



# メッセージルール

メッセージルールを使用すると、一部のタイプのメッセージを修復またはスキャンしないように指定できます。許可リストルール、判定のオーバーライドルール、およびバイパス分析ルールを作成できます。バイパス分析ルールは、フィッシングテストまたはセキュリティメールボックス用に作成できます。

**注:** [許可リスト (Allow List)] および [判定のオーバーライド (Verdict Override)] ルールは、認証なしモードのビジネスでは使用できません。

[設定 (Settings)] > [メッセージルール (Message Rules)] ページから、メッセージルールを作成および管理します。

バイパス分析ルールは、許可リストルールと判定のオーバーライドルールよりも優先されます。メッセージがルールの影響を受ける場合は、[メッセージ (Messages)] ページの [メッセージルール (Message Rules)] 列に表示されます。[メッセージルール (Message Rules)] 列の項目にカーソルを合わせると、適用されたルールが表示されます。

Verdict	Action	Rule	Received
Spam	Allow List	Allow List	
Graymail	Allow List	Allow List	

Rule Name: Allow List  
Rule Type: Allow List  
Criteria Type: Sender IP Addresses (CIDR)  
Effective: Apr 18 2022 11:10 AM  
Last Updated By:

**注:** ルールはサブドメインに自動的に適用されません。ドメインは、ルールに示されているとおりに正確に一致します。

## 許可リストルール

許可リストルールを使用すると、特定の送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレスからのスパムおよびグレイメールメッセージの修復を防ぐことができます。メッセージは引き続き分析されますが、自動修復は適用されません。たとえば、Secure Email Threat Defense で特定の送信者からのアイテムがスパムであると判断されたものの、そのアイテムをユーザーの受信トレイに残しておきたい場合は、許可リストルールを作成して、該当するメッセージを修正するポリシーをオーバーライドできます。許可リストルールは、ポリシーの例外として機能します。許可リストルールに一致するメッセージは、引き続き影響レポートに表示されます。

許可リストルール:

- グレイメールやスパムに適用します。
- 許可された送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレス (IPv4 または CIDR ブロック) を指定します。
- ルールごとに最大 50 の基準を設定できます。つまり、50 個の電子メールアドレス、ドメイン、またはアドレスを設定できます。

アクティブなルールは 20 に制限されています。ルールは非アクティブ化できますが、削除することはできません。

## 判定のオーバーライドルール

判定のオーバーライドルールを使用すると、ルールで指定された基準に一致するスパムおよびグレイメールの判定をオーバーライドできます。メッセージは「ニュートラル( Neutral )」判定とマークされ、修正されません。判定がオーバーライドされたメッセージは、影響レポートに表示されません。

判定のオーバーライドルール:

- グレイメールやスパムに適用します。
- 許可された送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレス( IPv4 または CIDR ブロック )を指定します。
- ルールごとに最大 50 の基準を設定できます。つまり、50 個の電子メールアドレス、ドメイン、または IP アドレスを設定できます。

アクティブなルールは 20 に制限されています。ルールは非アクティブ化できますが、削除することはできません。

## バイパス分析ルール

バイパス分析ルールを使用すると、フィッシングテストまたはセキュリティ メールボックス メッセージの分析をバイパスできます。ルール基準を満たすメッセージによってすべてのエンジン分析がバイパスされるため、エンジンに干渉することなくセキュリティテストを処理できます。添付ファイルとリンクは、Secure Email Threat Defense によって開かれたりスキャンされたりしません。

フィッシングテストルール:

- 指定した送信者の電子メールアドレス、送信者のドメイン、または IP アドレス( IPv4 または CIDR ブロック )から送信されたすべての受信メッセージに適用します。メッセージは分析されません。
- ルールごとに最大 50 の基準を設定できます。

セキュリティ メールボックス ルール:

- 指定した受信者の電子メールアドレスの受信メッセージに適用します。メッセージは分析されません。

**注:** 指定した受信者がメッセージの唯一の受信者である場合、セキュリティ メールボックス ルールが適用されます。他の受信者がコピーされているか、BCQ( ブラインドカーボンコピー )として含まれている場合、メッセージは分析エンジンをバイパスしません。

- ルールごとに最大 50 の基準を設定できます。

アクティブなバイパス分析ルールは 20 に制限されています。ルールは非アクティブ化できますが、削除することはできません。

## メッセージルールの追加

メッセージルールを追加する手順は、ルールのカテゴリによって若干異なります。

## 新しい許可リストまたは判定のオーバーライドルールの追加

新しいルールを作成するには、次の手順を実行します。

1. [設定( Settings )] > [歯車アイコン] > [メッセージルール( Message Rules )] を選択します。
2. 作成するルールのカテゴリを、[許可リスト( Allow List )] または [判定オーバーライド( Verdict Override )] のいずれかから選択します。

## ルールの編集

3. [新規ルールの追加( Add New Rule )] ボタンをクリックします。
4. ルール名を作成します。各ルールには固有の名前が必要です。
5. 基準のタイプを選択します。[送信者の電子メール( Sender Email )]、[送信者のドメイン( Sender Domain )]、[送信者の IP アドレス( IPv4 )( Sender IP Addresses (IPv4) )]、または [送信者の IP アドレス( CIDR )( Sender IP Addresses (CIDR) )] を選択できます。
6. 許可された項目をコンマで区切って入力します。
7. 許可する判定に応じて、[スパム( Spam )] や [グレイメール( Graymail )] を選択します。
8. [送信( Submit )] をクリックして、ルールの作成を終了します。

ルールがリストに追加されます。変更が適用されるまでに最大で 20 分かかる場合があります。

## 新しいバイパス分析ルールの追加

新しいルールを作成するには、次の手順を実行します。

1. [設定( Settings )](歯車アイコン) > [メッセージルール( Message Rules )] を選択します。
2. [バイパス分析( Bypass Analysis )] を選択します。
3. [新規ルールの追加( Add New Rule )] ボタンをクリックします。
4. ルール名を作成します。各ルールには固有の名前が必要です。
5. 作成するルールタイプを、[フィッシングテスト( Phish Test )] または [セキュリティメールボックス( Security Mailbox )] のいずれかから選択します。
6. [フィッシングテスト( Phish Test )] ルールの場合は、基準タイプを [送信者の電子メールアドレス( Sender Email Addresses )] または [送信者のドメイン( Sender Domains )]、[送信者の IP アドレス( IPv4 )( Sender IP Addresses (IPv4) )]、[送信者の IP アドレス( CIDR )( Sender IP Addresses (CIDR) )] のいずれかから選択します。次に、コンマで区切って項目を入力します。  
  
[セキュリティメールボックス( Security Mailbox )] ルールの場合は、受信者の電子メールアドレスをコンマで区切って入力します。
7. [送信( Submit )] をクリックして、ルールの作成を終了します。

ルールがリストに追加されます。変更が適用されるまでに最大で 20 分かかる場合があります。

## ルールの編集

編集できるのは有効なルールのみです。規則を編集するには、次の手順を実行します。

1. [設定( Settings )](歯車アイコン) > [メッセージルール( Message Rules )] を選択します。
2. 編集するルールのタイプを選択します。
3. [アクション( Action )] 列で、編集するルールの横にある鉛筆アイコンをクリックします。
4. 必要な変更を行ったら、[変更の保存( Save Changes )] をクリックします。

ルールが更新されます。変更が適用されるまでに最大で 20 分かかる場合があります。

## ルールの有効化または無効化

既存のルールを有効または無効にするには、次の手順を実行します。

1. [設定( Settings )] 歯車アイコン > [メッセージルール( Message Rules )] を選択します。
2. 有効または無効にするルールのタイプを選択します。
3. [アクション( Action )] 列で、ステータスを変更するルールの横にある有効または無効アイコンをクリックします。

ルールのステータスが更新されます。変更が適用されるまでに最大で 20 分かかる場合があります。

## Microsoft 許可リストと安全な送信者

Secure Email Threat Defense は、スパムおよびグレイメールメッセージに関して、Microsoft 365 のスパムフィルタ許可リストに追加された送信者とドメインを受け入れます。MS 許可リストは、悪意の判定やフィッシング判定では適用されません。詳細については、『[Cisco Secure Email Threat Defense FAQ: Secure Email Threat Defense and Microsoft 365](#)』を参照してください。

個々のユーザーがメールボックス内の許可リストを設定することを組織が許可している状況で、特定のメッセージがユーザーの許可リストに含まれる場合、Microsoft 許可リストが Secure Email Threat Defense で常に適用されることはありません。Secure Email Threat Defense でこれらの設定を適用する場合は、[ポリシー( Policy )] ページの [スパムまたはグレイメールと判定された Microsoft Safe Sender メッセージを修復しない( Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts )] チェックボックスをオンにします。Safe Sender フラグは、スパムとグレイメールの判定では適用されますが、悪意とフィッシングの判定では適用されません。つまり、スパムまたはグレイメールと判定された Safe Sender メッセージは修正されません。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。