IEEE802.1X認証

学習内容

ネットワーク接続に必要な認証の仕組みを理解する

1. IEEE802.1Xとは何か？
2. IEEE802.1Xの構成要素
3. EAP（Extensible Authentication Protocol）とは
4. IEEE802.1Xにおける認証の流れ
5. EAP認証方式の具体的な比較
6. EAP-TLS認証の構成と特徴

01

第1章：IEEE802.1Xの基礎

IEEE802.1Xとは？その役割と適用範囲

有線・無線LAN環境におけるユーザー認証の標準規格

IEEE802.1Xは、**有線・無線LAN**における**ユーザー認証**の仕組みを定めた規格

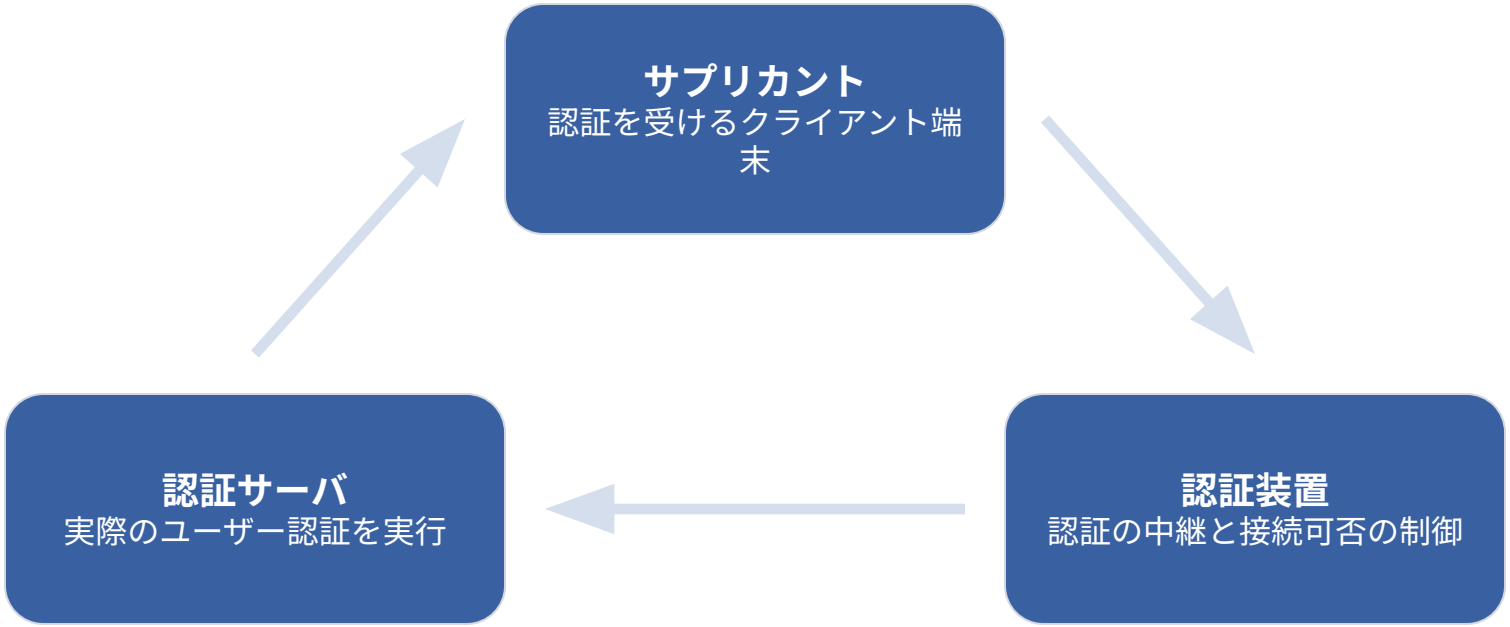
ネットワークへの接続を試みるユーザーの**正当性**を確認し、不正なアクセスを防ぐ

元々は有線LAN向けに策定されたが、**認証機能を持たない無線LANの初期**に強力な手段として普及

現在では、無線LAN（WPA2/3）はもちろん、**有線LAN**（LANスイッチ）でも幅広く適用可能

IEEE802.1X認証を支える3つの要素

この3要素が連携することでセキュアな認証が実現する



3要素の詳細：仲介役と認証の核

それぞれの役割と代表的な機器・プロトコル

サプリカント（Supplicant）

認証を受ける端末やソフトウェア。多くのOSに**標準搭載**されている。

認証装置（Authenticator）

LANスイッチやAP。サプリカントとサーバの仲介役。認証結果でポートを制御。

認証サーバ（Authentication Server）

ユーザ認証を実行するサーバ。IEEE802.1X/EAPに対応した**RADIUSサーバ**が利用される。

02

第2章：EAPプロトコルの概要と役割

EAP（Extensible Authentication Protocol）の役割

認証方式の汎用的なフレームワークを提供する

認証サーバとの通信経路

IPを使用しない認証通信はどのように実現されるのか？

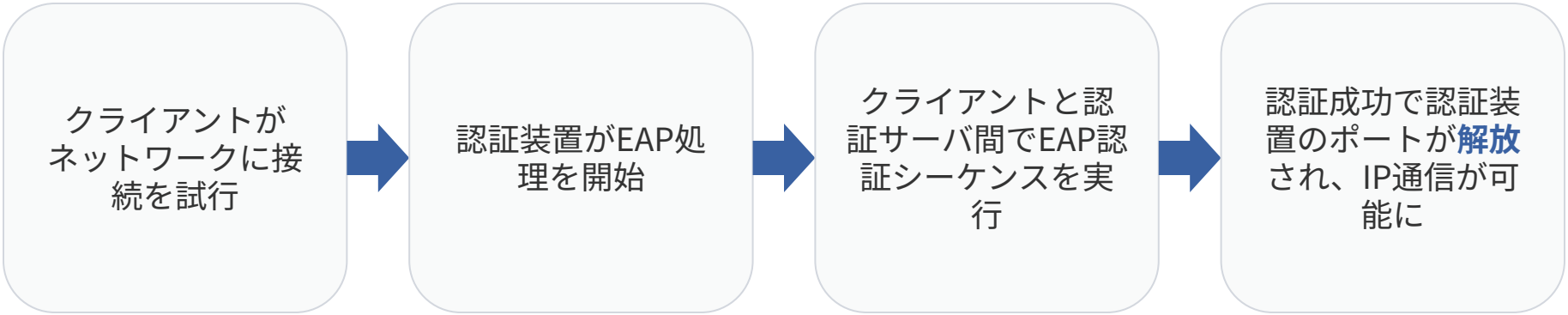
1. サプリカントはEAPメッセージを**EAPOL**（L2フレーム）で認証装置へ送信
2. 認証装置（スイッチ/AP）はEAPOLフレームを受け取り、それを**RADIUSプロトコル**に**変換**
3. 認証装置はRADIUSパケットを認証サーバへ**IP通信**で転送（ここで初めてIPが関与）
4. 認証サーバが認証結果をRADIUSで認証装置へ返信し、接続可否が決定

03

第3章：認証の流れと方式の比較

IEEE802.1Xによる認証の基本的な流れ

認証が成功するまで通常のIP通信はブロックされる



【重要】EAP-TLSとPEAPの違い

セキュリティの要件に応じた認証方式を選択する

EAP-TLS	PEAP
クライアント・サーバ双方で**証明書が必須**	サーバ証明書のみ必須、クライアントはパスワード利用が多い
セキュリティレベルは最高	セキュリティレベルは高い（TLSによるトンネル内での認証）
証明書管理の手間が非常に大きい	証明書管理の負担が比較的軽い
大企業やセキュリティ重視の組織向け	**Windows標準対応**で企業利用に最適

EAP-TLS認証の主要な構成要素

高いセキュリティを実現するために必要な4つの役割