

Cisco Registered Envelope Serviceから「via CRES

内容

[概要](#)

[Cisco Registered Envelope ServiceからCRES経由で応答を受信する理由](#)

[関連情報](#)

概要

このドキュメントでは、Eメールセキュリティアプライアンス(ESA)内またはCRES websafe経由でアクティブおよび設定されるCisco Registered Envelope Service(CRES)暗号化設定について説明します。mail-fromヘッダーとmessage-fromヘッダーが異なっており、DMARCのアラインメントが検証されていることがわかります。

著者：Cisco TACエンジニア、Erika Valverde Chavez

Cisco Registered Envelope Serviceから「via CRES <mail_delivery@res.cisco.com>」と応答を受信するのはなぜですか。

これは、DMARCの障害を回避するためにユーザガイドに従って想定される動作です。エンドユーザがWebSafe (Secure Replyを含む) を介してセキュアメッセージを送信できない場合は、DMARCの回避策として、送信者ドメインをリストに追加する必要があります。現在、次のドメインに対して有効になっています。gmail.com、yahoo.com、およびaol.com。ドメインがリストに追加されると、このドメインの電子メールアドレスを持つ送信者は、次のように置き換えられます。

mail_delivery@res.cisco.comにフレンドリ名を付けます。
Firstname Lastname <user@domain.com> via CRES <mail_delivery@res.cisco.com>
ただし、元の送信者は「返信先」ヘッダーに追加されます。

これは、次のドメインにのみ適用されます。gmail.com、yahoo.com、aol.com

関連情報

- [CRES管理ガイド](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)
- [CRES応答のDMARC検証の処理：バグID CSCvt18599](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。