Understanding Cisco Cybersecurity Operations Fundamentals v1.0 (200-201)

試験概要：Cisco Certified CyberOps Associate プログラムは、セキュリティオペレーションセンター（SOC）の現場で求められる最新のオペレーションスキルと知識を習得します。SOC アナリストは、サイバーセキュリティの脅威に対する防御の最前線として機能します。組織を守るための脅威を検出し防止します。 CyberOps Associate 認定は、この重要な機能におけるスキルを認定します。

次に、この試験の一般的な出題内容を示します。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　セキュリティの概念

1.1　CIA トライアドの説明

1.2　セキュリティ配備の比較

- 1.2.a　ネットワーク、エンドポイント、およびアプリケーションのセキュリティ システム
- 1.2.b　エージェントレスおよびエージェントベースの防御
- 1.2.c　従来型のアンチウィルスおよびアンチマルウェア
- 1.2.d　SIEM、SOAR、ログ管理

1.3　セキュリティ用語の説明

- 1.3.a　脅威インテリジェンス（TI）
- 1.3.b　脅威ハンティング
- 1.3.c　マルウェア分析
- 1.3.d　脅威のアクター
- 1.3.e　RBA（Run book automation）

1.3.f　リバース エンジニアリング

1.3.g　スライディング ウィンドウによる異常検出

1.3.h　最小特権アクセスの原理

1.3.i　ゼロトラスト

1.3.j　脅威インテリジェンス プラットフォーム（TI）

1.4　セキュリティ概念の比較

1.4.a　リスク（リスク スコアリング／リスク重み付け、リスク軽減、リスク評価）

1.4.b　脅威

1.4.c　脆弱性

1.4.d　エクスプロイト

1.5　多層防御（defense-in-depth）戦略

1.6　アクセス制御モデルの比較

1.6.a　任意アクセス制御（DAC）

1.6.b　強制アクセス制御（MAC）

1.6.c　非任意アクセス制御（NAC）

1.6.d　認証、許可、アカウンティング（AAA）

1.6.e　規則ベースのアクセス制御

1.6.f　時間ベースのアクセス制御

1.6.g　役割ベースのアクセス制御

1.7　CVSS で定義されている用語の説明

1.7.a　攻撃ベクトル

1.7.b　攻撃条件の複雑さ

1.7.c　必要な特権

1.7.d　ユーザー インタラクション

1.7.e　スコープ

1.8　検出におけるデータの可視性（ネットワーク、ホスト、クラウド）に関する課題の特定

1.9　提供されたトラフィック プロファイルからの潜在的データ損失の特定

1.10　グループ化されたログのセットで侵害されたホストを分離するための 5 組アプローチの解釈

1.11　規則ベースの検出と振る舞い／統計検出の比較

25 %　2.0　セキュリティ モニタリング

2.1　攻撃可能面と脆弱性の比較

2.2　以下のテクノロジーによって提供されるデータのタイプの特定

- 2.2.a　TCP ダンプ
- 2.2.b　NetFlow
- 2.2.c　次世代ファイアウォール
- 2.2.d　従来型のステートフル ファイアウォール
- 2.2.e　アプリケーション可視化と制御
- 2.2.f　Web コンテンツ フィルタリング
- 2.2.g　電子メール コンテンツ フィルタリング

2.3　以下のテクノロジーのデータ可視化に対する影響の説明

- 2.3.a　アクセス制御リスト
- 2.3.b　NAT/PAT
- 2.3.c　トンネリング
- 2.3.d　TOR
- 2.3.e　暗号化
- 2.3.f　P2P
- 2.3.g　カプセル化

2.3.h　ロード バランシング

2.4　セキュリティ モニタリングにおける以下のデータ タイプについての説明

2.4.a　フル パケット キャプチャ

2.4.b　セッション データ

2.4.c　トランザクション データ

2.4.d　統計データ

2.4.e　メタデータ

2.4.f　アラートデータ

2.5　プロトコルベース、サービス拒否、分散型サービス拒否、マンインザミドルなどのネットワーク攻撃

2.6　SQL インジェクション、コマンド インジェクション、クロスサイト スクリプティングなどの Web アプリケーション攻撃

2.7　ソーシャル エンジニアリング攻撃

2.8　バッファ オーバーフロー、コマンド アンド コントロール（C2）、マルウェア、ランサムウェアなどのエンドポイントベースの攻撃

2.9　トンネリング、暗号化、プロキシなどの回避および難読化テクニック

2.10　セキュリティに対する証明書の影響（PKI、パブリック／プライベート、非対称／対称など）

2.11　特定シナリオでの証明書コンポーネントの特定

2.11.a 暗号スイート

2.11.b X.509 証明書

2.11.c 鍵交換

2.11.d プロトコルのバージョン

2.11.e PKCS

20 %　3.0　ホストベースの分析

3.1　セキュリティ モニタリングに関する以下のエンドポイント テクノロジーの機能

- 3.1.a　ホストベースの侵入検出
- 3.1.b　アンチマルウェアとアンチウィルス
- 3.1.c　ホストベースのファイアウォール
- 3.1.d　アプリケーションレベル ホワイトリスティング／ブラックリスティング
- 3.1.e　システムベースのサンドボックス（Chrome、Java、Adobe Reader）

3.2　特定のシナリオにおけるオペレーティング システム（Windows や Linux など）のコンポーネントの特定

3.3　セキュリティ調査における属性の役割

- 3.3.a　アセット
- 3.3.b　脅威のアクター
- 3.3.c　不正アクセスの痕跡（IOC）
- 3.3.d　攻撃の痕跡
- 3.3.e　証拠保全（COC）

3.4　提供されたログに基づいて使用された証拠の種類

- 3.4.a　最良証拠
- 3.4.b　補強証拠
- 3.4.c　間接証拠

3.5　改ざんされたディスクイメージ／されていないディスクイメージの比較

3.6　オペレーティング システム、アプリケーション、またはコマンドライン ログの解釈によるイベントの特定

3.7　マルウェア分析ツール（デトネーション チャンバーやサンドボックス）の出力レポートの解釈

- 3.7.a　ハッシュ

3.7.b URL

3.7.c システム、イベント、ネットワーキング

20 % 4.0 ネットワーク侵入分析

4.1 指定されたイベントのソース テクノロジーへのマッピング

4.1.a IDS/IPS

4.1.b ファイアウォール

4.1.c ネットワーク アプリケーション コントロール

4.1.d プロキシログ

4.1.e アンチウィルス

4.1.f トランザクション データ（NetFlow）

4.2 以下の項目による影響あり／なしの比較

4.2.a 偽陽性

4.2.b 偽陰性

4.2.c 真陽性

4.2.d 真陰性

4.2.e 良性

4.3 ディープ パケット インスペクションとパケット フィルタリング、および ステートフル ファイアウォールの運用の比較

4.4 インライン トラフィック調査とタップ／トラフィック モニタリングの比較

4.5 ネットワーク トラフィックの分析における、タップ／トラフィック モニタリングとトランザクション データ（NetFlow）から取得したデータの特性の比較

4.6 指定された PCAP ファイルと Wireshark による TCP ストリームからのファイルの抽出

4.7 侵入の主要な要素の特定（指定された PCAP ファイルを使用）

4.7.a 送信元アドレス

4.7.b 宛先アドレス

4.7.c 送信元ポート

4.7.d 宛先ポート

4.7.e プロトコル

4.7.f ペイロード

4.8 侵入分析に関連するプロトコル ヘッダーのフィールドの解釈

4.8.a イーサネットフレーム

4.8.b IPv4

4.8.c IPv6

4.8.d TCP

4.8.e UDP

4.8.f ICMP

4.8.g DNS

4.8.h SMTP/POP3/IMAP

4.8.i HTTP/HTTPS/HTTP2

4.8.j ARP

4.9 イベントの一般的なアーティファクト要素の解釈によるアラートの解釈

4.9.a IP アドレス（送信元／宛先）

4.9.b クライアント／サーバ・ポートの ID

4.9.c プロセス（ファイルまたはレジストリ）

4.9.d システム（API コール）

4.9.e ハッシュ

4.9.f URI / URL

4.10 基本的な正規表現の解釈

15 % 5.0 セキュリティ ポリシーとプロシージャ

5.1 管理の概念

5.1.a アセットの管理

5.1.b コンフィグレーションの管理

5.1.c モバイルデバイスの管理

5.1.d パッチの管理

5.1.e　脆弱性の管理

5.2　NIST.SP800-61 に記載されているインシデント対応計画の要素

5.3　インシデント処理プロセス（NIST.SP800-61 など）のイベントへの適用

5.4　上記要素の NIST.SP800-61 に基づく以下の分析ステップへのマッピング

5.4.a　準備

5.4.b　検出および分析

5.4.c　封じ込め、根絶、および復旧

5.4.d　事後分析（教訓を生かす）

5.5　組織の利害関係者の NIST IR カテゴリ（CMMC、NIST.SP800-61）へのマッピング

5.5.a　準備

5.5.b　検出および分析

5.5.c　封じ込め、根絶、および復旧

5.5.d　事後分析（教訓を生かす）

5.6　NIST.SP800-86 に文書化された概念

5.6.a　証拠収集の順序

5.6.b　データの完全性

5.6.c　データの保全

5.6.d　揮発性データの収集

5.7　ネットワーク プロファイリングに使用される以下の要素の特定

5.7.a　総スループット

5.7.b　セッション期間

5.7.c　使用ポート

5.7.d　重要なアセットのアドレス空間

5.8　サーバ プロファイリングに使用される以下の要素の特定

5.8.a　リスニングポート

5.8.b　ログインユーザー／サービスのアカウント

5.8.c　実行中のプロセス

5.8.d　実行中のタスク

5.8.e　アプリケーション

5.9　ネットワーク内の保護されたデータの特定

5.9.a　PII

5.9.b　PSI

5.9.c　PHI

5.9.d　知的財産

5.10　侵入イベントをサイバー キル チェーン モデルや侵入分析のダイヤモンド モデルなどのセキュリティ モデルで定義されたカテゴリに分類

5.11　SOC メトリックとスコープ分析の関係（検出時間、封じ込め時間、対応時間、制御時間）