# Aironet AP での ACL フィルタの設定例

## 内容

<u>はじめに</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>設定</u> <u>ACL の作成場所</u> <u>MAC アドレス フィルタ</u> <u>IP フィルタ</u> <u>Ethertype フィルタ</u>

# はじめに

このドキュメントでは、GUI を使用して Cisco Aironet アクセス ポイント(AP)でアクセス コン トロール リスト(ACL)ベースのフィルタを設定する方法について説明します。

# 前提条件

#### 要件

次の項目に関する基本的な知識が推奨されます。

• Aironet AP および Aironet 802.11 a/b/g クライアント アダプタを使用する無線接続の設定。

ACL

使用するコンポーネント

**このドキュメントは、Cisco IOS<sup>® ソフトウェア</sup> リリース 15.2(2)JB が動作する Aironet 1040 シリーズ AP を** 使用します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在 的な影響について確実に理解しておく必要があります。

## 背景説明

AP でフィルタを使用すると、次の作業を実行できます。

- 無線 LAN(WLAN)ネットワークへのアクセス制限。
- 無線セキュリティのレイヤの追加。

以下の項目に基づいたトラフィックのフィルタリングには、さまざまなタイプのフィルタを使用 できます。

- 特定のプロトコル
- ・ クライアント デバイスの MAC アドレス
- ・ クライアント デバイスの IP アドレス

また、フィルタを有効にして、有線 LAN 上のユーザからのトラフィックを制限することもできま す。IP アドレスと MAC アドレスのフィルタによって、特定の IP アドレスや MAC アドレス間で 送受信されるユニキャストおよびマルチキャスト パケットの転送を許可または禁止できます。

プロトコル ベースのフィルタでは、さらに詳細なフィルタを行うことができ、AP のイーサネット インターフェイスと無線インターフェイスを通過する特定のプロトコルへのアクセスを制限で きます。AP 上でのフィルタの設定には、以下のいずれかの方法を使用できます。

- Web GUI
- CLI を使う場合:

このドキュメントでは、GUI でフィルタを設定するための、ACL の使用方法について説明します。

注:CLIを使用した設定の詳細については、シスコの記事「<u>アクセスポイントACLフィルタの</u> <u>設定例</u>」を参照してください。

# 設定

このセクションでは、GUI を使用して Cisco Aironet AP 上で ACL ベースのフィルタを設定する 方法について説明します。

ACL の作成場所

[Security] > [Advance Security] に移動します。[Association Access List] タブを選択し、[Define Filter] をクリックします。

cisco	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENT LOG
Security Admin Access	Hostname Autonomous
Encryption Manager SSID Manager	Security Summary Administrators
Server Manager AP Authentication	Username Read-Only
Intrusion Detection	Cisco  Service Set Identifiers (SSIDs)
Advance Security	SSID VLAN BandSelect Radio BSSID/Guest Mode
،،ا،،،ا،، cısco	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENTLOG
Security	AUTHENTICATION TIMERS
Admin Access Encryption Manager SSID Manager	Hostname Autonomous Security: Advanced Security- Association Access List
Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	Filter client association with MAC address access list: <b>Output</b> A Contract of the second

# MAC アドレス フィルタ

MAC アドレスベースのフィルタを使用すると、ハードコードされた MAC アドレスに基づくクラ イアント デバイスのフィルタリングを行うことができます。クライアントが MAC ベースのフィ ルタでアクセスを拒否されると、そのクライアントは AP と関連付けできません。MAC アドレス のフィルタによって、特定の MAC アドレスへ送受信されるユニキャストおよびマルチキャスト のパケットの転送を、許可または禁止することができます。

この例は、MAC アドレスが 0040.96a5.b5d4 のクライアントをフィルタリングするために、GUI を使用して MAC ベースのフィルタを設定する方法を説明しています。

1. MAC アドレスの ACL 700 を作成します。この ACL では、クライアント 0040.96a5.b5d4 が AP に関連付けられるのを禁止します。

ı. cısco	Saye Configuration Bing Logout Befre HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENTLOG
Security	APPLY FILTERS
Admin Access	Hostname Autonomous uptime is 4 weeks, 16 hours, 6 minutes
Encryption Manager SSID Manager	Services: Filters - MAC Address Filters
AP Authentication	Create/Edit Filter Index: < NEW > •
Local RADIUS Server Advance Security	Filter Index: 700 (700-799)
	Add MAC Address: 0040.96a5.b5d4 Mask: 0000.0000 Action: Block x Add (Hellek Johen Jacob) (Hellek Jacob) (Hellek Jacob)
	Default Action: None -
	Filters Classes:
	- Delate Class
	Apply: Delate Cancel

- 2. このフィルタをフィルタ クラスに追加するには、[Add] をクリックします。また、デフォル トのアクションを [Forward All] または [Deny All] として定義することもできます。
- 3. [APPLY] をクリックします。ACL 700 が作成されます。
- 4. ACL 700 を無線インターフェイスに適用するには、[Apply Filters] セクションに移動します 。これで、入力または出力の無線または GigabitEthernet インターフェイスに、この ACL を 適用できるようになります。

curity	APPLY FI	LTERS	MAC ADDRESS FILTERS	II IPFL	TERS II	ETHERTYPE RLTERS	
dmin Access	linetaome luteaou					Autonomous uptin	ne is 4 weeks, 16 hours, 11 minu
cryption Manager SID Manager	Services: Filters	- Apply Filters					
rver Manager		Radio	0-802.11N <sup>2.4GHz</sup>	Radi	o1-802.11N <sup>5GHz</sup>	Gig	jabitEthernet0
P Authentication trusion Detection	Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
cal RADIUS Server		EtherType	<none></none>	EtherType	< NONE > .	EtherType	< NONE > .
vance security		IP	< NONE > •	IP	< NONE > •	P	< NONE > .
	Outgoing	MAC	<none> x</none>	MAC	< NONE > x	MAC	< NONE >
		EtherType	< NONE > .	EtherType	< NONE >	EtherType	< NONE >
		IP	< NONE > *	IP	< NONE >	P	< NONE > .
	_						

#### IP フィルタ

標準または拡張 ACL を使用すると、クライアント デバイスの WLAN ネットワークへの参加を、 クライアントの IP アドレスに基づいて許可または禁止することができます。

この設定例では、拡張 ACL を使用しています。拡張 ACL では、クライアントへの Telnet アクセ スを許可する必要があります。この WLAN ネットワークでは、他のプロトコルをすべて制限する 必要があります。また、クライアントは DHCP を使用して IP アドレスを取得します。次のよう な拡張 ACL を作成する必要があります。

- DHCP と Telnet のトラフィックを許可する
- 他のすべてのタイプのトラフィックを拒否する

次の手順を実行して、拡張 ACL を作成します。

1. フィルタに名前を付け、[Default Action] ドロップダウン リストから [Block All] を選択しま す。これは、残りのトラフィックをブロックする必要があるためです。

cisco	HOME NETWORK ASSOCIATION	WIRELESS SECURITY SERVICES	SOFTWARE EVENTLOG	Salge Car	iguration ping Logous pa
Security	APPLY FILTERS	I MAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	
Admin Access Encryption Manager	Hostname Autonomous			Autonomous uptima i	s 4 weeks, 16 hours, 14 minutes
SSID Manager Server Manager AP Authentication	Create/Edit Filter Name:	< NEW > •			
Intrusion Detection Local RADIUS Server Advance Security	Filter Name: Default Action:	Allow_DHCP_Teinet			
	IP Address				
	Destination Address: Source Address:	0.0.0.0	Masic: 0.0.0.0 Masic: 255.255.255		
				Action:	Forward  Add
	IP Protocol				
	IP Protocol:	thentication Header Protocol (51)		Action:	Forward  Add

2. [TCP Port] ドロップダウン リストから [Telnet] を選択し、[UDP Port] ドロップダウン リストから [BOOTP client & BOOTP server] を選択します。

cisco	HOME NETWORK	ASSOCIATION WIRELES	s SECURITY SERVICE	S SOFTWARE EVENTLOG	Selfe	Computition ging L	odone i Pe
Security Admin Access Encryption Manager	IP Protocol:	Authentication     Custom	Header Protocol (51) (0-255)		Action:	Forward	Add
SSID Manager Server Manager	UDP/TCP Port			-			_
AP Authentication Intrusion Detection Local RADIUS Server Advance Security	TCP Port:	Teinet (23)     Gustom	(0-66535)	a	Action:	Forward	Add
	JDP Port:	<ul> <li>Bootstrap Protocol</li> <li>Custom</li> </ul>	BOOTP) server (67) (0-65535)		Action:	Forward •	Add
	Filters Classes	E.					
	TCP part: Tell UDP part: Bos Utor part: Dos Default - Block	et (23) - Forward tstrap Pretocol (BOOTP) client Aurop Interest (IDOOTD) account All	(68) - Forward (67) - Forward		<ul> <li>Delete Class</li> </ul>		
						Apply Delete	Cance

3. [APPLY] をクリックします。これでIPフィルタAllow\_DHCP?\_Telnetが作成され、この ACLを着信または発信の無線またはGigabitEthernetインターフェイスに適用できます。

սիսիս							Say	e Configuration	Eing Logo	ut Befreuh
CISCO	HOME DELMOIDS	ASSOCIATION	WIRELESS SECURITY	SERVICES SOFTWARE	EVENTLOG					
Security	APPL	FILTERS	B WAC ADDRESS I	FILTERS 1	IP FILTERS	1: 07	HERTYPE PLTER	8		
Admin Access	Hostname Autor	IOTIOUS					Autonomous	s uptime is 4 we	eks, 16 hours, 2	5 minutes
Encryption Manager	anager									
SSID Manager	Services: Filts	ers - Apply Filters								
Server Manager			Radio0-802.11N <sup>2.4GHz</sup>		Radio1-802.11NSGHz			GigabitEther	net0	
AP Authentication Intrusion Detection	Incoming	MAC	< NONE > .	MAC	< NONE >		MAC	< NONE >	]	
Local RADIUS Server Advance Security		EtherType	< NONE >	EtherType	< NONE >		EtherType	< NONE >	]	
		IP	< NONE >	P	< NONE >	-	P	< NONE >		
	Outgoing	MAC	Allow_DHCP_Telnet	MAC	< NONE >		MAC	< NONE >	]	
	_	EtherType	< NONE > .	EtherType	< NONE > •		EtherType	< NONE > •	]	
		IP	< NONE >	Ρ	< NONE >	-	Ρ	< NONE >		
							_		_	
									Apply	Gencel

### Ethertype フィルタ

Ethertype フィルタを使用すると、Cisco Aironet AP で Internetwork Packet Exchange(IPX)ト ラフィックをブロックできます。これが役立つ一般的な状況は、大規模な企業ネットワークで時 々発生する、IPX サーバのブロードキャストがワイヤレス リンクを抑制する場合です。

IPX トラフィックをブロックするフィルタを設定して適用するには、次の手順を実行してください。

- 1. [Ethertype Filters] タブをクリックします。
- 2. [Filter Index] フィールドで、フィルタに 200 ~ 299 の範囲で番号を付けます。ユーザが割 り当てた番号でフィルタの ACL が作成されます。
- 3. [Add Ethertype] フィールドに 8137 と入力します。
- 4. [Mask] フィールドの Ethertype のマスクは、デフォルト値のままにします。
- 5. アクション メニューから [Block] を選択し、[Add] をクリックします。

uluulu cisco	HOME DETWORK ASSOCIAT	TON WIRELESS SECURITY	SERVICES SOFTWARE EVENTLOG	Sage Confi	gunetion ging Logout Befreeh
Security Admin Access Encryption Manager	APPLY FILTERS Hostname Autonomous	H MAC ADDRESS FLT	ERS IF IP FLITERS	ETHERTYPE PLITERS Autonomous uptime is	4 weeks, til hours, 35 minutes
SSID Manager Server Manager AP Authentication Intrusion Detection	Services: Filters - EtherTyp Create/Edit Filter Index:	e Filters	•		
Local RADIUS Server Advance Security	Filter Index:	200 (200	299)		
	Add EtherType:	(0-8888) 8132	Mask: 0000 (0-FFFE)	Action: Block 💌	Add
	Default Action:	None •			
	Filters Classes: EtherType: 8137 Mask: 000	0 - Block	D		
	Default - None		- Delete Class		
					Apply. Delete Cancel

6. [Filters Classes] リストから Ethertype を削除するには、その Ethertype を選択して [Delete Class] をクリックします。上記の手順を繰り返して、フィルタにタイプ 8138、00ff、00e0

を追加します。これで、入力または出力の無線または GigabitEthernet インターフェイスに、この ACL を適用できるようになります。

	APPL	Y FILTERS	WAC ADDRESS	FILTERS	IP FILTERS	ETHERTYPE FILTERS	8
Dess.	Hostname Auto	nomous				Autonomous	uptime is 4 weeks, 16 hours, 3
m Manager nøger	Services: Filt	ers - Apply Filters					
anager			Radio0.802.11N <sup>2.4GHz</sup>		Radio1-802.11NSGHz		GigabitEthernet®
Detection	Incoming	MAC	< NONE > •	MAC	< NONE > •	MAC	< NONE > •
DIUS Server		EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE > m
Jon Carry		IP	200 ·	P	< NONE >	P	< NONE >
	Outgoing	MAC	< NONE > 💌	MAC	< NONE > .	MAC	< NONE > 💌
		EtherType	< NONE >	EtherType	< NONE > .	EtherType	< NONE > .
		IP	<none></none>	P	< NONE >	P	< NONE >

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。