Securing Email with Cisco Email Security Appliance v1.0（300-720）

試験概要：Securing Email with Cisco Email Security Appliance v1.0（SESA 300-720）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、アドミニストレーション、スパム コントロールおよびアンチスパム、メッセージ フィルタ、データ損失の防止、LDAP、電子メール認証および暗号化、システム検疫および配信方式など、Cisco Email 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 Email 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。

15%　1.0　Cisco Email Security Appliance のアドミニストレーション

1.1. Cisco Email Security Appliance の機能の構成
- 1.1.a ハードウェア性能に関する仕様
- 1.1.b 初期設定のプロセス
- 1.1.c ルーティングおよび配布機能
- 1.1.d GUI

1.2. Cisco Content SMA の集中型サービスの説明

1.3. メール ポリシーの構成
- 1.3.a. 受信および送信メッセージ
- 1.3.b. ユーザ マッチング
- 1.3.c. メッセージの分化

15%　2.0　Talos SenderBase によるスパム コントロールとアンチスパム

2.1 Talos SenderBase によるスパムのコントロールと アンチスパム
2.2 グレイメール管理ソリューションの説明
2.3 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機能の構成
2.4 悪意のある URL または望ましくない URL からの保護の実装
2.5 バウンス検証機能の説明

20%　3.0　コンテンツおよびメッセージ フィルタ

3.1 コンテンツ フィルタの機能および特徴の説明

3.2 テキスト リソースの作成（コンテンツ辞書、免責事項、およびテンプレートなど）
- 3.2.a 辞書のフィルタ ルール

3.2.b テキスト リソース管理

3.3 メッセージ フィルタの構成要素、ルール、処理順序、および添付ファイル スキャニングの構成

3.4 スキャンの動作の構成

3.5 Cisco ESA での Sophos および McAfee スキャニング エンジンを使用したウイルス スキャンの構成

3.6 アウトブレイク フィルタの構成

3.7 DLP（Data Loss Prevention）の構成

15% 4.0 LDAP および SMTP のセッション

4.1 LDAP サーバおよびクエリの構成および確認（クエリおよびディレクトリ ハーベスト攻撃）

4.2 スパム検疫機能

4.2.a スパム検疫機能におけるエンドユーザの認証

4.2.b スパム検疫エイリアスを利用したクエリの統合

4.3 SMTP の機能

4.3.a 電子メール パイプライン

4.3.b 送信者と受信者のドメイン

4.3.c クライアントの証明書を使用した SMTP セッションの認証

4.3.d SMTP TLS による認証

4.3.e TLS による電子メールの暗号化

20% 5.0 電子メール認証および暗号化

5.1 ドメイン キーおよび DKIM 署名の構成

5.2 SPF および SIDF の構成

5.3 DMARC 検証の構成

5.4 偽装メール検出機能の構成

5.5 電子メールの暗号化の構成

5.6 S/MIME セキュリティ サービスおよび他の MTA を使用した通信暗号化の説明

5.7 CA 証明書の管理

15% 6.0 システムの検疫および配信方式

6.1 検疫の構成（スパム、ポリシー、ウイルス、アウトブレイク）

6.2 セーフリストおよびブロックリストの利用による電子メール配信制御

6.3 ローカルまたは外部スパム検疫のメッセージの管理

6.4 仮想ゲートウェイの構成