

Implementing and Operating Cisco Security Core Technologies v1.1 (350-701)

試験の概要： Implementing and Operating Cisco Security Core Technologies v1.1 (SCOR 350-701) は、CCNP および CCIE Security 認定に関連する 120 分間の試験です。本試験では、ネットワークセキュリティ、クラウドセキュリティ、コンテンツセキュリティ、エンドポイントの保護と検出、セキュアなネットワークアクセス、可視性、および適用など、セキュリティのコアテクノロジーの実装および運用に関する受験者の知識が評価されます。本試験の対策として、「Implementing and Operating Cisco Security Core Technologies」コースが用意されています。

本試験の一般的な出題内容を以下に示します。ただし、実際の試験では、ここに記載のない関連するトピックが出題される場合もあります。また、試験の内容をより適切に反映し、明確にするため、以下に示す出題内容は予告なく変更される場合があります。

- 25% 1.0 **セキュリティの概念**
 - 1.1 オンプレミス、ハイブリッド、クラウド環境に対する一般的な脅威の説明
 - 1.1.a オンプレミス：ウイルス、トロイの木馬、DoS/DDoS 攻撃、フィッシング、ルートキット、中間者攻撃、SQL インジェクション、クロスサイトスクリプティング、マルウェア
 - 1.1.b クラウド：データ侵害、安全でない API、DoS/DDoS、ログイン情報の流出
 - 1.2 一般的なセキュリティ脆弱性の比較（ソフトウェアのバグ、脆弱なパスワードやハードコードされたパスワード、OWASP の上位 10 項目、暗号化の欠如、バッファオーバーフロー、パストラバーサル、クロスサイトスクリプティング/クロスサイトフォージェリなど）
 - 1.3 暗号技術コンポーネントの機能の説明（ハッシュ、暗号化、PKI、SSL、IPsec、IPv4 環境での NAT-T による IPsec、事前共有キー、および証明書ベースの認証など）
 - 1.4 サイト間 VPN とリモートアクセス VPN の展開タイプおよびコンポーネントの比較（仮想トンネルインターフェイス、標準ベースの IPsec、DMVPN、FlexVPN、Cisco Secure Client など。高可用性の考慮事項も含む）
 - 1.5 セキュリティ インテリジェンスの作成、共有、使用についての説明
 - 1.6 フィッシングおよびソーシャルエンジニアリング攻撃からの保護対策の説明
 - 1.7 SDN アーキテクチャにおけるノースバウンド API とサウスバウンド API の説明
 - 1.8 ネットワークのプロビジョニング、最適化、監視、障害対応のための Cisco DNA Center API の説明

- 1.9 Cisco Security アプライアンスの API 呼び出しに使用される基本的な Python スクリプトの理解
- 20%** **2.0 ネットワークセキュリティ**
 - 2.1 侵入防御とファイアウォール機能を備えたネットワーク セキュリティ ソリューションの比較
 - 2.2 侵入防御とファイアウォール機能を備えたネットワーク セキュリティ ソリューションおよびアーキテクチャの展開モデルの説明
 - 2.3 NetFlow レコードと Flexible NetFlow レコードのコンポーネント、機能、利点の説明
 - 2.4 ネットワーク インフラストラクチャのセキュリティ方式の設定と確認
 - 2.4.a レイヤ 2 方式 (VLAN を使用したネットワーク セグメンテーション、レイヤ 2 およびポートセキュリティ、DHCP スヌーピング、ダイナミック ARP インスペクション、ストーム制御、PVLAN によるネットワークトラフィックの分離、および MAC、ARP、VLAN ホッピング、STP、不正 DHCP 攻撃に対する防御)
 - 2.4.b ネットワーク インフラストラクチャおよびデバイスのセキュリティ強化 (コントロールプレーン、データプレーン、管理プレーン)
 - 2.5 セグメンテーション、アクセス コントロール ポリシー、AVC、URL フィルタリング、マルウェア防御、侵入ポリシーの実装
 - 2.6 ネットワーク セキュリティ ソリューションの管理オプションの実装 (シングルデバイスとマルチデバイスマネージャ、インバンドとアウトオブバンド、クラウドとオンプレミス)
 - 2.7 デバイスおよびネットワークアクセスでの AAA の設定 (TACACS+ や RADIUS など)
 - 2.8 境界セキュリティおよびインフラストラクチャ デバイスの安全なネットワーク管理の設定 (SNMPv3、NetConf、RestConf、API、セキュア syslog、認証付き NTP など)
 - 2.9 サイト間 VPN とリモートアクセス VPN の設定と確認
 - 2.9.a シスコのルータと IOS を使用したサイト間 VPN
 - 2.9.b Cisco AnyConnect セキュア モビリティ クライアントを使用したリモートアクセス VPN
 - 2.9.c IPsec トンネルの確立状態を表示するデバッグコマンドと障害対応
- 15%** **3.0 クラウドの保護**
 - 3.1 クラウド環境のセキュリティソリューションの特定
 - 3.1.a パブリック、プライベート、ハイブリッド、コミュニティの各クラウド
 - 3.1.b クラウドサービスモデル : SaaS、PaaS、IaaS (NIST 800-145)

- 3.2 さまざまなクラウドサービスモデルのセキュリティに関する責任の比較
 - 3.2.a クラウドでのパッチ管理
 - 3.2.b クラウドでのセキュリティアセスメント
- 3.3 DevSecOps の概念の説明 (CI/CD パイプライン、コンテナ オーケストレーション、セキュアなソフトウェア開発)
- 3.4 クラウド環境におけるアプリケーションとデータのセキュリティの実装
- 3.5 クラウドを保護するためのセキュリティ機能、展開モデル、ポリシー管理の特定
- 3.6 クラウドにおけるロギングおよび監視手法の設定
- 3.7 アプリケーションとワークロードのセキュリティ概念の説明
- 15%** **4.0 コンテンツセキュリティ**
 - 4.1 Web プロキシへのトラフィックリダイレクトとキャプチャ方式の実装
 - 4.2 透過的ユーザー識別を含む Web プロキシのアイデンティティと認証の説明
 - 4.3 オンプレミス、ハイブリッド、クラウドベースの E メールおよび Web ソリューション (Cisco Secure Email Gateway、Cisco Secure Email Cloud Gateway、Cisco Secure Web Appliance) のコンポーネント、機能、利点の比較
 - 4.4 オンプレミス、ハイブリッド、リモートユーザーの保護を目的とした Web および E メールセキュリティの展開方法の設定と確認
 - 4.5 E メールセキュリティ機能 (スパムフィルタリング、マルウェア対策、DLP、ブロックリスト、E メール暗号化など) の設定と確認
 - 4.6 Cisco Umbrella Secure Internet Gateway と Web セキュリティ機能 (ブロックリスト、URL フィルタリング、マルウェアスキャン、URL 分類、Web アプリケーション フィルタリング、TLS 復号など) の設定と確認
 - 4.7 Cisco Umbrella のコンポーネント、機能、利点の説明
 - 4.8 Cisco Umbrella での Web セキュリティ管理の設定と確認 (アイデンティティ、URL コンテンツ設定、接続先リスト、レポート作成)
- 10%** **5.0 エンドポイントの保護と検出**
 - 5.1 Endpoint Protection Platform (EPP) ソリューションと Endpoint Detection and Response (EDR) ソリューションの比較
 - 5.2 Cisco Secure Endpoint を使用したエンドポイントのマルウェア対策保護の設定
 - 5.3 感染拡大を防ぐためのアウトブレイクコントロールおよび検疫の設定と確認
 - 5.4 エンドポイントベースのセキュリティを導入する正当性の説明
 - 5.5 MDM などのエンドポイントデバイス管理および設備一覧 (アセットインベントリ) システムの価値の説明
 - 5.6 多要素認証 (MFA) 戦略の活用方法およびその重要性の説明
 - 5.7 エンドポイントセキュリティを確保するためのエンドポイント ポスチャアセスメント ソリューションの説明
 - 5.8 エンドポイントパッチ適用戦略の重要性の説明

- 15% 6.0 **セキュアなネットワークアクセス、可視性、適用**
- 6.1 アイデンティティ管理とセキュアなネットワークアクセスの概念の説明（ゲストサービス、プロファイリング、ポスチャアセスメント、BYOD など）
- 6.2 802.1X、MAB、WebAuth などのネットワーク アクセス コントロール メカニズムの設定と確認
- 6.3 CoA を使用したネットワークアクセスの説明
- 6.4 デバイスコンプライアンスとアプリケーション制御の利点の説明
- 6.5 データ窃取手法の説明（DNS トンネリング、HTTPS、Eメール、FTP/SSH/SCP/SFTP、ICMP、Messenger、IRC、NTP）
- 6.6 ネットワークテレメトリの利点の説明
- 6.7 以下のセキュリティ製品およびソリューションのコンポーネント、機能、利点の説明
 - 6.7.a Cisco Secure Network Analytics
 - 6.7.b Cisco Secure Cloud Analytics
 - 6.7.c Cisco pxGrid
 - 6.7.d Cisco Umbrella Investigate
 - 6.7.e Cisco Cognitive Intelligence
 - 6.7.f Cisco Encrypted Traffic Analytics
 - 6.7.g Cisco Secure Client Network Visibility Module (NVM)