



侵入検知システムの設定

- [機能情報の確認, 1 ページ](#)
- [Intrusion Detection System について, 1 ページ](#)
- [侵入検知システムを設定する方法, 2 ページ](#)
- [侵入検知システムのモニタリング, 3 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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、<TBD>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。

Intrusion Detection System について

Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/IPS) は、特定のクライアントに関わる攻撃がレイヤ 3 ~ レイヤ 7 で検出されたとき、これらのクライアントによるワイヤレスネットワークへのアクセスをブロックするよう controllers に指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウィルス、およびアプリケーションの不正使用などの脅威の検出、分類、阻止を支援することにより、強力なネットワーク保護を提供します。潜在的な攻撃を検出するには 2 つの方法があります。

- IDS センサー
- IDS シグニチャ

IDS センサーは、ネットワーク内のさまざまなタイプの IP レベルの攻撃を検出するように設定できます。センサーで攻撃が特定されたら、違反クライアントを回避 (shun) するよう controller に警告することができます。新規 IDS センサーが追加される場合、回避するクライアントのリストを取得するために controller がセンサにクエリを発行できるように、IDS センサーを controller と登録する必要があります。

IDS センサーは、疑わしいクライアントを検出すると、controller にこのクライアントを回避するよう警告します。回避エントリは、同じモビリティグループ内のすべての controllers に配信されます。回避すべきクライアントが現在、このモビリティグループ内の controller に join している場合、アンカー controller はこのクライアントを動的除外リストに追加し、外部 controller はクライアントを切り離します。次回、このクライアントが controller に接続を試みた場合、アンカー controller はハンドオフを拒否し、外部 controller にクライアントを除外することを通知します。

侵入検知システムを設定する方法

IDS センサーの設定

手順の概要

1. **configure terminal**
2. **wireless wps cids-sensor index [ip-address ip-addr username username password password_type password]**
3. **wireless wps cids-sensor index**
4. **[default exit fingerprint interval no port shutdown]**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : ControllerDevice# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless wps cids-sensor index [ip-address ip-addr username username password password_type password] 例 : ControllerDevice (config)# wireless wps cids-sensor 2 231.1.1.1 admin pwd123	内部インデックス番号を保持する IDS センサーを設定します。 index パラメータは、コントローラで IDS センサーが検索される順序を決定します。コントローラでは最大 5 つの IDS センサーをサポートします。 <ul style="list-style-type: none"> • ip-address : (任意) IDS に IP アドレスを提供します。 • username : (任意) IDS のユーザ名を設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • password : (任意) 対応するユーザ名のパスワードを設定します。
ステップ 3	wireless wps cids-sensor index 例 : ControllerDevice(config)# wireless wps cids-sensor 1	IDS コンフィギュレーション サブモードを開始します。
ステップ 4	[default exit fingerprint interval no port shutdown] 例 : ControllerDevice(config-cids-index)# default	さまざまな IDS パラメータを設定します。 <ul style="list-style-type: none"> • default : (任意) コマンドをデフォルトに設定します。 • exit : (任意) サブモードを終了します。 • fingerprint : (任意) センサーの TLS フィンガープリントを設定します。 • interval : (任意) センサーのクエリ間隔を設定します。範囲は 10 ~ 3600 秒です。 • no : (任意) コマンドを解除するか、デフォルトを設定します。 • port : (任意) センサーのポート番号を設定します。 • shutdown : (任意) 侵入検知センサーをシャットダウンします。
ステップ 5	end 例 : ControllerDevice(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。

侵入検知システムのモニタリング

表 1: ワイヤレス マルチキャストをモニタリングするためのコマンド

コマンド	説明
show wireless wps cids-sensor index	指摘されたインデックス値で IDS センサーの IDS 設定を表示します。

コマンド	説明
show wireless wps cids-sensor summary	すべての設定されたIDSのリストを、インデックス、IPアドレス、ポート番号、インターバル値、ステータスおよびクエリなどの対応する値とともに表示します。
show wireless wps shun-list	IDS回避リストを表示します。