Cisco Wireless Intrusion Prevention System コンフィギュレーション ガイド リリース 8.0

初版：2013 年 07 月 31 日

最終更新：2014 年 07 月 28 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-29331-01

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

© 2014 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xxi

対象読者 xxi

関連資料 xxi

マニュアルの入手方法およびテクニカル サポート xxii

Cisco MSE Prime Infrastructure ユーザ インターフェイス 1

概要 3

wIPS について 3

Cisco Unified Wireless Network 内の wIPS 5

Cisco Unified Wireless Network 内に統合された wIPS 5

Cisco Unified Wireless Network 内の wIPS オーバーレイ構成 6

自律ワイヤレス ネットワークまたはその他のワイヤレス ネットワークでの wIPS オーバーレイ 8

コントローラ IDS と wIPS の違い 8

注意事項と制約事項 9

偽陽性（False Positives）の削減 9

アラーム集約 9

ユーザ認証と暗号化 10

DoS 攻撃 12

セキュリティ ペネトレーション攻撃 14

ワイヤレス IPS アラーム フロー 17

パフォーマンス違反 18

フォレンジック 18

Rogue Detection 19

Anomaly Detection 19

デフォルトの設定プロファイル 19

有効なクライアントの自動 MAC 学習 20

Mobility Services Engine とライセンスの追加および削除 21

MSE のライセンス要件 21

MSE ライセンスの構成マトリクス 22

MSE ライセンス ファイルのサンプル 22

MSE ライセンスの取り消しと再使用 23

注意事項と制約事項 23

Prime Infrastructure へのモビリティ サービス エンジンの追加 24

Mobility Services Engine でのサービスの有効化 25

MSE 追跡パラメータおよび履歴パラメータの設定 27

MSE へのマップの割り当て 28

MSE ライセンス ファイルの削除 29

Prime Infrastructure からのモビリティ サービス エンジンの削除 29

デバイスと wIPS 製品認証キーの登録 30

デバイスおよび wIPS ライセンス ファイルのインストール 30

Mobility Services Engine の同期 33

Prime Infrastructure と Mobility Services Engine の同期 33

Mobility Services Engine の同期の前提条件 34

サードパーティ要素の操作 35

要素の削除またはサード パーティ要素としてのマーキング 35

Cisco WLC と Mobility Services Engine の同期 35

ネットワーク設計、Cisco WLC、Catalyst スイッチ、またはイベント グループの割り当てと同期 36

Cisco WLC への MSE の割り当て 37

ネットワーク設計、有線スイッチ、またはイベント グループの MSE からの割り当て解除 38

データベースの自動同期および Out-of-Sync アラートの設定 38

データベースの自動同期の設定 39

スマート コントローラの割り当てと選択のシナリオ 39

Out-of-Sync アラーム 40

Mobility Services Engine 同期ステータスの表示 40

Mobility Services Engine 同期ステータスの表示 41

同期履歴の表示 41

システム プロパティの設定および表示 43
ライセンス要件 43
一般プロパティの編集およびパフォーマンスの表示 43
一般プロパティの編集 44
パフォーマンス情報の参照 47
NMSP パラメータの変更 47
システムのアクティブ セッションの表示 48
トラップ宛先の追加および削除 49
トラップ宛先の追加 49
トラップ宛先の削除 51
詳細パラメータの表示および設定 51
詳細パラメータ設定の表示 51
詳細パラメータの開始 52
詳細パラメータの設定 52
詳細コマンドの開始 53
システムの再起動またはシャットダウン 54
システム データベースの消去 54
Working with Maps 55
マップについて 55
キャンパス マップへのビルディングの追加 56
フロア領域の追加 57
Adding Floor Areas to a Campus Building 58
Adding Floor Plans to a Standalone Building 60
キャンパス マップの追加 61
ビルディングの設定 62
キャンパス マップへのビルディングの追加 63
独立したビルディングの追加 64
ビルディングの表示 66
ビルディングの編集 67
ビルディングの削除 67
ビルディングの移動 68
フロア領域の追加 68
Adding Floor Areas to a Campus Building 68

Adding Floor Plans to a Standalone Building 70
フロア設定の構成 72
フロア上の包含リージョンと除外リージョンの定義 73
Cisco 1000 シリーズ Lightweight アクセス ポイントのアイコン 73
アクセス ポイントのフロア設定のフィルタリング 77
アクセス ポイント ヒートマップのフロア設定のフィルタリング 80
[AP Mesh Info] のフロア設定のフィルタリング 81
クライアントのフロア設定のフィルタリング 82
802.11 タグのフロア設定のフィルタリング 83
不正 AP のフロア設定のフィルタリング 83
不正アドホックのフロア設定のフィルタリング 84
不正クライアントのフロア設定のフィルタリング 85
干渉設定のフィルタリング 86
wIPS Attacker フロア設定のフィルタリング 86
マップおよび AP ロケーション データのインポート 88
フロア領域のモニタリング 89
Planning and Zooming with Next Generation Maps 89
アクセス ポイントのフロア領域への追加 90
アクセス ポイントの配置 92
マップ作成のための自動階層の使用方法 93
Map Editor の使用 97
Map Editor の使用に関するガイドライン 97
フロア上の包含領域と除外領域に関するガイドライン 98
Map Editor の表示 98
Map Editor を使用したカバレッジ領域の描画 99
フロア上の包含リージョンの定義 99
フロア上の除外リージョンの定義 100
フロアでのレール ラインの定義 101
屋外領域の追加 103
プランニング モードの使用 104
チョークポイントを使用したタグの位置報告の精度の向上 105
Prime Infrastructure へのチョークポイントの追加 106
Prime Infrastructure マップへのチョークポイントの追加 106

Prime Infrastructure からのチョークポイントの削除 107
wIPS およびプロファイルの設定 109
wIPS およびプロファイルの設定 109
注意事項と制約事項 109
前提条件 109
wIPS 設定およびプロファイル管理について 110
注意事項と制約事項 110
wIPS モニタ モードのアクセス ポイントの設定 111
wIPS プロファイルの設定 113
wIPS プロファイル 119
プロファイルの追加 120
プロファイルの削除 121
現在のプロファイルの適用 122
wIPS SSID グループ リストの設定 122
グローバル SSID グループ リスト 123
グループの追加 124
グループの編集 124
グループの削除 125
SSID グループ 125
グループの追加 126
グローバル リストからのグループの追加 126
グループの編集 127
グループの削除 127
プロファイル エディタを使用したプロファイル設定 128
システムとサービスのモニタリング 131
アラームの処理 131
注意事項と制約事項 132
アラームの表示 132
wIPS アラームの統合 133
Cisco Adaptive wIPS アラームの詳細のモニタリング 134
アラームの割り当てと割り当て解除 136
アラームの削除とクリア 137

電子メール アラーム通知 137
イベントの使用 138
ロケーション通知イベントの表示 138
ログの操作 138
注意事項と制約事項 139
ロギング オプションの設定 139
MAC アドレスに基づくロギング 140
ログ ファイルのダウンロード 140
アクセス ポイントの詳細のモニタリング 141
[General] タブ 141
[General]：Lightweight アクセス ポイント 142
[General]：Autonomous 150
[Interfaces] タブ 152
[CDP Neighbors] タブ 155
[Current Associated Clients] タブ 156
[SSID] タブ 158
[Clients Over Time] タブ 158
「Generating Reports」 159
レポート ラウンチ パッド 159
新規レポートの作成と実行 160
現在のレポートの管理 163
スケジュールされた実行結果の管理 163
保存したレポートの管理 164
デバイス使用率レポートの作成 164
保存した使用率レポートの表示 167
スケジュールされた使用率の実行の表示 167
MSE でのクライアントのサポート 167
IPv6 アドレスによる MSE 上の Prime Infrastructure のワイヤレス クライアントの検索 168
MSE で検出されたクライアントの表示 169
Geo-Location のモニタリング 176
フロア マップへの GPS マーカーの追加 176

GPS マーカーの編集 177
フロアからの GPS マーカーの削除 177
Ekahau Site Survey の統合 177
AirMagnet Survey と AirMagnet Planner の統合 178
セキュリティ ダッシュボードの解釈 178
不正 APの表示 179
クライアントの分類 180
Cisco MSE 管理ユーザ インターフェイス 183
Cisco MSE 管理ユーザ インターフェイス 185
MSE 管理 UI のホーム ページ 185
MSE 管理ユーザ インターフェイスの起動 185
MSE サービス 186
MSE サービスの有効化または無効化 187
MSE アプリケーション 188
データの精度ツールの使用 189
前提条件 189
ロケーション チューニングの使用 189
RSSI 最大しきい値に基づくデバイスのフィルタリング 190
固定デバイスと MAC アドレスに基づくデバイスのフィルタリング 191
システムとネットワークの健全性のモニタリング 191
健全性ダッシュボードの表示 191
CAS 遅延統計の表示 192
通知統計情報の表示 192
動態統計の表示 193
MSE システム設定とサービスの構成 195
一般プロパティの表示とサービスの有効化 195
ダッシュボードの表示 198
ライセンスの表示と追加 199
システムのアクティブ セッションの表示 199
トラップ宛先の追加 200
トラップ宛先の削除 202
詳細パラメータ設定の表示 202

詳細パラメータの設定 202
システムの再起動またはシャットダウン 203
システム データベースの消去 204
ロギング オプションの設定 204
ログ ファイルのダウンロード 205
wIPS ポリシー アラーム リファレンス 207
セキュリティ IDS/IPS の概要 207
ユーザ認証と暗号化 208
静的 WEP 暗号化 208
暗号化が無効な AP 208
アラームの説明と考えられる原因 208
wIPS による解決 209
暗号化が無効なクライアント 209
アラームの説明と考えられる原因 209
wIPS による解決 209
クラック可能な WEP IV キーの使用 210
アラームの説明と考えられる原因 210
wIPS による解決 210
オープン認証を使用するデバイス 210
アラームの説明と考えられる原因 210
wIPS による解決 210
共有キー認証を使用するデバイス 211
アラームの説明と考えられる原因 211
wIPS による解決 211
WEP IV キーの再利用 211
アラームの説明と考えられる原因 211
wIPS による解決 211
WPA および 802.11i 211
EAP-TTLS によって保護されていないデバイス 212
アラームの説明と考えられる原因 212
wIPS による解決 212
802.1X によって保護されていないデバイス 212

アラームの説明と考えられる原因 212
wIPS による解決 213
選択した認証方式によって保護されていないデバイス 213
アラームの説明と考えられる原因 213
wIPS による解決 214
802.1 X 暗号化されていないブロードキャストまたはマルチキャスト 214
アラームの説明と考えられる原因 214
wIPS による解決 214
802.1 X キー再生成のタイムアウトが長すぎます 214
アラームの説明と考えられる原因 214
wIPS による解決 215
EAP-TLS によって保護されていないデバイス 215
アラームの説明と考えられる原因 215
wIPS による解決 215
IEEE 802.11i/AES によって保護されていないデバイス 215
アラームの説明と考えられる原因 215
wIPS による解決 216
EAP-FAST によって保護されていないデバイス 217
アラームの説明と考えられる原因 217
wIPS による解決 217
PEAP によって保護されていないデバイス 217
アラームの説明と考えられる原因 217
wIPS による解決 218
TKIP によって保護されていないデバイス 218
アラームの説明と考えられる原因 218
wIPS による解決 218
WPA または 802.11i 事前共有キーの使用 218
アラームの説明と考えられる原因 218
wIPS による解決 218
侵入検知：DoS 攻撃 219
アクセス ポイントに対する DoS 攻撃 219
アラームの説明と考えられる原因 220

wIPS による解決 220
DoS 攻撃：アソシエーション テーブル オーバーフロー 220
アラームの説明と考えられる原因 220
wIPS による解決 221
DoS 攻撃：認証フラッディング 221
アラームの説明と考えられる原因 221
wIPS による解決 221
DoS 攻撃：EAPOL-Start 攻撃 222
アラームの説明と考えられる原因 222
wIPS による解決 222
DoS 攻撃：PS ポール フラッド攻撃 222
アラームの説明と考えられる原因 222
wIPS による解決 223
DoS 攻撃：プローブ要求フラッド 223
アラームの説明と考えられる原因 223
wIPS による解決 223
DoS 攻撃：再アソシエーション要求フラッド 223
アラームの説明と考えられる原因 223
wIPS による解決 224
DoS 攻撃：未認証アソシエーション 224
アラームの説明と考えられる原因 224
wIPS による解決 224
インフラストラクチャに対する DoS 攻撃 224
DoS 攻撃：ビーコン フラッド 225
アラームの説明と考えられる原因 225
wIPS による解決 225
DoS 攻撃：CTS フラッディング 225
アラームの説明と考えられる原因 225
wIPS による解決 226
DoS 攻撃: Destruction 攻撃 226
アラームの説明と考えられる原因 226
wIPS による解決 226

DoS 攻撃：クイーンズランド工科大学により検出された脆弱性 226
アラームの説明と考えられる原因 226
wIPS による解決 227
DoS 攻撃：RF 電波妨害攻撃 227
アラームの説明と考えられる原因 227
wIPS による解決 228
DoS 攻撃：RTS フラッディング 228
アラームの説明と考えられる原因 228
wIPS による解決 228
DoS 攻撃：仮想キャリア攻撃 229
アラームの説明と考えられる原因 229
wIPS による解決 229
クライアント ステーションに対する DoS 攻撃 229
DoS 攻撃：認証失敗攻撃 230
アラームの説明と考えられる原因 230
wIPS による解決 230
DoS 攻撃：ブロック ACK フラッド 231
アラームの説明と考えられる原因 231
wIPS による解決 231
DoS 攻撃: 認証解除ブロードキャスト 231
アラームの説明と考えられる原因 231
wIPS による解決 232
DoS 攻撃：認証解除フラッディング 232
アラームの説明と考えられる原因 232
wIPS による解決 232
DoS 攻撃：アソシエート解除フラッディング 233
アラームの説明と考えられる原因 233
wIPS による解決 233
DoS 攻撃：EAPOL-Logoff 攻撃 233
アラームの説明と考えられる原因 233
wIPS による解決 234
DoS 攻撃：FATA Jack ツールの検出 234

アラームの説明と考えられる原因 234

wIPS による解決 234

DoS 攻撃：不完全な EAP-Failure 攻撃 235

アラームの説明と考えられる原因 235

wIPS による解決 235

侵入検知：セキュリティ突破 235

ASLEAP ツール検出 236

アラームの説明と考えられる原因 236

wIPS による解決 237

AirDrop セッションの検出 237

アラームと考えられる原因 237

wIPS による解決 238

AirPwn 238

アラームの説明と考えられる原因 238

wIPS による解決 238

Airsnarf 攻撃の検出 238

アラームの説明と考えられる原因 238

wIPS による解決 238

不良 EAP-TLS フレーム 239

アラームの説明と考えられる原因 239

wIPS による解決 239

ビーコン ファジング フレーム検出 239

アラームの説明と考えられる原因 239

wIPS による解決 239

ブルートフォース非表示 SSID 240

アラームの説明と考えられる原因 240

wIPS による解決 240

ChopChop 攻撃 240

アラームの説明と考えられる原因 240

wIPS による解決 241

DHCP スターベーション攻撃の検出 241

アラームの説明と考えられる原因 241

wIPS による解決 241
WLAN のセキュリティ異常によるゼロデイ攻撃 242
wIPS による解決 242
デバイスのセキュリティ異常によるゼロデイ攻撃 242
wIPS による解決 242
XSS SSID をブロードキャストするデバイス 242
アラームの説明と考えられる原因 242
wIPS による解決 243
アクセス ポイントのデバイス プローブ 243
アラームの説明と考えられる原因 243
wIPS による解決 243
EAP メソッドへの辞書攻撃 244
アラームの説明と考えられる原因 244
wIPS による解決 244
疑似アクセス ポイントの検出 245
アラームの説明と考えられる原因 245
wIPS による解決 245
偽の DHCP サーバの検出 245
アラームの説明と考えられる原因 245
wIPS による解決 245
高速 WEP クラック（ARP リプレイ）の検出 246
アラームの説明と考えられる原因 246
wIPS による解決 246
フラグメンテーション攻撃 247
アラームの説明と考えられる原因 247
wIPS による解決 247
HT Intolerant Degradation Service 247
アラームの説明と考えられる原因 247
アラームの説明と考えられる原因 247
ハニーポット AP の検出 247
アラームの説明と考えられる原因 247
wIPS による解決 248

Hot-Spotter ツールの検出（潜在的なワイヤレス フィッシング） 248
アラームの説明と考えられる原因 248
wIPS による解決 249
Identical Send and Receive Address 249
アラームの説明と考えられる原因 249
wIPS による解決 249
Improper Broadcast Frames 250
アラームの説明と考えられる原因 250
Improper Broadcast Frames 250
Karma ツールの検出 250
アラームの説明と考えられる原因 250
wIPS による解決 250
中間者攻撃の検出 250
アラームの説明と考えられる原因 250
wIPS による解決 251
NetStumbler の検出 251
アラームの説明と考えられる原因 251
wIPS による解決 252
NetStumbler 犠牲者の検出 252
wIPS による解決 252
アラームの説明と考えられる原因 252
Publicly Secure Packet Forwarding（PSPF）違反 253
アラームの説明と考えられる原因 253
wIPS による解決 253
プローブ要求 ファジング フレームの検出 253
アラームの説明と考えられる原因 253
プローブ応答 ファジング フレームの検出 254
アラームの説明と考えられる原因 254
wIPS による解決 254
ソフト AP またはホスト AP の検出 254
アラームの説明と考えられる原因 254
wIPS による解決 255
スプーフされた MAC アドレスの検出 256

アラームの説明と考えられる原因 256
疑わしい営業時間外のトラフィックの検出 256
アラームの説明と考えられる原因 256
wIPS による解決 256
ベンダー リストによる未承認アソシエーション 257
アラームの説明と考えられる原因 257
wIPS による解決 257
未承認アソシエーションの検出 257
アラームの説明と考えられる原因 257
wIPS による解決 258
Wellenreiter の検出 258
アラームの説明と考えられる原因 258
wIPS による解決 259
WiFi Protected Setup Pin ブルートフォース 259
アラームの説明と考えられる原因 259
wIPS による解決 259
WiFiTap ツールの検出 259
アラームの説明と考えられる原因 259
wIPS による解決 260
パフォーマンス違反 260
チャネルまたはデバイスの過負荷 260
AP アソシエーションのキャパシティが上限に達しています 261
アラームの説明と考えられる原因 261
wIPS による解決 261
ステーションによる AP の過負荷 261
アラームの説明と考えられる原因 261
wIPS による解決 261
使用率による AP の過負荷 261
アラームの説明と考えられる原因 261
wIPS による解決 262
帯域の過剰な使用率 262
アラームの説明と考えられる原因 262

wIPS による解決 262
チャネル上の過剰なマルチキャスト/ブロードキャスト 262
アラームの説明と考えられる原因 262
wIPS による解決 263
ノード上の過剰なマルチキャスト/ブロードキャスト 263
アラームの説明と考えられる原因 263
wIPS による解決 263
不正アクセス ポイントの管理 265
不正アクセス ポイントの問題 265
不正アクセス ポイントのロケーション、タギング、および封じ込め 266
不正アクセス ポイントの検出と特定 267
「Monitoring Alarms」 268
不正アクセス ポイントに関するアラームの監視 268
不正アクセス ポイント監視の詳細 271
アクセス ポイントの検出 272
不正アドホック無線に関するアラームの監視 273
不正アドホック無線に関する詳細の監視 276
イベントのモニタリング 278
不正クライアントの監視 279
Prime Infrastructure での自動 SPT 基準の設定 279
Prime Infrastructure での自動封じ込めの設定 280
コントローラの設定 280
不正ポリシーの設定 281
不正 AP ルールの設定 281
コントローラ テンプレートの設定 282
不正ポリシーの設定 282
不正 AP ルールの設定 283
不正 AP ルール グループの設定 285
wIPS ソリューションの設定と展開 287
[Before You Begin] ウィザード ページの表示 287
不正ポリシーの設定 288
不正ルールの設定 289

現在追加されている不正ルールの表示 291
wIPS プロファイルの設定 292

はじめに

ここでは、『Cisco Wireless Intrusion Prevention System Configuration Guide』の対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。この章は、次の項で構成されています。

- 対象読者，xxi ページ
- 関連資料，xxi ページ
- マニュアルの入手方法およびテクニカル サポート，xxii ページ

対象読者

このガイドは、Wireless Intrusion and Prevention System (wIPS) を設定および管理する管理者向けです。作業を開始する前に、ネットワークの構造、用語、および概念を十分に理解しておく必要があります。

関連資料

Mobility Services Engine の設定とインストールの詳細については、Cisco 3350 または 3355 の『Mobility Services Engine Getting Started Guide』を参照してください。これらのマニュアルは、次の URL の Cisco.com で入手できます。

Cisco Unified Wireless Network ソリューションのユーザ向けマニュアルを参照するには、次のリンクをクリックしてください。

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_install_and_upgrade.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

第 I 部

Cisco MSE Prime Infrastructure ユーザ インターフェイス

- 概要，3 ページ
- Mobility Services Engine とライセンスの追加および削除，21 ページ
- Mobility Services Engine の同期，33 ページ
- システム プロパティの設定および表示，43 ページ
- Working with Maps，55 ページ
- wIPS およびプロファイルの設定，109 ページ
- システムとサービスのモニタリング，131 ページ

第 1 章

概要

この章では、Cisco Unified Wireless Network（CUWN）全体における Cisco Mobility Services Engine（MSE）および Cisco Wireless Intrusion Prevention System（wIPS）の役割について説明します。

Cisco wIPS は、侵入攻撃、不正ワイヤレス デバイス、DoS 攻撃からネットワークを保護し、セキュリティを強化してコンプライアンス目標の達成を可能にします。柔軟性と拡張性の高いワイヤレス ネットワーク セキュリティ機能を持ち、高度なモニタリング機能によってワイヤレス ネットワークの異常、無許可アクセス、RF 攻撃などを検出します。このソリューションには、ネットワーク全体の可視性とアクセス制御が統合されており、オーバーレイ ソリューションが必要ありません。

この章の内容は、次のとおりです。

- wIPS について，3 ページ
- Cisco Unified Wireless Network 内の wIPS，5 ページ
- コントローラ IDS と wIPS の違い，8 ページ

wIPS について

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

CUWN を基盤にし、Cisco Motion の効果を利用した wIPS は構成が強化され、企業に対応しています。wIPS は、連携して統合セキュリティ モニタリング ソリューションを実現する、次のコンポーネントで構成されています。

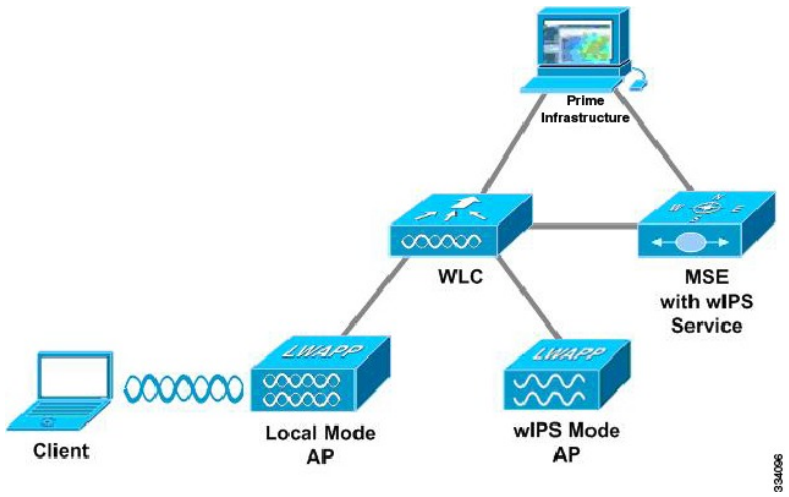
- wIPS ソフトウェアを実行する Mobility Services Engine（MSE）：すべてのコントローラおよびそれらの wIPS モニタ モード アクセス ポイントのアラーム集約の中央ポイントとして動作します。アラーム情報とフォレンジック ファイルは Mobility Services Engine 上に保存されアーカイブされます。

- wIPS モニタ モード アクセス ポイント：攻撃検出とフォレンジック（パケット キャプチャ）機能による固定チャネル スキャンを提供します。

（注） 3 つ目のモジュールを持つアクセス ポイントは、ローカル モードで実行してもモニタ モードの wIPS ライセンスが必要です。

- 拡張ローカル モード アクセス ポイント：タイムスライス型不正スキャンに加え、ワイヤレス サービスをクライアントに提供します。
- Cisco Wireless Security and Spectrum Intelligence（WSSI）：ワイヤレス ネットワークのカバレッジとパフォーマンスが向上するように、無線周波数（RF）の干渉を回避できます。
- ワイヤレス LAN コントローラ：wIPS モニタ モード アクセス ポイントから受信した攻撃情報を Mobility Services Engine に転送し、設定パラメータをアクセス ポイントに配布します。
- Cisco Prime Infrastructure：Mobility Services Engine 上での wIPS サービス設定、コントローラへの wIPS 設定内容のプッシュ、および wIPS モニタ モードのアクセス ポイント設定を行う管理者に、一元化された管理プラットフォームを提供します。Prime Infrastructure は、wIPS アラーム、フォレンジック、レポートの表示、および攻撃百科事典へのアクセスにも使用されます。この図は、Wireless Intrusion Prevention System（ワイヤレス侵入防御システム）を示しています。

図 *1*：*Wireless Intrusion Prevention System*（ワイヤレス侵入防御システム）



システム コンポーネント間の通信には、次のプロトコルが使用されます。

- Control and Provisioning of Wireless Access Points（CAPWAP）：このプロトコルは、LWAPP の後継で、アクセス ポイントとコントローラ間の通信に使用されます。これは、アラーム情報をコントローラに送信し、設定情報をアクセス ポイントに送信する双方向トンネルを提供します。

- ネットワーク モビリティ サービス プロトコル（NMSP）：コントローラと Mobility Services Engine 間の通信プロトコルです。wIPS 環境では、このプロトコルによりアラーム情報のコントローラからの集約と Mobility Services Engine への転送、および wIPS 設定情報のコントローラへの適用が行われます。このプロトコルは暗号化されます。
  - コントローラ TCP ポート：16113
- Simple Object Access Protocol（SOAP/XML）：Mobility Services Engine と Prime Infrastructure 間の通信の方法です。このプロトコルは、Mobility Services Engine で実行する wIPS サービスに設定パラメータを配布するために使用されます。
  - MSE TCP ポート：443
- 簡易ネットワーク管理プロトコル（SNMP）：このプロトコルは、Mobility Services Engine から Prime Infrastructure に wIPS アラーム情報を転送するために使用されます。また、コントローラから Prime Infrastructure に不正アクセス ポイント情報を伝えるためにも使用されます。

Cisco Unified Wireless Network 内の wIPS

CUWN インフラストラクチャ内で wIPS を統合したり、CUWN やシスコの自律ワイヤレス ネットワーク（またはサードパーティのワイヤレス ネットワーク）に wIPS をオーバーレイしたりできます。

ここでは、次の内容について説明します。

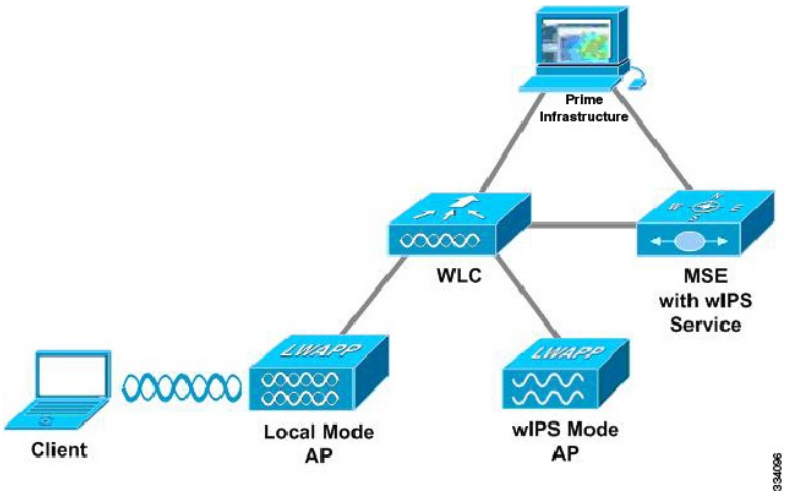
- Cisco Unified Wireless Network 内に統合された wIPS, （5 ページ）
- Cisco Unified Wireless Network 内の wIPS オーバーレイ構成, （6 ページ）
- 自律ワイヤレス ネットワークまたはその他のワイヤレス ネットワークでの wIPS オーバーレイ, （8 ページ）

Cisco Unified Wireless Network 内に統合された wIPS

統合 wIPS 構成は、ローカル モードと wIPS モニタ モードの両方のアクセス ポイントを同じコントローラ上で混合させ、同じ Prime Infrastructure によって管理するシステム設計です。これは、クライアント サービング インフラストラクチャとモニタリング インフラストラクチャ間の緊密な

統合を可能にするため、推奨される構成です。この図は、シスコのワイヤレス ネットワーク内で統合された wIPS 構成を示しています。

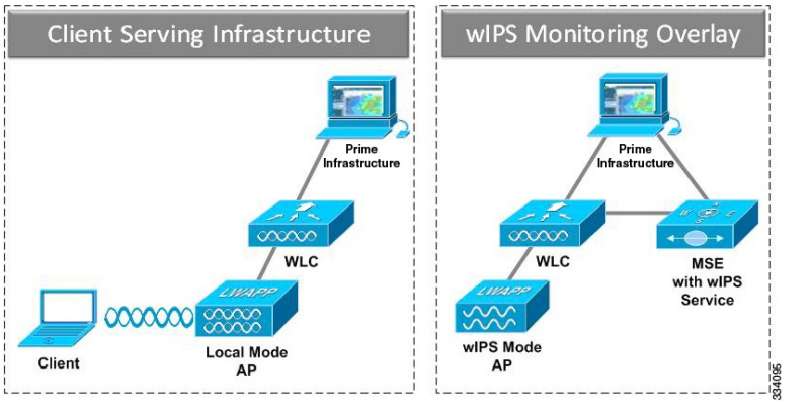
図 *2* : *CUWN* 内の統合された *wIPS*



Cisco Unified Wireless Network 内の wIPS オーバーレイ構成

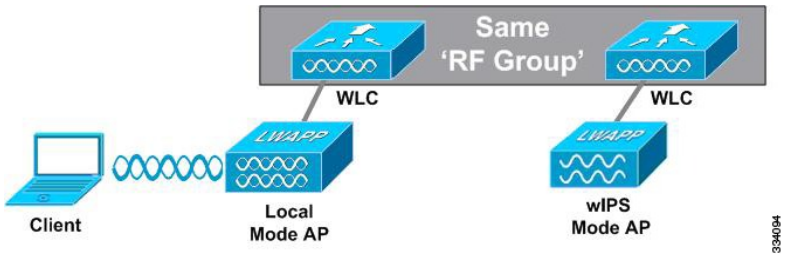
wIPS オーバーレイ構成では、wIPS モニタリング インフラストラクチャはクライアント サービング インフラストラクチャから完全に分離されます。各システムが独自のコントローラ、アクセス ポイント、およびPrime Infrastructure のセットを使用します。この構成モデルを選択する理由の多くは、個別の管理コンソールを使用した個別のネットワーク インフラストラクチャ システムとセキュリティ インフラストラクチャ システムを必要とするビジネス上の規定に起因します。また、この構成モデルは、アクセス ポイント（wIPS モニタとローカル モード）の合計数が NCS に含まれる 3000 アクセス ポイントの制限を超える場合にも使用されます。次の図は、ワイヤレス ネットワークでの wIPS オーバーレイ構成を示します。

図 *3* : *CUWN* 内の *wIPs* オーバーレイ モニタリング ネットワーク構成



wIPS オーバーレイ モニタリング ネットワークを構成して、クライアント サービング インフラストラクチャのセキュリティ査定を行うには、特定の構成手順を実行する必要があります。wIPS システムは、信頼されるデバイスに対する攻撃だけをログに記録するという前提で動作します。オーバーレイ システムで、個別の Cisco Unified WLAN インフラストラクチャを信頼されるものとして表示するには、コントローラが同じ RF グループに属している必要があります。

図 *4*：*wIPS* オーバーレイ モニタリング ネットワークの同じ *RF* グループに属しているコントローラ



クライアント サービング インフラストラクチャを wIPS オーバーレイ モニタリング ネットワークから分離した結果として、いくつかのモニタリングの警告が発生します。

- wIPS アラームは、wIPS オーバーレイ Prime Infrastructure インスタンスにだけ表示されます。
- 管理フレーム保護（MFP）アラームは、クライアントインフラストラクチャ Prime Infrastructure インスタンスにだけ表示されます。
- 不正アラームは、両方の Prime Infrastructure インスタンスに表示されます。
- 不正位置の精度は、クライアント サービング インフラストラクチャ Prime Infrastructure の方が高くなります。この構成では、wIPS オーバーレイ構成よりも高密度のアクセス ポイントを使用するためです。
- Over-the-Air 不正緩和は、ローカル モード アクセス ポイントを緩和操作で利用できるため、統合 wIPS モデルで拡張性が高くなります。
- セキュリティ モニタリング ダッシュボードは、両方の Prime Infrastructure インスタンスで不完全になります。wIPS などの一部のイベントが wIPS オーバーレイ Prime Infrastructure にだけ存在するためです。ワイヤレス ネットワークの包括的なセキュリティをモニタするには、両方のセキュリティ ダッシュボード インスタンスを監視する必要があります。

  次の表に、クライアント サービングとオーバーレイ構成のいくつかの主な違いの概要を示します。

表 *1*：*wIPS* クライアント サービングと *wIPS* モニタリング オーバーレイの比較

	クライアント サービング Prime Infrastructure	wIPS モニタリング オーバーレイ Prime Infrastructure
wIPS アラーム	No	Yes
MFP アラーム	Yes	No

不正アラーム	Yes	Yes
不正位置	高精度	低精度
不正封じ込め	Yes	Yes、ただし拡張性あり

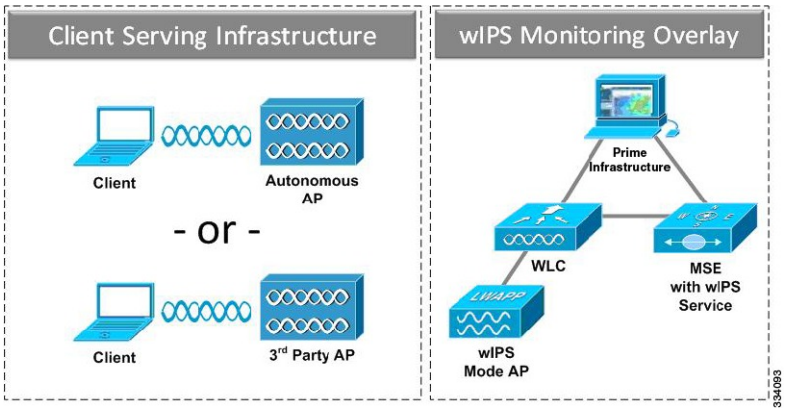
オーバーレイ ソリューションの課題の 1 つは、クライアント サービング インフラストラクチャまたは wIPS モニタリング オーバーレイ上の Lightweight アクセス ポイントが誤ったコントローラにアソシエートされる可能性です。誤ったコントローラとのアソシエーションは、各アクセス ポイント（ローカル モードと wIPS モニタ モード）で第 1、第 2、第 3 コントローラ名を指定することによって対処できます。さらに、各ソリューションのコントローラにそれぞれのアクセス ポイントとの通信用の個別の管理 VLAN を備え、アクセス コントロール リスト（ACL）を使用して CAPWAP トラフィックがこれらの VLAN 境界を超えないようにすることを推奨します。

自律ワイヤレス ネットワークまたはその他のワイヤレス ネットワークでの wIPS オーバーレイ

wIPS ソリューションは、CUWN 以外の既存の WLAN インフラストラクチャへのセキュリティ モニタリングも実行できます。この構成の用途は、シスコの自律アクセス ポイントまたはサードパーティ アクセス ポイントのセキュリティ モニタリングです。

この図は、自律ネットワークでの wIPS オーバーレイを示します。

図 *5*：自律ネットワークでの *wIPS* オーバーレイ



コントローラ IDS と wIPS の違い

ここでは、次の内容について説明します。

• 注意事項と制約事項, （9 ページ）

- 偽陽性（False Positives）の削減, （9 ページ）
- アラーム集約, （9 ページ）
- フォレンジック, （18 ページ）
- Rogue Detection, （19 ページ）
- Anomaly Detection, （19 ページ）
- デフォルトの設定プロファイル, （19 ページ）
- 有効なクライアントの自動 MAC 学習, （20 ページ）

注意事項と制約事項

フォレンジック

wIPS システムのフォレンジック機能はむやみに使用せず、目的の情報がキャプチャされたら無効にする必要があります。これは主に、アクセス ポイントにかかる負荷が大きく、スケジュールされたチャネル スキャンへの割り込みが発生するためです。wIPS アクセス ポイントでは、チャネル スキャンを実行しながら、フォレンジック ファイルを生成することはできません。フォレンジック ファイルがダンプされている間、チャネル スキャンは遅延します。

偽陽性（False Positives）の削減

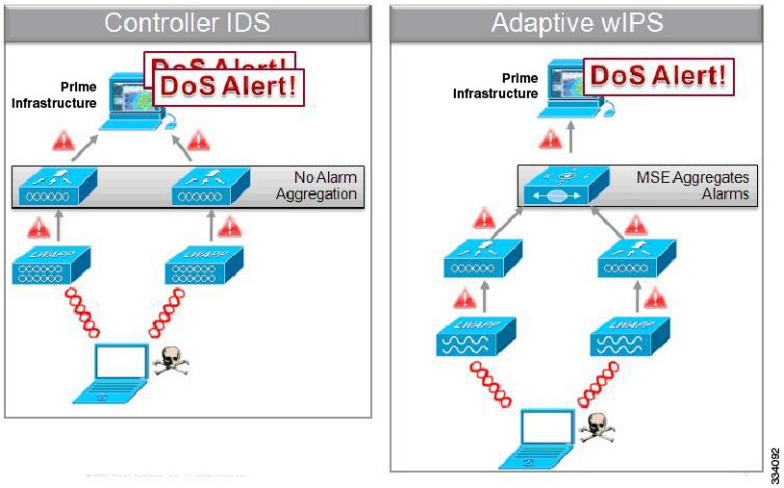
wIPS は、ワイヤレス ネットワークのセキュリティ モニタリングについて偽陽性の削減を促し、攻撃シグニチャを関連付けます。wIPS は、ワイヤレス インフラストラクチャ ネットワークに損傷を引き起こす、無線経由の多数の管理フレームを検出すると、アラームをトリガーします。これは、wIPS システムがワイヤレス インフラストラクチャ内に存在するアクセス ポイントとクライアントの状態および有効性を動的に識別できる結果です。

アラーム集約

シスコの既存のコントローラベースの IDS システムとシスコの wIPS システムの大きな違いの 1 つは、無線で検出された一意の攻撃が 1 つのアラームに関連付けられ、集約されることです。これは、ワイヤレス IPS システムによって、特定の各攻撃が初めて識別されたときに、それらに一意のハッシュ キーを自動的に割り当てることで実行されます。複数の wIPS アクセス ポイントで攻撃が受信された場合、Mobility Services Engine でアラーム集約が行われるため、攻撃は Prime Infrastructure に 1 回だけ転送されます。既存のコントローラベースの IDS システムはアラームを

集約しません。次の図に、シスコのコントローラ ベースの IDS を使用した場合と wIPS を使用した場合のアラーム集約を示します。

図 *6*：シスコのコントローラベースの *IDS* と *wIPS* を使用したアラームの集約



コントローラベースの IDS と wIPS のもう 1 つの大きな違いは、各システムで検出可能な攻撃数です。サブセクションの説明と下の表に示されているように、wIPS は多数の攻撃と攻撃ツールを検出できます。これらの攻撃には、サービス拒否（DoS）攻撃とセキュリティ突破攻撃の両方が含まれます。ここでは、次の内容について説明します。

- ユーザ認証と暗号化，（10 ページ）
- DoS 攻撃，（12 ページ）
- セキュリティ ペネトレーション攻撃，（14 ページ）
- ワイヤレス IPS アラーム フロー，（17 ページ）
- パフォーマンス違反，（18 ページ）

ユーザ認証と暗号化

ユーザ認証およびワイヤレストラフィックの暗号化は、WLANセキュリティの防御として機能します。ユーザ認証は、有線およびワイヤレス リソースへの不正アクセスを遮ります。トラフィック暗号化は、侵入者がワイヤレス トラフィックを傍受することを防止します。認証および暗号化のカテゴリにおける一般的なセキュリティ違反には、設定ミス、更新されていないソフトウェア、企業のセキュリティ ポリシーの不十分な規定などが含まれます。

次の表には、コントローラ ベースの IDS と wIPS サービスによって検出される wIPS セキュリティ攻撃が示されています。

表 *2* : コントローラ *IDS* と *wIPS* によって検出されるセキュリティ攻撃

アラーム名	コントローラ IDS によって検出	wIPS によって検出
静的 WEP 暗号化		
暗号化が無効な AP		X
暗号化が無効なクライアント		X
クラック可能な WEP IV キーの使用		X
オープン認証を使用するデバイス		X
共有キー認証を使用するデバイス		X
WEP IV キーの再利用		X
WPA および 802.11i		
802.1x キー変更のタイムアウトが長すぎます		X
802.1x 暗号化されないブロードキャストまたはマルチキャスト		X
EAP-TLS によって保護されていない AP		X
選択された認証方法によって保護されていないデバイス		X
EAP - TTLS を使用しないデバイス		X
802.11i/AES によって保護されていないデバイス		X
802.1x によって保護されていないデバイス		X
EAP-FAST によって保護されていないデバイス		X

アラーム名	コントローラ IDS によって検出	wIPS によって検出
PEAP によって保護されていないデバイス		X
TKIP によって保護されていないデバイス		X
WPA または 802.11i 事前共有キーの使用		X

DoS 攻撃

DoS 攻撃には、ワイヤレス ネットワーク内の正常な通信を妨害または遅延させるように設計されたメカニズムが含まれます。これらには、ワイヤレス ネットワーク内の正規の接続をドロップさせたり、不安定にさせるように設計された多数のスプーフされたフレームが組み込まれることがあります。DoS 攻撃は、ワイヤレス ネットワークの信頼できるサービスを提供する機能に打撃を与える可能性がありますが、データ違反にはならず、攻撃が停止すれば、多くの場合マイナスの影響はなくなります。

次の表に、コントローラ ベースの IDS と wIPS サービスによる DoS 攻撃の検出を比較して示します。

表 *3*：コントローラ *IDS* と *wIPS* によって検出される *DoS* 攻撃

アラーム名	コントローラ IDS によって検出	wIPS によって検出
AP に対する DoS 攻撃		
アソシエーション フラッド	X	X
アソシエーション テーブル オーバーフロー		X
認証フラッド	X	X
EAPOL-Start 攻撃	X	X
PS-Poll フラッド		X
プローブ要求フラッド		X
再アソシエーション要求フラッド		X
認証されないアソシエーション		X

アラーム名	コントローラ IDS によって検出	wIPS によって検出
インフラストラクチャに対する DoS 攻撃		
ビーコン フラッド		X
CTS フラッド		X
MDK3-Destruction 攻撃		X
Queensland University of Technology Exploit		X
RF 電波妨害攻撃		X
RTS フラッド		X
仮想キャリア攻撃	X	X
ステーションに対する DoS 攻撃		
認証失敗攻撃		X
ブロック ACK フラッド		X
De-Auth ブロードキャスト フラッド	X	X
De-Auth フラッド	X	X
Dis-Assoc ブロードキャスト フラッド		X
Dis-Assoc フラッド	X	X
EAPOL-Logoff 攻撃	X	X
FATA-Jack ツール		X
不完全な EAP-failure		X
不完全な EAP-Success		X
プローブ応答フラッド		X

セキュリティ ペネトレーション攻撃

ワイヤレス ネットワークを脅かす 2 つの攻撃タイプのうち、ほぼ間違いなく有害性の高いセキュリティ突破は、機密データや後で機密データを見るために使用できる暗号キーなどの情報をキャプチャしたり、公開したりするように設計されています。セキュリティ突破攻撃には、インフラストラクチャに対するクエリや暗号キーを解読することを目的とした応答攻撃が含まれることがあります。さらに、セキュリティ突破攻撃は、ハニーポットなどの疑似アクセス ポイントにクライアントの誘導を試みることによってクライアントに害を及ぼす可能性もあります。

次の表に、コントローラベースの IDS と wIPS サービスによって検出されるセキュリティ突破攻撃の比較を示します。

表 *4*：コントローラ *IDS* と *wIPS* によって検出されるセキュリティ突破攻撃

アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
ASLEAP ツール検出	X	X
AirDrop セッション検出		X
AirPwn		X
Airsnarf 攻撃		X
不良 EAP-TLS フレーム		X
ビーコン Fuzzed フレーム検出		X
ブルートフォース非表示 SSID	X	X
ChopChop 攻撃		X
DHCP スターベーション攻撃の検出		X
WLAN のセキュリティ異常による Day-Zero 攻撃	X	X
デバイスのセキュリティ異常による Day-Zero 攻撃		X
XSS SSID をブロードキャストするデバイス		X

アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
AP のデバイス プローブ		X
EAP メソッドへの辞書攻撃		X
802.1x 認証に対する EAP 攻撃		X
偽の AP の検出	X	X
偽の DHCP サーバの検出		X
高速 WEP クラック ツールの検出		X
フラグメンテーション攻撃		X
HT-Intolerant Degradation of Service		X
ハニーポット AP の検出	X	X
Hotspotter ツールの検出		X
Identical Send and Receive Address		X
Improper Broadcast Frames		X
Karma ツールの検出		X
不正 802.11 パケットの検出		X
中間者攻撃の検出		X
NetStumbler の検出	X	X
NetStumbler 犠牲者の検出	X	X
PSPF 違反の検出		X

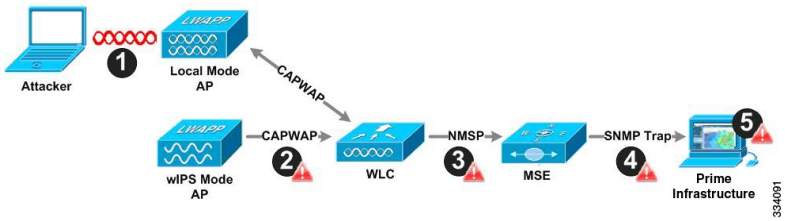
アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
プローブ要求ファジングフレームの検出		X
プローブ応答ファジングフレームの検出		X
ソフト AP またはホスト AP の検出		X
スプーフされた MAC アドレスの検出		X
疑わしい after-hours トラフィックの検出		X
ベンダー リストによる未承認アソシエーション		X
未承認アソシエーションの検出		X
Wellenreiter の検出	X	X
WiFi Protected Setup Pin ブルートフォース		X
WiFiTap ツールの検出		X
チャネルまたはデバイスの過負荷		
AP アソシエーションのキャパシティが上限に達しています		X
ステーションによる AP の過負荷		X
使用率による AP の過負荷		X
帯域の過剰な使用率		X

アラーム名	コントローラ IDS によって検出	ワイヤレス IPS によって検出
チャネル上の過剰なマルチキャスト/ブロードキャスト		X
ノード上の過剰なマルチキャスト/ブロードキャスト		X

ワイヤレス IPS アラーム フロー

wIPS システムは、通信のリニア チェーンに従って、エアウェーブの初期スキャンから取得した攻撃情報を伝播して、情報を NCS に転送します。この図には、ワイヤレス ネットワーク内のアラーム フローが示されています。

図 *7*: ネットワーク内のアラーム フロー



1. wIPS システムでアラームを生成させるには、正規のアクセス ポイントまたはクライアントに対して攻撃が仕掛けられる必要があります。正規のアクセスポイントおよびクライアントは、同じ RF グループ名をブロードキャストする信頼するデバイスによって、CUWN 内で自動的に検出されます。この設定では、ローカルモード アクセス ポイントとそれらにアソシエートされたクライアントのリストが動的に管理されます。SSID グループ機能を使用して、SSID によってデバイスを信頼するようにシステムを設定することもできます。WLAN インフラストラクチャに害を及ぼすと見なされた攻撃だけが残りのシステムに伝播されます。
2. wIPS モニタ モード アクセス ポイントによって攻撃が識別されると、アラームの更新がコントローラに送信され、CAPWAP 制御トンネル内にカプセル化されます。
3. コントローラは、アラームの更新をアクセス ポイントから、Mobility Services Engine を実行する wIPS サービスに透過的に転送します。この通信に使用されるプロトコルは NMSP です。
4. Mobility Services Engine 上の wIPS サービスが受信したアラームの更新は、アーカイブと攻撃の追跡のためにアラーム データベースに追加されます。SNMP トラップが Prime Infrastructure に転送されます。SNMP トラップには攻撃情報が含まれています。同じ攻撃を参照する複数のアラーム更新を受信した場合（たとえば、複数のアクセスポイントで同じ攻撃が認識された）、1 つの SNMP トラップだけが Prime Infrastructure に送信されます。

5 アラーム情報を含む SNMP トラップは Prime Infrastructure によって受信され、表示されます。

パフォーマンス違反

WLAN のパフォーマンス効率は、RF 環境の変動とクライアント デバイスの移動の影響を受けます。WLANのパフォーマンスと効率は、WLANを監視し、ワイヤレス管理者に問題の兆候を早期に警告することで、wIPS によって保証されます。wIPS の使用を最大化するために、パフォーマンス アラームをカスタマイズして WLAN 導入仕様に合わせることができます。

次の表は、コントローラ ベースの IDS と wIPS サービスによって検出されるパフォーマンス違反を示しています。

表 *5*: コントローラと *wIPS* によるパフォーマンス違反の検出

アラーム名	コントローラ IDS によって検出	wIPS によって検出
チャネルまたはデバイスの過負荷		
AP アソシエーションのキャパシティが上限に達しています		X
ステーションによる AP の過負荷		X
使用率による AP の過負荷		X
帯域の過剰な使用率		X
チャネル上の過剰なマルチキャスト/ブロードキャスト		X
ノード上の過剰なマルチキャスト/ブロードキャスト		X

フォレンジック

Cisco wIPS システムは、詳しい調査とトラブルシューティングの目的で、フォレンジック攻撃をキャプチャする機能を提供します。基本レベルでは、フォレンジック機能は、一連のワイヤレスフレームをログに記録し、取得する切り替えベースのパケットキャプチャファシリティです。この機能は wIPS プロファイル内で攻撃単位で有効になります。wIPS プロファイルは Prime Infrastructure で設定されます。

この機能を有効にすると、エアウェーブで特定の攻撃アラームが確認されると、フォレンジック機能がトリガーされます。元のアラームを生成した wIPS モニタ モード アクセス ポイントのバッファ内に格納されたパケットに基づいて、フォレンジック ファイルが作成されます。このファイルは CAPWAP によってコントローラに転送されます。次に、この CAPWAP によって、NMSP 経

由でフォレンジック ファイルが、Mobility Services Engine で実行されている wIPS に転送されます。このファイルは、ユーザがフォレンジックに設定したディスク容量制限に達するまで、Mobility Services Engine のフォレンジック アーカイブに保存されます。デフォルトでは、この制限は 20 GB で、この制限に達すると、最も古いフォレンジック ファイルが削除されます。フォレンジック ファイルには、フォレンジック ファイルへのハイパーリンクを含むアラームを Prime Infrastructure で開くことでアクセスできます。このファイルは、.CAP ファイル形式で保存されており、WildPacket Omnipeek、AirMagnet WiFi Analyzer、Wireshark、またはこの形式をサポートしているその他のパケット キャプチャ プログラムを使用してアクセスできます。Wireshark は次の URL から入手できます。 http://www.wireshark.org

Rogue Detection

wIPS に最適化されたモニタ モードのアクセス ポイントは、現在の CUWN 実装と同じロジックを使用して、不正の脅威の査定と緩和を行います。これにより、ワイヤレス IPS モード アクセス ポイントは、不正アクセスポイントおよびアドホック ネットワークをスキャンし、検出して、封じ込めることができます。不正ワイヤレス デバイスに関するこの情報が発見されると、不正アラーム集約が行われる Prime Infrastructure に報告されます。

ただし、この機能を使用すると、ワイヤレス IPS モード アクセス ポイントを使用して、攻撃封じ込めが起動された場合、封じ込めの間、系統的な攻撃を狙いとしたチャネル スキャンを実行する機能が中断されます。

Anomaly Detection

wIPS には、キャプチャされた攻撃パターンやデバイス特性の異常性に関する特定のアラームが含まれます。異常検出システムでは、Mobility Services Engine 内に格納された攻撃履歴ログおよびデバイス履歴を考慮して、ワイヤレス ネットワークの一般的な特性の基準を定めます。システム上のイベントまたは攻撃に、Mobility Services Engine に保存されている履歴データと比較して、ある程度の変化が見られた場合に、異常検出エンジンがトリガーされます。たとえば、システムで毎日わずかな MAC スプーフィング イベントを定期的にキャプチャしており、別の日に MAC スプーフィング イベントが 200 % 増加した場合、その Mobility Services Engine で異常アラームがトリガーされます。次に、このアラームが Prime Infrastructure に送信され、システムで発生する可能性のある従来の攻撃を超えた何かがワイヤレス ネットワークで発生していることが管理者に通知されます。さらに、異常検出アラームは、wIPS システムに既存のシグニチャがない可能性のある Day-Zero 攻撃を検出するためにも使用できます。

デフォルトの設定プロファイル

特定の各 WLAN セキュリティ構成に合わせた設定の調整を容易にするため、wIPS には、特定の産業や導入のセキュリティ ニーズに合わせて作られた多数のデフォルトのプロファイルが用意されています。テンプレートには、さまざまなリスク プロファイルおよび導入ごとに異なるセキュリティ モニタリングの要件が要約されています。特定のプロファイルには、Education、Enterprise（Best）、Enterprise（Rogue）、Financial、Healthcare、Hotspot（Open Security）、Hotspot（802.1x Security）、Military、Retail、Tradeshow、Warehouse などがあります。プロファイルは、目的の構成の特定のニーズに合わせてさらにカスタマイズできます。

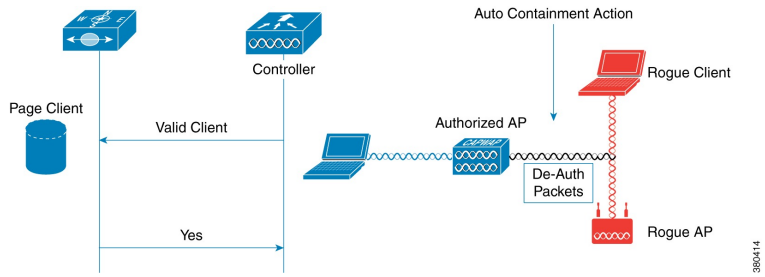
有効なクライアントの自動 MAC 学習

リリース 7.5 では、自動 MAC 学習機能を導入しています。この機能は、ネットワーク上の有効なクライアントを不正アクセス ポイントへの接続から保護します。MSE は、MSE での事前設定なしにクライアントを検証するために使用します。

クライアントが不正アクセス ポイントに接続すると、コントローラは MSE によってクライアントが有効かどうかを検証します。クライアントが有効な場合、コントローラはクライアントの不正アクセス ポイントへの接続を自動的に封じ込めます。コントローラは、MSE の自動 MAC 学習データベースを使用して、再アソシエーション要求の MAC アドレスをチェックします。

（注） 有効なクライアントの自動 MAC 学習機能は、Cisco Controller UI から有効にする必要があります。

図 *8*：有効なクライアントの自動 *MAC* 学習



第 2 章

Mobility Services Engine とライセンスの追加および削除

この章では、Cisco 3300 シリーズ Mobility Services Engine（MSE）を Cisco Prime Infrastructure に対して追加および削除する方法について説明します。

（注） [Identity Services] タブの [MSEs]、[Synchronization History]、[High Availability]、[Context-Aware Notifications]、および [Mobile Concierge] ページは、リリース 7.3.101.0 の ルート仮想ドメインでのみ使用できます。

- MSE のライセンス要件，21 ページ
- 注意事項と制約事項，23 ページ
- Prime Infrastructure へのモビリティ サービス エンジンの追加，24 ページ
- MSE ライセンス ファイルの削除，29 ページ
- Prime Infrastructure からのモビリティ サービス エンジンの削除，29 ページ
- デバイスと wIPS 製品認証キーの登録，30 ページ
- デバイスおよび wIPS ライセンス ファイルのインストール，30 ページ

MSE のライセンス要件

MSE ライセンスの詳細については、『Cisco Mobility Services Ordering and Licensing Guide』を参照してください。

- MSE ライセンスの構成マトリクス，（22 ページ）
- MSE ライセンス ファイルのサンプル，（22 ページ）
- MSE ライセンスの取り消しと再使用，（23 ページ）

MSE ライセンスの構成マトリクス

次の表 に、MSE、ロケーション サービスまたはContext-Aware Service ソフトウェア、およびwIPS について、ハイエンド、ローエンド、および評価ライセンスのライセンス内容を示します。

表 *6* : *MSE* ライセンスの構成マトリクス

	ハイエンド	ローエンド	評価
MSE プラットフォーム	ハイエンドアプライアンスおよびインフラストラクチャプラットフォーム	ローエンドアプライアンスおよびインフラストラクチャプラットフォーム	120 日間
ロケーション サービスまたは Context-Aware Service ソフトウェア	3000、6000、12,000 アクセス ポイント	1000 アクセス ポイント	120 日間、100 タグおよび 100 要素
	3000、6000、12,000 アクセス ポイント	1000 要素	
wIPS	6000 アクセス ポイント	2000 アクセス ポイント	120 日間、20 アクセス ポイント

（注） 必要に応じて評価ライセンスを延長するには、シスコの顧客担当者にお問い合わせください。

MSE ライセンス ファイルのサンプル

次に、MSE ライセンス ファイルのサンプルを示します。

```
FEATURE MSE cisco 1.0 permanent uncounted \
VENDOR_STRING=UDI=udi,COUNT=1 \
HOSTID=ANY \
NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</Li cLineID> \
<PAK>dummyPak</PAK>" \
SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

このサンプル ファイルには、ライセンス エントリが 5 つあります。どのライセンス エントリでも最初の行の先頭の語は、どのタイプのライセンスであるかを示します。これは、Feature または Increment ライセンスのいずれかになります。Feature（機能）ライセンスは、単一アイテムの固定

ライセンスです。Increment（増分）ライセンスは、追加型のライセンスです。MSE では、個々のサービス エンジンが Increment ライセンスとして扱われます。

最初の行の 2 番めの語は、ライセンス付与する特定のコンポーネントを定義します（MSE など）。3 番めの語はライセンスのベンダーを示します（Cisco など）。4 番めの語はライセンスのバージョンを示します（1.0 など）。5 番めの語は有効期限を示します。これは、期限のないライセンスの場合は permanent、それ以外の場合は dd-mmm-yyyy の形式の日付になります。最後の語は、このライセンスをカウントするかどうかを定義します。

MSE ライセンスの取り消しと再使用

MSE アプリケーション ライセンスをあるシステムから取り消し、別のシステムで再使用できます。ライセンスを取り消すと、ライセンス ファイルはシステムから削除されます。ライセンスを別のシステムで再使用する場合は、ライセンスをリホストする必要があります。

別のシステムでアップグレード SKU を使用してライセンスを再使用する場合は、対応する Base ライセンス SKU を、アップグレード SKU を再使用するシステムにインストールする必要があります。対応する Base ライセンス SKU がシステムから削除された場合、そのシステムではアップグレード ライセンス SKU を再使用できません。

ライセンスを取り消すと、ライセンスに対して変更を反映するため、MSE により個別のサービス エンジンが再起動されます。次に、サービス エンジンは、起動時に MSE から更新された容量を受け取ります。

ライセンスの詳細については、『*Cisco Prime Infrastructure Configuration Guide, Release 1.4*』を参照してください。

注意事項と制約事項

MSE を Prime Infrastructure に追加し、デバイスおよび wIPS 製品認証キーを登録する場合、次のガイドラインに従います。

- リリース 7.5 以降は、wIPS サービスには個別の MSE が必要です。
- 新しい MSE を追加すると、ネットワーク設計（キャンパス、ビルディング、および屋外マップ）、Cisco WLC、スイッチ（Catalyst 3000 シリーズおよび 4000 シリーズのみ）、および Mobility Services Engine のイベント グループと Prime Infrastructure を同期できます。

（注） リリース 7.5 以降は、Cisco Engine for Clients and Tags を使用してタグを追跡します。リリース 7.2 以降からリリース 7.5 にアップグレードした場合にタグのライセンスが検出されると、AeroScout ライセンスとエンジンの削除に関する警告メッセージが表示されます。承諾すると、すべてのパートナー エンジンのサブ サービスが削除され、その後 Cisco Tag Engine サブ サービスがデフォルトで有効になります。パートナー エンジンの削除を承諾しない場合は、インストールを続行します。アップグレード時にタグのライセンスが検出されない場合、インストールはそのまま進行します。

- 自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、MSE を Prime Infrastructure に追加する際に変更後の値をここで入力します。デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

Prime Infrastructure へのモビリティ サービス エンジンの追加

[Mobility Service] ページの [Add Mobility Services Engine] ダイアログボックスを使用して MSE を追加できます。このダイアログボックスでは、ライセンス ファイルと追跡パラメータを追加し、マップを MSE に割り当てることができます。設定のために既存の MSE でウィザードを起動する場合、[Add MSE] オプションの代わりに [Edit MSE Details] として表示されます。

ヒント Cisco Adaptive wIPS 機能の詳細については、http://www.cisco.com/ にアクセスして、マルチメディア プレゼンテーションをご覧ください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールがあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

（注） Prime Infrastructure リリース 1.0 は MSE 3355 を認識し、適切にサポートしています。

（注） [Services] > [Mobility Services Engine] ページは、リリース 7.3.101.0 の仮想ドメインでのみ使用可能です。

Mobility Services Engine を Prime Infrastructure に追加するには、Prime Infrastructure にログインし、以下のステップに従います。

ステップ 1 Mobility Services Engine に対して ping を実行できることを確認します。

ステップ 2 [Services] > [Mobility Services] > [Mobility Services Engines] の順に選択し、[Mobility Services] ページを表示します。

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

ステップ 4 [Device Name] テキスト ボックスに、MSE の名前を入力します。

ステップ 5 [IP Address] テキスト ボックスに、MSE の IP アドレスを入力します。

ステップ 6 （任意）[Contact Name] テキスト ボックスに、MSE 管理者の名前を入力します。

ステップ 7 [User Name] および [Password] テキスト ボックスに、MSE のユーザ名とパスワードを入力します。これは、設定時に作成された Prime Infrastructure 通信ユーザ名とパスワードです。

設定時にユーザ名とパスワードを指定しなかった場合は、デフォルトを使用します。

デフォルトのユーザ名とパスワードはどちらも *admin* です。

（注） 自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、変更後の値をここに入力してください。デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

ステップ 8 [HTTPS] チェックボックスをオンにして、MSE とサードパーティ アプリケーションの間の通信を許可します。デフォルトでは、Prime Infrastructure は MSE との通信に HTTPS を使用します。

ステップ 9 MSE からすべてのサービス割り当てを完全に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。
このオプションは、ネットワーク設計、有線スイッチ、Cisco WLC、およびイベント定義に適用されます。既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 10 [Next] をクリックします。Prime Infrastructure により、選択されている要素と MSE が自動的に同期されます。
同期完了後、[MSE License Summary] ページが表示されます。[MSE License Summary] ページから、ライセンスのインストール、ライセンスの追加、ライセンスの削除、アクティベーション ライセンスのインストール、サービス ライセンスのインストールを実行します。[Select Mobility Service] ページが表示されます。

ステップ 11 Mobility Services Engine 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスには Context-Aware Service および wIPS が含まれます。
CAS を選択すると、クライアント、不正アクセス ポイント、干渉、有線クライアント、およびタグを追跡できます。

タグを追跡するために、[Cisco Tag Engine] を選択します。

ステップ 12 [Save] をクリックします。

（注） 新しい MSE を追加すると、Prime Infrastructure を使用して、ネットワーク設計（キャンパス、ビルディング、および屋外マップ）、Cisco WLC、スイッチ（Catalyst シリーズ 3000 のみ）、およびローカル MSE のイベント グループを同期できます。この同期は、新しい MSE を追加した直後、または後で実行できます。ローカルデータベースと Prime Infrastructure データベースを同期するには、Mobility Services Engine の同期, （33 ページ）を参照してください。

Mobility Services Engine でのサービスの有効化

Mobility Services Engine 上のサービスを有効にするには、以下のステップに従います。

ステップ 1 ライセンス ファイルを追加すると、[Select Mobility Service] ページが表示されます。

ステップ 2 MSE 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスのタイプは次のとおりです。

- [Context Aware Service]：[Context Aware Service] チェックボックスをオンにすると、ロケーション計算を実行するためにロケーションエンジンを選択する必要があります。[CAS to track clients]、[rogues]、[interferers]、および [tags] を選択できます。クライアントとタグに [Cisco Context-Aware Engine] を選択し、タグを追跡できます。
- [Wireless Intrusion Prevention System]：[Wireless Intrusion Prevention System] チェックボックスをオンにすると、無線およびパフォーマンスの脅威が検出されます。
- [Mobile Concierge Service]：[Mobile Concierge Service] チェックボックスをオンにすると、モバイル デバイスで使用可能なサービスが記述されるサービス アドバタイズメントが提供されます。
- [CMX Analytics Service]：[CMX Analytics Service] チェックボックスをオンにすると、MSE からの Wi-Fi デバイス位置データを分析するためにパッケージされた各種データ分析ツールを利用できます。

（注） リリース 7.5 以降は、wIPS サービスが同一 MSE 上の CAS と wIPS をサポートしないため、専用の MSE が必要になります。

ステップ 3 [Next] をクリックして、追跡パラメータを設定します。

ステップ 4 MSE でサービスを有効にすると、[Select Tracking & History Parameters] ページが表示されます。

（注） 追跡パラメータの設定を省略すると、デフォルト値が選択されます。

ステップ 5 追跡するクライアントを選択するには、対応する [Tracking] チェックボックスをオンにします。追跡パラメータを以下に示します。

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

ステップ 6 デバイスの履歴トラッキングを有効にするには、対応するデバイスのチェックボックスをオンにします。履歴パラメータを以下に示します。

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

（注） 履歴トラッキングが無効の場合は、MSE サービスは機能しません。

ステップ 7 [Next] をクリックして MSE にマップを割り当てます。

（注） [Assigning Maps] ページは、MSE で有効にするサービスの 1 つとして CAS を選択する場合にだけ使用可能です。

ステップ 8 MSE 追跡パラメータおよび履歴パラメータを設定すると、[Assigning Maps] ページが表示されます。[Assign Maps] ページには以下の情報が表示されます。

- Map Name
- [Type]（ビルディング、フロア、キャンパス）
- Status（ステータス）

ステップ 9 必要なマップ タイプを確認するには、ページで使用可能な [Filter] オプションから [All]、[Campus]、[Building]、[Floor Area]、または [Outdoor Area] を選択します。

ステップ 10 マップを同期するには、[Name] チェックボックスをオンにし、[Synchronize] をクリックします。ネットワーク設計の同期が完了すると、特定のネットワーク設計で AP が割り当てられている適切な Cisco WLC が MSE と自動的に同期されます。[Done] をクリックして MSE 設定を保存します。

MSE 追跡パラメータおよび履歴パラメータの設定

ステップ 1 Mobility Services Engine でサービスを有効にすると、[Select Tracking & History Parameters] ページが表示されます。

（注） 追跡パラメータの設定を省略すると、デフォルト値が選択されます。

ステップ 2 追跡するクライアントを選択するには、対応する [Tracking] チェックボックスをオンにします。追跡パラメータを以下に示します。

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

ステップ 3 デバイスの履歴トラッキングを有効にするには、対応するデバイスのチェックボックスをオンにします。履歴パラメータを以下に示します。

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

ステップ 4 [**Next**] をクリックして MSE にマップを割り当てます。

MSE へのマップの割り当て

（注） [Assigning Maps] ページは、MSE で有効にするサービスの 1 つとして CAS を選択する場合にだけ使用可能です。

MSE にマップを割り当てるには、以下のステップに従います。

ステップ 1 MSE 追跡パラメータおよび履歴パラメータを設定すると、[Assigning Maps] ページが表示されます。[Assign Maps] ページには以下の情報が表示されます。

- Map Name
- [Type]（ビルディング、フロア、キャンパス）
- Status（ステータス）

ステップ 2 必要なマップ タイプを確認するには、ページで使用可能な [Filter] オプションから [All]、[Campus]、[Building]、[Floor Area]、または [Outdoor Area] を選択します。

ステップ 3 マップを同期するには、[Name] チェックボックスをオンにし、[Synchronize] をクリックします。ネットワーク設計の同期が完了すると、特定のネットワーク設計で AP が割り当てられている適切な Cisco WLC が MSE と自動的に同期されます。[Done] をクリックして MSE 設定を保存します。

MSE ライセンス ファイルの削除

MSE ライセンス ファイルを削除するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Service Engine] の順に選択します。
[Mobility Services] ページが表示されます。

ステップ 2 対応する [Device Name] チェック ボックスをオンにして、削除する Mobility Services Engine を選択します。

ステップ 3 [Select a command] ドロップダウン リストから [Edit Configuration] を選択します。
[Edit Mobility Services Engine] ダイアログボックスが表示されます。

ステップ 4 [Edit Mobility Services Engine] ダイアログボックスの [Next] をクリックします。
[MSE License Summary] ページが表示されます。

ステップ 5 [MSE License Summary] ページで削除する MSE ライセンス ファイルを選択します。

ステップ 6 [Remove License] をクリックします。

ステップ 7 [OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてライセンスを削除せずにこのページを閉じます。

Prime Infrastructure からのモビリティ サービス エンジンの削除

Prime Infrastructure データベースから 1 つ以上の Mobility Services Engine を削除するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services]> [Mobility Services Engines] の順に選択します。
[Mobility Services] ページが表示されます。

ステップ 2 削除する MSE を選択するため、対応する [Device Name] チェックボックスをオンにします。

ステップ 3 [Select a command] ドロップダウン リストから [Delete Service(s)] を選択します。[Go] をクリックします。

ステップ 4 選択した MSE を Prime Infrastructure データベースから削除することを確定するには、[OK] をクリックします。

ステップ 5 削除を中止するには、[Cancel] をクリックします。

デバイスと wIPS 製品認証キーの登録

CAS 要素、wIPS、またはタグのライセンスをシスコに発注すると、製品認証キー（PAK）が配布されます。Mobility Services Engine 上にインストールするライセンス ファイルを受け取るには、PAK を登録する必要があります。PAK の登録に成功すると、ライセンス ファイルが電子メールで送信されます。クライアントおよびワイヤレス IPS の PAK は、シスコに登録します。

インストールするライセンス ファイルを入手するために PAK を登録するには、以下のステップに従います。

ステップ 1 Web ブラウザで、http://tools.cisco.com/SWIFT/LicensingUI/Homeに移動します。

ステップ 2 PAK を入力し、[SUBMIT] をクリックします。

ステップ 3 ライセンスの購入内容を確認します。正しい場合は [Continue] をクリックします。ライセンス入力ページが表示されます。

（注） ライセンスが正しくない場合は、[TAC Service Request Tool] URL をクリックして問題をレポートしてください。

ステップ 4 [Designate Licensee] ページで、[Host Id] テキスト ボックスに MSE の UDI を入力します。これは、ライセンスがインストールされている Mobility Services Engine です。

（注） MSE の UDI 情報は、[Services] > [Mobility Services Engine] > [Device Name] > [System] の [General Properties] に表示されます。

ステップ 5 [Agreement] チェックボックスをオンにします。[Agreement] チェックボックスの下に登録者情報が表示されます。

ステップ 6 登録者とエンド ユーザが異なる場合は、登録者情報の下の [Licensee (End-User)] チェックボックスをオンにしてエンド ユーザ情報を入力します。

ステップ 7 [Continue] をクリックします。入力したデータの概要が表示されます。

ステップ 8 [Finish and Submit] ページで、登録者データとエンド ユーザ データを確認します。情報を訂正するには、[Edit Details] をクリックします。[Submit] をクリックします。`確認用のページが表示されます。

デバイスおよび wIPS ライセンス ファイルのインストール

Prime Infrastructure からデバイス ライセンスと wIPS ライセンスをインストールできます。リリース 7.5 以降は、Cisco Engine for Clients and Tags を使用してタグを追跡します。リリース 7.2 以降からリリース 7.5 にアップグレードした場合にタグのライセンスが検出されると、AeroScout ライセンスとエンジンの削除に関する警告メッセージが表示されます。承諾すると、すべてのパートナー エンジンのサブ サービスが削除され、その後 Cisco Tag Engine サブ サービスがデフォルトで有効になります。パートナー エンジンの排除を承諾しない場合、インストールが続行されます。タグのライセンスが検出されない場合、インストールはそのまま進行します。

[Administration] > [License Center] ページは、リリース 7.3.101.0 以降の仮想ドメインでのみ使用可能です。

PAK の登録後にクライアント ライセンスまたは wIPS ライセンスを Prime Infrastructure に追加するには、以下のステップに従います。

ステップ 1 [Administration] > [License Center]> [Licenses] の順に選択します。

ステップ 2 左側のサイドバー メニューから、[Files] > [MSE Files] の順に選択します。

ステップ 3 [Add] をクリックします。[Add a License File] ダイアログボックスが表示されます。

ステップ 4 [MSE Name] ドロップダウン リストから該当する MSE 名を選択します。

（注） 選択されている Mobility Services Engine の UDI が、PAK 登録時に入力したものと一致していることを確認します。

ステップ 5 [Choose File]> [Browse] をクリックし、ライセンス ファイルを選択します。

ステップ 6 [Upload]> [OK] をクリックします。新たに追加されたライセンスが MSE ライセンス ファイル リストに表示されます。

第 3 章

Mobility Services Engine の同期

この章では、Cisco WLC と Prime Infrastructure を Cisco Mobility Services Engine と同期する方法について説明します。

（注） [Services] タブの [Mobility Services Engines]、[Synchronization History]、[High Availability]、[Context-Aware Notifications]、および [MSAP] ページは、リリース 7.3.101.0 でのみ使用できます。

- Prime Infrastructure と Mobility Services Engine の同期，33 ページ
- Mobility Services Engine の同期の前提条件，34 ページ
- サードパーティ要素の操作，35 ページ
- Cisco WLC と Mobility Services Engine の同期，35 ページ
- データベースの自動同期および Out-of-Sync アラートの設定，38 ページ
- Mobility Services Engine 同期ステータスの表示，40 ページ

Prime Infrastructure と Mobility Services Engine の同期

ここでは、Prime Infrastructure と Mobility Services Engines を手動および自動的に同期する方法を説明します。

（注） [Services] > [Synchronize Services] ページは、リリース 7.3.101.0 以降の仮想ドメインでのみ使用可能です。

Prime Infrastructure に MSE を追加したら、ネットワーク設計（キャンパス、ビルディング、フロア、および屋外マップ）、コントローラ（名前と IP アドレス）、特定の Catalyst 3000 シリーズおよび 4000 シリーズ スイッチ、およびイベント グループを MSE と同期できます。

- ネットワーク設計：施設全体でのアクセス ポイントの物理的配置の論理マッピング。1 つのキャンパス、そのキャンパスを構成するビルディング、および各ビルディングのフロアという階層構造が、1 つのネットワーク設計を構成します。
- Cisco WLC：関連があり、ロケーション情報を MSE と定期的に交換する選択済み Cisco WLC です。定期的な同期により、正確なロケーション情報を維持できます。
- 有線スイッチ：ネットワーク上の有線クライアントへのインターフェイスを提供する有線 Catalyst スイッチ。定期的な同期によって、ネットワーク上の有線クライアントのロケーションが正確に追跡されます。
  - MSE は、Catalyst スタッカブル スイッチ（3750、3750-E、3560、2960、IE-3000 スイッチ）、スイッチ ブレード（3110、3120、3130、3040、3030、3020）、およびスイッチ ポートと同期できます。
  - また、次の Catalyst 4000 シリーズ スイッチと同期することもできます。WS-C4948、WS-C4948-10GE、ME-4924-10GE、WS-4928-10GE、WS-C4900M、WS-X4515、WS-X4516、WS-X4013+、WS-X4013+TS、WS-X4516-10GE、WS-X4013+10GE、WS-X45-SUP6-E、WS-X45-SUP6-LE。
- イベント グループ：イベントを生成するトリガーを定義する事前定義イベントのグループ。定期的な同期により、最新の定義イベントが追跡されます。イベント グループはサードパーティ アプリケーションでも作成できます。サードパーティ アプリケーションにより作成されたイベント グループの詳細については、データベースの自動同期および Out-of-Sync アラートの設定，（38 ページ）を参照してください。
- サードパーティ要素：要素を MSE と同期する場合、サードパーティ アプリケーションにより MSE にイベント グループが作成されていることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。
- サービス アドバタイズメント：モバイル コンシェルジュ サービスは、モバイル デバイスにサービス アドバタイズメントを提供します。これにより、MSE と同期されたサービス アドバタイズメントが示されます。

Mobility Services Engine の同期の前提条件

- 同期を実行する前に、Cisco WLC、Prime Infrastructure、および Mobility Services Engine 間のソフトウェアの互換性を確認してください。http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html で、Mobility Services Engine の最新リリース ノートを参照してください。
- MSE、Prime Infrastructure、および Cisco WLC 間の通信は、協定世界時（UTC）で実行されます。各システムで NTP を設定すると、デバイスに UTC 時刻が提供されます。MSE とその関連コントローラは、同一 NTP サーバと同一 Prime Infrastructure サーバにマップする必要があります。NTP サーバは、コントローラ、Prime Infrastructure、および MSE 間で時刻を自動的に同期する必要があります。ただし、MSE およびコントローラのタイムゾーンは引き続き

UTC に設定する必要があります。これは、wIPS アラームには MSE とコントローラの時刻を UTC に設定する必要があるからです。

サードパーティ要素の操作

要素を MSE と同期する場合、MSE にサードパーティ アプリケーションによって作成されたイベント グループがあることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。

要素の削除またはサード パーティ要素としてのマーキング

要素を削除またはサード パーティ要素としてマークするには、以下のステップに従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。
[Network Designs] ページが表示されます。

ステップ 2 [Network Designs] ページで、左側のサイドバーのメニューから [Third Party Elements] を選択します。
[Third Party Elements] ページが表示されます。

ステップ 3 1 つ以上の要素を選択します。

ステップ 4 次のいずれかのボタンをクリックします。

- [Delete Event Groups]：選択されているイベント グループを削除します。
- [Mark as 3rd Party Event Group(s)]：選択されているイベント グループをサードパーティ イベント グループとしてマークします。

Cisco WLC と Mobility Services Engine の同期

ここでは、Cisco WLC を同期し、MSE を任意の Cisco WLC に割り当て、ネットワーク設計、Cisco WLC、有線スイッチ、またはイベント グループを Mobility Services Engine から割り当て解除する方法について説明します。

- ネットワーク設計、Cisco WLC、Catalyst スイッチ、またはイベント グループの割り当てと同期, （36 ページ）
- Cisco WLC への MSE の割り当て, （37 ページ）
- ネットワーク設計、有線スイッチ、またはイベント グループの MSE からの割り当て解除, （38 ページ）

ネットワーク設計、Cisco WLC、Catalyst スイッチ、またはイベント グループの割り当てと同期

ネットワーク設計、Cisco WLC、Catalyst スイッチ、またはイベント グループを Mobility Services Engine と同期するには、以下のステップに従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。
左側のサイドバーのメニューには、[Network Designs]、[Controllers]、[Event Groups]、[Wired Switches]、[Third Party Elements]、および [Service Advertisements] のオプションがあります。

ステップ 2 左側のサイドバーのメニューから、該当するメニュー オプションを選択します。

ステップ 3 MSE にネットワーク設計を割り当てるには、[Synchronize Services] ページの左側のサイドバーのメニューから、[Network Designs] を選択します。
[Network Designs] ページが表示されます。

ステップ 4 対応する [Name] チェックボックスをオンにして、MSE と同期させるすべてのマップを選択します。

（注） リリース 6.0 では、MSE に割り当てることができる最も詳細なレベルはキャンパス レベルです。リリース 7.0 以降では、このオプションはフロア レベルまで拡大されました。たとえば、floor1 を MSE 1 に、floor2 を MSE 2 に、floor3 を MSE 3 に割り当てることを選択できます。

ステップ 5 [Change MSE Assignment] をクリックします。

ステップ 6 マップと同期する MSE を選択します。

ステップ 7 [MSE Assignment] ダイアログボックスで次のいずれかをクリックします。

- [Synchronize]：MSE 割り当てを同期します。
- [Cancel]：MSE 割り当ての変更内容を取り消し、[Network Designs] ページに戻ります。

また、[Reset] をクリックして MSE 割り当てを取り消すこともできます。

（注） ネットワーク設計には、キャンパス内のフロアや、複数のビルディングが含まれている大規模キャンパス（各ビルディングが異なる MSE によりモニタされる）などがあります。このため、単一ネットワーク設計を複数の MSE に割り当てる必要がある場合があります。ネットワーク設計割り当てでは、同期対象の Cisco WLC が自動的に選択されます。

ステップ 8 [Synchronize] をクリックし、MSE データベースを更新します。
項目が同期されると、同期済みエントリの [Sync. Status] 列に緑色の 2 つの矢印のアイコンが表示されます。

有線スイッチまたはイベント グループを MSE に割り当てるときにも同じ手順を使用できます。MSE に Cisco WLC をり当てるには、「コントローラと Mobility Services Engine の同期」（3-3 ページ）を参照してください。

（注） 正しく同期できるように WLC と MSE の間のクロックを同期することが重要です。同期が失敗した場合は、この 2 つのデバイスが同じ NTP クロック ソースを共有しているかを確認します。

Cisco WLC への MSE の割り当て

サービス単位（CAS または wIPS）で Mobility Services Engine を任意の Cisco WLC に割り当てるには、以下のステップに従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。

ステップ 2 [Network Designs] ページで、左側のサイドバーのメニューから [Controller] を選択します。

ステップ 3 対応する [Name] チェックボックスをオンにして、Mobility Services Engine に割り当てる Cisco WLC を選択します。

ステップ 4 [Change MSE Assignment] をクリックします。

ステップ 5 [Choose MSEs] ダイアログ ボックスが表示されます。[CAS]、[wIPS]、または [MSAP] オプションを選択できます。

ステップ 6 Cisco WLC を同期する必要のある MSE を選択します。

ステップ 7 [Choose MSEs] ダイアログボックスで次のいずれかをクリックします。

- [Synchronize]：MSE 割り当てを同期します。
- [Cancel]：MSE 割り当ての変更内容を取り消し、[Controllers] ページに戻ります。

  また、[Reset] をクリックして MSE 割り当てを取り消すこともできます。

ステップ 8 [Synchronize] をクリックし、同期プロセスを実行します。

ステップ 9 MSE が、選択されているサービスの各 Cisco WLC とだけで通信していることを確認します。これは、ステータス ページの [NMSP status] リンクをクリックして確認できます。

（注） Cisco WLC の同期後、関連付けられている Cisco WLC でタイムゾーンが設定されていることを確認します。

（注） MSE と同期するコントローラの名前は固有でなければなりません。同じ名前のコントローラが 2 つある場合は 1 つの Cisco WLC だけが同期されます。Catalyst スイッチまたはイベント グループを MSE に割り当てるときにも同じ手順を使用できます。

（注） スイッチは、1 つの MSE とだけ同期できます。ただし、MSE には複数のスイッチを接続できます。

ネットワーク設計、有線スイッチ、またはイベント グループの MSE からの割り当て解除

Mobility Services Engine からネットワーク設計、コントローラ、有線スイッチ、またはイベント グループの割り当てを解除するには、以下のステップに従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。

ステップ 2 左側のサイドバーのメニューから、該当するメニュー オプションを選択します。

ステップ 3 [Name] チェックボックスをオンにして 1 つ以上の要素を選択し、[Change MSE Assignment] をクリックします。
[Choose MSEs] ダイアログボックスが表示されます。

ステップ 4 該当するタブで 1 つ以上の要素をクリックし、[Change MSE Assignment] をクリックします。

ステップ 5 MSE に要素を関連付けない場合は、[CAS] または [MSAP] のいずれかのチェックボックスをオンにして MSE の選択を解除します。

ステップ 6 [Synchronize] をクリックします。
[Sync Status] 列がブランクになります。

ステップ 7 [Cancel] をクリックすると、MSE 割り当ての変更を破棄し、[Controllers] ページに戻ります。

データベースの自動同期および Out-of-Sync アラートの設定

Prime Infrastructure と Mobility Services Engine のデータベースの手動同期はただちに実行されます。ただし、将来のデプロイメントの変更（マップやアクセス ポイントの位置の変更など）が原因で、再同期までは、ロケーションの計算やアセットの追跡が正しく行われないことがあります。

同期していない状態が発生しないようにするため、Prime Infrastructure を使用して同期を実行します。このポリシーにより、Prime Infrastructure と MSE のデータベース間の同期が定期的に実行され、関連アラームがすべてクリアされます。

1 つ以上の同期コンポーネントに加える変更は、MSE と自動的に同期されます。たとえば、アクセス ポイントが設置されているフロアを特定の MSE と同期し、その後 1 つのアクセス ポイントが同じフロアの新しいロケーション、または別のフロア（MSE と同期されるフロア）に移動すると、アクセス ポイントの変更後のロケーションが自動的に伝達されます。

Prime Infrastructure と MSE が同期されるようにするため、バックグラウンドでスマート同期が実行されます。

- データベースの自動同期の設定，（39 ページ）
- スマート コントローラの割り当てと選択のシナリオ，（39 ページ）
- Out-of-Sync アラーム，（40 ページ）

データベースの自動同期の設定

スマート同期を設定するには、以下のステップに従います。

ステップ 1 [Administration] > [Background Tasks] の順に選択します。

ステップ 2 [Mobility Service Synchronization] チェック ボックスを選択し、[Mobility Service Synchronization] へのリンクをクリックします。
[Mobility Services Synchronization] ページが表示されます。

ステップ 3 Mobility Services Engine が Out-of-Sync アラートを送信するように設定するには、[Out of Sync Alerts] の [Enabled] チェックボックスをオンにします。

ステップ 4 スマート同期を有効にするには、[Smart Synchronization] の [Enabled] チェックボックスをオンにします。

（注） スマート同期は、MSE に割り当てられていない要素（ネットワーク設計、コントローラ、またはイベント グループ）には適用されません。ただし、これらの未割り当て要素に関する out-of-sync アラームは生成されます。スマート同期をこれらの要素に適用するには、これらの要素を MSE に手動で割り当てる必要があります。

（注） Prime Infrastructure に MSE が追加されると、Prime Infrastructure のデータは常に、MSE と同期するプライマリ コピーとして扱われます。MSE に含まれているが、Prime Infrastructure には含まれていない同期対象のネットワーク設計、コントローラ、イベント グループ、および有線スイッチはすべて、MSE から自動的に削除されます。

ステップ 5 スマート同期の実行間隔を分数単位で入力します。
デフォルトでは、スマート同期は有効になっています。

ステップ 6 [Submit]> [Save] をクリックします。
スマート コントローラの割り当てと選択のシナリオについては、スマート コントローラの割り当てと選択のシナリオ，（39 ページ）を参照してください。

スマート コントローラの割り当てと選択のシナリオ

シナリオ 1

[Synchronize Services] ページの [Network Designs] メニューで、コントローラからのアクセス ポイントが 1 つ以上存在するフロアを Mobility Services Engine と同期することを選択した場合、アクセス ポイントに接続しているコントローラが、CAS サービスの Mobility Services Engine への割り当て対象として自動的に選択されます。

シナリオ 2

コントローラからの 1 つ以上のアクセス ポイントが、Mobility Services Engine と同期されるフロアに配置されている場合、アクセス ポイントに接続しているコントローラは、CAS サービスの同じ MSE に自動的に割り当てられます。

シナリオ 3

アクセス ポイントがフロアに追加され、MSE に割り当てられます。このアクセス ポイントをコントローラ A からコントローラ B に移動すると、コントローラ B が MSE と自動的に同期されます。

シナリオ 4

MSE と同期するフロアに配置されているすべてのアクセス ポイントが削除されると、そのコントローラは自動的に MSE 割り当てから削除されるか、または同期されなくなります。

Out-of-Sync アラーム

Out-of-Sync アラームは、重大度が Minor（黄色）のアラームであり、次の条件に対して出されます。

- Prime Infrastructure で要素が変更される（自動同期ポリシーによりこれらの要素がプッシュされます）。
- Cisco WLC 以外の要素が Mobility Services Engine データベースに存在するが、Prime Infrastructure に存在しない。
- 要素が MSE に割り当てられていない（自動同期ポリシーは適用されません）。

Out-of-Sync アラームは、次の条件が発生するとクリアされます。

- MSE が削除される

（注） MSE を削除すると、そのシステムの Out-of-Sync アラームも削除されます。また、使用可能な最後の MSE を削除すると、「どのサーバにも割り当てられていない要素」のイベントに対するアラームが削除されます。

- 要素が手動または自動で同期される
- ユーザがアラームを手動でクリアする（ただしスケジュールされているタスクが次回実行されるときに、アラームが再び表示される可能性があります）

Mobility Services Engine 同期ステータスの表示

Prime Infrastructure でサービスの同期機能を使用して、ネットワーク設計、コントローラ、スイッチ、およびイベント グループと Mobility Services Engine との同期のステータスを表示できます。

- Mobility Services Engine 同期ステータスの表示, （41 ページ）
- 同期履歴の表示, （41 ページ）

Mobility Services Engine 同期ステータスの表示

同期ステータスを表示するには、以下のステップに従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。

ステップ 2 左側のサイドバーのメニューから、[Network Designs]、[Controllers]、[Wired Switches]、[Third Party Elements]、または [Service Advertisements] を選択します。
各要素の [Sync. Status] 列に、同期ステータスが表示されます。緑色の 2 つの矢印のアイコンは、対応する要素が指定サーバ（Mobility Services Engine など）と同期されていることを示します。灰色の 2 つの矢印と赤い円のアイコンは、対応する項目が指定のサーバと同期していないことを示します。

[Message] 列には、要素が同期していない場合の障害の原因が表示されます。

[Monitor] > [Maps] > [System Campus] > [Building] > [Floor] の順に選択して、同期ステータスを表示することもできます。

このビルディングはキャンパス内のビルディング、フロアはキャンパス ビルディング内の特定のフロアです。

左側のサイドバーのメニューの [MSE Assignment] オプションに、フロアが現在割り当てられている Mobility Services Engine が表示されます。このページから Mobility Services Engine 割り当てを変更することもできます。

同期履歴の表示

Mobility Services Engine の過去 30 日間の同期履歴を表示できます。アラームが自動的にクリアされるため、これは特に自動同期が有効な場合に便利です。同期履歴には、クリアされたアラームの要約が表示されます。

同期履歴を表示するには、[Services] > [Synchronization History] の順に選択します。[Synchronization History] ページが表示されます。次の表に、[Synchronization History] ページのパラメータを示します。

表 *7*：*[Synchronization History]* ページ

テキスト ボックス	説明
Timestamp	同期が実行された日時。
サーバ	Mobility Services Engine サーバ。
Element Name	同期された要素の名前。
タイプ	同期された要素のタイプ。

テキスト ボックス	説明
Sync Operation	実行された同期動作。 [Update]、[Add]、または [Delete] です。
Generated By	同期の方法。 [Manual] または [Automatic] です。
Status（ステータス）	同期のステータス。[Success] または [Failed] のいずれかです。
メッセージ	同期に関するその他のメッセージ。

第 4 章

システム プロパティの設定および表示

この章では、Cisco Mobility Services Engine でシステム プロパティを設定および表示する方法を説明します。

- ライセンス要件，43 ページ
- 一般プロパティの編集およびパフォーマンスの表示，43 ページ
- NMSP パラメータの変更，47 ページ
- システムのアクティブ セッションの表示，48 ページ
- トラップ宛先の追加および削除，49 ページ
- 詳細パラメータの表示および設定，51 ページ

ライセンス要件

Mobility Services Engine には CAS および wIPS の評価ライセンスが付属しています。評価版は 60 日間（480 時間）有効で、各サービスに対してデバイスの制限が事前設定されています。これらは、120 日間のライセンスとともに提供されます（残り日数は暦上の経過日数ではなく、使用した日数によって減少します）。

ライセンスの購入およびインストールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

一般プロパティの編集およびパフォーマンスの表示

[General Properties]：Cisco Prime Infrastructure を使用して Mobility Services Engine の一般プロパティを編集できます。一般プロパティには、連絡先名、ユーザ名、パスワード、システム上で有効なサービス、サービスの有効化または無効化、同期のための MSE の有効化などがあります。詳細については、一般プロパティの編集，（44 ページ）を参照してください。

（注） MSE の初期設定時に定義したユーザ名とパスワードを変更するには、一般プロパティを使用します。

[Performance]：Prime Infrastructure を使用して特定の MSE の CPU およびメモリの使用率を表示できます。詳細については、パフォーマンス情報の参照，（47 ページ）を参照してください。

ここでは、次の内容について説明します。

- 一般プロパティの編集，（44 ページ）
- パフォーマンス情報の参照，（47 ページ）

一般プロパティの編集

Mobility Services Engine の一般プロパティを編集するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services]> [Mobility Services Engines] の順に選択して、[Mobility Services] ページを表示します。

ステップ 2 編集する MSE の名前をクリックします。[General] と [Performance] の 2 つのタブが表示されます。

（注） デフォルトで [General Properties] ページが表示されない場合は、左側のサイドバーのメニューから [Systems] > [General Properties] の順に選択します。

ステップ 3 [General] タブで、必要に応じてフィールドを変更します。この表に、[General Properties] ページのフィールドを示します。

表 *8*：*[General]* タブ

フィールド	設定オプション
Device Name	MSE のユーザ定義名です。
Device Type	MSE のタイプ（Cisco 3310 MSE など）を示します。デバイスが仮想アプライアンスであるかどうかを示します。
Device UDI	デバイス UDI（Unique Device Identifier）ストリングは二重引用符で囲まれています（ストリングの末尾にスペースがある場合はスペースも含まれます）。
Version	製品 ID のバージョン
Start Time	サーバが起動された起動時刻を示します。
IP Address	MSE の IP アドレスを示します。
Contact Name	MSE の連絡先名を入力します。

フィールド	設定オプション
User Name	MSE を管理する Prime Infrastructure サーバのログイン ユーザ名を入力します。これにより、初期設定時に設定されたユーザ名を含む、以前に定義されたユーザ名が置き換えられます。
Password	MSE を管理する Prime Infrastructure サーバのログイン パスワードを入力します。これにより、初期設定時に設定されたパスワード名を含む、以前に定義されたパスワードが置き換えられます。
Legacy Port	HTTPS 通信をサポートするモビリティ サービスのポート番号を入力します。[Legacy HTTPS] オプションも有効にする必要があります。
Legacy HTTPS	これは MSE に適用されません。ロケーション アプライアンスにのみ適用されます。
Delete synchronized service assignments and enable synchronization	MSE からすべてのサービス割り当てを完全に削除するには、このチェックボックスをオンにします。このオプションが表示されるのは、MSE を追加するときに [Delete synchronized service assignments] チェックボックスをオフにした場合のみです。

フィールド	設定オプション
Mobility Services	MSE 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスには、Context Aware、wIPS、Mobile Concierge、CMX Analytics、CMX Browser Engage、Proxy サービスが含まれます。 CAS を選択すると、クライアント、不正アクセス ポイント、干渉、有線クライアント、およびタグを追跡できます。 タグを追跡するには、次のいずれかのエンジンを選択します。 • Cisco Tag Engine または • Partner Tag Engine （注） Partner Tag Engine は、タグ追跡にのみ使用します。クライアントは、引き続き Cisco Context-Aware Engine によって追跡されます。 （注） 選択すると、サービスは [Up]（アクティブ）として表示されます。アクティブでないサービスはすべて、選択された（現行）システム上およびネットワーク上で [Down]（非アクティブ）として表示されます。 （注） リリース 7.5 以降は、wIPS サービスが同一 MSE 上の CAS と wIPS をサポートしないため、専用の MSE が必要になります。 現在のシステムで割り当て可能なデバイスの数を確認するには、[here] リンクをクリックします。 ネットワーク上のすべての MSE のライセンスの詳細を表示するには、[License Center] ページで、左側のサイドバーのメニュー オプションから [MSE] を選択します。 （注） ライセンスの購入およびインストールの詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

（注） 次の tcp ポートはリリース 6.0 の MSE で使用中です。tcp：22 MSE SSH ポート、tcp 80：MSE HTTPポート、tcp 443：MSE HTTPS ポート、tcp 1411：、tcp 8001：レガシー・ポート。ロケーション API に使用されます。

（注） 次の udp ポートはリリース 6.0 の MSE で使用中です。udp：123 NTPD ポート（NTP 設定後にオープン）、udp 32768：ロケーション内部ポート。

（注） MSE で **enable http** コマンドを入力した場合、MSE でポート 80 が有効になります。CA が発行する証明書が MSE にインストールされている場合、MSE でポート 8880 および 8843 は閉じられます。

ステップ 4 [Save] をクリックし、Prime Infrastructure および MSE のデータベースを更新します。

パフォーマンス情報の参照

パフォーマンスの詳細を表示するには、以下のステップに従います。

ステップ 1 [Services] >> [Mobility Services] > [Mobility Services Engines] の順に選択し、[Mobility Services] ページを表示します。

ステップ 2 表示する Mobility Services Engine の名前をクリックします。[General] と [Performance] の 2 つのタブが表示されます。

ステップ 3 [Performance] タブをクリックします。

1 日を超える期間のパフォーマンスの数値を表示するには、y 軸上の期間（[1w] など）をクリックします。

パフォーマンスの概要をテキストで表示するには、CPU の下の 2 つ目のアイコンをクリックします。

ページを拡大するには、右下にあるアイコンをクリックします。

NMSP パラメータの変更

ネットワーク モビリティ サービス プロトコル（NMSP）は、Mobility Services Engine と Cisco WLC 間の通信を管理するプロトコルです。Mobility Services Engine と Cisco WLC 間のテレメトリ、緊急、およびチョークポイント情報の転送は、このプロトコルによって管理されます。

このメニュー オプションは、MSE Release 7.0.105.0 以前のみで使用できます。

- ネットワークの応答が遅くなっている場合や大幅な遅延が発生している場合を除き、デフォルトのパラメータ値を変更しないでおくことを推奨します。
- テレメトリ、緊急、およびチョークポイント情報は、コントローラおよびソフトウェア リリース 4.1 以降でインストールされた Prime Infrastructure でのみ表示されます。
- コントローラと MSE との通信には、TCP ポート 16113 が使用されます。コントローラと MSE の間にファイアウォールがある場合は、NMSP を機能させるにはこのポートが開放されている（ブロックされていない）ことが必要です。

NMSP パラメータを設定するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services]> [Mobility Services Engines] の順に選択します。

ステップ 2 プロパティを編集する MSE の名前をクリックします。

ステップ 3 [System] > [NMSP Parameters] の順に選択します。設定オプションが表示されます。

ステップ 4 必要に応じて、NMSP パラメータを変更します。次の表に、NMSP パラメータを示します。

表 *9*：*NMSP* パラメータ

フィールド	説明
IP Address	コントローラまたは IOS 3E スイッチの IP アドレス。
Target Type	コントローラのタイプ：コントローラまたは IOS 3E スイッチ。
Version	ターゲット デバイスのバージョン。
NMSP Status	MSE とターゲット タイプ間の NMSP 接続ステータス。
Echo Request Count	作成されたエコー要求の数。
Echo Response Count	受信したエコー要求の数。
Last Message Received	最後のメッセージを受信したときのタイムスタンプ。

ステップ 5 [Save] をクリックし、Prime Infrastructure および MSE のデータベースを更新します。

システムのアクティブ セッションの表示

Mobility Services Engine のアクティブなユーザ セッションを表示できます。

アクティブなユーザ セッションを表示するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 アクティブ セッションを表示する MSE の名前をクリックします。

ステップ 3 [System] > [Active Sessions] の順に選択します。
Prime Infrastructure は各セッションに関する次の情報を表示します。

- セッション ID
- MSE アクセス元の IP アドレス

- 接続ユーザのユーザ名
- セッションが開始された日時
- MSE が最後にアクセスされた日時
- 最終アクセス以降セッションがアイドルになっていた期間

トラップ宛先の追加および削除

Mobility Services Engine により生成される SNMP トラップを受信する Prime Infrastructure または Cisco Security Monitoring, Analysis, and Response System（CS-MARS）ネットワーク管理プラットフォームを指定できます。

ユーザが Prime Infrastructure を使用して Mobility Services Engine を追加すると、その Prime Infrastructure プラットフォームはデフォルトのトラップ宛先として自動的に確立されます。Prime Infrastructure に冗長設定がある場合、プライマリの Prime Infrastructure に障害が発生しバックアップ システムが引き継ぐまでは、バックアップ用の Prime Infrastructure はデフォルトのトラップ宛先としてリストされません。アクティブな Prime Infrastructure だけがトラップ宛先としてリストされます。

- トラップ宛先の追加, （49 ページ）
- トラップ宛先の削除, （51 ページ）

トラップ宛先の追加

トラップ宛先を追加するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 新しい SNMP トラップ宛先サーバを定義する Mobility Services Engine の名前をクリックします。

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

ステップ 4 [Select a command] ドロップダウン リストから、[Add Trap Destination] を選択します。[Go] をクリックします。

[New Trap Destination] ページが表示されます。

次の表は、[Trap Destination] ページのフィールドを示しています。

表 *10* : *[Add Trap Destination]* ページのフィールド

フィールド	説明
IP Address	トラップ宛先の IP アドレス。
Port Number	トラップ宛先のポート番号。デフォルト ポート番号は、162 です。
Destination Type	このフィールドは編集できず、値 [Other] が表示されます。
SNMP Version	[SNMP Version] ドロップダウン リストから [v2c] または [v3] を選択します。
SNMP バージョンとして v3 を選択した場合にだけ表示されるフィールドを以下に示します。	
ユーザ名	SNMP バージョン 3 のユーザ名。
Security Name	SNMP バージョン 3 のセキュリティ名。
Authentication Type	ドロップダウン リストから、次のいずれかのオプションを選択します。 **HMAC-MD5** **HMAC-SHA**
Authentication Password	SNMP バージョン 3 の認証パスワード。
Privacy Type	ドロップダウン リストから、次のいずれかのオプションを選択します。 **CBC-DES** **CFB-AES-128** **CFB-AES-192** **CFB-AES-256**
Privacy Password	SNMP バージョン 3 のプライバシー パスワード。

（注） 自動的に作成されるデフォルトのトラップ宛先を除き、すべてのトラップ宛先はその他として識別されます。

ステップ 5 [Save] をクリックします。
[Trap Destination Summary] ページが表示され、新たに定義されたトラップがリストされます。

トラップ宛先の削除

トラップ宛先を削除するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 SNMP トラップ宛先サーバを削除する Mobility Services Engine の名前をクリックします。

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

ステップ 4 削除するトラップ宛先エントリの横にあるチェックボックスをオンにします。

ステップ 5 [Select a command] ドロップダウン リストから、[Add Trap Destination] を選択します。[Go] をクリックします。

ステップ 6 表示されるダイアログボックスで、[OK] をクリックして削除を実行します。

詳細パラメータの表示および設定

[Prime Infrastructure Advanced Parameters] ページで、Mobility Services Engine の一般的なシステム レベル設定を表示し、モニタリング パラメータを設定することができます。

- 現在のシステム レベルの詳細なパラメータを表示するには、詳細パラメータ設定の表示を参照してください。
- 現在のシステム レベルの詳細パラメータを変更するか、またはシステムの再起動やシャットダウンなどの拡張コマンドを実行するか、またはコンフィギュレーション ファイルをクリアするには、詳細コマンドの開始を参照してください。

詳細パラメータ設定の表示

Mobility Services Engine の詳細パラメータ設定を表示するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 ステータスを表示する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Advanced Parameters] の順に選択します。[Advanced Parameters] ページが表示されます。

詳細パラメータの開始

Prime Infrastructure の [Advanced Parameters] ページでは、イベントを維持する日数およびセッション タイムアウト値を設定できます。また、システムの再起動またはシャットダウンを開始したり、システム データベースを消去したりできます。

（注） Prime Infrastructure を使用して、Mobility Services Engine またはロケーション アプライアンスのトラブルシューティング パラメータを変更できます。

[Advanced Parameters] ページで、次の目的で Prime Infrastructure を使用できます。

- イベントを維持する期間およびセッション タイムアウトまでの期間を設定する。

  詳細については、詳細パラメータの設定を参照してください。

- システムの再起動またはシャットダウンを開始したり、システムデータベースを消去する。

  詳細については、詳細コマンドの開始を参照してください。

詳細パラメータの設定

詳細パラメータを設定するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Advanced Parameters] の順に選択します。

ステップ 4 必要に応じて詳細パラメータを確認または変更します。

- 一般情報
  - 製品名
  - Version
  - Started At
  - Current Server Time
  - Hardware Resets
  - Active Sessions

- Advanced Parameters

  注意 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

  - [Number of Days to keep Events]：ログを維持する日数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。

- [Session Timeout]：セッションがタイムアウトになるまでの分数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。現時点では、このオプションは淡色表示されます。

- Cisco UDI
  - [Product Identifier (PID)]：MSE の製品 ID。
  - [Version Identifier (VID)]：MSE のバージョン番号。
  - [Serial Number (SN)]：MSE のシリアル番号。

- Advanced Commands
  - [Reboot Hardware]：モビリティ サービス ハードウェアを再起動する場合にクリックします。詳細については、システムの再起動またはシャットダウン，（54 ページ）を参照してください。
  - [Shutdown Hardware]：モビリティ サービス ハードウェアをオフにする場合にクリックします。詳細については、システムの再起動またはシャットダウン，（54ページ）を参照してください。
  - [Clear Database]：モビリティ サービス データベースをクリアする場合にクリックします。詳細については、システム データベースの消去，（54 ページ）を参照してください。Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除するには、[Retain current service assignments in the Prime Infrastructure] チェックボックスをオフにします。[Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。デフォルトでは、このオプションが選択されています。

ステップ 5 [Save] をクリックし、Prime Infrastructure および MSE のデータベースを更新します。

詳細コマンドの開始

システムの再起動またはシャットダウンを開始したり、システム データベースを消去するには、[Advanced Parameters] ページで該当するボタンをクリックします。

- システムの再起動またはシャットダウン
- システム データベースの消去

システムの再起動またはシャットダウン

Mobility Services Engine を再起動またはシャットダウンするには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 再起動またはシャットダウンする Mobility Services Engine の名前をクリックします。

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

ステップ 4 [Advanced Commands] グループ ボックスで、該当するボタン（[Reboot Hardware] または [Shutdown Hardware]）をクリックします。
確認のダイアログボックスで [OK] をクリックして、再起動またはシャットダウン プロセスを開始します。プロセスを中止するには、[Cancel] をクリックします。

システム データベースの消去

Mobility Services Engine 設定をクリアし、出荷時の初期状態に戻すには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

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

ステップ 4 Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除するには、[Advanced Commands] グループボックスの [Retain current service assignments in the Prime Infrastructure] チェックボックスをオフにします。
[Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。デフォルトでは、このオプションが選択されています。

ステップ 5 [Advanced Commands] グループ ボックスで [Clear Database] をクリックします。

ステップ 6 [OK] をクリックし、Mobility Services Engine データベースをクリアします。

第 5 章

Working with Maps

Maps provide a summary view of all your managed systems on campuses, buildings, outdoor areas, and floors.

- マップについて，55 ページ
- キャンパス マップの追加，61 ページ
- ビルディングの設定，62 ページ
- フロア領域の追加，68 ページ
- フロア領域のモニタリング，89 ページ
- マップ作成のための自動階層の使用方法，93 ページ
- Map Editor の使用，97 ページ
- チョークポイントを使用したタグの位置報告の精度の向上，105 ページ

マップについて

次世代マップ機能は、デフォルトで有効になっています。

次世代マップ機能には、次のような利点があります。

- マップで大量の情報を表示します。さまざまなクライアント、干渉、アクセスポイントがある場合、Prime Infrastructure のマップ ページの表示を乱す原因となり、ページのロードが遅くなる場合があります。リリース 7.3 は情報のクラスタリングおよび階層化を導入しています。情報のクラスタにより、高レベルでノイズを軽減し、オブジェクトをクリックすると、より多くの情報を表します。詳細については、フロア領域のモニタリング，（89 ページ）を参照してください。
- AP をマップに追加するプロセスを効率化し、迅速化します。従来のマップでは、マップへのアクセス ポイントの追加プロセスは手作業で手間がかかりました。リリース 7.3 では、自動階層作成を使用して、アクセスポイントを追加し命名できます。詳細については、マップ作成のための自動階層の使用方法，（93 ページ）を参照してください。

- 容易なナビゲーションとズーム/パン コントロールによる高品質なマップ イメージを提供します。従来のマップでは、マップイメージの品質が低く、ナビゲーション、ズーム、パンが低速でした。リリース 7.3 では、次世代のタイル対応マップ エンジンを使用して、マップを迅速にロードしズーム/パンを容易に操作できます。次世代マップでは、高解像度のマップをより高速にロードし、マップ内を容易に移動できます。詳細については、Planning and Zooming with Next Generation Maps, （89 ページ）を参照してください。

- キャンパス マップへのビルディングの追加, （56 ページ）
- フロア領域の追加, （57 ページ）

キャンパス マップへのビルディングの追加

Prime Infrastructure データベース内のキャンパス マップにビルディングを追加するには、以下のステップに従います。

ステップ 1 [Design] > [Site Maps] の順に選択して、[Maps] ページを表示します。

ステップ 2 目的のキャンパスをクリックします。[Site Maps] > [Campus Name] ページが表示されます。

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

ステップ 4 [Campus Name] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、以下のステップに従います。

1. ビルディング名を入力します。
2. ビルディング問い合わせ先の名前を入力します。
3. 地上のフロア数と地下のフロア数を入力します。
4. 水平位置（ビルディングの四角形の隅からキャンパス マップの左端までの距離）と垂直位置（ビルディングの四角形の隅からキャンパス マップの上端までの距離）をフィート単位で入力します。

   （注） 測定単位（フィートまたはメートル）を変更するには、[Design] > [Site Maps] の順に選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。
5. ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

   （注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

   ヒント Ctrl キーを押した状態でクリックすることで、キャンパス マップの左上にある境界領域のサイズを変更できます。境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。
6. [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更されたビルディングの四角形が作成されます。
7. ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

8 [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。Prime Infrastructure では、キャンパス マップ上のビルディングの四角形の中にビルディング名が保存されます。

（注） ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5 （任意）新しい屋外領域に位置プレゼンス情報を割り当てる手順は、次のとおりです。

1 [Select a command] ドロップダウン リストから、[Edit Location Presence Info] を選択します。[Go] をクリックします。[Location Presence] ページが表示されます。

2 [Civic Address] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注） 選択した各フィールドには、上記のすべてが含まれています。たとえば、[Advanced] を選択した場合、クライアントからの要求により Civic 位置情報も提供できます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

3 デフォルトでは、[Override Child's Presence Information] チェックボックスはオンになっています。独立したビルディングについては、この設定を変更する必要はありません。

ステップ 6 [Save] をクリックします。

フロア領域の追加

ここでは、Prime Infrastructure データベース内のキャンパスのビルディングまたは独立したビルディングにフロア図面を追加する方法を説明します。

- Adding Floor Areas to a Campus Building, （58 ページ）
- Adding Floor Plans to a Standalone Building, （60 ページ）
- フロア設定の構成, （72 ページ）
- マップおよび AP ロケーション データのインポート, （88 ページ）

Adding Floor Areas to a Campus Building

（注） Use the zoom controls at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which displays the map size in feet or meters).

To add a floor area to a campus building, follow these steps:

ステップ 1 Save your plan maps in .PNG, .JPG, ,JPEG, or .GIF format.

（注） The maps can be of any size because Prime Infrastructure automatically resizes the maps to fit the workspace.

（注） If there are problems converting the auto-cad file, an error message is displayed. The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .png. If the native library cannot be loaded, the Prime Infrastructure displays an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you have to install the required libraries and restart Prime Infrastructure.

（注） The floor map image is enhanced for zooming and panning. The floor image is not visible completely until this operation is complete. You can zoom in and out to view the complete map image. For example, if you have a high resolution image (near 181 megapixels) whose size is approximately 60 megabytes, it may take two minutes to appear on the map.

ステップ 2 Choose **Design** > **Site Maps**.

ステップ 3 From the Maps Tree View or the Design > Site Maps list, choose the applicable campus building to open the Building View page.

ステップ 4 Hover your mouse cursor over the name within an existing building rectangle to highlight it.

（注） You can also access the building from the Campus View page. In the Campus View page, click the building name to open the Building View page.

ステップ 5 From the Select a command drop-down list, choose **New Floor Area**.

ステップ 6 Click **Go**. The New Floor Area page appears.

ステップ 7 In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

1. Enter the floor area and contact names.
2. Choose the floor or basement number from the Floor drop-down list.
3. Choose the floor or basement type (RF Model).
4. Enter the floor-to-floor height in feet.

   （注） To change the unit of measurement (feet or meters), choose **Design** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.
5. Select the **Image or CAD File** check box.
6. Browse to and choose the desired floor or basement image or CAD filename, and click **Open**.

   （注） If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

ヒント We do not recommend a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.

7 Click **Next**. At this point, if a CAF file was specified, a default image preview is generated and loaded.

（注） The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, Prime Infrastructure displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library." For more information see Prime Infrastructure online help or Prime Infrastructure documentation.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

（注） When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.

（注） The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

（注） The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

8 If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Enter the remaining parameters for the floor area.

9 Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

10 Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

（注） The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.

11 If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

ヒント Use **Ctrl-click** to resize the image within the building-sized grid.

12 If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.

13 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

（注） Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

14 Click any of the floor or basement images to view the floor plan or basement map.

（注） You can zoom in or out to view the map at different sizes and you can add access points.

Adding Floor Plans to a Standalone Building

To add floor plans to a standalone building, follow these steps:

ステップ 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

（注） The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

ステップ 2 Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.

（注） If there are problems converting the auto-cad file, an error message is displayed. the Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure displays an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls the Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you must install the required libraries and restart the Prime Infrastructure.

ステップ 3 Choose **Design** > **Site Maps**.

ステップ 4 From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the desired building to display the Building View page.

ステップ 5 From the Select a command drop-down list, choose **New Floor Area**.

ステップ 6 Click **Go**.

ステップ 7 In the New Floor Area page, add the following information:

- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet
- Select the **Image or CAD File** check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

（注） If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

ヒント A .JPEG (.JPG) format is not recommended for an auto-cad conversion. Unless a .JPEG is specifically required, use a .PNG or .GIF format for higher quality images.

ステップ 8 Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

（注） The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the Prime Infrastructure displays the following error: “Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or the Prime Infrastructure documentation”.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

（注） When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.

（注） The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

（注） The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

ステップ 9 Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

  （注） The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure Prime Infrastructure database.
- If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

  （注） Use **Ctrl-click** to resize the image within the building-sized grid.
- Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to Launch Map Editor. See the “Using the Map Editor” section on page 10-17 for more information regarding the map editor feature.

ステップ 10 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

ステップ 11 Click any of the floor or basement images to view the floor plan or basement map.

（注） You can zoom in or out to view the map at different sizes and you can add access points.

キャンパス マップの追加

単一のキャンパス マップを Prime Infrastructure データベースに追加するには、以下のステップに従います。

ステップ 1 マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure が作業領域に適合するようマップを自動的にサイズ変更するためです。

ステップ 2 ファイル システムの任意の場所にあるマップを参照して、インポートします。

ステップ 3 [Design] > [Site Maps] の順に選択して、[Maps] ページを表示します。

ステップ 4 [Select a command] ドロップダウン リストから [New Campus] を選択し、[Go] をクリックします。

ステップ 5 [Maps] > [New Campus] ページで、キャンパス名とキャンパスの連絡先の名前を入力します。

ステップ 6 キャンパス マップが含まれているイメージ ファイル名を参照および選択してから、[Open] をクリックします。

ステップ 7 [Maintain Aspect Ratio] チェックボックスをオンにして、Prime Infrastructure でマップのサイズが変更されたときに、縦横比が変わらないようにします。

ステップ 8 マップの水平方向スパンと垂直方向スパンをフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Design] > [Site Maps] の順に選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。水平方向スパンと垂直方向スパンは、キャンパスに追加するビルディングやフロア図面よりも大きい値にする必要があります。

ステップ 9 [OK] をクリックして、このキャンパス マップを Prime Infrastructure データベースに追加します。Prime Infrastructure に、データベース内のマップ、マップの種類、およびキャンパスのステータスの一覧を含む [Maps] ページが表示されます。

ステップ 10 （任意）位置プレゼンス情報を割り当てるには、[Design] > [Site Maps] ページで新たに作成したキャンパスのリンクをクリックします。

ビルディングの設定

キャンパス マップをデータベースに追加したことがあるかどうかに関係なく、ビルディングを Prime Infrastructure データベースに追加できます。 ここでは、ビルディングをキャンパス マップに追加する方法、または独立したビルディング（キャンパスの一部ではないビルディング）を Prime Infrastructure データベースに追加する方法を説明します。

ここでは、次の内容について説明します。

- キャンパス マップへのビルディングの追加
- 独立したビルディングの追加
- ビルディングの表示, （66 ページ）
- ビルディングの編集, （67 ページ）
- ビルディングの削除, （67 ページ）
- ビルディングの移動, （68 ページ）

キャンパス マップへのビルディングの追加

NCSデータベース内のキャンパス マップにビルディングを追加するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択して、[Maps] ページを表示します。

ステップ 2 目的のキャンパスをクリックします。[Site Maps] > [Campus Name] ページが表示されます。

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

ステップ 4 [Campus Name] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、以下のステップに従います。

a) ビルディング名を入力します。

b) ビルディング問い合わせ先の名前を入力します。

c) 地上のフロア数と地下のフロア数を入力します。

d) 水平位置（ビルディングの四角形の隅からキャンパス マップの左端までの距離）と垂直位置（ビルディングの四角形の隅からキャンパス マップの上端までの距離）をフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] の順に選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

e) ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

ヒント Ctrl キーを押した状態でクリックすることで、キャンパス マップの左上隅にある境界領域のサイズを変更できます。境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。

f) [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。NCS では、キャンパス マップのサイズに合せてサイズ変更されたビルディングの四角形が作成されます。

g) ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

h) [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。NCS では、キャンパス マップ上にあるビルディングの四角形の中にビルディング名が保存されます。

（注） ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5 （任意）新しい屋外領域に位置プレゼンス情報を割り当てる手順は、次のとおりです。

a) [Select a command] ドロップダウン リストから、[Edit Location Presence Info] を選択します。[Go] をクリックします。[Location Presence] ページが表示されます。

（注） デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパスマップにビルディングを追加する際は、キャンパスのロケーション情報をインポートできます。チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。?1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

b) [Civic Address] タブ、[GPS Markers] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [GPS Markers] では、経度と緯度でキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注） 選択した各フィールドには、上記のすべてが含まれています。たとえば、[Advanced] を選択した場合、クライアントからの要求により GPS および Civic 位置情報も提供されます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

（注） クライアントが、キャンパスに対して GPS Markers フィールドで設定されていないビルディング、フロア、または屋外領域などのロケーション情報を要求した場合、エラーメッセージが返されます。

c) デフォルトでは、[Override Child's Presence Information] チェックボックスはオンになっています。独立したビルディングについては、この設定を変更する必要はありません。

ステップ 6 [Save] をクリックします。

独立したビルディングの追加

Prime Infrastructure データベースに独立したビルディングを追加するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択して、[Maps] ページを表示します。

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

ステップ 3 [Maps] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、以下のステップに従います。

a) ビルディング名を入力します。

b) ビルディング問い合わせ先の名前を入力します。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

c) 地上のフロア数と地下のフロア数を入力します。

d) ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > *[Site Maps]* の順に選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

（注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

e) [OK] をクリックして、このビルディングをデータベースに保存します。

ステップ 4 （任意）新しいビルディングに位置プレゼンス情報を割り当てる手順は、次のとおりです。

a) [Select a command] ドロップダウン リストから、[Location Presence] を選択します。[Go] をクリックします。[Location Presence] ページが表示されます。

b) [Civic] タブ、[GPS Markers] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [GPS Markers] では、経度と緯度でキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注） 選択した各フィールドには、上記のすべてが含まれています。たとえば、[Advanced] を選択した場合、ユーザからの要求により GPS および Civic 位置情報も提供されます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

（注） クライアントが、キャンパスに対して GPS Markers フィールドで設定されていないビルディング、フロア、または屋外領域などのロケーション情報を要求した場合、エラーメッセージが返されます。

c) デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパス マップにビルディングを追加する際は、ロケーション情報をインポートできます。チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

ステップ 5 [Save] をクリックします。

（注） 独立したビルディングは、システム キャンパス内に自動的に配置されます。

ビルディングの表示

現在のビルディング マップを表示するには、次の手順を実行します。

ステップ 1 **Monitor** > **[Site Maps]** を選択します。.

ステップ 2 ビルディング マップの名前をクリックして、詳細ページを開きます。 [Building View] ページには、各フロアのフロア マップの一覧とマップの詳細が表示されます。

（注） [Building View] ページの [Floor] 列見出しをクリックして、一覧をフロアの昇順または降順にソートできます。

マップの詳細には、次の情報が含まれます。

- フロア領域
- フロア インデックス：フロア レベルを示します。 マイナスの数は地下のフロア レベルを示します。
- Contact
- ステータス：このマップ上に配置されているアクセス ポイントまたは子のアクセス ポイントで、重大度の最も高いアラームを示します。
- マップに配置されているアクセス ポイントの総数。
- マップに配置されている 802.11a/n 無線および 802.11b/g/n 無線の数。
- 停止している（OOS）無線の数。
- クライアント数：数字のリンクをクリックすると、[Monitor] > [Clients] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストには、次のオプションが表示されます。

- [New Floor Area]：詳細については、キャンパス マップへのビルディングの追加を参照してください。
- [Edit Building]：詳細については、 ビルディングの編集, （67 ページ） を参照してください。
- [Delete Building]：詳細については、ビルディングの削除, （67 ページ） を参照してください。

ビルディングの編集

現在のビルディング マップを編集するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択します。

ステップ 2 ビルディング マップの名前をクリックして、詳細ページを開きます。

ステップ 3 [Select a command] ドロップダウン リストから [Edit Building] を選択します。

ステップ 4 [Building Name]、[Contact]、[Number of Floors]、[Number of Basements]、および [Dimensions (feet)] に必要な変更を加えます。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] の順に選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

ステップ 5 [OK] をクリックします。

ビルディングの削除

現在のビルディング マップを削除するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択します。

ステップ 2 削除するビルディングのチェックボックスをオンにします。

ステップ 3 マップ リスト下部の [Delete] をクリックします（または、[Select a command] ドロップダウン リストから [Delete Maps] を選択して、[Go] をクリックします）。

ステップ 4 [OK] をクリックして、削除を実行します。

（注） ビルディングを削除すると、そのコンテナ マップもすべて削除されます。削除されるすべてのマップのアクセス ポイントが、未割り当てステートに移行されます。

ビルディングの移動

別のキャンパスにビルディングを移動するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択します。
ステップ 2 該当するビルディングのチェックボックスをオンにします。
ステップ 3 [Select a command] ドロップダウン リストから [Move Buildings] を選択します。
ステップ 4 [Go] をクリックします。
ステップ 5 ドロップダウン リストから対象のキャンパスを選択します。
ステップ 6 移動するビルディングを選択します。現在のロケーションを維持するビルディングをオフにします。
ステップ 7 [OK] をクリックします。

フロア領域の追加

ここでは、Prime Infrastructure データベース内のキャンパスのビルディングまたは独立したビルディングにフロア図面を追加する方法を説明します。

- Adding Floor Areas to a Campus Building, （58 ページ）
- Adding Floor Plans to a Standalone Building, （60 ページ）
- フロア設定の構成, （72 ページ）
- マップおよび AP ロケーション データのインポート, （88 ページ）

Adding Floor Areas to a Campus Building

（注） Use the zoom controls at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which displays the map size in feet or meters).

To add a floor area to a campus building, follow these steps:

ステップ 1 Save your plan maps in .PNG, .JPG, ,JPEG, or .GIF format.
（注） The maps can be of any size because Prime Infrastructure automatically resizes the maps to fit the workspace.

（注） If there are problems converting the auto-cad file, an error message is displayed. The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .png. If the native library cannot be loaded, the Prime Infrastructure displays an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you have to install the required libraries and restart Prime Infrastructure.

（注） The floor map image is enhanced for zooming and panning. The floor image is not visible completely until this operation is complete. You can zoom in and out to view the complete map image. For example, if you have a high resolution image (near 181 megapixels) whose size is approximately 60 megabytes, it may take two minutes to appear on the map.

ステップ 2 Choose **Design** > **Site Maps**.

ステップ 3 From the Maps Tree View or the Design > Site Maps list, choose the applicable campus building to open the Building View page.

ステップ 4 Hover your mouse cursor over the name within an existing building rectangle to highlight it.

（注） You can also access the building from the Campus View page. In the Campus View page, click the building name to open the Building View page.

ステップ 5 From the Select a command drop-down list, choose **New Floor Area**.

ステップ 6 Click **Go**. The New Floor Area page appears.

ステップ 7 In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

1. Enter the floor area and contact names.
2. Choose the floor or basement number from the Floor drop-down list.
3. Choose the floor or basement type (RF Model).
4. Enter the floor-to-floor height in feet.

   （注） To change the unit of measurement (feet or meters), choose **Design** > **Site Maps**, and choose **Properties** from the Select a command drop-down list.
5. Select the **Image or CAD File** check box.
6. Browse to and choose the desired floor or basement image or CAD filename, and click **Open**.

   （注） If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

   ヒント We do not recommend a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.
7. Click **Next**. At this point, if a CAF file was specified, a default image preview is generated and loaded.

   （注） The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, Prime Infrastructure displays the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library.” For more information see Prime Infrastructure online help or Prime Infrastructure documentation.

   The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

   （注） When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.

（注） The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

（注） The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

8 If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Enter the remaining parameters for the floor area.

9 Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

10 Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

（注） The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.

11 If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

ヒント Use **Ctrl-click** to resize the image within the building-sized grid.

12 If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.

13 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

（注） Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

14 Click any of the floor or basement images to view the floor plan or basement map.

（注） You can zoom in or out to view the map at different sizes and you can add access points.

Adding Floor Plans to a Standalone Building

To add floor plans to a standalone building, follow these steps:

ステップ **1** Save your floor plan maps in .PNG, .JPG, or .GIF format.

（注） The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

ステップ **2** Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.

（注） If there are problems converting the auto-cad file, an error message is displayed. the Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure displays an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls the Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you must install the required libraries and restart the Prime Infrastructure.

ステップ 3 Choose **Design** > **Site Maps**.

ステップ 4 From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the desired building to display the Building View page.

ステップ 5 From the Select a command drop-down list, choose **New Floor Area**.

ステップ 6 Click **Go**.

ステップ 7 In the New Floor Area page, add the following information:

- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet
- Select the **Image or CAD File** check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

（注） If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

ヒント A .JPEG (.JPG) format is not recommended for an auto-cad conversion. Unless a .JPEG is specifically required, use a .PNG or .GIF format for higher quality images.

ステップ 8 Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

（注） The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the Prime Infrastructure displays the following error: “Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or the Prime Infrastructure documentation”.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

（注） When you choose the floor or basement image filename, the Prime Infrastructure displays the image in the building-sized grid.

（注） The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

（注） The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

ステップ 9 Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

（注） The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure Prime Infrastructure database.

- If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

（注） Use **Ctrl-click** to resize the image within the building-sized grid.

- Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to Launch Map Editor. See the “Using the Map Editor” section on page 10-17 for more information regarding the map editor feature.

ステップ 10 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

ステップ 11 Click any of the floor or basement images to view the floor plan or basement map.

（注） You can zoom in or out to view the map at different sizes and you can add access points.

フロア設定の構成

さまざまなフロア設定のチェックボックスをオンまたはオフにすることにより、フロア マップの外観を変更できます。オンにしたフロア設定はマップ イメージに表示されます。

（注） Prime Infrastructure に Mobility Services Engine があるかどうかに応じて、フロア設定の一部が表示されない場合があります。[Clients]、[802.11 Tags]、[Rogue APs]、[Adhoc Rogues]、[Rouge Clients]、および [Interferers] は、MSE が Prime Infrastructure に存在する場合のみ表示されます。

[Floor Settings] オプションには次の項目が含まれます。

- [Access Points]：詳細については、アクセス ポイントのフロア設定のフィルタリングを参照してください。
- [AP Heatmaps]：詳細については、アクセス ポイント ヒートマップのフロア設定のフィルタリングを参照してください。
- [AP Mesh Info]：詳細については、[AP Mesh Info] のフロア設定のフィルタリングを参照してください。
- [Clients]：詳細については、クライアントのフロア設定のフィルタリングを参照してください。
- [802.11 Tags]：詳細については、802.11 タグのフロア設定のフィルタリングを参照してください。
- [Rogue APs]：詳細については、不正 AP のフロア設定のフィルタリングを参照してください。

- [Rogue Adhocs]：詳細については、不正アドホックのフロア設定のフィルタリングを参照してください。
- [Rogue Clients]：詳細については、不正クライアントのフロア設定のフィルタリングを参照してください。
- Coverage Areas
- Location Regions
- Rails
- Markers
- Chokepoints
- Wi-Fi TDOA Receivers
- [Interferers]：詳細については、干渉設定のフィルタリングを参照してください。
- [wIPS Attackers]：詳細については、wIPS Attacker フロア設定のフィルタリング，（86 ページ）を参照してください。

青色の矢印を使用して、アクセス ポイント、アクセス ポイント ヒートマップ、クライアント、802.11 タグ、不正アクセス ポイント、不正アドホック、および不正クライアントに関するフロア設定フィルタにアクセスします。フィルタリング オプションを選択したら、[OK] をクリックします。

最後のドロップダウン リスト内の [Show MSE data] を使用して、Mobility Services Engine のデータの期間を選択します。過去 2 分間から最大 24 時間の範囲で、Mobility Services Engine のデータを表示できます。このオプションは、Mobility Services Engine が Prime Infrastructure に存在する場合のみ表示されます。

[**Save** Settings] をクリックすると、現在のビューとフィルタ設定がすべてのマップに対する新しいデフォルトになります。

フロア上の包含リージョンと除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含める領域（包含領域）と計算に含めない領域（除外領域）を定義できます。

たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外して、作業領域（小個室、研究室、製造現場など）を含めることができます。

Cisco 1000 シリーズ Lightweight アクセス ポイントのアイコン

アイコンは、アクセス ポイントの現在のステータスを示します。アイコンの円部分は水平方向に半分に分割できます。2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。

（注） アイコンが 802.11a/n と 802.11b/n を表している場合は、上半分が 802.11a/n ステータスを示し、下半分が 802.11b/g/n ステータスを示します。アイコンが 802.11b/g/n のみを表している場合は、アイコン全体が 802.11b/g/n ステータスを示します。三角形はより重大な色を示します。

次の表に、Prime Infrastructure ユーザインターフェイスのマップ表示で使用されるアイコンを示します。

表 *11*：アクセス ポイント アイコンの説明

アイコン	説明
	緑色のアイコンは、障害のないアクセス ポイント（AP）を示します。円の上半分は、オプションの 802.11a Cisco Radio を表します。円の下半分は、802.11b/g Cisco Radio のステートを示します。
	黄色のアイコンは、比較的重大でない障害があるアクセス ポイントを示します。円の上半分は、オプションの 802.11a Cisco Radio を表します。円の下半分は、802.11b/g Cisco Radio のステートを示します。 （注） 黄色の点滅するアイコンは、802.11a または 802.11b/g の干渉、ノイズ、カバレッジ、または負荷プロファイル違反があることを示します。黄色の点滅するアイコンは、802.11a および 802.11b/g のプロファイル違反があることを示します。
	赤色のアイコンは、やや重大な障害または重大な障害があるアクセス ポイント（AP）を示します。円の上半分は、オプションの 802.11a Cisco Radio を表します。円の下半分は、802.11b/g Cisco Radio のステートを示します。
	中央に疑問符が付いている灰色のアイコンは、到達不能なアクセス ポイントを表します。ステータスが判断できないため、灰色になっています。
	中央に疑問符が付いていない灰色のアイコンは、アソシエートされていないアクセス ポイントを表します。
	円の中央に赤い「x」が付いているアイコンは、管理目的で無効にされているアクセス ポイントを表します。

アイコン	説明
	上半分が緑色で下半分が黄色のアイコンは、障害のないオプションの 802.11a Cisco Radio（上）と、比較的重大でない障害がある 802.11b/g Cisco Radio（下）を示します。2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が緑色で下半分が赤色のアイコンは、障害がなく正常に動作している、オプションの 802.11a Cisco Radio（上）と、やや重大な障害または重大な障害がある 802.11b/g Cisco Radio（下）を示します。2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が黄色で下半分が赤色のアイコンは、比較的重大でない障害がある、オプションの 802.11a Cisco Radio（上）と、やや重大な障害または重大な障害がある 802.11b/g Cisco Radio（下）を示します。2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が黄色で下半分が緑色のアイコンは、比較的重大でない障害がある、オプションの 802.11a Cisco Radio（上）と、障害のないオプションの 802.11b/g Cisco Radio（下）を示します。2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が赤色で下半分が緑色のアイコンは、やや重大な障害または重大な障害がある、オプションの 802.11a Cisco Radio（上）と、障害がなく正常に動作している 802.11b/g Cisco Radio（下）を示します。2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が赤色で下半分が黄色のアイコンは、やや重大な障害または重大な障害がある、オプションの 802.11a Cisco Radio（上）と、比較的重大でない障害がある 802.11b/g Cisco Radio（下）を示します。2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。

アイコン	説明
	上半分（オプションの 802.11a）に赤い「x」が付いているアイコンは、示されている Cisco Radio が管理目的で無効にされていることを表します。記載されている 6 つのカラー コーディングが存在します。

各アクセス ポイント アイコンには、内部の Side A アンテナの方向を示す、小さい黒矢印があります。

下の表に、Prime Infrastructure ユーザ インターフェイスのマップ表示で使用される矢印の例を示します。

表 *12*：矢印

矢印の例	方向
	0 度、またはマップ上の右方向。
	45 度、またはマップ上の右下方向。

矢印の例	方向
	90 度、またはマップ上の下方向。
これらは、矢印の角度を 45 度ずつ増加させた例の最初の 3 つ分を示しています。45 度ずつ増加させた例はあと 5 つあります。	

アクセス ポイントのフロア設定のフィルタリング

アクセス ポイントのフロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、フィルタリング オプションを含む [Access Point Filter] ダイアログボックスが表示されます。

アクセス ポイントのフィルタリング オプションには、次の項目が含まれます。

- [Show]：このオプション ボタンを選択すると、無線ステータスまたはアクセス ポイントのステータスが表示されます。

（注） アクセス ポイント アイコンの色はアクセス ポイントのステータスに基づいており、選択されているステータスによってアイコンの色は異なります。フロア マップのデフォルトは無線ステータスです。

- [Protocol]：ドロップダウン リストから、表示する無線タイプを選択します（802.11a/n、802.11b/g/n、または両方）。

（注） 表示されるヒートマップは、選択した無線タイプに対応します。

- [Display]：ドロップダウン リストから、マップ イメージ上に表示されるアクセス ポイントの識別情報を選択します。
  - [Channels]：Cisco Radio のチャネル番号を表示するか、「Unavailable」（アクセス ポイントが接続されていない場合）を表示します。

（注） 使用可能なチャネルは、国コードの設定によって定義され、各国で規制されています。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/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

  - [TX Power Level]：現在の Cisco Radio の送信電力レベル（1 が高い）または「Unavailable」（アクセス ポイントが接続されていない場合）を表示します。

（注） 電力レベルはアクセス ポイントのタイプによって異なります。1000 シリーズのアクセス ポイントでは 1 ～ 5 の値、1230 アクセス ポイントでは 1 ～ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ～ 8 の値をとります。

次の表には、送信電力レベルの数値と対応する電力設定を示します。

表 *13*：送信電力レベル値

送信電力?レベルの数値	電力設定
1	国コード設定で許可される最大の電力
2	50% の電力
3	25% の電力
4	12.5 ～ 6.25 % の電力
5	6.25 ～ 0.195% の電力

（注） 電力レベルは、国コードの設定によって定義され、各国で規制されています。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/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

- [Channel and Tx Power]：チャネルと送信電力レベルの両方（またはアクセス ポイントが接続されていない場合は「Unavailable」）を表示します。
- [Coverage Holes]：接続が切断されるまでに信号が弱くなったクライアントの割合を表示します。接続されていないアクセス ポイントに対しては「Unavailable」を表示し、監視専用モードのアクセス ポイントに対しては「MonitorOnly」を表示します。

（注） カバレッジ ホールとは、クライアントがワイヤレス ネットワークから信号を受信できない領域のことです。無線ネットワークを展開する場合、初期ネットワーク展開のコストとカバレッジ ホール領域の割合を考慮する必要があります。展開するにあたってのカバレッジ ホールの妥当な条件とは、2 ～ 10% です。これは、100 か所のランダムに選択したテスト ロケーションのうち、2 ～ 10 か所でサービスが制限される可能性があることを意味します。展開後、Cisco Unified Wireless Network Solution の Radio Resource Management（RRM; 無線リソース管理）によってこれらのカバレッジ ホール領域が特定され、IT マネージャに報告されます。IT マネージャはユーザからの要求に基づいてカバレッジ ホールに対応します。

- [MAC Addresses]：アクセス ポイントがコントローラにアソシエートされているかどうかに関係なく、アクセス ポイントの MAC アドレスを表示します。
- [Names]：アクセス ポイント名を表示します。これはデフォルト値です。
- [Controller IP]：アクセス ポイントがアソシエートされているコントローラの IP アドレスを表示します。アソシエーションを解除されたアクセス ポイントでは、「Not Associated」を表示します。
- [Utilization]：アソシエートされたクライアント デバイスで使用されている帯域幅の割合（受信、送信、およびチャネル使用率を含む）を表示します。アソシエーションを解除されたアクセス ポイントでは [Unavailable]、monitor-only モードのアクセス ポイントでは [MonitorOnly] が表示されます。
- [Profiles]：対応するオペレータ定義の閾値の負荷、ノイズ、干渉、およびカバレッジ コンポーネントを表示します。超えていないしきい値には「Okay」、超えているしきい値には「Issue」、接続されていないアクセス ポイントには「Unavailable」を表示します。

（注） [Profile Type] ドロップダウン リストを使用して、[Load]、[Noise]、[Interference]、または [Coverage] を選択します。

- [CleanAir Status]：アクセス ポイントの CleanAir ステータスと、アクセス ポイントで CleanAir が有効かどうかを表示します。
- [Average Air Quality]：このアクセス ポイントの平均電波品質を表示します。詳細には、帯域と平均電波品質が含まれます。
- [Minimum Air Quality]：このアクセス ポイントの最小電波品質を表示します。詳細には、帯域と最小電波品質が含まれます。
- [Average and Minimum Air Quality]：このアクセス ポイントの平均電波品質と最小電波品質を表示します。詳細には、帯域、平均電波品質、および最小電波品質が含まれます。

- [Associated Clients]：アソシエートされているクライアントの数を表示します。接続されていないアクセス ポイントに対しては「Unavailable」を表示し、monitor-only モードのアクセス ポイントに対しては「MonitorOnly」を表示します。

（注）

- Bridge Group Names
- [RSSI Cutoff]：ドロップダウン リストから、RSSI Cutoff レベルを選択します。RSSI Cutoff の範囲は -60 dBm ～ -90 dBm です。
- [Show Detected Interferers]：チェックボックスをオンにすると、アクセス ポイントで検出されるすべての干渉を表示します。
- [Max. Interferers/label]：ドロップダウン リストから、ラベルごとに表示される干渉の最大数を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

アクセス ポイント ヒートマップのフロア設定のフィルタリング

RF ヒートマップは、変数から取得した値をマップに色として表した、RF ワイヤレス データのグラフィック表示です。現在のヒートマップは、RSSI 予測モデル、アンテナの方向、および AP 送信電力に基づいて計算されます。

[Access Point Heatmap] フロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、ヒートマップのフィルタリング オプションを含む [Contributing APs] ダイアログが表示されます。詳細については、RF ヒートマップの計算についてを参照してください。

Prime Infrastructure ではダイナミック ヒートマップが導入されました。ダイナミック ヒートマップを有効にすると、Prime Infrastructure は変更された RSSI 値を表すためにヒートマップを再計算します。ダイナミック ヒートマップを設定する手順の詳細については、マップ プロパティの編集を参照してください。

アクセス ポイント ヒートマップのフィルタリング オプションには、次の項目が含まれます。

- [Heatmap Type]：[Coverage] または [Air Quality] を選択します。[Air Quality] を選択した場合は、アクセス ポイントのヒート マップ タイプを平均電波品質または最小電波品質でさらにフィルタリングできます。該当するオプション ボタンを選択します。

（注） フロア計画にモニタ モード アクセス ポイントがある場合、IDS ヒートマップ タイプまたはカバレッジ ヒートマップ タイプのいずれかを選択できます。カバレッジ ヒートマップでは、モニタ モード アクセス ポイントは除外されます。

（注） カバレッジ ヒートマップおよび電波品質ヒートマップには、ローカル モード、FlexConnect モード、またはブリッジ モードの AP のみが関係します。

- [Total APs]：マップに配置されているアクセス ポイントの数を表示します。
- アクセス ポイントのチェックボックスをオンにして、イメージ マップ上に表示するヒートマップを決定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

[AP Mesh Info] のフロア設定のフィルタリング

（注） [AP Mesh Info] チェックボックスは、ブリッジ アクセス ポイントがフロアに追加されているときのみ表示されます。

このチェックボックスをオンにすると、Prime Infrastructure はコントローラとの通信を開始し、ブリッジ アクセス ポイントの情報を表示します。次の情報が表示されます。

- 子アクセス ポイントと親アクセス ポイントとの間のリンク。
- 子アクセス ポイントから親アクセス ポイントへの方向を示す矢印。
- 信号対雑音比（SNR）を示す、色分けされたリンク。緑色のリンクは高い SNR（25 dB 超）を表し、オレンジ色のリンクは許容範囲内の SNR（20 ～ 25 dB）を表し、赤色のリンクは非常に低い SNR（20 dB 未満）を表します。

[AP Mesh Info] フロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、メッシュのフィルタリング オプションを含む [Mesh Parent-Child Hierarchical View] ページが表示されます。

マップ上に表示するアクセス ポイントを選択することにより、マップ ビューを更新できます。[Quick Selections] ドロップダウン リストから、ルート アクセス ポイントのみを選択するか、1 番めのホップから 4 番めのホップの間のさまざまなホップを選択するか、またはすべてのアクセス ポイントを選択します。

（注） 子アクセス ポイントを表示するには、その親が選択されている必要があります。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

クライアントのフロア設定のフィルタリング

（注） [Clients] オプションは、モビリティ サーバが Prime Infrastructure に追加されている場合のみ表示されます。

[Clients] フロア設定を有効にし、右側の青い矢印をクリックすると、[Client Filter] ダイアログボックスが表示されます。

クライアントのフィルタリング オプションには、次の項目が含まれます。

- [Show All Clients]：チェックボックスをオンにすると、マップ上のすべてのクライアントが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各クライアントのアイコンが表示されます。

（注） [Show All Clients] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。??[Small Icons] チェックボックスをオフにすると、ラベルに MAC アドレス、アセット名、アセット グループまたはアセット カテゴリを表示するかどうか選択できます。[Show All Clients] チェックボックスをオフにすると、クライアントをフィルタリングする方法を指定し、特定の SSID を入力できます。

- [Display]：マップ上に表示するクライアントの識別子（IP アドレス、ユーザ名、MAC アドレス、アセット名、アセット グループ、またはアセット カテゴリ）を選択します。
- [Filter By]：クライアントをフィルタリングするパラメータを選択します（IP アドレス、ユーザ名、MAC アドレス、アセット名、アセット グループ、アセット カテゴリ、またはコントローラ）。選択したら、特定のデバイスをテキスト ボックスに入力します。
- [SSID]：入力可能なテキスト ボックスにクライアントの SSID を入力します。
- [Protocol]：ドロップダウン リストから [All]、[802.11a/n]、または [802.11b/g/n] を選択します。
  - [All]：領域内のすべてのアクセス ポイントを表示します。
  - [802.11a/n]：802.11a/n 無線通信機を使用するクライアントに対するカバレッジ パターンを示す色付きのオーバーレイを表示します。色は、赤（-35dBm）～濃い青（-85dBm）までの受信信号強度を表します。
  - [802.11b/g/n]：802.11b/g/n 無線通信機を使用するクライアントに対するカバレッジ パターンを示す色付きのオーバーレイを表示します。色は、赤（-35dBm）～濃い青（-85dBm）までの受信信号強度を表します。これはデフォルト値です。
- [State]：ドロップダウン リストから [All]、[Idle]、[Authenticated]、[Probing]、または [Associated] を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

802.11 タグのフロア設定のフィルタリング

[802.11 Tags] フロア設定を有効にし、右側の青い矢印をクリックすると、[Tag Filter] ダイアログが表示されます。

タグのフィルタリング オプションには、次の項目が含まれます。

- [Show All Tags]：チェックボックスをオンにすると、マップ上のすべてのタグが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各タグのアイコンが表示されます。

（注） [Show All Tags] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Small Icons] チェックボックスをオフにすると、ラベルに MAC アドレス、アセット名、アセット グループまたはアセット カテゴリを表示するかどうか選択できます。 [Show All Tags] チェックボックスをオフにすると、タグをフィルタリングする方法を指定できます。

- [Display]：マップ上に表示するタグの識別子（MACアドレス、アセット名、アセット グループ、またはアセット カテゴリ）を選択します。
- [Filter By]：クライアントをフィルタリングするパラメータを選択します（MAC アドレス、アセット名、アセットグループ、アセットカテゴリ、またはコントローラ）。選択したら、特定のデバイスをテキスト ボックスに入力します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正 AP のフロア設定のフィルタリング

[Rogue APs] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue AP filter] ダイアログボックスが表示されます。

不正 AP のフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue APs]：チェックボックスをオンにすると、マップ上のすべての不正アクセス ポイントが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正アクセス ポイントのアイコンが表示されます。

（注） [Show All Rogue APs] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Show All Rogue APs] チェックボックスをオフにすると、不正アクセス ポイントをフィルタリングする方法を指定できます。

- [Show Rogue AP Zone of Impact]：不正アクセスによる影響ゾーンを表示する場合に、このチェックボックスをオンにします。不正による影響ゾーンは、不正 AP の送信電力と、不正 AP に関連付けられたクライアントの数により決まります。
  - 不正 AP に関連付けられたクライアントの数によって、マップのゾーンの色の濃さが決まります。
  - 影響ゾーンの半径は、次の不正 AP の送信電力に基づいて決まります。

表 *14*：送信電力

帯域	送信電力	Tx Power 前提
2.5 GHz	20 dBm	18 dBm
5 GHz	17 dBm	15 dBm

- [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Known]、[Acknowledged]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。
- [On Network]：ドロップダウン リストを使用して、ネットワーク上の不正アクセス ポイントを表示するかどうか指定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正アドホックのフロア設定のフィルタリング

[Rogue Adhocs] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue Adhoc filter] ダイアログが表示されます。

不正アドホックのフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue Adhocs]：チェックボックスをオンにすると、マップ上のすべての不正アドホックが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正アドホックのアイコンが表示されます。

（注） [Show All Rogue Adhocs] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Show All Rogue Adhocs] チェックボックスをオフにすると、不正アドホックをフィルタリングする方法を指定できます。

- [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Known]、[Acknowledged]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。
- [On Network]：ドロップダウン リストを使用して、ネットワーク上の不正アドホックを表示するかどうか指定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正クライアントのフロア設定のフィルタリング

[Rogue Clients] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue Clients filter] ダイアログが表示されます。

不正クライアントのフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue Clients]：チェックボックスをオンにすると、マップ上のすべての不正クライアントが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正クライアントのアイコンが表示されます。

（注） [Show All Rogue Clients] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。[Show All Rogue Clients] チェックボックスをオフにすると、不正クライアントをフィルタリングする方法を指定できます。

- [Assoc.Rogue AP MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

干渉設定のフィルタリング

[Interferer] フロア設定を有効にし、右側の青い矢印をクリックすると、[Interferers filter] ダイアログボックスが表示されます。

干渉のフィルタリング オプションには、次の項目が含まれます。

- [Show active interferers only]：チェックボックスをオンにすると、すべてのアクティブな干渉が表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各干渉のアイコンが表示されます。
- [Show Zone of Impact]：おおまかな干渉の影響領域を表示します。円の不透明度はその重大度を示します。赤一色の円は Wi-Fi 通信を妨害する可能性がある非常に強い干渉を表し、薄いピンク色の円は弱い干渉を表します。
- 該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

wIPS Attacker フロア設定のフィルタリング

[wIPS Attacker] フロア設定を有効にし、右側の青い矢印をクリックすると、[wIPS Attack Filter] ダイアログボックスが表示されます。

wIPS Attack フィルタリングのオプションには次が含まれます。

- [Show All wIPS Attacks]：チェックボックスをオンにすると、マップ上のすべての wIPS 攻撃が表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各 wIPS 攻撃のアイコンが表示されます。

（注） [Show All wIPS Attacks] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。[Small Icons] チェックボックスをオフにすると、ラベルに MAC アドレス、アラーム カテゴリ、アラーム名を表示するかどうかを選択できます。[Show All wIPS Attacks] チェックボックスをオフにすると、wIPS 攻撃をフィルタリングする方法を指定できます。

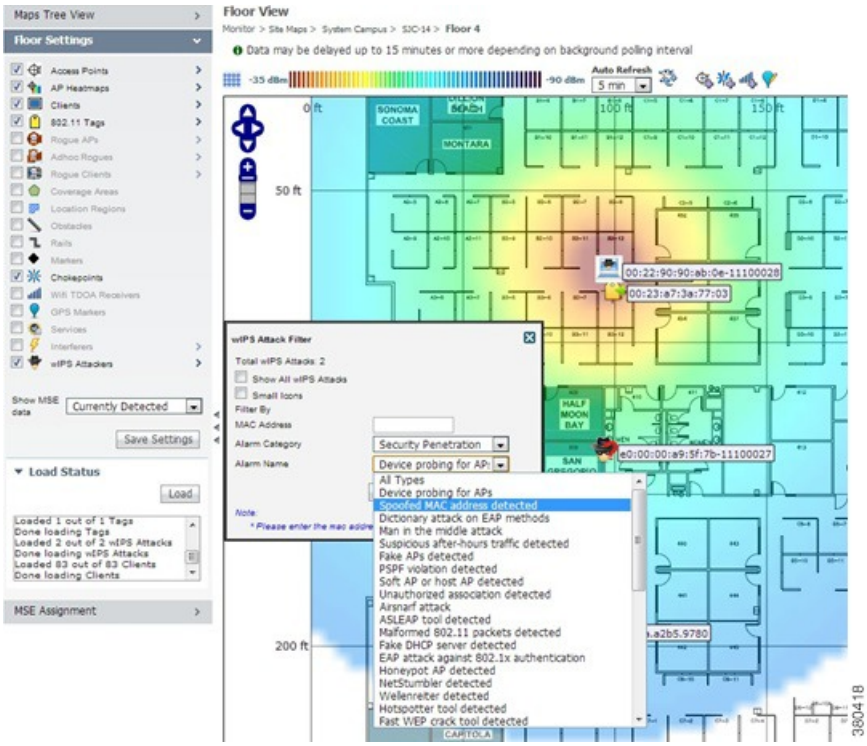
- [Filter By]：wIPS 攻撃のフィルタリングの基準にするパラメータを選択します。
  - [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
  - [Alarm Category]：[Alarm Category] ドロップダウン リストからアラームのカテゴリを選択します。利用可能なカテゴリには、[All Types]、[Security Penetration]、[User Authentication and Encryption]、[DoS]、[Performance Violation]、および [Channel or Device overload] があります。

（注） アラーム名は、選択したアラーム カテゴリに基づいて入力されます。

- [Alarm Name]：[Alarm Name] ドロップダウン リストからアラーム名を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

図 *9*：*wIPS* 攻撃名のフィルタリング



マップに表示される各デバイスを区別するために、次のアイコンが使用されます。

図 *10*：アイコン

攻撃者

犠牲者

不明なデバイス

（注） wIPS で報告されるすべてのアラームのうち、次の 4 つのアラームは、アクセス ポイントではなく、Mobility Services Engine（MSE）で検出されます。これらのアラームについて、場所の情報は現在ありません。アラームのリストは次のとおりです。

- 124 Hotspotter ツールの検出
- 133 デバイスのセキュリティ異常による Day-Zero 攻撃
- 135 WLAN のセキュリティ異常による Day-Zero 攻撃
- 138 ベンダー リストによる未承認アソシエーション

マップおよび AP ロケーション データのインポート

Autonomous から Lightweight アクセス ポイントに、および WLSE から Prime Infrastructure に変換する場合、変換手順の 1 つとして、アクセス ポイント関連情報を手動で Prime Infrastructure に再入力する方法があります。この処理を高速化するために、WLSE からアクセス ポイントに関する情報をエクスポートして、Prime Infrastructure にインポートすることができます。

（注） Prime Infrastructure は、.tar ファイルを想定しているため、ファイルをインポートする前に .tar 拡張子かどうかをチェックします。インポートしようとしているファイルが .tar ファイルでない場合は、Prime Infrastructure にエラー メッセージが表示され、別のファイルをインポートするためのプロンプトが表示されます。

（注） WLSE データ エクスポート機能（WLSE バージョン 2.15）の詳細については、http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp を参照してください。

Prime Infrastructure Web インターフェイスを使用して、プロパティをマップし、WLSE データを含む tar ファイルをインポートするには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択します。

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

ステップ 3 [WLSE Map and AP Location Data] オプションを選択して、[Next] をクリックします。

ステップ 4 [Import WLSE Map and AP Location Data] ページで、[Browse] をクリックしてインポートするファイルを選択します。

ステップ 5 インポートする .tar ファイルを見つけて選択し、[Open] をクリックします。

Prime Infrastructure では、[Import From] テキスト ボックスにファイルの名前が表示されます。

ステップ 6 [Import] をクリックします。
CS によってファイルがアップロードされ、ファイルが処理されている間は一時的にファイルはローカル ディレクトリに保存されます。ファイルに処理できないデータが含まれている場合、Prime Infrastructure は問題を修正して再試行するようユーザに促します。ファイルのロードが完了すると、Prime Infrastructure に追加された内容を示すレポートが Prime Infrastructure に表示されます。レポートには、追加できない内容とその理由も記載されます。

インポートするデータの一部がすでに存在している場合、Prime Infrastructure では、キャンパスの場合は既存のデータを使用し、ビルディングとフロアの場合はインポートされたデータで既存のデータを上書きします。

（注） WLSE サイトとビルディングの組み合わせ、および Prime Infrastructure キャンパス（または最上位レベルのビルディング）とビルディングの組み合わせの間に重複する名前がある場合、Prime Infrastructure の実行前インポート レポートに、既存のビルディングを削除することを示すメッセージが表示されます。

ステップ 7 [Import] をクリックして、WLSE データをインポートします。
Prime Infrastructure にインポートされた内容を示すレポートが表示されます。

ステップ 8 インポートされたデータを表示するには、[Monitor] > [Site Maps] の順に選択します。

フロア領域のモニタリング

フロア領域は、ビルディングの各フロアの領域で、外壁の外面に対して測定されます。この領域には、ロビー、地下室、エレベータ シャフトが含まれ、集合住宅ビルディングではすべての共有空間が含まれます。

ここでは、次の内容について説明します。

- Planning and Zooming with Next Generation Maps, （89 ページ）
- アクセス ポイントのフロア領域への追加, （90 ページ）
- アクセス ポイントの配置, （92 ページ）

Planning and Zooming with Next Generation Maps

Planning

To move the map, click and hold the left mouse button and drag the map to a new place. You ca also move the map North, South, East, or West using the pan arrows. These can be found on the top left-hand corner of the map.

（注） You can also perform the panning operations using the arrow keys on a keyboard.

Zooming in and out - changing the scale

The zooming levels depend upon the resolution of an image. A high resolution image may provide more zoom levels. Each zoom level is made of a different style map shown at different scales, each one showing more or less detail. Some maps will be of the same style, but at a smaller or larger scale.

To see a map with more detail you need to zoom in. You can do this using the zoom bar on the left hand side of the map. Click the + sign on the top of the zoom bar. To center and zoom in on a location, double-click the location. To see a map with less detail you need to zoom out. To do this, click the - sign on the bottom of the zoom bar.

（注） You can perform zooming operations using the mouse or keyboard. With the keyboard, click the + or - signs to zoom in or zoom out. With the mouse, use the mouse scroll wheel to zoom in or zoom out or double-click to zoom in.

アクセス ポイントのフロア領域への追加

.PNG、.JPG、.JPEG、または .GIF 形式のフロア図面と屋外領域のマップを Prime Infrastructure データベースに追加した後に、Lightweight アクセス ポイント アイコンをマップ上に配置して、ビルディング内の設定位置を示すことができます。アクセス ポイントをフロア領域と屋外領域に追加するには、以下のステップに従います。

（注） MSE でフロアごとにサポートする AP の数に制限はありませんが、Prime Infrastructure で各フロアに 100 以上の AP を追加すると、パフォーマンスの問題が発生することがあります。

ステップ 1 [Design] > [Site Maps] の順に選択します。

ステップ 2 [Maps Tree View] または左側のサイドバー メニューの [Design] > [Site Maps] から、該当するフロアを選択し、[Floor View] ページを開きます。

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

ステップ 4 [Add Access Points] ページで、フロア領域に追加するアクセス ポイントのチェックボックスをオンにします。

（注） アクセス ポイントを検索する場合は、AP 名または MAC アドレス（イーサネット/無線）/IP を [Search AP] の [Name/MacAddress (Ethernet/Radio)/IP] テキスト ボックスに入力して、[Search] をクリックします。検索では大文字と小文字は区別されません。

（注） フロアおよび屋外領域にまだ割り当てられていないアクセス ポイントのみがリストに表示されます。

（注） リストの上部にあるチェックボックスをオンにして、すべてのアクセス ポイントを選択します。

ステップ 5 該当するすべてのアクセス ポイントが選択されたら、アクセス ポイント リストの下部にある [OK] をクリックします。[Position Access Points] ページが表示されます。
フロア マップに追加するために選択した各アクセス ポイントは、灰色の円で表され（アクセス ポイント名や MAC アドレスにより区別）、フロア マップの左上部分に並べられます。

ステップ 6 各アクセス ポイントをクリックし、適切な位置にドラッグします。アクセス ポイントは選択されると青色に変わります。

（注） マップ上にアクセス ポイントをドラッグすると、[Horizontal] テキスト ボックスと [Vertical] テキスト ボックスにアクセス ポイントの水平位置と垂直位置が表示されます。

（注） 各アクセス ポイントの横の小さい黒矢印は各アクセス ポイントの Side A を表し、各アクセス ポイントの矢印は、アクセス ポイントが設置された方向と一致する必要があります。Side A はそれぞれの 1000 シリーズ アクセス ポイント上で明確に記されており、802.11a/n 無線とは関係ありません。方向の矢印を調整するには、[Antenna Angle] ドロップダウン リストから適切な方向を選択します。

アクセス ポイントを選択すると、そのアクセス ポイントの詳細がページの左側に表示されます。アクセス ポイントの詳細には、次の情報が含まれます。

- [AP Model]：選択したアクセス ポイントのモデル タイプを示します。
- [Protocol]：ドロップダウン リストから、このアクセス ポイントのプロトコルを選択します。
- [Antenna]：ドロップダウン リストから、このアクセス ポイントの適切なアンテナ タイプを選択します。
- [Antenna/AP Image]：[Antenna] ドロップダウン リストから選択したアンテナがアンテナ イメージに反映されます。アンテナイメージの右上の矢印をクリックすると、画像のサイズが拡大します。
- [Antenna Orientation]：アンテナ タイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。

（注） [Omnidirectional] アンテナのパターンでは方位角が存在しなくなるため、[Azimuth] オプションは表示されません。

（注） 内部アンテナでは、同じ垂直方向の角度が両方の無線に適用されます。

アンテナの角度は、マップの X 軸に対して相対的です。X（水平）座標および Y（垂直）座標の原点はマップの左上の角であるため、0 度はアクセス ポイントの Side A を右に、90 度は Side A を下に、180 度は Side A を左に向けることになります。

アンテナの Elevation（垂直面）は、最大 90 度までアンテナを垂直（上下）に移動するために使用されます。

（注） 各アクセス ポイントがマップ上の正しい位置に設置されていること、またアンテナの方向が正しいことを確認します。マップを使って、カバレッジ ホールや不正アクセス ポイントを発見するときは、正確なアクセス ポイントの位置決めが重要です。

アンテナの垂直方向の角度および方位角のパターンの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

ステップ 7 各アクセス ポイントの配置と調整が完了したら、[Save] をクリックします。

（注） [Save] をクリックすると、アクセス ポイントのアンテナ ゲインが選択したアンテナに一致します。これにより、無線がリセットされる可能性があります。

Prime Infrastructure によって、カバレッジ領域の RF 予測が計算されます。この RF 予測は、カバレッジ領域マップ上の RF 信号の相対強度を示しているため、一般的には「ヒート マップ」として知られています。

（注） （注）

ここでは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値だけが表示されています。

（注） マップへのアクセス ポイントの配置の詳細については、「アクセス ポイントの配置」（10-14 ページ）を参照してください。

（注） ファイルをインポートまたはエクスポートすることにより、アクセス ポイントの位置を変更できます。詳細については、「Wi-Fi TDOA 受信機の配置」（10-30 ページ）を参照してください。

アクセス ポイントの配置

無線 LAN のカバレッジ領域での全デバイスの最適な位置を判断するには、アクセス ポイントの密度と位置を考慮する必要があります。

少なくとも 3 個、可能な場合は 4 個か 5 個のアクセス ポイントが、デバイス位置を必要とする各領域にカバレッジを提供していることを確認します。デバイスを検出するアクセス ポイントは多いほうが効果があります。この高水準のガイドラインが生み出す最良の実施例は次のとおりです。優先度順に並べられています。

1. 最も重要なのは、アクセス ポイントが目的の位置を囲むことです。
2. 約 17 ～ 20m（50 ～ 70 リニア フィート）ごとに 1 つのアクセス ポイントが配置される必要があります。これは変換すると、230 ～ 450 平方メートル（2,500 ～ 5,000 平方フィート）ごとに 1 つのアクセス ポイントとなります。

（注） アクセス ポイントは、約 6m（20 フィート）未満の高さで設置する必要があります。性能を最も引き出すためには、約 3m（10 フィート）で設置すると理想的です。

これらのガイドラインに従うと、アクセス ポイントが追跡したデバイスをより検出しやすくなります。2 つの物理環境が同じ RF 特性を持つことはほとんどありません。ユーザは特定の環境や要件に合わせてこれらのパラメータを変更しなければならない場合があります。

（注） Cisco WLC が情報を Location Appliance に転送するために、-75 dBm を超える信号でデバイスを検出する必要があります。3 つ以上のアクセス ポイントが、-75dBm 以下の信号でデバイスを検出できなければなりません。

（注） 全方向性アンテナを内蔵した天井マウント型APがある場合は、Prime Infrastructureでアンテナの方向を必ずしも設定する必要はありません。ただし、同じAPを壁にマウントする場合は、アンテナの方向を90度に設定する必要があります。アクセス ポイントの方向については、アクセス ポイントの配置, （92 ページ）を参照してください。

表 *15*：アクセス ポイントのアンテナ方向

アクセス ポイント	アンテナの方向
1140（天井に取り付けた場合）	Cisco ロゴは床面に向いている必要があります。垂直方向：0 度。
1240（天井に取り付けた場合）	アンテナはアクセス ポイントと垂直にする必要があります。 垂直方向：0 度。
1240（壁面に取り付けた場合）	アンテナはアクセス ポイントと平行にする必要があります。 垂直方向：0 度。 アンテナが AP と垂直な場合、角度は 90 度になります（ダイポール アンテナは全方向性のため、方向の上下は関係ありません）。

マップ作成のための自動階層の使用方法

自動階層作成は、すばやくマップを作成し、Prime Infrastructureのマップにアクセス ポイントを割り当てる方法です。Cisco WLC を Prime Infrastructure に追加し、アクセス ポイントに名前を付けたら、自動階層作成を使用してマップを作成できます。また、ネットワークにアクセス ポイントを追加した後、自動階層作成をしようして、Prime Infrastructureのマップにアクセス ポイントを割り当てることができます。

（注） 自動階層作成機能を使用するには、マップのキャンパス、ビルディング、フロア、または屋外領域名を指定する、ワイヤレス アクセス ポイントに対して確立された命名パターンを必要とします。たとえば、San Jose-01-GroundFloor-AP3500i1 などです。

自動階層を使用してマップを作成するには、以下のステップに従います。

ステップ 1 [Design] > [Automatic Hierarchy Creation] の順に選択して、[Automatic Hierarchy Creation] ページを表示します。

ステップ 2 テキスト ボックスに、システムのアクセス ポイントの名前を入力します。または、リストから名前を 1 つ選択できます。
この名前は、マップを作成する正規表現を作成するために使用されます。

（注） 以前に作成した正規表現を更新するには、式の横の [Load and Continue] をクリックし、式を適宜更新します。

正規表現を削除するには、式の横にある [Delete] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 アクセス ポイントの名前にデリミタがある場合は、それをテキスト ボックスに入力し、[Generate] をクリックします。システムではデリミタに基づいてアクセス ポイントの名前と一致する正規表現が作成されます。
たとえば、ダッシュ（-）のデリミタをアクセス ポイント名、San Jose-01-GroundFloor-AP3500i1 で使用すると、正規表現 /(.*)-(.*)-(.*)-(.*)/ が作成されます。

より複雑なアクセス ポイント名がある場合は、手動で正規表現を入力できます。

（注） 先頭と末尾のスラッシュを入力する必要はありません。

ステップ 5 [Test] をクリックします。システムは、アクセス ポイント名に対して作成されたマップと、入力された正規表現を表示します。

ステップ 6 [Group] フィールドを使用して、階層型に一致するグループを割り当てます。
たとえば、アクセス ポイントに SJC14-4-AP-BREAK-ROOM の名前が付けられた場合

この例では、キャンパス名が SJC、ビルディング名が 14、フロア名が 4、AP 名が AP-BREAK-ROOM です。

正規表現 /([A-Z]+)(\d+)-(\d+)-(.*)/ を使用します。

AP 名から、次のグループが抽出されます。

1. SJC
2. 14
3. 4
4. AP-BREAK-ROOM

一致するグループは、1 から始めて、左から右へ割り当てられます。一致するグループを階層要素と一致させるには、各グループ番号のドロップダウン リストを使用して、適切な階層要素を選択します。

これにより、アクセス ポイント名内の位置は、ほとんどどのような順番でも可能になります。

たとえば、アクセス ポイントに EastLab-Atrium2-3-SanFrancisco の名前が付けられた場合

正規表現 /(.*)-(.*)-(.*)-(.*)/ を次のグループと使用する場合：

1. Building
2. デバイス名（Device Name）
3. Floor
4. Campus

自動階層作成では、SanFrancisco というキャンパス、EastLab というビルディング、EastLab の 3 というフロアを作成します。

（注） デバイス名がない、またはデバイスが影響を与えない 2 つの階層タイプでは、他の目的で一致するグループを使用する必要がある場合は、グループを省略できます。

自動階層作成は、アクセス ポイントを配置するマップを計算するためにマップする次のグループが必要です。

表 *16*：グループ

一致内に存在するキャンパス グループ	一致内に存在するビルディング グループ	一致内に存在するフロア グループ	結果の位置
Yes	Yes	Yes	キャンパス > ビルディング > フロア
Yes	Yes	No	不一致
Yes	No	Yes	キャンパス > フロア（フロアが屋外領域の場合）
Yes	No	No	不一致
No	Yes	Yes	システム キャンパス > ビルディング > フロア
no	yes	no	不一致
no	yes	no	不一致
no	no	yes	不一致
no	no	no	不一致

自動階層作成では、フロア名からフロア インデックスを推測しようとします。フロア名が数値の場合、AHC はフロアを正数のフロア インデックスに割り当てます。フロア名が負の数値または文字 B で始まる場合（b1、-4、または B2 など）、AHC はフロアを負数のフロア インデックスに割り当てます。これは、フロアが地下であることを示します。

アクセス ポイントを配置する既存のマップを検索する場合、AHC は、アクセス ポイントの名前と同じフロア インデックスを持つアクセス ポイントのビルディング内のフロアを考慮します。

たとえば、SF > MarketStreet > Sublevel1 というマップがあり、フロア インデックスが -1 の場合、そのフロアにはアクセス ポイント SF-MarketStreet-b1-MON1 が割り当てられます。

ステップ 7 [Next] をクリックします。アクセス ポイントの対象を増やしてテストできます。[Add more device names to test against] フィールドにアクセス ポイントを入力して [Add] をクリックすると、より多くのアクセス ポイントに対する正規表現と一致グループのマッピングをテストできます。
次に、[Test] ボタンをクリックして、テーブル内の各アクセス ポイント名をテストします。各テストの結果がテーブルに表示されます。

必要に応じて、現在の正規表現の正規表現またはグループ マッピングを編集するには、前のステップに戻ります。

ステップ 8 [Next] をクリックしてから、[Save and Apply] をクリックします。これでシステムに正規表現が適用されます。システムはマップに割り当てられていないすべてのアクセス ポイントを処理します。

（注） フロア イメージ、正しい寸法などを含めるようにマップを編集できます。自動階層作成でマップを作成する場合は、20 フィート X 20 フィートのデフォルト寸法が使用されます。正しい寸法などの属性を指定するには、作成されたマップを編集する必要があります。自動階層作成を使用して作成されるマップは、不完全なアイコンがマップ リストに表示されます。マップの編集を完了すると、不完全なアイコンが消えます。[Edit View] リンクをクリックして、不完全なマップの列を非表示にできます。

Map Editor の使用

Map Editor を使って、フロア図面情報を定義、描画、および拡張します。また、Map Editor では、アクセスポイントに対する RF 予測ヒートマップを計算するときに反映できるように、障害物を作成できます。その特定の領域にあるクライアントとタグを特定する、Location Appliances のカバレッジ領域を追加することもできます。

- Map Editor の使用に関するガイドライン, （97 ページ）
- フロア上の包含領域と除外領域に関するガイドライン, （98 ページ）
- Map Editor の表示, （98 ページ）
- Map Editor を使用したカバレッジ領域の描画, （99 ページ）
- フロア上の包含リージョンの定義, （99 ページ）
- フロア上の除外リージョンの定義, （100 ページ）
- フロアでのレール ラインの定義, （101 ページ）

Map Editor の使用に関するガイドライン

Map Editor を使用してビルディングまたはフロア マップを変更する際には、次の内容を考慮してください。

（注） 以前の Floor Plan Editor から .FPE ファイルをインポートするのではなく、Map Editor を使用して壁やその他の障害物を描画することを推奨します。必要に応じて .FPE ファイルを引き続きインポートできます。そのためには、目的のフロア領域に移動します。[Select a command] ドロップダウン リストから、[Edit Floor Area] を選択し、[Go] をクリックします。[FPE File] チェックボックスをオンにしてから、.FPE ファイルを参照して選択します。

- Map Editor でフロア図面に追加できる壁の数に制限はありません。ただし、クライアントワークステーションの処理能力およびメモリによって、Prime Infrastructure でのリフレッシュやレンダリングが制限されることがあります。

  （注） RAM が 1 GB 以下のコンピュータでは、実用的な制限として、フロアごとの壁数を 400 個までにすることを推奨します。

- すべての壁は、Prime Infrastructure が RF カバレッジ ヒートマップを生成する際に使用されます。

フロア上の包含領域と除外領域に関するガイドライン

包含領域と除外領域は、最低 3 点で構成される多角形で表されます。

フロア上の包含リージョンを 1 つだけ定義できます。デフォルトでは、各フロアの包含リージョンは、そのリージョンが Prime Infrastructure に追加されるときに定義されます。包含リージョンは水色の実線で示され、通常はリージョンの輪郭を描きます。

フロア上の除外リージョンを複数定義できます。

新たに定義された包含リージョンと除外リージョンは、Mobility Services Engine によってロケーションがフロアで再計算された後にヒートマップ上に表示されます。

Map Editor の表示

Map Editor を開くには、以下のステップに従います。

ステップ 1 [Design] > [Site Map Design] の順に選択します。

ステップ 2 目的のキャンパスをクリックします。[Site Maps] > [Campus Name] ページが表示されます。

ステップ 3 キャンパスをクリックし、次にビルディングをクリックします。

ステップ 4 目的のフロア領域をクリックします。[Site Maps] > [Campus Name] > [Building Name] > [Floor Area Name] ページが表示されます。

ステップ 5 [Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。[Map Editor] ページが表示されます。

Map Editor を使用したカバレッジ領域の描画

長方形以外のビルディングがある場合、またはフロア内に長方形以外の領域をマークする場合には、Map Editor を使用してカバレッジ領域を描画できます。

Map Editor を使用してカバレッジ領域を描画するには、以下のステップに従います。

ステップ 1 フロア図面が Prime Infrastructure にまだ表示されていない場合は、フロア図面を追加します。

ステップ 2 [Monitor] > [Site Maps] の順に選択します。

ステップ 3 編集する屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 4 [Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。

ステップ 5 [Map Editor] ページで、ツールバーの [Draw Coverage Area] アイコンをクリックします。
ポップアップ メニューが表示されます。

ステップ 6 定義する領域の名前を入力します。[OK] をクリックします。
描画ツールが表示されます。

ステップ 7 輪郭を描く領域に描画ツールを移動します。

- 左マウス ボタンをクリックして、線の描画を開始および終了します。
- 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。

  マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。

ステップ 8 ツールバーの [ディスク] アイコンをクリックして、新たに描画した領域を保存します。

フロア上の包含リージョンの定義

包含領域を定義するには、以下のステップに従います。

ステップ 1 [Design] > [Site Maps] の順に選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 マップで、ツールバーの水色のボックスをクリックします。

（注） 一度に 1 つの包含領域のみ定義できることを示すメッセージ ボックスが表示されます。新しい包含リージョンを定義すると、以前に定義されていた包含リージョンは自動的に削除されます。デフォルトでは、各フロアの包含リージョンは、そのリージョンが Prime Infrastructure に追加されるときに定義されます。包含リージョンは水色の実線で示され、通常はリージョンの輪郭を描きます。

ステップ 6 表示されるメッセージ ボックスで [OK] をクリックします。包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7 包含領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8 含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。再びクリックすると、次の境界線を定義できます。

ステップ 9 領域の輪郭が描画されるまでフロア上の包含リージョンの定義を繰り返したら、描画アイコンをダブルクリックします。水色の実線によって包含領域が定義されます。

ステップ 10 [Command] メニューから [Save] を選択するか、ツールバーの**ディスク** アイコンをクリックして、包含リージョンを保存します。

（注） 包含領域を誤って定義した場合は、領域をクリックします。選択された領域の輪郭が水色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 11 [Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。これをすべてのフロア マップに適用する場合は、[Save settings] をクリックします。[Layers configuration] ページを閉じます。

ステップ 12 Prime Infrastructure と MSE データベースを再同期するには、[Services] > [Synchronize Services] の順に選択します。

（注） 2 つの DB がすでに同期されている場合は、変更があるたびに自動的に再同期が実行されます。明示的に再同期する必要はありません。

ステップ 13 [Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

（注） 新たに定義された包含リージョンと除外リージョンは、Mobility Services Engine によって既存デバイスのロケーションが再計算された後のみにロケーション計算に含まれます。

フロア上の除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外できます。通常、除外領域は包含領域の境界内に定義されます。

除外領域を定義するには、以下のステップに従います。

ステップ 1 [Design] > [Site Maps] の順に選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 マップで、ツールバーの紫色のボックスをクリックします。

ステップ 6 表示されるメッセージ ボックスで [OK] をクリックします。除外領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7 除外領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8 除外する領域の境界に沿って描画アイコンを移動させます。1回クリックして境界線を開始し、再びクリックして境界線を終了します。

ステップ 9 領域の輪郭が描画されるまでフロア上の除外リージョンの定義を繰り返したら、描画アイコンをダブルクリックします。定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。除外された領域は紫色で網掛けされます。

ステップ 10 すべての除外領域を定義したら、[Command] メニューから [Save] を選択するか、ツールバーの**ディスク**アイコンをクリックして、除外リージョンを保存します。

（注） 除外領域を削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 11 [Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。これをすべてのフロア マップに適用する場合は、[Save settings] をクリックします。完了したら、[Layers configuration] ページを閉じます。

ステップ 12 Prime Infrastructure と MSE データベースを再同期するには、[Services] > [Synchronize Services] の順に選択します。

（注） 2 つの DB がすでに同期されている場合は、変更があるたびに自動的に再同期が実行されます。明示的に再同期する必要はありません。

ステップ 13 [Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

フロアでのレール ラインの定義

フロア上にコンベヤ ベルトを表すレール ラインを定義できます。また、レール領域の周囲にスナップ幅とも呼ばれる、ロケーション計算を一層サポートする領域を定義できます。この領域は、クライアントが表示されると予測される領域を表します。スナップ幅の領域内に配置されたクラ

イアントは、レール ライン上に表示されるか（多数）、スナップ幅領域の外側に表示されます（少数）。

（注） レール ラインの設定はタグには適用されません。

スナップ幅領域は、フィートまたはメートル（ユーザ定義）単位で定義され、レールの片側（東および西、または北および南）からモニタされる距離を表します。

レールをフロアに定義するには、以下のステップに従います。

ステップ 1 [Design] > [Site Maps] の順に選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから、[Map Editor] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 マップで、ツールバーの**レール** アイコン（紫色の除外アイコンの右側）をクリックします。

ステップ 6 表示されるメッセージ ダイアログボックスで、レールのスナップ幅（フィートまたはメートル）を入力し、[OK] をクリックします。描画アイコンが表示されます。

ステップ 7 レールラインの開始ポイントで**描画**アイコンをクリックします。ラインの描画を停止するときやラインの方向を変えるときは、再びクリックします。

ステップ 8 フロア マップ上にレール ラインを完全に描画したら、**描画**アイコンを 2 回クリックします。レール ラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。

（注） レール ラインを削除するには、削除する領域をクリックします。選択された領域の輪郭が紫色の破線で描かれます。次に、ツールバーの [X] アイコンをクリックします。領域がフロア マップから削除されます。

ステップ 9 フロア マップで、[Layers] ドロップダウン リストを選択します。

ステップ 10 完了したら、[Rails] チェックボックスがまだオンになっていない場合にはオンにし、[Save settings] をクリックし、[Layers configuration] パネルを閉じます。

ステップ 11 Prime Infrastructure と Mobility Services Engine を再同期するには、[Services] > [Synchronize Services] の順に選択します。

ステップ 12 [Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。
[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを確認できます。

屋外領域の追加

（注） 屋外領域マップをデータベースに追加したことがあるかどうかに関係なく、屋外領域を Prime Infrastructure データベース内のキャンパス マップに追加することができます。

屋外領域をキャンパス マップに追加するには、以下のステップに従います。

ステップ 1 屋外領域のマップをデータベースに追加する場合は、マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。ファイル システムの特定の場所にあるマップを参照して、インポートします。

（注） 屋外領域を追加するのにマップは必要ありません。屋外領域をデータベースに追加するため、領域の寸法を定義する必要があるだけです。Prime Infrastructure では、作業領域に合わせてマップのサイズが自動的に調整されるため、マップは任意のサイズにすることができます。

ステップ 2 [Design] > [Site Maps] の順に選択します。

ステップ 3 目的のキャンパスをクリックすると、[Design] > [Site Maps] > [Campus View] ページが表示されます。

ステップ 4 [Select a command] ドロップダウン リストから、[New Outdoor Area] を選択します。

ステップ 5 [Go] をクリックします。[Create New Area] ページが表示されます。

ステップ 6 [New Outdoor Area] ページで、次の情報を入力します。

- [Name]：新しい屋外領域のユーザ定義の名前。
- [Contact]：ユーザ定義の連絡先の名前。
- [Area Type (RF Model)]：[Cubes And Walled Offices]、[Drywall Office Only]、[Outdoor Open Space]（デフォルト）。
- [AP Height (feet)]：アクセス ポイントの高さを入力します。
- [Image File]：屋外領域マップを含むファイルの名前。[Browse] をクリックしてファイルを検索します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Place] をクリックして屋外領域をキャンパス マップに配置します。Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更された屋外領域の四角形が作成されます。

ステップ 9 屋外領域の四角形をクリックし、キャンパス マップ上の目的の位置までドラッグします。

ステップ 10 [Save] をクリックして、この屋外領域とキャンパス上の位置をデータベースに保存します。

（注） 屋外領域には、該当する [Maps] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 11 （任意）新しい屋外領域に位置プレゼンス情報を割り当てるには、[Edit Location Presence Info] を選択し、[Go] をクリックします。

（注） デフォルトでは、[Override Child Element Presence Info] チェックボックスがオンになっています。屋外領域については、この設定を変更する必要はありません。

プランニング モードの使用

プランニング モードでは、プランニング ツールが起動されるブラウザ ウィンドウで Map Editor を開きます。元のブラウザ ウィンドウがフロアのページから移動している場合は、フロアのページに戻って、Map Editor を起動する必要があります。

データ トラフィック、音声トラフィック、および位置がそれぞれアクティブかどうかに基づいて、アクセス ポイントの推奨される数および位置を計算できます。

（注） プランニング モードでは、各プロトコル（802.11a または 802.11 b/g）に指定されるスループットに基づいて、ネットワーク内で最適カバレッジを提供するために必要な合計アクセス ポイント数が計算されます。

プランニング モードのオプション：

- [Add APs]：マップへのアクセス ポイントの追加を可能にします。詳細については、「アクセス ポイントのフロア領域への追加」（10-11 ページ）を参照してください。
- [Delete APs]：選択したアクセス ポイントを削除します。
- [Map Editor]：[Map Editor] ウィンドウを開きます。
- [Synchronize with Deployment]：プランニング モードのアクセス ポイントを現在の導入シナリオと同期します。
- [Generate Proposal]：現在のアクセス ポイント導入のプランニング概要を表示します。
- [Planned AP Association Tool]：Excel または CSV ファイルから AP アソシエーションの追加、削除、またはインポートを実行できます。アクセス ポイントを定義したら、[Planned AP Association Tool] を使用して、そのアクセス ポイントをベース無線の MAC アドレスにアソシエートできます。AP が検出されない場合、AP はスタンバイ バケットに送られ、AP が検出されたときにアソシエートされます。

（注） AP アソシエーションには、AP はフロアまたは屋外領域に属さないという制限があります。AP がすでにフロアまたは屋外領域に割り当てられている場合は、スタンバイ バケットが AP を保持し、フロアまたは屋外領域から AP が削除されたときに、指定されたフロアに配置されます。1 つの MAC アドレスを複数のフロアまたは屋外領域のバケットに入力することはできません。

（注） マップの同期は、AP がベース無線の MAC アドレスにアソシエートされている場合のみ動作し、イーサネット MAC アドレスにアソシエートされている場合は動作しません。

チョークポイントを使用したタグの位置報告の精度の向上

チョークポイントは、チョークポイントのベンダーによって推奨されるとおりに設置および設定されます。チョークポイントのインストールが完了して動作可能になったら、チョークポイントをロケーション データベースに入力して、Prime Infrastructure マップ上に表示できます。

アクティブな Cisco CX 準拠のタグと一緒にチョークポイントを使用すると、タグとそのアセットに関するロケーション情報が即座に提供されます。Cisco CX タグがチョークポイントの範囲外に

出ると、後続のビーコン フレームには、チョークポイントの識別情報が何も含まれません。タグのロケーションは、デフォルトで、タグに関連付けられたアクセス ポイントにより報告されるRSSI に基づいた標準の計算方法で決定されます。

- Prime Infrastructure へのチョークポイントの追加, （106 ページ）
- Prime Infrastructure マップへのチョークポイントの追加, （106 ページ）
- Prime Infrastructure からのチョークポイントの削除, （107 ページ）

Prime Infrastructure へのチョークポイントの追加

Prime Infrastructure データベースにチョークポイントを追加するには、以下のステップに従います。

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

ステップ 2 [Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 3 [Go] をクリックします。

ステップ 4 チョークポイントの MAC アドレスと名前を入力します。

ステップ 5 [Entry/Exit Chokepoint] チェックボックスをオンにします。

ステップ 6 チョークポイントのカバレッジ範囲を入力します。

（注） チョークポイントの範囲は視覚的に表示されるだけです。これは製品固有です。実際の範囲は、該当するチョークポイント ベンダー ソフトウェアを使用して別個に設定する必要があります。

ステップ 7 [OK] をクリックします。

（注） データベースにチョークポイントを追加したら、適切な Prime Infrastructure フロア マップに配置できます。

Prime Infrastructure マップへのチョークポイントの追加

チョークポイントをマップに追加するには、以下のステップに従います。

ステップ 1 [Design] > [Site Maps] の順に選択します。

ステップ 2 [Maps] ページで、チョークポイントのフロアの位置に対応するリンクを選択します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 4 [Go] をクリックします。

（注） [Add Chokepoints] 概要ページには、データベースには存在しているが、まだマップされていない、最近追加されたチョークポイントがすべて一覧表示されます。

ステップ 5 マップ上に配置するチョークポイントの横にあるチェックボックスを選択します。

ステップ 6 [OK] をクリックします。
チョークポイントアイコンが左上隅に配置されたマップが表示されます。これで、マップ上にチョークポイントを配置する準備ができました。

ステップ 7 チョークポイント アイコンを左クリックし、適切な位置までドラッグします。
（注） チョークポイント アイコンを配置するためにクリックすると、左側のダイアログボックスにチョークポイントの MAC アドレス、名前、およびカバレッジ範囲が表示されます。

ステップ 8 [Save] をクリックします。
フロア マップ ページが再び表示され、追加されたチョークポイントがマップに表示されます。

（注） 新たに作成されたチョークポイント アイコンは、そのフロアの表示設定に応じて、マップに表示される場合と表示されない場合があります。

（注） チョークポイントの周囲の輪は、カバレッジ領域を示しています。CCX タグとそのアセットがカバレッジ領域内を通過すると、位置の詳細がブロードキャストされ、タグはチョークポイント カバレッジ円上に自動的にマップされます。タグがチョークポイントの範囲外に出ると、その位置は以前と同様に計算されるので、チョークポイントの輪の上にはマップされなくなります。

（注） チョークポイントのマップ アイコンの上にマウス カーソルを移動すると、チョークポイントの MAC アドレス、名前、Entry/Exit チョークポイント、スタティック IP アドレス、および範囲が表示されます。

ステップ 9 チョークポイントがマップ上に表示されない場合は、[Floor Settings] メニューにある [Chokepoints] チェックボックスを選択します。

（注） すべてのマップに対してこの表示条件を保存しない場合には、[Save Settings] をクリックしないでください。

（注） チョークポイント情報を適用するには、ネットワーク設計を Mobility Services Engine またはロケーション サーバと同期する必要があります。

Prime Infrastructure からのチョークポイントの削除

一度に 1 つ以上のチョークポイントを削除できます。チョークポイントを削除するには、以下のステップに従います。

ステップ 1 [Configure] > [Chokepoints] の順に選択します。[Chokepoints] ページが表示されます。

ステップ 2 削除するチョークポイントの隣のチェックボックスをオンにします。

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

ステップ 4 チョークポイントの削除を確認するには、表示されるダイアログボックスで [OK] をクリックします。
[Chokepoints] ページが再度表示され、チョークポイントの削除を確認します。削除されたチョークポイントはページには表示されなくなります。

第 6 章

wIPS およびプロファイルの設定

この章では、wIPSプロファイルおよびwIPSを操作するために併せて設定する必要がある項目の設定方法について説明します。

この章の内容は、次のとおりです。

- wIPS およびプロファイルの設定，109 ページ

wIPS およびプロファイルの設定

この章では、wIPS プロファイルおよび wIPS を操作するために併せて設定する必要がある項目の設定方法について説明します。

この章の内容は、次のとおりです。

注意事項と制約事項

- Mobility Services Engine（MSE）は 1 つの Prime Infrastructure からのみ設定できます。
- ご使用の wIPS がコントローラ、アクセス ポイント、および MSE で構成されている場合、コントローラと MSE を UTC タイムゾーンに設定する必要があります。
- コントローラは 1 つの設定プロファイルに関連付けられます。そのコントローラに接続されている wIPS モード アクセス ポイントはすべて同じ wIPS 設定を共有します。

前提条件

wIPS プロファイルを設定する前に、次の手順を実行する必要があります。

1. Mobility Services Engine をインストールします（まだネットワーク内で動作していない場合）。『*Cisco 3350 Mobility Services Engine Getting Started Guide*』または『*Cisco 3310 Mobility Services Engine Getting Started Guide*』を参照してください。
2. Mobility Services Engine を Prime Infrastructure に追加します（まだ追加されていない場合）。

3 wIPS モニタ モードまたはローカル wIPS モードで動作するようにアクセス ポイントを設定します。

4 wIPS プロファイルを設定します。

wIPS 設定およびプロファイル管理について

wIPS プロファイルの設定は、プロファイルの表示と変更に使用される Prime Infrastructure から始まるチェーン階層を進みます。実際のプロファイルは、MSE で実行するワイヤレス IPS サービス内に保存されます。

プロファイルは、Mobility Services Engine 上の wIPS サービスから、特定のコントローラに伝播され、次に、その各コントローラに関連付けられている wIPS モード アクセス ポイントに透過的にこのプロファイルが伝達されます。

Prime Infrastructure で wIPS プロファイルへの設定変更が行われ、一連の Mobility Services Engine およびコントローラに適用される場合、次のようになります。

1 Prime Infrastructure で設定プロファイルが変更され、バージョン情報が更新されます。

2 XML ベースのプロファイルが Mobility Services Engine で実行する wIPS エンジンに適用されます。この更新は、SOAP/XML プロトコルを介して行われます。

3 Mobility Services Engine 上の wIPS は、NMSP を使用して設定プロファイルを適用することによって、そのプロファイルに関連付けられている各コントローラを更新します。

4 コントローラは更新された wIPS プロファイルを受け取り、それを NVRAM に保存し（以前のすべてのバージョンのプロファイルを置き換える）、CAPWAP 制御メッセージを使用して、更新されたプロファイルをそれに関連付けられた wIPS アクセス ポイントに伝播します。

5 wIPS モード アクセス ポイントはコントローラから更新されたプロファイルを受け取り、その wIPS ソフトウェア エンジンに変更を適用します。

ここでは、次の内容について説明します。

- 注意事項と制約事項, （110 ページ）
- wIPS モニタ モードのアクセス ポイントの設定, （111 ページ）
- wIPS プロファイルの設定

注意事項と制約事項

- wIPS モニタ モードをサポートしているのは、Cisco Aironet 1130、1140、1240、1250、1260、1600、2600、3600、3502E、および 3502I シリーズのアクセス ポイントだけです。

wIPS モニタ モードのアクセス ポイントの設定

wIPS モニタ モードで動作するようにアクセス ポイントを設定するには、以下のステップに従います。

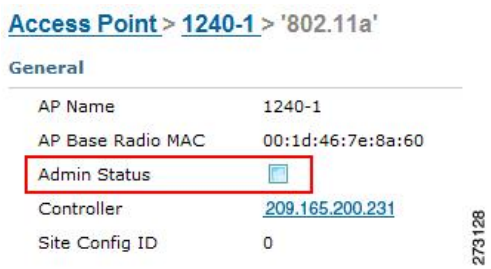
ステップ 1 [Configure] > [Access Points] の順に選択します。

ステップ 2 [802.11a] または [802.11b/g] 無線リンクをクリックします。

図 *11*：*[Configure] > [Access Points] > [Radio]*

ステップ 3 [Access Point] ページで、[Admin Status] チェックボックスをオフにして無線を無効にします。

図 *12*：*[Access Points] > [Radio]*



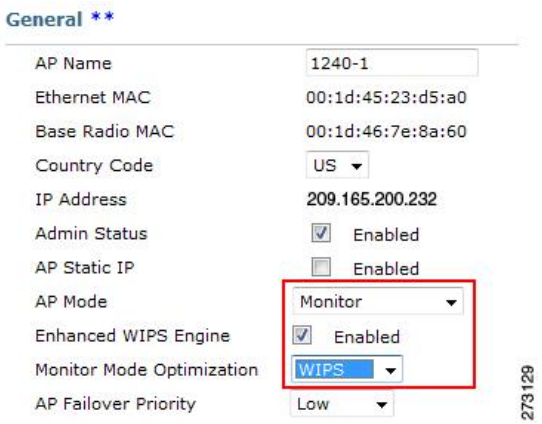
ステップ 4 [Save] をクリックします。

（注） wIPS モニタ モードに設定されるアクセス ポイント上の各無線について、これらの手順を繰り返します。

ステップ 5 無線が無効になったら、[Configure] > [Access Points] の順に選択し、無効にした無線のアクセス ポイントの名前をクリックします。

ステップ 6 アクセス ポイントのダイアログボックスで、[AP Mode] ドロップダウン リストから [Monitor] を選択します。

図 *13*：*[Configure] > [Access Points] >* アクセス ポイントの詳細



ステップ 7 [Enhanced WIPS Engine] の [Enabled] チェックボックスをオンにします。

ステップ 8 [Monitor Mode Optimization] ドロップダウン リストから [WIPS] を選択します。
これにより、モニタ モードで AP 無線とモジュール無線が配置されます。

ELM モードで AP 無線を配置する場合、またはモニタ モードでモジュール無線を配置する場合、AP モードとしてローカルおよび wIPS として submide を選択する必要があります。

ステップ 9 [Save] をクリックします。

ステップ 10 アクセス ポイントをリブートするように求められたら、[OK] をクリックします。

ステップ 11 アクセス ポイント無線を再度有効にするには、[Configure] > [Access Points] の順に選択します。

ステップ 12 適切なアクセス ポイント無線をクリックします。

図 *14*：*[Configure] > [Access Points] > [Radio]*

ステップ 13 [Radio Detail] ページで、[Admin Status] の [Enabled] チェックボックスをオンにします。

ステップ 14 [Save] をクリックします。
wIPS モニタ モードに設定した各アクセス ポイントおよびその各無線について、この手順を繰り返します。

wIPS プロファイルの設定

デフォルトで、Mobility Services Engine と対応する wIPS アクセス ポイントは Prime Infrastructure からデフォルトの wIPS プロファイルを継承します。このプロファイルは、デフォルトで有効にされている大部分の攻撃アラームによってあらかじめ調整されており、wIPS アクセス ポイントと同じ RF グループ内のアクセス ポイントに対する攻撃を監視します。このように、システムは WLAN インフラストラクチャと wIPS アクセス ポイントの両方が同じコントローラ上に混合されている統合ソリューションを利用する構成モデルに対する攻撃を監視するようにあらかじめ設定されています。

（注） 次の設定手順の一部はオーバーレイだけとしてマークされており、Autonomous や完全に個別のコントローラベースの WLAN などの既存の WLAN インフラストラクチャを監視するように適応型 wIPS ソリューションを導入している場合にだけ実行されます。

wIPS プロファイルを設定するには、以下のステップに従います。

ステップ 1 [Configure] > [wIPS Profiles] の順に選択します。
[wIPS Profiles] ページが表示されます。

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

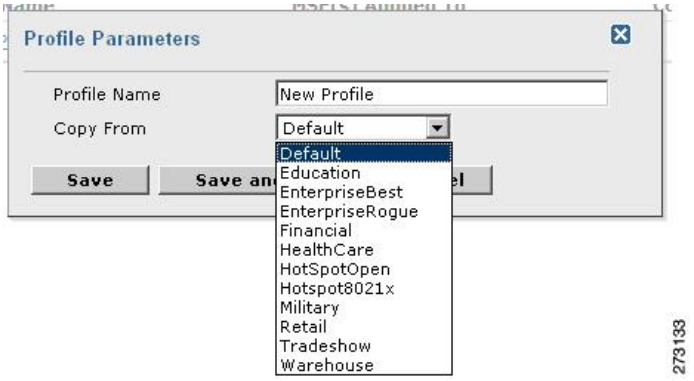
ステップ 3 プロファイル テンプレートの選択
[Profile Parameters] ダイアログボックスで、[Copy From] ドロップダウンリストからプロファイル テンプレートを選択します。

（注） wIPS には一連のプロファイルテンプレートがあらかじめ定義されているので、それらをベースとして使用してカスタム プロファイルを作成できます。各プロファイルは、そのプロファイルで有効な特定のアラームと同様に、特定の業務または用途に合わせて作成されています。

（注） デフォルト プロファイルは編集できません。

（注）　プロファイルをコントローラに適用するために NMSP セッションがアクティブなことを確認します。

図 *15* : *[Profile Parameters* ダイアログボックス



ステップ 4　プロファイルを選択し、プロファイル名を入力したら、[Save and Edit] をクリックします。詳細については、wIPS プロファイル，（119 ページ）を参照してください。

ステップ 5　**監視する SSID を設定します。**

（任意）[SSID Group List] ページで SSID を設定します。デフォルトで、ローカル ワイヤレス LAN インフラストラクチャ（同じ RF グループ名を持つ AP によって定義された）に対して仕掛けられた攻撃が監視されます。オーバーレイ構成モデルで構成する場合など、他のネットワークに対する攻撃を監視させる必要がある場合は、SSID グループ機能を使用する必要があります。

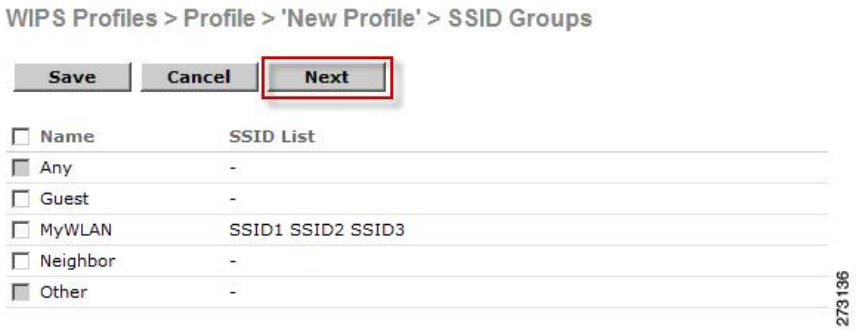
（注）　この手順が必要ない場合は、単に [Next] をクリックします。

図 *16*：*[SSID Groups Summary]* ペイン

1. [MyWLAN] チェックボックスをオンにし、ドロップダウン リストから [Edit Group] を選択して、[Go] をクリックします。
2. 監視する SSID を入力します。この手順は、オーバーレイ構成モデルで一般的な別の WLAN インフラストラクチャに対する攻撃を監視するためにシステムが使用される場合に必要です。
3. SSID 名を入力し（複数の名前を入力する場合は 1 つのスペースで区切る）、[Save] をクリックします。

   SSID が正常に追加されたことを確認する [SSID Groups] ページが表示されます。詳細については、wIPS SSID グループ リストの設定, （122 ページ）を参照してください。

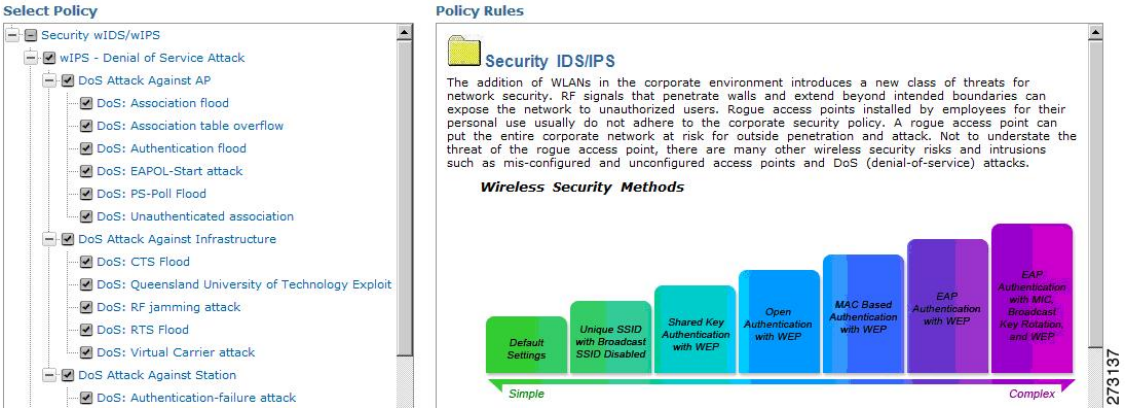
図 *17*：*[New Profile] > [SSID Groups]* ページ



4. [Next] をクリックします。

   [Select Policy] および [Policy Rules] 概要ペインが表示されます。

図 *18*：*[Next] > [Select Policy Summary]* ペイン



ステップ 6　プロファイルの編集

検出および報告対象の攻撃を有効または無効にするには、[Select Policy] ペインでその攻撃タイプの横にあるチェックボックスをオンにします。

ステップ 7　プロファイルを編集するには、攻撃タイプの名前（DoS：アソシエーションフラッドなど）をクリックします。

その攻撃タイプの設定ペインが、ポリシー ルールの説明の上の右側のペインに表示されます。

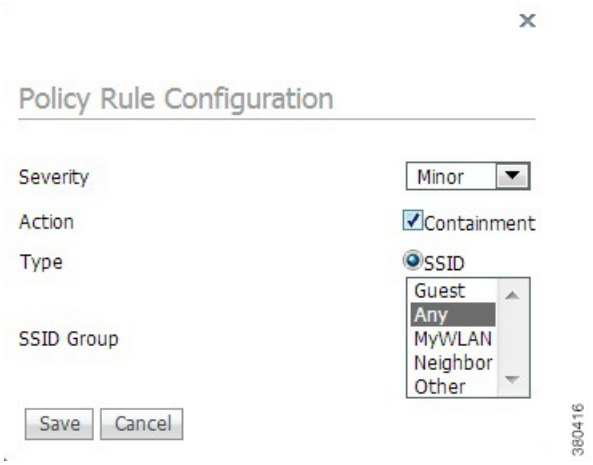
図 *19*：*[Policy Rules]*ペイン

ステップ 8　ポリシー ルールの編集

ポリシー ルールを変更するには、[Policy Rules] ページで、ポリシー ルールの横にあるチェックボックスをオンにし、[Edit] をクリックします。

[Policy Rule Configuration] ダイアログボックスが表示されます。ポリシーの[Policy Rule Configuration] ダイアログボックスで次を設定します。

図 *20* : *[Policy Rule Configuration]* ダイアログボックス



a) [Severity] ドロップダウン リストから、変更するアラームの重大度を選択します。使用可能なオプションは、[Minor]、[Major]、[Critical]、[Warning]です。

b) 自動封じ込め動作を有効にするには、[Containment] チェックボックスをオンにします。

（注） 次のセキュリティ突破攻撃は、リリース 7.5 で不正 AP 封じ込めに対して設定できます。

- ソフト AP またはホスト AP の検出
- Airsnarf 攻撃の検出
- ハニーポット AP の検出
- Hotspotter ツールの検出
- Karma ツールの検出
- デバイス ブロードキャスト XSS SSID

c) このアラームのパケットをキャプチャする場合は、[Forensic] チェックボックスをオンにします。

d) 必要に応じて、アクティブなアソシエーションの数を変更します。（この値はアラーム タイプによって異なります。）

e) [SSID Group] ドロップダウン リストから、攻撃を監視する WLAN インフラストラクチャのタイプ（[SSID] または [Device Group]）を選択します。

- [SSID] を選択した場合は、ステップ 9 に進みます。
- [Device Group]を選択した場合は、ステップ 10 に進みます。

（注） デフォルト タイプは [Device Group] と [Internal] です。.Internal は、同じ RF グループ内のすべてのアクセス ポイントを示します。タイプに [SSID] を選択すると、オーバーレイ構成に一般的な個別ネットワークを監視できます。

ステップ 9 ポリシー ルールの追加（任意）

（任意）オーバーレイ構成に限り、SSID のポリシー ルールを追加するには、以下の手順に従います。

1 ポリシー ルールを追加するには、[Add] をクリックします。

図 *21*：ポリシー ルールの追加

2 [Policy Rule Configuration] ダイアログボックスで、[SSID Group] リストから [MyWLAN] を選択します。

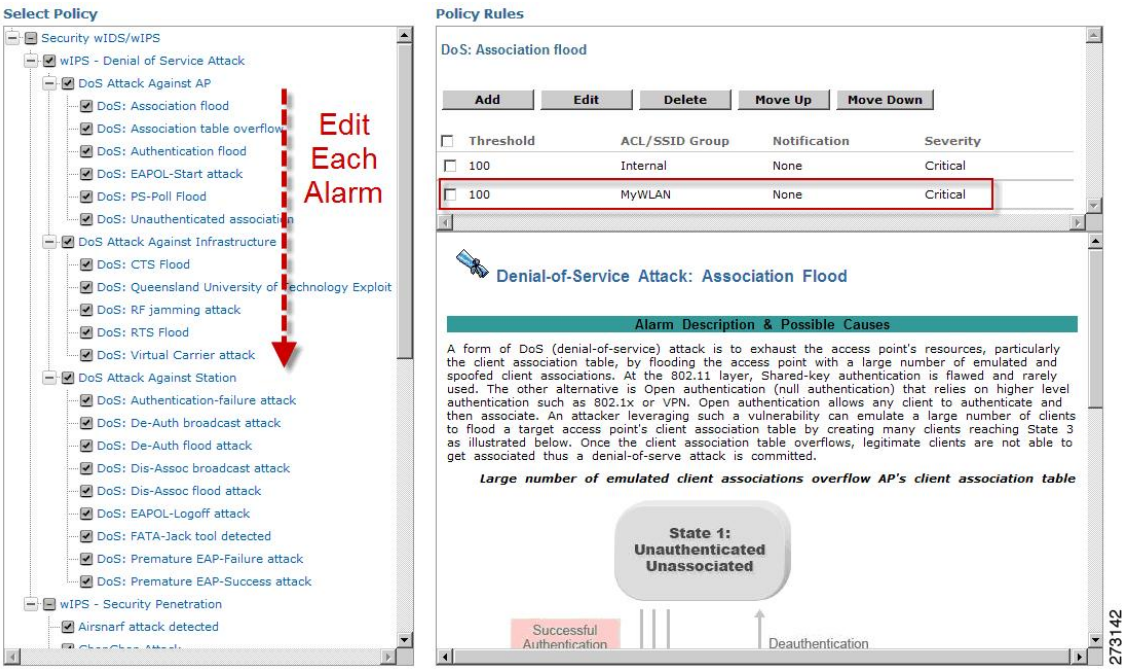
（注） タイプに SSID がすでに選択されています。

3 すべての変更が完了したら、[Save] をクリックします。

4 各ポリシー ルールを変更します。すべての変更を完了したら、ステップ 10 に進みます。

（注） SSID によって別の WLAN インフラストラクチャを監視するようにシステムを設定する場合、監視するすべてのポリシー ルールごとに変更する必要があります。個別の各アラームに、システムで以前に作成した SSID グループに対する攻撃を監視するように定義したポリシー ルールを作成する必要があります。

図 *22*：*SSID* モニタリングに関するポリシー ルールの編集

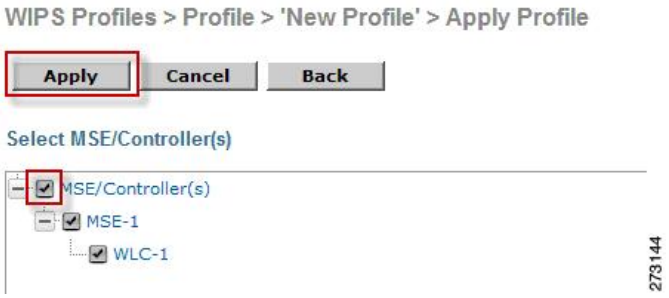


ステップ 10 [Profile Configuration] ダイアログボックスで、[Save] をクリックしてプロファイル（SSID またはデバイス グループ）を保存し、[Next] をクリックします。

図 *23*：*[Profile Configuration]* ダイアログボックス

ステップ 11 プロファイルを適用する MSE/コントローラの組み合わせを選択して、[Apply] をクリックします。

図 *24*：*[Apply Profile]* ダイアログボックス



wIPS プロファイル

[wIPS Profiles] > [Profile List] ページでは、現在の wIPS プロファイルの表示、編集、適用、削除を行ったり、新しいプロファイルを追加したりできます。

ヒント　Cisco Adaptive wIPS の特長と機能の詳細については、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps9817/index.html

Prime Infrastructure の wIPS プロファイル リストにアクセスするには、[Configure] > [wIPS Profiles] の順に選択します。ページは [wIPS Profiles] > [Profile List] から表示されます。[Profile List] が現在表示されていない場合は、wIPS プロファイル左側のサイドメニュー バーから [Profile List] を選択します。

[Profile List] には、各プロファイルの次の情報が表示されます。

- [Profile Name]：現在のプロファイルのユーザ定義名を示します。プロファイルの詳細を表示または編集するには、プロファイル名をクリックします。

（注） マウスをプロファイル名に合わせると、プロファイル ID とバージョンが表示されます。

- [MSE(s) Applied To]：このプロファイルが適用されている Mobility Services Engine（MSE）の数を示します。MSE 番号をクリックすると、プロファイルの割り当ての詳細が表示されます。
- [Controller(s) Applied To]：このプロファイルが適用されているコントローラの数を示します。コントローラ番号をクリックすると、プロファイルの割り当ての詳細が表示されます。

ここでは、次の内容について説明します。

- プロファイルの追加
- プロファイルの削除
- 現在のプロファイルの適用

プロファイル エディタを使用すると、新しいプロファイルの作成や現在のプロファイルの変更が可能です。詳細については、プロファイル エディタを使用したプロファイル設定を参照してください。

プロファイルの追加

デフォルトまたは事前設定されたプロファイルを使用して、新しいwIPSプロファイルを作成できます。

ヒント Cisco Adaptive wIPS 機能の詳細については、Cisco.com にアクセスして、マルチメディア プレゼンテーションをご覧ください。Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

wIPS プロファイルを追加するには、以下のステップに従います。

ステップ 1 [Configure] > [wIPS Profiles] の順に選択します。ページは [wIPS Profiles] > [Profile List] です。

ステップ 2 [Select a command] ドロップダウン リストから [Add Profile] を選択します。

ステップ 3 [Go] をクリックします。

ステップ 4 [Profile Parameters] ページの [Profile Name] テキスト ボックスにプロファイル名を入力します。

ステップ 5 ドロップダウン リストから、該当する定義済みのプロファイルを選択するか、[Default] を選択します。定義済みのプロファイルには次のものがあります。

- Education

- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

ステップ 6 次のいずれかを選択します。

- [Save]：プロファイルを、Mobility Services Engine やコントローラを割り当てずに、変更なしで Prime Infrastructure データベースに保存します。プロファイルはプロファイル リストに表示されます。
- [Save and Edit]：プロファイルを保存し、編集します。
- [Cancel]：プロファイルを作成せずに [Profile Parameters] ページを閉じます。

プロファイルの削除

wIPS プロファイルを削除するには、以下のステップに従います。

ステップ 1 [Configure] > [wIPS Profiles] の順に選択します。ページのデフォルトは、[wIPS Profiles] > [Profile List] です。

ステップ 2 削除する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3 [Select a command] ドロップダウン リストから [Delete Profile] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 [OK] をクリックして、削除を実行します。

（注） プロファイルがコントローラに適用されている場合、そのプロファイルは削除できません。

現在のプロファイルの適用

ヒント　Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html.Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

MSE 7.6 リリースの PI 1.4.x または PI 2.x を使用して、wIPS プロファイルを WLC 7.5 以前のリリースに適用することはできません。

wIPS プロファイルを適用するには、以下のステップに従います。

ステップ 1　[Configure] > [wIPS Profiles] の順に選択します。ページのデフォルトは、[wIPS Profiles] > [Profile List] です。

ステップ 2　適用する wIPS プロファイルのチェックボックスをオンにします。

ステップ 3　[Select a command] ドロップダウン リストから [Apply Profile] を選択します。

ステップ 4　[Go] をクリックします。

ステップ 5　プロファイルを適用する Mobility Services Engine とコントローラを選択します。

（注）　新しい割り当てが現在の割り当てと異なる場合、プロファイルを異なる名前で保存するよう求められます

ステップ 6　該当する Mobility Services Engine とコントローラが選択されている場合、次のいずれかを選択します。

- [Apply]：現在のプロファイルを、選択された Mobility Services Engine またはコントローラに適用します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。

wIPS SSID グループ リストの設定

SSID（Service Set IDentifier）は、802.11（Wi-Fi）ネットワークを識別するトークンまたはキーです。802.11 ネットワークに参加するには、SSID を知っている必要があります。SSID は、SSID グループ リスト機能を使用して、グループとして wIPS プロファイルに関連付けることができます。

SSID グループは、[Global SSID Group List] ページ（[Configure] > [wIPS Profiles] > [SSID Group List]）からインポートするか、[SSID Groups] ページから直接追加することで、プロファイルに追加できます。

ここでは、次の内容について説明します。

- グローバル SSID グループ リスト

- SSID グループ

ヒント　Cisco Adaptive wIPS の特長と機能の詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.htmlここでは、Prime Infrastructure のさまざまなトピックについてモジュールを学習することもできます。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

グローバル SSID グループ リスト

[SSID Group List] ページでは、グローバル SSID グループを追加または設定できます。このグローバル SSID グループは、後で該当する wIPS プロファイルにインポートできます。

ヒント　Cisco Adaptive wIPS の特長と機能に関する詳細を確認するには、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

[SSID Group List] ページにアクセスするには、[Configure] > [wIPS Profiles] の順に選択します。左側のサイドバー メニューから、[SSID Group List] を選択します。[SSID Group List] ページには、現在の SSID グループとそれに関連付けられた SSID が表示されます。

ここでは、次の内容について説明します。

- グループの追加
- グループの編集
- グループの削除

グループの追加

SSID グループを追加するには、以下のステップに従います。

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

ステップ 2 左側のサイドバー メニューから、[SSID Group List] を選択します。

ステップ 3 [Select a command] ドロップダウン リストから [Add Group] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 SSID 設定ページで、テキスト ボックスに SSID グループ名を入力します。

ステップ 6 [SSID List] テキスト ボックスに SSID を入力します。SSID が複数ある場合はスペースで区切ります。

ステップ 7 終了したら、次のいずれかを選択します。

- [Save]：SSID グループを保存し、SSID グループ リストに追加します。
- [Cancel]：新しい SSID グループを保存せずに SSID 設定ページを閉じます。

（注） SSID グループをプロファイルにインポートするには、[Configure] > [wIPS Profile] の順に選択します。[SSID Groups] ページを開くには、適切なプロファイル名をクリックします。[Select a command] ドロップダウン リストから、[Add Groups from Global List] を選択します。インポートする SSID グループのチェックボックスをオンにし、[Save] をクリックします。

グループの編集

現在の SSID グループを編集するには、以下のステップに従います。

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

ステップ 2 左側のサイドバー メニューから、[SSID Group List] を選択します。

ステップ 3 編集する SSID グループのチェックボックスをオンにします。

ステップ 4 [Select a command] ドロップダウン リストから [Edit Group] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 SSID 設定ページで、SSID グループ名または SSID リストに必要な変更を行います。

ステップ 7 終了したら、次のいずれかを選択します。

- [Save]：現在の変更内容を保存し、SSID 設定ページを閉じます。
- [Cancel]：変更内容を保存せずに SSID 設定ページを閉じます。

グループの削除

現在の SSID グループを削除するには、以下のステップに従います。

ステップ 1 [Configure] > [wIPS Profiles] の順に選択します。
ステップ 2 左側のサイドバー メニューから、[SSID Group List] を選択します。
ステップ 3 削除する SSID グループのチェックボックスをオンにします。
ステップ 4 [Select a command] ドロップダウン リストから [Delete Group] を選択します。
ステップ 5 [Go] をクリックします。
ステップ 6 [OK] をクリックして、削除を実行します。

SSID グループ

[SSID Groups] ページは、プロファイル エディタにアクセスしたときに表示される最初のページです。このページには、現在の wIPS プロファイルに含まれている SSID グループが表示されます。

このページから、現在のプロファイルの SSID グループを追加、インポート、編集、または削除できます。

ヒント Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html.Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

ここでは、次の内容について説明します。

- グループの追加
- グローバル リストからのグループの追加
- グループの編集
- グループの削除

グループの追加

SSID グループを現在の wIPS プロファイルに追加するには、以下のステップに従います。

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

ステップ 2 左側のサイドバー メニューから、[Profile List] を選択します。

ステップ 3 該当する wIPS プロファイルのプロファイル名をクリックします。

ステップ 4 [Select a command] ドロップダウン リストから [Add Group] を選択します。

ステップ 5 [Go] をクリックします。

ステップ 6 SSID 設定ページで、テキスト ボックスに SSID グループ名を入力します。

ステップ 7 [SSID List] テキスト ボックスに SSID を入力します。複数の SSID を指定する場合は、カンマで区切ります。

ステップ 8 終了したら、次のいずれかを選択します。

- [Save]：SSID グループを保存し、SSID グループ リストに追加します。
- [Cancel]：新しい SSID グループを保存せずに SSID 設定ページを閉じます。

グローバル リストからのグループの追加

SSID グループは、グローバル SSID グループ リストからインポートして追加することもできます。グローバル SSID グループ リスト作成の詳細については、グローバル SSID グループ リストを参照してください。

SSID グループをプロファイルにインポートするには、以下のステップに従います。

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

ステップ 2 [SSID Groups] ページを開くには、該当するプロファイルのプロファイル名をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Groups from Global List] を選択します。

ステップ 4 インポートする SSID グループのチェックボックスをオンにします。

ステップ 5 [Save] をクリックします。

グループの編集

現在の SSID グループを編集するには、以下のステップに従います。

ステップ 1 [Configure] > [wIPS Profiles] の順に選択します。
ステップ 2 左側のサイドバー メニューから、[Profile List] を選択します。
ステップ 3 該当する wIPS プロファイル名をクリックします。
ステップ 4 編集する SSID グループのチェックボックスをオンにします。
ステップ 5 [Select a command] ドロップダウン リストから [Edit Group] を選択します。
ステップ 6 [Go] をクリックします。
ステップ 7 SSID 設定ページで、SSID グループ名または SSID リストに必要な変更を行います。
ステップ 8 終了したら、次のいずれかを選択します。

- [Save]：現在の変更内容を保存し、SSID 設定ページを閉じます。
- [Cancel]：変更内容を保存せずに SSID 設定ページを閉じます。

グループの削除

現在の SSID グループを削除するには、以下のステップに従います。

ステップ 1 [Configure] > [wIPS Profiles] の順に選択します。
ステップ 2 左側のサイドバー メニューから、[Profile List] を選択します。
ステップ 3 該当する wIPS プロファイルのプロファイル名をクリックします。
ステップ 4 削除する SSID グループのチェックボックスをオンにします。
ステップ 5 [Select a command] ドロップダウン リストから [Delete Group] を選択します。
ステップ 6 [Go] をクリックします。
ステップ 7 [OK] をクリックして、削除を実行します。

プロファイル エディタを使用したプロファイル設定

ヒント　Cisco Adaptive wIPS 機能の詳細については、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps6305/tsd_products_support_online_learning_modules_list.html.Prime Infrastructure に関するさまざまなトピックについての学習モジュールもあります。今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

プロファイル エディタを使用すると、次のものを含むプロファイルの詳細を設定できます。

- SSID グループ：SSID グループを追加、編集、または削除します。
- ポリシーの包含：プロファイルに含めるポリシーを決定します。
- ポリシー レベル設定：閾値、重大度、通知の種類、ACL または SSID グループなど、各ポリシーの設定を行います。
- MSE またはコントローラ アプリケーション：プロファイルを適用する Mobility Services Engine またはコントローラを選択します。

プロファイルの詳細を設定するには、以下のステップに従います。

ステップ 1　プロファイル エディタにアクセスします。これには、次の 2 つの方法があります。

- 新しいプロファイルを作成するときは、[Profile Parameters] ページで [Save and Edit] をクリックします。
- [Profile List] ページからプロファイル名をクリックします。

ステップ 2　[SSID Groups] ページから、現在のグループの編集および削除、または新しいグループの追加を行うことができます。SSID グループの追加、編集、削除の詳細については、wIPS SSID グループ リストの設定を参照してください。

ステップ 3　SSID グループを必要に応じて追加または編集した後、次のいずれかを選択します。

- [Save]：SSID グループに対して行った変更を保存します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。
- [Next]：[Profile Configuration] ページに進みます。

ステップ 4　[Profile Configuration] ページでは、現在のプロファイルに含めるポリシーを決定できます。ポリシー ツリーのチェックボックス（左側の [Select Policy] ペインにあります）は、現在のプロファイルで有効または無効になっているポリシーを示します。該当するブランチまたはポリシーのチェックボックスをオンにすることで、必要に応じてブランチ全体または個別のポリシーを有効または無効にできます。

（注）　デフォルトでは、すべてのポリシーが選択されています。

（注） 各 wIPS ポリシーの詳細については、wIPS ポリシー アラーム リファレンスを参照してください。

ステップ 5 [Profile Configuration] ページで、個々のポリシーをクリックしてポリシーの説明を表示したり、現在のポリシー ルール設定を表示または変更します。
各ポリシーで次のオプションを使用できます。

- [Add]：このポリシーに新しいルールを作成するには、[Add] をクリックして [Policy Rule Configuration] ページにアクセスします。
- [Edit]：このルールの設定を編集するには、該当するルールのチェックボックスをオンにし、[Edit] をクリックして [Policy Rule Configuration] ページにアクセスします。
- [Delete]：削除するルールのチェックボックスをオンにし、[Delete] をクリックします。[OK] をクリックして、削除を実行します。

  （注） 1 つ以上のポリシー ルールが存在する必要があります。リスト内で唯一のポリシー ルールは削除できません。

- [Move Up]：リスト内で上に移動するルールのチェックボックスをオンにして、[Move Up] をクリックします。
- [Move Down]：リスト内で下に移動するルールのチェックボックスをオンにして、[Move Down] をクリックします。

  ポリシー レベルで次の設定を行うことができます。

- [Threshold]（すべてのポリシーに適用されるわけではありません）：選択したポリシーに関連付けられた閾値または上限を示します。ポリシーの閾値に達すると、アラームが生成されます。

  （注） すべてのポリシーに 1 つ以上のしきい値が含まれている必要があるため、標準的なワイヤレス ネットワークの問題に応じて、各ポリシーにデフォルトのしきい値が定義されています。

  （注） 閾値オプションは、選択したポリシーに応じて異なります。

  （注） Cisco Adaptive wIPS DoS およびセキュリティ ペネトレーション攻撃からのアラームは、セキュリティ アラームとして分類されます。これらの攻撃の概要は [Security Summary] ページにあります。このページにアクセスするには、[Monitor] > [Security] の順に選択します。wIPS の攻撃は [Threats and Attacks] セクションにあります。

- [Severity]：選択したポリシーの重大度を示します。パラメータとしては、[critical]、[major]、[info]、および [warning] があります。このフィールドの値は、ワイヤレス ネットワークに応じて変わります。
- [Notification]：閾値に関連付けられた通知の種類を示します。
- [ACL/SSID Group]：この閾値が適用される ACL または SSID グループを示します。

  （注） 選択されたグループに対してのみポリシーが適用されます。

ステップ 6 プロファイルの設定が完了したら、次のいずれかを選択します。

- [Save]：現在のプロファイルに対して行った変更を保存します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。
- [Back]：[SSID Groups] ページに戻ります。
- [Next]：[MSE/Controller(s)] ページに進みます。

ステップ 7 [Apply Profile] ページで、現在のプロファイルを適用する Mobility Services Engine とコントローラのチェックボックスをオンにします。

ステップ 8 該当する Mobility Services Engine とコントローラが選択されている場合、次のいずれかを選択します。

- [Apply]：現在のプロファイルを、選択された Mobility Services Engine またはコントローラに適用します。
- [Cancel]：変更を行わずにプロファイル リストに戻ります。

（注） 作成したプロファイルは、プロファイル リストから直接適用することもできます。[Profile List] ページから、適用するプロファイルのチェックボックスをオンにし、[Select a command] ドロップダウン リストから [Apply Profile] をクリックします。[Apply Profile] ページにアクセスするには、[Go] をクリックします。

第 7 章

システムとサービスのモニタリング

この章では、アラーム、イベント、およびログの設定と表示による Cisco Mobility Services Engine のモニタ方法、システムの使用率および要素（タグ、クライアント、不正クライアント、干渉、およびアクセス ポイント）のカウントについてのレポートの生成方法について説明します。また、Prime Infrastructure を使用して、クライアント（有線と無線）、タグ、チェックポイント、および Wi-Fi TDOA 受信機をモニタする方法についても説明します。

- アラームの処理，131 ページ
- イベントの使用，138 ページ
- ログの操作，138 ページ
- アクセス ポイントの詳細のモニタリング，141 ページ
- 「Generating Reports」，159 ページ
- デバイス使用率レポートの作成，164 ページ
- MSE でのクライアントのサポート，167 ページ
- Geo-Location のモニタリング，176 ページ
- Ekahau Site Survey の統合，177 ページ
- AirMagnet Survey と AirMagnet Planner の統合，178 ページ
- セキュリティ ダッシュボードの解釈，178 ページ

アラームの処理

この項では、Prime Infrastructure を使用した Mobility Services Engine のアラームの表示、割り当て、およびクリア方法について説明します。また、アラーム通知（All、Critical、Major、Minor、Warning）の定義方法、およびそれらのアラーム通知を電子メール送信する方法についても説明します。

- 注意事項と制約事項，（132 ページ）

- アラームの表示, （132 ページ）
- Cisco Adaptive wIPS アラームの詳細のモニタリング, （134 ページ）
- アラームの割り当てと割り当て解除, （136 ページ）
- アラームの削除とクリア, （137 ページ）
- 電子メール アラーム通知, （137 ページ）

注意事項と制約事項

重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。

アラームの表示

Mobility Services Engine のアラームを表示するには、以下のステップに従います。

ステップ 1 [Monitor] > [Alarms] の順に選択します。

ステップ 2 ナビゲーション バーにある [Advanced Search] リンクをクリックします。アラーム用の設定可能な検索ダイアログボックスが表示されます。

ステップ 3 [Search Category] ドロップダウン リストから [Alarms] を選択します。

ステップ 4 [Severity] ドロップダウン リストから、[Severity of Alarms] を選択します。オプションは、[All Severities]、[Critical]、[Major]、[Minor]、[Warning]、または [Clear] です。

ステップ 5 [Alarm Category] ドロップダウン リストから、[Mobility Service] を選択します。

ステップ 6 [Condition] コンボ ボックスから [Condition] を選択します。または、[Condition] テキスト ボックスに条件を入力できます。

ステップ 7 [Time Period] ドロップダウン リストから、アラームを確認するタイム フレームを選択します。オプションの範囲は、分単位（5、15、および 30）から、時間単位（1 ～ 8）、日数単位（1 ～ 7）までです。すべてを表示するには、[Any time] を選択します。

ステップ 8 [Alarm Summary] ページの認知しているアラームとそれぞれのカウントを除外するには、[Acknowledged State] チェックボックスをオンにします。

ステップ 9 [Alarm Summary] ページの割り当て済みのアラームとそれぞれのカウントを除外するには、[Assigned State] チェックボックスをオンにします。

ステップ 10 [Items per page] ドロップダウン リストから、各ページに表示するアラーム数を選択します。

ステップ 11 後で使用するために検索条件を保存するには、[Save Search] チェックボックスをオンにして、検索の名前を入力します。

（注） その後は、[Saved Search] リンクをクリックすることで、その検索を開始できます。

ステップ 12 [Go] をクリックします。[alarms summary] ダイアログボックスが表示され、検索結果が表示されます。

（注） アラームをソートするには、列見出し（[Severity]、[Failure Source]、[Owner]、[Date/Time]、[Message]、および [Acknowledged]）をクリックします。

ステップ 13 Mobility Services Engine の Context-Aware Service Notification を表示するには、ステップ 2 からステップ 12 までを繰り返します。ステップ 5で、アラーム カテゴリとして「Context Aware Notifications」と入力します。

wIPS アラームの統合

wIPS アラームの統合機能は、リリース 7.5 で導入されました。wIPS アラームの統合は、アクセス ポイントによって報告されるさまざまなワイヤレス侵入のインシデントを集約し、簡潔でわかりやすいアラームを発信します。この機能は、潜在的なセキュリティの問題を迅速に特定するために役立ちます。アラーム統合は、MSE の wIPS サービス モジュールで実行されます。統合ルールが MSE でトリガーされると、MSE は SNMP トラップを送信して Prime Infrastructure に通知します。

次の 3 種類の攻撃統合カテゴリが作成されます。

- ビーコン フラッド：システムは、デバイスから送信される適切な順番でない多くのビーコン フレームを検出します。擬似ビーコン フレームを送信することで、ハッカーは不正なアクセス ポイント設定やサポートされるデータレート、SSID、チャネル情報などの設定をアドバタイズできます。このアラーム統合カテゴリには、次のアラームが含まれています。
  - スプーフされた MAC アドレスの検出
  - DoS: ビーコン フラッド
- De-auth フラッド：これは、DoS 攻撃の一種です。トラフィック パターンが、スプーフされた De-auth フレームを使用してアクセス ポイントとそのクライアント ステーション間のアソシエーションを断ち切る DoS 攻撃と一致します。

  このアラーム統合カテゴリには、次のアラームが含まれています。
  - スプーフされた MAC アドレス
  - DoS：De-Auth フラッド
- MDK3-Destruction 攻撃：これは、AP とアソシエートしている、またはアソシエートしようとするすべてのクライアントにアソシエーションの障害を引き起こします。この統合カテゴリには、次のアラームが含まれています。
  - DoS：De-Auth ブロードキャスト フラッド
  - DoS：Dis-Assoc ブロードキャスト フラッド
  - DoS：認証されないアソシエーション
  - DOS: MDK3-Destruction 攻撃

Cisco Adaptive wIPS アラームの詳細のモニタリング

MSE アラームの詳細を表示するには、以下のステップに従います。

選択した Cisco wIPS アラームの詳細を表示するには、[Monitor] > [Alarms] > [failure object] の順に選択します。Cisco Adaptive wIPS アラームについて、次のアラームの詳細が表示されます。

- [General Properties]：全般情報は、アラームのタイプによって異なる場合があります。たとえば、アラーム詳細の中に、ロケーションおよびスイッチ ポート トレーシング情報を含む場合もあります。次の表に、MSE アラームと wIPS トラップ条件に関連付けられた一般パラメータの説明を示します。
  - [Detected By wIPS AP]：アラームを検出したアクセス ポイント。
  - [wIPS AP IP Address]：wIPS アクセス ポイントの IP アドレス。
  - [Owner]：このアラームに割り当てられている個人の名前またはブランク。
  - [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。
  - [Category]：wIPS の場合、アラーム カテゴリは [Security] です。
  - [Created]：アラームが作成された日時（月、日、年、時、分、秒、AM/PM）。
  - [Modified]：アラームが最後に変更された日時（月、日、年、時、分、秒、AM/PM）。
  - [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。

    [NMS (Network Management System - Prime Infrastructure)]：ポーリングによって生成されます。Prime Infrastructure は、Cisco WLC を定期的にポーリングして、イベントを生成します。Prime Infrastructure がイベントを生成するのは、トラップを無効にしたときか、これらのイベントのトラップが失われたときです。この場合、「Generated by」は NMS です。

    [Trap]：コントローラによって生成されます。Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。この場合、「Generated by」は controller です。
  - [Severity]：重大度（Critical、Major、Minor、Warning、Clear）。
  - [Last Disappeared]：潜在的な攻撃が最後になくなった日時。
  - [Channel]：潜在的な攻撃が発生したチャネル。
  - [Attacker Client/AP MAC]：攻撃を開始したクライアントまたはアクセス ポイントの MAC アドレス。
  - [Attacker Client/AP IP Address]：攻撃を開始したクライアントまたはアクセス ポイントの IP アドレス。

- [Target Client/AP IP Address]：攻撃者により攻撃対象となったクライアントまたはアクセス ポイントの IP アドレス。
- [Controller IP Address]：アクセス ポイントがアソシエートされているコントローラの IP アドレス。
- [MSE]：関連付けられている Mobility Services Engine の IP アドレス。
- [Controller MAC Address]：アクセス ポイントがアソシエートされているコントローラの MAC アドレス。
- wIPS access point MAC address
- Forensic File
- [Event History]：[Monitoring Alarms] ページに移動し、このアラームのすべてのイベントを表示します。

- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。注釈は [Annotations] 表示領域に表示されます。
- [Messages]：アラーム名を表示します。
- [Description]：アラームに関する総合情報を表示します。
- [Mitigation Status]：どの緩和手段が攻撃に対して行われたかを表示します。
- [Audit Report]：クリックして、設定監査アラームの詳細を表示します。このレポートは、設定監査アラームにだけ使用できます。

  監査の矛盾が設定グループに施行されると、設定監査アラームが生成されます。

（注） 施行が失敗すると、設定グループに重大なアラームが生成されます。施行が成功すると、設定グループに比較的重大でないアラームが生成されます。アラームには監査レポートへのリンクがあり、各コントローラの矛盾のリストを表示できます。

- [Event History]：[MSE Alarm Events] ページを開き、このアラームのイベントを表示します。アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。
- [Rogue Clients]：障害が発生したオブジェクトが不正なアクセス ポイントの場合、不正なクライアントに関する情報が表示されます。
- [Map Location]：アラームのマップ位置を表示します。
  - [Floor]：この攻撃が検出された場所。
  - [Last Located At]：前回攻撃が発生した場所。
  - [On MSE]：この攻撃が特定されたモビリティ サーバ エンジン。

- [Location History]：現在の攻撃者および攻撃対象の場所の詳細を表示するには、[Location History] をクリックします。

（注） wIPS で報告されるすべてのアラームのうち、次の 4 つのアラームは、アクセス ポイントではなく、Mobility Services Engine（MSE）で検出されます。これらのアラームについて、場所の情報は現在ありません。アラームのリストは次のとおりです。

- 124 Hotspotter ツールの検出
- 133 デバイスのセキュリティ異常による Day-Zero 攻撃
- 135 WLAN のセキュリティ異常による Day-Zero 攻撃
- 138 ベンダー リストによる未承認アソシエーション

- [Related Alarm List]：特定の攻撃に関連するすべてのアラームを示します。これは、アラームを統合するときにどの統合のルールを使用したかを示します。
  - [Alarm Name]：アラームの名前。
  - [First Heard]：攻撃が最初に検出された日時を示します。
  - [Last Heard]：攻撃が最後に検出された日時を示します。
  - [Status]：攻撃のステータス。

アラームの割り当てと割り当て解除

アラームの割り当ておよび割り当て解除を行うには、以下のステップに従います。

ステップ 1 [Monitor] > [Alarms] の順に選択して、[Alarms] ページを開きます。

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

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

ステップ 3 [Assign] > [Assign to Me]（または [Unassign]）の順に選択します。

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

アラームの削除とクリア

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

Mobility Services Engine からアラームを削除またはクリアするには、以下のステップに従います。

ステップ 1 [Monitor] > [Alarms] の順に選択して、[Alarms] ページを開きます。

ステップ 2 対応するチェックボックスをオンにして、削除またはクリアするアラームを選択します。

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

電子メール アラーム通知

Prime Infrastructure では、特定の電子メール アドレスにアラーム通知を送信できます。電子メール経由で通知を送信することで、必要な場合に迅速なアクションをとることができます。

自分に電子メールで送信されるアラーム重大度のタイプ（Critical、Major、Minor、およびWarning）を選択できます。

メールにアラーム通知を送信するには、以下のステップに従います。

ステップ 1 [Monitor] > [Alarms] の順に選択します。

ステップ 2 対応するチェック ボックスをオンにして、アラームを選択します。 [Select a command] ドロップダウン リストから [Email Notification] をクリックします。[Email Notification] ページが表示されます。

（注） SMTP メール サーバは、電子メール通知の対象となる電子メール アドレスを入力する前に定義しておく必要があります。[Administrator] > [Settings] > [Mail Server Configuration] の順に選択して、適切な情報を入力します。

ステップ 3 [Mobility Service] の隣にある [Enabled] チェックボックスをオンにします。

（注） [Mobility Service] アラーム カテゴリを有効にすると、Mobility Services Engine とロケーション アプライアンスに関連するすべてのアラームが定義済みの電子メール アドレスに送信されます。

ステップ 4 [Mobility Service] リンクをクリックします。Mobility Services Engine に報告されるアラーム重大度のタイプを設定するページが表示されます。

ステップ 5 電子メール通知を送信するすべてのアラーム重大度のタイプの隣にあるチェックボックスをオンにします。

ステップ 6 [To] テキスト ボックスに、電子メール通知を送信する 1 つまたは複数の電子メール アドレスを入力します。電子メール アドレスはカンマで区切ります。

ステップ 7 [OK] >[Save] をクリックします。

[Alarms > Notification] ページに戻ります。報告されたアラーム重大度のレベルに対する変更と電子メール通知の受信者の電子メール アドレスが表示されます。

イベントの使用

Prime Infrastructure を使用して、Mobility Services Engine とロケーション通知イベントを表示できます。イベントは、それぞれの重大度（Critical、Major、Minor、Warning、Clear、Info）およびそれらのカテゴリに基づき検索して表示できます。

ここでは、ロケーション通知イベントの表示の手順について説明します。

ロケーション通知イベントの表示

ロケーション通知イベントを表示するには、以下のステップに従います。

ステップ 1 [Monitor] > [Events] の順に選択します。

ステップ 2 [Events] ページでは、次の操作を実行できます。

- 特定の要素のイベントを表示する場合に、その IP アドレス、名前、WLAN SSID、または MAC アドレスがわかっている場合は、ナビゲーション バーの [Search] テキスト ボックスにその値を入力します。[Search] をクリックします。
- 重大度やカテゴリでイベントを表示するには、ナビゲーション バーで [Advanced Search] をクリックして、[Severity] および [Event Category] ドロップダウン リスト ボックスから適切なオプションを選択します。[Go] をクリックします。

ステップ 3 Prime Infrastructure は検索条件に一致するイベントを見つけると、それらのイベントを一覧表示します。

（注） イベントの詳細を表示するには、イベントに関連付けられている [Failure Source] をクリックします。また、イベントの概要を各列見出しで並べ替えることができます。

ログの操作

この項では、ロギング オプションの設定方法と、ログ ファイルのダウンロード方法について説明します。

- 注意事項と制約事項, （139 ページ）
- ロギング オプションの設定, （139 ページ）
- MAC アドレスに基づくロギング, （140 ページ）

• ログ ファイルのダウンロード, （140 ページ）

注意事項と制約事項

- ログ レベルから適切なオプションを選択する際には、Cisco TAC 担当者から [Error] と [Trace] のみ使用するように指示があった場合は、指示に従ってください。
- 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

ロギング オプションの設定

Prime Infrastructure を使用して、ログに記録するメッセージのタイプとログ レベルを指定できます。

ロギング オプションを設定するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services]> [Mobility Services Engines] の順に選択します。

ステップ 2 設定する MSE の名前をクリックします。

ステップ 3 [System] メニューから [Logs] を選択します。選択されている MSE のロギング オプションが表示されます。

ステップ 4 [Logging Level] ドロップダウン リストから適切なオプションを選択します。
ロギング オプションは、[Off]、[Error]、[Information]、および [Trace] の 4 つです。

ログ レベルが [Error] またはこれよりも上のレベルに設定されているログ レコードはすべて、新しいエラー ログ ファイル locserver-error-%u-%g.log に記録されます。これは、ロケーション サーバの locserver-%u-%g.log ログ ファイルとともに維持される追加のログ ファイルです。このエラー ログ ファイルには、[Error] レベルのログとそのコンテキスト情報が記録されます。コンテキスト情報には、当該エラーよりも前の 25 ログ レコードが含まれています。最大 10 のエラー ログ ファイルを維持できます。各ログ ファイルの最大許容サイズは 10 MB です。

注意 Cisco Technical Assistance Center（TAC）担当者から [Error] と [Trace] のみ使用するように指示があった場合は、その指示に従います。

ステップ 5 イベントのロギングを開始する各要素の隣にある [Enabled] チェックボックスをオンにします。

ステップ 6 [Advanced Parameters] の [Enable] チェックボックスをオンにして、詳細デバッグを有効にします。デフォルトでは、このオプションは無効になっています。

注意 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

ステップ 7 サーバからログ ファイルをダウンロードするには、[Download Logs] をクリックします。詳細については、ログ ファイルのダウンロードを参照してください。

ステップ 8 [Log File] グループ ボックスに、以下の情報を入力します。

- MSE で維持するログ ファイルの数。MSE で維持できるログ ファイルの数は 5 ～ 20 です。

- 最大ログ ファイル サイズ（MB 単位）。ログ ファイルのサイズは 10 ～ 50 MB です。

ステップ 9 [MAC Address Based Logging] ページで、次の手順を実行します。

- [Enable] チェックボックスをオンにし、MAC アドレス ロギングを有効にします。デフォルトでは、このオプションは無効になっています。
- ロギングを有効にする 1 つ以上の MAC アドレスを追加します。また、以前に追加した MAC アドレスを削除できます。削除するには、リストから MAC アドレスを選択して [Remove] をクリックします。

  MAC アドレス ベースのロギングの詳細についてはMAC アドレスに基づくロギングを参照してください。

ステップ 10 [Save] をクリックして変更を適用します。

MAC アドレスに基づくロギング

この機能では、指定されている MAC アドレスのエンティティ固有のログ ファイルを作成できます。ログ ファイルは次に示すパスの locserver ディレクトリ内に作成されます。

```
/opt/mse/logs/locserver
```

一度に最大で 5 つの MAC アドレスをログに記録できます。MAC アドレス aa:bb:cc:dd:ee:ff のログ ファイルの形式は次のとおりです。

macaddress-debug-aa-bb-cc-dd-ee-ff.log

1 つの MAC アドレスに対して最大 2 つのログ ファイルを作成できます。2 つのログ ファイルは、1 つのメインと 1 つのバックアップまたはロールオーバー ログ ファイルで構成できます。

MAC ログ ファイルの最小サイズは 10 MB です。最大許容サイズは、MAC アドレスあたり 20 MB です。24 時間以上更新されていない MAC ログ ファイルはプルーニングされます。

ログ ファイルのダウンロード

Mobility Services Engine ログ ファイルを解析する必要がある場合は、Prime Infrastructure を使用してログ ファイルをシステムにダウンロードできます。Prime Infrastructure ではログ ファイルを含む .zip ファイルがダウンロードされます。

ログ ファイルが含まれている .zip ファイルをダウンロードするには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 ステータスを表示する Mobility Services Engine の名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、[Logs] を選択します。

ステップ 4 [Download Logs] をクリックします。

ステップ 5 [File Download] ダイアログボックスの指示に従い、ファイルを表示するか、または .zip ファイルをシステムに保存します。

アクセス ポイントの詳細のモニタリング

[Access Points Details] ページでは、1 つのアクセス ポイントのアクセス ポイント情報を参照できます。

このページにアクセスするには、[Monitor] > [Access Points] の順に選択し、[AP Name] 欄で項目をクリックします。アクセス ポイントの種類に応じて、次のタブが表示されます。この項では、各 [Access Points Details] ページのタブについて詳しく説明します。内容は次のとおりです。

- [General] タブ
- [Interfaces] タブ
- [CDP Neighbors] タブ
- [Current Associated Clients] タブ
- [SSID] タブ
- [Clients Over Time] タブ

[General] タブ

（注） [General] タブのフィールドは、Lightweight アクセス ポイントと Autonomous アクセス ポイントで異なります。

ここでは、次の内容について説明します。

- [General]：Lightweight アクセス ポイント
- [General]：Autonomous

[General]：Lightweight アクセス ポイント

表 5-47 は、[General]（Lightweight アクセス ポイント用）タブのフィールドを示しています。

表 *17*：*[General (for Lightweight Access Points)]* タブのフィールド

フィールド	説明
General	
AP Name	オペレータが定義したアクセス ポイント名。
AP IP address、Ethernet MAC address、および Base Radio MAC address	IP アドレス、イーサネット MAC アドレス、および無線 MAC アドレス。
Country Code	サポートされる国コード。1 台のコントローラで最大 20 の国をサポートできます。 （注） 運用する国向けに設計されていない場合、アクセス ポイントは正しく動作しない可能性があります。製品ごとにサポートされる国コードの完全なリストについては、次の URL を参照してください。 http://www.cisco.com/en/US/docs/wireless/wcs/4.0/configuration/guide/wcscod.html.

フィールド	説明
Link Latency Settings	コントローラでリンク遅延を設定して、アクセスポイントおよびコントローラの間のリンクを計測できます。詳細については、アクセスポイントのリンク遅延の設定を参照してください。 • [Current Link Latency (in msec)]：アクセスポイントからコントローラ、およびコントローラからアクセス ポイントの間のハートビートパケットの現在のラウンドトリップ時間（ミリ秒）。 • [Minimum Link Latency (in msec)]：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間のハートビート パケットの最短ラウンドトリップ時間（ミリ秒）。 • [Maximum Link Latency (in msec)]：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間のハートビート パケットの最長ラウンドトリップ時間（ミリ秒）。
LWAPP/CAPWAP Uptime	LWAPP/CAPWAP 接続がアクティブになっていた時間が表示されます。
LWAPP/CAPWAP Join Taken Time	LWAPP/CAPWAP 接続が参加していた時間が表示されます。
Admin Status	アクセスポイントの管理状態が、有効または無効で表示されます。
AP モード	

フィールド	説明
ローカル	デフォルトモード。設定したチャネルをスキャンしてノイズと不正を探す間、データクライアントにサービスが提供されます。アクセスポイントは 50 ミリ秒間、チャネルの不正をリッスンします。Auto RF 設定の下で指定された期間の間、各チャネルを巡回します。 （注） Local または FlexConnect アクセス ポイントで Cisco Adaptive wIPS 機能を設定するには、[Local] または [FlexConnect] を選択し、[Enhanced wIPS Engine Enabled] チェックボックスをオンにします。
Monitor	無線受信専用モード。アクセスポイントは、設定されたすべてのチャネルを12秒ごとにスキャンします。このように設定されたアクセスポイントでは、認証解除のパケットだけが無線で送信されます。モニタ モード アクセス ポイントは、不正アクセスポイントにクライアントとして接続できます。 （注） アクセス ポイントで Cisco Adaptive wIPS 機能を設定するには、[Monitor] を選択します。[Enhanced wIPS Engine Enabled] チェックボックスをオンにして、[Monitor Mode Optimization] ドロップダウン リストから [wIPS] を選択します。アクセスポイントでwIPSモードを有効にする前に、アクセス ポイントの無線を無効にする必要があります。アクセス ポイントの無線を無効にしないと、エラー メッセージが表示されます。 （注） アクセスポイントでwIPSを有効にした後、無線を再度有効にします。

フィールド	説明
Rogue Detector	アクセスポイントの無線がオフに切り替わり、アクセス ポイントは有線トラフィックだけをリッスンします。このモードで動作するコントローラは、不正アクセスポイントをモニタします。コントローラはすべての不正アクセスポイントとクライアントの MAC アドレスのリストを不正検出器に送信して、不正検出器がこの情報を WLC に転送します。MAC アドレスの一覧が、WLC アクセス ポイントがネットワーク上で取得した内容と比較されます。MAC アドレスが一致する場合は、どの不正アクセスポイントが有線ネットワークに接続されるかを判別できます。
スニファ	アクセスポイントは特定チャネル上のすべてのパケットを取得して、AiroPeek を実行するリモートマシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケットサイズなどの情報が含まれます。この機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである AiroPeek を実行する場合のみ有効にできます。
FlexConnect	最大 6 個のアクセス ポイントに対して FlexConnect を有効にします。FlexConnect アクセスポイントは、コントローラへの接続を失ったとき、クライアント データ トラフィックをローカルにスイッチングし、クライアント認証をローカルで実行できます。 （注） OfficeExtend アクセス ポイントを設定するには、[FlexConnect] を選択する必要があります。AP モードが FlexConnect の場合、FlexConnect の設定オプションが表示されます。これには、OfficeExtend AP を有効にするオプションと、Least Latency Controller Join を有効にするオプションが含まれます。

フィールド	説明
Bridge	これは、Autonomous アクセス ポイントが無線クライアントのように機能して、Lightweight アクセスポイントに接続する特殊なモードです。AP モードが [Bridge] に設定され、アクセス ポイントがブリッジ対応である場合、ブリッジとその有線クライアントは、Prime Infrastructure にクライアントとしてリストされます。
Spectrum Expert	このモードでは、CleanAir 対応のアクセス ポイントを、すべてのモニタ対象チャネル上の干渉源検出のために広範囲に使用できます。IDS スキャンや Wi-Fi などのその他の機能はすべて一時停止されます。
Enhanced wIPS Engine	[Enabled] または [Disabled] のいずれかが設定され、Cisco Adaptive wIPS 機能を使用したセキュリティ攻撃のモニタが可能となります。
Operational Status	[Registered] または [Not Registered] のいずれかとなり、コントローラで決定されます。
Registered Controller	アクセスポイントが登録されているコントローラ。登録済みのコントローラの詳細を表示します。詳細については、「Monitoring System Summary」（5-4 ページ）を参照してください。
Primary Controller	このアクセスポイントのプライマリ コントローラの名前。
Port Number	アクセス ポイントのプライマリ コントローラの SNMP 名。アクセス ポイントは、すべてのネットワーク操作について、ハードウェア リセットが発生した場合、このコントローラに最初にアソシエートしようとします。
AP Uptime	アクセスポイントがアクティブで送受信できる状態になっている時間を表示します。
Map Location	アクセスポイントのカスタマー定義の場所名。クリックするとマップ上で実際の場所が表示されます。詳細は、[Monitor] > [Access Points] > [*name*] > [Map Location] の順に選択してください。

フィールド	説明
Google Earth Location	Google Earth の場所が割り当てられているかどうかを示します。
場所	アクセスポイントが配置されている物理的な場所（または Unassigned）。
Statistics Timer	このカウンタは、アクセス ポイントがその DOT11 統計情報をコントローラに送信する時間を秒単位で設定します。
PoE Status	アクセス ポイントの Power over Ethernet ステータス。可能な値は次のとおりです。 • [Low]：イーサネットから供給されるアクセス ポイントの電力が低い。 • [Lower than 15.4 volts]：イーサネットから供給されるアクセスポイントの電力が 15.4 V 未満。 • [Lower than 16.8 volts]：イーサネットから供給されるアクセスポイントの電力が 16.8 V 未満。 • [Normal]：アクセス ポイントの操作に十分な電力が供給されている。 • [Not Applicable]：電源がイーサネットではない。
Rogue Detection	不正検出が有効になっているかどうかを示します。 （注） 家庭環境に導入されるアクセス ポイントは、多数の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出は自動的に無効にされます。OfficeExtend アクセス ポイントの詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。
OfficeExtend AP	アクセス ポイントが OfficeExtend アクセス ポイントとして有効になっているかどうかを示します。デフォルトは [Enabled] です。

フィールド	説明
暗号化	暗号化が有効になっているかどうかを示します。 （注） 暗号化機能を有効または無効にすると、アクセス ポイントがリブートし、クライアントの接続が失われます。 （注） DTLS データ暗号化は、セキュリティを維持するため、OfficeExtend アクセス ポイントで自動的に有効になります。暗号化は、Plus ライセンスが設定された 5500 シリーズ コントローラにアクセス ポイントが接続されている場合のみ使用できます。
Least Latency Join	アクセスポイントは、プライオリティ順序検索（プライマリ、セカンダリ、ターシャリ コントローラ）から、遅延測定値が最善（最短遅延）のコントローラの検索に切り替えます。遅延が最短のコントローラが、最善のパフォーマンスを提供します。
Telnet Access	Telnet アクセスが有効になっているかどうかを示します。
SSH Access	SSH が有効になっているかどうかを示します。 （注） OfficeExtend アクセス ポイントは、デフォルトのパスワードがアクセス ポイントで使用されている場合に外部アクセスを許可する可能性がある WAN に直接接続されていることがあります。このため、Telnet と SSH アクセスは、OfficeExtend アクセス ポイントでは自動的に無効になります。
Versions	
Software Version	現在コントローラで実行されているコードのオペレーティング システムの release.version.dot.maintenance 番号。
Boot Version	オペレーティング システムのブートローダのバージョン番号。
Inventory Information	

フィールド	説明
AP タイプ	アクセス ポイントの種類
AP Model	アクセス ポイントのモデル番号。
Cisco IOS Version	Cisco IOS Release の詳細。
AP Certificate Type	Self Signed または Manufacture Installed のいずれか。
FlexConnect Mode Supported	FlexConnect モードがサポートされているかどうかを示します。
wIPS Profile（該当する場合）	
Profile Name	ユーザ定義プロファイル名をクリックすると、wIPS プロファイルの詳細が表示されます。
Profile Version	
Unique Device Identifier (UDI)	
名前	アクセス ポイントの Cisco AP の名前。
説明	アクセス ポイントの説明。
Product ID	注文可能な製品 ID
Version ID	製品 ID のバージョン
Serial Number	一意の製品シリアル番号
[Run Ping Test Link]：クリックしてアクセス ポイントに ping します。結果はポップアップ ダイアログボックスに表示されます。次に、関連付けられたパラメータを示します。 • コントローラ IP アドレス • Destination • Send Count • Received Count • Maximum Time Interval • Minimum Time Interval • Average Time Interval	

フィールド	説明
[Alarms Link]：クリックすると、このアクセス ポイントに関連付けられたアラームが表示されます。 • Severity • メッセージ • [Failure Source]：アラーム検出デバイス • Timestamp • 所有者 • カテゴリ • Condition	
[Events Link]：クリックすると、このアクセス ポイントに関連付けられたイベントが表示されます。 • 説明 • [Failure Source]：アラーム検出デバイス • Timestamp • Severity • カテゴリ • Condition • Correlated	

[General]：Autonomous

（注） 自律クライアントについては、Prime Infrastructure はクライアント数のみを収集します。[Monitor] ページとレポートのクライアント数には、自律クライアントが含まれています。クライアント検索、クライアント トラフィック グラフ、その他のクライアント レポート（Unique Clients、Busiest Clients、Client Association など）には、Autonomous アクセス ポイントからのクライアントは含まれていません。

表 5-48 は、[General]（自律アクセス ポイント用）タブのフィールドを示しています。

表 *18* : *[General (for Autonomous Access Points)]* タブのフィールド

フィールド	説明
AP Name	オペレータが定義したアクセス ポイント名。
AP IP address and Ethernet MAC address	アクセス ポイントの IP アドレス、イーサネット MAC アドレス。
AP UpTime	アクセスポイントが送受信できる状態になっている時間（日、時間、分、秒）を示します。
Map Location	アクセスポイントのカスタマー定義の場所名。クリックするとマップ上で実際の場所が表示されます。
WGB Mode	アクセス ポイントがワーク グループ ブリッジ モードかどうかを示します。
SNMP Info	
SysObjectId SysDescription SysLocation SysContact	システム オブジェクト ID。 システムデバイスの種類とファームウェアの現在のバージョン。 デバイスが設置されている建物の名前や部屋など、デバイスの物理的な場所。 デバイスを担当するシステム管理者の名前。
Versions	
Software Version	現在コントローラで実行されているコードのオペレーティング システムの release.version.dot.maintenance 番号。
CPU Utilization	指定した期間の最大、平均、および最小 CPU 使用率が表示されます。
Memory Utilization	指定した期間の最大、平均、および最小メモリ使用率が表示されます。
Inventory Information	
AP タイプ	autonomous または lightweight。
AP Model	アクセス ポイントのモデル番号。

フィールド	説明
AP Serial Number	このアクセスポイントの一意のシリアル番号。
FlexConnect Mode Supported	FlexConnectモードがサポートされているかどうか。
Unique Device Identifier (UDI)	
名前	アクセス ポイントの Cisco AP の名前。
説明	アクセス ポイントの説明。
Product ID	注文可能な製品 ID
Version ID	製品 ID のバージョン
Serial Number	一意の製品シリアル番号

（注） メモリと CPU 使用率のグラフが表示されます。

（注） [Alarms]クリックすると、このアクセス ポイントに関連付けられたアラームが表示されます。[Events] クリックすると、このアクセス ポイントに関連付けられたイベントが表示されます。

[Interfaces] タブ

表 5-49 は、[Interfaces] タブのフィールドを示しています。

表 *19*：*[Interfaces]* タブのフィールド

フィールド	説明
インターフェイス	
Admin Status	イーサネットインターフェイスが有効になっているかどうかを示します。
Operational Status	イーサネットインターフェイスが動作可能かどうかを示します。
Rx Unicast Packets	受信したユニキャスト パケットの数を示します。

フィールド	説明
Tx Unicast Packets	送信したユニキャスト パケットの数を示します。
Rx Non-Unicast Packets	受信した非ユニキャスト パケットの数を示します。
Tx Non-Unicast Packets	送信した非ユニキャスト パケットの数を示します。
Radio Interface	
Protocol	802.11a/n または 802.11b/g/n。
Admin Status	アクセス ポイントが有効か無効かを示します。
CleanAir Capable	アクセス ポイントが CleanAir を使用できるかどうかを示します。
CleanAir Status	CleanAir のステータスを示します。
Channel Number	Cisco 無線がブロードキャストしているチャネルを示します。
Extension Channel	Cisco 無線がブロードキャストしているセカンダリ チャネルを示します。
Power Level	アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。
Channel Width	この無線インターフェイスのチャネル帯域幅を示します。チャネル帯域幅の設定の詳細については、802.11a/n RRM 動的チャネル割り当ての設定を参照してください。 最小（デフォルト）設定は 20 MHz です。最大設定は、この無線でサポートされている最大チャネル幅です。
アンテナの名前	アンテナの種類を示します。

プロパティを表示するインターフェイスの名前をクリックします（表 5-50 を参照）。

表 *20*：インターフェイスのプロパティ

フィールド	説明
AP Name	アクセス ポイントの名前。
Link speed	インターフェイスの速度を Mbps 単位で示します。

フィールド	説明
RX Bytes	インターフェイス上で受信したエラーのないパケットの総バイト数を示します。
RX Unicast Packets	インターフェイス上で受信したユニキャスト パケットの総数を示します。
RX Non-Unicast Packets	インターフェイス上で受信した非ユニキャストまたはマルチキャスト パケットの総数を示します。
Input CRC	インターフェイス上で受信したパケット内の CRC エラーの総数を示します。
Input Errors	インターフェイスでの受信中に発生した、パケットのすべてのエラーの合計を示します。
Input Overrun	入力レートがレシーバのデータ処理能力を超えたために、レシーバ ハードウェアが受信データをハードウェア バッファに送信できなかった回数を示します。
Input Resource	インターフェイス上で受信したパケット内のリソース エラーの総数を示します。
Runts	メディアの最小パケット サイズよりも小さいために廃棄されたパケット数を示します。
Throttle	インターフェイスが、送信中のパケットが多すぎるため、配信速度を落とすように、送信 NIC にアドバイスを送信した合計回数を示します。
Output Collision	イーサネット コリジョンにより再送信したパケットの総数を示します。
Output Resource	インターフェイス上で送信したパケットのリソース エラーの総数を示します。
Output Errors	最終的にインターフェイスからのパケットの送信ができなかった原因となるエラーの合計数を示します。
Operational Status	AP 上の物理イーサネット インターフェイスの動作状態を示します。
Duplex	インターフェイスのデュプレックス モードを示します。

フィールド	説明
TX Bytes	インターフェイス上で送信したエラーのないパケットの総バイト数を示します。
TX Unicast Packets	インターフェイス上で送信したユニキャスト パケットの総数を示します。
TX Non-Unicast Packets	インターフェイス上で送信した非ユニキャストまたはマルチキャスト パケットの総数を示します。
Input Aborts	インターフェイス上で受信中に中断されたパケットの総数を示します。
Input Frames	インターフェイス上で受信した、CRC エラーがあり、オクテット数が整数でないパケットの総数を示します。
Input Drops	インターフェイス上での受信中に、キューが一杯だったためにドロップされたパケットの総数を示します。
Unknown Protocol	不明なプロトコルが原因でインターフェイス上で廃棄されたパケットの総数を示します。
Giants	メディアの最大パケットサイズを超過したために廃棄されたパケット数を示します。
Interface Resets	インターフェイスが完全にリセットされた回数を示します。
Output No Buffer	バッファ領域がなかったために廃棄されたパケットの総数を示します。
Output Underrun	ルータの処理能力を超えた速度でトランスミッタが動作した回数を示します。
Output Total Drops	インターフェイスからの送信中に、キューが一杯だったためにドロップされたパケットの総数を示します。

[CDP Neighbors] タブ

表 5-51 は[CDP Neighbors] タブのフィールドを示します。

（注） このタブは、CDP が有効になっている場合のみ表示されます。

表 *21*：*[CDP Neighbors]* タブのフィールド

フィールド	説明
AP Name	アクセス ポイントに割り当てられた名前。
AP IP アドレス	アクセス ポイントの IP アドレス。
Port No	アクセス ポイントに接続されているか割り当てられているポート番号。
Local Interface	ローカル インターフェイスを示します。
Neighbor Name	隣接するシスコ デバイスの名前。
Neighbor Address	隣接するシスコ デバイスのネットワーク アドレス。
Neighbor Port	隣接するシスコ デバイスのポート。
Duplex	全二重なのか半二重なのかを示します。
Interface Speed	インターフェイスが動作している速度。

[Current Associated Clients] タブ

表 5-52 は、[Current Associated Clients] タブのフィールド示しています。

（注） このタブは、AP（CAPWAP または Autonomous AP）に関連付けられているクライアントがある場合にのみ表示されます。

表 *22*：*[Current Associated Clients]* タブのフィールド

フィールド	説明
[Username]	ユーザ名をクリックすると、このクライアントの [Monitor Client Details] ページが表示されます。詳細については、クライアントとユーザのモニタリングを参照してください。
IP Address	関連付けられているクライアントの IP アドレス。

フィールド	説明
Client MAC Address	クライアントの MAC アドレスをクリックすると、このクライアントの [Monitor Client Details] ページが表示されます。
アソシエーション時間	アソシエーションの日時。
UpTime	アソシエーションの継続時間。
SSID	ユーザ定義の SSID 名。
SNR (dB)	関連付けられているクライアントの、信号対雑音比（dB 単位）。
RSSI	受信信号強度インジケータ（dBm）。
Bytes Tx	イーサネットインターフェイスをいずれかの方向に通過したデータの合計量を示します。
Bytes Rx	イーサネットインターフェイスでいずれかの方向で受信したデータの合計量を示します
アクセス ポイントがコントローラに関連付けられていない場合、コントローラ自身ではなく、データベースを使用してデータが取得されます。アクセス ポイントが関連付けられていない場合、次のフィールドが表示されます。	
ユーザ名	クライアントのユーザ名。
IP Address	ローカル IP アドレス。
Client MAC Address	Client MAC Address
アソシエーション時間	クライアントアソシエーションのタイムスタンプ。
Session Length	セッションの時間の長さ。
SSID	ユーザ定義の SSID 名。
Protocol	
Avg.Session Throughput	
Traffic (MB) as before	

（注） [Current Associated Clients] テーブルの列を追加、削除、順序変更するには、[Edit View] リンクをクリックします。[Edit View] を使用した新規フィールド追加の詳細については、「アクセス ポイント リストの表示の設定」（5-47 ページ）を参照してください。

[SSID] タブ

表 5-53 は、[SSID] タブのフィールドを示しています。

（注） このタブは、アクセス ポイントが Autonomous AP であり、AP で SSID が設定されている場合のみ表示されます。

表 *23*：*[SSID]* タブ

フィールド	説明
SSID	アクセスポイントの無線によってブロードキャストされているサービス セット ID。
SSID Vlan	アクセス ポイント上の SSID は、特定の VLAN ID または名前を認識するために設定されます。
SSID Vlan Name	アクセス ポイント上の SSID は、特定の VLAN ID または名前を認識するために設定されます。
MB SSID Broadcast	SSID ブロードキャストを無効にすると、ワイヤレス クライアントがすでに SSID を知っているか、AP の関連付けられたクライアントからのトラフィックをモニタまたは「スニフィング」しない限り、アクセスポイントが基本的に認識不能になります。
MB SSID Time Period	この指定された期間中に SSID 内の内部通信が動作し続けます。

[Clients Over Time] タブ

このタブには、次のグラフが表示されます。

- [Client Count on AP]：アクセス ポイントに現在関連付けられているクライアントの総数が、時間とともに表示されます。

- [Client Traffic on AP]：AP に接続されているクライアントによって生成されたトラフィックが、時間とともに表示されます。

（注） 上記のグラフに表示される情報は、時間ベースのグラフに表示されます。時間ベースのグラフでは、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。詳細については、「時間ベースのグラフ」（6-71 ページ）を参照してください。

「Generating Reports」

Prime Infrastructure では、さまざまな種類のレポートを生成できます。この項では、Prime Infrastructure Report Launch Pad を使用して、Context Aware レポートを生成する方法について説明します。デフォルトでは、レポートは Prime Infrastructure サーバに保存されます。

レポート基準を定義したら、今後の診断で使用するためにレポートを保存し、臨時的に、またはスケジュール ベースでレポートを実行できます。

レポートの次の基準を定義できます。

- モニタする Mobility Services Engine またはエンジン
- レポートの生成頻度
- グラフ上でのデータの表示方法
- レポートを電子メールで送信するか、ファイルにエクスポートするか

レポート ラウンチ パッド

レポート ラウンチ パッドでは、1 つのページからすべての Prime Infrastructure レポートにアクセスできます。このページでは、現在のレポートを表示し、特定のタイプのレポートを開き、新しいレポートを作成して保存し、スケジュール設定された実行を管理できます。レポート ラウンチ パッドの [ContextAware reports] セクションにアクセスすると、ContextAware レポートを生成できます。

ヒント レポート タイプの横のツール チップ上にマウス カーソルを合わせると、レポートの詳細が表示されます。

- 新規レポートの作成と実行, （160 ページ）
- 現在のレポートの管理, （163 ページ）
- スケジュールされた実行結果の管理, （163 ページ）

• 保存したレポートの管理, （164 ページ）

新規レポートの作成と実行

レポートを新規作成して実行するには、以下のステップに従います。

ステップ 1 [Reports] > [Report Launch Pad] の順に選択します。
レポートは、ページのメインセクションおよび左側のサイドバーのメニューに、カテゴリ別にリストされます。

ステップ 2 レポート ラウンチ パッドのメイン セクションで該当するレポートを見つけてください。
（注） レポート ラウンチ パッドでレポート名をクリックするか、[Report Launch Pad] ページの左側にあるナビゲーションを使用して、該当するレポート タイプに対する、現在保存されているレポートを表示します。

ステップ 3 [New] をクリックします。[Report Details] ページが表示されます。

ステップ 4 [Report Details] ページで、次の [Settings] パラメータを入力します。

（注） 一部のパラメータは、レポート タイプによっては表示されることも、表示されないこともあります。

- [Report Title]：保存したレポートとしてこれを使用する場合は、レポート名を入力します。
- [Report By]：ドロップダウン リストから該当する [Report By]（レポート単位）のカテゴリを選択します。
- [Report Criteria]：事前に選択した [Report By] に応じて、結果をソートできます。[Edit] をクリックして、[Filter Criteria] ページを開きます。

  （注） [Select] をクリックしてフィルタ条件を確認するか、[Close] をクリックして前のページに戻ります。

- [Connection Protocol]：[All Clients]、[All Wired (802.3)]、[All Wireless (802.11)]、[All 11u Capable Clients]、[802.11a/n]、[802.11b/g/n]、[802.11a]、[802.11b]、[802.11g]、[802.11n (5 GHz)]、[802.11n (2.4 GHz)]
- Reporting Period
  - [Select a time period…]ドロップダウン リストからレポート期間を選択します。指定できる値は、[Today]、[Last 1 Hour]、[Last 6 Hours]、[Last 12 hours]、[Last 1 Day]、[Last 2 Days]、[Last 3 days]、[Last 4 Days]、[Last 5 Days]、[last 6 Days]、[Last 7 Days]、[Last 2 Weeks]、[Last 4 weeks]、[Previous Calendar Month]、[Last 8 Weeks]、[Last 12 Weeks]、[Last 6 Months]、[Last 1 Year] です。
  - [From]：[From] オプション ボタンを選択して、開始日時と終了日時を入力します。テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして日付を選択できます。ドロップダウン リストから時間と分を選択します。
  - [Show]：各ページに表示するレコード数を入力します。

    （注） すべてのレコードを表示するには、テキスト ボックスをブランクのままにします。

ステップ 5 このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、[Schedule] パラメータを入力します。[Schedule] パラメータを使用すると、レポートの実行時と実行頻度を管理できます。

- [Scheduling]：設定したスケジュールに従ってレポートを実行するには、[Enable] チェックボックスをオンにします。
- [Export Format]：エクスポートするファイルの形式（CSV または PDF）を選択します。
- [Destination]：宛先タイプ（[File] または [E-mail]）を選択します。該当するファイルの場所または電子メール アドレスを入力します。

  （注） CSV ファイルおよび PDF ファイルのデフォルトの場所は、次のとおりです。

  /localdisk/ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv

  /localdisk/ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

（注） 電子メール用のメール サーバ セットアップを設定するには、[Administration] > [Settings] の順に選択し、左側のサイドバーのメニューの [Mail Server] を選択して [Mail Server Configuration] ページを開きます。SMTP およびその他の必要な情報を入力します。

- [Start Date/Time]：表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。時間と分のドロップダウン リストから時刻を選択します。このデータに対するレポートの実行が、この日時に開始されます。
- [Recurrence]：このレポートの頻度を入力します。
  - [No Recurrence]：レポートは 1 度だけ実行されます（[Start Date/Time] で示した時間に実行）。
  - [Hourly]：レポートは、[Entry] テキスト ボックスに入力する時間数で示す間隔で実行されます。
  - [Daily]：レポートは、[Every] テキスト ボックスに入力する日数で示す間隔で実行されます。
  - [Weekly]：レポートは、[Every] テキスト ボックスに入力する週数およびチェックボックスをオンにした曜日に実行されます。
  - [Monthly]：レポートは、[Every] テキスト ボックスに入力する月数で示す間隔で実行されます。

[Create Custom Report] ページでは、レポート結果をカスタマイズできます。

カスタマイズ可能なレポートの詳細について、『*Cisco Prime Infrastructure User Guide*』を参照してください。

ステップ 6 別の [Create Custom Report] ページを開くには、[Customize] をクリックします。

a) □Custom Report Name□ドロップダウン リストから、実行するレポートを選択します。[Available and Selected] 列見出しの選択肢は、選択したレポートに応じて異なる場合があります。

b) [Report View] ドロップダウン リストから、レポートを表形式、グラフ形式、または両方を組み合わせた形式のいずれで表示するかを指定します。このオプションは、一部のレポートでは使用できません。

c) 2 つのグループ ボックス（[Available data fields] と [Data fields to include]）間で強調表示された列見出しを移動するには、[Add >] ボタンと [< Remove] ボタンを使用します。

（注）

青の列見出しは、現在のサブレポートでは必須です。これらは、[Selected Column] グループ ボックスから削除できません。

d) 結果テーブルの列の順序を決定するには、順序変更ボタン（[Move Up] または [Move Down]）を使用します。[Selected Columns] リストで上方の列見出しが、結果表の左方に表示されます。

e) [Data field sorting] グループ ボックスで、ソート設定（[Ascending] または [Descending]）を指定します。レポート データのソート方法を指定します。

- ソート順序を指定できる 4 つのデータ フィールドを選択できます。[Sort by] および [Then by] ドロップダウン リストを使用して、ソートする各データ フィールドを選択します。
- ソートされたデータ フィールドごとに、[Ascending] でソートするか [Descending] でソートするかを選択します。

（注） 表形式のレポートのみソートできます（グラフおよび複合形式は不可）。ソートできるフィールドのみが [Data field sorting] ドロップダウン リストに表示されます。

f) 変更内容を確定するには [Apply] を、列をデフォルトに戻すには [Reset] を、変更せずにこのページを閉じるには [Cancel] をクリックします。

（注） [Create Custom Report] ページで行った変更は、[Report Details] ページで [Save] をクリックしないうちは保存されません。

ステップ 7 すべてのレポート パラメータを設定したら、次のいずれかを選択します。

- [Save]：レポートをすぐに実行せずにこのレポート設定を保存するには、[Save] をクリックします。スケジュールしておいた時間になるとレポートは自動的に実行されます。
- [Save and Run]：このレポート設定を保存して、すぐにレポートを実行するには、[Save and Run] をクリックします。
- [Run Now]：レポート設定を保存せずにレポートを実行するには、[Run Now] をクリックします。
- [Cancel]：このレポートを実行も保存もせずに前のページに戻るには、[Cancel] をクリックします。

現在のレポートの管理

特定のレポート タイプに対するレポートが保存されている場合は、レポート ラウンチ パッドから現在のレポートにアクセスできます。

新しいチョークポイントが作成されると、すべての仮想ドメインで使用できます。フロアに配置したあと、フロアと同じ仮想ドメインで使用できるように更新されます。チョークポイントをフロアから削除すると、すべての仮想ドメインで再び利用可能になります。

[Report Launch Pad] から現在のレポートまたは保存されたレポートにアクセスするには、以下のステップに従います。

ステップ 1 [**Reports**] > [**Report Launch Pad**] の順に選択します。

ステップ 2 左側のサイドバーのメニューまたはレポート ラウンチ パッドのメイン セクションから、特定のレポートを選択します。[Report Launch Pad] ページには、このレポート タイプの現在のレポートのリストが表示されます。
保存されたレポートのリストを表示するには、[**Reports**] > [**Saved Reports**] の順に選択します。

スケジュールされた実行結果の管理

（注） スケジュールされた実行のリストは、レポート カテゴリ、レポート タイプ、およびタイム フレームでソートできます。

保存したレポートの管理

[Saved Reports] ページでは、保存したレポートを作成および管理できます。Prime Infrastructure でこのページを開くには、[Reports] > [Saved Reports] の順に選択します。

（注） 保存したレポートのリストは、レポート カテゴリ、レポート タイプ、およびスケジュールされたステータス（有効、無効、または期限切れ）でソートできます。

[Saved Reports] ページには、次の情報が表示されます。

- [Report Title]：ユーザが割り当てたレポート名を示します。このレポートの詳細を表示するには、レポート タイトルをクリックします。
- [Report Type]：特定のレポート タイプを示します。
- [Scheduled]：このレポートが有効か無効かを示します。
- [Next Schedule On]：このレポートの次にスケジュールされた実行の日時が示されます。
- [Last Run]：このレポートの最後にスケジュールされた実行の日時が示されます。
- [Download]：レポートの結果の .csv ファイルを開くか保存するには、[Download] アイコンをクリックします。
- [Run Now]：現在のレポートをすぐに実行するには、[Run Now] アイコンをクリックします。

デバイス使用率レポートの作成

Mobility Services Engine のデバイス使用率レポートを作成するには、以下のステップに従います。

ステップ 1 [Reports] > [Report Launch Pad] の順に選択します。

ステップ 2 [Device] > [Utilization] の順に選択します。

ステップ 3 [New] をクリックします。[Utilization Report Details] ページが表示されます。

ステップ 4 [Report Details] ページで、次の [Settings] パラメータを入力します。

（注）　一部のパラメータは、レポートタイプによっては機能することも、機能しないこともあります。

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- [Report Type]：デフォルトでは、レポート タイプは MSE が選択されます。
- [Report By]：ドロップダウン リストから該当する [Report By]（レポート単位）のカテゴリを選択します。カテゴリはレポートごとに異なります。各レポートの [Report By] カテゴリについては、特定のレポートの項を参照してください。
- [Report Criteria]：このパラメータを指定すると、事前に選択した [Report By] に応じて、結果をソートできます。[Edit] をクリックして、[Filter Criteria] ページを開きます。
- [Connection Protocol]：[All Clients]、[All Wired (802.3)]、[All Wireless (802.11)]、[802.11a/n]、[802.11b/g/n]、[802.11a]、[802.11b]、[802.11g]、[802.11n (5-GHz)]、または [802.11n (2.4-GHz)] からいずれかのプロトコルを選択します。
- [SSID]：[All SSIDs] がデフォルト値です。
- [Reporting Period]：時間単位、週単位、または特定の日時にデータを収集するようにレポートを定義できます。選択したレポート期間のタイプは、x 軸に表示されます。

（注）　レポート期間には、12 時間表記ではなく 24 時間表記が使用されます。たとえば、午後 1 時の場合は、13 時を選択します。

ステップ 5　[Schedule] グループ ボックスで、[Enable Schedule] チェックボックスをオンにします。

ステップ 6　[Export Report] ドロップダウン リストから、レポート形式（[CSV] または [PDF]）を選択します。

ステップ 7　レポートの保存先として、[File] または [Email] を選択します。

- [File] オプションを選択する場合は、先に [Administration] > [Settings] > [Report] ページで保存先パスを定義しておく必要があります。[Repository Path] テキスト ボックスに、ファイルの保存先パスを入力します。
- [Email] オプションを選択する場合は、目的の電子メール アドレスを入力する前に、SMTP メール サーバを定義しておく必要があります。[Administrator] > *[Settings]* > *[Mail ServerConfiguration]* の順に選択して、適切な情報を入力します。

ステップ 8　開始日（MM:DD:YYYY）を入力するか、[Calendar] アイコンをクリックして日付を選択します。

ステップ 9　[hour] と [minute] のドロップダウン リストを使用して開始時刻を選択します。

ステップ 10　[Recurrence] オプション ボタンを選択して、レポートの実行頻度を決定します。可能な値は次のとおりです。

- No Recurrence
- Hourly
- Daily
- Weekly
- Monthly

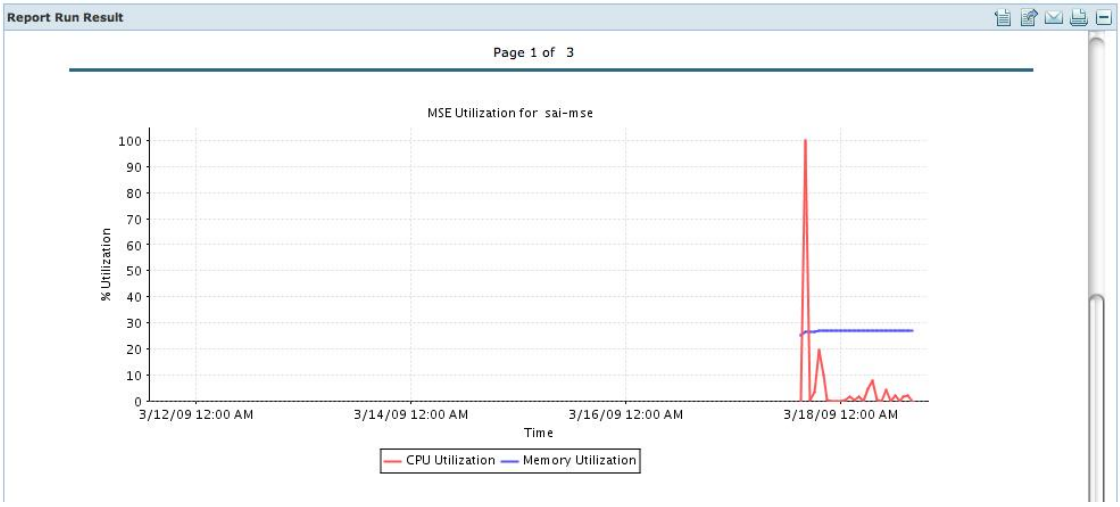
（注）　曜日は [Weekly] オプションを選択した場合のみページ上に表示されます。

ステップ 11　ステップ 1 からデバイス使用率レポートの作成 までが終了したら、次のいずれかを実行します。

- [Save] をクリックして編集を保存します。指定した時刻にレポートが実行され、[Schedule] グループボックスでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
- [Save and Run] をクリックして、変更内容を保存し、レポートをすぐに実行します。レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。結果はページの一番下に表示されます。レポートは指定した時刻にも実行され、[Schedule] グループボックスでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
  - 結果のページで、[Cancel] をクリックして、定義済みのレポートをキャンセルします。
- レポートをすぐに実行して結果を [Prime Infrastructure] ページで確認するには、[Run Now] をクリックします。レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。結果はページの一番下に表示されます。入力したレポート条件を保存する場合は [Save] をクリックします。

（注）　[Run Now] をクリックして、保存する前に定義済みのレポート条件を確認したり、必要に応じてレポートを実行したりすることもできます。次の例には、CPU とメモリの使用率レポートのみ表示されています。

図 *25*：*[Devise] > [MSE Utilization] > [Results]*



スケジュールされているレポートは、「enabled」として表示され、次の実行スケジュール日が表示されます。

実行済みで次の実行がスケジュールされていないレポートは、「expired」として表示されます。

実行済みで再度実行するようにスケジュールされているレポートは、「disabled」として表示されます。

ステップ 12 レポートを有効化、無効化、または削除するには、そのレポートタイトルの隣にあるチェックボックスをオンにして、適切なオプションをクリックします。

保存した使用率レポートの表示

保存したレポートをダウンロードするには、以下のステップに従います。

ステップ 1 [Reports] > [Saved Reports] の順に選択します。

ステップ 2 レポートの [Download] アイコンをクリックします。レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

スケジュールされた使用率の実行の表示

スケジュールされたレポートのステータスを確認するには、以下のステップに従います。

ステップ 1 [Reports] > [Scheduled Runs] の順に選択します。

ステップ 2 [History] アイコンをクリックして、レポートの最終実行日を確認します。

ステップ 3 レポートの [Download] アイコンをクリックします。レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

MSE でのクライアントのサポート

Prime Infrastructure の Advanced Search 機能を使用して、特定のカテゴリおよびフィルタに基づいて、クライアントリストを絞り込むことができます。[Show] ドロップダウンリストを使用して、現在のリストをフィルタリングすることもできます。

- IPv6 アドレスによる MSE 上の Prime Infrastructure のワイヤレス クライアントの検索
- MSE で検出されたクライアントの表示

IPv6 アドレスによる MSE 上の Prime Infrastructure のワイヤレス クライアントの検索

Prime Infrastructure の Advanced Search 機能を使用して、MSE の配置されたクライアントを検索するには、以下のステップに従います。

ステップ 1 Prime Infrastructure UI の右上隅にある [Advanced Search] をクリックします。

ステップ 2 [New Search] ダイアログで、[Search Category] ドロップダウン リストから検索カテゴリとして [Clients] を選択します。

ステップ 3 [Media Type] ドロップダウン リストから、[Wireless Clients] を選択します。

（注） メディア タイプとして [Wireless Clients] を選択した場合だけ、[Wireless Type] ドロップダウン リストが表示されます。

ステップ 4 [Wireless Type] ドロップダウン リストから、[All]、[Lightweight]、または [Autonomous Clients] のうちいずれかのタイプを選択します。

ステップ 5 [Search By] ドロップダウン リストから、[IP Address] を選択します。

（注） IP アドレスによるクライアントの検索は、IP アドレス全体または一部を対象にできます。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

ステップ 6 [Clients Detected By] ドロップダウン リストから、[clients detected by MSE] を選択します。
Cisco WLC と直接通信することで、MSE の Context-Aware Service で検索されるクライアントが表示されます。

ステップ 7 [Last detected within] ドロップダウン リストから、クライアントが検出された時間帯を選択します。

ステップ 8 [Client IP Address] テキスト ボックスにクライアント IP アドレスを入力します。IPv6 アドレスの一部または全体を入力できます。

（注） IPv4 アドレスを使用して、MSE 上で Prime Infrastructure のクライアントを検索している場合は、[Client IP address] テキスト ボックスに IPv4 アドレスを入力します。

ステップ 9 [Client States] ドロップダウン リストから、クライアントの状態を選択します。ワイヤレス クライアントに指定できる値は、[All States]、[Idle]、[Authenticated]、[Associated]、[Probing]、または [Excused] です。有線クライアントに指定できる値は、[All States]、[Authenticated]、および [Associated] です。

ステップ 10 [Posture Status] ドロップダウン リストからポスチャ ステータスを選択すると、デバイスがクリーンであるかどうかを判別します。指定できる値は、[All]、[unknown]、[Passed]、および [Failed] です。

ステップ 11 [CCX Compatible] チェックボックスをオンにすると、Cisco Client Extensions と互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、[V2]、[V3]、[V4]、[V5]、および [V6] です。

ステップ 12 [E2E Compatible] チェックボックスをオンにすると、エンドツーエンドの互換性のあるクライアントを検索します。指定できる値は、[All Versions]、[V1]、および [V2] です。

ステップ 13 [NAC State] チェックボックスをオンにすると、特定のネットワーク アドミッション コントロール（NAC）の状態で特定されるクライアントを検索します。指定可能な値は、[Quarantine]、[Access]、[Invalid]、および [Not Applicable] です。

ステップ 14 [Include Disassociated] チェックボックスをオンにすると、ネットワーク上には存在しなくなったが、Prime Infrastructure には履歴レコードが残っているクライアントが含まれます。

ステップ 15 [Items per page] ドロップダウン リストから、検索結果ページに表示するレコードの数を選択します。

ステップ 16 [Save Search] チェックボックスをオンにして、選択した検索オプションを保存します。

ステップ 17 [Go] をクリックします。
[Clients and Users] ページに、MSE で検出されたすべてのクライアントが表示されます。

MSE で検出されたクライアントの表示

MSE で検出されたすべてのクライアントを表示するには、以下のステップに従います。

ステップ 1 [Monitor] > [Clients and Users] の順に選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。
[Client and Users] ページが表示されます。

[Clients and Users] 表にはデフォルトでいくつかの列が表示されます。使用可能な列を追加して表示する場合は、 をクリックし、[Columns] をクリックします。使用可能な列が表示されます。[Clients and Users] 表に表示する列を選択します。列内の任意の場所をクリックすると、その列が選択され、クライアントの詳細が表示されます。

ステップ 2 [Show] ドロップダウン リストから [Clients detected by MSE] を選択して、現在のリストをフィルタリングし、MSE で検出されるクライアントをすべて選択します。
有線およびワイヤレスを含め、MSE で検出されたすべてのクライアントが表示されます。有線およびワイヤレスを含め、MSE で検出されたすべてのクライアントが表示されます。

[Clients Detected by MSE] 表では、次のさまざまなパラメータを使用できます。

- [MAC Address]：クライアント MAC アドレス。

- [IP Address]：クライアント IP アドレス。

  [IP Address] 列に表示される IP アドレスは、定義済みの優先順位によって決まります。使用可能な最初の IP アドレスが次の順番で [IP address] テキスト ボックスに表示されます。

  - IPv4 アドレス

    （注） このリリースでは、ワイヤレス クライアントだけが IPv6 アドレスを使用します。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

  - IPv6 グローバル固有アドレス。このタイプのアドレスが複数ある場合は、クライアントが受信した最新の IPv6 アドレスが表示されます。ユーザがグローバル IPv6 アドレスを 2 つ持っていても、どちらかが期限切れになっている古いルータ アドバタイズメントによって取得したアドレスである場合があるためです。

  - IPv6 ローカル固有アドレス。複数ある場合は、最新の IPv6 ローカル固有アドレスがクライアントによって使用されます。

  - IPv6 リンク ローカル アドレス。他の IPv6 アドレスが割り当てられる前に、セルフアサインされ、通信に使用されるクライアントの IPv6 アドレス。

    次のようなさまざまな IPv6 アドレス タイプがあります。

  - リンクローカルユニキャスト：リンクローカルアドレスは、自動アドレス設定、ネイバー探索、ルータが存在しないときなどのために、単一リンクでのアドレス指定に使用するように設計されています。

  - サイトローカル ユニキャスト：サイトローカル アドレスは、グローバル プレフィックスには必要のない、サイト内部でのアドレス指定に使用するように設計されています。

  - 集約可能グローバルユニキャスト：集約可能グローバルユニキャストアドレスは、グローバル ネットワーク内でクライアントを一意に特定します。パブリック IPv4 アドレスと同等です。クライアントは複数の集約可能グローバルユニキャストアドレスを持つことができます。

- [IP Type]：クライアントの IP アドレス タイプ。指定できるのは、IPv4、IPv6、またはデュアル スタック（IPv4 アドレスと IPv6 アドレスの両方があるクライアントを表す）です。

  - グローバル固有

  - 固有ローカル

  - リンク ローカル

- [User Name]：802.1x 認証に基づいたユーザ名。ユーザ名を使用しないで接続されたクライアントの場合は [Unknown] と表示されます。

- [Type]：クライアント タイプを示します。

- [Vendor]：OUI から導き出されたデバイス ベンダー。

- [Device Name]：ネットワーク認証デバイス名。たとえば、WLC、スイッチなどです。
- [Location]：接続しているデバイスのマップ位置。
- [VLAN]：このクライアントのアクセス VLAN ID を示します。
- [Status]：現在のクライアントのステータス。
  - [Idle]：正常の動作。クライアントのアソシエーション要求は拒否されていません。
  - [Auth Pending]：AAA トランザクションを実行しています。
  - [Authenticated]：802.11 認証が完了しています。
  - [Associated]：802.11 アソシエーションが完了しています。これは、現在クライアントがネットワークに接続されていることを示すために有線クライアントでも使用されます。
  - [Disassociated]：802.11 ディスアソシエーションが完了しています。これは、現在クライアントがネットワーク上に存在しないことを示すために有線クライアントでも使用されます。
  - [To Be Deleted]：ディスアソシエーション後にクライアントが削除されます。
  - [Excluded]：セキュリティの脅威と見なされたため、システムによって自動的に無効化されています。
- [Interface]：クライアントが接続する Cisco WLC インターフェイス（ワイヤレス）またはスイッチ インターフェイス（有線）。
- プロトコル
  - [802.11]：ワイヤレス
  - [802.3]：有線
- [Association Time]：最後のアソシエーションの開始時間（ワイヤレス クライアントの場合）。有線クライアントの場合、これは、クライアントがスイッチ ポートに接続した時間です。クライアントがアソシエートされているが、ネットワーク上で問題がある場合は空欄になります。
- [CCX]：Lightweight ワイヤレスのみ。
  - [Client and User] ページの MAC アドレスの横にあるオプション ボタンを選択して、アソシエートされたクライアント情報を表示します。次のクライアント パラメータが表示されます。
- クライアント属性
- クライアント IPV6 アドレス
- Client Statistics

（注） クライアントの統計には、クライアント詳細情報の後に統計情報が表示されます。

- クライアント アソシエーション履歴

- クライアント イベント情報
- クライアント ロケーション情報
- 有線ロケーション履歴
- クライアント CCX 情報
- クライアント属性

[Clients and Users] リストからクライアントを選択すると、次のクライアント詳細情報が表示されます。クライアントは、MAC アドレスを使用して特定されます。

- 全般：次の情報がリストされます。
  - ユーザ名
  - IP Address
  - MAC アドレス
  - ベンダー
  - エンドポイント タイプ
  - クライアント タイプ
  - メディア タイプ
  - モビリティ ロール
  - Hostname
  - E2E
  - ファンデーション サービス
  - 管理サービス
  - 音声サービス
  - ロケーション サービス

- [Session]：次の情報が表示されます。
  - コントローラ名
  - AP Name
  - AP IP アドレス
  - AP タイプ
  - AP ベース無線 MAC
  - アンカー アドレス
  - 802.11 ステート

- アソシエーション ID
- Port
- インターフェイス
- SSID
- Profile Name
- プロトコル
- VLAN ID
- AP モード

- セキュリティ（ワイヤレス クライアントおよびアイデンティティ有線クライアントのみ）：次のセキュリティ情報をリストします。
  - セキュリティ ポリシー タイプ
  - EAP タイプ
  - ネットワーク上
  - 802.11 認証
  - 暗号化方式
  - SNMP NAC の状態
  - RADIUS NAC の状態
  - AAA Override ACL 名
  - AAA Override ACL の適用された状態
  - リダイレクト URL
  - ACL 名
  - ACL の適用された状態
  - FlexConnect ローカル認証
  - Policy Manager ステート
  - 認証 ISE
  - 認可プロファイル名
  - ポスチャ ステータス
  - TrustSec セキュリティ グループ
  - Windows AD ドメイン

（注） アイデンティティ クライアントは、認証タイプが 802.1x、MAC 認証バイパス、または Web 認証のクライアントです。アイデンティティ クライアント以外の認証タイプは N/A です。

（注） クライアント属性の下に表示されるデータは、アイデンティティ クライアントかそうでないかによって異なります。アイデンティティ クライアントの場合は、認証ステータス、監査セッション ID などのセキュリティ情報を確認できます。

- [Statistics]（ワイヤレスのみ）
- [Traffic]：クライアントのトラフィック情報を表示します。
- ワイヤレス クライアントの場合、クライアントのトラフィック情報は Cisco WLC から取得します。有線クライアントの場合、クライアントのトラフィック情報はISEから取得するため、スイッチ上でアカウンティング情報およびその他の必要な機能を有効にする必要があります。

統計情報

[Statistics] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- クライアント AP アソシエーション履歴。
- クライアント RSSI 履歴（dBm）：クライアントがアソシエートされたアクセス ポイントで検出された RSSI（受信信号強度インジケータ）の履歴。
- クライアント SNR 履歴：クライアントがアソシエートされたアクセス ポイントで検出された SNR（クライアント RF セッションの信号対雑音比）の履歴。
- 送受信バイト（Kbps）：アソシエートされたアクセス ポイントで送受信したバイト数。
- 送受信パケット（毎秒）：アソシエートされたアクセス ポイントで送受信したパケット数。
- クライアントのデータ レート

この情報は、インタラクティブ グラフで表示されます。

クライアント IPV6 アドレス

[Client IPv6 Address] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- IP アドレス：クライアント IPv6 アドレスを表示します。
- スコープ：グローバル固有、ローカル固有、およびリンク ローカルの 3 つのスコープ タイムがあります。
- アドレス タイプ：アドレス タイプを表示します。
- 検出時間：IP が検出された時間です。

アソシエーション履歴

[Association History] グループ ボックスには、選択したクライアントの過去 10 件のアソシエーション時間に関する情報が表示されます。この情報は、クライアントのトラブルシューティングの際に役立ちます。

- アソシエーション時間
- 持続時間
- ユーザ名
- IP Address
- IP アドレス タイプ
- AP Name
- コントローラ名
- SSID

Event

[Client Details] ページの [Event] グループ ボックスには、イベント タイプやイベントの日時など、このクライアントのすべてのイベントが表示されます。

- イベント タイプ
- イベント時間
- 説明

マップ

[View Location History] をクリックすると、有線クライアントおよびワイヤレス クライアントのロケーション履歴の詳細が表示されます。

有線クライアントまたはワイヤレス クライアントの次のロケーション履歴情報が表示されます。

- Timestamp
- 状態
- ポート タイプ
- スロット
- Module
- Port
- ユーザ名
- IP Address
- スイッチ IP
- サーバ名
- マップ位置の都市ロケーション

Geo-Location のモニタリング

MSE は、有線クライアント、有線エンドポイント、スイッチ、Cisco WLC、ワイヤレス ネットワーク構成内にあるアクセス ポイントの物理ロケーションを提供します。現在、MSE はノースバウンドエンティティからサウスバウンドエンティティまでの外部エンティティに Geo-Location 形式でロケーション情報を提供しています。

MSE によって提供される Geo-Location 情報の精度を向上するために、この機能はデバイスのジオメトリック ロケーション座標を Geo-Location 座標（経度と緯度）に変換し、ノースバウンドインターフェイスとサウスバウンド インターフェイスを介して外部エンティティに提供します。

（注） Geo-Location の計算には、少なくとも 3 つの GPS マーカーが必要です。追加できる GPS マーカーの最大数は 20 です。

- フロア マップへの GPS マーカーの追加, （176 ページ）
- GPS マーカーの編集, （177 ページ）
- フロアからの GPS マーカーの削除, （177 ページ）

フロア マップへの GPS マーカーの追加

GPS マーカーをフロア マップに追加するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択して、[Maps] ページを表示します。

ステップ 2 [Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3 左上のメニューの [Add/Edit GPS Markers Information] メニュー オプションを選択して、[Add/Edit GPS] ページを表示します。
マップの左上隅（X = 0、Y = 0）に [GPS Marker] アイコンが表示されます.

ステップ 4 [GPS Marker] アイコンをドラッグして、マップ上の希望する場所に配置することができます。また、左側のサイドバー メニューにある [GPS Marker Details] テーブルに X と Y の位置の値を入力して、マーカーを希望する位置に移動することができます。
（注） 追加したマーカーの位置が近すぎると、Geo-Location 情報の精度は低下します。

ステップ 5 左側のサイドバー メニューで選択した [GPS Marker] アイコンの経度と緯度を入力します。

ステップ 6 [Save] をクリックします。
[GPS Marker] の情報がデータベースに保存されます。

ステップ 7 [Apply to other Floors of Building] をクリックして、ビルディングの 1 フロアの GPS マーカーをそのビルディングの残りのすべてのフロアにコピーします。

GPS マーカーの編集

フロアにある GPS マーカーを編集するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択して、[Maps] ページを表示します。

ステップ 2 [Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3 [Add/Edit GPS Markers Information] メニュー オプションを選択して、[Add/Edit GPS] ページを表示します。

ステップ 4 左側のサイドバー メニューから、フロアにある既存の GPS マーカーを選択します。

ステップ 5 左側のサイドバー メニューから、その GPS マーカーにアソシエートされている [Latitude]、[Longitude]、[X Position]、および [Y Position] を変更できます。

ステップ 6 [Save] をクリックします。
これで、変更した GPS マーカーの情報がデータベースに保存されます。

フロアからの GPS マーカーの削除

フロアから GPS マーカーを削除するには、以下のステップに従います。

ステップ 1 [Monitor] > [Site Maps] の順に選択して、[Maps] ページを表示します。

ステップ 2 [Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3 [Add/Edit GPS Markers Information] メニュー オプションを選択して、[Add/Edit GPS] ページを表示します。

ステップ 4 左側のサイドバー メニューから、フロアにある既存の GPS マーカーを選択します。

（注） [Multiple GPS Markers] チェックボックスをオンにすることで、フロアにある複数の GPS マーカーを削除できます。

ステップ 5 [Delete GPS Marker] をクリックします。
選択した GPS マーカーがデータベースから削除されます。

Ekahau Site Survey の統合

Ekahau Site Survey（ESS）ツールは、高機能 Wi-Fi ネットワークの設計、導入、維持、およびトラブルシューティングに使用します。ESS はあらゆる 802.11 ネットワーク上で機能し、集中管理型の 802.11n Wi-Fi ネットワーク用に最適化されています。

ESS ツールを使用して、Prime Infrastructure から既存のフロア マップをインポートし、プロジェクトを Prime Infrastructure にエクスポートできます。詳細については、ESS オンライン ヘルプの「Cisco Prime Infrastructure Integration」を参照してください。

（注） Prime Infrastructure サイト調査のキャリブレーションでは、150 以上の調査データ ポイントが 50 の異なる場所で収集されている必要があります。十分な調査データ ポイントがない場合は、調査データをエクスポートしようとすると警告が表示されます。

（注） サイト調査時に Prime Infrastructure にアクセス ポイントがない場合、サイト調査は実施されません。

（注） Prime Infrastructure でフロア マップのスケールが正しくない場合、ESS の視覚的な表示が乱れます。

AirMagnet Survey と AirMagnet Planner の統合

AirMagnet Survey と AirMagnet Planner は、Cisco Prime Infrastructure に統合されます。この統合により、一般的にワイヤレス LAN ネットワークの導入と管理に付随するワイヤレス計画と実地調査の作業を何度も行う必要がなくなり、運用効率性を高めることができます。

AirMagnet Survey ツールにより、現実世界の調査データを Prime Infrastructure にエクスポートして、Planner モデリングのキャリブレーションに利用できます。AirMagnet Planner では、Planner プロジェクトを作成し、直接 Prime Infrastructure にエクスポートできます。これにより Prime Infrastructure で、インポートした AirMagnet Planner ツールから独自のプロジェクトを作成できます。詳細については、Fluke Networks の Web サイトで提供されている『AirMagnet Survey and Planning』マニュアルを参照してください。

セキュリティ ダッシュボードの解釈

Prime Infrastructure セキュリティ ダッシュボードでは、次の機能が追加されました。

- Valid Client on Rogue AP
- ソフト AP
- Good Guy Gone Bad（GGGB）

上記の機能は、すべてセキュリティ ダッシュボードの [Client Classification] の表に分類されます。不正 AP の数には、ハイパーリンクが関連付けられています。表に設定されているハイパーリンクをクリックすると、不正アクセス上のソフト AP、GGGB、有効なクライアントを表示できます。

不正 APの表示

不正アクセス ポイント（AP）を表示するには、以下のステップに従います。

手順の概要

1. 以前は企業ネットワークに関連付けられ現在は不正 AP に関連付けられているクライアントを表示するには、[Valid Client connected to Rogue AP] 番号をクリックします。
2. このページには、以下の項目が表示されます。
3. [Soft AP] 番号をクリックして、以前はプローブで現在は不正 AP のクライアントを表示します。
4. このページには、以下の項目が表示されます。
5. [Good Guy Gone Bad] 番号をクリックして、以前はアソシエーションされており現在は不正 AP のクライアントを表示します。
6. このページには、以下の項目が表示されます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	以前は企業ネットワークに関連付けられ現在は不正 AP に関連付けられているクライアントを表示するには、[Valid Client connected to Rogue AP] 番号をクリックします。	
ステップ 2	このページには、以下の項目が表示されます。	• [Client Mac Address]：クライアントの MAC アドレス • [Rogue AP Mac Address]：不正 AP の MAC アドレス。 • [First Detected]：不正 AP が最初に検出された日時を表示します。 • [Last Detected]：不正 AP が最後に検出された日時を表示します。 • [Containment Start Time] • [Containment Stop Time] • [State]：有効なクライアントが不正 AP に接続したときの、不正 AP の状態。状態には、[Alert] と [Threat] の 2 つがあります。

	コマンドまたはアクション	目的
ステップ 3	[Soft AP] 番号をクリックして、以前はプローブで現在は不正 AP のクライアントを表示します。	
ステップ 4	このページには、以下の項目が表示されます。	• [Type]：クライアントのタイプを表示します。 • [Soft AP MAC Address]：ソフト AP の MAC アドレス。 • [TimeStamp]：ソフト AP が検出された正確な日時を表示します。
ステップ 5	[Good Guy Gone Bad] 番号をクリックして、以前はアソシエーションされており現在は不正 AP のクライアントを表示します。	
ステップ 6	このページには、以下の項目が表示されます。	• [Type]：クライアントのタイプを表示します。 • [Good Guy Gone Bad Mac Address]：「Good Guy Gone Bad」クライアントの MAC アドレス。 • [TimeStamp]：ソフト AP が検出された正確な日時を表示します。

クライアントの分類

クライアントには 3 種類があります。

不正アクセス ポイントに接続された有効なクライアント：クライアントが不正アクセス ポイントと関連付けられると、MSE はクライアントが有効なクライアントかどうかを確認します。有効なクライアントの場合、両デバイスの MAC アドレスを含む不正アクセス ポイント テーブルにエントリが追加されます。実行された封じ込めの操作に応じて、封じ込めフィールドが更新されます。次のシナリオを検討する必要があります。

- クライアントがアソシエートされた後、消失する
- クライアントのアソシエーション解除の情報がある
- 不完全な封じ込め

ソフト AP：ソフト アクセス ポイント（ソフト AP）は Wi-Fi アダプタでセットアップされ、物理 Wi-Fi ルータは必要ありません。Windows 7 コンピュータまたは Windows 7 仮想 Wi-Fi 機能がある Windows Vista コンピュータで、ソフト AP を容易にセットアップできます。稼働状態になると、コンピュータで利用可能なネットワーク アクセスを、ソフト AP に接続する他の Wi-Fi ユーザと容易に共有できます。従業員が社屋内の自分のコンピュータでソフトアクセスポイントをセット

アップし、それを介して社内ネットワークを共有すると、このソフト AP は不正アクセス ポイントとして動作します。 スマートフォンで Wi-Fi テザリングをオンにして、不正アクセス ポイントとして動作することもできます。MSE は、このソフト不正 AP シナリオを検出し、自動封じ込めを行うように応答をコントローラに送信します。

善良クライアントの不正化：有効なクライアントがソフト AP になると、至急の対策が必要なより重大な脅威になります。MSE はこれらのシナリオを検出し、善良クライアントの不正化を報告します。

第 II 部

Cisco MSE 管理ユーザ インターフェイス

- Cisco MSE 管理ユーザ インターフェイス，185 ページ
- MSE システム設定とサービスの構成，195 ページ

第 8 章

Cisco MSE 管理ユーザ インターフェイス

- MSE 管理 UI のホーム ページ，185 ページ
- データの精度ツールの使用，189 ページ
- システムとネットワークの健全性のモニタリング，191 ページ

MSE 管理 UI のホーム ページ

MSE 管理者 UI のホーム ページでは、ネットワーク内の最も重要なデータおよびさまざまなサービスのステータスが分かりやすく表示されるため、MSE システム設定を構成できます。また、ページ右上で [admin] > [enable beta features] の順に選択すると、Health and Data Accuracy Tool など、さまざまなアプリケーションのベータ版を表示することもできます。

MSE 管理ユーザ インターフェイスの起動

MSE 管理ユーザ インターフェイスを起動するには、以下のステップに従います。

手順の概要

1. MSE 管理ユーザ インターフェイス（UI）を起動します。起動するには、Web ブラウザで https://*mseip*/*mseui* と入力するか、または Cisco Prime Infrastructure（PI）の [Services] > [Mobility Services Engines] ページで MSE 名リンクをクリックして起動します。
2. ユーザ名とパスワードを入力します。
3. [Sign In] をクリックします。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	MSE 管理ユーザ インターフェイス（UI）を起動します。起動するには、Web ブラウザで https://*mseip*/*mseui* と入力するか、または Cisco Prime Infrastructure（PI）の [Services] > [Mobility Services Engines] ページで MSE 名リンクをクリックして起動します。	（注） MSE 管理 UI は、Prime Infrastructure ユーザ インターフェイスの [Administration] > [User Preference Page] で [MSE Admin View] チェック ボックスをオンにしたときのみ表示されます。
ステップ 2	ユーザ名とパスワードを入力します。	
ステップ 3	[Sign In] をクリックします。	MSE 管理 UI ホームページが表示されます。

MSE サービス

このセクションでは、Cisco MSE が Cisco Unified Wireless Network（CUWN）内全体でサポートするさまざまなサービスについて簡単に説明します。

使用可能なサービスはすべて、[Services] グループ ボックスの MSE 管理者 UI ホームページに記載されています。

- **CMX Analytics**：CMX Analytics サービスは、特定のネットワーク上のワイヤレス デバイスのロケーション情報を分析します。CMX Analytics サービスは、Cisco Mobility Services Engine（MSE）が提供するデータを使用して、ワイヤレス ローカルエリア ネットワーク（WLAN）内の Wi-Fi デバイスのロケーションを計算します。ネットワーク内でワイヤレス デバイスが有効化されている場合、そのワイヤレスデバイスはプローブ要求パケットを送信して、その近隣のワイヤレス ネットワークを識別します。WLAN のアクセス ポイントに接続した後でも、クライアント デバイスはより良い QoS のために、その他のアクセス ポイントを特定するためのプローブ要求パケットの送信を続けます。アクセスポイントは、各種のワイヤレス デバイスからこれらの要求と関連する RSSI を収集し、それらをワイヤレス LAN コントローラ（WLC）に送信します。コントローラは、この情報を MSE に送信します。

  各種 AP から収集された基本データを分析すると、建物内で Wi-Fi デバイスを使用しているユーザの移動および行動パターンについて情報や知識を得ることができます。たとえば、建物として、空港、ショッピング モール、シティ センターなどが考えられます。CMX Analytics サービスは、空港局や建物の所有者が自分の建物内の通行人または顧客の動向を認識できます。これは、これらの所有者が建物内の標示を改善したり、使用率の低い場所に変更を加えたりするのに役立ちます。

- **Context Aware Service**：ロケーション サービスとも呼ばれます。これは Mobility Services Engine（MSE）の中核サービスで、Wi-Fi クライアント追跡およびロケーション API 機能をオンにします。プレゼンス、ロケーション、テレメトリ データ、および履歴情報などのコンテキスト情報を取得することで、MSE はモバイル資産とクライアントを同時に追跡できます。

- **CMX Connect & Engage**：これまでは Browser Engage Service と呼ばれていました。CMX Connect and Engage サービスは、CMX ソフトウェア開発キット（SDK）の接続、ゲスト Wi-Fi オンボード ソリューション、ゾーン、メッセージ設定を提供します。
- **Mobile Concierge**：Cisco Mobility Services Advertisement Protocol（MSAP）を有効にします。このプロトコルにより、MSE とモバイル デバイス間の直接通信が有効になるため、モバイルデバイスのプレアソシエーションにコンテンツを直接適用できます。この機能は、802.11u および MSAP をサポートするモバイル デバイスに依存します。
- **Wireless Intrusion Prevention**：CUWN インフラストラクチャ内の悪意のある攻撃、セキュリティの脆弱性、パフォーマンス阻害のソースから、ワイヤレス固有のネットワーク脅威を検出して軽減します。wIPS は、ワイヤレスの脅威を可視化、分析、および識別し、シスコのモニタ モードと拡張ローカル モード（ELM）アクセス ポイントを使用して、セキュリティとパフォーマンスの問題の軽減策と解決策を一元的に管理します。また、ほとんどのワイヤレス攻撃では侵入不可能な強化無線ネットワーク コアを作成するために予防的な脅威対策もサポートされます。

MSE サービスの有効化または無効化

MSE サービスを有効または無効にするには、以下のステップに従います。

手順の概要

1. MSE 管理 UI を起動します。
2. サービスを有効にするには、以下のステップに従います。
3. サービスを無効にするには、以下のステップに従います。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	MSE 管理 UI を起動します。	MSE Admin UI のホーム ページが表示されます。[Services] グループ ボックスに表示されるさまざまなサービスは次のとおりです。 • CMX 分析 • Context Aware Service • CMX Connect & Engage • Mobile concierge • Wireless Intrusion Prevention
ステップ 2	サービスを有効にするには、以下のステップに従います。	（注） 有効なサービスは緑色で、無効なサービスは赤色で表示されます。 • [Services] グループ ボックスで有効にする任意のサービス タブをクリックします。

	コマンドまたはアクション	目的
		• [Up/Down] ボタンをクリックします。 「Do you really want to change the service status」ダイアログ ボックスが表示されます。 • [OK] をクリックします。 サービスが有効になると、[Up]ボタンの色が緑に変わります。また、[Services] グループ ボックスの対応するサービス名も緑色に変わります。
ステップ 3	サービスを無効にするには、以下のステップに従います。	• [Services] グループ ボックスで無効にする任意のサービス タブをクリックします。 • [Up/Down] ボタンをクリックします。 「Do you really want to change the service status」ダイアログ ボックスが表示されます。 • [OK] をクリックします。 サービスが無効になると、[Down] ボタンの色が赤に変わります。また、[Services] グループ ボックスの対応するサービス名も赤色に変わります。

MSE アプリケーション

管理者 UI は、サービスのフロント エンドとして動作する次の Web アプリケーションで構成されています。

- 新機能
- CMX Connect and Engage
- マップ
- データの精度ツール
- 状態

データの精度ツールの使用

前提条件

ロケーションチューニングまたはデバイスフィルタを使用してデバイスをフィルタリングする前に、Cisco Prime Infrastructure ユーザ インターフェイスを使用して次の手順を実行する必要があります。

- ビルのフロア領域と MSE を同期します。
- フロアに境界を作成します。

同期化およびマップ エディタの詳細については、『*Cisco Prime Infrastructure Classic View Configuration Guide*』の「マップのモニタリング」を参照してください。

ロケーション チューニングの使用

施設外部のデバイスをフィルタリングするには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 [admin] > [Enable Beta Features] の順に選択して、ベータ機能を表示します。

ステップ 3 [Data Accuracy Tool] タイルをクリックします。
ロケーション チューニングのページが表示されます。

ステップ 4 ドロップダウン リストからキャンパス名を選択します。

ステップ 5 ドロップダウン リストからビルディング名を選択します。

ステップ 6 ドロップダウン リストからビルディングのフロアを選択します。

ステップ 7 [Show Map] をクリックします。
フロア マップが表示されます。

ステップ 8 [Inside Training] をクリックします。

ステップ 9 フロアに描かれた境界領域内でローミングするデバイスの MAC アドレスをカンマ区切りで入力します。

ステップ 10 [Start Data Collection] をクリックし、境界領域内にあるデバイスのデータの収集を開始します。
モデルの作成には、データを 100% 以上収集する必要があります。100% とは、フロアの各稼働 AP ごとに 20 RSSI 以上の値があることを表します。

ステップ 11 [Outside Training] をクリックします。

ステップ 12 フロアに描かれた領域外でローミングするデバイスの MAC アドレスをカンマ区切りで入力します。

ステップ 13 [Start Data Collection] をクリックし、境界領域外にあるデバイスのデータの収集を開始します。
モデルの作成には、データを 100% 以上収集する必要があります。この 100% はトレーニング データ内も考慮されています。

ステップ 14 収集したデータに基づいてモデルを作成するには、[Create Model] をクリックします。

[Create Model] ボタンを有効にするには、データを 100% 収集したら、データ収集を停止する必要があります。収集データをすべて削除するには、[Delete Data] をクリックします。

RSSI 最大しきい値に基づくデバイスのフィルタリング

デバイスをフィルタリングするには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 [admin] > [Enable Beta Features] の順に選択して、ベータ機能を表示します。

ステップ 3 [Data Accuracy Tool] タイルをクリックします。

ステップ 4 [Device Filters] タブをクリックします。

ステップ 5 ドロップダウン リストからビルディング名を選択します。

ステップ 6 ドロップダウン リストからビルディングのフロアを選択します。

ステップ 7 フロアのゾーンを選択します。

ステップ 8 レポート ドロップダウン リストから RSSI 最大しきい値を選択します。

ステップ 9 選択したゾーンで使用可能なデバイスの MAC アドレスをカンマ区切りで入力します。

ステップ 10 RSSI しきい値を選択します。

ステップ 11 [View] をクリックします。
データを表示するまでに最大 10 分間かかる場合もあります。

デバイスの RSSI レポートを表示できるようになります。

固定デバイスと MAC アドレスに基づくデバイスのフィルタリング

デバイスをフィルタリングするには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。
ステップ 2 [admin] > [Enable Beta Features] の順に選択します。
ステップ 3 [Data Accuracy Tool] タイルをクリックします。
ステップ 4 [Device Filters] タブをクリックします。
ステップ 5 ドロップダウン リストからビルディング名を選択します。
ステップ 6 ビルディングのフロアを選択します。
ステップ 7 フロアのゾーンを選択します。
ステップ 8 レポート ドロップダウン リストから [Stationary Devices] と [MAC Addresses] を選択します。
ステップ 9 選択したゾーンで使用可能なデバイスの MAC アドレスをカンマ区切りで入力します。
ステップ 10 期間を選択します。
ステップ 11 [View] をクリックします。
特定したデバイスの MAC アドレスを表示できるようになります。
これにより、固定デバイスのレポートをダウンロードできます。

システムとネットワークの健全性のモニタリング

健全性ダッシュボードの表示

固有の Mobility Services Engine の健全性ダッシュボードを表示するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
ステップ 2 設定する Mobility Services Engine の名前をクリックします。
ステップ 3 MSE 管理 UI ホームページから [Health] タイルをクリックします。
ステップ 4 [Application Statistics] > [Health Dashboard] の順に選択します。
CPU、システム メモリ、ディスク容量、分析 CPU、分析メモリ、CAS CPU、および CAS メモリの使用率を表示できます。

CAS 遅延統計の表示

固有の Mobility Services Engine の CAS 統計情報を表示するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

ステップ 3 MSE 管理 UI ホームページから [Health] タイルをクリックします。

ステップ 4 [Application Statistics] > [CAS Latency Statistics] の順に選択します。
CAS 遅延統計、CAS キュー遅延、および CAS 計算時間を表示できるようになります。

通知統計情報の表示

固有の Mobility Services Engine の通知の統計情報を表示するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

ステップ 3 MSE 管理 UI ホームページから [Health] タイルをクリックします。

ステップ 4 [Application Statistics] > [Notification Statistics] の順に選択します。
次の表に、[Notification Statistics] ページのフィールドを示します。

フィールド	説明
Destination Summary	
Total Destinations	Destinations の合計数。
Unreachable Destinations	到達不能宛先の数。
Statistics Summary	
Host Address	通知送信先の宛先 IP アドレス。
Port	通知送信先の宛先ポート。
Destination Type	宛先のタイプ。例：SOAP_XML。
Status（ステータス）	宛先デバイスのステータス。ステータスは [Up] または [Down] です。

フィールド	説明
Last Sent	最終通知が宛先デバイスに送信された日時。
Last Failed	通知に失敗した日時。
Track Definition（ステータス）	トラック定義は、[Northbound] または [CAS event notification] です。
Total Count	宛先に送信された通知の合計数。宛先デバイスの通知統計詳細情報を表示するには、カウント リンクをクリックします。

動態統計の表示

固有の Mobility Services Engine の動態統計情報を表示するには、以下のステップに従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

ステップ 3 MSE 管理 UI ホームページから [Health] タイルをクリックします。

ステップ 4 [Application Statistics] > [Vital Statistics] の順に選択します。
特定期間の動態統計情報をグラフで表示できます。

第 9 章

MSE システム設定とサービスの構成

- 一般プロパティの表示とサービスの有効化，195 ページ
- ダッシュボードの表示，198 ページ
- ライセンスの表示と追加，199 ページ
- システムのアクティブ セッションの表示，199 ページ
- トラップ宛先の追加，200 ページ
- トラップ宛先の削除，202 ページ
- 詳細パラメータ設定の表示，202 ページ
- 詳細パラメータの設定，202 ページ
- システムの再起動またはシャットダウン，203 ページ
- システム データベースの消去，204 ページ
- ロギング オプションの設定，204 ページ
- ログ ファイルのダウンロード，205 ページ

一般プロパティの表示とサービスの有効化

一般プロパティを表示し、MSE サービスを有効にするには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

ステップ 3 左側サイドバー メニューから [System] > [General Properties] の順に選択します。
[General Properties] ページが表示されます。この表に、[General Properties] ページのフィールドを示します。

表 *24* : *[General]* タブ

フィールド	設定オプション
モデル	MSE のモデル詳細。
ビルド	MSE 上で実行されているソフトウェアのバージョン。
UDI	デバイス UDI（Unique Device Identifier）ストリングは二重引用符で囲まれています（ストリングの末尾にスペースがある場合はスペースも含まれます）。
IP Address	Mobility Services Engine の IP アドレスを示します。
Hostname	ホスト名。

フィールド	設定オプション
Mobility Services	Mobility Services Engine 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。サービスには、Context Aware、wIPS、Mobile Concierge、CMX Analytics、CMX Browser Engage、Proxy サービスが含まれます。 CAS を選択すると、クライアント、不正アクセス ポイント、干渉、有線クライアント、およびタグを追跡できます。 タグを追跡するには、次のいずれかのエンジンを選択します。 • Cisco Tag Engine または • Partner Tag Engine （注） Partner Tag Engine は、タグ追跡にのみ使用します。クライアントは、引き続き Cisco Context-Aware Engine によって追跡されます。 （注） 選択すると、サービスは [Up]（アクティブ）として表示されます。アクティブでないサービスはすべて、選択された（現行）システム上およびネットワーク上で [Down]（非アクティブ）として表示されます。 （注） リリース 7.5 以降は、wIPS サービスが同一 MSE 上の CAS と wIPS をサポートしないため、専用の MSE が必要になります。 現在のシステムで割り当て可能なデバイスの数を確認するには、[here] リンクをクリックします。 ネットワーク上のすべての Mobility Services Engine のライセンスの詳細を表示するには、[License Center] ページで、左側のサイドバーのメニュー オプションから [MSE] を選択します。 （注） ライセンスの購入およびインストールの詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html
Current Server Time	サーバの現在の時刻。
Server Time Zone	サーバが配置された場所の現在のタイム ゾーン。
Server Start Time	サーバが起動された起動時刻を示します。
Server Restarts	サーバが再起動する回数。
Maximum Memory (MB)	MSE にインストールする最大メモリ。

フィールド	設定オプション
Allocated Memory (MB)	MSE で使用可能な最大メモリ。
Used Memory (MB)	MSE で使用されている最大メモリ。
DB Disk Usage (GB)	MSE データベース ディスクのデータ量。
CAS Element Limit (licensed)	MSE が追跡のライセンスを付与された要素（クライアント、タグ、干渉など）の数。
Current Active Element Count	MSE が現在追跡している要素（クライアント、タグ、干渉など）の数。
Elements not tracked due to limiting	MSE のライセンス制限を超える要素の数。

ステップ 4 [Save] をクリックして、Prime Infrastructure データベースと Mobility Services Engine データベースを更新します。

ダッシュボードの表示

ダッシュボードを表示するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

ステップ 3 [System] > [Dashboard] の順に選択します。
ダッシュボードで次の詳細を表示できるようになります。

- アクティブ クライアントの数
- メモリ使用率のパーセンテージ
- CPU 使用率のパーセンテージ
- 通知先
- MAC フィルタリング ステータス：有効化または無効化
- クライアント ロケーションの履歴：有効化または無効化
- ロケーションの計算遅延

- 使用ライセンスのタイプ
- 同期済みコントローラの数

ライセンスの表示と追加

ライセンスを表示して MSE に追加するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

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

ステップ 4 [License] ページには、次の情報が表示されます。

フィールド	説明
タイプ	サービスのタイプ。
Platform Limit	Platform Limit
Installed Limit	MSE 上でライセンス付与されたクライアント要素の合計数を表示します。
License Type	3 つの異なるタイプのライセンス。永久、評価、および拡張があります。

ステップ 5 [Select File] をクリックし、ライセンス ファイルを参照します。

ステップ 6 [Add] をクリックし、MSE にライセンスを追加します。

システムのアクティブ セッションの表示

Mobility Services Engine のアクティブなユーザ セッションを表示できます。

アクティブなユーザ セッションを表示するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

ステップ 3 [System] > [Active Sessions] の順に選択します。
Prime Infrastructure は各セッションに関する次の情報を表示します。

- セッション ID
- MSE アクセス元の IP アドレス
- 接続ユーザのユーザ名
- セッションが開始された日時
- MSE が最後にアクセスされた日時
- 最終アクセス以降セッションがアイドルになっていた期間

トラップ宛先の追加

トラップ宛先を追加するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

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

ステップ 4 [Add Trap Destination] をクリックします。
次の表は、[Trap Destination] ページのフィールドを示しています。

表 *25* : *[Add Trap Destination]* ページのフィールド

フィールド	説明
IP Address	トラップ宛先の IP アドレス。
ポート	トラップ宛先のポート番号。デフォルト ポート番号は、162 です。
Community	トラップ宛先の SNMP コミュニティ ストリング。

フィールド	説明
Destination Type	このフィールドは編集できず、値 [Other] が表示されます。
SNMP Version	[SNMP Version] ドロップダウン リストから [v2c] または [v3] を選択します。
SNMP バージョンとして v3 を選択した場合にだけ表示されるフィールドを以下に示します。	
ユーザ名	SNMP バージョン 3 のユーザ名。
Security Name	SNMP バージョン 3 のセキュリティ名。
Authentication Type	ドロップダウン リストから、次のいずれかのオプションを選択します。 **HMAC-MD5** **HMAC-SHA**
Authentication Password	SNMP バージョン 3 の認証パスワード。
Privacy Type	ドロップダウン リストから、次のいずれかのオプションを選択します。 **CBC-DES** **CFB-AES-128** **CFB-AES-192** **CFB-AES-256**
Privacy Password	SNMP バージョン 3 のプライバシー パスワード。

（注） 自動的に作成されるデフォルトのトラップ宛先を除き、すべてのトラップ宛先はその他として識別されます。

ステップ 5 [Save] をクリックします。
[Trap Destination Summary] ページが表示され、新たに定義されたトラップがリストされます。

トラップ宛先の削除

トラップ宛先を削除するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。
ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。
ステップ 3 [System] > [Trap Destinations] の順に選択します。
ステップ 4 削除するトラップ宛先エントリに対応する [Delete] アイコンをクリックします。
ステップ 5 表示されるダイアログボックスで、[OK] をクリックして削除を実行します。

詳細パラメータ設定の表示

Mobility Services Engine の詳細パラメータ設定を表示するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。
ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。
ステップ 3 [System] > [Advanced Parameters] の順に選択します。[Advanced Parameters] ページが表示されます。

詳細パラメータの設定

詳細パラメータを設定するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。
ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。
ステップ 3 左側のサイドバーのメニューから、[System] > [Advanced Parameters] の順に選択します。
ステップ 4 必要に応じて詳細パラメータを確認または変更します。

- ◦ [Number of Days to keep Events]：ログを維持する日数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。
  ◦ [Session Timeout]：セッションがタイムアウトになるまでの分数を入力します。モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。現時点では、このオプションは淡色表示されます。

- Advanced Commands
  - [Reboot Hardware]：モビリティ サービス ハードウェアを再起動する場合にクリックします。詳細については、システムの再起動またはシャットダウン，（54 ページ）を参照してください。
  - [Shutdown Hardware]：モビリティ サービス ハードウェアをオフにする場合にクリックします。詳細については、システムの再起動またはシャットダウン，（54 ページ）を参照してください。
  - [Clear Database]：モビリティ サービス データベースをクリアする場合にクリックします。詳細については、システム データベースの消去，（54 ページ）を参照してください。Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除するには、[Retain current service assignments in the Prime Infrastructure] チェックボックスをオフにします。[Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。デフォルトでは、このオプションが選択されています。

ステップ 5 [Save] をクリックして、Prime Infrastructure データベースと Mobility Services Engine データベースを更新します。

システムの再起動またはシャットダウン

Mobility Services Engine を再起動またはシャットダウンするには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

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

ステップ 4 [Advanced Commands] グループ ボックスで、該当するボタン（[Reboot Hardware] または [Shutdown Hardware]）をクリックします。
確認のダイアログボックスで [OK] をクリックして、再起動またはシャットダウン プロセスを開始します。プロセスを中止するには、[Cancel] をクリックします。

システム データベースの消去

Mobility Services Engine 設定をクリアし、出荷時の初期状態に戻すには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

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

ステップ 4 [Advanced Commands] グループ ボックスで [Clear Database] をクリックします。

ステップ 5 [OK] をクリックし、Mobility Services Engine データベースをクリアします。

ロギング オプションの設定

Prime Infrastructure を使用して、ログに記録するメッセージのタイプとログ レベルを指定できます。

ロギング オプションを設定するには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

ステップ 3 [System] > [Logging] の順に選択します。選択されている Mobility Services Engine のロギング オプションが表示されます。

ステップ 4 [Logging Level] ドロップダウン リストから適切なオプションを選択します。
ロギング オプションは、[Off]、[Error]、[Information]、および [Trace] の 4 つです。

ログ レベルが [Error] またはこれよりも上のレベルに設定されているログ レコードはすべて、新しいエラー ログ ファイル locserver-error-%u-%g.log に記録されます。これは、ロケーション サーバの locserver-%u-%g.log ログ ファイルとともに維持される追加のログ ファイルです。このエラー ログ ファイルには、[Error] レベルのログとそのコンテキスト情報が記録されます。コンテキスト情報には、当該エラーよりも前の 25 ログ レコードが含まれています。最大 10 のエラー ログ ファイルを維持できます。各ログ ファイルの最大許容サイズは 10 MB です。

注意 Cisco Technical Assistance Center（TAC）担当者から [Error] と [Trace] のみ使用するように指示があった場合は、その指示に従います。

ステップ 5 イベントのロギングを開始する各要素の隣にある [Enabled] チェックボックスをオンにします。

ステップ 6 [Advanced Parameters] の [Enable] チェックボックスをオンにして、詳細デバッグを有効にします。デフォルトでは、このオプションは無効になっています。

注意 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

ステップ 7 サーバからログ ファイルをダウンロードするには、[Download Logs] をクリックします。詳細については、ログ ファイルのダウンロードを参照してください。

ステップ 8 [Log File] グループ ボックスに、以下の情報を入力します。

- Mobility Services Engine で維持するログ ファイルの数。Mobility Services Engine で維持できるログ ファイルの数は 5 ～ 20 です。
- 最大ログ ファイル サイズ（MB 単位）。ログ ファイルのサイズは 10 ～ 50 MB です。

ステップ 9 [MAC Address Based Logging] ページで、次の手順を実行します。

- [Enable] チェックボックスをオンにし、MAC アドレス ロギングを有効にします。デフォルトでは、このオプションは無効になっています。
- ロギングを有効にする 1 つ以上の MAC アドレスを追加します。また、以前に追加した MAC アドレスを削除できます。削除するには、リストから MAC アドレスを選択して [Remove] をクリックします。

  MAC アドレス ベースのロギングの詳細についてはMAC アドレスに基づくロギングを参照してください。

ステップ 10 [Save] をクリックして変更を適用します。

ログ ファイルのダウンロード

Mobility Services Engine ログ ファイルを解析する必要がある場合は、Prime Infrastructure を使用してログ ファイルをシステムにダウンロードできます。Prime Infrastructure ではログ ファイルを含む .zip ファイルがダウンロードされます。

ログ ファイルが含まれている .zip ファイルをダウンロードするには、以下のステップに従います。

ステップ 1 MSE 管理 UI を起動します。

ステップ 2 ホームページの右上で、[Configuration] アイコンをクリックします。

ステップ 3 [System] > [Logging] の順に選択します。

ステップ 4 [Download Logs] をクリックします。

ステップ 5 [File Download] ダイアログボックスの指示に従い、ファイルを表示するか、または .zip ファイルをシステムに保存します。

付 録 A

wIPS ポリシー アラーム リファレンス

- セキュリティ IDS/IPS の概要，207 ページ
- 侵入検知：DoS 攻撃，219 ページ
- 侵入検知：セキュリティ突破，235 ページ
- パフォーマンス違反，260 ページ

セキュリティ IDS/IPS の概要

企業環境に WLAN を追加すると、ネットワーク セキュリティに対する新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無認可のユーザに公開する可能性があります。個人の使用のために従業員によって設置された不正アクセス ポイントは通常、企業のセキュリティ ポリシーに準拠していません。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正アクセス ポイントの脅威以外にも、アクセス ポイントの設定ミスや未設定、DoS（サービス拒否）攻撃といったさまざまなワイヤレス セキュリティ リスクや侵入の可能性が存在します。

Cisco Adaptive Wireless IPS（wIPS）は適切なセキュリティ設定を検証し、侵入攻撃の可能性を検出することで、セキュリティの脅威への対処を支援します。wIPS は、包括的なセキュリティ モニタリング テクノロジー スイートを使用して、次のカテゴリ内の 100 件を超えるさまざまな脅威状況をユーザに警告します。

- ユーザ認証とトラフィック暗号化
- 不正デバイスとアドホック モード デバイス
- 設定の脆弱性
- 侵入検知（セキュリティ突破）
- 侵入検知（DoS 攻撃）
- パフォーマンス違反

wIPSの機能を最大限に活用するために、セキュリティ導入ポリシーに最も適したものになるようにセキュリティ アラームをカスタマイズできます。たとえばWLANの導入時に特定ベンダーのアクセスポイントを導入する場合、そのアクセスポイントまたはセンサーによって別のベンダーのアクセス ポイントが検出されると不正アクセス ポイント アラームを生成するように製品をカスタマイズできます。

ユーザ認証と暗号化

WLANセキュリティの防御の中心となる要素は、ユーザ認証とワイヤレス トラフィックの暗号化です。バックエンドのRADIUSサーバを使用したIEEE 802.1xの標準に基づく集中型WLANユーザ認証は、柔軟で高機能なメカニズムです。また、VPNなどの他の認証方式も同様の目的で使用できます。

ユーザ認証は、有線およびワイヤレス リソースへの不正なアクセスを遮ります。ユーザ認証と組み合わせてトラフィック暗号化を行い、その間に暗号化された秘密データがAPと認可されたユーザ間で交換されます。トラフィック暗号化は、侵入者がワイヤレス トラフィックを傍受することを防止します。Cisco wIPSは、認証トランザクションおよびトラフィック暗号化方法を、（Cisco wIPSポリシー設定に）指定されたセキュリティ導入ポリシーに照らして監視することで、WLANのセキュリティ展開を評価します。たとえば、Cisco wIPSは、**802.1x EAP** タイプの **PEAP** が企業の標準認証プロトコルの場合、「**PEAP によって保護されていないデバイス**」アラームを発生します。このカテゴリ（認証および暗号化）の一般的なセキュリティ違反には、設定ミス、更新されていないソフトウェア/ファームウェア、企業セキュリティ ポリシーの不十分な規定などが含まれます。Cisco wIPSはこれらの問題を管理者に通知し、対策を講じることができます。

ユーザ認証および暗号化には、次の2つのサブカテゴリがあります。

静的 WEP 暗号化

静的WEP暗号化は、1999年にIEEE 802.11標準で指定されました。セキュリティを重視するWLAN向けの暗号化手法には、WPA （Wireless Protected Access - TKIPおよび802.1x）および802.11iといった別の手段があります。

統計によると、WLANの50%以上が暗号化方式をまったく導入していません。WEPには潜在的な脆弱性があっても、暗号化が皆無よりは安全です。静的WEPの使用を決めた場合、WEPによるセキュリティを可能な限り維持する方法があります。Cisco wIPSはその実現を支援するために、静的WEPの使用率を監視し、解読可能なWEPキーの使用や共有キー認証などのセキュリティホールを特定し、WEPを使用しないデバイスを検出する各種機能を備えています。

静的WEP暗号化には次のタイプがあります。

暗号化が無効な AP

アラームの説明と考えられる原因

Cisco wIPSは **WEP、TKIP、 AES** など、 WLANレイヤ2データ暗号化機能なしで動作するすべてのAPを管理者に警告します。レイヤ3以上で使われるVPNテクノロジーは、WLANレイヤ2データ暗号化メカニズムの代わりに最も一般的に使用されています。いずれの暗号化メカニズム

も使用しない場合、APとそのクライアントステーション間で交換されるデータは、侵入者によって盗聴される可能性があります。暗号化メカニズムを何も使用していない AP では、暗号キーを持たない不正なクライアントが AP とアソシエートして企業の有線ネットワークにアクセスできる場合もあります。これは、ユーザのプライバシーをリスクに晒すと同時に、社内の有線ネットワークへのアクセスを公開してしまうことも考えられます。このアラームは、企業のゲストWLANネットワーク、または暗号不要のホットスポット展開に対してはオフにできます。Publicly Secure Packet Forwarding（PSPF は基本的に Cisco Aironet アクセス ポイントでの呼び方です。異なる呼び方を使う他のベンダーもあります）アラームをオンにして、暗号なしに運用されるワイヤレス ネットワークを保護できます。PSPF はワイヤレス クライアント同士の通信を無効にする機能であり、WLAN アクセス ポイントに実装されています。PSPF は、ワイヤレス クライアント間のワイヤレス トラフィックを禁止することで、パブリック ネットワークを保護します。

wIPS による解決

Cisco wIPS は、他のワイヤレス クライアントと通信しているワイヤレス クライアントを検出し、Publicly Secure Packet Forwarding（PSPF）違反の可能性について管理者に警告します。ほとんどの WLAN 環境では、ワイヤレス クライアントは主に有線ネットワーク上の Web サーバなどのデバイスとだけ通信します。アクセス ポイントの PSPF 機能を有効にすることで、管理者はワイヤレス クライアントを他のワイヤレス侵入者からハッキングされないように保護できます。PSPF は、特に空港、ホテル、喫茶店、大学構内など、認証がなく誰もがアクセス ポイントにアソシエートできるワイヤレス パブリック ネットワーク（ホットスポット）に導入する場合に効果的です。PSPF 機能により、クライアント デバイスが誤ってワイヤレス ネットワーク上の他のクライアント デバイスとファイルを共有することを防止できます。

暗号化が無効なクライアント

アラームの説明と考えられる原因

Cisco wIPS は WEP、TKIP、AES など、WLAN レイヤ 2 データ暗号化機能なしで動作するクライアント ステーションに関して管理者に警告します。レイヤ 3 以上で使われる VPN テクノロジーは、WLAN レイヤ 2 データ暗号化メカニズムの代わりに最も一般的に使用されています。いずれの暗号化メカニズムも使用しない場合、APとそのクライアントステーション間で交換されるデータは、侵入者によって盗聴される可能性があります。WEPを無効にしたクライアントは、社外秘情報を含む場合もあるそのファイル システムを、ワイヤレス侵入者による危険にさらします。このようなクライアントは、侵入者が企業ネットワークへのエントリ ポイントとして利用できるようになります。このアラームは、企業のゲストWLANネットワーク、または基本的に暗号不要のホットスポット展開に対してはオフにできます。PSPF（Publicly Secure Packet Forwarding、基本的に Cisco Aironet アクセス ポイントでの呼び方で、異なる呼び方を使う他のベンダーもあります）アラームをオンにして、暗号なしに運用されるワイヤレス ネットワークを保護できます。PSPF はワイヤレス クライアント同士の通信を無効にする機能であり、WLAN アクセス ポイントに実装されています。

wIPS による解決

Cisco wIPS は、他のワイヤレス クライアントと通信しているワイヤレス クライアントを検出し、PSPF 違反の可能性を管理者に警告します。ほとんどの WLAN 環境では、ワイヤレス クライアントは主に有線ネットワーク上のWebサーバなどのデバイスとだけ通信します。アクセス ポイントの PSPF 機能を有効にすることで、管理者はワイヤレス クライアントを他のワイヤレス侵入者か

らハッキングされないように保護できます。PSPF は、特に空港、ホテル、喫茶店、大学構内など、認証がなく誰もがアクセスポイントにアソシエートできるワイヤレスパブリック ネットワーク（ホットスポット）に導入する場合に効果的です。PSPF 機能により、クライアント デバイスが誤ってワイヤレス ネットワーク上の他のクライアントデバイスとファイルを共有することを防止できます。

クラック可能な WEP IV キーの使用

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは WEP キー クラッキング攻撃に対して脆弱です。攻撃者によって WEP 秘密キーがクラックされると、暗号化による保護がなくなり、結果としてデータ プライバシーが侵害されます。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）に結合される秘密キーで構成され、64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。送信ステーションが決定する IV を頻繁に再利用したり、連続するフレームで再利用したりできるので、ワイヤレス侵入者がこの秘密キーを復元できる可能性が高まります。「脆弱なキー」を作成する特定の IV 値を除外することにより、WEP の脆弱性を回避できます。

wIPS による解決

Cisco wIPS は弱い WEP 実装について警告し、IV 使用の問題を訂正するためのデバイス ファームウェアアップグレードがデバイスベンダーからリリースされている場合はこのアップグレードを推奨します。企業 WLAN ネットワークで TKIP（Temporal Key Integrity Protocol）暗号化メカニズムを使用して WEP の脆弱性を保護することが理想的です。TKIP はほとんどのエンタープライズ レベル ワイヤレス装置でサポートされています。TKIP 対応デバイスはこのような WEP キー攻撃の対象となりません。

オープン認証を使用するデバイス

アラームの説明と考えられる原因

802.11 オープン認証は現在（共有キー認証とは対照的に）、802.1x などの高度な認証プロトコルと組み合わせて広く使用され、WLAN セキュリティに貢献しています。構成によっては、静的 WEP キーが AP にアソシエートしようとするクライアント ステーションのチャレンジのために使用される場合に、共有キー認証がオープン認証の代わりに使用されています。他方、オープン認証ではどのクライアントからのアソシエーションも受け入れられ、クライアントの ID 検証はありません。共有キー認証はセキュリティが高いと考えられがちですが、ワイヤレス侵入者による WEP キーのクラックに対して脆弱なことが判明しています。これは、チャレンジテキストと応答が両方ともクリアで暗号化されていないからです。

wIPS による解決

802.11 オープン認証は、802.1x/EAP フレームワークまたは VPN など、より高度な認証メカニズムとともに使用することが推奨されます。共有キー認証など、オープン認証以外の方式を採用する場合に、このアラームを有効にできます。Cisco wIPS は、オープン認証は使用しないことを定めた構成ポリシーに違反するデバイスについての警告を通知します。

共有キー認証を使用するデバイス

アラームの説明と考えられる原因

IEEE 802.11 標準により設計された共有キー認証プロトコルは、静的 WEP キー暗号化とともに機能して、未認証の WLAN デバイスを AP またはアドホック ステーションとのアソシエーションからロックアウトします。共有キー認証は、802.11 クライアントとアクセス ポイント間の認証に、標準のチャレンジおよび応答の手法を使用します。チャレンジ テキストは暗号化されないクリアテキストです。チャレンジ応答のアルゴリズム（共有秘密キーでない）は、標準で一般的な知識として共有されています。共有キー認証は、傍受によるパッシブな攻撃で容易に悪用されることが判明しています。攻撃者は総当たりを使用して、クリアテキストのチャレンジテキストをキャプチャした後に、チャレンジ応答をオフラインで計算できます。一致が見つかれば、攻撃者は共有秘密キーを取得したことになります。

wIPS による解決

Cisco wIPS は、共有キー認証の使用を検出し、別の認証方式を助言します。現在、802.11 WLAN を展開する多くの企業は、共有キー認証の代わりに、802.1x および EAP 方式による LEAP、PEAP、TLS などのより高度な認証メカニズムとオープン認証を組み合わせて使用しています。

WEP IV キーの再利用

アラームの説明と考えられる原因

攻撃者によって WEP 秘密キーがクラックされると、暗号化による保護がなくなり、結果としてデータ プライバシーが侵害されます。WEP キーは、ユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーで構成され、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。送信ステーションが決定する IV を頻繁に再利用したり、連続するフレームで再利用したりできるので、ワイヤレス侵入者がこの秘密キーを復元できる可能性が高まります。

wIPS による解決

Cisco wIPS は弱い WEP 実装について警告し、IV 使用の問題を訂正するためのデバイス ファームウェア アップグレードがデバイス ベンダーからリリースされている場合はこのアップグレードを推奨します。企業 WLAN ネットワークで TKIP（Temporal Key Integrity Protocol）暗号化メカニズムを使用して WEP の脆弱性を保護することが理想的です。TKIP はほとんどのエンタープライズ レベル ワイヤレス装置でサポートされています。TKIP 対応デバイスはこのような WEP キー攻撃の対象となりません。

WPA および 802.11i

Wi-Fi アライアンスが公開した Wireless Protected Access（**WPA**）仕様は、IEEE **802.11i** 標準のサブセット機能を指定するものです。WPA は、元の IEEE 802.11 仕様で特定されている静的 WEP のよく知られた脆弱性に対する回答です。ほとんどのワイヤレス ベンダーは **WPA** をサポートし、静的 **WEP** に代わるより安全な方式と考えています。

WPA 製品には、エンド ユーザにとって 3 つの主なメリットがあります。

- **802.1x** では、脆弱なグローバル暗号キー方式の代わりに、ユーザ単位の認証が可能です。
- Temporal Key Integrity Protocol（**TKIP**）は、動的なキー生成によって暗号化を業務用に強化しています。
- 事前共有マスター キー（**PMK**）は、中小規模の展開によって、**RADIUS** などの複雑なインフラストラクチャ バックエンド サーバなしで **802.1x** および **TKIP** を使用できます。

wIPS サーバは、**WPA** のトランザクションをモニタし、不順守デバイスと脆弱な設定を検出すると管理者に警告します。

WPA および 802.11i には次のタイプがあります。

EAP-TTLS によって保護されていないデバイス

アラームの説明と考えられる原因

Extensible Authentication Protocol（EAP）は、802.11 トランザクションの暗号化を強化する手段を提供する、基本的なセキュリティ フレームワークです。このフレームワークは、Tunneled Transport Layer Security（TTLS）と呼ばれるバージョンなど、さまざまなタイプの認証メカニズムと組み合わせることができます。EAP-Tunneled Transport Layer Security（EAP-TTLS）は、Transport Layer Security（TLS）を拡張した EAP プロトコルです。EAP-TTLS のセキュリティは EAP-TLS と同等に強力であり、しかもクライアントで証明書を発行する必要はありません。パスワードでユーザ認証を行う点は変わりませんが、資格情報はトンネリングされます。TTLS 認証メカニズムではなく EAP プロトコルを使用するように設定されているデバイスでは、ワイヤレス ネットワーク接続のセキュリティが低下する可能性があります。これらは、エンド ユーザが素早く接続するための容易なメカニズムですが、反面ワイヤレスの攻撃者が重要な企業データにアクセスできるようになります。TTLS 認証で保護されていない EAP 交換情報は、攻撃者が容易に傍受して復号できるので、有効なユーザから送信される機密データの漏洩の原因になります。

wIPS による解決

Cisco wIPS は、EAP トランザクションをモニタし、EAP-TTLS メカニズムを実装していないデバイスを検出して、管理者に脆弱性を知らせるためにアラームをトリガーします。AirWISE 画面に表示されるアラームのテキストには、問題のあるデバイスと、使用中の別の認証メカニズムが表示されます。IT 担当者がアラーム発生元のデバイスを特定し、EAP-TTLS メカニズムを使用するように設定することが推奨されます。

802.1X によって保護されていないデバイス

アラームの説明と考えられる原因

WLAN セキュリティ構成が認証と暗号化のために 802.1x を使用する必要がある場合、Cisco wIPS は 802.1x 保護を使用するように設定されていないデバイスについて警告します。Wireless Protected Access（**WPA**）は、要件の 1 つとして 802.1x を指定しています。802.1x フレームワークでは、一元的なユーザ認証および暗号キー管理を行います。802.1x は、Lightweight Extensible Authentication Protocol（**LEAP**）、Transport Layer Security（**TLS**）、Tunneled Transport Layer Security（**TTLS**）、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（**EAP-FAST**）、Protected Extensible Authentication Protocol（**PEAP**）など、さまざまな Extensible Authentication Protocol（**EAP**）

と使用され、認証と暗号化メカニズムを実装します。WLAN セキュリティが WPA または 802.1x に依存する場合、802.1x は、非正規のユーザを誤って認証し有線ネットワークへのアクセスを許可することで、WLAN のセキュリティを弱めます。802.1x 保護なしで正しく設定されていないクライアント ステーションも、セキュリティ リスクを誘引します。たとえば、802.1x フレームワークが備える相互認証メカニズムがないので、誤って侵入者の偽 AP とアソシエートする危険性があります。

wIPS による解決

Cisco wIPS は、**PEAP、TLS、TTLS、LEAP、EAP-FAST** などすべての 802.1x **EAP** タイプを認識し、802.1x によって保護されていない AP とクライアント ステーションを、拒否された 802.1x 認証チャレンジを監視することで検出します。

選択した認証方式によって保護されていないデバイス

アラームの説明と考えられる原因

Cisco wIPS は、802.1x トランザクションとそれらに固有の各 Extensible Authentication Protocol（EAP）方式をモニタします。固有の EAP 方式を使用しない場合、Cisco wIPS はアラームを発生させます。Cisco wIPS は、次の EAP 方式でこのアラームをサポートします。

- [Leap]：これはシスコが開発した独自の EAP 方式です。 Cisco LEAP ソリューションには、セッションごとまたはユーザ キーに基づいて動的な相互認証と設定可能な WEP セッション キー タイムアウトが含まれています。
- [PEAP]：Protected Extensible Authentication Protocol、または Protected EAP と呼ばれます。暗号化および認証される Transport Layer Security（TLS）トンネルに EAP をカプセル化するプロトコルです。
- [EAP-TLS]： EAP-Transport Layer Security（EAP-TLS）。EAP-TLS メカニズムは、標準共有キーパスワード認証セッションに加えて、セッション単位で新しいキーを作成することでセキュリティをさらに強化します。
- [EAP-TTLS]：EAP-Tunneled Transport Layer Security（EAP-TTLS）は、TLS を拡張した EAP プロトコルです。EAP-TTLS のセキュリティは EAP-TLS と同等に強力であり、しかもクライアントで証明書を発行する必要はありません。パスワードでユーザ認証を行う点は変わりませんが、資格情報はトンネリングされます。
- [EAP-FAST]：シスコは、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling （EAP-FAST）プロトコルを開発しました。EAP-FAST では、クライアントとサーバ間に PAC（Protected Access Credential）を使用して相互認証するトンネルが作成されます。トンネル確立プロセスが完了したら、クライアントはユーザ名とパスワードのクレデンシャルを使用して認証されます。
- [EAP-MD5]：これは、最低限のセキュリティを可能にするパスワード ベースの認証方式です。EAP-MD5 は、EAP ピアから EAP サーバへの認証を行い相互認証は行わない点で、他の EAP 方法と異なります。

wIPS による解決

Cisco wIPS は、EAP トランザクションをモニタし、有効な認証方式を実装していないデバイスを検出して、管理者に脆弱性を知らせるためにアラームをトリガーします。AirWISE 画面のアラームのテキストには、問題のあるデバイスが表示されます。IT 担当者がアラーム発生元のデバイスを特定し、正しい認証方式を使用するように設定することが推奨されます。

802.1 X 暗号化されていないブロードキャストまたはマルチキャスト

アラームの説明と考えられる原因

802.1x に含まれるフレームワークによって、システムでセッション単位の暗号キーを使用し、グローバルな静的 WEP キー メカニズムから引き継がれた脆弱性に対する防御を行えます。802.1x には、セッション単位の暗号キーがあり、さらにセッション キーのローテーション メカニズムを促進し、暗号キーの定期的な更新を保証します。このような機能によって、静的暗号キーの使用を廃止し、1 つの静的キーで暗号化された大量のデータを必要とする攻撃を防御することで、セキュリティを強化できます。複数の受信者が存在するマルチキャストおよびブロードキャスト パケットの場合、セッション単位の暗号化キーを適用できません。マルチキャストおよびブロードキャストの通信を保護するために、共有暗号キーとキー変更メカニズムを実装する必要があります。マルチキャストとブロードキャストの暗号キー メカニズムを正しく実装しているワイヤレス デバイスは、ほとんどないことが判明しています。実際には、マルチキャストおよびブロードキャスト パケットは暗号化されません。さらに状況を複雑にしているのは、複数の SSID をともなうエンタープライズ グレード AP が、1 つの SSID （企業 WLAN）用の 802.1X セキュリティによって実装され、別の SSID （ゲスト WLAN）の暗号化を使用していないことです。この導入シナリオは、通常、VLAN 設定と組み合わされるので、ゲスト SSID を使用するクライアント デバイスはインターネットのみにアクセスでき、社内の有線ネットワークにはアクセスできません。複数の SSID をサポートする AP はブロードキャストとマルチキャスト フレームを送信するので、暗号がオプション選択となり（802.1x または暗号化なし）実装を難しくします。

wIPS による解決

Cisco wIPS は、設定ミスまたはベンダー実装エラーにより暗号化されていないマルチキャスト フレームおよびブロードキャスト フレームを検出します。マルチキャスト フレームおよびブロードキャスト フレームの暗号化を適切な方法で実装した AP を使用することをお勧めします。

802.1 X キー再生成のタイムアウトが長すぎます

アラームの説明と考えられる原因

WEP 秘密キーがクラックされると、暗号化による保護がなくなり、結果としてデータ プライバシーが侵害されます。動的な暗号キーまたは TKIP（Temporal Key Integrity Protocol）などのキー ローテーション メカニズムは、シングル セッション内でも暗号キーを定期的に変更することによって、そのような脆弱性を解決します。マルチキャストおよびブロードキャスト トラフィックでのキー ローテーションの管理は、複数のデバイスを新しいキーに同期的に更新する必要があるので、技術的に難しい面があります。ベンダーのマルチキャストまたはブロードキャストのキー ローテーションの実装は、認証なしから完全な認証までさまざまです。マルチキャストおよびブロードキャスト キーのローテーションは皆無かごく稀なので、静的 WEP と同程度にセキュリティが弱く、キー復元攻撃の対象になります。WLAN 802.1x 認証と暗号化のトランザクションの継続的な監視によって、Cisco wIPS は、暗号キー ローテーションなしの設定またはキー ローテーショ

ンのタイムアウトが長い設定の AP を検出できます。WLAN 802.1x 設定には、合理的な暗号キー変更のタイムアウトを含めることが重要です。暗号キーが陳腐化すると暗号が静的になり、静的 WEP キー暗号化のように脆弱になります。キー変更のメカニズムは、ユニキャスト、マルチキャストおよびブロードキャストのデータ ストリームに適用する必要があります。TKIP が有効なデバイスは、WEP キー ハッシュ アルゴリズムを実装し、通常はユニキャスト データ ストリーム上でキー ローテーションを行いますが、マルチキャストまたはブロードキャストのデータ ストリームでは行いません。

wIPS による解決

Cisco wIPS アラームは、すべてのデータ ストリームのキー再生成メカニズムの適用に役立ちます。問題を解決するには、この設定について AP の構成をチェックするなど、適切な手段を講じてください。

EAP-TLS によって保護されていないデバイス

アラームの説明と考えられる原因

Extensible Authentication Protocol（EAP）は、802.11 トランザクションの暗号化を強化する手段を提供する、基本的なセキュリティ フレームワークです。このフレームワークは、証明書ベースのプロトコルである Transport Layer Security（TLS）と呼ばれるバージョンなど、幅広い各種の認証メカニズムと組み合わせて使用できます。EAP-TLS メカニズムは、標準共有キー パスワード認証セッションに加えて、セッション単位で新しいキーを作成することでセキュリティをさらに強化します。これは、EAP-TLS 認証を使用した AP へのアクティブな接続ごとに、その接続に固有の新しい共有キーが毎回生成されることを意味します。これにより、プロトコルがワイヤレス攻撃に対抗する力が、標準の共有キー メカニズムに比べて格段に高まります。TLS 認証メカニズムではなく EAP プロトコルを使用するように設定されているデバイスでは、ワイヤレス ネットワーク接続のセキュリティが低下する可能性があります。ネットワーク セキュリティが低いとはいえ EAP-TLS よりも便利な多くの代替メカニズム（EAP-TTLS や EAP-FAST など）があります。これらは、エンドユーザが素早く接続するための容易なメカニズムですが、反面ワイヤレスの攻撃者が重要な企業データにアクセスできるようになります。TLS 認証で保護されていない EAP 交換情報は、攻撃者が容易に傍受して復号できるので、有効なユーザから送信される機密データの漏洩の原因になります。

wIPS による解決

Cisco wIPS は、EAP トランザクションをモニタし、TLS メカニズムを実装していないデバイスを検出して、管理者に脆弱性を知らせるためにアラームをトリガーします。AirWISE 画面に表示されるアラームのテキストには、問題のあるデバイスと、使用中の別の認証メカニズムが表示されます。IT 担当者がアラーム発生元のデバイスを特定し、EAP-TLS メカニズムを使用するように設定することをお勧めします。

IEEE 802.11i/AES によって保護されていないデバイス

アラームの説明と考えられる原因

新しい 802.11i 標準には、3つの重要なネットワーク セキュリティ機能として、認証とプライバシーが含まれています。Cisco wIPS は、IEEE 802.11i 標準を使用していないデバイスを検出すると、警告を通知します。このセキュリティ標準を使用していないデバイスは、企業ネットワーク

のセキュリティを侵害するさまざまな攻撃に対して脆弱になる可能性があります。IEEE 802.11 標準は、その批准時に、セキュリティ標準として 64 ビット WEP キーの導入を提唱していました。その後、この提案は 128 ビット キーに引き上げられました。構成によっては、256 ビット WEP キーを使用するケースも見られました。それ以降、静的 WEP には、認証、暗号化、および整合性チェックに関して欠陥があることが判明しました。Wi-Fi アライアンスは、WEP に代わる認証方式の開発が重要であることを、即座に認識しました。IEEE 802.11i 標準は、企業ワイヤレス ネットワーク環境が直面していたすべてのセキュリティ問題を軽減するために導入されました。この標準は、Robust Secure Networks（RSN）を形成します。802.11i 標準批准の遅れを受けて、Wi-Fi アライアンスは IEEE 802.11i 標準のサブセットである、Wi-Fi Protected Access（WPA）を策定しました。WPA/802.11i はユーザ認証とキー配布用に 802.1x を実装しています。802.1x は、LEAP、TLS、TTLS、EAP-FAST、PEAP などさまざまな EAP （Extensible Authentication Protocol）タイプとともに使用され、認証と暗号化のメカニズムを実装します。IEEE 802.11i 標準では、認証方法の選択はユーザに委ねられます。

IEEE 802.11i 標準では、事前共有キー（PSK）機能および 802.1x サーバ ベースのキー管理方式に対応します。サーバ ベースのメカニズムには、セッション キー（Pairwise Master Key、PMK）を安全かつ動的に配布するために、RADIUS サーバなどの認証サーバが必要となります。802.1x の代わりにPSK を使用する場合、式を使用してパスフレーズ PSK を PMK に必要な 256-ビット値に変換します。PSK モードでは、802.11i で定義される 4-方向ハンドシェイクを暗号キー管理に使用して、は、 EAP 交換情報は使用しません。RADIUS サーバと EAP メソッド（EAP-TLS、LEAP）を使用しないため、 PSK モードのセキュリティは高くありません。IEEE 802.11i 標準で定義される暗号化規格には、Temporal Key Integrity Protocol（TKIP）と Advanced Encryption Standard-Counter Mode-CBC MAC Protocol の 2 つがあります。TKIP および MIC で暗号化された WLAN トラフィックは、パケット偽造攻撃およびリプレイ攻撃を撃退します。TKIP の最も重要な点は、静的 WEP キーとキー再利用に起因する攻撃から生まれる脆弱性に抵抗力があることです。MIC とともに、TKIP にはパケット単位のキー混合が含まれており、多くのキー攻撃の防御に役立ちます。

IEEE 802.11i 標準では、AES-CCMP の実装は必須です。IEEE 標準は、128-ビット AES のみをサポートします。AES は基本的に 128-ビット ブロックで機能するので、CCMP はデータ ブロックのビット サイズを増やすために必要なパディングを提供します。このパディングは暗号化の前に追加され、復号化後に廃棄されます。AES-CCMP モードでは、AES ブロック暗号を使用して認証と暗号化が行われます。CCMP は、データ プライバシーのためのカウンター（CTR）モード暗号化と、Cipher Block Chaining Message Authentication Code （CBC-MAC）認証（処理対象のデータ ブロックごとの認証-暗号セキュリティ プロセス）の組み合わせです。CCMP は、IEEE 802.11 ヘッダー長での CBC-MAC、IEEE 802.11 MAC Payload Data Unit（MPDU）ヘッダーの指定部分、平文 MPDU データを計算する一方、以前の IEEE 802.11 WEP メカニズムには MPDU ヘッダーの保護がありませんでした。もう1つ、CCMP の暗号化と複合化の両方で転送 AES ブロック暗号機能のみを使用し、コードとハードウェア両方のサイズを大幅に節約できます。

wIPS による解決

Cisco wIPS は、IEEE 802.11i 規格を使用しないためにワイヤレス ネットワーク セキュリティを侵害しているデバイスを検出します。Cisco wIPS は、ネットワークのセキュリティ ホールを回避するために適切な手段を講じ、より安全な IEEE 802.11i 規格を使用できるようにワイヤレス ネットワークのインフラストラクチャとデバイスをアップグレードすることを推奨します。このようなデバイスが Cisco wIPS によって特定、報告された場合、WLAN 管理者は Cisco wIPS Console にあるデバイス ロケータ機能を使用して、デバイスが不正なデバイスかどうかを判断できます。既知

のデバイスはモニタ対象のノードとしてマークされ、三角測量機能を使用して位置を確認できます。

EAP-FAST によって保護されていないデバイス

アラームの説明と考えられる原因

シスコは、辞書攻撃を阻止する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）プロトコルを開発しました。EAP-FAST は中間者攻撃、辞書攻撃、パケットおよび認証偽造攻撃を阻止します。EAP-FAST では、クライアントとサーバ間に PAC（Protected Access Credential）を使用して相互認証するトンネルが作成されます。トンネル確立プロセスが完了したら、クライアントはユーザ名とパスワードのクレデンシャルを使用して認証されます。EAP-FAST の主な利点には、この方式が独自仕様ではなく、IEEE 802.11i 標準に準拠し、TKIP と WPA をサポートすること、証明書を使用しないので複雑な PKI インフラストラクチャを回避できること、PC とポケット PC で複数のオペレーティング システムに対応することがあります。

wIPS による解決

Cisco wIPS は、802.1x 認証メカニズムを使用していても EAP-FAST プロトコルを使用していないデバイスについて、ワイヤレス管理者に警告します。EAP-FAST をワイヤレス環境に実装することが推奨されます。

PEAP によって保護されていないデバイス

アラームの説明と考えられる原因

Cisco wIPS は、**802.1x** トランザクションとそれらに固有の各 Extensible Authentication Protocol（**EAP**）タイプをモニタします。Protected EAP（**PEAP**）を認証方式として導入することで、802.1x セキュリティ認証プロトコルが Transport Layer Security（TLS）によってさらにラップされ保護されます。PEAP 内で動作する EAP 方式には、次のような利点が含まれています。

- ID 保護
- 辞書攻撃への対抗
- リプレイ攻撃からのネゴシエーション保護
- ヘッダーの保護
- パケット スプーフィング、フラッド、および DoS 攻撃からの終端保護
- フラグメンテーションおよび再アセンブリ
- 高速再接続
- 方式に依存せず定評あるキー管理

最近ではシスコなど多くの WLAN 機器ベンダーが、ファームウェア アップグレードにより新たに PEAP に対応しています。

wIPS による解決

この Cisco wIPS アラームは、Protected Extensible Authentication Protocol（**PEAP**）を使用していないデバイスの警告を通知します。PEAP認証方式がワイヤレス環境のさまざまなデバイスに実装されていることを確認してください。

TKIP によって保護されていないデバイス

アラームの説明と考えられる原因

最新の **IEEE 802.11i** 標準には、Temporal Key Integrity Protocol（**TKIP**）と Message Integrity Checksum（**MIC**）が、推奨されるデータ プライバシー プロトコルの 1 つとして含まれます。WiFi アライアンスは、同団体の Wireless Protected Access（**WPA**）仕様で **TKIP** と **MIC** を推奨しています**TKIP** および **MIC** で暗号化された WLAN トラフィックは、パケット偽造攻撃およびリプレイ攻撃を撃退します。**TKIP** には、静的 WEP キーとキー再利用に起因する攻撃から生まれる脆弱性に抵抗力があります。**MIC とともに、TKIP** にはパケット単位のキー混合が含まれており、多くのキー攻撃の防御に役立ちます。**AES** ベースの **CCMP** 暗号化とは異なり、TKIP にはハードウェア アップグレードが必要ありません。シスコなど多くの WLAN 機器ベンダーが、最新ファームウェア とドライバで新たに TKIP と MIC に対応しています。

wIPS による解決

Cisco wIPS は、TKIP 暗号化によって保護されていない WLAN トラフィックを検出し、警告を発生させます。Cisco wIPS は、これらのデバイスを最新のファームウェアに更新し、TKIP 暗号化を含むように再設定することを推奨します。

WPA または 802.11i 事前共有キーの使用

アラームの説明と考えられる原因

WPA および **802.11i** 標準では、IEEE 802.1x ベースのキー確立を使用する代わりとして、事前共有キー（**PSK**）のメカニズムを提供します。802.1x ベースのキー管理では、**RADIUS** サーバなどの認証サーバがセッション キー（ペアワイズ マスター キー、**PMK**）を安全かつ動的に配布する必要があります。802.1x の代わりに **PSK** を使用する場合、式を使用してパスフレーズ **PSK** を PMK に必要な 256-ビット値に変換します。**PSK** モードでは、802.11i で定義された 4-方向ハンドシェイクを暗号キー管理に使用して、**EAP** 交換情報は使用しません。**RADIUS** サーバと **EAP** メソッド（EAP-TLS、LEAP）を使用しないため、PSK モードのセキュリティは高くありません。**PSK** は、セキュリティの低下と引き換えに認証サーバ（RADIUS）のセットアップを不要にするために使用します。802.11i の仕様では、パス フレーズが 20 文字より少ない場合セキュリティが低いと見なせる可能性があることが示されています。これは、4 方向ハンドシェイクがキャプチャされるとオフラインの辞書攻撃によってパスフレーズが簡単に解読されるためです。問題は、ベンダーが 20 文字パスフレーズを生成、管理できる使いやすいツールを提供しないことです。

wIPS による解決

Cisco wIPS は、事前共有キー（**PSK**）モードの使用を検出し、より安全な 802.1x EAP ベースのキー管理および認証システムに切替えることを推奨します。**PSK** モードのキー管理を引き続き採用する場合は、使用するパスフレーズが 20 文字より長く、辞書の単語を侵害しないようにして、潜在的な攻撃を回避してください。

侵入検知：DoS 攻撃

ワイヤレス DoS（サービス拒否）攻撃は、レイヤ 1 またはレイヤ 2 における WLAN のさまざまな脆弱性を悪用してワイヤレス サービスを妨害することを狙いとしています。DoS 攻撃は、物理的な RF 環境、アクセス ポイント、クライアント ステーション、またはバックエンド認証 RADIUS サーバをターゲットとする可能性があります。たとえば、オフィスがある建物の外部から、高出力指向性アンテナを使用した遠隔 RF 電波妨害攻撃が行われることがあります。侵入者が使用する攻撃ツールは、スプーフされた 802.11 管理フレームやスプーフされた 802.1x 認証フレームなどのハッキング技法、または単に総当たりのパケット フラッディング方法を利用します。

このような攻撃の中には、ワイヤレスの特性とワイヤレス プロトコル標準を対象にするものがあります。このため、シスコは、このような攻撃の多くを未然に防ぐため、802.11i のベースとなる管理フレーム保護を開発しました。（MFP の詳細については、Cisco Prime Infrastructure オンライン ヘルプを参照してください。）wIPS は、攻撃シグニチャを一致させる早期検出システムによって、このソリューションに貢献します。wIPS の DoS 検出機能は WLAN レイヤ 1（物理層）とレイヤ 2（データ リンク層、802.11、802.1x）を対象にしています。強力な WLAN 認証および暗号化メカニズムが採用されている場合、上位層（IP 層以上）への DoS 攻撃が困難になります。wIPS サーバでは強力な認証および暗号化ポリシーを検証することで、WLAN 防衛が強化されます。さらに、Dos 攻撃およびセキュリティ突破に対する wIPS の侵入検知は、潜在的なワイヤレス攻撃に対する毎日 24 時間年中無休の完璧なモニタリングを提供します。

DoS 攻撃には、次の 3 種類のサブカテゴリがあります。

- アクセス ポイントに対する DoS 攻撃, （219 ページ）
- インフラストラクチャに対する DoS 攻撃, （224 ページ）
- クライアント ステーションに対する DoS 攻撃, （229 ページ）

アクセス ポイントに対する DoS 攻撃

アクセス ポイントに対する DoS 攻撃は主に次の事項を前提として実行されます。

- アクセス ポイントのリソースが限られている。（クライアントごとのアソシエーション ステート テーブルなど）。
- WLAN 管理フレームおよび認証プロトコル 802.11 と 802.1x に暗号化メカニズムがない。

ワイヤレス侵入者は、スプーフした MAC アドレスを使って多数のワイヤレス クライアントをエミュレートし、アクセス ポイントのリソース（最も重要なものとしてクライアント アソシエーション テーブル）を枯渇させます。エミュレートされた各クライアントはターゲット アクセス ポイントとのアソシエートと認証を試行しますが、プロトコル トランザクションは未完了のままになります。アクセス ポイント リソースとクライアント アソシエーション テーブルがこのようなエミュレートされたクライアントとその未完了認証ステートでいっぱいになるため、攻撃を受けたアクセス ポイントは正規のクライアントに対処できなくなります。このようにして DoS 攻撃が成立します。

wIPS はクライアント認証プロセスを追跡し、アクセス ポイントに対する DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、攻撃検知および統計的シグニチャ照合プロセスが開始されます。DoS 攻撃が検出されると wIPS アラームが発行されます。このアラームには、標準のアラーム詳細記述とターゲット デバイス情報が含まれます。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、Prime Infrastructure オンライン ヘルプを参照してください。

アクセス ポイントに対する DoS 攻撃には、次のタイプがあります。

アラームの説明と考えられる原因

この DoS（サービス拒否）攻撃では、アクセス ポイントに大量のスプーフィングされたクライアント アソシエーションを送り付け、アクセス ポイントのリソース（特にクライアント アソシエーション テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、この認証が使用されることはほとんどありません。別の方法として、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）が使用されることがあります。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントをエミュレートし、多数のクライアントを状態 3 にしてターゲット AP のクライアント アソシエーションテーブルのフラッディングを発生させます（以下を参照）。クライアント アソシエーション テーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃が成立します。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するために、クライアントのアソシエートが正常に完了した後で、スプーフされた MAC アドレスを検出し、802.1x アクションとデータ通信を追跡します。Cisco Adaptive Wireless IPS によりこの攻撃が報告されたら、このアクセス ポイントにログオンし、アソシエーションテーブルでクライアント アソシエーションの数を検査します。

また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『Cisco Prime Infrastructure Configuration Guide』またはオンライン ヘルプを参照してください。

-

DoS 攻撃：アソシエーション テーブル オーバーフロー

アラームの説明と考えられる原因

ワイヤレス侵入者は、スプーフした MAC アドレスを使って多数のワイヤレス クライアントを偽装し、アクセス ポイントのリソース（最も重要なのものとしてクライアント アソシエーション テーブル）を枯渇させます。それぞれの偽装クライアントがターゲット アクセス ポイントとのアソシエートと認証を試行します。通常、802.11 認証は完了します。これは、ほとんどのデプロイ

メントでは 802.11 オープン システム認証（Null 認証プロセス）が採用されているためです。このような偽装クライアントとのアソシエートの後に認証プロセスが実行されます。ただし偽装クライアントは 802.1x や VPN のような高度な認証は行わないため、プロトコル トランザクションが未完了状態になります。この時点で、攻撃を受けたアクセス ポイントでは各偽装クライアントのステートがクライアント アソシエーション テーブルに維持されます。アクセス ポイントのリソースとクライアント アソシエーション テーブルがこのような偽装クライアントとそのステート情報でいっぱいになるため、攻撃を受けたアクセス ポイントは正規のクライアントに対処できなくなります。このようにして DoS 攻撃が成立します。

wIPS による解決

Cisco Adaptive Wireless IPS はクライアント認証プロセスを追跡し、アクセス ポイントに対する DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、Cisco Adaptive Wireless IPS 攻撃検知および統計的シグニチャ照合プロセスが開始されます。

DoS 攻撃：認証フラッディング

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に準拠してこのようなステート マシンを実装しています（次の図を参照）。アクセス ポイントでは各クライアントのステートがアクセス ポイントのクライアント テーブル（アソシエーション テーブル）に記録されます。この記録されるステートのサイズは制限されています。この制限は、ハードコーディングされた数値または物理メモリ制約に基づく数値のいずれかです。

この DoS 攻撃は、多数のクライアント ステーションを偽装（MAC アドレス スプーフィング）してアクセス ポイントに認証要求を送信し、アクセス ポイントのクライアント ステート テーブル（アソシエーション テーブル）のフラッディングを引き起こします。ターゲット アクセス ポイントでは、個々の認証要求を受け取るたびにアソシエーション テーブルに状態 1 のクライアント項目が作成されます。オープン システム認証が使用されているアクセス ポイントは、認証成功フレームを戻し、クライアントを状態 2 にします。共有キー認証が使用されているアクセス ポイントは、攻撃者が偽装しているクライアントに認証チャレンジを送信します。この場合攻撃者から応答はありません。この場合アクセス ポイントはクライアントを状態 1 のままにします。いずれの場合でも、アクセス ポイントに状態 1 または状態 2 のクライアントが多数あり、アクセス ポイント アソシエーション テーブルがいっぱいになります。テーブルが上限に達すると、正規のクライアントがこのアクセス ポイントに対して認証およびアソシエートできなくなります。これにより DoS 攻撃が成立します。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイント

が特定されます。WLAN セキュリティ アナリストは、そのアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

DoS 攻撃：EAPOL-Start 攻撃

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、クライアント ステーションから送信された EAPOL-Start フレームで認証トランザクションを開始します。アクセス ポイントは EAPOL-Start フレームに対し EAP-Identity-Request および内部リソース割り当てによって応答します。

攻撃者は、アクセス ポイントに EAPOL-Start フレームを大量に送り付け、アクセス ポイント内部リソースを枯渇させることでアクセス ポイントを妨害しようとします。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS（サービス拒否）攻撃を検出するため、802.1x 認証ステート遷移および特定の攻撃シグニチャを追跡します。

DoS 攻撃：PS ポール フラッド攻撃

アラームの説明と考えられる原因

電源管理は、おそらくワイヤレス LAN デバイスにおいて最も重要な機能の 1 つです。電源管理は、ステーションを長期にわたり省電力モードで維持し、アクセス ポイントから特定の間隔でのみデータを受信するようにすることで、電力を節約します。ワイヤレス クライアントはアクセス ポイントに対し、スリープ モード（省電力モード）になる期間の長さを通知する必要があります。この期間が終わるとクライアントは再起動し、待機データ フレームがあるかどうかを確認します。アクセスポイントとのハンドシェイクが完了すると、データ フレームを受信します。アクセスポイントからのビーコンには、クライアントが再起動してマルチキャスト トラフィックを受け入れる必要がある時点でクライアントにその旨を通知する Delivery Traffic Indication Map（DTIM）も含まれています。

アクセス ポイントは引き続き、スリープ中のワイヤレス クライアントのためにデータ フレームをバッファします。アクセス ポイントは Traffic Indication Map（TIM）を使用してワイヤレス クライアントに対しアクセス ポイントにデータがバッファされていることを通知します。マルチキャスト フレームは、DTIM を通知するビーコンの後に送信されます。

クライアントは、PS-Poll フレームを使用してアクセス ポイントへバッファ フレームを配信することを要求します。すべての PS-Poll フレームに対し、アクセス ポイントはデータ フレームで応答します。ワイヤレス クライアントのためにバッファされているフレームが多数ある場合、アクセスポイントはフレーム応答のデータ ビットを設定します。その後、クライアントは次のデータ フレームを取得するために別の PS-Poll フレームを送信します。この処理は、バッファされたデータをすべて受信するまで行われます。

ハッカーがワイヤレス クライアントの MAC アドレスをスプーフし、大量の PS-Poll フレームを送信することがあります。この場合アクセス ポイントはバッファ データ フレームをワイヤレス クライアントに送信します。実際には、クライアントは省電力モードになっておりデータ フレームを受信しないことがあります。

wIPS による解決

Cisco Adaptive Wireless IPS は、ワイヤレス クライアントが正規のデータを失う可能性があるこの DoS 攻撃を検出できます。デバイスを特定し、適切な手順でワイヤレス環境からそのデバイスを削除します。また、Cisco 管理フレーム保護（MFP）は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Prime Infrastructure Configuration Guide*』またはオンライン ヘルプを参照してください。

DoS 攻撃：プローブ要求フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者は存在しないクライアントに供給するワイヤレス パケットの一定のストリームをターゲット AP に処理させます。プローブ要求フラッドの間、攻撃者は特定の AP を対象にした大量のプローブ要求を生成します。一般的なワイヤレスの設計では、AP がプローブ応答を送信することでプローブ要求に応答するように指定します。この応答には、企業ネットワークに関する情報が含まれます。フラッド攻撃中に大量のプローブ要求が送信されるため、AP は連続的に応答するためにスタックします。そのため、その AP に依存しているすべてのクライアントのサービスが拒否されます。

wIPS による解決

wIPS サーバは、検出されたプローブ要求フレームのレベルをモニタして、しきい値を超えた場合にプローブ要求フラッド アラームを生成します。要求が有効な場合でも、大量のフレームが原因でワイヤレス アクティビティに問題が生じることがあります。その結果、問題となっているフレームの発生源を特定して、企業環境から削除する必要があります。

DoS 攻撃：再アソシエーション要求フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、AP に大量のエミュレートおよびスプーフィングされたクライアント再アソシエーションを送り付け、AP のリソース（特にクライアント アソシエーション テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、今後はこの認証が使用されることはほとんどありません。唯一の代替策は、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）です。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントをエミュレートし、多数のクライアントを状態 3 にしてターゲット AP のクライアント アソシエーション テーブルのフラッディングを発生さ

せます（以下を参照）。クライアントアソシエーションテーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃が成立します。

wIPS による解決

wIPS サーバは、ネットワークの再アソシエーション要求のレベルをモニタして、しきい値を超えた場合にこのアラームを生成します。

DoS 攻撃：未認証アソシエーション

アラームの説明と考えられる原因

この DoS 攻撃では、アクセス ポイントに大量のスプーフィングされた偽装のクライアント アソシエーションを送り付け、アクセス ポイントのリソース（特にクライアント アソシエーション テーブル）を枯渇させます。802.11 層では共有キー認証に欠陥があるため、この認証が使用されることはほとんどありません。別の方法として、802.1x や VPN などの高度な認証を利用するオープン認証（Null 認証）が使用されることがあります。オープン認証では、すべてのクライアントを認証してアソシエートできます。攻撃者はこの脆弱性を利用して大量のクライアントを偽装し、多数のクライアントを状態 3 にしてターゲット AP のクライアント アソシエーション テーブルのフラッディングを発生させます（以下を参照）。クライアントアソシエーションテーブルがオーバーフローすると、正規のクライアントをアソシエートできなくなり、DoS 攻撃が成立します。

wIPS による解決

DoS 攻撃には、それを封じ込める大半の方法が通用しないという特徴があります。未認証アソシエーション攻撃も例外ではありません。膨大な数の MAC アドレスをランダムに生成しそれらをアソシエーションフレームに仕立ててターゲットのアクセスポイントに迅速に送信する攻撃者が存在します。この種の攻撃に対するワイヤレス封じ込めは、明らかに不可能です。どのような方法があるでしょうか。

攻撃の原因の特定が最善策です。

- ワイヤレス アナライザを使用して、攻撃が送信されているチャネルをロックします。
- アソシエーションフレームのストリーミングが表示されるので、それらのフレームから信号強度をの値を記録しておきます。
- これらの信号強度の数値を使用して、攻撃が生成されていると見られる領域を探りながら、攻撃の発生源を特定します。

インフラストラクチャに対する DoS 攻撃

アクセス ポイントやクライアント ステーションに対する攻撃の他に、ワイヤレス侵入者は RF スペクトラムまたはバックエンド認証 RADIUS サーバをターゲットにして DoS（サービス拒否）攻撃を行うことがあります。遠隔から高出力アンテナを使って RF ノイズを発生させることで、RF

スペクトラムを容易に妨害できます。DDoS（分散型サービス拒否）攻撃で複数のワイヤレス攻撃者がバックエンド RADIUS サーバに対して認証要求を送り付けると、この RADIUS サーバが過負荷になります。この攻撃を行う上で、認証が成功する必要はありません。

インフラストラクチャに対する DoS 攻撃には、次のタイプがあります。

DoS 攻撃：ビーコン フラッド

アラームの説明と考えられる原因

DoS 形式の攻撃では、攻撃者は、有効な AP とステーション間の新しいアソシエーションを妨げることで、企業の全体的なインフラストラクチャのアクティビティを阻害できます。通常、企業 AP は、範囲内にあるすべての受信者にビーコン フレームをブロードキャストし、ユーザにネットワークの存在を知らせます。このビーコンを受信すると、ステーションは各自の設定を打診し、これが適切なネットワークであることを確認できます。ビーコン フラッド攻撃では、ネットワークをアクティブに探しているステーションは、異なる MAC アドレスと SSID を使用して生成されたビーコンでネットワークから攻撃されます。このフラッドによって、有効なクライアントは企業 AP によって送信されるビーコンを検出できなくなり、DoS 攻撃を受けることになります。

wIPS による解決

wIPS サーバは、検出されたビーコン フレームのレベルをモニタして、しきい値を超えた場合にビーコンフラッドアラームを生成します。ビーコンが有効な場合でも、大量のフレームが原因でワイヤレス アクティビティに問題が生じることがあります。その結果、問題となっているフレームの発生源を特定して、企業環境から削除する必要があります。

DoS 攻撃：CTS フラッディング

攻撃ツール：CTS Jack

アラームの説明と考えられる原因

IEEE 802.11 標準には、ステーションによる RF 媒体へのアクセスを制御する RTS/CTS（Request-To-Send/Clear-To-Send）機能がオプションとして含まれています。送信準備が整ったワイヤレス デバイスは、指定された期間にわたって RF 媒体への送信権限を獲得するため、RTS フレームを送信します。レシーバは同じ期間の CTS フレームを送信して RF 媒体への権限をトランスミッタに付与します。CTS フレームを監視するワイヤレス デバイスはすべて、競合がない状態で送信できるようにトランスミッタに対してこの媒体を生成します。

ワイヤレス DoS 攻撃を行うハッカーが、CTS フレームに付与された特権を悪用して RF 媒体を送信用に予約することがあります。攻撃者はバックツーバック CTS フレームを送信することで、攻撃者が CTS フレームの送信をやめるまで RF 媒体を共有する他のワイヤレス デバイスが送信を行わないようにできます。

wIPS による解決

Cisco Adaptive Wireless IPS は DoS 攻撃のための CTS フレームの不正使用を検出します。

DoS 攻撃: Destruction 攻撃

アラームの説明と考えられる原因

MDK3 はハッキング ツールのスイートであり、ユーザは企業のインフラストラクチャに対して多数の異なるセキュリティ突破方式を利用することができます。MDK3-Destruction モードは、ワイヤレス導入を効果的かつ完全にシャットダウンするために一連のツールを使用するスイートの特定の実装です。MDK-Destruction 攻撃の間、ツールは次のことを同時に行います。

- ビーコン フラッド攻撃を開始して、環境内に疑似 AP を作成する。
- 有効な企業 AP に対する認証フラッド攻撃を開始し、企業 AP のクライアントへのサービス機能を阻止して、有効なクライアントとのアクティブな接続をすべて切断します。

追加の機能拡張により、ツールを使用して、ビーコン フラッドで生成された疑似 AP に有効なクライアントを接続できるため、環境内でさらなる混乱が生じます。

wIPS による解決

wIPS サーバは、MDK3-Destruction 攻撃の症状の組み合わせをモニタして、検出時にアラームを生成します。この攻撃はワイヤレス導入に多大な影響を及ぼす可能性があるため、通常のネットワーク オペレーションを再開するために、攻撃の発生源を特定し、ただちに削除することを強く推奨します。

DoS 攻撃：クイーンズランド工科大学により検出された脆弱性

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02

アラームの説明と考えられる原因

802.11 WLAN デバイスは、基本アクセス メカニズムとしてキャリア検知多重アクセス/衝突回避（CSMA/CA）を採用しています。このメカニズムでは、WLAN デバイスが送信開始前に媒体を待機し、すでに実行中の送信を検出するとバックオフします。衝突回避では、媒体が送信可能になる前の時点で物理検知メカニズムと Network Allocation Vector（NAV）を含む仮想検知メカニズムが組み合わせられます。DSSS プロトコルのクリア チャネル アセスメント（CCA）は、WLAN チャネルがクリアであり 802.11b デバイスがこのチャネルを介して送信できるかどうかを判断します。

802.11b プロトコル標準に DoS 無線周波数電波妨害攻撃を可能にする脆弱性があることが、オーストラリアのブリスベンにあるクイーンズランド工科大学 Information Security Research Centre 所属の Mark Looi、Christian Wullems、Kevin Tham、および Jason Smith により明らかになりました。

この攻撃では特に CCA 機能が攻撃を受けます。AusCERT の勧告では「この脆弱性に対する攻撃では、物理層の CCA 機能が悪用され、攻撃中に範囲内のすべての WLAN ノード（クライアントとアクセス ポイントの両方）によるデータ送信が遅延します。攻撃を受けたデバイスは、チャネルが使用中であるかのように動作し、ワイヤレス ネットワーク経由でのデータ送信が妨害されます。」と述べられています。

この DoS 攻撃は、IEEE 802.11、802.11b、および低速（20 Mbps 以下）802.11g ワイヤレス デバイスを含む DSSS WLAN デバイスに影響します。IEEE 802.11a（OFDM を使用）、高速（OFDM 使用で 20 Mbps を上回る速度）802.11g ワイヤレス デバイスはこの攻撃の影響を受けません。FHSS を使用するデバイスは影響を受けません。

攻撃者は WLAN カードを装着したラップトップや PDA を使い、SOHO WLAN と企業 WLAN に対してこの攻撃を行うことができます。この DoS 攻撃に対する唯一の回避策は、802.11a プロトコルに切り替えることです。

この DoS 攻撃の詳細については、以下を参照してください。

- http://www.auscert.org.au/render.html?it=4091
- http://www.qut.edu.au/institute-for-future-environments
- http://www.kb.cert.org/vuls/id/106678

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出すると、アラームを発行します。原因デバイスを特定し、適切な手順でワイヤレス環境からそのデバイスを削除します。

DoS 攻撃：RF 電波妨害攻撃

アラームの説明と考えられる原因

（注） RF 電波妨害攻撃はチャネル アラームで、アラーム ソースまたは宛先 MAC アドレスが含まれません。このようなアラームではロケーションが生成されません。

RF 電波妨害攻撃では、攻撃者の MAC アドレスを入力しません。RF 電波妨害は、特定のチャネルに対する攻撃です。攻撃者は、1 秒あたり数千のフレームを送信してチャネルを妨害します。フレームは異なる MAC アドレスで送信されます。そのため、攻撃者を識別する固有の MAC アドレスを得られません。

WLAN の信頼性と効率は、無線周波数（RF）媒体の品質に基づきます。各 RF は RF ノイズの影響を受けます。この WLAN 脆弱性を利用する攻撃者は、「WLAN サービス妨害」と「AP ハードウェアの物理的な損傷」の 2 種類のDoS （サービス拒絶）攻撃を実行できます。

- WLAN サービスの妨害：無免許の 2.4 GHz スペクトラムでは、攻撃が意図的ではないことがあります。コードレス電話、Bluetooth デバイス、電子レンジ、ワイヤレス監視ビデオ カメラ、ベビー モニタなどはすべて RF エネルギーを放出し、WLAN サービスを妨害する可能性

があります。悪意のある攻撃では、高出力指向性アンテナを使い 2.4 GHz または 5 GHz スペクトラムで RF 出力を操作し、遠隔から攻撃の影響を増幅させることができます。自由空間と建物内での減衰により、建物から 300 フィート離れた位置にある 1-kW 電波妨害デバイスは、オフィス エリアへ 50 ～ 100 フィートの電波妨害が可能です。同じ 1-kW 電波妨害デバイスを建物の中に配置すると、オフィス エリアへ 180 フィートの電波妨害が可能です。攻撃中は、ターゲット エリア内の WLAN デバイスはワイヤレス サービスを利用できません。

- 物理的な損傷を受けた AP ハードウェア：攻撃者は指向性高利得アンテナを備えた高出力トランスミッタをアクセス ポイントから 30 ヤード離れた位置で使い、アクセス ポイント内の電子部品に損害を与え、アクセス ポイントを永久に使用不能にするのに十分な高出力 RF 出力を発生できます。このような高エネルギー RF（HERF）ガンは効果的であり、安価で製作できます。

wIPS による解決

RF に基づく妨害と同様に、これを解決する最善の方法は、RF 電波妨害アラームの原因デバイスを物理的に特定し、オフラインにすることです。または Cisco CleanAir とシグニチャ ライブラリを使用すると、このデバイスの詳しい情報を取得できます。

- このアラームをトリガーした wIPS アクセス ポイントを検出します。
- 移動式スペクトル アナライザを使用して周辺を探りながら、妨害電波の発生源を特定します。
- デバイスを見つけたら、デバイスの電源を切るか WLAN に影響を与えない領域に移動します。

DoS 攻撃：RTS フラッディング

アラームの説明と考えられる原因

IEEE 802.11 標準には、ステーションによる RF 媒体へのアクセスを制御する RTS/CTS（Request-To-Send/Clear-To-Send）機能がオプションとして含まれています。送信準備が整ったワイヤレス デバイスは、指定された期間にわたって RF 媒体への送信権限を獲得するため、RTS フレームを送信します。レシーバは同じ期間の CTS フレームを送信して RF 媒体への権限をトランスミッタに付与します。CTS フレームを監視するワイヤレス デバイスはすべて、競合がない状態で送信できるようにトランスミッタに対してこの RF 媒体を生成します。

ワイヤレス DoS 攻撃を行うハッカーが、CTS フレームに付与された特権を悪用して RF 媒体を送信用に予約することがあります。攻撃者は大きな送信期間テキスト ボックスを含むバックツーバック RTS フレームを送信して無線媒体を予約し、RF 媒体を共有する他のワイヤレス デバイスが送信を行わないようにします。

wIPS による解決

Cisco Adaptive Wireless IPS は DoS 攻撃のための RTS フレームの不正使用を検出します。

DoS 攻撃：仮想キャリア攻撃

アラームの説明と考えられる原因

仮想キャリア検知攻撃を実行するには、ランダムな持続時間値を定期的に送信できるように802.11 MAC 層実装を改ざんします。この攻撃は ACK、データ、RTS、および CTS フレームに対し、大きな持続時間値を使用して実行されます。これにより攻撃者は正規ユーザに対しチャネルへのアクセスを妨害できます。通常の状況では、ACK フレームに大きな持続時間値が含まれているのは、ACKがフラグメンテーションパケットシーケンスの一部である場合だけです。データフレームに大きな持続時間値が含まれているのは、そのデータフレームがフラグメンテーションパケット交換の一部である場合だけです。

この攻撃への対処の 1 つとして、ノードにより受け入れられる持続時間値を制限する方法があります。この制限を超える大きな持続時間値が含まれているパケットはすべて、最大許容値になるように切り捨てられます。ロー キャップ値とハイ キャップ値が使用されます。ロー キャップの値は、ACK フレームの送信に必要な時間にフレームのメディア アクセス バックオフを加算した値です。ロー キャップが使用されるのは、監視対象パケットの後に送信可能なパケットが ACK または CTS のみである場合です。これには、RTS およびすべての管理（アソシエーションなど）フレームが含まれます。ハイ キャップが使用されるのは、監視対象フレームの後にデータ パケットが送信可能である場合です。この場合の制限には、最大データ フレームの送信に必要な時間とそのフレームのメディア アクセス バックオフが含まれている必要があります。ハイ キャップを使用する必要があるのは、ACK 監視時（ACK が MAC レベルのフラグメンテーション パケットの一部である可能性があるため）と CTS 監視時です。

RTS フレーム受信するステーションはデータ フレームも受信します。IEEE 802.11 標準では、後続の CTS フレームとデータ フレームの正確な時間が指定されています。次のデータ フレームが受信されるかまたは受信されない時点まで、RTS の持続時間値が順守されます。監視対象 CTS が非請求であるか、または監視ノードが隠れ端末です。この CTS が有効な範囲内のステーション宛てである場合、有効なステーションは持続時間がゼロの Null ファンクション フレームを送信することでこれを無効にできます。この CTS が範囲外のステーション宛てである場合、防御策の 1 つとして、暗号を使用して署名された前の RTS のコピーを含む認証済み CTS フレームを導入する方法があります。この方法では、オーバーヘッドまたはフィジビリティの問題が発生する可能性があります。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS（サービス拒絶）攻撃を検出します。デバイスを特定し、適切な手順でワイヤレス環境からそのデバイスを削除します。

クライアント ステーションに対する DoS 攻撃

ワイヤレス クライアント ステーションに対する DoS 攻撃は通常、802.11 管理フレームと 802.1x 認証プロトコルには暗号化メカニズムがないためにスプーフィング可能であるという事実に基づいて実施されます。たとえば、ワイヤレス侵入者はアクセス ポイントからクライアント ステー

ションへの 802.11 ディスアソシエーション フレームまたは認証解除フレームを継続的にスプーフィングすることで、クライアント ステーションへのサービスを妨害できます。

802.11 認証およびアソシエーション ステート攻撃の他に、802.1x 認証でも同様の攻撃シナリオがあります。たとえば 802.1x EAP-Failure メッセージまたは EAP-logoff メッセージは暗号化されていないため、これらのメッセージをスプーフして 802.1x 認証済みステートを妨害し、ワイヤレス サービスを妨害できます。

Cisco Adaptive Wireless IPS はクライアント認証プロセスを追跡し、DoS 攻撃シグニチャを特定します。未完了の認証およびアソシエーションのトランザクションが検出されると、攻撃検知および統計的シグニチャ照合プロセスが開始されます。DoS 攻撃が検出されると wIPS アラームが発行されます。このアラームには、標準のアラーム詳細記述とターゲット デバイス情報が含まれます。

クライアント ステーションに対する DoS 攻撃には、次のタイプがあります。

DoS 攻撃：認証失敗攻撃

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは IEEE 標準に基づいてこのクライアント ステート マシンを実装します（次の図を参照）。適切にアソシエートされたクライアント ステーションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信プロセスに参加できません。IEEE 802.11 ではオープン システム認証と共有キー認証という 2 種類の認証サービスが定義されています。ワイヤレス クライアントはいずれかの認証プロセスによってアクセス ポイントにアソシエートされます。

DoS（サービス拒否）攻撃では、状態 3 のアソシエートされているクライアントからアクセス ポイントへ送信される無効な認証要求フレームが（不正な認証サービスおよびステータス コードで）スプーフされます。アクセス ポイントは無効な認証要求を受信するとクライアントを状態 1 に更新しますが、これによりクライアント ワイヤレス サービスが切断されます。

wIPS による解決

Cisco Adaptive Wireless IPS は、この DoS 攻撃を検出するためスプーフィング MAC アドレスと認証失敗をモニタします。このアラームは侵入が試みられたことを示すこともあります。アクセス ポイントとの認証段階でワイヤレス クライアントの失敗回数が多すぎると、サーバは侵入者がセキュリティを侵害しようとしている可能性を示すため、このアラームを生成します。

（注） このアラームは、802.11 の認証方式（オープン システムおよび共有キーなど）を対象にしています。802.1x および EAP ベースの認証は、他のアラームによってモニタされます。

DoS 攻撃：ブロック ACK フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者は 802.11n AP を妨害し、特定の有効な企業クライアントからフレームを受信できないようにします。802.11n 規格の導入に伴い、クライアントがフレームの大きなブロックをセグメントに分割することなく、同時に送信することができるトランザクション メカニズムが導入されました。この交換を開始するために、クライアントは、送信ブロックのサイズを AP に知らせるシーケンス番号が含まれている Add Block Acknowledgement（ADDBA）を AP に送信します。AP は指定されているシーケンス内のすべてのフレームを受け入れ（範囲外のフレームはすべて削除し）、トランザクションが完了したら BlockACK メッセージをクライアントに送信します。

攻撃者はこのプロセスを悪用するために、有効なクライアントの MAC アドレスをスプーフィングしている間に無効な ADDBA フレームを送信できます。このプロセスにより、AP は無効なフレーム範囲の終わりに達するまで、クライアントから送信される有効なトラフィックを無視することになります。

wIPS による解決

wIPS サーバは、スプーフされたクライアント情報の兆候を確認するため Block ACK トランザクションをモニタします。攻撃者がブロック ACK 攻撃を開始しようとしていることが検出されると、アラームが生成されます。危険性のあるデバイスを特定し、特定したら早急にワイヤレス環境からそのデバイスを削除することを推奨します。

DoS 攻撃: 認証解除ブロードキャスト

攻撃ツール：WLAN Jack、Void11、Hunter Killer

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアント ステーションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません。

この DoS 攻撃では、アクセス ポイントからブロードキャスト アドレスへの認証解除フレームをスプーフして、アクセス ポイントのすべてのクライアントを状態 1（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃は複数クライアントに対してワイヤレス サービスを妨害する点で非常に効果的であり即効性があります。通常、攻撃者が別のデアソシエーション フレームを送信するまで、クライアント ステーションはアソシエーションと認証を再度実行してサービスを回復します。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフィングされた認証解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ アナリストは、そのアクセスポイントにログインして現在のアソシエーションテーブルのステータスを確認できます。

また、Cisco 管理フレーム保護（MFP）は、MAC のスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『Cisco Prime Infrastructure Configuration Guide』またはオンライン ヘルプを参照してください。

DoS 攻撃：認証解除フラッディング

攻撃ツール：WLAN Jack、Void11

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアント ステーションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません。

この DoS 攻撃では、アクセス ポイントからクライアント ユニキャスト アドレスへの認証解除フレームをスプーフィングして、アクセス ポイントのクライアントを状態 1（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃はクライアントに対するワイヤレス サービスを妨害する点で非常に効果的かつ即効性があります。通常、攻撃者が別のデアソシエーションフレームを送信するまで、クライアントステーションはアソシエーションと認証を再度実行してサービスを回復します。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフィングされた認証解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ オフィサは、アクセスポイントにログインして現在のアソシエーションテーブルのステータスを確認できます。

DoS 攻撃：アソシエート解除フラッディング

アラームの説明と考えられる原因

IEEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは、IEEE 標準に従ってこのステート マシンを実装します。適切にアソシエートされたクライアント ステーションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信に参加できません。

この DoS 攻撃では、アクセスポイントからブロードキャストアドレス（すべてのクライアント）へのディスアソシエーションフレームをスプーフィングしてアクセスポイントのクライアントを状態 2（未アソシエートまたは未認証）にします。現在のクライアント アダプタ実装では、この攻撃は複数クライアントに対してワイヤレス サービスを妨害する点で効果的かつ即効性があります。通常は、攻撃者が新たなディスアソシエーションフレームを送信するまで、クライアントステーションは再アソシエートしてサービスを回復します。攻撃者は繰り返しディスアソシエーション フレームをスプーフし、すべてのクライアントを使用不能な状態にします。

wIPS による解決

Cisco Adaptive Wireless IPS はこの DoS 攻撃を検出するため、スプーフィングされた認証解除フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ オフィサは、アクセスポイントにログインして現在のアソシエーションテーブルのステータスを確認できます。

DoS 攻撃：EAPOL-Logoff 攻撃

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-start フレームで開始します。認証セッションの終了時にクライアント ステーションがログオフするときに、クライアント ステーションは 802.1x EAPOL-logoff フレームを送信し、アクセス ポイントとのセッションを終了します。

EAPOL-logoff フレームは認証されないため、攻撃者はこのフレームをスプーフし、ユーザをアクセス ポイントからログオフさせることができます。これにより DoS 攻撃が成立します。クライアント ステーションは、WLAN 経由での通信を試行するまで、アクセス ポイントからログオフされていることに気付きません。通常、クライアント ステーションは切断された接続状態を検知すると、再アソシエーションを行い自動で認証して、ワイヤレス接続を回復しようとします。攻撃者はスプーフィング EAPOL-logoff フレームを継続的に送信することで、この攻撃の効果を維持できます。

wIPS による解決

Cisco Adaptive Wireless IPS は、FATA-jack の利用を検出するためスプーフィング MAC アドレスと認証失敗をモニタします。このアラームは侵入が試みられたことを示すこともあります。アクセス ポイントとの認証段階でワイヤレス クライアントの失敗回数が多すぎると、Cisco Adaptive Wireless IPS はセキュリティを侵害しようとする侵入者の可能性を示すため、このアラームを生成します。

（注） このアラームは 802.11 認証方式（オープン システム、共有キーなど）を監視の対象とします。EAP および 802.1x ベースの認証は、他のアラームによってモニタされます。

DoS 攻撃：FATA Jack ツールの検出

アラームの説明と考えられる原因

EEE 802.11 は、ステーションの認証およびアソシエーション ステータスをトラッキングするためのクライアント ステート マシンを定義しています。ワイヤレス クライアントとアクセス ポイントは IEEE 標準に基づいてこのステート マシンを実装します。適切にアソシエートされたクライアント ステーションは状態 3 のままとなり、ワイヤレス通信を続行します。状態 1 および状態 2 のクライアント ステーションは、認証され状態 3 にアソシエートされるまでは WLAN データ通信プロセスに参加できません。IEEE 802.11 ではオープン システム認証と共有キー認証という 2 種類の認証サービスが定義されています。ワイヤレス クライアントはいずれかの認証プロセスによってアクセス ポイントにアソシエートされます。

この DoS 攻撃では、状態 3 のアソシエートされているクライアントからアクセス ポイントへ送信される無効な認証要求フレームが（不正な認証サービスおよびステータス コードで）スプーフされます。アクセス ポイントは無効な認証要求を受信するとクライアントを状態 1 に更新しますが、これによりクライアント ワイヤレス サービスが切断されます。

FATA-jack は、同様の攻撃を実行するために最もよく使用されるツールの 1 つです。これは WLAN-jack を改変したツールであり、認証失敗パケットと、前回の認証失敗の理由コードをワイヤレス ステーションに送信します。これは、アクセス ポイントの MAC アドレスをスプーフィングした後に行われます。FATA-jack は最もアクティブな接続を閉じるため、時には、ユーザは通常の処理を続行するためにステーションをリブートする必要があります。

wIPS による解決

Cisco Adaptive Wireless IPS は、スプーフされた不完全な EAP-failure フレームと各クライアント ステーションおよびアクセス ポイントの 802.1x 認証ステートを追跡することで、この DoS 攻撃を検出します。デバイスを特定し、適切な手順でワイヤレス環境からそのデバイスを削除します。

DoS 攻撃：不完全な EAP-Failure 攻撃

アラームの説明と考えられる原因

IEEE 802.1x 標準では、Extensible Authentication Protocol over LAN（EAPOL）を使用して認証プロトコルが定義されています。802.1x プロトコルは、認証トランザクションを開始する EAPOL-start フレームで開始します。バックエンド RADIUS サーバとの 802.1x 認証パケット交換が完了すると、アクセス ポイントからクライアントに対し、認証の成功を示す EAP-success または失敗を示す EAP-failure が送信されます。

IEEE 802.1X 仕様では、必要な相互認証が完了していない場合にクライアントによるインターフェイスの表示が禁止されています。これにより、適切に実装された 802.1x クライアント ステーションが、不完全な EAP-success パケットを送信する疑似アクセス ポイントにだまされることを回避できます。

攻撃者はアクセスポイントからクライアントへの不完全な EAP-failure フレームを継続的にスプーフしてクライアントの認証ステートを妨害し、クライアント インターフェイスが表示されないようにします（DoS 攻撃の成立）。

wIPS による解決

Cisco Adaptive Wireless IPS は、スプーフされた不完全な EAP-success フレームと各クライアント ステーションおよびアクセス ポイントの 802.1x 認証ステートを追跡することで、この DoS 攻撃を検出します。デバイスを特定し、適切な手順でワイヤレス環境からそのデバイスを削除します。

侵入検知：セキュリティ突破

ワイヤレス侵入の 1 つに、WLAN 認証メカニズムを突破し、有線ネットワークまたはワイヤレス デバイスへのアクセスを獲得するものがあります。認証方式への辞書攻撃は、アクセス ポイントに対する一般的な攻撃の 1 つです。侵入者は、アクセス ポイントとのアソシエーション プロセス中にワイヤレス クライアント ステーションを攻撃することもあります。たとえば何も知らないワイヤレス クライアントに対する疑似アクセスポイント攻撃により、そのクライアントが疑似アクセス ポイントにアソシエートすることがあります。この攻撃によって、侵入者はワイヤレス ステーションへのネットワーク アクセスを取得して、ファイル システムをハッキングできる可能性があります。その後、侵入者はそのステーションを使用して企業の有線ネットワークにアクセスできます。

セキュリティに対するこのような脅威は、相互認証と強力な暗号化手法を使用することで防止できます。wIPS は弱いセキュリティ構成と侵入攻撃の試みを検出します。wIPS は最良のセキュリティ ポリシー実装を検証し、侵入の試みを検出することで強力なワイヤレス セキュリティ保護を実現します。このような脆弱性や攻撃の試みが検出されると、wIPS はこのような侵入の試みを管理者に通知するアラームを生成します。

セキュリティ突破攻撃には、次のタイプがあります。

ASLEAP ツール検出

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは WEP キー クラッキング攻撃に対して脆弱です。

シスコは、既存の 802.1x フレームワークを利用して WEP キー攻撃を回避する LEAP（Lightweight Extensible Authentication Protocol）を導入しました。Cisco LEAP ソリューションには、セッションごとまたはユーザ キーに基づいて動的な相互認証と設定可能な WEP セッション キー タイムアウトが含まれています。LEAP ソリューションは安定したセキュリティ ソリューションとして見なされており、容易に設定できます。

LEAP を実行する無線 LAN ネットワークを侵害するためオフライン辞書攻撃で LEAP パスワードを解読するハッキング ツールがあります。このツールは LEAP を採用している WLAN ネットワークを検出すると、ユーザを認証解除します。これによりユーザは再接続しなければならないため、ユーザ名とパスワードのクレデンシャルを入力します。ハッカーはネットワークへ再アクセスする正規ユーザのパケットをキャプチャします。その後攻撃者はトラフィックをオフラインで解析し、辞書の値をテストしてパスワードを推測できます。

ASLEAP ツールの主な機能を以下に示します。

- libpcap を使用して RFMON モードでワイヤレス インターフェイスからリアルタイムに読み取る。
- 1 つのチャネルをモニタするか、またはチャネル ホッピングを実行して LEAP を実行しているターゲット ネットワークを探す。
- LEAP ネットワークのユーザをアクティブに認証解除し、ユーザに再認証を実行させる。これにより LEAP パスワードを迅速にキャプチャできます。
- LEAP を実行していないユーザではなく、まだ確認されていないユーザのみを認証解除する。
- 保存されている libpcap ファイルを読み取る。
- ダイナミック データベース テーブルと索引を使用して大きなファイルを迅速に検索できるようにする。これにより、フラット ファイルの検索とは対照的に、最悪検索時間が .0015 % 短くなります。
- LEAP 交換情報のみを libpcap ファイルに書き込む。

これは、ディスク スペースが少ないデバイス（iPaq など）で LEAP クレデンシャルをキャプチャするときに使用できます。キャプチャされた LEAP クレデンシャルは、辞書攻撃を実行するためにそのデバイスよりもストレージ リソースが多いシステムの libpcap ファイルに保存されます。

このツールのソースと Win32 バイナリ ディストリビューションは http://asleap.sourceforge.net から入手できます。

シスコは、辞書攻撃を阻止する Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）プロトコルを開発しました。EAP-FAST は中間者攻撃、辞書攻撃、パケッ

トおよび認証偽造攻撃を阻止します。EAP-FAST では、クライアントとサーバ間に PAC（Protected Access Credential）を使用して相互認証するトンネルが作成されます。トンネル確立プロセスが完了したら、クライアントはユーザ名とパスワードのクレデンシャルを使用して認証されます。

EAP-FAST の特長を以下に示します。

- 独自のプロトコルではない。
- IEEE 802.11i 標準に準拠している。
- TKIP と WPA に対応している。
- 証明書を使用しないため複雑な PKI インフラストラクチャを回避する。
- PC および Pocket PC の複数のオペレーティング システムに対応している。

wIPS による解決

Cisco Adaptive Wireless IPS は ASLEAP ツールの認証解除シグニチャを検出します。検出すると、サーバはワイヤレス管理者に警告します。攻撃を受けたステーションのユーザはパスワードをリセットする必要があります。最良の ASLEAP ツール対処策は、企業 WLAN 環境で LEAP を EAP-FAST に置き換える方法です。

Cisco WCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、弱い暗号化または認証を使用するように設定されているアクセス ポイントを事前予防的に報告します。自動セキュリティ脆弱性スキャンの詳細については、Cisco WCS オンライン ヘルプを参照してください。

AirDrop セッションの検出

アラームと考えられる原因

Apple の OSX Lion 以降には AirDrop という新機能があります。この新しい機能は、「新しい」MacBook、MacBook Pro、iMac でサポートされます。ユーザはこの新しい機能を利用して、ワイヤレス ファイル転送システムを迅速にセットアップできます。このセットアップを行うには、ファイルを共有しようとする両方のユーザが Finder を開いて AirDrop リンクをクリックする必要があります。両方のシステムが互いの範囲内でリンクをセットアップすると、相手ユーザのログイン アイコンが AirDrop ウィンドウに表示されます。この状態で、ファイルを相手ユーザのアイコンにドラッグ アンド ドロップすると、ファイル転送が開始します。

これによりセキュリティ リスクが発生する可能性があります。WLAN環境で未承認のピアツーピア ネットワークが動的に作成されるからです。ここではファイル共有も問題になります。

wIPS による解決

システムは、ワイヤレス ネットワークで、AirDrop セッションに該当するトラフィックをモニタします。AirDrop セッションを形成しているユーザを特定し、無許可のピアツーピア ネットワークに関する社内ポリシーをそのユーザに知らせることをお勧めします。

AirPwn

アラームの説明と考えられる原因

Airpwn は 802.11 パケット インジェクションのフレームワークです。Airpwn は、着信するワイヤレス パケットをリスニングし、データがコンフィギュレーション ファイルに指定されているパターンと一致すると、カスタムのコンテンツがワイヤレス アクセス ポイントから挿入（スプーフィング）されます。クライアントがインターネットに要求を送信すると、Airpwn は固有の遅延を利用します。Airpwn の攻撃者は近いところにいるため、迅速に応答できます。たとえば、ハッカーは Web サイトで閲覧者が表示しようとするイメージを、ハッカーが閲覧者に見せたいものだけを表示するように、すべて差し替えることもできます。

Airpwn は、オープンのワイヤレス ネットワークと、攻撃者が WEP キーを知っている WEP 暗号化ネットワークのみで機能します。

wIPS による解決

Cisco Enterprise は、ワイヤレス ネットワークで、オープン AP または WEP 暗号解読された AP に対する Airpwn 攻撃に該当するトラフィックをモニタし、WLAN 管理者に通知します。セキュリティ担当者が Floor Plan 画面を使用してデバイスを特定し位置を確認することをお勧めします。攻撃ステーションをワイヤレス環境から速やかに取り除く必要があります。

Airsnarf 攻撃の検出

アラームの説明と考えられる原因

wIPS による解決

Cisco Adaptive Wireless IPS は AirSnarf ツールを実行しているワイヤレス デバイスを検出します。AirSnarf ツールを WLAN 環境から削除するために管理者が適切な措置をとる必要があります。

不良 EAP-TLS フレーム

アラームの説明と考えられる原因

有効な企業クライアントから AP への特定のフレーム送信により、データが不十分または無効なために、一部の AP モデルでクラッシュが生じることがあります。ワイヤレス攻撃者は、企業 AP をダウンさせるために、欠陥のあるフレームを送信することでこの脆弱性を悪用することができます。フラグを「c0」に設定した EAP-TLS パケットを送信し、TLS メッセージ長もデータも送信しないことで、一部のベンダーの AP は、リブートされるまで動作不能になることがあります。このリブート プロセスの間、攻撃者は企業ネットワークにアクセスする機会を得ることができ、セキュリティ リークとなる可能性があります。

wIPS による解決

wIPS サーバは、EAP-TLS の送信をモニタして、欠陥フレームや無効フレームを検出した場合にアラームを生成します。この問題は、必ずしもワイヤレス攻撃を示すものではありませんが、ワイヤレス導入全体の健全性を維持するためには修復する必要がある問題です。

ビーコン ファジング フレーム検出

アラームの説明と考えられる原因

802.11 ファジングは、無効、予想外、またはランダムなデータを 802.11 フレームに取り入れ、修正されたフレームを送信するプロセスです。このプロセスは送信先のデバイスに、ドライバのクラッシュ、オペレーティング システムのクラッシュ、スタック ベースのオーバーフローなど予想外の動作を引き起こす場合があり、影響を受けたシステムで任意コードを実行できる状態にします。802.11 フレームのファジングに基づく脆弱性のさまざまな報告事例については、CVE Web サイト（http://cve.mitre.org/index.html）を参照してください。

システムは、各ビーコン フレームを検査して、ファジング アクティビティの兆候を調べます。ビーコン ファジングの一般的な形式は、SSID フィールドを 32 バイトの制限を超えて拡大し、サポートされるデータ レートを無効なレートに変更するものです。システムはこれらの異常を検索し、フィールド値が 802.11 仕様の範囲を超えると、ビーコン ファジング アラームを生成します。

wIPS による解決

システムは、ワイヤレス ネットワークでビーコン ファジングに該当するトラフィックをモニタします。デバイスを特定しオフラインにすることが推奨されます。

ブルートフォース非表示 SSID

アラームの説明と考えられる原因

WLAN 管理者が行っている一般的な手段は、アクセス ポイントで SSID のブロードキャストを無効にすることです。この手法は、ワイヤレス ネットワークをスキャンしている相手から自分が見えなければ、自分は安全だという発想に基づきます。基本的に、そのワイヤレス ネットワークに接続するために SSID を把握する必要があります。これは、見えないネットワークから SSID を抽出するツールを持たないユーザが、ワイヤレス ネットワークに気ままにアクセスすることを阻止します。しかしハッカーの場合、話は別です。ハッカーは、ツールを使い、見えないネットワークから SSID を抽出するまで時間をかけて粘ります。このタイプのスヌーピングを実行するツールは、数多くあります。見えない SSID が通常の方法で検出できない場合、ハッカーはツール mdk3 を使用してブルートフォース方式を適用できます。ツール mdk3 を使用することで、辞書攻撃またはワードリスト攻撃を見えないネットワークに対して実行し SSID を抽出できます。

wIPS による解決

Cisco Enterprise は、ワイヤレス ネットワークで非表示 SSID に対するブルートフォース攻撃に該当するトラフィックをモニタし、WLAN 管理者に通知します。セキュリティ担当者が Floor Plan 画面を使用してデバイスを特定し位置を確認することをお勧めします。攻撃ステーションをワイヤレス環境から速やかに取り除く必要があります。

ChopChop 攻撃

アラームの説明と考えられる原因

この攻撃は、WEPプロトコルで実装されている安全でない冗長性チェック用アルゴリズムを利用します。いくつかの既知のプロパティを利用することで、攻撃者は暗号化されたパケットを取得してそのパケットを復号し、パケットの暗号化に使用されているキーストリームを取得できます。

攻撃の手順としては、攻撃者はパケットをキャプチャし ICV の前にパケット末尾から1バイト切り離します。

次に、復号化されたバイト値に「推測」を加えます。パケットは ICV を再計算して修正され、さらにこのパケットをターゲットの AP に挿入します。ターゲットの AP がこのフレームを再びブロードキャストすれば、攻撃者は復号化されたバイトの値を正しく推測できたことがわかります。攻撃者は、さらに次のバイトに移ります。推測が成功するにつれて、挿入されるパケットは小さくなり続けます。パケットが再ブロードキャストされない場合、攻撃者は推測を別の候補に変えてプロセスを繰り返し、256 通りの可能性を推測しながら試します。次に、さまざまな推測を試みているツールの例を示します。

プロセスが完了すると、攻撃者はバイトごとの WEP パケット 全体の複合化を完了し、元の暗号化されたパケットで XOR 化して平文データを生成できます。

wIPS による解決

ChopChop 攻撃は WEP ベースのアクセス ポイントを狙い、WEP キーを解読してワイヤレス ネットワークに直接アクセスしようとします。この特定の攻撃には 5 分もかからないため、すでに攻撃者がワイヤレス ネットワークにアクセスしている可能性が高いとも考えられます。可能であれば、WLAN を WEP から移行してください。WPA2-AES が推奨されます。これを採用しない場合には、状況を解決するために役立つ手段があります。

- 影響を受けた AP の無線をオフにします。これにより、現在接続しているすべてのクライアントが切断されます。
- WEP キーを変更します。
- 再び電源スイッチをオンにします。
- 設定したばかりの新しい WEP キーに接続しているすべてのデバイスで WEP キーを変更する必要があります。
- NCS をモニタし、ChopChop アラームが再度発生するかどうかを確かめます。

DHCP スターベーション攻撃の検出

アラームの説明と考えられる原因

DHCP スターベーションは、悪意のあるユーザがスプーフィングされた MAC アドレスで大量の DHCP 要求をブロードキャストする攻撃です。十分な量の DHCP 要求フレームがネットワークでフラッドすると、攻撃者は有効なユーザが利用可能な残りの DHCP IP アドレスをすべて使い切ってしまいます。これにより、ネットワークは DoS 攻撃の状態になります。これを非常に容易に実行できる 2 種類のツールとして、Gobbler および Yersinia が公開されており、この種の攻撃を可能にします。このタイプの攻撃は、ゲスト ネットワークやホットスポット ネットワークで特に有害で、これらの環境ではユーザが認証前に IP アドレスを取得できます。

このタイプの攻撃を緩和する手段は、スイッチ レベルで扱われます。Cisco IOS スイッチでは、DHCP スヌーピングを有効にします。Cisco CatOS では、ポート セキュリティを有効にします。

wIPS による解決

システムは、ワイヤレス ネットワークで、DHCP スターベーション攻撃に該当するトラフィックをモニタします。攻撃を実行するユーザを特定するか、またはより強固なスイッチ セキュリティを実装することが推奨されます。

WLAN のセキュリティ異常によるゼロデイ攻撃

wIPS による解決

Cisco Adaptive Wireless IPS は、ワイヤレス ネットワーク上の多数のデバイスにおける 1 つのセキュリティ IDS/IPS ポリシー違反を検出します。指定の期間内に特定のポリシーに違反しているデバイス数が検出されたか、またはアラームの閾値設定に指定されているデバイス数のパーセンテージが突然増加しています。セキュリティ IDS/IPS 違反に応じて、違反を個別にモニタし、この攻撃の送信元と宛先を判定することをお勧めします。不正デバイスの数が増加している場合は、ネットワークに対して攻撃が行われている可能性があります。

暗号化が無効な状態でクライアントデバイスの数が突然増加した場合は、企業セキュリティポリシーを再確認し、ポリシー ルールに基づいてユーザが最高レベルの暗号化と認証を強制的に使用するようにする必要があります。

デバイスのセキュリティ異常によるゼロデイ攻撃

wIPS による解決

Cisco Adaptive Wireless IPS は、多数のセキュリティ IDS/IPS ポリシーに違反するデバイスを検出します。指定の期間内にこのデバイスで多数のセキュリティ IDS/IPS 違反が発生したか、またはさまざまなアラームの閾値設定に指定されている突然のパーセンテージ上昇が発生しています。詳しい分析のためにデバイスをモニタおよび特定し、デバイスがエンタープライズ ワイヤレス ネットワークを何らかの形（攻撃または脆弱性）で侵害していないかどうかを確認することを推奨します。不正デバイスの場合、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、デバイスを検出する不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースします。

XSS SSID をブロードキャストするデバイス

アラームの説明と考えられる原因

クロスサイト スクリプティングの脆弱性はよく知られており、Web アプリケーションを標的にして基礎となるサーバまたは Web アプリケーション自体にアクセスしようとする自明の攻撃から構成されます。これは、クライアント側のスクリプトをユーザが表示する Web ページに挿入することで実行されます。

この攻撃は、クライアント側コードを SSID としてブロードキャストするデバイスを使用して行われます。WLAN 監視システムが悪意のある SSID を取得して記録すると、システムが Web ベースでクロスサイト スクリプティングの脆弱性がある場合、悪意的な SSID を持つデバイスをクリックするとそのシステムの脆弱性が悪用されます。

wIPS による解決

Cisco Enterprise は、ワイヤレス ネットワークで、悪意のある Cross-Site Scripting （XSS）トラフィックをブロードキャストしているアクセスポイントとアドホックデバイスをモニタします。セキュリティ担当者が Floor Plan 画面を使用してデバイスを特定し位置を確認することをお勧めします。デバイスはワイヤレス環境から速やかに取り除く必要があります。

アクセス ポイントのデバイス プローブ

よく使用されるスキャン ツールには、NetStumbler（新しいバージョン）、MiniStumbler（新しいバージョン）、MACStumbler、WaveStumbler、PrismStumbler、dStumbler、iStumbler、Aerosol、Boingo Scans、WiNc、AP Hopper、NetChaser、Microsoft Windows XP scan などがあります。

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、WLAN をプローブしアソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を試行するワイヤレス デバイスを検出します。

このようなデバイスは、次のいずれかでセキュリティの脅威となる可能性があります。

- ウォードライビング、WiLDing（ワイヤレス LAN 検出）、ウォーチョーキング、ウォーサイクルイング、ウォーライトトレイリング、ウォーブッシング、ウォーフライング。
- 危険な無差別アソシエーションを試行する正規ワイヤレス クライアント。

ウォードライビング、ウォーチョーキング、ウォーウォーキング、ウォーフライングでは次のような行動が行われます。

- ウォードライビング：ワイヤレスのハッカーはウォードライビング ツールを使用してアクセス ポイントを検出し、インターネットに利用されている MAC アドレス、SSID、セキュリティなどの情報を、アクセスポイントの地理的位置情報とともに公開します。
- ウォーチョーキング：ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に共通シンボルを使って WLAN 設定をマーキングします。
- ウォーフライング：ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS で、ビーコンで SSID をブロードキャスト（アナウンス）しているアクセス ポイントを確認してください。

EAP メソッドへの辞書攻撃

アラームの説明と考えられる原因

IEEE 802.1x は、ワイヤレス LAN および有線 LAN の認証のEAP（Extensible Authentication Protocol）フレームワークを定義します。EAP フレームワークにより、柔軟な認証プロトコルを実装できます。一部の 802.1x または WPA 実装では LEAP、MD5、OTP（ワンタイム パスワード）、TLS、TTLS などの認証プロトコルが使用されています。このような認証プロトコルの一部で使用されるユーザ名とパスワードのメカニズムでは、ユーザ名が暗号化されずに送信され、認証チャレンジへの応答にパスワードが使用されます。

ほとんどのパスワード ベースの認証アルゴリズムは、辞書攻撃の影響を受けます。辞書攻撃では、攻撃者が、暗号化されていない 802.1x ID プロトコル交換からユーザ名を獲得します。その後攻撃者は、一般的なパスワードの辞書のすべての単語またはパスワードの可能な組み合わせからユーザのパスワードを推測してネットワーク アクセスを獲得しようとします。辞書攻撃は、パスワードに一般的な単語、名前、またはこの両方の組み合わせと一部の変更（末尾の 1 桁または 2 桁の番号など）がよく使用されることに依存しています。

辞書攻撃がオンラインでアクティブに行われる場合、攻撃者はあらゆるパスワードの組み合わせを繰り返し試行します。オンライン辞書攻撃を防止するには、認証サーバ（RADIUS サーバ）で使用可能なロックアウト メカニズムを利用し、無効なログインが特定の回数を超えた後にユーザをロックアウトします。辞書攻撃はオフラインで行われることもあります。この場合、攻撃者は正常に完了した認証チャレンジ プロトコル交換をキャプチャし、チャレンジ応答に対してあらゆるパスワードの組み合わせを突き合わせます。オンライン攻撃とは異なり、オフライン攻撃は容易に検出されません。強力なパスワードポリシーを採用し、定期的にユーザパスワードの有効期限が切れるように設定することで、オフライン攻撃ツールによる攻撃の成功率を大幅に削減します。

wIPS による解決

Cisco Adaptive Wireless IPS はオンライン辞書攻撃を検出するため、802.1x 認証プロトコル交換とユーザ ID の利用状況を追跡します。辞書攻撃が検出されると、ユーザ名と攻撃ステーションの MAC アドレスがアラーム メッセージに示されます。

Cisco Adaptive Wireless IPS は、ユーザ名とパスワードに基づく認証方式から、シスコをはじめとする多くのベンダーによりサポートされている暗号化トンネルに基づく認証方式（PEAP や EAP-FAST など）に切り替えるように指示します。

疑似アクセス ポイントの検出

アラームの説明と考えられる原因

Fake AP ツールは、NetStumbler、Wellenreiter、MiniStumbler、Kismet などを利用するウォードライバをかく乱するためにおとりとして機能することで、WLAN を保護します。このツールは、大量の偽 802.11b アクセス ポイントを偽装するビーコン フレームを生成します。大量のアクセス ポイントに遭遇したウォードライバは、ユーザが展開している本物のアクセス ポイントを特定できなくなります。このツールはウォードライバを阻止するには非常に有効ですが、帯域幅消費、正規クライアント ステーションの誤誘導、WLAN 管理ツールとの干渉といったデメリットがあります。Cisco Adaptive Wireless IPS では、WLAN での Fake AP ツールの使用を推奨しません。

wIPS による解決

Cisco Adaptive Wireless IPS は、管理者が疑似 AP 攻撃ツールを実行しているデバイスを特定し、ワイヤレス環境から除外するための適切な手段を講じることを推奨します。

偽の DHCP サーバの検出

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、DHCP サービスを実行し、気づいていないユーザに IP アドレスを提供するワイヤレス STA を検出します。

クライアントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、デバイスを検出します。

wIPS による解決

Cisco Adaptive Wireless IPS は、DHCP サービスを実行し、気づいていないユーザに IP アドレスを提供するワイヤレス STA を検出します。

クライアントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、デバイスを検出します。

高速 WEP クラック（ARP リプレイ）の検出

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは WEP キー クラッキング攻撃に対して脆弱であることがよく知られています（『Weaknesses in the Key Scheduling Algorithm of RC4 - I』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照）。

攻撃者によって WEP 秘密キーがクラックされると、暗号化による保護がなくなり、結果としてデータ プライバシーが侵害されます。WEP キーはユーザにより指定され、24 ビット IV（初期化ベクトル）にリンクされる秘密キーからなり、ほとんどの場合 64 ビットまたは 128 ビットです（ベンダーによっては 152 ビット暗号化も提供されています）。送信ステーションが決定する IV を頻繁に再利用したり、連続するフレームで再利用したりできるので、ワイヤレス侵入者がこの秘密キーを復元できる可能性が高まります。

WEP キーに対する攻撃で最も重要な点は、キーのサイズです。十分な固有 IV の数は、64 ビット WEP キーで約 15 万、128 ビット WEP キーで約 50 万から 100 万です。トラフィックが不十分な場合に、ハッカーはこのような攻撃を行うために十分なトラフィックを生成する手法を編み出しています。これは、arp-request パケットに基づくリプレイ アタックと呼ばれます。このようなパケットの長さは一定であるため、容易に検出できます。1 つの正規 arp-request パケットをキャプチャして繰り返し再送信すると、他のホストは暗号化された応答で対応し、新しい（そして弱い場合もある）IV を提供します。

wIPS による解決

Cisco Adaptive Wireless IPS は弱い WEP 実装について警告し、IV 使用の問題を訂正するためのデバイス ファームウェア アップグレードがデバイス ベンダーからリリースされている場合はこのアップグレードを推奨します。企業 WLAN ネットワークで TKIP（Temporal Key Integrity Protocol）暗号化メカニズムを使用して WEP の脆弱性を保護することが理想的です。TKIP はほとんどのエンタープライズ レベル ワイヤレス装置でサポートされています。TKIP 対応デバイスはこのような WEP キー攻撃の対象となりません。

Cisco WCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、弱い暗号化または認証を使用するように設定されているアクセス ポイントを事前予防的に報告します。自動セキュリティ脆弱性スキャンの詳細については、Cisco WCS オンライン ヘルプを参照してください。

フラグメンテーション攻撃

アラームの説明と考えられる原因

暗号化に静的 WEP キーを使用する WLAN デバイスは、さまざまな WEP クラッキング攻撃の対象となるリスクがあることはよく知られています。詳しくは、『Weaknesses in the Key Scheduling Algorithm of RC4 - I』（Scott Fluhrer、Itsik Mantin、および Adi Shamir 著）を参照してください。

wIPS による解決

Cisco Adaptive Wireless IPS は、進行中のフラグメンテーション攻撃の可能性を検出すると警告を出します。また、企業環境で WEP を使用せず、ネットワークのセキュリティ ホールを回避するための処置を講じ、ワイヤレスネットワークインフラストラクチャとデバイスをアップグレードしてより安全な IEEE 802.11i 標準を使用することを推奨します。

HT Intolerant Degradation Service

アラームの説明と考えられる原因

802.11n の実装には、レガシー実装よりもワイヤレス範囲と速度を大幅に向上できる可能性がありますが、これらの利点は、1 台でもレガシー デバイスがネットワークに導入されると、簡単に失われたり、相殺されたりします。この状況を回避するために、wIPS サーバは、n 個の対応デバイス間において n 以下の速度で送信されているパケットを検出した場合に、HT-Intolerant Degradation of Service アラームを生成します。

アラームの説明と考えられる原因

802.11n の実装には、レガシー実装よりもワイヤレス範囲と速度を大幅に向上できる可能性がありますが、これらの利点は、1 台でもレガシー デバイスがネットワークに導入されると、簡単に失われたり、相殺されたりします。この状況を回避するために、wIPS サーバは、n 個の対応デバイス間において n 以下の速度で送信されているパケットを検出した場合に、HT-Intolerant Degradation of Service アラームを生成します。

ハニーポット AP の検出

アラームの説明と考えられる原因

企業環境に WLAN を追加すると、ネットワーク セキュリティに対するまったく新たな脅威が発生します。壁を通過し、意図した境界を超える RF 信号は、ネットワークを無認可のユーザに公

開する可能性があります。不正アクセス ポイントが原因で、企業ネットワーク全体が外部からの侵入や攻撃の危険にさらされる可能性があります。不正アクセス ポイントの脅威以外にも、アクセス ポイントの設定ミスや未設定、DoS（サービス拒否）攻撃といったさまざまなワイヤレス セキュリティ リスクや侵入の可能性が存在します。

企業のワイヤレス ネットワークを対象とする最も効果的な攻撃の 1 つに、「ハニー ポット」アクセス ポイントを使用した攻撃があります。攻撃者は NetStumbler、Wellenreiter、MiniStumbler などのツールを使い、企業アクセス ポイントの SSID を検出します。次に建物の外（可能な場合は同じ建物の中）にアクセス ポイントをセットアップし、検出した企業 SSID をブロードキャストします。何も知らないクライアントが、信号強度が高いこの「ハニーポット」アクセスポイントに接続します。アソシエートが完了すると、トラフィックが「ハニーポット」アクセスポイントを経由するため、攻撃者はクライアント ステーションに対して攻撃を実行します。

wIPS による解決

Cisco Adaptive Wireless IPS により「ハニー ポット」アクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

Hot-Spotter ツールの検出（潜在的なワイヤレス フィッシング）

アラームの説明と考えられる原因

ホットスポットとは、Wi-Fi ネットワーク アクセスが一般向けに開放されている場所を指します。ホットスポットは空港、ホテル、喫茶店をはじめ、ビジネスマンが集まることが多い場所にあります。現在、ホットスポットは出張旅行者にとっては最も重要なネットワーク アクセス サービスです。正規のアクセス ポイントに接続してサービスを利用するには、ワイヤレス対応ラップトップまたは携帯機器が必要です。ほとんどのホットスポットで、ユーザはアクセス ポイントの接続に高度な認証メカニズムを設定する必要はありません。ログイン用の Web ページを使用するだけです。エントリの条件は、利用者が利用料金を支払っているかどうかだけです。ワイヤレス ホットスポット環境では誰も信用すべきではありません。現在のセキュリティ上の懸念から、一部の WLAN ホットスポット ベンダーはユーザ ID の検証に 802.1x 以上の認証メカニズムを採用しています。

ホットスポット ネットワークの 4 つの基本コンポーネントを次に示します。

- ホットスポット利用ユーザ：ワイヤレス対応のラップトップまたは携帯機器を所持し、ホットスポット ネットワークにアクセスするための有効なログイン情報を持つユーザ。
- WLAN アクセス ポイント：ホットスポット実装に応じて、SOHO ゲートウェイまたはエンタープライズ レベル アクセス ポイントのいずれかです。
- ホットスポット コントローラ：ユーザ認証に対応し、課金情報の収集、使用時間の追跡、機能のフィルタリングなどを行います。これは、独立したマシンで機能するか、またはアクセス ポイントへの組み込みが可能です。

- 認証サーバ：利用者のログイン資格情報を保持します。ほとんどの場合、ホットスポット コントローラは認証サーバを使用して利用ユーザのクレデンシャルを検証します。

Hotspotter は、採用されている暗号メカニズムに依存せずに、ワイヤレス クライアントに対する侵入操作を自動化します。攻撃者はHotspotterツールを使用してワイヤレス ネットワークでプローブ要求フレームを受動的にモニタし、Windows XP クライアント ネットワークの SSID を特定します。

攻撃者は優先ネットワーク情報を獲得した後に、提供されるよく使用されるホットスポット ネットワーク名のリストに対してネットワーク名（SSID）を照合します。一致するネットワーク名が見つかると、Hotspotter クライアントがアクセス ポイントとして動作します。クライアントはこの状況を知らずにこの疑似アクセス ポイントを認証してアソシエートします。

クライアントがアソシエートされたら、DHCP デーモンやその他のスキャンを新たなターゲットに対して実行するコマンド（スクリプトなど）を実行するように Hotspotter ツールを設定できます。

異なる環境（ホームとオフィスなど）で稼働しているが、Windows XP ワイヤレス接続設定で同じホットスポット SSID を使用するように設定されているクライアントも、この攻撃の影響を受けます。クライアントはその SSID を使用してプローブ要求を送信するため、ツールに対して脆弱になります。

wIPS による解決

Cisco Adaptive Wireless IPS により不正なアクセス ポイントが特定、報告されると、WLAN 管理者は統合無線物理ロケーション検出機能を使用するか、または不正ロケーション検出プロトコル（RLDP）またはスイッチポート トレースを使用して有線ネットワーク上のデバイスをトレースし、不正なデバイスを検出します。

Identical Send and Receive Address

アラームの説明と考えられる原因

攻撃者は、企業ネットワーク内のワイヤレス アクティビティを抑制するために、ワイヤレス パケットを変更して（パケットの送信元および宛先 MAC 情報に対する変更など）、さまざまな異なる特性をエミュレートすることがよくあります。これらのフィールドが同一の場合、IT 担当者に潜在的な攻撃について警告するために Identical Send and Receive Address アラームが生成されます。

wIPS による解決

通常のネットワーク環境では、パケットの送信元と宛先が同一になることはありません。そのため、企業の管理者は迅速な措置をとり、変更されたパケットの根本原因を特定する必要があります。

Improper Broadcast Frames

アラームの説明と考えられる原因

802.11 の標準の導入では、特定のフレーム（ユニキャスト フレームとも呼ばれる、ACK など）を個別の宛先に送信し、他のフレームをワイヤレス導入内のすべての受信者に「ブロードキャスト」することができます。一般的に、この 2 つのカテゴリはオーバーラップできません。たとえば、Association Request フレームをすべてのリスニング デバイス向けのブロードキャストとして送信することはできません。このシナリオでは、wIPS サーバは、潜在的な問題をスタッフに警告するために Improper Broadcast Frames アラームを生成します。

Improper Broadcast Frames

Karma ツールの検出

アラームの説明と考えられる原因

Karma ツールを使用すると、ワイヤレス攻撃者は、検出されたプローブ要求に応答するソフト AP としてクライアントを設定できます。この実装は、複数の異なるネットワーク（仕事の場合は SSID「Corporate」、家庭での使用の場合は SSID「Home」など）に接続するように設定されているステーションからのクエリに応答するように設計されています。この例では、ソフト AP は、クライアントが仕事中の場合に「Home」のプローブに応答するように設定することができます。この方法で、攻撃者は企業クライアントをだまし、潜在的に機密のネットワーク トラフィックを疑似 AP にルーティングします。

wIPS による解決

wIPS サーバは、企業環境内でこのツールを使用しているワイヤレス ステーションが検出されたときに Karma ツール アラームを生成します。ユーザは攻撃しているデバイスを特定して、ただちに取り除く必要があります。

中間者攻撃の検出

アラームの説明と考えられる原因

中間者（MITM）攻撃は、最も一般的な 802.11 攻撃の 1 つであり、企業の機密情報や個人情報がハッカーに漏れる可能性があります。MITM 攻撃ではハッカーは 802.11 ワイヤレス アナライザを使用し、WLAN 上で送信される 802.11 フレームをモニタします。ハッカーはアソシエーション フェーズでワイヤレス フレームをキャプチャし、ワイヤレス クライアント カードとアクセス ポ

イントの IP アドレスと MAC アドレスの情報、クライアントのアソシエーション ID、ワイヤレスネットワークの SSID を取得します。

MITM 攻撃を実行するための一般的な方法では、ハッカーはスプーフィングされたデアソシエーションフレームまたは認証解除フレームを送信します。ハッカーステーションがクライアントの MACアドレスをスプーフし、アクセスポイントとのアソシエートを継続します。同時にハッカーはスプーフされたアクセス ポイントを別のチャネルにセットアップし、クライアントとのアソシエーションを維持します。これにより、有効なクライアントとアクセス ポイント間のすべてのトラフィックがハッカーのステーションを素通りできます。

最もよく使用される MITM 攻撃ツールの 1 つに Monkey-Jack があります。

wIPS による解決

Cisco Adaptive Wireless IPS は、ハッカーによる MITM 攻撃を阻止するために強力な暗号化および認証メカニズムを使用することを推奨します。このような攻撃を回避する方法の 1 つに、MAC アドレス除外リストを使用し RF チャネル環境をモニタして、MAC のスプーフを防止する方法があります。

また、Cisco 管理フレーム保護（MFP）は MITM 攻撃に対して完全な予防的保護を提供します。MFP の詳細については、『Cisco Wireless Control System Configuration Guide』または WCS オンライン ヘルプを参照してください。

NetStumbler の検出

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。ハッカーが新しいバージョンの NetStumbler ツールを使っている場合、「アクセス ポイントをプローブするデバイス」アラームが生成されます。古いバージョンの場合、Cisco Adaptive Wireless IPS は「NetStumbler の検出」アラームを生成します。

NetStumbler は、ウォードライビングとウォーチョーキングに最も広く使用されているツールです。ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティの情報などを、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセスポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。このツールは Windows 2000、Windows XP、およびこれ以降のバージョンが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。

オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

Cisco WCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、SSID をブロードキャストするように設定されているアクセス ポイントをすべて報告します。自動セキュリティ脆弱性スキャンの詳細については、WCS オンライン ヘルプを参照してください。

NetStumbler 犠牲者の検出

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、NetStumbler ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。ハッカーが新しいバージョンの NetStumbler ツールを使っている場合、「アクセス ポイントをプローブするデバイス」アラームが生成されます。古いバージョンの場合、Cisco Adaptive Wireless IPS は「NetStumbler の検出」アラームを生成します。

NetStumbler は、ウォードライビング、ウォーウォーキング、ウォーチョーキングに最も広く使用されているツールです。ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティの情報などを、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、不正処理をハッカーが車ではなく徒歩で行います。NetStumbler Web サイト（http://www.netstumbler.com/）は、ウォーウォーカーが重たいラップトップを持ち歩かずにすむように、Pocket PC ハードウェアで使用できる MiniStumbler ソフトウェアを提供します。このツールは Windows 2000、Windows XP、およびこれ以降のバージョンが稼働するマシンで実行できます。また、よく使用される別のスキャン ツールである Wellenreiter よりも多くのカードがサポートされます。ウォーウォーカーは、MiniStumbler や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライ

ングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

Cisco Adaptive Wireless IPS は、NetStumbler を実行するステーションが企業アクセス ポイントにアソシエートされていることを検出すると、ユーザに対して警告を出します。

Publicly Secure Packet Forwarding（PSPF）違反

アラームの説明と考えられる原因

Publicly Secure Packet Forwarding（PSPF）はワイヤレス クライアント同士の通信を無効にする機能であり、WLAN アクセス ポイントに実装されています。PSPF が有効になっている場合、ワイヤレス ネットワーク上のクライアント デバイス同士は通信できません。

ほとんどの WLAN 環境では、ワイヤレス クライアントは有線ネットワーク上の Web サーバなどのデバイスとだけ通信します。PSPF を有効にすると、ワイヤレス クライアントをワイヤレス侵入者によるハッキングから保護できます。PSPF は特に、空港、ホテル、喫茶店、大学構内など、認証がなく誰もがアクセス ポイントにアソシエートできるワイヤレス パブリック ネットワーク（ホットスポット）環境でワイヤレス クライアントを保護する場合に効果的です。PSPF 機能により、クライアント デバイスが誤ってワイヤレス ネットワーク上の他のクライアント デバイスとファイルを共有することが防止されます。

wIPS による解決

Cisco Adaptive Wireless IPS は PSPF 違反を検出します。ワイヤレス クライアントが別のワイヤレス クライアントと通信しようとすると、Cisco Adaptive Wireless IPS は侵入攻撃の可能性に関するアラームを生成します。WLAN にワイヤレス プリンタまたは VoWLAN アプリケーションを導入している場合、このようなアプリケーションはクライアント間ワイヤレス通信を利用するため、このアラームは適用されません。

プローブ要求 ファジング フレームの検出

アラームの説明と考えられる原因

802.11 ファジングは、無効、予想外、またはランダムなデータを 802.11 フレームに取り入れ、修正されたフレームを送信するプロセスです。このプロセスは送信先のデバイスに、ドライバのクラッシュ、オペレーティング システムのクラッシュ、スタック ベースのオーバーフローなど予想外の動作を引き起こす場合があり、影響を受けたシステムで任意コードを実行できる状態にします。802.11 フレームのファジングに基づく脆弱性のさまざまな報告事例については、CVE Web サイト（http://cve.mitre.org/index.html）を参照してください。

システムは、各プローブ要求フレームを検査して、ファジング アクティビティの兆候を調べます。プローブ要求ファジングの一般的な形式は、SSID フィールドを 32 バイトの制限を超えて拡

大し、サポートされるデータ レートを無効なレートに変更するものです。システムはこれらの異常を検索し、フィールド値が 802.11 仕様の範囲を超えると、プローブ要求ファジング アラームを生成します。

プローブ応答 ファジング フレームの検出

アラームの説明と考えられる原因

802.11 ファジングは、無効、予想外、またはランダムなデータを 802.11 フレームに取り入れ、修正されたフレームを送信するプロセスです。このプロセスは送信先のデバイスに、ドライバのクラッシュ、オペレーティング システムのクラッシュ、スタック ベースのオーバーフローなど予想外の動作を引き起こす場合があり、影響を受けたシステムで任意コードを実行できる状態にします。802.11 フレームのファジングに基づく脆弱性のさまざまな報告事例については、CVE Web サイト（http://cve.mitre.org/index.html）を参照してください。

システムは、各プローブ応答フレームを検査して、ファジング アクティビティの兆候を調べます。プローブ応答ファジングの一般的な形式は、SSID フィールドを 32 バイトの制限を超えて拡大し、サポートされるデータ レートを無効なレートに変更するものです。システムはこれらの異常を検索し、フィールド値が 802.11 仕様の範囲を超えると、プローブ応答ファジング アラームを生成します。

wIPS による解決

システムは、ワイヤレス ネットワークで、プローブ応答ファジングに該当するトラフィックをモニタします。デバイスを特定しオフラインにすることが推奨されます。

ソフト AP またはホスト AP の検出

ホスト AP ツール：Cqure AP

アラームの説明と考えられる原因

ホットスポットとは、Wi-Fi ネットワーク アクセスが一般向けに開放されている場所を指します。ホットスポットは空港、ホテル、喫茶店をはじめ、ビジネスマンが集まることが多い場所にあります。現在、ホットスポットは出張旅行者にとっては最も重要なネットワーク アクセス サービスです。正規のアクセス ポイントに接続してサービスを利用するには、ワイヤレス対応ラップトップまたは携帯機器が必要です。ほとんどのホットスポットで、ユーザはアクセス ポイントの接続に高度な認証メカニズムを設定する必要はありません。ログイン用の Web ページを使用するだけです。エントリの条件は、利用者が利用料金を支払っているかどうかだけです。ワイヤレス ホットスポット環境では誰も信用すべきではありません。現在のセキュリティ上の懸念から、一部の WLAN ホットスポット ベンダーはユーザ ID の検証に 802.1x 以上の認証メカニズムを採用しています。

WLAN ホットスポット ネットワークの基本コンポーネント

ホットスポット ネットワークの 4 つの基本コンポーネントは、次のとおりです。

- ホットスポット利用ユーザ：ワイヤレス対応のラップトップまたは携帯機器を所持し、ホットスポット ネットワークにアクセスするための有効なログイン情報を持つユーザ。
- WLAN アクセス ポイント：ホットスポット実装に応じて、SOHO ゲートウェイまたはエンタープライズ レベル アクセス ポイントのいずれかです。
- ホットスポット コントローラ：ユーザ認証、課金情報の収集、利用時間の追跡、機能のフィルタリングを実行します。これは独立したマシンであるか、またはアクセス ポイント自体に組み込まれています。
- 認証サーバ：利用ユーザのログイン クレデンシャルが保管されています。ほとんどの場合、ホットスポット コントローラは認証サーバを使用して利用ユーザのクレデンシャルを検証します。

Hotspotter は、採用されている暗号メカニズムに依存せずに、ワイヤレス クライアントに対する侵入操作を自動化します。攻撃者は Hotspotter ツールを使用してワイヤレス ネットワークでプローブ要求フレームを受動的にモニタし、Windows XP クライアント ネットワークの SSID を特定します。

攻撃者は優先ネットワーク情報を獲得した後に、提供されるよく使用されるホットスポット ネットワーク名のリストに対してネットワーク名（SSID）を照合します。一致するネットワーク名が見つかると、Hotspotter クライアントがアクセス ポイントとして動作します。クライアントはこの状況を知らずにこの疑似アクセス ポイントを認証してアソシエートします。

クライアントがアソシエートされたら、DHCP デーモンやその他のスキャンを新たなターゲットに対して実行するコマンド（スクリプトなど）を実行するように Hotspotter ツールを設定できます。

異なる環境（ホームとオフィスなど）で稼働しているが、Windows XP ワイヤレス接続設定で同じホットスポット SSID を使用するように設定されているクライアントも、この攻撃の影響を受けます。クライアントはその SSID を使用してプローブ要求を送信するため、ツールに対して脆弱になります。

wIPS による解決

ソフト AP、またはソフトウェアのアクセス ポイントは、不正デバイスとして扱う必要があります。次の手順は、この脅威を排除するために役立ちます。

- 統合無線物理ロケーション検出機能を使用して不正なデバイスを特定します。
- すべてのデバイスのソフト AP 接続を防ぐワイヤレス封じ込め
- Rogue Location Discovery Protocol（RLDP）またはスイッチ ポート トレーシングを使用して、有線ネットワークのデバイスを追跡し、不正なデバイスを検出します。

スプーフされた MAC アドレスの検出

アラームの説明と考えられる原因

スプーフィングされた MAC アドレスが検出された場合、ハッカーが出荷時割り当て済みのワイヤレス MAC アドレスを変更することで、接続権限を持つ有効なユーザになりすましてアクセス制限付きワイヤレス ネットワークにアクセスするか、またはワイヤレス ネットワークで自らの存在を隠そうとする攻撃と考えられます。

スプーフィングされた MAC アドレス攻撃には、クライアント ベースと AP ベースの 2 種類があります。クライアント ベースのスプーフィングされた MAC アドレス攻撃では、クライアントが有効なユーザになりすますことができます。たとえば、ワイヤレスのハッカーがすでに接続しているクライアントのワイヤレス MAC アドレスをスプーフィングしてアクセス制限付きホットスポットにアクセスする、接続の「ただ乗り」などです。他にも、ホテル環境で料金を払って接続しているユーザのワイヤレス MAC アドレスをスプーフィングすることで、支払処理を迂回してワイヤレス ネットワークに接続しようとするハッカーなどの例があります。

もう 1 つのスプーフィングされた MAC アドレス攻撃は、AP ベースです。この場合、ハッカーは企業のアクセス ポイントの MAC アドレスをスプーフィングすることで、ワイヤレス ネットワーク上で自らの存在を隠そうとします。これは、典型的な不正シナリオです。

疑わしい営業時間外のトラフィックの検出

アラームの説明と考えられる原因

ワイヤレス セキュリティ突破試行を検出する方法の 1 つに、ワイヤレス トラフィックが発生することにはなっていない時間とワイヤレス利用状況を照合する方法があります。wIPS サーバはこのアラームで設定された営業時間を基準にしてトラフィック パターンをモニタし、異常が検出されるとアラートを生成します。営業時間外に wIPS サーバにより追跡される疑わしいワイヤレス利用には、次のものがあります。

- セキュリティ侵害を示す可能性があるオフィス WLAN への認証要求またはアソシエート要求を発行するクライアント ステーション。
- ワイヤレス ネットワーク上での疑わしいダウンロードまたはアップロードを示す可能性があるワイヤレス データ トラフィック。

wIPS による解決

wIPS をグローバルに導入する場合、設定可能な営業時間範囲は現地時間で定義されます。管理を容易にするため、アクセス ポイントまたはセンサーを特定の時間帯に基づいて設定できます。オフィスと製造現場が混在する WLAN では、オフィスの WLAN SSID にオフィスの営業時間を定義し、製造現場の WLAN SSID に別の（午前 6 時から午後 9 時までなど）営業時間を定義できます。

このアラームがトリガーされたら、管理者は、疑わしいトラフィックの原因デバイスを探し、その位置を特定して適切な手順でワイヤレス環境から削除する必要があります。

ベンダー リストによる未承認アソシエーション

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS では、ネットワーク管理者がベンダー情報をポリシー プロファイルに組み込むことができます。これにより、WLAN 上にある承認ベンダー以外のステーションを検出できます。このようなポリシー プロファイルを作成すると、未承認ベンダーによりステーションとアクセス ポイントがアソシエートされると常にアラームが生成されます。次の図を参照してください。

この図の ACL-1 のアクセス ポイントはシスコ製のステーションとだけアソシエート可能であり、ACL-2 のアクセス ポイントは Intel 製のステーションとだけアソシエート可能です。この情報は wIPS システムのポリシー プロファイルに入力されます。アクセス ポイントとシスコおよび Intel 以外のベンダーのステーションとのアソシエーションはすべて承認されず、アラームが生成されます。

企業WLAN環境では、不正なステーションが原因でセキュリティの問題が発生し、ネットワークパフォーマンスが低下します。このような不正なステーションは空間を占有し、ネットワーク帯域幅をめぐって競合します。アクセス ポイントが対応できるステーションの数が限られているため、アクセス ポイントは対応するステーションの数が上限に達すると、ステーションからのアソシエート要求を拒否します。多数の不正なステーションに対応しており、これ以上のステーションに対応できないアクセス ポイントは、ネットワークにアクセスする正規のステーションを拒否します。不正なステーションによってよく引き起こされる問題には、接続の問題やパフォーマンス低下があります。

wIPS による解決

Cisco Adaptive Wireless IPS は、アクセス ポイントとステーション間で非準拠ステーションが関与する未承認アソシエーションについて、このアラームを使用してネットワーク管理者に警告します。このアラームが生成されたら、未承認ステーションを特定し、この問題を解決するための措置をとる必要があります。この措置の 1 つに、不正の封じ込め処理を使用してブロックする方法があります。

未承認アソシエーションの検出

アラームの説明と考えられる原因

通常、企業ネットワーク環境では従業員が導入した不正なアクセス ポイントはネットワークの標準導入プラクティスに従っておらず、ネットワークの整合性を侵害します。このような不正なアクセス ポイントはネットワーク セキュリティの抜け穴であり、侵入者はこのアクセス ポイント

からが企業の有線ネットワークに容易にハッキングできるようになります。多くのワイヤレス ネットワーク管理者が抱える主な課題の 1 つに、ACL に登録されているステーションと不正なアクセス ポイントの間の未承認アソシエーションがあります。ステーションと不正なアクセス ポイントの間でデータが転送されるため、ハッカーが機密情報を盗み出すことが可能になります。

不正なステーションはセキュリティの問題を引き起こし、ネットワーク パフォーマンスを低下させます。このような不正なステーションは空間を占有し、ネットワーク帯域幅をめぐって競合します。アクセス ポイントが対応できるステーションの数が限られているため、アクセス ポイントは対応するステーションの数が上限に達すると、ステーションからのアソシエート要求を拒否します。多数の不正なステーションに対応しており、これ以上のステーションに対応できないアクセス ポイントは、ネットワークにアクセスする正規のステーションを拒否します。不正なステーションによってよく引き起こされる問題には、接続の妨害やパフォーマンス低下があります。

wIPS による解決

アクセス ポイントとステーション間の未承認アソシエーションがネットワーク上で検出されると、Cisco Adaptive Wireless IPS はネットワーク管理者に対してこのアラームで通知します。WLC の新しい「MAC アドレス学習」機能はこの違反の発生を阻止します。この機能を有効にすることをお勧めします。

Wellenreiter の検出

アラームの説明と考えられる原因

Cisco Adaptive Wireless IPS は、Wellenreiter ツールを使用して匿名アソシエート（任意の SSID のアクセス ポイントに対するアソシエーション要求など）を実行するために WLAN をプローブするワイヤレス クライアント ステーションを検出します。

Wellenreiter は、ウォードライビングとウォーチョーキングによく利用されるツールです。ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティの情報などを、アクセス ポイントの位置情報と共にインターネット上で公開します。ウォーチョーキングでは、ハッカーが WLAN アクセス ポイントを検出し、公共の場所に上に示す共通シンボルを使って WLAN 設定をマーキングします。ウォーウォーキングはウォードライビングに似ていますが、ハッカーが車ではなく徒歩で徘徊します。ウォーウォーカーは、Wellenreiter や類似製品を使ってショッピングセンターや大型小売店舗を徘徊します。ウォーフライングは、上空からのワイヤレス ネットワークのスニッフィングです。高出力アンテナを備えた自家用飛行機から同じ機器を使います。オーストラリアのパースを本拠地とするウォーフライングのグループが、高度 1,500 フィートから電子メールとインターネット リレー チャット セッションを傍受した例が報告されています。

このツールは、Prism2、Lucent、およびシスコ ベースのカードに対応しています。このツールは SSID と WEP 機能をブロードキャストしているインフラストラクチャとアドホック ネットワークを検出し、ベンダー情報を自動的に提供することができます。また、ethereal/tcpdump 互換ダンプ ファイルとアプリケーション savefile を作成します。GPS にも対応しています。ユーザは Wellenreiter の Web サイトからツールをダウンロードできます。

wIPS による解決

アクセス ポイントがこれらのハッキング ツールで検出されないようにするには、SSID をブロードキャストしないようにアクセス ポイントを設定します。Cisco Adaptive Wireless IPS を使用して、ビーコンで SSID をブロードキャストしているアクセス ポイントを確認できます。

Cisco WCS からも自動セキュリティ脆弱性スキャン機能が提供されています。この機能は、SSID をブロードキャストするように設定されているアクセス ポイントをすべて報告します。自動セキュリティ脆弱性スキャンの詳細については、WCS オンライン ヘルプを参照してください。

WiFi Protected Setup Pin ブルートフォース

アラームの説明と考えられる原因

WiFi Protected Setup は、民生グレードのアクセス ポイントの大半に装備される機能で、複雑なパスワードを必要とせずにデバイスを容易にセットアップできます。この機能では、ユーザは押しボタンを使うか、またはアクセス ポイントの裏面にある PIN を入力して接続できます。2011 年 12 月に、Stefan Viehböck によって脆弱性が公表され、Craig Heffner も単独でそれを発見していました。この脆弱性は、デバイスの PIN だけを必要とする外部レジストラにあります。このモードは、ピンに対するブルートフォース攻撃を受けやすくなります。現在も、この脆弱性を利用する 2 つの有効なツールが出回っています。

攻撃の背景には、PIN 認証が失敗すると、アクセス ポイントが EAP-NACK メッセージをクライアントに送信するという考え方があります。攻撃者はこの EAP-NACK メッセージを利用して、PIN の前半が正しいかどうかを判断できます。PIN のチェックサムである PIN の最後の数字は自明です。これにより、PIN のブルートフォース回数は 11,000 回まで下がります。

アクセス ポイントの WiFi Protected Setup の外部レジストラ機能を無効にすることを推奨します。ほとんどの製造メーカは、デフォルトでこの機能をオンにしています。

wIPS による解決

システムは、ワイヤレス ネットワークで、WiFi Protected Setup Pin ブルートフォースに該当するトラフィックをモニタします。デバイスを特定しオフラインにすることが推奨されます。

WiFiTap ツールの検出

アラームの説明と考えられる原因

WiFiTap ツールを使用すると、ワイヤレス攻撃者は、企業 AP に接続せずに、他のクライアントと直接通信するようにクライアントを設定できます。この実装により、攻撃者は、企業ネットワークに設定されているセキュリティ対策をすべて迂回して、個別のクライアントに攻撃することが

できます。これで、攻撃者は犠牲者のクライアント ステーションに保存されているすべてのファイルと情報にアクセスできます。

wIPS による解決

wIPS サーバは、WiFiTap ツールの使用をモニタして、使用を検出した場合にアラームを生成します。ユーザは、攻撃しているデバイスを特定し、ワイヤレス環境から取り除く必要があります。

パフォーマンス違反

WLAN のパフォーマンス効率は、常に RF 環境の変動とクライアント デバイスの移動の影響を受けます。注意深くモニタされ、適切に調整されている WLAN システムでは、適切に管理されていない WLAN システムよりも高いスループットを実現できます。Cisco wIPS は、WLAN を継続的にモニタし、ワイヤレス管理者に問題の兆候を早期に警告することで、WLAN のパフォーマンスと効率を維持します。

Cisco wIPS の機能を最大限に活用するために、WLAN 導入仕様に最も適したものになるようにパフォーマンス アラームをカスタマイズできます。

パフォーマンス違反には、次のサブカテゴリがあります。

チャネルまたはデバイスの過負荷

WLAN テクノロジーは、無線周波数スペクトルを、元の10 Mbps イーサネット テクノロジーに類似する共有物理メディアとして使用します。最新の 802.11a および 802.11g WLAN 規格の場合でも、54 Mbps の共有メディア帯域幅の制限があります。実際にはこの上限は、必要な MAC プロトコル オーバーヘッド、フレーム間スペース、コリジョンおよびランダムな送信バックオフを考慮すると、さらに大幅に低くなります。

無線メディアには、独自の帯域幅制限があります。WLAN アクセス ポイントには、大量のトラフィックまたは多数の関連付けられているクライアントにより過負荷となる限界があります。 有線 LAN のように、マルチキャストおよびブロードキャスト フレームが多すぎると、WLAN デバイスの過負荷の原因になります。過負荷状態のデバイスでは、パフォーマンスが低下し接続の問題が発生します。たとえば、多数のクライアントによる AP アソシエーション テーブル オーバーフローなどです。

チャネル帯域幅の制限や WLAN デバイス リソース容量の限界があっても、Cisco wIPS は、負荷を監視および追跡して円滑な運用を保証します。Cisco wIPS は、プロビジョニングの不足や過度な拡張により WLAN のパフォーマンスが不十分な場合に、アラームを生成し詳細情報を表示します。RF には、ネイバーが隣接チャネルで新しい WLAN デバイス取り付けを行った場合でも、WLAN チャネルの使用率を大幅に増加させる境界はありません。Cisco wIPS は WLAN をモニタして、適切な帯域幅とリソースのプロビジョニングを確保します。

パフォーマンス違反には以下の種類があります。

AP アソシエーションのキャパシティが上限に達しています

アラームの説明と考えられる原因

すべてのWLANアクセスポイントには、アクセスポイントにアソシエートしてワイヤレス・サービスを受けることができるクライアント ステーションの数についてリソース制限があります。通常、この制限は AP でのユーザ設定可能な数です。AP がこの制限に達すると、新しいクライアント アソシエーション要求を受け付けなくなります。

wIPS による解決

Cisco wIPS は、拒否されたアソシエーションの要求と応答をモニタして、アソシエーション障害の原因を判定します。このアラームは、Cisco wIPS が原因について、AP アソシエーション容量のオーバーフローの問題と判断した場合に生成されます。このアラームは、WLAN 構成でのプロビジョニング不足、またはロード バランシングの障害を示しています。

ステーションによる AP の過負荷

アラームの説明と考えられる原因

WLANアクセスポイントは、リソースの制約により、限定された数のクライアントに対してのみサービスを実行できます。限定数に到達すると、以降のクライアントが拒否されるか、または既存のクライアントのパフォーマンスが低下します。WLAN 機器の導入の設計、およびサービスのプロビジョニングを行う場合、この制限を考慮する必要があります。展開後に、ユーザー数の拡大によってこの制限が課題となるため、展開におけるプロビジョニングの不足を常に監視する必要があります。

wIPS による解決

Cisco wIPS は、AP のアクティブなクライアント ステーションを追跡することで、AP ワークロードを監視します。ワークロードのしきい値（アクティブなクライアント セッションのカウント）によって、異なる重大度レベルのアラームを発生するようにシステムを設定できます。たとえば、64 のアクティブなクライアント セッションの警告や、128 のアクティブなクライアント セッションの緊急アラームなどです。

使用率による AP の過負荷

アラームの説明と考えられる原因

WLAN 導入の設計には、AP がサポート可能な最大クライアント数への期待値が含まれます。同様に、AP でサポートされる最大の帯域利用率への期待値もあります。このような期待値を利用し

て、WLANプロビジョニングが十分かどうか、ロードバランシングが効果的かどうかを監視できます。

wIPS による解決

Cisco wIPS は、AP 帯域利用率（発信と着信のトラフィックを合わせたもの）を追跡し、持続的な使用率がユーザ設定のしきい値を超えるとアラームを発生させます。

帯域の過剰な使用率

アラームの説明と考えられる原因

WLAN 環境は、帯域幅に制限のある共有メディアです。802.11b が 11 mbps、802.11a/g が 54 mbps の伝送速度でそれぞれ機能する場合でも、帯域使用率をチャネル単位およびデバイス単位で綿密にモニタし、すべてのクライアント デバイスで十分な WLAN プロビジョニングを確保する必要があります。帯域消費量が多いことは、WLAN が高スループットであることを意味しません。問題となるのは低速な伝送速度で、その原因には認証ユーザがインターネットから音楽や動画をダウンロードする行為などが考えられ、これにより企業ネットワークの帯域幅に目詰まりが起こります。Cisco wIPS は、WLAN 帯域使用率をチャネル単位およびデバイス単位で追跡します。

wIPS による解決

Cisco wIPS は、チャネルおよびワイヤレス デバイスに基づいて、帯域幅使用率を追跡します。帯域幅の計算には、PLCPヘッダー、プリアンブルおよび実際のフレームペイロードが含まれます。CSMA 衝突回避プロトコルにより、100% の使用率に近づくことはほとんど不可能です。60～70% の使用率は非常に高いと見なされ、きわめて高速な伝送などの、プロビジョニングの改善や効率性の強化が必要になります。ユーザ定義のしきい値（使用率%）を超えると、Cisco wIPS はこのアラームを発生させます。この問題を解決するための適切な手段を講じてください。たとえば、インターネットからの過剰なファイル ダウンロードなどでこの問題の原因となっているユーザを特定します。

チャネル上の過剰なマルチキャスト/ブロードキャスト

アラームの説明と考えられる原因

有線ネットワークのように、WLAN に過剰なブロードキャスト フレームおよびマルチキャスト フレームがあると、WLAN 上のすべてのデバイスに余分な負荷がかかります。WLAN は、有線ネットワークよりも、マルチキャストおよびブロードキャスト フレームに影響されやすい環境です。これは、すべてのマルチキャストおよびブロードキャスト フレームが低速で送信されるためです（802.11b WLAN では 1 または 2 Mbps など）。このように低速な伝送は、WLAN の帯域幅をより多く消費します。帯域幅の効率性に加えて、低速なマルチキャストおよびブロードキャスト フレームでは伝送処理の完了に時間がかかるので、ワイヤレス メディアが空くのを待つ他のデバイスに対してより大きな遅延をもたらします。過剰なマルチキャストおよびブロードキャスト フ

レームによって、VoIP のような遅延に影響されやすい WLAN アプリケーションにジッタが発生します。たとえば、1000 バイトのブロードキャスト フレームは 1 Mpbs での伝送に 8 ミリ秒以上かかり、これは音声アプリケーションには大きな遅延の原因になります。

wIPS による解決

Cisco wIPS は、チャネルまたはデバイス単位でマルチキャストおよびブロードキャスト フレームの使用率を追跡し、不正使用を報告します。アラームのしきい値は、マルチキャストおよびブロードキャスト フレームのデバイスまたはチャネルによるフレーム合計に対する割合です。

ノード上の過剰なマルチキャスト/ブロードキャスト

アラームの説明と考えられる原因

有線ネットワークのように、WLAN に過剰なブロードキャスト フレームおよびマルチキャスト フレームがあると、WLAN 上のすべてのデバイスに余分な負荷がかかります。WLAN は、有線ネットワークよりも、マルチキャストおよびブロードキャスト フレームに影響されやすい環境です。これは、すべてのマルチキャストおよびブロードキャスト フレームが低速で送信されるためです（802.11b WLAN では 1 または 2 Mbps など）。このように低速な伝送は、WLAN の帯域幅をより多く消費します。帯域幅の効率性に加えて、低速なマルチキャストおよびブロードキャスト フレームでは伝送処理の完了に時間がかかるので、ワイヤレス メディアが空くのを待つ他のデバイスに対してより大きな遅延をもたらします。過剰なマルチキャストおよびブロードキャスト フレームによって、VoIP のような遅延に影響されやすい WLAN アプリケーションにジッタが発生します。たとえば、1000 バイトのブロードキャスト フレームは 1 Mpbs での伝送に 8 ミリ秒以上かかり、これは音声アプリケーションには大きな遅延の原因になります。

wIPS による解決

Cisco wIPS は、チャネルまたはデバイス単位でマルチキャストおよびブロードキャスト フレームの使用率を追跡し、不正使用を報告します。アラームのしきい値は、マルチキャストおよびブロードキャスト フレームのデバイスまたはチャネルによるフレーム合計に対する割合です。

チャネルまたはデバイスの過負荷

付 録 B

不正アクセス ポイントの管理

この付録では、不正アクセス ポイントのセキュリティ問題とソリューションについて説明します。

この付録の構成は、次のとおりです。

- 不正アクセス ポイントの問題，265 ページ
- 不正アクセス ポイントのロケーション、タギング、および封じ込め，266 ページ
- 「Monitoring Alarms」，268 ページ
- Prime Infrastructure での自動 SPT 基準の設定，279 ページ
- コントローラの設定，280 ページ
- コントローラ テンプレートの設定，282 ページ

不正アクセス ポイントの問題

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

オペレーティング システムのセキュリティ ソリューションでは、不正アクセス ポイントのロケーション、タギング、および封じ込め，（266 ページ）の説明にあるように、Radio Resource Management（RRM）機能を使用して、すべての近隣アクセス ポイントを継続的に監視し、不正アクセス ポイントを自動的に検出し、それらを特定します。

不正アクセスポイントのロケーション、タギング、および封じ込め

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

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

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

不正アクセス ポイントの検出と特定

無線 LAN 上のアクセス ポイントの電源が入りコントローラにアソシエートされると、Prime Infrastructure はただちに不正アクセス ポイントのリスニングを開始します。コントローラによって不正アクセス ポイントが検出されると、ただちに Prime Infrastructure に通知され、Prime Infrastructure によって不正アクセス ポイントのアラームが作成されます。

Prime Infrastructure が不正アクセス ポイント メッセージをコントローラから受け取ると、すべての Prime Infrastructure ユーザ インターフェイス ページの左下隅にアラーム モニタが表示されます。

不正アクセス ポイントを検出して特定するには、以下のステップに従います。

ステップ 1 [Rogues] インジケータをクリックして、[Rogue AP Alarms] ページを表示します。このページには、アラームの重大度、不正アクセス ポイントの MAC アドレス、不正アクセス ポイントのタイプ、不正アクセス ポイントが最初に検出された日時、および SSID が表示されます。

ステップ 2 [Rogue MAC Address] のリンクをクリックして、それに関連付けられた [Alarms > Rogue - AP MAC Address] ページを表示します。このページには、不正アクセス ポイントのアラームに関する詳細情報が表示されます。

ステップ 3 アラームを変更するには、[Select a command] ドロップダウン リストから次のコマンドのいずれかを選択し、[Go] をクリックします。

- [Assign to me]：選択されたアラームを現在のユーザに割り当てます。
- [Unassign]：選択されたアラームの割り当てを解除します。
- [Delete]：選択されたアラームを削除します。
- [Clear]：選択されたアラームをクリアします。
- [Event History]：不正アラームのイベントを表示できます。
- [Detecting APs]（無線帯域、場所、SSID、チャネル番号、WEP 状態、短いプリアンブルまたは長いプリアンブル、RSSI、および SNR を含む）：不正アクセス ポイントを現在検出しているアクセス ポイントを表示できます。
- [Rogue Clients]：この不正アクセス ポイントとアソシエートしているクライアントを表示できます。
- [Set State to 'Unknown - Alert']：不正アクセス ポイントを最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Known - Internal']：不正アクセス ポイントを内部としてタグ付けして既知の不正アクセス ポイント リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment] ～ [4 AP Containment]：level 1 containment を選択した場合は、不正な機器の近辺にある 1 つのアクセス ポイントが、その不正な機器にアソシエートされたクライアント デバイスに認証解除とアソシエート解除のメッセージを送信します。level 2 containment を選択した場合は、不正

な機器の近辺にある 2 つのアクセス ポイントが、その不正な機器のクライアントに認証解除とディスアソシエーションのメッセージを送信します。この動作は level 4 まで同様です。

ステップ 4 [Select a command] ドロップダウン リストから [Map (High Resolution)] を選択して、[Go] をクリックします。[Maps > Building Name > Floor Name] ページに、計算された不正アクセス ポイントの現在位置が表示されます。

Prime Infrastructure Location を使用している場合は、複数のアクセス ポイントからの RSSI 信号強度を比較することによって、不正アクセスポイントが存在する可能性が最も高い位置が特定され、その位置に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。アクセス ポイント 1 つと全方向性アンテナ 1 つだけの低展開ネットワークの場合、不正アクセスポイントが存在する可能性が最も高い位置はアクセス ポイント周辺のリング上のいずれかの位置です。ただし、存在する可能性が高い位置の中心はアクセス ポイントとなります。Prime Infrastructure Base を使用している場合は、不正アクセス ポイントからの RSSI 信号強度を頼りに、不正な機器から最も強力な RSSI 信号を受信しているアクセス ポイントの隣に小さなドクロと交差した 2 本の骨の形のインジケータが表示されます。

「Monitoring Alarms」

ここでは、次の内容について説明します。

- 不正アクセス ポイントに関するアラームの監視, （268 ページ）
- 不正アクセス ポイント監視の詳細, （271 ページ）
- アクセス ポイントの検出, （272 ページ）
- 不正アドホック無線に関するアラームの監視, （273 ページ）
- 不正アドホック無線に関する詳細の監視, （276 ページ）
- イベントのモニタリング, （278 ページ）
- 不正クライアントの監視, （279 ページ）

不正アクセス ポイントに関するアラームの監視

不正アクセス ポイント無線は、Cisco Lightweight アクセス ポイントによって検出された未許可のアクセス ポイントです。このページには、[Alarm Monitor] でクリックした重大度に基づいて、不正アクセス ポイントのアラームが表示されます。

[Rogue AP Alarms] ページを表示する手順は、次のとおりです。

- [Monitor] > [Alarms] の順に選択します。[Search] をクリックし、[Alarm Category] ドロップダウン リストから [Rogue AP] を選択します。[Go] をクリックして、該当するアラームを表示します。

- [Monitor] > [Security] の順に選択します。左側のサイドバーから、[Rouge AP] を選択します。
- 左側のサイドバー メニューの [Alarm Summary] ボックスで、[Malicious AP] の件数のリンクをクリックします。

（注） アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

次の表では、[Rogue Access Point Alarms] ページにあるパラメータについて説明します。

表 *26*：アラーム パラメータ

パラメータ	説明
Check box	操作対象となるアラームを選択します。
Severity	アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
Rogue Adhoc MAC Address	不正アドホック無線デバイスのMACアドレス。
ベンダー	不正アドホック無線デバイスのベンダー名、または Unknown（不明）。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
Radio Type	この不正アドホック無線の種類。
Strongest AP RSSI	受信信号強度インジケータの最大値（dBm）。
No. of Rogue Clients	この不正アドホック無線にアソシエートされている不正クライアントの数。
所有者	不正アドホック無線の「オーナー」。
Date/Time	アラームの発生時刻。
状態	State of the alarm：Alert（アラート）、Known（既知）、または Removed（削除済み）。
SSID	不正アドホック無線によってブロードキャストされている Service Set Identifier。（SSID がブロードキャストされない場合は空欄になります）。
Map Location	この不正アドホック無線のマップ位置。

Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。

対応するチェックボックスを選択して 1 つ以上のアラームを選択し、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。

（注） アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Detecting APs]：不正アドホック無線を現在検出している Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントを表示します。詳細については、「ネットワーク上のアクセス ポイントの検出」を参照してください。
- [Map (High Resolution)]：ここをクリックすると、不正アドホック無線の位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アドホック無線にアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アドホック無線が表示されます。
- [Set State to 'Alert']：このコマンドを選択して、不正アドホック無線を最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Internal']：このコマンドを選択して、不正アドホック無線を内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [Set State to 'External']：このコマンドを選択して、不正アドホック無線を外部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アドホック無線を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アドホック無線を 2 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。

- [3 AP Containment]：不正アドホック無線を 3 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アドホック無線を 4 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

注意 不正 AP の阻止は法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

不正アクセス ポイント監視の詳細

[Rogue AP Alarms] ページでは、各不正アクセス ポイントに関するアラーム イベントの詳細を確認できます。不正アクセス ポイント無線のアラーム イベントを確認するには、[Rogue AP Alarms] ページで [Rogue MAC Address] の下にある項目をクリックします。

このページには、不正アクセスポイント無線のアラームイベントが表示されます。不正アクセスポイント無線は、Cisco Lightweight アクセス ポイントによって検出された未許可のアクセス ポイントです。表示される情報は次のとおりです。

- [General Info]：
  - [Rogue MAC Address]：不正アクセス ポイントの MAC アドレス。
  - [Vendor]：不正アクセス ポイントのベンダー名、または Unknown（不明）。
  - [On Network]：不正アクセス ポイントがネットワーク上にあるかどうかを示します。
  - [Owner]：オーナー（または空白）。
  - [Acknowledged]：担当ユーザがこのアラームを認知しているかどうかを示します。
  - [Classification Type]：Malicious、Friendly、Unclassified。
  - [State]：Alert（アラート）、Known（既知）、または Removed（削除済み）のアラームの状態を示します。
  - [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。SSID がブロードキャストされない場合は空欄になります。
  - [Channel Number]：不正アクセス ポイントのチャネル。
  - [Containment Level]：不正アクセス ポイントの封じ込めレベル、または Unassigned（未割り当て）。
  - [Radio Type]：この不正アクセス ポイントの無線タイプ。
  - [Strongest AP RSSI]：受信信号強度インジケータの最大値（dBm）。

- [No. of Rogue Clients]：このアクセス ポイントにアソシエートされている不正クライアントの数。
- [Created]：アラーム イベントが作成された日時。
- [Modified]：アラーム イベントが修正された日時。
- [Generated By]：アラーム イベントの生成元。
- [Severity]：アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
- [Previous Severity]：アラームの以前の重大度：Critical、Major、Minor、Clear が色分けして表示されます。

- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。
- [Message]：アラームに関する説明が表示されます。
- [Help]：アラームに関する最新情報が表示されます。
- [Event History]：ここをクリックすると、[Monitor Alarms > Events] ページが開きます。
- [Annotations]：このアラームの現在の注釈が表示されます。

アクセス ポイントの検出

[Rogue AP Alarms] ページにアクセスするには、以下のステップに従います。

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

- 不正 AP の検索を実行します。
- NCS ホームページで、[Security] ダッシュボードをクリックします。このダッシュボードには、過去 1 時間と過去 24 時間に検出された不正アクセス ポイントがすべて表示されます。不正アクセス ポイント アラームを表示するには、不正アクセス ポイント番号をクリックします。
- [Alarm Summary] ボックスの [Malicious AP] の件数のリンクをクリックします。

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

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

ステップ 4 [Go] をクリックします。
いずれかのリスト項目をクリックすると、その項目に関するデータが表示されます。

- AP Name
- Radio

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

不正アドホック無線に関するアラームの監視

[Rogue Adhoc Alarms] ページには、不正アドホック無線のアラーム イベントが表示されます。

[Rogue Adhoc Alarms] ページを表示する手順は、次のとおりです。

- [Monitor] > [Alarms] の順に選択します。左側のサイドバー メニューから [Search] をクリックし、[Alarm Category] ドロップダウン リストから [Adhoc] を選択します。[Go] をクリックして、該当するアラームを表示します。
- [Monitor] > [Alarms] の順に選択します。左側のサイドバー メニューで [New Search] を選択し、[Alarm Category] ドロップダウン リストから [Rogue Adhoc] を選択します。[Go] をクリックして、該当するアラームを表示します。
- [Monitor] > [Security] をクリックします。左側のサイドバー メニューで、[Rogue Adhocs] を選択します。

（注） アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。これらのスクロール矢印を使用して、その他のアラームを表示します。

次の表には、[Rogue Adhoc Alarms] ページにあるパラメータを示します。

表 *27*：アラーム パラメータ

パラメータ	説明

Check box	操作対象となるアラームを選択します。
Severity	アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
Rogue Adhoc MAC Address	不正アドホック無線デバイスのMACアドレス。
ベンダー	不正アドホック無線デバイスのベンダー名、または Unknown（不明）。
Classification Type	Malicious（危険性あり）、Friendly（危険性なし）、Unclassified（未分類）。
Radio Type	この不正アドホック無線の種類。
Strongest AP RSSI	受信信号強度インジケータの最大値（dBm）。
No. of Rogue Clients	この不正アドホック無線にアソシエートされている不正クライアントの数。
所有者	不正アドホック無線の「オーナー」。
Date/Time	アラームの発生時刻。
状態	State of the alarm：Alert（アラート）、Known（既知）、または Removed（削除済み）。
SSID	不正アドホック無線によってブロードキャストされている Service Set Identifier。（SSID がブロードキャストされない場合は空欄になります）。
Map Location	この不正アドホック無線のマップ位置。
Acknowledged	対象ユーザがこのアラームを確認済みであるかどうかが表示されます。

対応するチェックボックスを選択して 1 つ以上のアラームを選択し、[Select a command] ドロップダウン リストから次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択したアラームを現在のユーザに割り当てます。
- [Unassign]：選択したアラームの割り当てを解除します。
- [Delete]：選択したアラームを削除します。
- [Clear]：選択したアラームをクリアします。
- [Acknowledge]：[Alarm Summary] ページに表示されないように、アラームを承認します。

（注） アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。

- [Unacknowledge]：すでに認知しているアラームを未認知にします。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Detecting APs]：不正アドホック無線を現在検出している Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントを表示します。詳細については、「ネットワーク上のアクセス ポイントの検出」を参照してください。
- [Map (High Resolution)]：ここをクリックすると、不正アドホック無線の位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アドホック無線にアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アドホック無線が表示されます。
- [Set State to 'Alert']：このコマンドを選択して、不正アドホック無線を最も低い脅威としてタグ付けして不正アクセス ポイントの監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Internal']：このコマンドを選択して、不正アドホック無線を内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [Set State to 'External']：このコマンドを選択して、不正アドホック無線を外部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アドホック無線を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。
- [2 AP Containment]：不正アドホック無線を 2 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アドホック無線を 3 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アドホック無線を 4 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

注意 不正 AP の阻止は法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

不正アドホック無線に関する詳細の監視

[Rogue Adhoc Alarms] ページでは、各不正アドホック無線に関するアラーム イベントの詳細を確認できます。

不正アドホック無線のアラーム イベントを確認するには、[Rogue Adhoc Alarms] ページで [Rogue MAC Address] の下にある項目をクリックします。

このページには、不正アクセスポイント無線のアラームイベントが表示されます。不正アクセスポイント無線は、Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントによって検出された無許可のアクセス ポイントです。表示される情報は次のとおりです。

- General:
  - [Rogue MAC Address]：不正アドホック無線デバイスの MAC アドレス。
  - [Vendor]：不正アドホック無線デバイスのベンダー名、または Unknown（不明）。
  - [On Network]：不正アドホック無線デバイスがネットワーク上にあるかどうかを示します。
  - [Owner]：オーナー（または空白）。
  - [Acknowledged]：担当ユーザがこのアラームを認知しているかどうかを示します。
  - [Classification Type]：Malicious、Friendly、Unclassified。
  - [State]：Alert（アラート）、Known（既知）、または Removed（削除済み）のアラームの状態を示します。
  - [SSID]：不正アドホック無線によってブロードキャストされている Service Set Identifier。（SSID がブロードキャストされない場合は空欄になります）。
  - [Channel Number]：不正アドホック無線のチャネル。
  - [Containment Level]：不正アドホック無線の封じ込めレベル、または Unassigned（未割り当て）。
  - [Radio Type]：この不正アドホック無線の種類。
  - [Strongest AP RSSI]：受信信号強度インジケータの最大値（dBm）。
  - [No. of Rogue Clients]：このアドホックに関連する不正クライアントの数を示します。
  - [Created]：アラーム イベントが作成された日時。
  - [Modified]：アラーム イベントが修正された日時。
  - [Generated By]：アラーム イベントの生成元。
  - [Severity]：アラームの重大度：Critical、Major、Minor、Clear が色分けして表示されます。
  - [Previous Severity]：アラームの以前の重大度：Critical、Major、Minor、Clear が色分けして表示されます。

- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、アラームが更新されます。
- [Message]：アラームに関する説明が表示されます。
- [Help]：アラームに関する最新情報が表示されます。
- [Annotations]：このアラームの現在の注釈が表示されます。

Select a Command

対応するチェックボックスを選択して 1 つ以上のアラームを選択し、次のいずれかのコマンドを選択して、[Go] をクリックします。

- [Assign to me]：選択されたアラームを現在のユーザに割り当てます。
- [Unassign]：選択されたアラームの割り当てを解除します。
- [Delete]：選択されたアラームを削除します。
- [Clear]：選択されたアラームをクリアします。
- [Acknowledge]：アラームを認識した後は、[Alarm Summary] ページで表示されないようにできます。アラームは Prime Infrastructure に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge]：すでに認知しているアラームの認知を解除できます。
- [Email Notification]：電子メール通知を表示して設定するために、[All Alarms] > [Email Notification] ページを表示します。
- [Detecting APs]：不正アドホック無線を現在検出している Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントを表示します。
- [Map (High Resolution)]：ここをクリックすると、不正アドホック無線の位置を示す高解像度マップが表示されます。
- [Rogue Clients]：ここをクリックすると、この不正アドホック無線にアソシエートされている不正クライアントが一覧表示されます。[Rogue Clients] ページには、クライアントの MAC アドレス、最終通信日時、現在のステータス、関連付けられているコントローラ、および不正アドホック無線が表示されます。
- [Set State to 'Alert']：このコマンドを選択して、不正アドホック無線を最も低い脅威としてタグ付けして不正アドホック無線の監視を継続し、封じ込め機能をオフにします。
- [Set State to 'Internal']：このコマンドを選択して、不正アドホック無線を内部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [Set State to 'External']：このコマンドを選択して、不正アクセス ポイントを外部としてタグ付けして既知の不正 AP リストに追加し、封じ込め機能をオフにします。
- [1 AP Containment]：不正アドホック無線を 1 つのアクセス ポイントで封じ込めます。（最小封じ込めレベル）。

- [2 AP Containment]：不正アドホック無線を 2 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [3 AP Containment]：不正アドホック無線を 3 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。
- [4 AP Containment]：不正アドホック無線を 4 つの Cisco Aironet 1000 シリーズ Lightweight アクセス ポイントで封じ込めます。（最大封じ込めレベル）。

イベントのモニタリング

[Alarm Monitor] にある [Rogues] アラーム枠をクリックし、[Rogue MAC Addresses] のリスト項目をクリックします。次に、[Select a command] ドロップダウン リストから [Event History] を選択して、[Go] をクリックします。このページが表示されます。

[Monitor] > [Alarms] の順に選択し、左側のサイドバー メニューで [New Search] を選択します。[Severity] > [All Severities] および [Alarm Category] > [Rogue AP] の順に選択して、[Go] をクリックします。[Monitor Alarms > failure object] ページが表示されます。[Rogue MAC Address] 列の項目をクリックして、[Monitor Alarms > Rogue AP Details] ページを開きます。[Select a command] ドロップダウン リストから [Event History] を選択して、[Go] をクリックします。このページが表示されます。

このページでは、不正アラーム イベントに関する情報を参照できます。これらのイベントは発生した順に一覧表示されます。

各列のタイトルをクリックすると、表示順序を変更することができます。

- [Severity]：イベントの重大度が色分けして表示されます。
- [Rogue MAC Address]：リスト項目をクリックすると、そのエントリに関する情報が表示されます。
- [Vendor]：不正アクセス ポイントの製造業者名。
- [Type]：AP（アクセス ポイント）または AD-HOC（アドホック）。
- [On Network]：不正アクセス ポイントが、アソシエートされているポートと同じサブネットにあるかどうか。
- [On 802.11b]：不正アクセス ポイントが 802.11b/802.11g 帯でブロードキャストしているかどうか。
- [Date/Time]：アラームの日時。
- [Classification Type]：Malicious、Friendly、Unclassified。
- [State]：アラームの状態。Alert（アラート）、Removed（削除済み）など。
- [SSID]：不正アクセス ポイント無線によってブロードキャストされているサービス セット ID（SSID）。
- [On 802.11a]：不正アクセス ポイントが 802.11a 帯でブロードキャストしているかどうか。

不正クライアントの監視

[Monitor] > [Alarms] の順に選択し、左側のサイドバー メニューで [New Search] を選択します。[Severity] > [All Severities] および [Alarm Category] > [Rogue AP] の順に選択して、[Go] をクリックします。[Monitor Alarms > failure object] ページが表示されます。[Rogue MAC Address] 列の項目をクリックして、[Monitor Alarms > Rogue AP Details] ページを開きます。[Select a command] ドロップダウン リストから [Rogue Clients] を選択します。このページが表示されます。

このページでは、不正アクセス ポイントにアソシエートされているクライアントに関する次の情報を参照できます。

- [Client MAC Address]：不正アクセス ポイントのクライアントの MAC アドレス。
- [Last Heard]：シスコ アクセス ポイントが不正アクセス ポイントのクライアントを最後に検出した時刻。
- [Status]：不正アクセス ポイントのクライアントの状態。

Prime Infrastructure での自動 SPT 基準の設定

Prime Infrastructure で自動スイッチ ポート トレーシングを設定するには、以下のステップに従います。

ステップ 1 [Administration] > [System Settings] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Rogue AP Settings] を選択します。
[Rogue AP Settings] ページが表示されます。

ステップ 3 [Enable Auto Switch Port Tracing] チェックボックスをオンにして、Prime Infrastructure が、不正アクセス ポイントが接続されているスイッチ ポートを自動的にトレースできるようにします。次のパラメータを設定できます。

- [Repeat Search After]：分単位の時間を入力します。この時間が経過した後、Prime Infrastructure は不正 AP の検索を自動的に繰り返します。デフォルトでは、Prime Infrastructure は 120 分おきに不正 AP の検索を繰り返します。
- [Allow Trace For Found On Wire Rogue AP]：有線の不正 AP をトレースする自動 SPT を有効にするには、このチェックボックスをオンにします。
- [Critical]：アラーム重大度を critical に設定するには、このチェックボックスをオンにします。
- [Major]：アラーム重大度を major に設定するには、このチェックボックスをオンにします。
- [Minor]：アラーム重大度を minor に設定するには、このチェックボックスをオンにします。

ステップ 4 [OK] をクリックします。

Prime Infrastructure での自動封じ込めの設定

Prime Infrastructure で自動封じ込めを設定するには、以下のステップに従います。

ステップ 1 [Administration] > [Settings] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Rogue AP Settings] を選択します。
[Rogue AP Settings] ページが表示されます。

ステップ 3 [Enable Auto Containment] チェックボックスをオンにして、Prime Infrastructure が不正 AP を受信した場合に自動封じ込めをトリガーできるようにします。次の自動封じ込めパラメータを設定できます。

- [Exclude Rogue APs Found On Wire By Switch Port Tracing]：自動 SPT を通じて有線ネットワークで検出された AP を自動的に除外するには、このチェックボックスをオンにします。
- [Critical]：アラーム重大度を critical に設定するには、このチェックボックスをオンにします。
- [Major]：アラーム重大度を major に設定するには、このチェックボックスをオンにします。
- [Containment Level]：自動封じ込めレベルを有効にするには、このチェックボックスをオンにします。これは、不正 AP の封じ込めレベルを示します。
  - [1 AP Containment through 4 AP Containment]：1 から 4 までの値を入力することで、自動封じ込めレベルを設定します。レベル 1 封じ込めを選択すると、不正な機器の近辺にある 1 つのアクセス ポイントが、不正な機器にアソシエートされているクライアント デバイスに、認証解除とアソシエート解除のメッセージを送信します。レベル 2 封じ込めを選択した場合は、不正な機器の近辺にある 2 つのアクセス ポイントが、その不正な機器のクライアントに認証解除とディスアソシエーションのメッセージを送信します。この動作は level 4 まで同様です。

（注） 不正アクセス ポイントの脅威が高いほど、高い封じ込め処理が必要です。

注意 不正アクセス ポイントの封じ込めは法的責任を伴う場合があります。いずれかの AP 封じ込めコマンドを選択し、[Go] をクリックすると、メッセージ「Containing a Rogue AP may have legal consequences.Do you want to continue?」が表示されます。処理を続行する場合は [OK] をクリックします。アクセス ポイントを封じ込めない場合は [Cancel] をクリックします。

ステップ 4 [OK] をクリックします。

コントローラの設定

ここでは、次の内容について説明します。

• 不正ポリシーの設定，（281 ページ）
• 不正 AP ルールの設定，（281 ページ）

不正ポリシーの設定

このページでは、不正アクセス ポイントのポリシーを設定できます。

[Rogue Policies] ページにアクセスするには、以下のステップに従います。

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

ステップ 2 [IP Address] 列で IP アドレスをクリックします。

ステップ 3 左側のサイドバー メニューから、[Security] > [Rogue Policies] の順に選択します。

- [Rogue Location Discovery Protocol]：[Enabled]、[Disabled]。
- Rogue APs
  - [Expiration Timeout for Rogue AP Entries (seconds)]：1 ～ 3600 秒（デフォルトは 1200）。
- Rogue Clients
  - [Validate rogue clients against AAA (check box)]：[Enabled]、[Disabled]
  - [Detect and report ad hoc networks (check box)]：[Enabled]、[Disabled] コマンド ボタン。
- [Save]：クライアント除外ポリシーへの変更を保存して、前のページに戻ります。
- [Audit]：NCS 値を、コントローラで使用された値と比較します。

不正 AP ルールの設定

このページでは、現在の不正 AP ルールの表示と編集ができます。

[Rogue AP Rules] ページにアクセスするには、以下のステップに従います。

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

ステップ 2 [IP Address] 列で IP アドレスをクリックします。

ステップ 3 左側のサイドバー メニューから、[Security] > [Rogue AP Rules] の順に選択します。[Rogue AP Rules] ページに、不正 AP ルール、ルール タイプ（[Malicious] または [Friendly]）、およびルールの順序が表示されます。

ステップ 4 ルールの詳細を表示または編集するには、不正 AP ルールを選択します。

コントローラ テンプレートの設定

ここでは、次の内容について説明します。

- 不正ポリシーの設定, （282 ページ）
- 不正 AP ルールの設定, （283 ページ）
- 不正 AP ルール グループの設定, （285 ページ）

不正ポリシーの設定

現在のテンプレート、テンプレートが適用されているコントローラ数を表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue Policies] の順に選択します。

新しい不正ポリシー テンプレートを作成するには、以下のステップに従います。

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

ステップ 2 左側のサイドバー メニューから、[Security] > [Rogue Policies] の順に選択します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Template] を選択します。

ステップ 4 [Go] をクリックします。

（注） 既存の不正ポリシーテンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue Policies] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5 [Rogue Location Discovery Protocol] チェックボックスをオンにして、有効にします。Rogue Location Discovery Protocol（RLDP）では、企業の有線ネットワークへの不正な接続の有無を判断します。

（注） RLDP が有効の場合、コントローラは管理対象のアクセス ポイントに対して、不正アクセス ポイントをアソシエートし、特殊なパケットをコントローラへ送信するよう指示します。コントローラがこのパケットを受信すると、不正アクセス ポイントが企業ネットワークに接続されます。この方法は、暗号化を有効にしていない不正アクセス ポイントに対して機能します。

ステップ 6 不正アクセス ポイント エントリの失効タイムアウトを秒単位で設定します。

ステップ 7 [Validate rogue clients against AAA] チェックボックスをオンにして、不正クライアントの AAA 検証を有効にします。

ステップ 8 [Detect and report Adhoc networks] チェックボックスをオンにして、アドホック ネットワーキングに参加している不正クライアントの検出とレポートを有効にします。

ステップ 9 次のいずれかのボタンをクリックします。

- [Save]：クリックして現在のテンプレートを保存します。
- [Apply to Controllers]：クリックして現在のテンプレートをコントローラに適用します。 [Apply to Controllers] ページで該当するコントローラを選択し、[OK] をクリックします。
- [Delete]：クリックして現在のテンプレートを削除します。 現在コントローラにそのテンプレートが適用されている場合は、[OK] をクリックして、テンプレートが適用されている選択したコントローラから、テンプレートを削除することを確定します。
- [Cancel]：クリックして現在のテンプレート作成または現在のテンプレートの変更をキャンセルします。

不正 AP ルールの設定

不正 AP ルールを使用すると、不正アクセス ポイントを自動的に分類するルールを定義できます。NCS は、不正アクセス ポイントの分類ルールをコントローラに適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

（注） 不正 AP ルールは、誤アラームを減らすのにも役立ちます。

現在の分類ルール テンプレート、ルールの種類、適用されているコントローラ数を表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rules] の順に選択します。

（注） 不正クラスには次のタイプが含まれます。[Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。[Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。[Unclassified Rogue]：検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

不正アクセス ポイントの新しい分類ルール テンプレートを作成するには、以下のステップに従います。

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

ステップ 2 左側のサイドバー メニューから、[Security] > [Rogue AP Rules] の順に選択します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Classification Rule] を選択します。

ステップ 4 [Go] をクリックします。

（注） 既存の不正 AP ルールのテンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rules] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5 次のフィールドに入力します。

- General:
  - [Rule Name]：テキスト ボックスにルールの名前を入力します。
  - [Rule Type]：ドロップダウン リストから [Malicious] または [Friendly] を選択します。

    （注） [Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。[Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。
  - [Match Type]：ドロップダウン リストから [Match All Conditions] または [Match Any Condition] を選択します。
- Malicious Rogue Classification Rule
  - [Open Authentication]：オープン認証を有効にするには、このチェックボックスをオンにします。
  - [Match Managed AP SSID]：管理対象 AP SSID のルール条件との一致を有効にするには、このチェックボックスをオンにします。

    （注） 管理対象 SSID は、WLAN に対して設定された SSID で、システムが既知のものです。

- [Match User Configured SSID]：ユーザ設定の SSID のルール条件との一致を有効にするには、このチェックボックスをオンにします。

  （注） ユーザ設定の SSID は、手動で追加された SSID です。[Match User Configured SSID] テキスト ボックスに、ユーザ設定の SSID を（1 行に 1 つずつ）入力します。

- [Minimum RSSI]：最小 RSSI 閾値制限を有効にするには、このチェックボックスをオンにします。

  （注） テキスト ボックスに RSSI 閾値の最小レベル（dB 単位）を入力します。検出されたアクセス ポイントがここで指定した RSSI 閾値を超えていると、そのアクセス ポイントは悪意のあるものとして分類されます。

- [Time Duration]：時間制限を有効にするには、このチェックボックスをオンにします。

  （注） テキスト ボックスに制限時間（秒単位）を入力します。検出されたアクセス ポイントが指定した制限時間よりも長く表示されているとき、そのアクセス ポイントは悪意のあるものとして分類されます。

- [Minimum Number Rogue Clients]：悪意のあるクライアントの最小数の制限を有効にするには、このチェックボックスをオンにします。

  （注） 悪意のあるクライアントを許可する最小数を入力します。検出されたアクセス ポイントにアソシエートされたクライアントの数が指定した値以上になると、そのアクセス ポイントは悪意のあるものとして分類されます。

ステップ 6 次のいずれかのボタンをクリックします。

- [Save]：クリックして現在のテンプレートを保存します。
- [Apply to Controllers]：クリックして現在のテンプレートをコントローラに適用します。 [Apply to Controllers] ページで該当するコントローラを選択し、[OK] をクリックします。
- [Delete]：クリックして現在のテンプレートを削除します。 現在コントローラにそのテンプレートが適用されている場合は、[OK] をクリックして、テンプレートが適用されている選択したコントローラから、テンプレートを削除することを確定します。
- [Cancel]：クリックして現在のテンプレート作成または現在のテンプレートの変更をキャンセルします。

不正 AP ルール グループの設定

不正 AP ルール グループ テンプレートを使用すると、複数の不正 AP ルールをコントローラに統合できます。

現在の不正 AP ルール グループ テンプレートを表示するには、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rule Groups] の順に選択します。

不正 AP ルール グループを設定するには、以下のステップに従います。

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

ステップ 2 左側のサイドバー メニューから、[Security] > [Rogue AP Rule Groups] の順に選択します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Rogue Rule Group] を選択します。

ステップ 4 [Go] をクリックします。

（注） 既存の不正ポリシーテンプレートに変更を加える場合、または現在のテンプレートをコントローラに適用する場合は、[Configure] > [Controller Templates] > [Security] > [Rogue AP Rule Groups] の順に選択し、[Template Name] 列でテンプレート名をクリックします。テンプレートに必要な変更を加え、[Save] または [Apply to Controllers] をクリックします。

ステップ 5 次のパラメータを入力します。

- General
  - [Rule Group Name]：テキスト ボックスにルール グループの名前を入力します。

ステップ 6 Rogue AP ルールを追加するには、左の列のルールをクリックして強調表示します。[Add] をクリックして、強調表示したルールを右側の列に移動します。

（注） 不正 AP ルールは、[Rogue AP Rules] グループ ボックスから追加できます。詳細については、不正 AP ルールの設定を参照してください。

ステップ 7 不正 AP ルールを削除するには、右の列のルールをクリックして強調表示します。[Remove] をクリックして、強調表示したルールを左側の列に移動します。

ステップ 8 [Move Up]/[Move Down] ボタンをクリックして、ルールが適用される順序を指定します。任意のルールを強調表示し、[Move Up] または [Move Down] をクリックして、現在のリストで上下に移動させます。

ステップ 9 不正 AP ルール リストを保存するには、[Save] をクリックします。

ステップ 10 現在のリストに変更を加えずにページを終了するには [Cancel] をクリックします。

（注） コントローラに適用されたルールを表示または編集するには、[Configure] > [Controller] の順に選択し、コントローラ名をクリックしてコントローラを開きます。

付 録 C

wIPS ソリューションの設定と展開

ここでは、Prime Infrastructure UI の Lifecycle テーマを使用して、wIPS ソリューションを設定、展開する方法について説明します。

Prime Infrastructure UI の Lifecycle テーマから、[**Design**] > [**Wireless Security**] の順に選択します。Wireless Security ウィザードのページが表示され、次の wIPS 関連の設定を行うことができます。

- 不正ポリシーによって、アドホック ネットワークを検出およびレポートできます。
- 不正ルールによって、不正アクセス ポイントを自動的に分類するルールを定義できます。
- 新しい wIPS プロファイルを追加できます。

ここでは、次の内容について説明します。

- [Before You Begin] ウィザード ページの表示，287 ページ
- 不正ポリシーの設定，288 ページ
- 不正ルールの設定，289 ページ
- 現在追加されている不正ルールの表示，291 ページ
- wIPS プロファイルの設定，292 ページ

[Before You Begin] ウィザード ページの表示

Before You Begin ウィザード ページには、Wireless Security ウィザード の使用方法の情報が表示され、さらに次の情報が含まれています。

- [Rogue Policy]：[Rogue Policy] ページでは、不正ポリシーを設定できます。このページには、不正アクセス検出と封じ込めのための 3 つの不正ポリシー事前設定があります。
- [Rogue Rules]：[Rogue Rules] ページでは、認証タイプ、一致条件設定済みの SSID、クライアント数、RSSI 値などの基準に基づいて、不正アクセス ポイントを自動的に分類できます。不正アクセスのルールは、不正アクセスを [Malicious] または [Friendly] として分類するように作成できます。

- [wIPS Profile]：[wIPS Profile] ページでは、いくつかの定義済みプロファイルからプロファイルを選択できます。これらのプロファイルによって、Cisco Adaptive wIPS を通じて使用可能な追加のワイヤレスの脅威保護をすばやくアクティブにできます。プロファイルは、検出して封じ込める wIPS シグニチャを選択することでさらにカスタマイズできます。
- [Devices]：[Devices]ページでは、不正ポリシー、不正アクセス ルール、wIPS プロファイルをコントローラに適用できます。

[Next] をクリックして、アドホック ネットワークを検出およびレポートする不正ポリシーを設定します。

不正ポリシーの設定

このページでは、コントローラに適用される（アクセス ポイントとクライアントに対する）不正ポリシーを設定できます。

不正ポリシーを設定するには、以下のステップに従います。

ステップ 1 [Design] > [Wireless Security] > [Rogue Policy] の順に選択します。

ステップ 2 [Configure the rogue policy settings] スライドバーをマウスで移動するか [Custom] チェックボックスをオンにしてポリシー設定を行うことで、ポリシー設定を [Low]、[High]、または [Critical] に設定できます。

ステップ 3 [General] グループ ボックスで、次のフィールドを設定します。

- [Rogue Location Discovery Protocol]：Rogue Location Discovery Protocol（RLDP）が企業の有線ネットワークに接続されているかどうかを判断します。ドロップダウン リストから、次のいずれかのオプションを選択します。
  - [Disable]：すべてのアクセス ポイント上で RLDP を無効にします。
  - [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。
  - [Monitor Mode APs]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。

（注） RLDP が有効の場合、コントローラは管理対象のアクセス ポイントに対して、不正アクセス ポイントをアソシエートし、特殊なパケットをコントローラへ送信するよう指示します。コントローラがこのパケットを受信すると、不正アクセスポイントが企業ネットワークに接続されます。この方法は、暗号化を有効にしていない不正アクセス ポイントに対して機能します。

- [Expiration Timeout for Rogue AP and Rogue Client Entries]：不正アクセス ポイント エントリの失効タイムアウトを秒単位で設定します。有効範囲は 240 ～ 3600 秒です。
- [Validate rogue clients against AAA]：[Validate rogue clients against AAA] チェックボックスをオンにして、不正クライアントの AAA 検証を有効にします。
- [Detect and report Adhoc networks]：[Detect and report Adhoc networks] チェックボックスをオンにして、アドホック ネットワーキングに参加している不正クライアントの検出とレポートを有効にします。

- [Rogue Detection Report Interval]：[Rogue Detection Report Interval] テキスト ボックスに、AP が不正検出レポートをコントローラに送信するまでの時間間隔を秒数で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。この機能は、モニタ モードの AP のみに適用されます。
- [Rogue Detection Minimum RSSI]：[Rogue Detection Minimum RSSI] テキスト ボックスに、AP により検出され、不正エントリがコントローラに作成する RSSI の最小値を入力します。有効な範囲は -70 dBM ～ -128 dBm です。この機能は、すべての AP モードに適用できます。
- [Rogue Detection Transient Interval]：[Rogue Detection Transient Interval] テキスト ボックスに、不正が AP により最初にスキャンされてから、必ずスキャンされる時間間隔を入力します。一時的な間隔を入力することで、AP が不正をスキャンする間隔を制御できます。AP は、一時的な間隔の値に基づいて、不正をフィルタできます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。この機能は、モニタ モードの AP のみに適用されます。

ステップ 4 [Auto Contain] グループ ボックスで、次のフィールドを設定します。

- [Rogue on Wire]：[Rogue on Wire] チェックボックスをオンにして、有線ネットワークで検出された AP を自動的に封じ込めます。
- [Using our SSID]：[Using our SSID] チェックボックスをオンにします。
- [Valid client on Rogue AP]：[Valid client on Rogue AP] チェックボックスをオンにして、有効なクライアントを不正 AP への接続から封じ込めます。
- [AdHoc Rogue]：[AdHoc Rogue] チェックボックスをオンにして、アドホック不正 APs を自動的に封じ込めます。

ステップ 5 [Apply] をクリックして、コントローラに現在のルールを適用します。[Devices] ウィザードのページで、該当するコントローラを選択して、[Apply to Controllers] をクリックします。

ステップ 6 [Next] をクリックして不正ルールを設定します。

不正ルールの設定

このページでは、不正アクセス ポイントを自動的に分類するルールを定義できます。Prime Infrastructure では、不正アクセス ポイントの分類ルールをコントローラに適用します。これらのルールでは、RSSI レベル（それよりも弱い不正アクセス ポイントは無視）、または時間制限（指定された時間内に表示されない不正アクセス ポイントにはフラグを立てない）に基づいて、マップ上の不正表示を制限できます。

（注） 不正クラスには次のタイプが含まれます。[Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。[Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。[Unclassified Rogue]：検出されたアクセス ポイントのうち、Malicious ルールまたは Friendly ルールに該当しないアクセス ポイント。

不正アクセス ポイントの新しい分類ルールを作成するには、以下のステップに従います。

ステップ 1 [Design] > [Wireless Security] > [Rogue Rules] の順に選択します。

ステップ 2 新しい不正ルールを作成するには、[Create New] をクリックします。
[Add/Edit Rogue Rule] ウィンドウが表示されます。

ステップ 3 [General] グループ ボックスで、次のフィールドを設定します。

- [Rule Name]：テキスト ボックスにルールの名前を入力します。
- [Rule Type]：ドロップダウン リストから [Malicious] または [Friendly] を選択します。

  （注） [Malicious Rogue]：検出されたアクセス ポイントのうち、ユーザが定義した Malicious ルールに一致したアクセス ポイント、または危険性のない AP カテゴリから手動で移動されたアクセス ポイント。[Friendly Rogue]：既知、認識済み、または信頼できるアクセス ポイント、または検出されたアクセス ポイントのうち、ユーザが定義した Friendly ルールに該当するアクセス ポイント。

- [Match Type]：ドロップダウン リストから [Match All Conditions] または [Match Any Condition] を選択します。

ステップ 4 [不正分類ルール] グループ ボックスで、次のフィールドを設定します。

- [Open Authentication]：オープン認証を有効にするには、[Open Authentication] チェックボックスをオンにします。
- [Match Managed AP SSID]：管理対象 AP SSID のルール条件との一致を有効にするには、[Match Managed AP SSID] チェックボックスをオンにします。

  （注） 管理対象 SSID は、WLAN に対して設定された SSID で、システムが既知のものです。

- [Match User Configured SSID]（1 行に 1 つずつ入力）：ユーザ設定の SSID のルール条件との一致を有効にするには、[Match User Configured SSID] チェックボックスをオンにします。

  （注） ユーザ設定の SSID は、手動で追加された SSID です。[Match User Configured SSID] テキスト ボックスに、ユーザ設定の SSID を（1 行に 1 つずつ）入力します。

- [Minimum RSSI]：最小 RSSI 閾値制限を有効にするには、[Minimum RSSI] チェックボックスをオンにします。

（注） テキスト ボックスに RSSI 閾値の最小レベル（dB 単位）を入力します。検出されたアクセス ポイントがここで指定した RSSI 閾値を超えていると、そのアクセス ポイントは悪意のあるものとして分類されます。

- [Time Duration]：時間制限を有効にするには、[Time Duration] チェックボックスをオンにします。

（注） テキスト ボックスに制限時間（秒単位）を入力します。検出されたアクセス ポイントが指定した制限時間よりも長く表示されているとき、そのアクセス ポイントは悪意のあるものとして分類されます。

- [Minimum Number Rogue Clients]：悪意のあるクライアントの最小数の制限を有効にするには、[Minimum Number Rogue Clients] チェックボックスをオンにします。

（注） 悪意のあるクライアントを許可する最小数を入力します。検出されたアクセス ポイントにアソシエートされたクライアントの数が指定した値以上になると、そのアクセス ポイントは悪意のあるものとして分類されます。

ステップ 5 [OK] をクリックしてルールを保存するか、または [Cancel] をクリックして現在のルールの作成または変更をキャンセルします。
[Rogue Rules]ページに戻り、新しく追加された不正ルールが表示されます。

ステップ 6 [Apply] をクリックして、コントローラに現在のルールを適用します。[Devices] ウィザードのページで、該当するコントローラを選択し、[Apply to Controllers] をクリックします。
（注）

ステップ 7 [Next] をクリックし、wIPS プロファイルを設定します。

現在追加されている不正ルールの表示

現在追加されている不正ルールを表示するには、以下のステップに従います。

Prime Infrastructure UI の Lifecycle テーマから、[Design] > [Wireless Security] > [Rogue Rules] の順に選択します。
[Rogue Rules] ページに、次のパラメータが表示されます。

- 既存のルールを追加
- Rule Name
- ルール タイプ
- 最後の保存場所
- Actions

wIPS プロファイルの設定

Prime Infrastructure には、いくつかの定義済みプロファイルが用意されており、そこからプロファイルを選択できます。これらのプロファイル（カスタマータイプ、ビルディングタイプ、業界タイプなどに基づきます）を使用すると、Cisco Adaptive wIPS を通じて使用可能な追加のワイヤレスの脅威保護をすばやくアクティブにできます。プロファイルは「そのまま」使用することも、要件に合わせてカスタマイズすることもできます。

wIPS プロファイル設定の詳細については、wIPS およびプロファイルの設定, （109 ページ）を参照してください。

wIPS プロファイルを設定したら、[**Next**] をクリックして [Devices] ページを開き、設定を適用するコントローラを選択できます。

索 引

A

AP 141, 142, 150, 152, 155
  details 141, 142, 150, 152, 155
    CDP Neighbors 155
    general 141, 142, 150
    インターフェイス 152
AP ロケーション データ 88

C

Civic Address 64
clear 137

G

\ 64

M

Mesh Parent-Child Hierarchical View ウィンドウ 81
Monitor Access Points 141
  details 141
Monitor AP 141, 142, 150, 152, 155
  details 141, 142, 150, 152, 155
    CDP Neighbors 155
    general 141, 142, 150
      Lightweight 142
    インターフェイス 152

O

Out-of-Sync 40

P

Profile 119
  List 119

S

SSID グループ 124, 125, 126, 127
  add 126
  delete 127
  edit 127
  wIPS 125
  グローバル リストから追加 126
  グローバルの削除 125
  グローバルを追加 124
  グローバルを編集 124
SSID グループ リスト 122, 123
  global 123
  wIPS 122

W

wIPS 119, 120, 122, 128
  Profile 120
    add 120
  SSID グループ リスト 122
  プロファイル エディタ 128
  プロファイル リスト 119
wIPS プロファイル 120, 121, 122
  add 120
  apply 122
  delete 121

あ

アイデンティティ クライアント 174

アラーム通知 137
　電子メールの送信 137

く

グローバル SSID グループ 124, 125
　add 124
　delete 125
　edit 124

た

ダウンロード 140, 205

ね

ネットワーク設計 33

ひ

ビルディング 64
　PI データベースへの追加 64

ふ

プロファイル エディタ 128

ろ

ロケーション表示 63
　割り当て 63