Implementing Cisco Network Security（210-260）

試験の内容：Implementing Cisco Network Security（IINS）試験（210-260）は、制限時間 90 分、出題数 60–70 問で実施されます。この試験では、セキュアなネットワーク インフラストラクチャ、セキュリティの中心概念の理解、セキュアなアクセスの管理、VPN 暗号化、ファイアウォール、侵入防御、Web と電子メールのコンテンツ セキュリティ、およびエンドポイント セキュリティに関する受験者の知識をテストします。また、データやデバイスの完全性、機密性、および可用性を維持するためのセキュアなネットワークのインストール、トラブルシューティング、および監視に関するスキルを評価します。さらに、シスコのセキュリティ インフラストラクチャで使用されているテクノロジーに関する能力も査定します。受験者は、受験準備として Implementing Cisco Network Security（IINS）コースを受講できます。

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分野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　セキュリティの概念

- 1.1 一般的なセキュリティ原則
  - 1.1.a 機密性、完全性、および可用性（CIA）の説明
  - 1.1.b SIEM テクノロジーの説明
  - 1.1.c 一般的なセキュリティ用語の特定
  - 1.1.d 一般的なネットワーク セキュリティ ゾーンの特定
- 1.2 一般的なセキュリティ脅威
  - 1.2.a 一般的なネットワーク攻撃の特定
  - 1.2.b ソーシャル エンジニアリングの説明
  - 1.2.c マルウェアの特定
  - 1.2.d データ損失/漏洩のベクトルの分類
- 1.3 暗号化の概念
  - 1.3.a キー交換の説明
  - 1.3.b ハッシュ アルゴリズムの説明
  - 1.3.c 対称/非対称暗号化の比較対照
  - 1.3.d デジタル署名、証明書、および PKI の説明
- 1.4 ネットワークトポロジの説明
  - 1.4.a キャンパス エリア ネットワーク（CAN）
  - 1.4.b クラウド、ワイド エリア ネットワーク（WAN）
  - 1.4.c データセンター
  - 1.4.d スモール オフィス/ホーム オフィス（SOHO）
  - 1.4.e 仮想環境のネットワーク セキュリティ

14% **2.0** **セキュアなアクセス**

2.1 セキュアな管理

- 2.1.a 帯域内と帯域外の比較
- 2.1.b セキュアなネットワーク管理の設定
- 2.1.c ACL を使用した SNMP v3 経由のセキュア アクセスの設定と検証
- 2.1.d NTP のセキュリティの設定と検証
- 2.1.e ファイル転送での SCP の使用

2.2 AAA の概念

- 2.2.a RADIUS テクノロジーと TACACS+ テクノロジーの説明
- 2.2.b TACACS+ を使用したシスコ ルータ上での管理アクセスの設定
- 2.2.c シスコ ルータでの TACACS+ サーバ接続の検証
- 2.2.d Active Directory と AAA の統合の説明
- 2.2.e ACS と ISE を使用した認証と許可の説明

2.3 802.1X 認証

- 2.3.a 802.1X コンポーネントの機能の特定

2.4 BYOD

- 2.4.a BYOD アーキテクチャ フレームワークの説明
- 2.4.b モバイル デバイス管理（MDM）の機能の説明

17% **3.0** **VPN**

3.1 VPN の概念

- 3.1.a IPsec プロトコルとデリバリ モード（IKE、ESP、AH、トンネル モード、トランスポート モード）の説明
- 3.1.b ヘアピニング、スプリット トンネリング、Always-On、NAT トラバーサルの説明

3.2 リモート アクセス VPN

- 3.2.a ASDM を使用した基本的なクライアントレス SSL VPN の実装
- 3.2.b クライアントレス接続の検証
- 3.2.c ASDM を使用した基本的な AnyConnect SSL VPN の実装
- 3.2.d AnyConnect 接続の検証
- 3.2.e エンドポイント ポスチャ アセスメントの特定

3.3 サイト間 VPN

- 3.3.a シスコ ルータと ASA ファイアウォール上での事前共有キー認証を使用した IPsec サイト間 VPN の実装
- 3.3.b IPsec サイト間 VPN の検証

18% **4.0** **セキュアなルーティングとスイッチング**

4.1 シスコ ルータのセキュリティ

- 4.1.a 複数の特権レベルの設定
- 4.1.b Cisco IOS ロールベースの CLI アクセスの設定
- 4.1.c Cisco IOS Resilient Configuration の実装

4.2 ルーティング プロトコルの保護
- 4.2.a OSPF でのルーティング アップデート認証の実装

4.3 コントロール プレーンの保護
- 4.3.a コントロール プレーン ポリシングの機能の説明

4.4 一般的なレイヤ 2 攻撃
- 4.4.a STP 攻撃の説明
- 4.4.b ARP スプーフィングの説明
- 4.4.c MAC スプーフィングの説明
- 4.4.d CAM テーブル（MAC アドレス テーブル）オーバーフローの説明
- 4.4.e CDP/LLDP 予備調査の説明
- 4.4.f VLAN ホッピングの説明
- 4.4.g DHCP スプーフィングの説明

4.5 軽減手順
- 4.5.a DHCP スヌーピングの実装
- 4.5.b ダイナミック ARP インスペクションの実装
- 4.5.c ポート セキュリティの実装
- 4.5.d BPDU ガード、ルート ガード、ループ ガードの説明
- 4.5.e 軽減手順の検証

4.6 VLAN セキュリティ
- 4.6.a PVLAN のセキュリティの影響の説明
- 4.6.b ネイティブ VLAN のセキュリティの影響の説明

18% 5.0 シスコ ファイアウォール テクノロジー

5.1 さまざまなファイアウォール テクノロジーの運用上の長所と短所の説明
- 5.1.a プロキシ ファイアウォール
- 5.1.b アプリケーション ファイアウォール
- 5.1.c パーソナル ファイアウォール

5.2 ステートフル ファイアウォールとステートレス ファイアウォールの比較
- 5.2.a 運用
- 5.2.b ステート テーブルの機能

5.3 Cisco ASA 9.x での NAT の実装
- 5.3.a 静的
- 5.3.b 動的
- 5.3.c PAT
- 5.3.d ポリシー NAT
- 5.3.e NAT 運用の検証

5.4 ゾーンベース ファイアウォールの実装
- 5.4.a ゾーン間
- 5.4.b セルフ ゾーン

5.5 Cisco 適応型セキュリティ アプライアンス（ASA）9.x のファイアウォール機能
- 5.5.a ASA アクセス管理の設定
- 5.5.b セキュリティ アクセス ポリシーの設定
- 5.5.c Cisco ASA インターフェイス セキュリティ レベルの設定
- 5.5.d デフォルト Cisco モジュラ ポリシー フレームワーク（MPF）の設定
- 5.5.e 展開モード（ルーテッド ファイアウォール、トランスペアレント ファイアウォール）の説明
- 5.5.f 高可用性の実装方法の説明
- 5.5.g セキュリティ コンテキストの説明
- 5.5.h ファイアウォール サービスの説明

9% 6.0 IPS

6.1 IPS 展開の留意点の説明
- 6.1.a ネットワークベース IPS とホストベース IPS の比較
- 6.1.b 展開モード（インライン、プロミスキャス - SPAN、TAP）
- 6.1.c 配置（ネットワーク内での IPS の位置付け）
- 6.1.d false positive、false negative、true positive、true negative

6.2 IPS テクノロジーの説明
- 6.2.a ルール/署名
- 6.2.b 検出/署名エンジン
- 6.2.c トリガー アクション/応答（ドロップ、リセット、ブロック、アラート、モニタ/ログ、回避）
- 6.2.d ブラックリスト（静的および動的）

12% 7.0 コンテンツとエンドポイントのセキュリティ

7.1 電子メール ベースの脅威に対する軽減テクノロジーの説明
- 7.1.a SPAM フィルタリング、マルウェア対策フィルタリング、DLP、ブラックリスト化、電子メール暗号化

7.2 Web ベースの脅威に対する軽減テクノロジーの説明
- 7.2.a ローカルおよびクラウドベースの Web プロキシ
- 7.2.b ブラックリスト化、URL フィルタリング、マルウェア スキャン、URL カテゴリ化、Web アプリケーション フィルタリング、TLS/SSL 復号化

7.3 エンドポイントの脅威に対する軽減テクノロジーの説明
- 7.3.a ウイルス対策/マルウェア対策
- 7.3.b パーソナル ファイアウォール/HIPS
- 7.3.c ローカル データのハードウェア/ソフトウェア暗号化