wIPS の設定

- 機能情報の確認，1 ページ
- wIPS について，1 ページ
- アクセス ポイントで wIPS を設定する方法，9 ページ
- wIPS 情報のモニタリング，10 ページ
- 例：wIPS の設定，10 ページ
- wIPS の設定に関する追加情報，11 ページ
- wIPS 設定実行の機能履歴，12 ページ

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を使用します。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して、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 は、Cisco 3300 シリーズ Mobility Services Engine（MSE）の一部です。MSE は、Cisco Aironet AP を継続的に監視して、収集された情報を一元処理します。シスコの適応型 wIPS の機能と、Cisco MSE への Cisco Prime Infrastructure の統合により、wIPS は wIPS ポリシーとアラームを設定、監視して、脅威をレポートします。

（注） お使いの wIPS が Cisco WLC、アクセス ポイント、Cisco MSE で構成されている場合、これら 3 つのエンティティはすべて UTC タイム ゾーンに設定してください。

シスコの適応型 wIPS は Cisco WLC には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 Cisco WLC に転送されます。このプロファイルは、Cisco WLC のフラッシュ メモリに保存され、Cisco WLC に参加するときに AP に送信されます。アクセス ポイントのアソシエーションを解除して、別の Cisco WLC に参加するとき、そのアクセス ポイントは新しい Cisco WLC から新しい 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 AP を、拡張ローカル モード アクセス ポイント、または ELM AP と呼びます。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 AP を wIPS モードで動作するように設定できます。

- Monitor
- ローカル

通常のローカル モードまたはの AP は、wIPS 機能のサブセットで拡張します。この機能を使用すると、独立したオーバーレイ ネットワークがなくても、AP を展開して保護機能を提供できます。

wIPS ELM の、オフチャネル アラーム検出機能は限定的です。AP は定期的にオフチャネルになり、動作していないチャネルを短時間監視し、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。そのため ELM AP が断続的にアラームを検出しては（確認できないため）クリアする、という場合があります。上記のいずれかのモードの AP は、ポリシー プロファイルに基づくアラームを Cisco WLC 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 Cisco 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はすべて有効です。

（注） Cisco WLC が SNMP トラップの送信に使用するのは SNMPv2 のみです。

表 *1*：*SNMP* トラップ コントロールと対応トラップ

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 アソシエーション	bsnDot11StationAssociate
	802.11 ディスアソシエーション	bsnDot11StationDisassociate
	802.11 認証解除	bsnDot11StationDeauthenticate
	802.11 認証失敗	bsnDot11StationAuthenticateFail
	802.11 アソシエーション失敗	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
自動 RF プロファイル トラップ	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
自動 RF 更新トラップ	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* トラップ制御と対応トラップ」の表に記載されているトラップについて説明します。

- General 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 Cisco WLC 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 でログインしました。
  - [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]：Cisco WLC 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 Cisco WLC とアソシエートまたはディスアソシエートすると送信される通知。
- [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 Association]：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]：クライアントが除外リストに掲載（blacklisted）されてい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最大数のクライアントが Cisco WLC とアソシエートされ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 上のクライアントがその存在に関する情報を NAC アプライアンスに通知するために Layer2 認証を完了したときに生成されます。cldcClientWlanProfileName は、802.11 ワイヤレス 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 Cisco WLC とアソシエートするときや、ローミングするときに、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、送受信されたバイトとパケットが含まれます。
- [Disassociation with Stats]：クライアントが Cisco WLC からディスアソシエートするときに、データ統計とともに送信されるディス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とバイト、SSID、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]：Cisco WLC 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 Cisco WLC にアクセスを試みると、認証が失敗し、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 でログインしました。

• 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 Profie]：[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 Profie]：[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、Cisco WLC 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、ネットワークに参加するときに、除外された親 MAC アドレスを記憶しており、それを Cisco WLC 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、ネットワークに再度参加するときに、親の変更について Cisco WLC 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 ノードが Cisco WLC に通知します。
- [Excessive Children]：RAP や MAP で子の数が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が通知を送信します。
- [Default Bridge Group Name]：デフォルトのブリッジ グループ名で MAP メッシュ ノードがその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。Cisco WLC で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、Cisco WLC は純粋に転送デバイスとして機能します。

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] 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	タイトル
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	リンク
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。