

Cisco無線LAN

学習内容

- 1 Cisco無線LANの2つの管理方式
- 2 集中管理を支えるCAPWAPプロトコル
- 3 APが通信可能になるまでの流れ
- 4 ネットワーク構成と通信の仕組み
- 5 APの動作モード変換手順

01

Cisco無線LANの2つの管理方式

管理方式の比較

ネットワークの規模や運用方針に応じて最適な方式を選択することが重要です

分散管理型 (自律型)

AP単体で動作しクライアントを直接管理

WLC不要で**低コスト**

小規模環境（数台）に適している

AP毎の個別設定が必要で**管理が煩雑**

集中管理型

WLCが一括でAPとクライアントを管理

高度な認証や電波調整が可能

大規模環境（10台以上）に**最適**

管理コストを**大幅に削減**できる

FlexConnectによる柔軟な運用

集中管理型の弱点を補い、WAN越しの拠点管理を実現する仕組み

通常時の課題

すべての無線トラフィックがWLCを経由するため、WAN障害時に通信が停止するリスクがある

FlexConnectの解決策

本社のWLCで管理しつつ、各拠点のトラフィックは**ローカルで処理**。障害時も業務継続が可能

トラフィック処理の決定的な違い

SSIDとVLANのマッピングを「どこで」行うかが両方式の大きな違いです

分散管理型 (自律型AP)

集中管理型 (WLC)

AP自体

処理主体

WLC

各APに個別設定

設定場所

WLCに一括設定

APから直接転送

通信フロー

一度WLCを経由

集中管理型における接続方式

耐障害性と拡張性を考慮し、一般的には間接接続と冗長構成が採用されます

非推奨：直接接続

WLCとAPを同じスイッチに接続

構成はシンプルだが**単一障害点**となる

推奨：間接接続

APとWLCがIPで通信できればOK

WAN越しの構成も可能で**冗長化しやすい**

Split MAC vs Local MAC

トラフィックの処理方式を理解し、利用シーンに応じて使い分けることが重要です

Split MACアーキテクチャ

対象: 通常の集中管理モード

無線処理をAPとWLCに**分割**

APは電波関連と暗号化のみ担当

データは**全てWLCを経由**する

Local MACアーキテクチャ

対象: FlexConnectモード

APがある程度の自律性を持つ

データはWLCに戻さず**ローカル処理**

WAN越しの環境で特に効果を発揮

02

集中管理を支えるCAPWAPプロトコ ル

CAPWAPとは？

APとWLC間の通信を確立し、制御情報やデータを安全にやり取りするためのプロトコルです

Control And Provisioning of Wireless Access Points の略称

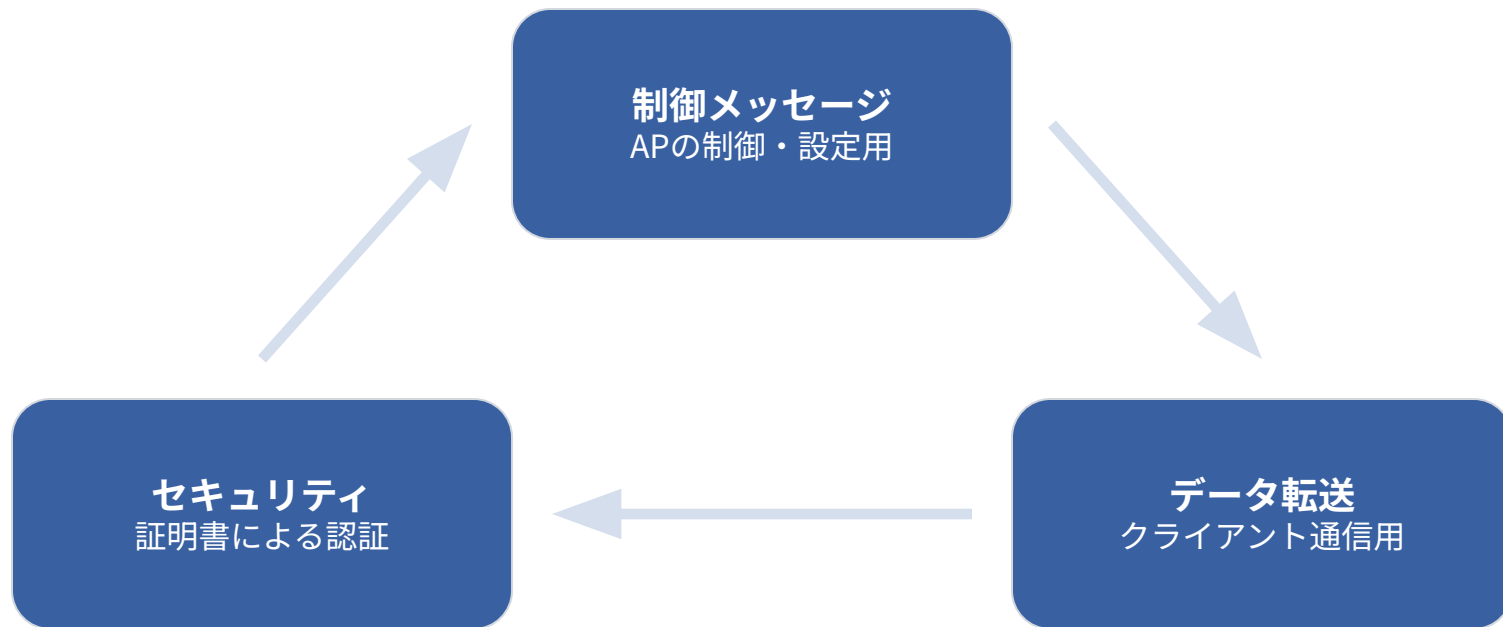
Cisco独自のLWAPPを基に標準化されたプロトコル

APとWLC間でCAPWAPトンネルを形成し、その中で通信を行う

クライアントからのデータはCAPWAPでカプセル化されて転送される

CAPWAPの主要要素

CAPWAPは「制御」「データ」「セキュリティ」の3つの要素で構成されています



使用されるポート番号

CAPWAPはUDPを使用し、旧プロトコルのLWAPPとは異なるポート番号が割り当てられています

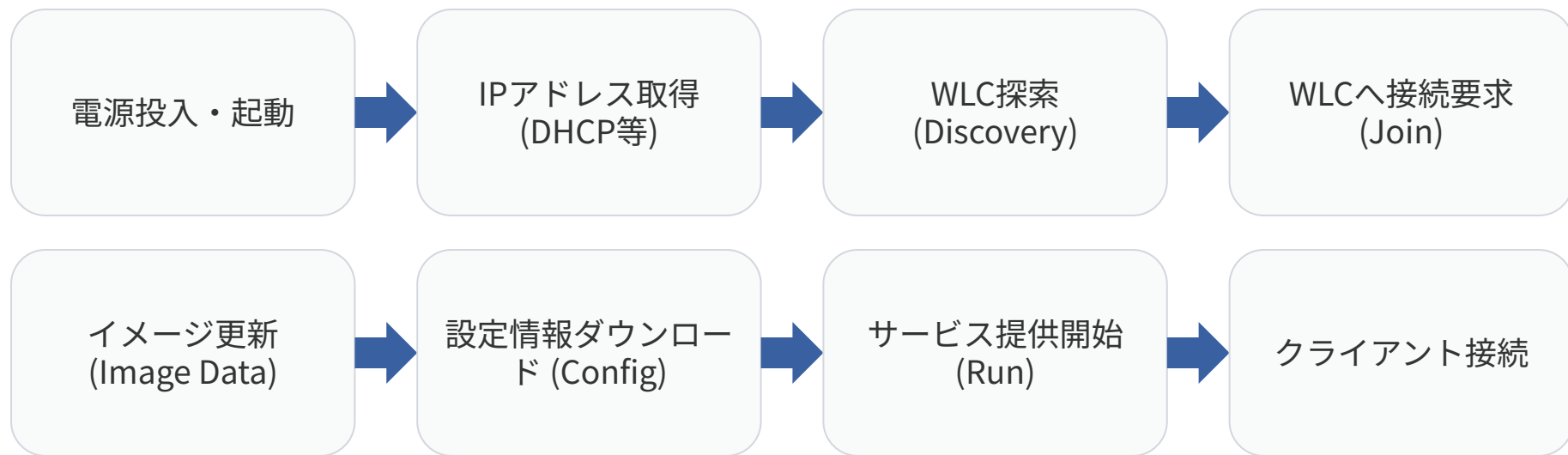
| プロトコル | 制御メッセージ | データ |
|-----------|-----------|-----------|
| CAPWAP | UDP 5246 | UDP 5247 |
| LWAPP (旧) | UDP 12223 | UDP 12222 |

03

APが通信可能になるまでの流れ

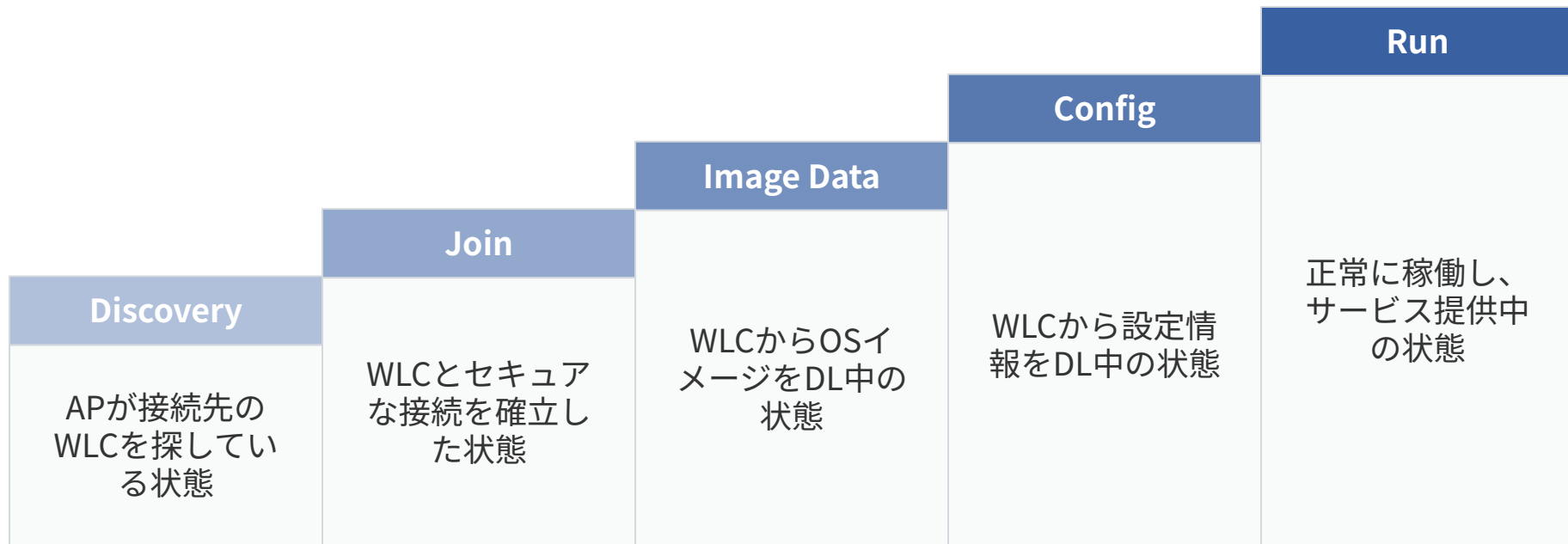
APの起動からサービス開始までのフロー

APはWLCの探索、接続確立、設定ダウンロードを経て、無線LANサービスを提供します



APの状態遷移

APとWLCの関係は「状態」で定義され、トラブルシューティングにも役立ちます



WLCの探索（Discovery）プロセス

APは複数の方法を順に試行し、接続先となるWLCのIPアドレスを特定します

- 1 CLIコマンドで静的に設定されたIPアドレス
- 2 ローカルサブネットへのブロードキャスト
- 3 DHCPのオプション43から取得
- 4 DNSで `Cisco-CAPWAP-Controller` を名前解決
- 5 上記で見つからなければ最初から繰り返す

WLCの選定基準

複数のWLC候補が見つかった場合、APは優先順位に従って接続先を決定します

優先度1：手動設定

APにプライマリ・セカンダリ等が設定されている場合はその順序に従う

優先度2：Master Controller

Master Controllerフラグが有効なWLCを優先する

優先度3：空き容量

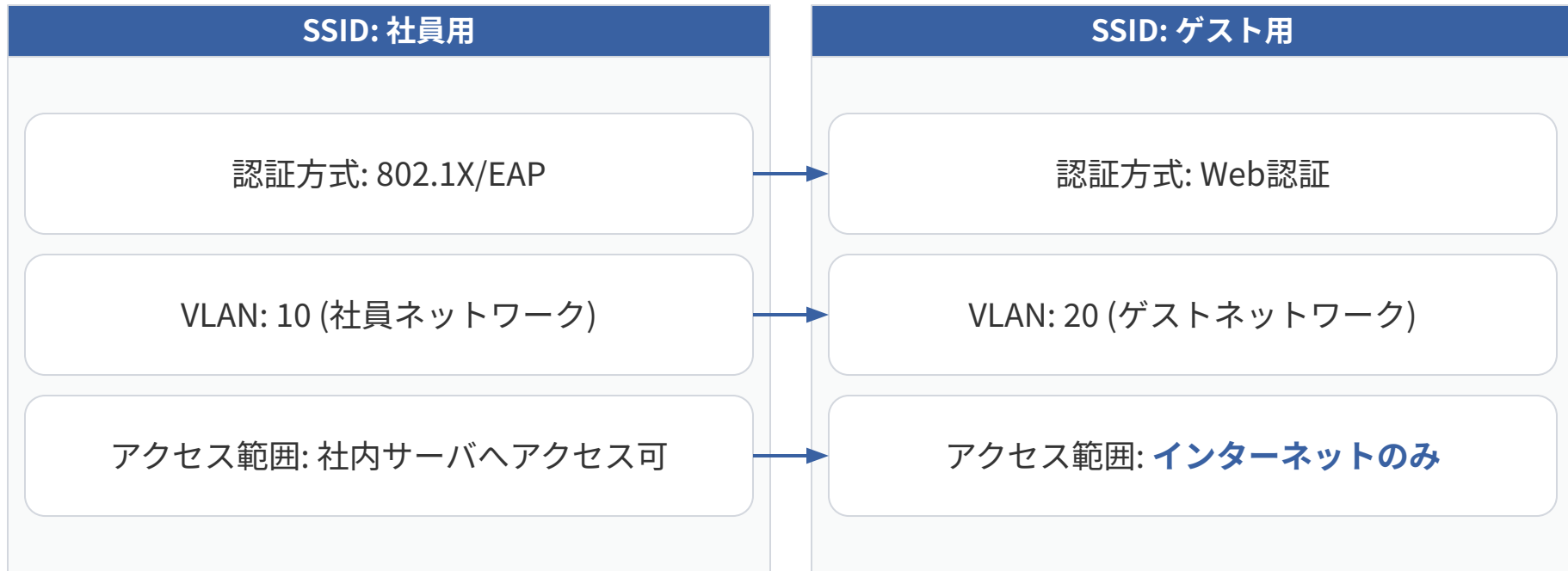
最も多くのAPを収容できる（空きキャパシティが大きい）WLCを選択する

04

ネットワーク構成と通信の仕組み

SSIDとVLANのマッピング

SSIDごとにVLANを割り当てることで、ネットワークを論理的に分割し、セキュリティを向上させます



WLCのインターフェース

WLCには役割の異なるインターフェースが存在し、通信制御の基盤となります

スタティック (固定)

Management, Service-Port, Virtualなど、システムが定義する基本的なIF

ダイナミック (可変)

管理者が作成するVLANインターフェース。SSIDとVLANを紐づけるために使用

通信の流れとIPアドレッシング

集中管理型では、クライアントの通信は必ずWLCを経由します

ポイント

- クライアントのDGはL3スイッチ等になる
- WLCはルーティングを行わない
- APとスイッチ間は**アクセスポート**で接続
- WLCとスイッチ間は**トランクポート**で接続

通信フロー

クライアントからのパケットは、AP → CAPWAPトンネル → WLC → L3スイッチの順で転送される。**WLCが全ての無線通信を制御**している。

05

APの動作モード変換手順

自律型 → 集中管理型 (CAPWAP) への変更

APにCAPWAPイメージをダウンロードさせ、WLC配下で動作するように変換します

- 1 CiscoサイトからCAPWAPイメージをダウンロード
- 2 管理PCでFTPサーバを準備し、イメージを配置
- 3 APにログインし、FTP接続情報を設定
- 4 `archive download-sw` コマンドを実行してイメージを書き換え
- 5 APが自動的に再起動し、CAPWAPモードで起動

集中管理型 → 自律型への変更

WLCのCLIからコマンドを実行し、APに自律型IOSを転送します

- 1 CiscoサイトからAutonomous IOSをダウンロード
- 2 管理PCでTFTPサーバを準備し、IOSを配置
- 3 WLCにログインし、対象APのホスト名を確認
- 4 ``config ap tftp-downgrade`` コマンドを実行
- 5 APが自動的に再起動し、自律型モードで起動（初期設定が必要）