

ENCOR試験のマイナーアップデート (v1.1 ⇒ v1.2)

ENCOR試験マイナーアップデートの概要

350-401 ENCOR 試験は、**2026年3月19日より** ENCOR v1.2 にマイナーアップデートされます。

新バージョンでは無線LAN関連のコンテンツ削除、一部の製品名の最新化、マルチキャスト関連のコンテンツ追加などが予定されています。ENCOR v1.1は**2026年3月18日まで**受験可能です。

詳細はCisco社の公式ページをご参照ください。

<https://learningnetwork.cisco.com/s/encor-exam-topics>

試験範囲の比較

ENCOR v1.1 (2026/3/18まで)		ENCOR v1.2 (2026/3/19~)	
1.0 アーキテクチャ (15%)		1.0 アーキテクチャ (15%)	
1.1	エンタープライズネットワークにおける設計原則を説明する	1.1	エンタープライズネットワークにおける設計原則を説明する
1.1.a	2層、3層、ファブリック、クラウドなどの高レベル設計	1.1.a	2層、3層、ファブリック、クラウドなどの高レベル設計
1.1.b	冗長化、FHRP、SSOなどの高可用性技術	1.1.b	冗長化、FHRP、SSOなどの高可用性技術
1.2	無線ネットワーク設計の原則を説明する	1.2 無線ネットワーク設計の原則を説明する を削除	
1.2.a	無線展開モデル（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、リモートプランチ）	1.2.a	SD-WANの制御プレーンとデータプレーン要素
1.2.b	WLAN設計における位置情報サービス	1.2.b	Catalyst SD-WANソリューションの利点と制限
1.2.c	クライアント密度	1.3	Cisco SD-Accessソリューションの動作原理を説明する
1.3	Cisco SD-WANソリューションの動作原理を説明する	1.3.a	SD-Accessの制御プレーンとデータプレーン要素
1.3.a	SD-WANの制御プレーンとデータプレーン要素	1.3.b	SD-WANソリューションの利点と制限
1.4	Cisco SD-Accessソリューションの動作原理を説明する	1.4	QoS設定を理解する（「有線および無線」の記載を削除）
1.4.a	SD-Accessの制御プレーンとデータプレーン要素	1.4.a	QoSの詳細な項目は記載なし
1.4.b	従来型キャンバスとSD-Accessの相互運用	1.6 CEF、CAM、TCAM、FIB、RIB、隣接テーブルなどのハードウェア・ソフトウェアスイッチング機構を説明する を削除	
1.5	有線および無線のQoS設定を理解する	2.0 仮想化 (10%)	
1.5.a	QoSの構成要素	2.1	デバイス仮想化技術を説明する
1.5.b	QoSポリシー	2.1.a	ハイパーバイザタイプ1と2
1.6	CEF、CAM、TCAM、FIB、RIB、隣接テーブルなどのハードウェア・ソフトウェアスイッチング機構を説明する	2.1.b	仮想マシン
2.0 仮想化 (10%)		2.1.c	仮想スイッチング
2.1	デバイス仮想化技術を説明する	2.2	データバス仮想化技術を設定および検証する
2.1.a	ハイパーバイザタイプ1と2	2.2.a	VRF
2.1.b	仮想マシン	2.2.b	GREとIPsecトンネリング
2.1.c	仮想スイッチング	2.3	ネットワーク仮想化の概念を説明する
2.2	データバス仮想化技術を設定および検証する	2.3.a	LISP
2.2.a	VRF	2.3.b	VXLAN
2.3	ネットワーク仮想化の概念を説明する	3.0 インフラストラクチャ (30%)	
2.3.a	LISP	3.1	レイヤ2
2.3.b	VXLAN	3.1.a	静的および動的802.1qトランクのトラブルシュート
3.0 インフラストラクチャ (30%)		3.1.b	静的および動的イーサチャネルのトラブルシュート
3.1	レイヤ2	3.1.c	RSTP、MSTなどのスパニングツリープロトコルとroot guardやBPDU guardなどの拡張機能を設定、検証する
3.1.a	静的および動的802.1qトランクのトラブルシュート	3.2	レイヤ3
3.1.b	静的および動的イーサチャネルのトラブルシュート	3.2.a	EIGRPとOSPFのルーティング概念を比較（ディスタンスペクター、リンクステート、負荷分散、経路選択、経路操作、メトリック、エリアタイプ）
3.1.c	RSTP、MSTなどのスパニングツリープロトコルとroot guardやBPDU guardなどの拡張機能を設定、検証する	3.2.b	OSPFv2/v3のシンプルな環境を設定（複数の通常エリア、集約、フィルタリング、隣接関係、ポイントツーポイント、ブロードキャストネットワークタイプ、パッシブインターフェース）
3.2	レイヤ3	3.2.c	直接接続されたネイバー間でのeBGPを設定・検証する（ベストパス選択アルゴリズム、隣接関係）
3.2.a	EIGRPとOSPFのルーティング概念を比較（ディスタンスペクター、リンクステート、負荷分散、経路選択、経路操作、メトリック、エリアタイプ）	3.2.d	ポリシーベースルーティングを説明する
3.2.b	OSPFv2/v3のシンプルな環境を設定（複数の通常エリア、集約、フィルタリング、隣接関係、ポイントツーポイント、ブロードキャストネットワークタイプ、パッシブインターフェース）	3.3 無線 を削除	
3.2.c	直接接続されたネイバー間でのeBGPを設定・検証する（ベストパス選択アルゴリズム、隣接関係）	3.3	IPサービス
3.2.d	ポリシーベースルーティングを説明する	3.3.a	NTPやPTPなどの時刻同期プロトコルの設定を理解する
3.3	無線	3.3.b	NAT/PATを設定する
3.3.a	レイヤ1の概念（RFパワー、RSSI、SNR、干渉、ノイズ、バンド、チャネル、クライアント末端の能力）	3.3.c	HSRP、VRRPなどのファーストホップ冗長プロトコルを設定する
3.3.b	APモードとアンテナタイプを説明する	3.3.d	マルチキャストプロトコル（RPFチェック、PIM、IGMP v2/v3）を説明する
3.3.c	APの検出と参加プロセス（検出アルゴリズム、WLC選択プロセス）	3.3 無線 を説明する	
3.3.d	レイヤ2およびレイヤ3ローミングの原則とユースケース	Copyright © CTC Technology Corporation All rights reserved.	
3.3.e	GUIを使用したWLAN構成およびクライアント接続問題のトラブルシュート		
3.3.f	グループ、プロファイル、タグによる無線セグメンテーション		
3.4	IPサービス		
3.4.a	NTPやPTPなどの時刻同期プロトコルの設定を理解する		
3.4.b	NAT/PATを設定する		
3.4.c	HSRP、VRRPなどのファーストホップ冗長プロトコルを設定する		
3.4.d	マルチキャストプロトコル（RPFチェック、PIM-SM、IGMP v2/v3、SSM、bidir、MSDP）を説明する		

ENCOR試験のマイナーアップデート (v1.1 ⇒ v1.2)

4.0 ネットワークアシュアランス (10%)		4.0 ネットワークアシュアランス (10%)	
4.1	debug、条件付きdebug、traceroute、ping、SNMP、syslogを使ったネットワーク問題の診断	4.1	debug、条件付きdebug、traceroute、ping、SNMP、syslogを使ったネットワーク問題の診断
4.2	Flexible NetFlowを設定・検証する	4.2	Flexible NetFlowを設定・検証する
4.3	SPAN/RSPAN/ERSPANを設定する	4.3	SPAN/RSPAN/ERSPANを設定する
4.4	IPSLAを設定・検証する	4.4	IPSLAを設定・検証する
4.5	Cisco DNA Centerワークフローを用いた構成・監視・管理	4.5	Cisco Catalyst Center (旧Cisco DNA Center) を用いて従来型およびAIワークフローで構成・監視・管理を行う方法を説明する
4.6	NETCONFとRESTCONFを設定・検証する	4.6	NETCONFとRESTCONFを設定・検証する
5.0 セキュリティ (20%)		5.0 セキュリティ (20%)	
5.1	デバイスアクセス制御を設定・検証する	5.1	デバイスアクセス制御を設定・検証する
5.1.a	ラインおよびローカルユーザ認証	5.1.a	ラインおよびローカルユーザ認証
5.1.b	AAAによる認証・認可	5.1.b	AAAによる認証・認可
5.2	インフラストラクチャセキュリティ機能を設定・検証する	5.2	インフラストラクチャセキュリティ機能を設定・検証する
5.2.a	ACL	5.2.a	ACL
5.2.b	CoPP	5.2.b	CoPP
5.3	REST APIセキュリティを説明する	5.3	REST APIセキュリティを説明する
5.4	無線セキュリティ機能を設定・検証する	「5.4 無線セキュリティ機能を設定・検証する」を削除	
5.4.a	802.1X	5.4.a	脅威防御
5.4.b	WebAuth	5.4.b	エンドポイントセキュリティ
5.4.c	PSK	5.4.c	次世代ファイアウォール
5.4.d	EAPOL (4ウェイハンドシェイク)	5.4.d	TrustSecとMACsec
5.5	ネットワークセキュリティ設計の要素を説明する	5.4	ネットワークセキュリティ設計の要素を説明する
5.5.a	脅威防御	5.4.a	脅威防御
5.5.b	エンドポイントセキュリティ	5.4.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	5.4.c	次世代ファイアウォール
5.5.d	TrustSecとMACsec	5.4.d	TrustSecとMACsec
5.5.e	802.1X、MAB、WebAuthによるネットワークアクセス制御	「5.5.e 802.1X、MAB、WebAuthによるネットワークアクセス制御」を削除	
6.0 自動化 (15%)		6.0 自動化と人工知能 (AI) (15%)	
6.1	Pythonの基本要素とスクリプトを理解する	6.1	Pythonの基本要素とスクリプトを理解する
6.2	JSON形式のファイルを作成する	6.2	JSON形式のファイルを作成する
6.3	YANGなどのデータモデリング言語の原則と利点を説明する	6.3	YANGなどのデータモデリング言語の原則と利点を説明する
6.4	Cisco DNA CenterおよびvManageのAPIを説明する	6.4	Cisco Catalyst CenterおよびSD-WAN ManagerのAPIを説明する
6.5	Cisco DNA CenterおよびRESTCONFを使用したREST APIレスポンスコードとペイロードの理解	6.5	Cisco Catalyst CenterおよびRESTCONFを使用したREST APIレスポンスコードとペイロードの理解
6.6	設定、トラブルシュート、データ収集を自動化するEEMアプレットを作成する	6.6	設定、トラブルシュート、データ収集を自動化するEEMアプレットを作成する
6.7	Chef、Puppet、Ansible、SaltStackなどのエージェント型とエージェントレス型のオーケストレーションツールを比較する	6.7	エージェント型とエージェントレス型のオーケストレーションツールを比較する (「Chef、Puppet、Ansible、SaltStackなどの」の記載を削除)