WLC上のACL：ルール、制限事項、および例

内容

概要

このドキュメントでは、ワイヤレス LAN コントローラ（WLC）でのアクセス コントロール リスト（ACL）について説明します。現在の制限とルールを説明し、関連の例を示します。このドキュメントは、「Wireless LAN Controller での ACL の設定例」の代わりとなるものではなく、補足情報を提供しています。

注：レイヤ2 ACLまたはレイヤ3 ACLルールの柔軟性を高めるには、コントローラに接続されたファーストホップルータにACLを設定することをお勧めします。

最も間違いが起こりやすいのは、IP パケットを許可または拒否するために ACL 行でプロトコル フィールドを IP（プロトコル = 4）に設定する場合です。このフィールドでは、TCP、User Datagram Protocol（UDP）、Internet Control Message Protocol（ICMP）など、IP パケット内にカプセル化された内容が実際には選択されるため、IP-in-IP パケットをブロックまたは許可するように変換されます。モバイル IP パケットをブロックしない場合、ACL 行で IP を 選択しないでください。Cisco Bug ID CSCsh22975（登録ユーザ専用）で IP が IP-in-IP に変更されます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- WLC と Lightweight アクセス ポイント（LAP）の基本動作の設定方法に関する知識

- Lightweight アクセス ポイント プロトコル（LWAPP）とワイヤレスのセキュリティ方式に関する基本的な知識

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

WLC の ACL の理解

ACL は、1 行以上の ACL 行で構成され、ACL の終わりには暗黙の「deny any any」が続きます。各行には次のフィールドがあります。

- シーケンス番号
- 方向
- 送信元 IP アドレスとマスク
- 宛先の IP アドレスとマスク
- プロトコル
- 送信元ポート
- 宛先ポート
- DSCP
- アクション

このドキュメントでは、これらの各フィールドについて説明します。

- **シーケンス番号：ACL 行がパケットに対して処理される順序を示します。**パケットは、 初めて ACL 行に一致するまで ACL に対して処理されます。また、ACL の作成後でも ACL の任意の場所に ACL 行を挿入できます。たとえば、シーケンス番号 1 の ACL 行がある場合、その行の前に新しい ACL 行を挿入するには、新しい ACL 行にシーケンス番号 1 を付けます。これにより、ACL 内の現在の行が自動的に下に移動します。
- **方向：ACL 行を適用する方向をコントローラに通知します。**方向は、インバウンド、アウトバウンド、およびAnyの3つです。これらの方向はワイヤレス クライアントではなく、WLC に相対的な位置から取得されます。Inbound：ワイヤレス クライアントから送信された IP パケットが検査され、ACL 行に一致するかどうか確認されます。Outbound：ワイヤレス クライアント宛ての IP パケットが検査され、ACL 行に一致するかどうか確認されます。Any：ワイヤレス クライアントに対して送受信される IP パケットが検査され、ACL 行に一致するかどうか確認されます。ACL 行は、Inbound と Outbound 両方向に適用されます。**注：**方向に[Any]を選択した場合に使用する必要があるアドレスとマスクは、0.0.0.0/0.0.0.0(Any)だけです。リターン トラフィックを許可するために交換されたアドレスまたはサブネットには新しい行が必要になるため、「Any」方向では特定のホストまたはサブネットを指定しないでください。Any 方向は、ワイヤレス クライアントを宛先とする方向（Outbound）およびワイヤレス クライアントを発信元とする方向（Inbound）の両方向で、特定の IP プロトコルやポートを拒否または許可する特定の状況でのみ使用する必要があります。IP アドレスまたはサブネットを指定する場合は、方向を Inbound または Outbound として指定し、逆方向のリター

ン トラフィック用に 2 つ目の新しい ACL 行を作成する必要があります。ACL がインターフェイスに適用されていて、ACL 経由でそのリターン トラフィックを特に許可していない場合、ACL リストの終わりにある暗黙の「deny any any」によって拒否されます。

- **送信元 IP アドレスおよびマスク：単一のホストから複数のサブネットへの送信元 IP アドレスを定義します。これは、マスクによって異なります。**マスクは、IP アドレスをパケット内の IP アドレスと比較するときにどのビットを無視すべきかを判断するために、IP アドレスとともに使用されます。**注：**WLC **ACL**のマスクは、Cisco IOS® ACLで使用されるワイルドカードや逆マスクとは異なります。コントローラの ACL では、255 は IP アドレスのオクテットと完全に一致することを意味し、0 はワイルドカードを意味します。アドレスとマスクはビット単位で組み合わされます。マスク ビット 1 は、対応するビット値を確認することを示します。マスクの 255 の指定は、検査するパケットの IP アドレスのオクテットが ACL アドレスの対応するオクテットと正確に一致する必要があることを意味します。マスク ビット 0 は、その対応するビット値をチェックしない（無視する）ことを示します。マスクの 0 の指定は、検査するパケットの IP アドレスのオクテットが無視されることを示します。0.0.0.0/0.0.0.0 は「Any」IP アドレス（0.0.0.0 のアドレスと 0.0.0.0 のマスク）と同じです。
- **宛先 IP アドレスとマスク：送信元 IP アドレスおよびマスクと同じマスク ルールに従います。**
- **プロトコル：IP パケット ヘッダーのプロトコル フィールドを指定します。**プロトコル番号の一部は、ユーザが使用しやすいように変換され、プルダウン メニューで定義されています。次のようなさまざまな値があります。Any（すべてのプロトコル番号が一致）TCP（IP プロトコル 6）UDP（IP プロトコル 17）ICMP（IP プロトコル 1）ESP（IP プロトコル 50）AH（IP プロトコル 51）GRE（IP プロトコル 47）IP（IP プロトコル 4 IP-in-IP（CSCsh22975））Eth Over IP（IP プロトコル 97）OSPF（IP プロトコル 89）その他（具体的にご記入ください）Any 値は、パケットの IP ヘッダーのどのプロトコルとも一致します。これは、特定のサブネットに対して送受信する IP パケットを完全にブロックまたは許可するために使用されます。IP-in-IP パケットと一致する IP を選択します。通常は、特定の送信元ポートと宛先ポートを設定できる UDP と TCP が選択されます。[Other]を選択すると、IANAで定義されている任意のIPパケットプロトコル番号を指定できます。
- **送信元ポート：TCP と UDP プロトコルの場合のみ指定できます。**0 ~ 65535 は Any ポートと同等です。
- **宛先ポート：TCP および UDPプロトコルの場合のみ指定できます。**0 ~ 65535 は Any ポートと同等です。
- **DiffServ コード ポイント（DSCP）：IP パケット ヘッダーで一致する特定の DSCP 値を指定できます。**プルダウン メニューの選択項目は specific または Any です。specific を設定する場合は、DSCP フィールドで値を指定します。たとえば、0 ~ 63 の値を使用できます。
- **アクション：deny（拒否）または permit（許可）の 2 つのアクションです。**deny では指定されたパケットがブロックされます。permit ではパケットが転送されます。

ACL ルールと制限事項

WLC ベースの ACL に関する制限事項

WLC ベースの ACL には次の制限があります。

- パケットに一致した ACL 行は確認できません（Cisco Bug ID CSCse36574 を参照（登録ユーザのみ））。
- 特定の ACL 行と一致するパケットをログに記録できません（Cisco Bug ID CSCse36574 を

参照（登録ユーザのみ））。

- IP パケット（IP と一致するイーサネット プロトコル フィールド [0x0800] を含むパケット）は ACL で検査される唯一のパケットです。イーサネット パケットの他のタイプは ACL でブロックできません。たとえば、ARP パケット（イーサネット プロトコル 0x0806）は ACL でブロックまたは許可できません。
- コントローラには最大64個のACLを設定でき、各ACLには最大64個の回線を設定できます。
- ACL は、アクセス ポイント（AP）とワイヤレス クライアントに転送されるマルチキャストおよびブロードキャスト トラフィックに影響を与えません（Cisco Bug ID CSCse65613 を参照（登録ユーザのみ））。
- WLC バージョン 4.0 よりも前のバージョンでは、管理インターフェイスでは ACL をバイパスするため、管理インターフェイス宛てのトラフィックに影響を与えることはできません。WLC バージョン 4.0 以降では、CPU ACL を作成できます。このタイプの ACL の設定方法の詳細については、「CPU ACL の設定」を参照してください。**注：管理イン**ターフェイスとAPマネージャインターフェイスに適用されたACLは無視されます。WLC での ACL は、有線ネットワークと WLC ではなく、ワイヤレス ネットワークと有線ネットワーク間のトラフィックをブロックする設計になっています。したがって、特定のサブネットの AP が WLC 全体と通信するのを回避する場合は、一時的にスイッチやルータにアクセス リストを適用する必要があります。これにより、これらの AP（VLAN）から WLC への LWAPP トラフィックはブロックされます。
- ACL はプロセッサ依存であるため、負荷の重いコントローラのパフォーマンスに影響する可能性があります。
- ACL は仮想 IP アドレス（1.1.1.1）へのアクセスをブロックすることはできません。したがって、DHCP はワイヤレス クライアントに対してブロックできません。
- ACL は WLC のサービス ポートには影響しません。

WLC ベースの ACL に関するルール

WLC ベースの ACL には次のルールがあります。

- ACL 行では IP ヘッダー（UDP、TCP、ICMP など）でのみプロトコル番号を指定できます。それは、ACL が IP パケットのみに制限されているためです。IP を選択すると、IP-in-IP パケットを許可または拒否することを示します。Any を選択すると、任意の IP プロトコルを使用するパケットを許可または拒否することを示します。
- 方向に Any を選択する場合は、送信元と宛先を Any（0.0.0.0/0.0.0.0）にする必要があります。
- 送信元または宛先 IP アドレスが Any でない場合、フィルタの方向を指定する必要があります。また、リターン トラフィックの場合は反対方向の逆ステートメント（送信元 IP アドレス/ポートと宛先 IP アドレス/ポートが入れ替わった）を作成する必要があります。
- すべての ACL の最後には、暗黙の「deny any any」があります。パケットが ACL のどの行とも一致しない場合、コントローラによってドロップされます。

設定

DHCP、PING、HTTP、および DNS を使用する ACL の例

この設定例では、クライアントは以下のみ実行できます。

- DHCP アドレスの受信（DHCP は ACL によってブロックできません）
- ping の実行と ping の応答（任意の ICMP メッセージ タイプ：ping のみに制限できません）
- HTTP 接続の確立（Outbound）
- ドメイン ネーム システム（DNS）解決（Outbound）

これらのセキュリティ要件を設定するには、ACL に次を許可する行が必要です。

- いずれかの方向のすべての ICMP メッセージ（ping のみに制限できません）。
- UDP ポートから DNS へのすべての着信
- DNS から UDP ポートへすべての発信（リターン トラフィック）
- TCP ポートから HTTP へのすべての着信
- HTTP から TCP ポートへのすべての発信（リターン トラフィック）

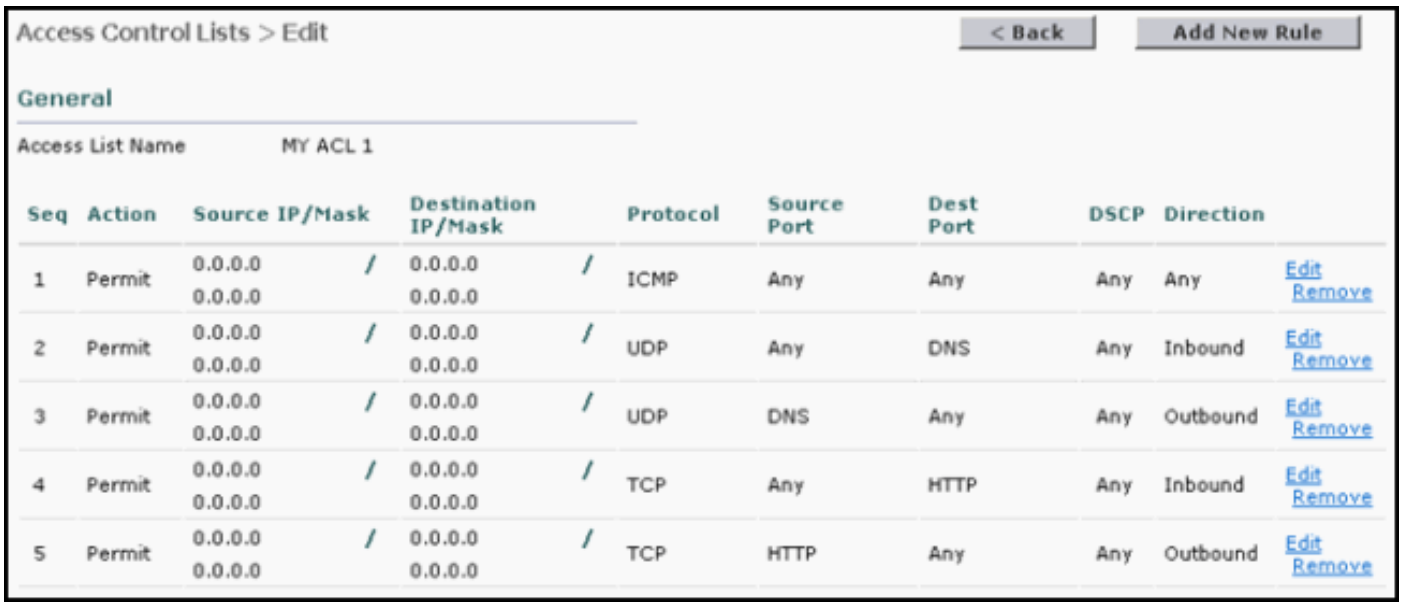
show acl detailed "MY ACL 1"（引用符は、ACL 名が 1 文字を超える場合にのみ必要）コマンド出力の ACL は次のようになります。

```
Seq  Direction  Source IP/Mask    Dest IP/Mask      Protocol  Src Port  Dest Port  DSCP  Action
---  ---------  ---------------   ---------------   --------  --------  ---------  ----  ------
1       Any     0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0       1     0-65535   0-65535     Any  Permit
2       In      0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0      17     0-65535   53-53       Any  Permit
3       Out     0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0      17     53-53     0-65535     Any  Permit
```

DNS および HTTP ACL 行の Any IP アドレスの代わりに、ワイヤレス クライアントが存在するサブネットを指定すると、ACL はより限定的になります。

注：クライアントは最初に0.0.0.0を使用してIPアドレスを受信し、サブネットアドレスを使用してIPアドレスを更新するため、DHCP ACL行はサブネット制限できません。

GUI では同じ ACL が次のように表示されます。



DHCP、PING、HTTP、および SCCP を使用する ACL の例

この設定例では、7920 IP フォンは次のみを実行できます。

- DHCP アドレスの受信（ACL によってブロックできません）
- ping の実行と ping の応答（任意の ICMP メッセージ タイプ：ping のみに制限できません）
- DNS 解決の許可（Inbound）

- IP フォンから CallManager への接続とその逆（Any 方向）
- IP フォンからTFTP サーバへの接続（CallManager は UDP ポート 69 への初期の TFTP 接続後にダイナミック ポートを使用します）（Outbound）
- 7920 IP フォンから IP フォンへの通信の許可（Any 方向）
- IP フォンの Web または Phone Directory の拒否（Outbound）。これは、ACL の最後にある暗黙の「deny any any」ACL 行で実行されます。これによって IP フォン間の音声通信、および IP フォンと CallManager間の通常の起動操作が可能になります。

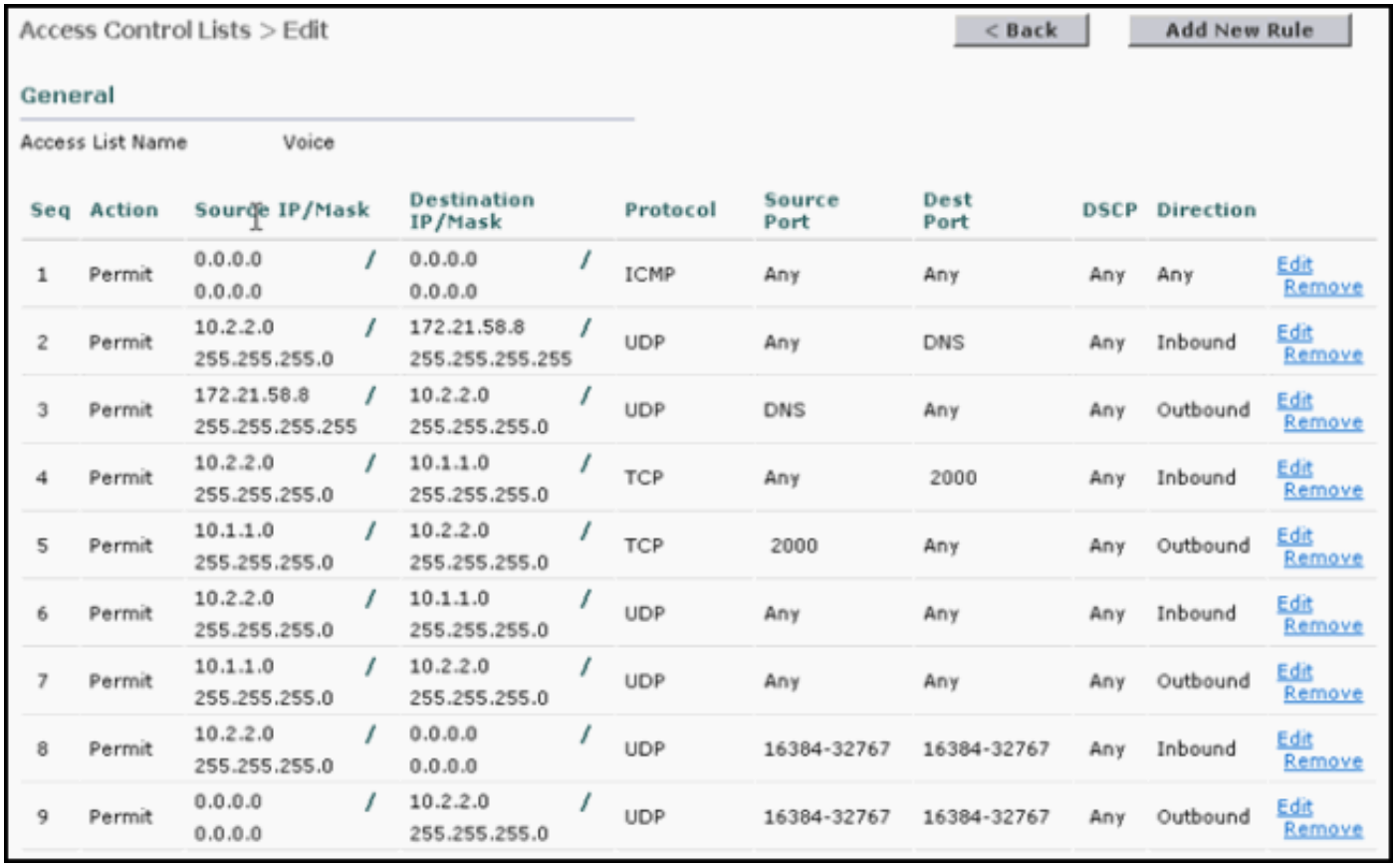
これらのセキュリティ要件を設定するには、ACL に次を許可する行が必要です。

- すべての ICMP メッセージ（ping のみに制限できません）（Any 方向）
- IP フォンから DNS サーバ（UDP ポート 53）（Inbound）
- DNS サーバから IP フォン（UDPポート 53）（Outbound）
- IP フォンの TCP ポートから CallManager の TCP ポート 2000（デフォルト ポート）（Inbound）
- CallManager の TCP ポート 2000 から IP フォン（Outbound）
- IP フォンの UDP ポートから TFTP サーバ。CallManager はデータ転送の最初の接続要求後にダイナミック ポートを使用するため、これは標準の TFTP ポート（69）に制限できません。
- IP フォン間の音声トラフィック RTP 用の UDP ポート（UDP ポート 16384 ~ 32767）（Any 方向）

この例では、7920 IP フォンのサブネットは 10.2.2.0/24 で、CallManager のサブネットは 10.1.1.0/24 です。DNS サーバは 172.21.58.8 です。以下は、**show acl detail Voice コマンドの出力です。**

```
Seq Direction Source IP/Mask          Dest IP/Mask            Protocol Src Port  Dest Port  DSCP
Action
--- --------- ---------------         ---------------         -------- --------  ---------  ----
------
1     Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0            1     0-65535   0-65535    Any
Permit
2     In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53      Any
Permit
3     Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535    Any
Permit
4     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     6     0-65535   2000-2000  Any
Permit
5     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     6     2000-2000 0-65535    Any
Permit
6     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
7     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
8     In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0            17 16384-32767 16384-32767 Any
Permit
9     Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0     17 16384-32767 16384-32767 Any
Permit
```

GUI では次のように表示されます。



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name Voice

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound	Edit Remove
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound	Edit Remove
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound	Edit Remove
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound	Edit Remove
8	Permit	10.2.2.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	16384-32767	16384-32767	Any	Inbound	Edit Remove
9	Permit	0.0.0.0 / 0.0.0.0	10.2.2.0 / 255.255.255.0	UDP	16384-32767	16384-32767	Any	Outbound	Edit Remove

付録：7920 IP Phoneポート

ここでは、7920 IP フォンが Cisco CallManager（CCM）や他の IP フォンとの通信に使用するポートの概要を示します。

- 電話から CCM（TFTP）（UDP ポート 69 は最初にデータ転送用にダイナミック ポート（一時的）に変更）：ファームウェアとコンフィギュレーション ファイルをダウンロードするために使用されるトリビアル ファイル転送プロトコル（TFTP）。
- 電話から CCM [Web サービス、ディレクトリ]（TCP ポート 80）：XML アプリケーション、認証、ディレクトリ、サービスなどのためのフォンの URL。これらのポートは、サービス単位で設定可能です。
- 電話から CCM（ボイス シグナリング）（TCP ポート 2000）：Skinny Client Control Protocol（SCCP）。このポートは、設定可能です。
- 電話から CCM（セキュアなボイス シグナリング）（TCP ポート 2443）：セキュアな Skinny Client Control Protocol（SCCP）。
- フォンから CAPF（証明書）（TCPポート 3804）：IP フォンへのローカルで有効な証明書（LSC）を発行するポートをリスニングする認証局プロキシ機能（CAPF）。
- 音声ベアラーとフォン間（通話）（UDPポート 16384 ~ 32768）：Real-Time Protocol（RTP）Secure Real Time Protocol（SRTP）。**注：**CCMはUDPポート24576 ~ 32768のみを使用しますが、他のデバイスは全範囲を使用できます。
- IP フォンから DNS サーバ（DNS）（UDP ポート 53）：システムが IP アドレスではなく名前を使用するように設定されている場合、IP フォンは DNS を使用して TFTPサーバ、CallManager、および Web サーバのホスト名を解決します。
- IP フォンから DHCP サーバ（DHCP）（UDP ポート 67（クライアント）および 68（サーバ））：静的に設定されていない場合、IP フォンは DHCP を使用して IP アドレスを取得します。

5.0 CallManager が通信に使用するポートは、「Cisco Unified CallManager 5.0 における TCP および UDP ポートの状況」を参照してください。ここには、7920 IP フォンとの通信に使用する特定のポートも記載されています。

4.1 CallManager が通信に使用するポートは、「Cisco Unified CallManager 4.1 における TCP および UDP ポートの状況」を参照してください。ここには、7920 IP フォンとの通信に使用する特定のポートも記載されています。

関連情報

- Wireless LAN Controller での ACL の設定例
- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0
- テクニカル サポートとドキュメント – Cisco Systems

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。