

## SECFND (Understanding Cisco Cybersecurity Fundamentals)

---

サイバーセキュリティアナリストを目指す方にオススメです。  
トラフィック分析やインシデント対応のスキルを習得できます。

### 前提条件

- Windowsの基本操作を理解できていること

下記のコースを受講済み、または同等の知識を有する方

- [ICND1 \(Interconnecting Cisco Networking Devices, Part 1\)](#)

### 受講対象者

- SOCにてセキュリティアナリスト担当の方
- セキュリティインシデントの検出や対応を担当する方
- ネットワークセキュリティサポートエンジニアの方
- サイバーセキュリティ分野を学び始めた方
- Ciscoチャネルパートナーの方
- CCNA Cyber Ops 認定の取得を目指している方

### 概要

このコースでは、TCP/IP プロトコルスイートのネットワーク インフラストラクチャのデバイス、運用、および脆弱性、基本的な情報セキュリティの概念、一般的なネットワークアプリケーションの動作と攻撃、Windows および Linux オペレーティングシステム、セキュリティ インシデントの調査に使用されるデータの種類について説明します。このコースを完了すると、脅威中心型セキュリティ オペレーションセンターで、エントリレベルのサイバーセキュリティアナリストの職務を行うために必要な基本知識が得られます。

### 目的

このコースを修了すると、次のことができるようになります。

- TCP/IP プロトコルスイートとその基本動作
- ネットワーク インフラストラクチャのデバイスとその基本動作

TCP/IP プロトコルスイートの脆弱性  
基本的な暗号化の概念とアルゴリズム  
情報セキュリティの重要概念  
一般的なネットワークアプリケーションの動作と攻撃  
Windows および Linux オペレーティングシステムの基本操作  
一般的なエンドポイント攻撃  
ネットワークとエンドポイントのセキュリティテクノロジーとその基本動作  
セキュリティインシデントの調査に使用されるデータの種類  
セキュリティ  
オペレーション組織がサイバーセキュリティ分析を実行する際に参照できる脅威モデル

---

## アウトライン

- TCP/IPプロトコルスイートの理解
- ネットワークインフラストラクチャの理解
- 一般的なTCP/IP攻撃の理解
- 基本的な暗号化の概念の理解
- 情報セキュリティの概念の説明
- ネットワークアプリケーションの理解
- 一般的なネットワークアプリケーション攻撃を理解する
- Windowsオペレーティングシステムの基本を理解する
- Linuxオペレーティングシステムの基本を理解する
- 一般的なエンドポイント攻撃の理解
- ネットワークセキュリティテクノロジーの理解
- エンドポイントセキュリティテクノロジーの理解
- セキュリティデータ収集の説明
- セキュリティイベント分析の説明