Implementing Cisco Threat Control Solutions（300-210）

試験の説明：300-210 Implementing Cisco Threat Control Solutions（SITCS）は、CCNP Security 認定試験の一つです。アクセス ポリシーとアイデンティティ ポリシーを利用するシスコ次世代ファイアウォールの高度なファイアウォールのアーキテクチャと構成に関して、ネットワーク セキュリティ エンジニアの知識が評価されます。この新しいリビジョンの SITCS 試験は 300-207 に代わるものであり、対象範囲から一部の古いテクノロジーが除外され、Cisco FirePOWER NGIPS と Cisco AMP（Advanced Malware Protection）の両方が追加されています。この 90 分の試験（65 ～ 75 問）では、侵入防御システム（IPS）とコンテキスト認識型ファイアウォールのコンポーネントの統合のほか、Web（クラウド）および E メールのセキュリティ ソリューションに関する受験者の知識が評価されます。受験者は、受験準備として Implementing Cisco Threat Control Solutions（SITCS）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。

27 %　1.0　コンテンツ セキュリティ

- 1.1 Cisco クラウド Web セキュリティ（CWS）
  - 1.1.a 特徴と機能の説明
  - 1.1.b IOS および ASA コネクタの実装
  - 1.1.c Cisco AnyConnect Web セキュリティ モジュールの実装
  - 1.1.d Web 利用の制御の実装
  - 1.1.e AVC の実装
  - 1.1.f マルウェア対策の実装
  - 1.1.g 復号ポリシーの実装
- 1.2 Cisco Web セキュリティ アプライアンス（WSA）
  - 1.2.a 特徴と機能の説明
  - 1.2.b データ セキュリティの実装
  - 1.2.c トランスペアレント ユーザ識別を含む、WSA アイデンティティと認証の実装
  - 1.2.d Web 利用の制御の実装
  - 1.2.e AVC の実装
  - 1.2.f マルウェア対策と AMP の実装
  - 1.2.g 復号ポリシーの実装
  - 1.2.h トラフィック リダイレクトとキャプチャ方式（明示的なプロキシと透過的なプロキシ）の実装
- 1.3 Cisco E メール セキュリティ アプライアンス
  - 1.3.a 特徴と機能の説明
  - 1.3.b 電子メール暗号化の実装
  - 1.3.c スパム対策ポリシーの実装
  - 1.3.d ウイルス感染フィルタの実装
  - 1.3.e DLP ポリシーの実装

1.3.f マルウェア対策と AMP の実装
1.3.g インバウンド/アウトバウンド メール ポリシーと認証の実装
1.3.h トラフィック リダイレクトとキャプチャ方式の実装
1.3.i メッセージ トラッキングのための ESA GUI の実装

22 % 2.0 ネットワークの脅威に対する防御

2.1 シスコ次世代ファイアウォール（NGFW）セキュリティ サービス
2.1.a アプリケーション認識の実装
2.1.b アクセス制御ポリシーの実装（URL フィルタリング、レピュテーションに基づくファイル フィルタリング）
2.1.c トラフィック リダイレクトの設定と確認
2.1.d Cisco AMP for Networks の実装

2.2 Cisco Advanced Malware Protection（AMP）
2.2.a クラウド検出テクノロジーの説明
2.2.b AMP アーキテクチャ（パブリック クラウド、プライベート クラウド）の比較対照
2.2.c AMP エンドポイントの導入の設定
2.2.d 分析ツールの説明
2.2.e インシデント対応機能の説明
2.2.f サンドボックス分析の説明
2.2.g AMP の統合の説明

20 % 3.0 Cisco FirePOWER 次世代 IPS（NGIPS）

3.1 構成

3.2 トラフィック リダイレクトとキャプチャ方式の説明
3.2.a プリプロセッサと検出エンジンの説明
3.2.b イベント アクションと抑制しきい値の実装
3.2.c 相関ポリシーの実装
3.2.d SNORT ルールの説明
3.2.e SSL 復号ポリシーの実装

3.3 導入
3.3.a インラインまたはパッシブの導入
3.3.b ASA 内のアプライアンス、仮想アプライアンス、またはモジュールとしての NGIPS の導入
3.3.c シンメトリックなトラフィックの必要性に関する説明
3.3.d インライン モードの比較：インライン インターフェイス ペアとインライン タップ モード

17 % 4.0 セキュリティ アーキテクチャ

4.1 Web セキュリティ ソリューションの設計
4.1.a Cisco FirePOWER NGFW、WSA、および CWS の比較対照
4.1.b 物理 WSA と仮想 WSA の比較対照

4.1.c 使用可能な CWS コネクタの説明

4.2 電子メール セキュリティ ソリューションの設計
- 4.2.a 物理 ESA と仮想 ESA の比較対照
- 4.2.b ハイブリッド モードの説明

4.3 Cisco FirePOWER ソリューションの設計
- 4.3.a 仮想ルーテッド インターフェイス、スイッチド インターフェイス、およびハイブリッド インターフェイスの設定
- 4.3.b 物理ルーテッド インターフェイスの設定

14 % 5.0 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

5.1 Web セキュリティ ソリューションの設計
- 5.1.a FirePOWER NGFW、WSA、および CWS の比較対照
- 5.1.b 物理 WSA と仮想 WSA の比較対照
- 5.1.c 使用可能な CWS コネクタの説明

5.2 Cisco Web セキュリティ アプライアンス（WSA）
- 5.2.a WSA ポリシー トレース ツールの実装
- 5.2.b WSA レポート作成機能の説明
- 5.2.c CLI ツールを使用したトラブルシューティング

5.3 Cisco E メール セキュリティ アプライアンス（ESA）
- 5.3.a ESA ポリシー トレース ツールの実装
- 5.3.b ESA レポート作成機能の説明
- 5.3.c CLI ツールを使用したトラブルシューティング

5.4 Cisco FirePOWER
- 5.4.a Cisco FirePOWER Management Center のダッシュボードとレポートの説明
- 5.4.b 正常性ポリシーの実装
- 5.4.c 電子メール、SNMP、および syslog アラートの設定
- 5.4.d CLI ツールを使用した NGIPS のトラブルシューティング