ワイヤレス ゲスト アクセス FAQ

内容

はじめに

このドキュメントでは、Cisco Unified Wireless Networkの一部であるワイヤレスゲストアクセス機能に関するよくある質問(FAQ)について説明します。

表記法の詳細については、『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。

セキュリティで保護されていないネットワーク エリアへの Ethernet over IP（EoIP）トンネルとは何ですか。

ゲスト トラフィック専用のコントローラの使用が推奨されます。このコントローラはゲスト アンカー コントローラと呼ばれます。

ゲスト アンカー コントローラは通常、非武装地帯（DMZ）と呼ばれるセキュリティで保護されていないネットワーク エリアにあります。トラフィックの発信元である他の内部 WLAN コントローラは、企業の LAN 上にあります。企業のデータ トラフィックからのゲスト トラフィックのパス分離を確実にするために、内部 WLAN コントローラとゲスト アンカー コントローラとの間に EoIP トンネルが確立されます。パス分離は、ゲスト アクセスに向けた重要なセキュリティ管理機能です。この機能は、セキュリティと Quality of Service（QoS）ポリシーを分離し、ゲスト トラフィックと企業または内部トラフィックとの間で区別されることを確実にします。

Cisco Unified Wireless Network アーキテクチャの重要な機能は、ネットワーク内の特定のゲスト アンカー コントローラに 1 つ以上のプロビジョニングされた WLAN（つまり、SSID）を静的にマップするために 1 つの EoIP トンネルを使用できることです。マッピングされたWLANとの間のすべてのトラフィックは、リモートコントローラとゲストアンカーコントローラの間に確立されたスタティックEoIPトンネルを通過します。

この方法を使用し、関連付けられたすべてのゲスト トラフィックを企業ネットワークからセキュリティで保護されていないネットワーク エリアに存在するゲスト アンカー コントローラに透過的に転送できます。

ゲスト アンカー コントローラとして導入する適切なコントローラを選択するにはどうすればよいのですか。

ゲスト アンカー コントローラの選択は、アクティブなゲスト クライアント セッションの数によって定義されているか、またはコントローラ上のアップリンク インターフェイスの容量によって定義されているか、あるいはその両方で定義されたとおりのゲスト トラフィック量に依存します。

ゲスト アンカー コントローラあたりの総スループットとクライアントの制限は次のとおりです。

- Cisco 2504ワイヤレスLANコントローラ：1 Gbpsインターフェイス X 4およびゲストクライアントX 1,000
- Cisco 5508 Wireless LAN Controller(WLC):8 Gbpsおよび7,000のゲストクライアント
- Cisco Catalyst 6500シリーズWireless Services Module(WiSM-2):20 Gbpsおよび15,000クライアント
- Cisco 8500ワイヤレスLANコントローラ(WLC):10 Gbpsおよび64,000クライアント

注:Cisco 7500 WLCは、ゲストアンカーコントローラとして設定できません。ゲストアンカー機能をサポートするWLCのリストについては、『セキュリティで保護されていないネットワークエリアでのゲストアクセスのサポートに使用できるコントローラ』を参照してください。

各コントローラのデータベースには、最大2048のゲストユーザ名とパスワードを保存できます。したがって、アクティブなゲストクレデンシャルの総数がこの数を超える場合は、複数のコントローラが必要です。また、ゲストのクレデンシャルは外部 RADIUS サーバに保存できます。

ネットワーク内のアクセス ポイントの数は、ゲスト アンカー コントローラの選択には影響しません。

ゲスト アンカー コントローラではいくつの Ethernet over IP（EoIP）トンネルを終端させることができますか。

1 つのゲスト アンカー コントローラは、内部 WLAN コントローラから最大 71 個の EoIP トンネルを終端できます。このキャパシティは WLC- 2504 を除く、Cisco ワイヤレス LAN コントローラのどのモデルで同じです。2504 コントローラは、最大 15 個の EoIP トンネルを終端できます。追加のトンネルが必要な場合は、複数のゲスト アンカー コントローラを設定できます。

EoIP トンネルは、各 EoIP でトンネリングされた WLAN や Secure Set Identifier（SSID）の数とは関係なく、WLAN コントローラごとにカウントされます。

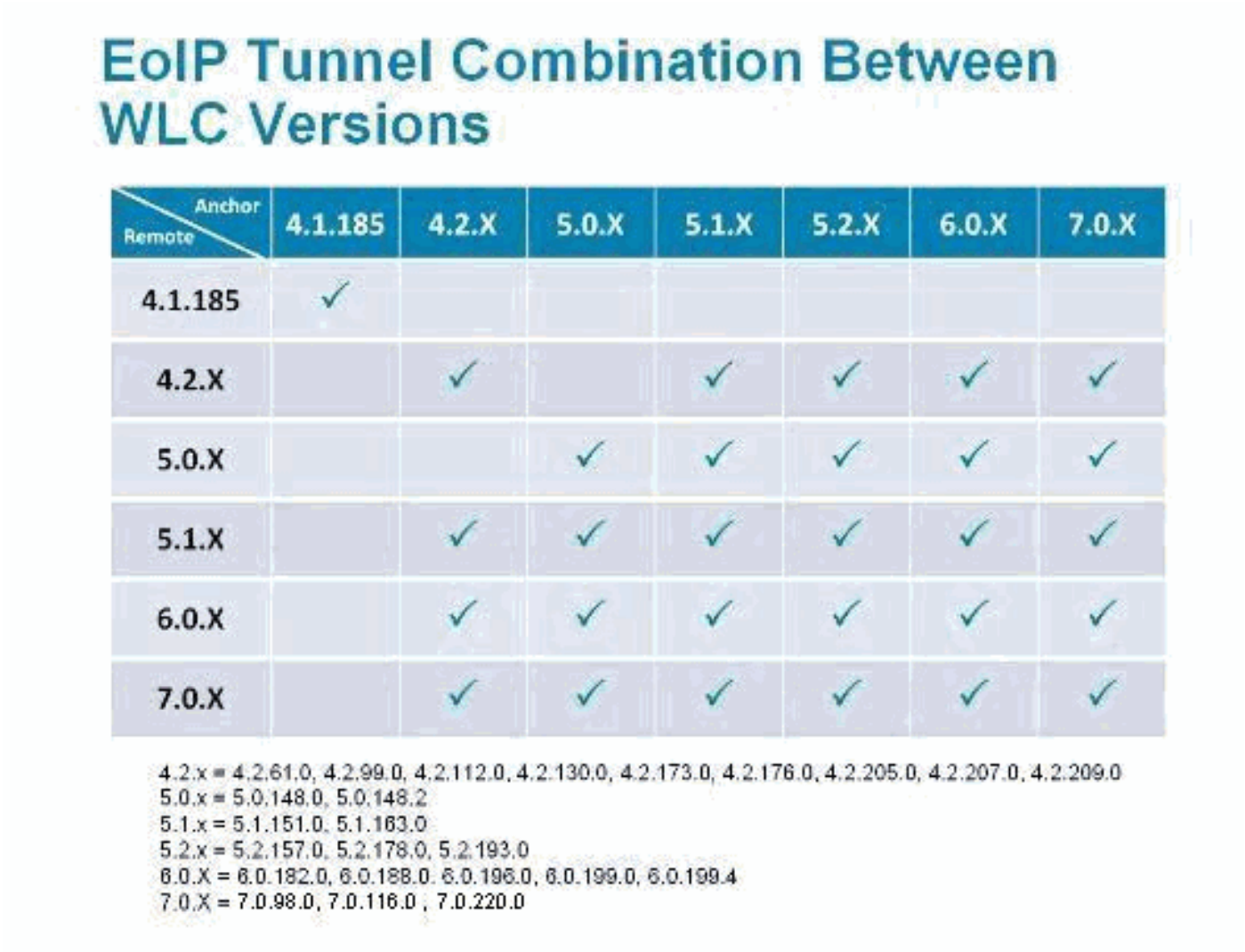
ゲスト アンカー コントローラと内部の各コントローラとの間には、ゲスト クライアントの関連付けに使用するアクセス ポイントをサポートする 1 つの EoIP トンネルが設定されます。

異なるソフトウェア バージョンを実行するコントローラ間に Ethernet over IP（EoIP）トンネルを作成できますか。

すべてのワイヤレス LAN コントローラのソフトウェア バージョンで EoIP がサポートされているわけではありません。このような場合、リモートコントローラとアンカーコントローラでは、同じバージョンのWLCソフトウェアを実行する必要があります。ただし、最新のソフトウェア バージョンではリモート コントローラとアンカー コントローラが異なるバージョンを持つことができ

ます。

次の表に、EoIP トンネルを作成できるワイヤレス LAN コントローラのソフトウェア バージョンを示します。



Cisco 2100/2500 シリーズ ワイヤレス LAN コントローラはセキュリティで保護されていないネットワーク エリアのゲスト アンカー コントローラとして使用できますか。

はい。Cisco Unified Wireless Networkソフトウェアリリース7.4以降、Cisco 2500シリーズワイヤレスLANコントローラは、ファイアウォールの外部でゲストトラフィックを（最大15のEoIPトンネルまで）終端できます。Cisco 2000 シリーズ ワイヤレス LAN コントローラは、ゲスト トンネルを開始できるだけです。

サービス統合型ルータ用の Cisco ワイヤレス LAN コントローラ モジュール（WLCM または WLCM2）はセキュリティで保護されていないネットワーク エリアのゲスト アンカー コントローラ

として使用できますか。

いいえ。WLCM または WLCM2 はゲスト トンネルを終端できません。WLCM はゲスト トンネルを開始できるだけです。

セキュリティで保護されていないネットワーク エリアのゲスト アクセスをサポートするには、どのコントローラを使用できますか。

EoIP トンネルの終端、Web 認証、およびゲスト クライアントのアクセス制御を含む、ゲスト トンネルのアンカー機能は、次のバージョン 4.0 以降のソフトウェア イメージの Cisco ワイヤレス LAN コントローラ プラットフォームでサポートされています。

- Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM2）
- Cisco WiSM-2 シリーズ ワイヤレス LAN コントローラ
- Cisco Catalyst 3750G 統合ワイヤレス LAN コントローラ
- Cisco 5508 シリーズ ワイヤレス LAN コントローラ
- Cisco 2500 シリーズ ワイヤレス LAN コントローラ（サポート導入はソフトウェア リリース 7.4）

ゲスト アンカー コントローラがファイアウォールの外側で使用される場合、正しく動作するにはどのファイアウォール ポートをゲスト アクセスに対してオープンにしますか。

ゲスト アンカー コントローラとリモート コントローラの間にあるファイアウォールで、次のポートをオープンする必要があります。

- レガシーモビリティ：ユーザデータトラフィック用IPプロトコル97、UDPポート16666
- 新しいモビリティ：UDPポート16666および16667

オプションで管理するため、次のファイアウォール ポートをオープンする必要があります。

- SSH/Telnet - TCPポート22/23
- TFTP:UDPポート69
- NTP:UDPポート123
- SNMP:UDPポート161（getおよびset）および162（トラップ）
- HTTPS/HTTP - TCPポート443/80

- Syslog:TCPポート514
- RADIUS 認証/アカウント：UDP ポート 1812 および 1813

Network Address Translation（NAT）が設定されたファイアウォールをゲスト トラフィックは通過できますか。

ファイアウォールを通過する EoIP トンネルでは、1 対 1 の NAT を使用する必要があります。

アンカーと外部 WLC のシナリオでは、どちらの WLC が RADIUS アカウンティングを送信しますか。

このシナリオでは、認証は必ずアンカー WLC で行われます。したがって、RADIUS のアカウンティングはアンカー WLC によって送信されます。

注：中央Web認証(CWA)や認可変更(CoA)の導入では、RADIUSアカウンティングをアンカーで無効にし、外部WLCでのみ使用する必要があります。

内部コントローラとアンカー コントローラの間のゲスト トンネルに障害が発生します。WLCに次のログが表示されます。

mm_listen.c:5373 MM-3-INVALID_PKT_RECVD: Received an invalid packet from 10. 40.220.18.Source member:0.0.0.0. source member unknown..これは、なぜですか。

[WLANs] ページで WLC GUI からのトンネルの状態をチェックします。WLAN の近くにあるドロップダウン ボックスをクリックし、コントロールとデータ パスの状態を含む [Mobility Anchors] を選択します。エラー メッセージが表示される原因としては、次のいずれかが考えられます。

1. アンカー コントローラと内部コントローラのコードのバージョンが異なります。これらが同じバージョンのコードを実行していることを確認します。
2. モビリティ アンカーの設定が間違っています。DMZ でモビリティ アンカーとして DMZ が設定されていることを確認し、内部 WLC にモビリティ アンカーとして DMZ WLC が設定されていることを確認します。モビリティ アンカーを設定する方法の詳細については、『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 7.0』の「自動アンカー モビリティの設定」セクションを参照してください。この結果、ゲスト ユーザはトラフィックを渡すことができなくなります。

ワイヤレス ゲスト アクセスの設定で、クライアントが DHCP サーバから IP アドレスを取得しません。「Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP dropping REPLY from

Export-Foreign STA」というエラーメッセージが内部コントローラに表示されます。これは、なぜですか。

ワイヤレス ゲスト アクセスの設定では、ゲスト アンカー コントローラと内部コントローラの DHCP プロキシ設定が一致する必要があります。そうでない場合、クライアントからの DHCP 要求がドロップされて、次のエラー メッセージが内部コントローラに表示されます。

```
Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX  DHCP dropping REPLY from Export-Foreign STA
```

WLC で DHCP プロキシ設定を変更するには、次のコマンドを使用します。

```
<#root>

(Cisco Controller) >

config dhcp proxy ?


enable          Enable DHCP processing's proxy style behaviour.
disable         Disable DHCP processing's proxy style behaviour.
```

両方のコントローラで show dhcp proxy コマンドを使用し、両方のコントローラの DHCP プロキシ設定が同じことを確認します。

```
<#root>

(Cisco Controller) >

show dhcp proxy


DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

ゲスト トラフィックがセキュリティで保護されていないネットワーク領域にトンネリングされている場合、ゲスト クライアントはどこから IP アドレスを取得しますか。

ゲスト トラフィックは、EoIP 経由のレイヤ 3 で企業内で転送されます。したがって、ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) サービスをローカルに実装できる最初のポイントはゲスト アンカー コントローラか、またはゲスト アンカー コントローラは外部サ

ーバにクライアントの DHCP 要求をリレーできます。これは、ドメイン ネーム システム（DNS）のアドレス解決が処理される方法でもあります。

Cisco ワイヤレス LAN コントローラでは、ゲスト認証用の Web ポータルがサポートされていますか。

Cisco ワイヤレス LAN コントローラ、ソフトウェア バージョン 3.2 以降では、免責事項およびアクセプタブル ユース ポリシー情報を表示する機能とともに、認証のためにゲスト クレデンシャルを取得して、簡単なブランド化機能を提供する組み込みの Web ポータルが提供されています。

Web ポータルをカスタマイズするにはどうすればよいのですか。

Web ポータルをカスタマイズする方法の詳細については、「Web 認証のログイン ページを選択する」を参照してください。

ゲストのクレデンシャルはどのように管理されるのですか。

ゲストのクレデンシャルは、Cisco Wireless Control System（WCS）バージョン 7.0 または Network Control System（NCS）ver 1.0 を使用して作成および一元的に管理できます。ネットワーク管理者はゲストのクレデンシャルを作成するために、「Lobby Ambassador」アクセスを許可する限られた特権の管理者アカウントを設定できます。WCS または NCS では、Lobby Ambassador アカウントのユーザは、ゲスト アンカー コントローラとして機能するコントローラのゲストのクレデンシャルを作成、割り当て、監視、削除することができます。

Lobby Ambassador はゲストのユーザ名（またはユーザ ID）とパスワードを入力するか、またはクレデンシャルを自動生成できます。すべてのゲストが 1 種類のユーザ名とパスワードを使用できるようにするか、または各ゲストが一意のユーザ名とパスワードを使用できるようにするグローバル設定パラメータがあります。

WCS で Lobby Ambassador アカウントを設定するには、『Cisco Wireless Control System コンフィギュレーション ガイド、リリース 7.0』の「ゲスト ユーザ アカウントの作成」セクションをを参照してください。

Cisco ワイヤレス LAN コントローラでは、Wireless Control System（WCS）や NCS に加えて Lobby Ambassador 機能を使用できますか。

はい。WCS または NCS が導入されていない場合、ネットワーク管理者はゲスト アンカー コントローラで Lobby Ambassador アカウントを作成できます。ロビーアンバサダーアカウントを使用してゲストアンカーコントローラにログインするユーザは、ゲストユーザ管理機能にのみアクセスできます。

複数のゲスト アンカー コントローラがある場合、複数のゲスト アンカー コントローラでユーザ名を同時に設定するには、WCS または NCS を使用する必要があります。

ワイヤレス LAN コントローラを使用して Lobby Ambassador アカウントを作成する方法の詳細については、『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 7.0』の「Lobby Ambassador アカウントの作成」セクションを参照してください。

外部の認証、許可、およびアカウンティング（AAA）サーバを使用してゲストを認証することはできますか。

はい。ゲストの認証要求は外部 RADIUS サーバにリレーできます。

ゲストがログインすると、何が起こりますか。

ワイヤレス ゲストが Web ポータルを介してログインすると、ゲスト アンカー コントローラは、次の手順を実行して認証を処理します。

1. ゲスト アンカー コントローラは、ユーザ名とパスワードがローカル データベースがあるかどうかをチェックし、それらがある場合はアクセスを許可します。
2. ユーザ クレデンシャルがゲスト アンカー コントローラのローカルに存在しない場合、ゲスト アンカー コントローラは外部 RADIUS サーバがゲスト WLAN に設定されているかどうかを確認するため WLAN 設定を確認します。そのように設定されている場合は、コントローラが、そのユーザ名とパスワードで RADIUS アクセス要求パケットを作成し、選択された RADIUS サーバに転送して認証します。
3. 特定の RADIUS サーバが WLAN に設定されていない場合、コントローラはグローバルの RADIUS サーバの設定をチェックします。「ネットワークユーザ」を認証するオプションが設定された外部RADIUSサーバはゲストユーザのクレデンシャルを使用して照会されます。「ネットワークユーザ」が選択されているサーバがなくステップ1または2でユーザが認証されていない場合、認証は失敗します。

ゲストのユーザ認証を省略し、Web ページの免責事項オプションだけを表示することはできますか。

はい。ワイヤレス ゲスト アクセスの別の設定オプションは、ユーザ認証をすべて省略して、オープン アクセスを可能にすることです。ただし、アクセスを許可する前に、ゲストにアクセプタブル ユース ポリシーおよび免責事項のページを表示する必要がある場合があります。これを行うには、Web ポリシーのパススルーをゲスト WLAN に設定できます。このシナリオでは、ゲスト ユーザが、免責情報を含む Web ポータル ページにリダイレクトされます。ゲスト ユーザを識別できるようにするため、パススルー モードには接続前に電子メール アドレスをユーザが入力するオプションもあります。

リモート コントローラとゲスト アンカー コントローラを同じモ

ビリティ グループにする必要がありますか。

いいえ。ゲストアンカーコントローラとリモートコントローラは、別々のモビリティグループ上に存在できます。

複数のゲスト SSID がある場合、それぞれの WLAN（SSID）を一意の Web ページ ポータルにダイレクトすることはできますか。

はい。単一または複数のいずれでも WLAN 上のすべてのゲスト トラフィックは、1 つの Web ページにリダイレクトされます。WLC バージョン 4.2 以降では、それぞれの WLAN を一意の Web ポータル ページにダイレクトすることができます。詳細については、『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 7.0』の「WLAN ごとのログイン ページ、ログイン失敗ページ、ログアウト ページの割り当て」セクションを参照してください。

WLC リリース 7.0 の新しい設定、MAC フィルタ障害時の WebAuth の機能とは何ですか。

WLAN にレイヤ 2（mac-filter）およびレイヤ 3（webauth-on-macfilter-failure）セキュリティの両方が設定されている場合、クライアントはいずれかに適合すると、RUN の状態になります。また、レイヤ 2 セキュリティ（mac-filter）で失敗すると、クライアントはレイヤ 3 セキュリティ（webauth-on-macfilter-failure）に移行します。

ブラウザでプロキシ サーバが設定されている場合、クライアントは正しく動作しますか。

リリース 7.0 より前では、クライアントはブラウザでプロキシ サーバが設定されているときは TCP 接続を確立できませんでした。リリース 7.0 以降では、WebAuth プロキシ サーバのサポートが追加され、プロキシ サーバの IP アドレスとポートをコントローラで設定できるようになりました。

ワイヤレス ゲスト アクセスの導入ガイドはありますか。

以下は、導入ガイドのリンクです。

導入ガイド：Cisco Wireless LAN Controllerを使用したシスコゲストアクセス

有線およびワイヤレス ゲスト アクセスのデザイン ガイドはありますか。

設計ガイドへのリンクは次のとおりです。

- Cisco ユニファイド ワイヤレス ゲスト アクセス サービス
- Cisco WLAN コントローラを使用した有線ゲスト アクセスの設定例

関連情報

- Cisco WLAN コントローラを使用した有線ゲスト アクセスの設定例
- 導入ガイド：Cisco Wireless LAN Controllerを使用したシスコゲストアクセスリリース4.1
- 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。