概要

Cisco Registered Envelope Service（CRES）は、Cisco 暗号化テクノロジーをサポートするホストサービスです。CRES は Cisco E メール セキュリティ アプライアンスおよび Cisco 暗号化アプライアンスと併用して、オンプレミス コンテンツ スキャン、ポリシー適用、暗号化を提供します。CRESはメッセージごとに暗号化されたメッセージの暗号キーを保存します。暗号化メッセージの受信者は、復号化キーを受信するサービスを使って自分自身を認証します。

（注） このガイドの最新バージョンと、CRES に関するその他のドキュメントは、この https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html から入手できます。

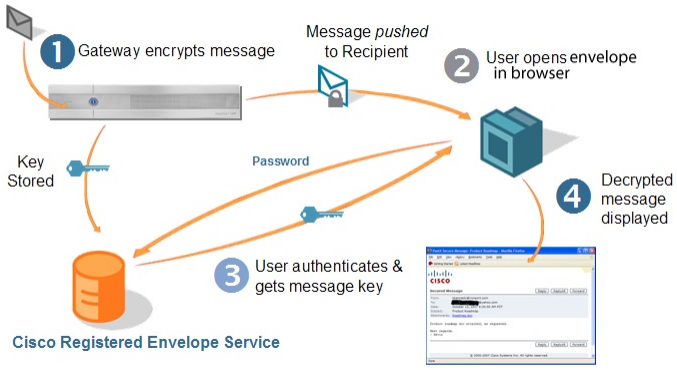
暗号化における Cisco Registered Envelope Service の役割

このサービスは、暗号化の次の要素を管理します。

- **登録済みエンベロープ**：登録済みエンベロープ（暗号化されたメッセージ）の受信者は、メッセージが低いセキュリティで送信される場合を除き、エンベロープを開くときにサービスに登録する必要があります。登録は無料です。
- **認証**：登録されたユーザは、シングルサインオン（SSO）を使用するかパスワードを入力して、登録髄エンベロープを開き、暗号化されたメッセージを読みます。
- **暗号化キー**：暗号化キーは、暗号化されたメッセージごとに作成されます。登録された受信者が登録済みエンベロープにパスワードを入力すると、サービスは復号化キーを送信してエンベロープを開封します。
- **メッセージの有効期限とロック**：登録されたユーザは送信する暗号化されたメッセージの有効期限を設定したりメッセージのロックを制御したりできます。企業アカウント管理者は、企業アカウントを使用して送信されるすべての暗号化されたメッセージの有効期限とロックを制御できます。

- **セキュリティ保護された転送メッセージと返信メッセージ**：企業アカウントの構成によっては、受信者が暗号化を使用して暗号化されたメッセージを転送および返信できることがあります。CRES は、メッセージのセキュリティで保護された転送と返信のために暗号化を処理します。

次の図は、CRES が Cisco E メール セキュリティ アプライアンスと共に動作する方法を示しています。サービスは、暗号化されたメッセージの登録された受信者に復号化キーを指定します。



上の図は、次のプロセスを示しています。

手順

ステップ 1 Cisco E メール セキュリティ アプライアンスは暗号化を使用してメッセージを暗号化し、送信します。

ステップ 2 受信者は、登録済みエンベロープに CRES パスワードを入力します。

（注） メッセージが低いセキュリティ向けに設定されている場合、受信者がセキュリティ保護されたエンベロープを開封するためにパスワードを入力する必要はありません。

ステップ 3 CRES がエンベロープを開封するための復号化キーを指定します。

ステップ 4 受信者の Web ブラウザに、復号化されたメッセージが表示されます。

企業アカウントの管理

CRES は組織の企業アカウントのための管理機能を提供します。最初の CRES 管理ロールは登録済みの技術担当者に割り当てられています。企業アカウントの管理者は、次のタスクを実行します。

- 登録済みエンベロープに表示されるロゴをカスタマイズします
- サービスから送信されるメッセージを管理します

- アカウント使用状況レポートを生成します
- ユーザを管理します（アカウントのロックやパスワードのリセットなど）
- エンベロープを必要としない暗号化されセキュリティ保護された返信のために TLS 設定を構成します