ワイヤレス不正侵入防御システム（WIPS）

Techinical Brief

WatchGuard Technologies,Inc.

発行：2016 年 8 月

はじめに

世界的な Wi-Fi の普及によって、サイバー攻撃者は、無防備なユーザのシステムに侵入し、データを不正に取得したり、システムを感染させたりする便利な手段を手に入れることになりました。本書の発行日現在、YouTube には、Wi-Fi ユーザのハッキング方法を解説する動画が 30 万以上も公開されていますが、いずれも、オンラインで簡単に入手でき、使い方も簡単でありながら、それでいて、強力な機能を備えたツールが利用されています。従業員や顧客、あるいは来客向けに Wi-Fi を提供したとしても、このような悪意ある行為を許すべきではありません。本書では、**ウォッチガードのワイヤレス不正侵入防御システム（WIPS）**でこの問題を解決する方法を解説します。WIPS は、ウォッチガードのクラウド対応アクセスポイントをウォッチガード Wi-Fi Cloud で管理する場合にご利用いただけます。Wi-Fi Cloud サービスの管理体系におけるサブスクリプション契約が有効であれば、 AP を Firebox ネットワークの配下で利用しても、別のファイアウォールネットワーク接続環境においても、この保護機能を利用できる柔軟性を兼ね備えています。

他社ソリューションに決定的に不足している機能

他社の無線不正侵入検知・防止システムのほとんどは、近接する正規の Wi-Fi ネットワークとの干渉に配慮して、防止よりも検知に主眼を置いています。他社ソリューションでは多数の誤検出が検知されるために、管理者がアラートを無視したり、通知そのものを無効にしたりし、結果的に組織全体が保護されないままの状態になります。

現在利用できる他社の WIPS テクノロジは、高度な管理作業を必要とし、不正 AP 検知が十分に機能しない場合も少なくありません。このようなシステムに頼る組織の多くは、セキュリティに対する認識が不十分で、不正 AP を介したデータ流出に対して自社ネットワークが脆弱であるという事実を正しく理解していません。

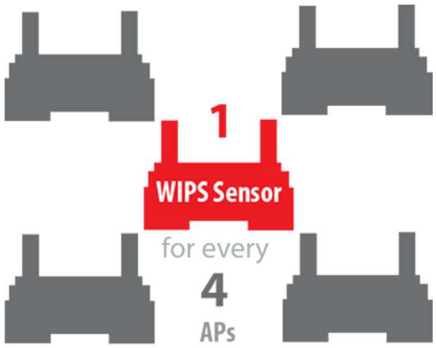
無線空間の完全な制御

ウォッチガードの WIPS を導入すると、エンタープライズクラスのセキュリティを最小限の管理作業で Wi-Fi ネットワークで実現し、PCI、HIPAA、サーベンスオクスリー法などの適合基準への準拠を可能にします。ウォッチガードの WIPS は、特許取得済みの Marker Packet テクノロジを活用することで、業界でも最も安定で信頼でき、誤検出の最も少ない WIPS を実現し、Wi-Fi 空間の完全な制御を可能にします。

ウォッチガードの WIPS の利用と導入の方法

ウォッチガード Wi-Fi Cloud の有効なライセンスを利用し、クラウド対応のすべてのアクセスポイントをウォッチガード Wi-Fi Cloud で管理することで、ウォッチガード WIPS がサポートされます。次の 2 つの方法で、WIPS を導入できます。

方法 1：専用 WIPS センサモード（推奨）



この導入オプションでは、クラウド対応 AP を専用の WIPS センサとして構成します。AP が専用の WIPS センサとして機能するこの方法では、専用 WIPS センサとして稼働する AP が無線クライアントの接続を許可しなくなり、代わりに、他の AP が一緒に設置されて、クライアントトラフィックを処理するように構成されます。WIPS センサ対 AP カバレッジの一般的なルールでは、4 台の AP に対して 1 台の WIPS センサを設置します。これは、ウォッチガードが推奨する導入モデルであり、専用の WIPS センサ機が常に空間を防御し、WIPS/AP モード機によって生じる時間枠を攻撃者が使用しないようにできるため、最も安全な無線環境が実現します。

方法 2：WIPS/AP 共有モード

すべてのクラウド対応 AP が WIPS センサ機能と AP 機能の 2 つの機能の併用となり、無線クライアントトラフィックの処理と WIPS のスキャンの割合をパーセントで指定します。このモードでは、1 台の AP がアクセスポイントと WIPS センサの両方として機能しますが、無線側のパケットインジェクション機能は利用できません。

専用 WIPS センサモード(推奨)	WIPS/AP 共有モード
スキャン専用の機器がデュアルバンドのラウンドロビンスキャンを実行（5 秒ごとに 100 ミリ秒間、各チャネルをスキャン）	AP として動作する機器がバックグラウンドでデュアルバンドのスキャンを実行（2 分ごとに 100 ミリ秒間、オフトラフィックチャネルをスキャン）
全チャネルで脅威を高速検知	オフトラフィックチャネルの脅威の検知に時間がかかる（Marker Packet™ インジェクションはチャネル訪問のタイミングで実行されるため、業界最高の不正 AP 検知であると言える）
無線と有線の防御が可能で、あらゆる種類の脅威をブロックできる	有線のみの防御（有線側の tarpitting（時間の引き伸ばし）による不正 AP のブロック）
主な用途：高度のセキュリティ／コンプライアンスが求められる環境（金融、公的機関、医療、技術、学校など）	主な用途：小売業の PCI コンプライアンス

AP が専用センサモードである場合の処理

防止レベルと攻撃を防御する同時チャネル数のバランスに応じて、3 つの防止レベルから選択できます。RF 通信では、各機器が一定の時間を使用して、各チャネルの攻撃を防御します。攻撃を同時に防御するチャネルの数が多いほど、機器が各チャネルの防御に使用できる時間が短くなります。複数の AP を WIPS センサモードに追加すると、最高レベルの防御を実現でき、より多くの WLAN チャネルをカバーできるようになります。

- **Block（ブロック）**：1 台のセンサが、2.4GHz 帯と 5GHz 帯のいずれか 1 チャネルの不正通信をブロックできます
- **Disrupt（遮断）**：1 台のセンサが、2.4GHz 帯と 5GHz 帯のいずれか 2 チャネルの不正通信を遮断できます
- **Interrupt（中断）**：1 台のセンサが、2.4GHz 帯と 5GHz 帯のいずれか 3 チャネルの不正通信を中断できます
- **Degrade（低下）**：1 台のセンサが、2.4GHz 帯と 5GHz 帯のいずれか 4 チャネルの不正通信のパフォーマンスを低下させることができます

ウォッチガードの WIPS の仕組み

有線側 Marker Packet インジェクション

WIPS が、WIPS/AP の有線側からの有線ネットワークに Marker Packet をインジェクションします。これらのパケットが監視対象の有線側ネットワークに接続された AP によって無線側にリレーされ、WIPS/AP の無線側によって無線経由で検知されます。AP は、1 つのサブネット内、または複数のサブネットの管理対象スイッチのトランクポートに配置され ます。

この方法には、次のような利点があります。

- ネットワーク内のスイッチの負担になるやり取りを必要としない
- 初期設定や運用に伴う継続的な設定を必要としない
- この方法では、AP が各ローカルサブネット上で同時に動作するため、ネットワークがどのような規模であっても、AP の接続が短時間で検知される
- パケットインジェクションによって発生するトラフィック量は極めて少ない（LAN ポートの処理能力の 0.1% 未満）
- この方法では、不正 AP を外部 AP としてマークせず、外部 AP を不正 AP としてマークすることもないため、誤検出アラームは発生しない

無線側 Marker Packet インジェクション

WIPS/AP が AP に関連付けられたクライアントを認識すると、WIPS/AP は、不正 AP の疑いのある AP の無線側から、既知の有線側ホストの IP アドレスを宛先として、一意の識別子（Marker Packet）が付加されたパケットを送信します。これらのパケットは、不正 AP の被疑のある AP とクライアントの接続とともに抱き合わせで付加されます。このようなパケットがターゲットホストで受信されると、AP が監視対象有線ネットワークに接続されていることが確認されます。

他のソリューションにはない独自の機能：AP の自動分類

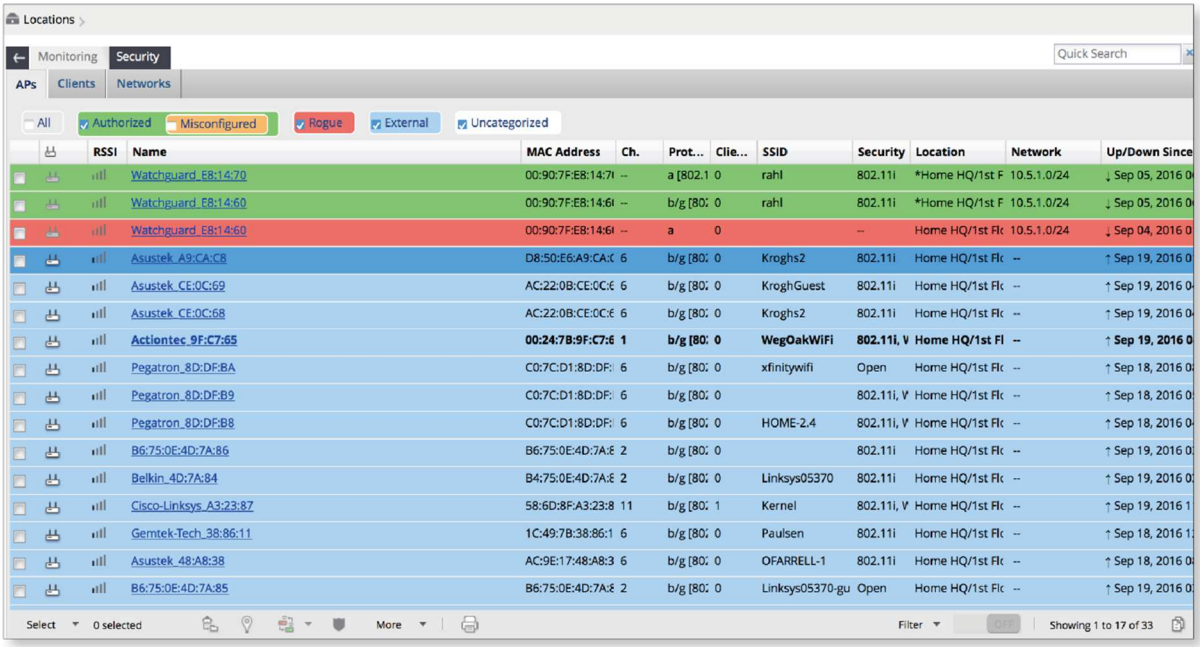
AP を自動分類する最も自然で効率的な方法は、ネットワーク接続の検知によるものです。このような自動分類には、SSID、ベンダ、パワーレベル、暗号化設定、チャネルに

基づく、信頼性が低く管理性の低い分類シグネチャは必要ありません。必要なのは、信頼性の高いネットワーク接続と宛先の VLAN へのアクセスだけです。

正確で信頼できる AP 自動分類は、「実用的な」ワイヤレス不正侵入防御システムの重要な要素です。ウォッチガードの WIPS は、AP ネットワーク接続ベースの自動分類を標準装備する唯一のテクノロジです。ウォッチガード独自の Marker Packet テクノロジを採用し、AP のすべての種類のネットワーク接続を正確に検知することで、このような自動分類が実現されています。Marker Packet は、他の WIPS ソリューションとの真の差別化要因である、ウォッチガード独自のテクノロジです。

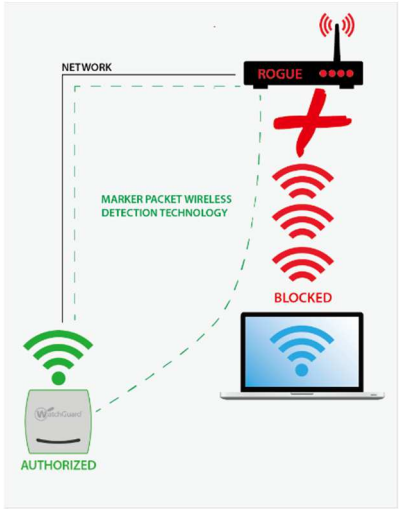
AP の自動分類では、AP が次の 3 つのカテゴリに分類されます。

- **Authorized（認証済み）** – 管理者が認識し、有線ネットワークで管理される AP
- **External（外部）** – 監視対象有線ネットワークに接続されていない、無線ネイバー内の管理対象外の AP
- **Rogue（不正）** – 管理者に認識されることなく有線ネットワークに設置された、未認証の AP



ウォッチガードの WIPS には、次のような利点があります。

- **検知**だけにとどまらない、真の**防御**
- Marker Packet テクノロジ
- 誤検出ほぼゼロで有線ネットワークのデバイスを正確に分類
- NAT、暗号化、ソフトウェア変換を使用する AP を検知／分類／防御
- 未認証クライアントの挙動を検知／ブロック
- 隣接するデバイスやネットワークに影響を与えることなく、自動防御が可能
- 複数チャネルの複数の脅威を 1 台のセンサから防御
- 複数の種類の 802.11 DoS 攻撃をブロック
- VLAN、SSID、および場所ごとに無線ポリシーを強制



- マルチ VLAN サポート（1 台のセンサで最大 100 の VLAN をサポート）
- CAM テーブルルックアップや SNMP に依存しない方法を活用
- モバイルデバイスウォッチリスト
- オフラインセンサモード（常時オンセキュリティ）
- 任意のセンサからのリモートパケットキャプチャ（R-PCAP）
- 1 台のセンサから最も正確に場所を追跡
- 1 つのコンソールから数千のセンサの管理が可能
- セキュリティ／コンプライアンスの豊富な自動レポート
- 使用と導入の容易性を最少の TCO で実現
- 米国防総省 8100.2WIDS 要件を上回る機能
- 同一の「Wi-Fi なし」のポリシー強制をネットワーク内の有線 VLAN に対して提供

他社 WIPS ソリューションの 5 つの落とし穴

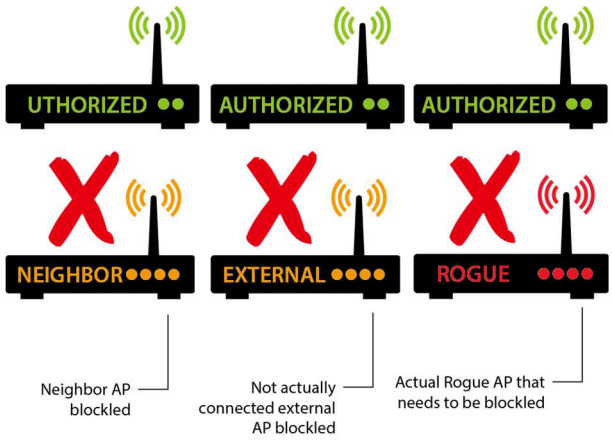
すべての WIPS が同じように設計されているわけではありません。そこで、この事実を理解するために、競合することが多いいくつかの WIPS ソリューションの 5 つの落とし穴を検証することにします。

（1）不正 AP の検知

不正 AP が、認証済みネットワークに接続している未認証の AP として定義されることがあります。不正 AP による未認証の無線アクセスが可能になるため、ネットワークにとって重大な脅威となります。従業員の不注意や内部からの不正アクセスの試行によって、不正 AP がネットワークに存在する事態が発生することがあります。

多くの競合 WIPS ソリューションでの LAN 内の不正 AP の検知では、領域内に存在し、認証済み AP のリストに属していないすべての AP を不正 AP であると宣言するという方法が使用されますが、これには、次のようないくつかの欠点があります。

- **誤検知/誤通知**：未認証 AP が領域内に存在するものの、実際には監視対象有線ネットワークに接続されておらず、従って、セキュリティ脅威にならない場合であっても、セキュリティ警告が発生する
- **手動介入**：システム管理者が領域内に存在する未認証 AP を手動で検証し、実際にはどれが不正 AP で、どれが外部 AP（近接 AP）であるのかを判断する必要がある
- **自動即時防御の欠如**：近接 AP を無差別に誤ってブロックすることがないようにする必要があるが、多くの競合 WIPS ソリューションでは、不正 AP を自動的かつ即時にブロックすることができない



（2）シグネチャベースの IPS

競合する多くの WIPS は、ユーザが構成した分類シグネチャに基づいてアプリケーションを分類しようとします。SSID、ベンダ、パワーレベル、暗号化設定、チャネルなどの多種多様な AP の特性を使用して、分類シグネチャを定義します。ネットワ

ークへの AP のネットワ―ク接続は、分類ルールの要素となることも、ならないこともあります。この方法には、次のようないくつかの欠点があります。

- **シグネチャの保守**：分類シグネチャの定義に伴う構成のオーバーヘッドが大量に発生し、シグネチャを定期的に更新する必要がある（たとえば、既知の近接する無害な WLAN 構成が変更されて、異なる SSID を使用するようになった場合など）。
- **継続的な手動の作業**:新たに検知された AP の無線構成が定義済みのシグネチャと完全に一致しない場合、新たに検知された AP を分類するための手動の作業が必要になる。
- **脅威の見落とし**：この方法では、本当の脅威を見落としてしまう可能性が高くなる。たとえば、「SSID=freewifi AND signal strength = Low; then classify as known neighbor AP（SSID が freewifi で signal strength が Low の場合は、既知の近接 AP に分類する）」といった分類シグネチャでは、SSID が「freewifi」に設定されている、伝送能力が Low である不正 AP の侵入を許すことになる。

3）MAC テーブルルックアップ

この方法では、領域内に存在する無線デバイスの MAC アドレスを有線ネットワーク内の管理対象スイッチのポートに登録されている MAC アドレスと比較します。無線側と有線側に共通する MAC アドレスが見つかれば、その MAC アドレスをもつデバイスが監視対象有線ネットワークに接続されていると判断されます。
ブリッジング AP の場合、クライアントが AP に接続するまで、検知が待たされることになり、クライアントの接続後に、クライアントの MAC アドレスが、AP が接続されているスイッチポートに登録されます。ネットワーク内の管理対象スイッチのポートに登録された MAC アドレスの収集は、SNMP 経由で各スイッチの CAM テーブルをポーリングすることで実行されます。

これには、いくつかの欠点があります。

- この方法では、スイッチングインフラで面倒な作業が発生します。すなわち、スイッチの MAC テーブルをポーリングできるようにするための、WIPS のスイッチ資格情報の保守が必要になります。また、異なるベンダ

のスイッチとの相互運用性の問題が発生します。

- ネットワーク内のすべての管理対象スイッチの MAC テーブルのポーリングは、特に何百ものスイッチが存在する大規模ネットワークにおいては、大量のリソースを消費する、時間のかかるタスクです。そのため、大規模ネットワークでは、この方法によるネットワーク接続の検知の頻度が少なくなる可能性があり、検知に「運」という要因が加わることになります。クライアントが非アクティブ状態になった後に、そのクライアントの MAC エントリが MAC テーブルから消去されると、MAC テーブルのポーリングの発生時（通常は、定期的な間隔でスケジュールされます）に、そのクライアントが実際には不正 AP に接続されているにもかかわらず、この方法が成功してしまうことになります。

（4）受動的な MAC 相関付け

この方法は、MAC テーブルルックアップの欠点を解消しようとするものであり、WIPS AP が有線側インターフェイスで、サブネットでアクティブである MAC アドレスを受動的にリスンします。そして、この方法で検知された MAC アドレスが、有線／無線の MAC アドレスの相関付けに使用されます。

ただし、この方法であっても、近接 AP などで AP が監視対象ネットワークに接続されていない場合にも、監視対象有線ネットワークに接続されているかのように認識されてしまう可能性があります。クライアントでこれらの AP 間での切り替えが発生すると、このような問題が発生します。

（5）無線側トレース

この方法では、WIPS AP が領域内の AP を検知した後に、無線側の AP への接続を能動的に試行します。WIPS AP は次に、不正である可能性がある AP 経由で有線ネットワークに対して何かを ping するか、ネットワークの有線側の既知のホストにパケットを送信することで、AP が企業内の有線ネットワークに接続されているかどうかを検知しようとします。AP への接続を能動的に試行する、この方法には、いくつかの制限があり、L2 と L3 の接続を完了することで AP に接続するまでに、かなりの時間（たとえば、最長で 5 秒）を要します。この間、WIPS AP は AP のチャネルにロックする必要があり、スキャン機能を実行できなくなります。したがって、WIPS AP が認識する潜在的な不正 AP が数多く存在する環境では、この方法を実行できる回数が少なくなり、結果として、AP 接続の検知でかなりのレイテンシが発生する可能性があります。さらには、たとえば、

無線インターフェイスに認証済みクライアント MAC アドレスなどの特別な設定が存在し、WIPS AP が潜在的な不正 AP への関連付けを能動的に実行できない状況では、この方法で不正 AP を検知することはできません。

ベストインクラスの WIPS と UTM の統合

ウォッチガードの革新的製品はいずれも、中小規模の環境にも適合するエンタープライズグレードのセキュリティを提供するという基本理念に基づいて設計されています。世界をリードする WIPS テクノロジとベストインクラスの UTM サービスが統合された、ウォッチガード Wi-Fi Cloud を利用することで、IT プロフェッショナルは、セキュリティを犠牲にすることなく、ユーザが求める高パフォーマンスの無線接続を提供できます。

ウォッチガード Wi-Fi Cloud の詳細については、ウォッチガードの販売パートナーにお問い合わせください。

ウォッチガード・テクノロジー・ジャパン株式会社
東京都港区麻布台 1－11－9　CR 神谷町ビル 5 階　　TEL:　03-5797-7205
WEB: https://www.watchguard.co.jp

ウォッチガードについて

WatchGuard® Technologies, Inc.は、業界標準のハードウェア、最高クラスのセキュリティ機能、およびポリシーベースの管理ツールをインテリジェントに組み合わせた統合型の多機能ビジネスセキュリティソリューションを提供する、グローバルリーダです。WatchGuard は、世界各国の数千の企業に使いやすく優れた防御機能を提供しています。WatchGuard の本社は、米国ワシントン州のシアトルにあり、北米、欧州、アジア太平洋、および南米にオフィスを展開しています。明示的または黙示的な保証は一切提供されません。すべての仕様は変更される可能性があり、今後新しい製品や機能が利用可能となり提供されることが予測されます。