

# WAP551およびWAP561アクセスポイントでのWiFi Protected Access Pre-Shared Key(WPA-PSK)複雑度の設定

## 目的

アクセスポイント(AP)でWiFi Protected Access(WPA)が設定されている場合、クライアントを安全に認証するためにWPA事前共有キーを選択できます。WPA-PSKの複雑度をイネーブルにすると、認証プロセスで使用されるキーの複雑度要件を設定できます。より複雑なキーは、セキュリティを強化します。

この記事では、WAP551およびWAP561アクセスポイントでWPA事前共有キー複雑度(WPA-PSK)を設定する方法について説明します。

## 適用可能なデバイス

- ・ WAP551
- ・ WAP561

## [Software Version]

- ・ v1.0.4.2

## WPA-PSKの複雑度の設定

ステップ 1 : Web設定ユーティリティにログインし、System Security > WPA-PSK Complexityの順に選択します。WPA-PSK Complexityページが開きます。

## WPA-PSK Complexity

WPA-PSK Complexity:  Enable

WPA-PSK Minimum Character Class: 3 ▼

WPA-PSK Different From Current:  Enable

Maximum WPA-PSK Length: 63

Minimum WPA-PSK Length: 8

Save

## WPA-PSK Complexity

WPA-PSK Complexity:  Enable

WPA-PSK Minimum Character Class: 4 ▼

WPA-PSK Different From Current:  Enable

Maximum WPA-PSK Length: 3

Minimum WPA-PSK Length: 8

Save

ステップ 2 : WPA-PSK ComplexityフィールドのEnableチェックボックスにチェックマークを付けて、APが新しいWPA事前共有キーの複雑度をチェックできるようにします。

ステップ 3 : WPA-PSK Minimum Character Class ドロップダウンリストから、キー文字列で表す必要がある文字クラスの最小数を選択します。 2つの文字クラスを選択した場合、事前共有キーには大文字、小文字、数字、特殊文字など、少なくとも2つの文字クラスが含まれている必要があります。

## WPA-PSK Complexity

WPA-PSK Complexity:	<input checked="" type="checkbox"/> Enable
WPA-PSK Minimum Character Class:	4 ▼
WPA-PSK Different From Current:	<input checked="" type="checkbox"/> Enable
Maximum WPA-PSK Length:	40
Minimum WPA-PSK Length:	9

ステップ4: ( オプション ) 現在のキーの有効期限が切れているときに別の事前共有キーを入力するには、WPA-PSK Different From CurrentフィールドのEnableチェックボックスにチェックマークを付けます。無効にした場合は、以前に使用したのと同じキーを再入力できます。

ステップ 5 : Maximum WPA-PSK Lengthフィールドにキーの最大文字数を入力します。範囲は 64 ~ 80 です。

手順 6 : Minimum WPA-PSK Lengthフィールドに、キーに設定できる最小文字数を入力します。範囲は 8 ~ 32 です。

手順 7 : [Save] をクリックして、設定を保存します。

## 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。