# Implementing and Operating Cisco Security Core Technologies v1.0（350-701）

**試験概要**：Implementing and Operating Cisco Security Core Technologies v1.0（SCOR 350-701）は、CCNP および CCIE Security 認定に関する試験であり、試験時間は 120 分です。この試験では、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および検出、セキュアなネットワーク アクセス、可視性、エンフォースメントなど、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問われます。本試験の受験対策として、Implementing and Operating Cisco Security Core Technologies コースの受講をお勧めします。

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。

**25%　1.0　セキュリティの概念**

1.1　オンプレミスおよびクラウド環境における一般的な脅威についての説明

- 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、マンインザミドル攻撃、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：データ漏洩、安全でない API、DoS/DDoS、証明書のセキュリティ侵害

1.2　セキュリティにおける一般的な脆弱性の比較（ソフトウェアのバグ、弱いパスワード、またはハードコートされたパスワード、SQL インジェクション、暗号化されないデータ、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 スクリプティングおよび偽造など）

1.3　暗号技術を構成する各要素の機能についての説明（ハッシュ、暗号化、PKI、SSL、IPsec、IPsec NAT-T IPv4、許可に基づく鍵および証明書の事前共有など）

1.4　サイト間 VPN およびリモート アクセス VPN VPN における展開のタイプの比較（SVTI、IPsec、Cryptomap、DMVPN、FLEXVPN（HA 要件を含む）、AnyConnect など）

1.5　セキュリティ インテリジェンスのオーサリング、共有、および消費についての説明

1.6　フィッシングやソーシャル エンジニアリングからユーザを守るエンドポイントの役割についての説明

1.7　SDN アーキテクチャにおけるノース バウンドおよびサウス バウンド API の説明

1.8　DNAC API によるネットワーク プロビジョニング、最適化、モニタリング、およびトラブルシューティングの説明

1.9 Cisco セキュリティ アプライアンス API のコールに使用される基本的な Python スクリプトの解釈

**20% 2.0 ネットワークセキュリティ**

2.1 侵入防御およびファイアウォール機能を提供するネットワーク セキュリティ ソリューションの比較

2.2 侵入防御およびファイアウォール機能を提供するネットワーク 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 および Flexible NetFlow のコンポーネント、機能、および利点の説明

2.4 ネットワーク インフラストラクチャ セキュリティ モデルの構成および確認（ルータ、スイッチ、ワイヤレス）

- 2.4.a レイヤ 2 方式（VLAN および VRF-Lite 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 コントロール、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、Rogue 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 セキュリティ デバイスのデバイス ハードニング（コントロール プレーン、データ プレーン、管理プレーン、およびルーティング プロトコルのセキュリティ）

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、およびマルウェア防御の実装

2.6 侵入防御や境界防御などのネットワーク セキュリティ ソリューション管理オプションの実装（シングルまたはマルチ デバイス マネージャ、インバンドまたはアウトオブバンド、CDP、DNS、SCP、SFTP、DHCP のセキュリティおよびリスクなど）

2.7 デバイスおよびネットワーク アクセスに対する AAA の構成（認証と許可、TACACS+、RADIUSおよびRADIUSのフロー、アカウンティング、および dACL）

2.8 境界防御およびインフラストラクチャ デバイスのセキュアなネットワーク管理の構成（セキュアなデバイス管理、SNMPv3、ビュー、グループ、ユーザ、認証、および暗号化、セキュアなロギング、および認証機能を実装した NTP）

2.9 サイト間 VPN およびリモート アクセス VPN の構成および確認

- 2.9.a Cisco ルータおよび IOS を利用したサイト間 VPN
- 2.9.b Cisco AnyConnect Secure Mobility 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 コマンドおよびトラブルシューティング

**15%　3.0　クラウドのセキュリティ対策**

3.1　クラウド 環境用のセキュリティ 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、およびコミュニティ 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　異なるクラウド サービス モデルにおける、カスタマーとプロバイダーのセキュリティに関する責任のありかたの比較

- 3.2.a　クラウド でのパッチ管理
- 3.2.b　クラウド でのセキュリティの割り当て
- 3.2.c　クラウド駆動型セキュリティ ソリューション（ファイアウォール、管理、プロキシ、セキュリティ インテリジェンス、および CASB など）

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、およびセキュリティ）

3.4　クラウド環境でのアプリケーションおよびデータ セキュリティの実装

3.5　クラウドのセキュリティを保護するために必要なセキュリティ機能、展開モデル、ポリシー管理の特定

3.6　クラウド ロギングおよびモニタリング機能の構成

3.7　アプリケーションおよびワークロード セキュリティの概念の説明

**15%　4.0　コンテンツ セキュリティ**

4.1　トラフィック リダイレクションおよびキャプチャ方式の実装

4.2　トランスペアレント ユーザ ID を含む Web プロキシでのアイデンティティおよび認証の説明

4.3　ローカルおよびクラウドベースの電子メールおよび Web ソリューションのコンポーネント、機能、利点の比較（ESA、CES、WSA）

4.4　オンプレミスおよびリモート ユーザを保護するための Web および電子メールのセキュリティ展開の構成（インバウンドおよびアウトバウンド コントロール、ポリシー管理）

4.5　電子メール セキュリティ機能の構成および確認（SPAM フィルタリング、アンチマルウェア フィルタリング、DLP、ブラックリスト、暗号化など）

4.6　セキュアなインターネット ゲートウェイおよびセキュリティ機能の構成および確認（ブラックリスト、URL フィルタリング、マルウェア スキャニング、URL カテゴリ、Web アプリケーション フィルタリング、TLS 複合など）

4.7　Cisco Umbrella のコンポーネント、機能、および利点の説明

4.8　Cisco Umbrella での Web セキュリティ コントロールの構成および確認（アイデンティティ、URL コンテンツの設定、宛先リスト、レポート）

**10%** **5.0** **エンドポイントの保護および検出**

5.1 EPP（EPP）ソリューションとEDR（Endpoint Detection & Response）ソリューションの比較

5.2 アンチマルウェア、レトロスペクティブ セキュリティ、IOC（Indication of Compromise）、アンチウイルス、動的ファイル分析、およびエンドポイントを起点とするテレメトリの説明

5.3 感染の拡大を防止するためのアウトブレーク コントロールと検疫の構成および確認

5.4 エンドポイントベース セキュリティの導入を正当化する理由についての説明

5.5 MDM などのエンドポイント デバイス管理およびアセット インベントリの価値についての説明

5.6 マルチファクタ認証（MFA）戦略の使用法および重要性の説明

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 ポスチャー 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 パッチ管理機能の重要性の説明

**15%** **6.0** **セキュアなネットワーク アクセス、可視性、およびエンフォースメント**

6.1 アイデンティティ管理および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、ポスチャー アセスメント、BYODなど）

6.2 ネットワーク アクセス デバイス機能の構成および確認（802.1X、MAB、WebAuth）

6.3 CoA によるネットワーク アクセスの説明

6.4 デバイスのコンプライアンスおよびアプリケーション コントロール機能の利点の説明

6.5 データ抜き取り（exfiltration）の手法についての説明（DNS トンネリング、HTTPS、電子メール、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、および利点の説明

- 6.7.a Cisco Stealthwatch
- 6.7.b Cisco Stealthwatch Cloud
- 6.7.c Cisco pxGrid
- 6.7.d Cisco Umbrella Investigate
- 6.7.e Cisco Cognitive Threat Analytics
- 6.7.f Cisco Encrypted Traffic Analytics
- 6.7.g Cisco AnyConnect Network Visibility Module （NVM）