Wifi（セキュリティ）

学習内容

1. WEPの基礎と脆弱性
2. 無線LANのセキュリティ課題と従来の対策
3. WPA/WPA2への進化とCCMPの採用
4. 最新規格 WPA3の特徴とセキュリティ強化

01

WEPの基礎と脆弱性

WEP（Wired Equivalent Privacy）とは

有線LAN同等の安全性を目指した初期の暗号化技術

無線LAN通信を暗号化し、盗聴対策として導入された初期の規格

暗号アルゴリズムに**RC4**を用いた**共通鍵方式**を採用

鍵長は40bitまたは104bitで、24bitのIV（初期化ベクトル）を加えて64bitまたは128bitとなる

データの完全性検証に**CRC32**を使用するが、改ざん検知には不十分な脆弱性を持つ

現在では**脆弱性（Weak IV、FMS攻撃など）**が明らかになり、利用は非推奨

WEPにおける2種類の認証方式

認証方法の違いがもたらすセキュリティ上の問題

Open認証 (オープンシステム認証)

端末からの認証要求にAPは必ず認証成功を返す

SSIDが一致すれば接続可能で実質的な認証は行わない

暗号化はWEPで行われる（通信内容は解読されやすい）

Shared-key認証 (共有キー認証)

端末とAPがWEPキーを用いた**チャレンジレスポンス**で認証

一見セキュリティが高そうに見える

認証に使ったWEPキーが盗聴されやすく**中間者攻撃に弱い**

02

無線LANのセキュリティ課題と従来の対策

無線LANが抱える代表的なセキュリティリスク

電波を利用するからこそ発生する主な脅威

不正接続（侵入）

電波の届く範囲にいれば、物理接続なしで容易にアクセスを試行される

不正傍受（盗聴）

認証・暗号化なしの場合、空中を飛ぶパケットは容易に傍受・解析される

不正AP（おとり）

正規APを偽装した偽APを設置し、接続させた利用者のIDやパスワードを盗み取る

従来実施されてきたセキュリティ対策とその限界

万全ではない、過去の一般的な防御策

ESSIDの隠蔽

ビーコンにSSIDを含めない設定。ただし、アソシエーション時にはSSIDが平文で流れるため、**完全な秘匿は不可能**。

MACアドレスフィルタリング

登録MACアドレスのみ接続許可する方式。しかし、MACアドレスは**簡単に偽装が可能**。

WEPによる暗号化

RC4を用いた暗号方式。すでに**脆弱性が明らか**であり、現在は使用非推奨。

ANY接続の拒否

ANY SSIDでの接続を無効化。不正な接続を防止できるが、設定変更の手間も生じる。

03

WPA/WPA2への進化とCCMPの採用

無線LANセキュリティ規格の進化の歴史

脆弱性への対応とより強固な暗号化の追求

1997年

WEPが策定されるも、脆弱性が発覚

2002年10月

暫定規格としてWPAが策定（TKIP採用）

2004年6月

IEEE802.11i標準化完了

2004年9月

IEEE802.11i準拠のWPA2が策定（CCMP/AES採用）

WEPとWPA/WPA2のセキュリティ進化比較

暗号化アルゴリズムと整合性検証の大きな改善点

WEP (旧規格)		WPA2 (現行標準)
RC4	暗号化アルゴリズム	AES
WEP	暗号化方式	CCMP
CRC32	整合性検証	MIC/CCM
24bit	IV長	48bit

WPA2の暗号化方式「CCMP」の動作

AESをベースにした高速かつ高セキュリティな暗号方式

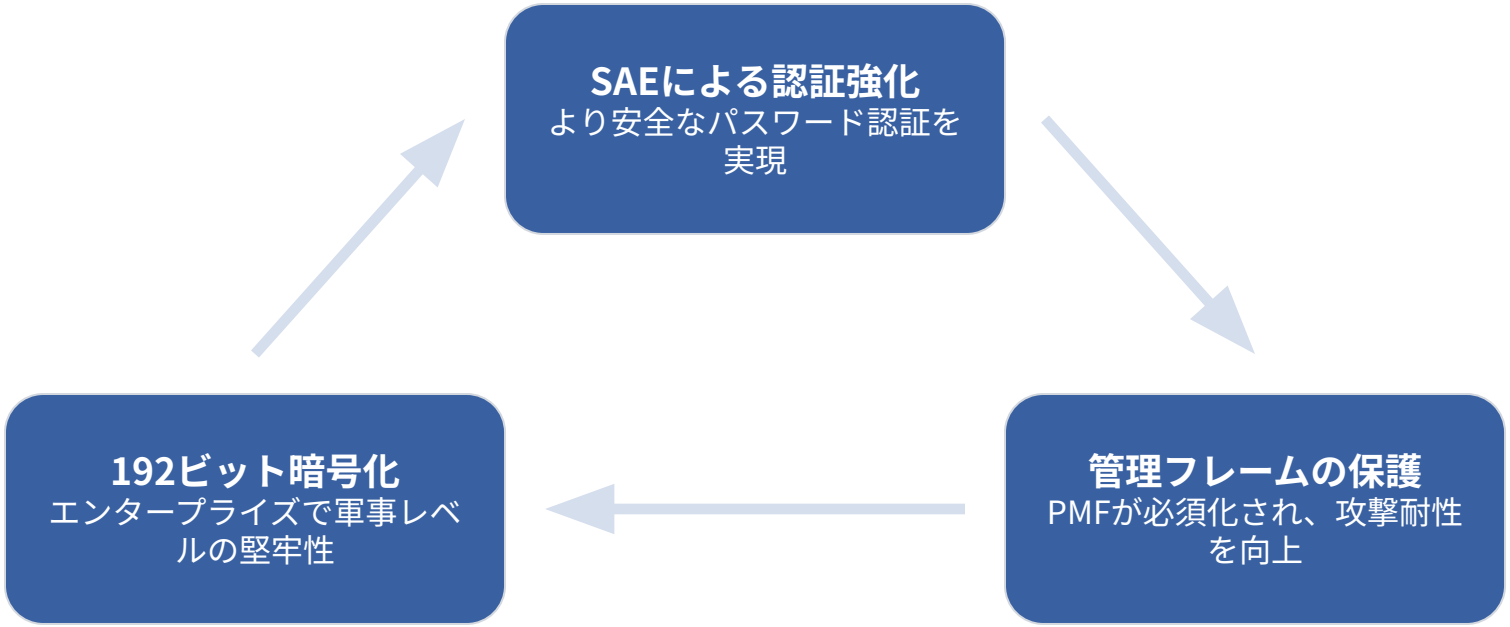
STEP 1	メッセージをブロックに区切る
STEP 2	カウンタ値をAESで暗号化
STEP 3	結果とメッセージをXOR演算して暗号文を生成
STEP 4	CBC-MACにより整合性を確認

04

最新規格 WPA3の特徴とセキュリティ強化

WPA3による主要なセキュリティ強化ポイント

WPA2の課題を克服し、次世代のセキュリティ標準へ



WPA3のモード別概要

用途に応じた2つのモード

モード	別名	用途	特徴的な認証技術
WPA3-Personal	WPA3-SAE	個人・小規模ネットワーク	SAE（より安全なパスワード認証）
WPA3-Enterprise	WPA3-EAP	企業ネットワーク	IEEE802.1X認証（192ビット暗号化）