Cisco WLC

学習内容

WLCの基本、主要な役割、および重要セキュリティ設定を学ぶ

1. WLCとは？役割とAPとの関係
2. WLC導入の主要なメリット
3. WLCの各種インターフェースの役割
4. IEEE802.1X認証の構成手順
5. MACアドレスフィルタリングの設定方法

01

WLCの基礎知識と主要な構成要素

WLC (Wireless LAN Controller) とは

大規模無線LAN環境におけるアクセスポイントの一元管理・集中制御装置

役割	重要性	APの役割
アクセスポイント（AP）の**設定と制御**を集中実行	APごとの個別設定が不要になり、**運用効率を大幅改善**	APは電波の送受信、最低限の暗号化・復号処理のみ実施

WLCとAPの関係性：CAPWAPプロトコル

WLCとAPはCAPWAPトンネルで結ばれ、制御とデータをやり取りする

WLCの役割 (集中制御)

- 電波出力の調整
- クライアントの認証処理
- 暗号化方式の制御
- ローミングの管理

APの役割 (電波送受信)

- WLCの探索とJoin
- WLCからの設定・OSイメージの受信
- クライアントとの電波送受信

WLC導入の主要なメリット

統一されたポリシー適用と高い無線品質の確保

運用効率化

複数APの**一元管理**による設定・監視工数の大幅削減

シームレスな通信

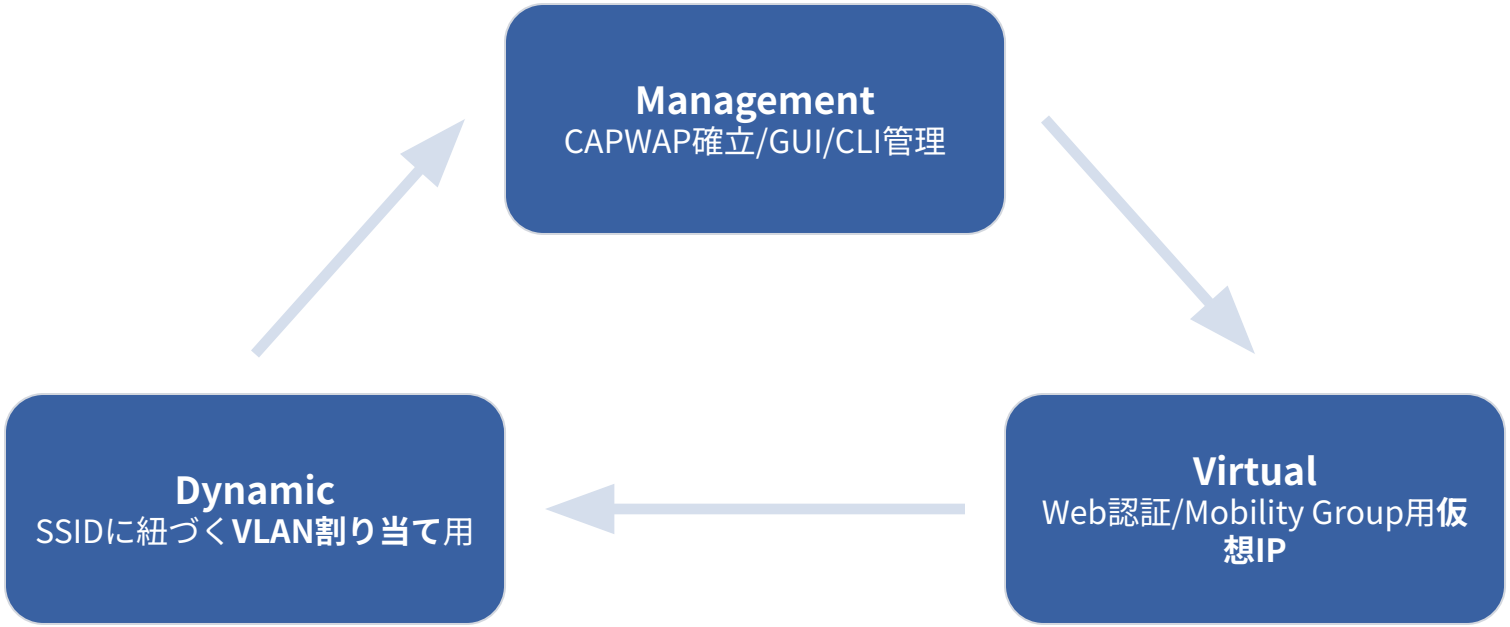
WLCによる**ローミング制御**で移動中の途切れのない通信を実現

セキュリティ向上

セキュリティポリシーの**集中管理**と統一的な適用

WLCの４つの主要インターフェース

用途に応じたWLCの論理/物理的な接続口を理解する



02

重要設定：IEEE802.1X認証の構成

IEEE802.1X認証の設定 3ステップ

WLCによるRADIUS認証に必要なVLAN、サーバ、SSIDの関連付け

STEP 1	VLANインターフェースの作成 (クライアント用VLANを定義)
STEP 2	RADIUSサーバの登録 (認証サーバの接続情報を設定)
STEP 3	SSIDの作成と認証設定 (SSIDをVLANとRADIUSに紐づけ)

Step 3: SSID認証設定の重要項目

WLANsのSecurityタブで認証方式とサーバを設定する

Layer 2 Security	Auth Key Mgmt	AAA Servers	Allow AAA Override
WPA+WPA2を選択し、WPA2 Encryptionで**AES**を指定	認証方式として**802.1X**を明示的に指定	登録済みの**RADIUSサーバ**を選択し関連付け	RADIUS属性に基づき**VLAN動的割当**を許可する

03

代替セキュリティ：MACアドレスフィルタリング

802.1X認証とMACフィルタリングの比較

セキュリティレベルの違いを理解し、適切な認証方式を選択する

IEEE802.1X認証	MACアドレスフィルタリング
ユーザー/デバイス単位の**強力な認証**	MACアドレスによる**簡易的なアクセス制御**
証明書やパスワードを使用	MACアドレスは偽装可能でセキュリティは低い
大規模環境の標準的なセキュリティ	小規模環境または互換性が必要な場合に利用

MACアドレスフィルタリングの設定：ローカルDBへの登録

WLC内部データベースに許可MACアドレスを直接登録する手順

GUIの「WLANs」から対象SSIDの「Security」⇒「Layer2」タブを開き、**MAC Filteringを有効化**する

GUIの「SECURITY」⇒「MAC Filtering」から「NEW」を選択し、許可するMACアドレスを登録する

登録時に「Interface Name」でMACフィルタを適用する**VLANを指定**する

CLIでの登録も可能: `config macfilter add [MACアドレス] [WLAN ID] [インターフェース名]`