Implementing Cisco Secure Access Solutions（300-208）

試験の説明：300-208 Implementing Cisco Secure Access Solutions（SISAS）は、802.1X および Cisco TrustSec を利用してセキュアなアクセスを実現するためのコンポーネントやアーキテクチャに関する、ネットワーク セキュリティ エンジニア向けの試験です。この 90 分の試験（65 ～ 75 問）では、ネットワーク脅威緩和全般とエンドポイント管理ソリューションとしての Cisco Identity Services Engine（ISE）のアーキテクチャ、ソリューション、コンポーネントの知識が評価されます。また、ISE のポスチャおよびプロファイリング サービスを使用した個人所有デバイス持ち込み（BYOD）の基本概念についても出題されます。受験者は、受験準備として Implementing Cisco Secure Access Solutions（SISAS）コースを受講できます。

試験は参考書持ち込み不可であり、いかなる外部の参考資料の使用も認められません。

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させ、明確にするために、次のガイドラインは事前の通告なく変更されることがあります。

33 %　1.0　アイデンティティ管理とセキュアなアクセス

- 1.1 デバイス管理の実装
  - 1.1.a AAA オプションの比較と選択
  - 1.1.b TACACS+
  - 1.1.c RADIUS
  - 1.1.d ネイティブ AD と LDAP の説明
- 1.2 アイデンティティ管理の説明
  - 1.2.a 認証/認可の特徴と機能の説明
  - 1.2.b 認証情報ストア オプションの説明（LDAP、AD、PKI、OTP、スマート カード、ローカルなど）
  - 1.2.c アカウンティングの実装
- 1.3 有線/ワイヤレス 802.1X の実装
  - 1.3.a RADIUS フローの説明
  - 1.3.b AV ペア
  - 1.3.c EAP タイプ
  - 1.3.d サプリカント、オーセンティケータ、サーバの説明
  - 1.3.e サプリカント オプション
  - 1.3.f 802.1X フェーズ（モニタ モード、ロー インパクト、クローズド モード）
  - 1.3.g AAA サーバ
  - 1.3.h ネットワーク アクセス デバイス
- 1.4 MAB の実装
  - 1.4.a 802.1X フレームワーク内の MAB プロセスの説明
  - 1.4.b 柔軟な認証設定

- 1.4.c ISE 認証/認可ポリシー
- 1.4.d ISE エンドポイント アイデンティティ設定
- 1.4.e MAB の運用の確認

1.5 ネットワーク認可処理の実装
- 1.5.a dACL
- 1.5.b ダイナミック VLAN 割り当て
- 1.5.c SGA の説明
- 1.5.d 名前付き ACL
- 1.5.e CoA

1.6 中央集中型 Web 認証（CWA）の実装
- 1.6.a Web 認証をサポートする CoA の機能の説明
- 1.6.b CWA を容易にするための認証ポリシーの設定
- 1.6.c URL リダイレクト ポリシー
- 1.6.d リダイレクト ACL
- 1.6.e Web ポータルのカスタマイズ
- 1.6.f 中央集中型 Web 認証運用の確認

1.7 プロファイリングの実装
- 1.7.a プロファイリング サービスの有効化
- 1.7.b ネットワーク プローブ
- 1.7.c IOS デバイス センサー
- 1.7.d フィード サービス
- 1.7.e プロファイリング ポリシー ルール
- 1.7.f 認可ポリシーでのプロファイル割り当ての利用
- 1.7.g プロファイリングの運用の確認

1.8 ゲスト サービスの実装
- 1.8.a スポンサー アカウントの管理
- 1.8.b スポンサー ポータル
- 1.8.c ゲスト ポータル
- 1.8.d ゲスト ポリシー
- 1.8.e 自己登録
- 1.8.f ゲストの有効化
- 1.8.g セキュアなアクセスの差別化
- 1.8.h ゲスト サービスの運用の確認

1.9 ポスチャリングの実装
- 1.9.a ポスチャリングをサポートする CoA の機能の説明
- 1.9.b エージェント オプション
- 1.9.c クライアント プロビジョニング ポリシーとリダイレクト ACL
- 1.9.d ポスチャ ポリシー
- 1.9.e 検疫/修復

1.9.f ポスチャリングの運用の確認

1.10 BYOD アクセスの実装
- 1.10.a BYOD ポリシーの要素の説明
- 1.10.b デバイスの登録
- 1.10.c My devices portal
- 1.10.d サプリカント プロビジョニングの説明

10 % 2.0 脅威に対する防御

2.1 TrustSec アーキテクチャの説明
- 2.1.a SGT の分類 – ダイナミック/スタティック
- 2.1.b SGT のトランスポート – インライン タギングと SXP
- 2.1.c SGT の適用 – SGACL と SGFW
- 2.1.d MACsec

7 % 3.0 トラブルシューティング ツール、監視ツールおよびレポート ツール

3.1 アイデンティティ管理ソリューションのトラブルシューティング
- 3.1.a Cisco ISE での認証イベント詳細を使用した問題の特定
- 3.1.b Cisco ISE 診断ツールを使用したトラブルシューティング
- 3.1.c エンドポイント問題のトラブルシューティング
- 3.1.d debug コマンドを使用した IOS スイッチおよびワイヤレス コントローラ上の RADIUS と 802.1X のトラブルシューティング
- 3.1.e バックアップ操作のトラブルシューティング

17 % 4.0 脅威に対する防御を実現するアーキテクチャ

4.1 ISE によるセキュアなワイヤレス ソリューションの設計
- 4.1.a アイデンティティ管理
- 4.1.b 802.1X
- 4.1.c MAB
- 4.1.d ネットワーク認可処理
- 4.1.e CWA
- 4.1.f プロファイリング
- 4.1.g ゲスト サービス
- 4.1.h ポスチャリング
- 4.1.i BYOD アクセス

33 % 5.0 アイデンティティ管理アーキテクチャの設計

5.1 デバイス管理
5.2 アイデンティティ管理
5.3 プロファイリング
5.4 ゲスト サービス
5.5 ポスチャリング サービス
5.6 BYOD アクセス