



Exchange Online

メール保護の管理





目次

1.保護.....	3
1.1「保護」.....	3
1.2設定手順.....	4
1.2.1マルウェアフィルター.....	4
1.2.2接続フィルター.....	7
1.2.3スパムフィルター.....	9
1.2.4送信スパム.....	12
1.2.5検疫.....	14

1. メールボックスの管理

この章では、「保護」の機能について説明します。

■ 1.1 保護

Exchange Onlineを使用すると、自動的にマルウェア※およびスパムメールのフィルタリングが行われ、ユーザーにとって有害または不要なメールは除去されるよう構成されています。

※マルウェア：ウイルスやスパイウェアなど、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称

以下の4つのフィルター機能が用意されており、既定で推奨値が設定されています。管理者は、自分の組織に合った設定に変更することができます。

【マルウェア対策】

1. マルウェアフィルター

マルウェアの検出を行います。マルウェアが検出されたときのメッセージの処置方法や、送信元へのメッセージ内容などを設定することができます。

【スパム対策】

2. 接続フィルター

Exchange Onlineへメッセージを送信してくるメールサーバーのIPアドレスのチェックを行います。スパムメールを送信してくるサーバーのIPアドレスを拒否したり、スパムメールと誤検知されないように特定のメールサーバーのIPアドレスを許可することができます。

3. コンテンツフィルター

メッセージのヘッダーや本文などチェックを行います。Microsoftが提供するスパム検出エンジンを利用し、スパムの判定を行います。管理者は、スパムと判定された場合の処置を設定することができます。また、特定の言語や地域から送信されたメッセージのブロックなども設定できます。

4. 送信スパム

組織内から外部に送信されるメッセージのスパムチェックを行います。送信メッセージがスパムと判断された場合、管理者にメッセージのコピーや通知を送信することができます。

■ 1.2 設定手順

各フィルターの変更手順を紹介します。

1.2.1 マルウェアフィルター

以下の手順でマルウェアフィルターの設定を変更することができます。




注意

管理者としてサインインし、以下の操作を行います。

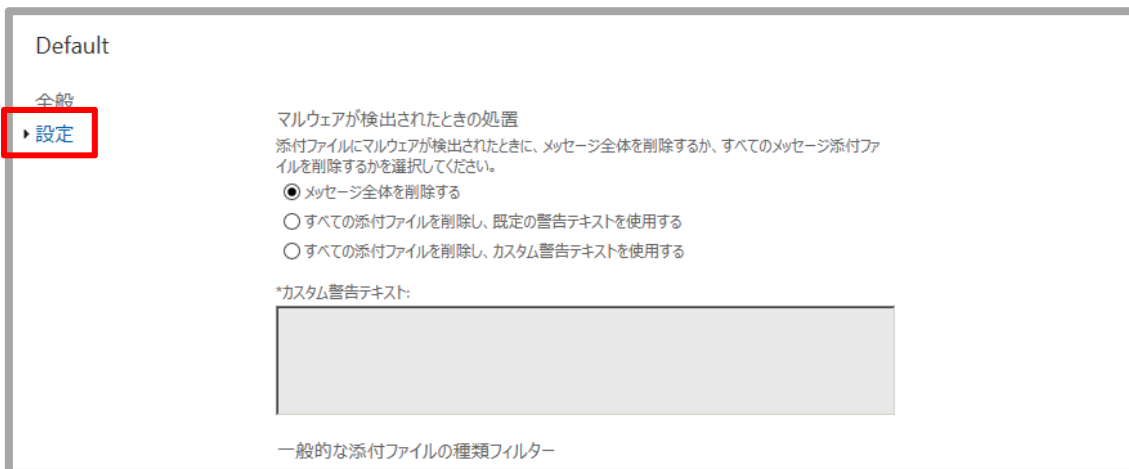
- ① Exchange管理センターで、[保護]>[マルウェアフィルター]の順にクリックします。

The screenshot shows the Exchange Management Center interface. On the left sidebar, the 'Protection' menu item is highlighted with a red box. In the main content area, the 'Malware Filter' link is also highlighted with a red box. Below the navigation links, there is a table with columns for '有効' (Enabled), '名前' (Name), and '優先度' (Priority). The table contains one entry: 'Default' with a checked '有効' box and a priority of '最低' (Lowest).

- ② [ (編集)] をクリックします。

This screenshot is similar to the previous one, but the edit icon (a pencil inside a square box) in the table's action column is highlighted with a red box. The table still shows the 'Default' filter with its '有効' box checked and priority set to '最低'.

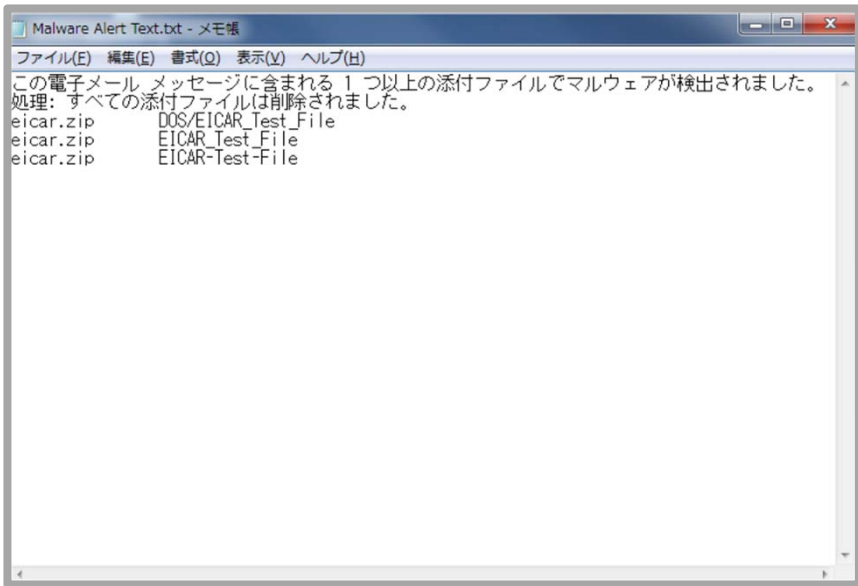
③ 設定をクリックします。



④ 設定を行い、[保存] をクリックします。

設定内容は、以下の通りです。

・ マルウェアが検出されたときの処置

設定値	説明
メッセージ全体を削除する	メッセージ全体を削除します。
すべての添付ファイルを削除し、既定の警告テキストを使用する	すべての添付ファイルを削除して、代わりに既定の警告テキストファイルが添付され、受信者に送信されます。 
すべての添付ファイルを削除し、カスタム警告テキストを使用する	すべての添付ファイルを削除して、代わりに管理者が指定した警告テキストファイルが添付され、受信者に送信されます。

・ 通知

設定値	説明
内部送信者に通知する	<p>組織内から送信したメッセージが削除され配信されなかった場合に、送信者に通知メッセージを送信します。</p> 
外部送信者に通知する	<p>組織外から受信したメッセージが削除され配信されなかった場合に、送信者に通知メッセージを送信します。 ※既定の通知メッセージの内容は、内部送信者と同じです。</p>

・ 管理者への通知

設定値	説明
内部送信者からの配信されなかったメッセージを管理者に通知する	<p>組織内から送信したメッセージが削除され配信されなかった場合に、指定した管理者のメールアドレスに通知メッセージを送信します。 ※通知メッセージの内容は、内部送信者への通知メッセージと同じです。</p>
外部送信者からの配信されなかったメッセージを管理者に通知する	<p>組織外から受信したメッセージが削除され配信されなかった場合に、指定した管理者のメールアドレスに通知メッセージを送信します。 ※通知メッセージの内容は、外部送信者への通知メッセージと同じです。</p>

カスタマイズした通知テキストを使用する

送信者と管理者に送信する通知メッセージの内容を、管理者が指定した内容で送信します。[発信者名] [差出人のアドレス] が指定可能です。

また、「内部送信者」「外部送信者」それぞれに対する通知メッセージの [件名] [メッセージ本文] を入力できます。

<サンプル通知メッセージ>



1.2.2 接続フィルター

以下の手順で接続フィルターの設定を変更することができます。




注意

管理者としてサインインし、以下の操作を行います。

- ① Exchange管理センターで、[保護]>[接続フィルター]の順にクリックします。



② [ (編集)] をクリックします。



Exchange 管理センター

ダッシュボード

受信者

アクセス許可

コンプライアンス管理

組織

保護

高度な脅威

メールフロー

マルウェア フィルター **接続フィルター** スпам フィルター 送信スパム 検疫 アクション センター dl

名前

Default

③ [接続フィルター]をクリックします。



Default

全般

▶ 接続フィルター

接続フィルター

IP 許可一覧
次の IP アドレスからのメッセージを常に許可します。

+  -

許可する IP アドレス

IP 禁止一覧
次の IP アドレスからのメッセージを常にブロックします。

+  -

ブロックする IP アドレス

セーフリストを有効にする

保存 キャンセル

- ④ 設定を行い、「保存」をクリックします。
設定内容は、以下の通りです。

設定値	説明
許可一覧	このIPアドレスからのメッセージを常に許可します。
禁止一覧	このIPアドレスからのメッセージを常にブロックします。
セーフリストを有効にする	Microsoftが信頼できると判断した送信者からのメッセージは、スパムのチェックをスキップさせることができます。

1.2.3 スпамフィルター

以下の手順でスパムフィルターの設定をすることができます。



注意
管理者としてサインインし、以下の操作を行います。

- ① Exchange管理センターで、[保護]>[スパムフィルター]の順にクリックします。

Exchange 管理センター

ダッシュボード マルウェアフィルター 接続フィルター **スパムフィルター** 送信スパム 検疫 アクションセンター d

受信者

アクセス許可

コンプライアンス管理

組織

保護

高度な脅威

+ ✎ 🗑️ ↑ ↓ ↻

有効	名前	優先度
<input checked="" type="checkbox"/>	Default	最低

- ② [+ (新規作成)] をクリックします。

Exchange 管理センター

ダッシュボード マルウェアフィルター 接続フィルター **スパムフィルター** 送信スパム 検疫 アクションセンター d

受信者

アクセス許可

コンプライアンス管理

組織

+ ✎ 🗑️ ↑ ↓ ↻

有効	名前	優先度
<input checked="" type="checkbox"/>	Default	最低

④ 以下の項目を設定し、[保存]をクリックします。

スパム フィルター ポリシーの新規作成

*名前:

説明:

スパムおよびバルクのアクション
受信したスパムおよびバルク メールに対する対処法を選びます。 [詳細情報](#)

スパム:
 ▼
精度の高いスパム:
 ▼

バルク メール:
 バルク メールをスパムとしてマーク
しきい値を選びます。1 を選ぶと、スパムとしてマークされるバルク メール数が最大になり、9 を選ぶと配信できるメール数が最大になります。
 ▼

検疫
次の期間スパムを保持する (日):

項目	説明	
名前	ポリシーの名前を指定します。	
説明	ポリシーの説明を入力します。	
スパム・制度の 高いスパム	迷惑メールフォルダーに メッセージを移動する	指定された受信者の迷惑メール フォルダーにメッセージを送信します。これは、両方の信頼度しきい値レベルに対する既定のアクションです
	X-ヘッダーを追加する	<p>指定した受信者にメッセージを送信しますが、メッセージをスパムとして識別する X-ヘッダー テキストをメッセージ ヘッダーに追加します。このテキストを目印にすると、必要に応じてメッセージをフィルター処理またはルーティングする規則をオプションで作成できます。既定の X-ヘッダー テキストは「This message appears to be spam」です。</p> <p>X-ヘッダー テキストをカスタマイズするには、[この X-ヘッダー テキストを追加する] 入力ボックスを使用します。X-ヘッダー テキストをカスタマイズする場合は、次の点に注意してください。</p> <ul style="list-style-type: none"> ● <ヘッダー> という形式でヘッダーのみを指定 (<ヘッダー> 内にスペースなし) した場合は、カスタム テキストにコロンが付加され、その後既定のテキストが続きます。たとえば、“This-is-my-custom-header” と指定した場合は、X-ヘッダー テキストに “This-is-my-custom-header: This message appears to be spam” と表示されます。 ● “X This is my custom header” や “X-This-is-my-custom-header:” のようにカスタム ヘッダー テキスト内にスペースを含めたりコロンを自分で追加した場合は、X-ヘッダー テキストは既定の “X-This-Is-Spam: This message appears to be spam” に戻されます。

スパム・制度の高いスパム		●<header>:<value> という形式でヘッダー テキストを指定することはできません。このように指定した場合は、コロンの前後の値が無視され、既定の X-ヘッダー テキストが代わりに表示されます。“X-This-Is-Spam:This message appears to be spam”
	件名行の先頭にテキストを追加する	本来の受信者にメッセージを送信しますが、[件名の先頭にこのテキストを追加する] テキストボックスに指定したテキストが件名行の先頭に追加されます。このテキストを目印にすると、必要に応じてメッセージをフィルター処理またはルーティングする規則をオプションで作成できます。
	メールアドレスにメッセージをリダイレクトする	メッセージを本来の受信者に送信せず、指定されたメール アドレスに送信します。「リダイレクト」アドレスを [このメール アドレスにリダイレクトする] ボックスに指定してください。
	メッセージを削除する	添付ファイルすべてを含め、メッセージ全体が削除されます。
	メッセージを隔離する	メッセージを本来の受信者に送信せず、検査に送信します。このオプションを選択した場合は、[次の期間スパムを保持する(日)] 入力ボックスで、スパム メッセージを検査する日数を指定します。(その時間が経過すると、自動的に削除されます。既定値は 15 日で、これが最大値です。最小値は 1 日です)。
バルクメール	<p>バルクメールをスパムとしてマークの設定を有効にすると、指定したしきい値に従って、一括送信で送付されるメールがスパムとしてマークされます。しきい値は1 ~ 9 で選択します。この場合、1 はほとんどのバルクメールをスパムとしてマークし、9 はほとんどのバルクメールの配信を許可します。</p> <p>迷惑メールは「常にある脅威」であるのに対して、バルクメールは、通常、繰り返し送られてくるわけではない広告メッセージまたはマーケティングメッセージで構成されます。バルクメールは一部のユーザーによって要求されたものであり、事実、彼らは意図的にそれらのメッセージの受信を申し込んでいるのに対して、それ以外のユーザーはその種のメッセージをスパムと見なしています。</p>	
検査 次の期間スパムを保持する(日)	スパム メッセージが検査に保持される日数を指定します。	
受信拒否一覧 受信拒否ドメイン一覧	送信者やドメインなどのエンTRIESを指定すると、それらのENTRIESからのメールが常にスパムとしてマークされます。サービスにより、これらのENTRIESに一致する電子メールに対して、構成された精度の高いスパム処理が適用されます。	
受信許可一覧 受信許可ドメイン一覧	送信者やドメインなどのENTRIESを指定すると、それらのENTRIESからのメールが常に受信トレイに配信されます。これらのENTRIESからのメールは、迷惑メール フィルターによって処理されません。	
海外からのスパム	特定の言語で書かれた電子メール メッセージや特定の国や地域から送信された電子メール メッセージにフィルターを適用することができます。最大 86 言語、250 地域を構成できます。サービスが信頼度の高いスパムに対して構成されたアクションを適用します。	

詳細オプション	オン	メッセージがそのオプションに関連付けられたルールに従って積極的にフィルター処理されます。どのオプションをオンにしたかにより、メッセージはスパムとしてマークされるか、メッセージのスパム スコアが上がります。
	オフ	スパム フィルター条件を満たしているメッセージに対してアクションが実行されません。すべてのオプションは既定でオフになっています。
	テスト	<p>スパム フィルター条件を満たしているメッセージに対してアクションが実行されません。ただしメッセージには、意図した受信者への配信前に X-ヘッダーでタグ付けできます。この X-ヘッダーにより、どの ASF オプションが一致したかを確認できます。任意の詳細オプションに [テスト] を指定した場合は、テスト対応オプションに一致したときに適用する、次のテスト モード設定を構成できます。</p> <p>[なし] メッセージにテスト モード アクションを行いません。既定ではこのオプションが選択されています。</p> <p>[既定のテスト X-ヘッダー テキストの追加] このオプションをオンにすると、指定された受信者にメッセージを送信しますが、メッセージが特定の高度なスパム フィルタリング オプションに一致したことを示す、特別な X-ヘッダーをメッセージに追加します。</p> <p>[次のアドレスに Bcc メッセージを送信] このオプションをオンにすると、入力ボックスで指定された電子メールアドレスにメッセージのブラインド カーボン コピーが送信されます。</p>
適用先	このポリシーを適用するユーザー、グループ、およびドメインを指定する条件ベースのルールを作成します。	

1.2.4 送信スパム

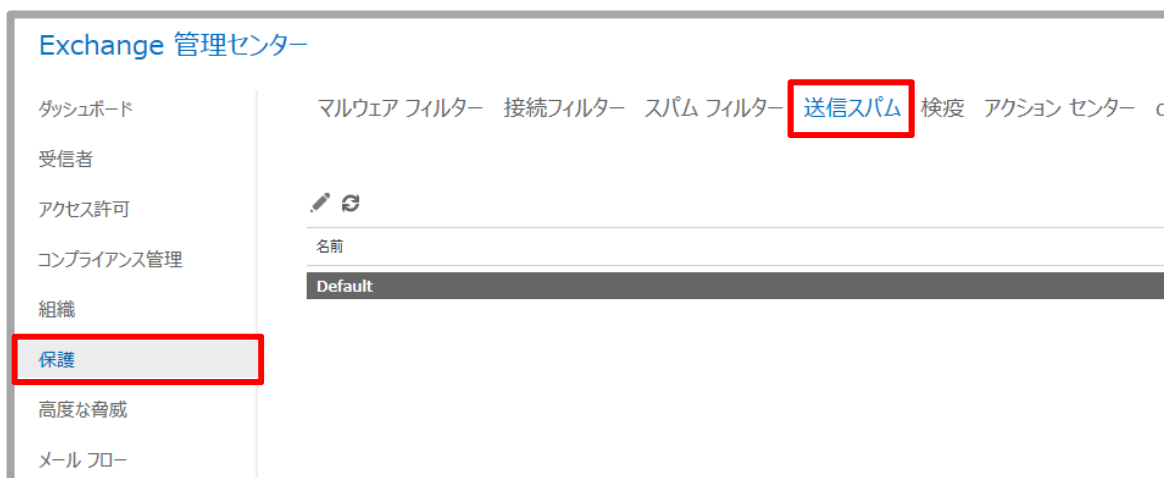
以下の手順で送信スパムの設定を変更することができます。




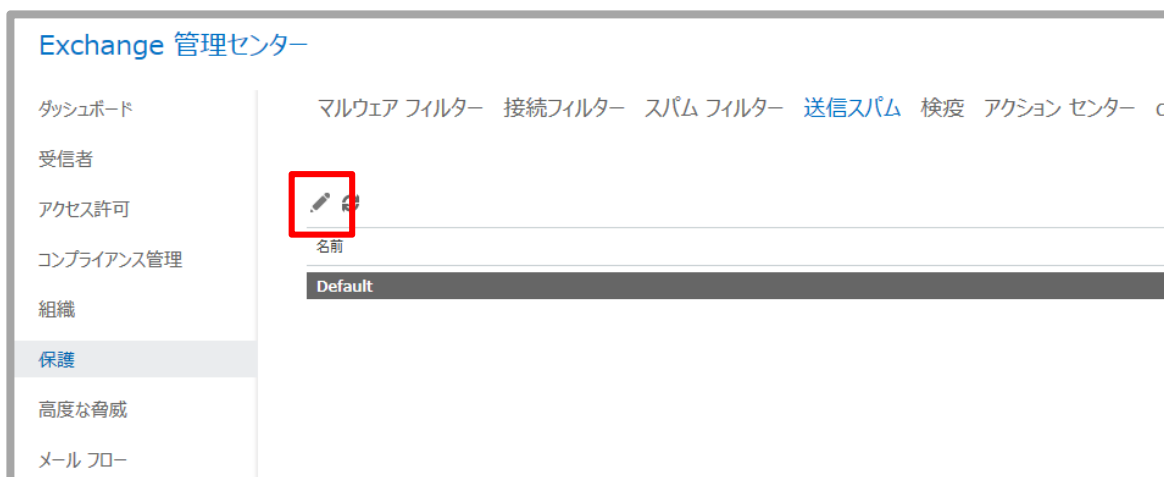
注意

管理者としてサインインし、以下の操作を行います。

① Exchange管理センターで、[保護]>[送信スパム]の順にクリックします。



② [ (編集)] ボタンをクリックします。



③ [送信スパム基本設定]をクリックします。



- ④ 設定を行い、「保存」をクリックします。
設定内容は、以下の通りです。

設定値	説明
すべての疑わしい送信メールメッセージのコピーを次のメールアドレスに送信する	すべての疑わしい送信メッセージのコピーを受信する管理者のメールアドレスを指定します。複数のアドレスを指定する場合は、セミコロンで区切ります。
送信者が外部へのスパムの送信をブロックされた場合、次のメールアドレスに通知を送信する	スパムと識別されたメッセージの送信者がブロックされた場合に通知する管理者のメールアドレスを指定します。複数のアドレスを指定する場合は、セミコロンで区切ります。

1.2.5 検疫

以下の手順で検疫されているメッセージの確認、処理を行うことができます。



注意

管理者としてサインインし、以下の操作を行います。

- ① Exchange管理センターで、[保護]>[検疫]の順にクリックします。

Exchange 管理センター

ダッシュボード マルウェア フィルター 接続フィルター スпам フィルター 送信スパム **検疫** アクション センター d

受信者

アクセス許可

コンプライアンス管理

組織

保護

高度な脅威

メール フロー

検疫のアイテムを確認してください。1 つ以上のメッセージを特定のユーザーまたはすべてのユーザーに解放できます。誤ってスパムとして検出された場合、ヒント: 解放するメッセージを複数選ぶには、Ctrl キーを押しながら複数のメッセージをクリックするか、Ctrl + A キーを使ってすべてのメッセージを選びます。

送信者	件名	受信日時	有効期限
このビューに表示するアイテムはありません。			

② 検疫されているメッセージを確認します。

The screenshot shows the Exchange Management Center interface. On the left is a navigation pane with options like 'ダッシュボード', '受信者', 'アクセス許可', 'コンプライアンス管理', '組織', '保護', 'メールフロー', 'モバイル', 'パブリックフォルダー', and 'ユニファイド メッセージング'. The main area is titled 'Exchange 管理センター' and has tabs for 'マルウェア フィルター', '接続フィルター', 'コンテンツ フィルター', '送信スパム', and '検疫'. Below the tabs, there is a message: '検疫のアイテムを確認してください。メッセージを特定のユーザーに解放できます。スパムとして検出された場合、誤検知として報告することもできます。' Below this is a table of quarantined messages:

送信者	件名	受信日時	有効期限	メッセージの状態
K.Tachikawa@otsuk...	検疫4	2014/08/05 ...	2014/08/20 ...	種類: スパム 有効期限: 2014/08/20 0:00
K.Tachikawa@otsuka...	検疫3	2014/08/05 ...	2014/08/20 ...	メッセージの詳細 送信者: K.Tachikawa@otsuka-shokal.co.jp 件名: 検疫4 受信日時: 2014/08/05 2:28

③ メッセージをもとの受信者に配信する場合は、メッセージを選択し、[解放]をクリックします。解放する際の選択肢は以下の4通りです。

The screenshot shows a context menu for a selected message. The menu is titled '解放' and contains four options:

- 選んだメッセージを解放して、受信を許可します...
- メッセージを特定の受信者に解放します...
- 選んだメッセージをすべての受信者に解放します...
- 選択したメッセージを解放し、誤検知として報告する...



注意

[解放]の処理は1通ずつ行う必要があります。複数のメッセージを一括して処理することはできません。

■ 選択したメッセージを解放し、送信者を許可します…

オプションで、メッセージを Microsoft に報告することを選択し、その後、**[解放して許可する]** をクリックすることもできます。メッセージは、アドレス指定されるすべての受信者に解放され、この送信者からの将来のメッセージはすべて許可されます。ただし、トランスポート ルールまたはブロックされている送信者のためにこのメッセージが検疫された場合、この送信者からの将来のメッセージは引き続きブロックされます。

■ メッセージを特定の受信者に解放します…

メッセージを解放できる受信者を選択します。メッセージは各受信者に 1 回しか解放できないため、解放先とすることができるユーザーのみがこの一覧に表示されます。複数選択がサポートされています。受信者を選択し、**[追加]** をクリックします。

■ 選んだメッセージをすべての受信者に解放します…

このオプションを選択する場合、同じ受信者に 2 回以上メッセージを解放することはできないので注意してください。受信者が既にメッセージを受け取っていた場合、メッセージがその受信者にもう一度解放されることはありません。

■ 選択したメッセージを解放し、誤検知として報告する…

このオプションを選択する場合、同じ受信者に 2 回以上メッセージを解放することはできないので注意してください。受信者が既にメッセージを受け取っていた場合、メッセージがその受信者にもう一度解放されることはありません。

また、そのメッセージをまだ受信していないすべての受信者にメッセージが解放されます。スパム検疫済みメッセージの場合は、メッセージの評価と分析を行う Microsoft スпам分析チームに報告されます。分析結果によっては、このメッセージが許可されるようにサービス全体のスパム コンテンツ フィルター ルールが調整されることがあります。