Securing the Web with Cisco Web Security Appliance v1.0（300-725）

試験概要：Securing the Web with Cisco Web Security Appliance v1.0（SWSA 300-725）は、CCNP Security 認定に関する試験であり、試験時間は 90 分です。この試験では、プロキシ サービス、認証、復号化のポリシー、差別化されたトラフィック アクセス ポリシーおよびアイデンティティ プロファイル、使用許可コントロールの設定、マルウェア防御、データ セキュリティおよびデータ損失の防止など、Cisco Web Security Appliance 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、Securing Web with Cisco Email Security Appliance 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。

10% **1.0** **Cisco WSA の特徴**

- 1.1 Cisco WSA の特徴および機能の説明
  - 1.1.a プロキシ サービス
  - 1.1.b Cisco Cognitive Threat Analytics
  - 1.1.c データ損失防止サービス
  - 1.1.d 内蔵 L4TM サービス
  - 1.1.e 管理ツール
- 1.2 WSA ソリューションの説明
  - 1.2.a Cisco Advanced Web Security Reporting
  - 1.2.b Cisco Content Security Management Appliance
- 1.3 Cisco WSA と Splunk の統合
- 1.4 Cisco WSA と Cisco ISE の統合
- 1.5 データ セキュリティおよび外部データ損失のトラブルシューティング（ログ ファイルを使用）

20% **2.0** **コンフィグレーション**

- 2.1 Cisco WSA での初期コンフィグレーション タスクの実行
- 2.2 使用許可ポリシーの構成

2.3 Web プロキシ機能の構成および確認
- 2.3.a 明示的プロキシの機能
- 2.3.b CLI を使用したプロキシ アクセス ログ
- 2.3.c アクティブ ディレクトリのプロキシ認証

2.4 Referer ヘッダの構成による Web カテゴリのフィルタリング

10% 3.0 プロキシ サービス

3.1 プロキシ用語の比較
- 3.1.a 明示的プロキシと透過プロキシ
- 3.1.b アップストリーム プロキシとダウンストリーム プロキシ

3.2 キャッシングの調整による動作の違いの説明（安全性または性能）

3.3 PAC（Proxy Auto-Configuration）ファイルの機能の説明

3.4 SOCKS プロトコルおよび SOCKS プロキシ サービスの説明

10% 4.0 認証

4.1 認証機能の説明
- 4.1.a サポートされる認証プロトコル
- 4.1.b 認証のレルム
- 4.1.c サポートされる認証サロゲート
- 4.1.d 問題のあるエージェントの認証のバイパス
- 4.1.e アカウンティング レコードのための認証ログ
- 4.1.f 再認証

4.2 Cisco WSA へのトラフィック リダイレクションの構成（明示的転送プロキシ モードを使用）

4.3 FTP プロキシ認証の説明

4.4 認証に関する問題のトラブルシューティング

10% 5.0 復号化ポリシーによる HTTPS トラフィックの制御

5.1 SSL および TLS 検査の説明

5.2 HTTPS 機能の構成
- 5.2.a HTTPS 復号化 ポリシー
- 5.2.b HTTPS プロキシ機能
- 5.2.c ACL タグ による HTTPS 検査
- 5.2.d HTTPS プロキシおよび TLS/SSL 復号化の検査

5.3 HTTPS 復号化に使用される認証タイプ

5.4 SSL/TLS トランザクション内での自己証明書および中間証明書の構成

10% **6.0** **差別化されたトラフィック アクセス ポリシーおよびアイデンティティ プロファイル**

- 6.1 アクセス ポリシーの説明
- 6.2 アイデンティティ プロファイルおよび認証の説明
- 6.3 アクセス ログを使用したトラブルシューティング

10% **7.0** **使用許可コントロール**

- 7.1 URL フィルタリングの構成
- 7.2 動的コンテンツ分析エンジンの構成
- 7.3 時間ベースおよびトラフィック量に基づく使用許可のポリシーおよびエンド ユーザ通知の構成
- 7.4 Web アプリケーションの可視性およびコントロールの構成（Office 365、サードパーティ フィード）
- 7.5 全社レベルの使用許可ポリシーの作成
- 7.6 ポリシー トレース ツールの実装による全社レベルの使用許可ポリシーの検証
- 7.7 WSA のコンフィグレーションによるアーカイブ ファイル タイプの検査

10% **8.0** **マルウェア防御**

- 8.1 アンチマルウェア スキャニングの説明
- 8.2 ファイル レピュテーション フィルタイリングおよびファイル分析の構成
- 8.3 AMP（Advanced Malware Protection）の説明
- 8.4 Cognitive Threat Analytics との統合の説明

10% **9.0** **Web トランザクションのレポーティングおよびトラッキング**

- 9.1 Web トラッキング レポートの構成および分析
- 9.2 Cisco Advanced Web Security Reporting（AWSR）の構成
  - 9.2.a 基本的な Web の使用
  - 9.2.b カスタム フィルタ
- 9.3 接続問題のトラブルシューティング