



wIPS およびプロファイルの設定

この章では、wIPS プロファイルおよび wIPS を操作するために併せて設定する必要がある項目の設定 方法について説明します。

この章は、次の内容で構成されています。

- 「ガイドラインと制限事項」(P.8-1)
- 「前提条件」(P.8-1)
- 「wIPS 設定およびプロファイル管理について」(P.8-2)

ガイドラインと制限事項

- モビリティ サービス エンジンは 1 つの NCS からのみ設定できます。
- ご使用の 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。
- コントローラは1つの設定プロファイルに関連付けられます。そのコントローラに接続されている wIPS モード アクセス ポイントはすべて同じ wIPS 設定を共有します。

前提条件

wIPS プロファイルを設定する前に、次の手順を実行する必要があります。

- モビリティサービスエンジンをインストールします(まだネットワーク内で動作していない場合)。次の URL にある『Cisco 3350 Mobility Services Engine Getting Started Guide』または 『Cisco 3310 Mobility Services Engine Getting Started Guide』を参照してください。 http://www.cisco.com/en/US/products/ps9742/prod installation guides list.html
- 2. モビリティ サービス エンジンを NCS に追加します (まだ追加されていない場合)。
- **3.** wIPS モニタ モードで動作するようにアクセス ポイントを設定します。「wIPS モニタ モードのア クセス ポイントの設定」(P.8-2) を参照してください。
- 4. wIPS プロファイルを設定します。「wIPS プロファイルの設定」(P.8-4)を参照してください。

wIPS 設定およびプロファイル管理について

wIPS プロファイルの設定は、プロファイルの表示と変更に使用される NCS から始まるチェーン階層 を進みます。実際のプロファイルは、MSE で実行するワイヤレス IPS サービス内に保存されます。

プロファイルは、モビリティ サービス エンジン上の wIPS サービスから、特定のコントローラに伝播 され、次に、その各コントローラに関連付けられている wIPS モード アクセス ポイントに透過的にこ のプロファイルが伝達されます。(図 8-1 を参照)。





NCS で wIPS プロファイルへの設定変更が行われ、一連のモビリティ サービス エンジンおよびコント ローラに適用される場合、次のようになります。

- 1. NCS で設定プロファイルが変更され、バージョン情報が更新されます。
- 2. XML ベースのプロファイルがモビリティ サービス エンジンで実行する wIPS エンジンに適用され ます。この更新は、SOAP/XML プロトコルを介して行われます。
- モビリティ サービス エンジン上の wIPS は、NMSP を使用して設定プロファイルを適用すること によって、そのプロファイルに関連付けられている各コントローラを更新します。
- コントローラは更新された wIPS プロファイルを受け取り、それを NVRAM に保存し(以前のす べてのバージョンのプロファイルを置き換える)、CAPWAP 制御メッセージを使用して、更新さ れたプロファイルをそれに関連付けられた wIPS アクセス ポイントに伝播します。
- 5. wIPS モード アクセス ポイントはコントローラから更新されたプロファイルを受け取り、その wIPS ソフトウェア エンジンに変更を適用します。

この項では、次のトピックを扱います。

- 「ガイドラインと制限事項」(P.8-2)
- 「wIPS モニタ モードのアクセス ポイントの設定」(P.8-2)
- 「wIPS プロファイルの設定」(P.8-4)

ガイドラインと制限事項

- wIPS モニタ モードをサポートしているのは、Cisco Aironet 1130、1140、1240、1250、3502E、 および 3502I シリーズのアクセス ポイントだけです。
- wIPS サブモードがサポートされるのは、アクセスポイントモードがモニタ、ローカル、または HREAP の場合だけです。ただし、1130 および 1240 アクセスポイントの場合、wIPS はモニタ モードだけでサポートされます。

wIPS モニタ モードのアクセス ポイントの設定

wIPS モニタ モードで動作するようにアクセス ポイントを設定するには、次の手順に従います。

- **ステップ1** [Configure] > [Access Points] の順に選択します。
- **ステップ2** [802.11a] または [802.11b/g] 無線リンクをクリックします(図 8-2 を参照)。

図 8-2 [Configure] > [Access Points] > [Radio]

AP Name	Ethernet MAC	IP Address	<u>Radio</u>	Map Location	127
<u>1240-1</u>	00:1d:45:23:d5:a0	209.165.200.230	<u>802.11a</u>	Unassigned	273

ステップ 3 [Access Point] ページで、[Admin Status] チェックボックスをオフにして無線を無効にします。

図 8-3 [Access Points] > [Radio]

Α	<u>Access Point</u> > <u>1240-1</u> > '802.11a'			
G	eneral			
	AP Name	1240-1		
	AP Base Radio MAC	00:1d:46:7e:8a:60		
	Admin Status			
	Controller	209.165.200.231	8	
	Site Config ID	0	7312	

- **ステップ 4** [Save] をクリックします。

(注) wIPS モニタ モードに設定されるアクセス ポイント上の各無線について、これらの手順を繰り 返します。

- **ステップ 5** 無線が無効になると、[Configure] > [Access Points] の順に選択し、無効にした無線のアクセス ポイン トの名前をクリックします。
- **ステップ6** アクセス ポイントのダイアログボックスで、[AP Mode] ドロップダウン リストから [Monitor] を選択 します(図 8-4 を参照)。

図 8-4 [Configure] > [Access Points] > アクセス ポイントの詳細

General **		
AP Name	1240-1	
Ethernet MAC	00:1d:45:23:d5:a0	
Base Radio MAC	00:1d:46:7e:8a:60	
Country Code	US 👻	
IP Address	209.165.200.232	
Admin Status	Enabled	
AP Static IP	Enabled	
AP Mode	Monitor 👻	
Enhanced WIPS Engine	🗹 Enabled	
Monitor Mode Optimization	WIPS -	29
AP Failover Priority	Low 🔻	2731

- **ステップ 7** [Enhanced WIPS Engine] の [Enabled] チェックボックスをオンにします。
- **ステップ8** [Monitor Mode Optimization] ドロップダウン リストから [WIPS] を選択します。

- **ステップ 9** [Save] をクリックします。
- **ステップ 10** アクセス ポイントをリブートするように求められたら、[OK] をクリックします。
- **ステップ 11** アクセス ポイント無線を再度有効にするには、[Configure] > [Access Points] の順に選択します。
- **ステップ 12** 該当するアクセス ポイント無線をクリックします (図 8-5 を参照)。

```
図 8-5 [Configure] > [Access Points] > [Radio]
```

<u>AP Name</u>	Ethernet MAC	IP Address	<u>Radio</u>	Map Location	
<u>1240-1</u>	00:1d:45:23:d5:a0	209.165.200.225	<u>802.11a</u>	Unassigned	
<u>1130-1</u>	00:14:6a:1b:3b:6a	209.165.200.226	802.11a	Unassigned	130
1250-1	00:1b:d5:13:15:e2	209.165.200.227	<u>802.11b/q/n</u>	Unassigned	273

- **ステップ 13** [Radio Detail] ページで、[Admin Status] の [Enabled] チェックボックスをオンにします。
- **ステップ 14** [Save] をクリックします。

wIPS モニタ モードに設定した各アクセス ポイントおよびその各無線について、この手順を繰り返します。

wIPS プロファイルの設定

デフォルトで、モビリティ サービス エンジンと対応する wIPS アクセス ポイントは NCS からデフォル トの wIPS プロファイルを継承します。このプロファイルは、デフォルトで有効にされている大部分の 攻撃アラームによってあらかじめ調整されており、wIPS アクセス ポイントと同じ RF グループ内のア クセス ポイントに対する攻撃を監視します。このように、システムは WLAN インフラストラクチャと wIPS アクセス ポイントの両方が同じコントローラ上に混合されている統合ソリューションを利用する 構成モデルに対する攻撃を監視するようにあらかじめ設定されています。



次の設定手順の一部は*オーバーレイだけ*としてマークされており、Autonomous や完全に個別のコント ローラベースの WLAN などの既存の WLAN インフラストラクチャを監視するように適応型 wIPS ソ リューションを導入している場合にだけ実行されます。

wIPS プロファイルを設定するには、次の手順に従います。

ステップ1 [Configure] > [wIPS Profiles] を選択します。 [wIPS Profiles] ページが表示されます(図 8-6 を参照)。 図 8-6 [wIPS Profiles] > プロファイル リスト

Home Monitor • Co	System Infigure • Services • Reports • Administration •	What Demini ROOT BORMS mot + Leg Dat D+ 4
PS Profiles ID Group List	WIPS Profiles Configure > WIPS Profiles	Add Peello 🔍
	None detected	

- ステップ2 [Select a command] ドロップダウン リストから、[Add Profile] を選択し、[Go] をクリックします。
- **ステップ3** [Profile Parameters] ダイアログボックスで、[Copy From] ドロップダウンリストからプロファイル テンプレートを選択します。



E) 適応型 wIPS には一連のプロファイル テンプレートがあらかじめ定義されており、お客様はそれらをベースとして使用して、独自のカスタム プロファイルを作成できます。各プロファイルは、そのプロファイルで有効な特定のアラームと同様に、特定の業務または用途に合わせて作成されています。

31534



(注) デフォルトプロファイルは編集できません。

<u>》</u> (注)

) プロファイルをコントローラに適用するために NMSP セッションがアクティブなことを確認し ます。

- ステップ4 プロファイルを選択し、プロファイル名を入力したら、[Save and Edit] をクリックします。
- **ステップ 5** (任意) [SSID Group List] ページで SSID を設定します。

デフォルトで、ローカル ワイヤレス LAN インフラストラクチャ(同じ RF グループ名を持つ AP に よって定義された)に対して仕掛けられた攻撃が監視されます。オーバーレイ構成モデルで構成する場 合など、他のネットワークに対する攻撃を監視させる必要がある場合は、SSID グループ機能を使用す る必要があります。



(注) この手順が必要ない場合は、単に [Next] をクリックします。

a. [MyWLAN] チェックボックスをオンにし、ドロップダウン リストから [Edit Group] を選択して、 [Go] をクリックします。

- **b.** 監視する SSID を入力します。
- **c.** SSID 名を入力し(複数の名前を入力する場合は1つのスペースで区切る)、[Save] をクリックします。

SSID が正常に追加されたことを確認する [SSID Groups] ページが表示されます。

d. [Next] をクリックします。

[Select Policy] および [Policy Rules] 概要ペインが表示されます。

(注)	

[Select Policy] ペインで、検出および報告対象の攻撃を有効または無効にすることができます。 アラームのしきい値を編集し、フォレンジックを有効にすることもできます。

- **ステップ6** 検出および報告対象の攻撃を有効または無効にするには、[Select Policy] ペインでその攻撃タイプの横にあるチェックボックスをオンにします。
- **ステップ7** プロファイルを編集するには、攻撃タイプの名前(DoS:アソシエーション フラッドなど)をクリックします。

その攻撃タイプの設定ペインが、ポリシールールの説明の上の右側のペインに表示されます。

- **ステップ8** ポリシールールを変更するには、次の手順に従います。
 - **a.** [Policy Rules] ペインで、ポリシー ルールの横にあるチェックボックスをオンにし、[Edit] をクリックします。

[Policy Rule Configuration] ダイアログボックスが表示されます(図 8-7 を参照)。

図 8-7 [Policy Rule Configuration] ダイアログボックス

Policy Rule Configuration	
Severity	Critical 💌
Notification	Forensic
Number of active associations	100
Туре	○ SSID ⓒ Device Group
Device Group	Internal 💌
Save Cancel	

- **b.** アラームの重大度を選択します。
- C. このアラームのパケットをキャプチャする場合は、[Forensic] チェックボックスをオンにします。
- **d.** 必要に応じて、アクティブなアソシエーションの数を変更します。(この値はアラーム タイプに よって異なります)。
- e. 攻撃を監視する WLAN インフラストラクチャのタイプ([SSID] または [Device Group])を選択 します。
 - 1. [SSID] を選択した場合は、ステップ 9 に進みます。
 - 2. [Device Group] を選択した場合は、ステップ 10 に進みます。



E) [Device Group] ([Type]) および [Internal] はデフォルトです。Internal は、同じ RF グループ内のすべてのアクセス ポイントを示します。タイプに [SSID] を選択すると、オーバーレイ構成に一般的な個別ネットワークを監視できます。

ステップ9 (任意)オーバーレイ構成に限り、SSID のポリシー ルールを追加するには、以下の手順に従います。 a. ポリシー ルールを追加するには、[Add] をクリックします(図 8-8 を参照)。

図 8-8	ポリシー ルールの追加	
Select Policy	Policy Rules	
Security wIDS/wIPS wIPS - Denial of Service Attack vos Attack Against AP DoS Attack Against AP	flow	K

b. [Policy Rule Configuration] ダイアログボックスで、[SSID Group] リストから [MyWLAN] を選択 します(図 8-9 を参照)。

A	
(注)	タイプに SSID がすでに選択されています。

図 8-9 SSID の [Policy Rule Configuration] ダイアログボックス

Policy Rule Configuration	×
Severity	Critical
Notification	Forensic
Number of active associations	100
Туре	● SSID ^C Device Group
SSID Group	Guest Arry MywLAN Neighbor Other
Save Cancel	

- C. すべての変更が完了したら、[Save] をクリックします。
- **d.** 各ポリシー ルールを変更します。すべての変更が完了したら、ステップ 10 に進みます。(図 8-10 を参照)。



SSID によって別の WLAN インフラストラクチャを監視するようにシステムを設定する場合、監視するすべてのポリシー ルールごとに変更する必要があります。個別の各アラームに、システムで以前に作成した SSID グループに対する攻撃を監視するように定義したポリシー ルールを作成する必要があります。

elect Policy	Policy Rules
Security wIDS/wIPS	A
wIPS - Denial of Service Attack	DoS: Association flood
DoS Attack Against AP	
- DoS: Association flood	Add Edit Delete Move Up Move Down
DoS: Association table overflow	
DoS: Authentication flood	Threshold ACL/SSID Group Notification Severity
- DoS: EAPOL-Start attack 合アフー	L 100 Internal None Critical
- 🗹 DoS: PS-Poll Flood を編集	D 100 MyWLAN None Critical
DoS: Unauthenticated association	3
DoS Attack Against Infrastructure	
DoS: CTS Flood	
DoS: Queensland University of echnology Expl	Denial-of-Service Attack: Association Flood
— DoS: RF jamming attack	
DoS: RTS Flood	Alarm Description & Possible Causes
DoS: Virtual Carrier attack	A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly
DoS Attack Against Station	spoofed client associations. At the 802.11 layer, Shared-key authentication is flawed and rarely
DoS: Authentication-failure attack	used. The other alternative is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and
DoS: De-Auth broadcast attack	then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target access point's client accessible by creation many clients reaching. State 2
DoS: De-Auth flood attack	as illustrated below. Once the client association table overflows, legitimate clients are not able to
DoS: Dis-Assoc broadcast attack	get associated thus a denial-of-serve attack is committed.
DoS: Dis-Assoc flood attack	Large number of emulated client associations overflow AP's client association table
- DoS: EAPOL-Logoff attack	
DoS: FATA-Jack tool detected	State 1:
DoS: Premature EAP-Failure attack	Unauthenticated
DoS: Premature EAP-Success attack	Onassociated
wiPS - Security Penetration	

ステップ 10 [Profile Configuration] ダイアログボックスで、[Save] をクリックしてプロファイル(SSID またはデバイス グループ)を保存します。[Next] をクリックします(図 8-11 を参照)。

273143

図 8-11 [Profile Configuration] ダイアログボックス

WIPS Profiles > Profile > 'New Profile' > Profile Configuration

Save	Cancel	Back	Next	1
------	--------	------	------	---

ステップ 11 プロファイルを適用する MSE/コントローラの組み合わせを選択して、[Apply] をクリックします (図 8-12 を参照)。

図 8-12 [Apply Profile] ダイアログボックス

WIPS Profiles > Profile > 'New Profile' > Apply Profile

Apply Cancel Back	
Select MSE/Controller(s)	
MSE/Controller(s)	
WLC-1	273144