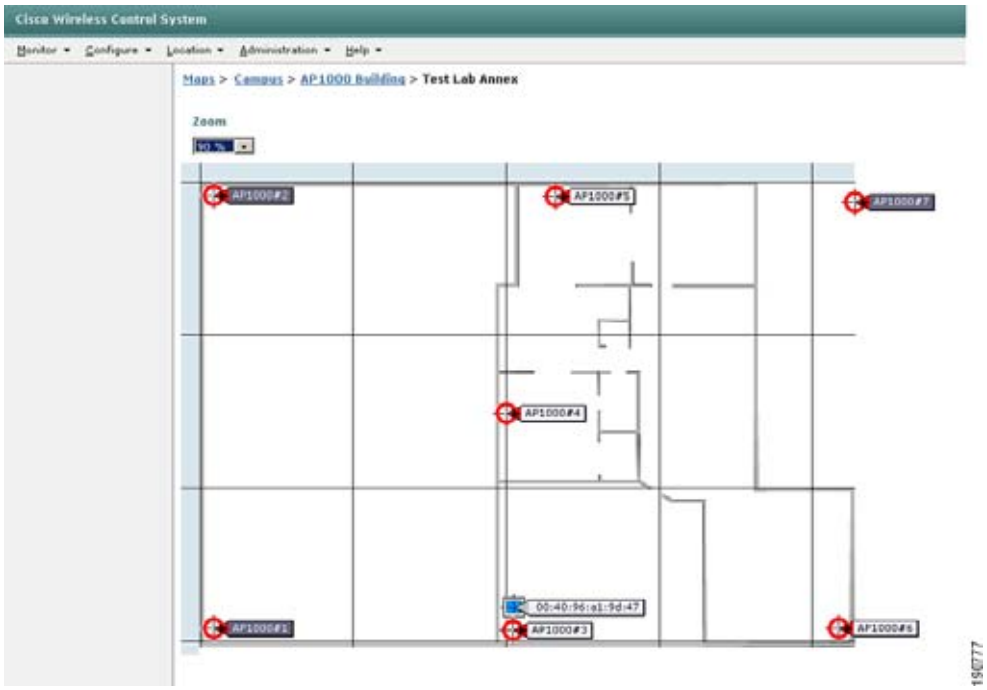
図 3-7 に示すように、WCS に基本的な機能のみがライセンス付与されている場合は、ロケーションの特定に RF フィンガープリントは使用されません。その代わり、1 台の WLAN クライアント、または不正デバイスに対するオンデマンド ロケーションがアクセス ポイントに基づいて実行されます。このアクセス ポイントは最も高い信号強度（*最近隣アクセス ポイント*概念から導出）でモバイル デバイスを検出します。

図 3-7　基本的な機能のみライセンス付与されている WCS



このアプローチを使用する場合、追跡対象デバイスのロケーションは、図 3-8 に示すように、最も高い信号強度でデバイスを検出するアクセス ポイントの位置にあるデバイス アイコンの配置により近似されます。この場合、ロケーションの確率は表示されません。

図 3-8　基本的なライセンスを持つ WCS を使用するオンデマンド クライアント ローカリゼーション



（注）　ロケーション ライセンスが付与されていない WCS サーバは、Cisco Wireless Location Appliance のロケーションまたはコントロール クライアントとして使用できません。Cisco UWN ソフトウェア リリース 4.1 の使用を開始する場合、ロケーション ライセンスが付与されていない WCS を使用しているときは資産タグのオンデマンド ロケーション トラッキングを行うことはできません。

確度と精度

ほとんどのユーザの場合、もっともよく知られており、重要性の高いパフォーマンス基準は*確度*です。これは通常、受信している情報の品質を表します。*ロケーションの確度*とは、特にトラッキング デバイスの予測位置と実際の位置の定量化可能な誤差を意味します。

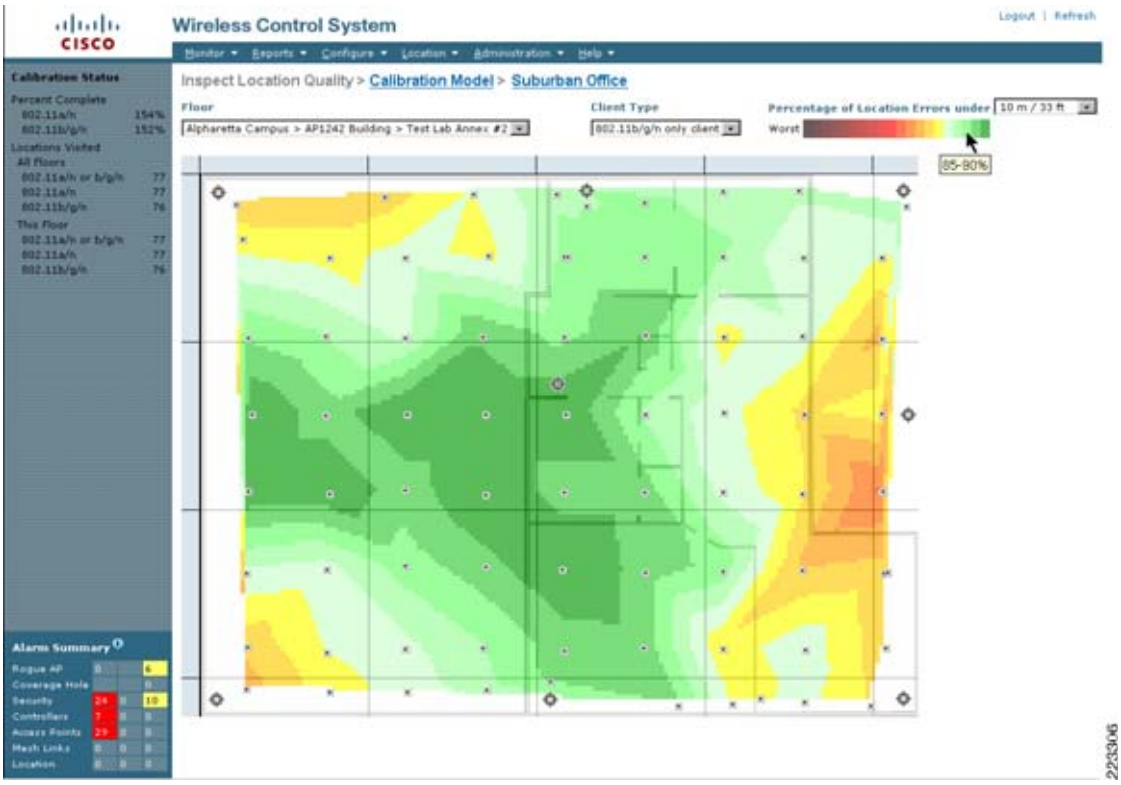
ただし、実際の用途では多くの場合、ロケーションの確度の記述は、ソリューションがそのレベルで何回も確実に実行できなければあまり価値がありません。*精度*はロケーション確度の記述の再現可能性に反映される直接的な指標です。ロケーション確度の記述には、信頼区間または成功したロケーション検出の確率に関する記述（*ロケーション精度*）も含める必要があります。

このマニュアルで説明したベスト プラクティスに準拠した展開を行うと、ロケーション認識 Cisco UWN は基本パフォーマンス仕様（最低 10 メートルの確度、90% の精度）を満たすことができます。チョークポイント ロケーション サポートと組み合わせると、チョークポイント ロケーション機能を持ち、Cisco Compatible Extensions Wi-Fi Tag 仕様に適合する資産タグのパフォーマンス レベルを高くすることができます。展開された特定のチョークポイント トリガーの設定済み範囲によっては、ロケーション解決半径を 1 フィートにすることができます。

この Location Appliance の基本パフォーマンス レベルは、ベスト プラクティスに従い、このマニュアル、および他の参考文献に記述した設計、調整、および展開ツールを使用して実現できます。これらのツールには、*Location Planning* および *Location Readiness* ユーティリティなどの展開前の予測ツールと、*Location Inspection* ツールなどの展開後のツールがあります。

基本パフォーマンスの改善が必要となる領域を特定するには、Location Inspection ツール（図 3-9 を参照）を使用して、環境内の現在、調整後の確度と精度のレベルを評価できます。Location Inspection ツールは（色分けされた形式で）、0 ～ 5% から最大 95 ～ 100% のあらゆる精度レベルを表示します。結果を参照後、システム アーキテクトはインストール チームおよび展開チームと協力して、システムのパフォーマンスが十分であることを確認するための必要な手順を行うことができます。

図 3-9　調整後のロケーション調査



これらのツールを使用すると、システム アーキテクトとインストール チームは、定められたパフォーマンス目標の達成のために計画するだけでなく、これらの目標が実際に達成されているかどうかを確認できます。

ロケーションのパフォーマンスの調整などを含む専門的なサービスの提供に関心がある場合、シスコでは Wireless LAN Location Planning and Design Professional Services を提供しています。このサービスでは、セキュリティで保護されたロケーションベースのサービス ソリューションの適切な展開に Cisco が重要と認識するサービスを含む統合ソリューションを提供するために、訓練された WLAN エンジニアのスキルを活用しています。

Cisco Wireless LAN Location Planning および Design Professional Services の詳細は、次の URL にある Cisco Wireless LAN Services Web サイトを参照してください。

http://www.cisco.com/en/US/products/ps8306/serv_home.html

クライアント、資産、不正なデバイスの追跡

ここでは、WLAN クライアントのプローブ メカニズムの背景にあるメカニズムについて説明し、クライアント プローブの変化がロケーションの確度にどのような影響があるかについて説明します。さらに、Cisco Compatible Extensions ロケーション測定の詳細、および WCS 内に存在するロケーション クライアントごとに、どのようにそれぞれのデバイス カテゴリのロケーションが表示されるかについての詳細についても説明します。

クライアント プローブ

基本的に、WLAN クライアントのロケーションは、アクセス ポイントによって検出されたプローブ要求の RSSI に基づいて特定され、登録された WLAN コントローラを介して Location Appliance に転送されます。そのため、WLAN とネットワーク内の不正クライアントのプローブ動作は、Location Appliance が正確なロケーション トラッキングを行う機能に重大な影響があると予測されます。

一貫性のある、定期的なネットワークのプローブは、WLAN クライアント ロケーションの忠実度を保つために重要であるため、このプロセスのメカニズムを理解することは重要です。プロセスは、近隣に 802.11 ネットワークが存在するかどうかを検出するためのプローブ要求を発行するクライアントによって開始されます。アソシエートされていないクライアントは、プローブ要求を定期的に生成する傾向がありますが、ネットワークに現在関連付けられているクライアントは、通常、プローブ要求をそれほど発行する傾向にありません。関連付けられているクライアントは、アクセス ポイントやネットワークが環境にないか定期的にチェックします。クライアントはこのアクセス ポイントやネットワークを*スキャン*と呼ばれるプロセスを通してローミングします。*アクティブ スキャン*では、クライアントはプローブ要求を発行し、圏内のアクセス ポイントからプローブ応答を要請します。これらの応答から、クライアントはアクセス ポイント ローミング候補のリストを生成します。ただし、クライアントはリッスンのみのアプローチを採用し、クライアントの近隣にあるアクセス ポイントから受信したビーコンとプローブ応答を記録するだけで、実際にこれらの応答を要請することはありません（*パッシブ スキャン*）。アクセス ポイント ローミング候補を特定するためにパッシブ スキャンを使用するクライアントはプローブ要求を発行しないため、パッシブ スキャン自体は、ロケーションの忠実度を向上させるうえでほとんど効果がありません。一部のクライアントが 両方の技術を組み合わせて使用することはよくあります。

ロケーション認識 Cisco UWN は、クライアント プローブを使用してクライアント ロケーションを特定します。クライアントがより一貫性のあるプローブ応答の転送を行えば、システムでそのクライアントのロケーション トラッキングをより正確に行うことができるというロジックに従っています。たとえば、クライアントが次の状態に該当する場合、ロケーションの確度は下がります。

- 長期間、アクティブ スキャンをしていない
- 使用中のすべてのチャネルにプローブ要求を送信しない
- すべての設定済み SSID にプローブ要求を送信しない
- RTLS で予期される値から異常に逸脱した電力レベルでプローブ要求を送信する

IEEE 802.11 規格では、これらの領域の解釈は未定義です。このため、複数のベンダー間で一貫性のあるプローブ動作が行われません。Cisco UWN の WLAN クライアント ロケーション忠実度の観点から、これには良い意味と、あまり良くない意味があります。一部のクライアントが、アクティブ スキャンを実行してプローブを定期的に発行する一方、その他のクライアントはそれほどプローブを実行しません。

Cisco Compatible Extensions ロケーション測定

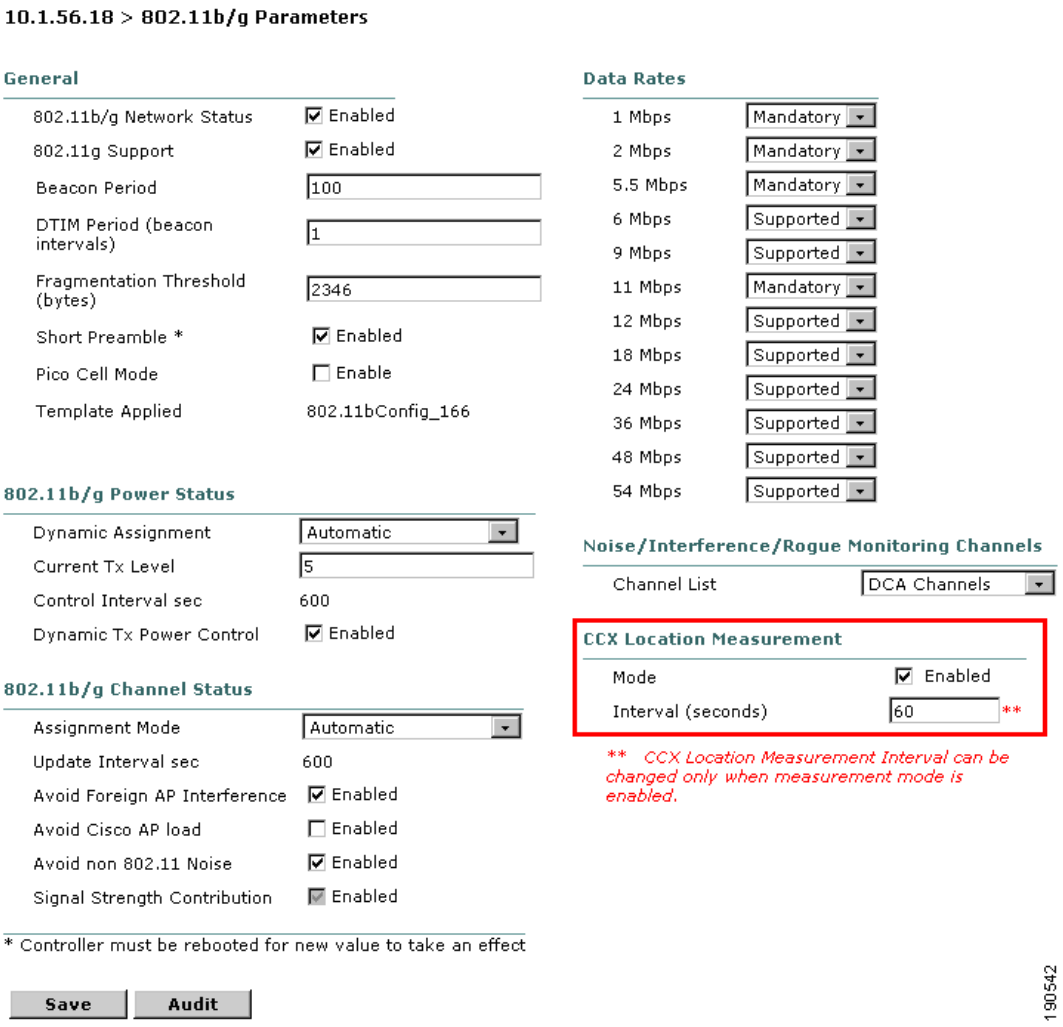
クライアント プローブの変化の影響は、Cisco Compatible Extensions WLAN デバイス仕様バージョン 2 以降に準拠したクライアントを標準にすることによって大幅に削減されます。Cisco Compatible Extensions WLAN デバイス仕様バージョン 2 で導入された S36 無線測定要求[1] をサポートする互換性のあるクライアントは、アクティブ スキャンを実行し、コマンド実行時にすべての設定済み SSID をプローブします。この機能のサポートにより、クライアントは Cisco Compatible Extensions ロケーション測定などの機能に参加できます。この機能が有効な場合、登録された Lightweight アクセス ポイントは、有効な各 SSID と無線インターフェイスを介して、無線測定要求フレームを関連付けられたクライアントにブロードキャストします。設定可能な間隔は、60（デフォルト）～ 32,400 秒（図 3-10 を参照）。

各無線測定要求には、無線測定要求内で指定されたチャネル上のプローブ要求を送信することによって、応答する互換性のあるクライアントを取り出す、ビーコン要求が含まれています。メカニズムに備わる一貫性により、このメカニズムを装備したクライアントのロケーション確度が高まります。ソフトウェア リリース 4.1 では、DFS チャネルは無線測定要求に含まれていないことに注意してください。

WCS またはコントローラ GUI を使用すると、各 WLAN コントローラ上の無線インターフェイス タイプ（802.11bg や 802.11a など）ごとに Cisco Compatible Extensions ロケーション測定を有効または無効にできます。WCS テンプレートを使用すると、コントローラ全体でグローバルに有効または無効にすることもできます。場合によっては、Cisco Compatible Extensions ロケーション測定パラメータに対して（特定の領域でテストを実行する場合など）より詳細な制御を行うことが適切な場合もあります。このようなケースに対処するために、WLAN コントローラ CLI では、必要な場合、Cisco Compatible Extensions ロケーション測定機能を特定のアクセス ポイントにのみ適用できます。WLAN コントローラ CLI を使用した Cisco Compatible Extensions ロケーション測定の詳細は、次の URL の『*Cisco WLAN Controller Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/wireless/controller/4.1/configuration/guide/c41rrm.html#wp1121089

1. これは、WLAN デバイス向け Cisco Compatible Extensions の *RF Scanning and Reporting* カテゴリに含まれている機能の 1 つです。Cisco Compatible Extensions 機能の詳細なリストは、次の URL を参照してください。
http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html

図 3-10　WCS コントローラ テンプレートを使用した CCX ロケーション測定の有効化



Cisco Compatible Extensions ロケーション測定パラメータが有効な場合、無線測定要求は、Cisco Compatible Extensions をサポートすることができるかどうかにかかわらず、関連付けられているすべての WLAN クライアントにブロードキャストされます。S36 無線測定要求をサポートしないクライアント（Cisco Compatible Extensions バージョン 1 をサポートするクライアント、または Cisco Compatible Extensions WLAN デバイス仕様との互換性がまったくないクライアント）は、受信した無線測定要求をすべて無視します。

（注）　Intel® PRO/Wireless 3945ABG Network Connection アダプタまたは Intel® PRO/Wireless 2915ABG Network Connection アダプタを搭載したクライアントを使用する場合は、Intel ProSet Configuration Utility のデフォルトの「Personal Security」設定には、Cisco Compatible Extensions 仕様との互換性がないことに注意することが重要です。無線セキュリティでこのデフォルトの「personal」レベル（企業での使用を目的としていない）を使用する場合、Intel 3945ABG または 2915ABG クライアント アダプタを搭載したクライアントは、S36 ブロードキャスト無線測定要求をサポートせず、Cisco Compatible Extensions WLAN デバイス仕様に準拠していません。Cisco Compatible Extensions 仕様との互換性と、S36 無線測定要求のサポートを有効にするには、Intel ProSet クライアント サプリカントを使用してクライアントを「Enterprise Security」用に再設定し、Cisco Compatible Extensions を有効にする必要があります。P.5-59 の図 5-42 および P.5-60 の図 5-43 に、実行方法を示します。

無線測定要求の例を図 3-11 に示します。802.11b/g インターフェイス MAC アドレス 00:14:1B:59:42:72 のアクセス ポイントから要求が出されています。

図 3-11　　ブロードキャスト無線測定要求

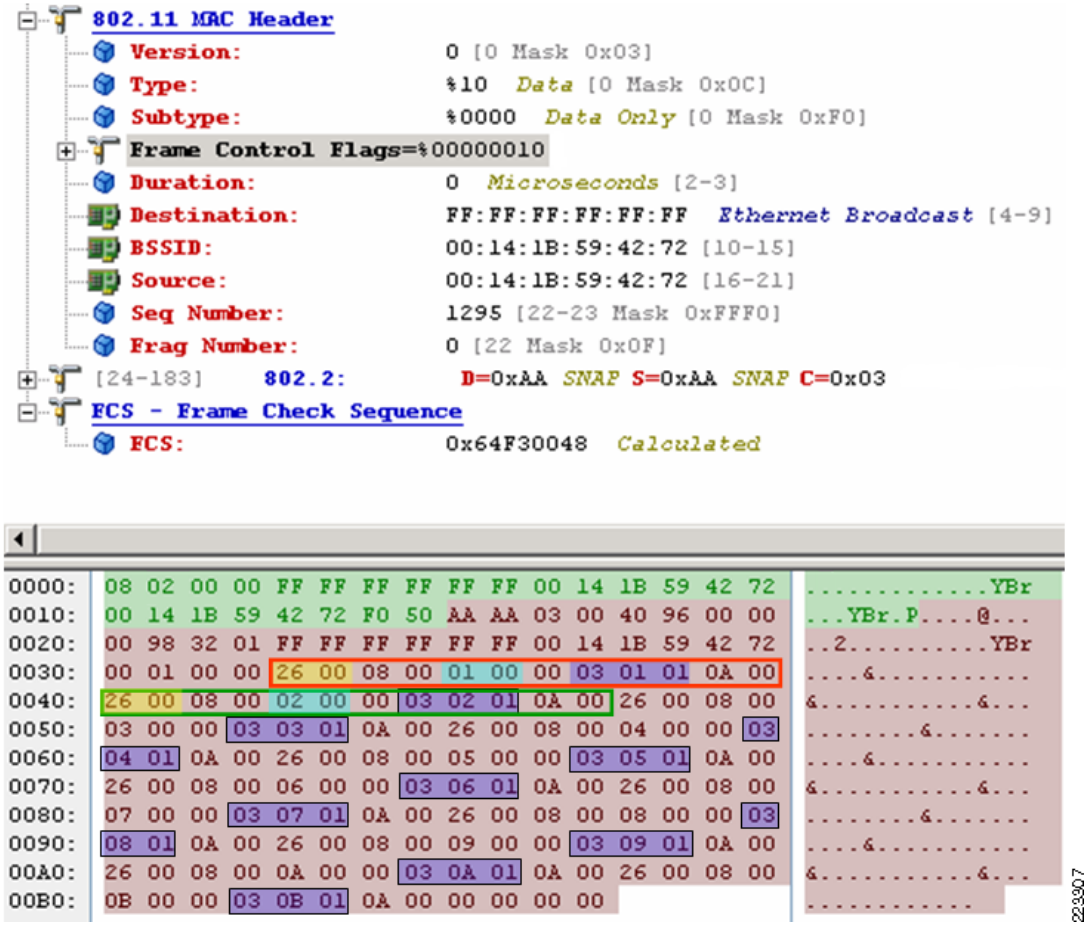


図 3-11 に、WLAN クライアントに対する無線測定要求の影響を理解するのに役立つ重要な情報をいくつか示します。図 3-11 では、関連付けられているクライアントに対するフレーム ブロードキャストには、実際に複数の無線測定要求要素が含まれている様子を示しています。16 進数オフセット 0x0034 から始まる最初の要素が赤の四角形で強調表示されています。無線測定要求要素をさらに詳しく見てみると、次のことがわかります[1]。

- 要素 ID 0x2600 が 16 進数オフセット 0x0034 に表示され、次に来るのが測定要求要素だということを示しています（黄色で表示）。
- 測定トークン 0x01 がオフセット 0x0038 に表示されています。これは 0 以外の 16 進数の値で、特定の測定要求フレーム内の測定要求要素の中で一意です。

1. 無線情報要素のフィールドでは、最下位バイトを最初に送信する 802.11 標準に従っています。

- 16 進数オフセット 0x003B で、いくつかの無線測定要求要素の詳細フィールドのうち最初のもの（青い四角形で強調表示された各フィールドの最初の 3 バイト）が見えます。詳しく見てみると、それぞれの詳細フィールドに次の情報が含まれていることを確認できます。
  - 測定タイプ定義 0x03 は、これがビーコン要求だということを示します。この測定タイプでは、受信クライアントステーションでアクティブまたはパッシブ スキャンを実行することを要求し（以下のスキャン モード定義フィールドを参照）、スキャン完了時にこれらのスキャンの結果をアップストリームの UWN に転送します。アクティブ スキャンの実行時、クライアント デバイスは受信アクセス ポイントからプローブ応答を要請するプローブ要求フレームを送信します。反対に、パッシブ モード スキャンでは、802.11 クライアント デバイスがビーコンまたはプローブ応答フレームをリッスンすることを要求し、アクティブな要請を求めません。
  - ビーコン要求が適用されるチャネル番号。これは測定要求の詳細フィールドの 2 番目のオクテットで、16 進数オフセット 0x003C（値 0x01）の位置にあります。
  - スキャン モード定義の 0x01 は、測定要求の詳細フィールドの 3 番目のオクテットです。これは 16 進数オフセット 0x003D の位置にあります。スキャン モード定義の 0x01 は、アクティブ スキャンが実行されることを示しています。ロケーション忠実度の観点から、パッシブ スキャンはクライアント ロケーション忠実度の向上にはほとんど効果はありません（プローブ要求が生成されないため）。そのため、CCX ロケーション測定がコントローラ上で有効な場合、スキャン モード定義は常にアクティブ スキャンの実行を要求するよう設定されます。

3 つすべての無線測定の詳細フィールドを考慮に入れると、この無線測定要求要素に、チャネル 1 でアクティブ スキャンが実行されるよう要求するビーコン要求が含まれていることがわかります。

無線測定要求には、11 の 測定要求要素フィールドが含まれていることに注意してください。図 3-11 ではそれらフィールドの 2 つのみを強調表示していますが、1 つ目は赤い四角形、2 つ目は緑の四角形で囲まれています。この無線測定要求が 802.11b/g 無線インターフェイス（11 の使用可能なチャネルを持つ、北米の規制区域で運用される）上で発行されていることを考えると、理解できます。後続の測定要求（緑の四角形）で、チャネル番号フィールド（16 進数オフセット 0x44 として表示）は最初の測定要求から 1 ずつ、順番に増分されます。これは測定要求要素フィールド内で継続され、0xB（11）に達するまで続きます。

Cisco Compatible Extensions WLAN デバイス仕様バージョン 2 またはそれ以降に準拠し、S36 無線測定要求をサポートする 802.11bg クライアントは、図 3-11 に示すフレームを受信し、無線測定プロセスの一部として、指定されたチャネルのアクティブ スキャンを実行します。このようなクライアントの圏内にあるアクセス ポイントでプローブ要求を受信した場合、クライアントは（登録済みのコントローラを介して）、クライアントのローカライズに使用される Location Appliance に信号強度測定を転送します。また、クライアントも測定時に受信したすべてのプローブ応答の RSSI 情報を収集し、これを無線測定レポート フレーム内の Cisco UWN に転送します。

Cisco Compatible Extensions WLAN デバイス仕様バージョン 2 に関して、S36 無線測定要求をサポートする WLAN クライアントは、次のことを行う必要があります。

- 測定要求を受信したチャネルで、パフォーマンスを著しく低下させずに無線測定を実行する。
- 一時的に発信トラフィックをバッファリングしながら、稼動していないチャネル上で測定を実行する。
- 無線測定レポート フレームで受信した各無線測定要求フレームに応答する。
- クライアント デバイスのパフォーマンスを著しく低下させる可能性のある測定要求はすべて無視する。
- アクティブ スキャンをサポートする。

WLAN クライアント

無線 LAN クライアントと適切に構成されたワークグループ ブリッジが、図 3-12 に示すように、青い四角形アイコンを使用して、WCS ロケーション フロア マップ上に表示されています。WCS ロケーション フロア マップに WLAN クライアントを表示するには、フロア マップ表示上部の [Layers] ドロップダウン セレクタにある [Clients] チェックボックス オプションをオンにし、左側の列の [Load] をクリックします。画面が見づらくなるのを避けるために、WCS は最初の 250 台の WLAN クライアントをフロア マップに表示します。最初の 250 台以降の WLAN クライアントを表示したい場合は、クライアントのフィルタリングを使用します。

図 3-12　　WCS WLAN クライアント ロケーション マップ

表示されたグラフィカルなロケーション情報は、情報の経過時間に基づいて WCS によってフィルタ処理できます。図 3-12 にあるように、最大 15 分経過したデバイス ロケーション情報が WCS に表示されます。受信した最新のロケーション情報を表示したい場合は、この値を 2 または 5 分に設定できます。古い情報を表示したい場合は、½、1、3、6、12、または 24 時間に設定できます。

[Clients] チェックボックス オプションの右に表示されている青い矢印 › をクリックすると、クライアント フィルタリング オプションを指定でき、次のような追加情報を取得できます。

- このフロアで検出された WLAN クライアントの合計数。
- 小さいアイコン（図 3-12 を参照）または標準サイズのアイコンを選択できます。小さいアイコンを使用する場合、クライアントのフロア マップに説明テキストは表示されません（マウスでポイントした場合を除く）。標準サイズのアイコンを使用する場合、オンスクリーン タグが表示されます。このタグは IP アドレス、ユーザ名、MAC アドレス、資産名、資産グループ、または資産カテゴリ用に設定できます。
- すべての WLAN クライアントを表示するか、またはフィルタ処理を実行してフロア マップに表示するクライアントを選択できます。フィルタは、IP アドレス、ユーザ名、MAC アドレス、資産名、資産グループ、資産カテゴリ、またはコントローラに基づいて行うことができます。SSID および RF プロトコル（802.11a または 802.11b/g）でさらにフィルタリングすることができます。前

述したとおり、フロア マップ上には一度に最大 250 台の WLAN クライアントのみが表示されます。250 台を超える WLAN クライアントが検出された場合、WCS と Location Appliance 間の各通信サイクル時に、左側の列のステータス領域に検出された合計数が表示されます。この警告を受け取った場合、表示するように選択する WLAN クライアントの合計数を減らすためにフィルタリングを使用することを推奨します。

Cisco UWN ソフトウェア リリース 4.1 で、WLAN コントローラは表 3-1 に一覧表示される WLAN クライアントの最大数をサポートします。

表 3-1　　WLC クライアントの最大キャパシティ

コントローラ モデル	サポートされる WLAN クライアント
2006	256
2106	256
4402	2,500
4404	5,000
WiSM	10,000
NM-WLC6	256
NME-WLC8/12	350
3750G	2,500

表示されている任意の WLAN クライアントに関する詳細情報は、図 3-13 に示すように、フロア マップ上の該当する青い四角形アイコンをクリックするだけで表示できます。[location] サブメニューの下のクライアントに名前、グループ、およびカテゴリ情報を割り当てることができます。そうすると、このサブメニューはフロア マップ表示上の資産の特定に使用できるようになります。

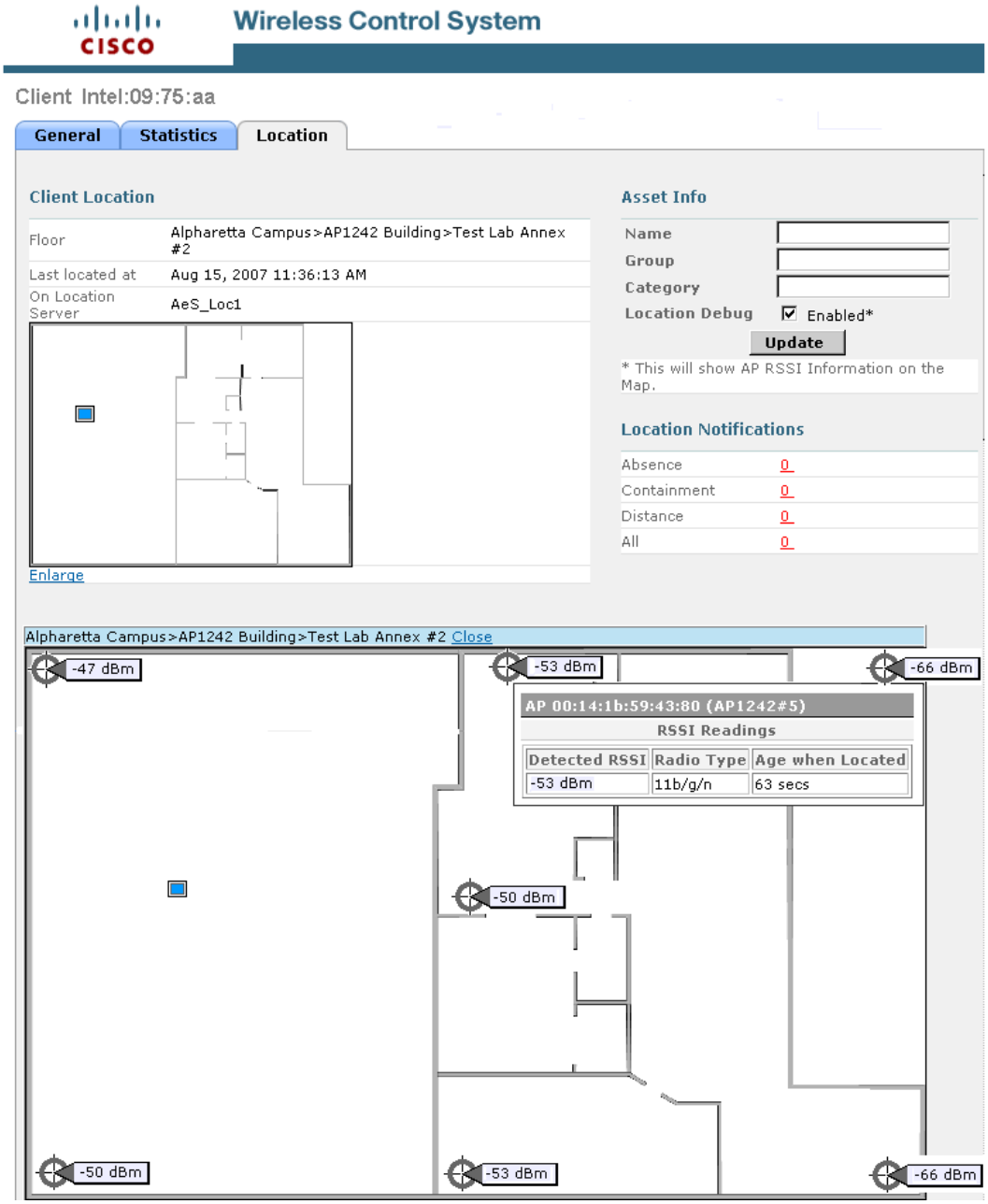
図 3-13　　WLAN クライアント詳細情報

また、ハイパーリンクされたロケーション通知のリストと、クライアント ロケーションを示す縮小版のロケーション マップを図 3-13 に示します。マップを拡大して、ロケーション デバッグ パラメータを有効にすることによって、図 3-14 に示すように、WLAN クライアントを検出中の各アクセス ポイントで検出された最新の RSSI レベルが WCS に表示されます。

（注）　[Location Debug Enable] チェックボックスの設定は、*locserverd* アプリケーションを再起動したり、Location Appliance をリブートしたりするとクリアされます。

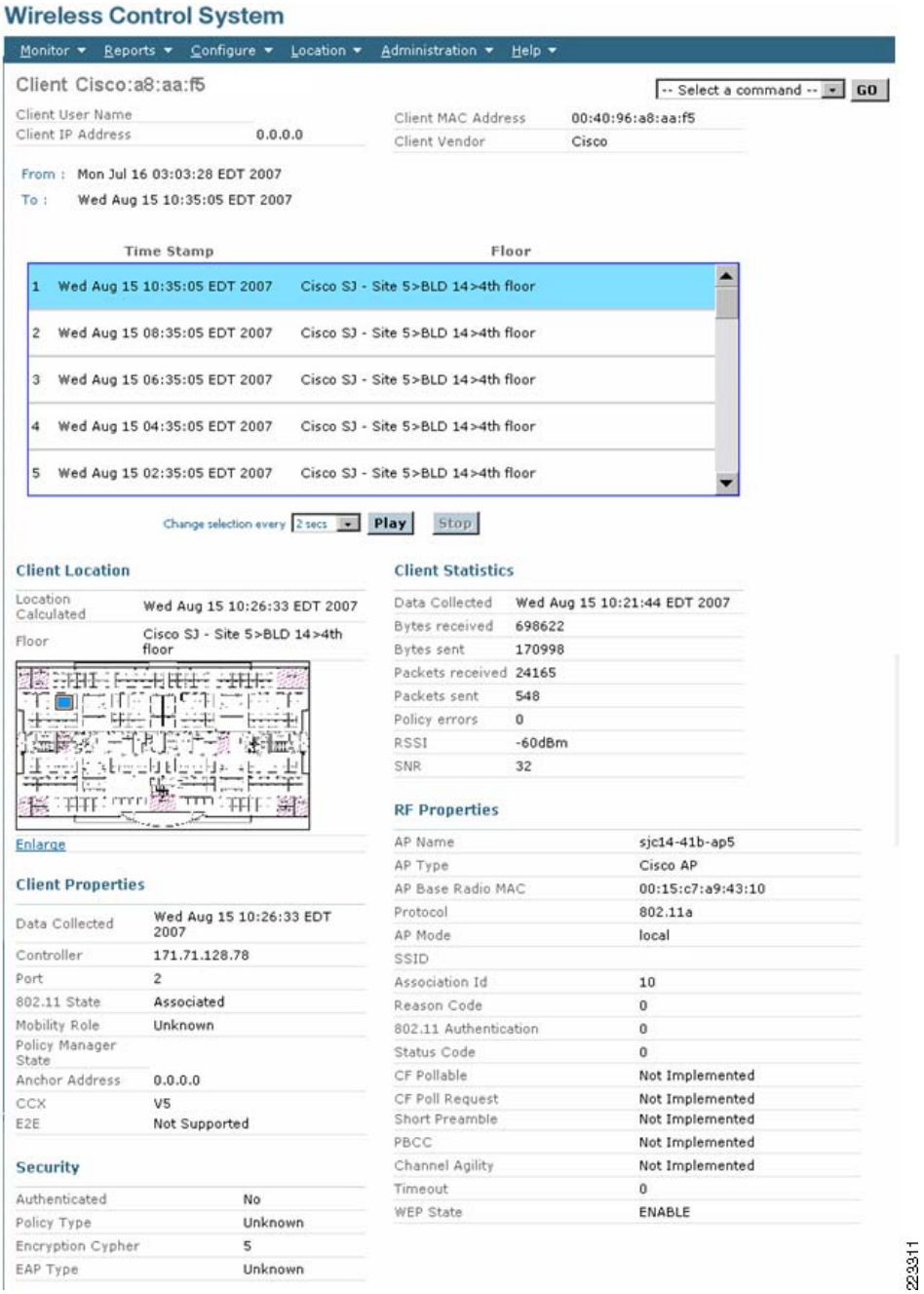
この RSSI 情報は、**show client detail** <*mac address*> コマンドを実行した場合と同様の方法で収集され、WLAN クライアントの検出済み RSSI を確認するための CLI コマンドの代替として使用できます（図 3-14 を参照）。

図 3-14　ロケーション デバッグを有効にした場合の WLAN クライアントの検出済み RSSI



無線クライアント デバイス ロケーション履歴は、画面の右上隅にあるドロップダウン メニューの [Location History] を選択し（図 3-14 のロケーション画面ビューに表示）、[Go] をクリックすると表示されます。Location Appliance 内に保存された無線クライアントの過去のロケーション履歴が、図 3-15 に示す画面に表示されます。

図 3-15　WLAN クライアント ロケーション履歴



多くの場合、環境全体のクライアントの経時的な移動を適切に視覚化し、追跡するために、クライアント デバイスのロケーション履歴を順番に表示することをお勧めします。これは、たとえばセキュリティおよび監視の用途で便利です。Cisco WCS および Location Appliance では、この方法で各ロケーション履歴の記録を設定可能な時間遅延で再生することができます。表示される「移動」の精度は、クライアント履歴レコードがデータベースに記録される間隔によって異なります。

この方法で再生されるロケーション履歴を表示するには、図 3-15 に示す [Play] ボタンをクリックします。

802.11 アクティブ RFID タグ

ロケーション認識 Cisco UWN は、Cisco Compatible Extensions Wi-Fi Tag 仕様（AeroScout、WhereNet、G2 Microsystems、InnerWireless（PanGo）など）に準拠する 802.11 Wi-Fi アクティブ RFID タグを検出し、図 3-16 に示すように黄色のタグ アイコンを使用して WCS フロア マップ上に表示します。これらの資産タグは通常、WLAN インフラストラクチャに関連付けられておらず、通常、プローブ要求に基づいて配置されていません。その代わりこれらの資産タグは、レイヤ 2 マルチキャストを使用して、定期的にロケーション認識 UWN にメッセージを送信します。資産タグにはオプション モードがあり、完全な WLAN アソシエーションが可能です。これらのタグは、このモ [ドで動作している間、青い四角形（WLAN クライアント）として WCS ロケーション フロア マップ上に表示されます。

WCS ロケーション フロア マップに資産タグのロケーションを表示するには、フロア マップ表示上部の [Layers] ドロップダウン セレクタにある [Clients] チェックボックス オプションをオンにし、左側の列の [Load] をクリックします。画面が見づらくなるのを避けるために、WCS は最初の 250 の資産タグをフロア マップに表示します。最初の 250 以降の資産タグを表示したい場合は、資産タグのフィルタリングを使用します。他のすべてのロケーション認識 Cisco UWN のコンポーネントで、資産タグ情報を収集するよう適切に設定されていることを前提としています。

図 3-16　RFID タグ ロケーション マップ

表示されたグラフィカルなロケーション情報は、情報の経過時間に基づいて WCS によってフィルタ処理できます。図 3-16 では、最大 15 分経過した Location Appliance の情報が WCS に表示されます。受信した最新のロケーション情報のみを表示したい場合は、この値を 2 または 5 分に設定できます。古い情報を表示したい場合は、½、1、3、6、12、または 24 時間に設定できます。

[802.11 Tags] チェックボックス オプションの右に表示されている青い矢印 › をクリックすると、タグ フィルタリング オプションを指定でき、次のような追加情報を取得できます。

- このフロアで検出された資産タグの合計数を表示できます。
- 小さいアイコン（図 3-16 を参照）または標準サイズのアイコンを選択できます。小さいアイコンを使用する場合、資産タグのフロア マップに説明テキストは表示されません（マウスでポイントした場合を除く）。標準サイズのアイコンを使用する場合、オンスクリーン タグが表示されます。このタグは MAC アドレス、資産名、資産グループ、または資産カテゴリ用に設定できます。
- すべての資産タグを表示するか、またはフィルタ処理を実行してフロア マップに表示する資産タグを選択することができます。フィルタは、MAC アドレス、資産名、資産グループ、資産カテゴリ、またはコントローラに基づいて行うことができます。前述したとおり、フロア マップ上には一度に最大 250 の資産タグのみが表示されます。250 を超える資産タグが検出された場合、WCS と Location Appliance 間の各通信サイクル時に、左側の列のステータス領域に検出された合計数が表示されます。この警告を受け取った場合、表示するように選択する資産タグの合計数を減らすために、フィルタリングを使用することをお推めします。

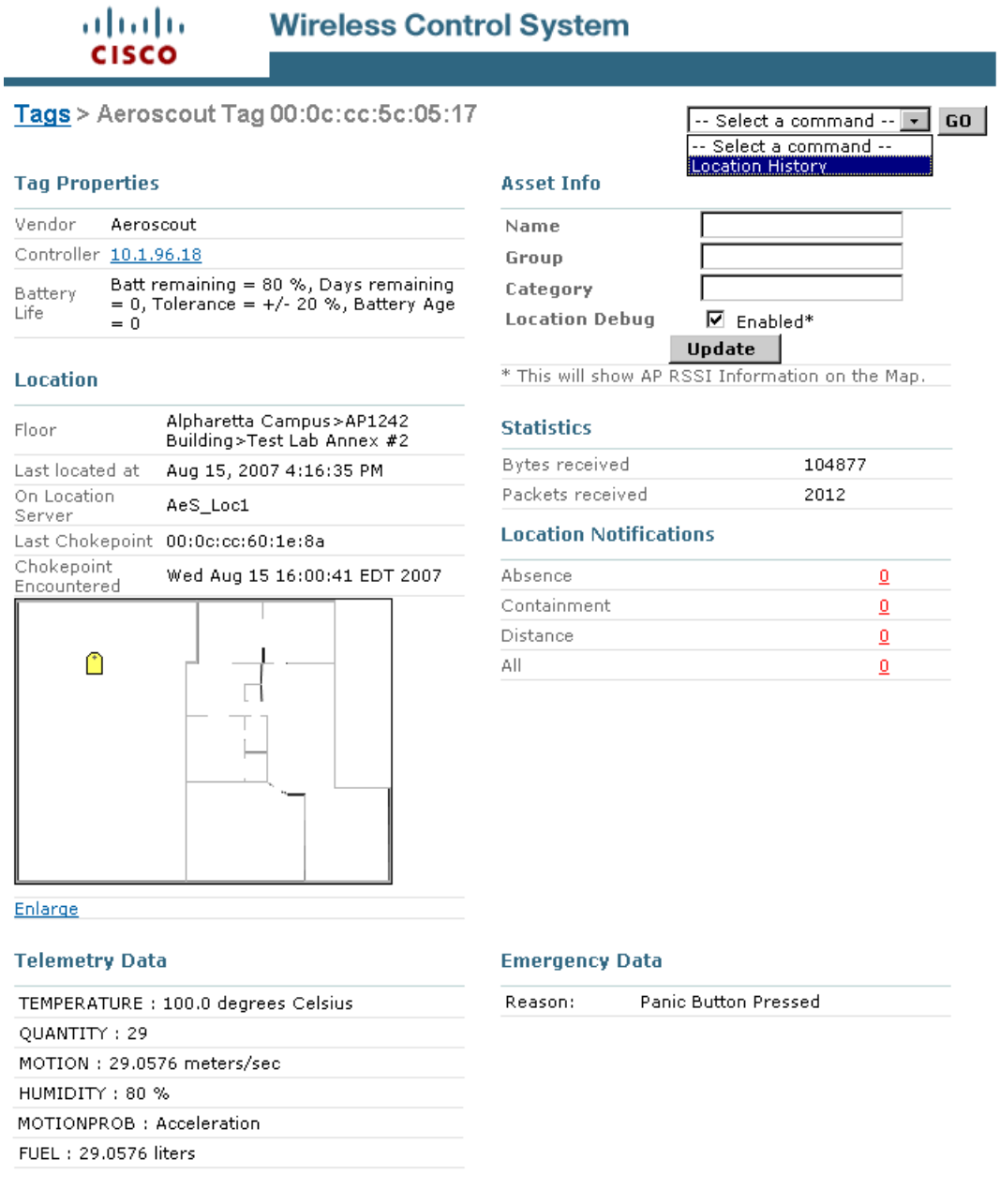
Cisco UWN ソフトウェア リリース 4.1 で、WLAN コントローラは表 3-2 に一覧表示される資産タグの最大数をサポートします。

表 3-2　WLC 資産タグの最大キャパシティ

コントローラ モデル	サポートされる資産タグ
2006	500
2106	500
4402	1250
4404	2500
WiSM	5000
NM-WLC6	500
NME-WLC8/12	500
3750G	1250

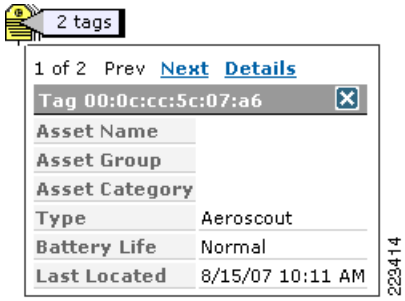
表示されている任意の資産タグに関する詳細情報は、タグに関連付けられている黄色のタグ アイコンをクリックするだけで表示できます。WCS は、図 3-17 に表示される情報で応答します。ロケーション認識 Cisco UWN ソフトウェア リリース 4.1 から、タグ テレメトリ、チョークポイント、タグ ステータス情報も、拡張されたバッテリ リポート情報とともに、図 3-17 に示すタグ詳細画面に表示されるようになりました。

図 3-17　RFID タグ詳細情報



場合によっては、Location Appliance で同一の予測ロケーションに 2 つ以上の資産タグが配置されることがあります。そのため、それらのタグを個別のアイコンとしてグラフィカルに表示しようとするとほぼ重なります。タグ サマリー アイコン（黒の水平線が引かれている黄色のタグ）は、図 3-18 に示すように、このような状況を解決するために使用されます。

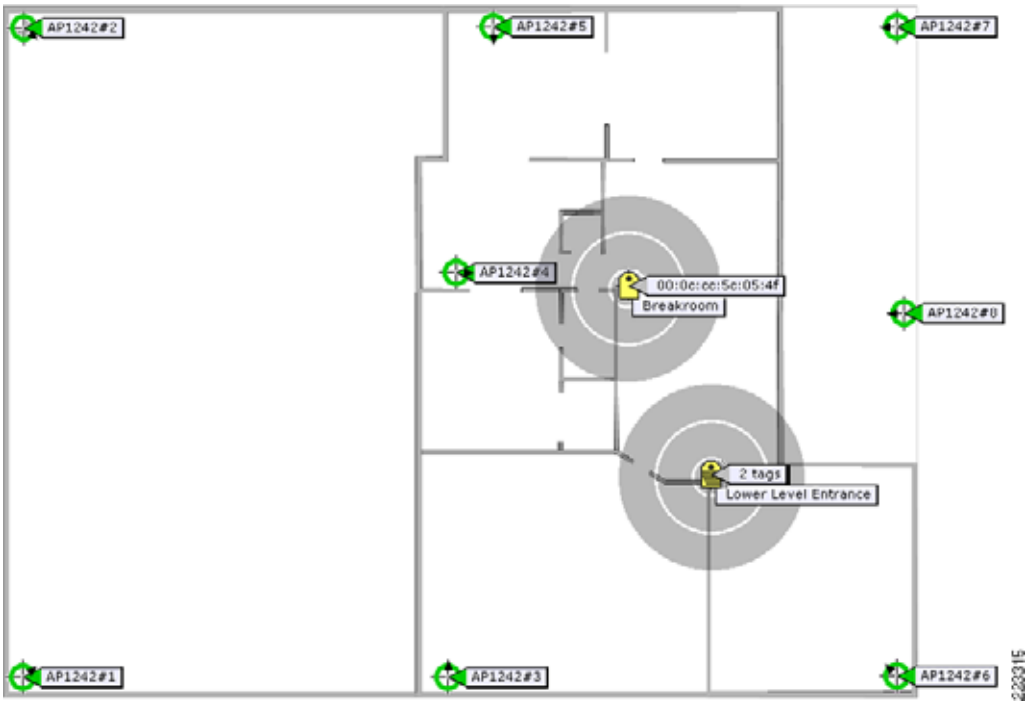
図 3-18　タグ サマリー アイコンとサマリー記述子



タグ サマリー アイコンをマウスでポイントすると、タグ サマリー記述子が表示されます。この記述子にはタグに関連する特性が要約されています。[Next] をクリックして、このロケーションにある各タグの MAC アドレスの記述子情報をスクロールします。[Details] をクリックすると図 3-17 に示すタグ詳細パネルが表示されます。

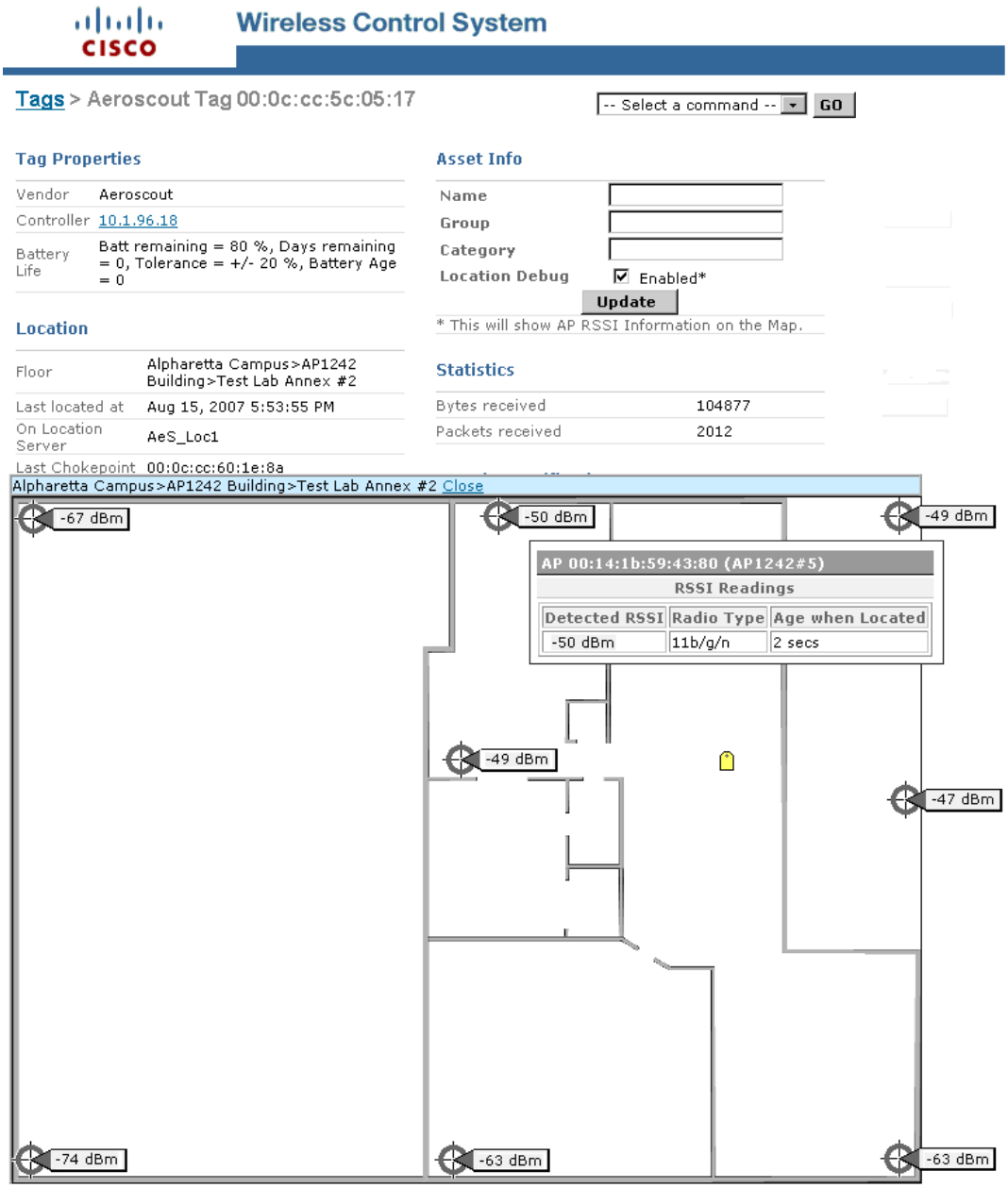
タグ サマリー アイコンは、*チョークポイント ロケーション*（Cisco UWN ソフトウェア リリース 4.1 で導入）を使用している場合、特に便利です。チョークポイントがシステムに対して定義され、フロアマップで適切に定義されている場合、チョークポイント トリガーの範囲内にあるすべての資産タグのアイコンは、チョークポイント アイコンの中心に配置されます（「Breakroom」チョークポイントの図 3-19 を参照）。ただし、2 つ以上の資産タグが同一のチョークポイントの範囲内にある場合、タグ アイコンが重なるため、操作しづらくなります。この場合、見やすくするためにもう一度図 3-18 に示すタグ サマリー アイコンを使用します。この用途で使用されているタグ サマリー アイコンの例は図 3-19 の「Lower Level Entrance」という名前のチョークポイントに示されています。

図 3-19　タグ サマリー アイコンとチョークポイント ロケーション



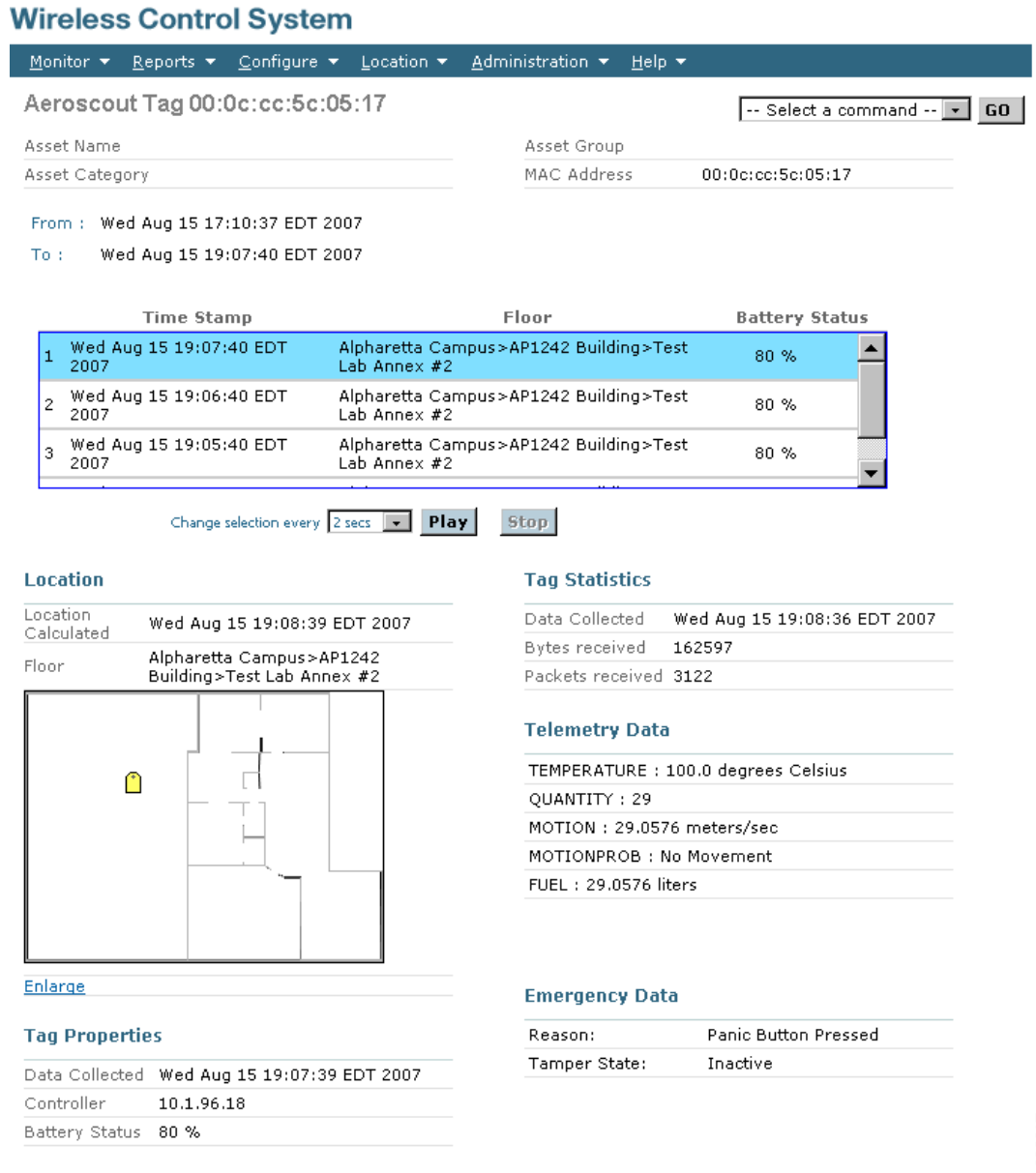
また、ハイパーリンクされたロケーション通知のリストと、資産タグのロケーションを示す縮小版のロケーション マップを図 3-20 に示します。ロケーション デバッグ パラメータを有効にし、マップを拡大することによって、資産タグを検出した各アクセス ポイントで検出された最新の RSSI レベルが WCS に表示されます。この RSSI 情報は、**show rfid detail** <*mac address*> コマンドを実行した場合と同様の方法で収集され、資産タグの検出済み RSSI を特定するための CLI コマンドの代替として使用できます。図 3-20 に示すように、任意のアクセス ポイントにマウスをポイントすることによって、検出された最新の信号強度読み取りの無線タイプおよび経過時間に関する追加情報を取得できます。

図 3-20　　ロケーション デバッグを有効にした場合の資産タグの検出済み RSSI



資産タグ ロケーション履歴は、図 3-20 に表示される、画面の右上隅にあるドロップダウン メニューの [Location History] を選択し、[Go] をクリックすると表示されます。Location Appliance 内に保存された資産タグの過去のロケーション履歴が、図 3-21 に示すように、ロケーション統計情報、タグ テレメトリ、バッテリ、および「emergency」ステータスとともに表示されます。

図 3-21　資産タグのロケーション履歴



多くの場合、環境全体の資産タグ（および付属する資産）の経時的な移動を適切に視覚化し、追跡するために、資産タグのロケーション履歴を順番に表示することをお勧めします。これは、たとえばセキュリティおよび監視の用途で移動の足跡を確立するうえで便利です。Cisco WCS および Location Appliance では、この方法で各ロケーション履歴の記録を設定可能な時間遅延で再生することができます。表示される「移動」の精度は、クライアント履歴レコードがデータベースに記録される間隔によって異なります。

この方法でロケーション履歴を再生するには、図 3-21 に示す [Play] ボタンをクリックします。そうすると、表形式、およびグラフ形式で過去のロケーション履歴の表示が開始されます。膨大なロケーション履歴データは、図 3-21 で示す [Change Selection Every] の間隔を 2 秒から 1 秒に減らすことで、より見やすくなります。

不正アクセス ポイント

不正アクセス ポイント。無線 LAN インフラストラクチャで検出され、同じ RF グループまたは WLAN システムのメンバではないと判断されたアクセス ポイントのことです。さらに、アドホック ネットワークのメンバとして参加しているデバイスも、不正アクセス ポイントとして検出されます（ただし Location Appliance の不正アクセス ポイント ポーリングがアドホックの不正を除外するように設定されている場合は、不正タイプ AD_HOC）。

不正アクセス ポイントは、図 3-22 に示すように、黒色の丸で囲まれたドクロと交差した 2 本の骨のアイコン を使用して、WCS ロケーション フロア マップ上に表示されます。これらは、完全な無線、検出中の WLAN として同一の有線インフラストラクチャに接続、またはまったく異なる有線インフラストラクチャに接続されている場合があります。WCS ロケーション フロア マップに不正アクセス ポイントを表示するには、フロア マップ表示上部の [Layers] ドロップダウン セレクタにある [Rogue APs] チェックボックス オプションをオンにし、左側の列の [Load] をクリックします。画面が見づらくなるのを避けるために、WCS は最初の 250 の不正アクセス ポイントをフロア マップに表示します。最初の 250 以降の不正アクセス ポイントを表示したい場合は、不正アクセス ポイントのフィルタリングを使用します。

図 3-22　　不正アクセス ポイントのロケーション マップ

情報の経過時間に基づいて、WCS に表示されるロケーション情報をフィルタ処理することができます。図 3-22 では、最大 15 分経過した Location Appliance の情報が WCS に表示されます。または、最新のロケーション情報を表示したい場合は、この値を 2 または 5 分に設定できます。古い情報を表示したい場合は、½、1、3、6、12、または 24 時間に設定できます。

[Rogue APs] チェックボックス オプションの右に表示されている青い矢印 › をクリックすると、不正アクセス ポイント フィルタリング オプションを指定でき、次のような追加情報を取得できます。

- このフロアで検出された不正アクセス ポイントの合計数。
- 小さいアイコン（上記を参照）または標準サイズのアイコンを選択できます。小さいアイコンを使用する場合、不正アクセス ポイントのフロア マップに説明テキストは表示されません（マウスでポイントした場合を除く）。標準サイズのアイコンを使用する場合、不正アクセス ポイントの MAC アドレスを表示するオンスクリーン タグが表示されます。
- すべての不正アクセス ポイントを表示するか、またはフィルタ処理を実行してフロア マップに表示する不正アクセス ポイントを選択することができます。これは主に MAC アドレスに基づきますが、不正検知の状態をフィルタ処理することによって拡張できます（Alert、Known、Acknowledged、Contained、Threat、または Known Contained）。また、不正アクセス ポイントが、検出中の無線システムと同じ有線ネットワークに接続されていたかどうかでもフィルタ処理できます。前述したとおり、フロア マップ上には一度に最大 250 の不正アクセス ポイントのみが表示されます。250 を超える不正アクセス ポイントが検出された場合、WCS と Location Appliance 間の各通信サイクル時に、左側の列のステータス領域に検出された合計数が表示されます。この警告を受け取った場合、表示するように選択する不正なアクセス ポイントの合計数を減らすためにフィルタリングを使用することを推奨します。

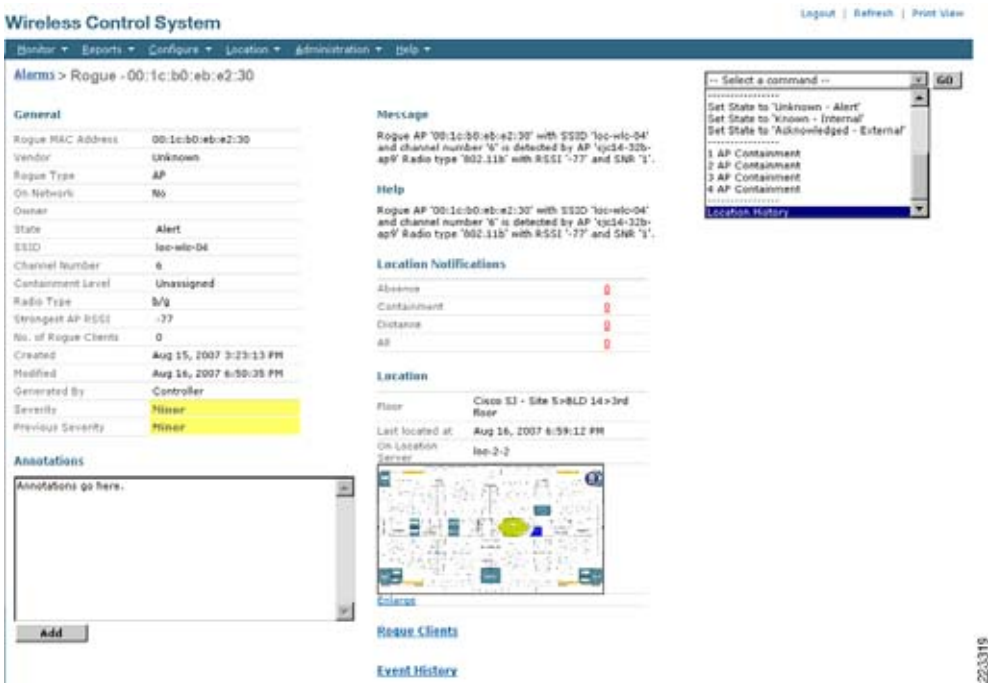
Cisco UWN ソフトウェア リリース 4.1 で、WLAN コントローラは表 3-3 に一覧表示される不正アクセス ポイントの最大数をサポートします。

表 3-3　WLC 不正なアクセス ポイントの最大キャパシティ

コントローラ モデル	サポートされる不正 AP
2006	125
2106	125
4402	625
4404	625
WiSM	1250
NM-WLC6	125
NME-WLC8/12	125
3750G	625

表示されるすべての不正アクセス ポイントについての詳細情報は、フロア マップ上の目的の不正アクセス ポイントを表す、丸で囲まれたドクロと交差した骨のアイコンをクリックするだけで表示できます。クリックすると、図 3-23 に示すように詳細情報を含む画面が表示されます。ただし、ロケーション マップを拡大している場合、不正アクセス ポイントの RSSI 情報は表示されません。右上隅にあるドロップダウン メニューを使用すると、対象の不正アクセス ポイントのロケーション履歴と再生情報を参照できます。形式と機能は、WLAN クライアントと 802.11 アクティブ RFID タグの項で説明したものと同様です。

図 3-23　不正アクセス ポイントの詳細情報



不正クライアント

不正クライアント。不正アクセス ポイントに関連付けられているクライアントです。不正クライアントは、図 3-24 に示すように、黒色の四角で囲まれたドクロと交差した 2 本の骨のアイコン を使用して、WCS ロケーション フロア マップ上に表示されます。WCS ロケーション フロア マップに不正アクセス ポイントを表示するには、フロア マップ表示上部の [Layers] ドロップダウン セレクタにある [Rogue Clients] チェックボックス オプションをオンにし、左側の列の [Load] をクリックします。画面が見づらくなるのを避けるために、WCS は最初の 250 台の不正クライアントをフロア マップに表示します。最初の 250 台以降の不正クライアントを表示したい場合は、不正クライアントのフィルタリングを使用します。

図 3-24　不正クライアントのロケーション マップ

情報の経過時間に基づいて、WCS に表示されるロケーション情報をフィルタ処理することができます。図 3-24 では、最大 15 分経過した Location Appliance の情報が WCS に表示されます。または、最新のロケーション情報を表示したい場合は、この値を 2 または 5 分に設定できます。古い情報を表示したい場合は、½、1、3、6、12、または 24 時間に設定できます。

[Rogue Clients] チェックボックス オプションの右に表示されている青い矢印 › をクリックすると、不正クライアント フィルタリング オプションを指定でき、次のような追加情報を取得できます。

- このフロアで検出された不正クライアントの合計数。
- 小さいアイコン（上記を参照）または標準サイズのアイコンを選択できます。小さいアイコンを使用する場合、不正クライアントのフロア マップにテキストは表示されません（マウスでポイントした場合を除く）。標準サイズのアイコンを使用する場合、オンスクリーン タグには不正クライアントの MAC アドレスが表示されます。
- すべての不正クライアントを表示するか、またはフィルタ処理を実行してフロア マップに表示する不正クライアントを選択することができます。フィルタリングは、不正クライアントが関連付けられている不正アクセス ポイントの MAC アドレスに基づいて実行します。または、不正クライアントの状態（alert、contained、または threat）に基づいてフィルタ処理します。前述したとおり、フロア マップ上には一度に最大 250 台の不正クライアントのみが表示されます。250 台を超える不正クライアントが検出された場合、WCS と Location Appliance 間の各通信サイクル時に、左側の列のステータス領域に検出された合計数が表示されます。この警告を受け取った場合、表示するように選択する不正クライアントの合計数を減らすためにフィルタリングを使用することを推奨します。

Cisco UWN ソフトウェア リリース 4.1 で、WLAN コントローラは表 3-4 に一覧表示される不正クライアントの最大数に対応します。

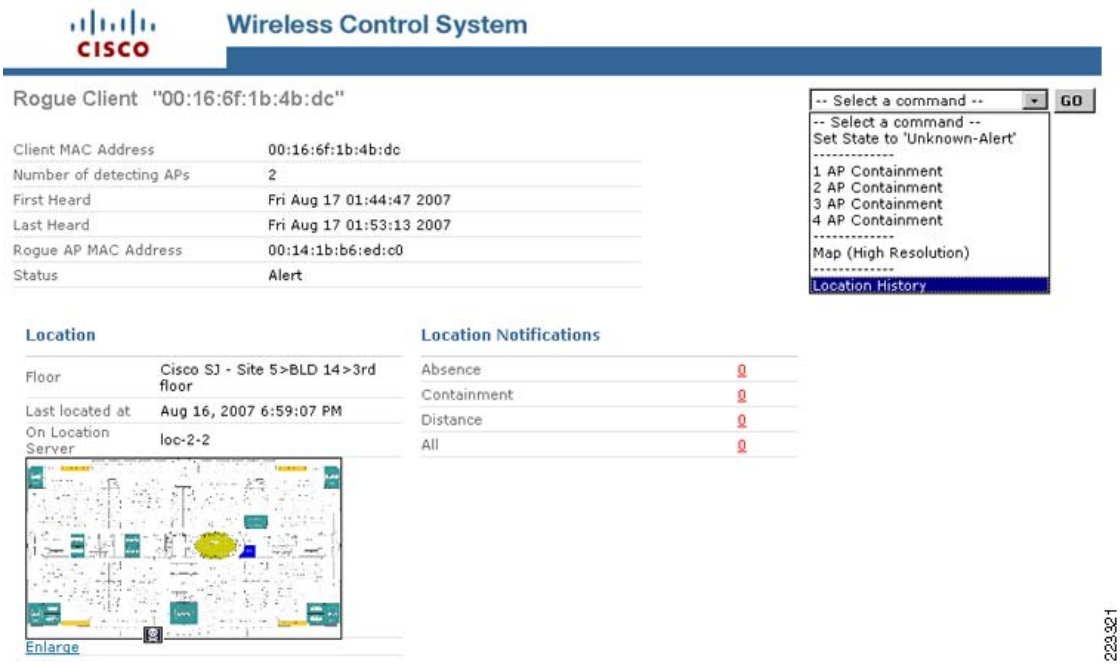
表 3-4　WLC 不正クライアントの最大キャパシティ

コントローラ モデル	不正クライアント
2006	100
2106	100
4402	500
4404	500
WiSM	1000
NM-WLC6	100
NME-WLC8/12	100
3750G	500

表示されるすべての不正クライアントについての詳細情報は、フロア マップ上の目的の不正クライアントを表す、黒色の四角形で囲まれたドクロと交差した骨のアイコンをクリックするだけで表示できます。クリックすると、図 3-25 に示す画面が表示されます。ただし、ロケーション マップを拡大している場合、不正なアクセス ポイントの RSSI 情報は表示されません。

右上隅にあるドロップダウン メニューを使用すると、対象の不正クライアントのロケーション履歴と再生情報を参照できます。形式と機能は、WLAN クライアント、アクティブ RFID タグ、不正アクセス ポイントの項で説明したものと同様です。

図 3-25　不正クライアント詳細情報



不正アクセス ポイントのローカリゼーションと、WLAN クライアントおよび資産タグのローカリゼーションの違いを理解することは重要です。WLAN クライアントが、複数のチャネルにプローブ要求を定期的に送信するという、前述の説明を思い出してください。インフラストラクチャ アクセス ポイントは、ほとんどの時間を割り当て済みのチャネルに費やします。これらのプローブ要求はすぐに検出さ

れ、アクセス ポイントが登録されているコントローラにリレーされます。資産タグはプローブ要求を送信せず、タグが設定されているチャネル上に、タグ メッセージをマルチキャストします。これらのマルチキャストは、資産タグの圏内にあるこれらのチャネル上で動作するインフラストラクチャのアクセス ポイントによってすぐに検出されます。

不正デバイスは、インフラストラクチャのアクセス ポイントが割り当てられているのと同じチャネル上では動作しません。このため、これらの不正デバイスは、インフラストラクチャのアクセス ポイントにより実行される、定期的なチャネル停止スキャンによって検出されます。ローカル モードで動作する LWAPP アクセス ポイントの場合、このチャネル停止スキャンは通常、180 秒の動作ごとに約 500 ミリ秒（またはプライマリ以外のチャネルで、180 秒間隔ごとに約 50 ミリ秒）実行されます。

ワークグループ ブリッジ

一部の Cisco autonomous アクセス ポイントは、ワークグループ ブリッジ（WGB）モードと呼ばれる特殊な動作モードで、Cisco UWN に接続できます。ワークグループ ブリッジとして設定されているアクセス ポイントは、Cisco UWN の有線クライアント グループに対する無線接続を提供し、有線クライアントが UWN で基本的に無線クライアントとして表示されるようにします。Cisco IOS Release 12.4(3g)JA 以降（32 MB アクセス ポイント）または Cisco IOS Release 12.3(8)JEB 以降（16 MB アクセス ポイント）を含む Cisco AP1121、AP1130、AP1231、AP1240、および AP1310 アクセス ポイントは、ワークグループ ブリッジ モード用に設定できます。

（注）　ワークグループ ブリッジの設定と Cisco UWN での役割の詳細については、次の URL にある『The Workgroup Bridge in a Lightweight Environment』を参照してください。
http://cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/configuration/guide/s43hot.html#wp1059452

ワークグループ ブリッジのデフォルトのローミング動作は、WGB がアソシエーションを失うまで、アクセス ポイント ローミング候補のアクティブ スキャンを遅延させることです。ワークグループ ブリッジが固定アプリケーションで使用する場合、このような動作を問題なく行えますが、モバイル WGB アプリケーションで使用する場合（一連のモバイル カートベースのイーサネットのみの医療機器）、次の理由で問題が生じる可能性があります。

- アソシエーションを失うまでアクセス ポイント ローミング候補の検索を遅延させると、必要のないアプリケーション遅延が生じ、時間調節が重要なモバイル アプリケーションのパフォーマンスに悪影響を与え、アプリケーション ロックアップまたはタイムアウトを引き起こす可能性があります。
- 環境によっては、同一のアクセス ポイントに関連付けられている間でも、モバイル ワークグループ ブリッジは相当の距離を移動する可能性があります。この場合、デフォルトの WGB 動作ではプローブ要求がなくなり、Location Appliance は古い RSSI 情報を使用するため、WGB がローミング イベントを検出するまで、WGB ロケーション忠実度が低下する可能性があります。

WGB モードで設定されたアクセス ポイントは、有効化された Cisco Compatible Extensions ロケーション測定パラメータの結果として送信されたブロードキャスト無線測定要求に応答しません。そのため、Cisco Compatible Extensions ロケーション測定は、ワークグループ ブリッジ内の一貫性のある定期プローブをトリガーするメカニズムとして使用することはできません。

Cisco IOS CLI **mobile station** コマンドは、ワークグループ ブリッジ ロケーションの忠実度を大幅に向上させるためにワークグループ ブリッジ上で使用できます。ワークグループ ブリッジ内でこの設定を有効にした場合、低いアクセス ポイント RSSI 値、過剰な無線の干渉、高い割合のフレーム損失を検出すると、アクティブ スキャンを実行します。ワークグループ ブリッジは、アクティブ スキャンで収集した情報を使用して、より優れたサービスを提供するアクセス ポイントがないかどうか判別し、現在のアソシエーションを失う前に、新しいアクセス ポイントにローミングします。

コマンドの基本形式は、次のようになります。

mobile station period <*seconds*> **threshold** <|*dBm*|>

ここで、**period** の値は、ワークグループ ブリッジが現在関連付けられているアクセス ポイントの RSSI をチェックする頻度を示し、**threshold** の値は、dBm 内の許容可能な最小アクセス ポイント RSSI の絶対値を示します。デフォルト値はそれぞれ、20 秒と 70 dBm です。

（注）　Cisco IOS **mobile station** コマンドの設定に関する詳細情報は、次の URL の「*Cisco IOS 12.4(3g)JA for Access Points and Bridges*」の *"mobile station"* コマンドリファレンス ページにあります。
http://cisco.com/en/US/docs/wireless/access_point/12.4_3g_JA/command/reference/cr43main.html#wp2593116

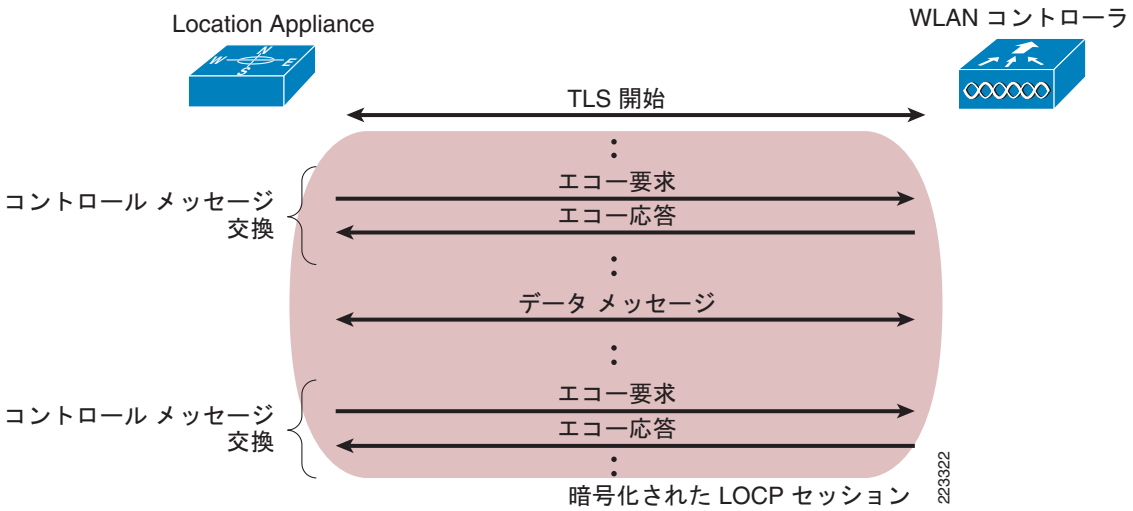
過度にローミングしないよう、period および threshold の値は、特定の環境に合わせて調節し、一貫性のある、定期的なプローブ要求を行うように調整する必要があります。threshold 値を低い値にすると、たとえば、各時間間隔で常にアクティブ スキャンが実行され、通常、あまり頻繁にローミングしないワークグループ ブリッジの忠実度が向上します。ただし、低い値に設定すると、ワークグループ ブリッジがローミングする頻度も高くなります。ただし、この代償は通常、妥当なものと見られています。それは、十分なカバレッジを持ち、アクセス ポイントが配置された、適切に展開された環境では、アクセス ポイント間でのローミングがほとんど実行されない場合、モバイル ワークグループ ブリッジ ロケーションの忠実度の向上が重要になるため、WGB ローミングの増加は無視できるようになるためです。

Cisco Location Control Protocol（LOCP）

Cisco Unified Wireless Network（CUWN）ソフトウェア リリース 4.1 では Cisco Location Control Protocol（LOCP）を導入しています。このプロトコルは、通信の効率性を高め、Location Appliance と 1 台以上の WLAN コントローラ間での新機能をサポートします。LOCP は、コネクション型転送またはコネクションレス型転送で実行できるプロトコルです。LOCP は、一方のエンドポイントがそのパートナー エンドポイントがまだアクティブであるかどうかを決定することを可能にする、コントロール メッセージの継続的な交換が提供されます。

図 3-26 に、Location Appliance と各 WLAN コントローラ間の基本的な LOCP パケット フローを示します。

図 3-26　Location Appliance と WLAN コントローラの LOCP セッション



リリース 4.1 では、Location Appliance は、通信先のコントローラの IP アドレスに関して、ユーザが事前設定します。コントローラと Location Appliance との通信がいったん開始されると、以降すべての LOCP トラフィックが送受信される 2 つのエンドポイント間で、暗号化された TLS セッションが確立されます。各エンドポイントで、パートナーがアクティブで、図 3-26 に示すように、Echo Request/Response コントロール メッセージ交換に参加することによって、要求を受け入れる準備ができていることを定期的に確認します。

Location Appliance で、WLC が応答しないことを検出した場合、WLC が再びアクティブになるまでその WLC への他のすべての要求を一時的に無効にします。Location Appliance および WLC 間の接続は、複数の交換用に維持できます（一般的なケース）。または、データ要求ごとに開始したり、切断したりできます。

Location Appliance およびそれに対して定義された WLAN コントローラ間の LOCP セッションを制御する基本パラメータは、図 3-27 に示すように、[Location Servers] > [LOCP Parameters] パネルを使用して指定します。

図 3-27　LOCP セッション パラメータの設定

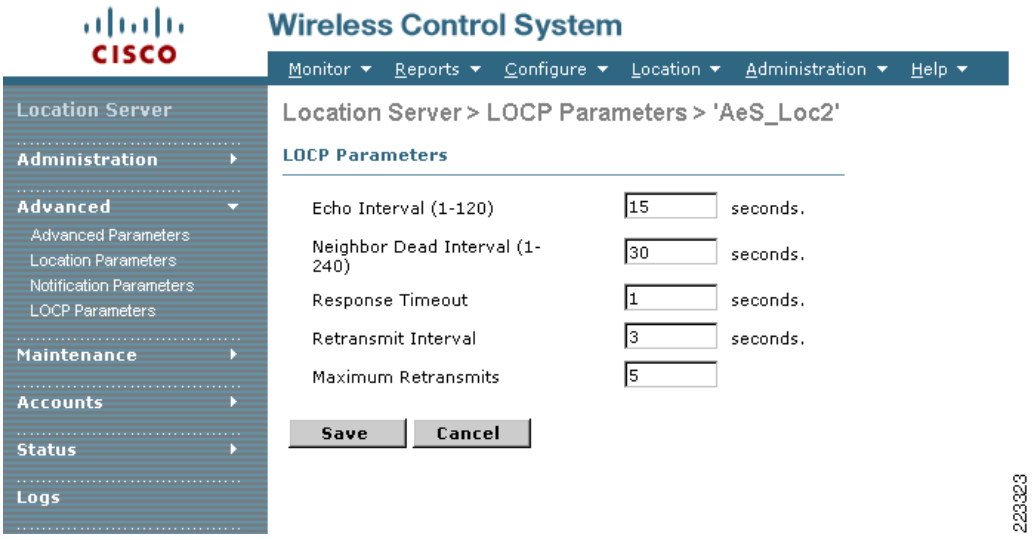


図 3-27 に示す LOCP セッション パラメータの意味は次のとおりです。

- *Echo Interval* : Location Appliance から WLAN コントローラに送信されるエコー要求の最短時間間隔（秒）。有効な値は 1 ～ 120 秒（デフォルト値は 15 秒）です。
- *Neighbor Dead Interval* : Location Appliance の待機時間。この時間を超えると、WLAN コントローラは「dead」としてエコー要求に応答しなくなります。この値は、エコー間隔の 2 倍を下回ってはいけません。推奨される値は 2 ～ 240 秒（デフォルト値は 30 秒）です。
- *Response Timeout* : 最大時間間隔（秒）。この時間内に WLAN コントローラが Location Appliance によって送信される要求に応答する必要があります。有効な値は 1 ～ 99,999 秒（デフォルト値は 1 秒）です。
- *Retransmit Interval* : LOCP 要求が WLAN コントローラからの応答を得られない場合に待機する最小時間間隔。この時間を超えると、Location Appliance は LOCP 要求を再送信します。有効な値は 1 ～ 99,999 秒（デフォルト値は 3 秒）です。
- *Maximum Retransmits* : 再送信の最大回数。LOCP 要求の応答を受け取らなかった場合に、Location Appliance によって試行されます。有効な値は 1 ～ 99,999 秒（デフォルト値は 5 回）です。

最初の 2 つのパラメータは、Echo Request および Echo Reply コントロール メッセージにのみ適用できます。その他のパラメータはすべてのデータ メッセージで使用できます（Information、Measurement Requests、および Responses など）。

Cisco Unified Wireless Network ソフトウェア リリース 4.1 で、LOCP の初期フェーズを導入しました。このリリースでは、Wi-Fi タグ テレメトリと、WLAN コントローラから Location Appliance への通知トラフィック用の Cisco Compatible Tag Extensions を転送することによる従来の SNMP ポーリングの拡張のために LOCP が使用されます。このトラフィックには、次のものが含まれます。

- 次のものを含む、Cisco Compatible Extensions Wi-Fi Tag テレメトリ
  - 動作、温度、気圧、湿度、距離、数量、およびステータス
  - バッテリ状態と予測残量
- Cisco Compatible Extensions の高優先順位タグ トラフィック。次のものがあります。
  - ボタン呼び出し、タグ剥離イベント、改ざんアラート イベント。
  - チョークポイント トリガーに入る。
  - ベンダ固有のタグ情報（サードパーティ製のロケーション クライアントが使用）。

（注）　Cisco UWN ソフトウェア リリース 4.2 の使用を開始する場合、Location Control Protocol（LOCP）は追加の機能拡張を入手して、Network Mobility Services Protocol（NMSP）になります。

LOCP を使用する資産タグ テレメトリ

Cisco UWN ソフトウェア リリース 4.1 の使用を開始すると、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する Wi-Fi RFID タグは、タグ メッセージ ペイロードの一部として、タグ テレメトリ情報をロケーション認識 Cisco UWN に渡します。このテレメトリ情報は、アクセス ポイントが受け取り、WLAN コントローラが収集します。Location Appliance は、LOCP Information Requests を使用して、WLAN コントローラでタグ テレメトリを定期的にポーリングします。LOCP Information Response フレームを介した最後の LOCP ポーリング サイクルから、コントローラは、タグの MAC アドレスごとに、受信したテレメトリ情報に応答します。これらのフレーム（ポーリング交換プロセスと同様）は、図 3-28 に示されています。図に示す、Location Appliance および WLAN コントローラ間を流れるすべてのフレームは暗号化されます。

図 3-28　LOCP 情報要求のポーリング

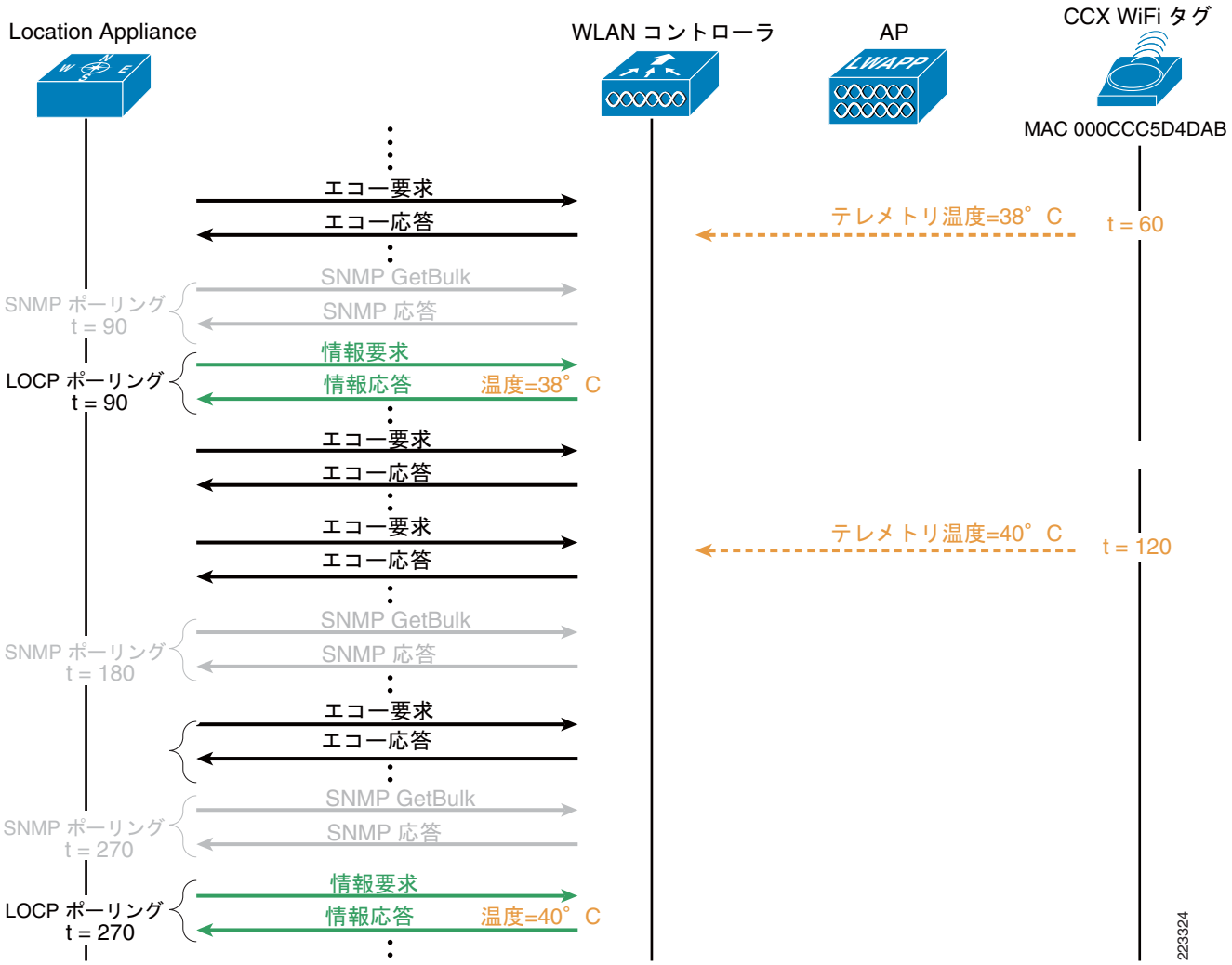


図 3-27 からもわかるとおり、LOCP ポーリング間隔は Location Appliance 設定で直接設定を行いません。代わりに、Location Appliance および WLAN コントローラ間で発生する資産タグ SNMP ポーリング間隔から導出されます。LOCP ポーリングをいつ送信するかを決定するために、Location Appliance では各ポーリング サイクルの間に次の条件を評価します。

- コントローラ ソフトウェア リリースが LOCP をサポートしているかどうか。LOCP ポーリングは、LOCP に対応していないコントローラには送信されません。
- 最後の LOCP ポーリングからの時間間隔が 180 秒の場合、SNMP ポーリング サイクルの間に LOCP ポーリングが実行されます。現在 Location Appliance に対して設定されているすべての LOCP 対応コントローラに LOCP Information Requests が送信されます。
- 最後の LOCP ポーリングからの間隔が 180 秒未満の場合、SNMP ポーリング サイクルの間に LOCP ポーリングは実行されません。

ソフトウェア リリース 4.1 で資産タグ テレメトリ情報を収集するために Location Appliance によって使用される LOCP ポーリング間隔は、次の式[1] を使用して、資産タグ SNMP ポーリング間隔から計算されます。

$$Poll_{NMSP} = \left\lceil \frac{180}{Poll_{TAG}} \right\rceil * Poll_{TAG}$$

$Poll_{LOCP}$ は LOCP ポーリング間隔を表し、$Poll_{TAG}$ はポーリング間隔を表します。この間隔で Location Appliance は SNMP を介してコントローラの資産タグロケーション情報をポーリングします。どちらの値も秒で指定します。PollTAG の値は、[Location Servers] > [Polling Parameters] を使用して WCS で設定されます。たとえば、資産タグ SNMP ポーリング間隔（$Poll_{TAG}$）の 120 秒を使用すると、Location Appliance によって使用される LOCP ポーリング間隔（$Poll_{LOCP}$）は 240 秒と計算されます。

LOCP および SNMP ポーリング間の関係と、タグ テレメトリを受信した場合の影響を明確に理解できるように図 3-28 を参照してください。ここで、温度テレメトリは Cisco Compatible Extensions Wi-Fi Tag 仕様に適合するタグ（MAC アドレス 00:0C:CC:5D:4D:AB、時間 t=60 秒）から送信されます。この送信は 1 つ以上のアクセス ポイントが受信します。これらのアクセス ポイントはテレメトリ情報（この例では温度 38° C）をそれぞれの登録済み WLAN コントローラに渡します。図 3-28 で、時間 t=90 秒で実行される SNMP ポーリングが最初のポーリングであるため（つまり、以前に LOCP ポーリングが実行されていないことも示す）、コントローラも時間 t=90 秒で LOCP ポーリングを受信します。これは図の、Information Request フレームの受信に示されています。コントローラは、すべての蓄積したタグ テレメトリ情報を LOCP Information Response フレームの Location Appliance に渡して、ポーリングに応答します。

タグが、チャネルごとに複数のフレーム コピー（またはバースト）を送信するよう設定されている場合、コントローラは重複するすべてのタグ テレメトリを削除し、重複を除外したテレメトリ値を Location Appliance に渡します。その後 Location Appliance はデータベースをこのテレメトリ情報で更新し、SOAP/XML API を介してロケーション クライアントが使用できるようにします。

後続のインバウンド テレメトリも類似の方法で処理されます。たとえば図 3-28 の時間 t=120 秒の、インバウンドの温度テレメトリ更新で、温度が 40 ºC に上がったことを示しているのがわかります。前述したイベント サイクルが再度実行され、テレメトリ更新が時間 t=270 秒で Location Appliance に送信されています。なぜ時間 t=180 秒ではなく時間 t=270 秒（この時点で SNMP ポーリングが実行されます）で Location Appliance にタグ テレメトリが渡されているのかを理解することが重要です。前述したとおり、LOCP ポーリングは、最後の LOCP ポーリングからの時間の差分が 180 秒以上の場合にのみ、実行されます。時間 t=180 秒で、以前の LOCP ポーリングからの時間の差分が 90 秒しか経っていないので、この場合は LOCP ポーリングは実行されません。

図 3-28 で、1 つのテレメトリ値のみを渡す 1 つのタグの例を示していますが、複数のタグからのテレメトリ値も同じように簡単に転送するように、LOCP は効率的に設計されています。各 Information Response フレームでは、複数のタグの MAC アドレスがコントローラで指定することができます。各 MAC アドレスは 1 つ以上のテレメトリ値と関連付けられています。たとえば、温度テレメトリのみを渡すのではなく、図 3-28 に示すタグには、温度、圧力、湿度などを含めることができます。これらすべての情報は、次の LOCP ポーリングで転送される Information Response に含められます。複数のタグからのインバウンド テレメトリ トラフィックは、同様の方法でコントローラによって集められ、各 LOCP エンドポイントでは、必要に応じて LOCP フレームのフラグメンテーションと再アセンブリを実行できます。

Location Appliance からの非同期ノースバウンド通知を介して「プッシュ」できるバッテリ状態情報を除いて、タグ テレメトリは SOAP/XML API を介して、ロケーション クライアントのみが使用できます。

1. $\lceil x \rceil$ は、正の整数 x に対する天井関数の適用を表します。これにより x が切り上げられ、x 以上の最小の整数が返されます。

タグ テレメトリ展開の検討事項については、「タグ テレメトリおよび通知に関する考慮事項」（P.6-26）を参照してください。

LOCP を使用する資産タグ通知

Cisco UWN ソフトウェア リリース 4.1 から、Cisco Compatible Extensions Wi-Fi tag 仕様に準拠する Wi-Fi アクティブ RFID タグが、オプションの高優先順位、チョークポイント、およびベンダー固有の通知イベントをロケーション認識 Cisco UWN に渡すことができるようになりました。高優先順位を示すタグ イベントは、タグ マルチキャスト メッセージ フレーム（イベントの特徴を示す追加のペイロード情報を含む）を介して 1 つ以上のアクセス ポイントで受信されます。この情報は、通常、イベントが発生したことをタグが検出したときに、資産タグによって送信されます。WLAN コントローラがいったん受信すると、これらのタイムクリティカルなイベントは、ポーリングされる LOCP ポーリング プロセスの外部で処理され、図 3-29 に示す LOCP 通知フレームを使用して Location Appliance にすぐに渡されます。

図 3-29　LOCP 通知

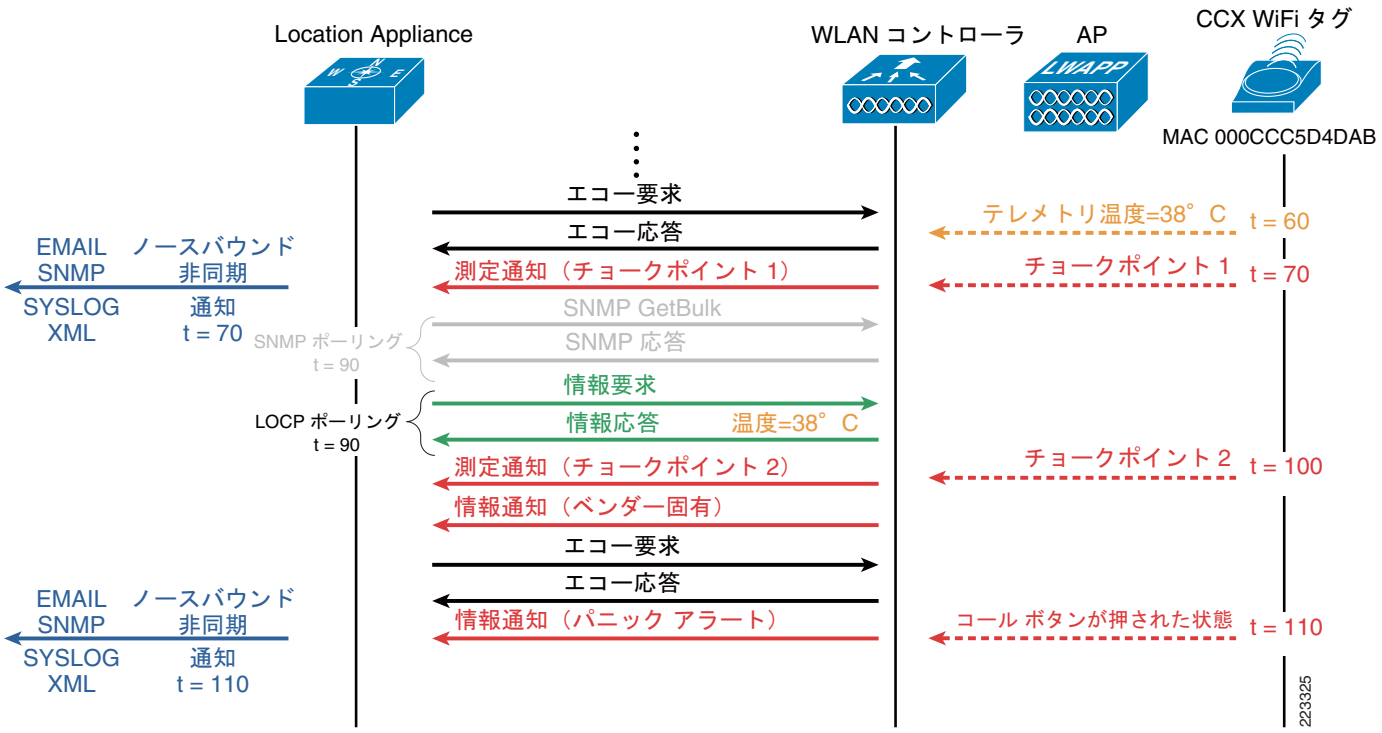


図 3-29 に、Cisco UWN ソフトウェア リリース 4.1、*Measurement Notification* および *Information Notification* でサポートされる、2 つの基本的な LOCP 通知タイプを示します。

- *Measurement Notifications*：リリース 4.1 で、測定通知は、タグが入るチョークポイント プロキシミティ デバイスの ID に関する情報の伝達に使用されます。Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するタグには、タグ コンテンツ フィールドのチョークポイント ID（チョークポイント MAC アドレスなど）が含まれています。この情報は、タグ MAC アドレスと同様に Location Appliance にリアルタイムで渡されます。また、ロケーション クライアント（WCS など）で使用して、タグが特定のチョークポイントの範囲内（または範囲外）にあるということを示すことができます。

- *Information Notifications*：リリース 4.1 では、情報通知はベンダー固有のデータと、次のようなタグの高優先順位イベントの伝達に使用されます。
  - タグ ユーザがタグのボタン呼び出しを抑制したとき
  - タグがフレームまたは付属の資産から取り除かれたことを検出したとき
  - タグが改ざんを検出したとき
  - 他のいずれかの高優先順位タグ イベントが発生したとき

  各タグ ベンダーが、製品の提供品に含めることを選択した機能を決定する一方で、Cisco Compatible Extensions Wi-Fi Tag 仕様では、タグ コンテンツ フィールドに含める一連の高優先順位情報を提供します。この情報は、タグ MAC アドレスと同様に Location Appliance に渡されます。また、ロケーション クライアント（WCS など）で使用して、高優先順位タグ イベントが発生したことを示すことができます。

  Cisco Compatible Extensions Wi-Fi Tag 仕様では、各タグ ベンダーが、タグからベンダー固有の情報（独自のタグ メッセージまたは追加のベンダー固有のチョークポイント情報など）を Cisco UWN にリアルタイムで渡すことができます。ベンダー固有の情報は、Cisco Location Appliance の SOAP/XML API インターフェイスを介して、変更されずにロケーション クライアントによって使用されるようになります。高優先順位イベント内で送信されるベンダー固有の情報もまた、SMTP、UDP-Syslog、SNMP トラップまたは SOAP トランスポートを使用して、Location Appliance からロケーション クライアントに非同期のノースバウンド通知を送信することができます。ロケーション クライアントは、これらのイベントをエンド ユーザにリアルタイムで提供するために、前述のポート上でこれらの通知を受信し、処理できる必要があります。

図 3-29 では、タグ テレメトリとは異なり、Location Appliance と WLAN コントローラ間のポーリング メカニズムには依存関係がないことを明確に示しています。LOCP 通知は、タグがこれらのイベントとやりとりし、WLAN コントローラから Location Appliance に対して生成されます。高優先順位タグ イベント、ベンダー固有データ、および範囲内のチョークポイント情報は、Cisco UWN リリース 4.1 の WLAN コントローラでは収集されません。このような情報を持つ各着信タグ マルチキャスト メッセージ（各登録済みアクセス ポイントからの WLAN コントローラによって受信）は、情報通知、または WLAN コントローラから Location Appliance への測定通知フレームを生成します。

タグ テレメトリの送信とチョークポイント、高優先順位またはベンダー固有の情報の送信間には、依存関係は存在しません。たとえば、タグは環境内のチョークポイント範囲を経由するときに、資産についてのテレメトリ情報をリレーします。図 3-29 に示すように、タグ テレメトリは次の LOCP ポーリング間隔まで、WLAN コントローラによって保持されます。ここで、範囲内のチョークポイントの表示は、WLAN コントローラによって測定通知の形式で Location Appliance にすぐに送信されます。

SOAP/XMP API を介してクライアントに更新情報を提供するほかに（たとえば、ロケーション クライアントが XML GetTagInfo または GetTagLocation 要求を発行したときなど）、Location Appliance は、LOCP 測定通知または情報通知を受信したときに、外部非同期ノースバウンド通知を送信することもできます（再度図 3-29 を参照）。これらの外部ノースバウンド通知は、SNMP、SMTP、SOAP、または UDP-Syslog トランスポートを使用して、次の条件のときに送信されます。

- ボタンの呼び出し、タグの改ざん、タグ剥離
- 範囲内のチョークポイント
- その他のプライオリティ イベント（ユーザ定義）

タグ通知展開の検討事項については、「タグ テレメトリおよび通知に関する考慮事項」（P.6-26）を参照してください。

CHAPTER 4

インストールおよび構成

Location Appliance のインストールと構成

Cisco Location Appliance のインストールと構成の詳細な手順は、次のドキュメントを参照してください。

- 『*Release Notes for Cisco Wireless Location Appliance Release 3.0*』
  http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html
- 『*Cisco Wireless Location Appliance: Installation Guide*』
  http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/loc27icg.html
- 『*Cisco Wireless Location Appliance: Configuration Guide*』
  http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html

ロケーション トラッキング用の Cisco WCS の設定

ここでは、Windows または Linux ベースの WCS をインストールし、Cisco Wireless Location Appliance のロケーション ライセンスが適切に付与されていることを前提として説明します。Cisco Wireless Location Appliance とともにロケーションで使用するための Wireless Control System 設定の詳細な手順は、次のドキュメントを参照してください。

- 『Cisco Wireless Control System Release Notes, Release 4.1』
  http://www.cisco.com/en/US/products/ps6305/prod_release_notes_list.html
- 『Cisco Wireless Control System Configuration Guide, Release 4.1』
  http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html
- 『Cisco Wireless Location Appliance: Deployment Guide』
  http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html

Location Appliance 履歴パラメータの設定

[Location Server] > [Administration] > [History Parameters] の設定については、次の URL にある『*Cisco Wireless Location Appliance Configuration Guide*』の「Editing History Parameters」を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg_ch4.html#wp1046373

これらパラメータの詳細については、以下の項で説明します。

Location Appliance の履歴機能についてよくある誤解は、クライアントでこれまで発生したすべてのロケーションの履歴レコードを何らかの形で保存しているというものです。次の 2 つの項で説明するように、Location Application は、アーカイブ期間とアーカイブ間隔パラメータの値に基づいて履歴情報を保存します。デバイスの履歴レコードが、時間 T_0、アーカイブ期間 30 で記録されている場合、そのデバイスに対する次の履歴レコードは T_{0+30} で書き込まれます。デバイスは T_0 と T_{0+30} の間で位置を何度か移動している可能性がありますが、時間 T_0 と T_{0+30} の時点のロケーション状態だけが履歴データベースに記録されます。

履歴アーカイブ期間

履歴アーカイブ期間（[Archive For] として表示される）では、Location Appliance が有効な履歴収集カテゴリごとにロケーション履歴レコードを保持する日数を指定します。デフォルトのアーカイブ期間は 30 日です。デフォルトの履歴アーカイブ期間に対する変更は、シスコのテクニカル担当者またはシスコの Technical Assistance Center に相談し、慎重に検討したうえで行う必要があります。履歴期間が長くなると、ロケーション履歴データベースで消費される容量が増えるためです。アーカイブ期間内の新しい履歴データは古いデータを上書きしないため、膨大なデバイスを対象に、履歴カテゴリを多数選択し、履歴アーカイブ期間を過度に長くすると、使用可能な空き領域を使い果たす可能性があります。

この点を理解するには、履歴カテゴリ、アーカイブ期間、アーカイブ間隔のある組み合わせを選択した場合に消費されるディスク ストレージ容量と、それ以外の場合を比較できます。比較のため、1100 台の WLAN クライアント、300 の資産タグ、20 の不正アクセス ポイント、30 台の不正クライアントからなる環境があると仮定します。図 4-1 に、次の場合のディスク ストレージ使用量への影響を示します。

- すべてのデバイス カテゴリでデフォルトのアーカイブ期間を 365 日に増やす。
- クライアント（「モバイル デバイス」）および資産タグに対するデフォルトの履歴アーカイブ間隔を 60 分に短縮する。

図 4-1　履歴間隔とアーカイブ期間のデータベース サイズに対する影響

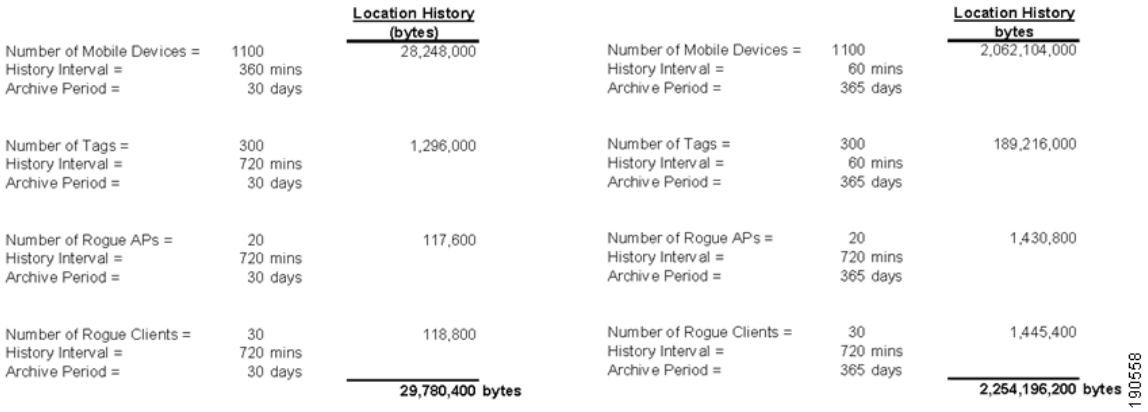


図 4-1 に示す推計は概算にすぎませんが（たとえば、これらはレコードあたりの表示文字列サイズとデータベースのオーバーヘッドを考慮していません）、ロケーション履歴の変更だけで、データベース サイズが約 30 MB から 2.25 GB 超まで増えています。Location Appliance 上のデータベース バックアップ メカニズムでは、少なくとも抽出と圧縮の確かな実行のために使用するだけの空き領域を確保する必要があります。そのため、推定される必要な領域合計は 5 GB を超えます。

履歴データベースの消去

データベースの消去は、ハードディスクの空き領域が少なくなっている場合に特に重要です。再びハードディスクの空き領域が少なくなった場合、データ消去間隔を短くして、ディスク領域が少なくなる前に消去をこまめに実行するようにします。データ消去間隔を短くする場合、ハードディスクの空き領域が少ない状況を解決するのに消去間隔の調整だけでは十分でないときは、履歴アーカイブ間隔を短くします。

Location Appliance 詳細パラメータの設定

[Location Server] > [Administration] > [Advanced Parameters] の設定は、次の URL にある『*Cisco Wireless Location Appliance Configuration Guide*』の「Editing Advanced Parameters」を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg_ch4.html#wp1050981

詳細パラメータの説明については、以下の項で説明します。

不明データのクリーンアップ間隔

「不明データのクリーンアップ間隔」または ADCI（1 ～ 99,999 分の範囲）では、アクティブ ロケーション データベース内で追跡エンティティ（WLAN クライアント、タグ、不正アクセス ポイント、不正クライアント）用にエントリが保持される合計時間を指定します。ADCI では、有効期限が切れる時間の長さを指定します。この時間を超えると、対象デバイスから最新の更新を受信しない場合、アクティブ ロケーション データベースから追跡対象デバイス エントリが削除されます。

たとえば、資産タグの RSSI 情報が、Location Appliance によって 2 日前に最後に記録され、クリーンアップ間隔がデフォルト値の 1440 分（24 時間または 1 日）に設定されている場合、不明データのクリーンアップ間隔（24 時間）の有効期限が切れた後、ステーションはアクティブ ロケーション データベースから削除されます。デバイスがアクティブ ロケーション データベースから削除された後は、[load location server data as old as] ドロップダウン メニュー コントロールを使用し、「スクロール バック」してデバイスの最後のロケーションを確認することはできません。

Location Appliance の合計 2,500 台の追跡対象デバイスという制限は、アクティブ ロケーション データベース内のデバイスに厳密に適用されます。アクティブ データベース内のデバイス合計数（クライアント、タグ、不正）が 2,500 台に達すると、現在アクティブ ロケーション データベース内に含まれているいくつかの追跡対象デバイスの有効期限が切れるか、データベースから消去するまで、この Location Appliance では追加デバイスの追跡はできません。

場合によっては、不明データのクリーンアップ間隔のデフォルト値のため、追跡環境から最近削除されたデバイスのクリーンアップが遅れている可能性があります。適切な例として、1,500 台の追跡対象の資産タグとクライアント ステーションを持つ Location Appliance で、オペレータが環境内での不正ロケーション トラッキング（不正デバイスを対象に）を有効にした場合を示します。たとえば、システムが 1,000 台の不正デバイスを検出した場合、これらはアクティブ ロケーション データベースに追加され、この Location Appliance での追跡対象デバイスの合計数が最大キャパシティの 2,500 台になります。タグ付き資産と WLAN クライアントのロケーション トラッキングの優先度が、不正デバイス追跡の優先度よりも高い場合、問題が発生する可能性があります。環境に新しいタグまたはクライアントが追加された場合、現在の追跡対象デバイス（既存の WLAN クライアント、資産タグ、不正デバイス）の有効期限が切れるか、アクティブ ロケーション データベースから消去するまで、追跡するための空き容量は確保できません。

（注）　ロケーション認識 Cisco UWN バージョン 4.2 では、Location Appliance の、どの追跡対象デバイスの容量を各追跡対象デバイス カテゴリ（たとえば、WLAN クライアント、資産タグ、不正デバイス）に割り当てるかを個別に制限できる拡張機能を導入しました。

この場合、Location Appliance 内で不正デバイスの追跡を完全に無効にしても、1,000 台の追跡対象デバイスはすぐに削除されず、不要な不正デバイスがアクティブ ロケーション データベースから削除されます。不明データのクリーンアップ間隔はデフォルトで、アクティブ ロケーション データベース内の現在の各追跡対象不正デバイスを、最後の RSSI 更新から 1440 分経過するまで保持します。簡潔に説明すると、ADCI のデフォルト値を使用したこの例では、不正なロケーション トラッキングを今日無効にしても、明日の同じ時刻になるまで、これらの追跡対象デバイスはアクティブ ロケーション データベースから完全に消去されません。

この問題に対処し、不要なデバイスをアクティブなロケーション データベースから即座に削除するには、一時的に不明データのクリーンアップ間隔を小さい値にし、アクティブなロケーション データベースから不要な追跡対象デバイスを早く消去できるようにします。たとえば、オペレータが、Location Appliance の不正デバイスに対するポーリングを無効にしてから、不明データのクリーンアップ間隔を 60 分後に一時的に設定することもできます。この設定が適用されてから 60 分後、Location Appliance はアクティブ ロケーション データベース（過去 1 時間、WLAN コントローラから更新情報を受信していない場合）から、不要な不正デバイスを含むすべてのデバイスを削除します。削除が実行されると、[Location Servers] > [Advanced Parameters] メニュー ページに表示される [Number of Tracked Elements] フィールドの値は、アクティブ ロケーション データベースから削除されたデバイスの数を反映して減少します。

不明データのクリーンアップ間隔は、すべてのデバイス カテゴリに適用される単一パラメータです。このように ADCI の値を一時的に小さくする際の短所は、アクティブなロケーション データベースからの追跡対象デバイスの削除が、非選択的に行われるということです。つまり、ADCI の時間条件を満たす Location Appliance によって更新情報が受信されていないすべてのデバイスは削除されます。この例では、不要な不正が削除されるだけではなく、過去 60 分間に更新を受信していないすべてのクラ

イアントまたは資産タグも削除されることを意味します。このような動作は、「失われた」資産（現在のロケーション情報を利用できない）を検出するために前もって 24 時間前からロケーション情報にアクセスしていたロケーション クライアント ユーザにとっては予期していないものです。

実験では、追跡対象デバイスがアクティブなロケーション データベースから削除されても、後から UWN によって再検出された場合、ロケーション履歴データベースを使用すると、部分的に移行できます。このような場合、履歴アーカイブ期間の有効期限が切れておらず、履歴レコードが消去されていなければ、以前収集したロケーション履歴レコードが再度参照できるようになります。アクティブなロケーション データベースから検出され、アクセス ポイントによって再検出されていないデバイスの履歴レコードは、ロケーション クライアントからアクセスできません。

場合によっては、不明データのクリーンアップ間隔のデフォルト値を、さらに大きくする必要があります。このような例として、ロケーション トラッキングを採用し、オンサイトに数時間だけいた後、移動して数日戻らないような、膨大な数の一時的な Wi-Fi デバイス（クライアント ラップトップ、PDA など）を持つファシリティが挙げられます。もう 1 つの例は、4 時間の間に 2,000 個のタグ付き資産コンテナのみしかないが、資産コンテナを通じて 10,000 個以上のタグ付き資産コンテナが 24 時間の間に通過するロジスティクス クロスドッキング ファシリティが挙げられます。

どちらの場合も、ある時点で実際にサイト上にある、追跡可能な Wi-Fi クライアント デバイスまたは資産タグの数は、Location Appliance の追跡対象デバイスの最大キャパシティよりかなり少ないです。ただし、24 時間の間にファシリティを通過する可能性のある一時的なデバイスの数は、容易に 2,500 台を超えます。不明データのクリーンアップ間隔のデフォルト値を使用している間にこの数を超えた場合、数時間前にファシリティを離れたデバイスが、ADCI の有効期限 24 時間が経つまでアクティブ ロケーション データベースから削除されないため、Location Appliance の追跡に使用する容量を使い果たすおそれがあります。不明データのクリーンアップ間隔に小さい値（たとえば、4 時間または 240 分）を設定すると、これらの移行されたデバイスのクリーンアップを迅速に処理し、Location Appliance の追跡対象デバイスの容量を解放して、到着する最新デバイスのために使用できます。

ただし、不明データのクリーンアップ間隔の値を小さくする方法に、欠点がないわけではありません。不明データのクリーンアップ間隔の詳細、値を変更した場合の欠点、この変更が全体の設計アプローチに与える影響については、「複数 Location Appliance の設計」（P.5-32）に示した例を参照することをお勧めします。

メモリ情報

- DB ディスク メモリ：適切な呼称ではありません。このパラメータは Location Appliance の「メモリ」を指しているのではありません。Location Appliance データベースによって消費されたディスク容量合計を表示します。この情報は、データベースの断片化解消を実行するかどうかを決定する場合に役立ちます（「詳細コマンド」（P.4-5）を参照）。
- Java GC の実行：このコマンドは、一般的なメモリ クリーンアップをすぐに実行します。通常、メモリ クリーンアップは自動的にシステムによって開始されるため、手動で開始する必要はありません。そのため、Java General Cleanup を実行する必要があるのは、Cisco Technical Assistance Center（TAC）または Cisco Engineering から指示があった場合のみです。

詳細コマンド

データベースの最適化詳細コマンドではロケーション データベースの断片化解消を行い、未割り当てで、未使用のディスク容量を再利用します。データベース サイズが大きくなったために Location Appliance 上の空きディスク容量が少なくなった場合、またはロケーション クライアントによってデータを要求されたときに Location Appliance の応答時間が著しく遅くなった場合に、データベースの断片化解消が役立ちます。

Location Appliance 上で現在利用可能な空き容量を確認するには、CLI シリアル コンソールまたは SSH セッションのいずれかから Location Appliance にログインする必要があります。ログインしたとき、次のように Linux コマンド **df -H** を使用してディスク空き容量を表示します。

```
[root@AeS_Loc root]# df -H

Filesystem            Size  Used Avail Use% Mounted on
/dev/sda2              77G  3.2G   70G   5% /
/dev/sda1             104M   16M   83M  16% /boot
none                  526M     0  526M   0% /dev/shm

[root@AeS_Loc root]#
```

（注） 上で **df –H** コマンドを使用するのは、1 GB = 1,000,000,000 バイトを前提とする、ほとんどのコンピュータ ディスクの製造業者の通例であるためです。**–H** オプションは、1,024 ではなく 1,000 の累乗で出力を表示します。1024 の累乗で表示したい場合は、**df –h** を使用します。

ここで示す **df** 表示出力は、未フォーマット、容量 80 GB のハードディスク ドライブを含む Location Appliance のものです。2 つの主なファイル システムが定義されていることに注意してください。/dev/sda1 は Linux ブート ファイル システムです。/dev/sda2 はルート ディレクトリ、ロケーション アプリケーション、すべてのデータベースを含みます。上の表示から、/dev/sda2 の空き容量全体の 5% のみを現在使用中だということがわかります。この場合、膨大な空き容量があるため、現時点では断片化解消の必要はありません。

df 出力情報とロケーション データベースのサイズを参照し（「メモリ情報」（P.4-5）で説明した DB ディスク メモリ）、Location Appliance データベースで設定できる、推奨最大サイズを見積もります。一見すると「最大推奨サイズ = 利用可能な空きディスク容量合計 – （OS サイズ + Location Application サイズ）」のように思われますが、データベース バックアップ プロセス時に使用されるフラット ファイル作成も考慮する必要があります。次の式を使用して、この追加の空き容量とシステム オーバーヘッド（Location Appliance のアップグレード イメージのダウンロードなど）を考慮に入れた、ロケーション データベースの最大推奨サイズを計算できます。

$$MaxDatabaseSize = \frac{TotalSpace - OSApplSpace}{2.3}$$

定義：

- *MaxDatabaseSize* は、データベースの最大推奨サイズ（バイト）です。

（注） *MaxDatabaseSize* は、残存する Location Appliance アップグレード イメージのクリーンアップをユーザが実行したことを前提としています。複数のアップグレード イメージが残っていると、これらの割り当てを超える追加の空き容量を消費します。

- *TotalSpace* は、/dev/sda2 上の利用可能な空き容量合計（GB）です。
- *OSApplSpace* は、Linux OS が占める容量と、/dev/sda2 上の Location Appliance に適用される容量の合計です。上に示した例では次のように計算できます。

  （使用済みのディスク容量（GB））–（Location Appliance データベースの現在のサイズ（GB））

Location Appliance データベースの現在のサイズは、[WCS] > [Location Server] > [Advanced Parameters] > [DB Disk Memory] で確認できます。この例で使用されているシステムの場合、DB ディスク メモリ = 24,608,768 バイトまたは .0246 GB です。このため、OSApplSpace = (3.2 - .0246 GB) つまり 3.175 GB です。

TotalSpace および OSApplSpace の値を等式に代入すると、Location Appliance データベースの最大推奨サイズを、(77 GB - 3.175 GB) / 2.3 = 73.825 / 2.3 = 32.0 GB のように計算できます。そのため、未フォーマット、容量 80 GB のハードディスク ドライブを持つ Location Appliance のデータベース バックアップ メカニズムを正常に動作させるために、Location Appliance の最大推奨サイズ（[DB Disk Memory] で表示されるとおり）は、32 GB を超えないようにしてください。

Location Appliance ロケーション パラメータの設定

[Location Server] > [Administration] > [Location Parameters] の設定については、次の URL の『*Cisco Wireless Location Appliance Configuration Guide*』の「Editing Location Parameters」を参照してください。

http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg_ch4.html#wp1050973

特定のパラメータについての説明は、後続の項で説明します。

計算回数の有効化

enable calculation time ロケーション パラメータは詳細デバッグ オプションで、内部ローカリゼーションの計算で使う合計時間のログ記録を有効にします。デフォルトでは無効にされています。位置の計算にオーバーヘッドが追加されるため、Cisco Technical Assistance Center（TAC）または Cisco Engineering に勧められた場合にのみ有効にします。

外壁（OW）ロケーションの有効化

WCS Map Editor では、内壁をフロア マップ上に配置できますが、Location Appliance では、パス損失モデルの評価、および位置の計算時に最大 50 の「厚肉」壁を考慮に入れることができます。厚肉壁とは、Map Editor で減衰値が 13 dB と定義されている壁です。WCS の "Wall Usage Calibration" パラメータ（[Monitor] > [Maps] > [Properties] > [Wall Usage Calibration]）が [Auto] に設定されている場合、Location Appliance は、調整プロセスの一部として実行された計算の間、厚肉壁によって取り込まれた減衰を動的に特定します。ただし、システム管理者はこのパラメータを [Use Walls] に設定することによって、すべてのケースで厚肉壁の減衰を考慮に入れるように選択することも、[Do Not Use Walls] を設定することによって、全体的に厚肉壁の使用を無効にすることもできます。

Enable OW Location は、Cisco UWN ソフトウェア リリース 4.0 以前（たとえば、Cisco Wireless Location Applianceor リリース 2.1 以前）で使用されていたパラメータです。*Enable OW Location* は、以前のリリースに対する下位互換性があるため、WCS リリース 4.1 の [Location Server] > [Administration] > [Location Parameters] メニューに表示されます。ただし、ソフトウェア リリース 4.1 では、このパラメータをデフォルト設定から変更しても、メリットはありません。

RSSI 破棄時間

- 相対的 RSSI 破棄時間：このパラメータは位置の計算で使用する RSSI サンプル時間の相対的な境界を意味します。最新の RSSI サンプルと最も古い使用可能な RSSI サンプル間の時間を指定します。デフォルトの相対的な RSSI 破棄時間は 3 分です。Location Appliance の通常動作時、このパラメータをデフォルト値のままにする必要があります。Cisco Technical Assistance Center（TAC）または Cisco Engineering に勧められた場合を除き、この値を*変更しないでください*。

- 絶対的 RSSI 破棄時間：このパラメータはロケーションの計算で使用する RSSI サンプル時間の絶対的な境界を意味します。デフォルトは 60 分です。これは、相対的な RSSI 破棄時間にかかわらず、60 分より古い RSSI サンプルはロケーションの計算に使用されないことを意味します。Location Appliance の通常動作時、このパラメータをデフォルト値のままにする必要があります。Cisco Technical Assistance Center（TAC）または Cisco Engineering に勧められた場合を除き、この値を*変更しないでください*。

RSSI の遮断

受信した RSSI レポートに対して、前述の相対的および絶対的時間制約を適用するほか、Location Appliance は *RSSI の遮断*として知られるパラメータも適用します。「*RSSI 破棄時間*」で説明した時間制約に従い、Location Appliance は最も高い 4 つの信号強度レポートと、RSSI の遮断で指定した値に合致する、または超えるすべての信号強度レポートを保持します。RSSI の遮断のデフォルト値は -75 dBm です。

RSSI の遮断しきい値の適用について、次の例に示します。

- 4 つの RSSI レポート（-68dBm、-70dBm、-72dBm、-80dBm）：最も高い 4 つのレポートのため、4 つすべてのレポートが保持されます。
- 5 つの RSSI レポート（-66dBm、-68dBm、-70dBm、-72dBm、-74dBm）：すべてのレポートはデフォルトの RSSI の遮断のしきい値に合致する、又は超えているため、5 つすべてのレポートが保持されます。
- 5 つの RSSI レポート（-66dBm、-68dBm、-70dBm、-72dBm、-80dBm）：最初の 4 つのレポートが保持されます。5 つ目のレポート -80dBm は、デフォルトの RSSI の遮断のしきい値 -75 dBm を満たしておらず、しきい値を満たす、または超える 4 つの信号レポートがすでに存在するため破棄されます。

Location Appliance 通知パラメータの設定

[Location Server] > [Administration] > [Notification Parameters] の設定は、次の URL にある『*Cisco Wireless Location Appliance Configuration Guide*』の「Configuring Notification Parameters」を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg_ch6.html#wp1053921

特定のパラメータについての説明は、次の項で説明します。

Queue Limit

Queue Limit パラメータは、Location Appliance の出力通知キューのサイズを指定します。この値は通常、デフォルトの 500 にします。Location Appliance は、出力通知キューサイズを超えた場合、この制限を超えたすべての出力通知を破棄します。そのため、出力通知が破棄されたことに気づいた場合（[Notifications Dropped] フィールドから）、キュー制限サイズを増やすこともできます。

Retry Count

一致条件ごとに、Retry Count は同じデバイスに対して許可されるノースバウンド通知の「発行」数を指定します（初回発行に加え、通知を発行する数）。この回数を超えると、[Refresh Time] パラメータで指定した待機時間が開始します。このように、Refresh Time 間隔の間で許可されるノースバウンド通知の「発行」の合計数は、[Retry Count] で指定した値に 1 を加えたものと等しくなります。Retry Count のデフォルト値は 1 です。

次の点に注意してください。

- 1 を超える実際のノースバウンド通知メッセージは、「発行」ごとに送信できます（たとえば、SMTP、Syslog、SNMP、または SOAP）。
- Retry Count と Refresh Time は個別に、一致したデバイスの MAC アドレスに適用されます。
- Retry Count と Refresh Time は個別に、イベント定義に適用されます。ただし、同じデバイスの MAC アドレスに対する同じトリガー条件に適用されるイベント定義では、Retry Count/Refresh Time パラメータ セットを共有しています。

例として、Location Appliance は、高プライオリティ条件が特定の資産タグで発生した場合、SNMP、電子メール、syslog ノースバウンド通知を転送するように設定されていると仮定します。この例の目的のため、高プライオリティ イベントで、資産タグ上のボタンの呼び出しが抑制されている（AeroScout T2 または T3）と仮定します。また、通知の Refresh Time が 60 分に設定されており、通知 Retry Count が 1 に設定されていると仮定します（デフォルト値）。この条件の下、Location Appliance は、このタグで発生する各高プライオリティ イベントの SNMP、電子メール、syslog ノースバウンド通知を生成します（最大 2 ノースバウンド通知）。Retry Count に 1 を加えた値に達した後、Location Appliance は、この条件、および Refresh Time で指定された時間間隔のデバイスでの、以降のノースバウンド通知の発行を省きます。Refresh Time の有効期限が切れると、イベントがクリアされないかぎり、このサイクルが繰り返されます。

Refresh Time

Refresh Time は、「Retry Count」（P.4-9）で説明したとおり、特定のイベント条件およびデバイスに対して設定されたノースバウンド通知の転送間の待機時間を指定します。Refresh Time の有効期限が切れた後、イベント条件は再評価の対象となります。依然として存在する場合は、ノースバウンド通知をもう一度生成します。

Refresh Time と Retry Count は、クリアされていないイベントに対して繰り返し生成されるノースバウンド通知の数を制限するために合わせて使用されます。Retry Count は、Location Appliance によって送信されたノースバウンド通知の数を制限します。一方 Refresh Time は「待機時間」を設定します。この時間の間は、このイベント条件およびデバイスに対してノースバウンド通知が送信されません。

Refresh Time は分で指定します。デフォルトは 60 分です。

Notifications Dropped

これは読み取り専用のカウンタ フィールドで、Location Appliance が起動されてから通知キューから破棄された通知の合計数を示します。Location Appliance ソフトウェア アプリケーション（locserverd）を再起動すると、このカウンタはリセットされます。破棄される通知の合計数を減らすために Notifications Dropped カウンタは Queue Limit パラメータとともに使用する必要があります。

Location Appliance LOCP パラメータの設定

[Location Server] > [Administration] > [LOCP Parameters] の設定は、次の URL にある『*Cisco Wireless Location Appliance Configuration Guide*』の「Configuring LOCP Parameters 」を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg_ch4.html#wp1050918

Location Appliance の二重イーサネット運用

Cisco Wireless Location Appliance には、2 つの 10/100/1000BASE-T Gigabit Ethernet ポートを備えられています。これらのポートは、2 つの異なる IP ネットワークに対して Location Appliance を「デュアルホーム接続」するために使用できます。このため、たとえば Location Appliance をネットワーク "A" 上のサービス用に設定し、同時に必要に応じてネットワーク "B" 上の帯域外で管理する機能を提供します。この詳細な手順については、次の URL の『*Cisco Wireless Location Appliance Installation Guide*』の「Configuring the Location Appliance」を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html#wp1040696

Location Appliance 上のデュアル オンボード Ethernet コントローラは、同一の IP ネットワークへの冗長または同時接続を目的としていないことに、特に注意する必要があります。同一の IP ネットワークへの並列、ロード バランシング、または冗長 Ethernet 接続を確立することを目的とした設定は、現時点ではお勧めしません。

Location Appliance のデフォルト パスワードの変更

"root" ユーザ Linux システム パスワードの変更

Location Appliance には、出荷時にデフォルト root ユーザ ID とパスワードが設定されています。Location Appliance の初期設定時に root ユーザ ID のパスワードを変更して、ネットワーク セキュリティを最適化することをお勧めします。この設定は、初期セットアップ スクリプトの実行時に実行できます。次の URL の『*Cisco 2700 Series Location Appliance Installation and Configuration Guide*』の「Installation and Configuration」を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html#wp1049597

ログインしたときに、Linux コマンド **passwd** を使用して、次のようにルート システム パスワードを変更できます。

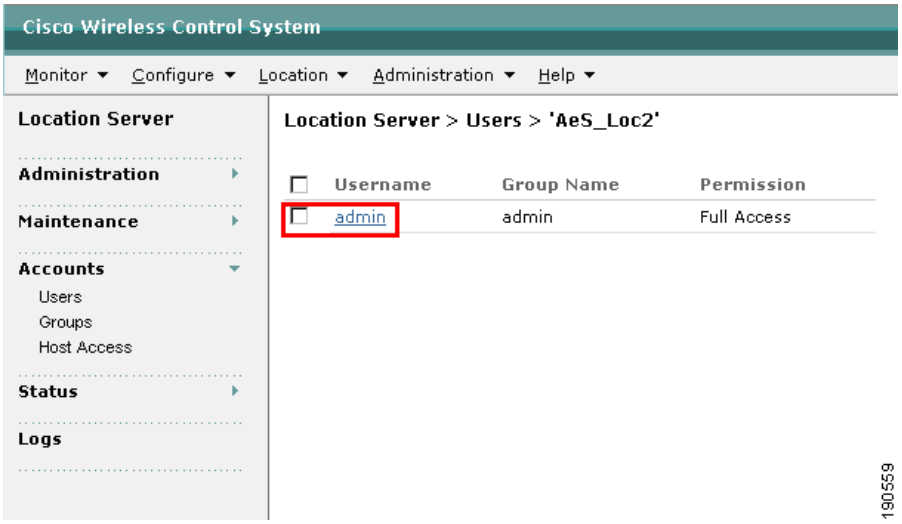
```
AeS_Loc login: root
Password:
Last login: Thu Oct 22 09:53:21 on ttyS0
[root@AeS_Loc root]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@AeS_Loc root]#
```

"admin" Location Server Application パスワードの変更

Location Appliance 上のロケーション サーバ アプリケーションには、出荷時に管理者ユーザ アカウントと定義済みのグループが設定されています。ユーザ ID は *admin* で、パスワードは *admin* です。WCS が、工場出荷時の管理者資格情報を使用して、正常にロケーション サーバ アプリケーションに接続した後、WCS メニューの [Location] > [Accounts] > [Users] メニューから、admin アカウント上のデフォルト パスワードをよく知られていない値に変更できます。

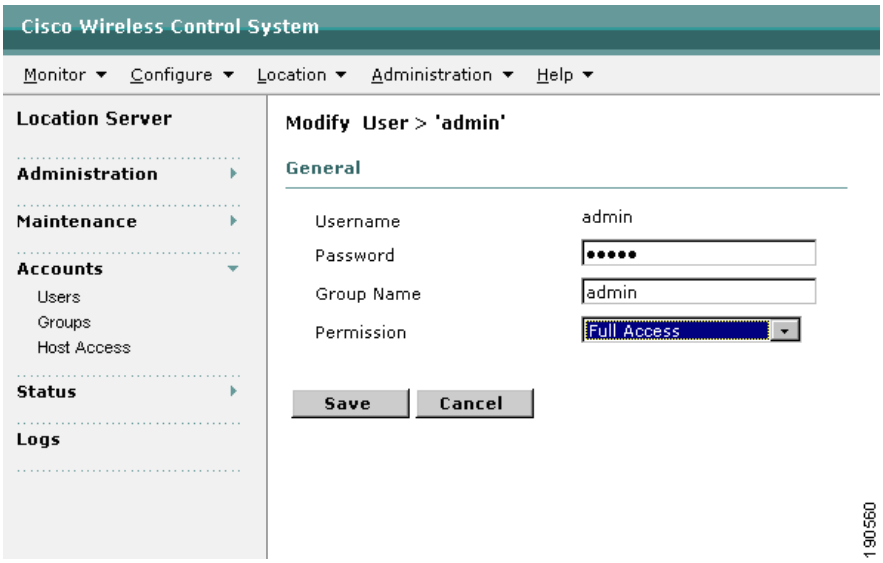
ステップ 1　図 4-2 に示すように、**admin** ユーザ ID をクリックして開始します。

図 4-2　デフォルトの Location Appliance ユーザ ID



ステップ 2　[Admin] ボックスをクリックすると、図 4-3 に示すメニューが表示されます。これにより、admin ユーザ ID のパスワードを変更できます。

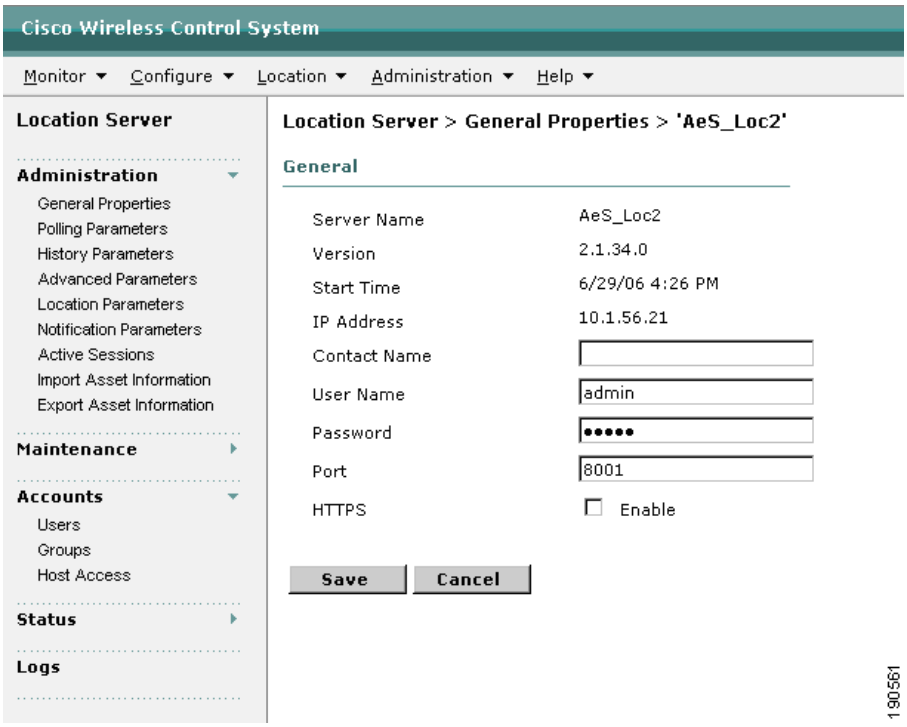
図 4-3　Admin パスワードの変更



ステップ 3　最後に、ロケーション サーバ アプリケーションにアクセスするために WCS が使用するパスワードの値を、図 4-3 で指定した新しい値に変更します。この変更は、図 4-4 に示すように、[Location Server] > [Administration] > [General Properties] から実行できます。

SOAP/XML API を介したロケーション サーバ アプリケーションへのアクセスに admin ユーザ ID を使用するように設定されたすべてのサードパーティ製のクライアントも、それぞれ変更する必要があります。クライアントの使用を許可する代わりに、Location Appliance にアクセスするサードパーティ製のロケーション クライアントごとに個別のユーザ ID を定義することもできます。

図 4-4　ロケーション サーバ アプリケーションのログイン資格情報の指定



Location Appliance の時間同期

ネットワーク全体で信頼性と一貫性のある操作を保証するために、Cisco UWN 内の WLAN コントローラ、Location Appliance および WCS システムで同期化された内部クロックを保持することをお勧めします。ネットワークに関する一般的な推奨事項として、同期化された内部クロックを設立すると、コンポーネント間の長いメッセージの相互関連付けが簡単になるため、トラブルシューティングに役立ちます。さまざまなコンポーネント、または結合した syslog から個別のログ ファイルを表示したり、ログ エントリを使用して一貫性のあるタイム スタンプ参照をメッセージ テキスト内で使用するようにする方法は、これらのメッセージを論理的にし、理解しやすくするのに役立ちます。

この一貫性のあるタイム スタンプの実用性は、複数の Location Appliance で非同期のノースバウンド通知を共通の宛先（たとえば電子メール メッセージなど）に送信するように設定したときに特に明らかになります。正しくないシステム時間が設定されている Location Appliance は、通知メッセージを発行することがあります（図 4-5 に示すように、正しくない、または一貫性のない時刻が設定されている場合、Network Operations Center（NOC; ネットワーク オペレーション センター）または他のコントロール ポイントにいるオペレータから見るとまぎらわしくなります）。

図 4-5　Location Appliance のタイム スタンプが設定されている電子メール通知メッセージ

Network Time Protocol（NTP; ネットワーク タイム プロトコル）は推奨される方法です。この方法を使用すると、共通クロック ソースを設立し、継続的に内部クロックの同期化を維持できます。Cisco Wireless Location Appliance には、*ntpd* として知られるユーティリティ デーモンが含まれており、企業ネットワーク内に配置されている NTP サーバの NTP クライアントとして動作します。ネットワーク NTP サーバがすべてのデバイスに対して共通の基準時刻ソースを提供します（通常、Coordinated Universal Time（UTC; 協定世界時）標準（以前は Greenwich Mean Time（GMT; グリニッジ標準時と呼ばれていた）を使用）。

（注）　ソフトウェア リリース 4.1 およびそれ以前では、時間の同期化を適切に行うことを推奨します。ただし、リリース 4.2 およびそれ以降では、Location Appliance と WLAN コントローラ間の認証を正しく行うために、適切な時間の同期化が必須です。

Location Appliance での ntpd デーモンの設定およびアクティブ化については、次の URL の「NTP Configuration and Synchronization for Unified Wireless Network Devices – Set Up NTP on the Location Appliance」を参照してください。
http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a0080811274.shtml#setup-la

NTP 設定情報については、次の URL の『*Cisco 2700 Series Location Appliance Installation and Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/li31main.html#wp1057105

ネットワーク内の NTP に関する追加のバックグラウンド情報および一般的なベストプラクティスについては、次の URL の「*Network Time Protocol: Best Practices*」を参照してください。
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Location Appliance の停止

Location Appliance は、継続的なインストール、操作向けに設計されているため、物理的な機器移動、またはデータ センターの所定のシャットダウンなどの特別なイベントに備えてアプライアンスを停止する必要がある場合があります。所定のシャットダウンを行わずに Location Appliance の電源を取り外すと、この時点で開いているファイルが破損する可能性があります。Location Appliance のオペレーティング システムで、ファイル システムの破損を最小限にする ext3 ジャーナリング ファイル システムを使用しているとしても、一般に、下記に示す手順に従ってすべてのアプライアンス ソフトウェア ファシリティの所定のシャットダウンを開始するのがベストプラクティスであるとされています。

Location Appliance の電源を切るには、アプライアンス CLI コンソールまたはリモート SSH デバイス セッションのいずれかから次の手順を実行します。

（注）　CLI コンソールを Location Appliance に接続する方法については、次の URL の『*Cisco Wireless Location Appliance: Installation Guide* 』の「Connecting and Using the CLI Console」を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/quick/guide/loc27icg.html

ステップ 1　次のコマンドを実行して Location Server ソフトウェアを手動で停止し、表示される以下の結果を確認します。

```
# /etc/init.d/locserverd stop
Shutting down locserverd: Request server shutdown now...
Waiting for server...2 secs
Waiting for server...4 secs
```

```
                .
                .
                .
                .
Waiting for server...60 secs
Server shutdown complete.
#
```

ステップ 2　Location Appliance の電源を取り外す前に、次のコマンドを実行してすべてのファイル システムをアンマウントし、すべてのサービスを停止し、Linux オペレーティング システムの所定のシャットダウンを開始します。

```
# shutdown -h now
```

CLI コンソール デバイスからこのコマンドを実行すると、次の出力が表示されます。

```
Shutting down console mouse services: [  OK  ]
Stopping sshd:[  OK  ]
Stopping xinetd: [  OK  ]
Stopping crond: [  OK  ]
Saving random seed:  [  OK  ]
Killing mdmonitor: [  OK  ]
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
Shutting down interface eth0:  [  OK  ]
Shutting down loopback interface:  [  OK  ]
Shutting down audit subsystem[  OK  ]
Starting killall:  [  OK  ]
Sending all processes the TERM signal...
Sending all processes the KILL signal...
Syncing hardware clock to system time
Turning off swap:
Turning off quotas:
Unmounting file systems:
Halting system...
md: stopping all md devices.
flushing ide devices:
Power down.
```

SSH セッションでリモート SSH クライアントから **shutdown** コマンドを実行すると、切断されます。Location Appliance はシャットダウン プロシージャを開始しますが、SSH セッションはコマンドが完了する前に切断されます。そのため、CLI コンソール デバイスで表示されるように、すべてのコマンド出力を表示することはできません。この可視性の阻害に対処するために、可能であれば SSH セッションではなく、Location Appliance コンソール端末に接続する端末または PC を使用してこのタスクを実行することをお勧めします。

ステップ 3　最後の手順で、前面パネルのオン / オフ スイッチを使用して Location Appliance の電源をオフにし、Location Appliance の電源を取り外します。この手順は、"power down" メッセージが CLI コンソール（上図に太字で表示）に表示された後に行います。リモート SSH セッションを使用する場合、shutdown コマンドの実行後すぐにセッションが切断されるため、"power down" メッセージは表示されません。この場合、shutdown コマンドが完了するまで約 2 分間待ってから、前面パネルの電源スイッチを使用して Location Appliance の電源を取り外します。

CHAPTER 5

ベスト プラクティス：ロケーション認識 WLAN 設計の考慮事項

この 10 年間で、エンタープライズ対応の無線 LAN の設計は、カバレッジの広さと最小限のアクセス ポイントを重視したモデルから、カバレッジの均一性と適切なセル間オーバーラップを最優先するモデルへと変化してきました。その背景には、無線音声（ジッタへの不耐性や高速ローミングでの遅延が見られます）など、新しい無線アプリケーション展開への関心が高まってきたことがあります。同様に、Wi-Fi 無線 LAN を使用したロケーションベースのアプリケーションを展開するには、「まったく新しい」ロケーション認識システムを設計すると同時に、既存の設計を拡張または改善する必要があります。

この章では、ロケーション認識無線 LAN の設計および展開でのベスト プラクティスについて説明します。この章は、主に次のような項で構成されています。

- 「信号レベルの最小しきい値」（P.5-2）
- 「アクセス ポイントの配置」（P.5-5）
- 「アクセス ポイントの間隔」（P.5-12）
- 「ロケーション準備の確認」（P.5-18）
- 「ロケーション、音声、データの共存」（P.5-20）
- 「ロケーション表示ジッタの回避」（P.5-31）
- 「複数 Location Appliance の設計」（P.5-32）
- 「アンテナに関する考慮事項」（P.5-44）
- 「調整」（P.5-48）
- 「ロケーション品質の検査」（P.5-63）
- 「テスト ポイントを使用した確度の確認」（P.5-67）

信号レベルの最小しきい値

モバイル デバイスを正確に追跡するには、最低 3 台のアクセス ポイント（最適な確度のためには 4 台以上が望ましい）が、追跡対象となるすべてのクライアント ステーション、資産タグ、または不正デバイスの受信信号強度（RSSI）を検出し、報告する必要があります。この場合、検出される信号強度レベルは、-75 dBm 以上であることが推奨されます。

（注）　WLAN コントローラ ソフトウェア リリース 4.1.185.0 以降、追跡される各エンティティ（WLAN クライアント、RFID タグ、不正アクセス ポイント、または不正クライアント）は、各 WLAN コントローラにおいて随時に最大 16 台の登録アクセス ポイントによって検出されます。これにより、最新のデバイス RSSI が適切に反映されることが確実になるため、多くのアクセス ポイント カバレッジ セル間で移動するデバイスをトラッキングする機能が改善されます。

クライアントまたはタグの追跡が行われる領域のサイト調査を実施するときは、代表的なデバイスの RSSI に関し、推奨されるアクセス ポイントの最小数および推奨される検出信号強度を確実に順守したうえで検証を行う必要があります。この検証は、以下の 2 つの方法のいずれかによって行うことができます。

- コントローラの CLI コマンド **show client detail <*mac address*>** または **show rfid detail <*mac address*>** を使用して、クライアントまたは資産タグに関して検出された RSSI を表示する（図 5-1 を参照）。
- ロケーション フロア マップ GUI を使用して、クライアントまたは資産タグに関して検出された RSSI を表示する（図 5-2 および図 5-3 を参照）。

図 5-1　WLAN コントローラでのクライアント RSSI のチェック

```
(Cisco Controller) >show client detail 00:07:50:d5:e4:77

Client MAC Address.............................. 00:07:50:d5:e4:77
Client Username ................................ N/A
AP MAC Address.................................. 00:14:1b:59:41:f0
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:14:1b:59:41:f0
Channel......................................... 1
IP Address...................................... 10.1.67.252
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
Client CCX version.............................. 2
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Local
Mobility Move Count............................. 0
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... vlan64
VLAN............................................ 64
Client Capabilities:
      CF Pollable.............................. Not implemented
      CF Poll Request.......................... Not implemented
      Short Preamble........................... Implemented
      PBCC..................................... Not implemented
      Channel Agility.......................... Not implemented
      Listen Interval.......................... 0
Client Statistics:
      Number of Bytes Received................. 2816
      Number of Bytes Sent..................... 872
      Number of Packets Received............... 19
      Number of Packets Sent................... 6
      Number of Policy Errors.................. 0
      Radio Signal Strength Indicator.......... -45 dBm
      Signal to Noise Ratio.................... 55 dB
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      AP1242#1(slot 0) .........................
antenna0: 82 seconds ago -63 dBm................. antenna1: 82 seconds ago -68 dBm
      AP1242#2(slot 0) .........................
antenna0: 82 seconds ago -54 dBm................. antenna1: 82 seconds ago -59 dBm
      AP1242#3(slot 0) .........................
antenna0: 82 seconds ago -45 dBm................. antenna1: 82 seconds ago -41 dBm
      AP1242#4(slot 0) .........................
antenna0: 82 seconds ago -65 dBm................. antenna1: 82 seconds ago -68 dBm
      AP1242#5(slot 0) .........................
antenna0: 82 seconds ago -64 dBm................. antenna1: 82 seconds ago -66 dBm
```

223326

これらの方法を行うとき、いずれの場合も、ローカリゼーションが必要な領域にある代表的なテスト クライアントと資産タグを使用する必要があります。このチェックを実施するとき、すべてのアクセス ポイントとアンテナが設置され、最終的な設定が行われていることを確認することが重要です。サポートされる最大送信電力レベルとテスト クライアントの調査はいずれも、可能な限り、追跡するプロダクション クライアントと同様になるようにする必要があります。図 5-1 は CLI コマンドの出力結果です。これは、同じコントローラに登録されているクライアントを検出するアクセス ポイントにおいて、すべてのアクセス ポイントで検出されたときの、そのクライアントの信号強度を示しています。検出用アクセス ポイントのレジストレーションが 2 台以上のコントローラに分散される状況では、複数の CLI セッションが必要になります。図 5-1 に示す赤枠内のデータから、対象のクライアントが 3 台以上のアクセス ポイントによって、推奨される信号強度レベル以上で検出されているかどうかが明らかに

なります。図 5-1 で WLAN クライアントについて示されているように、CLI コマンド **show rfid detail <*HHHH*mac address>** を使用して、資産タグについて検出された RSSI 情報を表示することができます。

これと同じ情報を、ロケーション マップ GUI によってグラフィカルに表示することもできます。いずれかの WLAN クライアント アイコン（青色の四角形）または資産タグ アイコン（黄色のタグ）をクリックすると、ロケーション デバッグ チェックボックスが有効になり、縮小版のロケーション マップが拡大されます（図 5-2 および図 5-3 を参照）。

図 5-2　　ロケーション デバッグの有効化

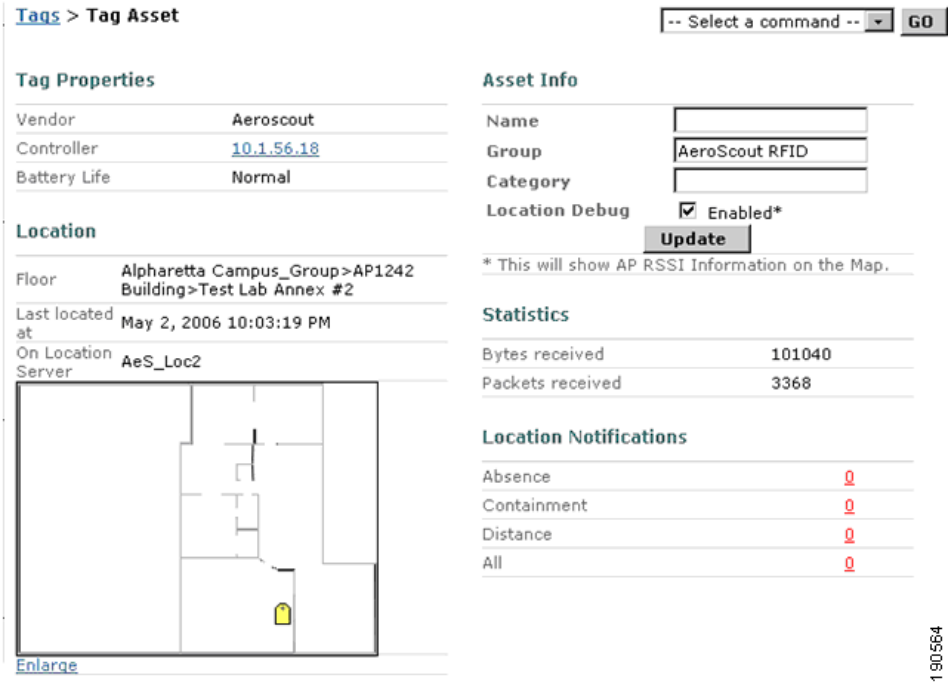
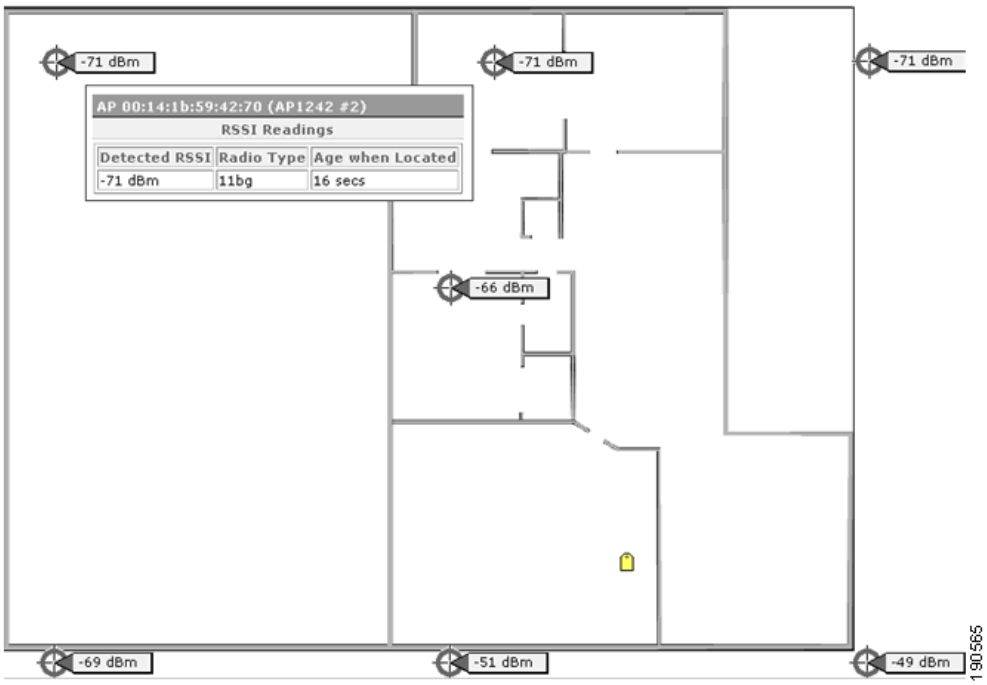


図 5-3　検出された RSSI の表示（GUI を使用）



アクセス ポイントの配置

アクセス ポイントの適切な配置は、ロケーション認識機能を提供する Cisco Unified Wireless Network の潜在的なパフォーマンスを十分に発揮させるために必要となるベスト プラクティスの 1 つとして挙げられます。多くの既存のオフィス無線 LAN では、アクセス ポイントが内部空間全体に分散されるため、周辺の作業領域にまでサービスを提供することになります。これらのアクセス ポイントのロケーションは、カバレッジ、WLAN の帯域幅、チャネルの再利用、セル間のオーバーラップ、セキュリティ、美観、および展開の実現可能性に基づいて選択されます。ロケーション認識 WLAN 設計では、基礎データと音声アプリケーションの要件を、良好なロケーション忠実度を実現するための要件と組み合わせて検討する必要があります。サイトによりますが、ロケーション認識機能を提供する Cisco UWN の要件には、Cisco ベスト プラクティスに従って設計されている音声システムにロケーション追跡機能を追加するなど、十分な柔軟性があります。この場合、広範囲にわたる再作業は求められません。対象領域の特性によっては、音声のベスト プラクティスに従って展開されているインフラストラクチャは、多くの場合、ロケーション トラッキングのベスト プラクティス要件も同様に満たすように増強できます（たとえば、周辺部アクセス ポイントの配置を行うなど）。

ロケーションの準備が完了した設計では、アクセス ポイントを内部で単にクラスタ化するだけではなく、フロアの中心部に向かうようにすることが重要です。より正確に言うと、周辺部アクセス ポイントがフロアの内部領域に配置されているアクセス ポイントを補完する必要があります。さらに、アクセス ポイントはフロアの四隅にそれぞれ配置しなければなりません。四隅以外にも、フロア周囲に隅（角）になるところがあれば、その場所にもアクセス ポイントを配置することが必要です。これらの周辺部アクセス ポイントは、その領域内での良好なロケーション忠実度を確保するうえで重要な役割を果たします。場合によっては、一般的な音声カバレッジやデータ カバレッジのプロビジョニングにも関与することがあります。

チョークポイント ロケーションを使用する場合は、チョークポイント トリガーの設置を予定しているすべての領域が、アクセス ポイントの範囲内にあることを確認してください。設計を厳密に行うことで、チョークポイント領域内に配置されている資産タグから送信されるメッセージがシステムによって

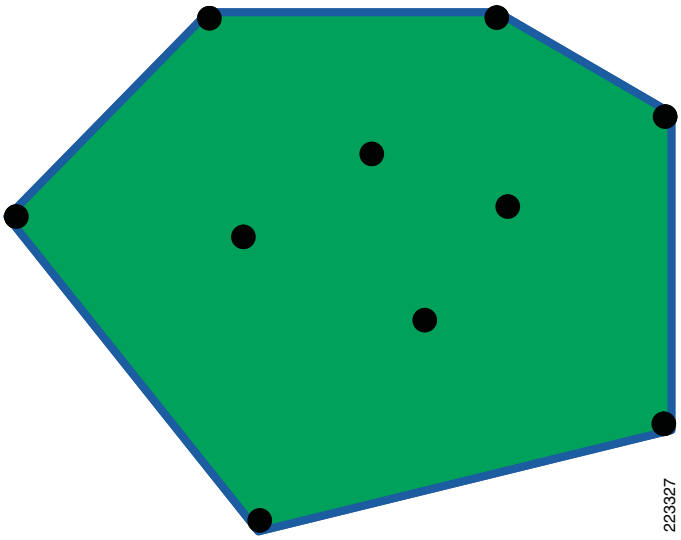
適切に受信されるだけでなく、資産タグがチョークポイントに向かうときやチョークポイントから離れるときに、RF フィンガープリントを使用して資産タグを追跡できるようになります。RF フィンガープリントを使用して資産タグを追跡する機能は、高い精度を備えたチョークポイント ロケーション技術を駆使してチョークポイント領域内にあるタグ付き資産の場所を特定するシステム機能を補完します。

フロア周辺部を形成するアクセス ポイントは、高い確度や精度を実現する可能性が最も高い「*凸包*」またはデバイス ロケーションのセットであると考えることができます。定義によると、*S* ポイントのセットである凸包（「*凸包（S）*」と示します）は、最小の多角形 *P* と見なすことができます。この場合、それぞれの *S* ポイントは *P* の境界線上または内部に配置されています。

図 5-4 は、凸包の概念を示したものです。図 5-4 では、アクセス ポイント ロケーションのセットは黒いドットで示されると仮定し、これを「セット S」と呼びます。セット S の凸包（凸包（S））は、ゴムバンド（青色の線で示されています）として比喩的に表現されています。このゴムバンドは、伸ばして、セットの最も外側にあるメンバー（このケースでは、周辺部アクセス ポイントを表します）にスナップすることができます。

このバンドで囲まれる内部領域（緑色で描かれています）は、良好なロケーション確度を実現する可能性が高いととらえることができます。追跡対象のデバイスが凸包の外側（図 5-4 に示す緑色の領域の外側）の領域に入り込むと、確度は下がり始めます。展開されているアクセス ポイントの数や、アクセス ポイント間の間隔によって異なることがありますが、一般的に、追跡対象のデバイスが凸包の外側から離れるほど、この確度は直線状に低下します。たとえば、凸包内部では 10m/90% 以下の確度を実現するデバイスは、その外側 20 フィートの位置に移動すると、その確度は 18m/90% まで低下することがあります。

図 5-4　　ポイントのセットによる凸包

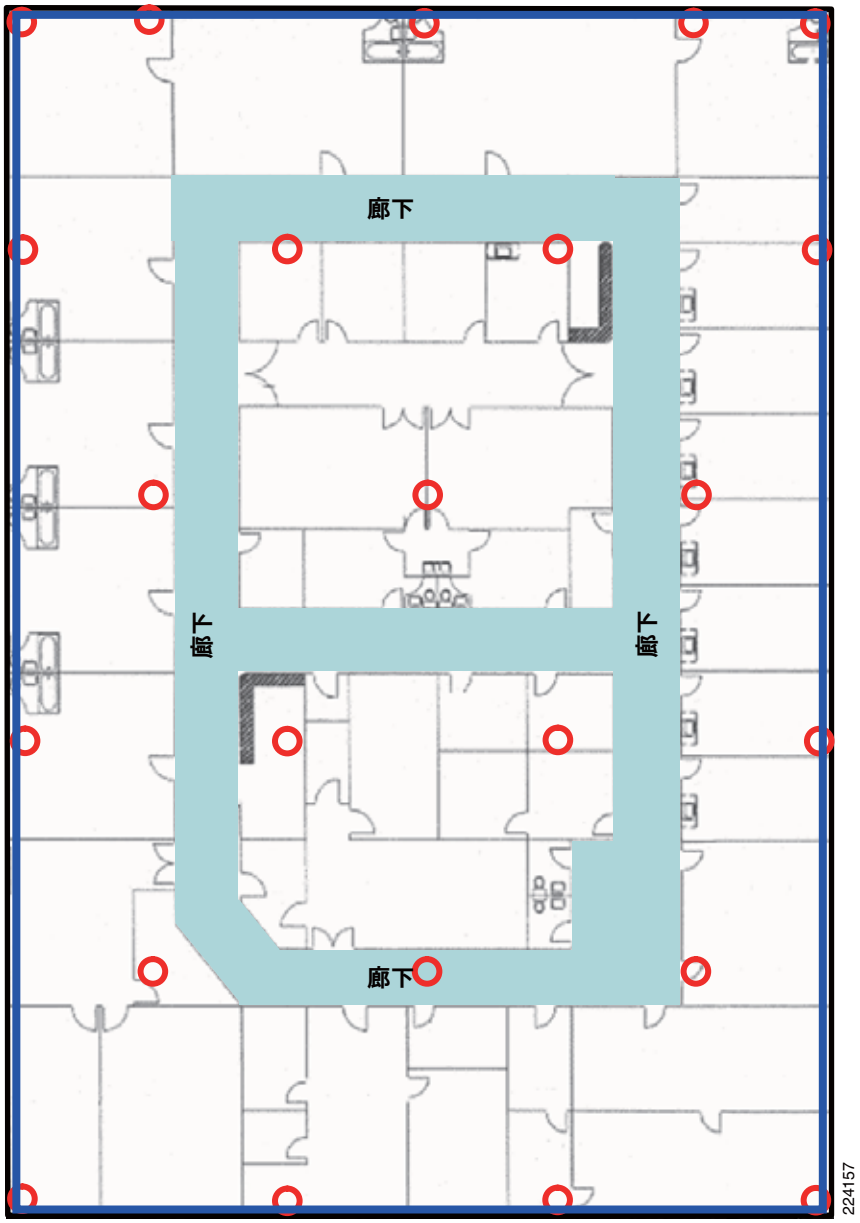


良好なロケーション確度を実現する可能性が高いロケーション データ ポイント セットを囲むように適切な凸包を構築するには、フロアの各隅と、隅と隅を結ぶフロア周囲に沿ってアクセス ポイントを配置する必要があります。周辺部に配置するアクセス ポイントの間隔は、一般的なアクセス ポイントの間隔についてのガイドライン（後述）に従ってください。これらのアクセス ポイントを使用してフロアで音声サービスやデータ サービスのプロビジョニングを行う場合、設計者は、必要に応じて間隔を狭くすることができます。

ここで説明した概念が、多くの企業に見られるフロア プラン（スペースや職場が屋内の廊下に囲まれています）を備えたフロアに適用される様子を図 5-5 に示します。このケースでは、フロア全体が、追跡対象資産の位置を特定する領域となっています。図 5-5 では、フロアの中心部に向かって配置されているアクセス ポイントが、周辺部に配置されているアクセス ポイントによって補完されていることに

注意してください。ロケーション認識が適切に設計されている大部分のケースに見られるように、良好なロケーション確度を実現する可能性が高いロケーション データ ポイント セットは凸包の内側にあります。図 5-5 では、この部分を青色の四角形で示しています（フロア全体を囲んでいます）。

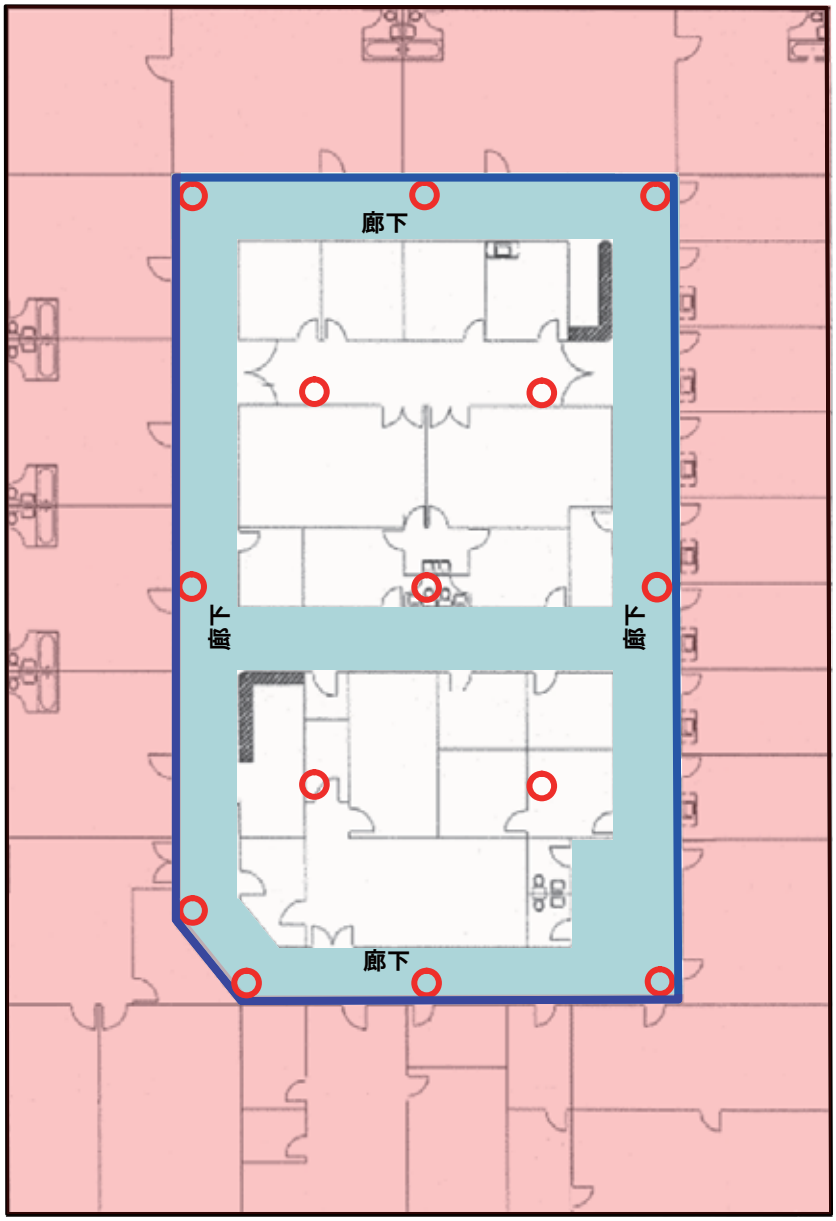
図 5-5　　周辺部でのアクセス ポイントの適切な配置



場合によっては、アクセス ポイントの配置について意思決定を下すときに、顧客の要望や展開上の制約事項を組み入れ、フロア周囲への配置がさまざまに制限されることがあります。基本的な RF カバレッジの提供という観点からは許容可能な配置になることもありますが、アクセス ポイントが囲む領域の外側（凸包の外側）での資産トラッキングが必要となり、その領域が広くなる場合には、該当する領域でのロケーション忠実度は低下する可能性があります。

図 5-6 は、望ましい状況よりも、そのレベルが低い例を示したものです。この例では、アクセス ポイントの配置は、廊下に取り囲まれている領域内にある屋内廊下や管理施設 / 保管設備によって制限されています。美観上の理由から、施設管理側は、屋内廊下と建物外周との間にある執務室や会議室にはアクセス ポイントを配置しないという決定を下しました。これらの制約により、凸包は、フロアの実際の周辺部（建物外周）ではなく、廊下の外側の端（青色の四角形で示しています）に位置しています。

図 5-6　人為的に制約を受けて周辺部に配置されたアクセス ポイント



凸包の外側で運用した場合のロケーション エラーの分布に関して認識していることを考慮すると、そのロケーション忠実度は凸包の内側に位置する職場やスペースでの忠実度ほど高くないと考えるのが道理に適っています。図 5-6 では、ロケーション確度が低くなるおそれのある領域を赤色で強調表示しています。

凸包はフロアの物理的な周辺部に構築することをお勧めしていますが、実際には凸包の内側に配置されているポイントと外側に配置されているポイント間のロケーション エラー率には相違があり、場合によっては、その率は許容範囲内に収まることがあります。これには、職場の周囲をほんの短い距離だけ外側に超える場合などがあります（廊下の壁に囲まれる 10 フィート x 10 フィートの小部屋など）。たとえば、図 5-6 で赤色で強調表示された領域に目を向けると、フロア プランの右側に位置する小さな職場では、影響を受けるその他の領域と比較してロケーション エラーが発生する可能性が低くなります。凸包の外側で運用しても、その度合いによっては、影響は最小限になると予想されます。対照的に、フロア プランの下部にある領域には、より広い職場と複数の壁で区切られたパーティションがあります。この領域では、より高い度合いで影響を受ける可能性があります。

周囲にある職場や会議室でのアクセス ポイントの配置が美観上の理由から制限される場合は、プレナム定格の筐体（国コードによって使用可能となります）に取り付けたアクセス ポイントと共に薄型アンテナ（Cisco AIR-ANT5959 や Cisco AIR-5145V-R など）を使用する方法があります。この方法では、周辺の適切なロケーションにアクセス ポイントを取り付けることができます（それにより、図 5-6 で説明したような困難な状況に陥ることを回避できます）が、機器を設置する最小限の場所を占め、だれの目にも留まることになります。

前述のとおり、図 5-5 および図 5-6 に示すフロア プランは一般的に見られるプランであり、限定的なものではありません。たとえば、近代的な建築設計では、実際のフロアと建物の周囲に沿って屋内廊下を配置し、訪問者が職場と会議室の間を移動するときにキャンパス周辺の全景を眺めることができるようになっています。このケースでは、すべての職場および会議室の施設は、廊下とフロア中心部との間の領域に位置しています。図 5-7 は、このようなフロア プランを図に示したものです。このフロア レイアウトでは、屋内廊下の外側の端に沿って配置すると、デフォルトで、実際の周辺部（建物外周）に沿ってアクセス ポイントを配置することになります。

図 5-7　周囲に廊下がある場合のフロア プラン

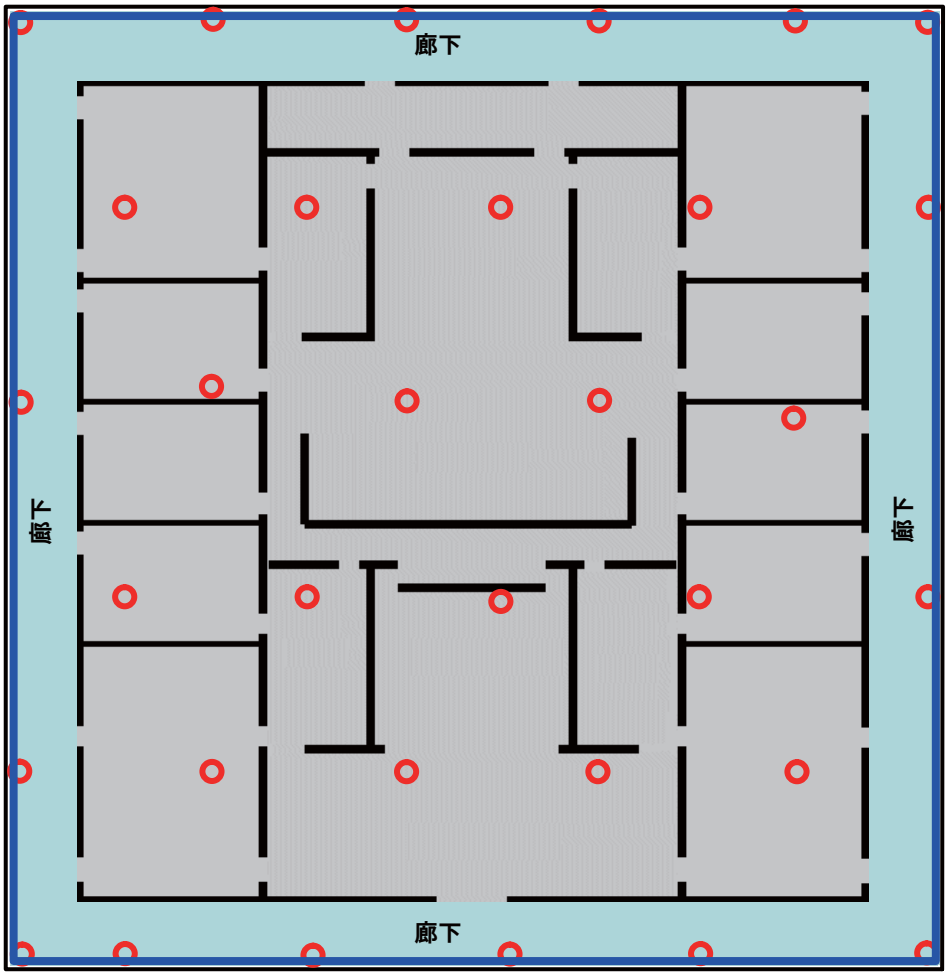
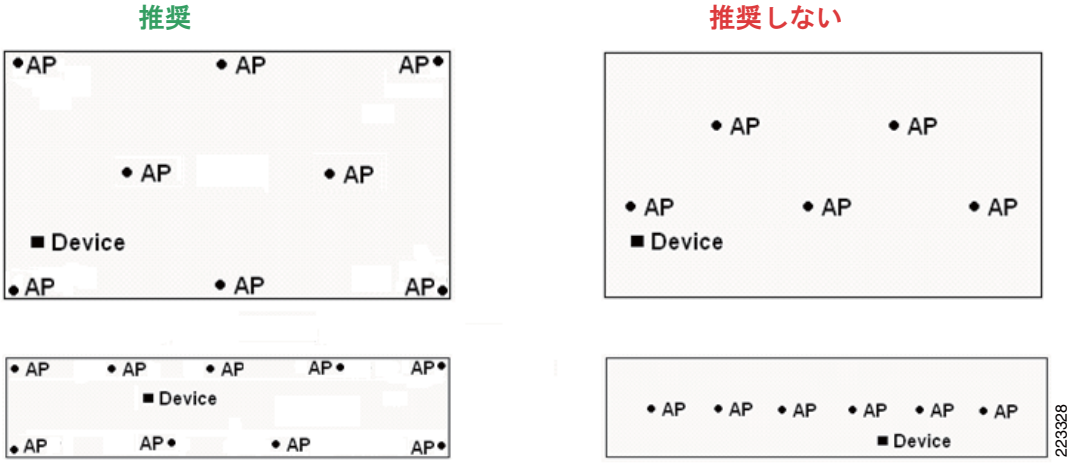


図 5-8 は、これまでにこの項で説明したアクセス ポイント配置の概念を簡単な図にまとめたものです。クラスタ化されたアクセス ポイントのみ、または直線状に配置されたアクセス ポイントのみを使用する設計では、中心部のアクセス ポイントの配置を、周辺部のアクセス ポイントの配置と組み合わせて増強または再設計することが必要になります。

図 5-8　　ロケーション認識アクセス ポイント展開の基本例



可能であれば、360º に渡って障害物がなく、近距離でブロックされることのないように、アンテナを取り付けます。たとえば、可能であれば、図 5-9 に示すように、鉄骨柱などの大きな障害物にアクセス ポイントのアンテナを直接取り付けることは避けてください。選択肢として、（取り付ける高さに対応可能であることを前提として）天井に取り付けたアンテナと一緒にアクセス ポイントを設置する方法があります。また別の選択肢として、短く低損失の延長ケーブルを使用して、アンテナと障害物の間隔を空けることもできます。

図 5-9　　鉄骨柱に直接取り付けたアクセス ポイント

アクセス ポイントの適切な配置に関するその他の説明は、『*Cisco Wireless Location Appliance: Deployment Guide*』（URL：http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html）に記載されています。

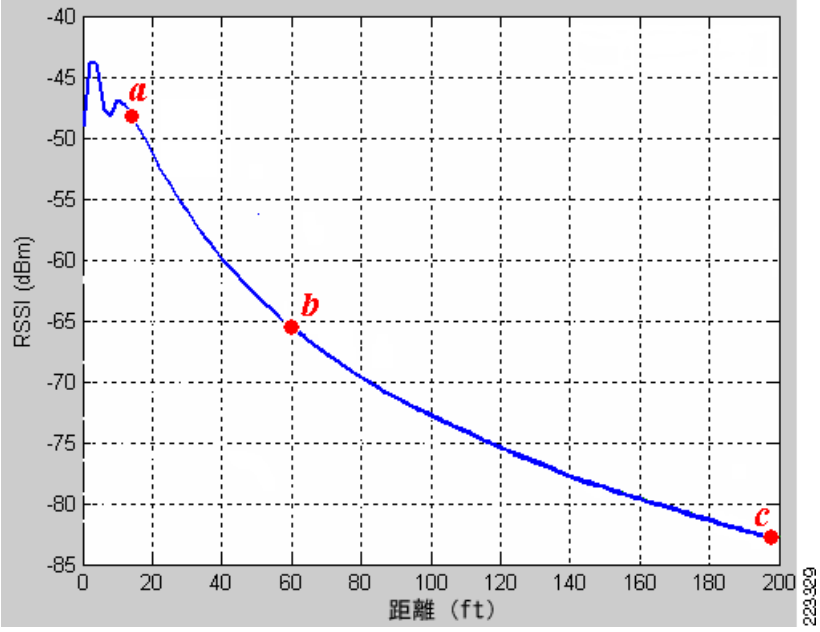
アクセス ポイントの間隔

展開されたアクセス ポイント間の距離が、ロケーション パフォーマンスや、共存する音声アプリケーションやデータ アプリケーションのパフォーマンスに影響を及ぼすことがあります。ロケーションの観点から考えると、ロケーション トラッキングを行うアクセス ポイント間の間隔要件は比較的に柔軟であり、基本アプリケーションのカバレッジに対するニーズを支援する傾向にありますが、一般には、アクセス ポイント間の距離を短くまたは長くしすぎることは避けることが推奨されます。

アクセス ポイント間の距離[1] が長すぎると、距離を延長したときに信号強度の十分な差異を提供できないため、良好なロケーション確度を損なうことになります。アクセス ポイント間の距離が短すぎると、短距離によるアンテナ パターン異常が生じ、この場合も良好なロケーション確度にとって良い結果をもたらしません。共存する音声アプリケーションやデータ アプリケーションの観点から見ると、アクセス ポイント間の距離は、求められる信号レベルの最小しきい値、データ レートのしきい値、Signal-to-Noise Ratio（SNR; 信号対雑音比）、必要なカバレッジ オーバーラップの条件が満たされるかどうかを判断するための主要な要因の 1 つです。ロケーション確度の観点からは、アクセス ポイント間の距離の許容範囲はむしろ広く、共存する大部分の音声アプリケーションやデータ アプリケーションのニーズを満たしながら、優れたロケーション確度を実現できます。

ロケーション認識 Cisco UWN において追跡対象デバイスの場所を特定するために採用されている技術は、RSSI と距離の間に明らかに「単調」な関係が見られる場合に最も効果的に機能します。これが意味することの理解を深めることができるように、追跡対象デバイスと検出アクセス ポイント間の距離を徐々に長くし、そのときにデバイスで検出された RSSI のシミュレーション プロットを分析します（図 5-10 を参照）。RSSI と距離の関係はアンテナ、アンテナの高さ、環境特性の組み合わせによって変化しますが、ここで説明する概念をより良く理解できるように、約 12 フィート上昇させて取り付けたアクセス ポイントに関するグラフ（図 5-10）を使用します。

図 5-10　　例：RSSI と距離の関係



1. このデザイン ガイドで後述するように、アンテナの高さが高すぎると、確度が下がることがあります。

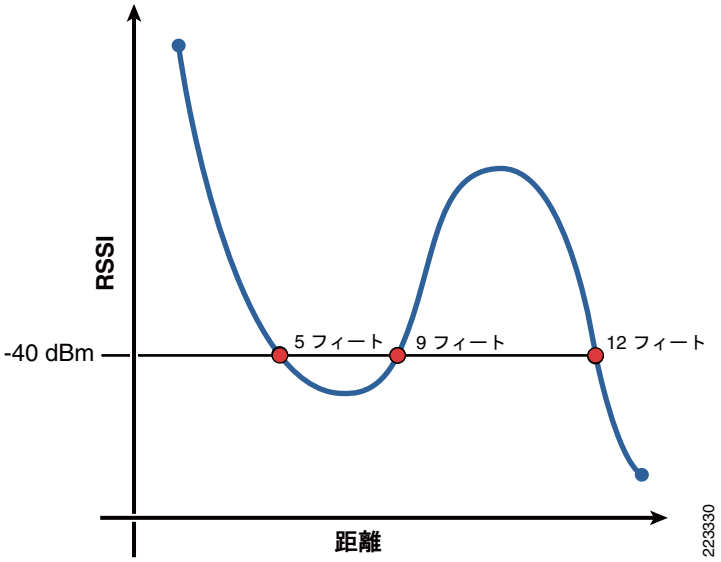
図 5-10 では、アクセス ポイントにかなり近い点（a）から、離れたところにある別の点（c）の範囲において、これらの 2 つの変数は厳密な単調減少の関係を示しています（追跡対象デバイスとアクセス ポイント間の距離が長くなるにつれて、アクセス ポイントがデバイスを検出するときの RSSI は下がっています）。点（a）と点（b）の間では、距離（フィート）の単位あたりの変化が生じるときの RSSI（dBm）の変化量には高い一貫性が見られ、距離が 20 フィート変化するごとに約 -5 dBm の変化が見られます。結果として、グラフでは、点（*a*）と点（*b*）の間の傾斜はかなり急になっています。点（b）を超えて距離を伸ばし続けると、グラフの傾斜は緩やかになり始め、RSSI レベルの差異は小さくなり、距離の単位あたりの変化が生じるときの受信信号強度の差異はますます小さくなります。グラフで、点（*b*）と点（*c*）の間の傾斜は、点（*a*）と点（*b*）の間ほど急傾斜ではないことに注意してください。この例では、距離が伸びて点（*b*）を超えるにつれて、グラフの傾斜はさらに緩やかになります。このように傾斜がかなり緩やかになると、結果として、距離が長くなるほど信号レベルの差異が小さくなります。距離を延長すると、RSSI で検出された変化（ラテレーション）に基づいて、距離の変化を正確に予測することが難しくなります。

RSSI の差異が不足し、ロケーション確度に重大な影響を及ぼすというリスクは、RSSI と距離の関係が曲線状になる領域（この領域では、この現象が顕著に見られます）を避けるための措置を講じることで軽減させることができます。一般に、アンテナの高さを 20 フィート以下にしてアクセス ポイントを屋内で展開する場合、フロアにあるどのアクセス ポイントについても、屋内環境の約 70 フィート以内の範囲に、同じフロアに少なくとも 3 台以上の検出アクセス ポイントがある（対象アクセス ポイントを中心として、4 つの四分円のうち少なくとも 3 つの四分円に 1 台の検出アクセス ポイントがある）環境を維持できれば、これを実現することができます。これは、アクセス ポイント間の距離が長すぎることが要因となってロケーション確度が下がることのないように、設計者を支援するための一般的な推奨事項です。図 5-10 に示すように、RSSI の差異が小さくなるという現象は、距離の延長とともに顕著になります。したがって、この推奨事項では柔軟度についても暗示しています。

実際のところ、この推奨事項は良好なロケーション確度の実現に役立つだけでなく、現在推奨されているベスト プラクティスに従って他の WLAN アプリケーション（音声アプリケーションや高速データ アプリケーションなど）と併せてロケーション トラッキングを展開している環境にも十分に該当します。このことは、期待されるパス損失指数が 3.5（壁で囲まれたオフィス環境）またはそれ以上であり、求められるアクセス ポイント間の間隔がほとんどこの範囲に収まる環境では、特に当てはまります。アクセス ポイント間の距離が 70 ～ 80 フィートを超えると、距離が極端に長い場合に RSSI 差異が不足するという潜在的な影響が生じるだけでなく、パス損失の高い環境での VoWLAN デバイス（Cisco 7921G や Vocera Communication Badge など）についてベスト プラクティスである信号強度要件やオーバーラップ要件を満たすことが一層困難になります。

ここで挙げた例で説明すると、点（a）よりも近いところでは、選択したアンテナの仰角パターン、アンテナを設置した高さ、追跡対象デバイスの現在の物理的なロケーションに起因して生じる伝播異常により、単調性が低下することがあります。結果として、検出された特定の RSSI レベルにおいて、距離に対して同程度の値が 2 つ以上存在する可能性があるため、RSSI は、この曲線部分での距離を予測するうえで信頼の置ける判断材料にはならないと言えます。図 5-11 は、このケースを図に示したものです。この図は、RSSI と距離の関係を示すグラフ上の近距離かつ非単調な領域において、追跡対象デバイスの RSSI の測定値（-40 dBm）と、アクセス ポイントのアンテナからの距離（5、9、12 フィートの異なる 3 つの距離）との関係を示しています。これは、デバイスがアンテナのほぼ真下の領域に入り込んだときに、オーバーヘッド アンテナの伝播パターンでの変動の結果として見られる典型的な現象です。当然ながら、これらの結果は、使用するアンテナの伝播パターンと、追跡対象デバイスが位置している領域に設置したアンテナの高さに応じて変化します。アクセス ポイントの設置密度を高くするとロケーション確度の向上に役立ちますが、この効果は無制限に続くものではないことに注意してください。

図 5-11　例：近距離かつ非単調な場合



明らかに、RSSI に見られるこのような両義性は混乱を招く原因になります。特に、RSSI を使用して距離のラテレーションを正確に行おうとする場合は混乱の度合いが大きくなります。このような両義性のある現象は、通常、良好なロケーション忠実度にとって良い結果をもたらしません。パス損失指数が 3.4 の環境で、高さ 10 フィートの位置に 2.2dBi の全方向性アンテナと共にアクセス ポイントを設置し、このテストを実施すると、約 14 フィート以上離れたところで、この現象が散在的に観察されます。この例の具体的なケースでは、この現象が発生する可能性を低くするため、アクセス ポイント間の間隔を 28 フィート（上記の現象が発生する距離の 2 倍の長さ）以上に保つことが最適と考えられます。

アプリケーションの設計によっては、ユーザが利用可能な RF 帯域幅を潜在的に増加させるようにするため、重複しないチャネル上に複数のアクセス ポイントを展開することが望ましい場合があります[1]（「同一場所に配置されている重複しないアクセス ポイント」）。この方法は、多くの場合、大多数のユーザがいる可能性のある教室や会議場で採用されています。同一場所に複数のアクセス ポイントが配置されている部屋がある状況で、WLAN クライアントなどのデバイスについてのロケーション トラッキングを行うことが望ましい場合は、配置されているアクセス ポイントが相互に近づきすぎない（数フィート以内に配置しない）ように展開することが推奨されます。より正確に言えば、良好なロケーション忠実度に害を及ぼすような近い距離に配置することを避けるため、同一場所に配置されているアクセス ポイント間の間隔を可能な限り長くするように最大限の努力を払うことが必要です。大教室において、同一場所に配置されているアクセス ポイントでこれを実現するための 1 つの方法として、適切な距離を保ちながら、アクセス ポイントを壁ごとに配置し、場合によっては天井にも配置する方法があります。

アクセス ポイント アンテナを 20 ～ 30 フィートの高さに設置して屋内でロケーション トラッキングを展開すると、一般に、アクセス ポイント間の間隔を 40 ～ 70 フィートにすると効果的です。特に、本書で前述した信号のしきい値とアクセス ポイントの配置についての推奨事項を組み合わせると、一層効果的です。ただし、信号強度のしきい値が高い場合、アプリケーションの要件を満たすためにアクセス ポイント間の間隔を 40 フィート以下にすることが必要な場合もあります。これは特に、高いパス損失が見られる環境に当てはまります。たとえば、このような環境（パス損失指数が 4.0 で、外因的なクラッタ レベルが高い環境など）に展開されている音声アプリケーションが例として挙げられます。Cisco 7921G VoWLAN 展開のベスト プラクティスとして、この種の状況においては、802.11g 規格の場合、最小信号レベル -67 dBm、セル間オーバーラップ 20%、Signal-to-Noise Ratio（SNR; 信号対雑音比）25 dB が推奨されます。これらの要件を数理的に適用すると、セル サイズについて 24 フィート、アクセス ポイント間の間隔について 33 フィートの推測値が算出されます。この場合、推奨される

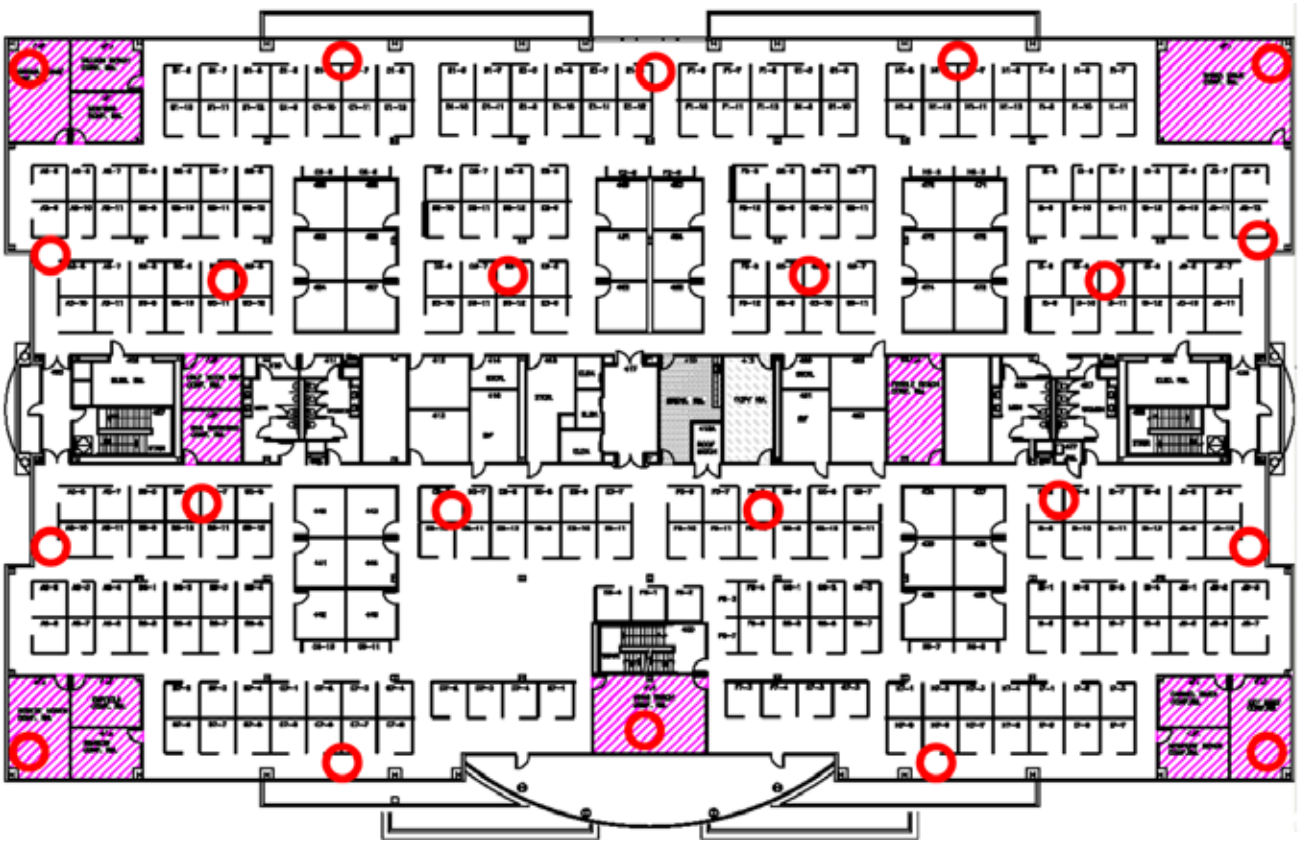
1. 同一場所に配置されているアクセス ポイントでは、同じチャネル上にある他のアクセス ポイントからの同一チャネル干渉があるため、その帯域幅の増加は制限を受けることに注意してください。

ベスト プラクティスに従って音声アプリケーションを展開するには、アクセス ポイント間の間隔を一般的なガイドラインである 40 フィートよりも狭くする必要があります。良好なロケーション確度は、アクセス ポイント間の間隔が 40 フィートよりも狭いときに実現可能です。ただし、これは非単調性が見られるほどには間隔を狭めないことを前提としています。一般に、屋内環境で約 10 フィートの高さに設置されたロー ゲインの全方向性アンテナを使用した場合、アクセス ポイント間の距離が 25 ～ 28 フィートであるときは、これは問題とはなりません。

図 5-12 は、アクセス ポイントの配置と間隔の例を図示したもので、ロケーション認識の基本的な設計を示します。図 5-12 に示す環境は、乾式壁工法で建築されたオフィスやパーティションで小さく区切ったオフィス スペースで構成されており、全空間の大きさはおおよそ 275 フィート× 159 フィートです。ここでは例示を目的としてロケーション トラッキング要件を考慮し、最初の見積として、アクセス ポイント間の直線状の推奨間隔 40 ～ 70 フィートに基づき、約 22 台のロケーション認識アクセス ポイントの配置が推奨されます。前述の配置計画を組み入れてフロアの内部領域や周辺部（周囲、隅）にアクセス ポイントを配置し、マルチラテレーションが容進になってフロア周囲に明確な凸包を構築できるようにします。

（注）　ロケーション トラッキングと共に展開した WLAN アプリケーションが関与する実際の設置環境では、ロケーション トラッキングを変更するために設計変更に着手する前に、内部アクセス ポイントの設計を行う必要があります。これにより、データ アプリケーションや音声アプリケーションの信号強度、オーバーラップ、Signal-to-Noise Ratio（SNR; 信号対雑音比）の要件が確実に満たされるようにします。

図 5-12　例：ロケーション認識アクセス ポイントの配置



設計者が「仮定」の設計シナリオをモデル化できるように、WCS には Planning ツールが備えられています。WCS Planning ツールにアクセスするには、[Monitor] > [Maps] > [（*フロアマップ名*）] > [Planning Mode] ドロップダウン メニューを選択します。これは予測的なモデリング ツールで、フロアごとにアクセス ポイント配置の初期ガイダンスを提供し、予測されるアクセス ポイントでの信号強度やデータ レートに関する情報を対話式に表示します。このツールは、すでにサービスを提供しているアクセス ポイントの実際の展開に影響を与えることなく、安全に使用することができます。Planning ツールの上部にあるハイパーリンク バーから WCS Map Editor にアクセスし、このエディタを使用してフロア マップに壁減衰情報を追加できます。Map Editor を使って追加した壁情報は、アクセス ポイントの配置やロケーションの設計に影響しませんが、計画段階のアクセス ポイントについて予測された RF カバレッジ マップを表示するときに Planning ツールによって使用されます。

Planning ツールは仮定に基づいて純粋に動作します。アクセス ポイントやコントローラに接続したり、これらを展開する必要はありません。Planning ツールは WCS 機能であるため、ツールを使用するには、ネットワーク上に WCS サーバをインストールしておくことが必要です。WCS に展開して定義された既存のアクセス ポイントがある場合、Planning ツールでは、実稼動環境と共にこれらのアクセス ポイントの設定を仮想環境にコピーして、安全にモデル化することができます。

RF カバレッジの計画に Planning ツールを使用する前に、計画を行うフロアに適切なパス損失モデルが割り当てられるようにしてください。WCS は、Planning ツールで各アクセス ポイントに基づいて予測されたカバレッジ ヒートマップをプロットするとき、カバレッジ基準パス損失とパス損失指数を使用します。WLAN に精通した経験豊かな設計者は、（送信電力やアンテナの種類などの）効果や影響を確かめるためにいくつかの基準を適合させて調整するときにマニュアル モードで Planning ツールを使用し、フロア マップにアクセス ポイントを配置することができます。また、WCS Planning ツールを使用して、目的とする展開モデルの種類に応じてアクセス ポイントを自動的に配置することもできます。設計に関する提案を最初にシステムに実行させることを望むユーザや設計者は、Planning ツールを自動化モードで使用することができます。これにより、設計の種類を指定することで、Planning ツールを使用して要件を分析し、適切な設計提案を作成することができます。Cisco VoWLAN ベスト プラクティスをロケーション トラッキングに適合させつつ、音声設計とデータ設計を組み合わせることを望む設計者には、ロケーション トラッキング要件とは別に、最初に Planning ツールを使用して音声設計とデータ設計のモデル化することをお勧めします。満足のいく音声設計とデータ設計を作成できたら、良好なロケーション忠実度を実現できるように、必要な変更を手動で加えることができます。

Planning ツールでは、送信電力は +18 dBm（802.11bg の場合）および +15 dBm（802.11a の場合）、アンテナの方位角は 180º、高さは 10 フィート、仰角は 0º を前提としています。送信電力、アクセス ポイントの種類、アンテナ タイプ、方位の位置は、アクセス ポイントごとに変更できます。Planning ツールのユーザはその他の基準を指定して、データ設計および音声設計を微調整することもできます。

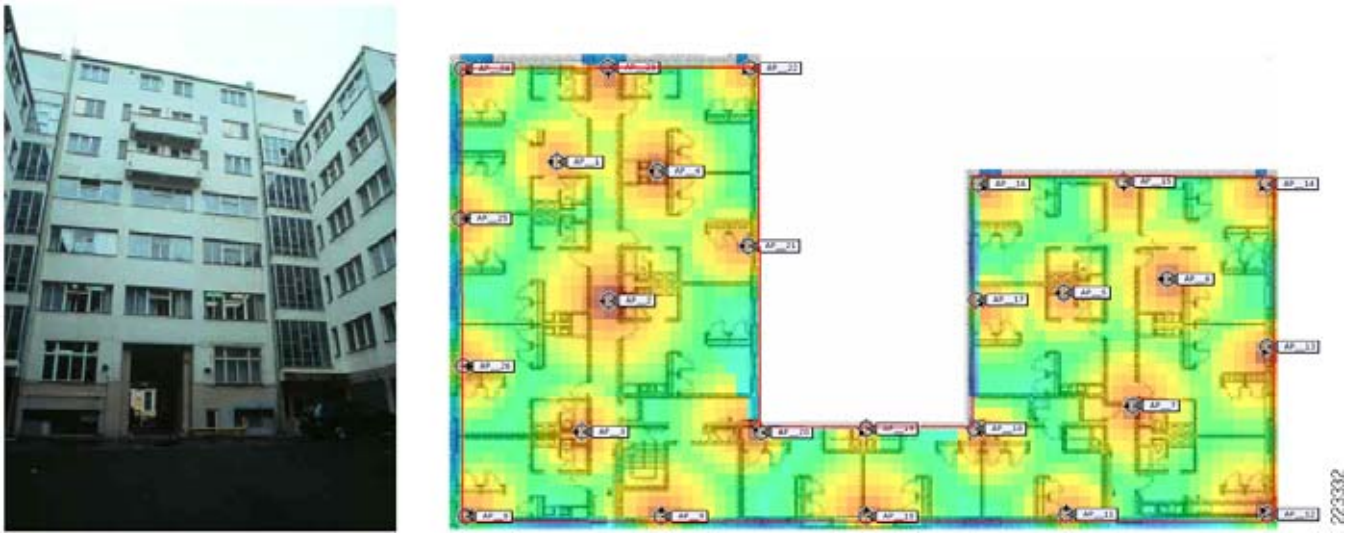
（注）　Planning ツールのオプション（データ / カバレッジ、音声、ロケーション、デマンド、オーバーライドなど）の詳細については、『*Cisco Wireless Control System Configuration Guide, Release 4.1*』の「*Using Planning Mode to Calculate Access Point Requirements*」を参照してください。このドキュメントは、http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsmaps.html#wp1104248 に掲載されています。

Location Planning ツールのオプションを選択すると、必要に応じて、フロアの内部および周辺（周囲や隅）に計画モードのアクセス ポイントが配置されます。ロケーション設計には、少なくとも 4 台のアクセス ポイントが存在し、最大でも 70 フィート間隔で配置することを前提としています。Location Planning ツールのオプションを使用すると、共存するアプリケーションの信号強度要件やオーバーラップ要件は明示的には考慮されませんが、音声アプリケーションおよびデータ アプリケーションのベスト プラクティスに適った設計が作成されます。そのため、音声データや高速データとの共存を意図するロケーション トラッキングを組み入れた設計では、提示されるベスト プラクティスに従って、最初にこれらのアプリケーション設計に取り組むことが推奨されます。アプリケーションの要件を満たす設計が完成したら、ロケーション トラッキング要件を満たすように、必要に応じて設計を変更したり増強したりすることができます。

リリース 4.1 以前のソフトウェアでは、Planning ツールの自動配置機能はフロアとビルディングに限定されており、またその形は正方形や長方形などの単純な多角形に制限されていました。本リリースに追加された新機能により、Planning ツールを使用して不規則な形をしたフロア領域に対応できるようになりました。WCS Map Editor を使用して、不規則な形をしたカバレッジ領域を囲むことができます。また、これを保存すると、Planning ツールで使用できるようになります。Planning ツールを使用して新しいフロア レイアウトを設計するとき、ユーザは従来の多角形と、新しく作成された不規則な形のどちらも選択できます。新しく導入されたこの機能についての詳細は、『*Cisco Wireless Control System Configuration Guide, Release 4.1*』の「*Using the Map Editor to Draw Polygon Areas*」に記載されています。このドキュメントは、http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsmaps.html#wp1104253 に掲載されています。

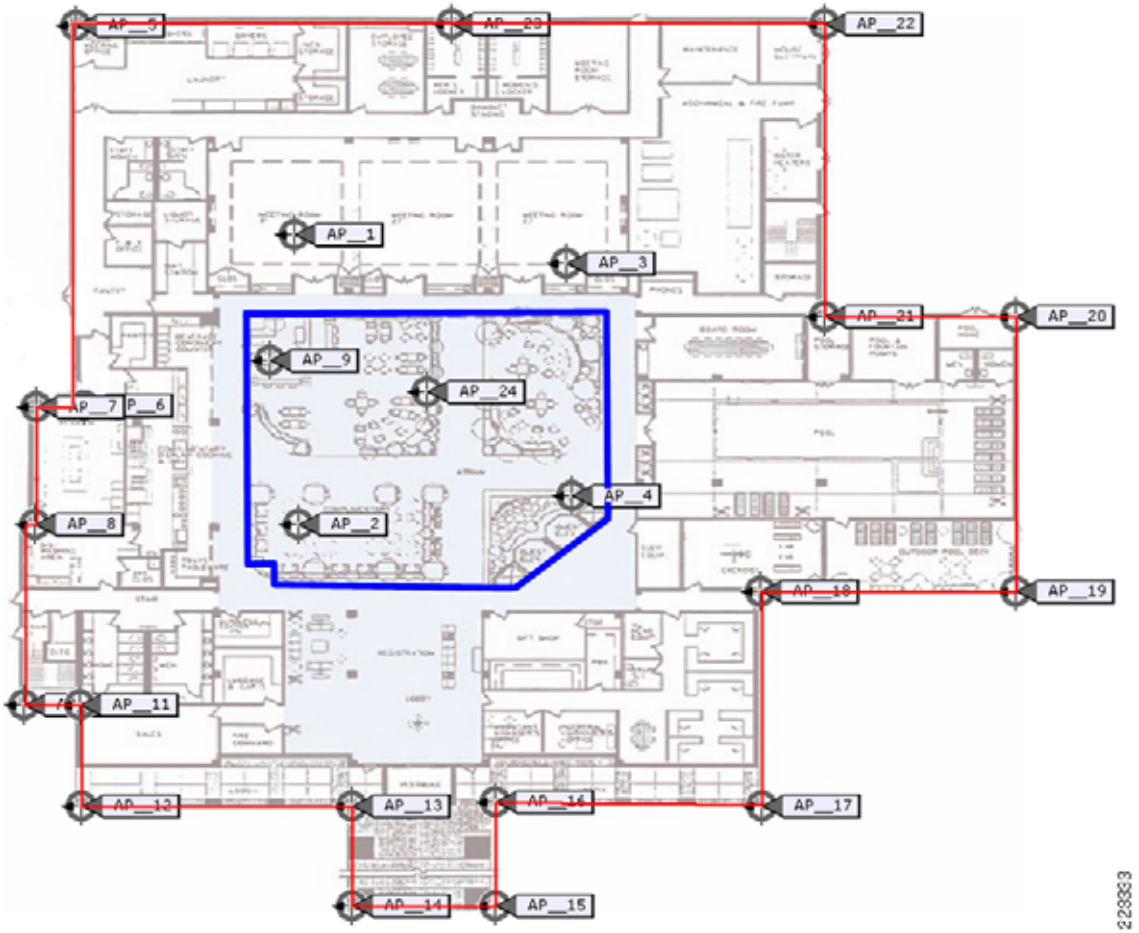
この機能強化により、Planning ツールは、図 5-13 に示す中庭のあるビルディングなど、不規則な形をしたビルディングを扱う仕事をするときに、設計者にとってより実用的なツールになりました。図 5-13 は、Planning ツールの自動モードを使用して行ったロケーション設計を示したものです。ビルディングの周囲にある赤色の縁取りは、Map Editor を使用してフロア イメージに追加したもので、Planning ツールで使用できるようになっています。

図 5-13　WCS Planning ツールを使用して不規則な形のフロア プランに対応



内部の空間を完全に密閉したような、より複雑な設計（たとえば、図 5-14 に示すような内側のアトリウムが完全に囲まれた状態にあるビルディング。ビルディングの周囲は赤色の縁取りで示しています）では、アクセス ポイントの自動配置機能は適さない場合があります。Planning ツールでは、現在のところ、アクセス ポイントを配置しないゾーンを除外することはできません。図 5-14 のアトリウム領域にあるアクセス ポイント 2、4、9、24（青色の縁取りで示しています）に注目してください。ビルディングの 3 階用のフロア マップであるため、この領域へのアクセス ポイントの配置は不適切です。この場合、手動で操作を行って、アクセス ポイントを適切な位置に移動するか、必要でない場合は完全に取り除く必要があります。

図 5-14　例：内側のアトリウムが完全に囲まれた状態にあるフロア プラン



ロケーション準備の確認

Inspect Location Readiness 機能（[Monitor] > [Maps] > *floormapname* > [Inspect Location Readiness]）では、ケーブルの引きまわし、装置の展開、調整の実行に時間を割く前に、ネットワーク設計者がフロアのロケーション パフォーマンス予測チェックを手早く実行できるようにします。[Inspect Location Readiness] の機能では、各アクセス ポイントの配置、およびフロア マップ上に示されるアクセス ポイント間の間隔を考慮に入れ、ロケーション トラッキングの推定確度が、すべてのケースの 90% で 10 メートル以内になるかどうかを予測します。ロケーション準備検査の出力では、このレベルの確度を満たす、または満たさない候補と予測される領域の「適 / 不適」をグラフィカルに表示します。

- 前述の計画ツールとは異なり、Location Readiness ツールでは、アクセス ポイントとコントローラが WCS に認識されており、[Monitor] > [Maps] > [Position APs] を使用して WCS フロア マップ上で定義されていることを前提としています。ロケーション準備検査を実施するために、実際にアクセス ポイントやアンテナを壁や天井に取り付ける必要はありませんが、適切なコントローラを WCS および登録アクセス ポイントに追加したり、アクセス ポイントを表すアイコンを適切なフロア マップに配置したりする必要があります。最初にこれを行うために、これらすべてのコントローラとアクセス ポイントが物理的に存在し、電源が入っており、ネットワークにオンライン接続されている必要があります。これらのアクセス ポイントとコントローラは展開、取り付けを行

う必要はありません。アクセス ポイントとコントローラが WCS と通信可能であれば、フロア、テーブルの上、他の一時的な場所に置いてもかまいません。ロケーション準備検査を実施するために Cisco Wireless Location Appliance が存在する必要はありません。

- フロア マップに配置したいアクセス ポイントを WCS データベースにいったん追加すると、その時点で WCS から到達不可能な場合でも、同じアクセス ポイントを使用してこれ以降のロケーション準備検査を実施できます。ロケーション準備検査は、アクセス ポイントの配置と、フロア マップ上に表示されるアクセス ポイント間の距離に基づいているため、アクセス ポイントを正確にマップに配置することを強くお勧めします。Location Readiness ツールは、RF フィンガープリントベースのロケーション トラッキングを実行するための設計の準備状態を調査するためだけに使用します。チョークポイント ロケーションを実行するための設計（特にチョークポイント トリガーの位置の定義に関して）を検証することはありません。アクセス ポイントの配置を行った後、ロケーションの準備状態を検証するフロア マップを選択し、右上のドロップダウン コマンド メニューから [Inspect Location Readiness] を選択します。

次の条件がすべて真だと判断された場合、「ロケーション準備完了」と定義されます。

- 少なくとも 4 つのアクセス ポイントがフロア上に展開されている。
- 対象ポイントを中心とする 4 つの四分円に、それぞれ少なくとも 1 台のアクセス ポイントが存在する。
- 対象ポイントを中心とする 4 つの四分円のうち少なくとも 3 つの四分円に 1 台のアクセス ポイントが存在し、対象ポイントから 70 フィート以内に配置されている。

図 5-15 に、3 つのロケーション準備ルールを示します。ここで緑と黄色の円はアクセス ポイントのロケーションを示し、問題のポイントは赤の点で表されています。

図 5-15　「ロケーション準備完了」ポイントの定義

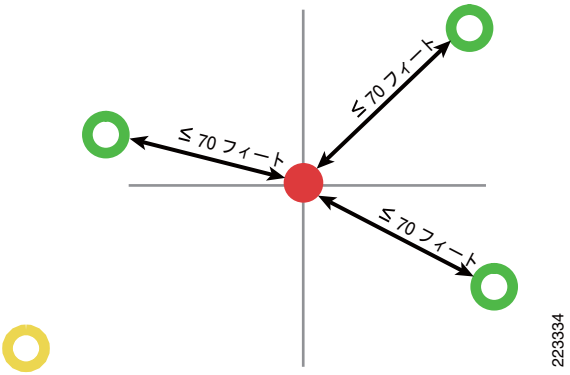
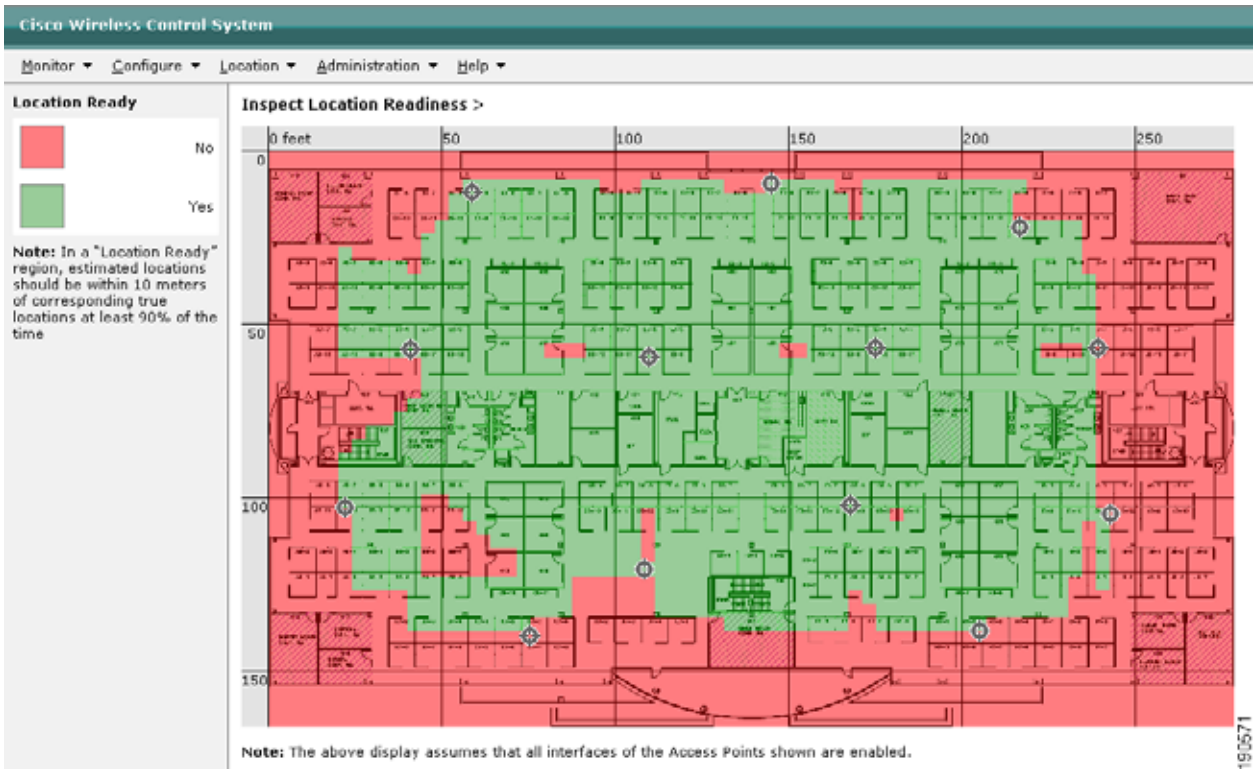


図 5-16 に、3 台のポイント ロケーション準備検査で、前述の 10m/90% の確度をすべての領域では満たしていないフロア展開の例を示します。図の中心に向かうほど緑の領域になっていますが、凸包を表す周辺部のアクセス ポイントの外側は赤くなっていることに注意してください。ロケーション準備状態を定義する要件を的確に理解するために、図 5-15 の情報を使用して、アクセス ポイントを再配置（または追加のアクセス ポイントを導入して）パフォーマンスを改善するための方法を決定できます。たとえば、赤色の領域内で 10m/90% またはそれ以上のロケーション確度が必要な場合、追加のアクセス ポイントを導入して（フロアの隅にアクセス ポイントを配置したり、アクセス ポイント間の距離を再チェックしたりするなど）フロア周囲の線引きをより明確にすることができます。このような変更を実施することにより、これらのハイライトされた領域での Cisco UWN の追跡対象デバイスのロケーション解決能力が大幅に強化されます。

図 5-16　Location Readiness ツールの使用方法の例



ロケーション準備検査は、距離に基づいた*予測*ツールであることに留意してください。ほとんどの予測ツールと同様に、予測の結果と実際の結果にある程度の差異があることが予期できます。Location Readiness ツールを、このマニュアルで説明した他のベストプラクティスの技術（ロケーション品質検査を含む）とともに使用することをお勧めします。

ロケーション、音声、データの共存

ロケーション認識 Cisco Unified Wireless Network は、多目的の無線プラットフォームで、企業のビジネス プロセスに一貫性と効率性を取り入れ、全体的な有効性を向上させます。ロケーション認識 Cisco UWN の重要な利点は、クライアント、資産タグ、不正デバイスの高品質なロケーション トラッキングを実行する機能から生まれる、統合およびコストの利点です。そのため、VoWLAN および高速データなどの、他の企業無線アプリケーションをサポートするために必要な要件以外では、妥当な追加投資だけが必要になります。

（注）　この項では、Cisco UWN のロケーション トラッキング機能との共存に関連する音声およびデータ設計に関する特性について説明します。Cisco Unified Wireless Network VoWLAN ソリューション設計の詳細な説明と、Cisco が推奨するベストプラクティスについては、次の URL の『*Voice Over Wireless LAN 4.1 Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

（注）　Cisco Unified Wireless Network データ ソリューション設計とベスト プラクティスの詳細な説明は、次の URL の『*Enterprise Mobility 4.1 Design Guide*』を参照してください。
http://www.cisco.com/go/srnd

VoWLAN および高速データ設計を行い、続いてアクセス ポイント配置を決定する場合、設計者にとっての主要な問題には次のものがあります。

- セルの信号レベルしきい値を最小にする：たとえば、Cisco 7921G VoWLAN ハンドセットについての VoWLAN ソリューションを設計する場合、現在の VoWLAN ベスト プラクティスでは、信号レベルしきい値の計画を最小の -67 dBm にすることをお勧めします。他の音声デバイスでは、異なる要件を持つ場合があります（Vocera Communications バッジなど。信号レベルしきい値 -65 dBm が必要）。データ デバイスの要件は、動作に必要な伝送レートによって異なります。低速のデバイス（携帯バーコード、つまり RFID コンピュータ。最大 11 Mbps のデータ レートで動作）では、信号の最小要件はそれほど厳しくなく、多くの場合 -73 ～ -76 dBm の範囲になります。ストリーミング マルチメディアと、その他の帯域幅を利用したアプリケーションを通過させるために使用するデータ デバイスは、通常、高いデータ伝送レート、その結果として高い最小信号レベルが必要です。
- Signal to Noise Ratio（SNR; 信号対雑音比）：これは、受信側の信号強度とノイズ フロアの比率です（単位は dB）。どちらの要素も dBm 単位で指定されるため、SNR は信号強度値からノイズ値を引くだけで計算できます。受信側が正常に動作するために必要な最小 SNR は、受信側の構造、およびビット レート（動作時に予測される変調）によって異なります。典型的な例を次に示します。

伝送レート（Mbps）	1	2	5.5	11	6	9	12	18	24	36	48	54
信号対雑音比（dB）	4	6	8	10	4	5	7	9	12	16	20	21

堅牢で信頼性のある無線アプリケーション サポートを設計する場合は、十分な SNR を確保することが重要です。無線音声アプリケーションでは、高確率のパケットを正常に各セルでデコードし、ジッタを最小に抑えられるようにするため、特にこれは重要です。たとえば、Cisco 7921G VoWLAN ハンドセットでは、VoWLAN の正常動作を保証するための推奨 SNR は 25 dB です。高いノイズ フロアのため信号対雑音比が不十分な場合、全体的な受信信号レベルが高くても、無線デバイスの正常動作を保証することが難しい場合があります。新しい展開が設計基準を満たし、実稼動環境でのパイロット テストを行えるように、SNR および最小受信信号レベルを合わせて考慮する必要があります。

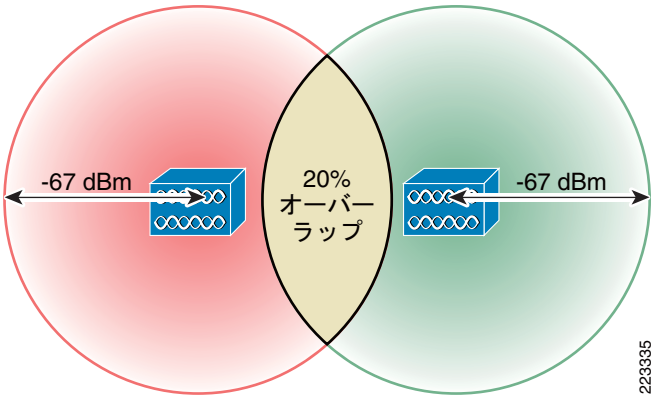
- データ レート：データ ビット レートが無線インフラストラクチャから有効または無効にされており、最小信号レベルしきい値と信号対雑音比で、有効化されたどのビット レートが実際に使用可能かを識別します。たとえば Cisco 7921G で、最小信号レベル -67 dBm と、信号対雑音比 25 dB の組み合わせでは、通常、24 Mbps 以上のデータ レートを使用できます。
- セル間のオーバーラップ：簡潔に言うと、各アクセス ポイントは RF 「セル」の中心にあり、その周りに RF カバレッジの球体境界があると考えることができます。第一の関心は、目的の最小信号しきい値に関連付けられたカバレッジ境界です。フロア全体の、一貫性のあるカバレッジと可用性を実現するには、各セルを、目的の最小信号しきい値を超えるカバレッジ境界で隣接する各セルと結合します。どれぐらい超えているかは、設計で実装するセル間のオーバーラップの程度によって決定されます。この程度は（前述した他のパラメータとともに）、ローミング イベントが発生する前に VoWLAN デバイスで生じるパケット損失に影響します。

セル間のオーバーラップの適用は、デバイスがセル境界に近づいたときに、過度のレート変動や再送信を行わずに、VoWLAN クライアントがすぐに隣接セルの検出とローミングが行えるようにする確率を高めることを目的としています。過度のレート変動やパケットの再送信は、特に VoWLAN デバイスにとって非生産的です。これらの動作は通常、パケット損失につながり、それらがジッタに変換されるためです。ジッタは、高品質の VoWLAN のユーザ エクスペリエンスにとって悪影響となるため、ユー

ザの音声コールの品質が落ちる前に、デバイスを自由に移動できるようにし、VoWLAN 設計内でのジッタを最小限にしています。このため、設計内で推奨される程度のセル間のオーバーラップが存在するようにします。

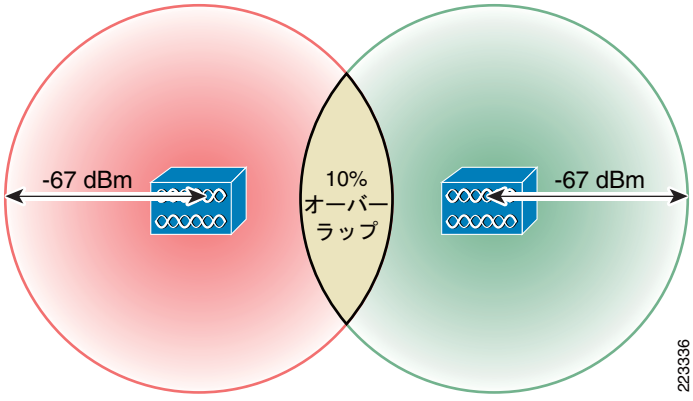
図 5-17 に、802.11bg を使用する Cisco 7921G VoWLAN ハンドセットのセル オーバーラップの概念を示します。Cisco 7921G の場合、『*Voice Over Wireless LAN 4.1 Design Guide*』に記載される、推奨されるベスト プラクティスでは、802.11bg を使用する場合はセル間のオーバーラップをおよそ 20%、802.11a を使用する場合は 15% にすることを提案しています。

図 5-17　　20% のセル間のオーバーラップ



一方、データ アプリケーションでは通常、音声アプリケーションで行うように、パケット損失に対する感度のレベルを表示しません。そのため、データ アプリケーションでは同じ程度のセル間のオーバーラップを要求することはほとんどありません。ほとんどの場合、図 5-18 に示すように、最小 10% のセル間のオーバーラップがあればデータ アプリケーションで信頼性のあるローミングを行うのに十分です。高速のデータ アプリケーションと、音声およびデータ機能を単一デバイスに結合したアプリケーション（たとえば、スマートフォン）では、データ設計より VoWLAN 設計に類似するセル間のオーバーラップを必要とします。

図 5-18　　10% のセル間のオーバーラップ



実装可能で、実際に存在しますが、使用例としてのロケーション トラッキングでしか実行されないロケーション認識 Cisco UWN のネットワーク設計は、すべての Cisco モビリティのカスタマー インストールでは少数派です。そのため、最適なロケーション設計の完成を目指す設計者は、VoWLAN の主要な 4 つの問題と、データ WLAN 設計者を同時に満足させようとする傾向があります。

資産タグ、クライアントまたは不正デバイスを追跡するほとんどの設計者の主要なロケーション トラッキングの問題には、次のものがあります。

- 周辺部のアクセス ポイントの配置：周辺部（周囲、隅）へのアクセス ポイントの配置は、ロケーション確度を保つために重要です。「凸包」の概念については、図 5-4 および前述の説明を参照してください。前述したように、フロア上のデバイスのロケーションを囲んだ凸包の外側にデバイスがあると、ロケーション確度は低下する傾向があります。
- 交互にずらす：許容可能なアクセス ポイント間の間隔を保つため、また、追跡対象デバイスの RSSI マルチラテレーションを実行するシステム機能をサポートするために、アクセス ポイントは交互にずらしてフロア上に配置する必要があります。
- アンテナ取り付けの高さ：ほとんどの屋内のロケーション アプリケーションでは、デバイスを追跡する対象領域上のアンテナ取り付けの高さを、10 ～ 15 フィート、推奨最大の高さを 20 フィートにするのが理想的です。
- アクセス ポイント間の間隔：ロケーション確度低下のリスクを最小化するようにアクセス ポイントを配置する必要があります。ロケーション確度低下は、次のために生じます。
  - 非単調の RSSI と近距離での距離動作
  - RSSI の変動に基づいて距離を解決するシステムの機能の低下

通常、この場合はアクセス ポイント間の距離を 40 ～ 70 フィートの間にしてアクセス ポイントを展開します。ただし、カバレッジ要件の厳しいアプリケーション（音声および高速データ）は、特定の状況ではより高密度の展開を行う必要があります。

ここで問題となるのは、前述の音声およびデータ アプリケーションに対する要件は、ロケーション トラッキングの要件も合わせて満たしているのか、ということです。この問いへの答えは「イエス」です。音声およびデータ アプリケーションの特定の要件に基づいて実行する正確な仕組みが備えられています。また、アクセス ポイントとアンテナ設定、インフラストラクチャが展開される環境の物理特性も考慮されます。詳細に説明するために、アクセス ポイントのレイアウト（主に高速データと 7921G 音声アプリケーションを対象）をさらに最適化してロケーション トラッキングを含めるようにした背景について検証します。

例として、最初に図 5-11 に示した 275 x 159 フィートのファシリティの音声アクセス ポイント レイアウトについて検証します。パス損失指数 3.5 の乾式壁工法のオフィスと屋内商用オフィス環境を表しています（図 5-19 を参照）。これらのアクセス ポイントのロケーションは、最初の設計者によって行われた、目的の信号強度とオーバーラップの計算に基づいて選択されました。この設計を行ううえで、設計者は『*Voice Over Wireless LAN 4.1 Design Guide*』に記載されている Cisco VoWLAN 設計のベスト プラクティスに従ったソリューションを提供することを目的としています。このマニュアルは、次の URL を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

7921G VoWLAN ハンドセットおよび高速 WLAN クライアント デバイスで使用される 802.11a 5 GHz WLAN を採用する、デュアル バンド インフラストラクチャを選択しました。802.11bg 2.4 GHz での動作もサポートされていますが、オーバーラップしないチャネルが 3 つしか存在しないために、802.11bg の全体的なキャパシティが著しく低下します。そのため、レガシー データおよび音声デバイス、および Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するアクティブ RFID 資産タグに使用は制限されます。レガシー データ デバイスには、クライアント ハードウエア デバイスの販売終了、バッテリ寿命の問題などの理由で 802.11a に移行できないデバイスも含まれます。対象となるレガシー デバイスには、PDA、バーコード スキャナ、簡単にアップグレードできない組み込みの無線オンボードを搭載するその他のデバイスが含まれます。この例では、802.11a に交換していない 802.11b 音声デバイスのユーザが依然として何人か環境内に存在すると仮定しています（たとえば、レガシー Cisco 7920 VoWLAN IP 電話、またはサードパーティ製の類似のレガシー 802.11b 専用デバイス）。

図 5-19　5GHz 音声および高速データ、2.4GHz レガシーのレイアウト

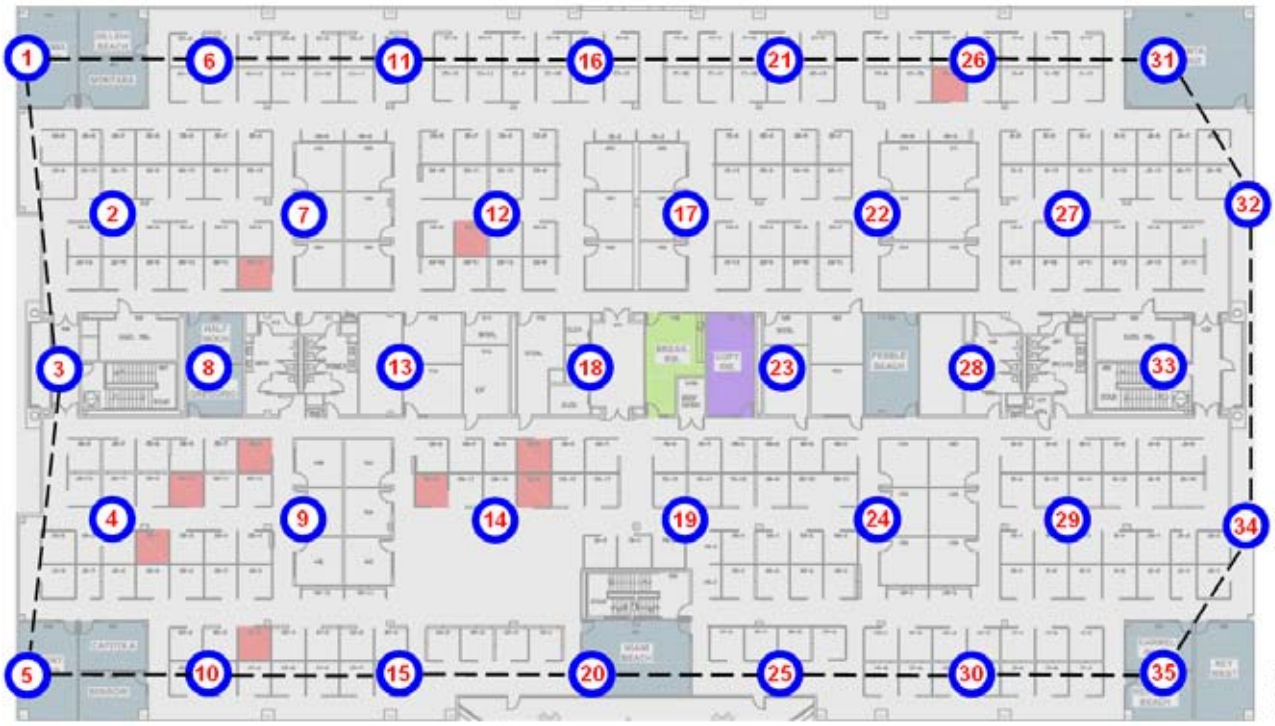


図 5-19 では、天井に取り付けた 35 の AP1240AG アクセス ポイントを使用していると仮定します。各アクセス ポイントには、802.11bg の場合 2.2dBi AIR-ANT4941 アンテナのペア、802.11a の場合 3.5 dBi AIR-ANT5951 アンテナのペアが取り付けられています。アクセス ポイントおよびアンテナは、10 フィートの高さに取り付けられています。設計は、VoWLAN および高速データ クライアント用の 802.11a 上で最小 -67 dBm の信号レベル、および少なくとも 24 Mbps のデータ レート、レガシー データおよび音声クライアント用の 802.11bg 上で最小 -67 dBm の信号レベル、および少なくとも 11 Mbps のデータ レートを提供することを目的としています。802.11a VoWLAN デバイスは、統合アンテナを持つ Cisco 7921G VoWLAN IP 電話であると仮定します。レガシーの音声およびデータ クライアント デバイスは、0 dBi の公称アンテナ ゲインがあると仮定します。アクセス ポイント間の間隔はおよそ 42.7 フィートで、フロア内部のアクセス ポイントが均等に分散されるように選ばれています。また、望ましいセル間のオーバーラップを形成するのに必要なアクセス ポイントの電力レベルは、クライアント デバイスの性能内に収まります。

次の点に注意してください。

- アクセス ポイント 1、5、32、34 を除いて、アクセス ポイントは直接フロア周囲に配置されていません。フロア全領域のロケーション確度を保つには、この配置は最適ではありません。
- 図 5-19 では、右側隅に周辺部アクセス ポイントがありません。このため、アクセス ポイント 31、32、34、35 の圏内には、4 つの四分円のうち少なくとも 3 つの四分円に範囲 70 フィート以内に 1 台のアクセス ポイントが存在する（4 つ目の四分円にあるアクセス ポイントの距離は問わない）というロケーション要件が満たされない領域が存在することになります。
- アクセス ポイントごとの送信電力は、802.11bg で + 5dBm、802.11a で +11 dBm に設定されています。この場合、-67 dBm のセルの半径がおよそ 28.72 フィート、802.11a VoWLAN と高速データ クライアントでセル間のオーバーラップが 15% になります。802.11bg レガシー クライアントの場合、-67 dBm のセルの半径がおよそ 31 フィート、セル間のオーバーラップが 20% になります。

（注）　アクセス ポイントで設定する送信電力は、クライアントによりサポートされる「単方向オーディオ」テレフォニー コールの可能性を回避するための送信電力レベルの範囲内に収める必要があります。シスコの Radio Resource Manager を使用してアクセス ポイントの電力レベルを管理する場合、設計者が送信電力レベルで必要なカバレッジ半径とオーバーラップ（クライアント デバイスでサポートされる最大送信電力レベルよりも少ない）の実現を目標とすることをお勧めします。Radio Resource Manager で、クライアント デバイスで達成可能な送信電力レベルを引き続き使用して、潜在的なカバレッジ ホールを解決するために使用できる、ある程度の電力割り当ての「ヘッドルーム」を確保するために、これを目標とすることをお勧めします。

この設計で最適なロケーション トラッキングをサポートするためには、いくつかの変更、追加、調整が必要になります。現在の音声とデータ設計、および関連するパラメータを検証すると、現在のアクセス ポイントの間隔、アンテナ取り付けの高さ、配置パターンはロケーションの使用の許容範囲内にあります。ただし、実際のフロア周囲、およびフロアの隅に配置するアクセス ポイントがないため、この問題を解決する必要があります。この様子は図 5-19 の破線で確認できます。アクセス ポイントの現在の境界を示す凸包を示します。それぞれの隅にある領域、および上部および下部の外周部は、この境界の外側にあります。これらの領域は一部のユーザには障害となりますが、この例の目的は、フロアのすべての領域で最適なロケーション確度を保証することです。これには、フロアの隅、およびすべての外周領域にある会議室も含まれます。そのため、最初に適切にフロア周囲を設定する必要があります。

最初の手順は、できるだけ建物の縁の近くに、上部と下部のアクセス ポイントの境界を実装し、一方で図 5-19 に示すアクセス ポイントの密度をできるだけ均等に保つようにします。Cisco Radio Resource Management（RRM）に依存して送信電力の制御を維持し、カバレッジ ホールの修正を行うユーザにとっては、特にアクセス ポイントの均等性を高く保つことが重要です。RRM は、フロア上のアクセス ポイントの分布が均等であるほど、最も効率的に機能します。

この時点で、次のオプションのいずれかを決定する必要があります。

1. 既存のアクセス ポイント コンステレーションからなる等辺の編成を広げて、アクセス ポイントの上部および下部の列を再配置し、フロア周囲の上部および下部を形成します。このオプション、およびこの例の環境では、右側と左側の外周にある欠けた領域を埋めるために必要なアクセス ポイントの追加は最小数ですみます。アクセス ポイント間の距離を広げる必要があるため、このオプションは下記のオプション 2 と比較して、よりアグレッシブな手段として検討します。アクセス ポイントの送信電力に対する制限を超えるほど設計を変更しないよう注意する必要があります（下記を参照）。
2. 既存のアクセス ポイント コンステレーションからなる等辺の編成を縮めて、アクセス ポイントの現在の最上部の列を上に移動し、最下部の 6 列目に、アクセス ポイントの外周を一番下に新たに形成します。このオプションでは、上記のオプション 1 と比較した場合、追加のアクセス ポイントの数が多くなります。ただし、アクセス ポイント間の距離を縮めたため、通常このオプションでは最初の設計よりもアクセス ポイントの送信電力を大きくする心配はありません。また、2 の場合、より慎重な手段として検討します。

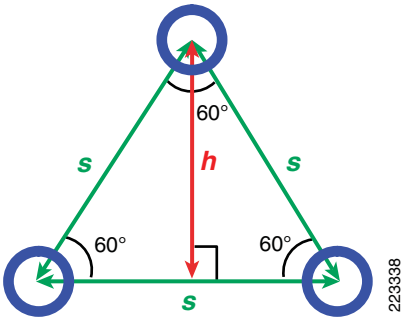
最初のオプションを検討する場合、現在のアクセス ポイント間の間隔と送信電力レベルを検証し、実際のフロア周囲の外側にある既存の列に配置するために必要な、アクセス ポイント間の間隔を推測する必要があります。現在のアクセス ポイントの送信電力レベルがクライアント デバイスの電力性能に対してすでに高いレベルにあり、アクセス ポイント間の距離が広いと推測される場合、外周の配置に合わせて既存のアクセス ポイントのコンステレーションを拡大することは最適な方法ではありません。この理由は主に、望ましいアクセス ポイントの電力レベルより高い電力使用量が必要になるためです。このような場合、オプション 2 を選択することをお勧めします。このオプションでは等辺の編成を縮小するため、アクセス ポイント間の距離が縮まります。通常、アクセス ポイントの送信電力レベルは同じか、それ以下に減ります。

送信電力レベルは 802.11bg の場合 +5 dBm、802.11a の場合 +11 dBm に設定されていることを思い出してください。現在の編成（図 5-19 の等辺三角形を参照）を均等に拡張した場合の、実際のアクセス ポイント間の新しい距離を求めるには、幾何学的計算を行う必要があります。必要なアクセス ポイント間の距離を求める場合、現在の上部および下部のアクセス ポイントの列は、実際のフロア周囲の上部および下部に配置されるとおりに再配置されると仮定します。図 5-19 の 275 x 159 フィートのフロアの場合、フロアの上部から下部の幅（159 フィート）を等辺の三角形（4）で割ることによって求められます。これにより予測される編成の高さは 39.75 フィートになります。

等辺三角形のそれぞれの角は 60°（図 5-20 を参照）であるという前提から、等辺三角形の高さ *h* から、任意の辺 *s* の長さを次のように計算します。

$$h = s(\sin 60°)$$

図 5-20　　等辺のアクセス ポイントの編成



s の値を求めるには、$s = \frac{h}{\sin 60°}$ または $\frac{39.75}{.866}$ = 45.9 フィートと計算します。このため、外側のアクセス ポイントの上部と下部の列を実際の建物の縁に移動させるために、現在のアクセス ポイント間の間隔を 42.7 フィートから 45.9 フィートに広げる必要があります。この場合、アクセス ポイント間の間隔がやや広がりますが、対応する送信電力の微弱な増加がある場合は、簡単に調節できます。次の手順で、推奨のオーバーラップのレベル（新しく計算したアクセス ポイント間の間隔を考慮して）をサポートするために必要な新しいセル サイズを求めます。

アクセス ポイント間の間隔の新しい値を使用して、802.11a の場合 15% のセル間のオーバーラップがある -67 dBm のセル信号境界を最初に計算します。その後、802.11bg で使用するレガシー データと音声デバイスの場合 20% のセル間のオーバーラップがある -67 dBm のセル信号境界を計算します。任意の 2 つの隣接アクセス ポイント セルの半径は、等しい（つまり R1=R2=R）という前提で、円と円の共通部分をこの計算の基盤とするこの等式を使用できます。アクセス ポイント間の距離とオーバーラップの割合は既知であることを考慮して、セル半径を求めるには、次のように計算します。

$$O\pi R^2 = 2R^2 arccos(\frac{d}{2R}) - \frac{1}{2} d\sqrt{4R^2 - d^2}$$

定義：

- O = 望ましいオーバーラップの割合の百分率
- $\arccos(\frac{d}{2R})$ はラジアンで表されます
- d = アクセス ポイント間の距離（フィート）

- *R* = セルの半径（フィート）

オーバーラップの割合 *O* として、15（802.11a の場合）または 10（802.11bg の場合）のいずれかを代入し、アクセス ポイント間の距離 *d* として 45.9 フィートを代入します。上に示した関数の近似根として *R* の値を求める場合、802.11a を使用する 15% のセル間のオーバーラップではセルの半径は 30.88 フィート、802.11bg を使用する 20% のセル間のオーバーラップでは 33.4 フィートと求められます[1]。

ここで、望ましいセル信号境界を実装するために必要なアクセス ポイントの送信電力設定の計算に必要な情報を説明します。これは、前に説明した受信信号強度（TX_{POWER}）の等式の形（基準パス損失、送信電力、およびその他の受信および送信のゲインとロス）を使用して実行できます。これについては、「受信信号強度（RSS）」（P.2-7）で説明します。求めるのがアクセス ポイントの送信電力（TX_{POWER}）で受信信号強度ではない場合、次のように変更された形の等式を使用します。

$$TX_{POWER} = RX_{POWER} + Loss_{TX} - Gain_{TX} + PL_{1METER} + 10\log D^{n} + s - Gain_{RX} + Loss_{RX}$$

この例の目的の場合、次のことを前提とします。

- ケーブル、コネクタなどのよる送信ロス（$Loss_{TX}$ と $Loss_{RX}$）は 0 dB に等しい。
- 0 dB のシャドウ フェーディングの標準偏差。
- レガシー 2.4 GHz データ クライアント デバイスの受信アンテナ ゲインは 0 dBi。

802.11a および 802.11bg に対して -67 dBm の最小受信信号強度（RX_{POWER}）、適切なアンテナ ゲイン、メートル単位のセル半径（30.88 フィート = 9.41 メートル、33.4 フィート = 10.18 メートル）、推定パス損失指数 *n* の 3.5 と基準パス損失の予測に従って適切な値を代入すると、次の結果が得られます。

802.11bg の場合：

TX_{POWER} = -67 dBm + 0 - 2.2 dBi + 40 dB + 10log($10.18^{3.5}$) - 0 + 0

= -29.2 + (10 * 3.527)

TX_{POWER} = +6.07 dBm、つまりおよそ +8 dBm

802.11a の場合：

TX_{POWER} = -67 dBm + 0 - 3.5 dBi + 46 dB + 10log($9.41^{3.5}$) - (-3.0) + 0

= -24.5 + (10 * 3.408) + 3

TX_{POWER} = +12.58 dBm、つまりおよそ +14 dBm

これらの電力レベルは、AP1240AG アクセス ポイントで使用可能な、次に使用可能な送信電力のインクリメントに切り上げられます。これは、セル信号境界の -67 dBm で推奨される 20% のオーバーラップ目標を達成するために必要な送信電力よりも +1.93 dBm 高いため、オーバーラップは 20% の目標を超えていると予測できます。20% のオーバーラップは最小ターゲットであるため、これは許容範囲内です。同様に、802.11a の場合、アクセス ポイント送信電力レベルの +14 dBm は、推奨の 15% オーバーラップを達成するために必要なレベルより +1.42 dBm 高いため、これもセル間のオーバーラップは予期していたものより高くなります。

この場合、代わりにアクセス ポイント間の距離を広げる方法で対処することもできます。アクセス ポイント間の距離が広げられたため（42.7 フィートから 45.9 フィート）、算出された要件への準拠を守るために 802.11a と 802.11bg のアクセス ポイント送信電力設定に対して a +3 dBm の増加が必要です。アクセス ポイント送信電力レベルが増加しても、環境の変化により生じる潜在的なカバレッジ ホールまたはその他の異常に対処するために、追加の送信電力は 2 つの帯域で予備のためそのまま確保されます。この方法を適用しない場合、アクセス ポイント間の間隔を縮め、アクセス ポイントの 6 列目を導入する、2 つ

1. Maple、Mathematica、または Maxima などの記号および数値計算が可能な Computer Algebra System（CAS; コンピュータ代数システム）は、以下のような計算を解くのに便利です。Maxima を使用して、閉区間（d/2, d）を越える前述の等式の近似根として R を計算する方法については、このマニュアルの「*付録 B*」を参照してください。

目のオプションを使用して続行します。計算の主な相違点は、フロアのサイズを、等辺三角形の編成の 5（4 ではなく）列で割ることです。これにより、編成の高さが低く、アクセス ポイント間の距離が短くなるため、セル間の半径が小さく、送信電力も低くなります。

（注）　この項で説明する信号レベルの測定と計算、および一般に受け入れられている RF 理論は、計画だけを目的としています。異なる環境のこれらの理論的な計算からある程度の信号レベルの変動を予測することは妥当な方法です。

静的にアクセス ポイントの送信電力レベルを管理するのではなく、代わりに Cisco Radio Resource Manager（RRM）を使用できます。RRM を使用し、リアルタイムの WLAN 状態に基づいて動的にアクセス ポイント送信電力を制御できます。普通の状況では、性能を保ち、干渉を少なくするために、すべてのアクセス ポイントで送信電力を管理する必要があります。エラーの発生したアクセス ポイントを検出した場合、周囲のアクセス ポイントで送信電力を自動的に増やし、カバレッジの損失で生まれた隙間を埋めることができます。カバレッジ ホールが発生した場合、RRM は、周囲のアクセス ポイントに残っている予備の送信電力を使用して、隣接カバレッジ レベルを上げ、調査、解決が終わるまでカバレッジ ホールに対処します。

どちらの場合でも、アクセス ポイントの送信電力設定の検証を定期的に実行することをお勧めします。アクセス ポイントの送信電力設定を手動で管理する場合、システム全体のパフォーマンスを検査して、元の設計の前提がまだ有効で、これらの前提を再検討しなくてはならないような大きな変更が環境内にないことを確認する必要があります。RRM を使用すると、システムの変更が監視され、アクセス ポイントの送信電力設定に増減がないかが確認されます。システムのインストール後、RRM に対してさまざまな調整を行い、アクセス ポイントの送信電力レベルや他のパラメータの選択内容を、環境で予測される範囲内に収めることができます。

インストール直後と、インストール後の一定の時間、RRM アクティビティを確認して、システムが安定し、最終パラメータ選択が行われたことを確認してください。「安定」期間の終わりに、システム設計者は RRM によって行われた選択が設計全体の予測範囲内に収まることを確認する必要があります。システムが安定したら、RRM で管理されているパラメータに経時的変動がほとんどないようにする必要があります。環境または装置の大きな変更を禁止することによって、アクセス ポイントの送信電力レベルの選択内容を静的に保つ必要があるためです。割り当てられたアクセス ポイントの送信電力レベルまたはチャネルが絶えず変動する場合、システム管理者はこの兆候を、環境内で発生する可能性のある潜在的な他の異常と見なす必要があります。このような頻繁な変動の根本原因は、迅速に調査し、解決する必要があります。

（注）　RRM のメカニズムの詳細な説明は、このマニュアルでは取り上げません。このメカニズムの詳細は、次の URL の『*Radio Resource Management under Unified Wireless Networks* document』を参照してください。
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml
また、VoWLAN 設計で RRM を使用することを検討しているすべてのユーザは、次の URL の『*Voice Over Wireless LAN 4.1 Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

図 5-21 に、上の計算で得られた情報、および次に説明する周辺部アクセス ポイントの配置を使用した、更新されたアクセス ポイント レイアウトを示します。

図 5-21　5GHz の音声および高速データ、2.4GHz のレガシー、ロケーションのレイアウト

図 5-21 に、アクセス ポイント間の距離を広げた影響を示します。

- 一番上の列（アクセス ポイント 1、6、11、16、21、26、31）と一番下の列（アクセス ポイント 5、10、15、20、25、30、35）のアクセス ポイントは、実際のフロア周囲の上部と下部に配置されています。
- フロア周囲の右側で、アクセス ポイント 31 と 35 がフロア右側の隅に移動されました。アクセス ポイント 33 は、フロア周囲の右側に移動されました。グループとして、アクセス ポイント 31 ～ 35 はフロア周囲の右側を形成します。
- フロア周囲の左側で、アクセス ポイント 1 と 5 がフロア左側の隅に移動されました。さらに、2 つの新しいアクセス ポイント（36 と 37。隣に黄色の星を表示）が設計に追加され、フロア周囲の左側の編成を完成させました。

図 5-21 に追加された 2 つの新しいアクセス ポイントによって、統合された音声、データ、およびロケーション設計のためのアクセス ポイント カウント合計が 37 になりました。この設計の音声およびデータ カバレッジの主要なソースは、フロア全体に見られる、等辺編成に参加するアクセス ポイントから生じます（つまり、赤で描かれるアクセス ポイントとして図 5-21 で確認できます）。アクセス ポイント 32、34、36、および 37 はロケーション外周を確立するのに必要ですが、ここで示した前提と計算に基づくと、どちらかの帯域に音声またはデータ カバレッジを提供する場合は必要ではありません。そのため、これらのアクセス ポイントは大幅に縮小された送信電力で動作するよう静的に設定できます（たとえば、-1 dBm など）。また、これによってこれらのアクセス ポイントの相互チャネルの干渉も最小化されます。

（注）　VoWLAN 設計での相互チャネルの干渉の詳細は、次の URL の『*Voice Over Wireless LAN 4.1 Design Guide*』を参照してください。
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.html

電力レベルを管理するために Cisco RRM を使用する場合、ロケーションの目的だけのために設計に配置されるアクセス ポイントを Radio Resource Management 送信電力制御またはカバレッジ ホールの修正プロセスに含めないでください。カスタムのアクセス ポイント送信電力レベルの設定（WCS またはコントローラ GUI で「カスタム」の TX 電力オプションを使用）では、自動的にこれらのアクセス ポイントが送信電力およびカバレッジ ホール修正アルゴリズムから除外されます。

計画出力と計算に基づき、図 5-19 に示す元の音声およびデータ設計はロケーション準備完了設計に移行できます。この設計は、『*Voice Over Wireless LAN 4.1 Design Guide*』で説明するベスト プラクティスに準拠しており、レイアウトと設定でわずかな変更があります。移行すると、VoWLAN、5 GHz での高速データおよびロケーション トラッキング、2.4 GHz でのロケーション トラッキングのレガシー データおよび音声サポートをサポートするのに最適な結合設計になります。

設計および設計の実装を改良するために実行できる追加アクティビティに次のものがあります。

- サイトを巡回し、アクセス ポイントの取り付けを行うフロア計画の領域が実際に適合するかどうかを確認します。フロア計画と設計図で、アクセス ポイントを取り付けるそれぞれのロケーションの状態を常に正確に示すとは限らないため、この方法は有効です。たとえば、「図面上」で実行可能な対象に見える特定のロケーションも、実際には手が届かなかったり（電気室など）、不適切であったり（屋外のバルコニーなど）、あるいは条件に合っていないことがあります。このような場合、アクセス ポイントを元の位置に近いところに再配置し、全体的な設計への影響を最小限にします。図 5-21 では、一般的な障害物は避け、影響を受けるアクセス ポイントをわずかに移動しています。
- いくつかのアクセス ポイントをフロアのさまざまなテスト領域に一時的に取り付けて RF 伝播およびカバレッジの前提を確認します。次に、適切な「サイト調査」ソフトウェア ツールを持つポータブル クライアント デバイスを使用して、実際の RF 信号強度とセル間のオーバーラップを測定します。これは、アクセス ポイント セルの周囲のノイズ レベルを測定し、予測された信号対雑音比が十分であるかどうかを判断するのに最適なタイミングでもあります。シスコの RRM 機能でもクライアント SNR を監視し、クライアント数が前述の SNR しきい値を下回る場合に、アクセス ポイントの電力を上げることに注意してください。RRM の詳細は、次の URL の『*Radio Resource Management under Unified Wireless Networks*』を参照してください。

  http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml
- DFS に属している追加の 802.11a に干渉する可能性のあるロケールに、レーダー ユーザが存在するかどうかを検証します。存在しない場合、WLAN コントローラ上で DFS を有効することにより、これらのチャネルを使用可能にできます。

（注）　Cisco Unified Wireless Network ソフトウェア リリース 4.1 では、DFS 操作を行う 802.11a チャネル上で、Cisco Compatible Extensions ロケーション測定は有効にされていません。DFS チャネルの場合、通常動作の一部として WLAN クライアントから送信されたプローブ要求からの RSSI は、ロケーション トラッキングの目的で使用されます。

この項で説明した技術と原則では、VoWLAN に合わせてどのように設計を実装するか、およびデータのベスト プラクティスをどのようにして「ロケーション準備完了」にアップグレードするかを示しています。アクセス ポイント間の距離、セルの半径と送信電力の背景にある主要な概念とは、どのように相互に関連しているか、またこれらの要素をどのように使用してカバレッジ オーバーラップを決定し、多様なサイズと形状の設計、および多様なパス損失特性とシャドウイングを持つ環境にどのように適用できるか、というものです。

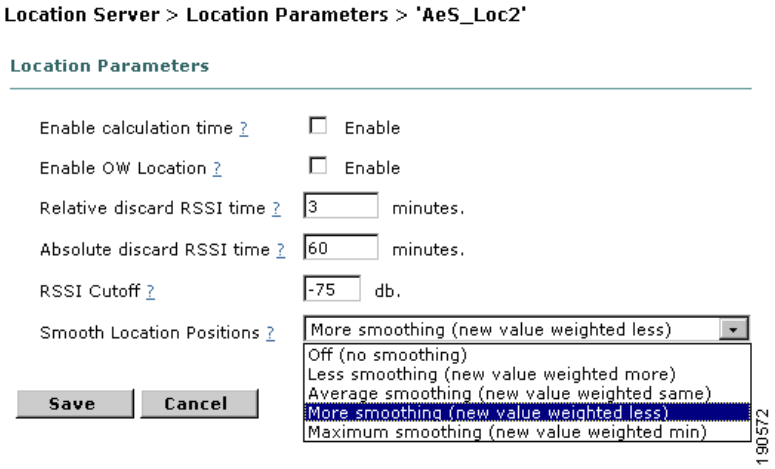
ロケーション表示ジッタの回避

ロケーション スムージングを取り入れて、ネットワーク管理者がロケーションの不安定さに対応することができます。この不安定さは実際に移動していないクライアントで見られます。この原因にはさまざまな要素があり、次のものが考えられます。

- 検出済みの RSSI の変動につながるクライアント送信電力の変動
- 環境の変化（位置を動かした半永久的な障害物を含む）は、減衰とマルチパスの変動につながります。
- クライアントの向きの変更
- シャドウ フェーディング

ロケーション スムージングは、デバイス ロケーションに適用されるさまざまなレベルの平均化が可能です。スムージング要素は、図 5-22 に示すように、[Location] > [Location Server] > [Administration] > [Location Parameters] の *Smooth Location Positions* パラメータから設定できます。

図 5-22　　ロケーション スムージングの設定



最後の既知の位置と対比した、デバイスの最新の計算済み位置にさまざまな重みを割り当てることによって、さまざまなスムージング ファクタ オプションは、表示されるロケーション位置に影響します。これらの重みは、表 5-1 に示すように割り当てられます。

表 5-1　スムージング ファクタの重み付け

Smooth Location Positions の値	以前の位置に割り当てられた重み	新しい位置に割り当てられた重み
Off（スムージングなし）	0%	100%
Less smoothing	25%	75%
Average smoothing	50%	50%
More smoothing（デフォルト）	75%	25%
Maximum smoothing	90%	10%

以前の位置に割り当てられる重みが、新しい位置に割り当てられる重みと比較して大きくなる場合、表示されるデバイスの変動は小さくなります。ロケーション スムージングを使用しても、そのデバイス用のロケーション表示のすべての監視対象の移動が除外されるわけではありません。ロケーション スムージングを使用すると、それらの移動がエンド ユーザに伝達される割合が制限されるだけです。

ロケーション スムージングを使用すると、ロケーション表示の安定性と、位置の変更に対するロケーション表示の反応時間のバランスが調整されます。ほとんどの環境で、デフォルト スムージング ファクタを使用すると、表示機能が改善されます。WLAN クライアントとタグ付き資産の移動があまりない環境では、スムージング ファクタを高くすることをお勧めします。タグ付き資産およびクライアントを頻繁に移動し、場合によっては常に、またはほとんど常に動いているケースでは、スムージング ファクタを低くすると（またはスムージングなし）良い結果が得られます。表示されるロケーション遅延を最小化することに主に関心があるユーザ（ある程度のロケーション ジッタがあるとしても）は、ロケーション スムージングの値を低くするか、ロケーション スムージングをすべて無効にする必要があります。

複数 Location Appliance の設計

前述したように、1 台の Cisco Wireless Location Appliance では、最大 2,500 台のデバイス（WLAN クライアント、資産タグ、不正アクセス ポイント、不正クライアントを含む）を追跡できます。この Location Appliance では、[Location] > [Location Server] > [Administration] > [Polling Parameters] で、特定の追跡対象デバイス カテゴリを有効できます。各 Location Appliance のキャパシティを最大限に活用するために、シスコでは、ポーリング カテゴリ（クライアント ステーション、不正デバイス、資産タグ、統計情報）のうち、目的に合致し同時追跡と過去のロケーションを必要とするものだけを有効にすることをお勧めします。たとえば、主要な目的が資産タグの追跡だけである場合は、クライアントや不正デバイスのポーリング カテゴリを有効にしないでください。これらのカテゴリを有効にすると、Location Appliance と WLAN コントローラ間のネットワーク トラフィック全体を増大させるだけでなく、追跡対象デバイス キャパシティ 2,500 台の一部を不要に使用することになります。あまり重要性のないデバイス カテゴリのポーリングを無効にすることによって、Location Appliance のフル キャパシティをより有効に活用できます。

（注） 本書の範囲外ですが、ロケーション認識 Cisco UWN のリリース 4.2 では、Location Appliance が持つデバイス追跡キャパシティ全体のうち追跡対象の各デバイス カテゴリ（WLAN クライアント、資産タグ、不正デバイス）に配分する割合に対して個別に制限を設けられる機能拡張が導入されています。

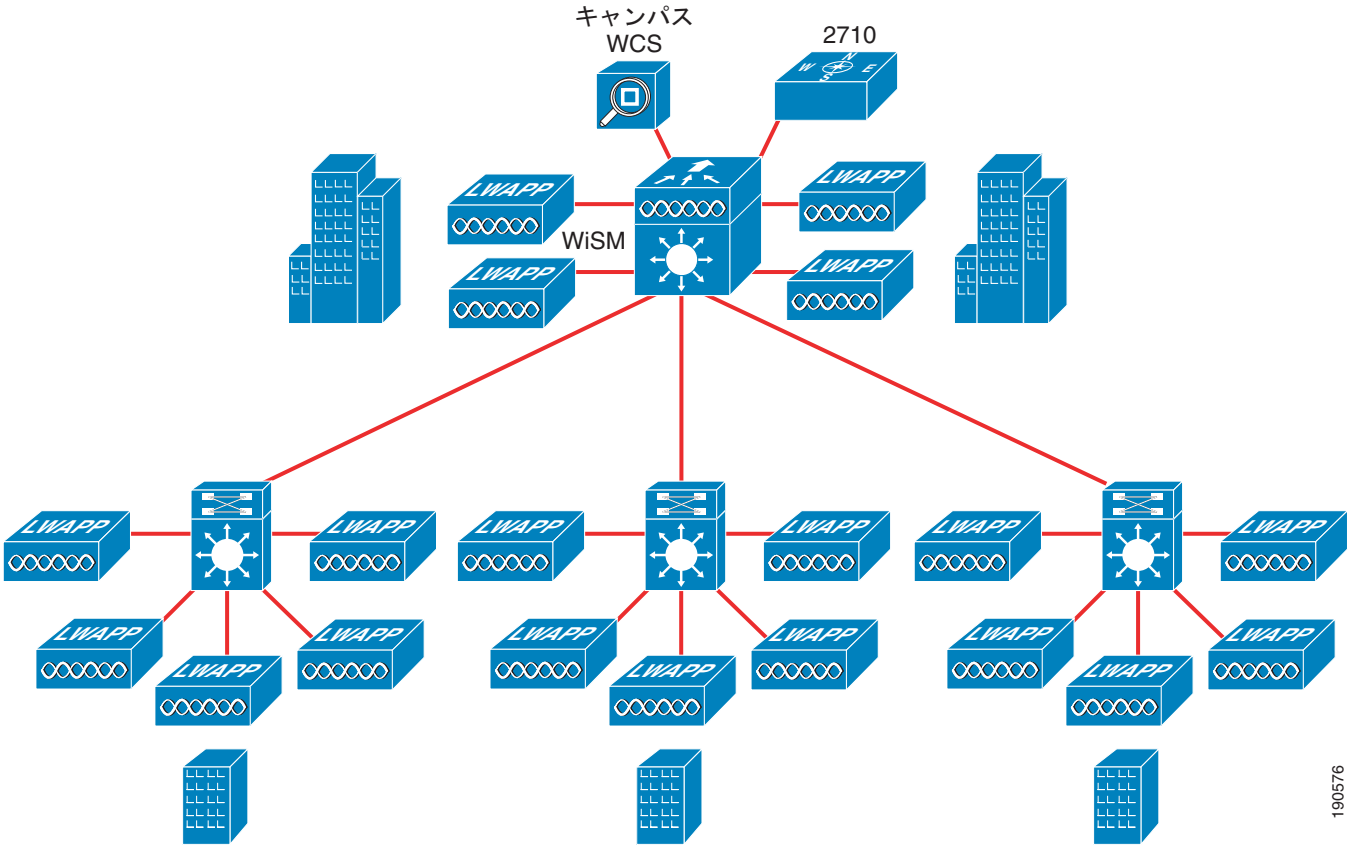
- Cisco WCS リリース 4.1 は、ハードウェアの構成に応じて、次のとおりアクセス ポイント 500 ～ 3,000 箇所、WLAN コントローラ 125 ～ 750 台をサポートできます。
- WCS ハイエンド サーバ：アクセス ポイント 3,000 箇所、WLAN コントローラ 750 台をサポート
- WCS 標準サーバ：アクセス ポイント 2,000 箇所、WLAN コントローラ 500 台をサポート
- Cisco Wireless LAN Solutions Engine（WLSE）ハードウェア上の WCS：アクセス ポイント 1,500 箇所、WLAN コントローラ 100 台をサポート
- WCS ローエンド サーバ：アクセス ポイント 500 箇所、WLAN コントローラ 125 台をサポート

（注）　詳細については、次の URL にある『*Cisco Wireless Control System Configuration Guide*』の「*System Requirements*」を参照してください。
http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcswst.html#wp1061082

WCS *管理ドメイン*の最大サイズ（つまり、1 台の WCS によって管理されるデバイスの総数）は、サーバ プラットフォームの選択と関係があります。非常に大規模なネットワークでは、個別の WCS が管理する複数の管理ドメインにネットワークを区分する必要がある場合があります。ソフトウェア リリース 4.1 から、シスコでは Cisco Unified Wireless Network の大規模実装においてスケーラビリティ、管理容易性、可視性を向上する管理集約プラットフォーム WCS Navigator を導入しています。WCS Navigator は、複数の Cisco WCS 管理プラットフォームをその物理的ロケーションにかかわらず全体的に管理できるソフトウェア ベースのソリューションです。Cisco WCS Navigator は、データベースを搭載した個別のサーバ プラットフォームで稼動し、最大 20 台の Cisco WCS 管理プラットフォームと最大 20,000 箇所のアクセス ポイントをサポートします。Cisco WCS Navigator の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps7305/index.html

各管理ドメインの最大サイズは、管理ドメインを管理する WCS プラットフォームのキャパシティに関係しますが、*ロケーション ドメイン*の最大サイズ（つまり、1 台の Location Appliance により追跡されるデバイス数）は Location Appliance の追跡対象デバイス キャパシティにより制限されます。中規模から大規模の展開の多くでは、単一の WCS 管理ドメインと単一のロケーション ドメインを組み合わせた標準の展開（図 5-23）でデバイス追跡と管理の要件を満たすことができます。

図 5-23　シングル管理ドメインおよびロケーション ドメイン



ただし、より大規模なキャンパスでは、追跡対象デバイスの総数が 1 台の Location Appliance のキャパシティを超えることがあり、設計で複数の Location Appliance（および複数のロケーション ドメイン）を使用する必要が生じます。組織によっては、組織内部のコスト計算や組織の成長に対応するためといった組織内の事情により、意図的に追跡対象デバイスの負荷を複数の Location Appliance に分散しているところもあります。その良い例として、組織内部の IT 資産に加え、多数にのぼる患者関連の医療資産の追跡が行われる大学医療センターの WLAN が挙げられます。このような環境では、資産追跡の分割と、部門間における設備およびコストの明確な区分のため、個別の Location Appliance を使用する必要があります。

（注）　特定のデバイス カテゴリで検出された追跡対象デバイスが 250 台を超える場合、WCS は最初に追跡された 250 台だけを表示することに注意してください。最初の 250 台の表示後、残りのデバイスを表示するために、WCS はユーザに対してデバイス フィルタリングを使用するように求めます。

ソフトウェア リリース 4.1 では、WLAN コントローラは各デバイスについて表 5-2 に示すキャパシティを備えています。

表 5-2　WLAN コントローラの各デバイスに対するキャパシティ

コントローラ モデル	サポートされる WLAN クライアント	サポートされる資産タグ	サポートされる不正 AP	不正クライアント
2006	256	500	125	100
2106	256	500	125	100
4402	2,500	1250	625	500
4404	5,000	2500	625	500
WiSM	10,000	5000	1250	1000
NM-WLC6	256	500	125	100
NME-WLC8/12	350	500	125	100
3750G	2,500	1250	625	500

以降のサブセクションでは、通常単一の管理ドメインとロケーション ドメインの組み合わせのキャパシティを超える、より条件の厳しい設計でのニーズを満たすために、どのように WCS、Location Appliance、WCS Navigator を組み合わせるかについて説明します。

シングル管理ドメイン（マルチ ロケーション ドメイン）

この設計アプローチでは、組織の WAN 環境におけるネットワーク管理の要件が、単一 WCS 管理ドメインのキャパシティで十分に対応可能な範囲内であると想定します。ただし、クライアント、不正デバイス、資産タグを合わせて 2,500 台以上の追跡を行う必要があります。これは、図 5-24 に示すように、単一管理ドメインを介して管理される複数ロケーション ドメインを使用することにより達成できます。

図 5-24　シングル管理ドメイン（マルチ ロケーション ドメイン）

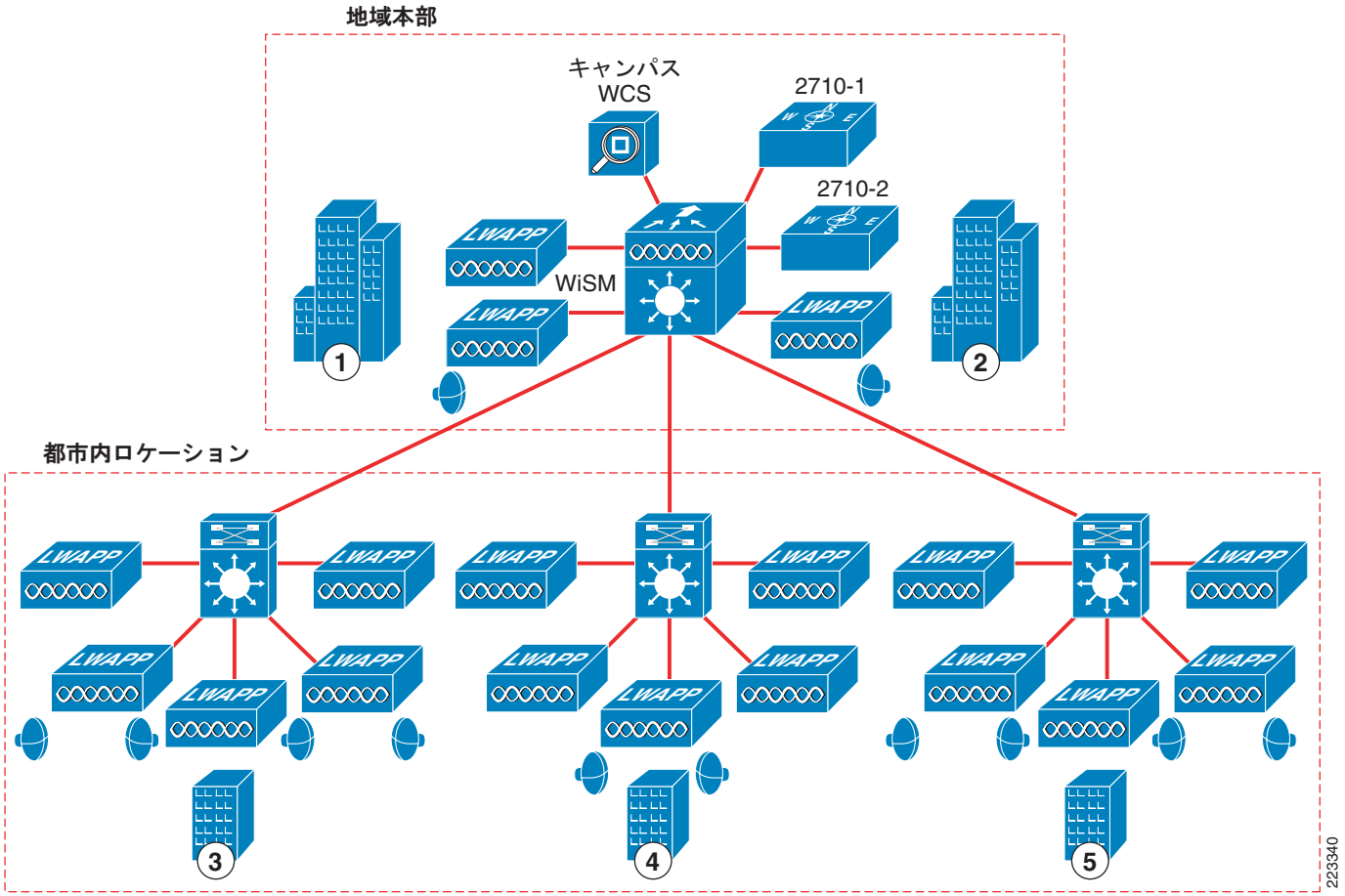


図 5-24 は、大規模な地域本部キャンパス ロケーションとその下に展開される 3 箇所の地域都市内キャンパス ロケーションに対して、WLAN 管理サービスを提供する単一のキャンパス WCS サーバを図示したものです。この場合、すべてのロケーションは大都市内に位置しています。

（注） この例でのロケーションは、地理的には分散していますが、複数ロケーション ドメインとコントローラの割り当てに関する前述の概念は、追跡対象デバイスの総数が 2,500 を超えるこのような単一の連続的なキャンパスにも適用されます。

図 5-24 に示す例では、地域本部ロケーションには 140 箇所のアクセス ポイント、各都市内ロケーションにはそれぞれ 50 箇所のアクセス ポイントが含まれ、不特定の数のチョークポイント トリガーを伴います。この設計には、Wireless Service Module（WiSM）を搭載した集中型 Cisco Catalyst 6500 を使用する必要があります。WiSM は、各サービス モジュールに 2 つの内蔵コントローラを備えており、それぞれ WiSM-1、WiSM-2 と呼ばれます。WiSM-1 は地域本部ロケーションにあるアクセス ポイントのサービス、WiSM-2 は都市内ロケーションにあるアクセス ポイントのサービスに使用します。2 台

の Cisco 2710 Wireless Location Appliance は、最大 5,000 台のデバイスの MAC アドレスを追跡可能なキャパシティを提供します。Location Appliance 2710-1 は、地域本部内のみの資産追跡に割り当てられ、Location Appliance 2710-2 は、3 箇所の都市内ロケーションすべての資産追跡を行います。Location Appliance 2710-2 は、地域本部内のデバイスの追跡は行いません。

WCS を使用して、図 5-24 に示す広域キャンパス全体を網羅する単一のネットワーク設計（アクセス ポイントとチョークポイントの配置を記載した屋外、キャンパス、建物、フロアのマップ一式）を作成することができます。最初に、地域本部ロケーションについて、建物 1 と 2 および各建物内のフロアを加えます。コントローラ WiSM-1 に対して登録されている 140 箇所のアクセス ポイントと、地域本部で使用されるチョークポイントは、このネットワーク設計に割り当てられます。さらに、地域本部ロケーションに対してイベント通知グループが作成されます。それから、WCS を使用して、リモート都市内ロケーションの建物 3、4、5 と各建物のフロアを追加します。コントローラ WiSM-2 に対して登録されている 150 箇所のアクセス ポイントと、都市内リモート ロケーションで使用されるチョークポイント トリガーは、このネットワーク設計に割り当てられます。都市内リモート ロケーションに対して、個別のイベント通知グループが作成されます。

このプロセスでの重要なステップは、両方の Location Appliance 間でネットワーク設計を共有することだけでなく、各 Location Appliance のロケーション ドメインに含めたい WLAN コントローラが、その Location Appliance *のみ*に対して確実に正しく同期されるようにすることです。つまり、このキャンパス ネットワーク設計は Location Appliance 2710-1 と 2710-2 の両方に同期していますが、Location Appliance 2710-1 に同期しているのはコントローラ WiSM-1 *のみ*、Location Appliance 2710-2 に同期しているのはコントローラ WiSM-2 のみとなります。

上記の操作を行った後は、追跡対象デバイスの総数を 2 つの個別のロケーション ドメイン間で配分して、単一の WCS 管理ドメインからキャンパス全体の管理を行えるようになります。設計の実装が完了すると、組織全体が単一の管理ドメインとして管理され、管理ポーリングや報告は集中型の WCS から発せられます。Location Appliance 2710-1 は、ロケーション ドメイン（地域本部）内の追跡対象デバイスに関するすべての情報について、コントローラ WiSM-1 のポーリングを処理します。Location appliance 2710-2 は、ロケーション ドメイン（都市内ロケーション）内の追跡対象デバイスに関するすべての情報について、コントローラ WiSM-2 のポーリングを処理します。これらの 2 つのロケーション ドメインは、1 つの共通のネットワーク上で稼動し、1 つの共通管理ドメインから管理され、地域本部において同一の物理 WiSM モジュール上に共存するコントローラを持つという点を除き、基本的には互いに独立して存在します。

代替的なアプローチでは、2 つの個別の Location Appliance ネットワーク設計を作成する必要があります。これらの設計には、それぞれのロケーション ドメインが網羅するキャンパス ネットワーク部分のみが含まれます。これらのネットワーク設計は、それぞれ適切な Location Appliance に同期されるほか、その Location Appliance がサービスするコントローラにも同期されます。このアプローチは非常に機能的ですが、一般的に、利便性と管理容易性の観点から、単一ネットワーク設計のアプローチが推奨されます。一方、非常に大規模なネットワーク設計を行う際には、デュアル ネットワーク設計のアプローチの方が適切である場合もあります。環境を 2 つの異なるネットワーク設計に区分することにより、不要なアクセス ポイント、建物、フロアに関する詳細やこれらを表すグラフィック画像を Location Appliance に読み込むことを回避できます。

複数の独立したロケーション ドメインを含む設計では、ドメイン間での追跡対象デバイスの移行がある場合に、その程度と頻度を把握することが重要です。複数ロケーション ドメインが使用される設計には、「閉ループ」システムとして機能することを意図したものがあります。つまり、新たに発見された不正デバイスを除き、追跡対象デバイスの追加や削除は厳密に管理された状況下で行われます。閉ループシステムでは、各ロケーション ドメインにおける不正デバイス以外の追跡対象デバイス数がほぼ一定に保たれます。ただし、実際の展開環境では「開ループ」の業務プロセスを導入する場合が多くあります。開ループのプロセスでは、管理されない状況下でのデバイスの追加、削除、移行がある程度生じる可能性があり、また実際に生じてしまうことがよくあります。

これには大きな影響があります。ロケーション ドメイン間で移行された追跡対象デバイスが移行元から削除されるまで、各 Location Appliance のアクティブ ロケーション データベースに表示される可能性があるためです。追跡対象デバイスは、次の条件がすべて満たされると、Location Appliance のアクティブ ロケーション データベースから削除されます。[1]

1. その Location Appliance がサービスするコントローラ（つまり、その Location Appliance に同期しているコントローラ）に登録されているアクセス ポイントによってデバイスが検出されないこと
2. アクセス ポイントで追跡対象デバイスの検出を行っていたすべてのコントローラが、Location Appliance に対してデバイスについての RSSI 報告を停止していること（通常は、コントローラの RFID タイムアウトまたはクライアント ユーザ タイムアウトの経過後）
3. Location Appliance の不明データのクリーンアップ間隔（ADCI）が経過していること（デフォルトは 1,440 分）

追跡対象デバイスが複数 Location Appliance に存在している間は、同一デバイスに対して複数のエントリが WCS クライアント、タグ、不正デバイスの表示メニューに表示される場合があります。この例として、ラボにおける実験でのすべての Location Appliance にわたる資産タグ検索結果を図 5-25 に示します。この実験では、MAC アドレス 00:0C:CC:5E:82:90 の資産タグが、Location Appliance「Loc1」のドメインから Location Appliance「Loc2」のドメインに移行しています。2 つの建物のアクセス ポイントは異なるコントローラに登録され、これらのコントローラはそれぞれ 2 つの異なるロケーション ドメインに含まれます。たとえば、Havermeyer Building という建物を対象とするコントローラが Location Appliance「Loc1」によりポーリングされており、Pupin Hall Building という建物を対象とするコントローラが Location Appliance「Loc2」によりポーリングされていると仮定します。

図 5-25　デバイス移行によるデバイス表示の重複

Tags

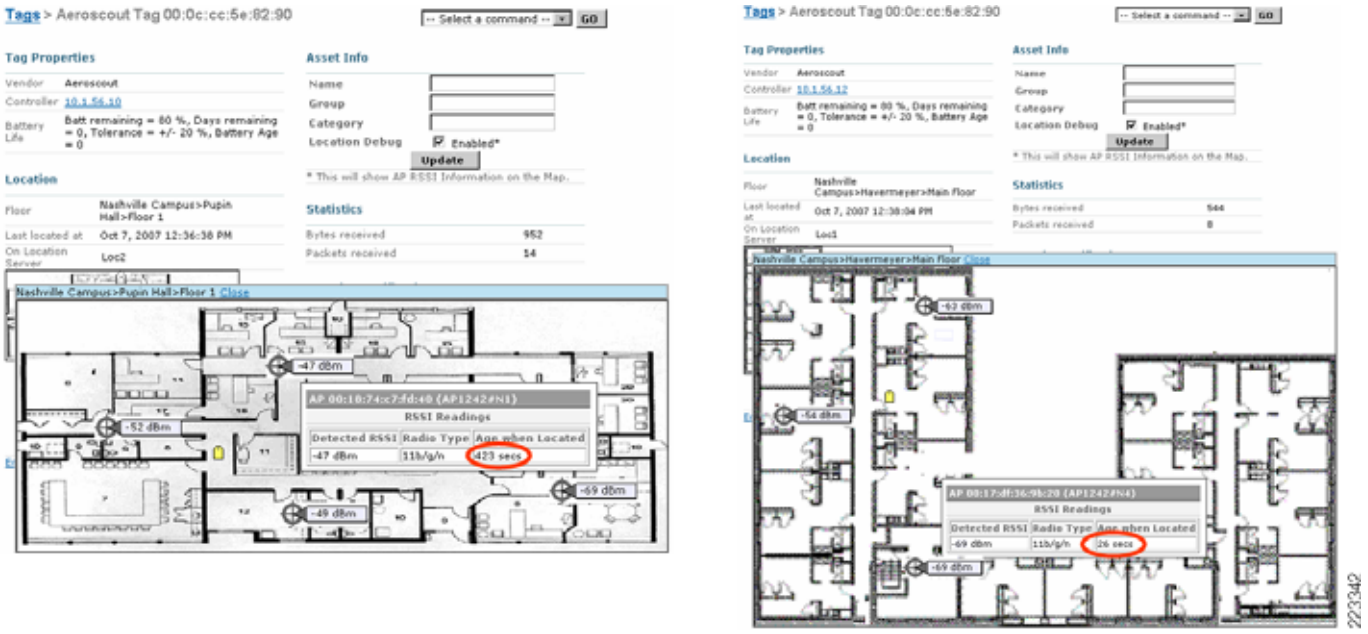
MAC Addr	Asset Name	Asset Group	Asset Category	Vendor	Loc Server	Controller	Battery Status	Map Location
00:0c:cc:5e:82:90	-	-	-	Aeroscout	Loc1	10.1.56.12	80 %	Nashville Campus>Havermeyer>Main Floor
00:0c:cc:5e:8d:cc	-	-	-	Aeroscout	Loc2	10.1.56.10	80 %	Nashville Campus>Pupin Hall>Floor 1
00:0c:cc:5e:82:90	-	-	-	Aeroscout	Loc2	10.1.56.10	80 %	Nashville Campus>Pupin Hall>Floor 1

229341

図 5-25 では、資産タグの MAC アドレス 00:0C:CC:5E:82:90 が 2 台の異なる Location Appliance で検出され、重複して表示されており、ロケーションには 2 つの異なる建物が記載されています。図 5-25 の右端からマップ ロケーションを表示すると、タグ アイコンが Havermeyer Building のメイン フロアと Pupin Hall のフロア番号 1 の両方に見られます。これらの 2 つのエントリのうち、どちらが資産タグ 00:0C:CC:5E:82:90 の正しい最新ロケーションを示しているかを見分けるには、[Last Located At] タイム スタンプからの情報と、デバイス ロケーションの特定に用いた RSSI 読み出しの経過時間を参考にします。RSSI 読み出しの経過時間に関する情報を得るには、デバイスの MAC アドレス 00:0C:CC:5E:82:90 をそれぞれクリックし、表示されるタグの詳細画面でロケーション デバッグ機能を有効にして、デバイスのロケーション特定に使用した RSSI 読み出しの経過時間を確認します（図 5-26 を参照）。

1. Location Appliance の特定のデバイス カテゴリに対するポーリング サイクルの長さも関与することがあります。正確な影響の度合いは、ポーリング サイクル内のどの時点で追跡対象デバイスがそのロケーション ドメインから移行されるかに左右されます。

図 5-26　重複タグ項目についての RSSI の経過時間の比較



Location Appliance の不明データのクリーンアップ間隔が経過すると、ラボにおける実験のタグ レポートは図 5-27 のようになりました。移行された MAC アドレス 00:0C:CC:5E:82:90 の資産タグは、Location Appliance 「Loc1」のアクティブ ロケーション データベースから削除されています。

図 5-27　デバイス削除後のタグ レポート

Tags

MAC Addr	Asset Name	Asset Group	Asset Category	Vendor	Loc Server	Controller	Battery Status	Map Location
00:0c:cc:5e:8d:cc	-	-	-	Aeroscout	Loc2	10.1.56.10	80 %	Nashville Campus>Pupin Hall>Floor 1
00:0c:cc:5e:82:90	-	-	-	Aeroscout	Loc2	10.1.56.10	80 %	Nashville Campus>Pupin Hall>Floor 1

223343

この問題を図 5-24 に示した例と関連付けて考えた場合、リモート都市内ロケーションにある建物 3、4、5 間で移動するデバイスは、この問題による影響を受けません。これは、これらの建物がすべて Location Appliance 2710-2 のロケーション ドメインの範囲内に含まれるためです。しかし、リモート都市内ロケーションのいずれかの建物と地域本部の建物 1 または 2 の間で移行するデバイスでは問題が生じます。これは、地域本部の建物が異なるロケーション ドメインの範囲内に含まれるためです。

ロケーション ドメイン間で追跡対象デバイスの移行がほぼ同じレート（つまり、ロケーション ドメインを出ていくデバイスのレートが、入ってくるデバイスのレートとほぼ同じ）で行われており、不明データのクリーンアップ間隔がシステムのデフォルト設定のままである場合、上記のような状態が約 1,440 分間（24 時間）続く可能性があります。かなりのデバイス移行が予想される場合は、そのサイトで予測される移行レベルに合わせて不明データのクリーンアップ間隔を設定することをお勧めします。これにより、Location Appliance のリソースをさらに有効活用し、追跡対象デバイス キャパシティの使い切りを防止できます。

たとえば、あるサイトにおいて次の状況で業務を開始すると仮定します。

- サイトの Location Appliance の追跡対象デバイス キャパシティは 60%（1,500 台）
- 移行レートは双方向で 1 分あたりデバイス 2 台（クライアントおよびタグ）
- その他の追跡対象デバイスの追加や削除はなし（不正デバイス追跡は無効）

この場合、Location Appliance の残存キャパシティ（追跡対象デバイス 1,000 台、「ヘッドルーム」とも呼ばれます）では、追跡対象デバイス キャパシティを使い切る懸念なく上記のレートで 500 分間稼動できます。キャパシティを使い切るような状況を回避するには、不明データのクリーンアップ間隔を 500 分*以下*（たとえば、440 ～ 470 分）に設定して、ヘッドルームを使い果たす前に追跡対象デバイス キャパシティを取り戻せるようにする必要があります。

そこでよく生じる疑問が、「不明データのクリーンアップ間隔を最初から非常に短い期間に設定してはどうか」ということです。その答えは、不明データのクリーンアップ間隔の短縮にトレードオフがまったくないわけではない、ということに関わってきます。

- Location Appliance の不明データのクリーンアップ間隔（ADCI）を任意の小さい値に設定すると、デバイス キャパシティを迅速に解放する効果がありますが、それだけでなく、ADCI 時間内に更新された RSSI 情報が 受信されなかった追跡対象デバイスのカテゴリすべて（資産タグ、クライアント、不正デバイス）について以前のロケーションや統計データを閲覧する機能にも影響を及ぼします。ADCI が短縮され、デバイスがアクティブ ロケーション データベースから削除されていると、WCS フロア マップ表示画面の左端にある [Load Location Data as Old As] ドロップダウン メニューを使用して過去のロケーション情報を閲覧する機能が、短縮された ADCI の長さに限定されます。通常は、この機能を使用して、アクティブ ロケーション データベースから最大 24 時間（ADCI のデフォルト期間に相当）にわたって情報を抽出することができます。ADCI が短縮されていると、[Load Location Data As Old As] ドロップダウン リストの最大範囲は、ドロップダウン セレクタにより大きい値が表示されていても、ADCI の新しい設定値の期間に短縮されます。
- デバイスがアクティブ ロケーション データベースから削除されると、これらのデバイスが再度ロケーション ドメインに入り、アクティブ ロケーション データベースに再び追加されるまで、その Location Appliance 上にあるこれらのデバイスの MAC アドレスに関する過去のロケーション情報にはアクセスできません。ここでは、過去のロケーション情報が、定期的に発生する独立したロケーション履歴削除プロセスにより削除されていないと仮定します。

マルチ管理ドメイン（マルチ ロケーション ドメイン）

この項では、次の両項目が当てはまる場合について説明します。

- 組織内で管理されるアクセス ポイントとコントローラの合計数が単一の管理ドメインに収まりきらない
- 組織内の追跡対象デバイス数が単一のロケーション ドメインのキャパシティを超過している

ここでも図 5-24 で図示した組織を再度取り上げますが、今回は組織階層のより上部からの観点で組織の構造を検討します。図 5-24 で説明した本部ロケーションとその下に展開するリモート都市内オフィス キャンパス ロケーションは 1 つの地域エンティティを構成し、図 5-24 での本部ロケーションは「地域」本部ロケーションの 1 つとなります。各地域本部は全国本部ロケーションの直属であり、これに類似した地域本部ロケーションが図 5-28 ではさらに 3 つあります。つまり、図 5-24 で図示した「組織」が、実際には非常に大規模な組織体の一部であることになります。この項では、この大規模な組織体について図 5-28 を用いて詳しく説明します。説明の多くは、前述の項および図 5-24 で取り扱った内容に基づきます。

図 5-28　マルチ管理ドメイン（マルチ ロケーション ドメイン）

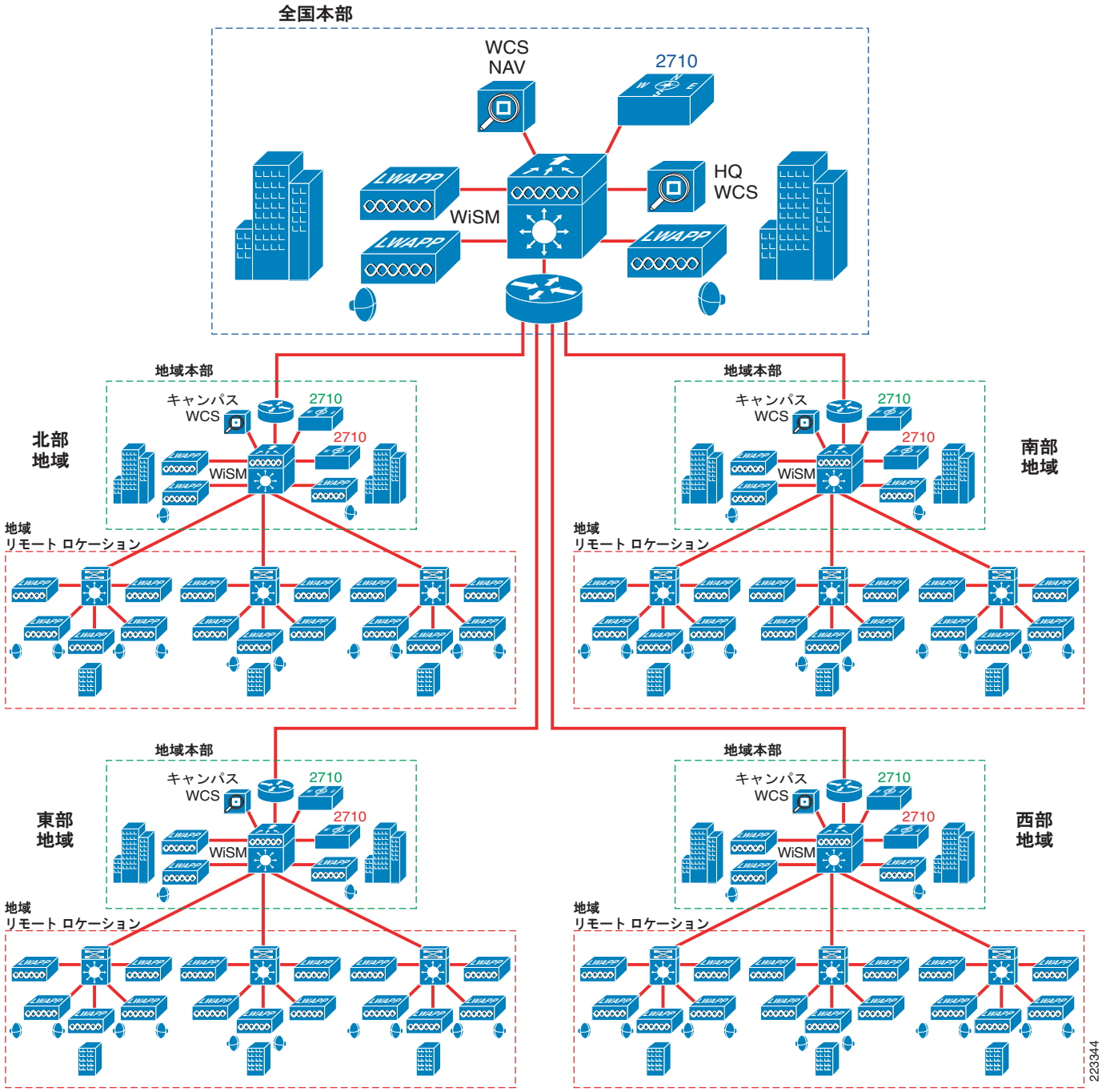


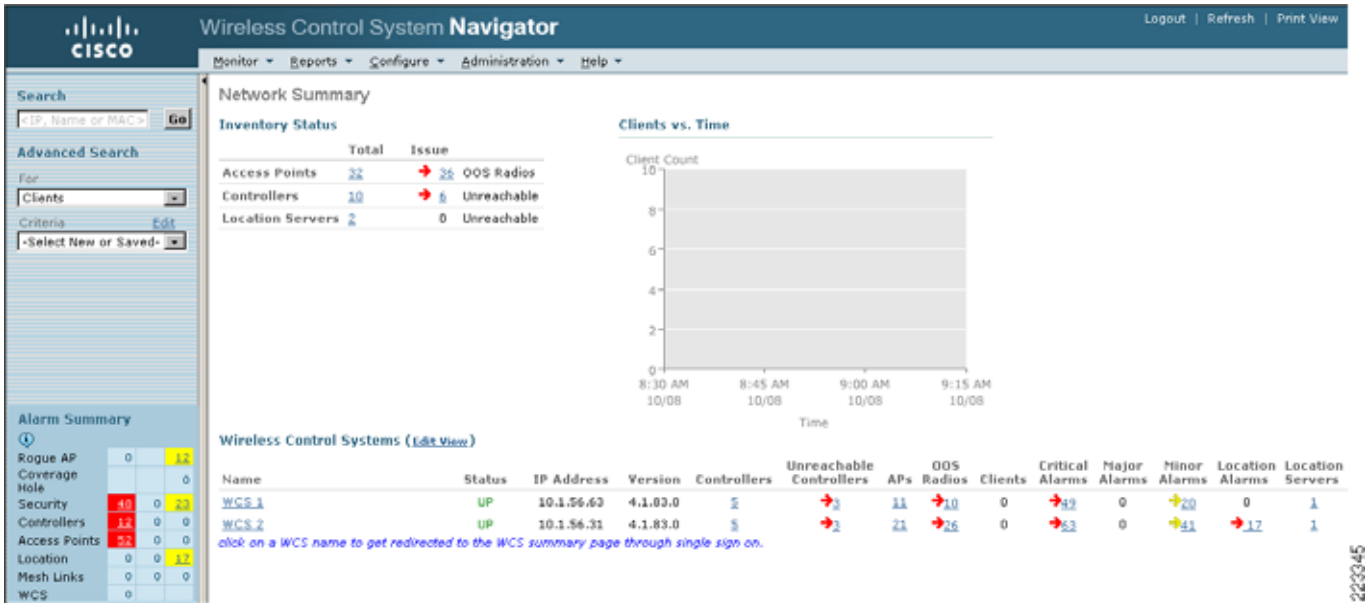
図 5-28 に示す 4 地域にはそれぞれ合計 290 箇所のアクセス ポイントが含まれ、各地域本部には WCS サーバが常駐しています。前述の項で説明したように、各地域につき 2 台の Location Appliance が配置されており、各地域本部ロケーション内に物理的に常駐して、各地域に存在する 2 つのロケーション ドメインを管理します。全国本部キャンパスは、全組織体に対する全体管理を提供します。このキャンパス自体にはアクセス ポイント 200 箇所と合計 2,100 台の追跡対象デバイスが含まれ、常駐の WiSM

搭載 Catalyst 6500 によって WLAN コントローラのサービスが提供されます。全国本部ロケーションには、単一の管理ドメインと単一のロケーション ドメインが含まれ、主に全国本部スタッフの WLAN およびロケーション追跡ニーズに対応するために使用されます。

この設計には、合計で 9 つのロケーション ドメインと 5 つの管理ドメインが含まれています。Unified Wireless Network 全体のトップダウン管理を提供するために、全国本部ロケーションには WCS Navigator が導入されており、管理とロケーション把握を全国本部内だけでなく 4 つの地域キャンパスすべてにも提供します。各 WCS サーバはノースバウンド API を介して WCS Navigator と通信し、各地域管理ドメインのイベントやアクティビティ、リソースを集中型のポータルで監視および管理できるようになっています。図 5-28 には、単一の管理ドメインと単一のロケーション ドメインが含まれ、主に全国本部スタッフの WLAN およびロケーション追跡ニーズに対応するために使用されます。

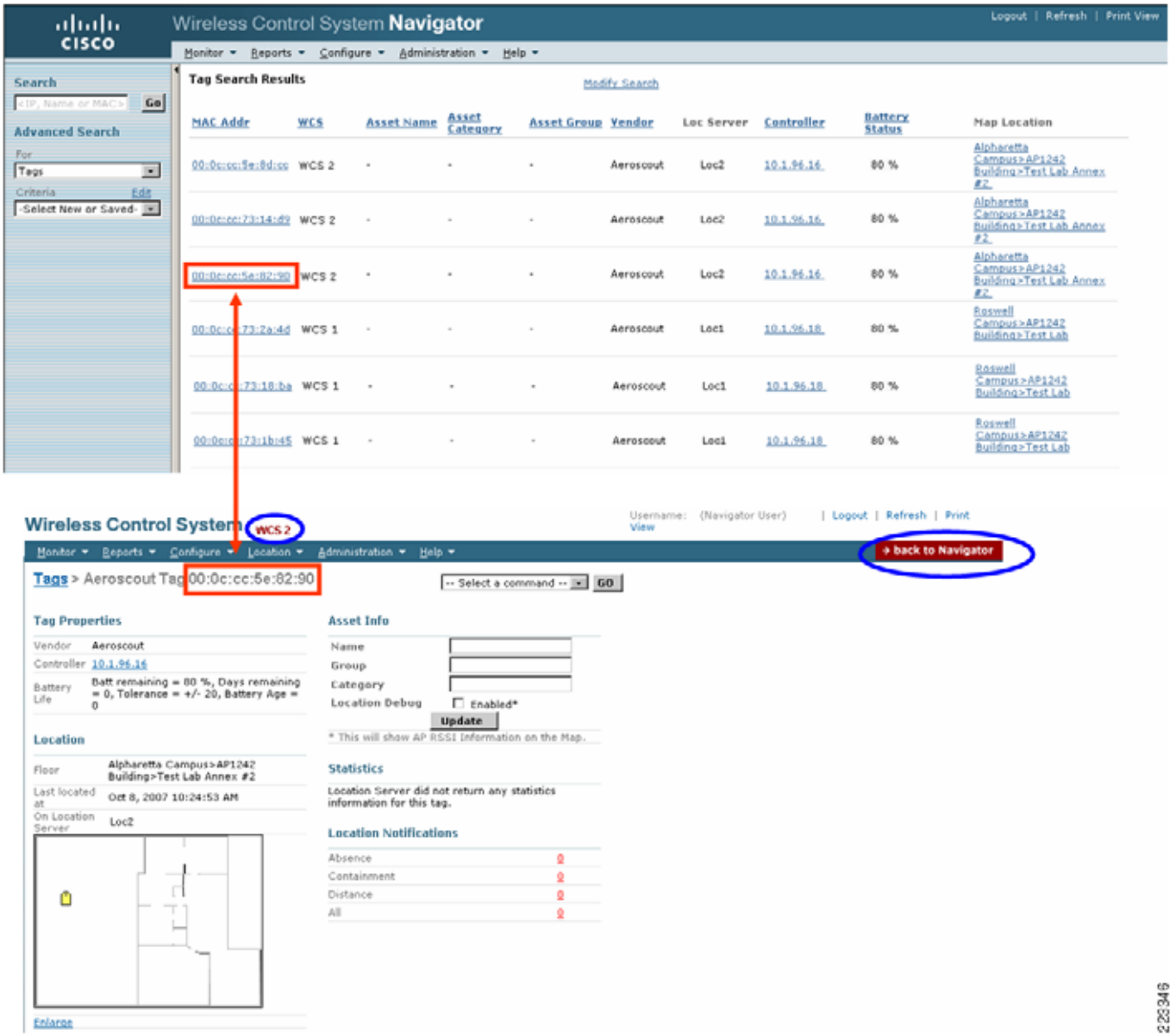
この設計には、合計で 9 つのロケーション ドメインと 5 つの管理ドメインが含まれています。Unified Wireless Network 全体のトップダウン管理を提供するために、全国本部ロケーションには WCS Navigator が導入されており、管理とロケーション把握を全国本部内だけでなく 4 つの地域キャンパスすべてにも提供します。WCS Navigator は、5 台の WCS サーバそれぞれと WCS サーバのノースバウンド API を介して通信し、各地域管理ドメインのイベントやアクティビティ、リソースを集中型のポータルで監視および管理できるようになっています。図 5-29 は、WCS Navigator のネットワーク サマリー画面です。この画面では、複数の WCS サーバとその Location Appliance のステータス監視機能を確認できます。この画面に表示されるアラーム データは、監視対象の全管理ドメインでの総数を示します。任意のリンクをクリックすると、クエリ対象の特定ドメインを担当する WCS サーバから取得した情報を用いた詳細画面が表示されます。

図 5-29　WCS Navigator サマリー画面



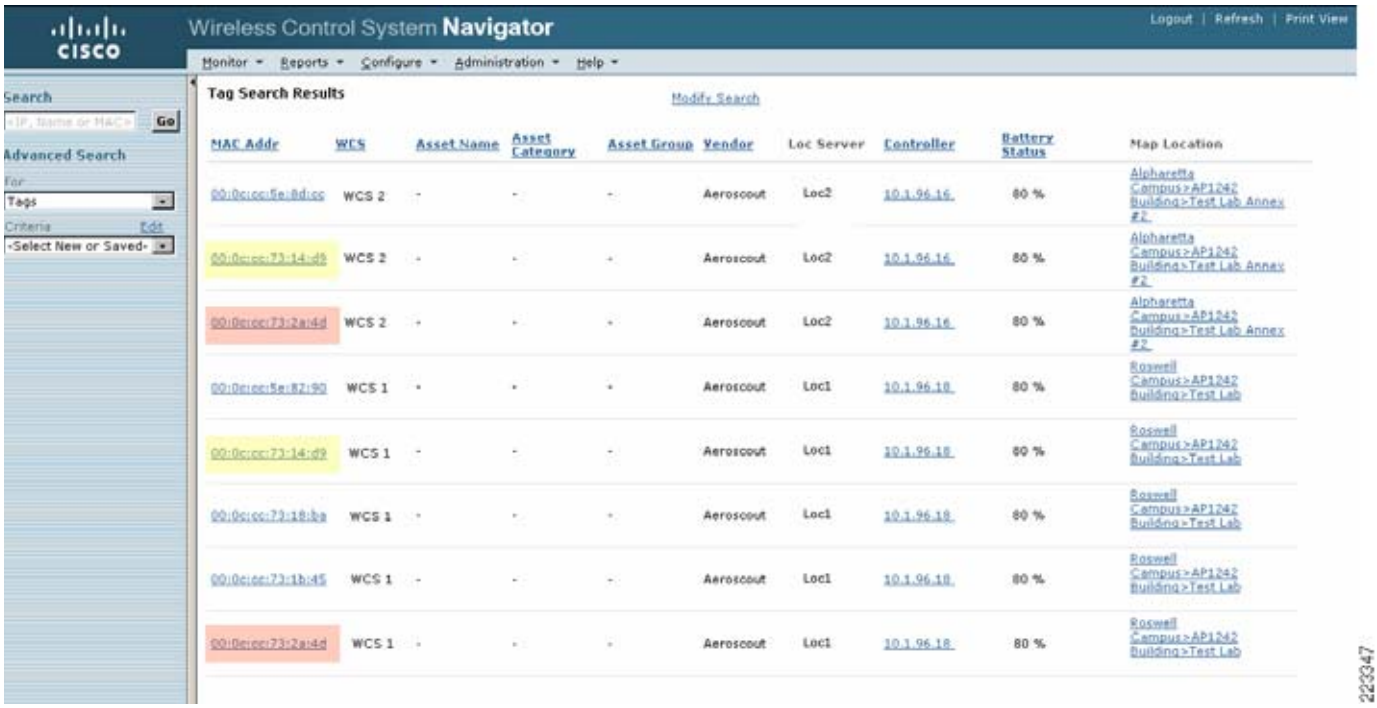
WCS Navigator では、全 WCS サーバを対象に検索を行って、個々のクライアント、資産タグ、不正デバイスのロケーションを特定することができます。追跡対象デバイスの検索は、IP アドレス、ユーザ名、MAC アドレスや、資産名、カテゴリ、グループに基づいて行うことができます。検索結果は WCS によってリスト形式で表示されます（図 5-30 の上半分を参照）。任意のタグの MAC アドレス、コントローラ、マップのリンクをクリックすると、該当する WCS サーバからの情報を用いた詳細画面が表示されます（図 5-30 の下半分を参照）。このとき、追加フィールド（青色の楕円でマークした箇所）が WCS メニューに挿入されます。これは、ユーザが WCS Navigator 経由で当該 WCS メニューにアクセスしていることを示し、これらを使用してメイン メニューに簡単に戻ることができます。

図 5-30　複数 WCS サーバに対するタグ検索の結果



前述したロケーション ドメイン間でのデバイス移行の程度と頻度に関する注意事項は、ここでも適用されます。つまり、地域内、地域間、あるいは地域と全国本部間で生じる追跡対象デバイスの移行のレベルに対して留意する必要があります。この場合、追跡対象デバイスがロケーション ドメイン間で移行し、複数 Location Appliance のアクティブ ロケーション データベースに含まれる場合、重複エントリはローカル WCS サーバだけでなく（前述）、WCS Navigator にも現れます。図 5-31 は、これを、追跡対象の 2 つの資産タグ 00:0C:CC:73:14:D9 と 00:0C:CC:73:2A:4D について図示したものです。前項で説明したように、不明データのクリーンアップ間隔を適切に調節して、重複エントリが表示される期間を短縮し、このような状況を軽減することができます。

図 5-31　デバイス移行による WCS Navigator における重複デバイス



アンテナに関する考慮事項

サードパーティ製のアンテナ

ビルディング内の WLAN ソリューションのエンジニアリング作業において設計や展開を行うときは、設備の大きさ、建材、内部の仕切りなど、一様でないすべての要素を考慮に入れて検討する必要があります。シスコシステムズは、産業界における最適な WLAN インフラストラクチャとクライアント コンポーネントだけでなく、完全な WLAN ソリューションを提供することにも取り組んでいます。このため、シスコシステムズは、どの無線 LAN 製造業者の製品でも利用できる、さまざまなアンテナ、ケーブル、アクセサリを用意しています。シスコシステムズ提供の無線ソリューションは課題の多い無線 LAN アプリケーションの要件を満たすため、それを使用する設置担当者や設計者は、方向性および全方向性のアンテナ、低損失ケーブル、取り付け型ハードウェア、その他のアクセサリの完全なスイートを利用することができます。

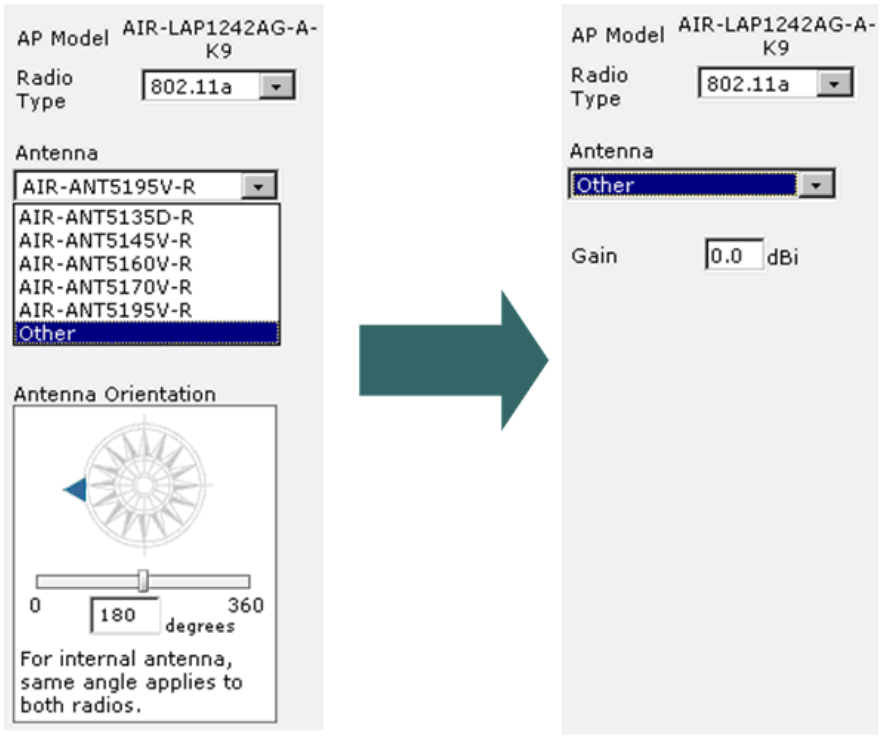
Cisco Unified Wireless Network では、シスコシステムズ提供のアンテナは WCS で利用できるようにあらかじめ設定されており、[Monitor] > [Maps] > [Position APs] のドロップダウン メニューを使ってアクセス ポイントに割り当てることができるようになっています。このリストからシスコシステムズ提供のアンテナを選択すると、アンテナのゲインと伝播パターンが WCS と Location Appliance に自動的に定義されるため、追跡対象デバイスの最適なローカリゼーションを容易に実現することができます。

ただし、特殊なケースでは、WCS のアンテナ リストに載っていないサードパーティ製のアンテナの使用について検討が必要となる場合があります。その理由として、次のようなものがあります。

- 以前から存在するアンテナの改造：以前から存在する自律的なネットワークを LWAPP ベースの UWN ソリューションにアップグレードする場合や、以前から存在する UWN システムをアップグレードする場合、サードパーティ製アンテナの大規模な基盤が既に展開されています。その物理的な条件（状態）に応じて、また最新の 802.11 テクノロジーの使用に向けて規制上の承認を得るために、設計者は展開のやり直しを検討することがあります。
- 特殊な製品要件：設計上の特殊な物理的要件や電気的要件により、WCS がサポートするアンテナ リストには含まれていない、適切なサードパーティ製アンテナの使用が求められることがあります。たとえば、アパレル販売店では、「場所を取らない」アンテナや、「Fifth Avenue」というブランド名を掲げた販売店の装飾を引き立てるために特殊な形や色をしたアンテナの使用を求められることがあります。また、電子機器の製造業者の施設では、プラント フロアの特殊な領域を対象としてそのアンテナ機能を高めることができるように、独自の（そして特殊性の高い）カバレッジ パターンや極性を備えた指向性アンテナの使用が求められます。その際、特定の位置にある感度の高い装置との干渉は最小限に抑えることが必要です。

WCS は、標準アンテナのドロップダウン リストには載っていないアンテナに指定されるアンテナ ゲインにも対応します。これは、[Other] アンテナ オプションを使用して設定できます（図 5-32 を参照）。「その他」のサード パーティ製アンテナのカスタムの方位角および仰角伝播パターンは、WCS や Location Appliance で定義することはできません（[Other] アンテナ オプションを使用すると、図 5-32 に示すようにアンテナの方向を決めるコンパスが表示されません）。このため、サード パーティ製アンテナに備えられているように定義されているアクセス ポイントは、カバレッジ ヒート マップに含まれず、クライアント、タグ、または不正デバイスのオンデマンド ロケーション トラッキングで機能しません。

図 5-32　　WCS フロア マップでの「その他」のアンテナの指定



サードパーティ製アンテナの伝播パターンを厳密に指定することはできないため、シスコシステムズ提供のアンテナがサードパーティ製アンテナに類似していると考えられるときに、シスコシステムズ提供のアンテナに事前定義されている伝播パターンを代用できるかという疑問が生じます。この一般的な質問への回答は、いくつかの要因によって異なります。最適なロケーション忠実度の観点からは、可能な限り、WCS のリスト上にあるいずれかのアンテナの使用が推奨されます。これが不可能な場合は、上記のパターン代用を行う前に、以下の点について検討してください。

- +6dBi 以下のゲインを提供するサードパーティ製アンテナの場合、サードパーティ製アンテナとシスコシステムズ提供の同等のアンテナでのゲインの差が 3 dBi を超えてはいけません。
- +6dBi 以上のゲインを提供するサードパーティ製アンテナの場合、サードパーティ製アンテナとシスコシステムズ提供の同等のアンテナでのゲインの差が 3 dBi を超えてはいけません。さらに、サードパーティ製アンテナのゲインが、シスコシステムズ提供の同等のアンテナのゲインを超えてはいけません。過剰なアンテナ ゲインによる規制準拠の問題を招く可能性があるため、後者の条件は強制的に回避する必要があります（FCC 規制ドメインと、その他の規制ドメインは異なる場合があります）。
- サードパーティ製アンテナは、シスコシステムズ提供の同等のアンテナと同じ種類であることが必要です。つまり、全方向性アンテナであれば全方向性アンテナで代用し、yagis アンテナであれば yagis アンテナで代用する必要があります。

（注） サードパーティ製アンテナを代用し、それに最も近いシスコシステムズ提供の同等のアンテナの WCS の設定を使用する場合は、TAC からのサポートは提供されないことに注意してください。

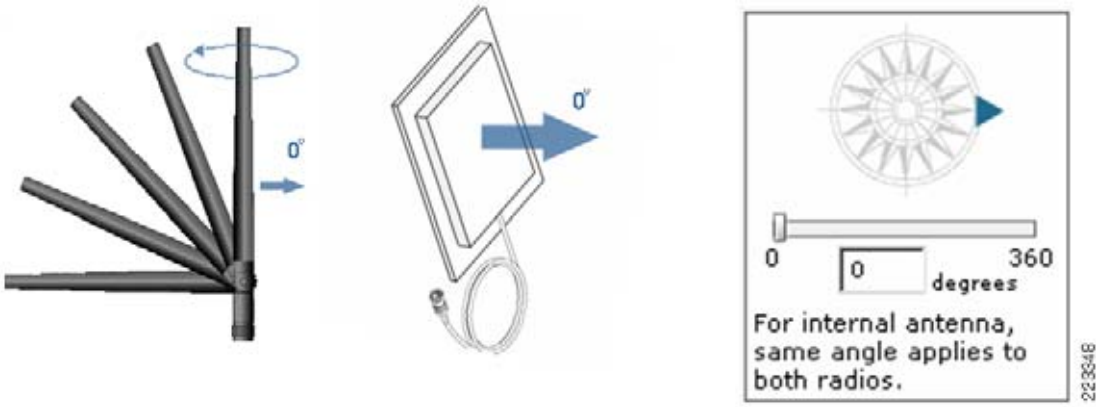
アンテナの方向とアクセス ポイントの配置

内部アンテナまたは外部アンテナを使用してアクセス ポイントを設置するとき、アクセス ポイントの配置と、WCS でアクセス ポイント アンテナに指定する方向は、実際の物理的なアクセス ポイントの配置とアンテナの方向に一致させることを強くお勧めします。これにより、ロケーション トラッキングと、ヒート マップの予測的表示の双方において、確度と精度を確保できます。

一般的な Cisco Aironet アクセス ポイントは、アンテナ ダイバーシティを使用して設置します。アンテナ ダイバーシティを使用することで、マルチパス環境における適切な範囲とスループットを確保できるようになります。一部例外はありますが、アンテナ ダイバーシティは常に有効にしておくことをお勧めします。ロケーション認識 Cisco UWN は、追跡対象デバイスのローカリゼーションを行うときに双方のアクセス ポイント アンテナからの RSSI 情報を考慮するように設計されています。良好な確度を保つため、有効になっているすべてのアクセス ポイント アンテナ ポートにアンテナが物理的に存在するようにしてください。そうしないと、アンテナが取り付けられていないのに有効に設定されているアンテナ ポートで、異常に低い RSSI 測定値が報告されることがあります。アンテナが取り付けられていないアンテナ ポートから得た異常に低い RSSI 測定値を使用することは、良好なロケーション確度に良い結果をもたらすものではなく、回避すべきです。

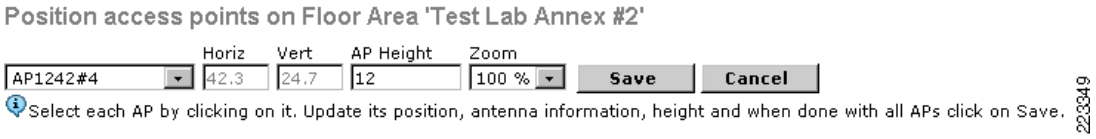
図 5-33 は、WCS でのアンテナの方位角の設定が、アンテナの実際の物理的な方向にどのように対応付けられるかを示したものです。方位角コンパスの円盤にある青色の三角形（図の右手）は、展開時に実際のアンテナが物理的に位置付けられる様子を示したものです（アンテナの各図にある青色の矢印に注目してください）。全方向性アンテナの場合、アンテナに関連付けられている独自の要因（図 5-33 の黒色の 2.2dBi ホイップ アンテナの底部に示されている、右向きに角度の付いたフレキシブル アンテナ コネクタなど）を使用して、適切に位置を決定できるようにします。指向性アンテナの場合、ケーブルの出口ロケーション（たとえば、ケーブル出口（上）またはケーブル出口（下）など）やその他の独自のしるし、構造上の特性など、アンテナに独自の物理的な特性を使用します。

図 5-33　アンテナの方向



ロケーション認識 Cisco UWN のソフトウェア リリース 4.1 では、設置されているアクセス ポイントとアンテナ特性を指定する機能が強化されています。以前のリリースではすべてのアクセス ポイント アンテナはフロア上の同じ高さに画一的に設置されていることを前提としていましたが、ソフトウェア リリース 4.1 ではさまざまな高さに設置されているアンテナを考慮できる機能を備えています。このソフトウェア リリースでは、フロアが定義されたときに設定された天井の高さが、各アクセス ポイントの初期のデフォルト値として使用されます。ただし、アクセス ポイントごとに簡単に上書きすることができます（図 5-34 を参照）。この機能により、Location Appliance を使用してアクセス ポイント アンテナの多様な高さを組み入れてラテレーションを算出することができ、より現実に近い方法で設置を見積もることができるようになります。特に、カーペットを敷いていないオフィスのような環境での作業に役立ちます。アクセス ポイント アンテナに指定するそれぞれの高さは、フロアの高さを超えることはできないことに注意してください。

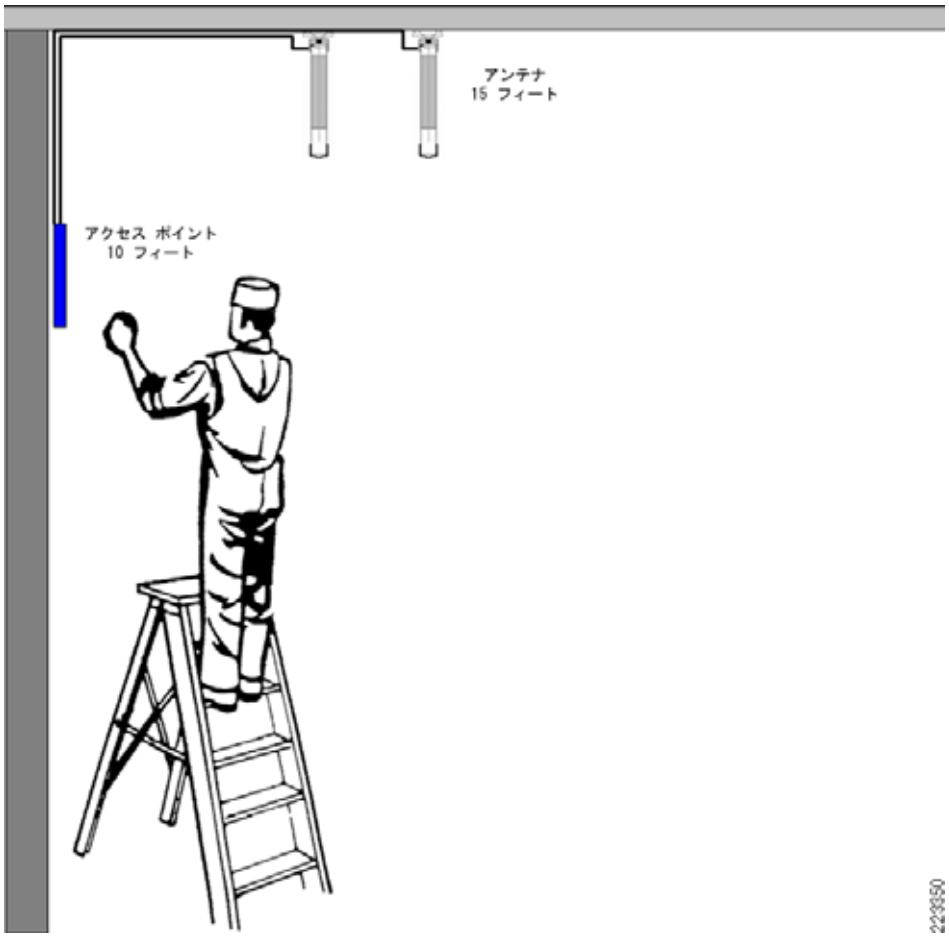
図 5-34　各アクセス ポイントの高さの定義



（注）　AP1131 アクセス ポイントのアンテナの伝播特性は、天井への取り付け時に方位角平面に対して最適化されています。AP1131 を使用する場合に最適なロケーション パフォーマンスを実現するには、アクセス ポイントは壁ではなく天井に取り付けることをお勧めします。

ただし、短い低損失ケーブル（10 フィート未満）を使用して、アクセス ポイントとアンテナを離して設置することが好ましい場合があります。このような設置が必要になるのは、障害物の回避を目的とする場合や、単に、はしごや脚立を使って現地の従業員が容易に作業できるようにアクセス ポイントやその他の電気・電子基盤を配置することが望ましい場合です。このように設置しておくと、万一再配置が必要になっても、これらのコンポーネントの取り外しや設置を容易に行うことができます。この例を図 5-35 に示します。この場合、全国の販売店では、各店舗で一般的に使用されている 10 段脚立を使って、店舗従業員が電気・電子基盤のすべてのコンポーネントを利用できるようにする必要があります。ここでは、（容易にアクセスできるように）10 フィートの高さにアクセス ポイントを取り付け、15 フィートの高さにアンテナを取り付けた例を示します。この例のような場合、図 5-34 の [AP Height] で指定した値を、（アクセス ポイントの高さではなく）アンテナの高さに反映させる必要があります。

図 5-35　例：アンテナの高さとアクセス ポイントの高さの相違



調整

Cisco WCS と Location Appliance は、デフォルトの RF モデルと共に出荷されます。このモデルにより、一般的な屋内のオフィス環境（2 種類）での設定が容易になります。2 種類の環境の 1 つはパーティションで小さく区切られたオフィス スペースや乾式壁工法で建築されたオフィスで構成される一般的な企業オフィス環境、もう 1 つは乾式壁工法で建築されたオフィスだけで構成される同様の環境です[1]。これらの RF モデルにより、屋内にある一般的な商業オフィスでのパス損失を見積もることができます。このモデルは、最短の期間でロケーション トラッキング システムを稼動させることが最も重要である場合に、とても役に立ちます。

屋内環境でも、一般的なオフィス環境よりも高い減衰が見られる場合があります。適切に設計され、屋内に設置されている場合でも、減衰が高いと最適なロケーション確度を低下させる要因となり、低下したパフォーマンスを復元するためにサイト*調整*が必要になることがあります。オンサイト調整を実行すると、システムは環境内にある既知のポイントからパス損失のサンプルをとることができ、その環境に特化した伝播特性を理解するための、カスタムの RF モデルを考案することができます。

1. 3 番目の RF 調整モデルは、Cisco Wireless Location Appliance を使用して屋外での展開を試みる設計者向けに用意されています。現時点で、このホワイト ペーパーでは屋外の設計ガイドラインは取り上げていません。

多くの場合、デフォルトのモデルからのデータではなく、調整中に収集したデータを使用することで、クライアント ロケーションで報告または観察されるエラーの度合いは顕著に低下します。多くのフロアでほとんど同一の減衰特性を共有している環境では（書棚を同じように配置した図書館のフロアなど）、この著しい類似性により、いずれかのフロアで行った調整で作成された RF モデルをすべてのフロアに適用し、良い結果を得ることができます。

調整は、実際には複数の段階プロセスで構成されます。プロセスは、新しい調整モデルを定義することから始めます（[Monitor] > [Maps] > [RF Calibration Models] > [Create New Model]）。調整プロセスの手順を追った説明については、次の 2 つのドキュメントを参照してください。

- 『*Cisco Wireless Control System Configuration Guide*』の「*Creating and Applying Calibration Models*」（http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsmaps.html#wp1089489）
- 『*Cisco Wireless Location Appliance: Deployment Guide*』（http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html）

データ ポイント収集プロセスにおいて、調整クライアントはすべてのチャネルでのプローブ要求を繰り返し送信します。使用する調整クライアントによっては、クライアントは、ネットワーク要求を通じてオンデマンドでプローブ要求を送信するようにトリガーされることがあります。これらの要求を認識できないクライアントは、無線媒体にプローブ要求を発行して再びアソシエート / 再認証が行われたため、認証が解除されてアソシエートが解除されている可能性があります。クライアントの圏内にあるアクセス ポイントは、これらのプローブ要求の RSSI を検出し、登録されているコントローラにその情報を渡します。コントローラは、調整プロセスで検出された RSSI 情報を Location Appliance と WCS に提供します。Location Appliance と WCS では、この情報を使用してパス損失の計算が行われ、最終的に新しい調整モデルに関連付けられます。

WCS における調整プロセスのデータ ポイント収集フェーズは、2 つの方法のうちいずれかの方法を使って実行できます。WLAN に関連付けられている単一 Web に対応したモバイル デバイス（ネットワーク調査と実際のデータ収集の両方を管理します）から実行できます。また、WLAN インフラストラクチャに関連付けられている 2 台の異なるデバイスからデータ ポイント収集フェーズを実行することもできます。この場合、WCS GUI との対話はキーボートとマウスの機能を備えている 1 台目のデバイスから制御し、実際のプローブ要求の生成は 2 台目のデバイス上で行います。

両方の帯域でロケーション調整データ収集を同時に実行するとデュアル バンド調整クライアントの使用に関して警告[1] が発せられるため、調整データ収集は、現時点では、帯域ごとに個別に実行することをお勧めします。デュアル バンド クライアントを使用する場合、次のいずれかの代替案を採用してください。

1. 帯域ごとに個別に Cisco Aironet 802.11a/b/g Wireless CardBus Adapter（AIR-CB21AG）を備えるラップトップ（1 台）を使用して調整データ収集を実行します。たとえば、5 GHz 帯域を無効にし、2.4 GHz 帯域のみを使用してデータ収集を完了します。次に、2.4 GHz 帯域を無効にし、5 GHz 帯域を有効にして、5 GHz 帯域のみを使用して繰り返しデータ収集を行います。
2. 調整には 2 人のオペレータを動員し、2 台のラップトップを使用して実行します。各ラップトップには Cisco AIR-CB21AG を装備し、それぞれ別の帯域を使用するインフラストラクチャに関連付けます。2 人のオペレータは個別に操作することができます。各データ ポイントのところまで一緒に足を運ぶ必要はありません。この方法では、上記の 1. の方法の半分の時間で、両方の帯域について調整データの収集を完了させることができます。

Cisco Compatible Extensions 仕様バージョン 2 以降と互換性のあるクライアントが WLAN インフラストラクチャに関連付けられており、WCS での調整クライアントとして指定されている場合、調整を行うフロア上にあるアクセス ポイントにサービスを提供するすべてのコントローラのロケーション調整テーブルに、そのクライアントの MAC アドレスが挿入されます。この挿入は、調整クライアントの MAC アドレスと、調整キャンパス、ビルディング、フロアが [WCS Maps] > [RF Calibration Models]

1. 詳細については、「CSCsh88795：CCX S36 ビーコン測定要求のデュアル バンド サポート」（P.7-1）を参照してください。

> [Add Data Points] で指定された直後に初めて行われます。収集したデータ ポイントをそれぞれ保存すると、クライアントの MAC アドレスは、コントローラのロケーション調整テーブルから削除されます。以降、データ ポイントが保存されるごとに、クライアントの MAC アドレスはコントローラのロケーション調整テーブルに一時的に再度挿入され、その後、すぐに削除されます。このプロセスは、収集されるデータ ポイントごとに繰り返されます。

Cisco Compatible Extensions 仕様バージョン 2 以降と互換性のあるクライアントの MAC アドレスがコントローラのロケーション調整テーブルに設定されると、ユニキャスト無線測定要求がこれらのクライアントに送信されます（図 5-36 を参照）。通常動作中、互換性のあるクライアントのロケーション確度の向上にブロードキャスト無線測定要求が役立つのと同様、一定の短い間隔（4 秒）で発行されるユニキャスト無線測定要求により、互換性のある調整クライアントが高い頻度でプローブ要求を送信することになります。Cisco Compatible Extensions の無線測定要求と Cisco Compatible Extensions バージョン 2 以降のクライアントを使用すると、クライアントのアソシエートの解除と設定を頻繁に強制することなく、これを実現できます。これにより、ネットワークの調査の一貫性と信頼性が高くなり、調整クライアントの動作がよりスムーズになります。これは、調整データ収集 GUI を使用して WCS と対話するワークステーションとしてクライアントを使用する場合には、特に顕著になります。

（注）　ユニキャスト無線測定要求は、サポートしているコントローラ上で Aironet Information Element（Aironet IE; Aironet 情報要素）が有効にされていない WLAN に関連付けられているクライアントには送信されません。Cisco Compatible Extensions 仕様バージョン 2 以降をサポートする調整クライアントで最適な調整結果を得るには、Aironet IE サポートを有効にする必要があります。

図 5-36　ユニキャスト無線測定要求

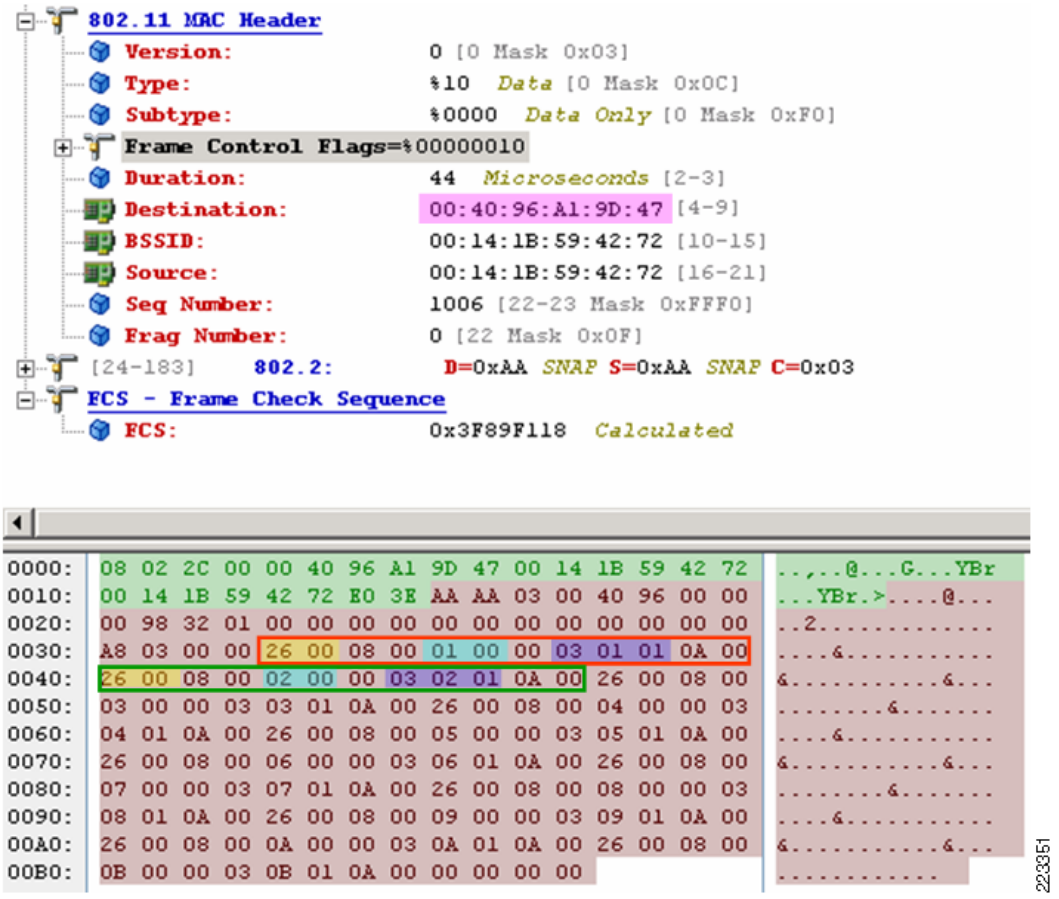


図 5-36 に示すユニキャスト無線測定要求のフィールド（色付けした四角形で強調表示されています）は、このガイドで前述したブロードキャスト無線測定要求のフィールドにとてもよく似ています。ただし、Cisco Compatible Extensions ロケーション測定は、調整データ収集中、関連付けられたすべてのクライアントに対して無線測定要求をブロードキャストするのに対し、無線測定要求は、WLAN コントローラ ロケーション調整テーブルに設定されている調整クライアントの MAC アドレスにユニキャストするだけです。たとえば、図 5-36 を見ると、無線測定要求をユニキャストしている MAC アドレスは 00:40:96:A1:9D:47 であることがわかります。

Cisco Compatible Extensions 仕様バージョン 1 に準拠している調整クライアント（または Cisco Compatible Extensions 仕様にまったく準拠していない調整クライアント）は、ユニキャスト無線測定要求に応答しません。代わりに、プローブ要求を生成するため、これらのクライアントはアソシエートの解除と設定が強制されます。Cisco Compatible Extensions 仕様バージョン 2 以降のクライアントが調整に使用されるコントローラ上で Cisco Compatible Extensions ロケーション測定パラメータ（「クライアント、資産、不正なデバイスの追跡」で説明します）が有効になっていると、調整クライアントは、Cisco Compatible Extensions ロケーション測定に使用されるブロードキャスト要求と、調整に使用されるユニキャスト無線測定要求の両方に応答します。

（注）　ロケーション調整データ収集には、Cisco Aironet 802.11a/b/g Wireless CardBus Adapter（AIR-CB21AG）の使用をお勧めします。

コントローラのロケーション調整テーブルのメンテナンスは、ほとんどの場合、WCS が行います。調整データ収集を行うために必要に応じてクライアント MAC アドレスを挿入し、不要になったらそのアドレスを削除します。このテーブルは、適切にメンテナンスを行うことが重要です。このテーブルに設定される、Cisco Compatible Extensions 仕様バージョン 2 に準拠する各クライアント（最大 5 クライアント）は、対象のコントローラに登録されたいずれかのアクセス ポイントに関連付けられるたびに、ユニキャスト無線測定要求を受け取るためです。クライアントが調整データ ポイントを収集している最中であるか、調整期間外に、関連付けられたモバイル ステーションとして単に使用されているかにかかわらず、ユニキャスト無線測定要求を受信します。

このため、コントローラのロケーション調整テーブルにクライアント MAC アドレスが残っていると、不要なロードとトラフィックが発生することになります。

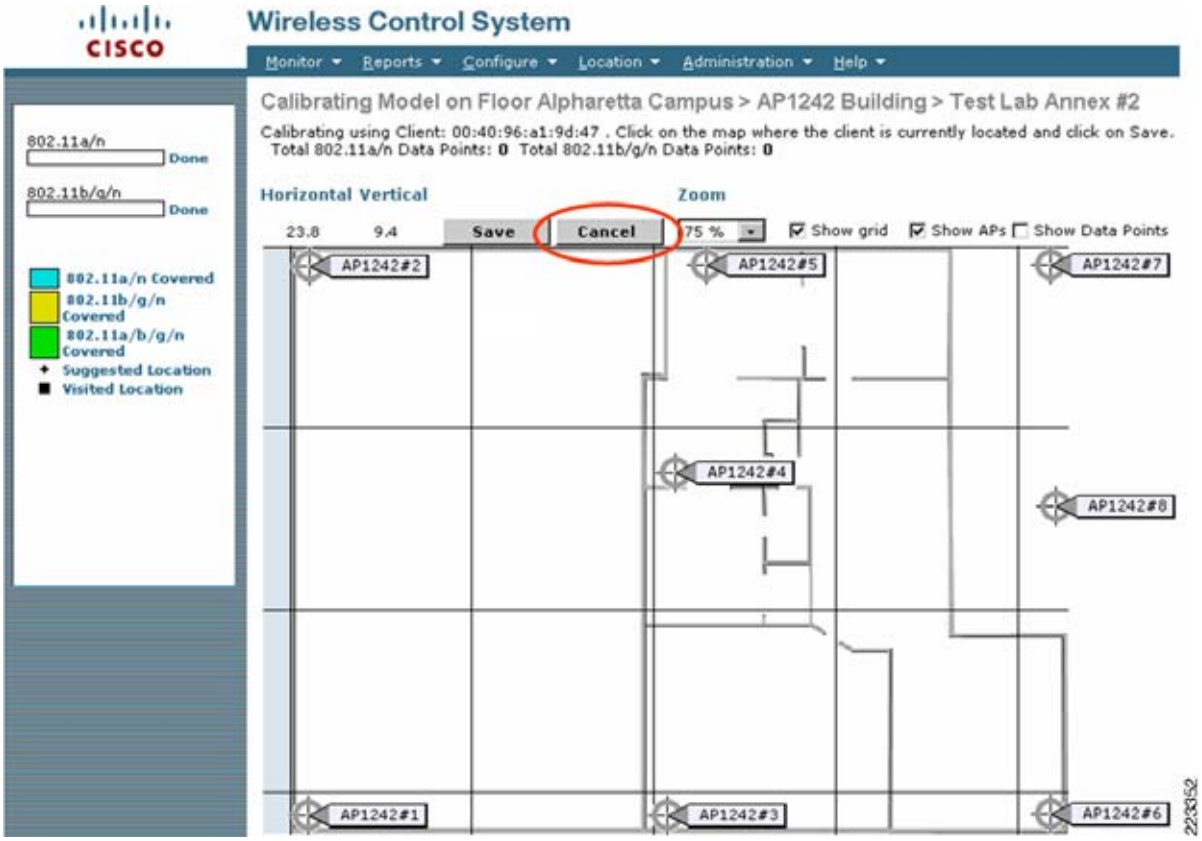
- これらのエントリを含む WLAN コントローラはそれぞれ、4 秒ごとに次の処理を実行する必要があります。
  - テーブルに設定されている各クライアントに無線測定要求を発行する。
  - テーブルに設定されている各クライアントから受け取ったプローブ要求を処理する。
  - テーブルに設定されている各クライアントから受け取った無線測定応答を処理する。
- ロケーション調整テーブルに設定されている WLAN クライアントはそれぞれ、4 秒ごとに次の処理を実行する必要があります。
  - 規制区域のためのチャネル セットにあるチャネルごとに、1 つ以上のプローブ要求を発行する。
  - 受け取った 1 つ以上の無線測定応答を処理する。
  - 受け取ったすべてのプローブ要求の結果を示す、無線測定応答レポートを生成する。

通常の調整手順において、WCS はロケーション調整テーブルに対するエントリの追加と削除を管理します。ただし、場合によっては、残っているエントリが見つかることがあります。このような現象が生じる一般的な原因として、ユーザが調整データ収集を適切に終了させなかったことが挙げられます。たとえば、次の 2 つの例のような場合があります。

- WCS は、通常、[Maps] > [RF Calibration Models] > [Add Data Points GUI] メニュー パネル上のパラメータが設定された直後に、クライアント MAC アドレスをロケーション調整テーブルに追加します。このとき、WCS メイン メニューから別の WCS 機能が選択され、データ ポイント収集が

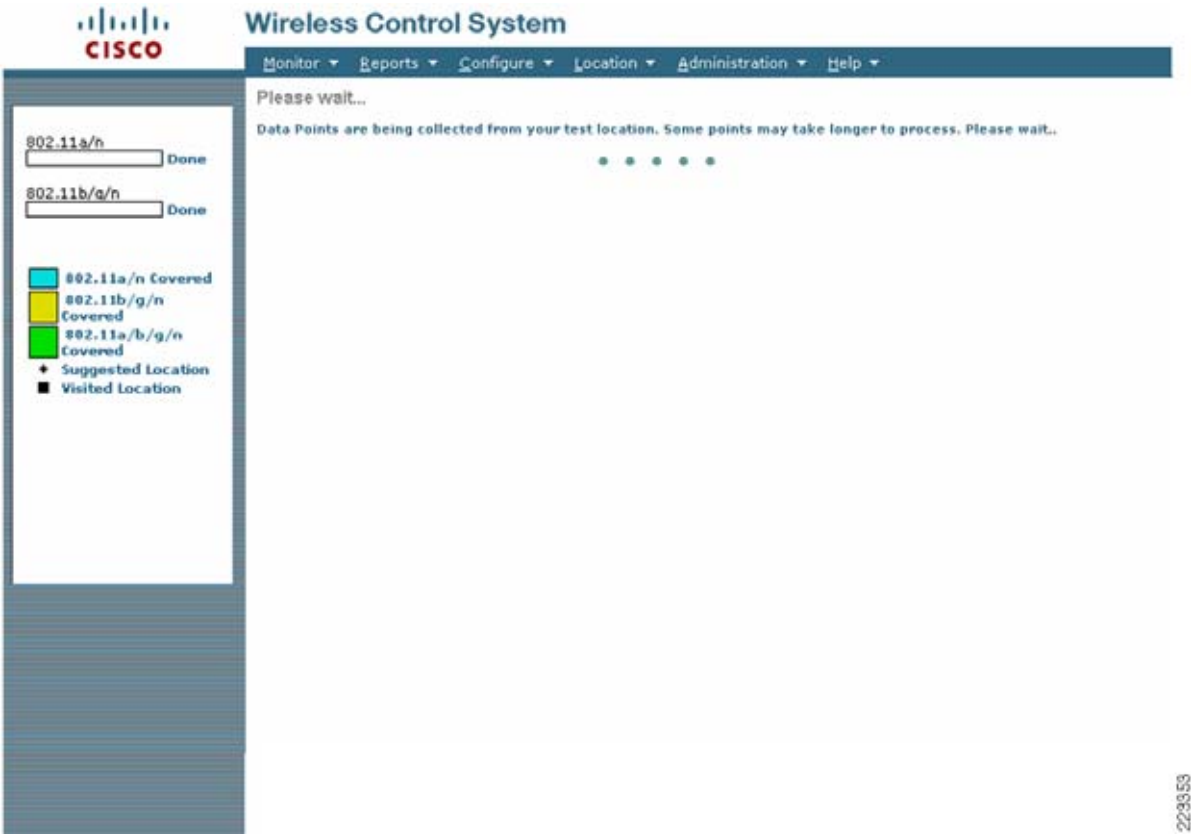
中止されると、コントローラのロケーション調整テーブルのエントリはテーブル上に残ります。この状況を回避するには、ユーザがデータ収集を中止する場合、前のメニューに戻る前に [Cancel] オプション（図 5-37 を参照）を使用することをお勧めします。

図 5-37　[Cancel] オプションを使用したロケーション調整テーブルのクリーンアップ



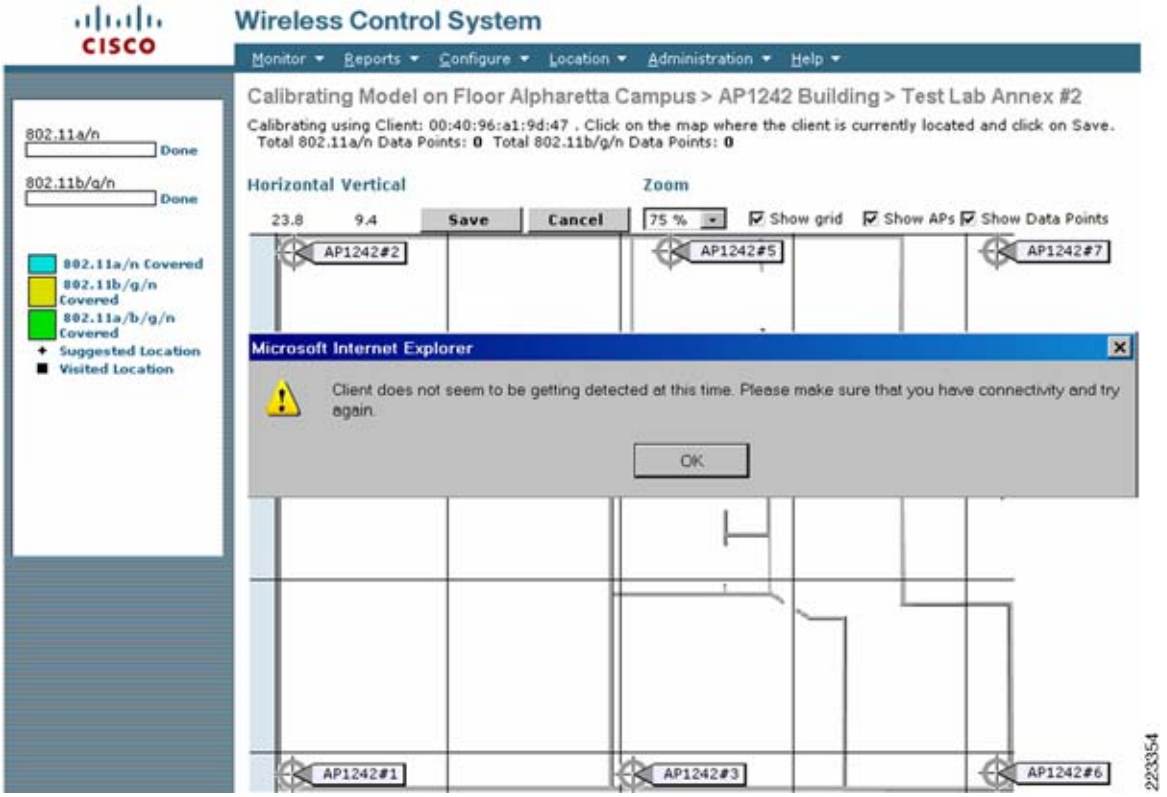
- WCS は、[Save] ボタンがクリックされ（図 5-37 を参照）、特定のデータ ポイントに対するデータ収集プロセスが開始された直後に、クライアント アドレスをロケーション調整テーブルに追加します。調整クライアントのデータが収集されている間、図 5-38 のような画面が表示されます。

図 5-38　データ ポイント収集を実行中の画面



データの収集が完了すると、データ収集画面が再表示され、新しいデータ ポイントがマップ上に描かれます。異常な状態では、調整クライアントとの接続に予期しない割り込み（カバレッジ ホールへの移動など）が発生し、データ収集プロセスが完了するまでに数分間を要することがあります（または 90 ～ 120 秒でタイムアウトが発生することがあります）。ユーザがこれを待ちきれず、WCS メイン メニューから別のメニュー オプションを選択して調整を突然終了させると、コントローラのロケーション調整テーブルのエントリはテーブル上に残ることがあります。これを回避するには、すべてのユーザがこのような操作を行うことを控え、データ収集の処理が完了するか、タイムアウトになるまで待機することをお勧めします（図 5-39 を参照）。

図 5-39　データ収集タイムアウト メッセージ



コントローラのロケーション調整テーブルの内容が問題となる場合には、CLI コマンドを使用して、クエリを直接実行することができます。

```
(Cisco Controller)>show client location-calibration summary
   MAC Address         interval
 -----------------   -------------
 00:40:96:a1:9d:47        4
```

以前に行った調整データ収集により、コントローラのロケーション調整テーブルに不要なエントリが残っている場合には、次のコントローラ CLI コマンドを使用して、エントリを手動で削除することができます。

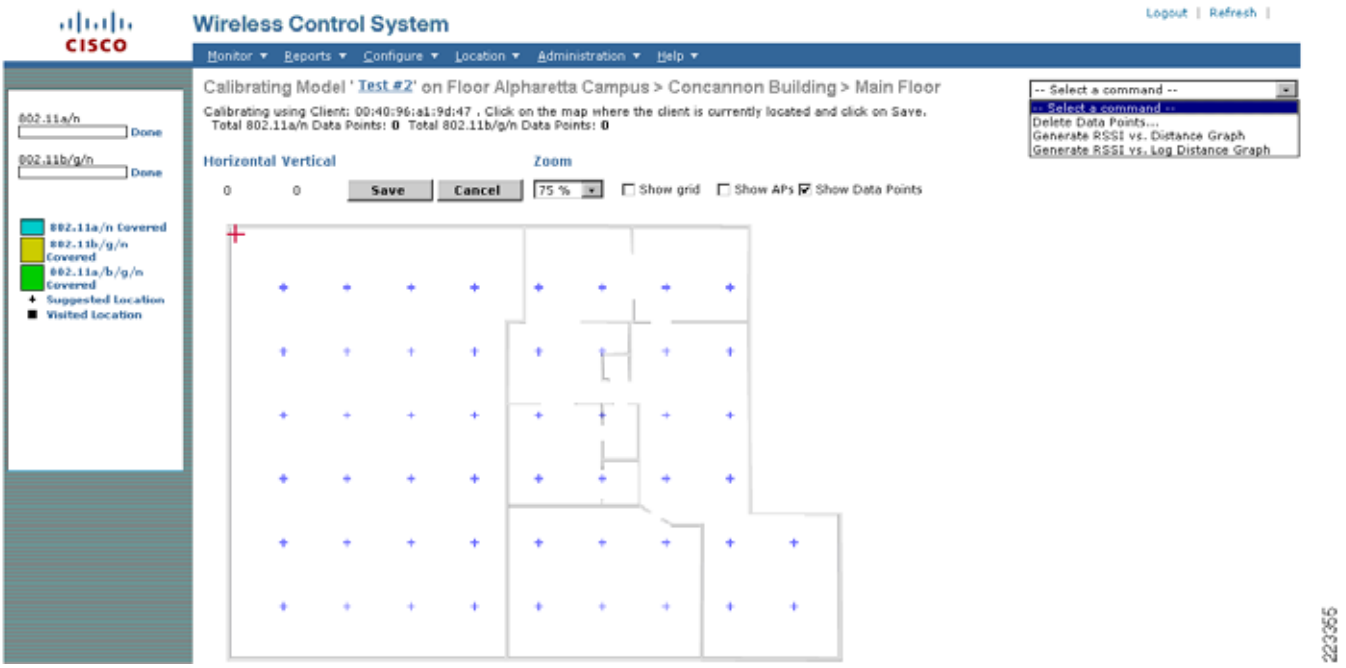
```
 (Cisco Controller)>config client location-calibration disable
00:40:96:a1:9d:47
```

（注）　コントローラのロケーション調整テーブルからエントリを削除する前に、そのエントリが調整データ収集を実行している他のユーザによって使用されていないことを確認してください。

調整データの収集は、システムが完全に設置され、基本的なカバレッジのチェックが完了し、最低 3 台のアクセス ポイントに対し、推奨される RSSI の遮断（通常は -75 dB 以上）が確認された後に行うことが必要です。すべてのアクセス ポイントは所定の場所に配置し、適切な方向に設定して、各コントローラに登録する必要があります。また、WCS と Location Appliance は完全に機能することが必要です。データ収集手順での使いやすさや見やすさを最適化するには、大型で明るくきれいに映る画面を備えたポータブル ラップトップやタブレット コンピュータ（移動型のカートに設定されたコンピュータ）の使用をお勧めします。周辺光が明るい領域では、特に推奨されます。

調整データ収集プロセスにおいて、WCS はデータを収集する必要のあるロケーションをフロア マップ上に示し（図 5-40 を参照）、処理の進行状況をグラフィカルに示します。調整データ収集プロセスの進行中、いつでも、調整データ収集画面の右上隅にあるドロップダウン メニューをクリックして、今までにデータが収集された調整ポイントをグラフィカルに表示することができます。調整データ収集プロセスは、1 つのセッションで完了させることもできますし、停止して後で再開することもできます。このプロセスは、フロアの調整データ収集が完了するまで、必要なだけ繰り返し実行できます。

図 5-40　　調整データ収集画面



調整の有効性

厳密に言えば、クライアントとアクセス ポイントの間の RF 伝播に影響を及ぼす基本的な環境要因が、調整が最初にされたときの状態から大きく逸脱していない限り、適切に実行されたサイト調整は有効であると見なされます。たとえば、対象の環境に置かれている物質的な内容に大きな変更が生じると、その環境で発生するパス損失に影響を及ぼすことがあります。再調整を実行することで、その環境に見られる減衰やフェーディングの現在のレベルについての理解を深め、パス損失モデルを再計算することができます。これは、多くの場合、低下した確度やパフォーマンスを復元させるのに役立ちます。

現実には、ロケーション認識 Cisco UWN は、現在使用されているパス損失モデルと比較して、高いパス損失が低くなる環境上の変化に対して、より高い耐性があるように見受けられます。そのため、季節に応じて物質的な内容が変化することが当り前な環境についてロケーション トラッキングを設計する場合は、パス損失が最も高くなると予想されるレベルでサイト調整を行うことが推奨されます。実際のパス損失が予想よりも低い場合にパス損失の高いモデルを使用すると、実際のパス損失が予想よりも高い場合にパス損失の低いモデルを使用する場合と比較して、より良好なロケーション パフォーマンスが実現することが観察されています。

パフォーマンスが大幅に低下した場合に再調整が推奨されるような、環境変化の例を次に示します（これらの例に限定されるわけではありません）。

- 保管されている資材の変更：ある倉庫のフロアについて最後に調整が行われたのは、紙製品を保管していたときでした。現在は、高密度液体（エンジン オイル、トランスミッション液、ギア オイルなど）の金属製容器を大量に保管するように変わっています。
- 内壁の変更：オフィス設備が新しくリフォームされましたが、最後に調整が行われたのは、防火機能を高め、防音材を装備した新しい壁を設置する前のことです。
- 保管密度の変更：大規模な図書館において、6 ～ 8 段の古い本棚を使用していたときに最初に調整を行いました。しかし、そのグレードを高め、現在では 10 ～ 12 段の新しい本棚を使用しています。
- アクセス ポイントの設置密度の変更：ある製造業者のサイトにおいて、50 台のアクセス ポイントが 40 フィート間隔で設置されていたときにロケーション トラッキング用の調整を行いました。しかし、景気が後退したため、工場の大部分が操業休止となり、アクセス ポイントの数も半減（50% 減）されました。現在では、65 フィート間隔でアクセス ポイントを設置しています。

調整を成功させるためのヒント

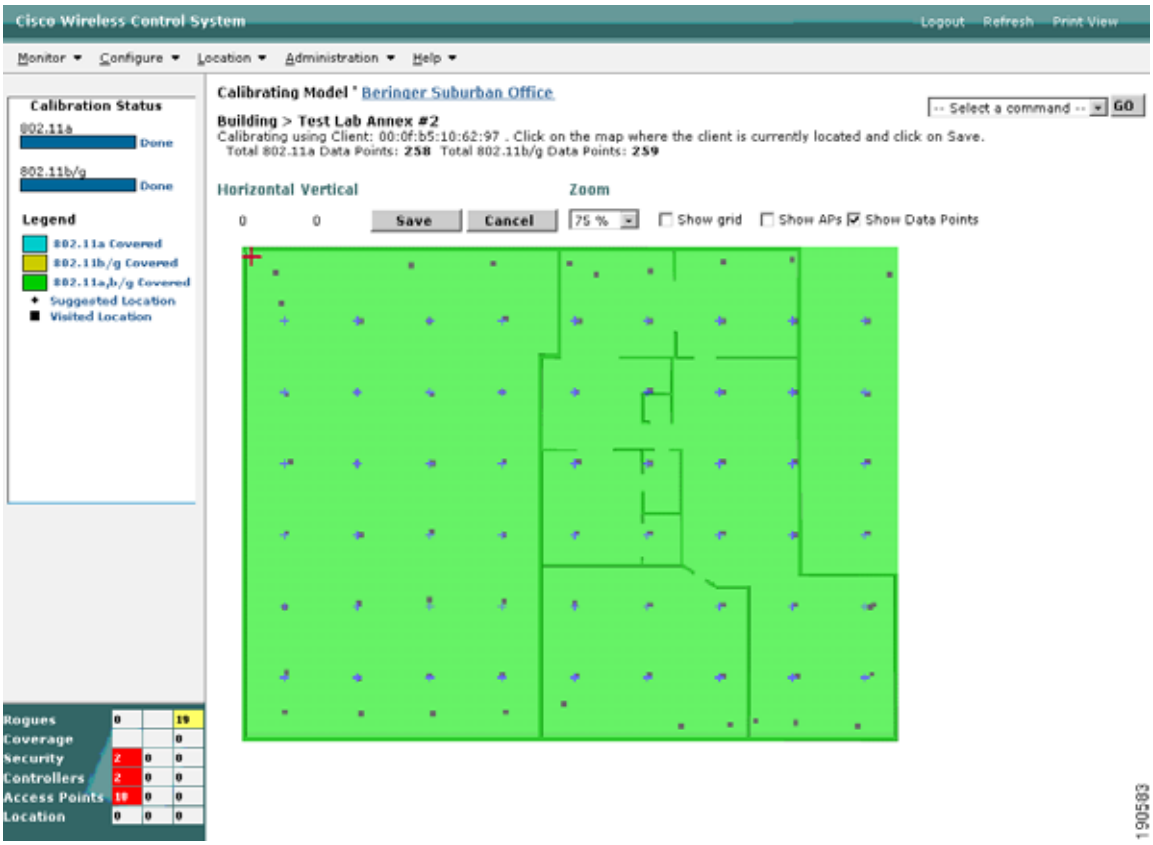
データ収集

前述したとおり、WCS 調整プロセスを行うと、モデルを調整してフロアに適用する作業をユーザが行う前に、調整データ ポイント測定のデータを十分に集めることができます。調整プロセスでは、データ ポイントを収集するときの調整クライアントの配置場所について、青色の十字線を使用して調整グリッド上に示すことができます（図 5-41 を参照）。[Save] をクリックしてデータ収集を開始する前に、必ず、赤色の十字線を正しい場所に配置していることを確認してください。

青色の十字線は推奨されたロケーションに過ぎませんが、この十字線を使って作業を順調に進め、フロア面を均等にカバーするようにします。これは、大規模環境では特に有用です。調整グリッドが更新され、実際に訪問したロケーションを表示します。ローカリゼーションの周辺領域が網羅され、802.11b/g の帯域は青色、802.11a の帯域は黄色、両方の帯域は緑色で表示されます（図 5-41 を参照）。

（注） ロケーション忠実度を高めるため、赤色の十字線を使用して調整クライアントの実際の物理的な位置を指定するときには、可能なかぎり正確に行うようにしてください（図 5-40 および図 5-41 を参照）。

図 5-41　例：両方の帯域について完了した調整データ収集



調整ユーティリティは、フロア プランの障害物（内壁、配管、ラック、その他の構成物）については認識できないことに注意してください。したがって、オペレータが物理的に近づくことのできない領域にデータ ポイントの十字線が表示されることがあります。このような場合は、そのロケーションにできる限り近い場所まで行き、そこで調整データ収集を実行します。赤色の十字線は、データ収集を実際に行った物理的なロケーションを正しく示すように配置されることに注意してください。

典型的な条件下での調整

前述のとおり、Location Appliance と Cisco WCS は調整データ収集中に集めた情報を使用して、環境に存在する伝播特性への理解を深めます。この情報は、調整データ収集時に蓄積された、すべてのデータ ポイントの集計から抜粋されます。正確な調整を容易にするため、調整データ収集が実行された環境を、実稼動環境の代表例として扱うことをお勧めします。存在する物や人の変化が生じた環境では、その変化のレベルがピークに達したとき、またはピーク近くのときに調整を行うことをお勧めします。

たとえば、施設内に平均的な数の人が存在し（人間による減衰）、棚にも物が置かれている（物による減衰）業務時間中に調整を実行します。カート、ラック、ベッドなどの大型の金属性の物が日常的に使用されている環境では、これらの物も存在している状態で調整を行います。大きなドアがある環境では、普段の業務時間中と同じように配置する必要があります。ほとんどの場合、通常の業務時間中に実行される調整では、業務時間外と比較して、日常的な実稼動環境に見られる代表的な減衰レベルが示されます。

多くの場合、人や物がサイトに移動する前でなく、建設が完了した後に調整を行う方が好都合ですが、このような「何もない部屋」で調整を行うことはお勧めしません。これらの領域に物が置かれ、人が使い始めた後、何もない環境で収集したデータに基づいて作成した RF モデルを使って追跡対象デバイス

のローカライズを試みても、最適な結果は生み出されません。倉庫の棚が半分だけ埋まっているときに調整を行うか、完全に埋まっているときに調整を行うかを選択できる場合、一般に、完全に埋まっているときに行った調整の方がより良好な確度を得ることができます。これは、倉庫の棚が半分だけ埋まる状況が時折生じる場合にも該当します。

新しく領域を構築する場合、その「初日」に運用するロケーション トラッキング システムを導入する必要がある場合、一時的な措置として、WCS と Location Appliance に用意されているいずれかの RF モデルを使用することができます。その領域に完全に物が運び込まれ、人が配置されたら、その収容がピークに達したと考えられるとき、または通常の状態と考えられるときに、その条件下でデータ収集を実行します。調整が完了したら、最初に選択した、あらかじめ用意されているモデルではなく、新しく作成された RF モデルを使用します。この方法では、最初に提供モデルを使用することでユーザや管理者はスムーズにシステムに慣れ親しむことができ、その後で適切に調整された RF モデルに切り替えて全体的なパフォーマンスを高めることができます。

領域の調整実行に最適な時間を計画するため、設計者は、そこで行われている業務のパターンやプロセスについて深い知識を有している担当者と緊密に仕事をする必要があります。これは、小売りや物流のサイトなど、保管するレベルに季節的変動が生じる場合には、特に当てはまります。サイトの担当者の情報では判断できない場合、調整を実行するのに適した時間を決めるための 1 つの方法として、事前にサイトを訪問し、設備と人員の両方について、その動向や活動パターンを観察する方法があります。このように動向や活動を事前に観察しておくと、設計者は最も代表的な結果を得るように調整を実行するのに最適な時間について計画を立てることができ、施設にいる人にひどく迷惑をかけることもありません。

推奨される調整クライアントとテクニック

調整クライアントには、Cisco Aironet 802.11a/b/g Wireless CardBus Adapter（AIR-CB21AG）を使用することをお勧めします。このクライアントは、Cisco Compatible Extensions WLAN デバイス仕様バージョン 5 と互換性があり、この項で前述したように、ブロードキャスト無線測定要求とユニキャスト無線測定要求の両方を完全にサポートしています。

調整クライアントとして Cisco Aironet 802.11a/b/g Wireless CardBus Adapter（AIR-CB21AG）を使用できない場合は、Cisco Compatible Extensions WLAN デバイス仕様バージョン 2 以降と互換性のあるサードパーティ製のクライアント デバイスを使用してください。信頼性の高い調整データ収集を行うため、ロケーション データ収集に使用するサードパーティ製の WLAN クライアントは、調整中に送信される S36 ユニキャスト無線測定要求を認識し、応答するための機能を備えている必要があります。また、プローブ要求を送信するときにサードパーティ製クライアントが使用する送信電力レベルについて、把握しておくことが必要です。

Cisco Compatible Extensions WLAN デバイス仕様と互換性のない WLAN クライアント デバイス、または仕様バージョン 1 とのみ互換性のある WLAN クライアント デバイスは、ロケーション調整データ収集での使用に適しません。

Intel® PRO/Wireless 3945ABG Network Connection アダプタまたは Intel® PRO/Wireless 2915ABG Network Connection アダプタを実装するラップトップ コンピュータを使用する場合は、そのセキュリティ設定はデフォルトで「パーソナル」（「エンタープライズ」での使用を意図していない）になっていることに注意してください。「パーソナル」設定は、Cisco Compatible Extensions 仕様とは互換性がありません。無線セキュリティにデフォルトの「パーソナル」レベルを使用する場合は、Intel 3945ABG クライアント アダプタまたは 2915ABG クライアント アダプタを実装するクライアントは、S36 ユニキャスト無線測定要求またはブロードキャスト無線測定要求をサポートせず、Cisco Compatible Extensions WLAN デバイス仕様と互換性がありません。

Cisco Compatible Extensions 仕様との互換性を有効にするには、Intel ProSet クライアント サプリカントを使用してクライアントをエンタープライズ セキュリティに再設定し、Cisco Compatible Extensions を有効にする必要があります。この設定を行う方法を図 5-42 と図 5-43 に示します。

図 5-42　Intel ProSet の [Security Settings] パネル

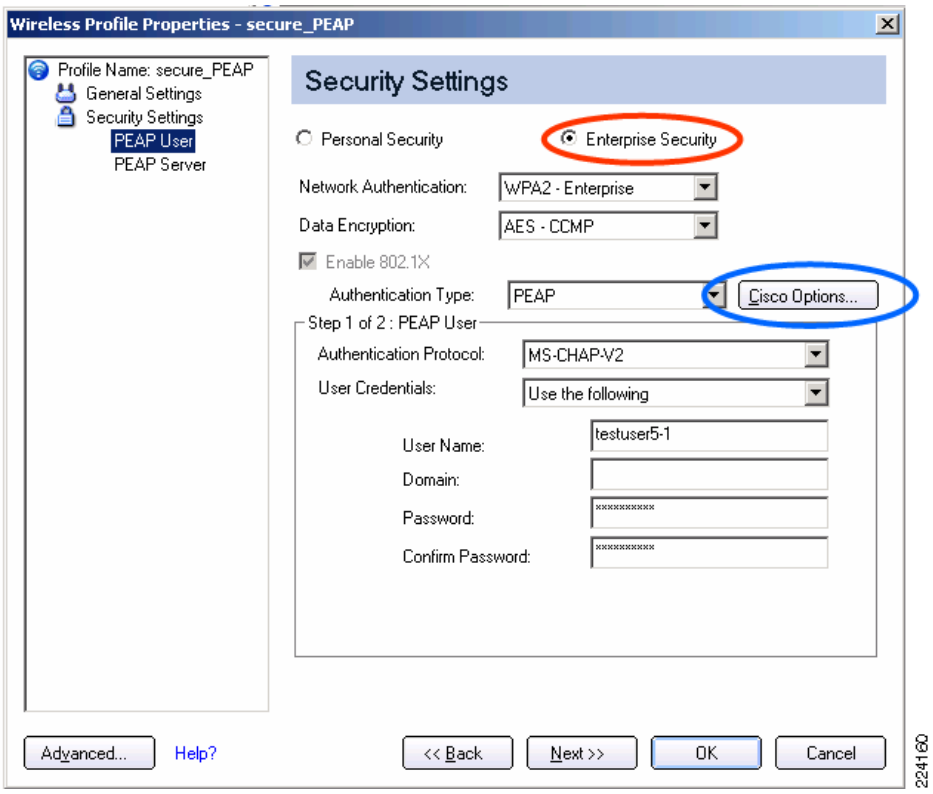


図 5-42 で、Intel ProSet 設定の [Security Settings] パネルで、デフォルトの [Personal Security] オプションではなく、[Enterprise Security] オプション（赤色の円で強調表示された部分）を選択します。適切な認証と、認証の種類を設定し、[Cisco Options] を選択します（青色の円で強調表示された部分）。すると、図 5-43 に示すパネルが表示されます。

図 5-43　Intel ProSet Cisco Compatible Extensions

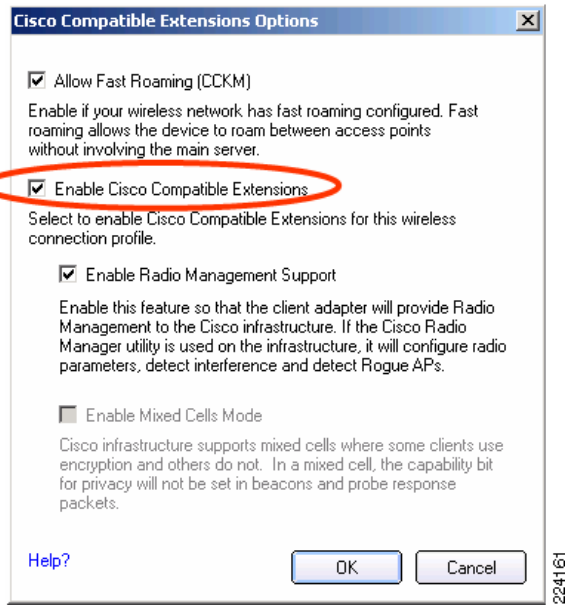


図 5-43 で、Cisco Compatible Extensions は有効に設定する必要があります（赤色の円で強調表示された部分）。CKIP、LEAP、または EAP-FAST のプロファイルを構成すると、Cisco Compatible Extensions は自動的に有効に設定されることに注意してください。

（注）　Intel® PRO/Wireless 3945ABG Network Connection アダプタまたは Intel® PRO/Wireless 2915ABG Network Connection アダプタの設定に関する詳細は、Intel Corporation のドキュメント（ftp://download.intel.com/support/wireless/wlan/sb/3945abgug.pdf、ftp://download.intel.com/support/wireless/wlan/pro2915abg/sb/2915ABG_UG.pdf）を参照してください。

調整は、調整クライアントと、完全に充電したラップトップ コンピュータを使用して実行する必要があります。調整データ収集を行うときには、次の推奨事項を検討してください。

1. 調整を実行するフロア上で、調整クライアントがアクセス ポイントによって検出されることを確認します。
2. 調整データ収集を行う前に、Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を一時的に無効にします。DTPC は、調整データ収集に関与することが期待されるアクセス ポイントの各コントローラに対し、コントローラ GUI、コントローラ CLI、WCS のいずれかを使用して、帯域ごとに無効にする必要があります。調整データ収集の実行後、DTPC を再び有効にし、通常の運用状態に戻す必要があります。
3. 調整クライアントが関連付けられている WLAN は、Aironet Information Element（Aironet IE; Aironet 情報要素）をサポートするように設定してください。このように設定することで、調整データ収集時にユニキャスト無線測定要求を使用できるようになり、より効率的に処理を進めることができます。

アクセス ポイントのカバレッジ ヒート マップを表示し、デバイスを追跡するときに、ほとんどのケースにおいて最適なパフォーマンスを実現するには、2.4 GHz 帯域の場合は 63 mW（+18 dBm）、5 GHz 帯域の場合は 32 mW（+15 dBm）にできるだけ近づけるように調整クライアントの送信電力レベルをあらかじめ設定しておく必要があります。調整データ収集中、これらの送信電力レベルが変動しないようにするため、DTPC を無効にしておく（上記の 2.）ことが必要です。

両方の帯域でデータ収集を同時に実行しようとするとデュアル バンド調整クライアントの使用に関して警告[1] が発せられるため、調整データ収集は、現時点では、帯域ごとに個別に実行することをお勧めします。デュアル バンド クライアントを使用する場合、次のいずれかの代替案を採用してください。

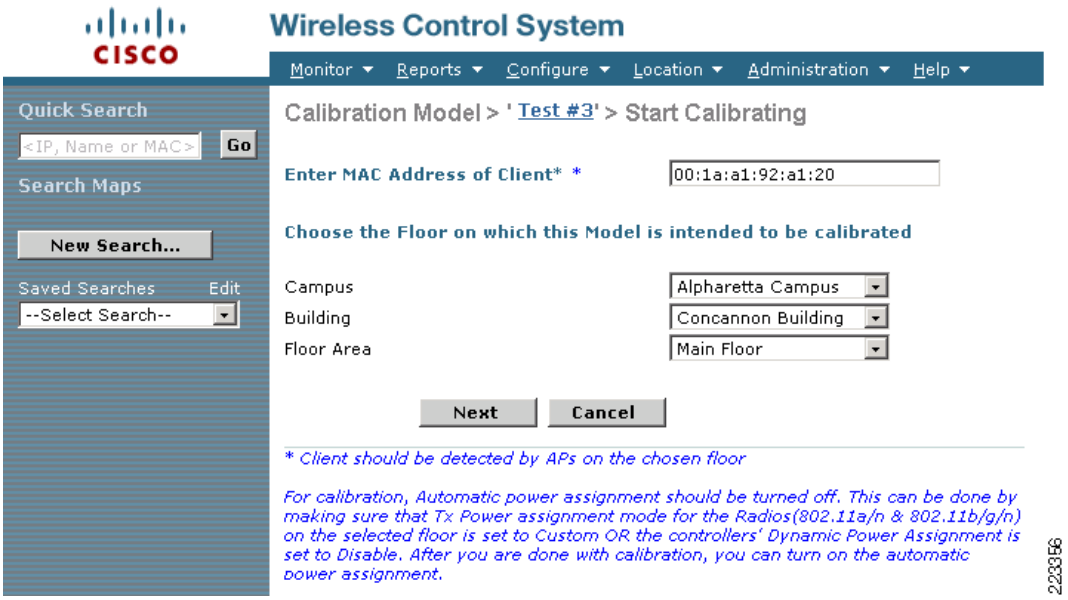
1. WLAN デバイス規格（バージョン 2 以降）に対応した Cisco Compatible Extensions 仕様と互換性があり、S36 ユニキャスト無線測定要求を認識して応答することができるデュアル バンド クライアント アダプタを装備した 1 台のラップトップを使用して、帯域ごとに個別に調整データの収集を行います。このようなクライアントの例として、Cisco AIR-CB21AG が挙げられます。たとえば、5 GHz 帯域を無効にし、2.4 GHz 帯域のみを使用してデータ収集を完了します。次に、2.4 GHz 帯域を無効にし、5 GHz 帯域を有効にして、5 GHz 帯域のみを使用して繰り返しデータ収集を行います。
2. 調整データの収集には 2 人のオペレータを動員し、2 台のラップトップを使用して実行します。各ラップトップには、Cisco Compatible Extensions WLAN デバイス仕様バージョン 2 以降と互換性があり、S36 ユニキャスト無線測定要求を認識して応答することのできるデュアル バンド クライアント アダプタが備えられている必要があります。このようなクライアントの例として、Cisco AIR-CB21AG が挙げられます。各ラップトップは、異なる帯域を使用するインフラストラクチャに関連付けられていることが必要です。調整データ収集を行う 2 人のオペレータは個別に操作することができます。各データ ポイントのところまで一緒に足を運ぶ必要はありませんし、行き先のデータ ポイントが同じでなくてもかまいません。この方法では、上記の 1. の方法と比較して半分の時間で、両方の帯域について調整データの収集を完了させることができます。

組み込み型のラップトップ クライアント アダプタの中には、これらの電力レベルではプローブ要求を送信しないものがあります。このようなアダプタでは、より低い送信電力レベル（2.4 GHz 帯域の場合に +15 dBm など）に制限されます。一般に、これらのクライアントは、上記に概説したガイドラインに従って調整データ収集を実行するときに、許容範囲内の確度でローカライズすることができます。ただし、組み込み型のラップトップ クライアントがプローブ要求を送信すると予想される電力レベルで調整データ収集を実行すると、ロケーション確度がわずかに高まることがあります。この方法を選択するときは、アクセス ポイントのヒート マップ確度が低下する可能性と比較検討する必要があります（ヒート マップは 2.4 GHz 帯域の場合は 63 mW（+18 dBm）、5 GHz 帯域の場合は 32 mW（+15 dBm）で調整を実行したときに確度が最も高くなります）。

調整データ収集が完了したら、一時的に設定を変更したすべてのパラメータを通常の設定に戻す必要があります。場合によっては、調整データ収集プロセスの制御に使用したデバイスが、プローブ要求の送信に使用したデバイスと同じデバイスではないことがあります。たとえば、Cisco Compatible Extensions 仕様バージョン 1 と互換性のある無線アダプタが組み込まれたラップトップが、そのユーザが希望する人間工学的機能や特殊な機能を備えるようにカスタマイズされている場合があります。このようなデバイスは Cisco Compatible Extensions 仕様バージョン 2 以降との互換性はないため、調整データ収集で最適な結果を得るためには、その使用は推奨されません。ただし、このデバイスを使用して UWN にログインし、プローブ要求の送信は別のデバイス（たとえば、Cisco AIR-CB21AG を備えたデバイスなど）で行うようにして、リモートでデータ収集プロセスを制御することはできます。図 5-44 に示すように、このように調整することで、調査クライアント（「リモート調整クライアント」とも呼ばれます）のロケーションと各データ収集のタイミングを、このラップトップから完全に制御できます。調査クライアント（図 5-44 では、MAC アドレスは 00:1a:a1:92:a1:20 になっています）はリモートから指示されて、ネットワーク インフラストラクチャに対して適切にプローブ要求を発行します。

1. 詳細については、「CSCsh88795：CCX S36 ビーコン測定要求のデュアル バンド サポート」（P.7-1）を参照してください。

図 5-44　調整データ収集のリモート制御



一様でない環境での調整

ネットワーク設計者は、建造物の環境が一様でないために問題に直面することがあります。たとえば、大規模なコール センターでパーティションで小さく区切ったオフィス スペースで構成されているフロア（パス損失指数は 3.3）、金属製の棚や電子装置が密集して配置されている領域（パス損失指数は 4.3）、多数の個室があり、乾式壁工法で建築されている領域（パス損失指数は 3.5）などが例として挙げられます。

このようなケースでは、次のいずれかの対策を講じます。

1. 減衰（パス損失）の期待値が最も高い領域で調整を行う。このような状況に対応するための最も直接的な方法は、全体的な減衰が最も顕著である（パス損失指数が最も高い）領域で調整を実行し、結果として得た RF モデルをそのフロアの全領域に適用します。数理的なシミュレーションや研究では、実際のパス損失は低い領域に高いレベルのパス損失を適用した RF モデルの方が、その逆の手法を採用した場合よりもロケーション確度が改善する結果が示されています。このことから、金属製の棚や電子装置が密集して配置されている領域（パス損失指数は 4.3）で調整を実行し、この調整から得られた結果をフロア全体で使用することをお勧めします。
2. フロアの全領域で調整を行う。この方法では、フロアの全領域を考慮に入れて、「バランスのとれた」RF 調整モデルを生成することを試みます。ロケーション アプリケーションが求める確度に応じてこの方法を使用すると、許容レベルのパフォーマンスを得ることができますが、研究室でのテストでは、一般に、上記 1. のオプションの方が良好な結果を得ることが示されています。フロアがいくつかの領域に分かれており、各領域で収集した調整データ ポイントの数が大きく異なるほど、フロア領域間のサイズに大きな相違がある場合は、この方法を使用して得た最終的なパス損失モデルは、より大きな領域に関連のあるパス損失に偏る可能性があります。
3. フロアの各領域を個別のフロアとして扱う。個別の領域ごとに扱うことで、確度を改善できる場合があります。ただし、管理面での負荷は高くなり、エッジ確度の低下が生じます。ソフトウェア リリース 4.1 では、WCS と Location Appliance を使用してサブフロア領域に対して異なる RF モデルをプロビジョニングすることはできないため、WCS では 1 つのサブフロア領域を独立したフロアとして定義する必要があります。そして、サブフロア領域ごとに調整を実行し、WCS で擬似

的なフロア定義に適用して、Location Appliance と同期させます。この方法では、サブフロア領域ごとの特性に適合したパス損失モデルを個別にプロビジョニングすることができ、確度と精度の向上が期待されます。ただし、WCS 管理者の作業に追加の負担がかかる場合があります。通常、フロアやサブフロアについて、WCS ユーザが容易に認識でき、論理的にグループとして見なされることができるように、系統立てた命名規則が必要になります。それぞれのサブフロア領域は、このガイドに記載されているロケーション認識設計の推奨事項が適用される、独立したロケーション領域として考えることが必要です。また、ソフトウェア リリース 4.1 では、Location Appliance 測位エンジンは別のフロアに存在するアクセス ポイントからの信号強度の測定値を認識しないため、サブフロアの境界に近いデバイスほど確度が低下する可能性があることに注意してください。

主流となる上記オプションのほか、WCS 内でこれらの 3 つの領域を独立した「フロア」として扱い、各領域の特性に適合した RF モデルを構築することもできます。ただし、この方法には重大な制限があることに注意してください。フロアやサブフロアの命名規則の構築など、管理面での負荷が高くなるのに加えて、技術的な限界が存在します。それは、Location Appliance は、現在のところ、追跡対象デバイス自体ではない、別のフロアに配置されていると見なされるアクセス ポイントから受け取った RSSI を考慮に入れない、ということです。このため、物理的なフロアを複数の領域に分割し、それらを個別のフロアとして WCS に定義すると、新しく定義された「フロア」の境界領域にあるデバイスの確度は低下することがあります。上記の制限事項と境界領域の確度に及ぼす潜在的な影響を設計者やシステム ユーザが受け入れることができる場合を除き、この方法は使用しないことをお勧めします。

フロアの環境が一様でなく、その程度が大きく異なる状況での理想的なソリューションはありませんが、一般には、上記オプション 1. の方法が、実装のしやすさとパフォーマンスの面で折り合いをつけることができます。

ロケーション品質の検査

「Location Inspection」ツールを使用すると、調整データ ポイントの実際のロケーションと予測されたロケーションを比較することで、パス損失モデルの確度を検証できます。単に予測するだけの Location Planning ツールや Location Readiness ツールとは異なり、ロケーションの検査を実行すると、調整データ ポイントの予測されたロケーションを、調整オペレータが最初に指定した実際の物理的なロケーションに対して直接比較することになります。ただし、Location Inspection ツールが事実に基づいた値を示すようにするには、調整データを収集するときに赤色の十字線を正確に配置することがとても重要です。

各データ ポイントを比較した結果を使用して、フロア上にある各種ポイントのパス損失モデルについて全体的な確度がグラフィカルに表示されます。これはシステム設計者や設置担当者に対し、調整時に使用される調整クライアントや環境条件を前提として、システムの予測されるパフォーマンスがどのように実際のパフォーマンスと比較されるかについて「現実の世界」のフィードバックを提供することになります。

Location Inspection ツールにアクセスするには、調整モデルのデータ収集が実行されたフロアの名前の横に表示される [Inspect Location Quality] ハイパーリンクから [Monitor] > [Maps] > [RF Calibration Model] > [（モデル名）WCS] を選択します（図 5-45 を参照）。

図 5-45　Location Inspection へのアクセス

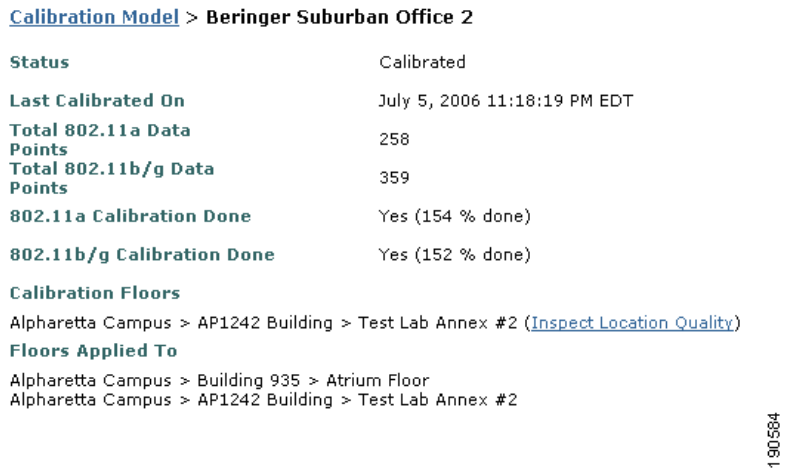
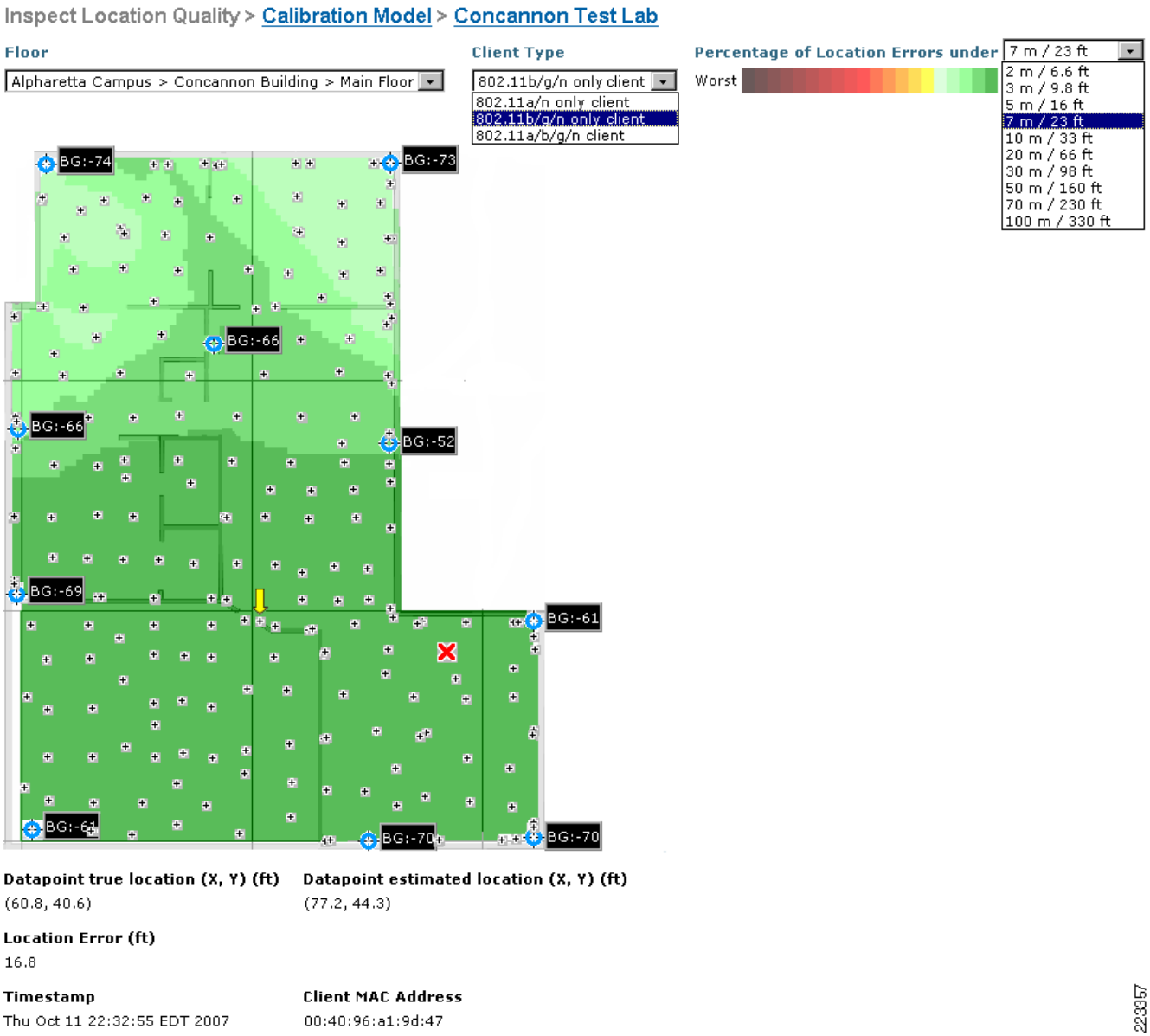


図 5-46 は、Location Inspection ツールの使用例を示したものです。ここでは、テスト ラボ施設での調整が完了した後、ロケーションの検査を実行しました。結果は、Location Appliance によって調整中に提示された確度と精度を示しています。この例では、調整クライアントとして 802.11bg のみを使用しました。Location Appliance は、テスト ラボ領域の大部分の領域で 90% の精度で 7 メートル（23 フィート）の確度レベルおよび精度レベル（調整時の条件下でのレベル）を示していることが観察されます。1 つの調整データ ポイントを見ると（図では、マウスを合わせたポイントは黄色い矢印で示しています）、予測されたロケーションは ✖ で示され、この具体的な事例でのロケーション エラーの程度について詳細が示されています（16.8 フィート）。

図 5-46　802.11bg を使用したロケーション検査



いずれかの調整データ ポイントにマウスを合わせると（調整データ ポイントのロケーションは小さな十字線 ⊞ を使用して表示されます。このロケーションは、調整オペレータから報告された実際の座標に基づいたものです）、次の情報が表示されます。

- 調整クライアントの予測されたロケーション（ロケーションの検査の表示は ✖ で描かれます）
- 使用するアクセス ポイントおよび帯域によって検出される RSSI（図 5-46 を参照。BG=-74 や A=-59 などの記号で表示されます）
- 調整データ ポイントの実際のロケーションおよび予測されたロケーション（x 座標と y 座標が数値で表示されます）
- 予測されたロケーション エラー
- 調整データが収集されたタイム スタンプ、および調整の実行に使用された調整クライアントの MAC アドレス

パフォーマンス条件と同様、帯域（2.4 GHz、5GHz、または両方）も指定できることに注意してください。このように柔軟に制御できるようになっているため、システム設計者はロケーション検査の結果に基づいて「仮定」の設計を行い、確度と精度の上限（または下限）レベルを調べることができます。これは、将来のロケーション アプリケーションを計画するときや、現在の環境で注意を払うことが必要な領域を分析するときなどに役立ちます。たとえば、これらの制御機能を使用すると、802.11bg ではなく 802.11a を使って確度レベルを 5 メートルに設定したときのロケーション精度の限界を視覚的に表現することができます（図 5-47 を参照）。

図 5-47　802.11a を使用した場合のロケーション検査の例（精度が 5 m の場合）

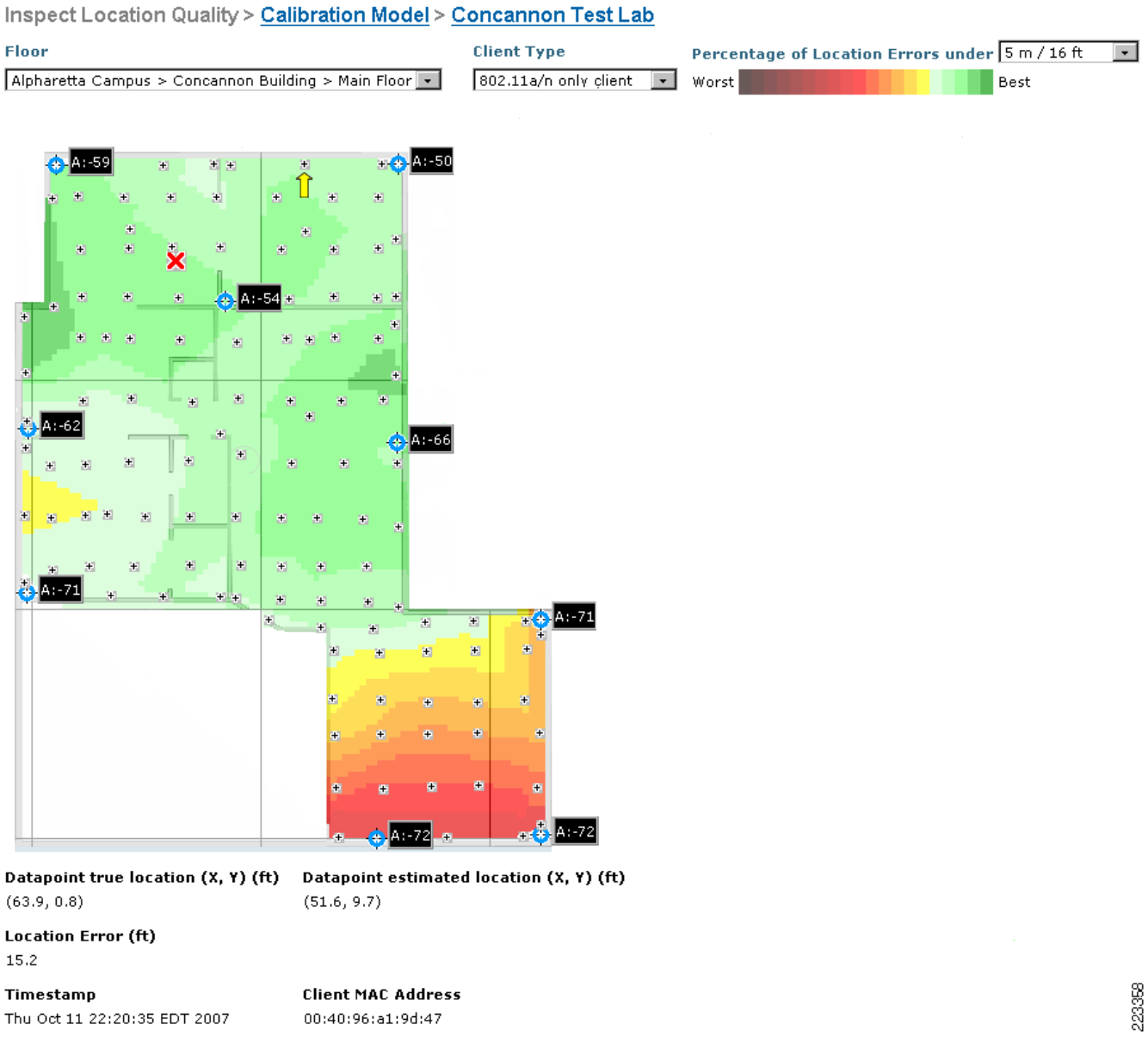


図 5-47 に示すテスト ラボの例では、802.11a を使用して精度を 5 メートルに設定した場合、テスト ラボ フロアの上側 3 分の 2 の部分で精度が 85% 以上になることがわかります。ただし、図の下の部分を見ると、フロアの下側 3 分の 1 の部分で確度レベルが満たされていないため、さらなる調査を行う必要

があります。ここで得られたロケーション検査の結果により、将来、確度を向上させる必要性が生じたときに、現在の調整データを使ってモデル化を行うことができます。その際、ユーザを関与させたり、試験的な実施やエラー テストにユーザを参加させたりする必要はありません。

図 5-46 と図 5-47 ではいずれも、調整データ ポイントはすべてテスト ラボ周囲の線上にあり、周辺部アクセス ポイントの間に位置していることに注意してください。これらのデータ ポイントは、ロケーション検査において「空白領域」が生じないように（または少なくとも減少させるように）意図的に配置されています。ロケーション検査で「空白領域」が生じる場合、その多くの原因として、それらの領域のデータが不足しており、Location Inspection ツールがそれらのポイントにおける確度と精度の有効な値を計算できないことが挙げられます。Location Inspection ツールは、情報が少ない、または情報がない状態での見積もりは行わず、該当する領域は空白として残します。

このような状況を回避するには、周囲の沿線上と、囲まれる領域内の両方に調整データ ポイントを配置することをお勧めします。初回の調整が終わった後でも、必要に応じて、周辺部にあるデータ ポイントを追加できます。これを行うには、調整モデルの [Add Data Points] データ収集フェーズに戻り、空白領域に新しいデータ ポイントを必要な数だけ直接追加します。完了したら、[Calibration] フェーズに戻り、もう一度、ロケーション品質を検査します。空白領域は完全になくなるか、有意に減少しているという結果を得られるはずです。空白領域がまだ残っている場合は、必要に応じて、このプロセスを繰り返します。

（注）　Location Inspection ツールで検査を行うフロアでは、指定した帯域での信号強度情報と、テスト クライアントの実際のロケーション座標を利用できる必要があります。複数のフロアで同じ RF モデルを共有している場合は、モデルの調整が実際に行われたフロアに対してのみ、ロケーション検査を行ってください。

テスト ポイントを使用した確度の確認

Location Inspection の機能を補完するため、ソフトウェア リリース 4.1 では、ロケーション認識 Cisco UWN を使用して特定のフロアにおける Location Appliance の基本確度および精度が仕様を満たしているかどうかについて即座に「適 / 不適」を確認できるようになりました。これはテスト ポイント機能を使用して実行できます。この機能にアクセスするには、WCS メイン メニューから [Monitor] > [Maps] > [（*フロア マップ名*）] > [Position Test Point] を選択します。デバイスの MAC アドレスが指定されると、テスト ポイント機能はロケーション テスト ポイントのすべてのサンプルを追跡し、そのロケーション確度が Location Appliance の基本仕様の範囲内に収まっているテスト ポイント サンプルの数をパーセンテージで示します。

テスト ポイント機能は、フロア上にタグ付き資産、無線クライアント デバイスや不正デバイスが存在し、その実際の物理的なロケーションを把握しており、めったにまたはまったくロケーションが変更されない場合に役立ちます。たとえば、運送用コンテナに展開された資産タグ（移動中には使用されないもの）や無線機能を装備したデスクトップ コンピュータ（スーパーバイザのワークステーションで展開されたロケーションから移動されないもの）が例として挙げられます。これらのデバイスの MAC アドレスがわかっている場合で、実際のロケーションが長期にわたり変わらないときは、テスト ポイント機能を使用して予測されるロケーションと実際のロケーションの比較を行い、ユーザに結果を報告することができます。

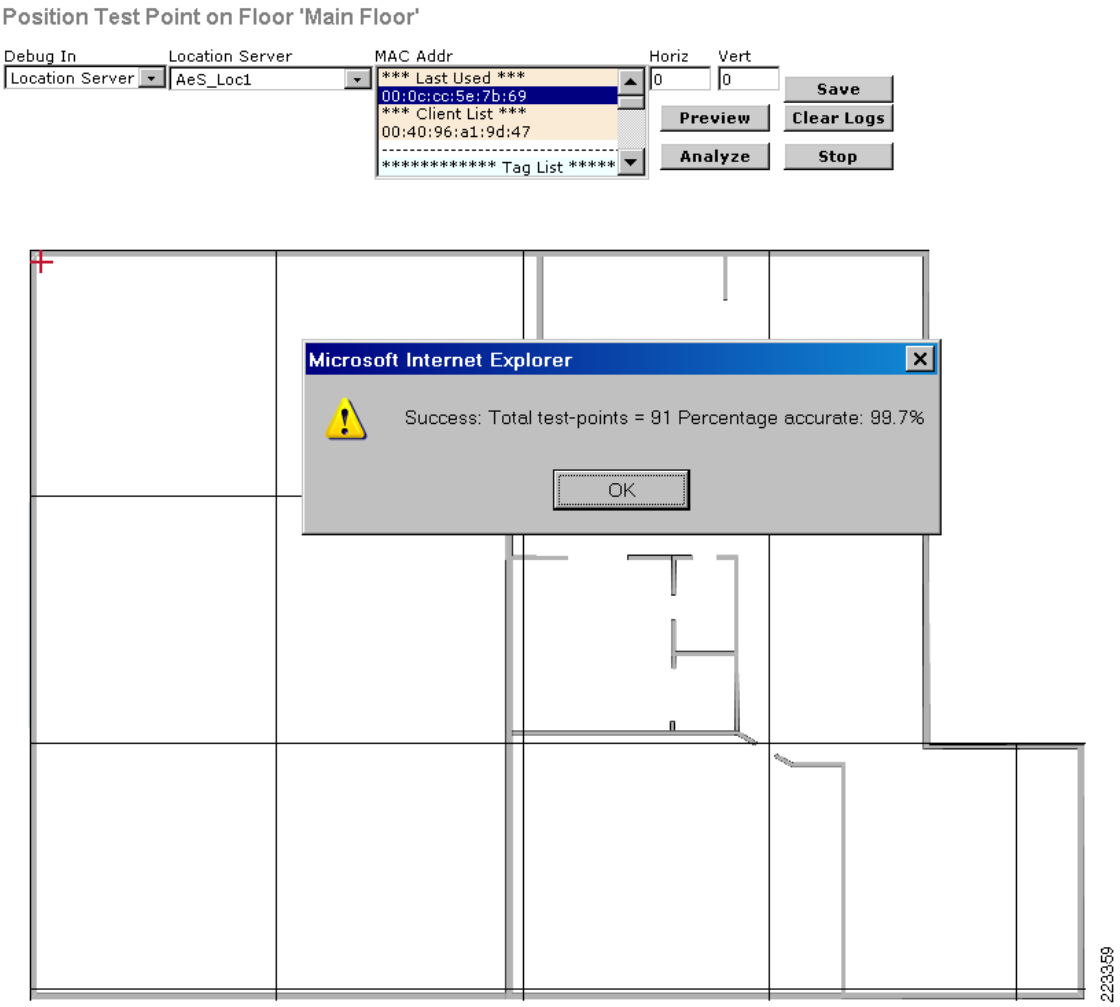
デバイスの実際のロケーションがテスト ポイント機能のユーザによって指定された場合で、デバイスの MAC アドレスをアクティブなテスト ポイントとして追加したときは、WCS を Location Appliance のデバッグ機能と共に動作させ、デバイス カテゴリの SNMP ポーリング期間の終了後、デバイスの実際のロケーションを予測ロケーションに対して比較することができます。WCS は比較処理を実行し、追跡対象デバイスの予測されるロケーションが Location Appliance の基本パフォーマンス仕様の範囲内にあるものについて、その発生率を計算します。WCS ユーザがテスト ポイントの MAC アドレスのドロップダウン メニューでデバイスの MAC アドレスを指定し、[Analyze] オプションをクリックする

と、ユーザはこの情報を受け取ることができます。特定の MAC アドレスの追跡が完了したら、テスト ポイントの MAC アドレスのドロップダウン メニューでデバイスの MAC アドレスを指定し、[Stop] オプションをクリックします。これにより、そのデバイスをテスト ポイントとして使用する処理が終了します。すべてのトラッキングが完了し、蓄積した追跡データが不要になったら、[Clear Logs] オプションを使用してすべてのテスト ポイントとそのトラッキング データを削除できます。

テスト ポイント機能を構成する方法の詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg_ch7.html#wp1066057

[Analyze] 機能で有用なフィードバック情報を受け取るには、少なくとも 1 つのデバイス カテゴリのポーリング期間が終了している必要があることに注意してください。これは、Location Appliance がテスト ポイントについてのロケーション情報を得るための十分な時間を確保するためです（テスト ポイント機能では過去のロケーション データは使用されません）。長期間のロケーション確度について最適な数値を得ることができるように、少なくとも数個のポーリング期間が経過する時間を確保することをお勧めします。図 5-48 は、テスト ポイント機能の [Analyze] 機能によって提供される出力サンプルを示したものです。

図 5-48　テスト ポイント機能



テスト ポイント機能を使用するときは、次の点に注意してください。

- テスト ポイント機能を使用する前に、Advanced Debug 機能を有効にしてください。WCS で Advanced Debug 機能が有効になっていないと、[Monitor] > [Maps] > [（*フロア マップ名*）] を選択したときにドロップダウン メニューに [Position Test Point] オプションが表示されません。
- テスト ポイント機能を使用する前に Location Appliance で Advanced Debug 機能を有効にすることがベスト プラクティスとして推奨されますが、[Save] オプションを使用してテスト ポイントを追加すると、この機能は自動的に有効に設定されます。
- ユーザが水平および垂直の (x,y) 座標を直接指定する場合、Position Test Point フロア マップに赤色の十字線を配置するには [Preview] オプションを使用します。これは、テスト ポイントの実際のロケーションに対して赤色の十字線を手動で配置する代わりに行う操作です。プレビュー機能は、入力された (x,y) 座標に対応するロケーションをユーザが視覚的に確認できるように提供されています。ユーザがテスト ポイントのロケーションに十字線を手動で配置し、プレビューを実行するようにクリックすると、何らかのフィードバックが表示されます。プレビュー機能は、テスト ポイント デバイスの予測ロケーションの表示を意図するものではありません。
- 図 5-48 では、解析コマンドの結果として出力された [Total Test Points] の数が、現在使用されているテスト ポイント デバイスの総数を指しているわけではないことに注意してください。解析コマンドの結果は、指定されたデバイスの MAC アドレスに対するテスト ポイント ロケーション サンプルの総数を示しています。
- WCS の [Position Test Point] 画面では複数のデバイスを選択できますが、（[Save] を使用して）一度に 1 台のデバイスに追加できるテスト ポイントの数は 1 つだけです。最後に [Save] または [Stop] を使用したデバイスの MAC アドレスは保持され、[Last Used] という見出しの下に表示されます。
- ユーザが WCS からログアウトして後でログインし直すと、そのユーザは [Save] を使用して追加されたテスト ポイントにアクセスすることはできません。新しいテスト セッションを開始する前に、残っているテスト ポイントをすべてクリアするには、新しいテスト ポイントのセットを定義する前に [Clear Logs] コマンドを発行することをお勧めします。
- Location Appliance をリブートまたはリスタートすると、追加されたテスト ポイントはクリアされますが、収集されたテスト データは Location Appliance に維持されるため、既に収集が行われたテスト ポイント データをさらに追加することはできません。テスト ポイント データの収集および分析の作業をさらに進めるには、デバイスの MAC アドレスで [Stop] オプションを使用するか、[Clear Logs] オプションを使用することをお勧めします。
- [Clear Logs] オプションを実行すると、すべてのテスト ポイント データ ログがクリアされ、割り当てられているテスト ポイント デバイスがリセットされます。ログをクリアすると、現在のユーザが作成したテスト ポイントだけでなく、他のユーザ（ログインしてテスト ポイント機能の使用を認められている他のユーザ）が作成したテスト ポイントも削除されることに注意してください。

ソフトウェア リリース 4.1 の [Analyze] オプションでは、デバイスの MAC アドレスに関する計算は、一度に 1 台のデバイスについて行われます。テスト ポイントとして複数のデバイスの MAC アドレスを追加する場合は、デバイスの MAC アドレスごとに個別にテスト ポイント データを調べます。これを行うには、ドロップダウンのオプションから対象デバイスの MAC アドレスを選択し、[Analyze] をクリックします。

CHAPTER 6

RFID タグの考慮事項

この章の内容は、次のとおりです。

- 「RFID タグ テクノロジー」（P.6-1）
- 「Cisco UWN での Wi-Fi RFID タグの使用」（P.6-15）
- 「タグ テレメトリおよび通知に関する考慮事項」（P.6-26）
- 「チョークポイントに関する考慮事項」（P.6-31）

RFID タグ テクノロジー

現在製造されている RFID タグの大部分は、超小型回路とアンテナで構成された*パッシブ*RFID タグです。このようなタグがパッシブ タグと呼ばれるのは、パッシブ RFID タグ リーダーまたは*送信機*から比較的近い距離にある場合にのみ活発に通信するからです。

現在市販されている一般的な RFID タグの一種として、*アクティブ*RFID タグと呼ばれるものがあります。このタグは、通常、RF 通信に直接電源を供給するバッテリを内蔵しています。この内蔵電源によって、アクティブ RFID タグは、それ自体に関する情報を遠距離にある RFID タグ リーダーに常時または要求に応じて*ビーコン送信*することができます。通常、アクティブ タグは純粋なパッシブ タグ設計よりもサイズが大きく、より多くの情報を格納できます（メモリ容量が大きいため）。図 6-1 の表は、アクティブ RFID タグとパッシブ RFID タグの一般的な相違点を要約したものです。これらの RFID タグの基本的なカテゴリに属するサブカテゴリとして、*セミパッシブ*RFID タグなどもあります。

（注） *ビーコン*という用語は、正式な 802.11 規格が確立される前から RFID 業界で使用されていました。アクティブ RFID タグが定期的にビーコン送信する場合、タグは一定間隔でタグ メッセージ（タグが送信する他のメッセージとほとんど同じ）を送信するだけです。似た用語を使用していますが、802.11 ビーコンとは*別のもの*です。802.11 ビーコンは、802.11 アクセス ポイント（または IBSS 内のビーコン送信元）が時間同期とモバイル ステーションによる BSS または IBSS の位置特定および識別に必要な PHY 関連のパラメータの提供を目的として送信する管理フレームです。

図 6-1　アクティブ RFID とパッシブ RFID の比較

	アクティブ RFID	パッシブ RFID
タグの電源	タグに内蔵	RF 経由でリーダーから転送されるエネルギー
タグ バッテリ	あり	なし
タグ電力の有効範囲	継続	リーダーのフィールド範囲内のみ
必要とされるリーダーからタグへの信号強度	非常に弱い	非常に強い（タグに電力を供給する必要あり）
利用可能なタグからリーダーへの信号強度	強い	非常に弱い

	アクティブ RFID	パッシブ RFID
通信範囲	遠距離（100 m 以上）	近距離（3 m 以下）
センサー機能	センサー入力（センサー イベントのデータとタイム スタンプ）を継続して監視、記録することが可能	タグがリーダーから電力を供給された場合のみセンサーの値の読み込みと転送が可能（データとタイム スタンプは含まれない）
データ ストレージ	大容量の読み込み/書き込みデータ ストレージ（128 KB）（高度なデータ検索とアクセス機能が利用可能）	小容量の読み込み/書き込みデータ ストレージ（例： 128 バイト）

190588

市場の発展により、最近はさらに新しい種類の RFID タグが注目を集めています。ハイブリッド タグまたは*マルチモード*タグと呼ばれ、複数のタグ テクノロジーを 1 つの汎用パッケージに統合したもので、1 つまたは複数のロケーション テクノロジーによって追跡することができます。マルチモード RFID タグは、通常は低電力で小型フォーム ファクタのデバイスで、1 つの物理タグが複数のパーソナリティを持ち、以前は資産にそれぞれ別の物理タグを付けなければ実行できなかったタスクを 1 つのタグだけで実行できるようになります。一例として、複数のアクティブ タグと 1 つのパッシブ タグを一体化したマルチモード タグがあります。

パッシブ RFID タグ

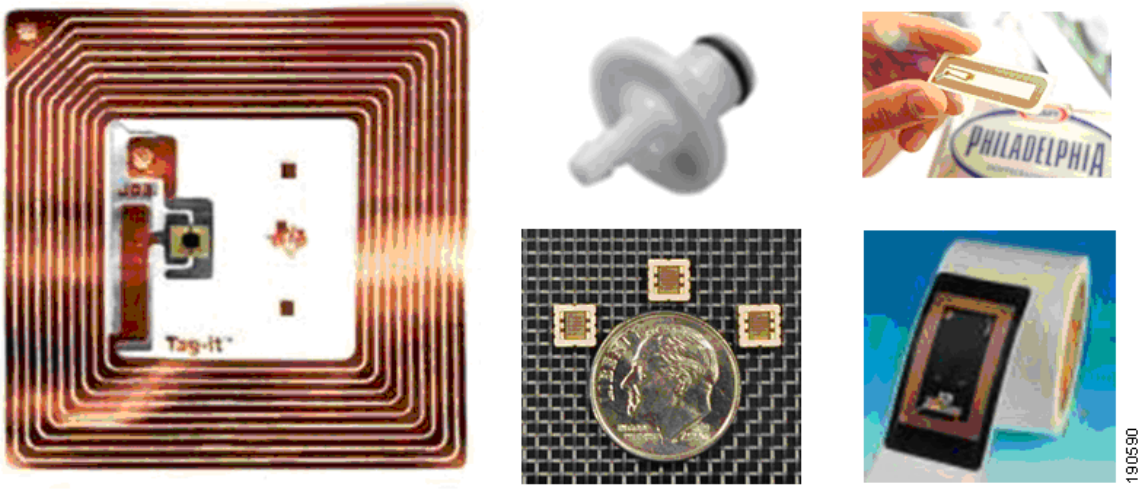
パッシブ RFID タグは、一般には電源を内蔵しておらず、RFID リーダー（または送信機）の電磁界から電力の供給を受けます。電磁界から供給されるエネルギーには、パッシブ タグの電子部品の電源として使用できるように整流と電圧増倍の処理が行われます。一般的なパッシブ RFID タグ設計では、タグが RFID リーダーの範囲内になければホスト アプリケーションと通信することはできません。

送信機にはさまざまな形式があります。代表的な例として、ハンドヘルド リーダー送信機（図 6-2 の左側）や通過する複数のタグを一度に読み取ることができる大型の据え置き型モデル（図 6-2 の中央）があります。埋め込み型の超小型パッシブ RFID リーダーおよびタグ（図 6-2 の右側）は、アクションの即時検証が必要な用途に利用できます。そうした用途の例として、供給ラインのホース接続の即時確認などがあります。こうした用途では、ホースのプラグとレセプタクルに埋め込まれたパッシブ RFID タグとマイクロリーダーによって、常に正しい供給ホースが正しい供給原料に接続されていることを確認できます。正しく接続されていない場合は、誤接続が検出され、システムは流れを制御する電磁弁を開きません。

図 6-2　パッシブ RFID 送信機

パッシブ RFID タグ（図 6-3）は、コイルとマイクロ回路で構成され、マイクロ回路には基本的な変調回路、アンテナ、および不揮発性メモリが含まれています。

図 6-3　パッシブ RFID タグ



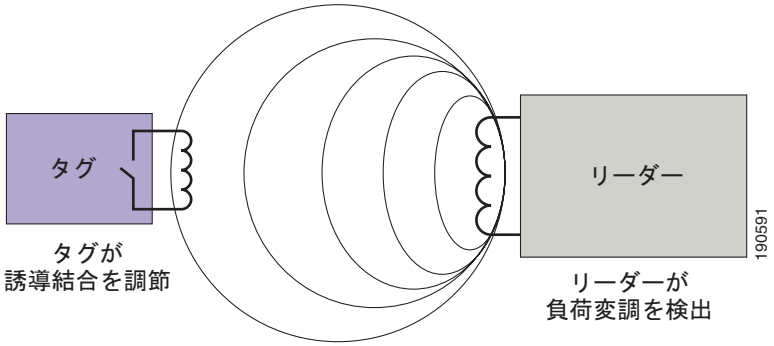
パッシブ RFID タグは、RFID リーダーへのデータ送信方法と RFID リーダーの誘導電磁界から電力の供給を受ける方法の違いによって、いくつかの種類に分けられます。これには、次の 2 つの基本的な方法があります。

- 近接場の負荷変調と誘導結合：この方法（図 6-4 を参照）では、RFID リーダーがショートレンジ交流電流磁界を提供し、それをパッシブ RFID タグが電源および通信媒体として利用します。この磁界が*誘導（または近接場）結合*[1] と呼ばれる方法によって RFID タグのアンテナ コイルに電圧を誘導し、そこからタグに電力が供給されます。タグは、RFID リーダーの磁界からタグがエネルギーを受け取る場合は必ず RFID リーダーがアンテナのリード線を通した電圧降下を検出できることを利用して、タグそれ自体の情報を RFID リーダーに送信します。タグは、この現象を利用し、負荷抵抗器のオンとオフを切り替えて*負荷変調*を行うことによって、バイナリ情報をリーダーに送信することができます。タグが負荷変調を行うと、RFID リーダーがそのアクションをリーダーのアンテナで信号電圧の振幅変調として検出します。負荷変調と誘導結合は、125 から 135 kHz および 13.56 MHz の周波数を使用するパッシブ RFID タグで採用されています。このような低い周波

1. ファラデーの法則に基づく磁界誘導方法

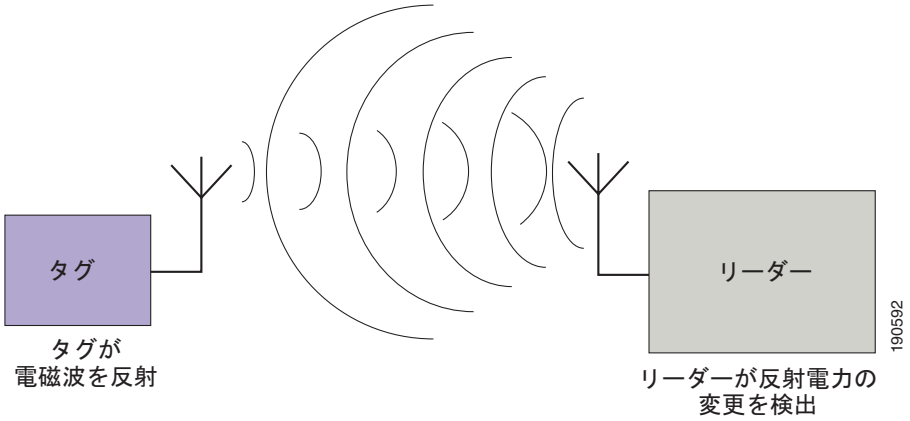
数を使用することに関連して、大型のアンテナ、低いデータ レートおよび帯域幅、および電磁界の強度の急激な減衰（$1/r^6$）が必要になるという制限が生じます。ここで、*r* は低周波送信機とパッシブ RFID タグとの距離を表します。

図 6-4　　パッシブ タグの負荷変調



- 遠距離場の後方散乱変調と電磁結合：この方法（図 6-5 を参照）では、RFID リーダーが中距離の電磁界を提供し、それをパッシブ RFID タグが電源および通信媒体として利用します。パッシブ RFID タグは、*電磁（または遠距離場）結合*と呼ばれる方法によって RFID リーダーの電磁界からエネルギーを獲得します。ただし、電磁界に含まれるエネルギーはパッシブ タグのアンテナによって一部 RFID リーダーに反射されます。この反射の厳密な特性はアンテナに接続された負荷（抵抗）によって異なります。タグは、反射された電磁波に振幅変調を適用するために、アンテナと並行して配置された負荷のサイズを変えることで、*後方散乱変調*によって情報のペイロードを RFID リーダーに返送することができます。後方散乱変調と電磁結合を利用するタグは、一般に、誘導結合を利用するタグより遠距離の通信が可能であり、その多くは 868 MHz 以上の周波数で動作するパッシブ RFID タグです。遠距離場結合を利用するタグは、一般に、誘導結合を利用するタグよりはるかに遠距離の通信が可能です。その主要因は、遠距離の電磁場であることから減衰率が大幅に低下する（1/r2）ことです。遠距離場結合を利用するタグでは、通常、誘導結合を利用するタグの場合より小さいアンテナが使用されます。

図 6-5　　パッシブ タグの後方散乱変調



これらのいずれの方法でも、パッシブ RFID タグは 802.11 インフラストラクチャのアクセス ポイントと*直接*通信することはできません。パッシブ RFID タグからの通信は、すべて RFID リーダーを介して行われます。

パッシブ RFID タグは、アクティブ RFID タグより製造コストが安く、保守をほとんど必要としません。このような長寿命で低コストという特徴があることから、パッシブ RFID タグは、*オープンループ* サプライ チェーンにおけるユニット、ケース、およびパレット レベルでのタグ付け用として、小売業者や製造業者の間で注目されています。オープンループ サプライ チェーンでは、通常、RFID タグがタグの所有者または発信者の管理を離れるかどうかについて、ほとんどまたはまったく規制することはできません。パッシブ RFID タグは、外部リーダーのエネルギー場とその低い反射電力に依存するため、アクティブ RFID タグに比べ、読み取り範囲は大幅に短く（最短は負荷変調を利用するタグで数インチ、長くても後方散乱変調を利用するタグで数メートル）、読み取りの信頼性も低くなります。

パッシブ RFID タグの市販パッケージには、簡素な基板に取り付けるタイプから接着剤と紙の間に挟まれた従来型の「ハード」タグ（一般には RFID「スマート」ラベルという）まで、さまざまな形式のものがあります。使用されるフォーム ファクタは、主としてパッシブ RFID タグの用途によって決まり、パッシブ RFID タグのコストの大部分に相当します。

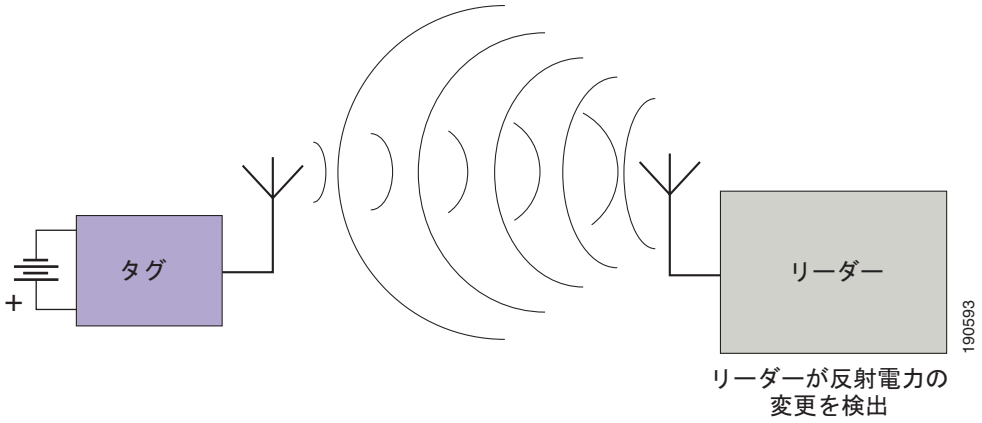
セミパッシブ RFID タグ

*セミパッシブ*RFID タグは、純粋なパッシブ RFID タグ設計の重要な 2 つの問題点を解消します。

- 内蔵テレメトリおよびセンサーの資産監視回路に電源が継続的に供給されない。
- 範囲が狭い。

セミパッシブ タグは、パッシブ タグとは異なり、内蔵バッテリを使用して、通信回路および温度や衝撃の監視などを行う補助回路に電源を供給します。注意すべき点は、セミパッシブ RFID タグが電源を内蔵しているといっても、その電源で直接 RF 電磁エネルギーを生成するわけではないことです。セミパッシブ RFID タグは、一般には後方散乱変調を利用し、RFID リーダーからの電磁エネルギーを反射することにより、標準のパッシブ タグの応答に似たタグ応答を生成します（図 6-6 を参照）。内蔵バッテリは、テレメトリ回路および後方散乱実現回路に電力を供給する目的にのみ使用され、RF エネルギーの生成には使用されません。

図 6-6　セミパッシブ RFID タグにおける後方散乱変調



ISM 帯域で動作するセミパッシブ RFID タグ（図 6-7 を参照）は、数年間の寿命を持つリチウム電池を内蔵しており、最大 30 メートルの範囲での通信が可能です。従来のパッシブ RFID タグより範囲が大幅に拡大された最大の理由は、後方散乱に対して最適化されたアンテナを使用していることです。従来の後方散乱変調を利用するパッシブ RFID タグとは異なり、セミパッシブ タグに内蔵されたアンテナは後方散乱変調専用であり、セミパッシブ RFID タグのアンテナに依存することなくタグへの電力の信頼できるコンジットとなります。したがって、セミパッシブ タグ アンテナは後方散乱の効率性を最大限に高められるように最適化でき、純粋なパッシブ RFID タグ アンテナ設計よりはるかに高いパフォーマンスを達成できます。

図 6-7　セミパッシブ RFID タグ

セミパッシブ RFID タグは、内蔵 NVRAM、リアルタイム クロック、各種の環境センサーの有無によって、さまざまな種類に分かれます。セミパッシブ RFID タグは、改ざんインジケータや衝撃センサーなどとのインターフェイスもサポートします。セミパッシブ RFID タグの一般的な用途には、車両資産の追跡、セキュリティ アクセス システム、サプライ チェーンの自動化、冷蔵管理、階層的資産追跡システムなどがあります。

アクティブ RFID タグ

*アクティブ タグ*は、一般には*クローズドループ システム*（タグがタグの所有者または発信者が管理する施設から物理的に離れることを前提としないシステム）での高価値資産のリアルタイム追跡に使用されます。通常は、資産の価値が高いほどアクティブ タグのコストが高くなることが正当化され、タグの再利用への機運が高まります。医療機器、電子試験装置、コンピュータ、再利用可能な輸送コンテナ、および組立ラインの仕掛品などが、アクティブ タグ テクノロジーの代表的な用途例です。アクティブ RFID タグ（図 6-8 を参照）では、*存在*の追跡（資産が特定の場所にあるかどうかを示す肯定または否定の表示）、つまりリアルタイム ロケーションが可能です。アクティブ RFID タグは、通常はパッシブ RFID タグより大型です。ほとんどの RTLS システムはアクティブ RFID タグ テクノロジーの利用を基礎としています。

図 6-8　アクティブ RFID タグ

アクティブ タグは 512 KB 以上の RAM を搭載できるため、取り付け先の資産に関する情報を格納し、次のビーコン間隔が到来したとき、またはポーリングされたときに情報を送信できます。このように大容量のメモリが内蔵されていることから、アクティブ RFID は、RFID タグを単に「ライセンス プレート」または参照として使用したのではホスト データベースの即時検索を行うことができない状況でパッシブ RFID より好適となります。このような状況の好例として、ホスト データベースが常に使用できるとは限らない遠隔地の軍事施設などがあります。重要な資産データをタグに格納することで、ホスト システムが利用できるかどうかにかかわらず、情報をタグから直接取得し、使用できます。

アクティブ RFID タグの動作周波数は 303 MHz、315 MHz、418 MHz、433 MHz、868 MHz、915 MHz、および 2400 MHz で、読み取り範囲は 60 ～ 300 フィートです。アクティブ RFID タグ テクノロジーは、トランスミッタ出力が高く、アンテナが最適化され、電源が内蔵されているため電力供給の信頼性が高いことから、一般に読み取り速度および読み取りの信頼性がきわめて高くなります。アクティブ RFID タグのコストは、メモリの容量、バッテリの寿命、および付加価値機能（内蔵温度センサー、動作検出、テレメトリ インターフェイスなど）の有無によって大きく異なります。タグ ハウジングの耐久性も価格に影響します。タグの用途によっては通常より耐久性のある特別なハウジングが必要であり、その場合はさらに価格が高くなります。この種のほとんどの電子機器と同じように、技術の進歩、生産の効率化、製品のコモディティ化によって市場価格が低下するに伴い、アクティブ タグも低価格化していくと考えられます。

アクティブ RFID タグのビーコン送信

*ビーコン送信*を行うアクティブ RFID タグは多くの RTLS システムで使用されており、特に資産をロケーション レシーバによって場所と時間を問わず追跡する必要がある場合に役立ちます。ビーコン送信を行うアクティブ RFID タグでは、RFID タグの一意の識別子を含む短いメッセージ ペイロードが事前にプログラミングされた間隔で送信されます。この間隔はタグの所有者またはユーザがプログラミングするもので、タグ RSSI の望ましい更新頻度に応じて設定できます。通常は、タグの送信間隔が短いほどバッテリの寿命が短くなりますが、場合によっては、タグ RSSI の報告頻度が増すため、タグ ロケーション確度が向上します。タグの送信間隔が長いほどバッテリの寿命も長くなりますが、タグ RSSI が頻繁に報告されないため、ロケーション更新の頻度が低下します。

802.11 アクティブ RFID タグ

*802.11（Wi-Fi）アクティブ*RFID タグ（図 6-9 を参照）は、2.4 ～ 2.4835 GHz または 5.8 ～ 5.825 GHz の無認可 ISM 帯域用に設計されています。このドキュメントの発行時点で製造されている 802.11 Wi-Fi アクティブ RFID タグの周波数は最高で 2.4 GHz です。

これらのタグはアクティブ RFID タグの特性を備えていますが、該当する IEEE 802.11 規格およびプロトコルにも準拠しています。Wi-Fi RFID タグは特別なハードウェアやファームウェアの変更なしで標準の Wi-Fi インフラストラクチャと直接通信でき、ラップトップや VoWLAN 電話などの Wi-Fi クライアントと共存できます。802.11 Wi-Fi クライアント無線機を装備した資産は、電源がオンの状態であれ

ば、資産タグを取り付けていなくても追跡することができます。802.11 Wi-Fi クライアント無線機を搭載していない資産は、物理的に取り付けられた 802.11 アクティブ RFID タグによって追跡できます。また、物理的に取り付けられた 802.11 アクティブ RFID タグによって、ロケーション認識 Cisco UWN を使用し、Wi-Fi クライアント無線機を搭載した資産を無線機の電源がオフの状態で追跡することもできます。

図 6-9　802.11 Wi-Fi アクティブ RFID タグ

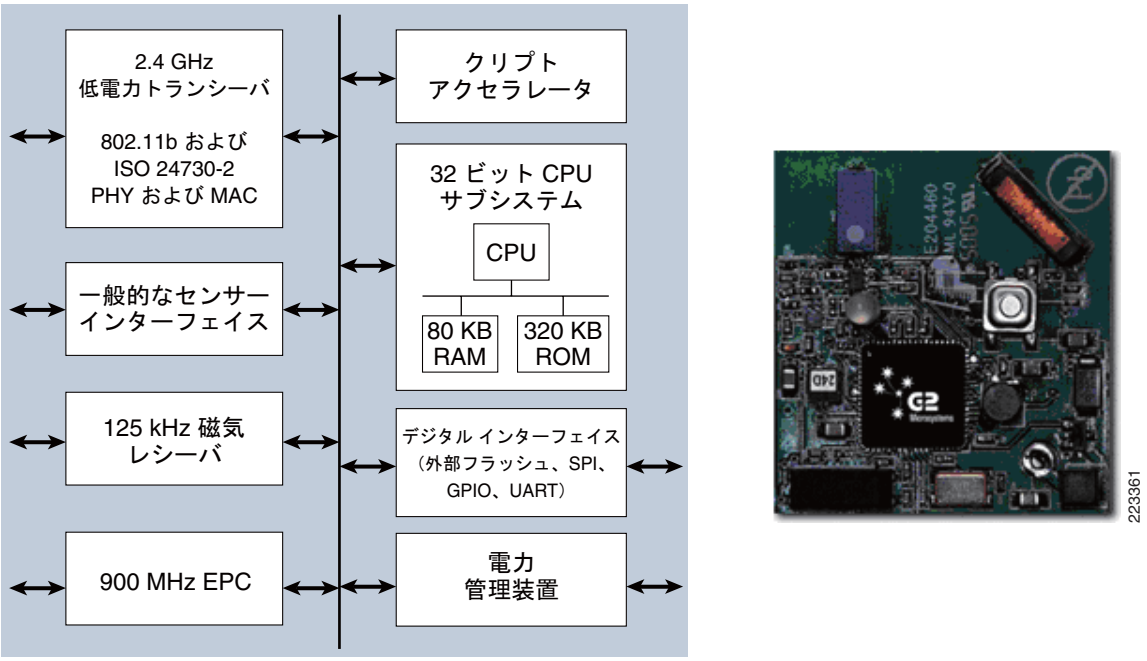
マルチモード RFID タグ

前述のとおり、トランスポンダ アクティブ RFID タグは、主要なタグ動作モードと、アクティベーション、非活動化、動作変更などのさまざまな付加価値機能で使用できる二次的な通信方法の組み合わせを提供します。このタイプのタグは、高速道路の料金所などでかなり以前から使用されています。この場合、高速のアクティベータが近づくと、タグがトリガーされてデータを送信し、それによってユーザのアカウントから高速料金が引き落とされます。

比較的最近の進展として、複数のロケーション テクノロジーを利用する *マルチモード* RFID タグの導入があります。マルチモード タグは、1 つの物理パッケージで資産に複数のタグを取り付けた場合と同じ機能を提供します。資産を 1 つのエンタープライズ クローズド ループ システムから同じロケーション追跡テクノロジーが使用されていない可能性のある別のシステムへ移動する必要がある場合に非常に便利です。たとえば、再利用可能な輸送コンテナを、製造元、販売代理店、および小売業者において、ISO24730-2 TDoA、802.11 Wi-Fi アクティブ RFID、およびパッシブ RFID の組み合わせを使用して追跡する必要があるとします。マルチモード タグであれば、これら 3 種類のテクノロジーを小型フォーム ファクタの低電力パッケージ 1 つだけで提供できます。このようなデバイスは、タグ磁気シグナリング近接通信デバイスも使用できる機能を備えていることもあります。これは、資産に 3 つ以上の RFID タグを取り付ける場合に比べ、管理、保守、および全体的な展開の容易さの点で明確な利点となります。

この種のマルチモード タグは、2 つ以上の異なる RFID タグ テクノロジーを 1 つのチップまたはチップセットに統合する高度集積タグ OEM シリコンの登場により、さらに実現可能性が高まりました。その例として G2 Microsystems の G2C501（図 6-10 を参照）があります。この製品は、802.11b Wi-Fi アクティブ RFID、900 MHz EPC Global Gen 1 Class 0 パッシブ RFID、2.4 GHz ISO24730-2 TDoA、32 ビット CPU、クリプト アクセラレータ、リアルタイム クロック、およびセンサー インターフェイスを搭載した完全な Wi-Fi システムオンチップ（SoC）です。

図 6-10　　G2C501 RFID システムオンチップ（SoC）



高度集積タグ シリコンの利用は、タグ ベンダーに次のような多くのメリットをもたらします。

- 小型フォーム ファクタ
- 低電力消費
- 詳しく文書化されたソフトウェアおよびハードウェア インターフェイス
- 複数のロケーション テクノロジーに対する柔軟なサポート

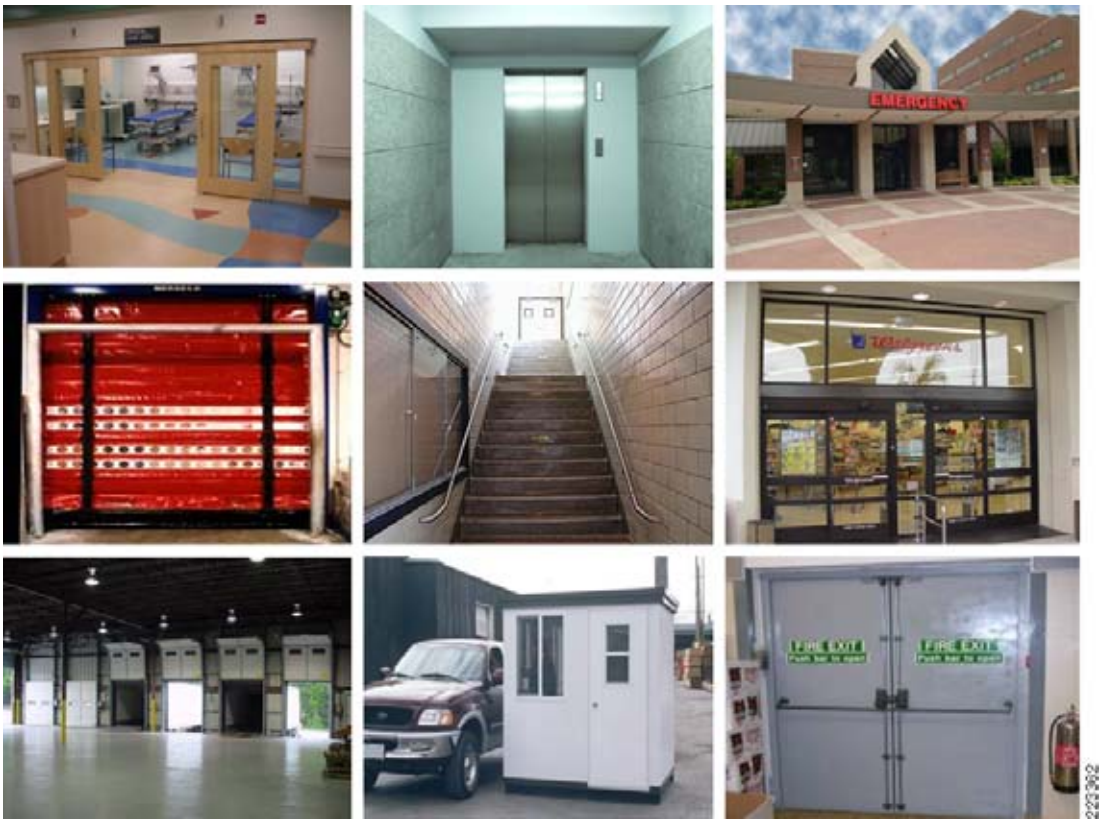
これらの機能を利用したマルチモード タグの好例は、図 6-9 の左下に示した WhereNet Corporation（http://www.wherenet.com）の WhereNet IV 資産タグです。WhereNet IV は、Cisco Compatible Extensions に準拠した 802.11 Wi-Fi アクティブ タグ実装に 125 kHz 磁気シグナリングおよび ISO 24730-2 機能を組み合わせ、小型の高度集積設計に集約したものです。

チョークポイント トリガー

*チョークポイント トリガー*は、資産タグがチョークポイント トリガーの動作領域に入ったときに資産タグをトリガーしてタグの設定や動作を変更する近接通信デバイスです。この変更は、資産タグに一意の識別子を送信させるような単純なものもあれば、タグにその内部設定やステータスを変更させるような複雑なものもあります。チョークポイント トリガーの最も重要な機能の 1 つは、資産タグに*チョークポイント*と呼ばれる領域に入った（またはこの領域から出た）ことを RTLS に通知するように促すことです。チョークポイントとは、接続された領域間の通路となる明確に定義された物理領域（入口、出口、その他の通路など）のことです。図 6-11 に一般的なチョークポイントの例を示します。

（注）　*チョークポイント トリガー*は、通常は*チョークポイント*内に展開されますが、*チョークポイント*がチョークポイント トリガーの意味で使用されている状況も多く見られます。

図 6-11　　一般的なチョークポイント領域



屋外のチョークポイントには、柵で囲まれたゲート、橋、料金所、これらに類する通路が含まれます。屋内のチョークポイントには、以下の場所を結ぶ入口や出口が含まれます。

- 建物内部の部屋やフロア（出入口、タラップ、ゲート、階段の吹き抜け、エレベータ昇降口など）
- 隣接建造物（通路やトンネルなど）または建造物の内部および外部（正面玄関、通用口、船積みドック、非常口など）

チョークポイント トリガーは、タグが付いた資産がチョークポイント領域に出入りしたことを直ちにロケーション システムに通知するようタグの動作を変更できます。チョークポイント トリガーの対象範囲は RTLS が対象とする領域全体から見ると狭いため、RTLS は資産がチョークポイント領域の範囲内にあることを比較的迅速に高い信頼性をもって確定できます。RTLS は、チョークポイント領域をフロア マップに表示するのに加え、チョークポイント領域内の資産の検出を利用して外部システムでイベントをトリガーすることもできます。そうしたイベントには、データベースの更新、通知アラート、アラームなどが含まれます。適切なアプリケーション ソフトウェアを追加することにより、チョークポイントを以下の目的に利用することもできます。

- 高価な資産の追跡：チョークポイント ロケーション トラッキングは、高価な資産が定められた場所にあることを確認するのに役立ちます。それらの資産が入口または出口から搬出されることを検出した場合などには、RTLS にアラートが通知されます。

- 製造工程管理：機器、部品、および完成品を生産工程間の移動に際して正確に追跡できます。これによって、必要なすべての工程を通過することだけでなく、正しい順序で通過したことも確認できます。
- 在庫管理：配送センターのすべての出入口にチョークポイント ロケーション トラッキング機能を戦略的に配備することにより、製品が配送センターに出入りするのに応じて自動的に在庫データベースを更新できます。
- セキュリティ：タグが付いた資産の移動を追跡および監視することにより、無許可での施設からの持ち出しや施設内での移動を防止できます。

チョークポイント トリガーは低電力の近距離通信機能であり、従来の出入口以外にも用途を広げることができます。出力電力が低いため、チョークポイント トリガーの有効範囲をきわめて狭い明確に定義された領域（棚、ラック、保存容器、作業現場、病床など）に適合するようにカスタマイズすることができます。このような限定的な領域における資産の出し入れ（ラックへの機器の取り付けまたは取り外しなど）を前述の高電力チョークポイント トリガーの場合と同じような方法で厳密に監視することができます。

チョークポイントによって行われるタグ動作の変更の具体的な内容はベンダーによって異なります。タグ動作の変更には、以下のものが含まれます。

- タグ マルチキャスト メッセージの即時送信
- タグのリアクティベーション
- タグの非活動化
- タグ送信間隔の変更
- インジケータ ランプのアクティベーション
- フロア識別子またはセル識別子の保存
- タグ マルチキャスト メッセージへの次のような補足メッセージの追加
  - チョークポイント識別子
  - 事前に設定されたメッセージ データ
  - テレメトリ データ

すべてのアクティブ タグ ベンダーがチョークポイント トリガーの使用をサポートしているわけではありません。チョークポイント トリガーをサポートしている場合でも、チョークポイント トリガーの使用方法はベンダーによって異なる傾向があります。Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグを提供する各ベンダーは、通常、それらのタグとの互換性を保持するように設計されたチョークポイント トリガーを提供しています。現時点では、チョークポイント トリガーを製造元が異なる資産タグ間で相互運用することはできません。

範囲はモデルや製造元によって異なることがあります。Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグで使用されるチョークポイント トリガーの平均的な有効範囲は 10 インチ～約 25 フィートです。これらの製品は低周波磁気シグナリングを使用して動作します。範囲は予測可能な傾向にあり、一般的な建築用材およびその内容物に対する優れたペネトレーションを発揮します。

図 6-12 は、AeroScout および WhereNet の低周波磁気シグナリング チョークポイント トリガー デバイスを示しています。AeroScout ではチョークポイント トリガーを *Exciter* と呼び、WhereNet では *WherePort* と呼んでいます。AeroScout EX-2000 Exciter と WhereNet WherePort は大型モデルで、広いチョークポイント領域や室内の存在検出に対応できる最大限の範囲を提供します。これらの製品は、乗り物の乗降口、ゲート、その他の広いチョークポイント領域用であり、調整可能な範囲は 20 フィートを超えます。コンパクトな AeroScout EX-3100 Exciter および EX-3200 Exciter は、出入口、棚、ラックなどの狭いチョークポイント領域での近距離通信用です。これらの製品の範囲は、前者が 8 インチ～ 6.5 フィート、後者が 8 インチ～ 9.75 フィートです。

図 6-12　AeroScout Exciter と WhereNet WherePort

これらの製品の追加情報については、以下のベンダー Web サイトをご覧ください。

http://www.aeroscout.com/content/library

http://zes.zebra.com/products/rtls/tags-and-call-tags/wheretag-iv.jsp

（注）　Cisco WCS は、チョークポイント トリガーをロケーション認識 Cisco UWN に定義するために使用されますが、現在のところチョークポイント トリガー自体を設定することはできません。チョークポイント トリガーを設定するには、チョークポイント トリガーのベンダーが提供するソフトウェア（AeroScout Network Exciter Manager（ANEM）、WhereNet SystemBuilder / WhereWand など）を使用する必要があります。チョークポイント トリガーをベンダーが提供するチョークポイント管理ソフトウェアで適切に設定することなく WCS に追加した場合、正しく機能しないことがあります。

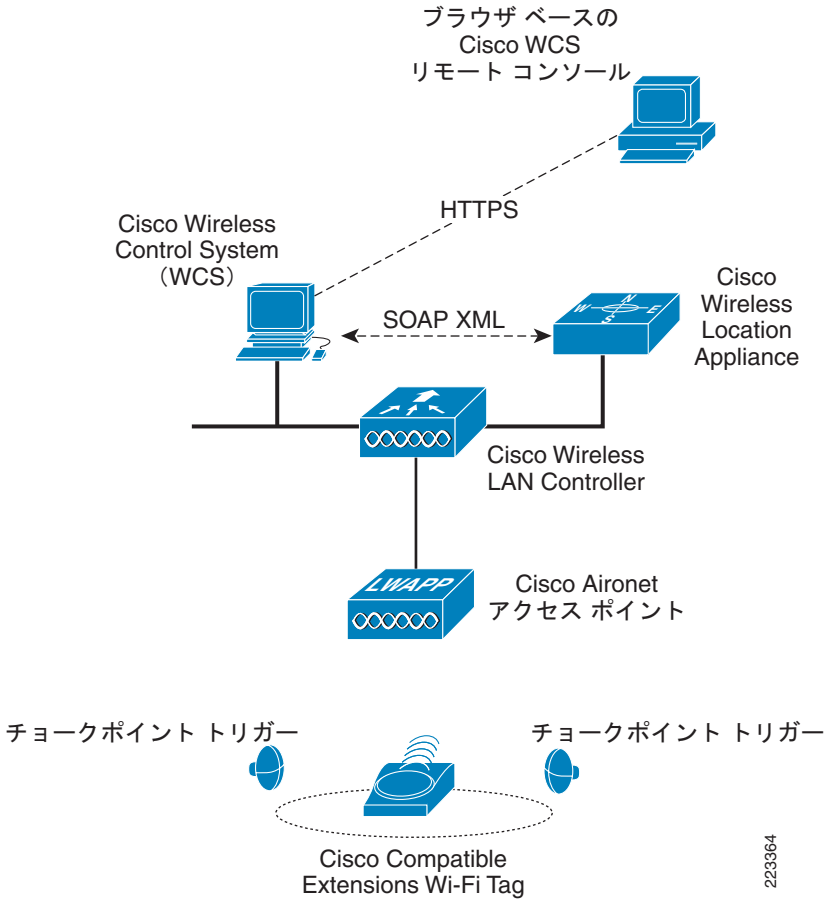
正しく設定されたチョークポイント トリガーは、次のいずれかのモードで動作します。

- *オンライン モード*：チョークポイント トリガーのステータスがチョークポイント トリガー ベンダー提供のソフトウェアでイーサネットまたはシリアル データ接続を介して監視されます。
- *オフライン モード*：設定済みのチョークポイント トリガーが電源接続のみで動作します。

チョークポイント トリガーは一意のアドレスで識別されます。このアドレスによって、受信したタグがスティミュレートしたチョークポイント トリガーを明確に特定できます。この識別子は、通常、イーサネット ベース モデルではチョークポイント トリガーの MAC アドレスですが、ローカルに管理され、割り当てられた識別子（WhereNet WherePort の「Transmit ID」など）の場合もあります。ロケーション認識 Cisco UWN のリリース 4.1（図 6-13 を参照）では、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグがチョークポイント トリガーの有効範囲内に入ると、タグがチョークポイント トリガーにスティミュレートされ、802.11 によって送信されるタグ マルチキャスト フレームを使用してスティミュレーションの送信元をロケーション認識 Cisco UWN と特定します。このタグ マルチキャスト フレームを検出したアクセス ポイントがそのタグ マルチキャスト フレームをそれぞれの登録されたコントローラに転送し、コントローラが Location Appliance 宛ての LOCP Measurement Notification フレームを生成します。

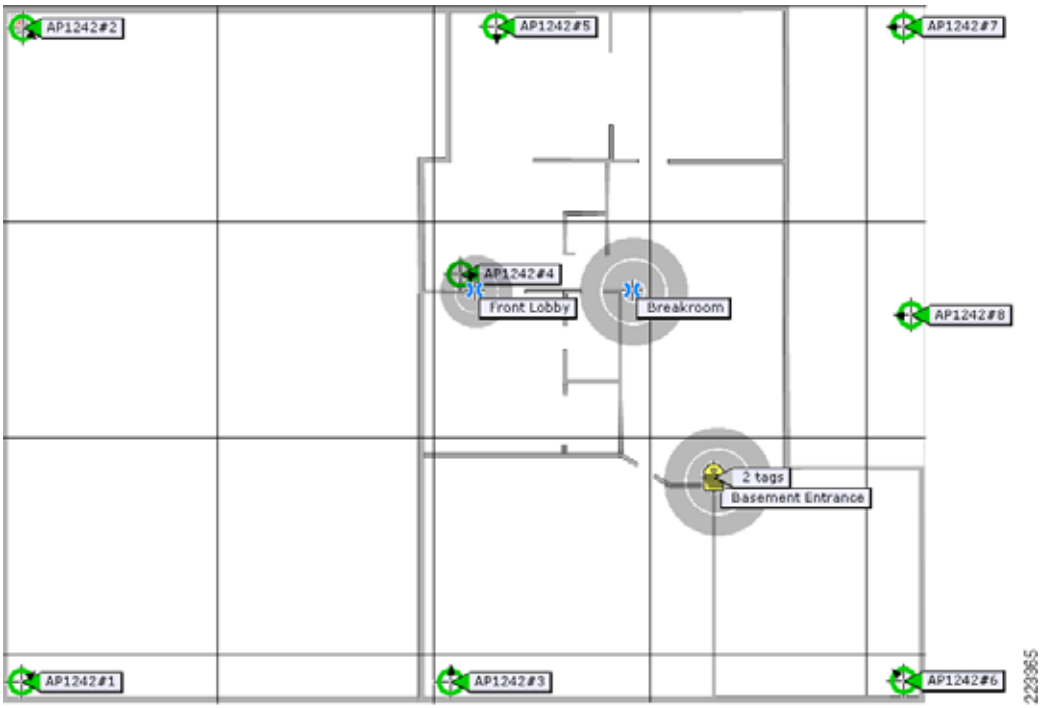
（注）　チョークポイント トリガーと資産タグの通信は、チョークポイント トリガーから資産タグへの単方向通信です。リリース 4.1 では、チョークポイント トリガーとロケーション認識 Cisco UWN が直接通信することはできません。

図 6-13　ロケーション認識 Cisco UWN とチョークポイント トリガー



Location Appliance は、LOCP 測定通知によって提供される情報を使用して、タグの現在の位置が指定されたチョークポイントの設定された範囲内にあることを示します。この情報は適切な Location Appliance データベースに保存され、Location Appliance API を介してロケーション クライアントから使用できます。ロケーション クライアントは、チョークポイント ロケーション情報をフロア マップに表示することがあります。一例として、WCS フロア マップを図 6-14 に示します。この図では、*Basement Entrance* というチョークポイントに 2 つの RFID タグがあります。Location Appliance は、電子メール、syslog、SOAP、または SNMP トラップを使用して、WCS や外部アプリケーションにアラートおよびその他の非同期ノースバウンド通知をトリガーすることもできます。

図 6-14　チョークポイントが示された WCS フロア マップ

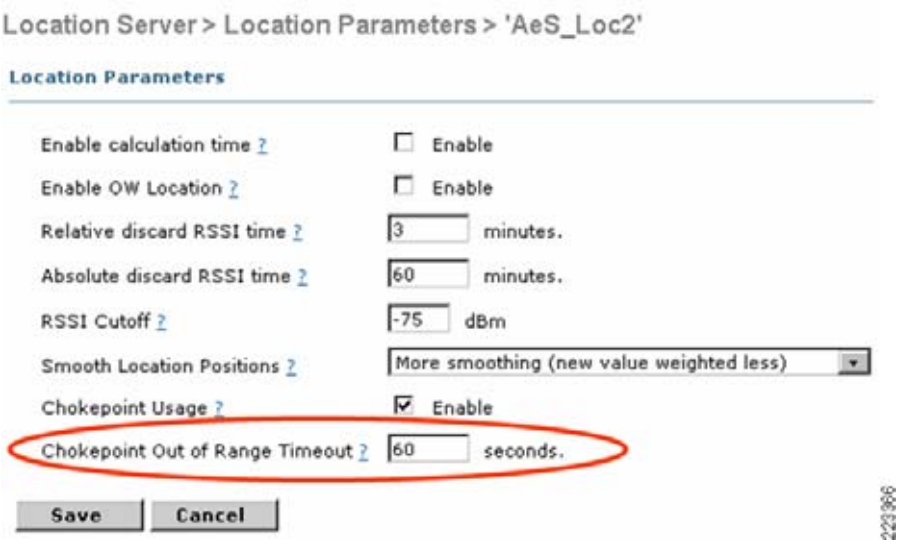


Cisco UWN の リリース 4.1 では、タグがチョークポイント トリガーの範囲から出た後も Location Appliance は次のイベントのいずれかが発生するまでタグがチョークポイント トリガーの設定された範囲内にあることを示します。

- タグがそのチョークポイント トリガーの範囲から出たことを示す。
- Chokepoint Out of Range Timeout に設定された時間（図 6-15 を参照。デフォルトは 60 秒）が経過する。

これらのイベントのどちらかが発生すると、Location Appliance は、デバイスが別のチョークポイント領域に入り、別のチョークポイント トリガーのスティミュレーション ゾーンに入るまで、RF フィンガープリントを使用してデバイスの位置を計算します。デバイスが後続のチョークポイント トリガーによってスティミュレートされ、そのスティミュレーションが Cisco UWN に報告されると、Location Appliance は追跡したデバイスを新しいチョークポイントの位置に配置します。

図 6-15　Chokepoint Out of Range Timeout



Cisco UWN での Wi-Fi RFID タグの使用

互換性のある RFID タグ

Cisco Location Appliance は 製品や耐久品の製造元が包括的な事業計画の一環として展開している RFID タグの追跡に利用できるのかという質問が多く寄せられます。RFID タグは製造または販売の過程で一斉に製品に取り付けられるもので、その多くはパッシブ RFID 設計ですが、高価な耐久品にはアクティブ RFID タグが使用されることもあります。多くの場合、製品のタグは、製造または初期出荷の段階で業界団体または政府機関の指示に従って取り付けられます。

質問の答えは、使用される RFID タグの種類によって異なります。Cisco UWN の リリース 4.1 では、802.11 Wi-Fi アクティブ RFID タグ（または 802.11 Wi-Fi アクティブ RFID 機能を備えたマルチモード資産タグ）だけが Wi-Fi アクセス ポイント（Cisco Wi-Fi アクセス ポイントを含む）と直接通信できます。現在、最も普及している「純粋な」パッシブ RFID タグまたは非 Wi-Fi アクティブ RFID タグは、ロケーション認識 Cisco UWN および Cisco Wireless Location Appliance とは通信できません。現在市販されている 802.11 Wi-Fi アクティブ タグは、すべてが Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠しているわけではありません。PanGo / InnerWireless および AeroScout Ltd. の資産タグは、この仕様に準拠していませんが、ロケーション認識 Cisco UWN には対応しています。ただし、これらのタグでは、Cisco Compatible Extensions Wi-Fi Tag 仕様に含まれ、リリース 4.1 に導入された拡張機能は使用できません。PanGo Networks および AeroScout 以外のベンダーが提供する、この仕様に準拠しない資産タグは、Cisco Wireless Location Appliance ではサポートされていません。

Wi-Fi アクティブ RFID タグが Cisco Compatible Extensions Wi-Fi Tag 仕様と互換性があり、ロケーション認識 Cisco UWN の拡張機能を利用できるかどうかを確認するには、Cisco Compatible Extensions Web サイト（http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html）を参照してください。このサイトでは、Cisco Compatible Extensions Wi-Fi Tag 仕様と互換性のあるタグおよびタグ ベンダーの最新リストを掲載しています。

Cisco Compatible Extensions Web サイトに掲載されたタグおよびタグ ベンダーのリストは、そこに含まれるタグが Cisco Compatible Extensions Wi-Fi Tag プログラムにおいて厳しい検証試験に合格したことを示しています。Cisco Compatible Extensions Wi-Fi Tag プログラムによって、ロケーション認識

Cisco Unified Wireless Network を使用しているお客様は、シスコのテクノロジー パートナーが提供する最新の革新的技術および高度化された技術を採用することができます。登録チャネル パートナーは、Cisco Compatible Extensions Wi-Fi Tag プログラムのガイドラインを次の URL でご覧いただけます。

http://www.cisco.com/web/partners/downloads/partner/WWChannels/download/wifiguide.pdf

パッシブ RFID リーダーまたは非 802.11 アクティブ RFID リーダーの送信機を Cisco LWAPP 対応のワイヤレス ネットワークも導入されている環境に Cisco UWN および Location Appliance のロケーション トラッキング機能とは関係なく展開する場合もあります。こうしたリーダー / 送信機には、ネットワークへのアップリンクとして従来型の有線イーサネットを使用するものもあれば、Wi-Fi クライアント無線機を内蔵しているものもあります（図 6-16 に示すようなポータブル RFID 送信機など）。現在のところ、このようなポータブル RFID タグ リーダーに対応する個々のパッシブ RFID タグを Cisco Location Appliance で追跡することはできませんが、ポータブル リーダー自体は、業界標準の 802.11 クライアント無線機を使用しているため、通常は追跡が可能です。これらのリーダーは、標準 WLAN クライアントとして機能し、Location Appliance に定義されたコントローラが提供する WLAN SSID に対して認証 / アソシエートする場合、他の WLAN クライアントと見なされ、フロア マップに青色の四角アイコンとして表示されます。

図 6-16　Wi-Fi アップリンク内蔵のポータブル RFID 送信機

802.11g 環境での 802.11b タグの使用

802.11g クライアントおよびアクセス ポイントだけで構成されるネットワークで 802.11b 資産タグを使用した場合のパフォーマンスに対する潜在的な影響についても、よく質問を受けます。このような問題では、一般に、保護メカニズム（RTS-CTS や CTS-to-Self など）が 802.11g ネットワークによって起動され、802.11b 資産タグと 802.11g ネットワークの互換性が確保されるかどうかが最も重要な点となります。

（注）　802.11g のパフォーマンス、キャパシティ、および保護メカニズムの詳細については、http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00801d61a3.shtml のホワイトペーパー『*Capacity, Coverage and Deployment Considerations for IEEE 802.11g*』を参照してください。

論点となることが多いのは、これらの保護メカニズムが以下のタグの 1 つまたは複数を純粋な 802.11g ワイヤレス インフラストラクチャに導入すると同時に起動されるかどうかです。

- タグ レイヤ 2 マルチキャスト メッセージを送信する 802.11b 資産タグ
- プローブ要求を発行する 802.11b 資産タグ（WLAN クライアントとして機能する）
- 活発にアソシエートする 802.11b 資産タグ（WLAN クライアントとして機能する）

まず、明確に理解しておく必要があるのは、レイヤ 2 マルチキャスト 802.11b を使用してタグ メッセージを送信する（WLAN にアソシエートしようとしない）資産タグはどのような状況でも 802.11g 保護モードを開始しないことです。これには、Cisco Compatible Extensions Wi-Fi Tag 仕様のバージョン 1 に厳密に準拠する資産タグの運用も含まれます。

調査や分析によって、802.11b 資産タグまたは WLAN クライアントの電源を入れただけではアクセス ポイントのネットワーク全体で保護メカニズムが起動されないことが証明されています。具体的には、以下の点が明らかになっています。

- 特定のチャネル上のアクセス ポイントに*アソシエートしない* 802.11b 資産タグからプローブ要求が発行されただけでは、それを検出した 802.11g アクセス ポイントが保護モードを開始しない。
- 802.11b 資産タグが当該セルまたは同一チャネル上の隣接するセルにアソシエートするまで保護モードは開始されない。資産タグがアソシエートすると、ターゲット セルだけでなく、同一チャネル上の他のセルや RF においてターゲット セルに隣接するセルでも保護モードが開始されます。
- 802.11b 資産タグと同じチャネル上にないか、RF において 802.11b 資産タグに隣接しないアクセス ポイントは、保護モードを開始しない。

802.11b 資産タグには、オプションの機能として、定期的にプローブ要求を発行し、Over-the-Air ファームウェアや設定を更新するためにワイヤレス インフラストラクチャに一時的にアソシエートしようとするものがあります。こうしたタグにも上記の点は当てはまりますが、それはこのような拡張通信モードが使用される短い時間に限られます。

資産タグ トラッキングの有効化

（注）　Cisco UWN Release 4.1 では、WLAN コントローラで CLI コマンドの **config status rfid enable** を使用して資産タグ トラッキングを有効にする必要がなくなりました。リリース 4.1 では、コントローラでの RFID タグ データの収集はデフォルトで有効になります。

資産タグ RF データ タイムアウトの有効化

RFID Data Timeout パラメータは、コントローラ上のアクセス ポイントが資産タグを検出しない場合、その資産タグをコントローラの内部テーブルから削除するまでに経過すべき時間の静的な値（秒数）を設定します。通常の運用では、このパラメータを一般的なタグ数の環境で使用される最大のタグ送信間隔の 3 倍以上（最大 8 倍）に設定することをお勧めします。これには、固定送信間隔だけでなく「移動中」送信間隔も含める必要があります。このパラメータに設定できる値の有効範囲は 60 ～ 7200 秒、デフォルト値は 1200 秒です。

たとえば、タグの固定送信間隔が 60 秒である場合は、RFID データ タイムアウトを次のように 480 に設定することを検討します。

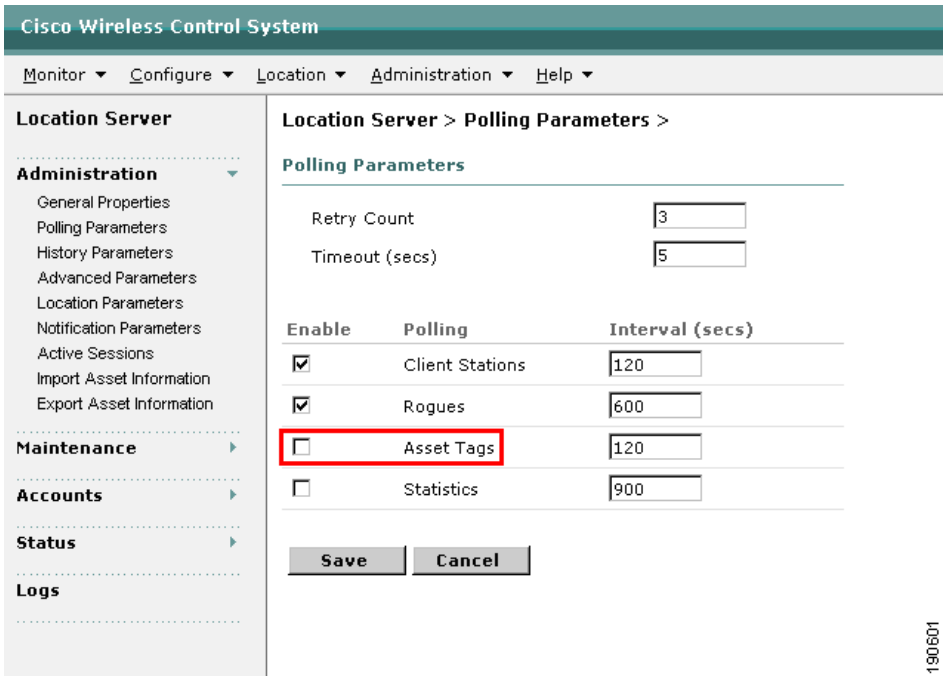
```
(Cisco Controller) >config rfid timeout 480
 (cisco Controller) >

(Cisco Controller) >show rfid config
RFID Tag data Collection..................... Enabled
RFID data timeout............................ 480 seconds
```

WLAN コントローラから最新の資産タグ RSSI が確実に収集されるようにするために、RFID データ タイムアウトを常に Location Appliance 上の資産タグ ポーリング間隔（次の項を参照）より大きな値に設定することをお勧めします。

資産タグ ポーリングの有効化

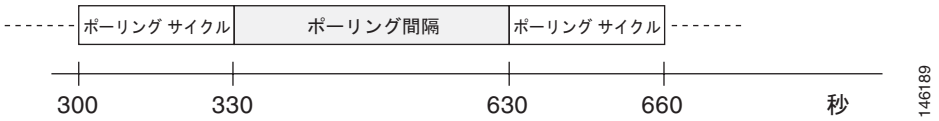
資産タグ トラッキングに Location Appliance を使用するためには、[Locate] > [Location Server] > [Polling Parameters] GUI パネルで SNMP 資産タグ ポーリングを明示的に有効にする必要があります。SNMP 資産タグ ポーリングを有効にするには、図 6-17 の赤い線で囲まれたチェックボックスを使用します。

図 6-17　RFID タグ ポーリングの有効化



ポーリング間隔のデフォルト値は、Location Appliance が SNMP を使用してコントローラをポーリングする以降のポーリング サイクルが開始されるまでの時間を表します。たとえば、ポーリング サイクルの完了に 30 秒を要し、ポーリング間隔が 300 秒である場合、ポーリング サイクルは、図 6-18 に示すように 330 秒ごとに開始されます。

図 6-18　ポーリング間隔



資産移動の度合いにもよりますが、更新されたタグ RSSI 情報が短いポーリング間隔で取得されることによって、より頻繁にロケーションが更新されることがあります。ただし、Location Appliance に設定された資産タグ ポーリング間隔とタグ群全体の平均送信間隔の時間差によって、資産タグ ポーリングの効率が低下する可能性があります。多数の WLAN コントローラからなる極端な構成では、資産タグ ポーリング間隔が短すぎる場合、Location Appliance と WLAN コントローラの両方にほとんど一定の（多くの場合、意味のない）ポーリングによる負荷がかかる可能性があります。その結果、より効果的な利用が可能であったリソースが無駄になり、パフォーマンスに悪影響が及ぶことがあります。

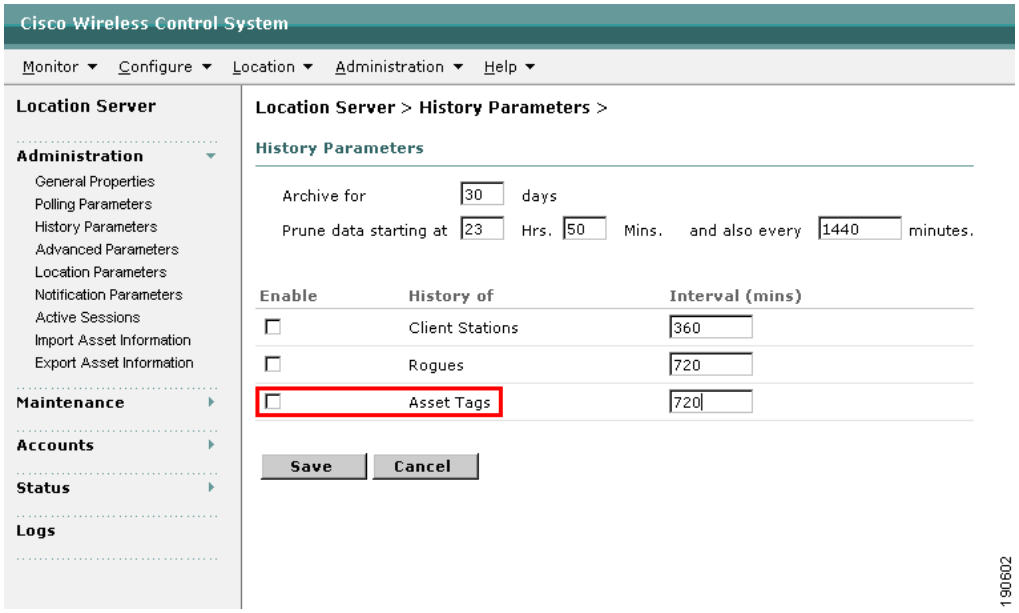
一般に、同じ送信間隔の資産タグ群では、Location Appliance の資産タグ ポーリング間隔を資産タグの送信間隔と同じか、それより大きな値に設定すると、ポーリングの効率を最大限に高めることができます。たとえば、それぞれの送信間隔が 60 秒である 100 個の資産タグ群では、Location Appliance の

資産タグ ポーリング間隔をデフォルトの 120 秒（タグ送信間隔の 2 倍）のままにすると、コントローラは更新された RSSI を 100 個のタグから 120 秒間に最低 1 回（おそらく 2 回）受け取る可能性があります。タグ ロケーションの更新頻度を高めようとして資産タグ ポーリング間隔を 30 秒に設定すると、一部のタグでは目的を達成できますが、全体的なポーリング効率は低下するおそれがあります。

送信間隔が一定ではない資産タグ群では、通常、送信間隔が最も短いタグから更新された RSSI 情報を頻繁に取得することによる利点とタグ群全体のポーリング効率のいずれかを選択する必要があります。資産タグ ポーリング間隔を短く設定すると、マルチキャスト フレームの送信頻度が高いタグには効果的ですが、展開されている WLAN コントローラの数によっては、資産タグ ポーリング間隔を Location Appliance がコントローラの頻繁なポーリングに多くの時間を費やすほど小さくしないことが必要です。コントローラの数が多い環境では、パフォーマンスの低下につながることがあります。ロケーション更新がロケーション クライアントの画面に表示される速度は、コントローラと Location Appliance 間の更新頻度だけでなく、ロケーション クライアントが Location Appliance をポーリングして更新を取得する頻度にも依存することに注意してください。

資産タグ ロケーション履歴の記録は、デフォルトで無効になっています。ロケーション傾向分析および資産タグ ロケーション履歴の分析が必要な場合は、図 6-19 に示す [Location] > [History Parameters] 画面でロケーション履歴の記録を有効にする必要があります。[Asset Tags] ライン アイテムを有効にし、データベースに履歴データを書き込む履歴アーカイブ間隔（デフォルトは 720 秒）を指定します。ロケーション履歴の記録は、資産タグ トラッキングを実行するうえで必須ではありませんが、資産タグが存在していた場所の履歴を Location Appliance が「再生」できるようになるため、多くの場合、有効にするのが望ましいと言えます。

図 6-19　RFID タグ履歴の有効化



資産タグ表示の有効化

WCS が資産タグの位置を表示するためには、図 6-20 に示す [Monitor] > [Maps] > [Campus] > [Building] > [Floor] で資産タグの表示を明示的に有効にする必要があります。資産タグの表示を有効にするには、[Layers] メニューで [802.11 Tags] を選択します。WCS フロア マップ ページをリフレッシュまたはリロードすると、検出された資産タグがフロア マップに黄色のタグ アイコンで示されます。

図 6-20　WCS での資産タグ表示の有効化

資産タグの設定

ロケーション認識 Cisco UWN と通信するためには、チャネル、送信間隔、データ形式などの資産タグ パラメータを適切に設定する必要があります。この項では、AeroScout タグが UWN に認識され、正しくローカライズされるために必要な基本的なパラメータ設定について説明します。

（注）　AeroScout 資産タグは、この項で Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠した資産タグの設定方法を示す例として取り上げただけです。実際に資産タグを設定するときには、必ずそのタグのベンダーが提供するツールを使用する必要があります。AeroScout、InnerWireless（PanGo）、WhereNet、G2、または類似の製品を提供する他の資産タグ ベンダーのユーザは、それぞれのベンダーの製品マニュアルで設定に関するガイドラインを確認してください。

AeroScout Tag Manager のバージョン 3.x には、最近導入された AeroScout T3 資産タグを含め、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する AeroScout 資産タグをサポートするための新機能がいくつも追加されています。

この項では、AeroScout 資産タグとロケーション認識 Cisco UWN との基本的な通信を設定する手順について説明します。この点について、AeroScout が提供する総合的なマニュアルに代わる詳しい説明を提供するつもりはありません。Tag Manager を使用した AeroScout 資産タグの設定については、以下の AeroScout マニュアルを主要な参照資料としてください。

- AeroScout Tag Manager Quick Start

- AeroScout Tag Manager 3.0 User Guide

Cisco Compatible Extensions Wi-Fi Tag 仕様で導入された新機能を活用するためには、AeroScout 資産タグが以下のレベルのタグ ファームウェアを搭載している必要があります（図 6-21 を参照）。

- AeroScout T2：Firmware Release 4.3x 以上
- AeroScout T3：Firmware Release 6.0x 以上

上記のリリースより以前のファームウェアを搭載した AeroScout 資産タグもロケーション認識 Cisco UWN のリリース 4.1 と相互運用できます。ただし、これらの仕様に適合しないタグでは、リリース 4.1 に含まれる、Cisco Compatible Extensions Wi-Fi Tag 仕様で導入された機能を利用することはできません。

図 6-21　AeroScout T2 および T3 資産タグ

AeroScout 資産タグは、2.4 GHz IEEE 802.11b トランシーバと低周波ショートレンジ 125 kHz 磁気シグナリング レシーバの両方を内蔵しています。2.4 GHz 出力電力は最大 +19dBm（81mW）まで設定できます。タグ設定では、AeroScout 資産タグは 802.11b インターフェイスを使用して *Tag Activator* と呼ばれるプログラミング デバイスから送信されるコマンドおよびデータに応答します。このデバイスはイーサネット アドレッシング可能な低周波 125 kHz 磁気シグナリング トランスミッタであり、802.11b レシーバも内蔵しています。Tag Activator は *Tag Manager* と呼ばれる Windows ベースのタグ設定ソフトウェアと組み合わせて使用します。

AeroScout 資産タグは Tag Activator から磁気シグナリング 125 kHz レシーバでのみ情報を受信できることに注意してください。AeroScout 資産タグは磁気シグナリング トランスミッタを内蔵しておらず、Tag Activator は磁気シグナリング レシーバを内蔵していません。AeroScout 資産タグは Tag Activator から磁気シグナリングによってコマンドやデータを受信し、Tag Manager アプリケーションに応答を返送します。送信の確認には、802.11b 機能と Tag Activator 内の 802.11b レシーバを使用します。

AeroScout Tag Activator（図 6-22 を参照）は、802.3af イーサネットまたは外部 5VDC 電源から電力の供給を受けます。Tag Activator は AeroScout Tag Manager と連携し、最大で約 3 フィートの範囲において同時に最大 50 個の AeroScout 資産タグを設定、プログラミング、起動、または停止できます。Tag Activator は AeroScout タグ ハードウェアに関して完全に非侵入型です。Tag Activator と AeroScout タグを接続するケーブルはありません。Tag Activator を使用すると、タグ ケースの環境用シールを取り除くことなく設定を変更することができます。タグ シールをほとんど取り除く必要がないことは、厳重な環境用シーリングが必要となる苛酷な環境または多湿環境で資産タグを使用する場合に役立ちます。

図 6-22　AeroScout Tag Activator

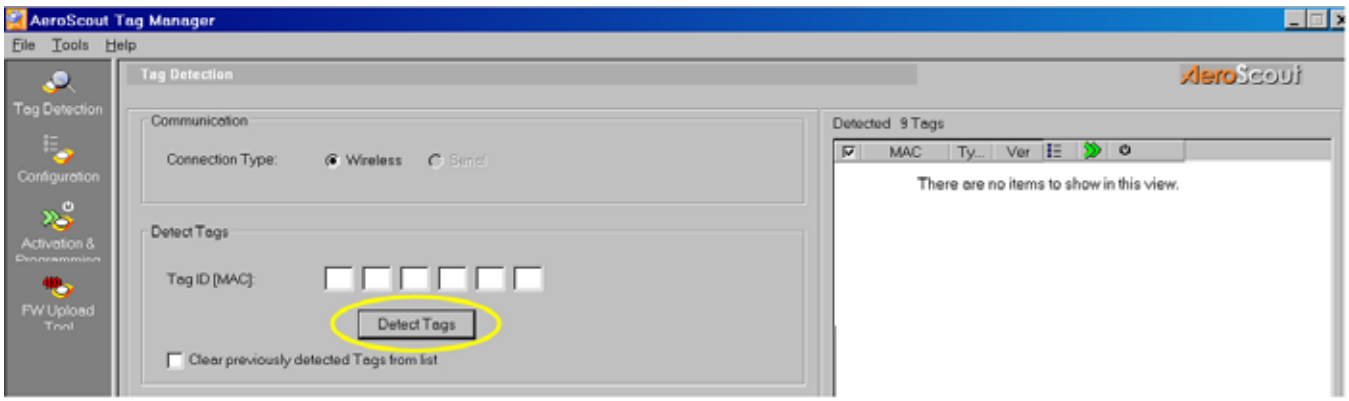
AeroScout Tag Activator については、次の AeroScout マニュアルを主要な参照資料としてください。

- *AeroScout Tag Activator User's Guide*

AeroScout T2 または T3 資産タグのリリース 4.1 との基本的な通信を設定するには、次の手順を実行します。

1. 『*AeroScout Tag Activator User's Guide*』に記載されたベンダーの指示に従って AeroScout Tag Activator を展開します。AeroScout Tag Activator の電源は、802.3af に準拠するスイッチから直接供給することもできれば、この製品に内蔵されている AC 電源を使用して非 802.3af スイッチから供給することも可能です。潜在的な不安定性を回避するために、AeroScout Tag Activator を接続するシスコ スイッチ ポートに**スパニング ツリー PortFast** を設定する必要があります。
2. 『*AeroScout Tag Activator User's Guide*』および『*AeroScout Tag Manager version 3.0, Quick Start Guide*』に記載されたベンダーの指示に従って AeroScout Tag Manager の Tag Activator との通信を設定します。Tag Activator が Tag Manager によって正しく認識されることを確認します。
3. Tag Activator から約 3 フィートの範囲に最大 50 個の AeroScout タグを配置し、図 6-23 に示す [Detect Tags] 機能を使用してタグを検出します。

図 6-23　Tag Manager v3.04 によるタグの検出



4. タグが検出されたら（図 6-24）、図 6-25 に示す画面の右側の領域で、それぞれのチェックボックスをクリックしてすべてのタグを選択します。

図 6-24　Tag Manager v3.04 によるタグの検出

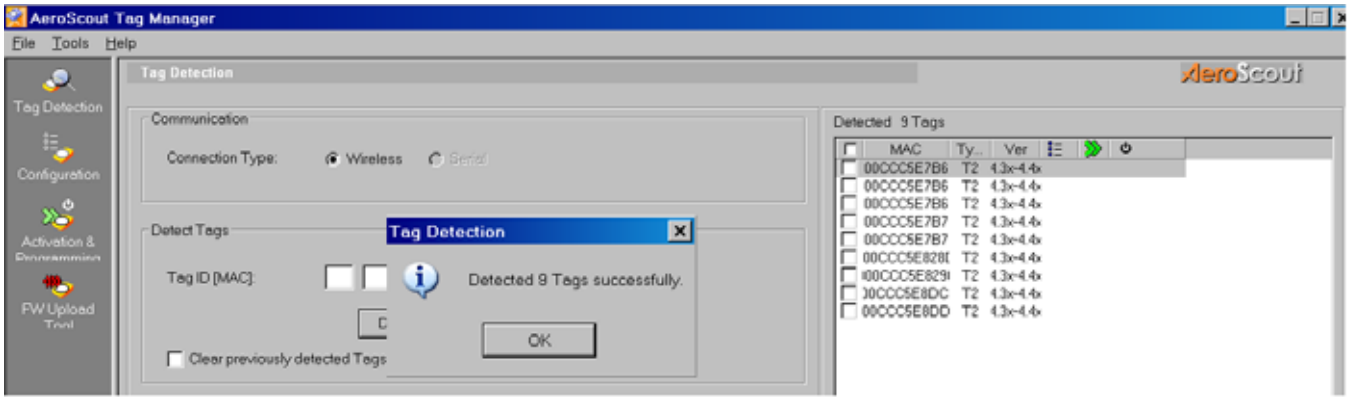
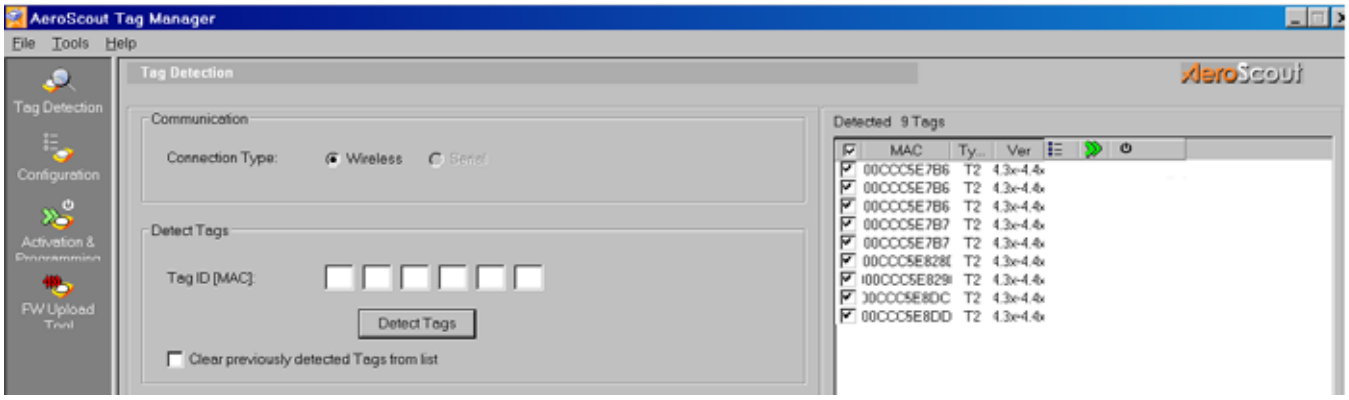


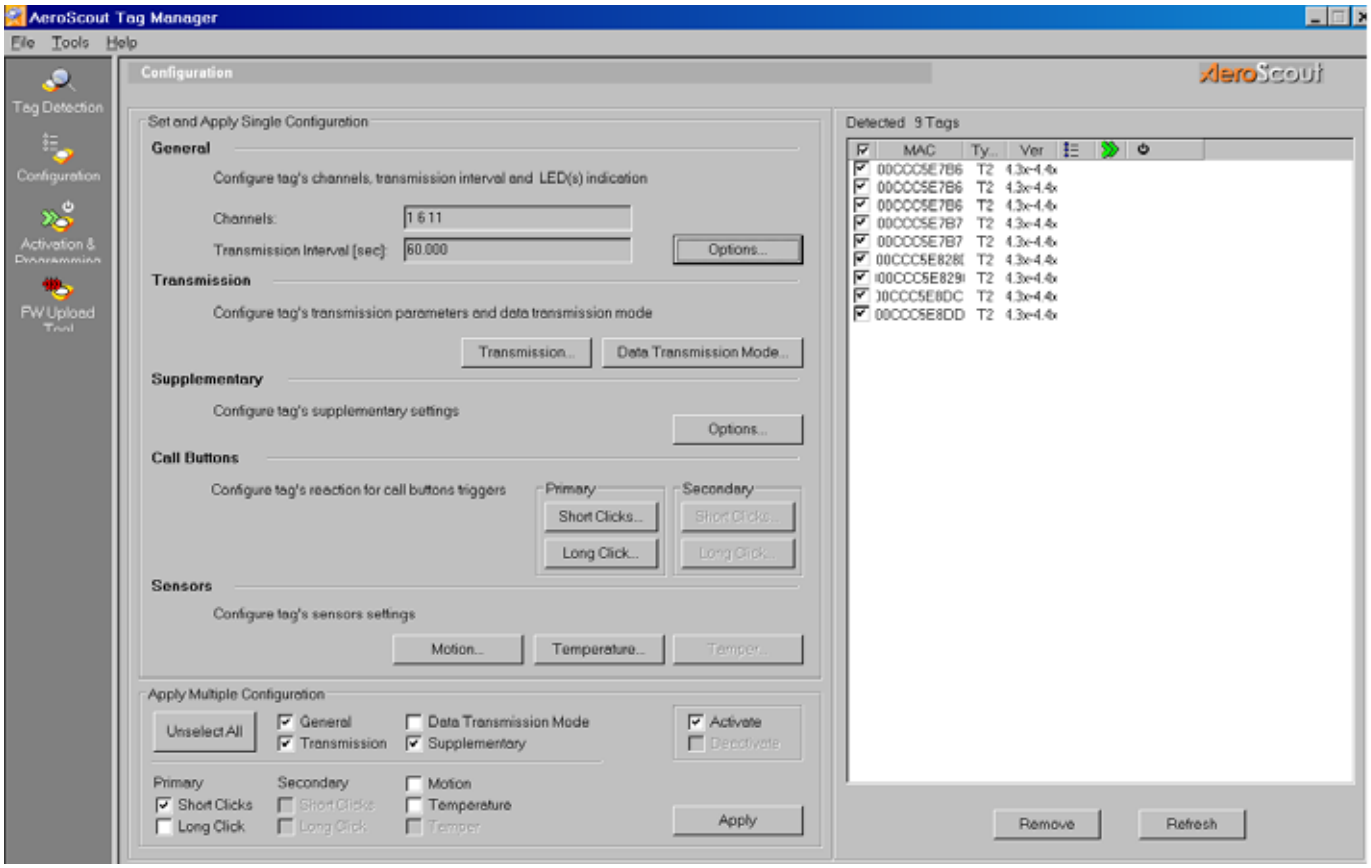
図 6-25　設定するタグの選択



5. [Tag Detection] メニューの左側の領域で [Configuration] オプションを選択します。[Tag Configuration] メニューが表示されます（図 6-26）。

（注）　既に設定されているタグで小さな設定変更を行う場合は、タグの現在の設定を Tag Manager にインポートして設定テンプレートとして使用し、その設定に変更を適用することをお勧めします。結果を 1 つ以上のタグに適用することができます。これを行うには、[Configuration] オプションを選択してから、テンプレートとして使用するタグにマウス カーソルを置きます。右クリックして [Get Tag Configuration] を選択し、操作の続行を確認するダイアログで [Yes] をクリックします。

図 6-26　Tag Manager 3.04 の [Configuration] パネル



6. T2 または T3 タグの Cisco UWN Release 4.1 での基本的な動作を指定する各パラメータ サブカテゴリを設定します。T2 タグと T3 タグの両方を選択した場合は、*両方のタグ* モデルに適用される設定オプションだけが使用できます。設定グループのすべてのパラメータを設定したら、各グループ内の [Apply] ボタンをクリックし、選択したタグに設定を適用します。また、すべてのグループの設定が完了した後で変更を適用することもできます（図 6-26 の下部にある [Apply Multiple Configuration] オプションを使用します）。選択したすべてのパラメータが選択したすべての資産タグに適用され、設定されている他の値を上書きします。

a. 一般的なパラメータ：

- Channel Selection：タグのチャネルは、重複しない標準の 802.11b チャネル セット（規制区域によって異なりますが、通常はチャネル 1、6、および 11）に設定することをお勧めします。
- LED Indication：ほとんどの場合、タグが通信インターフェイスを使用していることを視覚的な表示で確認できると便利です。セキュリティまたは秘匿のために光を避ける必要がある用途など、そのような表示が望ましくない理由がある場合は、LED を無効にすることができます。
- Transmission Interval When Not In Motion：資産タグの用途に適したタグ送信間隔を秒単位またはミリ秒単位で設定します。通常、このパラメータでは、固定タグの送信頻度を移動タグより低く設定します。移動送信間隔は [Motion Sensor] カテゴリで設定します。

b. 送信パラメータ：

- Message repetitions：AeroScout タグの標準動作では、定義されたすべてのチャネルで単一のマルチキャスト メッセージを送信します。このパラメータでは、送信メッセージのチャネルごとの反復回数を指定します。一般には、このパラメータをデフォルト値の 1 から 3 に増やすことが推奨されます。これにより、タグ送信データの損失によって RSSI 読み取りが失われる

ことを防止できます。RSSI 読み取りデータが失われると、特にタグ送信が輻輳や干渉によって妨害またはドロップされる可能性が高い環境では、ロケーション確度が低下する原因になることが確認されています。メッセージ反復回数を過度に大きくしないでください。この値を 3 より大きくすることが必要な状況はほとんどありません。大部分の環境では、メッセージ反復回数を 3 に設定することで、きわめて良好な動作状態が得られます。通常は、このパラメータを 5 より大きくする必要はないと考えられます。

- Message Repetitions Interval：同一チャネルでメッセージを反復送信するときの遅延時間を 128、256、512（ミリ秒）のいずれかに設定します。デフォルト値は 512 ミリ秒です。
- Transmission Power（dBm）: AeroScout 資産タグの T2 モデルの場合、送信電力のデフォルト値は、通常、+18dBm です。ロケーション認識 Cisco UWN は、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するタグの送信電力を識別できます。
- Data Rate : 2 Mbps のデータ レートは T3 タグにのみ指定できます。資産タグのメッセージ ペイロードおよびフレーム サイズはきわめて小規模ですが、送信速度を速くすると、T3 タグのペイロード送信が高速化するため、解放されたチャネルを他のステーションがより早く使用できるようになります。また、各フレームの送信時間が短縮されるため、バッテリの消費も低下します。
- Data Frame Format：このパラメータは、デフォルト値の [IBSS] から [CCX] に変更する必要があります。
- Destination Address : リリース 4.1 以降のリリースでは、このパラメータに 01:40:96:00:00:03 を指定する必要があります。

c. データ送信モード パラメータ：

- Normal Tag Transmission (without additional message) : 別のパラメータを選択する正当な理由がある場合を除き、このパラメータを選択してください。そのような理由としては、資産タグで使用しているロケーション クライアントがタグ ペイロードの一部として送信された追加の保存済みメッセージをタグ上で処理できることや、テレメトリをカスタム統合ホスト周辺機器に内蔵されたセンサーから直接読み取ることができる AeroScout T2 テレメトリ タグを使用していることなどが考えられます。

d. 補助的設定：

- CCX Options：[Transmit Out of Range Chokepoint Group] を有効にする必要があります。

e. Call Buttons – Primary：これらのオプションは、リリース 4.1 でコール ボタン シグナリング（パニック ボタン アラート）を使用する場合に設定します。

- Short Clicks（2 秒未満のボタン押下）：
  - [Enable Short Clicks] は必ずオンにします。
  - Number of Short Clicks：1
  - Tag Reaction Parameters：Send Standard Tag Transmission
  - Message Repetition：1
- Long Clicks（2 秒以上のボタン押下）：
  - [Enable Long Clicks] は必ずオンにします。
  - Number of Long Clicks：1
  - Tag Reaction Parameters：Send Standard Tag Transmission

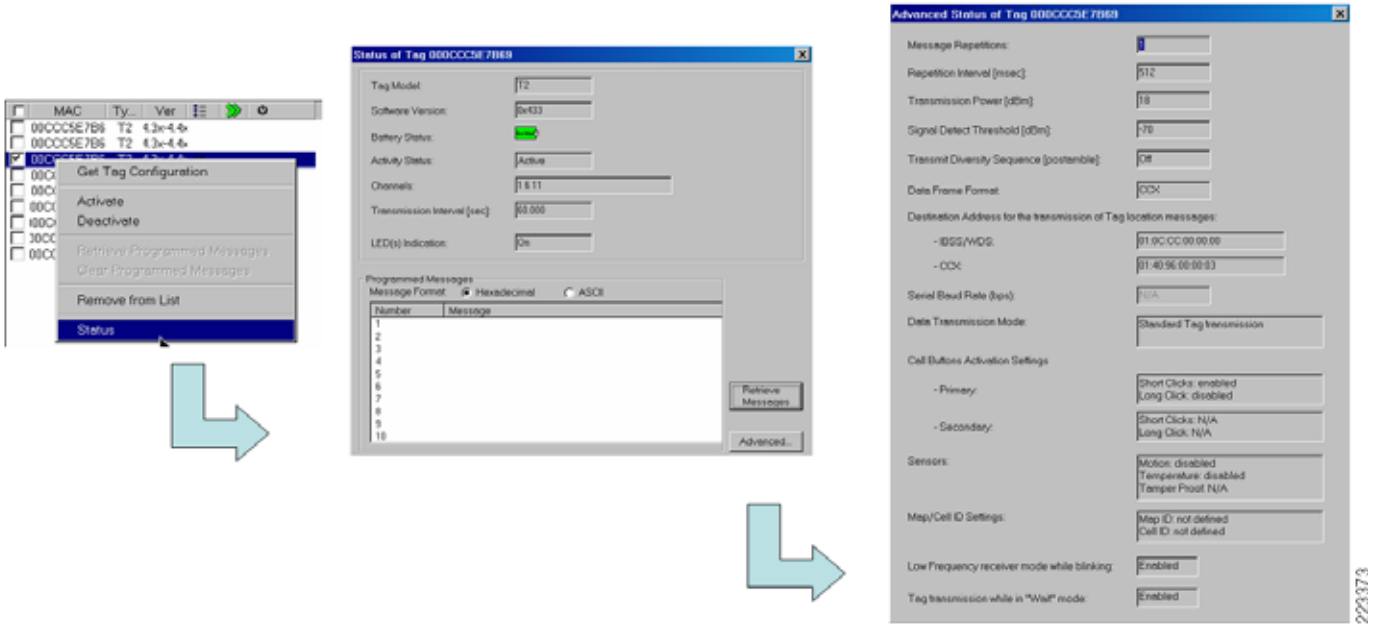
f. Call Buttons - Secondary :「Call Buttons – Primary」の欄と同じオプションがあります。ただし、これらのオプションは T3 資産タグを使用している場合のみ設定可能です。

g. Sensors :

- Motion：これらのオプションを使用すると、必要に応じて内蔵動作センサーを有効にできます。
- Temperature：これらのオプションを使用すると、必要に応じて内蔵温度センサーを有効にできます。内蔵温度センサーは、v4.3x ファームウェアを搭載した T2 タグではサポートされていません。
- Tamper：このオプションは T3 タグでのみオンにできます。このオプションをオンにすると、Cisco UWN にタグ改ざん通知が送信されます。

7. 場合によっては、AeroScout 資産タグの既存の設定が問題となり、確認が必要となることがあります。この確認は Tag Manager v3.04 で簡単に行うことができます。検出されたタグを右クリックし、ポップアップ メニューの [Status] をクリックします。基本的なタグ設定パラメータのリストが表示され、さらに [Advanced Configuration] を選択すると、図 6-27 に示す詳細が表示されます。

図 6-27　1 つのタグの設定の取得



上記の設定手順は、AeroScout タグを Cisco UWN Release 4.1 で使用できるように設定し起動するために必要な手順の概要を示したものです。詳しい手順および Tag Manager の他の役に立つ設定オプションについては、『*AeroScout Tag Manager v3.0 User's Guide*』を参照してください。

タグ テレメトリおよび通知に関する考慮事項

リリース 4.1 以降、ロケーション認識 Cisco UWN は Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するタグから送信されるタグ テレメトリおよび高優先順位の通知を認識するようになったため、これらの通知がロケーション認識 Cisco UWN に送信されることがあります。この情報は、WLAN コントローラから Cisco Wireless Location Appliance に Location Control Protocol（LOCP）を使用して送信されます。このプロトコルについては「Cisco Location Control Protocol（LOCP）」（P.3-36）を参照してください。

この項では、Cisco UWN Release 4.1 のテレメトリ機能および高優先順位の通知機能に依存するソリューションを設計する際に留意すべきベスト プラクティスの推奨事項およびその他の情報を提供します。

タグ テレメトリの展開

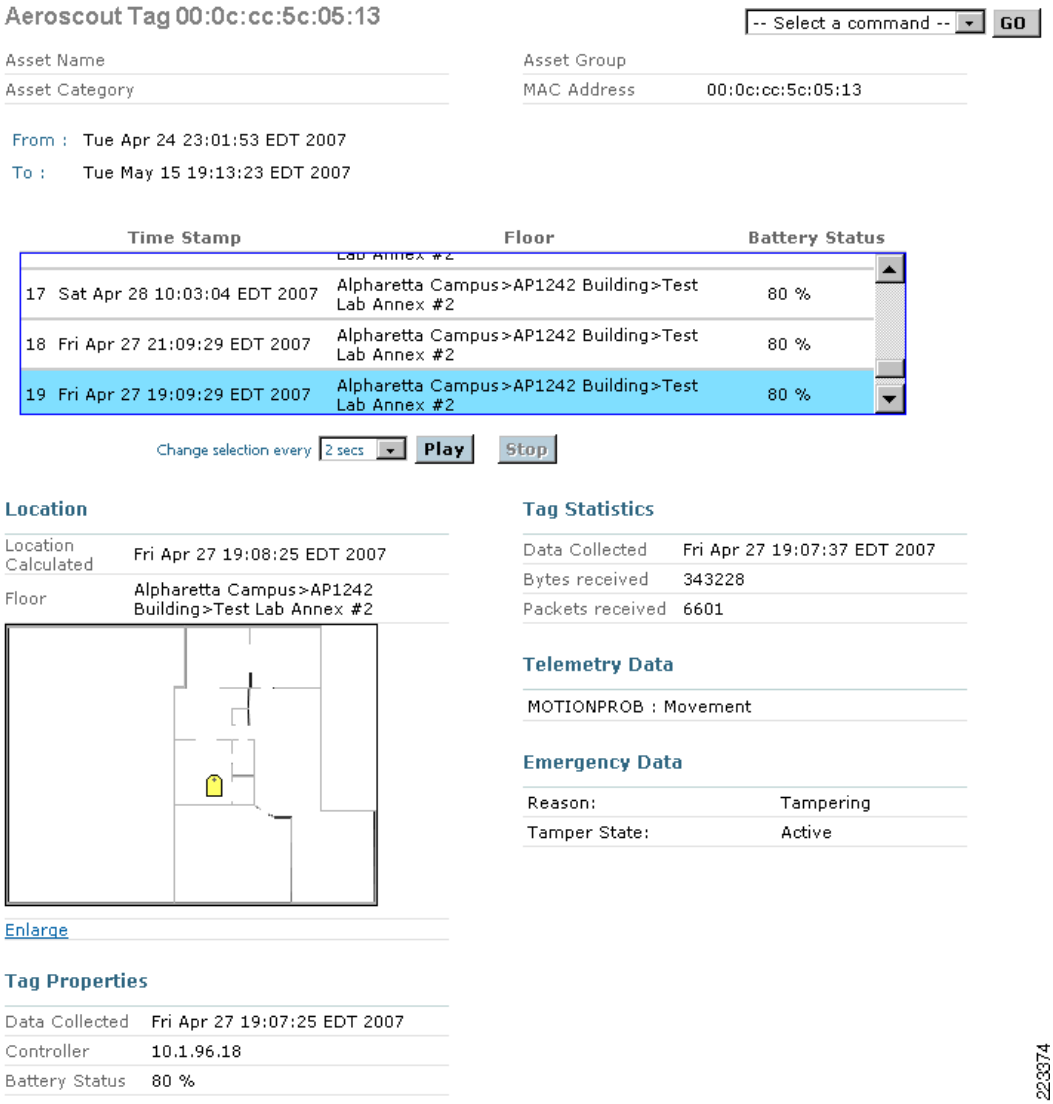
タグ ベンダーが提供する、Compatible Extensions Wi-Fi Tag 仕様に準拠したアクティブ RFID タグは、内蔵センサーまたはタグを取り付ける資産に搭載されたセンサーからテレメトリ データを受け取る機能を備えている場合があります。このようなアクティブ RFID タグは、適切に設定することにより、一定の送信間隔で、またはチョークポイント トリガーのスティミュレーション ゾーンに入ったときに Cisco UWN に送信されるタグ送信データの一部として、このテレメトリ データを渡すことができます。

たとえば、フォークリフトの燃料計に接続された資産タグであれば、Cisco UWN を介し、燃料の残量を示すテレメトリを Location Appliance およびそのロケーション クライアント（WCS やサードパーティ製ロケーション クライアントなど）に渡すことができます。このようなテレメトリ機能を実行する資産タグの能力は資産タグの製造元によって異なり、通常はタグと取り付け先の資産に搭載されたセンサーとの適切なレベルの統合および物理的な接続を必要とします。資産タグには、センサーを内蔵し、取り付け先の資産の周囲の環境条件（温度や湿度など）を資産に組み込まれたセンサーに頼ることなく測定できるものもあります。

内蔵タグ センサーは、資産タグおよび取り付け先の資産に影響する環境条件が主要な問題となるような場合に適しています。また、温度センサーを内蔵した資産タグは、取り付け先の資産の保管温度が推奨範囲から外れていないかどうかを検出するのに適しています。不適切な使用に起因する内部状態によって資産が破損するおそれがあり、速やかに対処しなければ多額の費用が発生することをシステム管理者に通報することが目的である場合など、資産に組み込まれたセンサーを利用する方が適していることもあります。その好例は、多額の修理費が発生する可能性のある潤滑油の不足を表示するエンジンです。

「LOCP を使用する資産タグ テレメトリ」（P.3-38）で説明したとおり、Cisco UWN Release 4.1 では、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するタグが送信するタグ テレメトリがすべて WLAN コントローラに集約され、Cisco Wireless Location Appliance に渡されます。リリース 4.1 では、その後、LOCP がポーリング メカニズムを使用してタグ テレメトリを収集します。そのタイミングは、資産タグの RSSI 情報の収集に使用される従来の SNMP ポーリング メカニズムに関連します。Location Appliance は、データベースに保存された、各資産タグのテレメトリ情報を各タグの MAC アドレスのテレメトリ情報が既に含まれている最近応答した WLAN コントローラから受け取ったテレメトリ情報で更新します。Location Appliance でタグ履歴情報のアーカイブを有効にした場合は、タグ情報にタグ テレメトリ情報も含まれます（図 6-28 を参照）。

図 6-28　タグ テレメトリおよび「緊急」データのアーカイブ再生



アクティブ RFID タグには、デフォルト設定で送信間隔ごとに 1 つのチャネルにつき 1 回しかタグ送信データを送信しないものがあります。この設定は、場合によってはタグのバッテリ寿命を最適化する効果がありますが、特に RF ノイズの多い環境や輻輳した環境では、各チャネルにつき 1 回しか送信されない送信データが予想される数のアクセス ポイントで必ず検出されるとは限りません。そのため、RSSI 読み取りデータが失われ、位置特定が不正確になる可能性があります。

したがって、そうした環境では、各送信間隔で 1 つのチャネルにつき送信を反復するようにタグを設定することをお勧めします。これにより、タグの検出および位置特定の確度だけでなくタグ テレメトリの信頼性も向上します。タグ ベンダーの設定ソフトウェアを使用し、タグ送信回数を各送信間隔につきチャネルあたり 3 回（最大 5 回）に設定することをお勧めします。

LOCP によるテレメトリの収集が最近の有線ネットワークおよび無線ネットワークに負荷をもたらすことはまずありませんが、ネットワーク設計者は、それぞれのネットワークで予想されるトラフィックの特性を把握しておくことが望まれます。次に、このドキュメントのために実施した LOCP テレメトリ テストによって明らかになったトラフィックおよびフレーム サイズに関する情報を示します。

- *エコー要求* : Echo Interval パラメータ（[Location Servers] > [Advanced] > [LOCP Parameters]）の設定に基づいて Location Appliance から定義された各 WLAN コントローラに定期的に送信されます。LOCP エコー要求イーサネット フレームは長さが 100 バイトで、TCP 宛先ポート 16113 に送信されます。
- *エコー応答* : エコー要求（上記を参照）への応答として各 WLAN コントローラから定期的に送信されます。エコー要求と同様、LOCP エコー応答イーサネット フレームも長さは 100 バイトです。
- *情報要求* : 情報を要求するために、Location Appliance から各 WLAN コントローラに定期的に送信されます。LOCP 情報要求イーサネット フレームは長さが 106 バイトで、TCP 宛先ポート 16113 に送信されます。LOCP 情報要求は、リリース 4.1 で LOCP ポーリングを実行するために使用される主要なメカニズムです。
- *情報応答* : 受信した LOCP 情報要求フレーム（LOCP ポーリング）への応答として、各 WLAN コントローラから定期的に送信されます。タグを検出していないコントローラの LOCP 情報要求イーサネット フレームの基本的なサイズは 113 バイトです。フレーム サイズはタグが 1 つ検出されると 144 バイトに増え、タグが 2 つ検出されると 175 バイトに増えます（これらのフレーム サイズにはテレメトリ データは含まれていません）。フレーム サイズは、コントローラのデータベースで現在アクティブなタグの数と収集されたテレメトリの量に応じて増加します。結合されたタグ ペイロードのフラグメンテーションおよび再アセンブリのサポートは LOCP に含まれています。

Location Appliance とそれに定義された WLAN コントローラの間で LOCP が適切に動作するためには、ポート 16113 がファイアウォールなどのセキュリティ デバイスによってブロックされないようにする必要があります。

リリース 4.1 によるタグ テレメトリの報告および収集を利用するソリューションを設計するときには、以下の点に留意してください。

1. *テレメトリ タイミング* : リリース 4.1 では、テレメトリが WLAN コントローラによってタグごとに収集され、定期的な LOCP ポーリング サイクル中にのみ Location Appliance へ渡されるため、リリース 4.1 のユーザはタグ テレメトリの受信に頼ることなく本質的なリアルタイム性を確保することができます。当然ながら、タグがテレメトリ情報を送信してから、その情報が Location Appliance データベースで更新され、ロケーション クライアントが使用できるようになるまでには遅延が生じると予想されます。
2. *ノースバウンド非同期通知* : ロケーション認識 Cisco UWN の リリース 4.1 では、Location Appliance はタグから受信したテレメトリについて非同期ノースバウンド通知（形式は、電子メール、SNMP メッセージ、SOAP メッセージ、UDP-Syslog メッセージのいずれか）を発行しません。そのため、これらの形式のノースバウンド通知に依存する外部アプリケーション（ページング システム、テキスト メッセージング、エンタープライズ管理コンソールなど）は、サードパーティ製のロケーション クライアントなど、タグ テレメトリを認識できる代替ソースから通知を受け取る必要があります。

ただし、バッテリ テレメトリは例外です。バッテリ テレメトリについては、Location Appliance が Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するタグのバッテリ残量に基づいてノースバウンド非同期通知をトリガーします。これらの通知は、以下のトリガー条件の定義に従って生成されます。

- バッテリ レベルが低：報告されたバッテリ残量が 30%
- バッテリ レベルが中：バッテリ残量が 30 ～ 75%
- バッテリ レベルが正常：バッテリ残量が 75% 超

タグ高優先順位通知の展開

Cisco UWN のリリース 4.1 では、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠した資産タグがロケーション認識 Cisco UWN に優先順位の高いベンダー固有の通知を送信できるようになりました。この情報はオンデマンドで送信されるタグ送信データの一部として送信され、LOCP によって WLAN

コントローラから Cisco Wireless Location Appliance に渡されます。留意すべき点は、高優先順位タイプのイベントが発生したときにタグが送信するタグ メッセージの形式が、高優先順位イベントの種類を示す追加情報が含まれることを除き、タグ送信間隔において送信される標準のタグ マルチキャスト送信データとよく似ていることです。

WLAN コントローラが RF で受信するタグ通知に含まれる情報が LOCP 情報通知の形式で Location Appliance に（最小限の遅延で）渡されることに注意する必要があります。そのため、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグのコール ボタンが押されたときなどには、WLAN コントローラの登録アクセス ポイントがタグ通知を受信した後すぐにコントローラから Location Appliance に LOCP 情報通知が送信されます。Location Appliance が LOCP 情報通知を受信すると、更新されたコール ボタン ステータスが Location Appliance データベースに反映され（「パニック ボタンの押下」など）、ロケーション クライアントによる使用が可能になります。Location Appliance でタグ履歴情報のアーカイブを有効にしている場合は、タグ情報とともにタグ「緊急」情報もアーカイブされます（図 6-28 を参照）。

LOCP 情報通知イーサネット フレームの基本的なサイズは約 130 バイトです。フレーム サイズは、改ざん情報やベンダー固有のデータなど、フレームに含まれる追加情報によって増加することがあります。リリース 4.1 では、LOCP 情報通知は WLAN コントローラによって収集されません。WLAN コントローラは、その登録された*各アクセス ポイント*を介して受信した*個々のタグ*からの高優先順位通知（反復送信された高優先順位通知を含む）について LOCP 情報通知フレームを Location Appliance に送信します。

数学的に表現すると、タグから送信される 1 つの通知イベントについて WLAN コントローラから Location Appliance に送信されると予想される LOCP 情報通知の総数は、次のように計算できます。

$$\textit{LOCP 情報通知}_{TOTAL} = \textit{検出する AP}_{TOTAL} * \textit{高優先順位通知の送信反復回数}_{PER\ CHANNEL}$$

$\textit{高優先順位通知}_{PER\ CHANNEL}$ は、タグが 1 つの RF チャネルで送信する高優先順位通知の総数を表します。高優先順位通知のチャネルあたりの反復回数とチャネルあたりのタグ メッセージ通知の標準設定を混同しないように注意してください。後者は、タグ送信間隔ごとに定期的に送信されるタグ送信データに適用されます。この計算では、タグから反復送信されるすべての通知が $\textit{検出する AP}_{TOTAL}$ に含まれるすべてのアクセス ポイントによって検出され、干渉、コンテンション、またはその他の RF 異常によってドロップされる通知がないことを前提としているため、$\textit{LOCP 情報通知}_{TOTAL}$ の最大値が算出されることにも注意してください。

この式を使用すると、次のリリース 4.1 環境において Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグのコール ボタンが 1 回押された場合に生成される LOCP 情報通知の予想数を計算できます。

- 2 つの WLAN コントローラ
- 各コントローラに 3 つのアクセス ポイントが登録（計 6 箇所の検出アクセス ポイント）
- コール ボタンが 1 回押されるたびにタグがチャネル 1、6、および 11 のそれぞれで 1 つの通知を送信

この情報を上記の式に代入すると、6 * 1 となり、この例で WLAN コントローラから Location Appliance に送信される LOCP 情報通知の総数は 6 であることがわかります。この例では両方の WLAN コントローラが LOCP 通知を送信しますが、この環境では、WLAN コントローラの数は Location Appliance に送信される LOCP 通知の数には無関係であることに注意してください。この例では、それぞれ 2 つのアクセス ポイントが登録された 3 つの WLAN コントローラを代入することもでき、その場合も $\textit{LOCP 情報通知}_{TOTAL}$ から同じ値が得られます。コントローラから Location Appliance に送信される LOCP 通知の数に関係するのは、高優先順位の通知情報が含まれるタグ マルチキャスト送信データを検出するアクセス ポイントの数です。

Location Appliance とそれに定義された WLAN コントローラの間で LOCP が適切に動作するためには、ポート 16113 がファイアウォールなどのセキュリティ デバイスによってブロックされないようにする必要があります。

タグのテレメトリおよび通知の設定

タグ テレメトリおよび通知のサポートは Cisco Compatible Extensions Wi-Fi Tag 仕様の基本コンポーネントですが、タグ ベンダーはそれぞれ固有の GUI または CLI ベースのタグ ソフトウェアを使用し、自社製品におけるこれらの機能のサポートを有効または無効にしたり、さまざまなカスタマイズを行ったりしています。このドキュメントでは、これまで AeroScout タグの設定について限られた情報しか提供していませんが、外部テレメトリ センサーおよび資産タグの設定に関する詳細は、資産タグ ベンダー提供の文書から入手でき、このドキュメントの対象範囲には含まれません。

そうした詳細情報が必要な場合は、以下の情報源を参照してください。

- AeroScout *T2 Tag User Guide*
- AeroScout *Tag Manager User Guide version 3.0*
- http://www.aeroscout.com または AeroScout の顧客サービスおよび技術サポート チーム

他のベンダーが提供する、Cisco Compatible Extensions Wi-Fi Tag 仕様と互換性の資産タグについては、直接ベンダーに問い合わせることをお勧めします。次に、2 つのベンダーを紹介します。

- InnerWireless（旧 PanGo Networks）http://www.innerwireless.com
- WhereNet http://www.wherenet.com

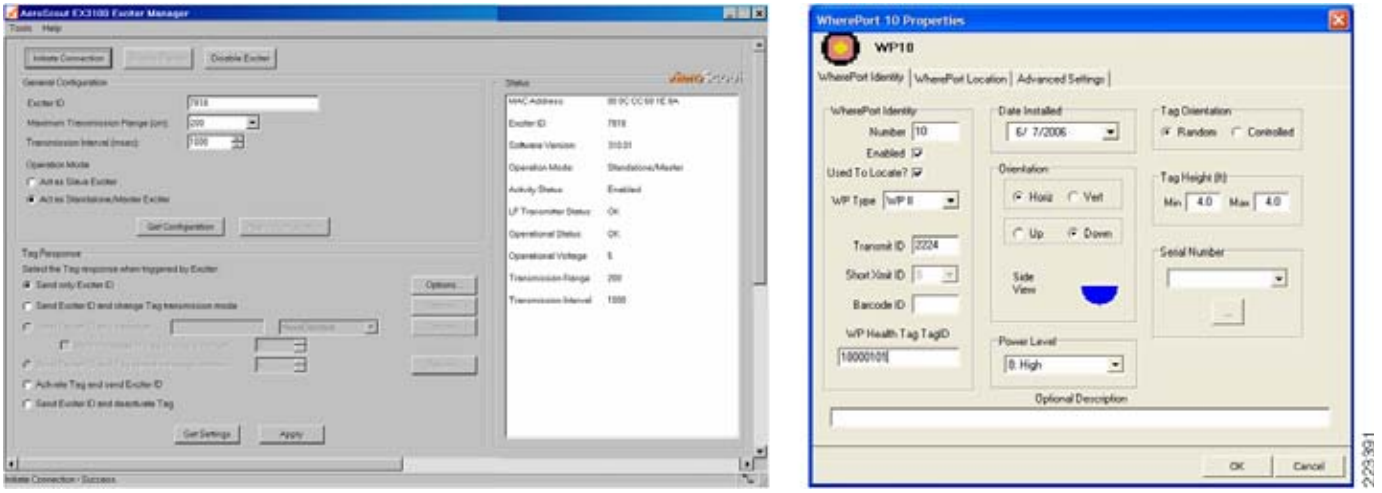
チョークポイントに関する考慮事項

チョークポイント トリガーの設定

Cisco UWN でチョークポイント トリガーを使用するためには、チョークポイント トリガーをベンダー提供のソフトウェア ユーティリティで適切に設定し、WCS に定義し、フロア マップに配置して、更新されたネットワーク設計の一部として Location Appliance と同期する必要があります。これらの準備が完了すると、Location Appliance は Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠した資産タグが特定のチョークポイント トリガー MAC アドレスによってスティミュレートされたことを認識し、資産タグをローカライズできます。これにより、ロケーション クライアントは資産タグの位置をチョークポイント トリガーの MAC アドレスに対応するチョークポイント アイコンに表示できます。

ベンダーが提供するユーティリティでは、送信範囲、IP アドレス、送信間隔、送信反復回数など、チョークポイント トリガーに関するさまざまなパラメータを設定します。IP アドレッシング可能でない AeroScout EX-3100 シリーズの Exciter では、AeroScout Exciter Manager スタンドアロン ソフトウェア ユーティリティを使用する必要があります（図 6-29 の左側）。WhereNet WherePort チョークポイント トリガーでは、WhereNet System Builder（図 6-29 の右側）と WhereNet WhereWand を使用します。

図 6-29　各ベンダーの設定ユーティリティ



各ベンダーがそれぞれのチョークポイント トリガーの設定に必要なソフトウェア ツール セットを提供しています。それらのソフトウェア設定ツールには、ベンダー間の相互運用性はありません（たとえば、AeroScout ソフトウェア設定ツールで WhereNet チョークポイント トリガーを設定することはできず、その逆のこともできません）。

基本的に、各ベンダーのチョークポイント トリガー デバイスの個別設定は、このホワイト ペーパーの対象範囲に含まれません。ただし、このドキュメントでは、設計上の問題を解決するうえで特に重要なチョークポイント トリガー設定パラメータについて説明します。このドキュメントの各項で、そのようなパラメータを必要に応じて取り上げます。ただし、各ベンダーのチョークポイント トリガーの具体的な設定に関する詳細な情報については、以下に挙げる各ベンダーのマニュアルを参照してください。

AeroScout Corporation 提供のマニュアル：

- AeroScout EX-3100 Exciters：
  - 『*AeroScout Exciter EX-3100 User Manual*』
  - 『*AeroScout EX-3100 Exciter Manager User's Manual*』
- AeroScout EX-3200 Exciters：
  - 『*AeroScout EX-3200 User Guide*』
- AeroScout EX-2000 Exciters：
  - 『*AeroScout Exciter EX-2000 User Guide*』

以下のリファレンス マニュアルは、AeroScout System Manager または AeroScout Network Exciter Manager（ANEM）を使用して AeroScout EX-2000 と EX-3200 Exciter を設定する場合に参照することをお勧めします。AeroScout Network Exciter Manager は、AeroScout Exciters および Cisco UWN のユーザ向けのスタンドアロン Exciter ソフトウェア設定ユーティリティです。

  - 『*AeroScout Engine Version 3.2 User's Guide*』
  - 『*AeroScout Network Exciter Manager (ANEM) User's Guide*』

WhereNet WherePort チョークポイント トリガーの技術マニュアルや WherePorts の設定に必要なソフトウェアおよびハードウェアは、WhereNet の代理店を通じて WhereNet Corporation（http://www.wherenet.com）から入手できます。

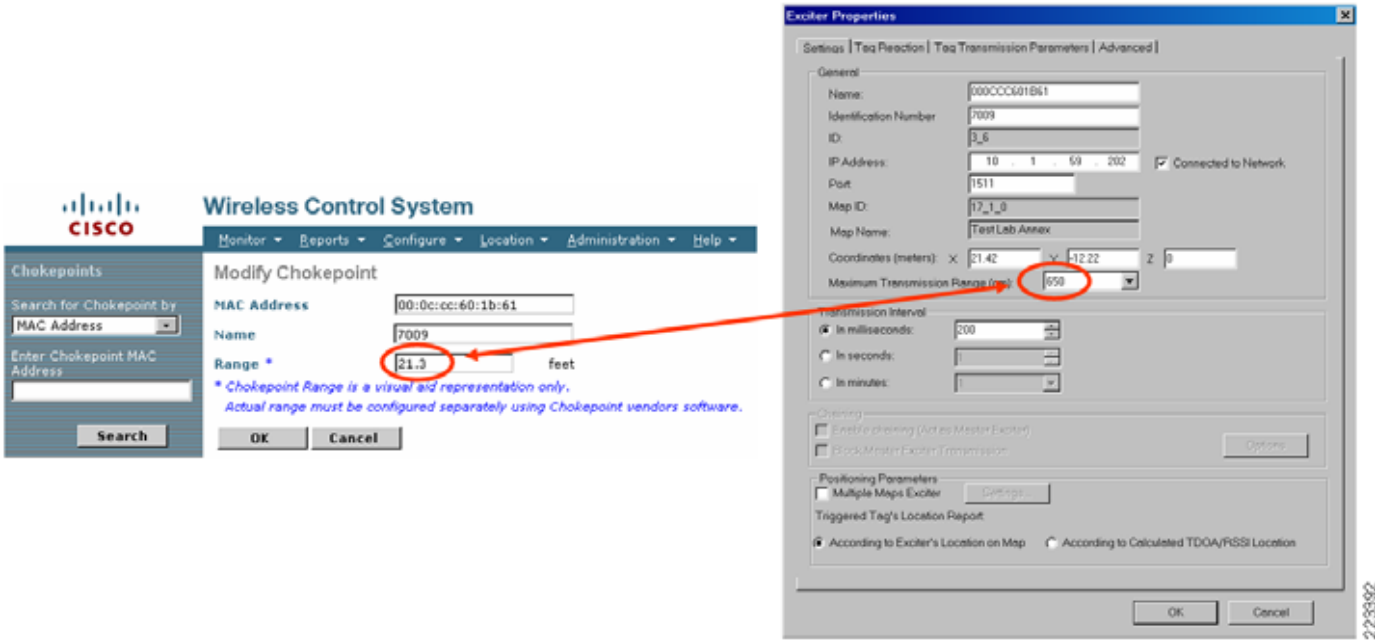
Cisco UWN へのチョークポイント トリガーの定義

前述のとおり、ベンダー提供のツールを使用してチョークポイント トリガーを個別に設定したら、それを WCS に定義し、適切なフロア マップに配置し、更新されたネットワーク設計の一部として Location Appliance と同期する必要があります。これらの準備を行って初めてチョークポイント トリガーで Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠した資産タグを追跡することができます。

互換性のあるチョークポイント トリガーを WCS および Location Appliance に定義する手順の詳細については、http://www.cisco.com/en/US/docs/wireless/location/2700/3.0/configuration/guide/lacg_ch6.html#wp1058654 を参照してください。

チョークポイント トリガーを定義するときには、ベンダーの設定プログラムと WCS の両方で範囲を指定する必要があることに注意してください（図 6-30 を参照）。ただし、チョークポイント トリガーの送信範囲を実際に設定するのは、WCS で設定する範囲ではなくベンダーの設定プログラムで指定する範囲設定パラメータです。WCS でチョークポイント トリガーの範囲として指定する値は、WCS フロア マップの各チョークポイント アイコンの周囲に表示される灰色の同心円リングのサイズを設定するだけです。これらの同心円リングは、チョークポイント トリガーの範囲を視覚的にわかりやすく示すものにすぎません。

図 6-30　WCS とベンダーの範囲パラメータの比較



これらの同心円リングは「特殊な」領域を表すわけではないことに注意してください。たとえば、タグのローカライズにチョークポイント ロケーションではなく RF フィンガープリントを使用すると、タグはフロア マップ上の Location Appliance が正しいと見なす任意の位置（灰色の同心円リングの内側を含む）に配置されることがあります。

[Location] > [Location Servers] > [Advanced] > [Location Parameters] メニュー画面には、図 6-31 に示すとおり、チョークポイントの使用に関するパラメータが他に 2 つあります。

図 6-31　高度なチョークポイント ロケーション パラメータ

- *Chokepoint Usage* : Location Appliance がチョークポイント ロケーション手法を使用してタグをローカライズするためには、このチェックボックス（図 6-31 の赤い線で囲まれた部分）をオンにする必要があります。タグのローカライズは、Location Appliance がタグ付きの資産がチョークポイント トリガーによってスティミュレートされたことを示す LOCP 測定通知を受信したときに行われます。Cisco Location Appliance およびロケーション認識 Cisco UWN に含まれるチョークポイント機能に関しては、これらの手法は Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグでのみ使用されます。このパラメータをオフにすると、Location Appliance は常に標準のメカニズムである RSSI ベースの RF フィンガープリントを使用してタグの位置を計算します。
- *Chokepoint Out of Range Timeout* : このパラメータ（図 6-31 の青い線で囲まれた部分）は、チョークポイント ロケーション手法によってローカライズされる資産タグから最後に受け取った「範囲内」報告からの経過時間を示すタイマーを指定します。このタイマーによって、チョークポイントの範囲外タイムアウトが経過すると、チョークポイント トリガーの範囲内にあることを示すフレームを送信しなくなったタグがアクティブ ロケーション データベースの該当するチョークポイントから削除されます。これらのタグは、チョークポイントの範囲から出たと見なされ、再び標準の RF フィンガープリント手法によってローカライズされます。

チョークポイント トリガーのトラフィックに関する考慮事項

Cisco UWN Release 4.1 では、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するタグが統一された方法でチョークポイント トリガーに近接している（またはその範囲から出た）ことを UWN に通知できるようになりました。この情報は、アクセス ポイントが受信し、登録されたコントローラに転送された後、「Cisco Location Control Protocol（LOCP）」（P.3-36）で説明した LOCP 測定によって Location Appliance に渡されます。

チョークポイント トリガーから受信したスティミュレーションへの応答として送信される 802.11 タグ マルチキャスト フレームの長さは、約 63 バイトです。これは 1 つのチョークポイント MAC アドレスだけのサイズであり、チョークポイントの履歴情報は含まれていません。フレームの長さは、通過したチョークポイントの履歴リストを含めることによって増加することがあり、ベンダー固有の情報が含まれると 63 バイトを超える場合もあります。たとえば、AeroScout T2 タグを使用したラボ テストでは、チョークポイント トリガーに近づいたときに送信されるタグ マルチキャスト フレームの平均的な長さ

が約 71 バイトとなり、同様のタグが通常の定期送信で送信するマルチキャスト フレーム（56 バイト）よりわずかに大きくなりました。この 71 バイトという長さは予想値の 63 バイトより大きく、詳しく調べたところ、ベンダー固有の情報が 8 バイト含まれていることがわかりました。

Cisco Compatible Extensions Wi-Fi Tag 仕様には、資産タグが通過したチョークポイントの履歴情報を Cisco UWN に送信する機能が定義されています。そのため、保存される履歴エントリの数によっては、フレーム サイズが通過したチョークポイント トリガーあたり約 10 バイト増える可能性があります。LOCP 測定通知イーサネット フレームの基本的なサイズは約 160 バイトです。フレーム サイズは、チョークポイントの履歴情報などの追加情報が含められることによって増加することがあります。

リリース 4.1 では、LOCP 測定通知は WLAN コントローラによって収集されません。WLAN コントローラは、登録されている各アクセス ポイントが受信した、タグがチョークポイント トリガーによってスティミュレートされたことを示すタグ マルチキャスト送信データごとに、LOCP 測定通知フレームを Location Appliance に送信します。したがって、タグがチョークポイント トリガーによってスティミュレートされたことを示す 1 つのタグ マルチキャスト フレームについて 1 つ以上の WLAN コントローラが生成する LOCP 測定通知の数は、以下の条件によって決まります。

- タグの範囲内にあり、タグのチョークポイント関連の送信データを検出した、登録されているアクセス ポイントの数
- 設定された各 802.11 チャネルにおいてチョークポイント トリガーによるスティミュレーションへの応答としてタグが送信するマルチキャスト フレームの数

これを式で表すと次のようになります。

$$LOCP\ 測定通知_{CHOKEPOINT} = 検出する\ AP_{TOTAL} * 802.11\ 反復回数_{PER\ CHANNEL}$$

以下の点に注意してください。

1. この式によって、1 つのチョークポイント スティミュレーション イベントに応答する 1 つのタグが送信する *LOCP 測定通知*の数が算出されます。
2. チョークポイント トリガーは、デフォルトでは磁気シグナリング媒体を介して複数のスティミュレーション パケットを送信します。その結果、複数のスティミュレーション イベントが生成される可能性があります。この点に大きく影響する条件として、チョークポイント スティミュレーション ゾーン内の経過時間などがあります。
3. この計算では、タグから送信されるすべてのフレームが *検出する* AP_{TOTAL} に指定された数のアクセス ポイントによって検出される（干渉、コンテンション、またはその他の RF 異常によってドロップされるフレームがない）ことを前提としているため、*LOCP 測定通知*の最大値が算出されます。

以下の条件はほとんどのケースに該当します。

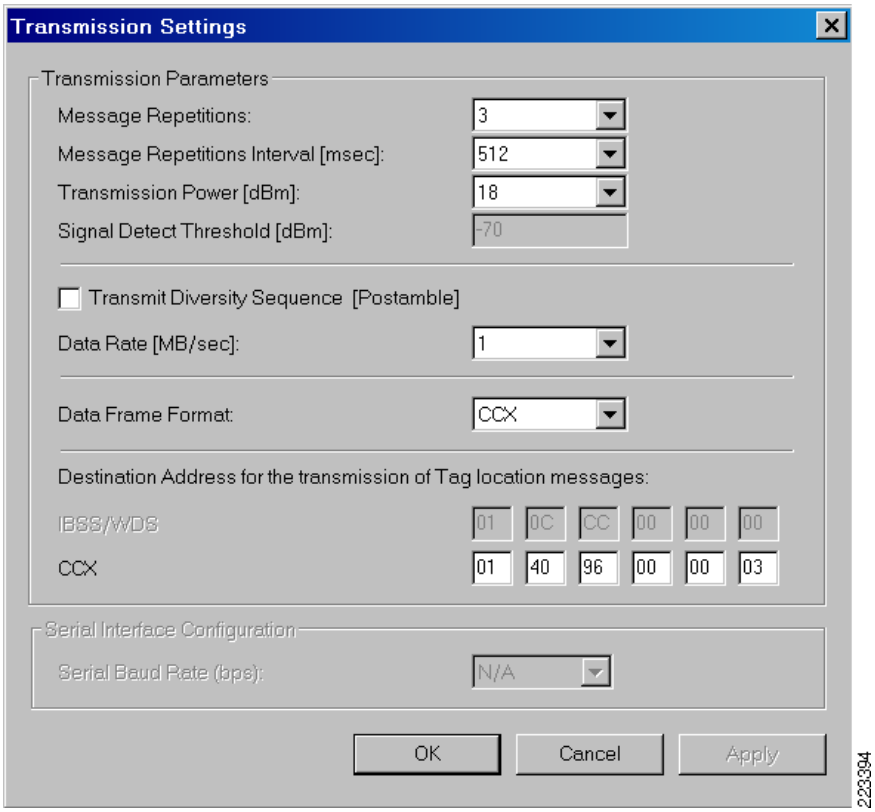
- チョークポイントは、周囲のアクセス ポイントの間隔が「アクセス ポイントの配置」（P.5-5）で説明した要件を満たす領域に展開されます。
- アクセス ポイントとタグは、重複しない 2.4 GHz チャネル（たとえば、米国ではチャネル 1（2412 GHz）、6（2437 GHz）、および 11（2462 GHz））で動作するように設定されます。

ほとんどのチョークポイント トリガーでは、タグがチョークポイント トリガーによってスティミュレートされたことを示すタグ マルチキャスト送信データのチャネルあたりの反復送信回数がデフォルトで 1 となります。*LOCP 測定通知*が生成されるためには、スティミュレートするチョークポイント トリガーの MAC アドレスが含まれるタグ マルチキャスト送信フレームが 1 つ受信されるだけで十分です。そのため、チョークポイント関連のタグ送信のチャネルあたりの反復回数は、通常はデフォルト値のままで十分です。このタグ送信は、通常、3 つの 2.4 GHz チャネルで反復されるため、反復回数の値を大きくしなくても、タグ送信データが複数のアクセス ポイントで受信されるからです。ただし、干渉や輻輳の発生頻度がきわめて高くなる可能性がある環境など、反復回数の値を少し高くした方がよい場合もあります。タグ付き資産がチョークポイントを高速で通過する場合や、チョークポイント トリガーから離れたフリンジ領域を通過する場合などは、このパラメータを使用してスティミュレーション

の確実性を高めることができます。ただし、いずれの場合も、タグの数が多い環境では、このパラメータがスティミュレートされたタグあたりのトラフィック増加量に影響するため、値を大きくするときには慎重に検討する必要があります。

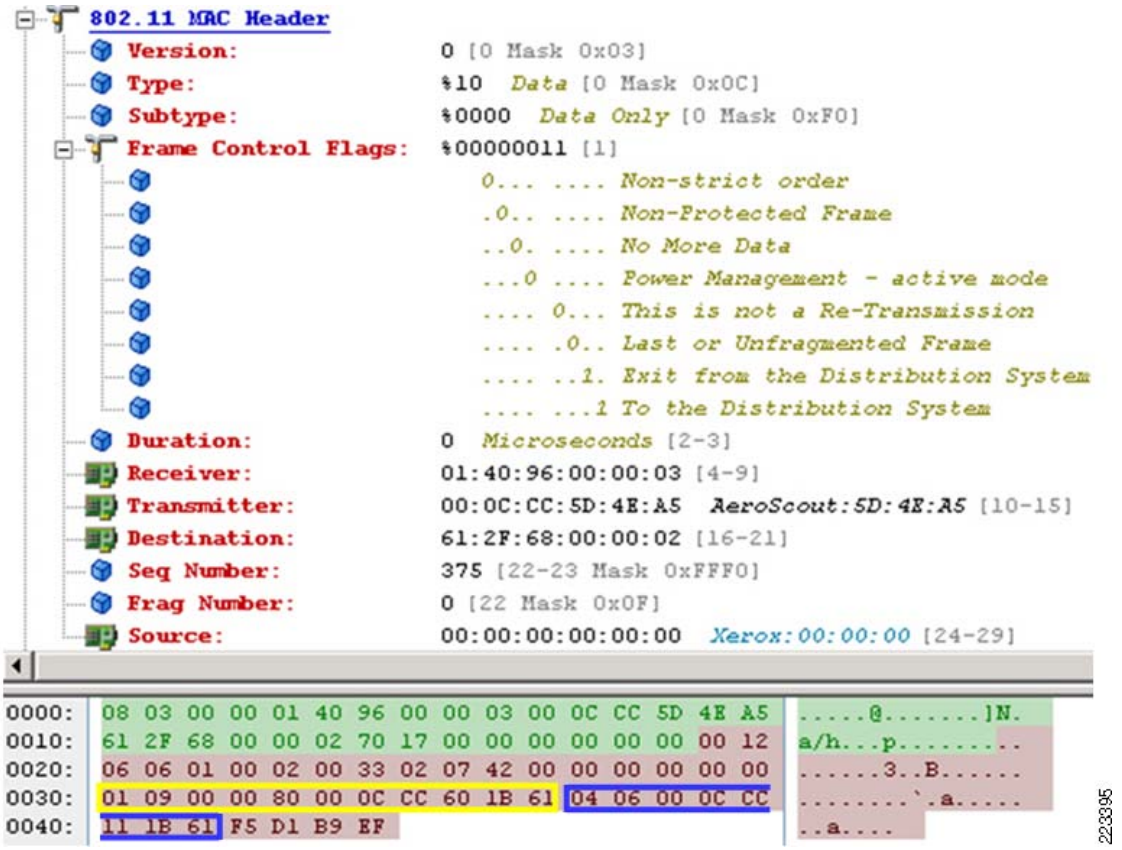
ここで注意しなければならないのは、チョークポイント スティミュレーションへの応答として送信されるタグ マルチキャスト フレームに適用される反復回数が、通常は、タグの設定された送信間隔に基づいて送信されるテレメトリ、高優先順位通知、定期的なタグ送信データなどの他のタグ イベントの反復回数とは別個に管理されることです。タグおよびチョークポイント トリガーを設定するときには、この区別を維持することが重要です。たとえば、AeroScout タグでは、チョークポイント スティミュレーション イベントへの応答としてタグが送信する 802.11 フレームに適用される反復回数を指定するのは Tag Repetition of an Exciter event パラメータです。このパラメータは、AeroScout System Manager、Exciter Manager、ANEM のいずれかを使用して Exciter 単位で設定します。これに対し、Exciter 以外に関連するイベントに適用される反復回数を指定するのは Message Repetitions 送信パラメータです。このパラメータは、図 6-32 に示す AeroScout Tag Manager の [Transmission Settings] パネルを使用してタグ単位で設定します。

図 6-32　AeroScout Tag Manager の [Transmission Settings] パネル（Exciter イベントには使用しない）



前述のとおり、チョークポイント スティミュレーションへの応答としてタグが送信する 802.11 マルチキャスト タグ フレームの長さは約 63 バイトです。これは 1 つのチョークポイント MAC アドレスだけのサイズであり、チョークポイントの履歴情報は含まれていません。前に説明したように、テストによって、AeroScout T2 タグが送信する 802.11 マルチキャスト フレームにはベンダー固有の情報も 8 バイト含まれていることが明らかになりました。その情報を図 6-33 に示します。黄色の線で囲んだ部分が必須のチョークポイント情報であり、青い線で囲んだ部分がベンダー固有の追加情報です。

図 6-33　タグ チョークポイント送信データに含まれるベンダー固有の情報



標準のチョークポイント情報と任意のベンダー固有の情報は、同じタグ マルチキャスト フレームとしてタグからアクセス ポイントに送信されますが、リリース 4.1 では、WLAN コントローラがこのフレームを次の 2 つの LOCP 通知として解析します。

- 160 バイトのチョークポイント グループ情報が含まれる LOCP 測定通知
- 138 バイトのベンダー固有の情報が含まれる LOCP 情報通知

ベンダー固有のフィールドの正確な構成はチョークポイントおよびタグ ベンダーによって異なります。たとえば、AeroScout では、AeroScout System Manager および AeroScout Network Exciter Manager の [Exciter Properties] メニューの [Tag Reaction] タブで Exciter ID に補足的なメッセージ情報を追加できます。AeroScout EX-3100 Exciter のユーザは、これらの機能を Exciter Manager ユーティリティでも使用できます。

ベンダー固有の情報には以下の特徴があります。

- Exciter 単位で直接入力し、保存できる。
- タグ メモリに保存されるため、再利用できる。
- 事前に設定され、タグにプログラミングされた 10 のメッセージのうち 1 つで構成される。
- タグに接続されたホストで生成される。

図 6-34 は、この機能を AeroScout EX-2000 Exciter および AeroScout タグで使用する方法を示しています。この図では、Exciter がタグに対し、ベンダー固有の Exciter ID とともにベンダー固有の情報を Exciter から受信したスティミュレーションへの応答として送信する各タグ送信フレームに追加するように指示しています。

図 6-34　AeroScout のベンダー固有の情報の設定オプション

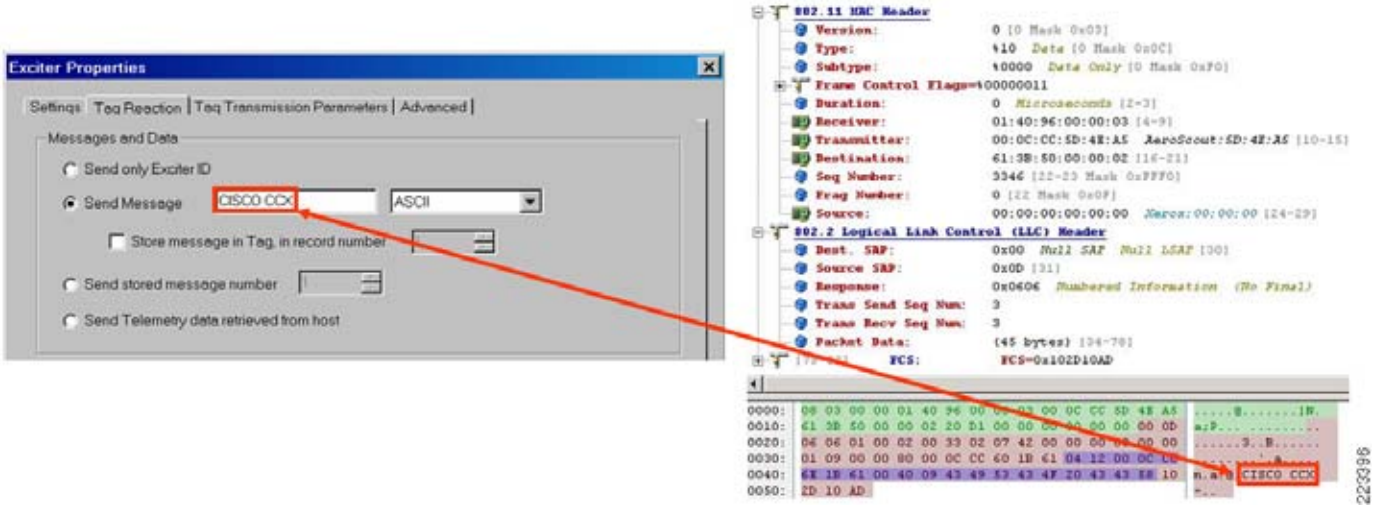


図 6-34 では、Exciter によってスティミュレートされたときにタグが送信する 83 バイトのメッセージに加え、「CISCO CCX」というメッセージを Exciter に定義しています。83 バイトのメッセージには、スティミュレートした Exciter の MAC アドレスに関する標準の情報とベンダー固有の情報が含まれています。AeroScout System Manager で Exciter に定義したテキストは、トレースのオフセット位置 x0046 にあります（図 6-34 の右側にある ASCII テキスト「CISCO CCX」）。この情報を受信した各アクセス ポイントがその情報を登録されたコントローラに転送し、そこから 160 バイトの LOCP 測定通知と 148 バイトの LOCP 情報通知が Location Appliance に送信されます。この情報は Exciter 側でハードコード化されますが、Exciter がタグに対し、埋め込まれているセンサーのデータなど、取り付けられている資産（ホスト）から取得したテレメトリ データを代わりに含めるように指示している場合もあります。

当社が行ったテストの結果は AeroScout のみに該当するものであり、他のベンダーでも同じようにベンダー固有の情報を追加できるとは限らないことに注意してください。

CHAPTER 7

注意事項

この章では、ラボにおける実験で認められた注意事項について説明します。

CSCse14724：モニター モード AP でのロケーション確度の低下

モニター モードのアクセス ポイントのラボ実験では、ローカル モードの場合と比較して、確度の低下が確認されました。

現時点では、ソフトウェア リリース 4.1 によるロケーション認識設計でのモニター モードの使用は推奨されません。

CSCsh88795：CCX S36 ビーコン測定要求のデュアル バンド サポート

*CCX S36 ビーコン要求*は、同じ帯域からのチャネルをアソシエーションとして含みますが、他の帯域のものは含みません。これにより、デュアル バンド クライアントを使用する場合、両帯域で調整データの収集を同時に行う際の信頼性に影響を及ぼす可能性があります。通常、現在アソシエートされている帯域では信頼性のある調整が行われますが、他方の帯域では、ユニキャスト無線測定要求の使用により生じるプローブ要求の生成で同等の信頼性は得られません。

回避策

現時点では、デュアル バンド クライアント使用時にも、帯域ごとに個別に調整データの収集を行うことをお勧めします。そのためには、次のいずれかの方法を使用します。

1. WLAN デバイス規格（バージョン 2 以降）に対応した Cisco Compatible Extensions 仕様と互換性があり、S36 ユニキャスト無線測定要求を認識して応答することができるデュアル バンド クライアント アダプタを装備した 1 台のラップトップを使用して、帯域ごとに個別に調整データの収集を行います。このようなクライアントの例として、Cisco Aironet 802.11a/b/g 無線 CardBus アダプタ（AIR-CB21AG）が挙げられます。たとえば、5 GHz 帯域を無効にし、2.4 GHz 帯域のみを使用してデータ収集を完了します。次に、2.4 GHz 帯域を無効にし、5 GHz 帯域を有効にして、5 GHz 帯域のみを使用して繰り返しデータ収集を行います。
2. 調整データの収集には 2 人のオペレータを動員し、2 台のラップトップを使用して実行します。各ラップトップは、WLAN デバイス規格（バージョン 2 以降）に対応した Cisco Compatible Extensions 仕様と互換性があり、S36 ユニキャスト無線測定要求を認識して応答することができるデュアル バンド クライアント アダプタを装備している必要があります。このようなクライアント

の例として、Cisco AIR-CB21AG が挙げられます。各ラップトップは、異なる帯域を使用するインフラストラクチャに関連付けられていることが必要です。調整データの収集を行う 2 名のオペレータは独立して作業を行えます。両オペレータが同時に各データ ポイントに行ったり、同じデータ ポイントに行ったりする必要はありません。この方法では、前述したオプション 1 の半分の所要時間で両帯域での調整データ収集を完了できます。

CSCsi95122：WCS がロケーション通知のためのノースバウンド電子メールを送信しない

WCS は、どのロケーション通知のアラーム カテゴリについても電子メールによる通知を送信しません。ロケーション通知のアラームはアラーム コンソールには表示されますが、電子メール通知は送信されません。

回避策

ソフトウェア リリース 4.1 では、WCS の代わりに、Location Appliance にある電子メール ノースバウンド通知を使用してください。

上記以外の注意事項については、次のドキュメントを参照してください。

- 『Release Notes for Cisco Wireless Location Appliance 3.0』: http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html
- 『Release Notes for the Cisco Wireless Control System (WCS) 4.1』: http://www.cisco.com/en/US/products/ps6305/prod_release_notes_list.html
- 『Release Note for Cisco WLAN Controllers and Lightweight Access Points 4.1』: http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html
- 『Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(11)JA1』: http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_release_notes_list.html
- 『Cisco Bug Toolkit』: http://www.cisco.com/pcgi-bin/Support/Bugtool/home.pl

APPENDIX A

Maxima 使用による概算ルートの算出

下記に示す円と円の交差式における各記号の意味は次のとおりです。

- *d* は、アクセス ポイント間の距離（フィート単位）を表す
- *Obg* は、802.11bg で必要となるオーバーラップのパーセント値を表す
- *Oa* は、802.11a で必要となるオーバーラップのパーセント値を表す
- *R* は、セル半径（フィート単位）を表す

2 つの円の中心間距離が半径の 2 倍に等しい場合（*d* = *2R*）、オーバーラップはゼロとなることに注意してください。*d* が *2R* を超えると交差領域の面積を計算できなくなるため、この関係は無効になります。*find_root* 関数が *d*/2 から *d* までの閉区間に限定されるのはこのためです。

```
wxMaxima 0.7.3a http://wxmaxima.sourceforge.net
Maxima 5.13.0 http://maxima.sourceforge.net
Using Lisp GNU Common Lisp (GCL) GCL 2.6.8 (aka GCL)
Distributed under the GNU Public License. See the file COPYING.
Dedicated to the memory of William Schelter.
(%i1) d:45.9;
(%o1) 45.9
(%i2) Obg:0.10;
(%o2) 0.1
(%i3) Oa:0.15;
(%o3) 0.15
(%i4) find_root(Obg*%pi*R^2=2*R^2*acos(d/(2*R))-(1/2*d*(sqrt(4*R^2-d^2))),R,d/2,d);
(%o4) 28.49573663945017
(%i5) find_root(Oa*%pi*R^2=2*R^2*acos(d/(2*R))-(1/2*d*(sqrt(4*R^2-d^2))),R,d/2,d);
(%o5) 30.87736860938116
```

（注） シスコは、Maxima の製造、販売、サポートを行っておりません。Maxima は、公開されている Computer Algebra System（CAS：数式処理システム）であり、GNU Public License に基づいてリリースされています。Maxima とその機能、使用方法（各種オペレーティング システム向けダウンロードを含む）の詳細については、次の URL を参照してください。
http://maxima.sourceforge.net.

APPENDIX B

WLAN コントローラでの資産タグ検出の確認

資産タグの検出

図 B-1 に示すプロトコル解析トレースには、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグがどのように認識され、ネットワーク内の他の追跡対象デバイスと区別されるかに関する重要な情報が記載されています。この例では、ファームウェア バージョン 4.33 の AeroScout T2 資産タグを使用しています。他ベンダーから提供されている資産タグでも、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠していれば、同様に Cisco UWN により認識されると想定できます。

図 B-1 は、操作パラメータの基本セットで設定されている AeroScout T2 資産タグのタグ送信間隔が経過するたびに送信されるレイヤ 2 マルチキャスト フレームを図示したものです。図 B-1 では、タグの設定は次のとおりです。

- 3 つのチャネル（1、6、11）にわたるタグの定期送信間隔は 60 秒
- チョークポイントの範囲外表示（図 B-1 で青い四角で囲っている箇所）
- 内蔵の動作および温度の検出センサーは無効に設定

図 B-1　タグのマルチキャスト フレームの RF プロトコル解析（Cisco Compatible Extensions Wi-Fi Tag 仕様準拠）

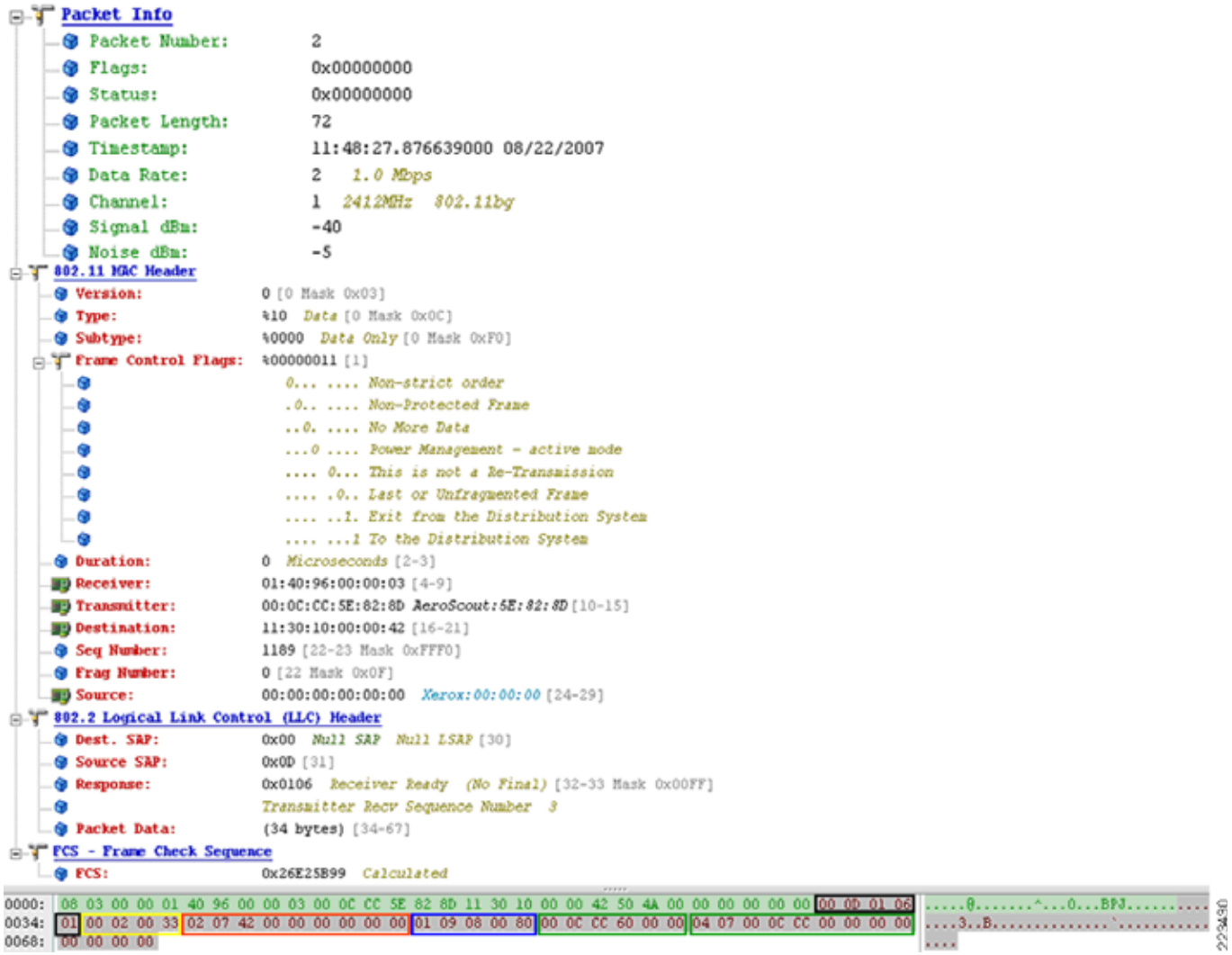


図 B-1 に示すこの資産タグは、外部センサーのテレメトリを送信する設定にはなっていません。また、RF フレームには次の情報も含まれています。

- 5 バイトの Cisco Compatible Extensions Wi-Fi Tag ヘッダー（黒い四角で囲っている箇所）
- タグのプロダクト タイプ ID（黄色の四角で囲っている箇所）
- オプションのバッテリのテレメトリ（赤い四角で囲っている箇所）
- オプションのベンダー固有情報（緑色の四角で囲っている箇所）

マルチキャスト フレームの長さは、タグの設定およびタグとそのベンダーがサポートするオプション機能によって異なります。この例では、図 B-1 に示すマルチキャスト フレームの長さは 72 バイトです。内蔵の温度センサー機能などの追加機能が有効になっている場合や、チョークポイント トリガーからの刺激によりタグがマルチキャスト メッセージを送信している場合は、フレームがより長くなります。たとえば、チョークポイント トリガーからの刺激により送信されるタグのマルチキャストの標準的な長さは 88 バイトです。この場合での追加分の長さは、主に刺激を加えるチョークポイント トリガーの MAC アドレスおよび追加的なベンダー固有情報が含まれることによるものです。

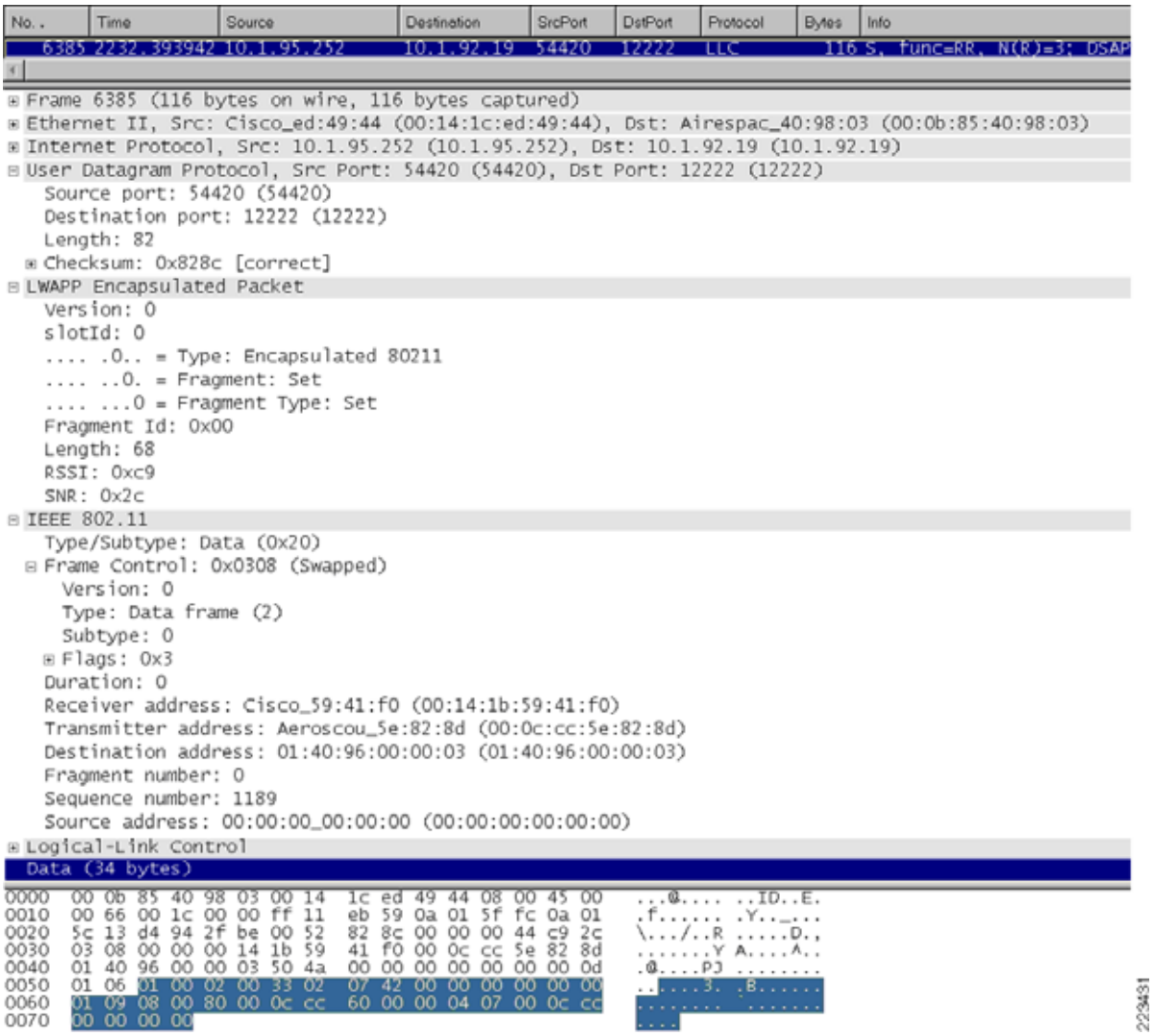
AeroScout T2 タグは、100 ミリ秒の Clear Channel Assessment（CCA; クリア チャネル アセスメント）を開始します。チャネルが空き状態の場合は、そのチャネルがペイロードを 1 Mbps でマルチキャスト転送します。これらのフレームは、802.11 MAC ヘッダーにおいて To Distribution System（ToDS）および Exit From Distribution System（FromDS）のビットが両方とも「1」に設定された状態で、1 Mbps で送信されます。図 B-1 に受信側と送信側のアドレスがあることからわかるように、Wireless Distribution System（WDS; 無線配信システム）の 4 アドレス フレーム フォーマットが使用されています。

送信側アドレスは必ずフレーム送信を行う資産タグの MAC アドレスとなり、受信側アドレスはベンダーにかかわらず Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠したすべての資産タグにより使用されるマルチキャスト アドレスとなります。Cisco UWN は、Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠する資産タグについては 802.11 MAC ヘッダー内に示される宛先アドレスと送信元アドレスを使用しません。通常、これらのアドレスはすべてゼロに設定されますが、図 B-1 の AeroScout T2 に示すように、タグのベンダーが宛先アドレスのフィールドをベンダー固有の用途で使用することは可能です。

アクセス ポイントが図 B-1 に示すフレームを受信すると、このフレームは、アクセス ポイントが登録されているコントローラに LWAPP プロトコルを使用して送信されます（図 B-2 を参照）。ここでは、受信アクセス ポイントに関連付けられた送信元 IP アドレス、および受信アクセス ポイントが登録されているコントローラの AP マネージャ インターフェイスに関連付けられた宛先 IP アドレスがわかります。2 つの図を比較すると、図 B-2 では LWAPP 経由でコントローラに送信する前に、Cisco Aironet アクセス ポイントが フレーム情報に対して 2 つの変更を加えていることがわかります。

- アクセス ポイントのベース無線 MAC アドレス（ベース BSSID）を、カプセル化された 802.11 ヘッダーにある受信側アドレス フィールドにコピーします。
- CCX マルチキャスト アドレス 01:40:96:00:00:03 を、カプセル化された 802.11 ヘッダーにある宛先アドレス フィールドにコピーします。

図 B-2　タグのマルチキャスト フレームの LWAPP キャプチャ（Cisco Compatible Extensions Wi-Fi Tag 仕様準拠）



タグのマルチキャスト アドレスがコントローラによって認識されると、フレームに含まれるペイロードの情報を介して送信側の ID とタイプが確認されます。タグのペイロードに含まれる情報のタイプに応じて、従来の SNMP ポーリング応答またはソフトウェア リリース 4.1 で導入された新しい LOCP のいずれかを使用してペイロードが Location Appliance に渡されます。

RF および LWAPP フレーム解析の両方で示されるシーケンス番号（1189）とフラグメント フィールド（0）に注意してください。これは、802.11 経由でアクセス ポイントに入り、LWAPP 経由でアクセス ポイントから出るパケットの照合に非常に役立つ重要情報となります。特定のタグ フレームのシーケンス番号はタグ メッセージの番号を示します。この番号は 1 つのモジュロ 4096 カウンタから割り当てられ、ゼロから始まって、各タグ メッセージのサイクルごとに 1 ずつ増加します。フラグメント番号は、1 つのチャネル上で送信されたフレーム バーストから特定のフレームを指定します。バースト長がゼロの場合でも、フラグメント番号は必ずゼロから始まります。パケット バーストの場合、フラグメント番号は、ゼロから始まるバースト内のパケット インデックス *n* に設定する必要があります。たとえば、バースト長 5 パケットを送信するようにタグが設定されている場合、フラグメント番号はバーストの最初のパケットでゼロから始まり、2 番目のパケットでは 1 というように順次増加していき、バーストの最後のパケットでは 4 となります。

例として、各チャネル（1、6、11）についてバースト長 3 パケットを送信するように資産タグが設定されていると仮定します。AeroScout 資産タグの場合、バースト長はタグ メッセージの反復送信パラメータを使用して設定されます。想定されるフラグメント番号とシーケンス番号を表 B-1 に示します。

表 B-1　パケットのフラグメント番号およびシーケンス番号

パケット インスタンス	フラグメント番号	シーケンス番号	チャネル
0	0	0	1
1	1	0	1
2	2	0	1
3	0	0	6
4	1	0	6
5	2	0	6
6	0	0	11
7	1	0	11
8	2	0	11

もう 1 つの資産タグが、各チャネル（1、6、11）上で 1 つのメッセージを 60 秒間隔で送信するように設定されていると仮定します。120 秒の間に見られると想定されるフラグメント番号とシーケンス番号を表 B-2 から表 B-4 に示します。

表 B-2　時間＋0

パケット インスタンス	フラグメント番号	シーケンス番号	チャネル
0	0	0	1
1	0	0	6
2	0	0	11

表 B-3　時間＋60

パケット インスタンス	フラグメント番号	シーケンス番号	チャネル
0	0	1	1
1	0	1	6
2	0	1	11

表 B-4　時間＋120

パケット インスタンス	フラグメント番号	シーケンス番号	チャネル
0	0	2	1
1	0	2	6
2	0	2	11

資産タグが検出されない場合

ベスト プラクティスに従ってシステムが設定されているにもかかわらず、資産タグが正しく検出されない場合は、設定が適切であるかどうかを再度確認する必要があります。また、資産タグの RSSI 検出およびメッセージ転送が正しく行われているかどうかを確認することをお勧めします。そのためには、次の手順を実行してください。

ステップ 1　WLAN コントローラによりタグが正しく検出されるかどうかを **show rfid summary** コマンドを使用して確認します。

```
(Controller) >show rfid summary

Total Number of RFID   : 12
-------------- -------- ------------------ ------ ---------------------
  RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
-------------- -------- ------------------ ------ ---------------------
00:0c:cc:5d:4c:5e Aerosct  AP0014.6a1b.41f0    -34     24 seconds ago
00:12:b8:00:20:52 G2       AP001a.a10e.2ffa    -61     16 seconds ago
00:14:7e:00:30:a1 Pango    AP0014.6a1b.41f0    -65      2 seconds ago
```

コントローラがタグを検出しない場合は、コントローラで RFID タグ検出が有効になっているかどうかを **show rfid config** コマンドを使用して確認します。

```
 (Controller) >show rfid config

RFID Tag data Collection..... Enabled
RFID Tag Auto-Timeout........ Disabled
RFID  timeout................ 1200 seconds
```

ステップ 2　RFID タグ検出が有効になっていない場合は、次のコマンドを使用して有効にします。Cisco UWN ソフトウェア リリース 4.1 以降では、RFID タグ検出はデフォルトで有効になっています。

```
config rfid status enable
```

ステップ 3　RFID タグのタイムアウトが、推奨最小値（固定、移動中を含むすべてのタグのうち最長のタグ送信間隔の 3 倍、推奨最大値は 8 倍）に設定されていることを確認します。このパラメータ値の有効範囲は 60 ～ 7,200 秒で、デフォルト値は 1,200 秒です。

例：

```
(Controller) >config rfid timeout 1200
```

ステップ 4　RSSI 失効タイムアウトが次のように設定されていることを確認します。

```
(Controller) >show advanced location summary

Advanced Location Summary :

Algorithm used:                     Average
Client RSSI expiry timeout:          150 sec, half life: 60 sec
Calibrating Client RSSI expiry timeout: 30 sec, half life: 0 sec
Rogue AP RSSI expiry timeout:             1200 sec, half life: 120 sec
RFID Tag RSSI expiry timeout:             1200 sec, half life: 120 sec
```

設定値が上記のデフォルト値と異なる場合は、次のコンフィギュレーション コマンドを使用してデフォルト値に設定します。

config advanced location expiry {**calibrating client** | **client** | **rogue-aps** | **tags** } <*seconds*>

config advanced location rssi-half-life {calibrating client | client | rogue-aps | tags} *<seconds>*

ステップ 5　***show rfid summary*** コマンドを使用してもコントローラによる資産タグ検出が見られない場合は、コントローラで次のデバッグを有効にします。

```
debug mac addr <tag mac addr>
debug dot11 rfid enable
00:0c:cc:5e:82:8d Parsing Cisco Tag RFID packet 68
00:0c:cc:5e:82:8d System group 51
00:0c:cc:5e:82:8d Battery group: status 0x42, days 0, age 0
00:0c:cc:5e:82:8d Chokepoint group, option 0x8, power 0, range 128
00:0c:cc:5e:82:8d Vendor group
00:0c:cc:5e:82:8d  LOCPBuffer 0x133245ec  buffer 0x13324611 msgLen 37 msgId 18 transId
816848706
00:0c:cc:5e:82:8d Notifying LBS of vendor specific data
00:0c:cc:5e:82:8d rfid Aerosct updated by AP 00:14:1B:59:41:F0 (Incoming rssi -47,snr 53),
New saved values rssi -48, snr 49, timestamp 3402186024
```

（注）　この方法でデバッグを行う場合は、**debug mac addr** コマンドを使用することをお勧めします。これにより、アクティブなタグが多数ある環境でデバッグ メッセージの大量発生を回避することができます。

ステップ 6　**debug** コマンド出力から、コントローラがこの資産タグからのパケットを受信していないことが示唆される場合は、この資産タグの範囲内にあることがわかっているアクセス ポイントのコンソールでデバッグを続行することができます。そのアクセス ポイントによる RFID タグの検出を確認するには、次の手順を実行します。

a.　アクセス ポイントと、アクセス ポイントが現在設定されているチャネルで RFID タグ検出が有効になっているかどうかを確認します。この作業は、アクセス ポイントのコンソールで次のコマンドを使用して行います。

show controller Dot11Radio 0

```
 <snipped capture>
Current Frequency: 2412 MHz  Channel 1
RFID Tag Detection: Enabled
```

アクセス ポイントでタグ検出が無効になっている場合は、コントローラで次のコマンドを発行してタグ検出を有効にします。

config rfid status enable

一部のアクセス ポイント コマンドは、アクセス ポイントのリモート デバッグ機能を使用して、コントローラからリモート実行できます。

debug ap enable <Cisco AP>
debug ap command <command> <Cisco AP>

b.　タグ検出が有効になっており、アクセス ポイントが設定されているチャネルで資産タグが送信を行うように設定されている場合は、アクセス ポイントで次のデバッグを有効にして、アクセス ポイントがタグのマルチキャスト パケットをコントローラに転送するかどうかを確認します。

debug dot11 Dot11Radio 0 trace print mcast

（注）　ソフトウェア リリース 4.1 では、debug **dot11 Dot11Radio 0 trace print mcast** コマンドの出力を見るためには、コマンドをアクセス ポイントのコンソールで直接入力する必要があります。コントローラからのリモート入力はできません。

```
4A1F8FB0 r  1 60/ 38- 0803 000 m014096 5D33CF m61356B 6D00   000000 173
   0012 0606 0100 0200 3302 0742 0000 0000 0000 0302 0A03 0109 0000 8000
  0CCC 6010 BF04 0800 0CCC 6E10 BF00 0000 019C 917C 00B8 F564 608F FD05 0000
```

- **m014096**：「m」に続く 3 バイトは、Cisco Compatible Extensions Wi-Fi Tag 仕様準拠の資産タグで使用されるマルチキャスト アドレスの最初の 3 バイトを表します。
- **5D33CF**：資産タグの MAC アドレスの最後の 3 バイトを表します。

マルチキャスト アドレスとタグの MAC アドレスを省略されていない形式で表示する場合は、アクセス ポイントのコンソールで **no debug dot11 Dot11Radio 0 print short** コマンドを発行します。

上記と同様の情報がデバッグ出力に見られた場合は、アクセス ポイントが資産タグのパケットを受信し、コントローラに送信していることを示します。コントローラで資産タグのパケット受信が見られない場合は、LWAPP カプセル化 802.11 フレームをデコードできるイーサネット プロトコル アナライザ（WireShark や OmniPeek など）をアクセス ポイントとコントローラ間の LWAPP イーサネット接続で使用して、実際に資産タグのパケットがコントローラに到達しているかどうかを確認します。これらのパケットのフォーマットは、図 B-2 に示したものと同様となります。これらのパケットがプロトコル アナライザのトレースに見られるにもかかわらず、コントローラで資産タグのパケットの正常な受信が見られない場合は、それまでに取得した詳細データ（プロトコル アナライザのトレースなど）をすべて収集し、デバッグのサポートについて TAC（Technical Assistance Center）にお問い合せください。

c. アクセス ポイントのデバッグ出力にタグのマルチキャスト メッセージが見られない場合は、RF プロトコル アナライザ（OmniPeek や WireShark など）を使用して、実際に資産タグが 3 つの 2.4 GHz チャネル（またはご使用のインフラストラクチャが設定されているチャネル）すべてにおいて想定されるフォーマットでパケット送信を正常に行っているかどうかを確認します（図 B-1 を参照）。プロトコル アナライザのトレースに適切なフレームのフォーマットが見られない場合は、資産タグの設定を調整して対処するか、必要に応じて資産タグを交換します（特に、資産タグのファームウェアが古い場合）。RF プロトコル アナライザで適切なフレームが見られる場合は、次のコマンドを発行して、コントローラでのタグ検出のリセットを試行します。

```
config rfid status disable
config rfid status enable
```

上記の推奨手順を実行しても問題が解決しない場合は、それまでに取得した詳細データ（プロトコル アナライザのトレースなど）をすべて収集し、デバッグのサポートについて TAC（Technical Assistance Center）にお問い合せください。

資産タグのテレメトリおよびイベントの確認

WLAN コントローラが資産タグのテレメトリと高優先度のイベントを検出し、その情報を LOCP を使用して Location Appliance に転送しているかどうかを確認するには、次の手順を使用します。

ステップ 1　前述の項で説明した手順に従って、資産タグが WLAN コントローラによって検出されていることを確認します。

ステップ 2　対象となるテレメトリまたは高優先度の「緊急」イベントの情報がコントローラの RFID データベースに記録されていることを確認します。

```
show rfid detail <tag mac addr>
```

たとえば、次に示す出力の抜粋からは、資産タグでパニック ボタンが押されたことを示唆する情報が、そのイベントに関するベンダー固有データとともに受信されたことがわかります。

```
<snip>
Telemetry Group
==================
Motion Probability.............................  No Motion

!! EMERGENCY !!
==================
Reason.........................................  Panic Button

Vendor Specific
==================
Group Length...................................  8
Vendor OUI:....................................  0x0  0xc  0xcc
Vendor Data: 0x6e  0x13  0xa3  0x0  0x0
```

ステップ 3　コントローラの RFID データベースに上記のような通知が見られない場合は、コントローラで次のデバッグを有効にして、コントローラが通知を受信しているかどうかを確認します。

```
debug mac addr <tag mac addr>
debug dot11 rfid enable

00:0c:cc:5e:82:8d Parsing Cisco Tag RFID packet 62
00:0c:cc:5e:82:8d System group 51
00:0c:cc:5e:82:8d Battery group: status 0x42, days 0, age 0
00:0c:cc:5e:82:8d Chokepoint group, option 0x8, power 0, range 128
00:0c:cc:5e:82:8d Emergency group
00:0c:cc:5e:82:8d  LOCP Buffer 0x133245ec  buffer 0x1332460a msgLen 30 msgId 18 transId
808989330
00:0c:cc:5e:82:8d Notifying LBS of emergency
00:0c:cc:5e:82:8d rfid Aerosct updated by AP 00:14:1B:59:41:F0 (Incoming rssi -49,snr 50),
New saved values rssi -48, snr 49, timestamp 3444175997
```

ステップ 4　上記と同様の出力が見られない場合は、RF プロトコル アナライザを使用して、テレメトリまたは高優先度のイベント送信時にタグによって送信されるパケットをキャプチャし、データが正しいフォーマットで送信されているかどうかを確認します。この確認作業では、TAC（Technical Assistance Center）によるサポートが必要となります。TAC により、タグが無線送信するパケットが有効でないと見なされた場合は､資産タグで使用されているファームウェアのレベルが Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠しており、所定のテレメトリや高優先度の機能をサポートしているかどうかを確認します。

ステップ 5　コントローラの RFID データベースにテレメトリや高優先度のイベントが見られる場合は、前述の出力で、これらの情報が Location Appliance に送信されているかどうかを確認します（**Notifying LBS of emergency** と記載されているかどうかを確認します)。次のコマンドを発行して、コントローラと Location Appliance 間の LOCP 接続が正常に機能しているかどうかを確認します。

```
(Cisco Controller) >show LOCP status

LocServer IP    TxEchoResp    RxEchoReq    TxData    RxData
--------------  ----------    ---------    --------   -------
10.1.56.21         5300          5300        83597      441
```

通常、LOCP 接続が正常に機能している場合は、エコー カウントの定期的な増加が見られます（Location Appliance でのエコー間隔設定に基づきます)。また、LOCP 経由での転送を必要とする緊急イベントやテレメトリ イベントが発生するにつれて、データ フィールドの数字も大きくなります。コントローラがリブートされ、Location Appliance との接続確立に繰り返し失敗する場合は、Location Appliance のための IP アドレスは表示されず、Tx と Rx のカウントは空欄になります。

既知の緊急イベントやテレメトリのデータがタグによって送信されているにもかかわらず、TxData フィールドの数字が大きくならない場合は、次のデバッグ コマンドを使用して、LOCP から Location Appliance への送信が正常に行われているかどうかを確認します。

debug LOCP event enable

出力は次のようになります。

```
LOCP TX message
Sending LOCP_APP_INFO_NOTIF_MSG to LocServer 0
Tx OK
```

LOCP に障害があることを示すメッセージが受信された場合は、トラブルシューティングのサポートについて TAC（Technical Assistance Center）にお問い合せください。