



CKIP の設定

- [CKIP について](#), 1 ページ
- [CKIP の設定 \(GUI\)](#), 2 ページ
- [CKIP の設定 \(CLI\)](#), 3 ページ

CKIP について

Cisco Key Integrity Protocol (CKIP) は、IEEE 802.11 メディアを暗号化するためのシスコ独自のセキュリティプロトコルです。CKIP では、インフラストラクチャモードでの 802.11 セキュリティを強化するために、キーの置換、メッセージの整合性チェック (MIC)、およびメッセージシーケンス番号が使用されています。ソフトウェアリリース 4.0 以降では、静的キーを使用した CKIP をサポートしています。この機能を正常に動作させるには、WLAN に対して Aironet 情報要素 (IE) を有効にする必要があります。

Lightweight アクセス ポイントは、ビーコンおよびプローブ応答パケットに Aironet IE を追加し、CKIP ネゴシエーションビット (キー置換およびマルチモジュラハッシュメッセージ整合性チェック [MMH MIC]) の一方または両方を設定することにより、CKIP のサポートをアドバタイズします。キー置換は、基本の暗号キーおよび現在の初期ベクトル (IV) を使用して新しいキーを作成するデータ暗号化技術です。MMH MIC では、ハッシュ関数を使用してメッセージ整合性コードを計算することにより、暗号化されたパケットでのパケット改ざん攻撃を回避します。

WLAN で指定された CKIP の設定は、アソシエートを試みるすべてのクライアントに必須です。WLAN で CKIP のキー置換および MMH MIC の両方が設定されている場合、クライアントは両方をサポートする必要があります。WLAN がこれらの機能の 1 つだけに設定されている場合は、クライアントではその CKIP 機能だけをサポートする必要があります。

CKIP では、5 バイトおよび 13 バイトの暗号キーは 16 バイトのキーに拡張される必要があります。キーを拡張するためのアルゴリズムは、アクセス ポイントで発生します。キーは、長さが 16 バイトに達するまで、そのキー自体に繰り返し追加されます。Lightweight アクセス ポイントはすべて CKIP をサポートしています。



- (注) CKIP は Static WEP での使用についてのみサポートされています。Dynamic WEP での使用はサポートされていません。したがって、Dynamic WEP で CKIP を使用するように設定された無線クライアントは、CKIP 用に設定されている WLAN にアソシエートできません。CKIP なしで Dynamic WEP を使用する (安全性がより低い) か、または TKIP または AES で WPA/WPA2 を使用する (安全性がより高い) ことを推奨します。

CKIP の設定 (GUI)

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。
- ステップ 3 [Advanced] タブを選択します。
- ステップ 4 [Aironet IE] チェックボックスをオンにして、この WLAN に対する Aironet IE を有効にし、[Apply] をクリックします。
- ステップ 5 [General] タブを選択します。
- ステップ 6 [Status] チェックボックスがオンになっている場合は、これをオフにしてこの WLAN を無効にし、[Apply] をクリックします。
- ステップ 7 [Security] タブおよび [Layer 2] タブを選択して、[WLANs > Edit] ([Security] > [Layer 2]) ページを開きます。
- ステップ 8 [Layer 2 Security] ドロップダウン リストから [CKIP] を選択します。
- ステップ 9 [CKIP Parameters] で、[Key Size] ドロップダウン リストから CKIP 暗号キーの長さを選択します。その範囲は、[Not Set]、[40 bits]、または [104 bits] です。デフォルトは、[Not Set] です。
- ステップ 10 [Key Index] ドロップダウン リストからこのキーに割り当てる番号を選択します。キーは、最高 4 つまで設定できます。
- ステップ 11 [Key Format] ドロップダウン リストから、[ASCII] または [HEX] を選択し、[Encryption Key] テキストボックスに暗号化キーを入力します。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。
- ステップ 12 この WLAN に対して MMH MIC データ保護を有効にする場合は、[MMH Mode] チェックボックスをオンにします。デフォルト値では無効 (またはオフ) になっています。
- ステップ 13 この形式の CKIP データ保護を有効にする場合は、[Key Permutation] チェックボックスをオンにします。デフォルト値では無効 (またはオフ) になっています。
- ステップ 14 [Apply] をクリックして、変更を確定します。
- ステップ 15 [General] タブを選択します。
- ステップ 16 [Status] チェックボックスをオンにして、この WLAN を有効にします。
- ステップ 17 [Apply] をクリックして、変更を確定します。
- ステップ 18 [Save Configuration] をクリックして、変更を保存します。

CKIP の設定 (CLI)

-
- ステップ 1 次のコマンドを入力して、WLAN を無効にします。
config wlan disable wlan_id
- ステップ 2 この WLAN の Aironet IE を有効にするには、次のコマンドを入力します。
config wlan ccx aironet-ie enable wlan_id
- ステップ 3 WLAN の CKIP を有効または無効にするには、次のコマンドを入力します。
config wlan security ckip {enable | disable} wlan_id
- ステップ 4 WLAN に対して CKIP 暗号化キーを指定するには、次のコマンドを入力します。
config wlan security ckip akm psk set-key wlan_id {40 | 104} {hex | ascii} key key_index
- ステップ 5 WLAN に対して CKIP MMH MIC を有効または無効にするには、次のコマンドを入力します。
config wlan security ckip mmh-mic {enable | disable} wlan_id
- ステップ 6 WLAN に対して CKIP キー置換を有効または無効にするには、次のコマンドを入力します。
config wlan security ckip kp {enable | disable} wlan_id
- ステップ 7 WLAN を有効にするには、次のコマンドを入力します。
config wlan enable wlan_id
- ステップ 8 次のコマンドを入力して、設定を保存します。
save config
-

