

コースコード：CT-N462

税込価格：143,000円 (税抜価格：130,000円)

日数：2日間

## 前提条件

- ・以下のすべての条件を満たしている方
- ・「無線LANシステム構築実践」コースを修了、または同等の知識を有している
- ・EthernetやTCP/IPプロトコルの仕組みを理解している
- ・パケットアナライザ(WireShark等)を用いたパケット解析の経験を有している

## 受講対象者

無線LANに携わるSE/CE

## コース概要

無線LANのトラブルシュー트에携わるネットワークエンジニアを対象としたコースです。トラブル発生時の無線LAN環境を調査し、その原因を特定・解析する方法を学習します。また、実際に無線LANに対してサイバー攻撃(DoS攻撃やセキュリティキーの解読など)を実施し、アクセスポイントが抱える脆弱性やインシデント(情報セキュリティに関する事件・事故)発生時の対処法について学習します。

## 目的

- ・トラブル発生時の初期対応(関連機器からの情報収集)を実施することができる
- ・専用ツールを用いた情報収集を実施することができる
- ・収集した無線LANパケットの情報から、トラブルの原因を推察することができる
- ・無線LANに対してペネトレーションテスト(システムを実際に攻撃し脆弱性を調べるテスト)を実施し、アクセスポイントが抱える脆弱性を調査することができる
- ・インシデント発生時の初期対応(関連機器からの情報収集)を実施することができる

## アウトライン

- ・トラブルシューティング概要
- ・無線LANのトラブル
- ・トラブル遭遇前の事前準備
- ・トラブルシューティングのフロー
- ・情報収集のポイント
- ステーションの調査
- APの調査
- 認証サーバの調査
- ・専用ツールを用いた調査
- 各種ツールの使用方法
- ・ネットワークコマンド
- ・スペクトラムアナライザ
- 安定した無線LAN通信の要件
- サンプルシグナル(コードレス電話、bluetooth、電子レンジ等)
- フリーの電波環境調査ツール
- 電波関連のトラブルと対策



- ・パケットアナライザ
- パケットアナライザの特徴
- パケットアナライザの使用方法
- 無線LAN通信の解析(基礎編)
- ・802.11 MAC Headerの解析
- フレームコントロールフィールド
- その他のフィールド
- ・管理フレームの解析
- Beacon
- Probe Request/Response
- Authentication
- Association Request/Response
- ・制御フレームの解析
- ACK
- RTS/CTS
- ・パケット解析によるトラブル原因の特定
- 無線LAN接続不可、パフォーマンス劣化 等
- 無線LAN通信の解析(応用編)
- ・WPA/WPA2
- 4 Way Handshake
- 2 Way Handshake
- パケットアナライザの復号機能
- ・IEEE802.1X/EAP認証
- EAPOLによるカプセル化
- EAPパケット本体
- EAP-TLSのシーケンス
- PEAPのシーケンス
- ・パケット解析によるトラブル原因の特定
- PSK認証、IEEE802.1X/EAP認証の失敗 等
- 無線LANへの攻撃とその調査手法
- ・無線LANをとりまく脅威
- ・攻撃ツールのセットアップ
- ・事前調査(攻撃対象の確認)
- ・DoS攻撃
- ・無線LANデータの盗聴
- ・WEPキーの解読
- ・WPA/WPA2-PSKの解読
- ・Fake AP(不正APの設置)
- ・インシデント発生時の調査手法

コースカリキュラムは予告なく変更となる可能性があります。

[テキスト]

テキスト、演習資料は紙を使用いたします。