APPENDIX A

wIPS ポリシー アラーム リファレンス

この付録では、wIPS が対応している脅威のタイプの概要について説明します。構成は次のとおりです。

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）

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。

さまざまな WLAN 環境用の設定済みのプロファイル

インストール中に、実装されている WLAN ネットワークに基づいて適切なプロファイルをユーザが選択できます。

wIPS は、次の項目に個別のプロファイルを提供します。

- Enterprise best practice
- Enterprise rogue detection only
- Financial（Gramm-Leach-Bliley 法に準拠）
- HealthCare（Health Insurance Portability and Accountability 法に準拠）
- Hotspot implementing 802.1x security
- Hotspot implementing NO security
- Tradeshow environment
- Warehouse/manufacturing environment
- Government/Military（8100.2 指令に準拠）
- Retail environment

適切なプロファイルを選択すると、wIPS は、該当 WLAN 環境に適したポリシー プロファイルのアラームを有効または無効にします。たとえば、医療機関の場合、[Helthcare] プロファイルを選択すると HIPAA 準拠のために必要なすべてのアラームが有効になります。管理者はインストール後にアラームを有効または無効にしたり、プリファレンスごとに閾値を変更したりできます。

wIPS システムは、IDS（侵入検知システム）であるだけではなく、IPS（侵入防御システム）でもあります。

Cisco Adaptive Wireless IPS のポリシーは、「wIPS：DoS（サービス拒否）攻撃」と「wIPS：セキュリティ突破」という 2 つのセキュリティ サブカテゴリに分類されます。

この項では、次のトピックを扱います。

- 「侵入検知：DoS 攻撃」（P.A-2）
- 「侵入検知：セキュリティ突破」（P.A-23）

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 NCS オンライン ヘルプを参照してください）。wIPS は、攻撃シグニチャの照合が行われる早期検知システムによってこのソリューションに寄与しています。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。

この項では、DoS 攻撃の 3 つのサブカテゴリについて説明します。この項は次のトピックで構成されています。

- 「アクセス ポイントに対する DoS 攻撃」（P.A-3）

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、NCS オンライン ヘルプを参照してください。

この項では、アクセス ポイントに対する DoS 攻撃について説明します。この項は次のトピックで構成されています。

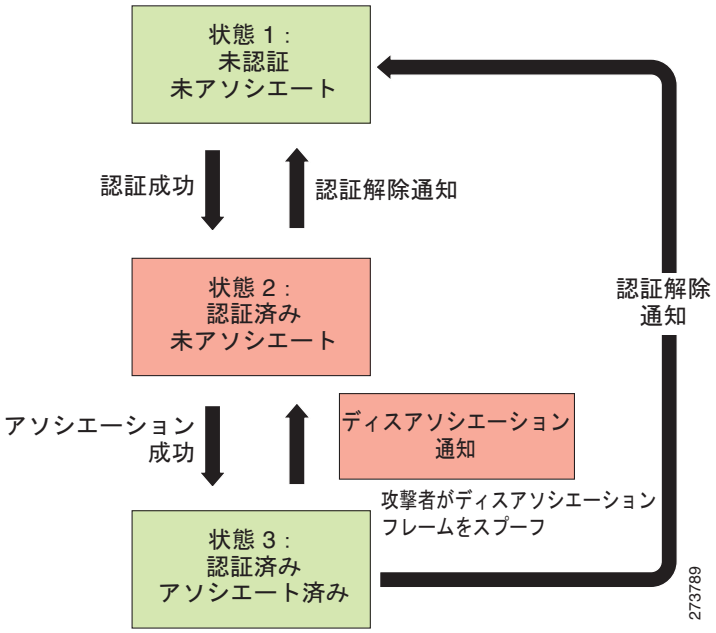
DoS 攻撃：アソシエーション フラッド

アラームの説明と考えられる原因

この DoS 攻撃は、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 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作成して、ターゲット アクセス ポイントのクライアント 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。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（図 A-1 を参照）。

図 A-1　アソシエーション フラッド



wIPS による解決

wIPS はこの DoS 攻撃を検出するために、クライアント アソシエーションが正常に完了した後で、スプーフィングされた 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。wIPS によりこの攻撃が報告されたら、このアクセス ポイントにログインし、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 Wireless Control System Configuration Guide*』または NCS 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

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により、wIPS の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。

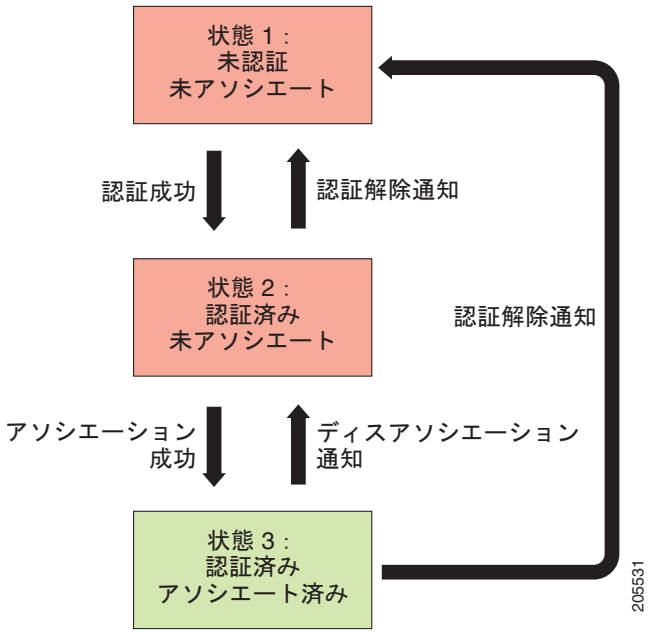
DoS 攻撃：認証フラッディング

攻撃ツール：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 標準に準拠してこのようなステート マシンを実装しています（図 A-2 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。

図 A-2　認証フラッド



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

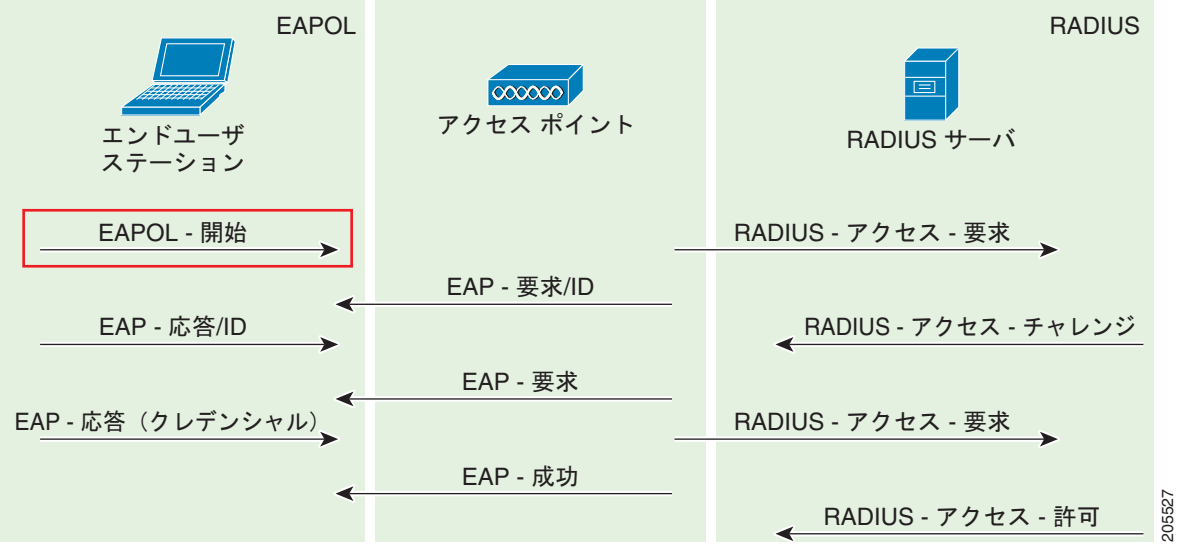
wIPS はこの DoS 攻撃を検出するため、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ アナリストはそのアクセス ポイントにログオンして現在のアソシエーション テーブルのステータスを確認できます。

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 標準は、EAP over LAN（EAPOL）を使用して認証プロトコルを定義します。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 ID 要求および内部リソース割り当てによって応答します（図 A-3 を参照）。

図 A-3　EAPOL-Start プロトコルおよび EAPOL-Start 攻撃



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

wIPS はこの DoS 攻撃を検出するため、802.1x 認証状態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 デバイスはアクセス 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

wIPS 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、ワイヤレス環境から削除します。

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 Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

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作成して、ターゲット アクセス ポイントのクライアント 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。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 攻撃の原因となります。

wIPS による解決

wIPS はこの DoS 攻撃を検出するために、クライアント アソシエーションが正常に完了した後で、スプーフィングされた 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。wIPS によりこの攻撃が報告されたら、このアクセス ポイントにログインし、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 Wireless Control System Configuration Guide*』または NCS 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

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。

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：CTS フラッディング」（P.A-9）

DoS 攻撃：CTS フラッディング

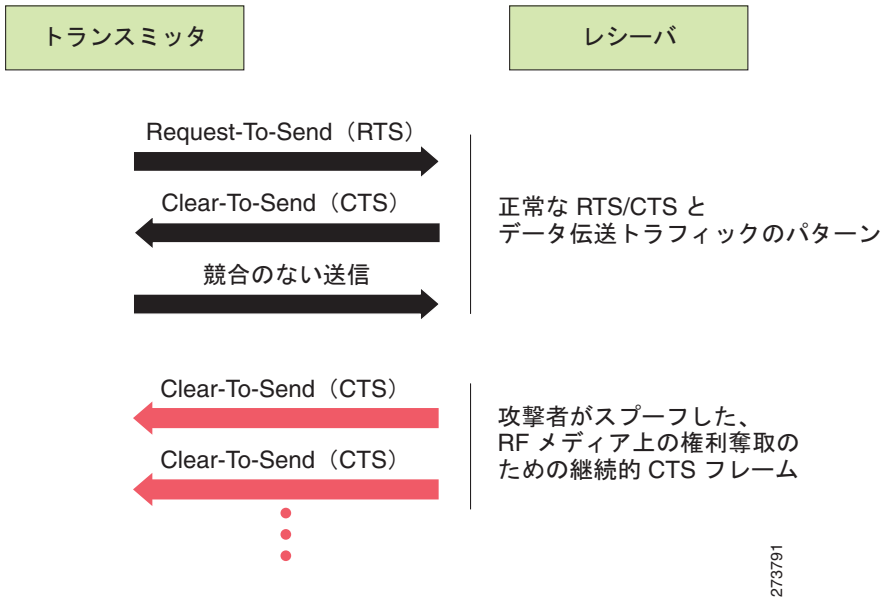
攻撃ツール：CTS Jack

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（図 A-4 を参照）。

図 A-4　RF 制御に対する CTS スプーフとチャレンジ



wIPS による解決

wIPS は、DoS 攻撃に対する CTS フレームの乱用を検出します。

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、次の URL を参照してください。

- www.isrc.qut.edu.au
- http://www.auscert.org.au/render.html?it=4091
- http://www.kb.cert.org/vuls/id/106678

wIPS による解決

wIPS は、この DoS 攻撃を検出して、アラームを発行します。当該デバイスを特定し、ワイヤレス環境から削除します。

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

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。攻撃者はこの WLAN の脆弱性を利用して 2 種類の DoS 攻撃を行う可能性があります。

- 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用して 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 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

wIPS は、RF 電波妨害攻撃の可能性のある特定しきい値を超える連続 RF ノイズを検出します。

Cisco Spectrum Intelligence にも、802.11 非準拠電波妨害デバイスを検出する機能があります。Cisco Spectrum Intelligence の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

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

wIPS は、DoS 攻撃に対する RTS フレームの乱用を検出します。

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 とすべての管理（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

wIPS は、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：ビーコン 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：MDK3-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 に対して認証フラッド攻撃を起動して、それらの AP がクライアントにサービスを提供しないようにする。
- 有効なクライアントとのすべてのアクティブな接続を切る。

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。

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。

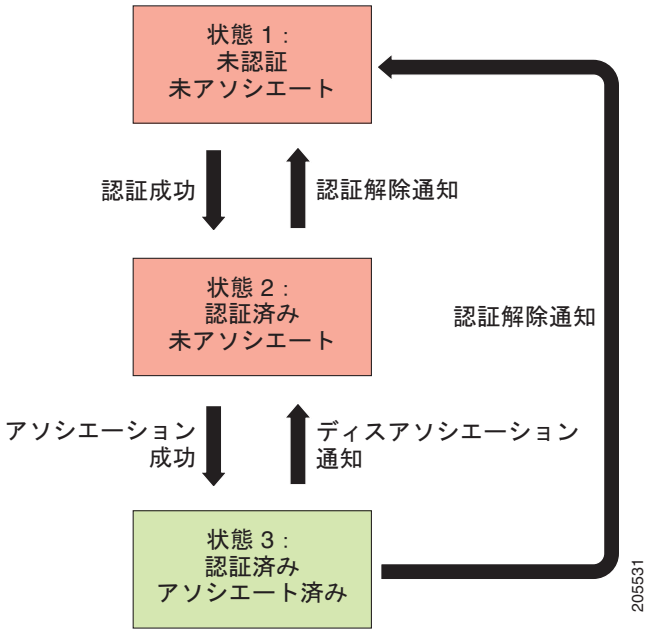
- 「DoS 攻撃：認証失敗攻撃」（P.A-13）
- 「DoS 攻撃：De-Auth ブロードキャスト フラッド」（P.A-15）
- 「DoS 攻撃：Dis-Assoc フラッディング」（P.A-18）
- 「DoS 攻撃：EAPOL-Logoff 攻撃」（P.A-19）
- 「DoS 攻撃：FATA Jack ツールの検出」（P.A-20）
- 「DoS 攻撃：不完全な EAP-Failure」（P.A-21）
- 「DoS 攻撃：不完全な EAP-Success」（P.A-22）

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（図 A-5 を参照）。適切にアソシエートされたクライアントは状態 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。

図 A-5　認証失敗攻撃



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）スプーフィングされます。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、これによりクライアントのワイヤレス サービスが切断されます。

wIPS による解決

wIPS は、この DoS 攻撃を検出するためスプーフィングされた 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、IEEE 802.11 の認証方式（オープン システムと共有キーなど）を対象にしています。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：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署名を確認するため ADDBA 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。

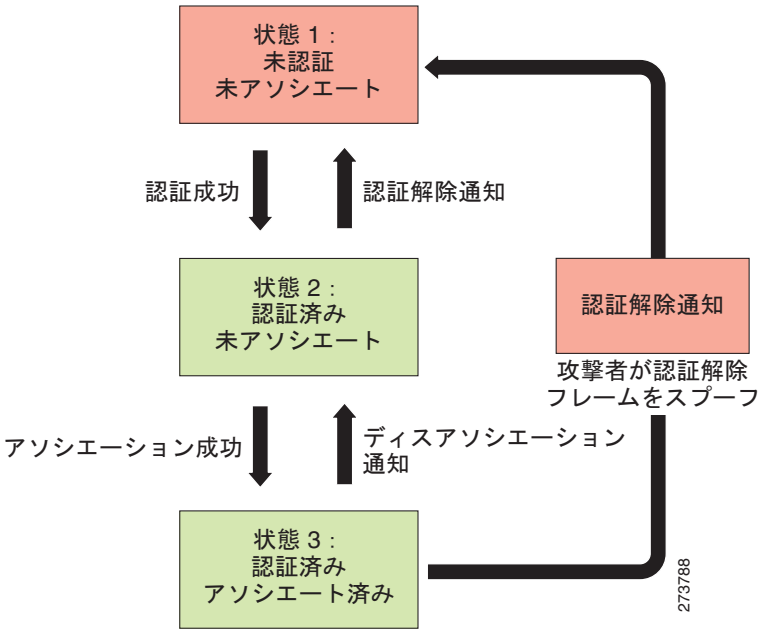
DoS 攻撃：De-Auth ブロードキャスト フラッド

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（図 A-6 を参照）。

図 A-6　認証解除ブロードキャスト攻撃



この DoS 攻撃は、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、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。

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 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。

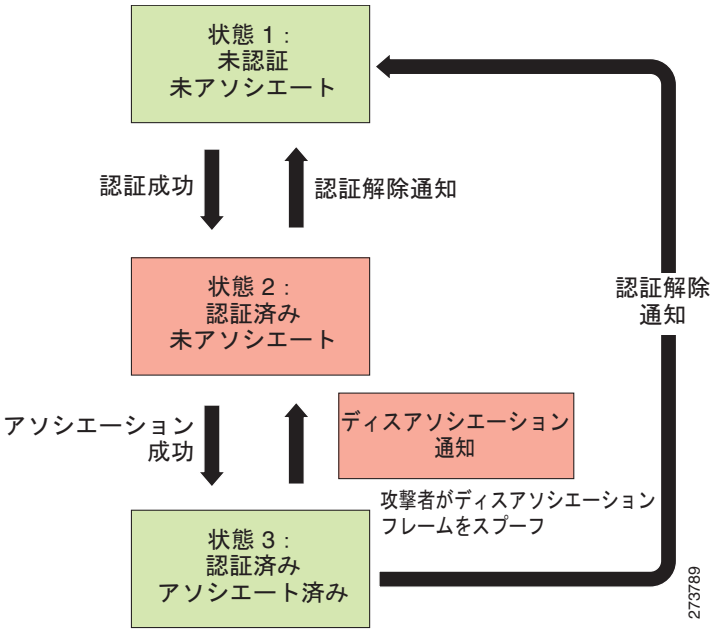
DoS 攻撃：De-Auth フラッド

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（図 A-7 を参照）。

図 A-7　認証解除フラッド攻撃



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、クライアント ステーションは攻撃者が新たな認証解除フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。攻撃者は繰り返し認証解除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 ポイントとクライア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。

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 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。

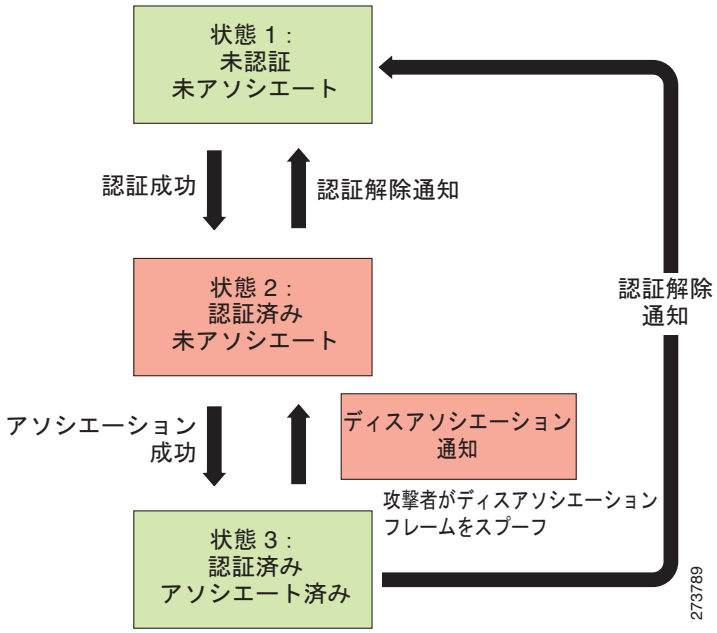
DoS 攻撃：ディスアソシエーション ブロードキャスト フラッド

攻撃ツール：ESSID Jack

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（図 A-8 を参照）。

図 A-8　ディスアソシエーション ブロードキャスト攻撃



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、クライ

アント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。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

wIPS はこの DoS 攻撃を検出するため、スプーフィングされたディスアソシエーション 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。

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 Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

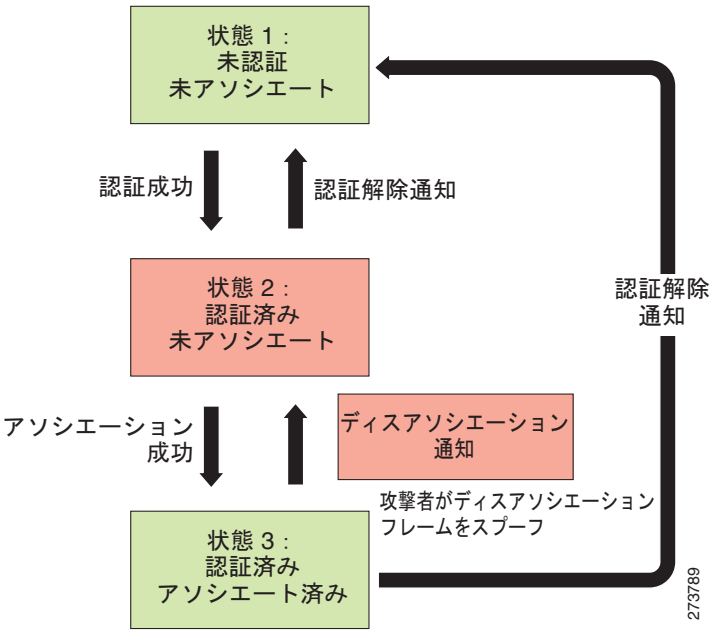
DoS 攻撃：Dis-Assoc フラッディング

攻撃ツール：ESSID Jack

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（図 A-9 を参照）。

図 A-9　ディスアソシエーション フラッド攻撃



この DoS 攻撃では、アクセス ポイントから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してアクセス ポイントを状態 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、この攻撃はこの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、クライアント ステーションは攻撃者が新たなディスアソシエーション フレームを送り付けるまで、サービスを回復するために再アソシエートと再認証を行います。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、クライアントを使用不能な状態にします。

wIPS による解決

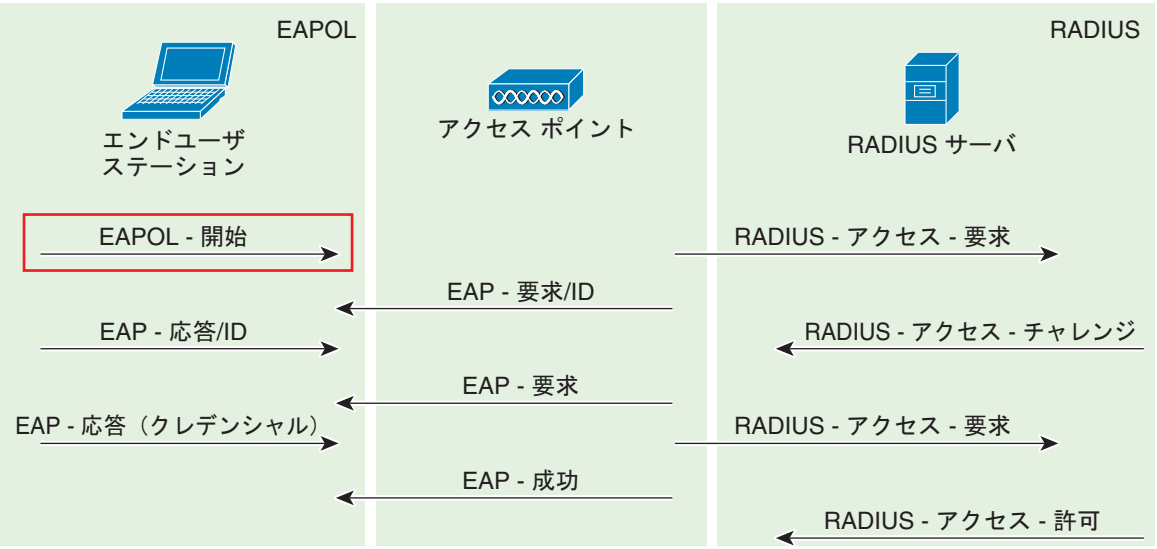
wIPS はこの DoS 攻撃を検出するため、スプーフィングされたディスアソシエーション フレームを検出し、クライアントの認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたアクセス ポイントが特定されます。WLAN セキュリティ オフィサはアクセス ポイントにログインして現在のアソシエーション テーブルのステータスを確認できます。

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 (EAP) 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（図 A-10 を参照）。

図 A-10　EAPOL-Logoff 攻撃



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。クライアントがアクセス ポイントからログオフしたことは、クライアントが WLAN 経由で通信を試行するまでは明らかではありません。通常この妨害が検出されると、クライアントはワイヤレス接続を回復するため自動的に再アソシエートと認証を行います。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

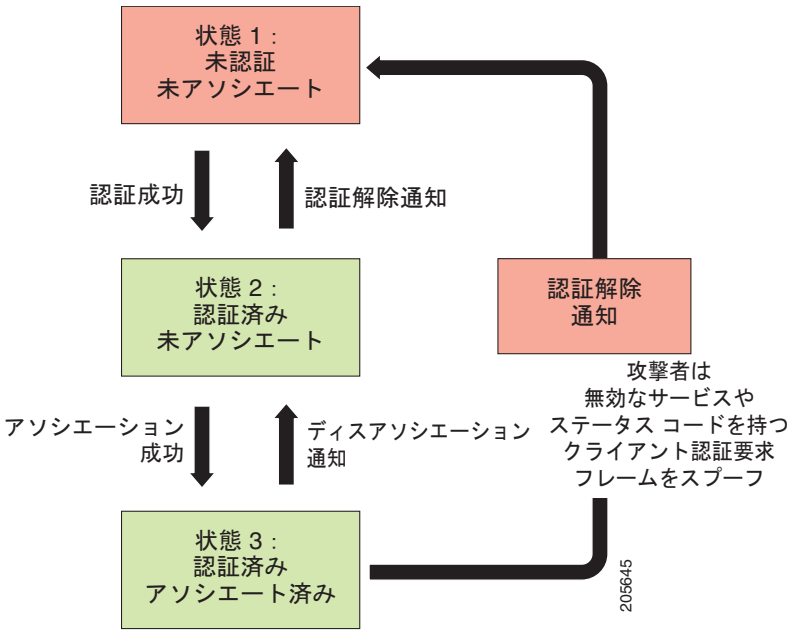
wIPS はこの DoS 攻撃を検出するため、802.1x 認証ステートとアソシエーション ステートを追跡します。アラームが生成されると、攻撃を受けたクライアントとアクセス ポイントが特定されます。WLAN セキュリティ オフィサはこのアクセス ポイントにログオンして現在のアソシエーション テーブルのステータスを確認できます。

DoS 攻撃：FATA Jack ツールの検出

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 システムと共有キーという 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（図 A-11 を参照）。

図 A-11　無効な認証要求のスプーフィング



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

wIPS は、FATA-jack の利用を検出するためスプーフィングされた 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、wIPS 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 システムと共有キーなど）を対象にしています。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。

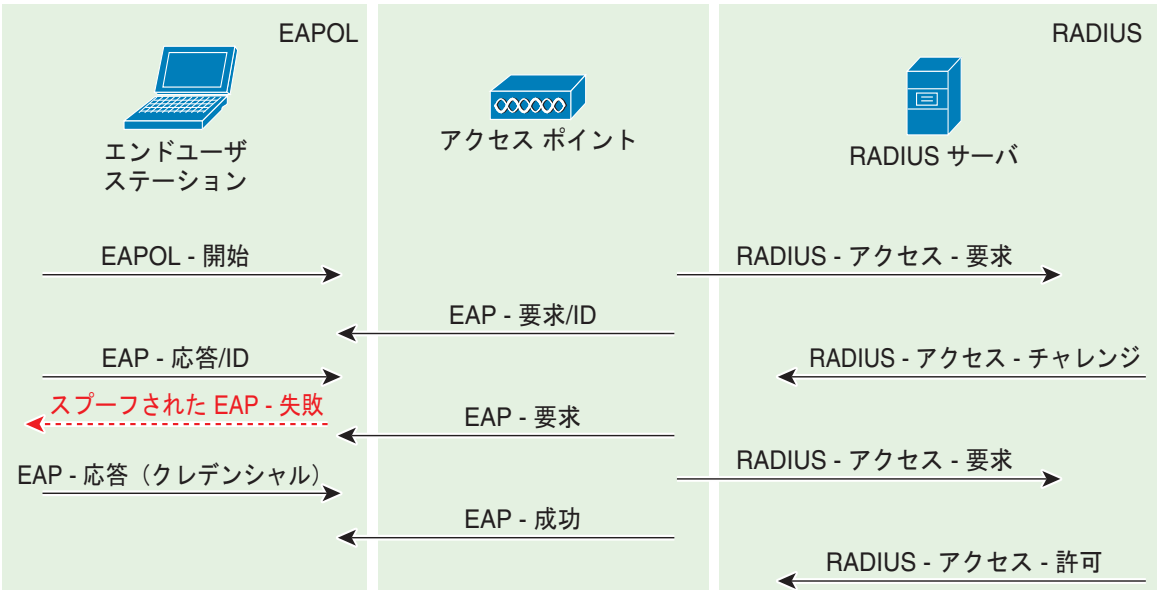
また、Cisco 管理フレーム保護は、フレームとデバイスのスプーフィングに対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

DoS 攻撃：不完全な EAP-Failure

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（図 A-12 を参照）。

図 A-12　不完全な EAP-Failure 攻撃



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ィング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。

wIPS による解決

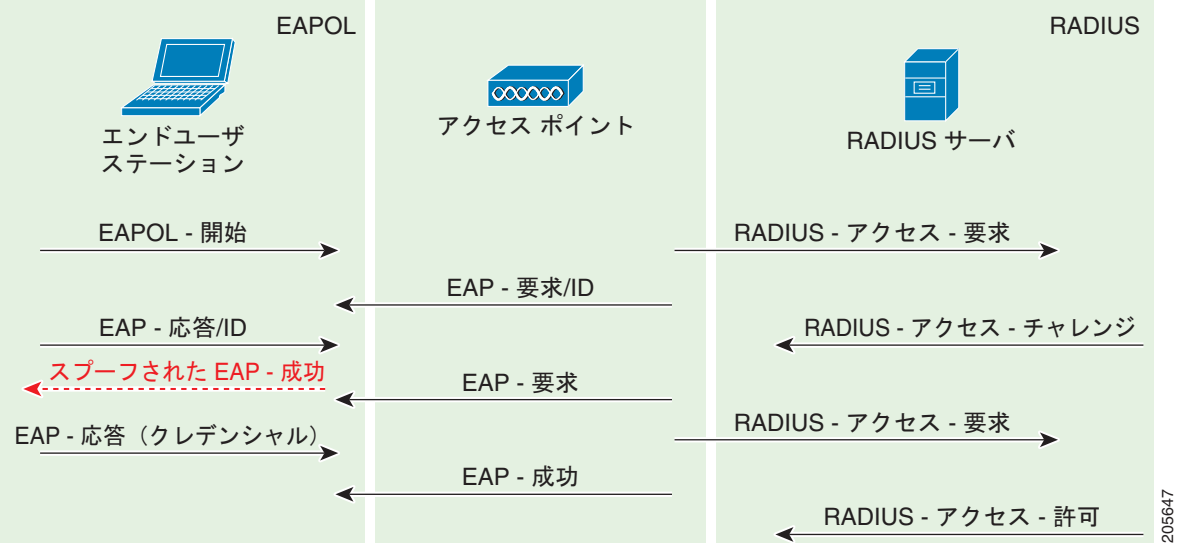
wIPS は、スプーフィングされた不完全な EAP-failure フレームと各クライアント ステーションおよびアクセス ポイントの 802.1x 認証ステートを追跡することで、この DoS 攻撃を検出します。デバイスを特定してワイヤレス環境から削除します。

DoS 攻撃：不完全な EAP-Success

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、認証が正常に完了したことを示す EAP-success フレームが送信されます（図 A-13 を参照）。

図 A-13　EAP-Success 攻撃



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 パケットを送信して相互認証プロセスを迂回する疑似アクセス 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-success フレームを継続的にスプーフして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。

wIPS による解決

wIPS は、スプーフィングされた不完全な 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。デバイスを特定してワイヤレス環境から削除します。

DoS 攻撃：プローブ応答フラッド

アラームの説明と考えられる原因

この DoS 攻撃では、攻撃者はステーションを有効な企業 AP にアソシエートできないようにします。一般的なワイヤレス トランザクションでは、ステーションは AP とアソシエーションする場合、AP のネットワークに関する情報を取得するためにプローブ要求を送信します。その後、ステーションは AP からのプローブ応答フレームを待ちます。攻撃者は、無効なプローブ応答を環境に大量に送り付けることで、このプロセスを悪用し、ステーションが有効な AP からの応答を受信できないようにできます。結果として、そのステーションはワイヤレス ネットワークに接続できなくなり、DoS 攻撃が開始されます。

wIPS による解決

wIPS サーバは、検出されたプローブ応答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。応答が有効な場合でも、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。

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
- 不良 EAP-TLS フレーム
- 「Airsnarf 攻撃」（P.A-25）
- 「ChopChop 攻撃」（P.A-27）
- 「WLAN のセキュリティ異常による Day-Zero 攻撃」（P.A-28）
- 「デバイスのセキュリティ異常による Day-Zero 攻撃」（P.A-29）
- 「AP のデバイス プローブ」（P.A-30）
- 「EAP メソッドへの辞書攻撃」（P.A-32）
- 「802.1x 認証に対する EAP 攻撃」（P.A-33）
- 「疑似 AP の検出」（P.A-34）
- 「疑似 DHCP サーバの検出（潜在的なワイヤレス フィッシング）」（P.A-34）

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（詳細については『Weaknesses in the Key Scheduling Algorithm of RC4-I』（Scott Fluhrer、Itsik Mantin、Adi Shamir 著）を参照）。

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。

Airsnarf 攻撃

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。ホットスポットは出張旅行者にとって最も重要なネットワーク アクセス サービスです。

ワイヤレス対応ラップトップや携帯機器から正規のアクセス ポイントに接続してサービスを利用できます。ほとんどのホットスポットでは、ユーザがアクセス ポイントに接続するときには、ログイン用の Web ページを開く操作以外の高度な認証メカニズムは不要です。ログインできるかどうかの条件は、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、スモール オフィス/ホーム オフィス（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などを実行します。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。

Airsnarf は、ハッカーがパブリック ワイヤレス ホットスポットからユーザ名とパスワードのクレデンシャルをどのように盗むことができるかを示すワイヤレス アクセス ポイント セットアップ ユーティリティです。

Airsnarf はシェル スクリプト ベースのツールであり、ユーザがログイン情報を入力するキャプティブ ポータルとホットスポットを作成します。ローカル ネットワーク情報、ゲートウェイ IP アドレス、SSID などの重要な値は airsnarf 設定ファイル内で設定できます。このツールは最初に、インターネットに接続されている認可済みのアクセス ポイントからホットスポット ワイヤレス クライアントをディスアソシエーションする非常に強力な信号をブロードキャストします。ワイヤレス クライアントは、何らかの不明な問題が原因でインターネットから一時的に切断されていると仮定して再度ログインしようとします。Airsnarf アクセス ポイントにアソシエートするワイヤレス クライアントが、ホットスポット オペレータにより導入された正規のアクセス ポイントではなく不正な Airsnarf アクセス ポイントから、IP アドレス、DNS アドレス、ゲートウェイ IP アドレスを受信します。Web ページからユーザ名とパスワードの入力が求められ、不正な Airsnarf アクセス ポイントによって DNS クエリが解決されます。ハッカーは入力されたユーザ名とパスワードを収集します。

そのユーザ名とパスワードは、ユーザに悪用を気づかれることなく、国内にある同じプロバイダーの他のホットスポット ロケーションで使用することができます。影響が小さくなる唯一のケースは、ホットスポット ユーザが利用時間課金制で接続している場合です。

Airsnarf ツールは、Airsnarf アクセス ポイントに知らないうちに接続しているラップトップ クライアントにも侵入する可能性があります。ハッカーは、http://airsnarf.shmoo.com/ から Airsnarf ツールをダウンロードすることができます。

wIPS による解決

wIPS 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。

ChopChop 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。詳細については、『*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。

クラックされた WEP 秘密キーでは送信データは暗号化保護されず、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あり、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）。chopchop ツールは Korek により Linux オペレーティング システム向けに開発されたツールで、WEP の脆弱性を悪用して WEP データ パケットの暗号化を解除します。ただし chopchop ツールはプレーンテキストのみを公開します。攻撃者は初期フェーズ中に以前にインジェクトされたパケットのパケット キャプチャ ファイルを使用し、改ざんしたパケットを攻撃対象ネットワークに再送信してパケットの暗号化を解除します。攻撃が完了すると、chopchop ツールは暗号化されていないパケット キャプチャ ファイルと、暗号化解除プロセスで判別された Pseudo Random Generation Algorithm（PRGA）情報を使用したもう 1 つのファイルを作成します。次に PGRA はプレーンテキストを取得するために暗号文と XOR されます。

次のコマンド例は、chopchop 攻撃を示しています。

```
aireplay-ng -4 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

値は次のとおりです。

4：chopchop 攻撃を示します

-h XX:XX:XX:XX:XX:XX：アソシエートされたクライアントの MAC アドレスを特定します

-b YY:YY:YY:YY:YY:YY：アクセス ポイントの MAC アドレスを特定します

ath0：ワイヤレス インターフェイス名を特定します

60 バイト未満のデータ パケットをドロップするアクセス ポイントは、この攻撃に対して脆弱ではありません。アクセス ポイントが 42 バイト未満のパケットをドロップする場合、aireplay はヘッダーが予測可能な限り、残りの欠落データを推測しようとします。IP パケットがキャプチャされると、ヘッダーの欠落部分を推測した後でヘッダーのチェックサムが正しいかどうかを検査します。攻撃者は 1 つ以上の WEP データ パケットを必要とします。chopchop 攻撃は動的 WEP 設定にも有効です。wIPS は、chopchop ツールを使用して潜在的な攻撃を検出できます。

wIPS による解決

wIPS は、潜在的な chopchop 攻撃が進行中の場合にアラートをアクティブにします。企業環境では WEP を使用しないでください。ネットワーク内でセキュリティ ホールが発生しないように適切な手段を講じ、よりセキュアな IEEE 802.11i 標準を使用するようにワイヤレス 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ください。

WLAN のセキュリティ異常による Day-Zero 攻撃

アラームの説明と考えられる原因

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 Unified Wireless Network に内蔵されている Radio Resource Management（RRM; 無線リソース管理）機能は、RF 環境をモニタし、この環境で検出されるパフォーマンスの問題を動的に修正します。さらなるパフォーマンス異常のモニタリングは、Wireless IPS システムを使用して行うことができます。RRM の詳細については、NCS オンライン ヘルプを参照してください。

wIPS は、WLAN を継続的にモニタし、ワイヤレス管理者に対して問題を警告する早期兆候を通知することで、WLAN のパフォーマンスと効率を維持します。パフォーマンスが低下すると生成されるパフォーマンス アラームは、次のカテゴリに分類されます。

- RF 管理：wIPS は物理 RF 環境をモニタします。この RF 環境は動的であり、WLAN パフォーマンスの問題の発生源となることがよくあります。RF 環境のモニタリング中に、サーバは以下の WLAN の基本情報を明らかにし、問題を報告します。
  - チャネルの干渉とチャネルの割り当ての問題
  - チャネル ノイズと非 802.11 信号
  - WLAN RF サービス対象エリア
  - 典型的な RF 隠れノードの問題
- 問題のあるトラフィック パターン：RF マルチパスの問題をはじめとする多くの WLAN パフォーマンスの問題は、MAC 層プロトコル トランザクションと統計に表れます。wIPS はワイヤレス トラフィックを追跡、分析することで、パフォーマンスの非効率性と低下を早期に検出できます。多くの場合、wIPS は検出されたパフォーマンスの問題の原因を判別し、対策を提案できます。wIPS は、次の項目を含む、MAC 層プロトコルの特性を追跡します。
  - フレーム CRC エラー
  - フレーム再送信
  - フレーム速度（1、2、5.5、11、... Mbps）の使用と分布
  - レイヤ 2 フレーム フラグメンテーション
  - アクセス ポイントとステーション アソシエーション、リレーションシップの再アソシエーションとディスアソシエーション
  - ローミング ハンドオフ
- チャネルまたはデバイスのオーバーロード：wIPS は、負荷をモニタおよび追跡して、チャネル帯域幅の制限と WLAN デバイスのリソース容量の両方でスムーズな運用ができるようにします。プロビジョニングの不足や過剰な増加のために、WLAN のパフォーマンスが十分でない場合、wIPS はアラームを生成して、詳細な情報を提供します。RF には、同僚が隣接チャネルに新しい WLAN デバイスを取り付けた場合でも、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。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。
- 導入および動作エラー：wIPS はエアウェーブをスキャンして、設定エラーと動作エラーを検出します。次に示す領域は継続的にモニタされます。
  - 同一 SSID を使用するアクセス ポイント間の矛盾する設定
  - ベスト プラクティスの原則に違反する設定
  - クライアントおよびアクセス ポイントの設定の不一致が原因で発生する接続の問題
  - WLAN インフラストラクチャのデバイスのダウンまたはリセット

  - WLAN デバイス実装の欠陥

- IEEE 802.11e および VoWLAN の問題：IEEE 802.11e 標準では、既存の 802.11 a/b/g ワイヤレス標準に加えて Quality of Service（QoS）機能とマルチメディア サポートが導入されました。これらの標準との完全な下位互換性を維持しながら、付加機能が追加されました。QoS 機能は、音声ビデオ アプリケーションで重要です。ワイヤレス LAN では帯域幅が制限されており、従来の有線イーサネットと比較するとオーバーヘッドが高くなっています。RTS/CTS メカニズム、パケット フラグメンテーション、パケット再送信、確認、コリジョンなど、さまざまな理由でスループットが低下します。

wIPS による解決

wIPS 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 つのパフォーマンス侵害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。パフォーマンス侵害違反によっては、詳しい分析のためにデバイスをモニタおよび特定することを推奨します。

例：

- 多数のデバイスによって「ステーションにより過負荷状態になったアクセス ポイント」アラームが生成される場合、ハッカーが数千のステーションを生成し、これらのステーションを企業アクセス ポイントに強制的にアソシエートしている可能性があります。この状況が発生すると、正規の企業クライアントがアクセス ポイントに接続できなくなります。
- ワイヤレス デバイスでフレーム再試行が過剰に行われる場合、ノイズ、干渉、パケット コリジョン、マルチパス、隠れノードの問題などが発生している可能性があります。

デバイスのセキュリティ異常による Day-Zero 攻撃

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。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。不正なアクセス ポイントの他にも、ワイヤレス ネットワークのセキュリティを侵害するワイヤレス セキュリティの脆弱性（アクセス ポイントの設定ミス、未設定のアクセス ポイントなど）があります。さまざまなソースから企業ネットワークに対して DoS（サービス拒否）攻撃が行われることもあります。

NCS は、ワイヤレス インフラストラクチャ内でセキュリティの脆弱性を自動的に評価する機能を提供します。この機能は、セキュリティの脆弱性または設定ミスを事前に報告します。さらに詳細な評価が Wireless IPS システムから無線で行われることがあります。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（静的 WEP 暗号化、VPN、Fortress、Cranite、802.11i、802.1x）：このカテゴリ（認証と暗号化）の一般的なセキュリティ違反には、設定ミス、古いソフトウェア/ファームウェア、最適ではない企業セキュリティ ポリシーの選択などがあります。
- 不正デバイス、モニタ対象デバイス、アドホック モード デバイス：企業ネットワーク（ワイヤレスおよび有線）の整合性を保護するために、不正デバイスを検出し、即時に削除する必要があります。
- 設定の脆弱性：セキュアな WLAN においては強力な導入ポリシーを実装することが重要です。ただしポリシーを適用するには、設定ミスや装置ベンダーの実装エラーにより引き起こされる違反を定期的なモニタによって捕捉する必要があります。ラップトップに Wi-Fi 機能が内蔵される傾向が

高まっていることから、WLAN 設定の複雑さは、アクセス ポイントからユーザ ラップトップに拡大しています。WLAN デバイス設定管理製品を利用すると設定プロセスが容易になりますが、内蔵 Wi-Fi 機能が未使用、未設定の状態のラップトップでは特に検証を行う必要があります。

- セキュリティ突破に関する侵入検知：このワイヤレス侵入には、WLAN 認証メカニズムの突破による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の獲得が含まれます。認証方式への辞書攻撃は、アクセス ポイントに対する非常に一般的な攻撃の 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 AP 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。
- DoS 攻撃の侵入検知：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。

wIPS による解決

wIPS 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 違反によっては、詳しい分析のためにデバイスをモニタおよび特定し、デバイスが企業ワイヤレス 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。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。

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。

AP 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

wIPS 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。

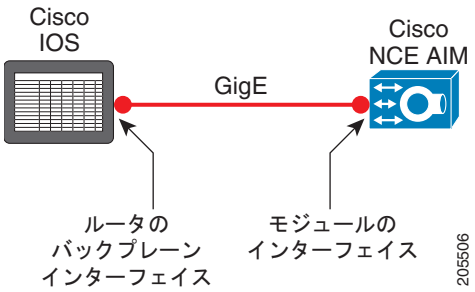
このようなデバイスは、次のいずれかの方法でセキュリティの脅威となる可能性があります。

- 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。

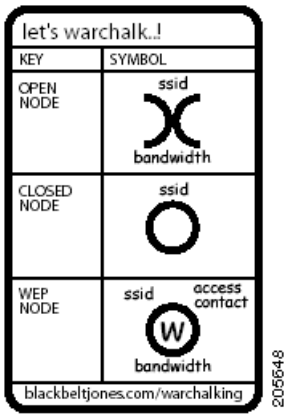
- ウォードライビング：ワイヤレス ハッカーがウォードライビング ツールを使用してアクセス ポイントを検出し、MAC アドレス、SSID、実装されているセキュリティなどの情報を、アクセス ポイントの位置情報と共にインターネット上で公開します（図 A-14 を参照）。

図 A-14　インターネットに投稿されたアクセス ポイント ロケーション



- 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用して WLAN 設定をマーキングします（図 A-15 を参照）。

図 A-15　ウォーチョーキングで使用される共通シンボル



- ウォーウォーキング：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。
- ウォーフライング：ウォーフライングは、ワイヤレス ネットワークを上空から探します。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。

危険なアソシエートを試行する正規ワイヤレス クライアント

このアラームでのもう 1 つのセキュリティの脅威は、より深刻な損害をもたらす可能性があります。これらのアラームの一部は、使用可能なアクセス ポイント（ネイバーのアクセス ポイントやより深刻な損害をもたらす不正なアクセス ポイントを含む）にアソシエートしようとしている WLAN 上の正規の認可ワイヤレス クライアントによって発生することがあります。このセキュリティの脅威は、Wi-Fi カード内蔵 Windows XP ラップトップや、Boingo または WiNc クライアント ユーティリティなどのワイヤレス接続ツールを使用するラップトップに起因することがあります。このクライアント ステーションへのアソシエートが完了すると侵入者がこのクライアント ステーションにアクセスできるようになり、これが原因で重大なセキュリティ侵害が発生する可能性があります。さらにクライアント ステーションが意図しないアクセス ポイントと企業の有線 LAN を接続するブリッジとなることがあります。一般にラップトップには Wi-Fi カードが内蔵されており、またこのようなラップトップは企業内 WLAN ネットワークに物理的に接続しています。Windows ラップトップで Windows ブリッジ サービスが有効になっている場合は有線ネットワークが外部に公開されます。セキュリティ保護のため、すべてのクライアント ステーションに固有の SSID を設定し、意図しないアクセス ポイントからのアソシエートを防止します。また、802.1x やさまざまな EAP 方式などの相互認証を検討してください。

wIPS 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。ハッカーが最新バージョンの 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、「NetStumbler の検出」アラームが生成されます。

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。NetStumbler の Web サイトでは、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ています。Windows 2000、Windows XP およびこれ以降のオペレーティング システム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小売店舗を徘徊します。

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。wIPS を使用して、ビーコンでそれぞれの SSID をブロードキャスト（アナウンス）しているアクセス ポイントを確認します。

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

EEE 802.1x は、ワイヤレス LAN および有線 LAN の認証の EAP フレームワークを規定しています。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わずかな変更（末尾の 1 桁または 2 桁の番号など）が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、無効なログインの試み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 アタック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

wIPS 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。

wIPS 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。

802.1x 認証に対する EAP 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 の認証の拡張認証プロトコル（EAP）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、EAP-FAST 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。

正規の 802.1x ユーザ ID とパスワードの組み合わせ（または有効な証明書）を使用する侵入者は、正確な EAP タイプを理解していなくても 802.1x 認証プロセスを突破できます。侵入者はさまざまな EAP（TLS、TTLS、LEAP、EAP-FAST、PEAP など）を使ってネットワークへのログオンを試みます。攻撃者がネットワークへの認証を試す EAP の種類が限られていることから、これは試行錯誤による攻撃です。

wIPS による解決

wIPS は、攻撃者がさまざまな 802.1x 認証タイプを使用してネットワークにアクセスしようとする試みを検出します。適切な手順に従ってデバイスを特定し、ワイヤレス環境から削除してください。

疑似 AP の検出

アラームの説明と考えられる原因

疑似 AP ツールは、NetStumbler、Wellenreiter、MiniStumbler、Kismet などを使うウォードライバを混乱させるおとりとして動作して WLAN を保護します。このツールは数千もの偽の 802.11b アクセス ポイントを模倣してビーコン フレームを生成します。ウォードライバは大量のアクセス ポイントを検出すると、ユーザが実際に導入している実際のアクセス ポイントを特定できません。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。WLAN 内で疑似 AP ツールを実行することは推奨しません。

wIPS による解決

管理者は疑似 AP ツールを実行するデバイスを特定してワイヤレス環境から削除する必要があります。

疑似 DHCP サーバの検出（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

ネットワーク上のデバイスへの動的 IP アドレスの割り当てにはダイナミック ホスト コンフィギュレーション プロトコル（DHCP）が使用されます。

DHCP アドレス割り当ては次のように行われます。

ステップ 1　クライアント NIC から、DHCP サーバの IP アドレスが必要であることを示す DHCP 検出パケットが送信されます。

ステップ 2　サーバは IP アドレスを含む DHCP オファー パケットを送信します。

ステップ 3　クライアント NIC が DHCP 要求を送信します。この要求は DHCP サーバに対し、サーバ オファーにより送信された IP アドレスをクライアントに割り当てることを求めます。

ステップ 4　サーバは、NIC から特定の IP アドレスに対する要求が送信されたことを確認する DHCP ACK を戻します。

ステップ 5　クライアントのインターフェイスが、DHCP サーバから最初に提供された IP アドレスを割り当てるかまたはバインドします。

DHCP サーバは専用マシンとし、企業内有線ネットワークの一部にする必要があります。また、ワイヤレス ゲートウェイおよび有線ゲートウェイにすることもできます。その他のワイヤレス デバイスでは、DHCP サービスが無害な状態で実行される場合と、WLAN IP サービスを妨害する目的で悪意を持って実行される場合があります。ワイヤレス クライアントにはサーバを認証する機能がないため、DHCP サーバの IP アドレスを要求するワイヤレス クライアントは、このような疑似 DHCP サーバに接続してこの疑似サーバの IP アドレスを取得する可能性があります。このような疑似 DHCP サーバはクライアントに対して機能しないネットワーク設定が提供するか、またはすべてのクライアント トラフィックを疑似サーバ経由にすることがあります。これで、ハッカーはクライアントから送信されるすべてのパケットを盗聴できます。ハッカーは不正な DNS サーバを利用して偽の Web ページ ログインにユーザを誘導し、ユーザ名とパスワードのクレデンシャルを取得しようとします。DoS 攻撃のために、機能しないルーティング不可能な IP アドレスを提供することもあります。通常、このような攻撃は暗号化されていない WLAN（ホットスポットやトレードショー ネットワークなど）が対象となります。

wIPS による解決

wIPS 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）ツールの検出

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。

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

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。

NCS 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、NCS 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。詳細については、『*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。

クラックされた WEP 秘密キーでは送信データは暗号化保護されず、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あり、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）。

http://www.aircrack-ng.org/doku.php?id=fragmentation&s=fragmentation によれば、aircrack プログラムはパケットからわずかな量のキー関連情報を収集し、ARP パケットまたは LLC パケット（あるいはこの両方）を判明している情報と共にアクセス ポイントに送信します。パケットがアクセス ポイントから正常にエコーバックされると、戻されるパケットからより多くのキー関連情報を取得できます。PRGA の 1500 バイト（場合によっては 1500 バイト未満）分を取得するまで、このサイクルが繰り返されます。

この攻撃では WEP キー自体は復元されず、PRGA が取得されるだけです。packetforge-ng によってさまざまなインジェクション攻撃に使用できるパケットが生成されるときにこの PRGA を使用できます。

次のコマンド例は、フラグメンテーション攻撃を示しています。

```
aireplay-ng -5 -h XX:XX:XX:XX:XX:XX -b YY:YY:YY:YY:YY:YY ath0
```

値は次のとおりです。

5：フラグメンテーション攻撃を示します

-h XX:XX:XX:XX:XX:XX：アソシエートされたクライアントの MAC アドレスを特定します

-b *YY:YY:YY:YY:YY:YY*：アクセス ポイントの MAC アドレスを特定します

ath0：ワイヤレス インターフェイス名を特定します

wIPS による解決

wIPS は、Wi-Fi ネットワークに対して進行中の潜在的なフラグメンテーション攻撃を検出します。さらに、wIPS は、企業環境では WEP を使用しないよう勧告を行います。適切な手段を講じて、ネットワーク内でのセキュリティ ホールの発生を防ぎ、よりセキュアな IEEE 802.11i 標準を使用できるようにワイヤレス 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することを促します。

HT-Intolerant Degradation of 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。

wIPS による解決

このサービスの低下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、伝送速度の低下はネットワークのパフォーマンスに悪影響を及ぼすことがあります。そのため、ユーザは 802.11n の最適な導入を維持するために、レガシー デバイスを特定して取り除く必要があります。

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は、ユーザがアクセス ポイントに接続するときには、ログイン用の Web ページを開く操作以外の高度な認証メカニズムは不要です。ログインできるかどうかの条件は、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

wIPS 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、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。

wIPS による解決

Improper Broadcast Frames アラームは、チェックしないでおくとネットワークのパフォーマンスを妨げる可能性がある潜在的な攻撃を示します。無効なフレームの発信元を特定する手順を実行し、早急にそのフレームをワイヤレス環境から削除する必要があります。

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。

不正 802.11 パケットの検出

アラームの説明と考えられる原因

不正なパケット（不正な非標準 802.11 フレーム）を使用するハッカーは、ワイヤレス デバイスを予期しない方法で動作させることができます。一部のベンダーのワイヤレス NIC のファームウェアは、不正なパケットによってクラッシュすることがあります。

このような脆弱性の例として、NULL プローブ応答フレーム（プローブ応答フレームの SSID が Null）や管理フレームの過大サイズの情報要素などがあります。このような不正なフレームがブロードキャストされると、複数のワイヤレス クライアントがクラッシュすることがあります。

wIPS による解決

wIPS は、一部の NIC のロックアップとクラッシュを引き起こす可能性がある不正なパケットを検出できます。また、攻撃を受けている間にブルー ページやロックアップの問題が発生するワイヤレス クライアントでは、WLAN NIC ドライバまたはファームウェアのアップグレードを検討する必要があります。

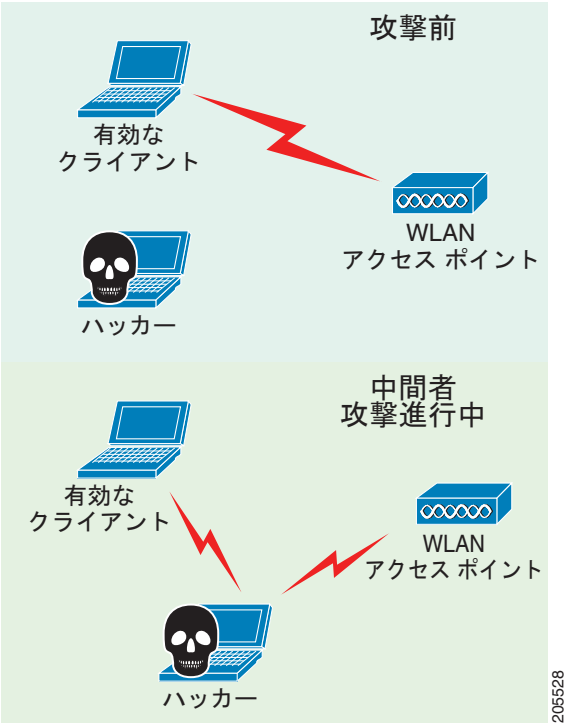
wIPS によりクライアントが特定、報告されると、WLAN 管理者はデバイス ロケータを使用してそのクライアントを見つけることができます。

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 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（図 A-16 を参照）。

図 A-16　中間者攻撃



一般的な MITM 攻撃では、ハッカーがスプーフされた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。有効なクライアントとアクセス ポイント間のトラフィックはすべてのこのハッカーのステーションを経由します。

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

wIPS 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 アドレスのスプーフを防止する方法があります。

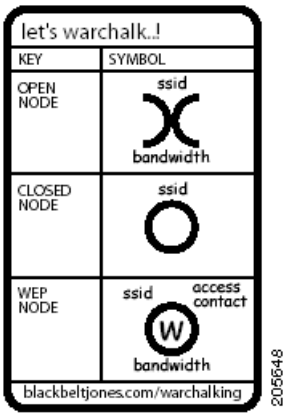
また、Cisco 管理フレーム保護（MFP）は MITM 攻撃に対して完全な予防的保護を提供します。MFP の詳細については、『*Cisco Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

NetStumbler の検出

アラームの説明と考えられる原因

wIPS 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、wIPS は *NetStumbler の検出*アラームを生成します（図 A-17 を参照）。

図 A-17　ウォーチョーキングで使用される共通シンボル



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。NetStumbler の Web サイトでは、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ています。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。

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。wIPS 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。

NCS 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、NCS オンライン ヘルプを参照してください。

NetStumbler 犠牲者の検出

アラームの説明と考えられる原因

wIPS 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、wIPS 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 の Web サイトでは、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ています。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

wIPS 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。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。wIPS 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。

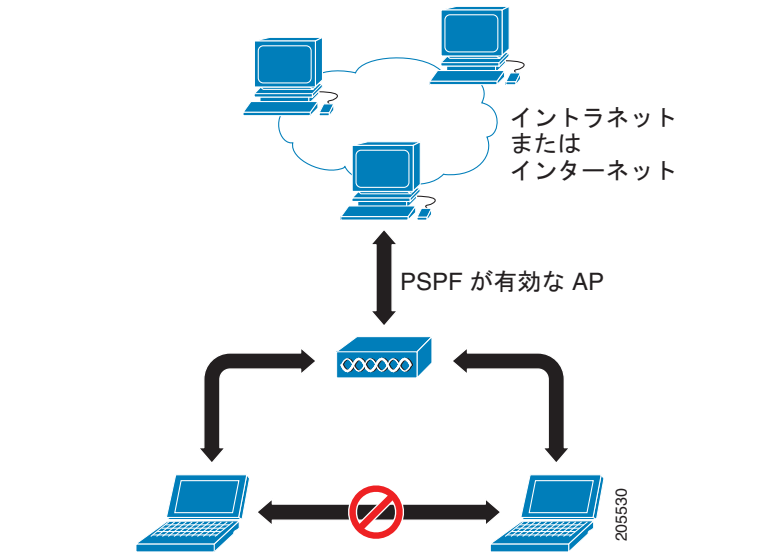
Publicly Secure Packet Forwarding（PSPF）違反の検出

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）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（図 A-18 を参照）。

図 A-18　ネットワーク上に有効になっている PSPF



wIPS による解決

wIPS 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、wIPS 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。

潜在的な ASLEAP 攻撃の検出

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す（詳細については『*Weaknesses in the Key Scheduling Algorithm of RC4-I*』（Scott Fluhrer、Itsik Mantin、Adi Shamir 著）を参照）。

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 を実行するワイヤレス 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 through 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 の特長には、次のものがあります。

- 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

wIPS は、ASLEAP ツールの認証解除シグニチャを検出します。シグニチャを検出すると、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。

NCS 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、NCS オンライン ヘルプを参照してください。

潜在的なハニーポット 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

wIPS 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。

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

ホストベースのアクセス ポイント（ワイヤレス アクセス スポットとして機能するデスクトップまたはラップトップ コンピュータ）は、企業のセキュリティに対する 2 つの脅威をもたらします。1 つ目の脅威は、ホストベース アクセス ポイントは一般に企業ワイヤレス インフラストラクチャに組み込まれておらず、企業のセキュリティ ポリシーに準拠しない不正なデバイスとなる可能性があることです。2 つ目の脅威は、ホストベースのアクセス ポイントは、ワイヤレス攻撃者によりさまざまな既知の攻撃（中間者攻撃、ハニーポット アクセス ポイント攻撃、アクセス ポイント偽装攻撃、DoS（サービス拒否）攻撃など）を実行するための便利なプラットフォームとして使用される点です。デスクトップまたはラップトップをアクセス ポイントとして設定するソフトウェア ツールはインターネットから簡単にダウンロードできるため、ホストベースのアクセス ポイントは単なる理論上の脅威の域を超えています。

一部のラップトップは、ホスト AP ソフトウェアがプリロードおよびアクティブにされた状態で出荷されます。このようなラップトップが企業ワイヤレス ネットワークに接続すると、ワイヤレス ネットワークがハッカーからの攻撃の危険性にさらされることになります。

wIPS による解決

wIPS が検出したソフト アクセス ポイントは、不正アクセス ポイントおよび侵入試行の可能性として処理する必要があります。wIPS によりソフト 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。

スプーフされた MAC アドレスの検出

スプーフィング ツールの一例：SMAC、macchanger、SirMACsAlot。

アラームの説明と考えられる原因

ワイヤレス攻撃者は、入手可能なさまざまな攻撃ツールを使ってワイヤレス ネットワークを妨害します。このようなツールの多くは、インターネットから無料でダウンロードできます。ほとんどのツールはスプーフされた MAC アドレスを利用します。スプーフされた MAC アドレスは、認可されたワイヤ

レス アクセス ポイントまたは認可されたクライアントとして動作します。攻撃者はこのようなツールを使ってさまざまな DoS（サービス拒否）攻撃を実行し、アクセス制御メカニズムを迂回し、ワイヤレス クライアントにサービスを不正にアドバタイズします。

wIPS による解決

wIPS はスプーフィングされた MAC アドレスを検出するため、IEEE 認可 OUI（ベンダー ID）と 802.11 フレーム シーケンス番号シグニチャを追跡します。

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 Wireless Control System Configuration Guide*』または NCS オンライン ヘルプを参照してください。

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 に別の営業時間を定義できます。アラームが生成されたら、管理者は疑わしいトラフィックに関与するデバイスを特定してワイヤレス環境から削除してください。

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

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は限られているため、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ション要求を拒否します。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

wIPS により、ネットワーク管理者は、ベンダー情報をポリシー プロファイルに含め、WLAN で使用中の未承認のベンダー製品であるステーションを効率的に検出できます。アラームが生成されます。

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 ポイントは一定の数のステーションにのみ対応できるため、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ション要求を拒否します。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、wIPS 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。このアラームが生成されたら、不正なデバイスまたは認可されていないデバイスを特定し、報告された問題を解決するための措置をとる必要があります。

Wellenreiter の検出

アラームの説明と考えられる原因

wIPS 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 http://wellenreiter.sourceforge.net/index.html からこの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。wIPS 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。

NCS 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、NCS オンライン ヘルプを参照してください。

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。