Understanding Cisco Cybersecurity Fundamentals (210-250)

試験概要：Understanding Cisco Cybersecurity Fundamentals (SECFND) 試験（210-250）は、Cisco CCNA Cyber Ops 認定に関する試験であり、試験時間は 90 分、問題数は 60 ～70 問です。試験に対応するトレーニングは、Understanding Cisco Cybersecurity Fundamentals (SECFND) v1.0 コースです。試験では、サイバーセキュリティの基本原則、基礎知識、コアスキルについての理解度をテストします。これらは、2 つ目の試験となる「Implementing Cisco Cybersecurity Operations (SECOPS)」を理解するために必要となります。

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。

12 %　1.0　ネットワークの概念

1.1　OSI および TCP/IP ネットワーク モデルで指定されているネットワーク層の機能についての説明

1.2　次の動作の説明
- 1.2.a　IP
- 1.2.b　TCP
- 1.2.c　UDP
- 1.2.d　ICMP

1.3　次のネットワーク サービスの動作の説明
- 1.3.a　ARP
- 1.3.b　DNS
- 1.3.c　DHCP

1.4　次のネットワーク デバイス タイプの基本動作の説明
- 1.4.a　ルータ
- 1.4.b　スイッチ
- 1.4.c　ハブ
- 1.4.d　ブリッジ
- 1.4.e　ワイヤレス アクセス ポイント（WAP）
- 1.4.f　ワイヤレス LAN コントローラ（WLC）

1.5 ホスト、ネットワーク、クラウドに導入されている次のネットワーク セキュリティ システムの機能についての説明
- 1.5.a ファイアウォール
- 1.5.b Cisco Intrusion Prevention System（IPS）
- 1.5.c Cisco Advanced Malware Protection（AMP）
- 1.5.d Web セキュリティ アプライアンス（WSA）/Cisco クラウド Web セキュリティ（CWS）
- 1.5.e E メール セキュリティ アプライアンス（ESA）/Cisco クラウド E メール セキュリティ（CES）

1.6 IP サブネット、および IP サブネット内や IP サブネット間の通信についての説明

1.7 VLAN 間の関係とデータの可視性についての説明

1.8 ネットワーク デバイスのインターフェイス上でパケット フィルタとして適用される ACL の動作についての説明

1.9 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動作の比較対照

1.10 インライン トラフィックの調査とタップまたはトラフィック ミラーリングの比較対照

1.11 ネットワーク トラフィック分析においてタップまたはトラフィック ミラーリング、および NetFlow から取得したデータの特性の比較対照

1.12 特定のトラフィック プロファイルに見られるデータ損失の可能性の特定

17 % 2.0 セキュリティの概念

2.1 多層防御戦略の原則についての説明

2.2 次の概念の比較対照
- 2.2.a リスク
- 2.2.b 脅威
- 2.2.c 脆弱性
- 2.2.d エクスプロイト

2.3 次の用語の説明
- 2.3.a 攻撃者
- 2.3.b Run Book Automation（RBA）
- 2.3.c Chain of Custody（証拠保管）
- 2.3.d リバース エンジニアリング
- 2.3.e スライディング ウィンドウ異常検出
- 2.3.f PII
- 2.3.g PHI

2.4 次のセキュリティ用語の説明
- 2.4.a 最小権限の原則

2.4.b リスク スコアリング/リスク重み付け
2.4.c リスク軽減
2.4.d リスク評価

2.5 次のアクセス制御モデルの比較対照
2.5.a 任意アクセス制御
2.5.b 強制アクセス制御
2.5.c 非任意アクセス制御

2.6 次の用語の比較対照
2.6.a ネットワークとホストのウイルス対策
2.6.b エージェントレスおよびエージェントベースの保護
2.6.c SIEM とログの収集

2.7 次の概念の説明
2.7.a 資産管理
2.7.b 構成管理
2.7.c モバイル デバイス管理
2.7.d パッチ管理
2.7.e 脆弱性管理

12 % **3.0** 暗号化

3.1 ハッシュ アルゴリズムの使い方の説明

3.2 暗号化アルゴリズムの使い方の説明

3.3 対称/非対称暗号化アルゴリズムの比較対照

3.4 デジタル署名の作成と検証のプロセスについての説明

3.5 PKI の動作についての説明

3.6 一般的に使われる次のハッシュ アルゴリズムのセキュリティの影響についての説明
3.6.a MD5
3.6.b SHA-1
3.6.c SHA-256
3.6.d SHA-512

3.7 一般的に使われる次の暗号化アルゴリズムおよびセキュア通信プロトコルのセキュリティの影響の説明
3.7.a DES
3.7.b 3DES
3.7.c AES
3.7.d AES256-CTR
3.7.e RSA
3.7.f DSA

3.7.g SSH
3.7.h SSL/TLS

3.8 暗号交換の成功または失敗がセキュリティ調査に与える影響についての説明

3.9 SSL/TLS に関する次の用語の説明
3.9.a 暗号スイート
3.9.b X.509 証明書
3.9.c キー交換
3.9.d プロトコルのバージョン
3.9.e PKCS

19 % 4.0 ホストベース分析

4.1 Microsoft Windows に関連する次の用語の定義
4.1.a プロセス
4.1.b スレッド
4.1.c メモリ割り当て
4.1.d Windows レジストリ
4.1.e WMI
4.1.f ハンドル
4.1.g サービス

4.2 Linux に関連する次の用語の定義
4.2.a プロセス
4.2.b フォーク
4.2.c アクセス権
4.2.d シンボリックリンク
4.2.e デーモン

4.3 セキュリティ モニタリングに関する次のエンドポイント技術の機能についての説明
4.3.a ホストベースの侵入検知
4.3.b マルウェア対策とウイルス対策
4.3.c ホストベースのファイアウォール
4.3.d アプリケーションレベルのホワイトリスト/ブラックリスト
4.3.e システムベースのサンドボックス（Chrome、Java、Adobe Reader など）

4.4 次のオペレーティング システムのログ データの解釈とイベントの特定
4.4.a Windows セキュリティ イベント ログ
4.4.b Unix ベースの syslog
4.4.c Apache アクセス ログ
4.4.d IIS アクセス ログ

19 %　5.0　セキュリティ モニタリング

5.1　次の技術で提供されるデータのタイプの特定

- 5.1.a　TCP ダンプ
- 5.1.b　NetFlow
- 5.1.c　次世代ファイアウォール
- 5.1.d　従来のステートフル ファイアウォール
- 5.1.e　アプリケーションの可視性と制御
- 5.1.f　Web コンテンツ フィルタリング
- 5.1.g　電子メールのコンテンツ フィルタリング

5.2　セキュリティ モニタリングで使用する次のデータ タイプについての説明

- 5.2.a　フル パケット キャプチャ
- 5.2.b　セッション データ
- 5.2.c　トランザクション データ
- 5.2.d　統計データ
- 5.2.f　抽出コンテンツ
- 5.2.g　アラート データ

5.3　セキュリティ モニタリングに関連する次の概念についての説明

- 5.3.a　アクセス コントロール リスト
- 5.3.b　NAT/PAT
- 5.3.c　トンネリング
- 5.3.d　ToR
- 5.3.e　暗号化
- 5.3.f　P2P
- 5.3.g　カプセル化
- 5.3.h　ロード バランシング

5.4　次世代 IPS の次のイベント タイプについての説明

- 5.4.a　接続イベント
- 5.4.b　侵入イベント
- 5.4.c　ホストまたはエンドポイント イベント
- 5.4.d　ネットワーク検出イベント
- 5.4.e　NetFlow イベント

5.5　セキュリティ モニタリングに関連する次のプロトコルの機能についての説明

- 5.5.a　DNS
- 5.5.b　NTP
- 5.5.c　SMTP/POP/IMAP
- 5.5.d　HTTP/HTTPS

21 % **6.0** 攻撃方法

6.1 攻撃対象領域と脆弱性の比較対照

6.2 次のネットワーク攻撃についての説明

- 6.2.a Denial of Service（DoS）
- 6.2.b 分散型 Denial of Service（DoS）
- 6.2.c 中間者

6.3 次の Web アプリケーション攻撃についての説明

- 6.3.a SQL インジェクション
- 6.3.b コマンド インジェクション
- 6.3.c クロスサイト スクリプティング

6.4 次の攻撃についての説明

- 6.4.a ソーシャル エンジニアリング
- 6.4.b フィッシング
- 6.4.c 回避方法

6.5 次のエンドポイントベース攻撃についての説明

- 6.5.a バッファ オーバーフロー
- 6.5.b コマンド アンド コントロール（C2）
- 6.5.c マルウェア
- 6.5.d ルートキット
- 6.5.e ポート スキャニング
- 6.5.f ホスト プロファイリング

6.6 次の回避方法についての説明

- 6.6.a 暗号化とトンネリング
- 6.6.b リソースの枯渇
- 6.6.c トラフィック フラグメンテーション
- 6.6.d プロトコルレベルの誤解釈
- 6.6.e トラフィックの代替と挿入
- 6.6.f ピボット

6.7 権限のエスカレーションの定義

6.8 リモート エクスプロイトとローカル エクスプロイトの比較対照