

AirMagnet Enterprise Version 6.1

リリースノート

2006年5月31日

目次:

- はじめに, page 1
 - 特記事項, page 1
 - 警告, page 2
 - 新しい機能, page 2
 - 既知の問題, page 9
 - テクニカルサポート, page 11
-

はじめに

このリリースノートには AirMagnet Enterprise 6.1 の新機能および既知の問題が記述されています。

特記事項

1. **重要!!!** 現在 AirMagnet Distributed 4.0 をご使用の方で、Enterprise 6.1 にアップグレードをご希望の方は、まず Enterprise 5.0 にアップグレードした後 Enterprise 6.1 にアップグレードしてください。AirMagnet Distributed 3.X をご使用の方で、Enterprise 6.1 にアップグレードをご希望の方は、まず Distributed 4.0、続いて Enterprise 5.0 にアップグレードした後 Enterprise 6.1 にアップグレードしてください。Distributed 3.X もしくは 4.0 から Enterprise 6.1 へ直接アップグレードすると、SmartEdge センサーが共有秘密鍵を失ったり、ログインや SmartEdge センサーの構成に失敗したりする恐れがあります。AirMagnet Distributed 4.0 や AirMagnet Enterprise 5.0 のインストールプログラムが必要な方は、東陽テクニカ情報通信システム営業部までご連絡ください。
2. AirMagnet Enterprise システムをアップグレードするには、インストールプログラムの[修正]を選択してください。
3. アップグレード終了後、すべてのセンサーがアップグレードを終了したことを確認した後、次のアップグレードを行ってください。
4. Distributed 3.X/4.0 もしくは Enterprise 5.0 からアップグレードするとき、3.X/4.0/5.0 でご利用のユーザ名をメモに書きとめてください。ユーザを作り直したり、権限を設定し直したりする必要がある場合があります。Enterprise 6.1 の『ユーザと権限』機能を用いてユーザに権限を設定することができます。

5. Enterprise 6.1 では警報や通知の種類が増えました。Distributed 3.X/4.0 もしくは Enterprise 5.0 からアップグレードするとき、必要な警報がすべて使用可能であり、通知が設定されていることを確認してください。作成した警報名が Enterprise 6.1 では変わっていることがあります。
6. Distributed 4.0 から Enterprise 5.0 にアップグレードするとき、ご利用の Distributed コンソールを **スタート > コントロールパネル > プログラムの追加と削除** を用いてアンインストールしてください。その後、新しい Enterprise コンソールを AirMagnet Enterprise サーバ WEB ページからダウンロードしてインストールしてください。
7. AirMagnet Enterprise コンソールをインストールしたマシンに Microsoft パッチ #832894、セキュリティアップデート(MS04-004) もしくはホットフィクス#821814 がインストールされていると、コンソールからサーバに接続するとき、バージョン ミスマッチ エラーを受け取ることがあります。この問題を解決するには、Microsoft WEB サイトのパッチ#831167 をインストールする必要があります。
8. 16 文字より長い Cisco AP 名は自動的に切り詰められます。しかし、このことが AirMagnet Enterprise システムの動作に悪影響を及ぼすことはありません。
9. Rogue Triangulation 操作をするとき、結果表示を最も良くするため、画面の解像度を 32bit(最大値)に設定してください。
10. 現在 ACL グループ機能を使用している場合は、すべての AP を各グループに再設定する必要があります。また、ポリシープロファイルの手続きを行い、正しい ACL グループを設定しなおす必要があります。

警告

4.0 以前のバージョンのファームウェアがロードされており、ネットワーク上で使用していない AirMagnet センサーをご利用の際は、AirMagnet Enterprise サーバ 6.1 が稼動しているネットワークに接続する前に、センサーをアップグレードしてください。アップグレードは一段階ずつ行う必要があります。すなわち、まず 4.0 から 5.0 にアップグレードし、続いて 5.0 から 6.1 にアップグレードしてください。5.0 から 6.1 へアップグレードする前に、4.0 から 5.0 へのアップグレードが完了したことを確認してください。

この警告に注意を払わないと、センサーが機能しなくなる恐れがあります。

新しい機能

AirMagnet Enterprise 6.1 には次の新機能が追加されました。詳細は、リストの次に列記していません。

- SmartEdge センサー Zero Configuration
- Cisco WLAN モニタ アクセスポイント用 AirMagnet AirWISE エージェント
- AirMagnet Enterprise Reporter の統合
- 4 つの規制コンプライアンスレポート
- 12 の新規 IDS/IPS およびパフォーマンス侵害アラーム

AirMagnet SmartEdge センサー Zero Configuration

センサー Zero Configuration 機能は、AM-5010、AM5012 および A5023 を含む AirMagnet SmartEdge センサーのすべてのモデルに適用されます。

センサー Zero Configuration は未設定のセンサーを使用可能にします。未設定のセンサーはネットワークに配置されると、自動的にすでにネットワークに存在する AirMagnet Enterprise サーバを検出し、接続します。この機能を使用すると、ネットワーク管理者は設置の際、手動で AirMagnet SmartEdge センサーの設定や管理をする手間を軽減することができます。また、通常メンテナンスサイクル期間内のオーバーヘッドを削減することができます。

センサー Zero Configuration の恩恵を受けるために、ユーザはセンサーを接続する前に、Enterprise サーバのセンサー Zero Configuration に関する設定をすべて使用可能にする必要があります。こうすると、センサーはネットワークに接続されると同時に Zero Configuration 機能を使用し始め、Enterprise サーバを探します。Enterprise サーバを見つけると、センサーは Enterprise サーバの IP アドレスと共に、ネットワーク設定を取得します。そして、Enterprise サーバと共有秘密鍵を用いた安全な方法で通信を開始します。Enterprise サーバはセンサーから稼動していることを示すハートビートを受信し続けます。

Enterprise コンソール上で、ネットワークに接続されたすべてのセンサーはセンサーツリー上で『未承認』とマークされて表示されます。これらのセンサーは基本的にこの時点ではまだ認可されていないため、いずれも警報や ACL データを送信していません。これらは、ネットワーク上に存在することを示すため、ハートビートをサーバに送信するだけです。センサーをコンソール上で見つけたとき、それらを承認し、センサーツリー上のそれぞれの配置にドラッグすることができます。また、センサーの管理ダイアログを用いてセンサーの配置し直しや編集をすることができます。

この方法は大規模・小規模の配置に適しています。

センサー Zero Configuration のクイックスタート

センサー Zero Configuration 機能を設定もしくは使用するには、次の条件を満たす必要があります：

- センサーがアクセス可能な DHCPサーバがネットワーク上に存在する必要があります。
- ネットワーク上にすでにインストールされた AirMagnet Enterprise サーバおよびコンソールが存在する必要があります。
- 同じサブネット上にインストールされたセンサーとサーバが存在する必要があります。

センサー Zero Configuration を使用可能にする方法:

1. コンソールから、管理 > 構成 の順にクリックしてください。マネジメントサーバ構成ダイアログボックスが表示されます。
2. 『Zero Configuration』タブを選択し、『Enterprise Zero Configuration』チェックボックスをチェックしてください。画面がリフレッシュします。図5を参照してください。

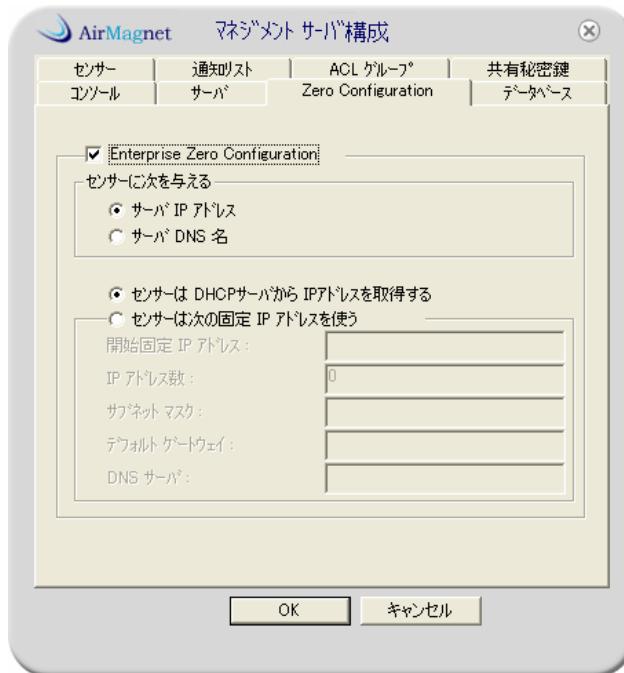


図 1: センサー Zero Configuration を使用可能にする

3. 「センサーに次を与える」項目では、「サーバ IP アドレス」を選択してください。
4. 「センサーはDHCPサーバからIPアドレスを取得する」ラジオボタンを選択してください。
5. [OK] をクリックし、マネジメントサーバ構成ダイアログボックスを終了してください。
6. AirMagnet EnterpriseサーバとDHCPサーバがインストールされているのと同じ(サブネット) ネットワークにセンサーを接続してください。
7. センサーの電源を入れてください。自動的に Enterprise サーバを見つけます。
8. Enterprise コンソール画面上で各センサーを右クリックし、ポップアップメニューから「承認」を選択してください。
9. センサーをセンサーツリーのそれぞれの場所へドラッグ アンド ドロップしてください。

注意: 上記の方法にはDNSサーバの使用法は含まれていません。そのため、センサーがDNS名前解決経由でEnterpriseサーバを見つけることができないときは、センサーはUDPパケットをブロードキャストします。Enterprise Serverが同一ローカルネットワーク(サブネット)に存在すると、そのUDPパケットを受信します。そして、センサーとサーバは情報を交換し、センサーはサーバにアクセスするための設定を行うことができます。ネットワークが単一のsingle-layeredネットワークのときは、UDP方式で十分です。しかし、たいいていのネットワークにおいてZero Configurationを適切に可能にするために、DNSエントリーを必要とします。

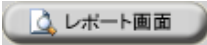
Cisco WLAN モニタ アクセスポイント用 AirMagnet AirWISE エージェント

Cisco WLSE との統合により、無線セキュリティにおいて最も時間がかかり、労力を必要とする仕事を合理化する、業界の最も進んだIDS/IPSソリューションと主要な無線ネットワークおよびデバイス管理プラットフォームが導かれます。これにより、簡単にACL(アクセスコントロールリスト)を

WLSE 配置から AirMagnet Enterprise システムに直接インポートすることができます。その後、Rogue Triangulation (三角測量)、トレースやブロックを行うため、AirMagnet のあらゆる機能を使用することができます。また、未承認のアソシエーションや不適切なセキュリティ構成などといった問題を探することも可能です。

Cisco WLAN モニタ アクセスポイント用 AirWISE エージェントを構成する詳細な方法は技術文書 “Integrating AirWISE Agent with Cisco Scanner APs” に述べられています。この文書は、登録された顧客は <http://www.airmagnet.com> から無償ダウンロード可能です。

AirMagnet Enterprise Reporter の統合

AirMagnet Enterprise 6.1 では AirMagnet Enterprise Reporter が統合されています。この機能により、無線 LAN データを専門的なレポートの形式で表示、エクスポートおよび印刷することが可能です。このレポートにより、ネットワーク管理者は容易にデータを保存、共有、解析することができます。この機能は開始、チャンネル、インフラストラクチャ、AirWISE およびチャート画面からアクセスできます。レポートにアクセスするには、画面上部のメニュー領域から  をクリックし、表示したいレポートを選択してください。下の図 2 にレポート画面の例を示します。

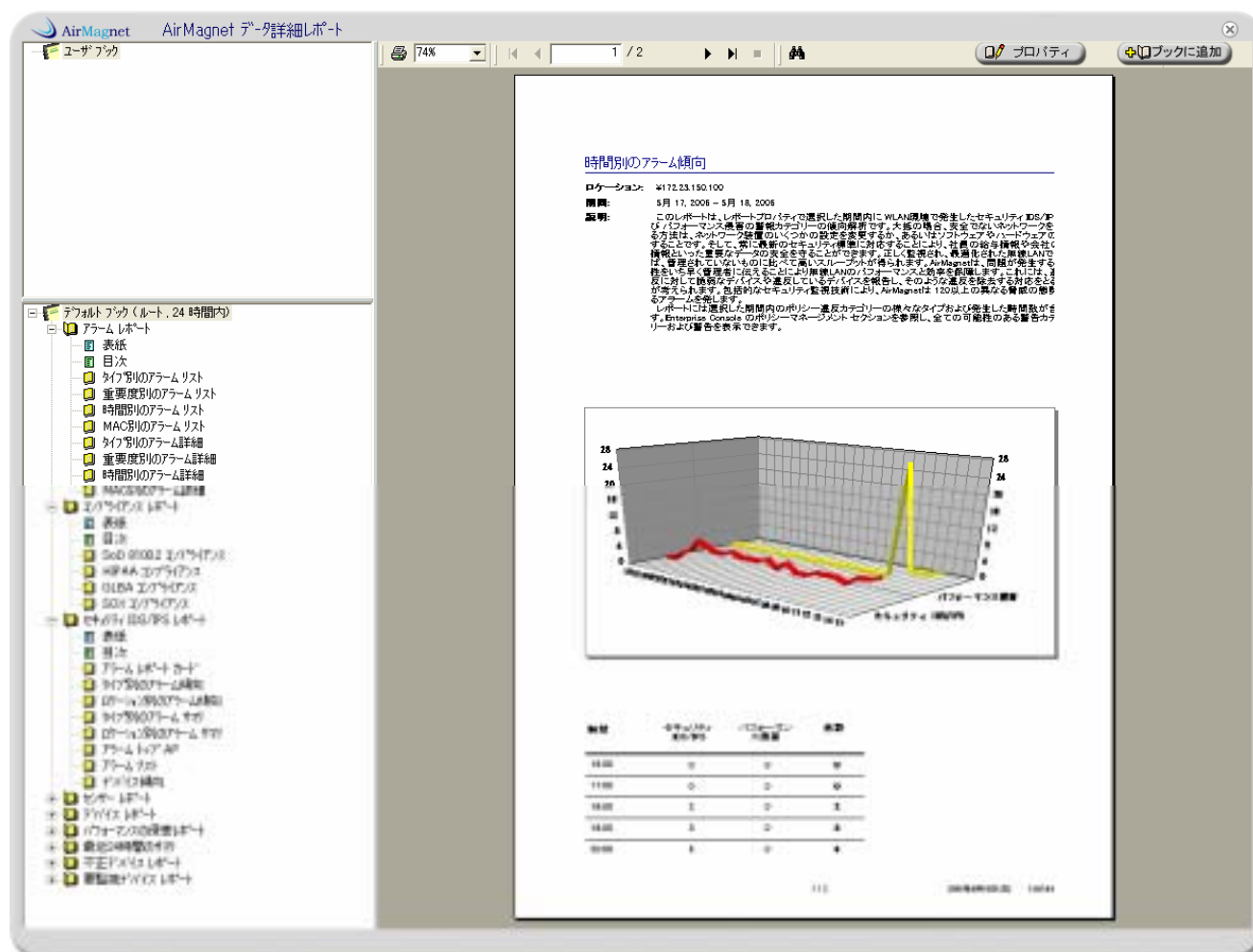


図 2: AirMagnet Enterprise レポート画面

規制コンプライアンスレポート

AirMagnet Enterprise 6.1 には次の 4 つの規制コンプライアンスレポートが含まれています。

- 米国国防総省 (Department of Defense Directive) 8100.2 コンプライアンスレポート (DoD 8100.2)
- 医療保険の携行性と責任に関する法律 (Health Insurance Portability and Accountability Act) コンプライアンスレポート (HIPAA)
- グラム・リーチ・プライリー法 (Gramm-Leach Bliley Act; 金融 機関向け顧客情報守秘に関する法律) コンプライアンスレポート (GLBA)
- サーベンス・オクスリー法 (Sarbanes-Oxley Act; 米国企業改革法) コンプライアンスレポート (SOX)

各コンプライアンスレポートは政府規制の紹介から始まっています。そして、さまざまなレベル、すなわち、システム、アラーム、およびデバイスのネットワークのコンプライアンス・ステータスを評価します。データは表およびグラフ形式で表示され、データを理解、解析しやすくなっています。これら全てのレポートは政府規制と、規則の監視および強化を支援する AirMagnet 無線ネットワークポリシー・アラームを結び付けます。これらレポートにより、Enterprise の無線 LAN に存在するコンプライアンスの問題を簡単に特定し、政府規制の適合を実現します。図 3 と 4 に DoD 8100.2 コンプライアンスレポートの例を示します。

1/ システムレベルのコンプライアンスレポート

このレポートは、ネットワーク全体の DoD 指令への適合性をポリシーごとに要約します。

DoD 指令 8100.2 ポリシー項目	適合性
4.10. DoD の無権限に関する無権限管理(レベル)マネジメントセスを確立し、脆弱性の評価、被害の防止策、および無権限バイスの検出と排除の手順を有すること。	AirMagnet のレポートおよび解決策は、無権限管理プロセスを促進し、コンプライアンスを確実にします。
5.1.3. 全ての DoD 無権限活動の管理方法とポリシー整備を! 視および提供すること。	監視およびレポートでポリシーを整備。
5.1.4. 無権限設備、サービス及びシステムのコストの最適化および相互操作性とセキュリティの促進。	無権限設備の情報を提供し、コストダウンの持続的相互操作性の促進およびセキュリティを促進。
5.1.5. DoD 無権限管理プロセスの整備および実施を指示し、DoD 無権限情報の共有を強化。	レポートおよび解決策が無権限管理プロセスの整備を確実にします。
5.2.3.1. DoD 要件に対応する無権限技術と関連する危険と性を査定。	AirMagnet アラームは DoD 要件に対応した危険と脆弱性を査定します。
5.5.3. 潜在的無権限解決策を評価するとき、無権限管理セスを確実に使用。	潜在的無権限解決策を評価するとき、AirMagnet は無権限管理プロセスを確実に使用します。
5.6.4. 無権限技術を評価している活動が脆弱、弱点、脆弱性無権限技術および関連するセキュリティ手順に無権限管理プロセスにフィードバックすることを確認。	無権限管理プロセスにフィードバック。

図 3: DOD 8100.2 コンプライアンスレポート サンプル 1

12 の新規 IDS/IPS およびパフォーマンス侵害アラーム

無線 LAN パフォーマンス管理に加え、侵入検出および防止を支援するため、次の新しいアラームが AirMagnet Enterprise 6.1 に追加されました。これらの説明は、AirMagnet Enterprise コンソールの AirWISE 画面を参照もしくは **管理 > ポリシープロファイル...** をクリックしてください。

- IEEE 802.11i/AES でプロテクトされていないデバイス
- ARP リクエストの繰り返し攻撃 - 高速 WEP クラックの実行中
- 音声トラフィックにより過負荷の AP
- 音声トラフィックによる高いチャンネル使用率
- 音声トラフィックに最適化されていないパワーセーブ DTIM 値
- VoWLAN マルチキャストトラフィックの検出
- VoWLAN 電話による過剰なローミングまたは再アソシエーションの検出
- 相互に干渉している AP による音声品質の低下
- デバイスセキュリティ異常による Day-Zero 攻撃
- 無線 LAN セキュリティ異常による Day-Zero 攻撃
- デバイスパフォーマンス異常による Day-Zero 攻撃
- パフォーマンス異常による Day-Zero 攻撃

既知の問題

1. パケットエラーメッセージを取得するには、ユーザはスイッチを固定デュプレックスモードに設定する必要があります。また、センサーが接続しているポートで過度のエラーが観測されるときは、スイッチポートを 100Mbps 全二重にする必要があります。
2. 手動でスイッチリストにスイッチを追加するとき、必須のコミュニティ読込文字列がブランクのままであってもユーザは注意を促されないことがあります。(4703)
3. センサー管理: Zero Configuration の 固定 IP セクションは機能しません。サーバの発見に UDP パケットを使用するとき、完了するにはセンサーをリポートする必要があります。(8062)
4. 終端されていない標準より長いシリアルケーブルが接続されている時、センサーはリポートから回復できないことがあります。(8096)
5. チャンネルフォーカスは Cisco スキャン AP を用いて動作することができません。そのため、リモートアナライザのチャンネルおよびインフラストラクチャ画面は Cisco スキャン AP を使用しているとき十分に機能することができません。(8245)
6. AirWISE エージェントセンサーは有線/無線トレースもしくは有線/無線ブロックができません。(8251)
7. AirMagnet Enterprise マネジメントサーバは現在 OpenSSL バージョン 0.9.7a を使用しています。このバージョンは脆弱性の配置で脆弱性を誘発することがあります。(8316)

8. ポリシープロファイルに多数の SSID を用い、6.1 から 5.2 にダウングレードすると、SSID グループが前のバージョンに戻るのを妨げ、混乱した反応を引き起こす可能性があります。(8457)
9. センサーを多数配置していると、ロードに問題が起こるレポートがあります。(8481)
10. センサーを多数配置していると、センサーの削除機能でセンサーツリーから指定したセンサーを削除しないことがあります。センサーはしばらく消えていますが、また表示されます。(8532)
11. ファイアウォール越しにリモートアナライザを起動するとき、プロキシ IP アドレスが、センサーをダブルクリックすると表示される『リモートセンサーログイン』画面に表示されないことがあります。この問題を解決するには、接続に失敗したとき、『センサー名』フィールドにプロキシ IP アドレス入力してください。
12. 『隣接』とマークされたデバイスが『MAC アドレスによる不正な AP (ACL)』警報を発生することがあります。
13. 2 番目のポリシー規定もしくはしきい値を『MAC アドレスによる不正な AP (ACL)』や『MAC アドレスによる不正な端末(ACL)』警報 - 通知に追加できることがあります。これらは、製品の設計上可能とはみなされていません。これら 2 つの警報に対して、2 つ以上のポリシーやしきい値を設定しないでください。
14. 開始画面の時間ごとのパフォーマンス侵害ポリシーのバブルヘルプの合計値が正しくないことがあります。
15. アラームおよびデバイスのレポートの位置別のフィルタは正しく動作しないことがあります。
16. 時々、ハブの相関関係(有線傍受)が予期しない距離のノードを表示することがあります。
17. アプリケーションが隠匿された SSID を用いた WEP128 を使用している AP とアソシエートできないことがあります。(9165)
18. 時々PING ツールはスムーズに動作しないことがあります。(9309)
19. ポリシープロファイルに緊急しきい値設定がないとき、センサーは緊急の『DoS: 認証解除フラット攻撃』警報を発生することがあります。(9400)
20. SOX(Sarbanes-Oxley) レポートはコンプライアンスカテゴリーに間違った表示をしたり、欠損をしたりすることがあります。(10351, 10353)
21. IDS/Rogue 画面上で、ある ACL グループに複数の AP を同時に設定すると、設定できない AP がある場合があります。(10221)
22. コンプライアンスレポートはコンソール上に表示されたデバイスの合計とは異なる数値をデバイスの合計として表示することがあります。(10361)
23. 『承認されていないアソシエーションの検出』警報の説明に、含まれるデバイスの ACL グループが表示されないことがあります。(10362)
24. AM5020 および AM5023 型のセンサーはリモート UI デコード画面上で、”not available” フレームを多数表示することがあります。これらのフレームは無視できる余分なゼロ長のフレームです(8515)

25. デバイスごとのコンプライアンスレポートは DoD、HIPAA、GLBA および SOC コンプライアンスレポートの各セクションに対して問題のあるデバイスの正確な個数を表示しないことがあります。(9707)
26. AirMagnet Enterprise5.0 から 6.1 にアップグレードするとき、日本語プロファイル名や通知名が文字化けすることがあります。AirMagnet Enterprise Server のアップグレードは AirMagnet Enterprise6.1 インストーラ画面で『修正』を選択するようにしてください。AirMagnet Enterprise Server 5.0 をアンインストールした後 6.1をインストールしなおすときは、<インストールディレクトリ>¥AirMagnet Inc¥AirMagnet Management Server¥web¥AMom¥Configs フォルダを削除しないでください。
27. リモートアナライザのポリシーマネジメント画面で新規追加した通知名が表示されないことがあります。ポリシーの内容はコンソール画面のポリシープロファイル画面を確認してください。
28. SSID が空白のとき、リモートアナライザのレポート画面で、AP/STA リストが正しく表示されません。コンソール・レポート画面のデバイスレポートを参照してください。
29. Windows 2000 をご使用のとき、AirMagnet Enterprise コンソールを使用するとき、コンソールおよびリモートアナライザのレポート画面上でレポートのプロパティを開くと、レポートタイプ、ロケーションフィルタ、デバイスフィルタ並びに AirWISE フィルタに日本語が表示されないことがあります。フィルタ名横の ボタンをクリックしてツリーを開き、選択項目を確認してください。
30. Windows2000 をご使用のとき、AirMagnet コンソール 警告ウィンドウの警告名が表示されることがあります。このときも、この警告名をクリックし、AirWISE 画面を表示すると警告内容を確認することができます。

テクニカルサポート

AirMagnet製品の技術的なお問い合わせ先は次の通りです。

お問合せ先: 株式会社 東陽テクニカ

TEL:03-3245-1250

E-mail: wlan@toyo.co.jp

テクニカル サポートは、月曜日～金曜日の午前 9 時 30 分～午後 5 時 30 分の間、ご利用いただけます。
