Cisco Secure Email Threat Defense リリースノート

はじめに

このドキュメントには、Cisco Secure Email Threat Defense の製品の更新、使用上の警告、および既知の問題に関する情報が含まれています。

2021 年 7 月 12 日から 2022 年 9 月 29 日までの Cisco Secure Email Cloud Mailbox のアーカイブリリースノートは、https://www.cisco.com/c/en/us/td/docs/security/cloud-mailbox/release-notes/cloud-mailbox-release-notes-archive.html [英語] から検索できます。

製品アップデート

2025 年 6 月 5 日

拡張機能

- Cisco Secure Email Threat Defense の影響力の高い人員リストのサポート：Cisco Secure Email Gateway 偽装電子メール検出（FED）を使用するお客様は、影響力の高い人員リストを活用することで、より効果的に脅威を特定し、軽減することができるようになりました。
- 高度なスキャン機能：クリック可能なリンクや TIFF ファイルに埋め込まれた QR コードが添付された SVG 添付ファイルをスキャンすることで、潜在的なセキュリティリスクが検出されるようになり、悪意のあるコンテンツに対して、強化されたセキュリティを確保します。

修正済みの問題

- 軽微なバグ修正。

2025 年 5 月 21 日

拡張機能

- UI 画面は、シスコのセキュリティ製品全体でより一貫したエクスペリエンスを提供するためのシスコの継続的な取り組みの一環として再設計されています。次の作業が含まれます。
  - 導入準備画面とウィザードが更新され、新しい設定オプションが反映されました。
  - [ポリシー（Policy）] ページの名前が、[構成（Configuration）] に変わり、[メールフロー構成（Mail flow configuration）]、[グローバル設定（Global settings）]、および [ポリシー構成（Policy configuration）] の 3 つの領域に分けました。

  - 変更前と変更後のビューおよび UI 変更の概要については、「Cisco Secure Email Threat Defense UI 変更」を参照してください。

- デフォルトベースポリシー設定の一部として、方向別に修復ポリシーを設定する新しい機能。

修正済みの問題

- 軽微なバグ修正。

2025 年 5 月 6 日

拡張機能

- パブリック API：新しい監査ログ SIEM 統合 API。この API は、SIEM 統合のために監査ログを S3 バケットに送信する機能を追加します。これを許可する設定には、**[管理（Administration ）] > [ビジネス（Business）]** ページの順に選択してアクセスします。詳細については、API ガイド（https://developer.cisco.com/docs/message-search-api/log-export-api/）を参照してください。

- 近日提供予定：UI の機能強化。今後数週間以内に [Cisco Secure Email Threat Defense ポリシー（Secure Email Threat Defense Policy）] ページに変更を加えます。これらの変更は、シスコのセキュリティサービス全体でより一貫したエクスペリエンスを提供するためのシスコの継続的な取り組みの一環です。変更前と変更後のビューおよび今後の変更の概要については、「Coming Soon: Secure Email Threat Defense UI Changes」を参照してください。

修正済みの問題

- 軽微なバグ修正。

2025 年 4 月 24 日

修正済みの問題

- 軽微なバグ修正。

2025 年 4 月 8 日

修正済みの問題

- 軽微なバグ修正。

2025 年 3 月 27 日

修正済みの問題

- 軽微なバグ修正。

2025 年 3 月 13 日

修正済みの問題

- 軽微なバグ修正。

2025 年 5 月 21 日

2025 年 2 月 12 日

拡張機能

- UI 画面は、シスコのセキュリティ製品全体でより一貫したエクスペリエンスを提供するためのシスコの継続的な取り組みの一環として再設計されています。このリリースでは、ダッシュボード、メッセージ、トレンド、および影響レポートが更新されています。再設計された各ページの上部にあるバナーを使用して、新しいデザインと従来のデザインを切り替えることができます。変更前と変更後のビューおよび変更の概要については、「Secure Email Threat Defense UI Changes」を参照してください。

修正済みの問題

- 軽微なバグ修正。

2025 年 1 月 30 日

修正済みの問題

- 軽微なバグ修正。

2025 年 1 月 23 日

拡張機能

近日提供予定：UI の機能強化。今後数週間から数ヵ月の間に Cisco Secure Email Threat Defense のインターフェイスに変更を加える予定ですので、お客様の準備ができているか確認したいと考えています。これらの変更は、シスコのセキュリティサービス全体でより一貫したエクスペリエンスを提供するためのシスコの継続的な取り組みの一環です。変更前と変更後のビューおよび今後の変更の概要については、「Coming Soon: Secure Email Threat Defense UI Changes」を参照してください。

2025 年 1 月 16 日

修正済みの問題

- 軽微なバグ修正。

2024 年 12 月 19 日

修正済みの問題

- 軽微なバグ修正。

2024 年 12 月 12 日

修正済みの問題

- 軽微なバグ修正。

2024 年 11 月 26 日

修正済みの問題

- 軽微なバグ修正。

2024 年 11 月 13 日

修正済みの問題

- 軽微なバグ修正。

2024 年 10 月 30 日

修正済みの問題

- 軽微なバグ修正。

2024 年 10 月 22 日

修正済みの問題

- 軽微なバグ修正。

2024 年 10 月 1 日

修正済みの問題

- 軽微なバグ修正。

2024 年 9 月 20 日

拡張機能

- 脅威ではないとして再分類されたメッセージに対する、エンジン分類子の応答性が改善されました。

修正済みの問題

- 軽微なバグ修正。

2024 年 9 月 4 日

修正済みの問題

- 軽微なバグ修正。

2024 年 8 月 23 日

拡張機能

- パブリック API クライアントのログイン情報は 1 年後に失効します。これは 2025 年 7 月から適用されます。ログイン情報の有効期限まで 90 日以内になると、バナーが表示されます。新しいログイン情報は、Cisco Secure Email Threat Defense UI の [管理（Administration）] > [API クライアント（API Clients）] から作成できます。

修正済みの問題

- 軽微なバグ修正。

2024 年 8 月 12 日

修正済みの問題

- 軽微なバグ修正。

2024 年 7 月 29 日

修正済みの問題

- 軽微なバグ修正。

2024 年 6 月 27 日

修正済みの問題

- 軽微なバグ修正。

2024 年 6 月 12 日

修正済みの問題

- .doc および .docx ファイルの QR コード分析が復旧しました。URL が抽出され、分析用としてエンジンに送信されます。

2024 年 5 月 29 日

修正済みの問題

- 最近の更新により、フィッシングテストのバイパスルールでの送信者情報の処理方法で予期しない問題が発生した可能性があります。これらの問題を解決するために、更新を取り消して 3 月 19 日より前の動作に戻します。既存のフィッシングテストのバイパスルールが再生成され、数日後に有効になる予定です。バイパスルールの使用に関するその他のガイダンスについては、バイパスルールに関するアドバイザリの概要（17 ページ）を参照してください。
- 軽微なバグ修正。

2024 年 5 月 14 日

修正済みの問題

- 軽微なバグ修正。

2024 年 4 月 30 日

拡張機能

- ユーザーアカウントが、[アカウント（Accounts）] ドロップダウンリストの下にアルファベット順で表示されるようになりました。
- パブリック API のレート制限が、北米とヨーロッパのリージョンの企業に適用されるようになりました。
  - API キーは、**[管理（Administration）] > [API クライアント（API Clients）]** から生成できます。
  - ヘッダー x-api-key の要求に API キーを含める必要があります。これを行わない場合、要求は失敗します。
  - テナントあたりの現在のレート制限は 5 リクエスト / 秒、バースト制限は 10 リクエスト / 秒、1 日のクォータは 5000 リクエストです。制限数に達した場合は、サポートに連絡して上限の引き上げを要求してください。
- W3C URL が電子メールから抽出されず、Cisco Secure Email Threat Defense UI に表示されなくなりました。

修正済みの問題

- 軽微なバグ修正。

2024 年 4 月 16 日

拡張機能

- メッセージ検索 API の最近の更新により、判定インジケータ、アクションインジケータ、添付ファイルとリンク、および最後のアクションに基づいてメッセージをフィルタ処理できます。
- パブリック API のレート制限が、インドとオーストラリアのリージョンの企業に適用されるようになりました。
  - API キーは、**[管理（Administration）] > [API クライアント（API Clients）]** から生成できます。
  - ヘッダー x-api-key の要求に API キーを含める必要があります。これを行わない場合、要求は失敗します。
  - テナントあたりの現在のレート制限は 5 リクエスト / 秒、バースト制限は 10 リクエスト / 秒、1 日のクォータは 5000 リクエストです。制限数に達した場合は、サポートに連絡して上限の引き上げを要求してください。

修正済みの問題

- 軽微なバグ修正。

2024 年 4 月 3 日

修正済みの問題

- 軽微なバグ修正。

2024 年 3 月 19 日

拡張機能

- このリリースでは、新しい [メッセージレポート（Message Report）] ページが導入されています。このページでは、拡張メッセージビューとタイムラインビューを組み合わせ、追加機能を導入します。新しい機能は次のとおりです。
  - ネットワーク管理者および管理者ユーザーがエンドユーザーに表示されるメッセージを確認できる電子メールプレビュー。この機能では、MS Graph API を使用してメールボックスからメッセージを取得します。

    注：ユーザーが電子メールをプレビューすると、監査ログレコードが作成されます。監査ログは、**[管理（Administration ）] > [ビジネス （Business）] > [初期設定（Preferences）]** からダウンロードできます。
  - 過去 30 日間にメッセージの送信者が送信したメッセージの合計数と脅威メッセージの合計数が表示される、[送信者メッセージ（Sender Messages）] グラフ。
  - メッセージを受信したエンドユーザーのメールボックスのリストを示すメールボックスリスト。このリストには、メッセージが最後の修復アクションの前に開封されたかどうかと、メッセージの修復エラーが表示されます。

  詳細については、『Cisco Secure Email Threat Defense User Guide』を参照してください。
- フィッシングテストのバイパスメッセージルールは、エンベロープ送信者の電子メールアドレスに対して、送信者の電子メールアドレスまたはドメインの基準のみと一致するようになりました。
- パブリックレポート API の最近の更新には、次のものが含まれます。
  - 上位 10 の脅威送信者レポートとレトロスペクティブ判定カウントレポート。
  - 日付範囲が最大 90 日に増加しました。
- 大きなファイルで断続的にクラッシュを引き起こす問題があるため、.doc ファイルの QR コード検出を削除しました。この機能はできるだけ早く元に戻す予定です。

修正済みの問題

- 軽微なバグ修正。

2024 年 3 月 4 日

拡張機能

- 修復の改善：発信メッセージと内部メッセージの場合、[受信トレイに移動（Move to Inbox）] アクションは、メッセージを受信トレイではなく、メッセージの最初の送信者の [送信済み（Sent）] フォルダに移動します。

修正済みの問題

- 軽微なバグ修正。

2024 年 2 月 21 日

拡張機能

- QR コード検出が、より多くのファイルタイプで使用できるようになりました。以前に発表されたグラフィックファイルに加えて、pdf、word、xls、および ppt ファイルに存在する QR コードから URL が抽出され、分析のためにエンジンに送信されます。

2025 年 5 月 21 日

修正済みの問題

軽微なバグ修正。

2024 年 2 月 6 日

拡張機能

- 混合方向は、UI と API から削除されました。この値は、Microsoft によって入力されなくなりました。
- パブリック API の最近の更新には、次のものが含まれます。
  - 新しいレポート API：方向ごとにスキャンされたメッセージの合計、判定ごとのトラフィックの合計、および脅威メッセージを受信した上位 10 のターゲット。
  - メッセージ検索 API の更新：テクニックでメッセージをフィルタリングできるようになりました。

修正済みの問題

- 軽微なバグ修正。

2024 年 2 月 1 日

拡張機能

- QR コードの検出
  - URL は、メッセージ本文と .jpg、.jpeg、および .png 添付ファイルにある QR コードから抽出されます。これらの URL は、メッセージに含まれる他の URL とともに分析されます。
  - QR コードの URL は、[リンク（Links）] セクションの展開されたメッセージビューに表示されます。
  - URL に悪意があると見なされると、悪意のある URL テクニックが表示されます。
  - QR コードのあるメッセージについては、QR コード検出テクニックが表示されます。このテクニックは、今後のリリースですべての QR コードに対して使用できるようになります。

2024 年 1 月 30 日

拡張機能

- Cisco Security 製品全体の一貫性を高めるために、Cisco Secure Email Threat Defense UI 全体でスタイルを変更します。変更点には次の項目が含まれます。
  - ダウンロード、ヘルプ、通知、およびユーザー設定には、ページヘッダーからアクセスできます。
  - 以前は画面の上部にあったメニュー項目には、左側のメニューからアクセスできます。

修正済みの問題

- 軽微なバグ修正。

2025 年 5 月 21 日

2024 年 1 月 18 日

修正済みの問題

- 軽微なバグ修正。

2023 年 12 月 13 日

拡張機能

- メッセージルールを削除できるようになりました。以前は、ルールを無効にすることしかできませんでした。
- 影響力の高い人員リストが一般に使用可能になりました。このリストを使用して、ユーザー偽装攻撃から組織を保護します。
  - 組織内の最大 100 人の重要人物のリストを作成できます。リストはエンジンに送信され、表示名と送信者の電子メールアドレスをより詳細に調査します。
  - 構成された情報からの逸脱は、有害と判定されたメッセージの [判定の詳細（Verdict Details）] パネルで [ユーザー偽装（User Impersonation）] として識別されます。
- パブリック API の最近の更新には、次のものが含まれます。
  - メッセージ検索 API のリクエスト本文に **“isRetroVerdict”: true** を追加することで、レトロ判定に基づいてメッセージをフィルタ処理する機能。
  - パブリック API にレート制限が実装されました。API キーは、**[設定（Settings）] > [管理（Administration）] > [API クライアント（API Clients）]** から生成できます。

    注： レート制限は 2024 年 2 月から適用されます。ヘッダー x-api-key の要求に API キーを含める必要があります。これを行わない場合、要求は失敗します。
- メッセージ ダウンロード レポートでは、[自動修復（Auto Remediation）] 列の名前が [修復方法（Remediation Method）] に変更され、メッセージが自動、手動、または API によって修復されたかどうかが示されます。

修正済みの問題

- 軽微なバグ修正。

2023 年 12 月 4 日

修正済みの問題

- 軽微なバグ修正。

2023 年 11 月 16 日

拡張機能

- パブリック API への追加により、プログラムでメッセージを修復および再分類できます。詳細については、API ガイドを参照してください。このガイドには、Cisco Secure Email Threat Defense の [ヘルプ（Help）] メニューまたは https://developer.cisco.com/docs/message-search-api からアクセスできます。

修正済みの問題

- 軽微なバグ修正。

2023 年 10 月 31 日

拡張機能

- Email Threat Defense は、エンジン分析のために添付ファイルをスキャンし、URL を抽出するようになりました。
  - 250 を超えるファイルタイプがサポートされ、エンジンに送信されます。
  - ファイル分析は、5 つのレベルのアーカイブファイル（.zip ファイルなど）をサポートします。
- 許可リストと判定のオーバーライド メッセージ ルールでは、スパムとグレイメールに加えて、脅威判定を選択できます。

修正済みの問題

- 軽微なバグ修正。

2023 年 10 月 18 日

修正済みの問題

- 軽微なバグ修正。

2023 年 10 月 3 日

拡張機能

- ホームページと影響レポートの [脅威（Threats）] および [不要なメッセージ（Unwanted Messages）] アイコンをクリックできるようになりました。

修正済みの問題

- 軽微なバグ修正。

2023 年 9 月 20 日

拡張機能

- タイムラインビューには次の情報が表示されるようになりました。
  - 修復時にメッセージを開封したメールボックスのリスト。
  - メッセージの修復エラーと、エラーが発生したメールボックスに関する情報。タイムラインからエラーログをダウンロードすることもできます。

修正済みの問題

- 軽微なバグ修正。

2023 年 9 月 8 日

修正済みの問題

- 軽微なバグ修正。

2023 年 8 月 28 日

拡張機能

- 小さな EML ファイルがすぐにダウンロードされるようになりました。より大きなファイルには、引き続き [ダウンロード（Downloads）] ページからアクセスできます。
- [受信者検索（Recipient Search）] フィールドに [エンベロープ受信者（Envelope To）] フィールドと [配信先（Delivered To）] フィールドが含まれるようになりました。

廃止通知

- ユーザーインターフェイスの Organizational-Bcc、およびパブリックメッセージ検索 API 応答の bccAddresses は廃止され、今後のリリースで削除される予定です。BCC アドレスが [To/Cc] フィールドでキャプチャされるようになりました。

修正済みの問題

- 軽微なバグ修正。

2023 年 8 月 10 日

拡張機能

- 管理者は、**[設定（Settings）] > [管理（Administration）] > [ユーザー（Users）]** ページでユーザーのロールを変更できるようになりました。
- 展開されたメッセージビューには、ジャーナルヘッダーから抽出された追加の受信者データが表示されます。[To/Cc]、[エンベロープ受信者（Envelope To）]、および [配信先（Delivered To）] の最大 3 つの個別のスクロール可能なセクションがあります。
- [メッセージルールのステータス（Message Rules Status）] 列のフィルタは、最後に選択した設定がデフォルトでブラウザに保存されます。

修正済みの問題

- 軽微なバグ修正。

2023 年 7 月 31 日

修正済みの問題

- 軽微なバグ修正。

2023 年 7 月 18 日

拡張機能

- [影響力の高い人員（High Impact Personnel）] ページには、ユーザーが過去 30 日間に偽装された回数が表示されます。

- パブリックメッセージ検索 API の最近の更新には、次のものが含まれます。
  - 拡張された検索機能：受信者の電子メールアドレス、送信者の電子メールアドレス、およびインターネットメッセージ ID。
  - API 応答で、メッセージが手動で再分類されたかどうかを示すことができるようになりました。
  - パブリック API ガイドへのリンクは、Cisco Secure Email Threat Defense の [ヘルプ（Help）] メニューからアクセスできます。このガイドは、https://developer.cisco.com/docs/message-search-api/ にあります。

修正済みの問題

- 軽微なバグ修正。

2023 年 6 月 29 日

修正済みの問題

- 軽微なバグ修正。

2023 年 6 月 19 日

拡張機能

- メッセージルールをステータスでフィルタ処理して、アクティブまたは無効なルールを表示または非表示にすることができます。

修正済みの問題

- 軽微なバグ修正。

2023 年 6 月 9 日

拡張機能

- メッセージグラフとクイックフィルタが更新されました。
  - 1 日の始まりが週単位のビューで明確に強調表示されるようになり、特定の日を掘り下げることができます。
  - メッセージのフィルタ処理に使用できるリンクであることを示すために、脅威と方向のメトリックが青色で表示されます。

修正済みの問題

- 軽微なバグ修正。

2023 年 5 月 19 日

拡張機能

- このリリースで Cisco Secure Email Threat Defense パブリック API が導入されました。API を使用すると、安全でスケーラブルな方法でプログラムからデータにアクセスして使用することができます。API ドキュメントについては、https://doc.api.etd.cisco.com/ を参照してください。

修正済みの問題

- 軽微なバグ修正。

2023 年 5 月 11 日

拡張機能

- 2023 年 5 月 11 日以降に作成されたビジネスについては、スパムとグレイメールの分析がデフォルトでオフになります。この設定は、[ポリシー（Policy）] ページで調整できます。
- メッセージグラフとクイックフィルタ
  - [メッセージ（Messages）] ページの上部に、脅威とメッセージのグラフィカル表示が表示されます。
  - 脅威とカテゴリのブレークアウトにより、合計を表示し、脅威を簡単にフィルタ処理できます。
  - 検疫の合計が表示され、フィルタ処理できます。
  - メッセージの方向の合計が表示され、フィルタ処理できます。
- ホームページの [スキャンされたメッセージ（Messages Scanned ）] グラフが、1 時間（日次表示）、3 時間（週次グラフポイント）、および 1 日（週次 X 軸ラベル）のカスタム期間を持つ [メッセージ（Messages）] ページにピボットするようになりました。

修正済みの問題

- 軽微なバグ修正。

2023 年 4 月 20 日

拡張機能

- Secure Malware Analytics の検出が [判定の詳細（Verdict Details）] パネルに [悪意のある侵入兆候（Malicious Behavioral Indicators）] のテクニックとして表示されます。
- Secure Endpoint の検出が [判定の詳細（Verdict Details）] パネルに [低スコアのファイルレピュテーション（Low File Reputation）] のテクニックとして表示されます。
- メッセージ受信者がソートされ、影響力の高い人員が最初にリストされます。

修正済みの問題

- 軽微なバグ修正。

2023 年 4 月 13 日

拡張機能

- Secure Email Threat Defense はさらに SecureX と統合されています。特定の監視可能なメッセージを統合型製品の SecureX ピボットメニューから直接隔離できるようになりました。さらに、ピボットを使用して、Secure Email Threat Defense で検索を開始できます。ピボットできる観測対象は次のとおりです。
  - [電子メールアドレス（Email Address）]
  - [電子メールメッセージ ID（Email Message ID）]

- [電子メールの件名（Email Subject）]
- [ファイル名（File Name）]
- [送信者 IP（Sender IP）]
- [SHA 256（SHA 256）]
- [URL（URL）]

2023 年 3 月 22 日

拡張機能

- メッセージソースとして Cisco Secure Email Cloud Gateway を使用するビジネス向けの新しい認証なしモードが導入されました。この可視性のみのモードを使用すると、Microsoft への認証を行わずに、トラフィックを Secure Email Threat Defense に送信できます。このモードでメッセージを修復することはできません。この構成をサポートするように、新しいビジネスの初期設定フローと [ポリシー（Policy）] ページの設定が更新されています。

修正済みの問題

- 2023 年 3 月 12 日の夏時間の調整で導入されたグラフの表示方法に関する問題が解決されました。

2023 年 3 月 15 日

拡張機能

- [ユーザ プロファイル（User Profile）] メニューから、Secure Email Threat Defense システムステータスページへのリンクを使用できます。

修正済みの問題

- 軽微なバグ修正。

2023 年 2 月 27 日

拡張機能

- [ポリシー（Policy）] ページに、スパムとグレイメールの分析と修復をオンまたはオフにする新しいオプションがあります。オフにすると、スパムとグレイメールおよび無用なメールのパネルとオプションが削除されます。
  - 既存のアカウントについては、スパムとグレイメールの分析がデフォルトでオンになります。
  - Cisco SEG 構成の今後のアカウントについては、スパムとグレイメールの分析がデフォルトでオフになります。スパムとグレイメールの分析は、SEG によってすでに実行されています。
- 影響力の高い人員リストの個人用に構成された情報からの逸脱は、有害と判定されたメッセージの [判定の詳細（Verdict Details）] パネルで [テクニック（Technique）] として識別されます。

修正済みの問題

- 一部のお客様の環境で、Secure Email Threat Defense に到達する前に HTTP ヘッダーが削除されるというログインの問題が発生していました。この問題は解決されました。

2023 年 2 月 8 日

修正済みの問題

- 軽微なバグ修正。

2023 年 1 月 31 日

拡張機能

- ホームページに、日次と週次のデータの表示を切り替えるオプションがあります。
- [ポリシー（Policy）] ページの [インポートされたドメイン（Imported Domains）] セクションに、インポートされたドメインの総数と自動修復用にマークされたドメインの数が表示されます。リストには、部分一致検索でリストをフィルタ処理できる検索機能があります。
- 影響レポートの開始日が編集可能になりました。これにより、30 日の範囲、またはカレンダーの月ビューの月の最初の日付を選択できます。
- [メッセージ（Messages）] ページのフィルタで、フィルタがいつ適用されたかが示されます。フィルタの設定をデフォルトに簡単に戻せるように、ページの上部に新しい [すべてリセット（Reset All）] リンクが追加されています。[フィルタのリセット（Reset Filters）] ボタンは、使いやすいようにフィルタパネルの下部にあります。
- タイムラインビューに、受信、修復、再分類などのイベントの秒数が表示されるようになりました。
- 再分類のホバーテキストに日付と時刻が表示されるようになりました。
- 初期フィールドトライアルの新機能：影響力の高い人員リスト
  - 管理者は、最大 100 人のリストを作成して Talos に送信し、表示名と送信者の電子メールアドレスをさらに精査することができます。
  - **注**：今すぐリストを構築すると、今後のリリースで [判定の詳細（Verdict Details）] に [ユーザのなりすまし（User Impersonation）] のテクニックが表示されるようになります。

修正済みの問題

- 軽微なバグ修正。

2022 年 12 月 15 日

拡張機能

- [メッセージ（Messages）] ページのフィルタを使用して、送信者の IP アドレスで検索できるようになりました。
- 通知に [すべて消去（Clear All）] ボタンが追加されました。
- [設定（Settings）] > [ダウンロード（Downloads）] > [EML ダウンロード（Download EML）] ページで、メッセージの件名をクリックしてメッセージに簡単に戻ることができます。

修正済みの問題

- 軽微なバグ修正。

2022 年 11 月 17 日

拡張機能

- [メッセージ（Messages）] ページの [送信者（Sender）] 列の名前が [送信者（表示名 / フレンドリ名）（Sender (Display Name/Friendly From)）] に変更されました。

修正済みの問題

- 軽微なバグ修正。

2022 年 11 月 9 日

拡張機能

- メッセージソースとして Cisco Secure Email Cloud Gateway を使用できるようになりました。この初期リリースでは、サポートは Microsoft O365 メールボックスに限定されています。この構成をサポートするように、新しいビジネスの初期設定フローと [ポリシー（Policy）] ページの設定が更新されています。
- ブランドのなりすましの検出がサポートされるようになりました。構成の変更は必要ありません。現在 1500 のブランドがインデックスに登録されており、今後さらに追加される予定です。
- ホームページのダッシュボードに、過去 24 時間のビジネスの状態をすばやく表示する新しいウィジェットとグラフがあり、フィルタ処理されたメッセージのリストにすばやくピボットできます。内容は次のとおりです。
  - 脅威：BEC、詐欺、フィッシング、悪意のある検出の数が表示されます。
  - 無用なメール：スパムとグレイメールの検出のスパークライングラフが表示されます。
  - スキャンされたメッセージ：メッセージトラフィックのグラフが表示されます。
  - 侵害された可能性のあるアカウント：組織内から脅威メッセージを送信していることが確認された内部アドレスがリストされます。
  - クイックメッセージフィルタ：レトロスペクティブ判定、隔離状態のメッセージ、およびメッセージルールが適用されたメッセージへのクイックリンクが表示されます。
- Secure Email Threat Defense の新しいステータスページは https://ciscosecureemailthreatdefense.statuspage.io で利用できます。登録すると、ステータスに変化があったときに更新情報を受け取ることができます。

修正済みの問題

- 軽微なバグ修正。

2022 年 10 月 25 日

拡張機能

- Cisco Secure Email Cloud Mailbox は、Cisco Secure Email Threat Defense に名前が変更されました。この名前は、インターフェイス、ドキュメント、およびマーケティング資料全体で、段階的に変更されます。

修正済みの問題

- 軽微なバグ修正。

使用上の注意

バイパスルールに関するアドバイザリの概要

バイパスルールを作成および使用する場合は、次の重要な注意事項に留意してください。

- バイパスルールによって、ルール条件に一致するメッセージのスキャンと保護がすべてバイパスされます。顧客の従業員に対するセキュリティ認識トレーニング（フィッシングテスト）以外のユースケース、または組織のセキュリティ メールボックスに送信されるエンド メールボックス ユーザーからの報告には、バイパスルールを使用しないでください。これらは、バイパスルールでサポートされている唯一のシナリオです。他のすべてのシナリオでは、判定のオーバーライドルールまたは許可ルールのみがサポートされます。
- バイパスルールの基礎として、フィッシングテストベンダーが提供する専用の送信者 IP アドレス /CIDR ブロックのみを使用することを強く推奨します。
- フィッシングテストベンダーが専用の送信者 IP アドレス /CIDR ブロックを提供できない場合は、バイパスルールの送信者ドメインまたは電子メールアドレスを使用すると、スプーフィングされた可能性のあるメッセージをバイパスできます。
- 送信者の電子メール認証が、ベンダーの SPF レコードによって厳密に適用されていること、組織のアップストリーム エッジ電子メール制御によって強力に適用されていること、および指定された送信者ドメインまたは送信者電子メール アドレスが、バイパスルールと一致させることを目的とするすべてのメッセージの最後の Return-Path ヘッダーと完全に一致していることを個別に検証した場合を除き、バイパスルールの送信者ドメインまたは電子メールアドレスは使用しないでください。
- サポートケースを開いて、既存のバイパスルールが上記のガイダンスに準拠していることを検証するための支援を依頼します。

Microsoft Excel のセルサイズの制限

Microsoft Excel では、セルあたり 32,767 文字の制限があります。データを CSV にエクスポートしてから Excel で開くと、文字数制限を超えるデータは次の行に移動されます。

Microsoft アカウントに姓が含まれていない場合、Microsoft で Security Cloud Sign On にサインインできない

Microsoft 365 では、アカウントに名前と姓を定義する必要はありません。姓が含まれていない Microsoft アカウントで認証しようとすると、Cisco Security Cloud Sign On から次のエラーが表示されます。

> *400 Bad Request. Unable to create the user. Required properties are missing.*

この問題を回避するには、Microsoft 365 アカウントに姓と名の両方が定義されていることを確認します。

メッセージを手動で再分類すると、トレンドが遅延する

メッセージを手動で再分類すると、[トレンド（Trends）] ページに変更が反映されるまでに最大で 1 時間の遅延が生じることがあります。

既知の問題

Microsoft 許可リストと安全な送信者

Microsoft の MSAllowList フラグにおける最近の変更により、個々のユーザ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おり、メッセージがユーザの許可リストに含まれる場合、Microsoft 許可リストが Cisco Secure Email Threat Defense で常に適用されることはありません。

Cisco 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。

カンバセーションビュー

カンバセーションビューを使用すると、次の問題が発生する場合があります。

- 追加のメッセージがない場合でも、[+] 記号はクリックするまで表示されたままです。
- 水平ノードは 9 個に制限されています。

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。