

## Implementing Cisco Enterprise Network Core Technologies v1.0 (350-401)

**試験概要:** Implementing Cisco Enterprise Network Core Technologies v1.0 (ENCOR 350-401) は、CCNP および CCIE Enterprise 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、デュアルスタック (IPv4 および IPv6) アーキテクチャ、仮想化、インフラストラクチャ、ネットワーク アシユアランス、セキュリティ、自動化など、コア エンタープライズ ネットワーク テクノロジーの実装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 Cisco Enterprise Network 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。

- 15%    **1.0    アーキテクチャ**
  - 1.1    エンタープライズネットワークに使用される各種の設計原理の相違点の説明
    - 1.1.a    ティア 2、ティア 3、ファブリックのキャパシティプランニングなどのエンタープライズ ネットワーク デザイン
    - 1.1.b    冗長性、FHRP、SSO などのハイ・アベイラビリティ機能
  - 1.2    WLAN 展開の設計原理の分析
    - 1.2.a    ワイヤレス展開モデル (集中型、分散型、コントローラレス、コントローラベース、クラウド、リモート ブランチ)
    - 1.2.b    WLAN 設計におけるロケーション サービス
  - 1.3    オンプレミス展開とクラウド インフラストラクチャ展開の相違点
  - 1.4    Cisco SD-WAN ソリューションの作動原理の説明
    - 1.4.a    SD-WAN のコントロールおよびデータ・プレーンの構成要素
    - 1.4.b    従来型の WAN ソリューションと SD-WAN ソリューション
  - 1.5    Cisco SD-Access ソリューションの作動原理の説明
    - 1.5.a    SD-Access のコントロールおよびデータ・プレーンの構成要素
    - 1.5.b    従来からのキャンパス LAN と SD-Access の相互運用
  - 1.6    有線およびワイヤレス QoS の概念の説明
    - 1.6.a    QoS の構成要素
    - 1.6.b    QoS ポリシー
  - 1.7    ハードウェア スイッチングとソフトウェア スイッチングにおけるメカニズムの相違点
    - 1.7.a    プロセスと CEF
    - 1.7.b    MAC アドレス テーブルと TCAM
    - 1.7.c    FIB と RIB

- 10% 2.0 仮想化
  - 2.1 デバイス仮想化技術の説明
    - 2.1.a ハイパーバイザタイプ 1 および 2
    - 2.1.b 仮想マシン
    - 2.1.c 仮想スイッチング
  - 2.2 仮想化データ経路の構成および確認
    - 2.2.a VRF
    - 2.2.b GRE および IPsec トンネリング
  - 2.3 ネットワーク仮想化の概念の説明
    - 2.3.a LISP
    - 2.3.b VXLAN
- 30% 3.0 インフラストラクチャ
  - 3.1 レイヤ 2
    - 3.1.a 802.1q 静的および動的トランキング プロトコルのトラブルシューティング
    - 3.1.b 静的および動的 EtherChannel のトラブルシューティング
    - 3.1.c 一般的なスパンニング ツリー プロトコル (RSTP および MST) の構成および確認
  - 3.2 レイヤ 3
    - 3.2.a EIGRP と OSPF のルーティング概念の比較対照 (拡張ディスタンス ベクタ型対リンク ステート型、負荷分散、経路選択、経路制御、メトリック)
    - 3.2.b 単純な OSPF 環境の構成および確認 (複数のノーマル エリア、サマライゼーション、フィルタリング (ネイバーおよびアジャセンシー、ポイントツーポイントおよびブロードキャスト ネットワーク タイプ、およびパッシブ インターフェイス))
    - 3.2.c 直接接続されたネイバー間での eBGP の構成および確認 (最適パス選択アルゴリズムとネイバー関係)
  - 3.3 ワイヤレス
    - 3.3.a レイヤ 1 の概念の説明 (RF 電力レベル、RSSI、SNR、干渉ノイズ、帯域とチャネル、ワイヤレス クライアント デバイスの機能)
    - 3.3.b AP モードおよびアンテナ タイプの説明
    - 3.3.c アクセス ポイント ディスカバリおよび join のプロセスの説明 (ディスカバリ アルゴリズム、WLC 選択プロセス)
    - 3.3.d レイヤ 2 および Layer 3 の主要原則と使用事例の説明
    - 3.3.e WLAN のコンフィギュレーションおよびワイヤレス クライアントの接続に関する問題のトラブルシューティング
  - 3.4 IP サービス
    - 3.4.a NTP (Network Time Protocol) の説明
    - 3.4.b NAT/PAT の構成および確認
    - 3.4.c ファースト ホップ冗長プロトコル (HSRP および VRRP など) の構成
    - 3.4.d マルチキャスト プロトコル (PIM および IGMP v2/v3 など) の説明

- 10% 4.0 **ネットワークアシュアランス**
  - 4.1 デバッグ、条件付きデバッグ、トレース ルート、ping、SNMP、syslog などのツールを使用したネットワーク問題の診断
  - 4.2 syslog によるリモート ロギングを使用したデバイス監視の構成および確認
  - 4.3 NetFlow および Flexible NetFlow の構成および確認
  - 4.4 SPAN/RSPAN/ERSPAN の構成および確認
  - 4.5 IPSLA の構成および確認
  - 4.6 ネットワーク コンフィグレーション、モニタリング、および管理を適用するための Cisco DNA Center の作業フローの説明
  - 4.7 NETCONF および RESTCONF の構成および確認
  
- 20% 5.0 **セキュリティ**
  - 5.1 デバイス アクセス コントロールの構成および確認
    - 5.1.a ラインおよびパスワード保護
    - 5.1.b AAA を使用した認証と認可
  
  - 5.2 インフラストラクチャのセキュリティ機能の構成および確認
    - 5.2.a ACL
    - 5.2.b CoPP
  
  - 5.3 REST API のセキュリティ
  
  - 5.4 ワイヤレス セキュリティ機能の構成および確認
    - 5.4.a EAP
    - 5.4.b WebAuth
    - 5.4.c PSK
  
  - 5.5 ネットワーク セキュリティ デザインの構成要素の説明
    - 5.5.a 脅威防御
    - 5.5.b エンドポイント セキュリティ
    - 5.5.c 次世代 ファイアウォール
    - 5.5.d TrustSec、MACsec
    - 5.5.e 802.1X、MAB、および WebAuth を使用したネットワーク アクセス制御
  
- 15% 6.0 **自動化**
  - 6.1 Python の基本要素およびスクリプトの解釈
  - 6.2 有効な JSON エンコード ファイルの作成
  - 6.3 YANG などのデータ モデリング言語のハイレベルの原理と利点
  - 6.4 Cisco DNA Center および vManage の API の説明
  - 6.5 Cisco DNA Center および RESTCONF を使用したペイロード内の REST API のレスポンス コードおよび結果の解釈
  - 6.6 設定、トラブルシューティング、データ収集を自動化するための EEM アプレットの作成
  - 6.7 エージェントとエージェントレス オーケストレーション ツールの比較 (Chef、Puppet、Ansible、および SaltStack)