wIPS の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

wIPS について

Cisco 適応型ワイヤレス侵入防御システム（wIPS）は、無線の脅威の検出およびパフォーマンス管理のための高度な手法です。 この手法では、ネットワーク トラフィック分析、ネットワーク デバイス/トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。 インフラストラクチャに完全に統合されたソリューションを採用すると、有線ネットワークと無線ネットワークの両方で無線トラ

フィックを継続的に監視し、ネットワークインテリジェンスを使用してさまざまなソースからの攻撃を分析することにより、損害または漏洩が発生する前に、攻撃をより正確に特定し事前に防止することができます。

シスコの適合型 wIPS には、Cisco 3300 シリーズ Mobility Services Engine（MSE）が必要です。MSE は、Cisco Aironet アクセス ポイントの継続的な監視によって収集された情報の処理を一元化します。 シスコの適応型 wIPS の機能と、MSE への Cisco Prime Infrastructure の統合により、wIPS サービスで wIPS ポリシーとアラームの設定、監視、およびレポートを行うことができます。

（注） お使いの 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、これら 3 つのエンティティをすべて UTC タイム ゾーンに設定する必要があります。

シスコの適応型 wIPS はコントローラに設定されていません。 代わりに、プロファイル設定が Cisco Prime Infrastructure から wIPS サービスに転送され、wIPS サービスによってそのプロファイルがコントローラに転送されます。 プロファイルはコントローラのフラッシュメモリに格納され、アクセス ポイントがコントローラに join するとアクセス ポイントへ送信されます。 アクセス ポイントのアソシエートが解除され、別のコントローラへ join すると、アクセス ポイントは新しいコントローラから wIPS プロファイルを受信します。

wIPS 機能のサブセットを備えたローカル モードのアクセス ポイントは、拡張ローカル モード アクセス ポイント、または ELM AP と呼ばれます。 アクセス ポイントが次のいずれかのモードであれば、そのアクセス ポイントを wIPS モードで動作するように設定できます。

- Monitor
- Local

通常のローカル モードのアクセス ポイントは、ワイヤレス侵入防御システム（wIPS）機能のサブセットによって拡張されています。 この機能を使用すると、分離されたオーバーレイ ネットワークがなくても、アクセス ポイントを展開して保護機能を提供できます。

wIPS ELM では、オフチャネルのアラームを検出する機能が制限されます。 アクセス ポイントは定期的にオフチャネルになり、短い期間内に動作していないチャネルを監視し、そのチャネルで攻撃を検出した場合はアラームをトリガーします。 ただし、オフチャネルのアラーム検出はベスト エフォートであり、攻撃を検出してアラームをトリガーするには時間がかかることがあります。これが原因となって ELM AP が断続的にアラームを検出し、確認できないためそれをクリアする場合があります。 上記のいずれかのモードのアクセス ポイントは、ポリシー プロファイルに基づくアラームをコントローラ経由で定期的に wIPS サービスに送信できます。 wIPS サービスはアラームを格納および処理して、SNMP トラップを生成します。 Cisco Prime Infrastructure は自身の IP アドレスをトラップの宛先として設定し、SNMP トラップを MSE から受信します。

次の表に SNMP トラップ制御とそれに対応するトラップを示します。 トラップ制御が有効な場合、そのトラップ制御のトラップもすべて有効です。

（注） コントローラは SNMP トラップの送信に SNMPv2 のみを使用します。

表 *1* : ***SNMP*** トラップ制御と対応トラップ

タブ名	トラップ コントロール	トラップ
General	Link (Port) Up/Down	linkUp、linkDown
	Spanning Tree	newRoot、topologyChange、stpInstanceNewRootTrap、stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated、bsnDot11EssDeleted、bsnConfigSaved、ciscoLwappScheduledResetNotif、ciscoLwappClearResetNotif、ciscoLwappResetFailedNotif、ciscoLwappSysInvalidXmlConfig
AP	AP Register	bsnAPDisassociated、bsnAPAssociated
	Ap Interface Up/Down	bsnAPIfUp、bsnAPIfDown
Client Traps	802.11 Association	bsnDot11StationAssociate
	802.11 Disassociation	bsnDot11StationDisassociate
	802.11 Deauthentication	bsnDot11StationDeauthenticate
	802.11 Failed Authentication	bsnDot11StationAuthenticateFail
	802.11 Failed Association	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName、cldcClientIPAddress、cldcApMacAddress、cldcClientQuarantineVLAN、cldcClientAccessVLAN

タブ名	トラップ コントロール	トラップ
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts、cLWAGuestUserLoggedIn、cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding、ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained、bsnRogueApAutoContained、bsnTrustedApHasInvalidEncryption、bsnMaxRogueCountExceeded、bsnMaxRogueCountClear、bsnApMaxRogueCountExceeded、bsnApMaxRogueCountClear、bsnTrustedApHasInvalidRadioPolicy、bsnTrustedApHasInvalidSsid、bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap
Auto RF Profile Traps	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
Auto RF Update Traps	channel update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged

タブ名	トラップ コントロール	トラップ
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR、ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

次に、「*SNMP* トラップ制御とそれぞれのトラップ」の表に記載されているトラップについて説明します。

- 一般トラップ
  - [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。

    （注） SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。

  - [Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。
  - [Link (Port) Up/Down]：リンクのステータスは、アップまたはダウンから変更されます。
  - [Multiple Users]：2 人のユーザが同じ ID でログインします。
  - [Rogue AP]：不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセス ポイントが存在しなくなっている場合にこのトラップが送信されます。
  - [Config Save]：コントローラ設定が変更されると送信される通知。
- Cisco AP トラップ

- [AP Register]：アクセス ポイントがコントローラとアソシエートまたはアソシエート解除すると送信される通知です。
- [AP Interface Up/Down]：アクセス ポイント インターフェイス（802.11X）の状態がアップまたはダウンになると送信される通知です。

• クライアント関連トラップ

- [802.11 Association]：クライアントがアソシエーション フレームを送信すると送信されるアソシエーション通知。
- [802.11 Disassociation]：クライアントがディスアソシエーション フレームを送信すると送信されるディスアソシエーション通知。
- [802.11 Deauthentication]：クライアントが認証解除フレームを送信すると送信される認証解除通知。
- [802.11 Failed Authentication]：クライアントが成功以外のステータス コードの認証フレームを送信すると送信される認証エラー通知。
- [802.11 Failed Authentication]：クライアントが成功以外のステータス コードのアソシエーション フレームを送信すると送信されるアソシエーション エラー通知。
- [Exclusion]：クライアントが Exclusion Listed（blacklisted）である場合に送信されるアソシエーション失敗通知。
- [Authentication]：クライアントが正常に認証されると送信される認証通知。
- [Max Clients Limit Reached]：[Threshold] フィールドに定義されているクライアントの最大数がコントローラとアソシエートした場合に送信される通知。
- [NAC Alert]：クライアントが SNMP NAC 対応 WLAN に join する場合に送信されるアラート。

  この通知は、NAC 対応 SSID のクライアントがレイヤ 2 認証を完了し、NAC アプライアンスにクライアントのプレゼンスについて通知する場合に生成されます。 cldcClientWlanProfileName は、802.11 無線クライアントが接続されている WLAN のプロファイル名を表します。 cldcClientIPAddress は、クライアントの一意の IP アドレスを表します。 cldcApMacAddress は、クライアントがアソシエートされている AP の MAC アドレスを表します。 cldcClientQuarantineVLAN は、クライアントの隔離 VLAN を表します。 cldcClientAccessVLAN は、クライアントのアクセス VLAN を表します。
- [Association with Stats]：クライアントがコントローラとアソシエートする、またはローミングする場合に、データ統計とともに送信されるアソシエーション通知。 データの統計情報には、送受信されたパケットおよびバイトが含まれます。
- クライアントがコントローラからアソシエート解除するときに、データ統計とともに送信される Stats—Disassociate 通知を持つディスアソシエーション。 データの統計情報には、送受信されたパケットおよびバイト、SSID、およびセッション ID が含まれます。

• Security Traps

- [User Auth Failure]：このトラップは、クライアントの RADIUS 認証の失敗が発生したことを通知します。
- [RADIUS Server No Response]：このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。
- [WEP Decrypt Error]：コントローラが WEP 復号化エラーを検出すると送信される通知です。
- [Rogue AP]：不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセス ポイントが存在しなくなっている場合にこのトラップが送信されます。
- [SNMP Authentication]：SNMPv2 エンティティが、適切に認証されていないプロトコル メッセージを受信しました。

（注） SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラー メッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。

- [Multiple Users]：2 人のユーザが同じ ID でログインします。

- SNMP Authentication
  - [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Interference Profile]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- 自動 RF プロファイル トラップ
  - [Load Profile]：[Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Noise Profile]：[Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Interference Profile]：[Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Coverage Profile]：[Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- 自動 RF 更新トラップ

- [Channel Update]：アクセス ポイントの動的チャネル アルゴリズムが更新されると送信される通知。
- [Tx Power Update]：アクセス ポイントの動的送信電力アルゴリズムが更新されると送信される通知。

• Mesh Traps

- Child Excluded Parent：親メッシュ ノードを介して、コントローラに対するアソシエーションの失敗数が定義された回数に達すると送信される通知。
- 子メッシュ ノード数が検出応答タイムアウトのしきい値制限を超えると送信される通知。子メッシュ ノードが、定義された間隔で除外された親メッシュ ノードのアソシエーションを試行することはありません。 子メッシュ ノードは、ネットワークに join するときに、除外された親 MAC アドレスをコントローラに通知します。
- Parent Change：子メッシュ ノードがその親を変更すると、通知がエージェントによって送信されます。 子メッシュ ノードは以前の親を記憶し、ネットワークに再 join する際に、親の変更についてコントローラに通知します。
- Child Moved：親メッシュ ノードが子メッシュ ノードとの接続を失うと送信される通知。
- Excessive Parent Change：子メッシュ ノードが親を頻繁に変更すると送信される通知です。 各メッシュ ノードは一定期間の親の変更回数のカウントを保持します。 これが、定義されたしきい値を超えると、子メッシュ ノードはコントローラに通知します。
- Excessive Children：子の数が RAP および MAP に関して超過すると送信される通知。
- Poor SNR：子メッシュ ノードが、バックホール リンクでより低い SNR を検出すると送信される通知です。 他のトラップの場合、子メッシュ ノードが、「clMeshSNRThresholdAbate」によって定義されるオブジェクトより高い SNR をバックホール リンクで検出すると、通知をクリアするための通知が送信されます。
- Console Login：MAP コンソールでのログインが成功するか、3 回の試行の後に失敗するとエージェントによって通知が送信されます。
- Default Bridge Group Name：「デフォルト」のブリッジ グループ名を使用して MAP メッシュ ノードが親に参加すると送信される通知。

（注） 上記以外のトラップにトラップ制御機能はありません。 これらのトラップは、頻繁に生成されないので、トラップ制御は必要ありません。 コントローラによって生成されるその他のトラップをオフにすることはできません。

（注） 上記のすべてのケースで、コントローラは単なる転送デバイスとして機能します。

（注） MIB をダウンロードするには、ここをクリックしてください。

アクセス ポイントで wIPS を設定する方法

アクセス ポイントでの wIPS の設定（CLI）

手順の概要

1. **apname** *name***mode** *submode wips*
2. **end**
3. **showwirelesswpswipssummary**
4. **showwirelesswpswipsstatistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**apname** *name***mode** *submode wips* 例： `Switch# ap name ap1 mode local wips`	ローカルまたはモニタ モードに対してアクセス ポイントを設定し、wIPS にサブモードを設定します。
ステップ 2	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 3	**showwirelesswpswipssummary** 例： `Switch# show wireless wps wips summary`	アクセス ポイントで wIPS 設定を表示します。
ステップ 4	**showwirelesswpswipsstatistics** 例： `Switch# show wireless wps wips statistics`	wIPS 設定の現在のステートを表示します。

アクセス ポイントでの wIPS の設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [Access Points] > [All APs] を選択します。
[All APs] ページおよび スイッチ と関連付けられたすべてのアクセス ポイントのリストが表示されます。

ステップ 2 wIPS を設定するアクセス ポイントの名前をクリックします。
[AP] > [Edit] ページが表示されます。

ステップ 3 [General] 領域で、[AP Mode] パラメータを設定します。wIPS 用のアクセス ポイントを設定するには、[AP Mode] ドロップダウン リストから次のモードのいずれかを選択します。

- ローカル
- Monitor

ステップ 4 [AP Sub Mode] ドロップダウン リストから [wIPS] を選択して、[AP Sub Mode] を wIPS に設定します。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save（保存）] をクリックします。

wIPS 情報のモニタリング

このセクションは、wIPS の新しいコマンドについて説明します。

以下のコマンドは、アクセス ポイント上で設定された wIPS をモニタするために使用できます。

表 *2*：*wIPS* コマンドのモニタリング

コマンド	目的
show wireless wps wips summary	アクセス ポイントで wIPS 設定を表示します。
show wireless wps wips statistics	wIPS 設定の現在のステートを表示します。

例：wIPS の設定

次に、AP1 上で wIPS を設定する例を示します。

```
Switch# ap name ap1 mode local submode wips
Switch# end
Switch# show wireless wps wips summary
```

wIPS の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
wIPS コマンド	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

wIPS 設定実行の機能履歴

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。