

Microsoft QuarantineおよびMicrosoft Quarantine Notificationを使用するためのセキュアなEメールゲートウェイの設定

内容

[はじめに](#)

[概要](#)

[前提条件](#)

[Microsoft 365の設定\(O365\)](#)

[Microsoft Exchange onlineで検疫通知を有効にする](#)

[メールフロールール作成](#)

[Cisco Secure Emailの設定](#)

[確認](#)

はじめに

このドキュメントでは、Cisco Secure Email(CES)をMicrosoft 365検疫と統合するために必要な設定手順について説明します。

概要

現代のEメールインフラストラクチャでは、複数のセキュリティレイヤが実装されることが多く、Eメールはさまざまなシステムによって隔離されます。ユーザエクスペリエンスを合理化し、通知の一貫性を向上させるには、検疫管理を1つのプラットフォームに一元化することが有益です。このガイドでは、Cisco CESによって識別されるスパムやグレイメールなどの不要なメッセージをMicrosoft 365ユーザ隔離にリダイレクトする方法について説明します。

前提条件

この設定を完了するには、次のことを確認します。

1. Cisco Secure Email Gatewayのアクティブなテナント
2. Microsoft Exchange onlineのアクティブなテナント。
3. Microsoft 365(O365)サービスへのアクセス
4. Microsoft 365 Defenderライセンス (検疫ポリシーと通知の設定に必要)

Microsoft 365の設定(O365)

隔離されたメッセージを受信および管理するようにMicrosoft 365を設定することから始めます。

Microsoft Exchange onlineで検疫通知を有効にする

Microsoftの公式ドキュメントを参照して、隔離されたメッセージのユーザ通知を設定できます。

[Microsoft検疫通知の設定](#)

メールフロールールを作成

通知がアクティブになったら、Cisco Secure Email GatewayによってマークされたメッセージをMicrosoftのホストされた隔離にリダイレクトするルールを設定します。

1. Microsoft Exchange Admin Centerを開きます。
2. 左側のメニューから、Mail Flow → Rulesに移動します。
3. Add a ruleをクリックし、Create a new ruleを選択します。
4. ルール名をCSE Quarantine Ruleに設定します。
5. Apply this rule ifの下で、The message headerを選択し、matches text patternsを選択します。
。
6. ヘッダー名に「X-CSE-Quarantine」と入力し、一致する値「true」を設定します。
7. Do the followingで、Redirect the message toを選択し、Hosted Quarantineを選択します。
8. 設定を保存します。
9. 保存後、ルールが有効になっていることを確認します。

写真では、ルールがどのように見えるかを見ることができます。

CSE Quarantine

 Edit rule conditions  Edit rule settings

Status: Disabled

Enable or disable rule

☒ Enabled

 Updating the rule status, please wait...



Rule settings

Rule name	Mode
CSE Quarantine	Enforce
Severity	Set date range
Not specified	Specific date range is not set
Senders address	Priority
Matching Header	1
For rule processing errors	
Ignore	

Rule description

Apply this rule if

'X-CSE-Quarantine' header matches the following patterns: 'true'

Do the following

Deliver the message to the hosted quarantine.

Rule comments

Cisco Secure Emailの設定

Cisco CESでは、Microsoftの検疫にリダイレクトするすべてのメッセージに、カスタムヘッダー (X-CSE-Quarantine: true)を追加できます。

これらのメッセージは、CES内の任意のコンテンツフィルタまたはエンジンでフラグを付けることができます。この例では、疑わしいスパムメッセージ用に設定します。

1. Cisco Secure Email Management Consoleを開きます。
2. Mail Policies → Incoming Mail Policiesの順に移動します。
3. 変更するポリシーを編集します(たとえば、デフォルトポリシーを選択します)。
4. 選択したポリシーのスパム設定をクリックします。
5. Suspect Spamの下で、アクションをQuarantineからDeliverに変更します。
6. Advancedをクリックして、カスタムヘッダーを追加します。
 - ヘッダー名:X-CSE-Quarantine
 - 値: true (Microsoftのルールで使用されている値と同じ)
7. Submitをクリックしてから、Commit Changesをクリックして設定を適用します。

次の図では、設定がどのように表示されるかを確認できます。

Suspected Spam Settings	
Enable Suspected Spam Scanning:	☐ No ☒ Yes
Apply This Action to Message:	Deliver ▼ Send to Alternate Host (optional):
Add Text to Subject:	Prepend ▼ [SUSPECTED SPAM]
▼ Advanced	Add Custom Header (optional): Header: X-CSE-Quarantine Value: True
	Send to an Alternate Envelope Recipient (optional): Email Address: (e.g. employee@company.com)
	Archive Message: ☒ No ☐ Yes

CESの設定

確認

これ以降、Cisco CESが潜在的なスパムとして識別する電子メールは、カスタムヘッダーでタグ付けされます。Microsoft 365はこのタグを検出し、メッセージをユーザ隔離にリダイレクトします。

Microsoft 365の設定に従って、ユーザwに隔離通知が送信されます。

Delete

Archive

Report

Move to

Reply

Reply all

Forward

Zoom

Read / Unread

Categorize

Flag / Unflag

Print

Microsoft 365 security: You have messages in quarantine

quarantine@messaging.microsoft.com

To: A

Reply

Reply all

Forward

Wed 6/18/2025 4:16 PM

Microsoft

Review These Messages

3 messages are being held for you to review as of 6/18/2025 1:22:21 PM (UTC).

Review them within 30 days of the received date by going to the [Quarantine page](#) in the Security Center.

Prevented high confidence phishing messages

Sender: support2@safeconnect.org

Subject: Final notice

Date: 6/18/2025 10:02:22 AM

Review Message

Request Release

Sender: contact@supportnow.net

Subject: Pre-approval

Date: 6/18/2025 10:03:52 AM

Review Message

Request Release

Sender: alan@dominio.com

Subject: Slash Your Monthly Power Bill by 70%

Date: 6/18/2025 10:05:48 AM

Review Message

Request Release

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。