# Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps v1.0 (300-215)

**試験の概要：**Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps v1.0（CBRFIR 300-215）は、Cisco CyberOps Professional 認定に関連する試験であり、試験時間は 90 分です。この試験では、フォレンジック分析とインシデント対応の基礎、テクニック、プロセスに関する知識が試されます。本試験の受験対策として、Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps コースの受講をお勧めします。

以下に、この試験の出題内容の概要を示します。ただし、試験によっては、ここに示されていない関連項目も出題される場合があります。試験内容をより適切に反映し、明確にするために、次のガイドラインは予告なく変更されることがあります。

## 20% 1.0 基礎

- 1.1 根本原因分析レポートに必要なコンポーネントの分析
- 1.2 インフラストラクチャ ネットワーク デバイスのフォレンジック分析を実行するプロセス
- 1.3 アンチフォレンジックの戦略、技術、および手順
- 1.4 エンコーディングおよび難読化の手法（base 64、16 進数エンコーディングなど）
- 1.5 マルウェアの識別、分類、文書化のための YARA ルール（基本）の使い方と特徴
- 1.6 以下のツールの役割：
  - 1.6.a DFIR 調査でのバイナリエディタ（HxD, Hiew, Hexfiend）
  - 1.6.b 基本的なマルウェア解析を行うための逆アセンブラやデバッガ (Ghidra、Radare、Evans Debugger など)
  - 1.6.c deobfuscation ツール（XORBruteForces、xortool、unpacker など）
- 1.7 仮想化環境からのエビデンス収集に関連する問題点（主なクラウドベンダー）

## 20% 2.0 フォレンジック技術

- 2.1 MITRE アタック フレームワークで有効とされているファイルレス マルウェア分析の実行方法
- 2.2 ホスト上の必要なファイルとその場所
- 2.3 ホスト上の IOC を識別するための出力の評価
  - 2.3.a プロセス分析
  - 2.3.b ログ分析
- 2.4 提供されたスニペットに基づくコードの種類の判定
- 2.5 ログや複数のデータソース（Cisco Umbrella、Sourcefire IPS、AMP for

Endpoints、AMP for Network、PX Grid など）を解析して検索する Python、PowerShell、Bash スクリプトの作成

2.6 ライブラリやツール（Volatility、Systernals、SIFTツール、TCPdump など）の目的、使用方法、機能

## 30% 3.0 インシデント対応技術

3.1 アラートログ（IDS/IPS や syslog など）の解釈

3.2 インシデントの種類（ホストベースおよびネットワークベースの活動）に基づいた関連データの決定

3.3 （所定のシナリオでの）攻撃ベクトルまたはアタックサーフェスの特定、および推奨される緩和策

3.4 インシデント発生後の分析に基づく対応策

3.5 ファイアウォール、侵入防止システム（IPS）、データ分析ツール（Cisco Umbrella Investigate、Cisco Stealthwatch、Cisco SecureX など）、その他のシステムから発行された評価済みアラートに対して、サイバー インシデントに対応するために推奨される緩和策

3.6 ゼロデイ攻撃に対する推奨される対応（脆弱性管理）

3.7 インテリジェンス アーティファクトに基づく対応策

3.8 （所定のシナリオでの）検出および予防のために推奨されるシスコ セキュリティ ソリューション

3.9 脅威インテリジェンス データの解釈による IOC および IOA（内部および外部ソース）の特定

3.10 脅威情報を基にしたアーティファクトの評価と脅威アクターのプロファイルの特定

3.11 脅威情報（Cisco Umbrella、Sourcefire IPS、AMP for Endpoints、AMP for Network など）に関連するシスコ セキュリティ ソリューションの機能

## 15% 4.0 フォレンジック プロセス

4.1 アンチ フォレンジック技術（デバッグ、ジオロケーション、難読化など）

4.2 最新のウェブ アプリケーションおよびサーバ（Apache と NGINX）のログの分析

4.3 ネットワーク監視ツール（NetFlow や Wireshark のディスプレイ フィルタリングなど）を使用した、悪意のある活動に関連するネットワーク トラフィックの分析

4.4 （所定のシナリオでの）ファイルの識別された特性に基づくファイル評価プロセスにおける推奨される次のステップ

4.5 objdump や 他の CLI ツール（Linux、Python、Bashなど）を使用したバイナリの解釈

## 15% 5.0 インシデント対応プロセス

5.1 インシデント対応の目標

5.2 インシデント対応プレイブックに必要な要素の評価

5.3 ThreatGrid レポートの関連するコンポーネントの評価

5.4 （所定のシナリオでの）エンドポイントのファイルの評価とアドホックスキャンを実行するプロセスにおける推奨される次のステップ

5.5 異なるフォーマット（STIX や TAXII など）で提供される脅威インテリジェンスの分析