Deep Discovery™ Email Inspector 5.1

管理者ガイド

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

P/N: APEM59194/210115_JP_R5 (2024/04)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Deep Discovery Email Inspector により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Deep Discovery Email Inspector における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

第 5 章：ポリシー

第 8 章：管理

はじめに

本書について

この章の内容は次のとおりです。

Deep Discovery Email Inspector のドキュメント

Deep Discovery Email Inspector のドキュメントには次のものがあります。

表 1. 製品ドキュメント

ドキュメント	説明
管理者ガイド	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 管理者ガイドには、Deep Discovery Email Inspector を配置、設定、および管理するための詳細な手順と、Deep Discovery Email Inspector の概念や機能に関する説明が記載されています。
インストールガイド	製品に付属の PDF ドキュメントです。トレンドマイクロの Web サイトからダウンロードすることもできます。 インストールガイドには、Deep Discovery Email Inspector をインストールおよび配置するための要件と手順が説明されています。
Syslog コンテンツマッピングガイド	Syslog コンテンツマッピングガイドには、Deep Discovery Email Inspector でサポートされるイベントログ形式に関する情報が含まれています。
クイックスタートガイド	クイックスタートガイドには、Deep Discovery Email Inspector をネットワークに接続して初期設定を実行するための手順がわかりやすく説明されています。
Readme	Readme には、オンラインヘルプや印刷されたドキュメントには記載されていない最新の製品情報が含まれています。新機能、既知の問題、および製品リリースの履歴に関する情報を確認できます。
オンラインヘルプ	Deep Discovery Email Inspector 管理コンソールからアクセスできる Web ベースのドキュメントです。 オンラインヘルプには、Deep Discovery Email Inspector のコンポーネントと機能、Deep Discovery Email Inspector を設定するために必要な手順が説明されています。

ドキュメント	説明
サポートポータル	サポートポータルは、問題の解決およびトラブルシューティングの情報を参照できるオンラインデータベースです。製品の既知の問題に関する最新の情報を得ることができます。サポートポータルにアクセスするには、以下の Web サイトをご覧ください。 https://success.trendmicro.com/dcx/s/?language=ja

対象読者

この Deep Discovery Email Inspector のドキュメントは、IT 管理者とセキュリティアナリストを対象としています。ここでは次のトピックを含め、読者にネットワークと情報セキュリティに関する十分な知識があることを前提としています。

- ネットワークトポロジ
- メールルーティング
- SMTP

ただし、サンドボックス環境や脅威イベントの相関分析については、読者がその知識を持っていないものとして説明します。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記規則	説明
 注意	設定上の注意
 ヒント	推奨事項

表記規則	説明
 重要	必要な設定や初期設定、および製品の制限事項に関する情報
 警告!	重要な操作と設定オプション

トレンドマイクロについて

トレンドマイクロは、サイバーセキュリティにおける 世界的企業として、安全にデジタル情報をやり取りできる環境の実現に向けて継続的に取り組んでいます。個人消費者、企業、および政府機関向けの革新的ソリューションである XGen セキュリティ戦略を巧みに利用することで、つながるセキュリティをデータセンター、クラウドワークロード、ネットワーク、およびエンドポイントにもたらします。

Amazon Web Services、Microsoft、および VMware などの主要な環境に合わせて最適化された階層化ソリューションにより、組織は、今日の脅威から重要な情報を自動的に保護することができます。トレンドマイクロの提供する Connected Threat Defense によって、脅威インテリジェンスのシームレスな共有が可能になるとともに、一元化された可視性と調査の提供によって、組織の柔軟性が最大限に高まります。

トレンドマイクロのお客さまには、自動車、銀行、医療、電気通信、および石油といった産業にわたる、Fortune Global 500 企業の上位 10 社のうち 9 社が含まれています。

世界 50 か国の 6,500 人を超える従業員と、最先端のグローバルな脅威調査および脅威インテリジェンスによって、トレンドマイクロは「つながる世界」のセキュリティを確保できるようお客さまを支援します。詳細については、次のサイトを参照してください。https://www.trendmicro.com

第 1 章

はじめに

この章では、製品の特長、機能、およびセキュリティテクノロジについて説明します。

この章の内容は次のとおりです。

Deep Discovery Email Inspector について

Deep Discovery Email Inspector は、メールメッセージ内の不審なリンクや添付ファイルがネットワーク上の脅威となる前に、対象の検索、シミュレーション、および分析を行い、高度な標的型攻撃やサイバー攻撃の発生を抑止します。既存のメールネットワークトポロジと統合するように設計されているため、メールトラフィックフロー内のメール転送エージェントとして、またはネットワーク上の脅威や望ましくないスパムメールメッセージを監視するアウトオブバンドアプライアンスとして 動作できます。

新機能

表 1-1. Deep Discovery Email Inspector5.1 の新機能

機能/強化点	詳細
Trend Vision One の統合	Trend Vision One との統合により、ハイブリッド環境における連携したセキュリティ分析が可能になります。 重要 統合設定を行う前に、サポート窓口までお問い合せのうえ、最新の HotFix または Patch を適用してください。
証明書の管理	Deep Discovery Email Inspector で証明書を管理することにより、Transport Layer Security (TLS) 環境での安全なコンソールアクセスと SMTP 通信が可能になります。
メールアドレスの変更	メールアドレスの変更機能により、次の操作を実行できるようになります。 • メッセージのエンベロープやヘッダの送信者または受信者のアドレスを書き換える • メールアドレスのドメインを書き換える

機能/強化点	詳細
TLS 通信の強化	TLS 通信が強化され、次のものがサポートされるようになります。 • TLS 1.3 • 指定されたドメインおよび IP アドレスに基づくメッセージ転送の安全な接続
送信メッセージの DANE	Deep Discovery Email Inspector は DANE (名前付きエンティティの DNS ベースの認証) をサポートしており、SMTP サーバ ID を検証することで送信メッセージを保護します。
ポリシー設定の強化	ポリシー管理機能が強化され、次の設定が提供されるようになります。 • 検出メッセージのブラインドカーボンコピー (BCC) の指定された受信者への送信 • 検出メッセージの受信者の変更 • ポリシーでの送信者と受信者の除外の設定 • ポリシーオブジェクトとしてのアドレスグループの設定 • 社内メールのスプーフィング防止 • ポリシールールに基づくメッセージスタンプの適用
受信メッセージの送信者と受信者の検証	受信メッセージのセキュリティを強化する、次のセキュリティ設定が提供されるようになります。 • 不明な送信者 IP アドレスまたはドメインからのメッセージの拒否 • 不明な受信者へのメッセージの拒否 • 送信者フィルタにおけるメッセージのヘッダ From アドレスの一致

機能/強化点	詳細
Time-of-Click プロテクションの強化	Time-of-Click プロテクション機能が強化され、次のものが含まれるようになります。 • 検出された URL のリダイレクトページのカスタマイズ • 検出された URL の Syslog 転送
仮想アナライザの機能強化	次の機能を含めるように仮想アナライザが強化されています。 • サンドボックス分析での OpenDocument ファイルタイプ • Windows 10 May 2020 Update イメージのサポート
検出機能の向上	検出機能の向上により保護機能が強化されます。このリリースでは次の機能がサポートされます。 • ALG および EGG アーカイブファイルの検索 • パスワード保護された ALG および EGG アーカイブファイルと OpenDocument ファイルの検索のための復号化 • 検索のための OpenDocument ファイルからの URL の抽出 • 検出画面での情報漏えい対策フォレンジックスデータの表示
承認済み送信者リストとブロックする送信者リストの強化	承認済み送信者リストとブロックする送信者リストの設定が強化され、次のものが含まれるようになります。 • 送信者リストのインポートとエクスポート • メールドメイン設定でのワイルドカードのサポート

機能/強化点	詳細
ライセンス管理の強化	ゲートウェイモジュール ライセンスのみでの利用をサポートします。 注意 日本語版では、引き続きゲートウェイモジュールライセンスはオプションのみでの提供となります。
新しいファイバネットワークインタフェースカード (NIC) のサポート	ハードウェアモデル 7200、7300、および 9200 に 10Gbps ファイバ NIC を取り付けることで、追加のデータポートがサポートされるようになります。 注意 日本語版では、本 NIC カードはサポートしておりません。
Deep Discovery Director 5.3 の統合	Deep Discovery Director 5.3 との統合がサポートされます。 注意 2021 年 7 月現在、日本における本製品のリリースは準備中です。最新の提供状況については、以下をご参照ください。 http://www.go-tm.jp/ddd
Deep Discovery Analyzer 7.0 の統合	Deep Discovery Analyzer 7.0 との統合がサポートされ、Linux の ELF ファイルとシェルスクリプトファイルを送信できるようになります。

機能/強化点	詳細
仮想配信の強化	VMware ESXi 6.7 および 7.0 での仮想アプライアンスのインストールがサポートされるようになります。 注意 日本語版では、仮想アプライアンスは提供しておりません。
インラインでのアップグレードのサポート	Deep Discovery Email Inspector では、次のバージョンから 5.1 への設定の自動移行オプションが提供されます。 • Deep Discovery Email Inspector 5.1 Critical Patch ビルド 1565

機能と利点

Deep Discovery Email Inspector には次の機能と利点があります。

高度な検出

Deep Discovery Email Inspector の高度な検出技術により、スピアフィッシング攻撃やソーシャルエンジニアリング攻撃などのメールメッセージ内の標的型の脅威を検出します。

- レピュテーション技術とヒューリスティック技術で、未知の脅威やドキュメントの脆弱性攻撃コードを捕捉します。
- ファイルハッシュ分析により、安全でないファイルやアプリケーションをブロックします。
- パスワード保護されたファイルや短縮 URL に隠された脅威を検出します。
- 機械学習型検索テクノロジで、未知のセキュリティリスクを検出します。
- メールメッセージ内の不正 URL をクリック時にブロックします。

可視性、分析、および処理

脅威をリアルタイムに視認して、直感的な方法で複数レベルの詳しい分析を実行できます。このため、セキュリティ担当者は、実際のリスクに集中してフォレンジック分析を詳細に行い、封じ込めや修正の措置をただちにとることができます。

柔軟な配置

既存のスパムメール対策/ウイルス対策ネットワークトポロジと統合するように設計されているため、メールトラフィックフロー内のメール転送エージェントとして、またはネットワーク上の脅威を監視するアウトオブバンドアプライアンスとして動作できます。

ポリシー管理

ポリシー管理を使用すると、管理者は、検索条件に基づいてメッセージに予防処置を実施できます。ポリシーを作成して、次のタスクを実行できます。

- 不審メールメッセージを削除します。
- 不審メールメッセージをブロックして隔離します。
- 特定のメールメッセージを受信者に配信できるようにします。
- 不審添付ファイルを削除します。
- 不審なリンクをブロックページや警告ページにリダイレクトします。
- メールの件名にカスタマイズした文字列をタグ付けします。
- ポリシールールに一致した場合に受信者に通知します。
- 検出されたメールメッセージのコピーをアーカイブサーバに 送信します。

カスタムの脅威シミュレーションサンドボックス

仮想アナライザのサンドボックス環境で、パスワード保護されたアーカイブや文書ファイルなどのファイル、あるいは URL を開いて、不正な動作をテストできます。仮想アナライザは、脆弱性攻撃コード、コマンド&コントロール (C&C) とボットネット接続、およびその他の不審な動作や特徴を検出します。

メール添付ファイルの分析

複数の検出エンジンとサンドボックスシミュレーションを使用して、添付ファイルを調査します。サポートされるファイルタイプは、実行可能ファイル、Microsoft Office、PDF、Web コンテンツ、および圧縮ファイルと広範囲にわたります。

埋め込まれた URL の分析

レピュテーション技術、ページの直接分析、およびサンドボックスシミュレーションを使用して、メールメッセージに埋め込まれた URL を調査します。

Email Encryption

Email Encryption により、Deep Discovery Email Inspector ではポリシーの設定に基づいて次のタスクを実行できます。

- トレンドマイクロの ID ベース暗号化 (IBE) を使用して暗号化されたメッセージを複合および検索する
- MTA モードでの安全な配信のためにメッセージを暗号化する

Deep Discovery Email Inspector では、メッセージの送信元のメールクライアントまたはプラットフォームに関わらずメッセージを復号または暗号化できます。

注意

TAP/BCC モードで動作する Deep Discovery Email Inspector が暗号化メッセージを受信した場合、Deep Discovery Email Inspector はメッセージの復号と検索のみを行います。TAP/BCC モードでは、Deep Discovery Email Inspector はメッセージを暗号化しません。

スパムメール検索

スパムメールとは、主に広告を目的とした迷惑メールのことです。Deep Discovery Email Inspector では、次のコンポーネントを使用してスパムメールメッセージのフィルタを 行います。

- トレンドマイクロのスパムメール対策エンジン

- トレンドマイクロのスパムメールパターンファイル

トレンドマイクロのスパムメール対策エンジンでは、スパムメールのシグネチャおよびヒューリスティックルールを 使用してメールメッセージをフィルタします。スパムメール対策エンジンは、メールメッセージを検索し、ルールやパターンファイル内のパターンに一致する程度に応じて各メールメッセージにスパムスコアを割り当てます。Deep Discovery Email Inspector は、このスパムスコアと、選択したスパムメール検出レベルまたはユーザ指定の検出しきい値を比較します。スパムスコアが検出レベルまたはしきい値を超えると、Deep Discovery Email Inspector はスパムメールメッセージに対して処理を実行します。

たとえば、スパムメールメッセージの送信者は、メールメッセージ内で感嘆符を多用したり連続して使用する (!!!!) ことがあります。そのようなメールメッセージを検出すると、Deep Discovery Email Inspector は当該メッセージのスパムスコアを高く設定します。

スパムメール対策エンジンには、メール添付ファイル (スクリプトファイルや Microsoft Office マクロウェアを含む) に高度な脅威検索を実行して不正プログラムを検出する、メール不正プログラム脅威検索エンジンも含まれています。

グレーメール検索

グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールです。Deep Discovery Email Inspector では、マーケティングメッセージ、ニュースレター、ソーシャルネットワークの通知、およびフォーラムの通知をグレーメールとして検出します。Deep Discovery Email Inspector では、次の 2 つの方法でグレーメールメッセージを 識別します。

- 送信元 IP アドレスにスコアを割り当てるメールレピュテーションサービス
- メッセージコンテンツを 識別するトレンドマイクロのスパムメール対策エンジン

送信者フィルタ

次の送信者フィルタ 設定を行うことで、スパムメールメッセージの送信者を IP アドレスまたはメールアドレスのレベルでブロックできます。

- 承認済み送信者リストとブロックする送信者リスト
- Email Reputation Services (ERS)
- ディレクトリハーベスト攻撃 (DHA) からの保護
- バウンスメール攻撃からの保護
- SMTP トラフィックスロットリング

送信者の認証

次の送信者の認証規格をサポートすることで、メールによるフィッシング詐欺やスプーフィングに使用される手法を効果的に検出し、防御します。

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)

さらにスプーフィング防止のため、DKIM 署名を使用して送信メッセージに署名するように Deep Discovery Email Inspector を設定できます。

コンテンツフィルタ

Deep Discovery Email Inspector でコンテンツフィルタルールを作成して、次のことを実行できます。

- メッセージの内容と添付ファイルを分析することで、適切でないと指定したコンテンツが受信者に配信されないようブロックする
- Microsoft Office や PDF ファイルの添付ファイル内のアクティブコンテンツ (マクロなど) を検出して削除する

情報漏えい対策

情報漏えい対策は、偶然のまたは意図的な漏えいから組織のデジタル資産を保護します。情報漏えい対策により、管理者は次のことが可能になります。

- 保護すべきデジタル資産の識別
- メールメッセージを介したデジタル資産の転送を制限または防止するポリシーの作成

- 組織で確立された個人情報保護基準への準拠

エンドユーザメール隔離

Deep Discovery Email Inspector には、スパムメールの管理を強化するエンドユーザメール隔離 (EUQ) 機能があります。スパムメールと判定されたメッセージは隔離されるため、エンドユーザがメッセージを再確認して、削除、隔離解除、または配信を許可することができます。インライン処理リンクを含むエンドユーザメール隔離通知を自動的に送信するように Deep Discovery Email Inspector を設定できます。Web ベースのエンドユーザメール隔離管理コンソールを使用することで、ユーザは各自の個人アカウントおよび、自分が所属する配布リストのスパムメールの隔離方法を管理したり、送信者を承認済み送信者リストに追加したりできます。

ソーシャルエンジニアリング攻撃対策

ソーシャルエンジニアリング攻撃対策は、メールメッセージからソーシャルエンジニアリング攻撃に関連する不審な動作を検出します。ソーシャルエンジニアリング攻撃対策が有効になると、Deep Discovery Email Inspector は、メールヘッダ、件名行、本文、添付ファイル、および SMTP プロトコル情報を含む、各メール転送の複数の要素から不審な動作を検出します。

パスワードの導出

さまざまなヒューリスティック技術とお客さま提供のキーワードを使用して、パスワード保護されたアーカイブや文書ファイルを復号します。

新しい脅威の特徴

Web サイトを書き換えたり、システムの大規模な中断によって悪評を得ることで満足していた攻撃者が、今度はサイバー戦争によって大金を稼いだり、重要なデータを盗んだり、主要なインフラシステムを妨害したりできることに気付きました。

標的型攻撃は、標的とするネットワークへの永続的なアクセスを目的とした、人物または組織に対する長期のサイバースパイ活動です。この攻撃によって、企業の機密データを抽出したり、標的のネットワークに損害を与えることができます。感染したネットワークは、他の組織への攻撃に使用することもできます。この場合は元の攻撃者を追跡することが難しくなります。

スピアフィッシング攻撃

スピアフィッシング攻撃とは、フィッシング攻撃と標的型不正プログラムを組み合わせたものです。攻撃者は、上司や同僚など正規の送信者を装った巧妙なメールメッセージにより、少数の標的となる従業員にスピアフィッシングメッセージを送信します。このようなスピアフィッシングメッセージには、多くの場合、不正 Web サイトへのリンクや不正な添付ファイルが含まれます。添付ファイルは、Microsoft Word、Excel、および Adobe 製品の脆弱性を悪用する場合があります。また添付ファイルは、実行可能ファイルを含む圧縮アーカイブである可能性もあります。受信者が添付ファイルを開くと、不正ソフトウェアがシステムの悪用を試みます。多くの場合、策略を実行するために、不正ソフトウェアは安全に見える無害なドキュメントを起動します。

いったん不正ソフトウェアが実行されると、システム上で休止状態となるか、またはコマンド&コントロール (C&C) サーバと通信してさらに指示を受信しようとします。

C&C コールバック

次の処理は、通常不正ソフトウェアがインストールされ、C&C サーバに通信が返されたときに実行されます。

- 「ダウンローダ」と呼ばれるソフトウェアが、不正プログラムを自動的にダウンロードしてインストールします。
- C&C サーバを監視している人物 (攻撃者) が、処理を実行して接続に応答します。「リモートアクセス型トロイの木馬」 (RAT) と呼ばれるソフトウェアにより、攻撃者はシステムを調べたり、ファイルを抽出したり、感染したシステムで実行するための新しいファイルをダウンロードしたり、システムのビデオカメラやマイクを起動したり、画面キャプチャやキーストロークを取得したり、コマンドシェルを実行できるようになります。

攻撃者はさらに永続的なアクセスポイントを取得して、感染したネットワーク内を動き回ります。また、ネットワーク上にあるデータの収集のためにユーザのアカウント情報を盗もうとします。成功すると、収集されたデータはネットワークから別の環境に持ち出され、さらに調査されます。

この移動は、ゆっくりとしたペースで行われるため、検出されません。検出された場合は、一時的に活動を休止し、その後再開します。組織によってネットワークから排除された場合は、攻撃サイクルを最初からやり直します。

新しい解決策

Deep Discovery Email Inspector は、メールメッセージ内の不審なリンク、添付ファイル、およびソーシャルエンジニアリング攻撃パターンがネットワークを脅かす前にこれらを調査することで、スピアフィッシング攻撃やサイバー攻撃を防ぎ、ビジネスメール詐欺 (BEC) から保護します。既存のメールネットワークトポロジと統合するように設計されているため、メールトラフィックフロー内のメール転送エージェントとして (MTA モード)、またはネットワーク上の脅威や望ましくないスパムメッセージを監視するアウトオブバンドアプライアンスとして (BCC モードまたは SPAN/TAP モード) 動作できます。

どちらの配置方法を選択しても、不審な添付ファイル、埋め込まれたリンク (URL)、スパムメール、コンテンツ違反、および特徴についてメールメッセージが調査されます。メールメッセージが不正な動作を示した場合は、そのメールメッセージがブロックされ、セキュリティ管理者に不正な活動が通知されます。

Trend Micro Smart Protection Network 内でメールメッセージの既知の脅威が検索された後、シミュレーションのために仮想アナライザのサンドボックス環境に不審なファイルと URL が渡されます。仮想アナライザはパスワード保護されたアーカイブや文書ファイルなどのファイルを開き、URL にアクセスして、脆弱性攻撃コード、コマンド&コントロール (C&C) とボットネット接続、およびその他の不審な動作や特徴をテストします。

Deep Discovery Email Inspector は、メールメッセージの調査後、複数階層の脅威分析を使用してリスクを評価します。Deep Discovery Email Inspector のメール検索機能、仮想アナライザ、または Trend Micro Smart Protection Network で割り当てられた最大のリスクまたはスパムスコアに基づいて、リスクレベルが計算されます。

メールメッセージは、割り当てられたリスクレベルまたはスパムスコアとポリシー設定に従って処理されます。メールメッセージをブロックおよび隔離したり、受信者にメールメッセージを送信したり、不審添付ファイルを削除したり、不審なリンクをブロックページまたは警告ページにリダイレクトしたり、メールメッセージに受信者に通知する文字列をタグ付けするように、

Deep Discovery Email Inspector を設定してください。Deep Discovery Email Inspector がネットワークの脅威や望ましくないスパムメールメッセージを監視する一方で、ユーザはダッシュボードウィジェットやレポートにアクセスしてさらに詳しく調査することができます。

仮想アナライザ

仮想アナライザは、統合製品、管理者、および調査担当者によって SSH 経由で送信されたオブジェクトを管理および分析するための安全な仮想環境です。カスタムサンドボックスイメージにより、ご使用のシステム設定に適した環境でファイル、URL、レジストリエントリ、API コール、およびその他のオブジェクトを監視できます。

仮想アナライザは静的および動的な分析を実行して、次に示すカテゴリオブジェクトの重要な特徴を特定します。

- 反セキュリティおよび自己保存
- 自動起動またはその他のシステムの設定
- ディセプション、ソーシャルエンジニアリング
- ファイルの削除、ダウンロード、共有、または複製
- ハイジャック、リダイレクト、またはデータ窃取
- 不正、不良、または既知の不正プログラムの兆候
- プロセス、サービス、またはメモリオブジェクトの変更
- ルートキット、クローキング
- 不審ネットワークまたは不審メッセージングアクティビティ

分析時、仮想アナライザはコンテキストで特徴を評価し、評価の累計に基づいてオブジェクトのリスクレベルを割り当てます。また、調査で使用可能な分析レポート、不審オブジェクトのリスト、PCAP ファイル、および OpenIOC ファイルも生成します。

高度な脅威検索エンジン

高度な脅威検索エンジン (以下、ATSE: Advanced Threat Scan Engine) はパターンベースの検索とヒューリスティック検索を組み合わせて使用し、ドキュ

メントのセキュリティホール悪用や標的型攻撃で使用されるその他の脅威を検出します。

新機能は次のとおりです。

- ゼロデイ 脅威の検出
- 埋め込まれたセキュリティホール悪用コードの検出
- 既知の脆弱性の検出ルール
- ファイル改変の処理が強化された解析機能

機械学習型検索

トレンドマイクロの機械学習型検索は、高度な機械学習技術を使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどのファイル機能を使用した詳細なファイル分析により未知のセキュリティリスクを検出します。

不明なファイルやあまり普及していないファイルを検出すると、Deep Discovery Email Inspector は、高度な脅威検索エンジン (ATSE) でファイルを検索してファイル特性を抽出し、Trend Micro Smart Protection Network でホストされる機械学習型検索エンジンにレポートを送信します。機械学習型検索では、不正プログラムモデリングにより、サンプルを不正プログラムモデルと比較し、可能性スコアを割り当て、ファイルに含まれる潜在的な不正プログラムの種類を判別します。

ネットワークへの脅威の拡散を防ぐために、Deep Discovery Email Inspector は該当するファイルの「隔離」を試みます。

機械学習型検索は、未知の脅威およびゼロデイ攻撃から環境を保護するのに役立つ強力な検索方法です。

Web レピュテーションサービス

トレンドマイクロの Web レピュテーションテクノロジは、世界最大規模のドメインレピュテーションデータベースを利用して、Web サイトの経過期間、場所の変更の履歴、および不正プログラムの動作分析により発見される不審な活動の兆候など (ユーザの個人情報を盗むために仕掛けたフィッシング詐欺など) の要素に基づいてレピュテーションスコアを割り当てることで、Web ドメインの信頼性を追跡します。精度を高めて誤検出を減らすために、トレンドマイクロの Web レピュテーションでは、サイト全体を分類またはブロッ

クする代わりに、レピュテーションスコアをサイト内の特定のページまたはリンクに割り当てます。これは、正規サイトの一部のみが不正侵入されることが多く、レピュテーションは時間の経過と共に動的に変化する可能性があるからです。

ソーシャルエンジニアリング攻撃対策

ソーシャルエンジニアリング攻撃対策は、メールメッセージからソーシャルエンジニアリング攻撃に関連する不審な動作を検出します。ソーシャルエンジニアリング攻撃対策が有効になると、Deep Discovery Email Inspector は、メールヘッダ、件名行、本文、添付ファイル、および SMTP プロトコル情報を含む、各メール転送の複数の要素から不審な動作を検出します。

Trend Vision One

Trend Vision One は検出と対応をエンドポイントを超えて拡張し、より広範な可視性と専門家によるセキュリティ分析を提供することで、より多くの脅威の検出と早期の迅速な対応を実現します。Trend Vision One により、効果的に脅威に対応し、侵害の重大度と範囲を最小限に抑えることができます。

Apex Central

Apex Central は、ゲートウェイ、メールサーバ、ファイルサーバ、および企業のデスクトップレベルでトレンドマイクロの製品やサービスを管理する一元化された管理コンソールです。Apex Central の Web ベースの管理コンソールによって、1 か所からネットワーク全体の管理対象製品とサービスを監視できます。

システム管理者は Apex Central を使用して、感染、セキュリティ違反、ウイルス侵入ポイントなどに関連した活動を監視し、レポートを生成できます。またコンポーネントをダウンロードして管理下製品に配信することで、一貫性のある最新の保護状態を維持できます。Apex Central では手動アップデートと予約アップデートの両方を実行でき、製品をグループでまたは個別に設定および管理できる柔軟性が追加されています。

Deep Discovery Director

Trend Micro Deep Discovery Director (以下、Deep Discovery Director) は、Deep Discovery 製品へのアップデート、アップグレード、および仮想アナライザイメージの配信と、Deep Discovery 製品の設定の複製およびログの集約

を一元管理する管理ソリューションです。さまざまな組織上およびインフラストラクチャ上の要求に対応するため、Deep Discovery Director には Distributed Mode や Consolidated Mode などの柔軟な配信オプションが用意されています。

詳細については、「Deep Discovery Director 管理者ガイド」を参照してください。

第 2 章

基本設定

この章では、Deep Discovery Email Inspector を起動して初期設定を行う方法について説明します。

この章の内容は次のとおりです。

導入タスク

導入タスクでは、Deep Discovery Email Inspector を可能なかぎり迅速に起動し稼働するために必要なすべての手順の概要を示します。各手順のリンクをクリックすると、ドキュメントで後述する詳細説明が表示されます。導入プロセスは、BCC モード、SPAN/TAP モード、および MTA モードのいずれも同じです。

手順

1. ネットワークを設定して管理コンソールにアクセスします。

   詳細については、23 ページの「管理コンソールのアクセス設定」を参照してください。

2. 管理コンソールを開きます。

   詳細については、25 ページの「管理コンソール」を参照してください。

3. Deep Discovery Email Inspector の製品ライセンスをアクティベートします。

   詳細については、457 ページの「製品ライセンスをアクティベートまたは更新する」を参照してください。

4. システム時刻を設定します。

   詳細については、421 ページの「システム時刻を設定する」を参照してください。

5. ネットワークを設定します。

   詳細については、411 ページの「ネットワークを設定する」を参照してください。

6. 動作モードを設定します。

   詳細については、414 ページの「動作モード」を参照してください。

7. SMTP サーバを設定します。

   詳細については、419 ページの「通知 SMTP サーバを設定する」を参照してください。

8. メールのサイズ制限と除外を設定します。

   詳細については、323 ページの「制限と除外を設定する」を参照してください。

9. 仮想アナライザのネットワークを設定します。

   詳細については、240 ページの「仮想アナライザのネットワークとフィルタを設定する」を参照してください。

10. 仮想アナライザのイメージをアップロードします。

    詳細については、236 ページの「仮想アナライザのイメージをアップロードする」を参照してください。

    重要

    分析を実行するには、仮想アナライザのイメージが 1 つ以上必要です。

11. アーカイブファイルと文書ファイルを開くためのパスワードを設定します。

    詳細については、258 ページの「ファイルのパスワードを追加する」を参照してください。

12. ダウンストリーム MTA のメールルーティングを設定します。

    詳細については、321 ページの「メッセージ配信を設定する」を参照してください。

13. すべての重大なアラートに、通知の受信者を 1 つ以上追加します。

    詳細については、178 ページの「アラート」を参照してください。

14. (オプション) ポリシーを設定します。

    詳細については、112 ページの「ポリシーを設定する」を参照してください。

15. (オプション) ポリシーの例外を設定します。

    詳細については、165 ページの「ポリシー除外」を参照してください。

16. (オプション) 一元管理のため、Apex Central または Deep Discovery Director に登録します。

詳細については、350 ページの「Apex Central」または 356 ページの「Deep Discovery Director」を参照してください。

17. アップストリーム MTA または SPAN/TAP デバイスを設定します。

    a. Deep Discovery Email Inspector が BCC モードまたは MTA モードで動作している場合は、アップストリーム MTA がメールトラフィックを Deep Discovery Email Inspector にルーティングするように設定します。

    注意

    アップストリーム MTA を設定する際には、MTA モードと BCC モードで異なる設定が必要です。MTA の設定については、MTA ベンダーが提供するサポート文書を参照してください。

    - MTA モードでは、MTA がメールトラフィックを Deep Discovery Email Inspector に転送するように設定します。
    - BCC モードでは、MTA がメールトラフィックを Deep Discovery Email Inspector にコピーするように設定します。

    b. Deep Discovery Email Inspector が SPAN/TAP モードで動作している場合は、SPAN/TAP デバイスがトラフィックを Deep Discovery Email Inspector にミラーリングするように設定します。

    注意

    SPAN/TAP デバイスの設定については、SPAN/TAP デバイスのベンダーが提供するサポート文書を参照してください。

Deep Discovery Email Inspector にアクセスするための要件

次の表は、Deep Discovery Email Inspector を管理するコマンドラインインタフェースと管理コンソールにアクセスするための最小要件を示しています。

表 2-1. Deep Discovery Email Inspector へのアクセス要件

アプリケーション	要件	詳細
SSH クライアント	SSH プロトコルバージョン 2	コマンドラインインタフェースの画面サイズを 80 列と 24 行に設定します。
Microsoft Edge	Windows 10 以降	管理コンソールへのアクセスがサポートされるブラウザのみを使用してください。 初期設定時に設定したデータポート IP アドレスを使用して、次の URL を指定します。 `https://[アプライアンスの IP アドレス]:443`
Mozilla Firefox	バージョン 75 以降	
Google Chrome	バージョン 81 以降	

注意

- 1280 x 1024 以上の解像度をサポートするモニタを使用してコンソールを表示することをお勧めします。
- SSH サービスは初期設定で無効になり、有効な場合は開始されません。SSH サービスを有効にするには、478 ページの「configure service ssh enable」を参照してください。SSH サービスを開始するには、491 ページの「start service ssh」を参照してください。

管理コンソールのアクセス設定

インストールの完了後、サーバが再起動されコマンドラインインタフェース (CLI) がロードされます。管理コンソールにアクセスするために、Deep Discovery Email Inspector のネットワークを設定します。

次の手順は、CLI にログオンして次に示す必要なネットワーク設定を行う方法を示します。

- ホスト名
- 管理 IP アドレスとネットマスク
- ゲートウェイ

- DNS

手順

1. 初期設定のアカウント情報で CLI にログオンします。
   - ユーザ名: `admin`
   - パスワード: `ddei`
2. プロンプトで「`enable`」と入力して <Enter> キーを押し、特権モードに切り替えます。
3. 初期設定パスワードの「`trend#1`」を入力し、<Enter> キーを押します。

   プロンプトが>から#に変更されます。
4. 次のコマンドでネットワークを設定します。

   ```
   configure network basic
   ```
5. 次のネットワーク設定を実行し、設定を入力するたびに <Enter> キーを押します。

   注意

   IPv6 の設定は任意です。

   - ホスト名 (Host name)
   - IPv4 アドレス (IPv4 address)
   - サブネットマスク (Subnet mask)
   - IPv4 ゲートウェイ (IPv4 gateway)
   - 優先 IPv4 DNS (Preferred IPv4 DNS)
   - 代替 IPv4 DNS (Alternate IPv4 DNS)
   - IPv6 アドレス (IPv6 address)
   - プレフィックス長 (Prefix length)
   - IPv6 ゲートウェイ (IPv6 gateway)

- 優先 IPv6 DNS (Preferred IPv6 DNS)
- 代替 IPv6 DNS (Alternate IPv6 DNS)

6. 「Y」と入力して設定を確認し、再起動します。

   Deep Discovery Email Inspector が指定されたネットワーク設定を行い、すべてのサービスを再起動します。

これで、初期設定が完了し、管理コンソールにアクセスできるようになりました。

注意

後で CLI にログオンして、追加の設定、トラブルシューティング、管理タスクを実行できます。CLI の詳細については、467 ページの「コマンドラインインタフェースの使用」を参照してください。

管理コンソール

Deep Discovery Email Inspector には管理コンソールが組み込まれており、これを使用して製品を設定し、管理できます。

管理コンソールは、サポートされる Web ブラウザを使用して表示します。サポートされるブラウザについては、22 ページの「Deep Discovery Email Inspector にアクセスするための要件」を参照してください。

管理コンソールにアクセスする前に必要なネットワーク設定の詳細については、23 ページの「管理コンソールのアクセス設定」を参照してください。

ログオンするには、ブラウザ画面を開き、次の URL を入力します。

`https://<アプライアンスの IP アドレス>`

注意

管理コンソールの初期設定の IP アドレス/サブネットマスクは `192.168.252.1/255.255.0.0` です。

Deep Discovery Email Inspector の管理コンソールには、次のいずれかの方法でログオンできます。

- 26 ページの「ローカルアカウントを使用してログオンする」
- 26 ページの「シングルサインオンでログオンする」

ローカルアカウントを使用してログオンする

手順

1. [ログオン] 画面で、管理コンソールのログオンアカウント情報 (ユーザ名とパスワード) を入力します。

   初めてログオンする場合は、次の初期設定の管理者ログオンアカウント情報を使用します。

   - ユーザ名: `admin`
   - パスワード: `ddei`

2. [ログオン] をクリックします。
3. 初めてログオンする場合は、アカウントのパスワードを変更した後、管理コンソールにアクセスできるようになります。

注意

ハードウェアモデル 7300 で、管理コンソールにハードウェアモデルの正しい情報を表示するには、HotFix (ビルド 1394) をダウンロードしてインストールします。

詳細については、https://success.trendmicro.com/dcx/s/solution/000291496?language=ja を参照してください。

シングルサインオンでログオンする

Deep Discovery Email Inspector で SAML 統合に必要な設定を行うことで、既存の ID プロバイダの認証情報を使用して Deep Discovery Email Inspector の管理コンソールにアクセスできます。

詳細については、392 ページの「SAML 統合」を参照してください。

手順

1. [ログオン] 画面で、ドロップダウンリストからサービス名を選択します。
2. [シングルサインオン (SSO)] をクリックします。

   組織のログオンページが自動的に表示されます。
3. 画面の指示に従ってアカウントの認証情報を入力し、Deep Discovery Email Inspector の管理コンソールにアクセスします。

管理コンソールの操作

管理コンソールには次の要素があります。

表 2-2. 管理コンソールの要素

セクション	詳細
バナー	管理コンソールのバナーには次の項目があります。 • 製品のロゴと名前:クリックするとダッシュボードに移動します。詳細については、30 ページの「ダッシュボードの概要」を参照してください。 • 現在ログオンしているユーザの名前:クリックし、[パスワードの変更] を選択してアカウントのパスワードを変更するか (439 ページの「パスワードを変更する」を参照)、[ログオフ] を選択して管理コンソールからログアウトします。 • システム時刻:現在のシステム時刻とタイムゾーンを表示します。 • アプライアンスの IP アドレス:Deep Discovery Email Inspector アプライアンスの IP アドレスを表示します。 • ネットワークトラフィック:受信および送信ネットワークスループットを表示します。
メインメニューバー	製品を設定するためのメニュー項目が含まれます。[ダッシュボード] など一部のメニュー項目は、クリックすると対応する画面が表示されます。その他のメニュー項目は、クリックしたりマウスを重ねたりするとサブメニュー項目が表示され、そのサブメニュー項目をクリックすると対応する画面が表示されます。
ヘルプ	[ヘルプ] をクリックすると、現在の画面の詳細情報が表示されます。

第 3 章

ダッシュボード

この章の内容は次のとおりです。

ダッシュボードの概要

ダッシュボードを使用して、ネットワークの健全性を監視します。管理コンソールのユーザアカウントのそれぞれに、独立したダッシュボードが存在します。ユーザアカウントのダッシュボードを変更しても、他のユーザアカウントのダッシュボードには影響しません。

ダッシュボードは、次のユーザインタフェース 要素で構成されます。

要素	説明
タブ	タブはウィジェットのコンテナを提供します。 詳細については、30 ページの「タブ」を参照してください。
ウィジェット	ウィジェットは、ダッシュボードの中核的なコンポーネントです。 詳細については、32 ページの「ウィジェット」を参照してください。

タブ

タブはウィジェットのコンテナを提供します。ダッシュボードのタブはそれぞれ 20 個までのウィジェットを保持できます。ダッシュボードは最大 30 のタブをサポートします。

事前定義済みのタブ

ダッシュボードには、それぞれに一連のウィジェットが格納された事前定義済みのタブが付属しています。これらのタブは、名前の変更、削除、およびウィジェットの追加が可能です。

次の事前定義済みタブがあります。

- 概要
- 脅威の監視
- 傾向の上位
- システムステータス
- 仮想アナライザ

タブのタスク

次の表は、タブ関連のすべてのタスクのリストです。

項目	解説
タブの追加	追加アイコン ( ) をクリックして、新しいタブの名前を入力します。
タブ名の変更	タブ名の上にマウスを重ねて下向き矢印をクリックし、[名前の変更] をクリックして新しいタブの名前を入力します。
タブのウィジェットレイアウトの変更	1. タブ名の上にマウスを重ねて下向き矢印をクリックします。 2. [レイアウトの変更] をクリックします。 3. 表示される画面から、新しいレイアウトを選択します。 4. [保存] をクリックします。
タブの削除	タブ名の上にマウスを重ねて下向き矢印をクリックし、[削除] をクリックして確定します。

項目	解説
タブのスライドショーの再生	1. タブ表示の右側にある [設定] ボタンをクリックします。  2. [タブのスライドショー] コントロールを有効にします。 3. 次のタブに切り替わるまで、各タブを表示する時間を選択します。

ウィジェット

ウィジェットはダッシュボードの中核的なコンポーネントです。ウィジェットにはグラフが表示され、システムステータスの監視と脅威の追跡を実行できます。

ウィジェットのタスク

すべてのウィジェットはウィジェットフレームワークに 従っており、同様のタスクオプションを用意しています。

表 3-1. ウィジェットオプションメニュー

タスク	手順
新しいウィジェットの追加	1. ダッシュボードでタブをクリックします。 2. タブ表示の右側にある [設定] ボタンをクリックします。 3. [ウィジェットの追加] をクリックします。 4. 追加するウィジェットを選択します。 • ウィジェットの上部にあるドロップダウンリストで、カテゴリを選択して対象を絞り込みます。 • 画面の上部にある検索テキストボックスを使用して、特定のウィジェットを検索します。 5. [追加] をクリックします。
ウィジェット名の変更	1. 設定アイコン (>) をクリックします。 2. 新しいタイトルを入力します。 3. [保存] をクリックします。
ウィジェットデータの更新	ウィジェットデータを更新するには、更新アイコン (>) をクリックします。
ヘルプの表示	ヘルプを表示するには、疑問符アイコン (>) をクリックします。オンラインヘルプにウィジェットの使用方法が表示されます。
ウィジェットの削除	削除アイコン (>) をクリックします。
同一タブ内でのウィジェットの移動	ドラッグアンドドロップを使用して、ウィジェットをタブ内の別の場所に移動できます。
異なるタブへのウィジェットの移動	ドラッグアンドドロップを使用して、ウィジェットをタブタイトルに移動します。ウィジェットのコピーまたは移動を選択するオプションが表示されます。
期間の変更	使用可能な場合は [期間] ドロップダウンメニューをクリックして、期間を選択します。

タスク	手順
ウィジェットのサイズ変更	複数列のタブでウィジェットのサイズを変更するには、カーソルでウィジェットの右端をポイントし、カーソルを左または右に移動します。

概要

[概要] ウィジェットには、検出のサマリー、隔離されたメッセージと処理されたメッセージ、違反件数の多いポリシー、およびメッセージキューのステータス情報が表示されます。

[検出のサマリー] ウィジェット

[検出のサマリー] ウィジェットには、脅威の種類別の検出件数が表示されます。

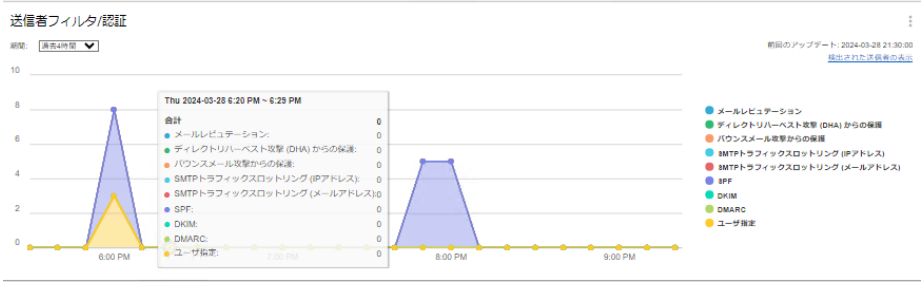
このグラフは選択した期間に基づいて作成されています。Y 軸は検出数を表しています。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、期間と検出数が表示されます。

凡例の検出カテゴリをクリックすると、グラフ上の関連するデータが表示または非表示になります。

[検出されたメッセージの表示] をクリックすると、すべて検出が表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

送信者フィルタ/認証ウィジェット



[送信者フィルタ/認証] ウィジェットには、送信者フィルタおよび認証の設定に基づいた検出数が表示されます。

このグラフは選択した期間に基づいて作成されています。Y 軸は検出数を表しています。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、期間と検出数が表示されます。

凡例の検出カテゴリをクリックすると、グラフ上の関連するデータが表示または非表示になります。

[検出された送信者の表示] をクリックすると、送信者フィルタ/認証ログが表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

隔離メッセージウィジェット

[隔離メッセージ] ウィジェットには、隔離フォルダのサイズと隔離メッセージの総数が表示されます。ドーナツグラフのセクションにマウスカーソルを重ねると、隔離の理由ごとのメッセージ数が表示されます。

凡例の検出カテゴリをクリックすると、グラフ上の関連するデータが表示または非表示になります。

[隔離メッセージの表示] をクリックすると、すべての隔離メッセージが表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

ポリシー違反の上位ウィジェット

[ポリシー違反の上位] ウィジェットには、選択した期間に検出されたメッセージが違反した、共通のポリシーと関連するルールの上位が表示されます。[違反] の数字をクリックすると、違反したポリシーに対して検出されたメッセージが表示されます。

[検出されたメッセージの表示] をクリックすると、検出されたすべてのメッセージが表示されます。

メッセージキューウィジェット

[メッセージキュー] ウィジェットには、受信したばかりのメッセージの数、配信可能なメッセージの数、および配信不能により遅延されたメッセージの数が表示されます。メッセージキューのログを表示する場合は、[メッセージ] の数字をクリックします。

処理されたメッセージウィジェット

[処理されたメッセージ] ウィジェットには、選択した期間内に Deep Discovery Email Inspector で処理されたメッセージ数がメッセージのカテゴリまたは方向ごとに表示されます。Y 軸はメールメッセージ件数を示しています。X 軸はメッセージのカテゴリまたは方向を示しています。

脅威の監視

脅威の監視関連のウィジェットを表示すると、不正な着信メッセージ、攻撃の発生元、影響を受ける受信者、および隔離されたメッセージについて理解できます。

攻撃元ウィジェット

[攻撃元] ウィジェットは、不審メールトラフィックを送信したすべての送信元 MTA を示すインタラクティブなマップを 表示します。

攻撃の発生元とは、不審メッセージをルーティングするパブリック IP アドレスを持つ最初の MTA です。たとえば、不審メッセージが IP1 (送信者)→IP2 (MTA: 225.237.59.52)→IP3 (会社のメールゲートウェイ)→IP4 (受信者) とルーティングされた場合は、225.237.59.52 (IP2) が攻撃の発生元として識別されます。攻撃の発生元を判別することで、地域の攻撃パターンまたは同じメールサーバが関係する攻撃パターンを特定できます。

マップ上の任意の位置にカーソルを重ねると、その攻撃の発生元で起きたイベントについて確認できます。

マップ上のハイライトされた地域をクリックすると、その地域を発生元とする攻撃について詳細を表示できます。

注意

[データがありません] グループの攻撃は、位置情報なしで検出された攻撃を表します。

たとえば、Deep Discovery Email Inspector がメッセージルーティング情報からパブリック IP アドレスを取得できない場合、位置情報を利用することはできません。

右上隅の [すべての攻撃元を表示] をクリックすると、[攻撃元] 画面が表示します。

リスク高のメッセージ数ウィジェット

[リスク高のメッセージ数] ウィジェットは、すべての着信不正メッセージを表示します。高リスクメッセージには、不正プログラムによる通信、不正な接続先、不正な動作パターン、または明確な危険を示す文字列が含まれます。

このグラフは選択した期間に基づいて作成されています。Y 軸はメールメッセージ件数を示しています。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、高リスクメッセージの件数と期間が表示されます。

[検出されたメッセージの表示] をクリックすると、すべて検出が表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

検出されたメッセージウィジェット

[検出されたメッセージ] ウィジェットは、不正な特徴および不審な特徴を示すすべてのメールメッセージを表示します。不審な特徴には、異常な動作、擬似データ、不審または不正な動作パターン、およびシステムが危険にさらされている可能性を示唆するためより詳しい調査を必要とする文字列が含まれます。

注意

Apex Central には [高度な脅威を含むメールメッセージ] という同様のウィジェットがあり、複数の Deep Discovery Email Inspector アプライアンスのデータが集計されます。

このグラフは選択した期間に基づいて作成されています。Y 軸はメールメッセージ件数を示しています。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、高リスクメッセージの件数と期間が表示されます。

凡例の項目をクリックすると、そのメトリックに関連するデータが表示または非表示になります。

[検出されたメッセージの表示] をクリックすると、すべて検出が表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

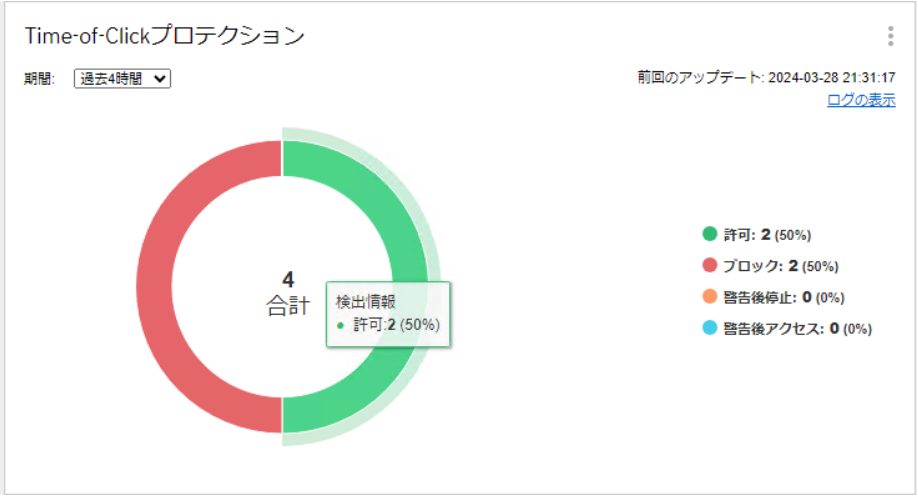
高度な脅威インジケータ

[高度な脅威インジケータ] ウィジェットには、すべてのメールメッセージで検出された高度な脅威インジケータの種類、件数、およびリスクレベルが表示されます。

この表は選択した期間の検出情報を示しています。[高]、[中]、[低]、または [合計] の数字をクリックすると、検出の詳細が表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

[Time-of-Click プロテクション] ウィジェット



[Time-of-Click プロテクション] ウィジェットには、ユーザのクリック時に検出された URL の総数が表示されます。ドーナツグラフのセクションにマウスカーソルを重ねると、検出の処理ごとの URL 数が表示されます。

凡例の検出の処理をクリックすると、グラフ上の関連するデータが表示または非表示になります。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

傾向の上位

傾向の上位関連のウィジェットを表示すると、不審メッセージのコンテンツやコールバック先を含むネットワーク内の上位の活動を把握し、ネットワークに影響を及ぼす脅威の特徴を理解できます。

添付ファイルの名前の上位ウィジェット

[添付ファイルの名前の上位] ウィジェットは、不審および高リスクのメールメッセージに含まれる最も一般的な添付ファイルを表示します。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出

数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

添付ファイルの種類の上位ウィジェット

[添付ファイルの種類の上位] ウィジェットは、検出されたメッセージに含まれる最も一般的な添付ファイルタイプを表示します。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

影響を受ける受信者の上位ウィジェット

[影響を受ける受信者の上位] ウィジェットは、最も大量の不審メッセージを受け取った受信者を表示します。

注意

Apex Central には [高度な脅威のメール受信者の上位] という同様のウィジェットがあり、複数の Deep Discovery Email Inspector アプライアンスのデータが集計されます。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

不審メッセージの影響を受けたすべての受信者を表示するには、[すべての受信者の表示] をクリックします。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

攻撃元の上位ウィジェット

[攻撃元の上位] ウィジェットは、ネットワークを攻撃する最も活動的な IP アドレスを表示します。

攻撃の発生元とは、不審メッセージをルーティングするパブリック IP アドレスを持つ最初の MTA です。たとえば、不審メッセージが IP1 (送信者)→IP2 (MTA: 225.237.59.52)→IP3 (会社のメールゲートウェイ)→IP4 (受信者) とルーティングされた場合は、225.237.59.52 (IP2) が攻撃の発生元として識別されます。攻撃の発生元を判別することで、地域の攻撃パターンまたは同じメールサーバが関係する攻撃パターンを特定できます。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

選択した期間に検出されたすべての攻撃の発生元を表示するには、[すべての攻撃元を表示] をクリックします。

注意

ダッシュ (-) は位置情報が利用できないことを意味します。

たとえば、Deep Discovery Email Inspector がメッセージルーティング情報からパブリック IP アドレスを取得できない場合、位置情報を利用することはできません。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

仮想アナライザからのコールバックホストの上位ウィジェット

[仮想アナライザからのコールバックホストの上位] ウィジェットは、不審および高リスクのメールメッセージに含まれる最も一般的なコールバックホストを表示します。コールバックホストは、C&C サーバの IP アドレスまたはホスト名です。

仮想アナライザは Deep Discovery Email Inspector のメール検索機能からオブジェクト (ファイルまたは URL) を受信すると、そのオブジェクトが外部ネットワークアドレスに接続するかどうかを監視します。高リスクのオブジェ

クトは、既知の C&C サーバホストへのコールバックを実行しようとします。仮想アナライザは、送信されたサンプルが実行したすべての接続 (URL、IP アドレス、およびホスト名) をレポートします。これには、不正プログラムの可能性があるコールバックやその他の不審な接続が含まれます。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

分析中に見つかったすべての不審ホストオブジェクトを表示するには、[すべてのコールバックホストの表示] をクリックします。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

仮想アナライザからのコールバック URL の上位ウィジェット

[仮想アナライザからのコールバック URL の上位] ウィジェットは、不審および高リスクのメールメッセージに含まれる最も一般的なコールバック URL を表示します。コールバック URL は、C&C サーバの Web アドレスです。

仮想アナライザは Deep Discovery Email Inspector のメール検索機能からオブジェクト (ファイルまたは URL) を受信すると、そのオブジェクトが外部ネットワークアドレスに接続するかどうかを監視します。高リスクのオブジェクトは、既知の C&C サーバホストへのコールバックを実行しようとします。仮想アナライザは、送信されたサンプルが実行したすべての接続 (URL、IP アドレス、およびホスト名) をレポートします。これには、不正プログラムの可能性があるコールバックやその他の不審な接続が含まれます。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

分析中に見つかったすべての不審 URL オブジェクトを表示するには、[すべてのコールバック URL の表示] をクリックします。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

メールの件名の上位ウィジェット

[メールの件名の上位] ウィジェットは、不審および高リスクのメールメッセージに含まれる最も一般的なメールメッセージの件名を表示します。

この表は選択した期間の検出情報を示しています。[検出数] または [リスク高のメッセージ] の数字をクリックすると、検出の詳細が表示されます。[検出数] には、高リスクのメッセージをはじめ、検出されたすべてのメールメッセージが含まれます。

選択した期間中に検出されたメッセージ内のメールの件名を表示するには、[すべてのメールの件名の表示] をクリックしてください。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

システムステータス

システムステータス関連のウィジェットを表示すると、異なる期間における異なるリスクレベルに対する全体的なメールメッセージ処理ボリュームと、現在の Deep Discovery Email Inspector アプライアンスハードウェアのステータスについて理解できます。ウィジェットは、システムパフォーマンスがメッセージの配信にどのように影響を及ぼしているかを視覚的に表します。

調査対象のボリュームウィジェット

[調査対象のボリューム] ウィジェットは、Deep Discovery Email Inspector が調査したすべてのメールメッセージ、添付ファイル、および埋め込みリンクを表示します。

このグラフは選択した期間に基づいて作成されています。Y 軸は、処理されたメールメッセージ、添付ファイル、または埋め込みリンクの合計数を表します。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、高リスクメッセージの件数と期間が表示されます。凡例内のアイテムをクリックすると、グラフ内でそのアイテムのオン/オフを切り替えることができます。

凡例の項目をクリックすると、そのメトリックに関連するデータが表示または非表示になります。

[ログの表示] をクリックすると、メッセージ追跡ログが表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

ハードウェアステータスウィジェット

[ハードウェアステータス] ウィジェットは、Deep Discovery Email Inspector アプライアンスの直前 5 秒間の CPU、メモリ、およびディスクの使用率を表示します。

注意

「ディスク使用量」とは、ディスクパーティションに格納されているデータ容量のことです。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

仮想アナライザ

仮想アナライザ関連のウィジェットを表示すると、処理時間、キューのサイズ、および分析中に発見された不審オブジェクトのボリュームに基づいて仮想アナライザのパフォーマンスを評価できます。

仮想アナライザに送信されるメッセージウィジェット

[仮想アナライザに送信されるメッセージ] ウィジェットには、処理するために仮想アナライザに送信されるメールメッセージの 5 分ごとの数が表示されます。

このグラフは選択した期間に基づいて作成されています。 Y 軸はメールメッセージ件数を示しています。 X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、仮想アナライザに送信されたメッセージの件数と期間が表示されます。

[キュー内の検出済みメッセージの表示] をクリックすると、現在分析中のメールメッセージが表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

仮想アナライザの平均処理時間ウィジェット

[仮想アナライザの平均処理時間] ウィジェットは、仮想アナライザがオブジェクトを受信した時点から分析を完了する時点までの平均時間を秒数で表示します。

このグラフは選択した期間に基づいて作成されています。Y 軸は、オブジェクトを分析するためにかかる平均時間を表します。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、高リスクメッセージの件数と期間が表示されます。

インスタンスを再割り当てするか、イメージを追加または削除するか、あるいは仮想アナライザ設定にその他の変更を行う場合は、[仮想アナライザの管理] をクリックします。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

仮想アナライザによって検出された不審オブジェクトウィジェット

[仮想アナライザによって検出された不審オブジェクト] ウィジェットは、仮想アナライザで見つかった不審オブジェクトを表示します。不審オブジェクトとは、システムの危険または損害を引き起こす可能性があるオブジェクトです。仮想アナライザでは、不審な IP アドレス、ホスト名、ファイル、および URL を検出して分析します。

このグラフは選択した期間に基づいて作成されています。Y 軸は検出された不審オブジェクトの件数を示しています。X 軸は期間を表しています。グラフ上の任意の場所にマウスカーソルを重ねると、高リスクメッセージの件数と期間が表示されます。

凡例の項目をクリックすると、そのメトリックに関連するデータが表示または非表示になります。

[不審オブジェクトの表示] をクリックすると、ネットワークに影響を及ぼす可能性のあるオブジェクトが表示されます。

ウィジェットの全般的なタスクについては、32 ページの「ウィジェットのタスク」を参照してください。

第 4 章

検出

この章の内容は次のとおりです。

検出されたリスク

検出されたリスクとは、不審メールメッセージによって示される潜在的な危険です。

Deep Discovery Email Inspector では、複数階層の脅威分析を使用してメールメッセージのリスクを評価します。メールメッセージを受信すると、Deep Discovery Email Inspector のメール検索機能により、トレンドマイクロ Smart Protection Network および高度な脅威検索エンジンで既知の脅威の有無が確認されます。そのメールメッセージに未知の特徴や不審な特徴がある場合は、メール検索機能により添付ファイルと埋め込まれた URL が仮想アナライザに送信され、さらに分析されます。仮想アナライザでは、不審なファイルおよび URL の動作をシミュレートして、潜在的な脅威を識別します。Deep Discovery Email Inspector の検索機能と仮想アナライザの間で割り当てられた最大のリスクに基づいて、メールメッセージにリスクレベルが割り当てられます。

Deep Discovery Email Inspector がメールメッセージを調査する方法の詳細については、13 ページの「新しい解決策」を参照してください。

メールメッセージのリスクレベル

次の表は、調査後のメールメッセージのリスクレベルを示しています。メールメッセージがどのような基準で高、中、低のリスクに分類されたかを確認するには、この表を参照してください。

表 4-1. メールメッセージのリスク定義

リスクレベル	説明
高	高リスクのメールメッセージは次のとおりです。 • 仮想アナライザに高リスクとして検出された未知の脅威の添付ファイル • YARA ルールに基づき高リスクとして検出された添付ファイル • 不審ファイルの一致に基づき高リスクとして検出された添付ファイル • 機械学習型検索およびメール不正プログラム脅威検索により検出された添付ファイル • ビジネスメール詐欺 • 仮想アナライザに高リスクとして検出されたリンク • 不審 URL の一致に基づき高リスクとして検出されたリンク
中	中リスクのメールメッセージは次のとおりです。 • 既知の不正プログラム • 既知のフィッシング脅威 • 既知の危険なリンク • YARA ルールに基づき中リスクとして検出された添付ファイル • 不審 URL の一致に基づき中リスクとして検出されたリンク 未知のリンクが高リスクとして判定されることはありません。
低	低リスクのメールメッセージは次のとおりです。 • 既知の極めて不審な、または不審なリンク (アグレッシブモード) • 仮想アナライザに低リスクとして検出されたリンク • 仮想アナライザに低リスクとして検出された添付ファイル • YARA ルールに基づき低リスクとして検出された添付ファイル • 不審 URL の一致に基づき低リスクとして検出されたリンク • ソーシャルエンジニアリング攻撃 • ビジネスメール詐欺 (BEC)

リスクレベル	説明
リスクは検出されませんでした	リスクが検出されなかったメールメッセージ: • 不審な添付ファイルやリンクは含まれない • 既知の極めて不審な、または不審なリンクを含む (標準モード) • ポリシー除外条件に一致する

未評価	未評価のメールメッセージは、次のいずれかのカテゴリに分類されます。
	• バイパスされた検索: 添付ファイルの圧縮レイヤが 20 を超えている (ファイルが 20 回を超えて圧縮された)
	• 検索不能なアーカイブ: パスワードリストやヒューリスティックに取得されたパスワードを使用しても抽出や検索ができないパスワード保護されたアーカイブ
	• 検索不能メッセージまたは添付ファイル: 次のいずれかの条件に一致
	  • メール形式が正しくない
	  • 仮想アナライザがメールメッセージを分析しようとしたときにシステムのタイムアウトが発生した
	  • 仮想アナライザが一部の添付ファイルまたはリンクを分析しようとしたときにシステムのタイムアウトが発生し、その他のリスクは検出されなかった
	  • 仮想アナライザがすべての 添付ファイルまたはリンクを分析できず、その他のリスクは検出されなかった

使用不可	Deep Discovery Email Inspector では、スパムメール/グレーメールメッセージ、またはコンテンツ違反や情報漏えい対策イベントにより検出されたメールメッセージにリスクレベルを割り当てません。

仮想アナライザのリスクレベル

次の表は、オブジェクト分析後の仮想アナライザのリスクレベルを示しています。不審オブジェクトがどのような基準で高または低のリスクに分類されたかを確認するには、この表を参照してください。

リスクレベル	説明
高	オブジェクトは、一般的に不正プログラムに関連付けられる非常に不審な特徴を示しています。 例: • 不正プログラムのシグネチャ、既知のセキュリティホール悪用コード • セキュリティソフトウェアエージェントの無効化 • 不正なネットワーク接続先への接続 • 自己複製、他のファイルへの感染 • ドキュメントによる、実行可能ファイルのドロップまたはダウンロード
低	オブジェクトは、無害である可能性が高い、軽度の不審な特徴を示しています。
リスクは検出されませんでした	オブジェクトは、不審な特徴を示していません。

脅威の種類の分類

次の表は、検索または分析時に検出される脅威の種類について説明しています。ネットワークに影響を及ぼす不正な活動について理解するには、この表を参照してください。

表 4-2. メールメッセージの脅威の種類

脅威の種類	分類
標的型不正プログラム	上司や同僚など、ユーザがメールメッセージの送信元として予期する相手から送信されたかのように見せかける不正プログラム
不正プログラム	コンピュータシステムに対する妨害、制御、盗難、データ喪失、スパイ、または無許可のアクセスを目的として攻撃者によって使用される不正なソフトウェア
不正 URL	既知の不正な Web サイトにリンクする、メールメッセージに埋め込まれたハイパーリンク

脅威の種類	分類
不審ファイル	不正な特徴を示すファイル 重要 不審ファイルは十分に注意して処理してください。
不審 URL	未知の不正な Web サイトにリンクする、メールメッセージに埋め込まれたハイパーリンク
フィッシング	ユーザを正規の Web サイトになりすましたサイトに誘導することで、個人情報を漏えいさせようとするメールメッセージ
スパムメール/グレーメール	受信者の意向を無視して複数の個人に無差別に送り付けられる、主に商品の宣伝を目的としたメールメッセージ グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールのことを指す
コンテンツ違反	私信やサイズの大きな添付ファイルなど、不適切だと思われるコンテンツ
情報漏えい対策イベント	組織のデジタル資産を含むメールメッセージの転送

検索結果をエクスポートする

検出されたメッセージや不審オブジェクトの検索結果をエクスポートできます。

手順

- 検索結果の上部にある [すべてエクスポート] をクリックします。

  検索結果が CSV ファイルとしてダウンロードされます。

注意

クエリ結果の最初の 50,000 件のエントリのみが CSV ファイルに出力されます。

検出されたメッセージ

検出されたメッセージとは、不正または不審なコンテンツ、埋め込みリンク、添付ファイル、あるいはソーシャルエンジニアリング攻撃に関連した特徴が含まれるメールメッセージです。Deep Discovery Email Inspector は、調査結果に基づいて、各メールメッセージにリスク評価を割り当てます。

検出されたメッセージにクエリを実行すると、以下のことが可能になります。

- ネットワークに影響する脅威とその関連リスクについての理解
- 検出されたメッセージの送信者と受信者の確認
- 検出されたメッセージのメールの件名の把握
- 検出されたメッセージをルーティングした、攻撃の送信元の調査
- 傾向および関連する検出メッセージの発見
- Deep Discovery Email Inspector での検出メッセージの処理方法の確認

検出されたメッセージを表示する

さまざまな側面から情報を調査することで、スピアフィッシング攻撃の状況を把握できます。メールヘッダをレビューすると、メールメッセージの発生元と、どのようにルーティングされたかを確認できます。共通の特徴を関連付けることで、ネットワークに対する攻撃の傾向を調査できます (例: 人事部門からのように見せかけるメールの件名や偽の内部メールアドレスなど)。検出に基づいてポリシーの設定を変更し、同様の攻撃に対して予防措置を講じるようにユーザに警告します。

手順

1. [検出] > [検出されたメッセージ] の順に選択します。
2. 検索条件を指定します。

55 ページの「検出されたメッセージの検索フィルタ」を参照してください。

3. <Enter> キーを押します。

   検索条件に合致するメールメッセージがすべて表示されます。

4. 結果を表示します。

ヘッダ	説明
▶	メールメッセージを調べて、潜在的な脅威についてさらに詳しい情報を取得します。 詳細については、59 ページの「検出されたメッセージを調査する」を参照してください。
検出	不審メールメッセージが最初に Deep Discovery Email Inspector で検出された日時を表示します。 **注意** Deep Discovery Email Inspector でメールメッセージを受信してから、そのメールメッセージが [検出されたメッセージ] 画面に表示されるまでには多少の時間差があります。
リスクレベル	不審メールメッセージに示される潜在的な危険のレベルを表示します。詳細については、48 ページの「検出されたリスク」を参照してください。 詳細については、48 ページの「検出されたリスク」を参照してください。
受信者	検出されたメッセージの受信者メールアドレスを表示します。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを表示します。
送信者	検出されたメッセージの送信者メールアドレスを表示します。
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを表示します。
メールの件名	不審メールメッセージの件名を表示します。

ヘッダ	説明
	不正なリンクが埋め込まれたメールメッセージの件数を表示します。
	ポリシールールにより検出された添付ファイルの数を表示します。
脅威	検出された脅威の名前と分類を表示します。詳細については、51 ページの「脅威の種類の分類」を参照してください。 詳細については、51 ページの「脅威の種類の分類」を参照してください。
処理	メールメッセージを検索し分析した後の最終的な結果を表示します。この結果が、実行されたポリシー処理です。  注意 BCC モードと SPAN/TAP モードでは、処理は常に [監視のみ] です。

検出されたメッセージの検索フィルタ

次の表は、不審メッセージにクエリを実行するための基本的な検索フィルタについて説明しています。検出されたメッセージを表示するには、[検出] > [検出されたメッセージ] の順に選択します。

 注意

検索フィルタでは、ワイルドカードを使用できません。Deep Discovery Email Inspector ではファジィ論理を使用して検索条件をメールメッセージデータに照会します。

フィルタ	説明
脅威の種類	[すべて] または脅威の種類をリストから選択します。 詳細については、51 ページの「脅威の種類の分類」を参照してください。

フィルタ	説明
リスクレベル	[すべて] またはメールメッセージのリスクレベルを選択します。
処理	[すべて] または処理をリストから選択します。 これは、ポリシールールで検索条件が一致したメールメッセージに適用する処理です。 詳細については、117 ページの「ポリシールール」を参照してください。 **注意** BCC モードと SPAN/TAP モードでは、処理は常に [監視のみ] です。
期間	事前に定義した時間範囲を選択するか、カスタム範囲を指定します。

詳細フィルタを適用する

基本的なフィルタに加え、詳細フィルタを適用して不審メッセージのクエリを実行できます。

手順

1. [詳細フィルタの表示] をクリックします。
2. フィルタする情報を指定します。

フィルタ	説明
送信者	送信者のメールアドレスを指定します。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを指定します。
メッセージ ID	一意のメッセージ ID を指定します。 例: `20160603021433.F0304120A7A@example.com`
件名	メールメッセージの件名を指定します。
方向	メッセージの方向を指定します。

フィルタ	説明
ルール	ルール名を指定します。
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを指定します。
URL	URL を指定します。
送信元 IP	メールの送信者に最も近い MTA の IP アドレスを指定します。送信元 IP は、攻撃元、感染 MTA、またはメールリレー機能を持つボットネットの IP アドレスです。 感染 MTA は通常、攻撃者が使用するサードパーティのオープンメールリレーで、不正なメールメッセージやスパムメールを検出せずに送信します。 **注意** [送信元 IP アドレス] 検索フィルタには、文字列の完全一致が必要です。Deep Discovery Email Inspector では、送信元 IP アドレスの検索結果の一致にファジィ論理を使用しません。
ファイル名	添付ファイルの名前を指定します。
データ識別子	データ識別子名を指定します。
YARA ルール名	YARA ルールの名前を指定します。
受信者	受信者のメールアドレスを指定します。アドレスは 1 つのみ指定できます。
脅威の名前	トレンドマイクロから提供される脅威名を指定します。ダッシュボードウィジェットと [検出数] タブには脅威名に関する情報が表示されます。 脅威の検出機能の詳細については、232 ページの「検索と分析」を参照してください。

フィルタ	説明
送信者 IP アドレス	送信者の IP アドレスを指定します。 Deep Discovery Email Inspector をネットワークのエッジ MTA として配置する場合、送信者の IP アドレスは、そのネットワークに最も近い外部 MTA のパブリック IP アドレスとなります。 Deep Discovery Email Inspector をネットワークのエッジ MTA として配置しない場合、送信者の IP アドレスは、エッジ MTA リレーサーバに最も近い MTA の IP アドレスとなります。 **注意** [送信者 IP アドレス] 検索フィルタには、文字列の完全一致が必要です。Deep Discovery Email Inspector では、送信者 IP アドレスの検索結果の一致にファジィ論理を使用しません。
ポリシー	ポリシー名を指定します。
情報漏えい対策テンプレート	情報漏えい対策テンプレート名を指定します。
YARA ルールファイル名	YARA ルールファイルの名前を指定します。
パスワード保護された添付ファイル	パスワードで保護されたファイルを含むメールメッセージを選択します。
手動によるメールの送信	分析のために管理者によって Deep Discovery Email Inspector に手動で送信されるメールメッセージを選択します。 詳細については、252 ページの「メールのサブミット」を参照してください。

3. [検索] をクリックします。

検出されたメッセージを調査する

手順

1. メールメッセージを検索します。

   53 ページの「検出されたメッセージを表示する」を参照してください。

2. 表内のメールメッセージの横にある矢印をクリックします。

   表の行が展開されて詳細が表示されます。

3. メールメッセージの詳細を確認します。

   59 ページの「メールメッセージの詳細」を参照してください。

メールメッセージの詳細

次の表は、検索結果の展開後に表示できるメールメッセージの詳細を示しています。表示されるフィールドは、検出される脅威の種類に応じて異なります。

フィールド	説明
Threat Connect で表示	[Threat Connect で表示] をクリックすると、環境内で検出された不審オブジェクトや Trend Micro Smart Protection Network の脅威データに関する情報を取得して、関連のある実行可能なインテリジェンスを確認できます。
仮想アナライザのレポートの表示	分析レポートを HTML または PDF 形式で表示するには、[仮想アナライザのレポートの表示] をクリックします。
スクリーンショットの表示	メールメッセージを画像として安全に表示するには、[スクリーンショットの表示] をクリックします。
ダウンロード	さらに詳しく調査するために情報をダウンロードするには、ドロップダウンリストからオプションを選択します。

フィールド	説明
概要	メールメッセージのメッセージ ID、受信者、前回の検出時刻、送信者と送信元の IP アドレス、および方向を表示して、メッセージの送信元やその他のトラッキング情報を確認します。 注意 送信者と送信元の IP アドレスで、[不明] は検出されたメッセージの発生元が不明である (位置情報と IP アドレス情報の両方が利用できない) ことを意味し、[データがありません] は位置情報が利用できないことを意味します。 メールメッセージが違反したポリシールールについての情報を取得します。
メッセージ	検索エンジン名と、スパムメールまたはグレーメールとして検出されたメールメッセージのカテゴリを表示します。
添付ファイル	メールメッセージに添付されたファイルについて情報を取得します。この情報にはファイル名、パスワード、ファイルタイプ、リスクレベル、SHA-1 および SHA-256 ハッシュ値、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。
YARA 検出	関連付けられた YARA ルールファイル内の一致する YARA ルールに基づいて検出されたファイルについて情報を取得します。
リンク	メールメッセージに埋め込まれた不審 URL について情報を取得します。この情報には URL、サイトのカテゴリ、リスクレベル、抽出元、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。
内容のキーワード/パターンの一致	メールメッセージ内の一致した内容のキーワードまたはパターンについて情報を取得します。
情報漏えい対策イベント	メールメッセージ、メッセージの場所、およびフォレンジックスデータ内の一致したデータ識別子と情報漏えい対策テンプレートについて情報を取得します。
メールヘッダ	メールメッセージのヘッダの内容を表示します。

影響を受ける受信者を表示する

影響を受ける受信者とは、不正または不審なメールメッセージの受信者です。ネットワーク内でスピアフィッシング攻撃またはソーシャルエンジニアリング攻撃の標的となっている受信者の情報を取得し、関連するメッセージで攻撃の動作を把握できます。企業の上層部が攻撃の標的となっている場合は、攻撃パターンについて注意を喚起します。攻撃者は、影響を受ける受信者が属している部門のコミュニティを検出することで、企業のアドレス帳にアクセスできる可能性があります。

手順

1. [検出] > [受信者] の順に選択します。
2. 検索条件を指定します。
   - 受信者 (メールアドレス)
   - 期間
3. <Enter> キーを押します。

   検索条件に合致するメールメッセージがすべて表示されます。
4. 結果を表示します。

ヘッダ	説明
受信者	検出されたメッセージの受信者メールアドレスを表示します。
検出数	不審な特徴を持つメールメッセージを表示します。署名ベースの検出には、実行可能コードまたは動作分析内にあるデータの既知のパターンの検索が含まれます。不審メッセージの詳細情報を表示するには、番号をクリックします。
リスク高	不正な特徴を持つ検出済みメッセージを表示します。
リスク中	不正な可能性が高い特徴を持つ検出済みメッセージを表示します。
リスク低	検出されたスパムメールメッセージ、またはコンテンツ違反や不審な特徴により検出されたメッセージを表示します。

ヘッダ	説明
スパムメール/グレーメール	検出されたスパムメールメッセージまたはグレーメールの数を表示します。
コンテンツ違反	コンテンツ違反により検出されたメッセージの数を表示します。
情報漏えい対策イベント	情報漏えい対策イベントにより検出されたメッセージの数を表示します。
	不正なリンクが埋め込まれたメールメッセージの件数を表示します。
	ポリシールールにより検出された添付ファイルの数を表示します。
前回の検出	検出されたメッセージの最新の検出時刻を表示します。

攻撃の発生元を表示する

攻撃の発生元とは、不審メッセージをルーティングするパブリック IP アドレスを持つ最初の MTA です。たとえば、不審メッセージが IP1 (送信者)→IP2 (MTA: 225.237.59.52)→IP3 (会社のメールゲートウェイ)→IP4 (受信者) とルーティングされた場合は、225.237.59.52 (IP2) が攻撃の発生元として識別されます。攻撃の発生元を判別することで、地域の攻撃パターンまたは同じメールサーバが関係する攻撃パターンを特定できます。

検出された攻撃の出現率、およびネットワークに対する相対的なリスクについて情報を取得できます。攻撃の場所 (特に攻撃の発生元が組織内の MTA かどうか、または組織がビジネスを展開している地域かどうか) について確認してください。

手順

1. [検出] > [攻撃元] の順に選択します。
2. 検索条件を指定します。
   - 攻撃元 (IP アドレス)
   - 国/地域

3. [期間] を選択します。
4. <Enter> キーを押します。

   検索条件に合致するメールメッセージがすべて表示されます。
5. 結果を表示します。

ヘッダ	説明
攻撃元	攻撃の発生元の IP アドレスを表示します。
国/地域	攻撃の発生元が所在する国を表示します。 注意 ダッシュ (-) は位置情報が利用できないことを意味します。
都市	攻撃の発生元が所在する都市を表示します。 注意 ダッシュ (-) は位置情報が利用できないことを意味します。
検出数	不審な特徴を持つメールメッセージを表示します。署名ベースの検出には、実行可能コードまたは動作分析内にあるデータの既知のパターンの検索が含まれます。不審メッセージの詳細情報を表示するには、番号をクリックします。
リスク高	不正な特徴を持つ検出済みメッセージを表示します。
リスク中	不正な可能性が高い特徴を持つ検出済みメッセージを表示します。
リスク低	検出されたスパムメールメッセージ、またはコンテンツ違反や不審な特徴により検出されたメッセージを表示します。
スパムメール/グレーメール	検出されたスパムメールメッセージまたはグレーメールの数を表示します。
コンテンツ違反	コンテンツ違反により検出されたメッセージの数を表示します。

ヘッダ	説明
情報漏えい対策イベント	情報漏えい対策イベントにより検出されたメッセージの数を表示します。
	不正なリンクが埋め込まれたメールメッセージの件数を表示します。
	ポリシールールにより検出された添付ファイルの数を表示します。
前回の検出	検出されたメッセージの最新の検出時刻を表示します。

送信者を表示する

不審な送信者とは、不正または不審なメールメッセージの送信者です。偽装された送信者アドレスのパターンを見つけ、採用されているソーシャルエンジニアリングの手法を確認してください。たとえば、送信者のメールアドレスは内部アドレス、金融サービス (PayPal、銀行)、またはその他のサービス (Gmail、Taobao、Amazon) などの偽装されたアドレスで表示されます。不審な送信者のメールアドレスをメールゲートウェイでブロックするには、送信者のドメインアドレスと関連するリスクレベルを確認し、ポリシー設定またはスパムメール対策ゲートウェイの設定を変更してください。

手順

1. [検出] > [送信者] の順に選択します。
2. 検索条件を指定します。
   - 送信者 (メールアドレス)
   - 期間
3. <Enter> キーを押します。

   検索条件に合致するメールメッセージがすべて表示されます。
4. 結果を表示します。

ヘッダ	説明
送信者	検出されたメッセージの送信者メールアドレスを表示します。
検出数	不審な特徴を持つメールメッセージを表示します。署名ベースの検出には、実行可能コードまたは動作分析内にあるデータの既知のパターンの検索が含まれます。不審メッセージの詳細情報を表示するには、番号をクリックします。
リスク高	不正な特徴を持つ検出済みメッセージを表示します。
リスク中	不正な可能性が高い特徴を持つ検出済みメッセージを表示します。
リスク低	検出されたスパムメールメッセージ、またはコンテンツ違反や不審な特徴により検出されたメッセージを表示します。
スパムメール/グレーメール	検出されたスパムメールメッセージまたはグレーメールの数を表示します。
コンテンツ違反	コンテンツ違反により検出されたメッセージの数を表示します。
情報漏えい対策イベント	情報漏えい対策イベントにより検出されたメッセージの数を表示します。
	不正なリンクが埋め込まれたメールメッセージの件数を表示します。
	ポリシールールにより検出された添付ファイルの数を表示します。
前回の検出	検出されたメッセージの最新の検出時刻を表示します。

メールの件名を表示する

不審な件名とは、不正または不審なメールメッセージの 件名です。共通のキーワードやその他のソーシャルエンジニアリングの 手法についての傾向を知ることができます。プリテキスティングは 、最も一般的な手口です。標的となった受信者が思わず開いてしまうような、なじみのあるメールの件名 (休日のパーティへの招待状、銀行の取引明細、または部門のニュースレターで使用される一般的な件名) を検索してください。ユーザがメールの件名を信頼した場合、さらに不正な添付ファイルをダウンロードさせたり、ドメインの

アカウント情報や顧客情報への正規のリクエストを装ったフィッシングリンクをクリックさせる場合があります。

手順

1. [検出] > [件名] の順に選択します。
2. 検索条件を指定します。
   - メールの件名
   - 期間
3. <Enter> キーを押します。

   検索条件に合致するメールメッセージがすべて表示されます。
4. 結果を表示します。

ヘッダ	説明
メールの件名	不審メールメッセージの件名を表示します。
検出数	不審な特徴を持つメールメッセージを表示します。署名ベースの検出には、実行可能コードまたは動作分析内にあるデータの既知のパターンの検索が含まれます。不審メッセージの詳細情報を表示するには、番号をクリックします。
リスク高	不正な特徴を持つ検出済みメッセージを表示します。
リスク中	不正な可能性が高い特徴を持つ検出済みメッセージを表示します。
リスク低	検出されたスパムメールメッセージ、またはコンテンツ違反や不審な特徴により検出されたメッセージを表示します。
スパムメール/グレーメール	検出されたスパムメールメッセージまたはグレーメールの数を表示します。
コンテンツ違反	コンテンツ違反により検出されたメッセージの数を表示します。
情報漏えい対策イベント	情報漏えい対策イベントにより検出されたメッセージの数を表示します。

ヘッダ	説明
	不正なリンクが埋め込まれたメールメッセージの件数を表示します。
	ポリシールールにより検出された添付ファイルの数を表示します。
前回の検出	検出されたメッセージの最新の検出時刻を表示します。

不審オブジェクト

不審オブジェクトとは、システムの危険や損害を引き起こす可能性があるオブジェクトです。

不審オブジェクトにクエリを実行すると、以下のことが可能になります。

- ネットワークに影響する脅威とその関連リスクについての理解
- 不審なホスト、URL、ファイル、および同期された不審オブジェクトの出現率の評価
- メールメッセージに埋め込まれたリンクまたはコールバックアドレスの有無の確認
- ネットワーク内の感染エンドポイントの検出
- 感染の予防的な封じ込めまたはブロック

不審ホストを表示する

不審ホストとは、システムの危険や損害を引き起こす可能性がある IP アドレスまたはホスト名です。不審ホストを表示することで、そのリスクを理解し、関連メッセージを確認して、相対的な出現率を評価できます。

手順

1. [検出] > [不審オブジェクト] > [ホスト] の順に選択します。
2. 検索条件を指定します。
    - ホスト (IP アドレスまたはホスト名)

- 期間

3. <Enter> キーを押します。

   検索条件に合致する不審オブジェクトがすべて表示されます。

4. 結果を表示します。

ヘッダ	説明
ホスト	不審オブジェクトで使用されている IP アドレスまたはホスト名を表示します。
ポート番号	不審オブジェクトで使用されているポート番号を表示します。
リスクレベル	仮想アナライザでファイルを実行した後または URL を開いた後のサンプルの潜在的な危険のレベルを表示します。
関連メッセージ	同じ不審オブジェクトが含まれるメッセージを表示します。
前回のメッセージ受信者	不審オブジェクトを含むメールメッセージの最新の受信者を表示します。
前回の検出	仮想アナライザが送信されたオブジェクトから最後に不審オブジェクトを検出した日時を表示します。

不審 URL を表示する

不審 URL とは、システムの危険や損害を引き起こす可能性がある Web アドレスです。不審 URL を表示することで、そのリスクを理解して、関連メッセージや最近の出現時点を確認できます。

手順

1. [検出] > [不審オブジェクト] > [URL] の順に選択します。
2. 検索条件を指定します。
   - URL
   - 期間

3. <Enter> キーを押します。

   検索条件に合致する不審オブジェクトがすべて表示されます。

4. 結果を表示します。

ヘッダ	説明
URL	不審オブジェクトの Web アドレスを表示します。
リスクレベル	仮想アナライザでファイルを実行した後または URL を開いた後のサンプルの潜在的な危険のレベルを表示します。
関連メッセージ	同じ不審オブジェクトが含まれるメッセージを表示します。
前回のメッセージ受信者	不審オブジェクトを含むメールメッセージの最新の受信者を表示します。
前回の検出	仮想アナライザが送信されたオブジェクトから最後に不審オブジェクトを検出した日時を表示します。

不審ファイルを表示する

不審ファイルとは、SHA-1 ハッシュ値がシステムの危険や損害を引き起こす可能性と関連付けられたものです。不審ファイルを表示することで、そのリスクを理解し、関連メッセージを確認して、相対的な出現率を評価できます。

手順

1. [検出] > [不審オブジェクト] > [ファイル] の順に選択します。
2. 検索条件を指定します。
   - SHA-1
   - 期間
3. <Enter> キーを押します。

   検索条件に合致する不審オブジェクトがすべて表示されます。

4. 結果を表示します。

ヘッダ	説明
SHA-1	ファイルを一意に識別する 160 ビットのハッシュ値を表示します。
関連メッセージ	同じ不審オブジェクトが含まれるメッセージを表示します。
前回のメッセージ受信者	不審オブジェクトを含むメールメッセージの最新の受信者を表示します。
前回の検出	仮想アナライザが送信されたオブジェクトから最後に不審オブジェクトを検出した日時を表示します。

同期された不審オブジェクトを表示する

Deep Discovery Email Inspector では、不審オブジェクトを Trend Vision One、Apex Central、Deep Discovery Director、または Deep Discovery Analyzer などの外部ソースと同期できます。同期された不審オブジェクトを表示することで、そのリスクを理解し、関連メッセージを確認して、不審オブジェクトの相対的な出現率を評価できます。

注意

- Deep Discovery Email Inspector が Apex Central と Deep Discovery Director 5.0 以降の両方に登録されている場合、Deep Discovery Email Inspector は不審オブジェクトを Deep Discovery Director と同期し、Apex Central の既存の不審オブジェクトを上書きします。
- Deep Discovery Email Inspector を Trend Vision One、Deep Discovery Director 3.0 以降、および Trend Micro Apex Central に登録すると、Deep Discovery Email Inspector は次の優先順位で不審オブジェクトおよび除外リストを統合製品と同期します。Trend Vision One、Deep Discovery Director、Apex Central。

手順

1. [検出] > [不審オブジェクト] > [同期された不審オブジェクト] の順に選択します。

2. 検索条件を指定します。
   - 不審オブジェクト (IP アドレス、ホスト名、URL、ファイルの SHA-1、またはファイルの SHA-256)
   - 期間 (前回の同期時刻に基づくフィルタの時間範囲)
3. <Enter> キーを押します。

   検索条件に合致する不審オブジェクトがすべて表示されます。
4. 結果を表示します。

ヘッダ	説明
不審オブジェクト	同期された不審オブジェクトに関連する IP アドレス、ホスト名、URL、ファイルの SHA-1、またはファイルの SHA-256 を表示します。
種類	不審オブジェクトの種類 (ドメイン、ファイル、IP、または URL) を表示します。
リスクレベル	仮想アナライザでファイルを実行した後または URL を開いた後のサンプルの潜在的な危険のレベルを表示します。
ソース	同期された不審オブジェクトのソースを表示します。 ソースは次のいずれかになります。 • Trend Vision One • Apex Central • Deep Discovery Analyzer • Deep Discovery Director
ユーザ指定	同期された不審オブジェクトがユーザ指定かどうかを表示します。
失効日	オブジェクトが不審と見なされなくなる日時を表示します。
前回の同期	前回エントリをソースと同期した日時を表示します。

隔離

Deep Discovery Email Inspector は、特定のポリシー条件に一致する不審メールメッセージを隔離します。メールメッセージの詳細を確認してから、メールメッセージを削除するか、隔離解除して本来の受信者に配信するか、または処理を再開するかを決定してください。

実行する処理を決定する前に、隔離されたメールメッセージのクエリを実行します。

次のいずれかの処理を実行します。

- 隔離されたメッセージをさまざまな条件に基づいて検索する
- 不正な添付ファイルと URL について詳しい情報を取得する
- 隔離されたメッセージを解除する
- 隔離されたメッセージを削除する
- スパムメール検出、コンテンツ違反、または情報漏えい対策イベントにより隔離されたメッセージの処理を再開する
- メッセージ内のパスワード保護されたファイルをロック解除して脅威検索を実行する

隔離されたメッセージを表示する

手順

1. [検出] > [隔離] の順に選択します。
2. 検索条件を指定します。

   74 ページの「隔離の検索フィルタ」を参照してください。
3. <Enter> キーを押します。

   検索条件に合致するメールメッセージがすべて表示されます。
4. 結果を表示します。

ヘッダ	説明
▶	メールメッセージを調べて、潜在的な脅威についてさらに詳しい情報を取得します。 詳細については、78 ページの「隔離されたメールメッセージを調査する」を参照してください。
検出	不審メールメッセージが最初に Deep Discovery Email Inspector で検出され隔離された日時を表示します。  注意 Deep Discovery Email Inspector でメールメッセージを受信してから、そのメールメッセージが [隔離] 画面に表示されるまでには多少の時間差があります。
リスクレベル	不審メールメッセージに示される潜在的な危険のレベルを表示します。詳細については、48 ページの「検出されたリスク」を参照してください。
受信者	検出されたメッセージの受信者メールアドレスを表示します。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを表示します。
送信者	検出されたメッセージの送信者メールアドレスを表示します。
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを表示します。
メールの件名	不審メールメッセージの件名を表示します。
	不正なリンクが埋め込まれたメールメッセージの件数を表示します。
	ポリシールールにより検出された添付ファイルの数を表示します。
脅威	検出された脅威の名前と分類を表示します。詳細については、51 ページの「脅威の種類の分類」を参照してください。

ヘッダ	説明
隔離の理由	メールメッセージの隔離の理由を表示します。 詳細については、77 ページの「隔離の判定理由」を参照してください。

隔離の検索フィルタ

次の表は、隔離されたメールメッセージにクエリを実行するための基本的な検索フィルタについて説明しています。詳細フィルタを適用するには、56 ページの「詳細フィルタを適用する」を参照してください。

隔離を表示するには、[検出] > [隔離] の順に選択します。

注意

検索フィルタでは、ワイルドカードを使用できません。Deep Discovery Email Inspector ではファジィ論理を使用して検索条件をメールメッセージデータに照会します。

フィルタ	説明
脅威の種類	[すべて] または脅威の種類をリストから選択します。 詳細については、51 ページの「脅威の種類の分類」を参照してください。
リスクレベル	[すべて] またはメールメッセージのリスクレベルを選択します。
隔離の理由	[すべて] または隔離の理由を選択します。
期間	事前に定義した時間範囲を選択するか、カスタム範囲を指定します。

詳細フィルタを適用する

基本的なフィルタに加え、詳細フィルタを適用して不審メッセージのクエリを実行できます。

手順

1. [詳細フィルタの表示] をクリックします。
2. フィルタする情報を指定します。

フィルタ	説明
送信者	送信者のメールアドレスを指定します。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを指定します。
メッセージ ID	一意のメッセージ ID を指定します。 例: `20160603021433.F0304120A7A@example.com`
件名	メールメッセージの件名を指定します。
方向	メッセージの方向を指定します。
ルール	ルール名を指定します。
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを指定します。
URL	URL を指定します。
送信元 IP	メールの送信者に最も近い MTA の IP アドレスを指定します。送信元 IP は、攻撃元、感染 MTA、またはメールリレー機能を持つボットネットの IP アドレスです。 感染 MTA は通常、攻撃者が使用するサードパーティのオープンメールリレーで、不正なメールメッセージやスパムメールを検出せずに送信します。 **注意** [送信元 IP アドレス] 検索フィルタには、文字列の完全一致が必要です。Deep Discovery Email Inspector では、送信元 IP アドレスの検索結果の一致にファジィ論理を使用しません。
ファイル名	添付ファイルの名前を指定します。

フィルタ	説明
データ識別子	データ識別子名を指定します。
YARA ルール名	YARA ルールの名前を指定します。
受信者	受信者のメールアドレスを指定します。アドレスは 1 つのみ指定できます。
脅威の名前	トレンドマイクロから提供される脅威名を指定します。ダッシュボードウィジェットと [検出数] タブには脅威名に関する情報が表示されます。 脅威の検出機能の詳細については、232 ページの「検索と分析」を参照してください。
送信者 IP アドレス	送信者の IP アドレスを指定します。 Deep Discovery Email Inspector をネットワークのエッジ MTA として配置する場合、送信者の IP アドレスは、そのネットワークに最も近い外部 MTA のパブリック IP アドレスとなります。 Deep Discovery Email Inspector をネットワークのエッジ MTA として配置しない場合、送信者の IP アドレスは、エッジ MTA リレーサーバに最も近い MTA の IP アドレスとなります。 注意 [送信者 IP アドレス] 検索フィルタには、文字列の完全一致が必要です。Deep Discovery Email Inspector では、送信者 IP アドレスの検索結果の一致にファジィ論理を使用しません。
ポリシー	ポリシー名を指定します。
情報漏えい対策テンプレート	情報漏えい対策テンプレート名を指定します。
YARA ルールファイル名	YARA ルールファイルの名前を指定します。
パスワード保護された添付ファイル	パスワードで保護されたファイルを含むメールメッセージを選択します。

フィルタ	説明
手動によるメールの送信	分析のために管理者によって Deep Discovery Email Inspector に手動で送信されるメールメッセージを選択します。 詳細については、252 ページの「メールのサブミット」を参照してください。

3. [検索] をクリックします。

隔離の判定理由

次の表は、[隔離] 画面に表示される隔離の判定理由の詳細を示しています。

隔離の判定理由	詳細
コンテンツ違反	内容がコンテンツフィルタルールに一致するメッセージ。
情報漏えい対策イベント	情報漏えい対策ポリシー違反が 1 つ以上あるメッセージ。
不正な形式	開いて処理できないメッセージ。
スパム検出	スパムメール/グレーメールとして検出されたメッセージ。
脅威の検出	不正プログラムを含むことが検出されたメッセージ。
検索不能	検索できないメッセージ。
暗号化失敗	暗号化できないメッセージ。
復号失敗	復号できないメッセージ。
仮想アナライザのエラー	処理のタイムアウトなど、仮想アナライザの予期しないエラーにより分析されなかったメッセージ。
仮想アナライザのタイムアウト	仮想アナライザの処理のタイムアウトにより分析されなかったメッセージ。

隔離されたメールメッセージを調査する

手順

1. メールメッセージを検索します。

   72 ページの「隔離されたメッセージを表示する」を参照してください。

2. 表内のメールメッセージの横にある矢印をクリックします。

   表の行が展開されて詳細が表示されます。

3. メールメッセージの詳細を確認します。

   79 ページの「隔離されたメッセージの詳細」を参照してください。

4. 隔離されたメッセージに対して処理を実行します。

   - メッセージを隔離したままにします。

     注意

     隔離されたメッセージは [ストレージの管理] 画面で指定した設定に基づいて削除されます。

     詳細については、448 ページの「ストレージ管理を設定する」を参照してください。

   - 隔離からメールメッセージを削除するには、[削除] をクリックします。
   - メールメッセージを配信するには、[隔離解除] をクリックします。
   - 前回の検索チェックポイントからメッセージの検索を続行するように Deep Discovery Email Inspector を設定するには、[プロセスの再開] をクリックします。

     注意

     Deep Discovery Email Inspector では、スパムメール検出、コンテンツ違反、または情報漏えい対策イベントにより隔離されたメッセージの処理のみを継続できます。

- [ファイルパスワード] 画面に指定されたパスワードとエントリを使用して検索不可能メッセージ内のパスワード保護されたファイルを開き、メッセージに脅威検索を実行するには、

  [ロック解除して再処理] をクリックします。

隔離されたメッセージの詳細

次の表は、検索結果の展開後に表示できるメールメッセージの詳細を示しています。表示されるフィールドは、検出される脅威の種類に応じて異なります。

フィールド	説明
Threat Connect で表示	[Threat Connect で表示] をクリックすると、環境内で検出された不審オブジェクトや Trend Micro Smart Protection Network の脅威データに関する情報を取得して、関連のある実行可能なインテリジェンスを確認できます。
仮想アナライザのレポートの表示	分析レポートを HTML または PDF 形式で表示するには、[仮想アナライザのレポートの表示] をクリックします。
スクリーンショットの表示	メールメッセージを画像として安全に表示するには、[スクリーンショットの表示] をクリックします。
ダウンロード	さらに詳しく調査するために情報をダウンロードするには、ドロップダウンリストからオプションを選択します。

フィールド	説明
概要	メールメッセージのメッセージ ID、受信者、前回の検出時刻、送信者と送信元の IP アドレス、および方向を表示して、メッセージの送信元やその他のトラッキング情報を確認します。 注意 送信者と送信元の IP アドレスで、[不明] は検出されたメッセージの発生元が不明である (位置情報と IP アドレス情報の両方が利用できない) ことを意味し、[データがありません] は位置情報が利用できないことを意味します。 メールメッセージが違反したポリシールールについての情報を取得します。
メッセージ	検索エンジン名と、スパムメールまたはグレーメールとして検出されたメールメッセージのカテゴリを表示します。
添付ファイル	メールメッセージに添付されたファイルについて情報を取得します。この情報にはファイル名、パスワード、ファイルタイプ、リスクレベル、SHA-1 および SHA-256 ハッシュ値、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。
YARA 検出	関連付けられた YARA ルールファイル内の一致する YARA ルールに基づいて検出されたファイルについて情報を取得します。
リンク	メールメッセージに埋め込まれた不審 URL について情報を取得します。この情報には URL、サイトのカテゴリ、リスクレベル、抽出元、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。
内容のキーワード/パターンの一致	メールメッセージ内の一致した内容のキーワードまたはパターンについて情報を取得します。
情報漏えい対策イベント	メールメッセージ、メッセージの場所、およびフォレンジックスデータ内の一致したデータ識別子と情報漏えい対策テンプレートについて情報を取得します。
メールヘッダ	メールメッセージのヘッダの内容を表示します。

送信者フィルタ/認証

次の設定に基づいて、ブロックする送信者の IP アドレスとメールアドレスのリストを表示できます。

- メールレピュテーション
- ディレクトリハーベスト攻撃 (DHA) からの保護
- バウンスメール攻撃からの保護
- SMTP トラフィックスロットリング (IP アドレス)
- SMTP トラフィックスロットリング (メールアドレス)
- SPF
- DKIM
- DMARC
- ユーザ指定

送信者フィルタ/認証の検出を表示する

Deep Discovery Email Inspector によりブロックされた送信者の IP アドレスとメールアドレスは、[送信者フィルタ/認証] 画面の [検出] で表示できます。

手順

1. [検出] > [送信者フィルタ/認証] の順に選択します。
2. 検索条件を 1 つ以上指定します。
   - [ルール] ドロップダウンリストからオプションを 選択します。
   - 送信者のメールアドレスまたは IP アドレスを選択して <Enter> キーを押すか、検索アイコン ( ) をクリックします。
   - ドロップダウンリストから期間を選択します。

   検索条件に一致する、ブロックされた送信者のすべてのメールアドレスまたは IP アドレスが表示されます。
3. 結果を表示します。

ヘッダ	説明
検出	送信者フィルタ/認証ルールに基づいて Deep Discovery Email Inspector が送信者からのメッセージをブロックする日時を表示します。
IP アドレス	Deep Discovery Email Inspector がブロックする送信者の IP アドレスまたはドメイン解決された IP アドレスを表示します。
メールアドレス	Deep Discovery Email Inspector がブロックする送信者のメールアドレスを表示します。
受信者	検出されたメッセージの受信者メールアドレスを表示します。
ルール	一致する送信者フィルタ/認証ルールの名前を表示します。
処理	送信者のアドレスを一時的にブロックするのか、常にブロックするのかを表示します。
認証結果	SPF、DKIM、または DMARC 検証に基づいて送信者の認証結果を表示します。

ヒント

[エクスポート] をクリックすると、クエリ結果をカンマ区切り値のファイルに保存できます。

第 5 章

ポリシー

この章の内容は次のとおりです。

ポリシーについて

ポリシーとは、Deep Discovery Email Inspector でメールメッセージの評価に使用するルールセットです。ポリシーを使用して、メールメッセージで検出された脅威や望ましくないコンテンツに適用する処理を判別します。

Deep Discovery Email Inspector でポリシーを設定し、メッセージの方向 (受信、送信、受信または送信) に基づいてメッセージを検索できます。

次の表は、ポリシーに必要なコンポーネントを示しています。

コンポーネント	説明
ポリシールール	次の種類のルールを作成して、組織のウイルス対策などのセキュリティを強化します。 • コンテンツフィルタルール: メッセージの内容を評価して、望ましくないコンテンツが受信者に配信されないようにし、Microsoft Office や PDF ファイルの添付ファイルからアクティブコンテンツ (マクロなど) を削除します。 • 情報漏えい対策ルール: メールメッセージを介したデジタル資産の転送を防止します。 • スパムメール対策ルール: スパムメールまたはグレーメールについてメッセージを検索します。 • 脅威対策ルール: スパイウェア、ワームなどのウイルスおよびその他の不正プログラムについてメッセージを検索します。 Deep Discovery Email Inspector には、ウイルスなどのインターネット上の脅威からネットワークを保護するためのルール設定を含む、初期設定のポリシーが組み込まれています。  注意 • 脅威対策ルールではスパムメールを防ぐことができません。スパムメールから保護するには、スパムメール対策ルールを設定して、送信者フィルタを有効にします。 • コンテンツフィルタ、情報漏えい対策、およびスパムメール対策の機能を使用するには、ゲートウェイモジュールのライセンスを有効にします。詳細については、453 ページの「ライセンス」を参照してください。

コンポーネント	説明
ポリシーオブジェクト	次の種類のオブジェクトを設定して、ポリシーのトラフィック処理の動作をカスタマイズできます。 • 通知 • メッセージタグ • リダイレクトページ • データ識別子 • 情報漏えい対策テンプレート • アーカイブサーバ
ポリシー除外	ポリシー除外により、誤検出が減少します。除外を設定し、メールの暗号化に制限と処理を設定するか、特定のメールメッセージを「安全」として分類します。安全な送信者、受信者、および X-Header コンテンツを指定し、ファイル、URL、IP アドレスとドメイン、および URL キーワードを追加するか、グレーメール検索をバイパスする送信者を指定します。安全なメールメッセージはそれ以上調査されず、BCC モードおよび SPAN/TAP モードでは破棄され、MTA モードでは受信者に配信されます。

Deep Discovery Email Inspector のポリシー作成手順を実行します。

1. (コンテンツフィルタルールおよび 情報漏えい対策ルールの場合) データ識別子を作成します。

   詳細については、143 ページの「データ識別子」を参照してください。

2. ポリシールールと通知テンプレートを作成します。

   詳細については、117 ページの「ポリシールール」および 135 ページの「受信者通知を設定する」を参照してください。

3. 対象となる送信者と受信者に適用するポリシーを作成します。

   詳細については、112 ページの「ポリシーを設定する」および 163 ページの「アドレスグループ」を参照してください。

4. 信頼された送信者/受信者、またはポリシー除外対象のオブジェクトを指定します。

   詳細については、165 ページの「ポリシー除外」を参照してください。

メッセージの一般的な検索順序

Deep Discovery Email Inspector では、メールメッセージを受信すると次の順序でメッセージに検索設定が適用されます。

- 承認済み送信者リスト
- SMTP トラフィックスロットリング
- 送信者フィルタ (Email Reputation Services (ERS)、ディレクトリハーベスト攻撃 (DHA)、およびバウンスメール攻撃)
- ドメインベースのメッセージ認証 (SPF、DKIM、および DMARC)
- メッセージレベルの除外
- ポリシールール:
  - コンテンツフィルタルール
  - 情報漏えい対策ルール
  - スパムメール対策ルール
  - 高度な脅威対策のルール

注意

送信者フィルタ/認証に承認済み送信者リストとブロックする送信者リストを設定すると、Deep Discovery Email Inspector では、送信者を確認する設定が次の順序で適用されます。

- SMTP トラフィックスロットリングの場合:
  - 承認済み送信者リスト (IP アドレス)
  - ブロックする送信者リスト (ユーザ指定の IP アドレス)
  - SMTP トラフィックスロットリング (IP アドレス)
  - 承認済み送信者リスト (メールアドレス)
  - ブロックする送信者リスト (ユーザ指定のメールアドレス)
  - SMTP トラフィックスロットリング (メールアドレス)
- 送信者フィルタ (ERS、DHA、バウンスメール攻撃) およびドメインベースのメッセージ認証 (SPF、DKIM、および DMARC) の場合:
  - 承認済み送信者リスト (IP アドレスとメールアドレス)
  - ブロックする送信者リスト (ユーザ指定の IP アドレスとメールアドレス)
  - 送信者フィルタ (ERS、DHA、バウンスメール攻撃)
  - ドメインベースのメッセージ認証 (SPF、DKIM、および DMARC)

ポリシー管理ガイドライン

Deep Discovery Email Inspector でポリシーを設定する際は、次のことを考慮してください。

- ポリシーを作成する前に、コンテンツフィルタルール、情報漏えい対策ルール、スパムメール対策ルール、および脅威対策ルールを作成します。
- [ゲートウェイモジュール] のライセンスをアクティベートして、コンテンツフィルタルールとスパムメール対策ルールを有効にします。[脅威対策] のライセンスをアクティベートして、脅威対策ルールを有効にします。[ゲートウェイモジュール] のライセンスがアクティベートされてい

ない場合、Deep Discovery Email Inspector ではコンテンツフィルタルールとスパムメール対策ルールが無効になります。

詳細については、453 ページの「ライセンス」を参照してください。

- 送信者アドレスのドメインが内部ドメインリストに存在する場合、Deep Discovery Email Inspector ではその送信者からのメッセージが送信メッセージと見なされ、メッセージの方向に基づいたポリシーが適用されます。
- 1 つのポリシーに複数のルールを設定する場合、Deep Discovery Email Inspector では次の順序でメッセージにルールが適用されます。
  - コンテンツフィルタルール
  - 情報漏えい対策ルール
  - スパムメール対策ルール
  - 高度な脅威対策のルール
- ポリシーの最終処理は [メッセージの削除]、[受信者の変更]、[ブロックして隔離]、および [直接配信] になります。ポリシーに複数のルールが設定されている場合、Deep Discovery Email Inspector は検出されたメッセージに最終処理を 1 つだけ適用します。一致したルールの最終処理をメッセージに適用したら、同じポリシー内の後続のルールに対してメッセージの一致は行われません。

  詳細については、90 ページの「ポリシーの処理」を参照してください。
- フィッシングメッセージを 隔離するには、脅威対策ルールで [添付ファイルを削除できない場合は元のメッセージを隔離] を選択します。

  詳細については、131 ページの「脅威対策ルールを設定する」および 90 ページの「ポリシーの処理」を参照してください。
- ポリシーには脅威検出ルールを 1 つ含める必要があります。コンテンツフィルタルール、情報漏えい対策ルール、およびスパムメール対策ルールはポリシーのオプションになります。
- ポリシーに複数のコンテンツフィルタルール 、情報漏えい対策ルール、またはスパムメール対策ルールを指定する場合は、ルール一致の優先度を設定できます。

- ドメイン内の任意のメールアドレスのすべての受信メッセージに適用するポリシーを作成できます (例: 受信者に*@example.com を指定)。
- ドメイン内の任意のメールアドレスのすべての送信メッセージに適用するポリシーを作成できます (例: 送信者に*@example.com を指定)。
- ウイルスの流出を防ぎ、すべてのメッセージが確実に検索されるようにするには、すべての受信者および送信者の受信または送信メッセージに適用されるポリシーを 1 つ、最も低い優先度で [ポリシーリスト] に作成することをお勧めします。
- Active Directory のクエリがタイムアウトした場合やメッセージのメールアドレスが有効でない場合、Deep Discovery Email Inspector では、すべての受信者および送信者を対象にしたポリシーがそのメッセージに適用されます。
- [ポリシーリスト] で、すべての受信者および送信者を対象に同じメッセージの方向に適用される複数のポリシーを設定する場合、Deep Discovery Email Inspector では最も優先度の高いポリシーが適用されます。

ポリシーの処理

次の表は、各動作モードにおいて、一致したポリシールールで選択されている処理に対して Deep Discovery Email Inspector が実行する処理について説明しています。

表 5-1. 処理および動作モード: コンテンツフィルタルール

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
メッセージの削除	• メールキューからメールメッセージを削除する • メールメッセージに同じポリシー内の後続のポリシールールを適用しない • メールメッセージを配信しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
受信者の変更	• 指定した 1 人以上の受信者にメールメッセージを配信する • メールメッセージに同じポリシー内の後続のポリシールールを適用しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
ブロックして隔離	• 隔離領域に複製を保存する • [検出] > [隔離] 画面で検索処理を再開するまで、メールメッセージに同じポリシー内の後続のルールを適用しない • Web コンソールを使用してメッセージを隔離解除できる	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
すべての添付ファイルの削除	• テキストファイルで不審な添付ファイルを置換 • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する • メールメッセージに同じポリシー内の後続のルールを適用する	• メールメッセージに同じポリシー内の後続のルールを適用する	• メールメッセージに同じポリシー内の後続のルールを適用する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	注意 検出されたメールメッセージの添付ファイルと添付ファイルから抽出された URL は、分析のために仮想アナライザに送信されません。メッセージ本文と件名から抽出された URL のみ、分析のために仮想アナライザに送信されます。		
放置およびタグ付け	• メールメッセージに同じポリシー内の後続のルールを適用する • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する	• メールメッセージに同じポリシー内の後続のルールを適用する	• メールメッセージに同じポリシー内の後続のルールを適用する
直接配信	• メールメッセージに同じポリシー内の後続のポ	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	リシールールを適用しない • メールメッセージを初期設定の SMTP サーバを使用して受信者に配信するか、指定した SMTP サーバに配信する		
メッセージの暗号化	• その他の最終処理以外のすべての処理を適用した後にメッセージを暗号化する • メールメッセージに同じポリシー内の後続のルールを適用する	• 該当なし	• 該当なし
ファイルのサニタイズ	• Microsoft Office ファイルからアクティブコンテンツ (マクロなど) を削除する • メールメッセージに同じポリシー内の後続のルールを適用する • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する	• メールメッセージに同じポリシー内の後続のルールを適用する	• メールメッセージに同じポリシー内の後続のルールを適用する
BCC	• メールメッセージのブラインドカーボンコピー	• 該当なし	• 該当なし

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	(BCC) を指定された受信者に送信する		
通知の送信	• 通知テンプレートで指定されたすべてのメッセージ受信者と連絡先メールアドレスに通知を送信する	• 通知テンプレートで指定されたすべてのメッセージ受信者と連絡先メールアドレスに通知を送信する	• 該当なし
スタンプの挿入	• 設定されている場合、選択されたスタンプを、検出されたメールメッセージの本文に挿入する	• 該当なし	• 該当なし

表 5-2. 処理および動作モード: 情報漏えい対策ルール

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
メッセージの削除	• メールキューからメールメッセージを削除する • メールメッセージに同じポリシー内の後続のポリシールールを適用しない • メールメッセージを配信しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
受信者の変更	• 指定した 1 人以上の受信者にメールメッセージを配信する	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	• メールメッセージに同じポリシー内の後続のポリシールールを適用しない		
ブロックして隔離	• 隔離領域に複製を保存する • [検出] > [隔離] 画面で検索処理を再開するまで、メールメッセージに同じポリシー内の後続のルールを適用しない • Web コンソールを使用してメッセージを隔離解除できる	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
すべての添付ファイルの削除	• テキストファイルで不審な添付ファイルを置換 • メールメッセージに同じポリシー内の後続のルールを適用する • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する	• メールメッセージに同じポリシー内の後続のルールを適用する	• メールメッセージに同じポリシー内の後続のルールを適用する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	注意 検出されたメールメッセージの添付ファイルと添付ファイルから抽出された URL は、分析のために仮想アナライザに送信されません。メッセージ本文と件名から抽出された URL のみ、分析のために仮想アナライザに送信されます。		
放置およびタグ付け	• メールメッセージに同じポリシー内の後続のルールを適用する • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する	• メールメッセージに同じポリシー内の後続のルールを適用する	• メールメッセージに同じポリシー内の後続のルールを適用する
直接配信	• メールメッセージに同じポリシー内の後続のポ	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	リシールールを適用しない • メールメッセージを初期設定の SMTP サーバを使用して受信者に配信するか、指定した SMTP サーバに配信する		
メッセージの暗号化	• その他の最終処理以外のすべての処理を適用した後にメッセージを暗号化する • メールメッセージに同じポリシー内の後続のルールを適用する	• 該当なし	• 該当なし
BCC	• メールメッセージのブラインドカーボンコピー (BCC) を指定された受信者に送信する	• 該当なし	• 該当なし
通知の送信	• 通知テンプレートで指定されたすべてのメッセージ受信者と連絡先メールアドレスに通知を送信する	• 通知テンプレートで指定されたすべてのメッセージ受信者と連絡先メールアドレスに通知を送信する	• 該当なし
スタンプの挿入	• 設定されている場合、選択されたスタンプを、検出されたメールメ	• 該当なし	• 該当なし

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	ッセージの本文に挿入する		

表 5-3. 処理および動作モード: スパムメール対策ルール

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
メッセージの削除	• メールキューからメールメッセージを削除する • メールメッセージに同じポリシー内の後続のポリシールールを適用しない • メールメッセージを配信しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
受信者の変更	• 指定した 1 人以上の受信者にメールメッセージを配信する • メールメッセージに同じポリシー内の後続のポリシールールを適用しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
ブロックして隔離	• 隔離領域に複製を保存する • [検出] > [隔離] 画面で検索処理を再開するまで、メールメッセージに同じポリシー内の後続のルールを適用しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	• Web コンソールを使用してメッセージを隔離解除できる		
放置およびタグ付け	• メールメッセージに同じポリシー内の後続のルールを適用する • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する	• メールメッセージに同じポリシー内の後続のルールを適用する	• メールメッセージに同じポリシー内の後続のルールを適用する
直接配信	• メールメッセージに同じポリシー内の後続のポリシールールを適用しない • メールメッセージを初期設定の SMTP サーバを使用して受信者に配信するか、指定した SMTP サーバに配信する	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
BCC	• メールメッセージのブラインドカーボンコピー (BCC) を指定された受信者に送信する	• 該当なし	• 該当なし
通知の送信	• 通知テンプレートで指定されたすべてのメッセージ受信者と連	• 通知テンプレートで指定されたすべてのメッセージ受信者と連	• 該当なし

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	絡先メールアドレスに通知を送信する	絡先メールアドレスに通知を送信する	
スタンプの挿入	• 設定されている場合、選択されたスタンプを、検出されたメールメッセージの本文に挿入する	• 該当なし	• 該当なし

表 5-4. 処理および動作モード: 脅威対策ルール

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
メッセージの削除	• メールキューからメールメッセージを削除する • メールメッセージを配信しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
受信者の変更	• 指定した 1 人以上の受信者にメールメッセージを配信する • メールメッセージに同じポリシー内の後続のポリシールールを適用しない	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
ブロックして隔離	• 隔離領域に複製を保存する • メールメッセージを配信しない	• 隔離領域に複製を保存する	• 隔離領域に複製を保存する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
添付ファイルの削除、ブロックページへのリンクのリダイレクト、およびタグ付け	• テキストファイルで不審な添付ファイルを置換 • 不審なリンクをブロックページにリダイレクト • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
添付ファイルの削除、警告ページへのリンクのリダイレクト、およびタグ付け	• テキストファイルで不審な添付ファイルを置換 • 不審なリンクを警告ページにリダイレクト • 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する • メールメッセージを受信者に配信	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
放置およびタグ付け	• 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入する	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
直接配信	• メールメッセージに同じポリシー内の後続のポリシールールを適用しない • 指定した SMTP サーバを使用してメールメッセージを受信者に配信する	• メールキューからメールメッセージを削除する	• メールキューからメールメッセージを削除する
添付ファイルを削除できない場合は元のメッセージを隔離	• 添付ファイルの削除処理が指定されていない場合、または添付ファイルが存在しない場合、隔離領域にメッセージを送信	• 該当なし	• 該当なし
添付ファイルの削除またはリンクのリダイレクト時に元のメッセージのコピーを隔離	• 添付ファイルの削除処理またはリンクのリダイレクトが指定されている場合、隔離領域にコピーを保存	• 該当なし	• 該当なし
添付ファイルを削除する前にウイルス駆除を試行	• 添付ファイルの削除処理が指定されている場合、添付ファイルのウイルス駆除処理を実行 • 添付ファイルのウイルス駆除処理が失敗した場合、または添付ファイルの削除処理が選択されて	• 該当なし	• 該当なし

処理	動作モード		
	MTA モード	SPAN/TAP モード	BCC モード
	いない場合、添付ファイルを削除		
通知の送信	• 通知テンプレートで指定されたすべてのメッセージ受信者と連絡先メールアドレスに通知を送信する	• 通知テンプレートで指定されたすべてのメッセージ受信者と連絡先メールアドレスに通知を送信する	• 該当なし
BCC	• メールメッセージのブラインドカーボンコピー (BCC) を指定された受信者に送信する	• 該当なし	• 該当なし
スタンプの挿入	• 設定されている場合、選択されたスタンプを、検出されたメールメッセージの本文に挿入する	• 該当なし	• 該当なし

注意

- ポリシーの最終処理は [メッセージの削除]、[受信者の変更]、[ブロックして隔離]、および [直接配信] になります。ポリシーに複数のルールが設定されている場合、Deep Discovery Email Inspector は検出されたメッセージに最終処理を 1 つだけ適用します。一致したルールの最終処理をメッセージに適用したら、同じポリシー内の後続のルールに対してメッセージの一致は行われません。

  たとえば、ポリシーにコンテンツフィルタルール、スパムメール対策ルール、および脅威対策ルールが 1 つずつ含まれており、一致したコンテンツフィルタルールに基づいて Deep Discovery Email Inspector がメッセージに [メッセージの削除] 処理を適用した場合、スパムメール対策ルールと脅威対策ルールはメッセージに適用されません。

- ポリシーに複数のルールが設定されている場合、Deep Discovery Email Inspector は、配信が行われるか最終処理が適用されるまで、一致したルールの最終処理以外のすべての処理をメッセージに適用します。

  たとえば、1 つ以上のコンテンツフィルタルール、情報漏えい対策ルール、およびスパムメール対策ルールと、1 つの脅威対策ルールを含むポリシーを設定するとします。最初に一致したコンテンツフィルタルールまたは情報漏えい対策ルールに基づいて Deep Discovery Email Inspector がメッセージに [すべての添付ファイルの削除] 処理を適用した場合、最終処理またはすべての後続のルールが適用されるまでメッセージの検索は継続されます (添付ファイルの仮想アナライザへの送信を除く)。

  一致した 1 つ以上の先行ルールに基づいて Deep Discovery Email Inspector がメッセージに添付ファイルの削除処理を適用しなかった場合、最終処理またはすべての後続のルールが適用されるまでメッセージの検索は継続されます (添付ファイルの仮想アナライザへの送信を含む)。

- メッセージに複数の処理を適用する場合、Deep Discovery Email Inspector は [メッセージの暗号化] を最後の最終処理以外の処理として適用します。

- Deep Discovery Email Inspector は、その他の最終処理または最終処理以外の処理をすべて適用した後に BCC 処理を実行します。

ポリシーの一致

Deep Discovery Email Inspector では最初に、ポリシーを適用するメッセージの方向 (受信または送信) を内部ドメインリストに基づいて判断します。詳細については、330 ページの「内部ドメイン」を参照してください。

受信者または送信者に複数のポリシーが当てはまる場合、Deep Discovery Email Inspector では最も優先度の高いポリシーが一致となり、関連する処理が適用されます。

次のようなポリシーを例に挙げて説明します。

表 5-5. ポリシーの例

優先度	ポリシー名	対象	方向
1	High_Profile_Recipient	受信者: • ceo@example.com • cfo@example.com	受信
2	High_Profile_Recipient_Sender	送信者: jim@partner.com 受信者: • finance_group (Active Directory) • alex@example.com	受信
3	Trusted_Partner	送信者: *@partner.com 送信者の除外: john_doe@partner.com	受信
4	Sales_Team	受信者: • joe@example.com • larry@exmple.com	受信
5	IT_Team	受信者: IT_group (Active Directory)	受信
6	Acquired_Domain	受信者: *@example.com	受信

優先度	ポリシー名	対象	方向
7	送信ポリシー	送信者: *@example.com 注意 ドメイン「example.com」は内部ドメインリストに存在します。 受信者の除外: jane_doe@partner.com	送信
8	初期設定ポリシー	すべての受信者と送信者	受信または送信

次の例は、メッセージの方向と優先度の設定に基づいてトップダウン形式でポリシーを一致させる方法を示しています。

- leo@partner.com から受信者 (joe@example.com) へのメッセージは Trusted_Partner ポリシーに一致します。これは、メッセージが受信メッセージ (ドメイン「partner.com」は内部ドメインリストに存在しない) であり、Trusted_Partner 受信ポリシー (送信者の設定が一致: *@partner.com) の優先度が Sales_Team 受信ポリシー (受信者の設定が一致: joe@example.com) よりも高いためです。
- メッセージが jim@partner.com から 3 人の受信者 (ceo@example.com、alex@example.com、および joe@exmple.com) に送信された場合、Deep Discovery Email Inspector ではメッセージが受信メッセージ (ドメイン「partner.com」は内部ドメインリストに存在しない) と見なされ、次の受信ポリシーに一致します。
  - High_Profile_Recipient: 受信メッセージの方向と受信者 ceo@example.com が一致
  - High_Profile_Recipient_Sender: 受信メッセージの方向と受信者 alex@example.com が一致
  - Trusted_Partner: 受信メッセージの方向と受信者 joe@exmple.com が一致

- メッセージが joe@yahoo.com から 4 人の受信者 (larry@example.com、alex@example.com、bill@example.com、および jane@newdomain.com) に送信され、bill@example.com のみが IT_Team Active Directory グループに所属する場合、Deep Discovery Email Inspector ではメッセージが受信メッセージ (ドメイン「yahoo.com」は内部ドメインリストに存在しない) と見なされ、次のポリシーに一致します。
  - Sales_Team: 受信メッセージの方向と受信者 larry@exmple.com が一致
  - Acquired_Domain: 受信メッセージの方向と受信者 alex@example.com が一致
  - IT_Team: 受信メッセージの方向と受信者 bill@example.com が一致
  - 初期設定ポリシー: 受信メッセージの方向と受信者 jane@newdomain.com が一致
- メッセージが alex@example.com から 2 人の受信者 (larry@example.com と jane@newdomain.com) に送信される場合、Deep Discovery Email Inspector ではメッセージが送信メッセージ (ドメイン「example.com」は内部ドメインリストに存在する) と見なされ、初期設定ポリシーよりも優先度が高い送信ポリシー (送信メッセージの方向、送信者、および受信者が一致) に一致します。
- メッセージが john_doe@partner.com から受信者 henry@example.com に送信された場合、Deep Discovery Email Inspector はそのメッセージを受信メッセージと見なしますが、送信者アドレス john_doe@partner.com はポリシー *Trusted_Partner* の除外リストにあるため、*Acquired_Domain* のみが一致します。
- メッセージが ceo@example.com から受信者 jane_doe@partner.com に送信された場合、Deep Discovery Email Inspector はそのメッセージを送信メッセージと見なしますが、受信者アドレス jane_doe@partner.com は送信ポリシーの除外リストにあるため、初期設定ポリシーのみが一致します。

注意

Deep Discovery Email Inspector では、複数の受信者宛のメッセージが複数のポリシーおよびポリシールールと一致する場合、メッセージ分割が行われます。詳細については、108 ページの「ポリシー分割」を参照してください。

ポリシー分割

Deep Discovery Email Inspector にはインテリジェントなメッセージ分割機能が用意されています。この機能を使用することで、複数の受信者宛のメッセージに複数の独立したポリシーを一致させることができます。メッセージ分割により、Deep Discovery Email Inspector ではトップダウン形式でポリシーリストに照らして各受信者を評価できます。ポリシーが一致すると、影響を受ける受信者の数にメッセージが分割 (メッセージ分割が作成) されます。

Deep Discovery Email Inspector では、複数の受信者宛のメッセージが異なるポリシーの異なるポリシールールに一致する場合にのみ、メッセージ分割が作成されます。メッセージのすべての受信者が同じポリシーに一致する場合や、異なるポリシーの同じルールに受信者が一致する場合、メッセージ分割は作成されません。

次のポリシーで説明します。

ポリシー名	ルール
ポリシー A	• コンテンツフィルタルール: メッセージをタグ付け (キーワード一致) • スパムメールフィルタルール: スパムメールメッセージを削除 • 脅威対策ルール: メッセージを削除 (すべてのリスクレベル)
ポリシー B	• コンテンツフィルタルール: 添付ファイルを削除 (実行可能ファイル) • スパムメールフィルタルール: スパムメールメッセージをタグ付け • 脅威対策ルール: メッセージを削除 (すべてのリスクレベル)

ポリシー名	ルール
ポリシー C	• コンテンツフィルタルール: メッセージをタグ付け (キーワード一致) • コンテンツフィルタルール: 添付ファイルを削除 (実行可能ファイル) • スパムメールフィルタルール: スパムメールメッセージをタグ付け • 脅威対策ルール: メッセージを隔離 (すべてのリスクレベル)
ポリシー D	• コンテンツフィルタルール: メッセージをタグ付け (キーワード一致) • 脅威対策ルール: メッセージを隔離 (すべてのリスクレベル)

次のシナリオは、ポリシーやルールの一致に基づいてメッセージ分割を作成する方法を示しています。

- メッセージが joe@test.com から受信者の alex@example.com と linda@example.com に送信されます。alex@example.com と linda@example.com が「ポリシー A」に一致し、メッセージがコンテンツフィルタルールの「メッセージをタグ付け (キーワード一致)」に一致する場合、一致する同じポリシーに対して同じポリシールールが適用されるのでメッセージ分割は作成されません。
- メッセージが joe@test.com から受信者の jane@example.com、mark@example.com、および leo@example.com に送信されます。jane@example.com と mark@example.com が「ポリシー B」に一致し、leo@example.com が「ポリシー C」に一致して、メッセージがポリシールールの「添付ファイルを削除 (実行可能ファイル)」と「スパムメールメッセージをタグ付け」に一致する場合、一致するポリシーに対して同じポリシールールが適用されるのでメッセージ分割は作成されません。
- メッセージが joe@test.com から受信者の jane@example.com と bill@example.com に送信されます。jane@example.com が「ポリシー B」に一致し、bill@example.com が「ポリシー D」に一致して、メッセージがポリシールールの「スパムメールメッセージをタグ付け」と「メッセージをタグ付け (キーワード一致)」に一致する場合、メッセージは 2 つに分割されます。この場合、ポリシールールの「スパムメールメッセージをタグ付け」が jane@example.com 宛の 1 通のメッセージに適用され、

ポリシールールの「メッセージをタグ付け (キーワード一致)」が bill@example.com 宛のもう 1 通のメッセージに適用されます。

ポリシーリスト

Deep Discovery Email Inspector では、ポリシーに定義されたルールに照らしてメールメッセージが評価されます。ポリシーは送信者または受信者に個別に適用することも、送信者または受信者のグループに適用することもできます。Deep Discovery Email Inspector では、メッセージ内の送信者および受信者の情報およびメッセージの方向に基づいてポリシーの一致が行われます。メッセージが複数のポリシーに一致する場合は、最も優先度の高いポリシールールの処理が実行されます。

次の表は、[ポリシーリスト] 画面の詳細を示しています。

フィールド	説明
優先度	ポリシーの優先度を表示します。数字が小さいほど優先度が高くなります。
ポリシー名	ポリシーの名前を表示します。
方向	ポリシーが適用されるメッセージの方向を表示します。
送信者と受信者	ポリシーを適用する送信者と受信者のリストを表示します。
ルール	ポリシーに含まれるルールのリストを表示します。
アーカイブサーバ	メッセージをアーカイブするサーバの名前を表示します。
前回のアップデート	ポリシーをアップデートした日時を表示します。
説明	ポリシーの説明を表示します。
ステータス	ポリシーの有効/無効を切り替えます。

次の表は、ポリシーにクエリを実行するための基本的な検索フィルタについて説明しています。

注意

[送信者] と [受信者] の検索フィルタには、完全なメールアドレスまたはローカル部を指定することをお勧めします。Deep Discovery Email Inspector はこのフィルタに基づき、送信者と受信者のメールアドレスおよび Active Directory のユーザとグループをポリシー内で検索します。

フィルタ	説明
ステータス	[すべて] またはステータスをリストから選択します。
方向	ポリシーが適用されるメッセージの方向を選択します。
除外	除外設定 ([なし] または [指定]) を選択して、リスト内のポリシーをフィルタします。
送信者	送信者の完全なメールアドレスを入力して、検索アイコン ( ) をクリックします。
受信者	受信者の完全なメールアドレスを入力して、検索アイコン ( ) をクリックします。
ルール名	ルール名を入力して検索アイコン ( ) をクリックします。 画面にテキストを含むエントリが表示されます。

[ポリシーリスト] 画面では次の操作を実行できます。

- 追加: 新しいポリシーを作成します。
- エクスポート: ポリシーを ZIP ファイルでダウンロードします。
- インポート: 元になる Deep Discovery Email Inspector アプライアンスからエクスポートしたポリシーをインポートします。これにより、同じポリシー設定を複数の Deep Discovery Email Inspector アプライアンス間で複製できます。
- 削除: 選択したポリシーをポリシーリストから削除します。
- コピー: 選択したポリシーのコピーを作成します。コピーを編集して、カスタマイズポリシーを作成できます。

ポリシーを設定する

ポリシーを設定することで、メッセージングシステムにおけるセキュリティ上の脅威を抑制し、生産性の低下を防ぐことができます。

ポリシーには次の設定が必要です。

- 一般設定: ポリシー名およびポリシーを適用するホストを指定します。
- ポリシールールの選択:
  - 1 つの脅威対策ルール
  - (オプション) 1 つ以上のコンテンツフィルタルール、情報漏えい対策ルール、またはスパムメール対策ルール

注意

- ポリシーを設定する前に、必要なポリシーコンポーネント (内部ドメイン、通知、およびポリシールール) を作成してください。
- 信頼された送信者/受信者またはポリシー除外対象のオブジェクトを指定できます。

  詳細については、165 ページの「ポリシー除外」を参照してください。

手順

1. 必要なポリシーコンポーネントを設定します。
   - 135 ページの「通知」
   - 117 ページの「ポリシールール」
2. [ポリシー] > [ポリシー管理] の順に選択します。

   [ポリシーリスト] 画面が表示されます。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいポリシーを作成します。
   - ポリシー名をクリックして設定を編集します。

4. [有効] を選択してポリシーを有効にします。
5. ポリシー名を入力します。
6. Deep Discovery Email Inspector が検索を実行する優先順位を入力します。Deep Discovery Email Inspector では、指定した順位に基づいてメッセージにポリシールールが適用されます。
7. ポリシーの説明を入力します。
8. ポリシーのメッセージの方向を選択します。
9. 送信者と受信者を指定します。次のいずれかを実行します。
   - ポリシールールをすべての送信者または受信者に適用するには、[すべて] を選択します。
   - [送信者の指定] または [受信者の指定] を選択し、次の手順を実行してアドレスリストを設定します。

注意

送信者のドメインが内部ドメインリストに存在する場合、Deep Discovery Email Inspector は、その送信者からのメッセージに受信ポリシーを適用しません。

a. 種類を選択して、必要な情報を入力します。
b. 必要な情報を入力します。

種類	説明
メールアドレス	有効なメールアドレスを入力します。 例: test@example.com
LDAP ユーザまたはグループ	ユーザまたはグループの名前を入力して <Enter> キーを押し、一致するユーザアカウントまたはグループを探します。

種類	説明
アドレスグループ	アドレスグループ名を入力して <Enter> キーを押し、一致するアドレスグループを探します。 アドレスグループを設定すると、同じポリシーを複数のメールアドレスに適用できます。 詳細については、164 ページの「アドレスグループを設定する」を参照してください。

c. 必要に応じて、検索結果からアドレスグループまたは LDAP ユーザ/グループを選択します。

d. [追加] をクリックします。

10. (オプション) [除外] で、指定された送信者と受信者のアドレスペアのメッセージに対するポリシー検索をバイパスするように Deep Discovery Email Inspector を設定できます。次の手順を実行します。

a. [除外の指定] を選択します。

a. [送信元 (送信者)] と [送信先 (受信者)] のドロップダウンリストからオプションを選択し、必要な情報を入力します。

種類	説明
任意	すべての送信者または受信者のメールアドレスを含めるには、このオプションを選択します。
メールアドレス	有効なメールアドレスを入力します。 例: test@example.com
LDAP ユーザまたはグループ	ユーザまたはグループの名前を入力して <Enter> キーを押し、一致するユーザアカウントまたはグループを探します。
アドレスグループ	アドレスグループ名を入力して <Enter> キーを押し、一致するアドレスグループを探します。 アドレスグループを設定すると、同じポリシーを複数のメールアドレスに適用できます。 詳細については、164 ページの「アドレスグループを設定する」を参照してください。

b. 必要に応じて、検索結果からアドレスグループまたは LDAP ユーザ/グループを選択します。

c. [追加] をクリックします。

11. (オプション) [アーカイブサーバ] ドロップダウンリストからオプションを選択して、ポリシーに一致するメッセージのコピーをアーカイブします。初期設定のオプション ([なし]) ではメッセージのアーカイブは 無効です。

注意

- メッセージが複数のポリシーに一致し、それぞれのポリシーに異なるアーカイブサーバが設定されている場合、Deep Discovery Email Inspector はメッセージのコピーを各アーカイブサーバに 送信します。
- メッセージが複数のポリシーに一致し、それぞれのポリシーに同じアーカイブサーバが設定されている場合、Deep Discovery Email Inspector はメッセージのコピーをそのアーカイブサーバにのみ 送信します。

詳細については、141 ページの「アーカイブサーバ」を参照してください。

12. 脅威対策ルールを指定します。

a. [脅威対策] タブをクリックします。

b. [ルール] ドロップダウンリストからオプションを 選択します。

c. [追加] をクリックします。

注意

- ルールの設定を表示するには、[表示] をクリックします。
- 脅威対策ルールの設定の詳細については、130 ページの「脅威対策ルール」を参照してください。

---

13. (オプション) コンテンツフィルタルールを 1 つ以上指定します。
    a. [コンテンツフィルタ] タブをクリックします。
    b. [ルール] ドロップダウンリストからオプションを 選択します。
    c. [追加] をクリックします。

    注意
    - ルールの設定を表示するには、[表示] をクリックします。
    - コンテンツフィルタルールの 設定の詳細については、117 ページの「コンテンツフィルタルール」を参照してください。

14. (オプション) 1 つ以上の情報漏えい対策ルールを指定します。
    a. [情報漏えい対策] タブをクリックします。
    b. [ルール] ドロップダウンリストからオプションを 選択します。
    c. [追加] をクリックします。

    注意
    - ルールの設定を表示するには、[表示] をクリックします。
    - 情報漏えい対策ルールの設定の詳細については、124 ページの「情報漏えい対策ルール」を参照してください。

15. (オプション) スパムメール対策ルールを 1 つ以上指定します。
    a. [スパムメール対策] タブをクリックします。
    b. [ルール] ドロップダウンリストからオプションを 選択します。
    c. [追加] をクリックします。

    注意
    - ルールの設定を表示するには、[表示] をクリックします。
    - スパムメール対策ルールの設定の詳細については、126 ページの「スパムメール対策ルール」を参照してください。

16. [保存] をクリックします。

ポリシールール

次の種類のルールを作成して、組織のウイルス対策などのセキュリティを強化します。

- コンテンツフィルタルール: メッセージの内容を評価して、望ましくないコンテンツが受信者に配信されないようにし、Microsoft Office や PDF ファイルの添付ファイルからアクティブコンテンツ (マクロなど) を削除します。
- 情報漏えい対策ルール: メールメッセージを介したデジタル資産の転送を防止します。
- スパムメール対策ルール: スパムメールまたはグレーメールについてメッセージを検索します。
- 脅威対策ルール: スパイウェア、ワームなどのウイルスおよびその他の不正プログラムについてメッセージを検索します。

オプションで、事前定義済みのポリシールールをコピーして編集することで、新しいポリシールールを作成できます。

コンテンツフィルタルール

コンテンツフィルタルールを 使用すると、メッセージの内容や添付ファイルに基づいてメールメッセージの配信を評価および制御できます。Deep Discovery Email Inspector では、コンテンツフィルタルールを 使用して受信および送信メッセージを監視し、不正な可能性がある添付ファイルや、嫌がらせ、攻撃、またはその他の不快な内容が含まれていないかどうかを確認します。

コンテンツフィルタルールで 定義された検索条件に一致するメッセージが検出されると、Deep Discovery Email Inspector はメッセージに処理を実行して、望ましくないコンテンツが Microsoft Exchange クライアントに配信されないようにします。

コンテンツフィルタルールのリストは、[コンテンツフィルタルール] 画面で表示できます。次の表は、ルールの詳細を示しています。

フィールド	説明
ルール名	ルールのわかりやすい名前を表示します。 ルールの設定を編集するには、ルール名をクリックします。
処理	ルール条件が一致した場合に適用する 1 つ以上の処理を表示します。
関連するポリシー	そのルールを含むポリシーの数を表示します。
前回の更新	前回エントリをアップデートした日時を表示します。

コンテンツフィルタルールを設定する

コンテンツフィルタルールを 作成し、次の検索条件に基づいて受信および送信メールメッセージを 評価できます。

- 添付ファイルの種類、ファイル名、ファイルサイズ、または添付ファイル数
- メールのヘッダ、本文、または添付ファイルの内容
- 送信者の認証結果
- 内部ドメインと許可された送信者アドレス

手順

1. [ポリシー] > [ポリシー管理] の順に選択します。
2. [コンテンツフィルタルール] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして、新しいルールを作成します。
   - ルール名をクリックして、設定を変更します。
4. ルール名を入力します。
5. 検索条件を設定します。
   a. [添付ファイル] で、添付ファイルの条件を指定します。

詳細については、121 ページの「添付ファイルの検索条件」を参照してください。

b. [内容] で、メッセージ内の一致するキーワードまたはパターンを 1 つ以上指定します。

詳細については、123 ページの「キーワードリストまたはパターンを追加する」を参照してください。

c. [送信者の認証結果] で、送信者の認証プロトコルを 1 つ以上選択し、ドロップダウンリストから認証結果を 1 つ以上選択します。

注意

- コンテンツフィルタルールで 送信者の認証結果の設定を有効にするには、[管理] > [送信者フィルタ/認証] の順に選択し、認証プロトコルのタブ ([SPF]、[DKIM 認証]、または [DMARC]) をクリックします。次に認証プロトコルを有効にして、[メールメッセージに X-Header を挿入する] を選択します。
- 選択した送信者の各認証プロトコルの認証結果が一致する場合、Deep Discovery Email Inspector はメールメッセージを一致と見なします。

---

d. (オプション) [送信者のアドレスがメッセージヘッダ (From) と一致しない場合にルールを適用する] を選択して、送信者のアドレスとメッセージヘッダ内の「From」フィールドのアドレスが一致しない場合はコンテンツフィルタルールを 適用します。

注意

このオプションは、Deep Discovery Email Inspector が BCC モードで動作している場合は適用されません。

---

e. (オプション) 内部ドメインのメッセージのうち、許可された送信者アドレスから発信されていないメッセージを検出するには、[内部メールスプーフィングの 防止を有効にする] を選択し、ドメインと IP アドレスの一致オプションを指定します。

- ドメインの一致: メッセージのエンベロープ送信者アドレスまたはヘッダ From アドレスを内部ドメインリストと照合します。

  一致が見つかった場合は、続いてメッセージの送信者または送信元 IP アドレスが確認されます。

- IP アドレスの一致: メッセージの送信者 IP アドレス、送信元 IP アドレス、またはその両方を許可された送信者アドレスリストと照合します。

  一致が見つからない場合、メッセージは社内メールのスプーフィング試行と見なされ、ルールの処理が適用されます。

注意

内部ドメインリストは [内部ドメイン] 画面で、許可された送信者 IP アドレスは [制限および除外] 画面で設定できます。

詳細については、330 ページの「内部ドメイン」および 323 ページの「制限と除外を設定する」を参照してください。

6. [処理] を指定します。

   詳細については、90 ページの「ポリシーの処理」を参照してください。

7. (オプション) 検出されたメッセージのブラインドカーボンコピーを 1 人以上の受信者に送信するには、[BCC] フィールドに受信者のメールアドレスを入力します。

注意

最大 50 件のメールアドレスを指定できます。ワイルドカード文字は使用できません。

8. (オプション) [通知の送信] ドロップダウンリストから、適用されたポリシー処理について受信者に知らせる通知メッセージを選択します。

重要

Deep Discovery Email Inspector では、[通知の送信] と通知メッセージを選択すると、受信者通知のみが送信されます。

通知メッセージは、[通知] 画面 ([ポリシー] > [ポリシーオブジェクト] > [通知] の順に選択) で設定できます。

詳細については、135 ページの「受信者通知を設定する」を参照してください。

9. (オプション) [スタンプの挿入] ドロップダウンリストから、検出されたメッセージに挿入するスタンプを選択します。

   詳細については、138 ページの「メッセージスタンプを設定する」を参照してください。

10. [保存] をクリックします。

    ルールの追加後、次の操作を実行できます。

    - ルールの設定を編集するには、ルール名をクリックします。
    - ルールを削除するには、ルールを選択して [削除] をクリックします。

添付ファイルの検索条件

コンテンツフィルタルールでは、次の検索条件を指定して、添付ファイルを含むメールメッセージをフィルタできます。すべての条件が満たされると、メールメッセージは一致と見なされます。

設定	説明

ファイルタイプ	一致オプションやファイルタイプに基づいてメールメッセージをフィルタする場合は、このオプションを選択します。
	• 一致オプション:
	  • 選択した添付ファイルの種類:選択した種類の添付ファイルを含むメッセージに対して処理を実行します。
	  • 選択した添付ファイルの種類以外:選択した種類以外の添付ファイルを含むメッセージに対して処理を実行します。
	• ファイルタイプ:
	  • 実際のファイルタイプ
	  • カスタムファイル拡張子
	  • パスワード保護されたアーカイブファイル
	  注意
	カスタムファイル拡張子にはワイルドカードを含めないでください。

ファイル名	ファイル名に基づいてメールメッセージをフィルタする場合は、このオプションを選択します。 ファイル名を入力して、<Enter> キーを押します。テキストフィールドには複数のファイル名を指定できます。  注意 ファイル名にはワイルドカードを含めないでください。
添付ファイルサイズ	添付ファイルサイズに基づいてメールメッセージをフィルタする場合は、このオプションを選択して次のように設定します。 • 比較記号を選択します。 • 添付ファイルサイズを表す値を入力します。 • 単位 (KB または MB) を選択します。

設定	説明
添付ファイル数	検出された添付ファイル数に基づいてメールメッセージをフィルタする場合は、このオプションを選択して次のように設定します。 • 比較記号を選択します。 • 添付ファイルの数を表す値を入力します。

キーワードリストまたはパターンを追加する

メールメッセージに一致させる 1 つ以上のキーワードリスト (キーワードを含む) とパターンを選択できます。

注意

キーワードリストまたはパターンをコンテンツフィルタルールに 追加する前に、[データ識別子] 画面でキーワードリストまたはパターンを設定します。

詳細については、156 ページの「キーワードリストを設定する」および 147 ページの「カスタマイズされたパターンを設定する」を参照してください。

手順

1. [内容] で [追加] をクリックします。

   [キーワードリストとパターンの追加] 画面が表示されます。

2. メッセージセクションを選択します。
3. 選択したメッセージセクションに必要な設定を行います。
   - [ヘッダ] メッセージセクションでは、次の操作を実行します。
     a. メッセージヘッダを選択するか指定します。
     b. リスト表示オプションを選択します。
     c. キーワードリストまたはパターンを 1 つ以上選択します。
     d. [追加] をクリックします。

ヒント

- コンテンツに一致させるエントリをさらに追加するには、この手順を繰り返します。
- ごみ箱アイコン () をクリックすると、表からエントリを削除できます。

- [本文] または [添付ファイル] メッセージセクションでは、次の操作を実行します。
  a. リスト表示オプションを選択します。
  b. キーワードリストまたはパターンを 1 つ以上選択します。

4. [保存] をクリックします。

情報漏えい対策ルール

Deep Discovery Email Inspector では、ポリシー内の一連の情報漏えい対策ルールに照らし合わせてファイルまたはデータを評価します。情報漏えい対策ルールにより、不正な転送から保護する必要のあるファイルまたはデータが判別され、転送の検出時に Deep Discovery Email Inspector が実行する処理が決定されます。

データ識別子を設定して情報漏えい対策テンプレートで編成したら、情報漏えい対策ルールの設定を開始できます。

注意

Deep Discovery Email Inspector の初期設定では、受信者および送信者の設定に基づいて送信メールメッセージに情報漏えい対策ポリシーが適用されます。

情報漏えい対策ルールを設定する

情報漏えい対策ルールを作成して、Deep Discovery Email Inspector がメールメッセージを使用した無許可のデータ転送を検出した場合に適用する処理を指定できます。

手順

1. [ポリシー] > [ポリシー管理] の順に選択します。
2. [情報漏えい対策ルール] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして、新しいルールを作成します。
   - ルール名をクリックして、設定を変更します。
4. ルール名を入力します。
5. リスト表示オプションを選択します。
6. [利用可能なテンプレート] リストでテンプレートを 1 つ以上選択します。

   選択した項目が [選択したテンプレート] リストに表示されます。
7. [処理] を指定します。

   詳細については、90 ページの「ポリシーの処理」を参照してください。
8. (オプション) 検出されたメッセージのブラインドカーボンコピーを 1 人以上の受信者に送信するには、[BCC] フィールドに受信者のメールアドレスを入力します。

   注意

   最大 50 件のメールアドレスを指定できます。ワイルドカード文字は使用できません。
9. (オプション) [通知の送信] ドロップダウンリストから、適用されたポリシー処理について受信者に知らせる通知メッセージを選択します。

   重要

   Deep Discovery Email Inspector では、[通知の送信] と通知メッセージを選択すると、受信者通知のみが送信されます。

   通知メッセージは、[通知] 画面 ([ポリシー] > [ポリシーオブジェクト] > [通知] の順に選択) で設定できます。

詳細については、135 ページの「受信者通知を設定する」を参照してください。

10. (オプション) [スタンプの挿入] ドロップダウンリストから、検出されたメッセージに挿入するスタンプを選択します。

    詳細については、138 ページの「メッセージスタンプを設定する」を参照してください。

11. [保存] をクリックします。

    ルールの追加後、次の操作を実行できます。

    - ルールの設定を編集するには、ルール名をクリックします。
    - ルールを削除するには、ルールを選択して [削除] をクリックします。
    - ルールのコピーを作成するには、ルールを選択して [コピー] をクリックします。コピーしたルールを編集して、カスタマイズルールを作成できます。

スパムメール対策ルール

Deep Discovery Email Inspector では、スパムメール対策ルールを使用して、スパムメールまたはグレーメールとして識別されたメッセージを検索します。

詳細については、8 ページの「スパムメール検索」および 9 ページの「グレーメール検索」を参照してください。

注意

- スパムメール対策機能を最大限活用するには、Email Reputation Services (ERS) テクノロジを使用するように Deep Discovery Email Inspector を設定します。

  詳細については、280 ページの「Email Reputation Services を設定する」を参照してください。

- グレーメールの除外を設定すると、信頼する IP アドレスからのメッセージについてグレーメール検索をバイパスできます。

  詳細については、171 ページの「グレーメールの除外」を参照してください。

次の表は、[スパムメール対策ルール] 画面の各フィールドを示しています。

フィールド	説明
ルール名	ルールのわかりやすい名前を表示します。 ルールの設定を編集するには、ルール名をクリックします。
処理	ルール条件が一致した場合に適用する 1 つ以上の処理を表示します。
関連するポリシー	そのルールを含むポリシーの数を表示します。
前回の更新	前回エントリをアップデートした日時を表示します。

スパムメール対策ルールを設定する

スパムメール対策ルールを作成して、次の種類の潜在的に不正なメッセージに対する処理を指定できます。

- スパムメール
- グレーメール

手順

1. [ポリシー] > [ポリシー管理] の順に選択します。
2. [スパムメール対策ルール] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして、新しいルールを作成します。
   - ルール名をクリックして、設定を変更します。
4. ルール名を入力します。
5. [スパム]、[グレーメール]、または両方のメッセージの種類を選択して、検索条件を設定します。

メッセージの種類	説明
スパムメール	指定したスパムメールの検出率または検出しきい値に基づいてスパムメールメッセージを検索できます。 • 高: スパムメール検出の最も厳格なレベルです。すべてのメールメッセージで不審なファイルやテキストを監視しますが、誤検出の可能性が高くなります。誤検出とは、実際には正当なメールメッセージがスパムメールとしてフィルタされることです。 • 中: 推奨設定です (初期設定)。誤検出の可能性を抑えながら、スパムメール検出を高レベルで行います。 • 低: スパムメール検出の最も緩やかなレベルです。一般に知られた明らかなスパムメールメッセージのみをフィルタしますが、誤検出の可能性は最も低くなります。 • 指定 {}: メッセージを分析してスパムメールかどうかを判断する基準を 3.0〜10.0 のしきい値で入力します。

メッセージの種類	説明
グレーメール	Email Reputation Services (ERS) のスコアに照らしてメッセージを検索し、グレーメールメッセージを識別します。 Deep Discovery Email Inspector でグレーメールと見なすメッセージのカテゴリを 1 つ以上選択します。 **注意** 信頼される送信者の IP アドレスまたはサブネットを [グレーメールの除外]リストに追加できます。このリストの IP アドレスまたはサブネットからのメールメッセージは、Deep Discovery Email Inspector のグレーメール検索をバイパスします。 詳細については、172 ページの「グレーメールの除外を追加する」を参照してください。

6. [処理] を指定します。

   詳細については、90 ページの「ポリシーの処理」を参照してください。

7. (オプション) 検出されたメッセージのブラインドカーボンコピーを 1 人以上の受信者に送信するには、[BCC] フィールドに受信者のメールアドレスを入力します。

   注意
   最大 50 件のメールアドレスを指定できます。ワイルドカード文字は使用できません。

8. (オプション) [通知の送信] ドロップダウンリストから、適用されたポリシー処理について受信者に知らせる通知メッセージを選択します。

   重要
   Deep Discovery Email Inspector では、[通知の送信] と通知メッセージを選択すると、受信者通知のみが送信されます。

通知メッセージは、[通知] 画面 ([ポリシー] > [ポリシーオブジェクト] > [通知] の順に選択) で設定できます。

詳細については、135 ページの「受信者通知を設定する」を参照してください。

9. (オプション) [スタンプの挿入] ドロップダウンリストから、検出されたメッセージに挿入するスタンプを選択します。

   詳細については、138 ページの「メッセージスタンプを設定する」を参照してください。

10. [保存] をクリックします。

    ルールの追加後、次の操作を実行できます。

    - ルールの設定を編集するには、ルール名をクリックします。
    - ルールを削除するには、ルールを選択して [削除] をクリックします。
    - ルールのコピーを作成するには、ルールを選択して [コピー] をクリックします。コピーしたルールを編集して、カスタマイズルールを作成できます。

脅威対策ルール

Deep Discovery Email Inspector では、脅威対策ルールにより、脅威からの保護を実現するセキュリティコントロールが提供されます。脅威対策ルールを設定すれば、トラフィック処理の動作を指定して通知メッセージをカスタマイズできます。

Deep Discovery Email Inspector では、次の検索テクノロジを使用してウイルスやその他の不正プログラムについてメッセージを検索します。

- 14 ページの「仮想アナライザ」
- 14 ページの「高度な脅威検索エンジン」
- 15 ページの「機械学習型検索」

次の表は、[脅威対策ルール] 画面の各フィールドを示しています。

フィールド	説明
ルール名	ルールのわかりやすい名前を表示します。 ルールの設定を編集するには、ルール名をクリックします。
処理	ルール条件が一致した場合に適用する 1 つ以上の処理を表示します。
関連するポリシー	そのルールを含むポリシーの数を表示します。
前回の更新	前回エントリをアップデートした日時を表示します。

脅威対策ルールを設定する

脅威対策ルールを作成して、スパイウェア、ワームなどのウイルスおよびその他の不正プログラムについてメッセージを検索できます。

手順

1. [ポリシー] > [ポリシー管理] の順に選択します。
2. [脅威対策ルール] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして、新しいルールを作成します。
   - ルール名をクリックして、設定を変更します。
4. ルール名を入力します。
5. リスク高、リスク中、リスク低、および未評価のメッセージについて設定を行います。
   a. [未評価] のメッセージについては、検出の理由を選択します。
   b. [処理] を指定します。

      詳細については、90 ページの「ポリシーの処理」を参照してください。
   c. (オプション) [通知の送信] ドロップダウンリストから、適用されたポリシー処理について受信者に知らせる通知メッセージを選択します。

重要

Deep Discovery Email Inspector では、[通知の送信] と通知メッセージを選択すると、受信者通知のみが送信されます。

通知メッセージは、[通知] 画面 ([ポリシー] > [ポリシーオブジェクト] > [通知] の順に選択) で設定できます。

詳細については、135 ページの「受信者通知を設定する」を参照してください。

d. (オプション) リスク低のメッセージについては、件名タグと X-Header を設定します。

- [件名タグ]: メールメッセージの件名に挿入する文字列を指定します。
- [X-Header]: X-Header に追加するテキストを指定します。

6. (オプション) [詳細設定] で、次の設定を 1 つ以上選択します。

- Deep Discovery Email Inspector で添付ファイルを削除できない場合に、検出したメールメッセージを隔離して保存するには、[添付ファイルを削除できない場合は元のメッセージを隔離] を選択します。受信者にメールメッセージは配信されません。

注意

- この設定は、Deep Discovery Email Inspector が MTA モードの場合にのみ有効になります。
- このオプションを選択すると、検出されたフィッシングメッセージも隔離されます。

- さらに詳しく調査するために、検出されたメールメッセージのコピーを添付ファイルや URL とともに隔離領域に保存するには、[添付ファイルの削除またはリンクのリダイレクト時に元のメッセージのコピーを隔離] を選択します。

注意

この設定は、Deep Discovery Email Inspector が MTA モードの場合にのみ有効になります。

- ルールに添付ファイルの削除処理も選択する場合は、[添付ファイルを削除する前にウイルス駆除を試行] を選択し、Deep Discovery Email Inspector で最初に添付ファイルのウイルス駆除を実行するようにします。添付ファイルのウイルス駆除を実行できない場合、Deep Discovery Email Inspector は添付ファイルを削除します。

  このチェックボックスをオフにすると、不正プログラムとして検出された添付ファイルが即座に削除されます。

注意

この設定は、Deep Discovery Email Inspector が MTA モードの場合にのみ有効になります。

- [仮想アナライザへのサブミッションの優先度設定] を選択して、検出されたメールメッセージを高い優先度で仮想アナライザにサブミットします。
- ポリシールールに一致したメールメッセージのうち、削除または隔離されていないメールメッセージを指定した SMTP サーバに送信するには、[直接配信] を選択します。

注意

この設定を選択する場合は、SMTP サーバのアドレスとポート番号を指定する必要があります。

- 検出されたメッセージのブラインドカーボンコピーを受信者に送信するには、[BCC] を選択し、フィールドに受信者のメールアドレスを 1 つ以上入力します。

注意

最大 50 件のメールアドレスを指定できます。ワイルドカード文字は使用できません。

- (オプション) [スタンプの挿入] ドロップダウンリストから、検出されたメッセージに挿入するスタンプを選択します。

  詳細については、138 ページの「メッセージスタンプを設定する」を参照してください。

7. [保存] をクリックします。

   ルールの追加後、次の操作を実行できます。

   - ルールの設定を編集するには、ルール名をクリックします。
   - ルールを削除するには、ルールを選択して [削除] をクリックします。

ポリシーオブジェクト

ポリシーオブジェクトを作成し、すべてのポリシールールで共有する設定を保存することで、ポリシー管理が簡単になります。

次の表は、Deep Discovery Email Inspector で設定できるポリシーオブジェクトを示しています。

ポリシーオブジェクト	説明
通知	受信者またはメール管理者に、Deep Discovery Email Inspector がメッセージに対して何らかの処理を実行したことや、メッセージが Deep Discovery Email Inspector ルールの検索条件に違反していることを通知するメッセージを作成します。
置換ファイル	受信者に Deep Discovery Email Inspector がメッセージに対して何らかの処理を実行したことや、メッセージがルールの検索条件に違反していることを通知するテキスト (処理されたすべてのメッセージに添付) およびファイル名 (削除された添付ファイルの置き換え) を指定します。
スタンプ	メッセージの方向に基づいて、メッセージに挿入するスタンプを最大 3 つ設定します。
リダイレクトページ	ユーザが不審なリンクを開かないようにブロックまたは警告するリダイレクトページを指定します。

ポリシーオブジェクト	説明
アーカイブサーバ	ポリシー設定に基づいてメールメッセージを保存する、最大 10 台のアーカイブサーバを設定します。
データ識別子	コンテンツフィルタルールや情報漏えい対策ポリシールールに適用可能なデータ識別子 (パターン、ファイル属性、キーワード) を設定します。
情報漏えい対策テンプレート	情報漏えい対策テンプレートを設定してデータ識別子と論理演算子を含め、情報漏えい対策ポリシールールで使用します。
アドレスグループ	アドレスグループを設定して、ポリシールールを複数のメールアドレスに一度に適用します。

通知

通知を設定して、ポリシールールに関連付けることができます。ルールが一致すると、Deep Discovery Email Inspector では、メールメッセージが処理されたことと、そのメールメッセージに不審または不正なコンテンツが含まれている可能性があることを、指定された受信者に通知します。

次の表は、[通知] 画面の詳細を示しています。

ヘッダ	説明
名前	通知の名前を表示します。
メッセージ	通知メッセージの一部を表示します。
関連するルール	通知に関連するルールの数を表示します。
前回の更新	前回エントリをアップデートした日時を表示します。

受信者通知を設定する

受信者通知を作成してポリシールールで使用できます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [通知] の順に選択します。

2. 次のいずれかを実行します。
   - [追加] をクリックして、新しい通知を作成します。
   - 名前をクリックして、設定を変更します。
3. [名前] に通知のわかりやすい名前を入力します。
4. [受信者] で、関連するポリシールールが一致した場合に通知を送信する受信者を指定します。
   - 元のメール受信者: 検出されたメールメッセージの本来の受信者に通知を送信するには、このオプションを選択します。
   - 元のメール送信者: 検出されたメールメッセージの本来の送信者に通知を送信するには、このオプションを選択します。
   - すべての連絡先とその他の通知受信者に送信: [連絡先] 画面に定義されたメールアドレスと指定された受信者に通知を送信するには、このオプションを選択します。

     詳細については、441 ページの「連絡先を管理する」を参照してください。

     (オプション) その他の受信者に通知を送信するには、[その他の通知受信者] テキストボックスにメールアドレスを入力します。複数のエントリはセミコロン (;) で区切ります。
5. Deep Discovery Email Inspector でメールメッセージを調査および処理した後に受信者に送信するメール通知を設定します。

   メッセージをカスタマイズするには、指定されたトークンを使用します。詳細については、506 ページの「受信者通知メッセージトークン」を参照してください。
6. [保存] をクリックします。

   通知の追加後、次の操作を実行できます。
   - 選択した通知を複製するには、[コピー] をクリックします。通知設定を編集して、新しい通知を作成できます。
   - エントリをリストから削除するには、通知を選択して [削除] をクリックします。

置換ファイル

Deep Discovery Email Inspector では、検出されたメッセージ内の削除された不審添付ファイルを置換ファイルで置き換え、メールメッセージが処理されたことと、不審または不正な添付ファイルが削除されたことを受信者に通知します。

置換ファイルを設定する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [置換ファイル] の順に選択します。
2. [置換ファイル] で、次の設定を行います。
   - ファイル名: 置換ファイルのファイル名を指定します。
   - テキスト: 置換ファイルに含めるテキストを指定します。

   ヒント

   [利用可能なトークン] リストからトークンをテキストに含めることができます。トークンは置換ファイルを送信する前に実際のデータに置き換えられます。
3. [保存] をクリックします。

メッセージスタンプ

メッセージスタンプはメールメッセージ 内に挿入され、メッセージが Deep Discovery Email Inspector によって処理されたことを受信者に通知します。

メッセージの方向に基づいて最大 3 つのメッセージスタンプ (受信、送信、受信および送信のメッセージの方向に 1 つずつ) を設定できます。ポリシールールに作成できるスタンプの数に制限はありません。

次の表は、[スタンプ] 画面の詳細を示しています。

フィールド	説明
名前	スタンプのわかりやすい名前を表示します。
内容	スタンプのテキストの内容を表示します。
挿入位置	メッセージ本文内のスタンプ挿入位置を表示します。
方向	スタンプが適用されるメッセージの方向を表示します。 スタンプが 1 つ以上のポリシールールで使用されている場合、このフィールドにはダッシュ「-」が表示されます。
関連するルール	スタンプが適用されるポリシールールの数を表示します。 スタンプがメッセージの方向に基づいて適用される場合、このフィールドにはダッシュ「-」が表示されます。
前回の更新	前回エントリをアップデートした日時を表示します。
ステータス	スタンプの有効/無効を切り替えます。 注意 • スタンプがメッセージの方向に対して有効な場合、指定した方向のメッセージに、Deep Discovery Email Inspector によって自動的にスタンプが挿入されます。 • ポリシールールで使用されていないスタンプのみ無効にすることができます。

メッセージスタンプを設定する

メッセージの方向に基づいて最大 3 つのメッセージスタンプ (受信、送信、受信および送信のメッセージの方向に 1 つずつ) を設定できます。ポリシールールに作成できるスタンプの数に制限はありません。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [スタンプ] の順に選択します。
2. 次のいずれかを実行します。

- [追加] をクリックして新しいスタンプを設定します。
- スタンプ名をクリックして設定を変更します。

3. ステータスオプションを選択して、スタンプを有効または無効にします。

注意

- スタンプがメッセージの方向に対して有効な場合、指定した方向のメッセージに、Deep Discovery Email Inspector によって自動的にスタンプが挿入されます。
- ポリシールールで使用されていないスタンプのみ無効にすることができます。

4. わかりやすい名前を入力します。
5. スタンプを挿入するメッセージの場所を選択します。
6. ポリシールールまたはメッセージの方向に基づいてスタンプを適用するオプションを選択します。

注意

- [ポリシールール] を選択した場合、1 つ以上のポリシールールでスタンプを選択すると、Deep Discovery Email Inspector によって検出されたメッセージにスタンプが挿入されます。
- スタンプがポリシールールで使用されていなければ、[スタンプを編集] 画面でこの設定を変更できます。

7. テキストフィールドにスタンプの内容を入力します。

   書式設定のオプションを使用して、テキストの内容を書式設定できます。[プレーンテキストのプレビュー] フィールドに、テキストの内容が読み取り専用のプレーンテキストで表示されます。

8. [保存] をクリックします。

リダイレクトページ

Deep Discovery Email Inspector では、不審なリンクを開こうとしているユーザに対して、リダイレクトページを使用して操作をブロックするか警告を表示するかをポリシー 処理で決定します。リダイレクトページは独自のロゴ、メッセージ本文、および管理者の連絡先情報でカスタマイズできます。

リダイレクトページをカスタマイズする

組み込みのリダイレクトページを使用する場合は、メッセージ受信者がリダイレクトページを開けることを確認してください。リダイレクトページを開けない場合は、ネットワーク設定を確認するか、外部のリダイレクトページを使用します。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [リダイレクトページ] の順に選択します。
2. 外部のリダイレクトページを使用するか、組み込みのリダイレクトページを使用するかを選択します。
   - 外部のリダイレクトページを使用する: 使用する [ブロックページ] のページ URL を入力します。
   - 組み込みのリダイレクトページを使用する: [警告ページ] と [ブロックページ] のどちらを表示するかを選択します。

     リダイレクトページを編集するには次の手順を実行します。
     - [リンクでホスト名を使用します。ホスト名を設定して、この設定を有効にします。] を選択します。

       ヒント
       この設定を有効にして、ユーザが誤って不正な Web サイトにアクセスしないようにすることをお勧めします。

     - [ホスト名] をクリックすると [システム設定] 画面にリダイレクトされます。[システム設定] > [ネットワーク] にて [ホスト名] を表示または変更できます。

注意

[ポリシー] 画面から移動する前に変更内容を保存してください。

- イメージファイルを参照して選択するには、[イメージを置換します] ( ) アイコンをクリックします。

重要

イメージは 500x60 ピクセル以下で、GIF、JPEG、または PNG 形式である必要があります。

- フィールドを開いて編集するには、[編集] ( ) アイコンをクリックします。
- [管理者の連絡先情報] フィールドを開いて編集するには、[有効] ハイパーリンクをクリックします。

3. [保存] をクリックします。

アーカイブサーバ

アーカイブサーバを設定して、ポリシーに一致するメールメッセージを保存できます。ポリシーに対してメッセージのアーカイブを有効にすると、Deep Discovery Email Inspector は自動的に一致するメッセージのコピーを指定されたアーカイブサーバに送信します。

注意

- 最大 10 台のアーカイブサーバを設定できます。
- メッセージが複数のポリシーに一致し、それぞれのポリシーに異なるアーカイブサーバが設定されている場合、Deep Discovery Email Inspector はメッセージのコピーを各アーカイブサーバに送信します。
- メッセージが複数のポリシーに一致し、それぞれのポリシーに同じアーカイブサーバが設定されている場合、Deep Discovery Email Inspector はメッセージのコピーをそのアーカイブサーバにのみ送信します。

次の表は、[アーカイブサーバ] 画面の各フィールドを示しています。

フィールド	説明
サーバ名	アーカイブサーバのわかりやすい名前を表示します。
メールアドレス	アーカイブサーバのメールアドレスを表示します。
サーバアドレス	アーカイブサーバの IP アドレスまたは完全修飾ドメイン名を表示します。
ポート	アーカイブサーバのポート番号を表示します。
関連するポリシー	このアーカイブサーバを使用するポリシーの数を表示します。
前回の更新	前回エントリをアップデートした日時を表示します。

アーカイブサーバを設定する

最大 10 台のアーカイブサーバを 設定して、ポリシー設定に基づいてメールメッセージを保存できます。

手順

1. [ポリシー] > [ポリシーオブジェクト] の順に選択します。
2. [アーカイブサーバ] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいアーカイブサーバを 設定します。
   - サーバ名をクリックして設定を変更します。
4. 一意のサーバ名を入力します (最大 64 文字)。
5. アーカイブサーバのメールアドレスを 入力ます。
6. SMTP サーバを設定してアーカイブのメッセージを 送信します。次のいずれかのオプションを選択して、必要な設定を行います。
   - サーバアドレスおよびポートの指定: SMTP サーバのアドレスとポートを指定します。

SMTP サーバを設定したら、[接続のテスト] をクリックしてサーバへの接続をテストします。

- MX レコードの検索を使用: MX レコードに基づいて SMTP サーバを検索します。

7. [保存] をクリックします。

アーカイブサーバの 追加後、次の操作を実行できます。

- 設定を編集するには、サーバ名をクリックします。
- サーバを削除するには、エントリを選択して [削除] をクリックします。

注意

アーカイブサーバがポリシーに関連付けられている場合は削除できません。

データ識別子

デジタル資産は、組織が不正な転送から保護する必要のあるファイルおよびデータです。次のデータ識別子を使用して、デジタル資産を定義できます。

注意

コンテンツフィルタルールまたは情報漏えい対策テンプレートで使用しているデータ識別子は削除できません。データ識別子を削除する前に、ルールまたはテンプレートを削除してください。

- パターン: 特定の構造を持つデータ。

  詳細については、144 ページの「パターン」を参照してください。

- ファイル属性: ファイルの種類やサイズなどのファイルのプロパティ。

  詳細については、149 ページの「ファイル属性」を参照してください。

- キーワードリスト: 特別な単語や語句のリスト。

詳細については、153 ページの「キーワードリスト」を参照してください。

パターン

パターンは特定の構造を持つデータです。たとえば、クレジットカード番号の多くは 16 桁の「nnnn-nnnn-nnnn-nnnn」という形式で表現されるため、パターンによる検出に適しています。

事前定義されたパターンやカスタマイズされたパターンをコンテンツフィルタルールおよび情報漏えい対策ルールで使用できます。

詳細については、144 ページの「事前定義されたパターン」および 145 ページの「カスタマイズされたパターン」を参照してください。

事前定義されたパターン

情報漏えい対策には、一連の事前定義されたパターンが用意されています。これらのパターンを変更または削除することはできません。

情報漏えい対策では、パターンマッチングと数学的方程式を使用してこれらのパターンを検証します。機密の可能性のあるデータがパターンに一致すると、そのデータに追加の検証チェックが実行されます。

事前定義されたパターンの完全なリストについては、次の場所にある「情報漏えい対策リスト」を参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

事前定義されたパターンを表示する

注意

事前定義されたパターンを変更または削除することはできません。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [パターン] タブをクリックします。

3. パターン名をクリックします。
4. 表示される画面で設定を確認します。

カスタマイズされたパターン

事前定義されたパターンが企業の要件を満たさない場合は、カスタマイズされたパターンを作成します。

パターンは文字列を一致させるための強力なツールです。パターンを作成する前に、その構文に慣れておいてください。適切に記述されていないパターンは、パフォーマンスに著しい影響を及ぼす可能性があります。

パターンを作成する際は、

- 有効なパターンを定義する方法の指針として、事前定義されたパターンを参照します。たとえば、日付を含むパターンを作成する場合は、「Date」を含む事前定義パターンを参照します。
- 情報漏えい対策は Perl 互換正規表現 (PCRE) で定義されたパターンの形式に従うことに注意してください。PCRE の詳細については、次の Web サイトを参照してください。

  http://www.pcre.org/

- 単純なパターンから始めます。不必要な警告が発生する場合や、検出結果を向上させるために調整する場合は、パターンを修正します。

パターンを作成する際に選択できる条件がいくつかあります。Deep Discovery Email Inspector でコンテンツフィルタルールや情報漏えい対策ポリシールールの対象となるパターンは、この選択された条件を満たしている必要があります。異なる条件のオプションの詳細については、146 ページの「カスタマイズされたパターンの条件」を参照してください。

カスタマイズされたパターンの条件

表 5-6. カスタマイズされたパターンの条件オプション

条件	ルール	例
なし	なし	すべて - 米国国勢調査局の名前 • パターン:[^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
特定の文字	パターンにはユーザの指定した文字を含める必要がある。 また、パターンの文字数は最小文字数と最大文字数の範囲内にある必要がある。	米国 - ABA 銀行ルーティング番号 • パターン:[^\w\\\/\{\.\-=&";]([0123678]\d{8})[^\w-\}+.;&] • 特定の文字:0123456789 • パターンの最小文字数:9 • パターンの最大文字数:9
サフィックス	サフィックスはパターンの最後のセグメントのことで、ユーザの指定した文字と一定の文字数を含める必要がある。 また、パターンの文字数は最小文字数と最大文字数の範囲内にある必要がある。	すべて - 自宅住所 • パターン:\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • サフィックスの文字:0123456789- • サフィックスの文字数:5 • パターンの最小文字数:25 • パターンの最大文字数:80

条件	ルール	例
単一の区切り文字	パターンには文字で区切られた 2 つのセグメントが必要。 また、区切り文字の左側の文字数は最小文字数と最大文字数の範囲内にある必要があり、区切り文字の右側の文字数は最大文字数内にある必要がある。	すべて - メールアドレス • パターン: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • 区切り文字: @ • 左側の最小文字数: 3 • 左側の最大文字数: 15 • 右側の最大文字数: 30

カスタマイズされたパターンを設定する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [パターン] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを作成します。
   - エントリをクリックして設定を変更します。
4. 名前を入力します。名前は 256 文字以下の長さにする必要があり、パイプ文字 (|) を含めることはできません。
5. 説明を 512 文字以内で入力します。
6. 表示データの形式を入力します。
7. 表示データの例を入力します。

   たとえば、ID 番号のパターンを作成している場合は、サンプルの ID 番号を入力します。このデータは参照用としてのみ使用され、製品の他の場所に表示されることはありません。
8. 次のいずれかの条件を選択し、選択した条件に追加の設定を行います (146 ページの「カスタマイズされたパターンの条件」を参照)。

- なし
- 特定の文字
- サフィックス
- 単一の区切り文字

9. 実際のデータでパターンをテストします。

   たとえば、国民 ID 用のパターンの場合は、[テスト用データ] に有効な ID 番号を入力して [テスト] をクリックし、結果を確認します。

10. 結果に間違いがなければ、[保存] をクリックします。

注意

テストが成功した場合にのみ設定を保存してください。データを検出できないパターンはシステムリソースを浪費し、パフォーマンスに影響を及ぼす可能性があります。

パターンをインポートする

このオプションは、パターンを含む適切な形式の XML ファイルがある場合に使用してください。現在アクセスしている Deep Discovery Email Inspector アプライアンスまたは別の Deep Discovery Email Inspector アプライアンスのどちらからでも、パターンをエクスポートすることでファイルを生成できます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [パターン] タブをクリックします。
3. [インポート] をクリックし、パターンを含む XML ファイルを指定します。
4. [開く] をクリックします。

パターンをインポートすることにより、Deep Discovery Email Inspector の既存のカスタマイズされたパターンが上書きされるというメッセージが表示されます。

5. インポート処理を開始するには、[インポート] をクリックします。

パターンをエクスポートする

エクスポート機能を使用して、パターンのすべてまたは選択した部分を XML ファイルにバックアップできます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [パターン] タブをクリックします。
3. 次のいずれかを実行します。
   - 1 つ以上のエントリを選択して [エクスポート] をクリックし、選択したエントリを含む XML ファイルをダウンロードします。
   - すべてのエントリを含む XML ファイルをダウンロードするには、[すべてエクスポート] をクリックします。

ファイル属性

ファイル属性はファイル独自のプロパティです。データ識別子を定義するときに、ファイルタイプとファイルサイズという 2 つのファイル属性を使用できます。たとえば、ソフトウェア開発会社では、会社のソフトウェアインストーラの共有を、ソフトウェアの開発とテストを担当している開発部門に制限しなければならない場合があります。この場合は、Deep Discovery Email Inspector 管理者はポリシーを作成して、サイズが 10～40MB の実行可能ファイルが開発以外の部門に転送されるのをブロックできます。

ファイル属性自体は、機密ファイルの識別子に適しているとは言えません。このトピックの例では、他の部門で共有されているサードパーティ製ソフトウェアがブロックされる可能性があります。そのため、ファイル属性と他の情報漏えい対策データ識別子を組み合わせて、機密ファイルの検出対象を絞り込むことをお勧めします。

サポートされるファイルタイプの全リストについては、こちらを参照してください。

事前定義されたファイル属性リスト

情報漏えい対策には、事前定義されたファイル属性リストが用意されています。このリストを変更または削除することはできません。このリストには、テンプレートがポリシー違反をトリガするかどうかを判断する独自の条件が組み込まれています。

ファイル属性を設定する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [ファイル属性] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを作成します。
   - エントリをクリックして設定を変更します。
4. 名前を入力します。名前は 256 文字以下の長さにする必要があり、パイプ文字 (|) を含めることはできません。
5. 説明を 512 文字以内で入力します。
6. 添付ファイルの種類の一致オプションを選択します。
   - 選択した添付ファイルの種類:選択した種類の添付ファイルを含むメッセージに対して処理を実行します。
   - 選択した添付ファイルの種類以外:選択した種類以外の添付ファイルを含むメッセージに対して処理を実行します。

注意

添付ファイルが、選択したいずれかのオプションに一致するファイルの種類を含むアーカイブファイルである場合も、メッセージに対して処理を実行します。

7. 目的の実際のファイルタイプを選択します。
8. 含めるファイルタイプがリストにない場合は、[カスタムファイル拡張子]を選択して、ファイルタイプの拡張子を入力します。指定した拡張子のファイルがチェックされますが、その実際のファイルタイプはチェックされません。ファイルの拡張子を指定する際は、次のガイドラインを参照してください。
   - 各拡張子の先頭にはアスタリスク (*) とピリオド (.) を付け、その後に拡張子を指定する必要があります。アスタリスクはワイルドカードであり、ファイルの実際の名前を表しています。たとえば、*.pol は 12345.pol や test.pol と一致します。
   - 拡張子にワイルドカードを含めることができます。1 文字のデータを表す場合は疑問符 (?) を使用し、複数の文字を表す場合はアスタリスク (*) を使用します。次の例を参照してください。

     - *.*m は、ABC.dem、ABC.prm、ABC.sdcm などのファイルと一致します。

     - *.m*r は、ABC.mgdr、ABC.mtp2r、ABC.mdmr などのファイルと一致します。

     - *.fm?は、ABC.fme、ABC.fml、ABC.fmp などのファイルと一致します。
   - 拡張子の末尾にアスタリスクを追加すると、ファイル名や関係のない拡張子の一部と一致する可能性があるので注意してください。例:*.do*は、abc.doctor_john.jpg や abc.donor12.pdf と一致します。
9. ファイルの最小および最大サイズを入力し、単位を選択します。サイズは両方ともゼロより大きな整数にする必要があります。

注意

ファイルサイズの一致を無効にするには、フィールドに「0」を入力してください。

10. [保存]をクリックします。

ファイル属性をインポートする

このオプションは、ファイル属性を含む適切な形式の XML ファイルがある場合に使用してください。現在アクセスしている Deep Discovery Email Inspector アプライアンスまたは別の Deep Discovery Email Inspector アプライアンスのどちらからでも、ファイル属性をエクスポートすることでファイルを生成できます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [ファイル属性] タブをクリックします。
3. [インポート] をクリックし、ファイル属性を含む XML ファイルを指定します。
4. [開く] をクリックします。

   ファイル属性をインポートすることにより、Deep Discovery Email Inspector の既存のカスタマイズされたファイル属性が上書きされるというメッセージが表示されます。
5. インポート処理を開始するには、[インポート] をクリックします。

ファイル属性をエクスポートする

エクスポート機能を使用して、ファイル属性のすべてまたは選択した部分を XML ファイルにバックアップできます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [ファイル属性] タブをクリックします。
3. 次のいずれかを実行します。
   - 1 つ以上のエントリを選択して [エクスポート] をクリックし、選択したエントリを含む XML ファイルをダウンロードします。

- すべてのエントリを含む XML ファイルをダウンロードするには、[すべてエクスポート] をクリックします。

キーワードリスト

キーワードは特殊な単語または語句です。関連するキーワードをキーワードリストに追加して、特定の種類のデータを識別できます。たとえば、「予後」、「血液型」、「ワクチン」、「医師」などは、診断書に記載される可能性のあるキーワードです。診断書ファイルが送信されないようにするには、これらのキーワードをコンテンツフィルタルールや 情報漏えい対策ルールで使用し、これらのキーワードを含むファイルをブロックするように Deep Discovery Email Inspector を設定できます。

一般的に使用される単語を組み合わせて、意味のあるキーワードを作成できます。たとえば、「end」、「read」、「if」、および「at」を組み合わせて、「END-IF」、「END-READ」、および「AT END」のようなソースコードに含まれるキーワードを形成できます。

事前定義されたキーワードリストを使用することも、カスタマイズされたキーワードリストを使用することもできます。詳細については、153 ページの「事前定義済みのキーワードリスト」および 153 ページの「カスタマイズされたキーワードリスト」を参照してください。

事前定義済みのキーワードリスト

情報漏えい対策では、あらかじめトレンドマイクロで定義したキーワードリストが用意されています。これらのキーワードリストは、変更や削除ができません。リストにはそれぞれ固有の条件が組み込まれており、テンプレートに照らしてポリシー違反と見なすかどうかを判別します。

情報漏えい対策の事前定義済みキーワードリストの詳細については、こちらを参照してください。

カスタマイズされたキーワードリスト

事前定義されたキーワードリストが要件を満たさない場合は、カスタマイズされたキーワードリストを作成します。

キーワードリストを設定する際に選択できる条件がいくつかあります。情報漏えい対策でポリシーの対象となるキーワードリストは、この選択された条

件を満たしている必要があります。各キーワードリストに次のいずれかの条件を選択します。

- 任意のキーワード
- すべてのキーワード
- <x>文字以内のすべてのキーワード
- 合計スコアがしきい値を超えるキーワード

条件のルールの詳細については、154 ページの「カスタマイズされたキーワードリストの条件」を参照してください。

カスタマイズされたキーワードリストの条件

表 5-7. キーワードリストの条件

条件	ルール
任意のキーワード	キーワードリストの 1 つ以上のキーワードをファイルに含める必要があります。
すべてのキーワード	キーワードリストのすべてのキーワードをファイルに含める必要があります。

条件	ルール
<x>文字以内のすべてのキーワード	キーワードリストのすべてのキーワードをファイルに含める必要があります。さらに、各キーワードのペアは互いに <X> 文字以内である必要があります。 たとえば、キーワードが WEB、DISK、および USB の 3 つで、指定した文字数が 20 であるとします。 本製品ですべてのキーワードを DISK、WEB、USB の順に検出した場合、DISK の「D」から WEB の「W」、「W」から USB の「U」、および「D」から「U」の文字数は 20 文字以下である必要があります。 次のデータがこの条件に一致します。 DISK####WEB#########USB 次のデータはこの条件に一致しません。 DISK####WEB############USB (「D」と「U」の間が 23 文字) DISK******************WEB****USB (「D」と「W」の間が 23 文字) 文字数を決定する際、10 などの小さな数は通常、検索時間の短縮につながるのですが、対象範囲が比較的狭くなることに注意してください。これにより、特に大きなファイルでは、機密データを検出する可能性が低下する場合があります。数字が大きくなるにつれて、対象範囲も広がりますが、検索時間が長くなる可能性があります。
合計スコアがしきい値を超えるキーワード	キーワードリストの 1 つ以上のキーワードをファイルに含める必要があります。キーワードが 1 つだけ検出された場合は、そのスコアがしきい値を超える必要があります。キーワードが複数ある場合は、その合計スコアがしきい値を超える必要があります。 各キーワードに、1〜10 のスコアを割り当てます。機密性の高い単語や語句、たとえば総務部で「昇給」などは、比較的高いスコアにします。単独ではあまり重要性が高くない単語や語句のスコアは低くしてもかまいません。 しきい値を考える場合は、キーワードに割り当てるスコアを考慮します。たとえば、キーワードが 5 つあり、そのうち 3 つの優先度が高い場合、しきい値は優先度の高い 3 つのキーワードの合計スコア以下にすることができます。これは、この 3 つのキーワードさえ検出されれば、そのファイルは脆弱だと十分に判断できるということです。

キーワードリストを設定する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [キーワードリスト] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを作成します。
   - エントリをクリックして設定を変更します。
4. 名前を入力します。名前は 256 文字以下の長さにする必要があり、パイプ文字 (|) を含めることはできません。
5. 説明を 512 文字以内で入力します。
6. 次の条件のいずれかを選択して、その条件に合わせて追加の設定値を指定します。
   - 任意のキーワード
   - すべてのキーワード
   - <x> 文字以下のすべてのキーワード
   - キーワードの合計スコアがしきい値を超過
7. キーワードを手動でリストに追加するには
   a. 3 バイト～40 文字のキーワードを入力して、大文字と小文字を区別するかどうかを指定します。

      たとえば、2 つの全角文字をキーワードとして指定できます。

   b. [追加] をクリックします。
8. キーワードを削除するには、そのキーワードを選択して、[削除] をクリックします。
9. [保存]をクリックします。

キーワードリストをインポートする

このオプションは、キーワードリストを含む適切な形式の XML ファイルがある場合に使用してください。現在アクセスしている Deep Discovery Email Inspector アプライアンスまたは別の Deep Discovery Email Inspector アプライアンスのどちらからでも、キーワードリストをエクスポートすることでファイルを生成できます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [キーワードリスト] タブをクリックします。
3. [インポート] をクリックし、キーワードリストを含む XML ファイルを指定します。
4. [開く] をクリックします。

   キーワードリストをインポートすることにより、Deep Discovery Email Inspector の既存のカスタマイズされたキーワードリストが上書きされるというメッセージが表示されます。
5. インポート処理を開始するには、[インポート] をクリックします。

キーワードリストをエクスポートする

エクスポート機能を使用して、キーワードリストのすべてまたは選択した部分を XML ファイルにバックアップできます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [データ識別子] の順に選択します。
2. [キーワードリスト] タブをクリックします。
3. 次のいずれかを実行します。
   - 1 つ以上のエントリを選択して [エクスポート] をクリックし、選択したエントリを含む XML ファイルをダウンロードします。

- すべてのエントリを含む XML ファイルをダウンロードするには、[すべてエクスポート] をクリックします。

情報漏えい対策テンプレート

情報漏えい対策テンプレートは、情報漏えい対策データ識別子と、条件文を形成する論理演算子 (および、または、除外) で構成されます。特定の条件文を満たすファイルやデータのみが情報漏えい対策ポリシーの対象となります。

たとえば、ファイルが「雇用契約」ポリシーの対象となるには、Microsoft Word ファイルであること (ファイル属性)、および特定の法律用語を含むこと (キーワード)、および ID 番号を含むこと (パターン) が必要です。このポリシーにより人事担当者は、そのファイルをドメイン内の受信者に送信することができます。同じファイルをドメイン外の受信者に送信することはブロックされます。

データ識別子を設定すれば、独自のテンプレートを作成できます。

事前定義されたテンプレートを使用することもできます。詳細については、159 ページの「カスタマイズした情報漏えい対策テンプレート」および 158 ページの「事前定義済みの情報漏えい対策テンプレート」を参照してください。

注意

情報漏えい対策ポリシーで使用されているテンプレートを削除することはできません。削除する前に、ポリシーからテンプレートを削除してください。

事前定義済みの情報漏えい対策テンプレート

情報漏えい対策には、次のように、さまざまな規制基準に準拠するために使用可能な事前定義済みのテンプレートが付属しています。これらのテンプレートは、変更や削除ができません。

- GLBA:Gramm-Leach-Billey Act
- HIPAA:Health Insurance Portability and Accountability Act (医療保険の相互運用性と説明責任に関する法律)

- PCI-DSS:Payment Card Industry Data Security Standard (PCI-DSS: カード会員データや取引情報を保護することを目的に作成されたクレジット業界のセキュリティ基準)
- SB-1386:US Senate Bill 1386
- US PII:United States Personally Identifiable Information (米国で個人を特定できる情報)

すべての事前定義済みのテンプレートの目的の一覧、および保護されるデータの例については、次の情報漏えい対策に関する Web サイトをご確認ください。http://tmqa.jp/dlp_list

カスタマイズした情報漏えい対策テンプレート

データ識別子の定義が完了したら、独自のテンプレートを作成します。テンプレートは、データ識別子と、条件文を形成する論理演算子 (And、Or、Except) で構成されます。

条件文と論理演算子の働きと例については、159 ページの「条件文と論理演算子」を参照してください。

条件文と論理演算子

情報漏えい対策は左から右に条件文を評価します。条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。

次の表の例を参照してください。

表 5-8. サンプル条件文

条件文	説明と例
[データ識別子 1] および [データ識別子 2] 除外 [データ識別子 3]	ファイルは、[データ識別子 1] と [データ識別子 2] の条件を満たすが、[データ識別子 3] の条件を満たしていない必要があります。 次に例を示します。 ファイルは、[Adobe PDF 文書] であり、[メールアドレス] を含むが、[キーワードリスト内のすべてのキーワード] を含まない必要があります。

条件文	説明と例
[データ識別子 1] または [データ識別子 2]	ファイルは [データ識別子 1] または [データ識別子 2] の条件を満たす必要があります。 例: ファイルは、[Adobe PDF 文書] であるか、[Microsoft Word ドキュメント] である必要があります。
除外 [データ識別子 1]	ファイルは [データ識別子 1] の条件を満たしていない必要があります。 例: ファイルは [マルチメディアファイル] 以外である必要があります。

表の最後の例で示したように、ファイルが条件文内のいずれのデータ識別子の条件も満たさないことが必要な場合は、条件文内の最初のデータ識別子に「除外」演算子を使用できます。ただし、ほとんどの場合、最初のデータ識別子に演算子は使用しません。

情報漏えい対策テンプレートを作成する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [情報漏えい対策テンプレート] の順に選択します。
2. 次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを作成します。
   - エントリをクリックして設定を変更します。
3. 名前を入力します。名前は 256 文字以下の長さにする必要があり、パイプ文字 (|) を含めることはできません。
4. 説明を 512 文字以内で入力します。
5. [条件文] で次の操作を実行して、条件文を作成します。
   a. 論理演算子を選択します。

注意

条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。正しい使用例については、159 ページの「条件文と論理演算子」を参照してください。

b. データ識別子の種類を選択します。

c. データ識別子を選択します。

ヒント

データ識別子を検索するには、データ識別子の名前全体または一部を入力します。

d. パターンの発生件数を指定します。

e. さらに条件を追加するには、追加アイコン () をクリックします。

文から条件を削除するには、削除アイコン () をクリックします。

f. [追加] をクリックして、条件文を [テンプレート定義] 表に追加します。

6. [テンプレート定義] で、各定義の論理演算子を選択します。

注意

条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。正しい使用例については、159 ページの「条件文と論理演算子」を参照してください。

7. テンプレートから定義を削除するには、ごみ箱アイコンをクリックします。

8. [保存]をクリックします。

情報漏えい対策テンプレートをインポートする

このオプションは、情報漏えい対策テンプレートを含む適切な形式の XML ファイルがある場合に使用してください。現在アクセスしている Deep Discovery Email Inspector アプライアンスまたは別の Deep Discovery Email Inspector アプライアンスのどちらからでも、情報漏えい対策テンプレートをエクスポートすることでファイルを生成できます。

注意

情報漏えい対策テンプレートをインポートすると、Deep Discovery Email Inspector の既存のカスタマイズされた情報漏えい対策テンプレートが上書きされます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [情報漏えい対策テンプレート] の順に選択します。
2. [インポート] をクリックし、情報漏えい対策テンプレートおよび関連付けられたデータ識別子を含む XML ファイルを指定します。
3. [開く] をクリックします。

   確認画面が表示されます。
4. インポート処理を開始するには、[インポート] をクリックします。

情報漏えい対策テンプレートをエクスポートする

エクスポート機能を使用して、情報漏えい対策テンプレートのすべてまたは選択した部分を XML ファイルにバックアップできます。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [情報漏えい対策テンプレート] の順に選択します。
2. 次のいずれかを実行します。

- 1 つ以上のエントリを選択して [エクスポート] をクリックし、選択した情報漏えい対策テンプレートおよび関連付けられたデータ識別子を含む XML ファイルをダウンロードします。
- [すべてエクスポート] をクリックし、すべての情報漏えい対策テンプレートおよびデータ識別子 (データ識別子が情報漏えい対策テンプレートで使用されていない場合でも) を含む XML ファイルをダウンロードします。

アドレスグループ

アドレスグループとは、組織内の複数のユーザのメールアドレスの集合です。ポリシーを作成して各アドレスに個別にポリシールールを適用する代わりに、アドレスグループを作成して、複数のメールアドレスに同時にポリシールールを適用できます。

ポリシーを設定する前に、メールアドレスを個別に追加するかテキストファイルからインポートすることでアドレスグループを作成します。

複数の Deep Discovery Email Inspector アプライアンスで同じアドレスグループを使用するには、元になる Deep Discovery Email Inspector アプライアンスからアドレスグループをエクスポートし、そのテキストファイルをインポート先の Deep Discovery Email Inspector アプライアンスでインポートします。

次の表は、[アドレスグループ] 画面で実行できるタスクを示しています。

タスク	説明
アドレスグループの追加	[追加] をクリックしてアドレスグループを設定します。 詳細については、164 ページの「アドレスグループを設定する」を参照してください。
アドレスグループの編集	アドレスグループ名をクリックして設定を変更します。 詳細については、164 ページの「アドレスグループを設定する」を参照してください。

タスク	説明
アドレスグループのエクスポート	アドレスグループを選択し、[エクスポート] をクリックして、選択したアドレスグループをテキストファイルにダウンロードします。 注意 一度にエクスポートできるアドレスグループは 1 つのみです。
アドレスグループの削除	アドレスグループを 1 つ以上選択して、[削除] をクリックします。

次の表は、[アドレスグループ] 画面の詳細を示しています。

フィールド	説明
名前	アドレスグループの名前を表示します。
説明	アドレスグループの説明を表示します。
アドレス件数	アドレスグループ内のメールアドレスの数を表示します。
関連するポリシー	このアドレスグループを使用するポリシーの数を表示します。
最終更新日	アドレスグループをアップデートした日時を表示します。

アドレスグループを設定する

手順

1. [ポリシー] > [ポリシーオブジェクト] の順に選択します。
2. [アドレスグループ] タブをクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいアドレスグループを設定します。
   - 名前をクリックして、設定を変更します。

4. 名前を入力します。
5. アドレスグループの説明を入力します。
6. 次のいずれかを実行します。
   - 個別にメールアドレスを追加する:

     メールアドレスを入力して [追加] をクリックします。

     
     注意
     メールアドレスにはワイルドカード文字 (*) を使用できます。たとえば、「*@example.com」のように入力します。

   - メールアドレスのリストをインポートする:

     
     注意
     Deep Discovery Email Inspector では、メールアドレスをテキストファイルからインポートできます。テキストファイルで、1 行に 1 つのメールアドレスのみが記載されていることを確認します。オプションで、ワイルドカード文字 (*) を使用してメールアドレスを指定できます。たとえば、「*@example.com」のように入力します。

     a. [インポート] をクリックします。
     b. メールアドレスのリストを含むテキストファイルを選択します。
     c. [OK] をクリックします。

   新しいエントリがアドレスリストに表示されます。
7. [追加] または [保存] をクリックします。

ポリシー除外

ポリシー除外により、誤検出が減少します。除外を設定し、メールの暗号化に制限と処理を設定するか、特定のメールメッセージを「安全」として分類します。安全な送信者、受信者、および X-Header コンテンツを指定し、ファ

イル、URL、IP アドレスとドメイン、および URL キーワードを追加するか、グレーメール検索をバイパスする送信者を指定します。安全なメールメッセージはそれ以上調査されず、BCC モードおよび SPAN/TAP モードでは破棄され、MTA モードでは受信者に配信されます。

メッセージの除外を設定する

Deep Discovery Email Inspector では、除外リストに指定された送信者、受信者、または X-Header のメッセージは安全と見なされ、ポリシールールが適用されません。ただし、送信者フィルタ設定と送信者の認証設定は引き続き適用されます。

手順

1. [ポリシー] > [除外] > [メッセージ]の順に選択します。
2. メールメッセージの除外基準を指定します。
   - 送信者
   - 受信者
   - X-Header

   注意

   Deep Discovery Email Inspector では、X-Header の除外について大文字/小文字区別をしません。

   Deep Discovery Email Inspector では、ドメイン全体を指定するためのワイルドカードとしてのアスタリスク (*) 文字をサポートします。たとえば、ドメイン `example.com` の [送信者] の除外を作成するには、次のように入力します。

   ```
   *@example.com
   ```
3. [保存] をクリックします。

オブジェクトの除外を管理する

次のいずれかのタスクを実行して、オブジェクトの除外を管理します。

手順

- 検索フィルタを指定して、表示を制御したり、現在の除外を表示したりします。

  次の表は、[ソース] フィルタオプションを 示しています。

オプション	説明
すべて	すべてのオブジェクトの除外を表示します。
ローカル	Deep Discovery Email Inspector に手動で追加されたオブジェクトの除外を表示します。
Web サービス	HTTP Web サービスを介してインポートされたオブジェクトの除外を表示します。
Deep Discovery Director	Deep Discovery Director と同期されたオブジェクトの除外を表示します。

注意

Deep Discovery Email Inspector が Deep Discovery Director 5.0 以降に登録されている場合、Deep Discovery Email Inspector はオブジェクトの除外を Deep Discovery Director と同期し、Apex Central の既存のオブジェクトの除外を上書きします。

- 安全と見なすオブジェクトを変更します。

  次の表は、オブジェクトの除外に対する処理を示しています。

処理	説明
 追加	除外リストに新しいオブジェクトを追加します。オプションで、オブジェクトの除外についての備考を入力します。 詳細については、168 ページの「オブジェクトの除外を追加する」を参照してください。

処理	説明
インポート	インポートする CSV ファイルを選択します。 各行の形式を次に示します。 <type>,<object>,[source],[notes] • <type> の値: IP address、Domain、URL、Files • <object> の値: IP アドレス、ドメイン、URL、または SHA-1 ハッシュ値 • (オプション) [source] の値: "local" • (オプション) [notes]: 任意の形式の追加情報 有効な CSV の例: • Links,www.example.com,local,顧客はこの Web サイトを参照できる • IP address,10.10.10.10,,人事部のアドレス • Files,3395856CE81F2B7382DEE72602F798B642F14140,local,CA 証明書の SHA-1 • Domain,example.com,,追加 詳細については、170 ページの「オブジェクトの除外をインポートする」を参照してください。
削除	選択したオブジェクトを削除します。
すべて削除	すべてのオブジェクトを削除します。
エクスポート	選択したオブジェクトをエクスポートします。
すべてエクスポート	除外リスト全体を CSV ファイルにエクスポートします。

オブジェクトの除外を追加する

Deep Discovery Email Inspector では、安全なファイル、URL、IP アドレス、およびドメインのみが含まれるメールメッセージは調査されずにシステムを通過します。メールメッセージに 1 つの安全な URL と 1 つの未知の URL が

含まれる場合は、未知の URL が調査されます。仮想アナライザも、サンドボックス分析で安全なファイルと URL を無視します。

手順

1. [ポリシー] > [除外] > [オブジェクト] の順に選択します。
2. [追加] をクリックします。
3. ファイル、URL、IP アドレス、またはドメインの除外条件を指定します。
   - ファイルの場合は、タイプに [ファイル] を選択して SHA-1 ハッシュ値を指定します。

     注意

     Threat Connect は環境内で検出された不審オブジェクトや Trend Micro Smart Protection Network の脅威データと相関して、関連する実行可能なインテリジェンスを提供します。
   - URL の場合は、タイプに [URL] を選択して Web アドレスを指定します。

     注意

     完全な URL を入力するか、サブドメインにワイルドカード (*) を使用します。
   - IP アドレスの場合は、タイプに [IP アドレス] を選択して Web アドレスを指定します。
   - ドメインの場合は、タイプに [ドメイン] を選択して Web アドレスを指定します。
4. (オプション) 備考を入力します。
5. (オプション) 複数のファイル、URL、IP アドレス、またはドメインの除外条件を同時に指定するには、[さらに追加] をクリックします。
   a. ファイル、URL、IP アドレス、またはドメインの除外条件を指定します。

b. [リストに追加] をクリックします。条件がオブジェクトリストに追加されます。

6. [保存] をクリックします。

オブジェクトの除外の追加後、次の操作を実行できます。

- 選択したエントリを削除するには、[削除] をクリックします。
- リストのすべてのエントリを削除するには、[すべて削除] をクリックします。
- 選択したエントリを CSV ファイルでダウンロードするには、[エクスポート] をクリックします。
- リストを CSV ファイルでダウンロードするには、[すべてエクスポート] をクリックします。

オブジェクトの除外をインポートする

正しく書式設定された CSV ファイルから例外をインポートできます。

手順

1. [ポリシー] > [除外] > [オブジェクト] の順に選択します。
2. [インポート] をクリックします。
3. 次のいずれかを実行します。
   - 初めて例外をインポートする場合は、[サンプル CSV のダウンロード] をクリックし、CSV ファイルを保存してオブジェクトを入力 (CSV ファイル内の指示を参照) した後、その CSV ファイルを参照して選択します。
   - 以前に除外リストをインポートしたことがある場合は、CSV ファイルの別のコピーを保存し、そのファイルに新しいオブジェクトを入力した後、その CSV ファイルを参照して選択します。
4. [インポート] をクリックします。

インポートされた例外がインポート元の [Web サービス] とともにリストに表示されます。

URL キーワードの除外を設定する

指定したいずれかのキーワードを含む URL はワンクリック URL と見なされ、Deep Discovery Email Inspector からアクセスされません。

注意

- 検出されたワンクリック URL は Web レピュテーションサービスによって検索されます。Deep Discovery Email Inspector は、これらの URL を分析のために仮想アナライザに送信しません。
- URL は [オブジェクト] タブで除外リストに追加できます。

  詳細については、168 ページの「オブジェクトの除外を追加する」を参照してください。

手順

1. [ポリシー] > [除外] > [URL キーワード] の順に選択します。
2. URL キーワードを指定します。

   注意

   - URL キーワードでは大文字小文字は区別されません。
   - 1 行に 1 つのキーワードを指定します。
3. [保存] をクリックします。

グレーメールの除外

グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールです。Deep Discovery Email Inspector では、ポリシールールに基づいて、マーケティングメッセージ、ニュースレター、およびソーシャルネットワークの通知をグレーメールとして検出できます。

グレーメールの除外リストの IP アドレスまたはサブネットからのメールメッセージは、Deep Discovery Email Inspector のグレーメール検索をバイパスします。

グレーメールの除外を追加する

Deep Discovery Email Inspector では、グレーメールの除外リストに追加した IP アドレスおよびサブネットからのメールメッセージについてグレーメール検索がバイパスされます。

手順

1. [ポリシー] > [除外] > [グレーメールの除外] の順に選択します。
2. [追加] をクリックします。

   [グレーメールの除外の追加] 画面が表示されます。
3. IPv4/IPv6 アドレスまたはサブネットを入力します。
4. 除外の説明を入力します。
5. (オプション) エントリをさらに追加するには、[さらに追加] をクリックして次の操作を実行します。

   リストからエントリを削除するには、[処理] 列のアイコン ( ) をクリックします。
6. [保存] をクリックします。

   グレーメールの除外の追加後、次の操作を実行できます。

   - リストのすべてのエントリを削除するには、[すべて削除] をクリックします。
   - リストを CSV ファイルでダウンロードするには、[すべてエクスポート] をクリックします。
   - 1 つ以上のエントリを削除するには、エントリを選択して [削除] をクリックします。
   - 1 つ以上のエントリを CSV ファイルにエクスポートするには、エントリを選択して [エクスポート] をクリックします。

グレーメール除外リストをインポートする

正しく書式設定された CSV ファイルからグレーメールの除外をインポートできます。

手順

1. [ポリシー] > [除外] > [グレーメールの除外] の順に選択します。
2. [アップロード] をクリックします。

   ファイルの選択画面が表示されます。
3. CSV ファイルを選択します。
4. [開く] をクリックして CSV ファイルをインポートします。

   グレーメールの除外のインポート後、次の操作を実行できます。

   - リストのすべてのエントリを削除するには、[すべて削除] をクリックします。
   - リストを CSV ファイルでダウンロードするには、[すべてエクスポート] をクリックします。

Email Encryption の除外を設定する

Deep Discovery Email Inspector では、[Email Encryption の除外] 画面に指定したしきい値または条件を満たすメッセージを暗号化または復号しません。

注意

日本語版では Email Encryption 機能をご利用いただけません。

手順

1. [ポリシー] > [除外] > [Email Encryption の除外] の順に選択します。
2. [検索条件] で、Deep Discovery Email Inspector が処理する暗号化または復号されたメッセージの制限を設定します。

フィールド	説明
暗号化メッセージの最大サイズ	暗号化メッセージの最大サイズを指定します。 注意 この設定は、受信メッセージと送信メッセージの両方に適用されます。メッセージがしきい値の上限に達すると、Deep Discovery Email Inspector は指定された処理をメッセージに適用します。
復号メッセージの最大サイズ	復号メッセージの最大サイズを指定します。 注意 この設定は、受信メッセージと送信メッセージの両方に適用されます。メッセージがしきい値の上限に達すると、Deep Discovery Email Inspector は指定された処理をメッセージに適用します。
最大受信者数	メッセージの最大受信者数を指定します。 注意 この設定は、受信メッセージと送信メッセージの両方に適用されます。メッセージがしきい値の上限に達すると、Deep Discovery Email Inspector は指定された処理をメッセージに適用します。
送信メッセージの暗号化失敗	Deep Discovery Email Inspector で暗号化できない送信メッセージに対して、[処理] に指定された処理を適用する場合は、このオプションを選択します。

フィールド	説明
送信メッセージの復号失敗	Deep Discovery Email Inspector で復号できない送信メッセージに対して、[処理] に指定された処理を適用する場合は、このオプションを選択します。

3. [処理] で、指定したしきい値に達したメッセージ、および Deep Discovery Email Inspector で暗号化または復号できない送信メッセージに適用する処理を設定します。

フィールド	説明
処理	メッセージに適用する次のいずれかの処理を選択します。 • [メッセージの削除]: メールキューからメールメッセージを削除します。 • [ブロックして隔離]: 隔離領域に複製を保存します。 • [放置およびタグ付け]: 設定されている場合、配信前にメールメッセージの件名にタグ付けして X-Header を挿入します。
件名タグ	[放置およびタグ付け] 処理を選択した場合、メッセージの件名に挿入する文字列を指定します。
X-Header	[放置およびタグ付け] 処理を選択した場合、X-Header に追加するテキストを指定します。

4. [保存] をクリックします。

第 6 章

アラートとレポート

この章の内容は次のとおりです。

アラート

アラートは、Deep Discovery Email Inspector の状態をただちに知らせる機能です。アラートは次の 3 つのカテゴリに分類されます。

- 重大なアラート。ただちに対応が必要なイベントで実行されます。
- 重要なアラート。監視が必要なイベントで実行されます。
- 情報アラート。限定的な監視が必要な (無害である可能性が高い) イベントで実行されます。

各アラートを実行するしきい値を設定できます。

注意

各アラート通知で使用できるメッセージトークンについては、507 ページの「アラート通知のメッセージトークン」を参照してください。

重大なアラート

次の表は、ただちに注意が必要なイベントによって実行される重大なアラートについて説明しています。Deep Discovery Email Inspector では、サンドボックスの機能不全、サービスの停止、リレー MTA の到達不能、およびライセンスの期限切れは重大な問題と見なされます。

表 6-1. 重大なアラート

名前	条件 (初期設定)	チェック間隔 (初期設定)
Virtual Analyzer Stopped	仮想アナライザが回復できない  注意 このアラートはローカルの仮想アナライザを使用している場合のみ使用できます。	即時
Service Stopped	サービスが停止し、再起動できない	即時

名前	条件 (初期設定)	チェック間隔 (初期設定)
Relay MTAs Unreachable	ドメインのすべてのリレー MTA に到達できない	5 分ごとに 1 回
License Expiration	ライセンス有効期限がもうすぐ切れるまたは切れている	即時

重要なアラート

次の表は、監視が必要なイベントによって実行される重要なアラートについて説明しています。Deep Discovery Email Inspector では、トラフィックの急増、不審メッセージの検出、ハードウェア容量の変化、特定のサンドボックスキューの活動、およびコンポーネントの更新における問題は重要なイベントと見なされます。

表 6-2. 重要なアラート

名前	条件 (初期設定)	チェック間隔 (初期設定)
Suspicious Messages Identified	1 件以上のメッセージで脅威が検出された	5 分ごとに 1 回
Watchlisted Recipients at Risk	脅威が検出された 1 件以上のメッセージがウォッチリストの受信者に送信された	5 分ごとに 1 回
Quarantined Messages with Detected Threats	10 件以上のメッセージが隔離された	30 分ごとに 1 回
Long Message Delivery Queue	500 件以上のメッセージが配信キューにある	5 分ごとに 1 回
High CPU Usage	CPU 使用率が 90%以上	5 分ごとに 1 回
Long Virtual Analyzer Submission Queue	仮想アナライザへのサブミッション用のキュー内で 20 件以上のメッセージが 5 分待機している	即時

名前	条件 (初期設定)	チェック間隔 (初期設定)
Long Virtual Analyzer Processing Time	仮想アナライザの平均処理時間が 15 分を超えている	1 時間ごとに 1 回
Low Free Disk Space	ディスク容量が 5GB 以下	30 分ごとに 1 回
Component Update/Rollback Unsuccessful	アップデート/ロールバックが失敗した	即時
Email Messages Timed Out Without Analysis Results	1 件以上のメールメッセージが分析結果なしでタイムアウトした	5 分ごとに 1 回
Email Message Encryption/ Decryption Unsuccessful	1 件以上のメッセージで暗号化または復号が失敗した	5 分ごとに 1 回
Low Free Threat Quarantine Disk Space	脅威が検出されたメッセージを保存するために残された隔離ディスク空き容量が 10%以下	30 分ごとに 1 回
High Memory Usage	メモリ使用率が 90%以上	5 分ごとに 1 回
Long Message Deferred Queue	100 件以上のメッセージが遅延キューにある	5 分ごとに 1 回
Low Free Spam Quarantine Disk Space	スパムメールメッセージを保存するために残された隔離ディスク空き容量が 10% 以下	30 分ごとに 1 回
Account Locked	1 つ以上のアカウントがロックされている	即時
Unsuccessful DKIM Signing	5 件以上のメッセージで DKIM 署名が失敗した	5 分ごとに 1 回
Connection Issue	必要なリソースへの接続を確立できない	30 分ごとに 1 回

情報アラート

次の表は、限定的な監視が必要なイベントによって実行されるアラートについて説明しています。検出、処理、およびアップデート完了の急増は、ほとんどが無害のイベントです。

表 6-3. 情報アラート

名前	条件 (初期設定)	チェック間隔 (初期設定)
Threat Detection Surge	10 件以上のメッセージが検出された	1 時間ごとに 1 回
Processing Surge	20,000 件以上のメッセージが処理された	1 時間ごとに 1 回
Component Update/Rollback Successful	アップデート/ロールバックが正常に完了した	即時
Data Loss Prevention Incident	10 件以上のメッセージが情報漏えい対策ルールに違反した	1 時間ごとに 1 回

アラート通知を設定する

すべての重要なアラートに、通知の受信者を 1 つ以上追加します。

注意

SMTP サーバを設定して通知を送信します。詳細については、419 ページの「通知 SMTP サーバを設定する」を参照してください。

手順

1. [アラート/レポート] > [アラート] > [ルール]の順に選択します。
2. [ルール] 列のアラート名をクリックします。

   アラートルールの設定画面が表示されます。
3. アラートパラメータの設定を行います。

詳細については、183 ページの「アラート通知パラメータ」を参照してください。

4. [保存] をクリックします。
5. [戻る] をクリックすると [アラートルール] 画面に戻ります。

実行されたアラートを表示する

手順

1. [アラート/レポート] > [アラート] > [実行されたアラート] の順に選択します。
2. 検索条件を指定します。
   - レベル
   - 種類
   - ルール名
   - 期間
3. アラートの詳細を表示します。

ヘッダ	説明
実行日時	アラートが発生した日付と時刻
レベル	アラートの重要性。Critical、Important、または Informational のいずれか
ルール	アラートルールの名前
基準	アラートを実行するアラートルールの条件
件数	実行されたアラートの発生数または発生期間。数字をクリックすると関連するログエントリが表示されます。
通知の受信者	最新のアラート通知の受信者
通知の件名	最新のアラート通知の件名

アラートを管理する

次のいずれかのタスクを実行して、アラートを管理します。

手順

- 検索フィルタを指定して、表示を制御したり、現在の除外を表示したりします。
- 実行されたアラートを確認して、エクスポートまたは削除します。

オプション	説明
削除	選択したアラートを削除します。
すべてエクスポート	最大 50,000 件のアラートを CSV ファイルにエクスポートします。

アラート通知パラメータ

アラートルールが実行された場合、カスタムメールメッセージを使用して受信者に通知できます。一部のアラートには、メッセージ件数やチェック間隔、リスクレベルなどのパラメータを追加できます。

重大なアラートのパラメータ

注意

各アラートで使用できるメッセージトークンについては、507 ページの「アラート通知のメッセージトークン」を参照してください。

表 6-4. Virtual Analyzer Stopped

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。

パラメータ	説明
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeviceIP% • %DeviceName%

表 6-5. Service Stopped

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeviceIP% • %DeviceName% • %ServiceName%

表 6-6. Relay MTAs Unreachable

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeviceName% • %DeviceIP% • %MessageList% • %MTAList%

表 6-7. License Expiration

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DaysBeforeExpirationATD% • %DaysBeforeExpirationSEG% • %DeviceName% • %DeviceIP% • %ExpirationDateATD% • %ExpirationDateSEG% • %LicenseStatusATD% • %LicenseStatusSEG% • %LicenseTypeATD% • %LicenseTypeSEG%

重要なアラートのパラメータ

注意

各アラートで使用できるメッセージトークンについては、507 ページの「アラート通知のメッセージトークン」を参照してください。

表 6-8. Suspicious Messages Identified

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
メールメッセージ	アラートを実行するメールメッセージのしきい値を指定します。
リスクレベル	アラートを実行するリスクレベルを選択します。

パラメータ	説明
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeviceIP% • %DeviceName% • %MessageList%

表 6-9. Watchlisted Recipients at Risk

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
受信者のウォッチリスト	ウォッチリストに受信者を追加します。ウォッチリストの受信者が不審または不正なメールメッセージを受信すると、アラートが実行されます。
メールメッセージ	アラートを実行するメールメッセージのしきい値を指定します。
リスクレベル	アラートを実行するリスクレベルを選択します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeviceIP% • %DeviceName% • %MessageList%

表 6-10. Quarantined Messages with Detected Threats

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
隔離されたメッセージ	アラートを実行する隔離されたメッセージのしきい値を指定します。
リスクレベル	アラートを実行するリスクレベルを選択します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	メッセージをカスタマイズするには、次のトークンを使用します。 • %MessageList% • %DateTime% • %DeviceName% • %DeviceIP% • %ConsoleURL%

表 6-11. Long Message Delivery Queue

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
メールメッセージ	アラートを実行するメールメッセージのしきい値を指定します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeliveryQueue% • %DeviceIP% • %DeviceName% • %QueueThreshold%

表 6-12. High CPU Usage

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
平均 CPU 使用率	アラートを実行する平均 CPU 使用率のしきい値を指定します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。

パラメータ	説明
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %CPUThreshold% • %CPUUsage% • %DateTime% • %DeviceIP% • %DeviceName%

表 6-13. Long Virtual Analyzer Submission Queue

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
サブミッション	アラートを実行するメールメッセージのしきい値を選択します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
平均待ち時間	送信キューに過去 1 時間以内に入ったサンプルがアラートを送信するまでの、平均待ち時間のしきい値を選択します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DeviceIP% • %DeviceName% • %DateTime% • %SandboxQueue% • %SandboxQueueThreshold%

表 6-14. Long Virtual Analyzer Processing Time

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
平均処理時間	アラートを実行するしきい値として、過去 1 時間にサンドボックスキュー内のサンプルの処理に要した平均時間を選択します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %AveSandboxProc% • %DateTime% • %DeviceIP% • %DeviceName% • %SandboxProcThreshold%

表 6-15. Low Free Disk Space

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
ディスク空き容量	アラートを実行する最小ディスク容量のしきい値を GB 単位で指定します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeviceIP% • %DeviceName% • %DiskSpace%

表 6-16. Component Update/Rollback Unsuccessful

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %ComponentList% • %DateTime% • %DeviceIP% • %DeviceName%

表 6-17. Email Messages Timed Out Without Analysis Results

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
メールメッセージ	アラートを実行するメールメッセージのしきい値を指定します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %MessageList% • %DateTime% • %DeviceName% • %DeviceIP% • %ConsoleURL%

表 6-18. Email Message Encryption/Decryption Unsuccessful

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
メールメッセージ	アラートを実行するメールメッセージのしきい値を指定します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %MessageList% • %DateTime% • %DeviceName% • %DeviceIP% • %ConsoleURL%

表 6-19. Low Free Threat Quarantine Disk Space

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
脅威隔離ディスク空き容量	アラートを実行する最小ディスク容量のしきい値を指定します。 注意 [脅威隔離ディスク空き容量] とは、脅威が検出されたメッセージを保存する、ディスクパーティションに 残っている空き容量の割合のことです。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %DiskSpace% • %DateTime% • %DeviceName% • %DeviceIP% • %ConsoleURL%

表 6-20. High Memory Usage

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。

パラメータ	説明
平均メモリ使用率	アラートを実行する平均メモリ使用率のしきい値を選択します。 注意 [ディスク空き容量] とは、ディスクパーティションに残っている空き容量のことです。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %MemoryThreshold% • %MemoryUsage% • %DateTime% • %DeviceIP% • %DeviceName% • %ConsoleURL%

表 6-21. Long Message Deferred Queue

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
遅延メッセージ	アラートを実行するメールメッセージのしきい値を指定します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。

パラメータ	説明
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeferredQueue% • %DeviceIP% • %DeviceName% • %QueueThreshold%

表 6-22. Low Free Spam Quarantine Disk Space

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
スパム隔離ディスク空き容量	アラートを実行する最小ディスク容量のしきい値を指定します。 注意 [スパム隔離ディスク空き容量] とは、スパムメールメッセージを保存する、ディスクパーティションに 残っている空き容量の割合のことです。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %DiskSpace% • %DateTime% • %DeviceName% • %DeviceIP% • %ConsoleURL%

表 6-23. Account Locked

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %Account% • %DeviceName% • %DeviceIP% • %DateTime% • %ConsoleURL%

表 6-24. Unsuccessful DKIM Signing

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。

パラメータ	説明
メールメッセージ	アラートを実行するメールメッセージのしきい値を指定します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %TotalMessages% • %Interval% • %DateTime% • %DeviceName% • %DeviceIP% • %ConsoleURL%

表 6-25. Connection Issue

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
監視対象サービス	監視するサービスを 1 つ以上選択します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ServiceList% • %DateTime% • %DiagnosisTip% • %DeviceName% • %DeviceIP% • %ConsoleURL%

情報アラートのパラメータ

注意

各アラートで使用できるメッセージトークンについては、507 ページの「アラート通知のメッセージトークン」を参照してください。

表 6-26. Threat Detection Surge

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
検出されたメッセージ	アラートを実行する検出しきい値を選択します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DetectionCount% • %DetectionThreshold% • %DeviceIP% • %DeviceName% • %Interval%

表 6-27. Processing Surge

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
処理されたメッセージ	アラートを実行するメールメッセージのしきい値です。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。

パラメータ	説明
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %DateTime% • %DeviceIP% • %DeviceName% • %Interval% • %ProcessingCount% • %ProcessingThreshold%

表 6-28. Component Update/Rollback Successful

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %ConsoleURL% • %ComponentList% • %DateTime% • %DeviceIP% • %DeviceName%

表 6-29. Data Loss Prevention Incident

パラメータ	説明
ステータス	アラートを有効または無効にするオプションを選択します。
アラートレベル	メールメッセージにアラートレベルを表示します。
検出されたメッセージ	アラートを実行する検出しきい値を選択します。
監視する情報漏えい対策テンプレート	リスト表示オプションと、監視する情報漏えい対策テンプレートを 1 つ以上選択します。
アラートの実行間隔	Deep Discovery Email Inspector がアラートルール条件を確認する時間間隔を表示します。
受信者	実行されたアラートのメールメッセージを受信する受信者を指定します。
件名	実行されたアラートのメールメッセージの件名を指定します。
メッセージ	実行されたアラートのメールメッセージの本文を指定します。 メッセージをカスタマイズするには、次のトークンを使用します。 • %DetectionCount% • %DetectionThreshold% • %Interval% • %MessageList% • %DateTime% • %DeviceIP% • %DeviceName% • %ConsoleURL%

レポート

Deep Discovery Email Inspector では、脅威の緩和やシステム設定の最適化に役立つレポートが提供されます。レポートは、手動または日次、週次、ある

いは月次のスケジュールで生成されます。各レポートのコンテンツは、柔軟な指定が可能です。

レポートは PDF 形式で生成されます。

レポートを予約する

予約レポートは、設定したスケジュールに従って自動的に生成されます。

注意

SMTP サーバを設定して通知を送信します。詳細については、419 ページの「通知 SMTP サーバを設定する」を参照してください。

手順

1. [アラート/レポート] > [レポート] > [スケジュール]の順に選択します。
2. 関連付けられた間隔を選択して、予約レポートを有効にします。
   - 日次レポートの作成
   - 週次レポートの作成
   - 月次レポートの作成
3. レポートを生成するタイミングを指定します。

注意

29 日、30 日、または 31 日に月次レポートを生成するように設定すると、これらの日付がない月では、その月の最後の日にレポートが生成されます。たとえば、31 を選択した場合、2 月のレポートは 28 日 (または 29 日) に、4 月、6 月、9 月、および 11 月は 30 日に生成されます。

4. 受信者を指定します。

注意

複数の受信者を指定する場合は、セミコロンで区切って入力します。

5. (オプション)分析中に見つかったリスクの高いメッセージ、アラート、および不審オブジェクトのリストを含めるには、[詳細情報を含める] をオンにします。
6. [保存] をクリックします。

手動レポートを生成する

手順

1. [アラート/レポート] > [レポート] > [手動] の順に選択します。
2. レポートを設定します。

オプション	説明
期間	レポート生成の範囲と開始時間を選択します。
詳細情報を含める	(オプション)分析中に見つかったリスクの高いメッセージ、アラート、および不審オブジェクトのリストを含めるには、[詳細情報を含める]をオンにします。
受信者	受信者を指定します。複数の受信者を指定する場合は、セミコロンで区切って入力します。

3. [生成] をクリックします。

   レポートが生成され、次の処理が実行されます。

   - レポートが [アラート/レポート] > [レポート] > [生成されたレポート] に表示されます。
   - レポート通知が受信者に送信されます。

第 7 章

ログ

この章の内容は次のとおりです。

時間ベースのフィルタと DST

時間ベースのフィルタを使用してログにクエリを実行すると、クエリでは、選択された時間範囲が現在の夏時間 (DST) ステータスに基づいているものと仮定されます。たとえば、DST によって時間が午前 2 時から午前 1 時に変わり、DST 後に 0100-0159 でクエリを実行すると、クエリは変更後の新しい 0100-0159 のログに一致します。ローカル時間が一致する場合でも、DST より前の時間と一致するログは表示されません。

メールメッセージの追跡

ブロックされたメッセージや配信されたメッセージなど、Deep Discovery Email Inspector を通過したメールメッセージを追跡します。Deep Discovery Email Inspector は送信者、受信者、および実施されたポリシー処理などのメッセージの詳細をログに記録します。

メッセージの追跡ログは、メールメッセージが Deep Discovery Email Inspector によって受信または送信されたかどうかを示します。メッセージの追跡ログは、Deep Discovery Email Inspector がメールメッセージを調査している証拠にもなります。

メッセージ追跡ログのクエリを実行する

手順

1. [ログ] > [メッセージ追跡]の順に選択します。
2. 検索条件を指定します。

注意

ワイルドカードはサポートされません。Deep Discovery Email Inspector ではファジィ論理を使用して検索結果を照会します。

フィルタ	説明
期間	事前に定義した時間範囲を選択するか、カスタム範囲を指定します。

フィルタ	説明
受信者	受信者のメールアドレスを指定します。アドレスは 1 つのみ指定できます。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを指定します。
送信者	送信者のメールアドレスを指定します。
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを指定します。
件名	メールメッセージの件名を指定します。
方向	メッセージの方向を指定します。
メッセージ ID	一意のメッセージ ID を指定します。 例: `20160603021433.F0304120A7A@example.com`
送信元 IP	メールの送信者に最も近い MTA の IP アドレスを指定します。送信元 IP は、攻撃元、感染 MTA、またはメールリレー機能を持つボットネットの IP アドレスです。 感染 MTA は通常、攻撃者が使用するサードパーティのオープンメールリレーで、不正なメールメッセージやスパムメールを検出せずに送信します。
リスクレベル	[すべて] またはメールメッセージのリスクレベルを選択します。
TLS (アップストリーム)	受信 SMTP トラフィックの TLS バージョンを選択します。
TLS (ダウンストリーム)	送信 SMTP トラフィックの TLS バージョンを選択します。

フィルタ	説明
最新のステータス	次のいずれかのチェックボックスをオンにします。 • 削除: コンテンツフィルタや脅威対策ルールに基づいて、または [隔離] から削除されたメッセージです。 • 配信/処理完了: 配信されたメッセージです。BCC モードおよび SPAN/TAP モードでは、このステータスのメールメッセージは破棄されます。 • 配信失敗: 配信できなかったメッセージです。BCC モードおよび SPAN/TAP モードでは、メールメッセージは配信されません。 • 受信者変更済み: 受信者が変更されたメッセージです。 • 隔離: Deep Discovery Email Inspector のポリシーに従って隔離されたメッセージです。BCC モードおよび SPAN/TAP モードでは、メールメッセージは隔離されません。 • 配信のためにキューに配置: 配信を保留しているメッセージです。BCC モードおよび SPAN/TAP モードでは、このステータスのメールメッセージはキューに入れられ破棄されます。 • サンドボックス分析のためにキューに配置: 分析を保留しているメッセージです。

3. [クエリ] をクリックします。

   検索条件に一致するログが表に表示されます。クエリ結果には、メッセージ ID、受信者、送信者、件名、リスクレベル、最新のステータス、および受信時のタイムスタンプが含まれます。

   注意

   検索条件をクリアするには、[フィルタをクリア] をクリックします。

4. 結果を表示します。

   • 行の横にあるアイコンをクリックして、メールメッセージの詳細情報を表示します。

フィールド	説明
メッセージの詳細	次の情報が表示されます。 • 送信元 IP: メールメッセージの送信者に最も近い MTA の IP アドレスを表示します。 例: `123.123.123.123.` • 送信者 IP アドレス: 送信者 IP アドレスを表示します。 • 方向: SMTP トラフィックの方向を表示します。 • TLS (アップストリーム): 受信 SMTP トラフィックの TLS バージョンを表示します。 • TLS (ダウンストリーム): 送信 SMTP トラフィックの TLS バージョンを表示します。

処理履歴	メールメッセージがどのように処理されたかを表示します。処理には次のものがあります。
	• 処理を「放置」に設定:
	  • メールメッセージに [放置] ポリシー処理が適用されました。
	  • ユーザによってメールメッセージのコピーが配信されました。これは [添付ファイルの削除、ブロックページへのリンクのリダイレクト、およびタグ付け] と [添付ファイルの削除、警告ページへのリンクのリダイレクト、およびタグ付け] のポリシーが元のメールメッセージに適用されている場合にのみ適用されます。
	• 削除: コンテンツフィルタや脅威対策ルールに基づいて、または [隔離] からメールメッセージが削除されました。
	• 配信済み: メールメッセージが配信されました。
	• 未分析: 指定された理由により仮想アナライザで分析を完了できませんでした。
	• 処理完了: 分析が完了し、メールメッセージが破棄されました。これは、BCC モードおよび SPAN/TAP モードの最終ステータスです。

フィールド	説明
	• 隔離 (理由): メールメッセージが Deep Discovery Email Inspector のポリシーに従って隔離されました。BCC モードおよび SPAN/TAP モードでは、メールメッセージは隔離されません。 • 配信のためにキューに配置: メールメッセージの配信が保留されています。BCC モードおよび SPAN/TAP モードでは、このステータスのメールメッセージはキューに入れられ破棄されます。 • 受信: メールメッセージが Deep Discovery Email Inspector によって受信されました。 • 受信者変更済み: メールメッセージの受信者が変更されました。 • 分析のために送信: メールメッセージが分析のため仮想アナライザに送信されました。 • 削除: メールメッセージから添付ファイルが削除され、配信処理が開始されました。
処理	次のいずれかを実行します。 隔離されたメッセージ: • [隔離] を表示 • 隔離から解除 • 検出されたメッセージで表示 隔離されていないメッセージ (高/中/低のリスクレベル): [検出されたメッセージ] を表示 リスクが検出されなかったメッセージ: [処理] リンクなし

注意

表示される時刻がローカル時間であっても、ログの並べ替えには UTC 0 時間が使用されます。

5. 追加の処理を実行します。
   - [エクスポート] をクリックして、クエリ結果を CSV ファイルに保存します。

     注意

     クエリ結果の最初の 50,000 件のエントリのみが CSV ファイルに出力されます。
   - 画面の最下部にあるパネルには、オブジェクトの合計数が表示されます。すべてのオブジェクトを同時に表示できない場合は、ページ区切りコントロールを使用して、ビューに表示されていないオブジェクトを表示します。

MTA イベント

ネットワーク上の Postfix と SMTP の活動について、接続の詳細を参照できます。

注意

Deep Discovery Email Inspector では、それぞれ 51200KB のログファイルが合計 100 件に達すると自動的にログが削除されます。最新 10 件のログに対してクエリを実行できます。

MTA イベントログのクエリを実行する

手順

1. [ログ] > [MTA] の順に選択します。
2. ログのクエリを実行する時間範囲を指定します。
3. [クエリ] をクリックします。

   時間の条件に合致するすべてのログが表に表示されます。
4. 結果を表示します。

フィールド	説明
タイムスタンプ	イベントが発生した日付と時刻
説明	ログイベントの説明

注意

表示される時刻がローカル時間であっても、ログの並べ替えには UTC 0 時間が使用されます。

5. 追加の処理を実行します。
   - [CSV 形式でエクスポート] をクリックして、クエリ結果を CSV ファイルに保存します。
   - 画面の最下部にあるパネルには、オブジェクトの合計数が表示されます。すべてのオブジェクトを同時に表示できない場合は、ページ区切りコントロールを使用して、ビューに表示されていないオブジェクトを表示します。

システムイベント

ユーザアクセス、ポリシーの変更、ネットワーク設定の変更、および Deep Discovery Email Inspector 管理コンソールで行われたその他のイベントの詳細を表示します。

Deep Discovery Email Inspector は、次の 3 種類のシステムイベントログを保持します。

- Update (アップデートイベント): すべてのコンポーネントアップデートイベント
- Audit (監査ログ): すべてのユーザアクセスイベント
- EUQ (エンドユーザメール隔離ログ): すべてのエンドユーザメール隔離イベント

注意

- ログは [ストレージの管理] 画面で指定した設定に基づいて削除されます。

  詳細については、448 ページの「ストレージ管理を設定する」を参照してください。

- 使用可能なシステムイベントログのリストについては、561 ページのシステムイベントログを参照してください。

システムイベントログのクエリを実行する

手順

1. [ログ] > [システム]の順に選択します。
2. ログのクエリを実行する時間範囲を指定します。
3. 結果を表示します。

フィールド	説明
タイムスタンプ	イベントが発生した日付と時刻
イベントの種類	Deep Discovery Email Inspector では、次の種類のシステムイベントログが記録されます。 • Update (アップデートイベント) • Audit (監査ログ) • エンドユーザメール隔離ログ
説明	ログイベントの説明

注意

表示される時刻がローカル時間であっても、ログの並べ替えには UTC 0 時間が使用されます。

4. 追加の処理を実行します。
   - 右上にある [表示] ドロップダウンメニューから、結果をフィルタ処理するイベントの種類を選択します。

- [エクスポート] をクリックして、クエリ結果を CSV ファイルに保存します。
- 画面の最下部にあるパネルには、オブジェクトの合計数が表示されます。すべてのオブジェクトを同時に表示できない場合は、ページ区切りコントロールを使用して、ビューに表示されていないオブジェクトを表示します。

メッセージキューのログ

Deep Discovery Email Inspector が受信したメールメッセージは、次のいずれかのメッセージキューに保存されます。

- 受信: 処理と配信を待機するメールメッセージが保存されます。
- アクティブ: 処理が開始されたメールメッセージが保存されます。
- 遅延: 処理後に配信できないメールメッセージが保存されます。

メッセージキューのログを表示して、メッセージがメッセージキューに追加された日時を確認したり、選択したメッセージに処理 (配信、再ルーティング、または削除) を実行したりすることができます。

次の表は、[メッセージキューのログ] 画面の詳細を示しています。

フィールド	説明
受信日時	メッセージを受信した日時を表示します
種類	メッセージキューの種類を表示します
メッセージ ID	メールメッセージの一意の ID を表示します
送信者	送信者のメールアドレスを表示します
受信者	メッセージ受信者のメールアドレスを表示します
件名	メッセージの件名を表示します
サイズ (バイト)	メッセージのサイズをバイト単位で表示します
アーカイブ/MTA サーバ	Deep Discovery Email Inspector がメッセージを送信するアーカイブサーバまたは MTA サーバのアドレスを表示します

フィールド	説明
メッセージの種類	メッセージの種類を表示します
前回の配信ステータス	前回の配信処理の実行ステータスを表示します

メッセージキューのログにクエリを実行する

メッセージキューを検索して、メッセージを配信、再ルーティング、または削除することができます。

手順

1. [ログ] > [メッセージキュー] の順に選択します。
2. 検索条件を指定します。

注意

- 検索条件を指定しない場合は、[メッセージキュー]画面に最大 10,000 件の最新のログエントリが表示されます。
- 検索条件をクリアするには、[フィルタをクリア] をクリックします。

フィルタ	説明
種類	メッセージキューの種類を選択します。
受信者	受信者のメールアドレスを指定します。アドレスは 1 つのみ指定できます。
件名	メールメッセージの件名を指定します。

フィルタ	説明
メッセージの種類	次のいずれかのオプションを選択します。 • すべて: すべての通知とアーカイブメッセージ • システム生成: Deep Discovery Email Inspector から送信した通知とアーカイブメッセージ • 受信: Deep Discovery Email Inspector で受信および検索したメッセージ
送信者	送信者のメールアドレスを指定します。
メッセージ ID	一意のメッセージ ID を指定します。 例: `20160603021433.F0304120A7A@example.com`
アーカイブ/MTA サーバ	アーカイブサーバまたは MTA サーバのアドレスを指定します。

3. [クエリ] をクリックします。

   検索条件に一致するメッセージが表に表示されます。

   次のいずれかの処理をメッセージに対して実行できます。

   - 配信: 選択したメッセージが受信者に配信されます。配信ステータスはログテーブルで確認できます。
   - すべて配信: 遅延メッセージキューのすべてのメッセージが受信者に配信されます。
   - 再ルーティング: 指定する SMTP サーバに選択したメッセージが再ルーティングされます。

     注意

     詳細については、219 ページの「メッセージキュー内のメッセージを再ルーティングする」を参照してください。

   - すべて再ルーティング: 指定する SMTP サーバに遅延キューおよび受信キュー内のすべてのメッセージが再ルーティングされます。

注意

詳細については、219 ページの「メッセージキュー内のメッセージを再ルーティングする」を参照してください。

- 削除: 選択したメッセージが削除されます。
- すべて削除: すべてのメッセージが削除されます。

メッセージキュー内のメッセージを再ルーティングする

注意

メッセージの再ルーティングの設定は、Deep Discovery Email Inspector が MTA モードの場合にのみ有効になります。

[メッセージキューのログ] 画面で、遅延キューおよび受信メッセージキュー内の選択したメッセージまたはすべてのメッセージを、指定した SMTP サーバに再ルーティングできます。

手順

1. [ログ] > [メッセージキュー] の順に選択します。
2. 次のいずれかを実行します。
   - 1 つ以上のエントリを選択して [再ルーティング] をクリックし、選択したメッセージを再ルーティングします。
   - [すべて再ルーティング] を選択し、遅延キューおよび受信キュー内のすべてのメッセージを再ルーティングします。
3. メッセージがアクティブなメッセージキュー 内に存在する場合、ダイアログボックスが表示されます。[OK] をクリックします。
4. 表示される [SMTP サーバの指定] 画面で、メールメッセージの転送先 SMTP サーバの IP アドレスまたは完全修飾ドメイン名とポート番号を指定します。
5. [再ルーティング] をクリックします。

メールのサブミットログ

メッセージサンプルを分析のために Deep Discovery Email Inspector に送信すると、送信結果がログに表示されます。

メールのサブミットログにクエリを実行する

手順

1. [ログ] > [メールのサブミット] の順に選択します。
2. 検索条件を指定します。

フィルタ	説明
リスクレベル	[すべて] またはメールメッセージのリスクレベルを選択します。
期間	事前に定義した時間範囲を選択するか、カスタム範囲を指定します。
メッセージ ID	一意のメッセージ ID を指定します。 例: `20160603021433.F0304120A7A@example.com`
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを指定します。
送信者名	ユーザアカウント名を指定します。
件名	メールメッセージの件名を指定します。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを指定します。
受信者	受信者のメールアドレスを指定します。アドレスは 1 つのみ指定できます。

3. [クエリ] をクリックします。

   検索条件に一致するログが表に表示されます。クエリ結果には、受信時のタイムスタンプ、メッセージ ID、送信者、件名、リスクレベル、詳細な検出情報へのリンク (利用可能な場合)、および分析の完了時間が含まれます。

注意

検索条件をクリアするには、[クリア] をクリックします。

Time-of-Click プロテクションログ

Time-of-Click プロテクションログには、URL の検出と、ユーザのクリック時に Deep Discovery Email Inspector が実行した処理に関する詳細情報が含まれています。

Time-of-Click プロテクションログのクエリを実行する

手順

1. [ログ] > [Time-of-Click プロテクション] の順に選択します。
2. 検索条件を指定します。詳細フィルタを適用するには、221 ページの「詳細フィルタを適用する」を参照してください。

フィルタ	説明
処理	検出された URL に対して実行する処理を選択します。
期間	事前に定義した時間範囲を選択するか、カスタム範囲を指定します。
URL	URL を検索するためのキーワードを指定して、[クエリ] をクリックします。

検索条件に一致するログが表に表示されます。

注意

検索条件をクリアするには、[キャンセル] をクリックします。

詳細フィルタを適用する

基本的なフィルタに加え、詳細フィルタを適用してログのクエリを実行できます。

手順

1. [詳細フィルタ] をクリックします。

   詳細フィルタが表示されます。

2. フィルタする情報を指定します。

フィルタ	説明
メッセージ ID	一意のメッセージ ID を指定します。 例: `20160603021433.F0304120A7A@example.com`
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを指定します。
送信者	送信者のメールアドレスを 1 つ以上指定します。複数入力する場合は、セミコロン (;) で区切ります。
件名	メールメッセージの件名を指定します。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを 1 つ以上指定します。複数入力する場合は、セミコロン (;) で区切ります。
受信者	受信者のメールアドレスを 1 つ以上指定します。複数入力する場合は、セミコロン (;) で区切ります。

3. [クエリ] をクリックします。

第 8 章

管理

この章の内容は次のとおりです。

コンポーネントのアップデート

脅威を調査するために使用する製品コンポーネントをダウンロードおよび配信します。トレンドマイクロでは最新のスピアフィッシング攻撃およびソーシャルエンジニアリング攻撃パターンに対応するためにコンポーネントの新しいバージョンを頻繁に作成しています。

コンポーネント

[コンポーネント] タブには、現在使用中のセキュリティコンポーネントが表示されます。

表 8-1. コンポーネント

コンポーネント	説明
高度な脅威相関パターンファイル	高度な脅威相関パターンファイルには、既知の脅威には関係のないファイル機能のリストが含まれます。
高度な脅威検索エンジン (Deep Discovery、Linux、64 ビット) 高度な脅威検索エンジン (Deep Discovery、Linux、32 ビット)	高度な脅威検索エンジンは、ウイルス、不正プログラム、および Java や Flash などのソフトウェアの脆弱性悪用からシステムを保護します。トレンドマイクロのウイルス検索エンジンと統合されており、シグネチャベースの検出、動作ベースの検出、および積極的なヒューリスティック検出を行います。
スパムメール対策エンジン (Enterprise Linux、32 ビット)	トレンドマイクロのスパムメール対策エンジンは、メールメッセージやメールの添付ファイルに含まれる不正プログラムおよびフィッシングコンテンツを検出します。 スパムメール対策エンジンには、メール添付ファイル (スクリプトファイルや Microsoft Office マクロウェアを含む) に高度な脅威検索を実行して不正プログラムを検出する、メール不正プログラム脅威検索エンジンも含まれています。
スパムメール対策パターンファイル	スパムメール対策パターンファイルは、メールメッセージやメールの添付ファイルに含まれる最新の不正プログラムを検出します。
CI クエリハンドラ (Linux、32 ビット) CI クエリハンドラ (Linux、64 ビット)	CI クエリハンドラは、CI エンジンにより特定された動作を処理して機械学習型検索エンジンにレポートを送信します。

コンポーネント	説明
不正プログラムパターンファイル (Deep Discovery)	不正プログラムパターンファイル (Deep Discovery) には、ウイルスや不正プログラムを検索するための検出ルーチンが含まれます。トレンドマイクロは、新しく識別された脅威の検出ルーチンで不正プログラムパターンファイル (Deep Discovery) を定期的にアップデートします。 Deep Discovery Email Inspector も不正プログラムパターンファイル (Deep Discovery) を使用してマスメール型攻撃を検出し、組織を保護します。
信頼済み証明書情報パターンファイル	信頼済み証明書情報パターンファイルには、PE シグネチャを検証するための信頼済み証明書情報が記載されています。
IntelliTrap 除外パターンファイル	IntelliTrap 除外パターンファイルには、IntelliTrap 機能による検索実行時の誤検出を減らすため、自動実行型の安全な圧縮ファイルの検出ルーチンが含まれます。
IntelliTrap パターンファイル	IntelliTrap パターンファイルには、一般に難読化された不正プログラムやその他の潜在的な脅威として知られる自動実行型圧縮ファイルタイプの検出ルーチンが含まれます。
ネットワークコンテンツ相関パターンファイル	ネットワークコンテンツ相関パターンファイルは、トレンドマイクロによって定義された検出ルールを実装します。
ネットワークコンテンツ検査エンジン (Linux、ユーザモード、64 ビット)	ネットワークコンテンツ検査エンジンは、ネットワーク検索を実行するために使用されます。
ネットワークコンテンツ検査パターンファイル	ネットワークコンテンツ検査パターンファイルは、ネットワーク検索を実行するためにネットワークコンテンツ検査エンジンによって使用されます。
スクリプトアナライザパターンファイル (Deep Discovery)	スクリプトアナライザパターンファイル (Deep Discovery) は、不正コードを識別するために Web ページスクリプトの解析時に使用されます。
スパイウェア/グレーウェアパターンファイル	スパイウェア/グレーウェアパターンファイルは、アドウェアやスパイウェアまたはグレーウェアなど、特定タイプの潜在的に望ましくないファイルおよびプログラムの存在を示すビットとバイトの一意のパターンを特定します。

コンポーネント	説明
仮想アナライザセンサ 仮想アナライザセンサ (Linux)	仮想アナライザセンサは、不正プログラムの実行と検出、および仮想アナライザでの動作の記録に使用されるユーティリティ群です。
仮想アナライザ設定パターンファイル	仮想アナライザ設定パターンファイルには、サポートされる脅威の種類やファイルタイプなど、仮想アナライザの設定情報が含まれます。

アップデート元

Deep Discovery Email Inspector は、初期設定のアップデート元であるトレンドマイクロのアップデートサーバからコンポーネントをダウンロードします。組織内で特別に設定された別のアップデート元からコンポーネントをダウンロードするようにトレンドマイクロを設定できます。組織内で特別に設定された別のアップデート元からコンポーネントをダウンロードするように Deep Discovery Email Inspector を設定できます。

注意

Deep Discovery Email Inspector が Apex Central に登録されている場合は、Apex Central から直接ダウンロードするように Deep Discovery Email Inspector を設定できます。Apex Central サーバをアップデート元として指定する方法の詳細は、「Trend Micro Apex Central 管理者ガイド」を参照してください。

アップデート元を設定する

最新の脅威から環境を保護するために、コンポーネントのアップデートは頻繁に行ってください。初期設定では、コンポーネントはトレンドマイクロのアップデートサーバから自動的にアップデートを受信します。別のアップデート元を設定して、異なるインターネットの場所からアップデートを受け取ることができます。

手順

1. [管理] > [コンポーネントのアップデート] > [ソース] の順に選択します。

2. アップデート元を設定します。

   - トレンドマイクロのアップデートサーバ

     トレンドマイクロのアップデートサーバから最新のコンポーネントを取得します (初期設定)。

   - その他のアップデートサーバ

     異なるアップデート元の場所を指定します。アップデート元の URL は「http://」または「https://」で始まる必要があります。

     例: `http://update.mycompany.com`

     注意

     アップデート元では、UNC パス形式はサポートされません。

3. [保存] をクリックします。

コンポーネントをアップデートする

コンポーネントのアップデートを実行して、アップデートサーバからコンポーネントのアップデートをただちにダウンロードします。アップデート元の詳細については、226 ページの「アップデート元を設定する」を参照してください。

手順

1. [管理] > [コンポーネントのアップデート] > [コンポーネント]の順に選択します。
2. コンポーネントを 1 つ以上選択します。
3. [アップデート] をクリックします。
4. 確認メッセージが表示されたら、[OK] をクリックして続行します。

コンポーネントをロールバックする

コンポーネントをロールバックして、すべてのコンポーネントを以前のバージョンに戻します。直前のバージョンへのロールバックのみ可能です。

手順

1. [管理] > [コンポーネントのアップデート] > [コンポーネント]の順に選択します。
2. コンポーネントを 1 つ以上選択します。
3. [ロールバック] をクリックします。

   コンポーネントが以前のバージョンに戻ります。
4. 確認メッセージが表示されたら、[OK] をクリックして続行します。

コンポーネントのアップデートを予約する

手順

1. [管理] > [コンポーネントのアップデート] > [スケジュール] の順に選択します。

   [スケジュール] タブが表示されます。
2. 予約アップデートを有効にします。
3. アップデートの間隔を選択します。
4. [保存] をクリックします。

製品のアップデート

[製品のアップデート] 画面を使用して、Deep Discovery Email Inspector に HotFix や Patch を適用したり、ファームウェアのアップグレードを実行したりします。

システムアップデート

トレンドマイクロからの製品リリース後に、各種問題への対応、製品パフォーマンスの向上、新機能の追加などの理由でシステムアップデートが配布されます。

表 8-2. システムアップデート

システムアップデート	説明
HotFix	HotFix は、特定の問題を修正するために提供されるプログラムです。サポートセンターにお問い合わせいただいた際に、このプログラムで障害が回避されると判断させていただいた場合、お問い合わせいただいたお客さまに個別に送付させていただくことがあります。 注意 トレンドマイクロが Patch を配布するまで、新しい HotFix には以前の HotFix が含まれる場合があります。
Critical Patch	至急対策の必要がある問題のみを修正する目的で一般公開されるプログラムです。特定の問題を修正するプログラムであるため、基本的に、他の修正は含まれませんが、同時期に発見された問題に対する複数の修正が含まれる場合があります。一般公開時期に応じて、後述の Patch に統合されます。問題発生条件に合致するすべてのお客さまに適用を推奨いたします。

これらを利用できるようになると、ベンダやテクニカルサポートから連絡がある場合があります。新しい Critical Patch、Patch、および Service Pack のリリースについては、次のトレンドマイクロの Web サイトで確認してください。

http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

Patch を管理する

トレンドマイクロでは、報告された既知の問題に対する新しいファームウェアバージョン、または製品に適用するアップグレードを不定期にリリースしています。使用可能なファームウェアバージョンについては、https://appweb.trendmicro.com/ecs/Default.aspx を参照してください。

Patch ファイルは次のいずれかの方法でトレンドマイクロにインストールできます。

- Deep Discovery Email Inspector 管理コンソール

- Deep Discovery Director からの計画配信。詳細については、Deep Discovery Director のドキュメントを参照してください。

手順

1. [管理] > [製品のアップデート] > [HotFix/Patch]の順に選択します。
2. [履歴] で、ソフトウェアのバージョン番号を確認します。
3. 製品の Patch を管理します。
   - トレンドマイクロのサポートで提供される Patch ファイルを参照し、[HotFix/Patch のインストール] で [インストール] をクリックして、Patch をアップロードします。
   - Patch をロールバックするには、[履歴] で [ロールバック] をクリックします。ロールバック後、Deep Discovery Email Inspector ではそれ以前の最新の設定を使用します。たとえば、Patch 3 をロールバックすると、Deep Discovery Email Inspector は Patch 2 の状態に戻ります。

ファームウェアをアップグレードする

トレンドマイクロでは、報告された既知の問題に対する新しいファームウェアバージョン、または製品に適用するアップグレードを不定期にリリースしています。使用可能なファームウェアバージョンについては、https://appweb.trendmicro.com/ecs/Default.aspx を参照してください。

ファームウェアをアップグレードすることで、新しいセキュリティ機能が利用可能になったとき、または機能強化されたときに、Deep Discovery Email Inspector からそれらの機能に確実にアクセスできるようになります。

Deep Discovery Email Inspector でファームウェアをアップグレードするには、次のいずれかの方法を使用します。

- Deep Discovery Email Inspector 管理コンソール
- Deep Discovery Director からの計画配信。詳細については、Deep Discovery Director のドキュメントを参照してください。

注意

続行する前に、すべての管理コンソールタスクを完了していることを確認してください。アップグレードプロセスには時間がかかり、アップグレード内容によっては 1 時間以上かかることがあります。 ピーク時間外の時間帯にアップグレードを開始することをお勧めします。アップデートをインストールすると、Deep Discovery Email Inspector が再起動されます。

手順

1. 設定をバックアップします。

   442 ページの「設定のバックアップと復元」

2. ファームウェアイメージを 入手します。
3. このイメージをコンピュータの任意のフォルダに保存します。
4. [管理] > [製品のアップデート] > [ファームウェア] の順に選択します。
5. [ソフトウェアのバージョン] の横で、ファームウェアのバージョンを確認します。
6. アップグレード用のファームウェアパッケージを 参照します。
7. [インストール] をクリックします。

   ヒント

   コマンドラインインタフェースからインストール 処理の進捗が確認できます。

   インストールが完了すると、Deep Discovery Email Inspector が自動的に再起動され、コマンドラインインタフェースが 表示されます。

8. 次のインストール後の手順を実行します。
   - ブラウザのキャッシュをクリアします。
   - Web コンソールにログオンします。

- プロキシサーバ経由でインターネットに接続する内部仮想アナライザを Deep Discovery Email Inspector で使用している場合は、内部仮想アナライザのプロキシを再設定します。

検索と分析

[検索と分析] 画面を使用して、次の機能を設定します。

- 14 ページの「仮想アナライザ」
- 255 ページの「ファイルのパスワード」
- 259 ページの「Smart Protection」
- 264 ページの「スマートフィードバック」
- 265 ページの「YARA ルール」
- 269 ページの「Time-of-Click URL プロテクション」
- 271 ページの「ビジネスメール詐欺」
- 274 ページの「いとこドメイン」

メール検索

メールメッセージがネットワークに到達すると、Deep Discovery Email Inspector は複数の Trend Micro Smart Protection Network サービスからセキュリティ情報を収集し、メールメッセージのリスクレベルを調査します。

- 添付ファイルの分析

  14 ページの「高度な脅威検索エンジン」を参照してください。

- 埋め込まれたリンク (URL) の分析

  15 ページの「Web レピュテーションサービス」を参照してください。

- ソーシャルエンジニアリング攻撃対策

  11 ページの「ソーシャルエンジニアリング攻撃対策」を参照してください。

- 機械学習型検索

15 ページの「機械学習型検索」を参照してください。

- ビジネスメール詐欺からの保護

271 ページの「ビジネスメール詐欺」を参照してください。

不審なファイル、URL、および特徴についてメールメッセージを検索したら、Deep Discovery Email Inspector は結果を相関分析し、リスクレベルを割り当てて、そのリスクレベルに基づいてすぐにポリシー処理を実行するか、またはファイル、URL、およびメールメッセージのサンプルを 仮想アナライザに送信してさらに分析します。

注意

ファイルのパスワード設定は、Deep Discovery Email Inspector のメール検索機能と仮想アナライザの両方に影響します。

仮想アナライザ

仮想アナライザは、統合製品、管理者、および調査担当者によって SSH 経由で送信されたオブジェクトを管理および分析するための安全な仮想環境です。カスタムサンドボックスイメージにより、ご使用のシステム設定に適した環境でファイル、URL、レジストリエントリ、API コール、およびその他のオブジェクトを監視できます。

仮想アナライザは静的および動的な分析を実行して、次に示すカテゴリオブジェクトの重要な特徴を特定します。

- 反セキュリティおよび自己保存
- 自動起動またはその他のシステムの設定
- ディセプション、ソーシャルエンジニアリング
- ファイルの削除、ダウンロード、共有、または複製
- ハイジャック、リダイレクト、またはデータ窃取
- 不正、不良、または既知の不正プログラムの兆候
- プロセス、サービス、またはメモリオブジェクトの変更
- ルートキット、クローキング

- 不審ネットワークまたは不審メッセージングアクティビティ

分析時、仮想アナライザはコンテキストで特徴を評価し、評価の累計に基づいてオブジェクトのリスクレベルを割り当てます。また、調査で使用可能な分析レポート、不審オブジェクトのリスト、PCAP ファイル、および OpenIOC ファイルも生成します。

仮想アナライザの概要

[概要] 画面は、Deep Discovery Email Inspector が内部または外部どちらの仮想アナライザサンドボックス環境を使用するように設定されているかによって異なります。

Deep Discovery Email Inspector で外部の仮想アナライザを使用している場合は、統合設定を行うことで、[外部統合] 画面から外部の仮想アナライザサンドボックス環境のステータスを確認できます。

Deep Discovery Email Inspector で内部の仮想アナライザを使用している場合は、[ステータス] をクリックして仮想アナライザサンドボックス環境のステータスを確認します。仮想アナライザとサンドボックスイメージのリアルタイムのステータスを確認するには、この表を参照してください。

仮想アナライザのステータス

次の表は、仮想アナライザのステータスを示しています。

表 8-3. 仮想アナライザのステータス

ステータス	説明
初期化しています...	サンドボックス環境を準備しています。
開始しています...	すべてのサンドボックスインスタンスを 起動しています。
停止しています...	すべてのサンドボックスインスタンスを 停止しています。
実行中	サンプルを分析しています。
イメージがありません	イメージが仮想アナライザにアップロードされていません。
インスタンスを変更しています...	1 つ以上のイメージでインスタンス数を増加または減少しています。

ステータス	説明
イメージをアップロードしています...	1 つのイメージをアップロードしています。

[全体のステータス] 表

仮想アナライザの [全体のステータス] の表には、各サンドボックスイメージの割り当てられたインスタンス、ステータス (ビジーまたはアイドル)、および使用率の情報が表示されます。

表 8-4. [全体のステータス] 表の説明

ヘッダ	説明
イメージ	イメージ名です (後から変更できません)。
インスタンス	配置されたサンドボックスインスタンスの数です。
現在のステータス	アイドル状態およびビジー状態のサンドボックスインスタンスの分散状況です。
使用率	現在サンプルを処理中のサンドボックスインスタンス数に基づく全体的な使用率をパーセントで表示します。

仮想アナライザのイメージ

初期設定では、仮想アナライザにイメージは含まれていません。仮想アナライザでサンプルを分析できるようにするには、イメージをアップロードする必要があります。

仮想アナライザでは、Open Virtualization Format Archive (OVA) ファイルがサポートされます。

注意

カスタムイメージをアップロードする前に、含まれているすべてのプラットフォームとアプリケーションに有効なライセンスが確保されていることを確認します。

仮想アナライザにイメージをアップロードする前に、イメージの仮想マシン設定が正しいかどうか、プラットフォームがサポートされているかどうか、

必要なアプリケーションが揃っているかどうか確認するには、Virtual Analyzer Image Preparation Tool を使用します。Virtual Analyzer Image Preparation Tool の詳細については、以下の法人カスタマーサイトからダウンロードできる「Virtual Analyzer Image Preparation Tool ユーザガイド」を参照してください。https://app.trendmicro.co.jp/ecs/login.asp?id_page=12

仮想アナライザイメージの準備

初期設定では、仮想アナライザにイメージは含まれていません。サンプルを分析するには、少なくとも 1 つのイメージを OVA (Open Virtual Appliance) 形式で準備してアップロードする必要があります。

既存の VirtualBox または VMware イメージを使用するか、VirtualBox を使用して新しいイメージを作成できます。詳細については、「Virtual Analyzer Image Preparation Tool ユーザガイド」 (https://appweb.trendmicro.com/ecs/default.aspx) の第 2 章と第 3 章を参照してください。

アップロードする前に、Virtual Analyzer Image Preparation Tool を使用してイメージを検証および設定します。詳細については、「Virtual Analyzer Image Preparation Tool ユーザガイド」の第 4 章を参照してください。

ご使用の製品のハードウェア仕様に応じて、アップロード可能なイメージ数、およびイメージごとに配信可能なインスタンス数が決まります。

仮想アナライザのイメージをアップロードする

仮想アナライザは 1〜30GB の OVA ファイルをサポートします。

注意

イメージが追加または削除された場合、またはインスタンスが変更された場合、仮想アナライザは分析を停止して、すべてのサンプルをキューに保持します。

Deep Discovery Email Inspector が Deep Discovery Director に登録されていれば、イメージの配信を介して Deep Discovery Director から Deep Discovery Email Inspector にイメージをインポートすることもできます。

手順

1. [管理] > [検索/分析] > [仮想アナライザ] > [概要] > [イメージ]の順に選択します。

2. [インポート] をクリックします。

   [イメージのインポート] 画面が表示されます。

3. [イメージ] フィールドに名前を指定します。

4. このイメージのインスタンス数を指定します。

5. OS の種類を選択します。

6. イメージソースを選択して、適切な設定を行います。

   - ローカルまたはネットワークフォルダ

     237 ページの「ローカルまたはネットワークフォルダからイメージをアップロードする」を参照してください。

   - HTTP または FTP サーバ

     238 ページの「HTTP または FTP サーバからイメージをアップロードする」を参照してください。

ローカルまたはネットワークフォルダからイメージをアップロードする

次の手順は、ローカルまたはネットワークフォルダから 仮想アナライザにイメージをアップロードする 方法を示しています。イメージをアップロードする前に、コンピュータと Deep Discovery Email Inspector の接続が確立されていることを確認します。[イメージ] 画面で、管理コンソールの [手順 1] で接続ステータスを確認します。

手順

1. [ローカルまたはネットワークフォルダ] を選択します。

2. 最大 260 文字/バイトでイメージの名前を指定します。

3. [接続] をクリックします。

4. 接続されたら、仮想アナライザイメージアップロードツールを 使用してイメージをアップロードします。

   a. [イメージアップロードツールのダウンロード] をクリックします。

   b. ファイル `VirtualAnalyzerImageImportTool.exe` を開きます。

c. Deep Discovery Email Inspector の管理 IP アドレスを指定します。

注意

Deep Discovery Email Inspector の管理 IP アドレスの設定の詳細については、411 ページの「ネットワークを設定する」を参照してください。

d. [参照] をクリックしてイメージファイルを選択します。

e. [アップロード] をクリックします。

次の場合にアップロードプロセスは停止します。

- デバイスへの接続が中断された場合
- メモリ割り当てが失敗した場合
- Windows のソケット初期化が失敗した場合
- イメージファイルが壊れている場合

5. アップロードが完了するまで待ちます。

注意

アップロード済みのイメージは、アップロード後ただちにサンドボックスインスタンスに配信されます。

HTTP または FTP サーバからイメージをアップロードする

次の手順は、HTTP または FTP サーバから仮想アナライザにイメージをアップロードする方法について示します。イメージの追加の詳細については、236 ページの「仮想アナライザのイメージをアップロードする 」を参照してください。

手順

1. [HTTP または FTP サーバ] を選択します。
2. HTTP または FTP の URL 設定を指定します。

オプション	説明
URL	HTTP または FTP の URL を指定します。 例: `ftp://custom_ftp:1080/tmp/test.ova`
ユーザ名	(オプション)認証が必要な場合にユーザ名を指定します。
パスワード	(オプション)認証が必要な場合にパスワードを指定します。
匿名ログイン	(オプション)ユーザ名とパスワードを無効にして、匿名で認証する場合に選択します。

3. [アップロード] をクリックします。
4. 配信が完了するまで待ちます。

注意

仮想アナライザはインスタンスをただちに配信します。

仮想アナライザのイメージを削除する

手順

1. [管理] > [検索/分析] > [仮想アナライザ] > [概要] > [イメージ]の順に選択します。
2. 左側の列内のボックスを選択して、イメージを選択します。
3. [削除] をクリックします。

   イメージが削除されます。

インスタンスを変更する

手順

1. [管理] > [検索/分析] > [仮想アナライザ] > [概要] > [イメージ]の順に選択します。

2. [変更] をクリックします。

   [インスタンスの変更] 画面が表示されます。

3. イメージに割り当てられたインスタンスを変更します。

4. [保存] をクリックします。

仮想アナライザのネットワークとフィルタを設定する

仮想アナライザキュー内のファイルとメッセージの数を減らすには、仮想アナライザへのサブミッションにフィルタを 設定します。

注意

- 仮想アナライザの設定の反映中は、オブジェクト分析が一時停止します。
- ファイルサブミッションフィルタや URL サブミッションフィルタを 使用して仮想アナライザへサブミットする対象を増やすと、システムのパフォーマンスが低下する可能性があります。

手順

1. [管理] > [検索/分析] > [仮想アナライザ]の順に選択します。
2. [設定] を指定します。

オプション	説明
ネットワーク接続	 注意 このセクションは Deep Discovery Email Inspector が内部仮想アナライザを使用している場合に利用できます。 内部仮想アナライザがプロキシサーバ経由でインターネットに接続するように設定されている場合は、Deep Discovery Email Inspector で設定を復元するかファームウェアをアップデートした後、プロキシを再設定してください。 [ネットワークの種類] ドロップダウンリストで、仮想アナライザからネットワークに接続する方法を選択します。ネットワークタイプの詳細については、243 ページの「仮想アナライザのネットワークの種類」を参照してください。 [カスタムネットワーク] を選択した場合は、[サンドボックスポート] ドロップダウンリストから仮想アナライザのトラフィック専用のポートを選択し、[IPv4 アドレスを設定] をクリックしてネットワーク設定を行います。 内部仮想アナライザからインターネットへの接続にプロキシサーバが必要な場合は、ドロップダウンリストから [専用のプロキシサーバを使用する] を選択して次の情報を入力します。 • サーバアドレス • ポート番号 • プロキシサーバへの接続に認証を使用: 認証が必要な場合は、このチェックボックスをオンにしてユーザ名とパスワードを入力します。

オプション	説明
ファイルサブミッションフィルタ	ファイル: ファイルタイプを選択して次のいずれかの処理を実行します。 • 極めて不審なファイルのみを送信する • 極めて不審なファイルを送信し、すべての選択されたファイルタイプを分析する 誤検出の可能性を減らすには、[ソフトウェア安全性評価サービスで安全が確認されたファイルは分析しない] を選択します。 詳細については、243 ページの「Certified Safe Software Service」を参照してください。
URL サブミッションフィルタ	安全が確認された URL は、初期設定で、仮想アナライザにサブミットする前に URL プレフィルタにサブミットされます。安全な URL を含むメッセージは、件名のキーワードを 1 つ以上追加することで仮想アナライザへのサブミッションからフィルタできます。一致したメッセージに含まれる安全な URL は、URL プレフィルタをバイパスして仮想アナライザに直接送信されます。 キーワード: 件名のキーワードを入力して [追加] をクリックし、キーワードをリストに追加します。 リストからキーワードを削除するには、エントリを選択して [削除] をクリックします。 注意 最大 50 件のキーワードを指定できます。
タイムアウト設定	送信されたオブジェクトがタイムアウトするまで仮想アナライザで待機する時間を選択します。初期設定では、サブミッションのタイムアウトに達すると、仮想アナライザによりキュー内で待機しているサブミットされたオブジェクトが分析なしで送信されます。タイムアウトしたオブジェクトは、その他の検索エンジンからリスクレベルを受け取ります。 タイムアウトしたオブジェクトに処理を実行するよう、ポリシーの脅威対策ルールを設定できます。 詳細については、131 ページの「脅威対策ルールを設定する」を参照してください。

3. [保存] をクリックします。

Certified Safe Software Service

CSSS (Certified Safe Software Service) は、既知の安全なファイルで構成されるトレンドマイクロのクラウドデータベースです。トレンドマイクロのデータセンターに対してクエリが実行されると、送信されたファイルがこのデータベースと照合されます。

CSSS を有効にすると、既知の安全なファイルが仮想アナライザキューに送信されることが防止されます。このプロセスにより、次のことが可能になります。

- 計算時間とリソースの節約
- 誤検出の可能性の低減

ヒント

CSSS は、初期設定で有効になっています。初期設定の値を使用することをお勧めします。

仮想アナライザのネットワークの種類

ファイルや URL の動作をシミュレートする場合、仮想アナライザは自身の分析エンジンを使用してそのオブジェクトの危険度を判別します。また、選択されたネットワークの種類により、送信されたオブジェクトがインターネットに接続できるかどうかが決定されます。

ネットワーク接続を設定した後、[インターネット接続テスト] をクリックして、仮想アナライザをインターネットに接続できることを確認してください。

注意

インターネットにアクセスすると、サンプルが C&C コールバックアドレスやその他の外部リンクにアクセスできるので、分析精度が向上します。

ネットワークの種類	説明
管理ネットワーク	仮想アナライザのトラフィックを管理ポートを介して転送します。 **重要** 管理ネットワークへの接続を有効にすると、ネットワーク内で不正プログラムの蔓延やその他の不正な活動を引き起こす可能性があります。
カスタムインタフェース	仮想アナライザでは、管理ポート以外のポートを使用してインターネットに接続します。 **注意** プロキシ設定、プロキシ認証、および接続制限なしでインターネットに接続されているテスト用ネットワークなど、管理ネットワークから隔離された環境を使用することをお勧めします。
ネットワークアクセスなし	仮想アナライザのトラフィックをサンドボックス環境内で隔離します。環境には外部ネットワークへの接続がありません。 **注意** 仮想アナライザはインターネットに接続せず、自身の分析エンジンに依存します。 分析のために URL が送信されることはありません。

仮想アナライザのファイルサブミッションフィルタ

極めて不審なファイルだけでなく、仮想アナライザは幅広いファイルタイプを検索できます。

次の表は、表示されるファイルのカテゴリ、含まれる完全なファイルタイプ、およびファイル拡張子を示しています。

表 8-5. 仮想アナライザのファイルサブミッションフィルタ

表示されるファイルのカテゴリ	完全なファイルタイプ	ファイル拡張子の例
Adobe Flash Player およびその他のマルチメディア	スケーラブルベクターグラフィックス (SVG) Adobe Shockwave Flash ファイル Apple QuickTime メディア	.svg .swf .mov
HTML	Hypertext Markup Language ファイル Web ページのアーカイブファイル	.htm .html .xht .xhtml .mht .mhtml .shtml
Java	Java Archive (JAR) Java クラスファイル	.jar .class
Office 文書	Microsoft Word ドキュメント Microsoft OLE ドキュメント Microsoft Office Word ドキュメント (Word 2007 以降) Microsoft PowerPoint プレゼンテーション Microsoft Office PowerPoint プレゼンテーション (PowerPoint 2007 以降) Microsoft Excel スプレッドシート Microsoft Office Excel スプレッドシート (Excel 2007 以降) Microsoft Office 2003 XML ファイル Microsoft Word 2003 XML ドキュメント Microsoft Excel 2003 XML スプレッドシート	.doc .dot .docx .dotx .pps .ppsx .ppt .pptx .pub .xla .xls .xlsx

表示されるファイルのカテゴリ	完全なファイルタイプ	ファイル拡張子の例
	Microsoft PowerPoint 2003 XML プレゼンテーション Microsoft Publisher 2016 Hancom Hancell 表計算ファイル Hancom Hangul Word Processor (HWP) ドキュメント Hancom Hangul Word Processor (2014 以降) (HWPX) ドキュメント JustSystems 一太郎ドキュメント JungUm Global ドキュメント Microsoft Outlook アイテム Microsoft シンボリックリンク形式 Microsoft Excel Web クエリファイル カンマ区切り値 (CSV) ファイル **注意** 不審な DDEAuto コマンドを持つ CSV ファイルのみ、分析のために仮想アナライザに送信されます。 OpenDocument フォーマット (ODF)	.xlt .xlm .cell .xml .xlsb .xltx .hwp .hwpx .jtd .gul .msg .slk .iqy .csv .odp .ods .odt
マクロが有効な Office 文書	マクロが有効な Microsoft Office Word ドキュメント (Word 2007 以降) マクロが有効な Microsoft Office PowerPoint プレゼンテーション (PowerPoint 2007 以降) マクロが有効な Microsoft Office Excel スプレッドシート (Excel 2007 以降)	.docm .dotm .potm .ppam .ppsm .pptm .xlam .xlsm

表示されるファイルのカテゴリ	完全なファイルタイプ	ファイル拡張子の例
		.xltm
その他の文書の形式	コンパイル済み HTML (CHM) ヘルプファイル Microsoft Windows Shell Binary Link ショートカット Microsoft リッチテキストフォーマット (RTF) ドキュメント Microsoft OneNote	.chm .lnk .rtf .one
PDF	Adobe Portable Document Format (PDF)	.pdf
スクリプト	Microsoft Windows バッチファイル Microsoft Windows コマンドスクリプトファイル JavaScript ファイル JavaScript エンコードスクリプトファイル HTML アプリケーションファイル Microsoft Windows PowerShell スクリプトファイル Visual Basic エンコードスクリプトファイル Visual Basic スクリプトファイル Microsoft Windows スクリプトファイル インターネットショートカットファイル Linux シェル実行可能ファイル  注意 実際のファイルタイプが.js または.vbs であるプレーンテキストファイルまたは汎用スクリプトファイルのみ、分析のために仮想アナライザに送信されます。	.bat .cmd .js .jse .hta .ps1 .vbe .vbs .wsf .url .sh
Portable Executable (PE)	AMD 64 ビット DLL ファイル Microsoft Windows 16 ビット DLL ファイル	.com .cpl

表示されるファイルのカテゴリ	完全なファイルタイプ	ファイル拡張子の例
	Microsoft Windows 32 ビット DLL ファイル	.crt
	Executable and Linkable Format (ELF) ファイル	.dll
	実行可能ファイル (EXE)	.drv
	AMD 64 ビット EXE ファイル	.elf
	DIET DOS EXE ファイル	.exe
	Microsoft DOS EXE ファイル	.ocx
	IBM OS/2 EXE ファイル	.scr
	LZEXE DOS EXE ファイル	.sys
	MIPS EXE ファイル	
	MSIL ポータブル実行可能ファイル	
	Microsoft Windows 16 ビット EXE ファイル	
	Microsoft Windows 32 ビット EXE ファイル	
	ARJ 圧縮 EXE ファイル	
	ASPACK 1.x 圧縮 32 ビット EXE ファイル	
	ASPACK 2.x 圧縮 32 ビット EXE ファイル	
	GNU UPX 圧縮 EXE ファイル	
	LZH 圧縮 EXE ファイル	
	LZH 圧縮 EXE ファイル、ZipMail 対応	
	MEW 0.5 圧縮 32 ビット EXE ファイル	
	MEW 1.0 圧縮 32 ビット EXE ファイル	
	MEW 1.1 圧縮 32 ビット EXE ファイル	
	PEPACK 圧縮実行可能ファイル	
	PKWARE PKLITE 圧縮 DOS EXE ファイル	
	PETITE 圧縮 32 ビット実行可能ファイル	
	PKZIP 圧縮 EXE ファイル	

表示されるファイルのカテゴリ	完全なファイルタイプ	ファイル拡張子の例
	WWPACK 圧縮実行可能ファイル	

注意

Deep Discovery Email Inspector は、次のタイプのファイルを外部仮想アナライザのみに送信します。

- Linux シェル実行可能ファイル (.sh)
- Executable and Linkable Format (ELF) ファイル

仮想アナライザは、アーカイブファイル内のサポートされるファイルタイプと一致するファイルを検索できます。次の表は、サポートされるアーカイブファイルタイプを示しています。

表 8-6. アーカイブファイルタイプ

実際のファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
7ZIP	7-zip アーカイブ	.7z
ACE	WinAce アーカイブ	.ace
ALZ	ALZip アーカイブ	.alz
AMG	富士通 AMG アーカイブ	.amg
ARJ	ARJ アーカイブ	.arj
BINHEX	BinHex ファイル	.hqx
BZIP2	BZIP2 アーカイブ	.bz2 .bzip2
CAB	Microsoft キャビネットファイル	.cab
CPIO	CPIO アーカイブ	.cpio .cpgz

実際のファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
EGG	ALZip アーカイブ	.egg
GZIP	GNU ZIP アーカイブ	.gzip .gz
ICS	iCalendar ファイル	.ics
LHA	LHARC 圧縮アーカイブ	.lha .lharc
LZH	Lempel-Ziv-Welch (LZW) Compressed Amiga アーカイブ	.lzh
MIME	Multipurpose Internet Mail Extensions (MIME) Base64 ファイル	.eml .email
MSG	Microsoft Outlook アイテム	.msg
RAR	Roshal Archive (RAR) アーカイブ	.rar
SIT	Smith Micro StuffIt アーカイブ	.sit .sitx
TAR	TAR アーカイブ	.tar .tgz
TNEF	Microsoft Outlook トランスポートニュートラルカプセル化形式 (TNEF) ファイル	.tnef .winmail.dat .win.dat
UDF	ユニバーサルディスクフォーマットファイル	.iso
UUCODE	Uuencode ファイル	.uue
VCS	vCalendar ファイル	.vcs
XZ	XZ アーカイブ	.xz
ZIP	PKWARE PKZIP アーカイブ (ZIP)	.zip

次の表は、送信設定にかかわらず、Deep Discovery Email Inspector が自動的に外部の macOS 向けサンドボックスに分析のために送信する Mac ファイルタイプを示しています。これらのファイルは内部仮想アナライザには送信されません。

注意

外部仮想アナライザを使用するように Deep Discovery Email Inspector を設定し、Java ファイルカテゴリを選択すると、Java アーカイブ (`.jar`) とクラス (`.class`) のファイルも外部の macOS 向けサンドボックスに分析のために送信されます。

表 8-7. Mac ファイルタイプ

実際のファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
DMG	Apple ディスクイメージファイル	`.dmg`
PKG	Mac OS X インストールファイル	`.pkg`
Mach-O	Mach オブジェクトファイル	`.o`

外部仮想アナライザを設定する

Deep Discovery Email Inspector と統合して不審オブジェクトを分析するように Deep Discovery Email Inspector を設定できます。

手順

1. [管理] > [検索/分析] > [仮想アナライザ] > [外部統合] の順に選択します。
2. [ソース] ドロップダウンリストから [外部] を選択します。
3. [サーバアドレス] フィールドで、Deep Discovery Analyzer サーバの IP アドレスまたは FQDN を入力します。
4. 組織でプロキシサーバを使用している場合、[システムのプロキシ設定を使用] を選択します。

注意

プロキシサーバの設定の詳細については、417 ページの「プロキシの設定」を参照してください。

5. API キーを入力します。
6. (オプション) [接続のテスト] をクリックしてサーバ設定を確認します。
7. [保存] をクリックします。

メールのサブミット

EML または MSG 形式のメールメッセージのサンプルを Deep Discovery Email Inspector に直接アップロードして分析できます。

ファイルのアップロードプロセスの完了後、メールヘッダ、受信者、一致するポリシーなど、メッセージの概要情報が表示されます。仮想アナライザに送信して分析プロセスが完了したら、メールのサブミットログにクエリを実行して送信結果を表示できます。

注意

- Deep Discovery Email Inspector では、EML および MSG 形式のメッセージサンプルのみがサポートされます。
- 手動で送信するメッセージサンプルに対して、Deep Discovery Email Inspector では次の処理が実行されません。
  - アーカイブサーバへのメッセージのコピーの 送信、または一致するポリシーの指定に基づく検出通知の送信
  - Email Reputation Services (ERS) または送信者フィルタ /認証の設定に基づく内容の分析
  - メッセージ追跡ログの生成
  - 隔離、およびエンドユーザメール隔離のログエントリの生成
  - Syslog サーバ、Apex Central、または Deep Discovery Director へのメール送信ログの送信

    送信したメッセージサンプルで 脅威が検出された場合、Deep Discovery Email Inspector は検出ログを Syslog サーバ、Apex Central、または Deep Discovery Director に送信します。
  - Deep Discovery Email Inspector が MTA モードに設定されている場合のメッセージの配信

メールメッセージのサンプルを手動で送信する

EML または MSG 形式の不審なメールメッセージのサンプルを Deep Discovery Email Inspector に送信して分析できます。

手順

1. [管理] > [検索/分析] > [その他の設定] > [メールのサブミット] の順に選択します。

   [メールのサブミット] 画面が表示されます。
2. 次のいずれかを実行します。

- [選択] をクリックして、アップロードする .eml または .msg ファイルを指定します。
- パネル領域に .eml または .msg ファイルをドラッグアンドドロップします。

管理コンソールの [メッセージの詳細] セクションに次の情報が表示されます。

フィールド	説明
メッセージ ID	一意のメッセージ ID を表示します。
メールヘッダ (From)	メールヘッダの作成者のメールアドレスを表示します。
メールヘッダ (To)	メールヘッダのプライマリ受信者のメールアドレスを表示します。
メールの件名	不審メールメッセージの件名を表示します。
メッセージ本文	メールメッセージの本文 (最大長 4K) を表示します。
ポリシー	一致するポリシーとルールを表示します。 Deep Discovery Email Inspector でのポリシーの一致方法の詳細については、105 ページの「ポリシーの一致」および 108 ページの「ポリシー分割」を参照してください。

3. [送信する] をクリックします。

   [メールのサブミットログ] 画面で送信結果を確認できます。

   詳細については、220 ページの「メールのサブミットログにクエリを実行する」を参照してください。

URL 検索

Deep Discovery Email Inspector の初期設定では、メールメッセージ内の URL を検索し、リスクレベルとレピュテーションスコアに基づいて処理を実行します。

Deep Discovery Email Inspector では、次の機能に対して URL 検索を実行します。

- Web レピュテーションサービス
- Time-of-Click プロテクション
- 不審オブジェクトの一致
- 仮想アナライザでの分析
- URL の除外

アプリケーションの必要に応じて、Deep Discovery Email Inspector の URL 検索を手動で無効にできます。

警告!

URL 検索を無効にすると、不正な URL を検出して分析する Deep Discovery Email Inspector の機能が著しく低下します。

URL 検索を無効にする

アプリケーションの必要に応じて、Deep Discovery Email Inspector の URL 検索を手動で無効にできます。

警告!

URL 検索を無効にすると、不正な URL を検出して分析する Deep Discovery Email Inspector の機能が著しく低下します。

手順

1. [管理] > [検索/分析] > [その他の設定] > [URL 検索] の順に選択します。
2. [URL 検索を無効にする] を選択します。
3. [保存] をクリックします。

ファイルのパスワード

不審ファイルは十分に注意して処理してください。このようなファイルをネットワーク経由で転送する場合は、パスワード保護されたアーカイブファイルやパスワード保護された文書ファイルに追加して開かれないようにするこ

とをお勧めします。Deep Discovery Email Inspector では、ファイルを抽出するためのメールメッセージ内のパスワードをヒューリスティックに検出することもできます。

Deep Discovery Email Inspector はユーザ設定のパスワードを使用して、ファイルを抽出するかパスワード保護された文書を開きます。パフォーマンスを向上させるには、一般的に使用されるパスワードをリストの最上部に配置します。

Deep Discovery Email Inspector でサポートされるパスワード保護されたファイルタイプについては、257 ページの「パスワード保護されたファイルタイプ」を参照してください。

注意

- ファイルのパスワードは、暗号されていないテキストとして製品内部に保存されます。
- Deep Discovery Email Inspector を Deep Discovery Director に登録すると、[ファイルパスワード] 画面では、ファイルパスワードのエクスポートのみを実行できます。Deep Discovery Email Inspector は Deep Discovery Director から自動的にファイルパスワードの設定を同期し、既存のファイルパスワード設定を上書きします。

次の表は、[ファイルのパスワード] 画面で実行できるタスクを示しています。

タスク	説明
分析のタイムアウトの設定	[パスワードアナライザのタイムアウト] に時間 (分数) を入力します。指定した時間内に Deep Discovery Email Inspector がメッセージ内のパスワード保護されたファイルを開いて分析できない場合、そのメッセージは隔離されます。
パスワードの追加	[パスワードの追加] をクリックしてリストにパスワードを追加します。 詳細については、258 ページの「ファイルのパスワードを追加する」を参照してください。

タスク	説明
パスワードのインポート	[パスワードのインポート] をクリックして、選択したファイルからパスワードをインポートします。 詳細については、258 ページの「ファイルのパスワードをインポートする」を参照してください。
すべてのパスワードのエクスポート	[パスワードのエクスポート] をクリックし、すべてのファイルパスワードをエクスポートして、コンピュータにファイルを保存します。

パスワード保護されたファイルタイプ

Deep Discovery Email Inspector は、次のパスワード保護されたアーカイブファイルのタイプをサポートします。

- 7z
- alz
- arj
- egg
- rar
- zip

Deep Discovery Email Inspector は、次のパスワード保護された文書ファイルのタイプをサポートします。

- doc
- docx
- odp
- ods
- odt
- pdf
- ppt

- pptx
- xls
- xlsx

ファイルのパスワードを追加する

最大 100 のパスワードが許容されます。

手順

1. [管理] > [検索/分析] > [その他の設定] > [ファイルパスワード] の順に選択します。
2. [パスワードの追加] をクリックします。
3. ASCII 文字のみを使用してパスワードを入力します。

   注意

   パスワードでは大文字と小文字が区別され、スペースを含めることはできません。

4. (オプション) [パスワードの追加] をクリックして、別のパスワードを入力します。
5. (オプション)パスワードをドラッグアンドドロップして、リストの上または下へ移動します。
6. (オプション)パスワードを削除するには、対応するテキストボックスの [x] アイコンをクリックします。
7. [保存] をクリックします。

ファイルのパスワードをインポートする

Deep Discovery Email Inspector では、最大 100 件のパスワードを追加できます。

手順

1. [管理] > [検索/分析] > [その他の設定] > [ファイルパスワード] の順に選択します。

   [ファイルパスワード] 画面が表示されます。

2. [パスワードのインポート] をクリックします。

   [パスワードのインポート] 画面が表示されます。

3. インポートするファイルを参照して選択します。

   注意

   正しいフォーマットのサンプルファイルを 表示するには、[サンプルファイルのダウンロード] をクリックします。

   選択されたファイル内のエントリを Deep Discovery Email Inspector が確認し、無効または重複するパスワードを検出します。

4. [インポート] をクリックします。

Smart Protection

トレンドマイクロの Smart Protection テクノロジは、ファイルレピュテーションサービスと Web レピュテーションサービスを提供する、次世代のクラウドベースの保護ソリューションです。Web レピュテーションサービスを統合することにより、Deep Discovery Email Inspector では、ユーザがアクセスしようとする Web サイトのレピュテーションデータを取得できます。Deep Discovery Email Inspector は、詐欺サイトや脅威の既知の発信源であることが Smart Protection テクノロジによって確認された URL をログに記録し、レポートを生成するためにログをアップロードします。

Deep Discovery Email Inspector は、Smart Protection ソースに接続して Web レピュテーションデータを取得します。

レピュテーションサービスは、Trend Micro Smart Protection Network と Smart Protection Server によって提供されます。次の表では、2 つのソースを比較します。

表 8-8. Smart Protection ソース

比較基準	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
目的	Smart Protection テクノロジを統合するトレンドマイクロ製品にファイルレピュテーションサービスと Web レピュテーションサービスを提供する、グローバルなインターネットベースのインフラストラクチャです。	企業ネットワーク内にファイルレピュテーションサービスや Web レピュテーションサービスを配置して、効率を最適化します。 さらに Smart Protection Server は次のものを提供します。 • ソフトウェア安全性評価サービス • コミュニティファイルレピュテーション • Web 検査サービス • Web レピュテーションサービス • 機械学習型検索エンジン • コミュニティドメイン/IP レピュテーションサービス 注意 動的な URL 検索サービスは、Smart Protection Network でのみ使用できます。
管理	トレンドマイクロがホストおよび管理します。	トレンドマイクロ製品の管理者がインストールおよび管理します。
接続プロトコル	HTTP	HTTP および HTTPS

比較基準	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
使用方法	Smart Protection Server をインストールしない場合に使用します。 Trend Micro Smart Protection Network をソースとして設定する方法については、262 ページの「Smart Protection を設定する」を参照してください。	プライマリソースとして使用し、Trend Micro Smart Protection Network を代替ソースとして使用します。 Smart Protection Server の導入時の設定方法や、ソースとしての設定方法については、262 ページの「Smart Protection Server を設定する」および 262 ページの「Smart Protection を設定する」を参照してください。

Smart Protection Server について

留意点	説明
導入	別のトレンドマイクロ製品で使用するために Smart Protection Server をインストールしたことがある場合は、同じサーバを Deep Discovery Email Inspector でも使用できます。複数のトレンドマイクロ製品からクエリを同時に送信できますが、クエリの量が増加すると、Smart Protection Server に対する負荷が過剰になる場合もあります。Smart Protection Server が、異なる製品から送信されたクエリを処理できることを確認してください。規模のガイドラインや推奨事項については、サポートプロバイダにお問い合わせください。
IP アドレス	Smart Protection Server と VMware ESX/ESXi サーバ (Smart Protection Server のホスト) には、一意の IP アドレスが必要です。VMware ESX/ESXi サーバと Deep Discovery Email Inspector の IP アドレスをチェックし、これらの IP アドレスが Smart Protection Server に割り当てられていないことを確認してください。
設置	インストールの手順と要件については、次の URL から「Trend Micro Smart Protection Server インストールガイド」をダウンロードしてご確認ください。https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

Smart Protection Server を設定する

手順

1. VMware ESX/ESXi サーバに Smart Protection Server をインストールします。

   詳細については、http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp を参照してください。

2. Deep Discovery Email Inspector 管理コンソールから Smart Protection Server を設定します。

   詳細については、262 ページの「Smart Protection を設定する」を参照してください。

   注意

   - Smart Protection Server では Trend Micro Smart Protection Network のデータベース全体を複製できないため、一部の URL のレピュテーションデータが含まれないことがあります。また更新頻度が低いと、古くなったレピュテーションデータが Smart Protection Server から返される場合があります。
   - このオプションを有効にすることで、レピュテーションデータの精度と関連性が向上します。
   - このオプションを無効にすると、データを取得するための時間と帯域幅を節約できます。

Smart Protection を設定する

手順

1. [管理] > [検索/分析] > [その他の設定] > [Smart Protection] の順に選択します。
2. [Web レピュテーションサービス用の Smart Protection Server に接続] を選択します。

3. Smart Protection Server を設定します。

   a. Smart Protection Server の IP アドレスまたは完全修飾ドメイン名を指定します。

      Smart Protection Server のコンソールで [Smart Protection] > [レピュテーションサービス] > [Web レピュテーション] の順に選択して、この IP アドレスを取得します。

      IP アドレスは画面にリストされている URL に含まれています。

   b. Smart Protection Server 接続で使用するように Deep Discovery Email Inspector のプロキシ設定が指定されている場合は、[システムのプロキシ設定を使用] を選択します。

      注意

      プロキシ設定を無効にすると、Smart Protection Server は Deep Discovery Email Inspector に直接接続を行います。

   c. ポート番号を指定します。

4. [接続のテスト] をクリックして、指定した Smart Protection Server からグローバルサービスに接続できることを確認します。

   重要

   Deep Discovery Email Inspector では、Smart Protection Server 3.0 Patch 2 以降への接続でグローバルサービスをサポートします。

5. (オプション) [Smart Protection Server 経由でグローバルサービスに接続] を選択して、グローバル Smart Protection サービスにクエリを実行するよう Deep Discovery Email Inspector を設定します。

   - 組織で CA 証明書を使用する場合は、[証明書を使用] を選択し、[参照] をクリックして証明書ファイルを選択し、[インポート] をクリックして証明書ファイルをインポートします。
     - 組織で証明書取り消しリスト (CRL) を使用する場合は、[CRL を使用] を選択し、[参照] をクリックして CRL ファイルを選択し、[インポート] をクリックして証明書取り消しリストファイルをインポートします。

6. [保存] をクリックします。

スマートフィードバック

Deep Discovery Email Inspector は、新しいトレンドマイクロスマートフィードバックエンジンと統合されています。このエンジンは、保護された脅威情報を Trend Micro Smart Protection Network に送信します。これにより、トレンドマイクロが新しい脅威を識別し、その脅威からユーザを保護できるようになります。スマートフィードバックに参加すると、特定の情報がトレンドマイクロに送信されるようになります。その際、個人および企業の情報は厳重に保護されます。

スマートフィードバックによって以下の情報が収集されます。

- 製品 ID およびバージョン
- 詐欺サイトや脅威の発信元であると疑われる URL
- 検出されたファイルのメタデータ (ファイルタイプ、ファイルサイズ、SHA-1 ハッシュ値、および親ファイルの SHA-1 ハッシュ値)
- 検出ログ (高度な脅威検索エンジン、機械学習型検索エンジン、仮想アナライザ、スクリプトアナライザ、およびスパムメール対策エンジンのログ)
- 検出された次のファイルタイプのサンプル (bat、class、cmd、dll、exe、htm、html、jar、js、lnk、macho、mov、ps1、svg、swf、url、vbe、vbs、wsf)
- Microsoft Office ファイル内のマクロ

スマートフィードバックを有効にする

手順

1. [管理] > [検索/分析] > [その他の設定] > [スマートフィードバック] の順に選択します。
2. スマートフィードバックの 設定を選択します。
   - ネットワークからトレンドマイクロに保護された情報を送信するには、[スマートフィードバックを 有効にする (推奨)] を選択します。

- 高リスクとして検出された不審ファイルをトレンドマイクロに送信して詳しく調査するには、[潜在的に不正な実行可能ファイルをトレンドマイクロに送信] を選択します。

  検出されたリスクレベルの詳細については、50 ページの「仮想アナライザのリスクレベル」を参照してください。

3. [保存] をクリックします。

YARA ルール

Deep Discovery Email Inspector では YARA ルールを使用して不正プログラムを識別します。不正プログラムを検出するためのパターンファイルである YARA ルールは、環境に固有の標的型攻撃やセキュリティ脅威を特定するようにカスタマイズできます。

Deep Discovery Email Inspector では、YARA ルールファイルの数に関係なく最大 5,000 件の YARA ルールを有効にできます。YARA ルール表の右上隅にある [使用中のルール] フィールドには、現在システムで有効な YARA ルールの数が示されます。

重要

Deep Discovery Email Inspector を Deep Discovery Director に登録すると、Deep Discovery Email Inspector は自動的に YARA ルールの設定を Deep Discovery Director から同期し、既存の YARA ルールの設定を上書きします。

次の表は、YARA ルールファイルの詳細を示しています。

表 8-9. YARA ルール

フィールド	説明
ファイル名	YARA ルールファイルの名前。
リスクレベル	YARA ルールのリスクレベル。
ルール	YARA ルールファイルに含まれる YARA ルールの数。
分析対象ファイル:	YARA ルールファイル内の YARA ルールを使用して分析するファイルタイプ。

フィールド	説明
前回の更新	YARA ルールファイルが最後に更新された日時。
ステータス	YARA ルールファイルの有効/無効の切り替え。

YARA ルールファイルを作成する

Deep Discovery Email Inspector では、バージョン 3.10.0 の公式な仕様に準拠する YARA ルールファイルをサポートしています。YARA ルールは、任意のテキストエディタを使用して作成可能なプレーンテキストファイルに保存されます。

YARA ルールの記述の詳細については、次のサイトを参照してください。

https://yara.readthedocs.io/en/v3.10.0/writingrules.html

不正プログラムを検出するために仮想アナライザに追加する YARA ルールファイルは、次の特定の要件を満たしている必要があります。

- ファイル名が一意であること
- ファイルコンテンツが空でないこと

次の例は単純な YARA ルールを示しています。

```
rule NumberOne
{
meta:
desc = "Sonala"
weight = 10
strings:
$a = {6A 40 68 00 30 00 00 6A 14 8D 91}
$b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
$c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
condition:
$a or $b or $c
}
```

次の表に、YARA ルールを構成する各要素とその使用方法を示します。

表 8-10. YARA ルールの構成要素と使用方法

要素	使用方法
rule	YARA ルールの名前です。一意である必要があり、スペースを含めることはできません。
meta:	「メタ」セクションの開始位置を示します。メタセクション内の要素は検出に影響しません。
desc	ルールについて説明するオプションの要素です。
weight	ルールの条件が一致した場合にリスクレベルを判断するオプションの要素です。1〜10 で指定する必要があります。 • 1〜9 = リスク低 • 10 = リスク高  注意 weight の値は、Deep Discovery Email Inspector によって割り当てられるリスクレベルに対応しません。
strings:	「文字列」セクションの開始位置を示します。文字列は、不正プログラムを検出するための主要な手段です。
$a / $b / $c	不正プログラムの検出に使用する文字列です。$文字で開始し、1 つ以上の英数字やアンダースコアが続きます。
condition:	「条件」セクションの開始位置を示します。条件は、文字列をどのように使用して不正プログラムを検出するかを決定します。
$a or $b or $c	条件はルールの論理を定義するブール演算式です。送信されたオブジェクトがルールを満たすかどうかを判断するための条件を示します。条件には、通常のブール演算子 (and、or、not) に加えて関係演算子 (>=、<=、<、>、==、!=) を指定できます。数式には算術演算子 (+、-、*、\、%) およびビット演算子 (&、|、<<、>>、~、^) を使用できます。

YARA ルールファイルを追加する

手順

1. [管理] > [検索/分析] > [その他の設定] > [YARA ルール] の順に選択します。

2. [追加] をクリックして YARA ルールファイルを追加します。

   [YARA ルールファイルの追加] 画面が表示されます。

3. 表示された新しい画面で、次の設定を行います。

   a. ルールファイル: 追加する YARA ルールファイルを参照して選択します。

   b. リスクレベル: ファイルの YARA ルールの検出リスクレベルを選択します。

   c. 分析対象のファイル: この YARA ルールファイルに固有の、仮想アナライザで処理するファイルタイプを入力または選択します。

4. 追加する YARA ルールファイルと分析対象のファイルタイプを選択したら、[追加] をクリックします。

   追加する際、仮想アナライザによって YARA ルールファイルが検証されます。有効な YARA ルールファイルの作成の詳細については、266 ページの「YARA ルールファイルを作成する」を参照してください。

YARA ルールファイルを編集する

手順

1. [管理] > [検索/分析] > [その他の設定] > [YARA ルール] の順に選択します。
2. 編集する YARA ルールファイル名をクリックします。

   [YARA ルールファイルの編集] 画面が表示されます。

3. 設定を変更します。
4. [保存] をクリックします。

YARA ルールファイルを削除する

手順

1. [管理] > [検索/分析] > [その他の設定] > [YARA ルール] の順に選択します。

2. 削除する YARA ルールファイルを 1 つ以上選択します。
3. [削除] をクリックします。

YARA ルールファイルをエクスポートする

手順

1. [管理] > [検索/分析] > [その他の設定] > [YARA ルール] の順に選択します。
2. エクスポートする YARA ルールファイルを選択します。

注意

一度にエクスポートできる YARA ルールは 1 つのみです。

3. [エクスポート] をクリックします。

Time-of-Click URL プロテクション

メールメッセージ内の不正 URL に対する Time-of-Click プロテクションが提供されます。この機能を有効にすると、さらに分析するためにメールメッセージ内の URL が書き換えられ、エンドポイントにブロックまたは警告のリダイレクトページが表示されます。URL がクリックされるたびに、Trend Micro Smart Protection Network (SPN) が書き換えられた URL を分析し、URL のリスクレベルに応じて指定された処理を適用します。

Time-of-Click プロテクションを設定する

手順

1. [管理] > [検索/分析] > [その他の設定] > [Time-of-Click プロテクション] の順に選択します。
2. [Time-of-Click プロテクションを有効にする] を選択してこの機能を有効にし、メールメッセージ内の仮想アナライザが安全と見なす URL と未評価の URL を書き換えて、さらに分析を行います。

3. (オプション) [すべての安全な URL を書き換える] を選択し、メールメッセージ内の Web レピュテーションサービスが安全と見なす URL も書き換えて、さらに分析を行います。
4. 各 URL 評価の処理を選択します。

フィールド	説明
リスク高	危険な URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [ブロック] です。 リスク高の URL とは、不正、または脅威の既知の発信源であると確認されたページです。
リスク中	極めて不審な URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [ブロック] です。 リスク中の URL とは、不正、または脅威の発信源である可能性が疑われたページです。
リスク低	不審な URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [警告] です。 リスク低の URL とは、スパムメールに関連付けられている、または感染している可能性のあるページです。
未評価	未評価の URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [警告] です。 トレンドマイクロは積極的に URL の安全性をテストしていますが、ユーザが新しい Web サイトやあまり一般的でない Web サイトにアクセスすると、未評価のページに遭遇することがあります。未評価のページへのアクセスをブロックすると安全性は向上しますが、安全なページへのアクセスが妨げられることがあります。

5. (オプション) リダイレクトページを設定するには、[リダイレクトページをカスタマイズする] を選択し、必要な設定を行います。
   - [インポート] および [エクスポート] をクリックして、テンプレートファイルを管理します。
   - 各リスクレベルの [内容] タブをクリックして、リダイレクトページのプレビューを表示します。

注意

[内容] 領域で次の HTML タグを使用して、リダイレクトページをカスタマイズできます。

- <a>
- <b>
- <i>

6. [保存] をクリックします。

ビジネスメール詐欺

ビジネスメール詐欺 (BEC 詐欺) を利用する攻撃者は、企業のメールアカウントにアクセスして所有者の ID になりすまし、不正な送金要求を行います。攻撃者は通常、トップレベルの役員になりすまして標的をだまし、攻撃者が用意した口座に送金を実行させます。「Man-in-the-Email (マンインザメール)」詐欺としても知られる BEC 詐欺は、多くの場合、日常的に海外の顧客に送金を行っている、不正プログラムやソーシャルエンジニアリングの 標的となる可能性のあるビジネスをターゲットにしています。

スパムメール対策エンジンを統合した Deep Discovery Email Inspector では、次を実行することにより組織を BEC 詐欺から効果的に保護します。

- 指定した高プロファイルユーザからのメールメッセージを 検索して、ソーシャルエンジニアリング攻撃をブロック
- 送信者と受信者のドメイン情報を確認して、メールメッセージのスプーフィングを防止
- 承認済み送信者からのメールメッセージをバイパスして、検出機能を向上

高プロファイルユーザを追加する

高プロファイルユーザ名を追加して、Deep Discovery Email Inspector でソーシャルエンジニアリング攻撃の可能性があるメールメッセージを 検索できます。

高プロファイルユーザとは、組織のトップレベルの役員のことです。たとえば、CEO、CFO、経営者などです。

手順

1. [管理] > [検索/分析] > [その他の設定] > [ビジネスメール詐欺からの保護] の順に選択します。
2. [高プロファイルユーザ] にユーザ名を入力します。

   注意

   - 姓、名、ミドルネームには最大 30 文字の UTF-8 エンコード文字を入力できます。ハッシュ (#) またはセミコロン (;) の文字は使用しないでください。
   - 完全なユーザ名を指定することが重要です。Deep Discovery Email Inspector では、メッセージの表示名に対して部分一致および完全一致の両方を実行します。

     たとえば、*John A. Smith* という高プロファイルユーザ名を追加すると、Deep Discovery Email Inspector では、表示名に *John A Smith*、*John Smith*、または *Smith John* を使用する偽造メールメッセージがブロックされます。
3. [追加] をクリックします。
   - 最大 500 件の高プロファイルユーザ名を追加できます。
   - ユーザ名を削除するには、エントリを選択して [削除] をクリックします。

内部ドメインを追加する

組織で使用するすべての内部ドメインを追加して、Deep Discovery Email Inspector で潜在的なメールメッセージのスプーフィングを 検出できます。

手順

1. [管理] > [検索/分析] > [その他の設定] > [ビジネスメール詐欺からの保護] の順に選択します。
2. [内部ドメイン] にドメイン名を入力します (例: `example.com`)。

   ドメイン名には印刷可能な ASCII 文字を最大 255 文字指定できます。セミコロン (;) 文字は使用しないでください。
3. [追加] をクリックします。
   - 最大 500 件のドメインを追加できます。
   - ドメインを削除するには、エントリを選択して [削除] をクリックします。

承認済み送信者を追加する

信頼する送信者のメールアドレスを追加して誤検出を減らし、ビジネスメール詐欺 (BEC 詐欺) の検出機能を向上させることができます。Deep Discovery Email Inspector は、承認済み送信者からのメッセージに対して BEC 詐欺の検索を実行しません。

注意

最大 1,000 人の信頼する送信者を追加できます。

手順

1. [管理] > [検索/分析] > [その他の設定] > [ビジネスメール詐欺からの保護] の順に選択します。
2. [承認済み送信者] で、送信者のメールアドレスを入力します (最大 255 文字)。
3. [追加] をクリックします。

   リストから承認済み送信者を削除するには、エントリを選択して [削除] をクリックします。

いとこドメイン

いとこドメイン (類似ドメイン) は、ユーザによく知られた、またはなじみのある正規の対象ドメインと視覚的に類似しており、多くの場合、フィッシング攻撃でユーザの機密情報を盗み出すために利用されます。一般的には、英字の「l」を数字の「1」に変換するなど 1 つ以上の文字を置き換えたり、ドメイン名の文字を追加または削除したりすることで作成されます。メールアドレスを注意深く観察しなければ、ユーザはこの手口に気付かず、偽装された正規のドメインからメールメッセージが送信されているとは考えない可能性があります。

Deep Discovery Email Inspector は高度なスパムメール対策エンジンを使用して、スパムメールやフィッシングメッセージの 検出設定に基づき、メールメッセージ (`from` および `replyto` ヘッダ) に含まれるドメインを検索できます。

いとこドメインを設定する

[いとこドメイン]画面には、正規の送信者ドメインと検出しきい値を設定できます。Deep Discovery Email Inspector はこの設定を使用して、メールメッセージに含まれるいとこドメインを検出します。

手順

1. [管理] > [検索/分析] > [その他の設定] > [いとこドメイン] の順に選択します。
2. 正規の送信者ドメインを 1 つ以上追加します。次の操作を実行します。
   a. ドメイン名を入力します (例: `example.com`)。

      ドメイン名には印刷可能な ASCII 文字を最大 255 文字指定できます。セミコロン (;) 文字は使用しないでください。

   b. [追加] をクリックします。

      - 最大 1,000 件のドメインを追加できます。
      - ドメインを削除するには、エントリを選択して [削除] をクリックします。
3. 検出しきい値を選択します。

- 積極的: あいまい一致に基づく最も多くの検出が提供されます。スパムメールおよびフィッシング検出の最も厳格なレベルです。
- 正常: 推奨設定です (初期設定)。中程度の数の検出が提供されます。
- 保守的: 類似一致に基づく最も精度の高い検出が提供されます。

4. (オプション) Deep Discovery Email Inspector の検索から除外するドメインを 1 つ以上指定します。エントリを追加するには、ドメインを入力して <Enter> キーを押します。
5. [保存] をクリックします。

送信者フィルタ/認証の設定

送信者フィルタと送信者の認証機能を使用することで、受信メールメッセージの送信者をフィルタおよび検証して、スパムメールメッセージを効果的にブロックできます。

注意

送信者フィルタ設定と送信者の認証設定は、Deep Discovery Email Inspector が MTA モードで配置されている場合にのみ有効になります。

次の表は、指定可能な設定を示しています。

設定	説明
承認済み送信者	Deep Discovery Email Inspector の送信者フィルタと送信者の認証の設定をバイパスする信頼された送信者のリストです。
ブロックする送信者	Deep Discovery Email Inspector で常にまたは一時的にブロックする送信者のリストです。

設定	説明
メールレピュテーション	エッジ MTA として配置された Deep Discovery Email Inspector では、送信者 IP アドレスのレピュテーションに基づいて、SMTP セッションを確立する際に送信者からの接続がフィルタされます。 エッジ MTA として配置されていない Deep Discovery Email Inspector では、メールメッセージのヘッダの送信者 IP アドレスのレピュテーションに基づいて、前のリレー MTA の送信者からの接続がフィルタされます。
ディレクトリハーベスト攻撃 (DHA) からの保護	次のいずれかの情報に基づいて、送信者が DHA 攻撃を利用してスパムメールメッセージ送信用のユーザメールアドレスを取得することを防ぎます。 • 送信者 IP アドレス (Deep Discovery Email Inspector がエッジ MTA として配置されている場合) • メールメッセージヘッダ内の送信者 IP アドレス (Deep Discovery Email Inspector が非エッジ MTA として配置されている場合)
バウンスメール攻撃からの保護	次の情報に基づいて、返されたメールメッセージの数が指定したしきい値に達した場合に送信者をブロックします。 • 送信者 IP アドレス (Deep Discovery Email Inspector がエッジ MTA として配置されている場合) • メールメッセージヘッダ内の送信者 IP アドレス (Deep Discovery Email Inspector が非エッジ MTA として配置されている場合)
SMTP トラフィックスロットリング	接続数またはメッセージ数が指定したしきい値に達した場合に、IP アドレスまたはメールアドレスに基づいて、送信者からのメッセージを一定期間ブロックします。
Sender Policy Framework (SPF)	次の情報に基づいて、ドメインに対して承認されたサーバから送信されるメッセージのみを許可することで、スプーフィングとフィッシングを阻止する送信者の認証機能です。 • 送信者 IP アドレス (Deep Discovery Email Inspector がエッジ MTA として配置されている場合) • メールメッセージヘッダ内の送信者 IP アドレス (Deep Discovery Email Inspector が非エッジ MTA として配置されている場合)

設定	説明
DomainKeys Identified Mail (DKIM) 認証	受信メッセージ内の署名を検証することでスプーフィングとフィッシングを阻止する送信者の認証機能です。
DomainKeys Identified Mail (DKIM) 署名	Deep Discovery Email Inspector が送信メッセージのメッセージヘッダに追加する DKIM 署名のリストです。
Domain-based Message Authentication, Reporting & Conformance (DMARC)	指定されたドメインに対してメッセージの送信者を検証し、スプーフィングを阻止する送信者の認証機能です。

送信者フィルタの評価の順序

Deep Discovery Email Inspector がメッセージに検索設定を適用する前に、メッセージ送信者のメールアドレスと IP アドレスに対して、承認済み送信者リストとブロックする送信者リストを使用したフィルタ処理が行われます。送信者のメールアドレスと IP アドレスは、最初の一致が検出されるまで評価されます。

- Deep Discovery Email Inspector の初期設定では、送信者フィルタ設定と送信者の認証設定が次の順序で適用されます。
  - SMTP トラフィックスロットリングの場合:
    - 承認済み送信者リスト (IP アドレス)
    - ブロックする送信者リスト (ユーザ指定の IP アドレス)
    - SMTP トラフィックスロットリング (IP アドレス)
    - 承認済み送信者リスト (メールアドレス)
    - ブロックする送信者リスト (ユーザ指定のメールアドレス)
    - SMTP トラフィックスロットリング (メールアドレス)
  - 送信者フィルタ (ERS、DHA、バウンスメール攻撃) およびドメインベースのメッセージ認証 (SPF、DKIM、および DMARC) の場合:

- 承認済み送信者リスト (IP アドレス)
- ブロックする送信者リスト (ユーザ指定の IP アドレス)
- 承認済み送信者リスト (メッセージのエンベロープ送信者アドレス)
- ブロックする送信者リスト (メッセージのエンベロープ送信者アドレスに対するユーザ指定のメールアドレス)
- 承認済み送信者リスト (メッセージのヘッダ FROM アドレス)
- ブロックする送信者リスト (メッセージのヘッダ FROM アドレスに対するユーザ指定のメールアドレス)
- 送信者フィルタ (ERS、DHA、バウンスメール攻撃)
- ドメインベースのメッセージ認証 (SPF、DKIM、および DMARC)

- 送信者の IP アドレスまたはメールアドレスが承認済み送信者リストに記載されておらず、ブロックする送信者リストのユーザ指定のエントリにも一致しない場合、Deep Discovery Email Inspector では送信者フィルタと送信者の認証の設定を次の順序で適用します。
  - SMTP トラフィックスロットリング (IP アドレスとメールアドレス)
  - Email Reputation Services (ERS)
  - ディレクトリハーベスト攻撃 (DHA) からの保護
  - バウンスメール攻撃からの保護
  - Sender Policy Framework (SPF)
  - DomainKeys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting & Conformance (DMARC)
- 承認済み送信者リストに送信者の IP アドレスまたはメールアドレスが記載されている場合、Deep Discovery Email Inspector ではその送信者からのメッセージに、ブロックする送信者リストのユーザ指定のエントリと、送信者フィルタ (ERS、DHA、バウンスメール攻撃) および送信者の認証 (SPF、DKIM、DMARC) の設定を適用しません。

- ブロックする送信者リストのユーザ指定のエントリに送信者の IP アドレスまたはメールアドレスが一致する場合、Deep Discovery Email Inspector ではその送信者からのメッセージを検索せずにブロックします。
- IP アドレスベースとメールアドレスベースの SMTP トラフィックスロットリングを有効にすると、次の両方の条件が満たされる場合、Deep Discovery Email Inspector では送信者からのメッセージをブロックします。
  - 送信者の IP アドレスがブロックする送信者リストに登録されている
  - 送信者のメールアドレスが承認済み送信者リストに登録されている

SMTP エラーコード

送信者フィルタの設定に基づいてメールメッセージをブロックすると、Deep Discovery Email Inspector は次の SMTP エラーコードをアップストリーム MTA に送信します。

注意

これらのエラーコードを受信した際、イベントログの作成や送信者への通知の送信など、アップストリーム MTA が必要な事前設定処理を実行できることを確認してください。

ブロック機能	SMTP エラーコード	メッセージ
送信者フィルタ/認証設定 (ディレクトリハーベスト攻撃 (DHA) からの保護、バウンスメール攻撃からの保護、SMTP トラフィックスロットリング、SPF、DKIM、DMARC)	421	一時的にブロック (送信者フィルタ/認証)
	521	常にブロック (送信者フィルタ/認証)
メールレピュテーションサービス	450	QIL に一致する接続を一時的に拒否 (450) (ERS)
	550	RBL+に一致する接続を常時拒否 (550) (ERS)

Email Reputation Services を設定する

Deep Discovery Email Inspector のスパムメール対策には Email Reputation Services (ERS) テクノロジが使用されています。ERS テクノロジを使用することで、送信元のメール転送エージェント (MTA) のレピュテーションに基づいてスパムメールを判別します。ERS を有効にすると、すべての受信 SMTP トラフィックを IP アドレスでチェックして、送信元の IP アドレスに問題がないかどうか、既知のスパムメール送信元としてブロックされたことがないかどうかを確認できます。

注意

Email Reputation Services が正常に機能するためには、受信 SMTP トラフィックのすべてのアドレス変換が、トラフィックが Deep Discovery Email Inspector を通過した後に実行される必要があります。受信 SMTP トラフィックが Deep Discovery Email Inspector に到達する前に NAT または PAT が実行されると、Deep Discovery Email Inspector では常にそのローカルアドレスが送信元の MTA として処理されます。ERS は不審な MTA パブリック IP アドレスからの接続のみをブロックし、プライベートまたはローカルアドレスからの接続はブロックしません。

手順

1. [管理] > [送信者フィルタ /認証] > [メールレピュテーション] の順に選択します。
2. [Email Reputation Services を有効にする] を選択します。
3. [検索設定] で [メッセージのヘッダ From アドレスに一致] を選択して、メッセージのエンベロープ送信者アドレスとヘッダ From アドレスを検索します。いずれかのアドレスが一致すると、一致が検出されます。

   Deep Discovery Email Inspector の初期設定では、エンベロープ送信者アドレスのみが検索されます。
4. https://ers.trendmicro.com/にアクセスしてメールレピュテーション管理コンソールにログオンし、グローバルスパムメール情報へのアクセス、レポートの表示、メールレピュテーション設定の管理、およびサービスの設定を実行します。

承認済み送信者リスト

承認済み送信者リストには、Deep Discovery Email Inspector の送信者フィルタ設定と送信者の認証設定をバイパスする信頼された送信者が含まれます。

注意

- MTA モードでのみ、Deep Discovery Email Inspector は送信者を承認済み送信者リストとブロックする送信者リストに照合します。
- Deep Discovery Email Inspector は Trend Micro Email Reputation Services (ERS) を使用して、トラフィックをブロックすることなく、承認済み送信者からの受信 SMTP トラフィックを引き続き確認します。
- Deep Discovery Email Inspector が承認済み送信者リストとブロックする送信者リストに基づいて送信者をフィルタする方法については、277 ページの「送信者フィルタの評価の順序」を参照してください。

次の表は、[承認済み送信者] リストで実行できるタスクを示しています。

タスク	説明
送信者の追加	[追加] をクリックしてリストに送信者を追加します。 詳細については、282 ページの「承認済み送信者を追加する」を参照してください。
送信者の削除	送信者を 1 人以上選択して、[削除] をクリックします。
送信者のインポート	[インポート] をクリックします。 詳細については、284 ページの「承認済み送信者をインポートする」を参照してください。

次の表は、承認済み送信者リストの詳細を示しています。

ヘッダ	説明
IP アドレス	Deep Discovery Email Inspector の送信者フィルタ設定と送信者の認証設定をバイパスする、送信者の IP アドレスまたはドメイン解決された IP アドレスを表示します。

ヘッダ	説明
ドメイン/メールアドレス	送信者のドメインまたはメールアドレスを表示します。
リソースレコード	送信者ドメインのリソースレコードの種類を表示します。
説明	エントリの説明を表示します。
前回の更新	エントリの前回のアップデート日時を表示します。

承認済み送信者を追加する

1 人以上の送信者を承認済み送信者リストに追加できます。Deep Discovery Email Inspector では、承認済み送信者からのメッセージには送信者フィルタ設定と送信者の認証設定が適用されません。

重要

- Deep Discovery Email Inspector では、承認済み送信者リストのエントリに一致する IP アドレス、ドメイン解決された IP アドレス、またはメールアドレスを持つメッセージには送信者フィルタ設定と送信者の認証設定が適用されません。
- SMTP トラフィックスロットリングでは、Deep Discovery Email Inspector は送信者を承認済み送信者リストとブロックする送信者リストに次の順序で照合します。
  - 承認済み送信者リスト (IP アドレス)
  - ブロックする送信者リスト (ユーザ指定の IP アドレス)
  - SMTP トラフィックスロットリング (IP アドレス)
  - 承認済み送信者リスト (メールアドレス)
  - ブロックする送信者リスト (ユーザ指定のメールアドレス)
  - SMTP トラフィックスロットリング (メールアドレス)

注意

リストには最大 2,048 のエントリを追加できます。

手順

1. [管理] > [送信者フィルタ /認証] > [承認済み送信者] の順に選択します。

   [承認済み送信者] 画面が表示されます。

2. [追加] をクリックします。

   [承認済み送信者の追加] 画面が表示されます。

3. 次のいずれかを選択して設定します。

   - ドメイン: 送信者のドメインを指定する場合は、このオプションを選択します。[リソースレコード] には 1 つ以上の種類を選択できます。

     注意

     Deep Discovery Email Inspector は指定されたドメインを定期的に解決し、解決された IP アドレスを承認済み送信者リストのエントリに追加するか、エントリ内の解決された IP アドレスを更新します。

   - IP アドレスまたはサブネット: 1 人の送信者の IPv4/IPv6 アドレスまたは複数の送信者のサブネットを指定する場合は、このオプションを選択します。
   - メールアドレス: 送信者のメールアドレスを指定する場合は、このオプションを選択します。

     ヒント

     Deep Discovery Email Inspector はメールドメインをサポートしています。たとえば、`*@*`はすべてのメールアドレスを表します。

4. 説明を入力します。
5. [保存] をクリックします。

承認済み送信者をインポートする

手順

1. [管理] > [送信者フィルタ/認証] > [承認済み送信者] の順に選択します。

   [承認済み送信者] 画面が表示されます。

2. [インポート] をクリックします。
3. [選択] をクリックして、インポートするファイルを指定します。
4. 次のいずれかのオプションを選択します。
   - 現在のリストにマージする: インポートしたエントリを現在のリストに追加します。
   - 現在のリストを上書きする: すべての既存のエントリを、インポートしたファイル内のエントリで上書きします。
5. [インポート] をクリックします。

ブロックする送信者リスト

Deep Discovery Email Inspector では、ブロックする送信者リストに指定した送信者の IP アドレス、解決済み IP アドレス、またはメールアドレスからのメッセージがブロックされます。

送信者は、次のいずれかの方法でブロックする送信者リストに追加されます。

- 送信者からのメッセージが送信者フィルタ (ディレクトリハーベスト攻撃 (DHA) からの保護、バウンスメール攻撃からの保護、および SMTP トラフィックスロットリング) に基づいて検出された場合は自動的に追加
- 管理者が手動で追加

注意

- MTA モードでのみ、Deep Discovery Email Inspector は送信者を承認済み送信者リストとブロックする送信者リストに照合します。
- ブロックの有効期限が切れると、Deep Discovery Email Inspector は自動的に送信者をリストから削除します。
- [ルール]ドロップダウンリストから [ユーザ指定] または [すべて] を選択する場合、ユーザ指定エントリに期間のフィルタ設定は適用されません。
- Deep Discovery Email Inspector が承認済み送信者リストとブロックする送信者リストに基づいて送信者をフィルタする方法については、277 ページの「送信者フィルタの評価の順序」を参照してください。

次の表は、[ブロックする送信者] リストで実行できるタスクを示しています。

タスク	説明
リストのフィルタ	選択したルールの種類と期間に基づいてリストをフィルタします。
送信者の検索	キーワードを入力して送信者を検索します。
送信者の追加	[追加] をクリックしてリストに送信者を追加します。 詳細については、287 ページの「ブロックする送信者を追加する」を参照してください。
送信者の削除	送信者を 1 人以上選択して、[削除] をクリックします。
送信者のインポート	[インポート] をクリックします。 詳細については、288 ページの「ブロックする送信者をインポートする」を参照してください。
すべてのユーザ指定ルールのエクスポート	リストに手動で追加されたすべてのエントリをエクスポートするには、[すべてのユーザ指定ルールのエクスポート] をクリックします。

タスク	説明
選択したユーザ指定ルールのエクスポート	ユーザ指定のエントリを 1 つ以上選択し、[選択したユーザ指定ルールのエクスポート] をクリックします。 ヒント エントリをフィルタするには、[ルール] ドロップダウンリストから [ユーザ指定] を選択します。
承認済み送信者リストへの送信者の移動	送信者を 1 人以上選択して、[承認済み送信者に移動] をクリックします。 詳細については、281 ページの「承認済み送信者リスト」を参照してください。

次の表は、ブロックする送信者リストの詳細を示しています。

ヘッダ	説明
IP アドレス	Deep Discovery Email Inspector がブロックする送信者の IP アドレスまたはドメイン解決された IP アドレスを表示します。
ドメイン/メールアドレス	送信者のドメインまたはメールアドレスを表示します。
ルール	一致する送信者フィルタ/認証ルールの名前を表示します。
リソースレコード	送信者ドメインのリソースレコードの種類を表示します。
処理	送信者のアドレスを一時的にブロックするのか、常にブロックするのかを表示します。
失効日	Deep Discovery Email Inspector が送信者の一時的なブロックを停止した時点を表示します。 一時的なブロック処理の有効期限が切れると、Deep Discovery Email Inspector では送信者がリストから削除されます。
説明	エントリの説明を表示します。
前回の更新	エントリの前回のアップデート日時を表示します。

ブロックする送信者を追加する

重要

SMTP トラフィックスロットリングでは、Deep Discovery Email Inspector は送信者を承認済み送信者リストとブロックする送信者リストに次の順序で照合します。

- 承認済み送信者リスト (IP アドレス)
- ブロックする送信者リスト (ユーザ指定の IP アドレス)
- SMTP トラフィックスロットリング (IP アドレス)
- 承認済み送信者リスト (メールアドレス)
- ブロックする送信者リスト (ユーザ指定のメールアドレス)
- SMTP トラフィックスロットリング (メールアドレス)

注意

リストには最大 2,048 のエントリを追加できます。

手順

1. [管理] > [送信者フィルタ /認証] > [ブロックする送信者] の順に選択します。

   [ブロックする送信者] 画面が表示されます。

2. [追加] をクリックします。

   [ブロックする送信者の追加] 画面が表示されます。

3. 次のいずれかを選択して設定します。

   - ドメイン: 送信者のドメインを指定する場合は、このオプションを選択します。[リソースレコード] には 1 つ以上の種類を選択できます。

注意

Deep Discovery Email Inspector は指定されたドメインを定期的に解決し、解決された IP アドレスをブロックする送信者リストのユーザ指定エントリとして追加するか、エントリ内の解決された IP アドレスを更新します。

- IP アドレスまたはサブネット: 1 人の送信者の IPv4/IPv6 アドレスまたは複数の送信者のサブネットを指定する場合は、このオプションを選択します。
- メールアドレス: 送信者のメールアドレスを指定する場合は、このオプションを選択します。

ヒント

Deep Discovery Email Inspector はメールドメインをサポートしています。たとえば、`*@*`はすべてのメールアドレスを表します。

4. 説明を入力します。
5. [保存] をクリックします。

ブロックする送信者をインポートする

手順

1. [管理] > [送信者フィルタ/認証] > [ブロックする送信者] の順に選択します。

   [ブロックする送信者] 画面が表示されます。
2. [インポート] をクリックします。
3. [選択] をクリックして、インポートするファイルを指定します。
4. 次のいずれかのオプションを選択します。
   - 現在のリストにマージする: インポートしたエントリを現在のリストに追加します。

- 現在のリストを上書きする: すべての既存のエントリを、インポートしたファイル内のエントリで上書きします。

5. [インポート] をクリックします。

DHA 攻撃からの保護を設定する

ディレクトリハーベスト攻撃 (DHA) からの保護を設定して、送信者が DHA 攻撃を利用してスパムメールメッセージ送信用のメールアドレスを取得することを防ぎます。

注意

- この機能を有効にする前に、Microsoft Active Directory を設定してください。

  詳細については、390 ページの「LDAP サーバを設定する」を参照してください。

- SMTP トラフィックが大量に発生すると、ルールトリガとアクティベーションの時間差のために、設定に応じて Deep Discovery Email Inspector でメールメッセージが正確にブロックされない場合があります。

手順

1. [管理] > [送信者フィルタ/認証] > [ディレクトリハーベスト攻撃 (DHA) からの保護] の順に選択します。
2. [DHA 攻撃からの保護を有効にする] を選択します。
3. 次の設定を行います。

フィールド	説明
監視期間	DHA 脅威を示すメッセージの割合が指定したしきい値を超えていないかどうかについて、Deep Discovery Email Inspector でメールトラフィックを監視する時間数を選択します。
比率	検出された脅威を含むメッセージの割合の最大値を入力します。

フィールド	説明
メッセージ総数	しきい値の割合の計算に使用する、(同じ送信者から受信した) メッセージの総数を入力します。
受信者しきい値	許可される受信者の最大数を入力します。
存在しない受信者	しきい値として可能な存在しない受信者の最大数を入力します。DHA には、受信者リスト内にランダムに生成されたメールアドレスが含まれることがあります。
処理	次のブロック処理のいずれかを選択します。 • 一時的にブロック: その IP アドレスからのメッセージを一時的にブロックし、ブロック期間終了後にアップストリーム MTA からの再試行を許可します。 • 常にブロック: その IP アドレスからの今後のメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
ブロック期間	[一時的にブロック] 処理を選択する場合は、ブロックする時間数を選択します。 注意 ブロック時間が終了すると、その送信者はブロックする送信者リストから削除されます。

たとえば、次のように設定するとします。

- 監視期間: 1 時間
- 比率: 20
- メッセージ総数: 100
- 受信者しきい値: 10
- 存在しない受信者: 5

DHA 攻撃からの保護が有効に設定された 1 時間単位の期間で、11 人以上の受信者 (組織外の受信者 6 人以上を含む) に送信されたメッセージの 20%を超えるメッセージを Deep Discovery Email Inspector が受信し、かつメッセージの総数が 100 を超える場合に、送信者のブロックを開始します。

4. [保存] をクリックします。

   初期設定を使用するには、[初期設定に戻す] をクリックして入力した設定を破棄します。

バウンスメール攻撃からの保護を設定する

バウンスメール攻撃からの保護を設定して、返されたメールメッセージの数が指定したしきい値に達した場合に送信者をブロックできます。

注意

- この機能を有効にする前に、Microsoft Active Directory を設定してください。

  詳細については、390 ページの「LDAP サーバを設定する」を参照してください。

- Deep Discovery Email Inspector では、存在しない受信者を含むメールメッセージをバウンス攻撃によるものと見なします。
- SMTP トラフィックが大量に発生すると、ルールトリガとアクティベーションの時間差のために、設定に応じて Deep Discovery Email Inspector でメールメッセージが正確にブロックされない場合があります。

手順

1. [管理] > [送信者フィルタ /認証] > [バウンスメール攻撃からの保護] の順に選択します。
2. [バウンスメール攻撃からの保護を有効にする] を選択します。
3. 次の設定を行います。

フィールド	説明
監視期間	バウンス攻撃を示すメッセージの割合が指定したしきい値を超えていないかどうかについて、Deep Discovery Email Inspector がメールトラフィックを監視する時間数を選択します。

フィールド	説明
比率	検出された脅威を含むメッセージの割合の最大値を入力します。
メッセージ総数	しきい値の割合の計算に使用する、(同じ送信者から受信した)メッセージの総数を入力します。
処理	次のブロック処理のいずれかを選択します。 • 一時的にブロック: その IP アドレスからのメッセージを一時的にブロックし、ブロック期間終了後にアップストリーム MTA からの再試行を許可します。 • 常にブロック: その IP アドレスからの今後のメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
ブロック期間	[一時的にブロック] 処理を選択する場合は、ブロックする時間数を選択します。 注意 ブロック時間が終了すると、その送信者はブロックする送信者リストから削除されます。

たとえば、次のように設定するとします。

- 監視期間: 1 時間
- 比率: 20
- メッセージ総数: 100

バウンスメールのブロックが有効に設定された 1 時間単位の期間で、Deep Discovery Email Inspector が受信したメッセージの 20%超がバウンスメッセージであり、かつメッセージの総数が 100 を超える場合に、送信者のブロックを開始します。

4. [保存] をクリックします。

   初期設定を使用するには、[初期設定に戻す] をクリックして入力した設定を破棄します。

SMTP トラフィックスロットリングを設定する

SMTP トラフィックスロットリングを設定して、接続数またはメッセージ数が指定したしきい値に達した場合に、単一の IP アドレスまたは送信者メールアドレスからのメッセージを一定期間ブロックします。

注意

- Deep Discovery Email Inspector をネットワーク内のエッジ MTA として配置しない場合は、SMTP トラフィックスロットリングを無効にします。
- SMTP トラフィックが大量に発生すると、ルールトリガとアクティベーションの時間差のために、設定に応じて Deep Discovery Email Inspector でメールメッセージが正確にブロックされない場合があります。
- Deep Discovery Email Inspector が承認済み送信者リストとブロックする送信者リストに基づいてメッセージをブロックする方法については、277 ページの「送信者フィルタの評価の順序」を参照してください。

手順

1. [管理] > [送信者フィルタ /認証] > [SMTP トラフィックスロットリング] の順に選択します。
2. 次のオプションを 1 つまたは両方選択します。
   - 送信者 IP アドレスに基づく SMTP トラフィックスロットリングを有効にする: 送信者 IP アドレスに基づいてトラフィックを監視します。
   - 送信者メールアドレスに基づく SMTP トラフィックスロットリングを有効にする: 送信者メールアドレスに基づいてトラフィックを監視します。

注意

メールアドレスに基づく SMTP トラフィックスロットリングが有効な場合、Deep Discovery Email Inspector では、承認済み送信者リストの送信者メールアドレスからのトラフィックに SMTP トラフィックスロットリングの設定を適用しません。

3. 次の設定を行います。

フィールド	説明
最大接続数	単一の IP アドレスに対して許可される最大接続数を入力します。
最大メッセージ数	単一の IP アドレスまたはメールアドレスに対して許可される最大メッセージ数を入力します。
ブロック期間	ブロックする時間数を選択します。 注意 ブロック時間が終了すると、その送信者はブロックする送信者リストから削除されます。

4. [保存] をクリックします。

   初期設定を使用するには、[初期設定に戻す] をクリックして入力した設定を破棄します。

Sender Policy Framework (SPF) について

Sender Policy Framework (SPF) は、サーバがドメインのメールメッセージを送信することについて承認されているかどうかを検証することで、スプーフィングとフィッシングを検出するメール検証システムです。Deep Discovery Email Inspector は SPF を使用して、メールメッセージの「エンベロープ from」アドレスを承認された送信元 IP アドレスのリストに照らして検証し、メールメッセージが偽装されていないかどうかを判別します。

SPF では、ドメインの所有者が Domain Name System (DNS) の SPF レコードにメール送信ポリシーを公開することが必要です。このメール送信ポリシーには、そのドメインから送信されるメールメッセージが使用するメールサーバなどの情報が記載されています。ドメインからメールメッセージを受信した Deep Discovery Email Inspector は、SPF レコードを確認して、そのメールメッセージがドメインの公開ポリシーに準拠しているかどうかを検証します。不明なサーバから送信されている場合、そのメールメッセージは偽装されていると見なすことができます。

SPF レコードの評価では、次のような結果が返されます。

結果	説明
Pass	この SPF レコードは送信が許可されるものとしてこのホストを指定しています。
Fail	この SPF レコードは送信が許可されないものとしてこのホストを指定しています。
SoftFail	この SPF レコードは送信が許可されないものとしてこのホストを指定していますが、移行中です。
Neutral	この SPF レコードは有効性について何も明言できないことを明示的に指定しています。
None	このドメインには SPF レコードがないか、SPF レコードを評価しても結果が生成されません。
PermError	恒久的なエラーが発生しました (不正な SPF レコードの形式など)。
TempError	一時的なエラーが発生しました。

SPF を設定する

SPF を設定すると、メールメッセージを目的の受信者に配信する前に、送信者がドメインのメールメッセージの送信を許可されているかどうかを Deep Discovery Email Inspector で判断できるようになります。

注意

非エッジ MTA として配置されている Deep Discovery Email Inspector では、HELO/EHLO ID 検証を実行できません。

手順

1. [管理] > [送信者フィルタ /認証] > [SPF] の順に選択します。
2. [SPF (Sender Policy Framework) を有効にする] を選択します。
3. [HELO/EHLO ID] で、HELO/EHLO コマンドの送信者情報を確認する場合は [有効] を、そうでない場合は [無効] を選択します。
4. 検証結果をメッセージヘッダに追加するには、[メールメッセージに X-Header を挿入する] を選択します。

5. 検証する送信者ドメインを指定します。すべての送信者ドメインからのメッセージについて SPF レコードを確認するには [すべて] を、そうでない場合は [送信者ドメインの指定] を選択し、次の手順を完了して送信者ドメインを検証リストに追加します。

   a. ドメインを入力します。

   b. [追加] をクリックします。

   注意

   - すべてのドメインの SPF 検証を有効にすると、システムのパフォーマンスが低下する可能性があります。
   - リストからドメインを削除するには、エントリを選択して [削除] をクリックします。

6. 検証結果に基づいて実行する処理を指定します。
   - バイパス: メッセージの処理が続行されます。
   - 一時的にブロック: メッセージが一時的にブロックされます。送信者は同じメッセージを Deep Discovery Email Inspector に送信して、再度検証を実行できます。
   - 常にブロック: メッセージが常にブロックされます。送信者から新しいメッセージを受信すると、Deep Discovery Email Inspector は再度検証を実行します。
7. [保存] をクリックします。

DomainKeys Identified Mail (DKIM) について

DomainKeys Identified Mail (DKIM) はメール検証システムであり、メッセージに関連付けられたドメイン名の同一性を暗号化認証を利用して検証することによってメールのスプーフィングを 検出します。また、受信メッセージの完全性の確保や、送信中のメッセージ改ざん防止にも使用されます。

メールメッセージの有効性と完全性を確保するために、DKIM では公開鍵と秘密鍵のペアシステムが使用されます。公開鍵と秘密鍵のペアは、送信ドメインに対して作成されます。秘密鍵はメールサーバに安全に保存され、送信メッセージの署名に使用されます。公開鍵は Domain Name System (DNS) で保

存され、公開されます。メールメッセージが送信されると、メールサーバはメッセージヘッダの一部である秘密鍵を使用して、メッセージのデジタル署名を行います。メールメッセージが受信されると、DKIM 署名をドメインの DNS 上にある公開鍵と照合できます。

Deep Discovery Email Inspector による DKIM 認証は、次の状況においてのみ実施されます。

- 指定した送信者ドメインまたはすべての送信者ドメインからの受信メッセージの DKIM 署名を検証する
- メッセージヘッダ内の「From」フィールドの値が MAIL FROM アドレス (エンベロープの差出人) と同じ場合にのみ、スプーフィング防止のために DKIM 署名を送信メッセージのヘッダに追加する

DKIM 認証を設定する

Deep Discovery Email Inspector は、受信メールメッセージ内の DKIM 署名を検証し、署名の検証に失敗したメッセージに対して処理を適用します。メッセージの DKIM 署名が検証に成功すると、そのメッセージは配信プロセスの次のステップに進みます。

手順

1. [管理] > [送信者フィルタ /認証] > [DKIM 認証] の順に選択します。
2. [DKIM (DomainKeys Identification Mail) 認証を有効にする] を選択します。
3. 検証結果をメッセージヘッダに追加するには、[メールメッセージに X-Header を挿入する] を選択します。
4. 1 つのメッセージで検証する署名の最大数を選択します。

注意

- 選択した最大数を超える署名がメッセージに含まれている場合、Deep Discovery Email Inspector はメッセージの DKIM 認証プロセスを終了します。
- 検証する署名の数を増やすと、処理の負荷が増大する可能性があります。

5. 検証する送信者ドメインを指定します。すべての送信者ドメインからのメッセージ内の DKIM 署名を検証するには [すべて] を、そうでない場合は [送信者ドメインの指定] を選択し、次の手順を完了して送信者ドメインを検証リストに追加します。

   a. ドメインを入力します。

   b. [追加] をクリックします。

   注意

   リストからドメインを削除するには、エントリを選択して [削除] をクリックします。

6. 検証結果に基づいて実行する処理を指定します。

   - バイパス: メッセージの処理が続行されます。
   - 一時的にブロック: メッセージが一時的にブロックされます。送信者は同じメッセージを Deep Discovery Email Inspector に送信して、再度検証を実行できます。
   - 常にブロック: メッセージが常にブロックされます。送信者から新しいメッセージを受信すると、Deep Discovery Email Inspector は再度検証を実行します。

7. [保存] をクリックします。

DKIM 署名

スプーフィングを防止するため、送信メッセージのヘッダにデジタル署名を追加するように Deep Discovery Email Inspector を設定できます。受信者は、特定のドメインからのメールメッセージがドメインの管理者によって承認されたものであり、添付ファイルを含むメッセージが転送中に変更されていないことを確認できます。

重要

すでにデジタル署名が追加された、Gmail など他のメールサービスや MTA からの受信メッセージに署名するよう設定する場合、Deep Discovery Email Inspector はすべての既存の署名を削除した後、新しい署名を追加してメッセージを送信します。

DKIM 署名を追加または削除したり DKIM 署名ファイルをインポートまたはエクスポートしたりするには、管理コンソールを使用します。

次の表は、[DKIM 署名] 画面で実行できるタスクを示しています。

タスク	説明
DKIM 署名の追加	ドメインからの送信メッセージに署名する DKIM 署名を設定します。 詳細については、299 ページの「DKIM 署名を設定する」を参照してください。
DKIM 署名の編集	ドメインをクリックして設定を編集します。
DKIM 署名の削除	エントリをリストから削除するには、エントリを選択して [削除] をクリックします。
DKIM 署名のリストのインポート	別の Deep Discovery Email Inspector アプライアンスから DKIM 署名のリストをインポートできます。 詳細については、301 ページの「DKIM 署名をインポートする」を参照してください。
DKIM 署名のリストのエクスポート	[エクスポート] をクリックして、DKIM 署名のリストをファイルに保存します。 エクスポートしたファイルを使用して、ネットワーク上の複数の Deep Discovery Email Inspector アプライアンスに同じ設定を複製できます。

DKIM 署名を設定する

Deep Discovery Email Inspector では、特定のドメインから送信するすべてのメッセージに使用する DKIM 署名を追加または編集できます。

手順

1. [管理] > [送信者フィルタ/認証] > [DKIM 署名] の順に選択します。
2. 次のいずれかを実行します。
   - [追加] をクリックして新しい署名を追加します。
   - ドメインをクリックして署名を編集します。
3. [DKIM 署名を有効にする] を選択します。
4. 一般設定を行います。

フィールド	説明
ドメイン	メッセージが送信されるドメインを入力します。たとえば、example.com や*.example.com のように入力します。
SDID	署名ドメイン ID を入力します。たとえば、example.com のように入力します。
署名するヘッダ	署名するヘッダを 1 つ以上選択するか、カスタムヘッダを追加します。
秘密鍵	次のいずれかを選択します。 • 既存の鍵のインポート: [選択] をクリックして、インポートする秘密鍵ファイルを指定します。 • 生成: 鍵長を選択して、秘密鍵を生成します。 注意 設定を保存したら、生成された [DNS TXT レコード名] と [DNS TXT レコード値] を使用して、DNS サーバに鍵のペアを公開します。

5. (オプション) 詳細設定を行います。

フィールド	説明
ヘッダの正規化	正規化のアルゴリズムを選択します。 • Relaxed: 空白文字の置換やヘッダフィールド行の再ラッピングなど、一般的な変更が許可されます。 • Simple: ヘッダの変更は許可されません。
本文の正規化	正規化のアルゴリズムを選択します。 • Relaxed: 空白文字の置換など、一般的な変更が許可されます。 • Simple: 本文の変更は許可されません。
署名の有効期限	署名の有効日数を入力します。
本文の長さ	メール本文に許可されるバイト数を入力します。
AUID	SDID が責任を負うエージェントまたはユーザ ID を入力します。
サブドメインの除外	DKIM 署名から除外するサブドメインを入力し、<Enter> キーを押します。

6. [保存] をクリックします。

注意

秘密鍵を生成するように Deep Discovery Email Inspector を指定する場合は、生成された [DNS TXT レコード名] と [DNS TXT レコード値] を使用して、DNS サーバに鍵のペアを公開します。

DKIM 署名をインポートする

別の Deep Discovery Email Inspector アプライアンスから DKIM 署名のリストをインポートできます。

手順

1. [管理] > [送信者フィルタ/認証] > [DKIM 署名] の順に選択します。

2. [インポート] をクリックします。

   [DKIM 署名のインポート] 画面が表示されます。

3. [選択] をクリックして、DKIM 署名のリストを含むファイルを指定します。

4. パスワードを指定します。

5. [インポート] をクリックします。

Domain-based Message Authentication, Reporting & Conformance (DMARC) について

Domain-based Message Authentication, Reporting & Conformance (DMARC) は、メールのスプーフィングを 検出および防止するために設計されたメール検証システムです。これは、正規の組織を装った送信者アドレスによるメールメッセージの送信など、フィッシング詐欺やスパムメールで頻繁に使用される手法に対抗することを目的としています。DMARC により、特定のドメインへのメールメッセージ認証、送信者へのフィードバック、および公開ポリシーに基づいた処理を行う方法が提供されます。

DMARC は、Deep Discovery Email Inspector の既存の受信メール認証プロセスに適合するように設計されています。これはメール受信者が、送信されたメッセージの内容が、送信者について受信者が知っている情報に適合しているかを判断するために役立ちます。適合しない場合、DMARC では、適合しないメッセージの処理方法に関する指針が示されます。

DMARC では次のことが必要です。

- メッセージが SPF チェックを通過する
- メッセージが DKIM 認証チェックを通過する
- 認証識別子 (ドメイン) が一致している

  認証識別子が一致していると見なすためには、SPF や DKIM によって認証されるドメインがメッセージヘッダドメインと同じであるか、その親ドメインである必要があります。

DMARC を設定することで、Deep Discovery Email Inspector では、メッセージに実行する処理を指定し、強制ピアを追加して、特定の送信者ドメインからのメールメッセージが常に DMARC 認証を通過するようにできます。

DMARC を設定する

[DMARC] 画面を使用して、特定のドメインに対する DMARC 設定を行い、DMARC 認証の結果に基づいた処理を指定します。

手順

1. [管理] > [送信者フィルタ /認証] > [DMARC] の順に選択します。
2. [DMARC (Domain-based Message Authentication, Reporting and Conformance) を有効にする] を選択します。
3. 検証結果をメッセージヘッダに追加するには、[メールメッセージに X-Header を挿入する] を選択します。
4. (オプション) [送信者に日次レポートを送信] を選択し、次の設定を行って、認証の失敗に関する日次の集約レポートをメールの送信者に送信します。

フィールド	説明
組織名	送信元の組織の名前またはドメインを入力します。
メールアドレス	Deep Discovery Email Inspector がレポートを送信する際に使用するメールアドレスを入力します。
連絡先情報	連絡先情報 (電話番号や URL など) を入力します。

5. 検証する送信者ドメインを指定します。すべての送信者ドメインからのメッセージを確認するには [すべて] を、そうでない場合は [送信者ドメインの指定] を選択し、次の手順を完了して送信者ドメインを検証リストに追加します。
   a. ドメインを入力します (ワイルドカード使用可)。たとえば、example.com や*.example.com のように入力します。
   b. [追加] をクリックします。

注意

リストからドメインを削除するには、エントリを選択して [削除] をクリックします。

6. 検証結果に基づいて実行する処理を指定します。
   - バイパス: メッセージの処理が続行されます。
   - 一時的にブロック: メッセージが一時的にブロックされます。送信者は同じメッセージを Deep Discovery Email Inspector に送信して、再度検証を実行できます。
   - 常にブロック: メッセージが常にブロックされます。送信者から新しいメッセージを受信すると、Deep Discovery Email Inspector は再度検証を実行します。
7. [保存] をクリックします。

エンドユーザメール隔離

Deep Discovery Email Inspector には、スパムメールの管理を強化するエンドユーザメール隔離 (EUQ) 機能があります。スパムメールと判定されたメッセージは隔離されるため、エンドユーザがメッセージを再確認して、削除、隔離解除、または配信を許可することができます。インライン処理リンクを含むエンドユーザメール隔離通知を自動的に送信するように Deep Discovery Email Inspector を設定できます。Web ベースのエンドユーザメール隔離管理コンソールを使用することで、ユーザは各自の個人アカウントおよび、自分が所属する配布リストのスパムメールの隔離方法を管理したり、送信者を承認済み送信者リストに追加したりできます。

隔離ストレージを管理するには、手動でデータを削除したり、自動データ削除のしきい値を設定したりできます。

詳細については、448 ページの「ストレージ管理を設定する」を参照してください。

注意

Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降に登録すると、Deep Discovery Director によってエンドユーザメール隔離設定の一元管理が行われます。登録に成功した Deep Discovery Email Inspector では、次の処理が行われます。

- エンドユーザメール隔離の設定を Deep Discovery Director から取得し、管理コンソールでの手動による設定を防止する
- エンドユーザメール隔離通知の送信を停止する
- エンドユーザメール隔離コンソールのアクセスを無効にする

ユーザ隔離アクセスを設定する

ユーザがエンドユーザメール隔離の管理コンソールにアクセスして隔離メッセージを管理するように Deep Discovery Email Inspector を設定できます。

注意

Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降に登録すると、Deep Discovery Director によってエンドユーザメール隔離設定の一元管理が行われます。登録に成功した Deep Discovery Email Inspector では、次の処理が行われます。

手順

1. [管理] > [エンドユーザメール隔離] の順に選択します。
2. [ユーザ隔離アクセス] タブをクリックします。
3. [エンドユーザメール隔離コンソールのアクセスを有効にする] を選択します。
4. エンドユーザメール隔離コンソールにアクセスする際の認証方法を選択します。
   - LDAP: LDAP のアカウント認証情報に基づいて、エンドユーザメール隔離コンソールにアクセスするユーザを認証します。このオプションを選択する場合は、次の設定を指定できます。

- [配布リスト EUQ の管理を有効にする] をオンにすると、ユーザは自分が所属する配布リストのエンドユーザメール隔離を管理できます。
- [選択したグループのユーザのみエンドユーザメール 隔離コンソールのアクセスを許可する] をオンにすると、選択した LDAP グループがエンドユーザメール 隔離コンソールにアクセスできます。

  テキストボックスにキーワードを入力し、[クエリ] をクリックしてユーザグループを 検索できます。[利用可能なグループ] リストでグループ名をクリックして、[選択したグループ] リストに追加します。

  ヒント

  グループを削除するには、[選択したグループ] リストでグループ名をクリックします。

注意

ユーザ認証に LDAP サーバを使用する前に、LDAP の統合設定を行います。

詳細については、390 ページの「LDAP サーバを設定する」を参照してください。

- SAML: ID プロバイダから取得した SAML シングルサインオンアカウント認証情報に基づいてユーザを認証します。

  選択したユーザグループのユーザにのみエンドユーザメール 隔離 (EUQ) 通知を送信するには、[選択した LDAP グループのユーザにのみ、エンドユーザメール隔離 (EUQ) 通知を送信します。] を選択し、[選択したグループ] リストにユーザグループを 1 つ以上追加します。
- SMTP: メールアドレスのアカウント認証情報に基づいて、エンドユーザメール隔離の管理コンソールにアクセスするユーザを認証します。

  SMTP サーバを追加するには、[+] (追加) をクリックします。

詳細については、307 ページの「EUQ 認証用に SMTP サーバを追加する」を参照してください。

5. [詳細設定] で、次の設定を行います。

   - [ユーザ 1 人あたりの承認済み送信者の最大数] ドロップダウンリストで、エンドユーザメール隔離の管理コンソールで追加できる承認済み送信者のメールアドレスの最大数を選択します。
   - [隔離解除したメッセージを再処理せずに直接配信する] をオンにすると、隔離されたメッセージを検索せずに隔離解除し、ユーザが受信者に直接配信できます。

   注意

   このオプションを選択しなくても、エンドユーザメール隔離通知内のインライン処理リンクをクリックするか、エンドユーザメール隔離の管理コンソールからメッセージを隔離解除することもできます。ただし、これらのメッセージは配信前に Deep Discovery Email Inspector で検索されるため、検索結果によっては再度隔離されることがあります。

6. [保存] をクリックします。

   [エンドユーザメール隔離コンソールのアクセスを有効にする] オプションの選択後、URL をクリックしてエンドユーザメール隔離の管理コンソールにアクセスしたり、URL をユーザに送信したりできるようになります。

   詳細については、312 ページの「エンドユーザメール隔離の管理コンソールにアクセスする」を参照してください。

EUQ 認証用に SMTP サーバを追加する

[エンドユーザメール隔離] 画面で、EUQ 認証に使用する SMTP サーバを 1 つ以上追加できます。

手順

1. [管理] > [エンドユーザメール隔離] の順に選択します。

   [エンドユーザメール隔離] 画面が表示されます。

2. [EUQ 認証に SMTP サーバを使用する] を選択します。

3. [+] (追加) をクリックします。

   [SMTP サーバの追加] 画面が表示されます。

4. SMTP サーバを設定します。

フィールド	説明
ドメイン	エンドユーザメール隔離の管理コンソールの認証に使用するドメイン名を入力します。 ドメイン名にはアスタリスク文字 (*) を使用できます。
サーバアドレス	サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
ポート番号	サーバのポート番号を入力します。
暗号化方法	データの暗号化方法 ([なし]、[StartTLS]、または [SSL/TLS]) をドロップダウンリストから選択します。

5. [追加] をクリックします。

エンドユーザメール隔離通知

エンドユーザメール隔離通知は、スパムメールとして検出され、一時的に [エンドユーザメール隔離] に保存されているメールメッセージについてユーザに知らせるために Deep Discovery Email Inspector から送信される通知です。

注意

- Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降に登録すると、Deep Discovery Director によってエンドユーザメール隔離設定の一元管理が行われます。登録に成功した Deep Discovery Email Inspector では、次の処理が行われます。
- Deep Discovery Email Inspector では、前回の通知以降に新しく隔離されたメッセージがある場合にのみ、エンドユーザメール隔離通知が送信されます。
- Active Directory 認証が有効な場合、Deep Discovery Email Inspector はユーザグループ (または配布リスト) にエンドユーザメール隔離通知を送信しません。
- SMTP 認証が有効であり、検出されたメッセージが配布リストに送信される場合、Deep Discovery Email Inspector は配布リストにエンドユーザメール隔離通知を送信します。

エンドユーザメール隔離通知では、次の情報が提供されます。

- スパムメールメッセージの総数: 前回の通知以降にエンドユーザメール隔離に新しく保存されたメールメッセージの総数
- 新しいスパムメールメッセージのサイズ : 前回の通知以降にエンドユーザメール隔離に新しく保存されたメールメッセージのサイズ
- メッセージリスト : スパムメールとして検出されたメールメッセージの概要
  - 送信者: 送信者のメールアドレス
  - 件名: メールの件名
  - サイズ: 添付ファイルを含むメッセージサイズ
  - 受信日時: メッセージを受信した日時
  - 処理: 隔離メッセージに処理を適用したり、送信者のメールアドレスを承認済みリストに追加したりするためのリンク

注意

インライン処理リンクは、[エンドユーザメール隔離通知] 画面でこの機能を有効にしている場合にのみ表示されます。

インライン処理リンク

エンドユーザメール隔離通知にインライン処理リンクを含めるように Deep Discovery Email Inspector を設定できます。ユーザはエンドユーザメール隔離通知のリンクをクリックすることで、エンドユーザメール隔離の管理コンソールにアクセスすることなく隔離メッセージを管理できます。

インライン処理リンクを使用すると、隔離されたメッセージに対して次の処理を実行できます。

- 削除: メッセージと関連する添付ファイルを削除します。
- 隔離解除: メッセージを隔離から直接隔離解除します。
- 隔離解除して承認済み送信者リストに追加: メッセージを隔離から直接隔離解除して、送信者のメールアドレスを承認済み送信者リストに追加します。

重要

[ユーザメール隔離アクセス] 画面で [隔離解除したメッセージを再処理せずに直接配信する] オプションを選択すると、Deep Discovery Email Inspector は隔離解除されたメッセージを検索せずに受信者に配信します。

詳細については、305 ページの「ユーザ隔離アクセスを設定する」を参照してください。

エンドユーザメール隔離通知を設定する

エンドユーザメール隔離通知を送信して、新規メッセージがスパムメールとして検出されたことをユーザに通知するように Deep Discovery Email Inspector を設定できます。

手順

1. [管理] > [エンドユーザメール隔離]。
2. [エンドユーザメール隔離通知] タブをクリックします。
3. [エンドユーザメール隔離 (EUQ) 通知を有効にする] を選択します。
4. [通知の頻度] ドロップダウンリストから、Deep Discovery Email Inspector がエンドユーザメール隔離通知を送信するまで待機する時間数を選択します。
5. エンドユーザメール隔離通知からユーザが処理を適用できるようにするには、[インライン処理を有効にする] を選択します。
6. 通知テンプレートを設定します。

フィールド	説明
件名	通知メールメッセージの件名を入力します。
内容	通知メールメッセージの内容を入力します。 メッセージには次のトークンを含めることができます。 • %USER_NAME% • %TOTAL_SPAM_COUNT% • %TOTAL_SPAM_SIZE% • %START_TIME% • %END_TIME%

7. [保存] をクリックします。

エンドユーザメール隔離の管理コンソール

エンドユーザメール隔離を設定する際は、エンドユーザメール隔離の管理コンソールで次のタスクを実行できます。

- ユーザ各自の個人アカウントのスパムメール隔離の管理
- ユーザが所属する Active Directory の配布リストのスパムメール隔離の管理

- 承認済み送信者リストへの送信者の追加

注意

エンドユーザメール隔離の管理コンソールへのアクセスは、[ユーザメール隔離アクセス] 画面で有効にできます。

詳細については、305 ページの「ユーザ隔離アクセスを設定する」を参照してください。

エンドユーザメール隔離の管理コンソールにアクセスする

隔離されたスパムメールメッセージや承認済み送信者リストを管理するには、エンドユーザメール隔離の管理コンソールにアクセスします。

手順

1. Web ブラウザに、Deep Discovery Email Inspector サーバの IP アドレスとポート番号 `4459` を入力します。

   `https://<ターゲットサーバの IP アドレス>:4459`

2. 次のいずれかを実行します。

   - ローカルユーザアカウントを使用してログオンするには:

     a. ログオンアカウント情報 (ユーザ名とパスワード) を指定します。

     次の表は、認証方法に応じたログオンユーザ名の形式を示しています。

認証方法	ログオン名形式
Active Directory	次のいずれかの形式のドメインアカウント情報: • ユーザプリンシパル名 (UPN) 例: `user1@example.com` • 下位ログオン名 例: `example\user1`

認証方法	ログオン名形式
• SMTP • OpenLDAP • Domino	有効なメールアドレス

b. [ログオン] をクリックします。

- シングルサインオンでログオンするには:

a. ドロップダウンリストからサービス名を選択します。

b. [シングルサインオン (SSO)] をクリックします。

組織のログオンページが自動的に表示されます。

c. 画面の指示に従ってアカウントの認証情報を入力し、Deep Discovery Email Inspector の管理コンソールにアクセスします。

隔離されたメッセージを表示する

ユーザは自分のアカウントで Deep Discovery Email Inspector によりスパムメール/グレーメールと見なされた隔離メールメッセージのリストを表示できます。

エンドユーザメール隔離の管理コンソールにアクセスして、[隔離メッセージ] 画面を表示します。

詳細については、312 ページの「エンドユーザメール隔離の管理コンソールにアクセスする」を参照してください。

次の表は、各フィールドの詳細を示しています。

フィールド	説明
▶	メッセージサイズ、メッセージ ID、添付ファイル名、およびメッセージの内容 (最初の 2K 分) など、メッセージに関する詳細情報を表示します。
送信者	検出されたメッセージの送信者メールアドレスを表示します。

フィールド	説明
受信者	検出されたメッセージの受信者メールアドレスを表示します。
メールの件名	不審メールメッセージの件名を表示します。
検出	不審メールメッセージを検出した日時を表示します。

次のいずれかの処理を実行して、隔離メッセージを管理できます。

- 隔離解除: 1 つ以上のメッセージを選択して [隔離解除] をクリックすると、選択したメッセージが隔離解除されます。
- 隔離解除して送信者を承認: 1 つ以上のメッセージを選択して [隔離解除して送信者を承認] をクリックすると、選択したメッセージが隔離解除され、送信者のメールアドレスが承認済み送信者リストに追加されます。
- 削除: 1 つ以上のメッセージを選択して [削除] をクリックすると、選択したメッセージが隔離フォルダから削除されます。

重要

- Deep Discovery Email Inspector では、隔離解除したメッセージを再処理せずに本来の受信者に直接送信します。
- 隔離解除されたメッセージを検索せずに直接配信できるようにするには、[ユーザメール隔離アクセス] 画面で [隔離解除したメッセージを再処理せずに直接配信する] を選択します。

  詳細については、305 ページの「ユーザ隔離アクセスを設定する」を参照してください。
- 削除したメッセージは回復できません。

承認済み送信者を追加する

エンドユーザメール隔離の管理コンソールで承認済み送信者リストを設定して、スパムメールの誤検出を減らすことができます。

注意

承認済み送信者リストはブロックする送信者リストよりも優先されます。ブロックする送信者リストと承認済み送信者リストの両方に送信者の IP アドレスが記載されている場合、Deep Discovery Email Inspector ではその送信者からのメッセージをブロックしません。

詳細については、284 ページの「ブロックする送信者リスト」を参照してください。

手順

1. エンドユーザメール隔離の管理コンソールにアクセスします。

   詳細については、312 ページの「エンドユーザメール隔離の管理コンソールにアクセスする」を参照してください。

2. [承認済み送信者] タブをクリックします。

3. リストにエントリを追加するには、テキストフィールドにメールアドレスを入力して [追加] をクリックします。

   [削除] をクリックすると、選択したエントリをリストから削除できます。

4. [保存] をクリックします。

配布リストの隔離メッセージを表示する

ユーザは自分が所属するメール配布リストで Deep Discovery Email Inspector によりスパムメール/グレーメールと見なされた隔離メールメッセージのリストを表示できます。

手順

1. エンドユーザメール隔離の管理コンソールにアクセスします。

   詳細については、312 ページの「エンドユーザメール隔離の管理コンソールにアクセスする」を参照してください。

2. [配布リスト隔離] タブをクリックします。

   次の表は、各フィールドの詳細を示しています。

フィールド	説明
送信者	検出されたメッセージの送信者メールアドレスを表示します。
受信者	検出されたメッセージの受信者メールアドレスを表示します。
メールの件名	不審メールメッセージの件名を表示します。
検出	不審メールメッセージを検出した日時を表示します。

次のいずれかの処理を実行して、隔離メッセージを管理できます。

- クエリ: 指定した LDAP グループ名に基づいてメッセージがフィルタされます。
- 隔離解除: 1 つ以上のメッセージを選択して [隔離解除] をクリックすると、選択したメッセージが隔離解除されます。
- 削除: 1 つ以上のメッセージを選択して [削除] をクリックすると、選択したメッセージが隔離フォルダから削除されます。

重要

- Deep Discovery Email Inspector では、隔離解除したメッセージを再処理せずに本来の受信者に直接送信します。

  配布リストのメッセージを隔離解除すると、そのメッセージは配布リスト内のすべての受信者に送信されます。

- 隔離解除されたメッセージを検索せずに直接配信できるようにするには、[ユーザメール隔離アクセス] 画面で [隔離解除したメッセージを再処理せずに直接配信する] を選択します。

  詳細については、305 ページの「ユーザ隔離アクセスを設定する」を参照してください。

- 削除したメッセージは回復できません。

メール設定

この項の内容は次のとおりです。

メッセージの配信

Deep Discovery Email Inspector では、ドメインとメールアドレスに基づくルーティングテーブルを 保持します。このルーティングテーブルを 使用して、受信者のドメインまたはメールアドレスが一致するメールメッセージを、指定された送信先サーバ、または指定された MX レコードに一致する送信先サーバにルーティングします。

次の 2 つのメッセージ配信方法があります。

- MX レコードの検索

  Deep Discovery Email Inspector は、指定された MX レコードのクエリを実行し、その MX レコードで識別された送信先サーバにメールメッセージを配信します。

- サーバの指定

  Deep Discovery Email Inspector は、最も優先度の高い送信先サーバにメールメッセージを送信します。そのサーバが利用できない場合は、残りのサーバが優先度に基づいて降順で選択されます。複数の送信先サーバが同じ優先度を持つ場合はランダムに選択されます。

指定されていないドメインやメールアドレス宛てのメールメッセージは、DNS (Domain Name Server) のレコードに基づいてルーティングされます。たとえば、ドメインに「example.com」が含まれ、関連する SMTP サーバが `10.10.10.10` でポート 25 の場合、「example.com」に送信されるすべてのメ

ールメッセージはポート 25 を使用して 10.10.10.10 の SMTP サーバに配信されます。

SMTP 接続を設定する

SMTP 接続を設定して、どの MTA およびメールユーザエージェントにサーバへの接続を許可するかを制御します。

注意

接続制御の設定は、メールリレー設定より優先されます。

手順

1. [管理] > [メール設定] > [ネットワーク接続] の順に選択します。
2. [SMTP 接続] 設定を指定します。

オプション	説明
ポート番号	SMTP サービスのリスニングポートを指定します。
タイムアウト{}分 (非アクティブ状態の経過時間)	タイムアウト値を指定します。
同時接続数	[無制限] または [{}接続まで許可する] をクリックして、接続可能な最大数を指定します。

3. [接続制御] 設定を指定します。
   a. 接続の「拒否リスト」または「許可リスト」を選択します。
      - 「拒否リスト」を設定するには、[次のリストに含まれているコンピュータを除くすべての接続を許可する] を選択します。
      - 「許可リスト」を設定するには、[次のリストに含まれているコンピュータを除くすべての接続を拒否する] を選択します。
   b. オプションを選択後、IP アドレスを指定します。

オプション	説明
コンピュータ別の指定	IPv4 または IPv6 のアドレスを指定し、[>>] をクリックしてリストに追加します。
グループ別の指定	1. IP のバージョンを選択します。 2. [サブネットアドレス] にアドレスを入力します。 3. IPv4 を選択した場合は、[サブネットマスク] を入力します。 4. [>>] をクリックしてリストに追加します。
ファイルからインポート	クリックすると、ファイルから IP リストをインポートします。次のリストは、IP リストのテキストファイルのサンプルコンテンツを示しています。 192.168.1.1 192.168.2.0:255.255.255.0 192.168.3.1:255.255.255.128 192.168.4.100 192.168.5.32:255.255.255.192

4. [Transport Layer Security] 設定を指定します。

   319 ページの「TLS を設定する」を参照してください。

5. [保存] をクリックします。

TLS を設定する

TLS (Transport Layer Security) はインターネット上のホスト間で安全な通信チャネルを提供して、伝送中のデータのプライバシーと整合性を確保します。

TLS の設定の詳細については、335 ページの「Transport Layer Security (TLS)」を参照してください。

注意

Deep Discovery Email Inspector では、TLS 1.2 以前のバージョンがサポートされます。

手順

1. [管理] > [メール設定] > [ネットワーク接続] の順に選択します。
2. ページ下部の [Transport Layer Security] というセクションに移動します。
3. [メール受信に TLS を有効にする] を選択します。

   このオプションを有効にした場合、Deep Discovery Email Inspector は TLS 接続と非 TLS 接続によるメッセージを許可します。
4. [TLS 経由の SMTP 接続のみを許可する] を選択すると、Deep Discovery Email Inspector ではセキュアな受信接続のみを許可します。

   このオプションを有効にした場合、Deep Discovery Email Inspector は TLS 接続によるメッセージのみを許可します。
5. 次のいずれかの横にある [参照] ボタンをクリックします。

オプション	説明
CA 証明書	CA 証明書は、SMTP メールリレーを検証します。ただし、Deep Discovery Email Inspector ではメールリレーを検証せず、TLS 接続の有効化には CA 証明書のみを使用します。
秘密鍵	SMTP メールリレーでは、Deep Discovery Email Inspector の SMTP サーバの公開鍵を使用してランダムな数字を暗号化することでセッションキーを作成します。 次に Deep Discovery Email Inspector の SMTP サーバでは、安全な接続を確立するために、秘密鍵を使用してランダムな数字を復号します。 TLS 接続を有効化するには、この鍵をアップロードする必要があります。

オプション	説明
SMTP サーバ証明書	SMTP メールリレーでは、Deep Discovery Email Inspector SMTP サーバの公開鍵でセッションキーを生成できます。 TLS 接続を有効化するにはこのキーをアップロードします。

6. [メール送信に TLS を有効にする] を選択します。
7. [保存] をクリックします。

メッセージ配信を設定する

次の手順は、ダウンストリームメールサーバへのメッセージ配信を設定する方法を示します。

接続の設定、メッセージ配信設定のインポート、およびメッセージルールの設定の詳細については、316 ページの「メール設定」を参照してください。

Deep Discovery Email Inspector のダウンストリームメールサーバへのメールメッセージ配信を設定します。Deep Discovery Email Inspector では、受信者のドメインまたはメールアドレスを確認し、送信先サーバを特定して、そのメッセージを一致したドメインまたはメールアドレスの次の SMTP ホストに送信します。

手順

1. [管理] > [メール設定] > [メッセージ配信] の順に選択します。
2. [追加] をクリックします。

   [配信プロファイルの追加] 画面が表示されます。
3. 配信プロファイルのステータスを選択します。
4. 受信者のドメインまたはメールアドレスを指定します。ドメインとすべてのサブドメインからのメールメッセージ配信を管理するには、ワイルドカード文字 (*) を入力します。
   - * (すべてのドメインを含める)
   - `example.com` (example.com のみを含める)

- `*.example.com` (example.com とすべてのサブドメインを含める)

5. [送信先サーバ] ドロップダウンリストから、次のいずれかを選択します。
   - MX レコードの検索: MX レコード名を指定し、初期設定以外のポートを使用して接続する場合はポート番号を指定します。
   - サーバの指定: IP アドレスまたは完全修飾ドメイン名、ポート番号、およびメールメッセージを転送する優先度を指定します。

   注意
   - 値が低いと優先度は高くなります。
   - オプションで、[サーバの追加] をクリックして複数の送信先サーバを追加します。
   - 送信先サーバを無効にするには、[優先度] フィールドの横でサーバのチェックマークをクリックします。これによりチェックマークがダッシュ記号に変わります。サーバを再度有効にするには、ダッシュ記号をクリックします。

6. [保存] をクリックします。

メッセージ配信の設定をインポートする

このオプションは、メッセージ配信設定を含む適切な形式の `.xml` ファイルがある場合に使用してください。オプションで、管理コンソールから既存の設定をエクスポートするか、[配信プロファイルのインポート] 画面からサンプル XML をダウンロードしてエクスポートしたファイルに従ってファイルを生成します。

Deep Discovery Email Inspector のダウンストリームメールサーバへのメールメッセージ配信を設定します。Deep Discovery Email Inspector では、受信者のドメインまたはメールアドレスを確認し、送信先サーバを特定して、そのメッセージを一致したドメインまたはメールアドレスの次の SMTP ホストに送信します。

手順

1. [管理] > [メール設定] > [メッセージ配信] の順に選択します。
2. [インポート] をクリックします。

   [配信プロファイルのインポート] 画面が表示されます。
3. [参照] をクリックして、インポートするファイルを指定します。
4. 次のいずれかのオプションを選択します。
   - 既存のプロファイルにマージする: インポートしたプロファイルを現在のメッセージ配信リストに追加します。
   - 既存のプロファイルの置換: すべての既存のプロファイルを XML ファイル内のプロファイルで上書きします。
5. [インポート] をクリックします。

   プロファイルが [メッセージ配信] リストに追加されます。

制限と除外を設定する

Deep Discovery Email Inspector で処理するメールメッセージの制限を設定します。

- 処理に必要なメールメッセージの合計数を減らすことでパフォーマンスを向上
- リレーするメッセージの送信者と受信者のドメインを制限して、Deep Discovery Email Inspector がオープンメールリレーとして機能しないよう防止
- 不明な送信者ドメインまたは送信者 IP アドレスからのメッセージを拒否して、不要なスパムメールメッセージを防止

注意

接続制御の設定は、メールリレー設定より優先されます。

手順

1. [管理] > [メール設定] > [制限および除外] の順に選択します。
2. [メッセージの制限] を設定します。

オプション	説明
最大メッセージサイズ	1〜2047MB の範囲で最大メッセージサイズを指定します。
最大受信者数	受信者数を 1〜99,999 の範囲で指定します。

3. [リレー管理] オプションを指定して、受信メッセージをフィルタします。

注意

- リレー管理設定は、Deep Discovery Email Inspector が MTA モードの場合のみ有効になります。
- メッセージ拒否オプションが有効な場合、Deep Discovery Email Inspector は、許可された送信者リストを一致させてから不明な受信者を確認します。

- 不明な送信者ドメインを拒否します: DNS 検索で一致するドメインがない送信者からのメッセージをブロックするには、このオプションを選択します。
- 不明な IP アドレスを拒否します: リバース DNS 検索で一致する IP アドレスがない送信者からのメッセージをブロックするには、このオプションを選択します。

注意

この機能を有効にすると、エッジ MTA からのすべてのメッセージがブロックされます。

- 不明な受信者を拒否します: 送信者が承認済みリストになく受信者が不明なメッセージをブロックするには、このオプションを選択します。LDAP クエリで結果が見つからない場合、受信者は不明と見なされます。

注意

このオプションを有効にする場合は、許可された受信者のドメインを設定してください。設定しない場合、Deep Discovery Email Inspector によってメッセージがブロックされます。

4. [許可された受信者のドメイン] を指定します。

   次のいずれかを実行します。

   - 単一のドメインを追加します。
     a. ドメイン名を入力します。
     b. [>] をクリックして、エントリを [許可された受信者のドメイン] リストに含めます。
   - ドメインのリストをインポートします。

注意

Deep Discovery Email Inspector では、ドメイン名をテキストファイルからインポートできます。テキストファイルで、1 行に 1 つのメールアドレスのみが記載されていることを確認します。

     a. [ファイルからインポート] をクリックします。
     b. テキストファイルを選択して、[OK] をクリックします。

   新しいエントリが [許可された受信者のドメイン] リストに表示されます。

注意

- 許可された受信者のドメインのリストをエクスポートするには、[エクスポート] をクリックして、テキストファイルをコンピュータに保存します。許可された受信者のドメインの設定を複数の Deep Discovery Email Inspector アプライアンスで 複製するには、対象となるアプライアンスにテキストファイルをインポートします。
- Deep Discovery Email Inspector は、[許可された受信者のドメイン] リストに設定されたドメインの SPF 検証および DKIM 検証をバイパスします。

  詳細については、294 ページの「Sender Policy Framework (SPF) について」および 296 ページの「DomainKeys Identified Mail (DKIM) について」を参照してください。

5. [メッセージリレーの許可] を指定します。
   - Deep Discovery Email Inspector のみ
   - 同じサブネット内のホスト
   - 同じアドレスクラス内のホスト

注意

このオプションを選択すると、Deep Discovery Email Inspector の IP アドレスとホストが同じアドレスクラスとサブネット内に存在するかどうかが確認されます。

- Deep Discovery Email Inspector は、ホストが同じアドレスクラスおよびサブネット内にある場合にのみホスト間のメッセージリレーを許可します。

  例:

  - クラス A: Deep Discovery Email Inspector の IP アドレスは 10.1.2.3 で、ホストの IP アドレスは 10.1.2.x です。

    クラス B: Deep Discovery Email Inspector の IP アドレスは 172.31.2.3 で、ホストの IP アドレスは 172.31.x.x です。

    クラス C: Deep Discovery Email Inspector の IP アドレスは 192.168.10.3 で、ホストの IP アドレスは 192.168.10.x です。

- Deep Discovery Email Inspector は、ホストが同じアドレスクラス内にあるが同じサブネット内にない場合はホスト間のメッセージリレーを許可しません。

  例:

  - クラス A: Deep Discovery Email Inspector の IP アドレスは 10.1.2.3 で、ホストの IP アドレスは 11.2.3.x です。

    クラス B: Deep Discovery Email Inspector の IP アドレスは 172.31.2.3 で、ホストの IP アドレスは 172.32.x.x です。

    クラス C: Deep Discovery Email Inspector の IP アドレスは 192.168.10.3 で、ホストの IP アドレスは 192.168.11.x です。

- 指定の IP アドレス

注意

設定をファイルからインポートするには、[ファイルからインポート] をクリックします。

設定をファイルにエクスポートするには、[エクスポート] をクリックします。

6. [保存] をクリックします。

SMTP グリーティングメッセージを設定する

Deep Discovery Email Inspector により SMTP セッションが確立されるたびに、メールリレーに SMTP グリーティングメッセージが表示されます。

手順

1. [管理] > [メール設定] > [SMTP グリーティング] の順に選択します。
2. テキストボックスにグリーティングメッセージを指定します。
3. [保存] をクリックします。

エッジ MTA リレーサーバ

Deep Discovery Email Inspector をネットワーク内のエッジ MTA として配置しない場合は、外部メールメッセージを内部ネットワークの Deep Discovery Email Inspector にリレーするエッジ MTA サーバを指定できます。

次の表は、[エッジ MTA リレーサーバ] 画面の詳細を示しています。

ヘッダ	説明
IP アドレス/ドメイン	エッジ MTA リレーサーバの IP アドレスまたはドメイン名を表示します。
詳細	エッジ MTA リレーサーバの詳細を表示します。

注意

- Deep Discovery Email Inspector をネットワークのエッジ MTA として配置する場合、送信者の IP アドレスは、そのネットワークに最も近い外部 MTA のパブリック IP アドレスとなります。
- Deep Discovery Email Inspector をネットワークのエッジ MTA として配置しない場合、送信者の IP アドレスは、エッジ MTA リレーサーバに最も近い MTA の IP アドレスとなります。

エッジ MTA リレーサーバを設定する

Deep Discovery Email Inspector がネットワークのエッジ MTA として配置されていない場合は、エッジ MTA リレーサーバを設定します。

注意

最大 256 のエッジ MTA リレーサーバを設定できます。

手順

1. [管理] > [メール設定] の順に選択します。
2. [エッジ MTA リレーサーバ]をクリックします。
3. [追加] をクリックします。

   [エッジ MTA リレーサーバの追加] 画面が表示されます。
4. 設定を行います。

フィールド	説明
IP アドレス/ドメイン	エッジ MTA リレーサーバの IP アドレスまたはドメイン名を入力します。
説明	エントリの説明を入力します。

5. (オプション) エントリをさらに追加するには、[さらに追加] をクリックして次の操作を実行します。

リストからエントリを削除するには、[処理] 列のアイコン ( ) をクリックします。

6. [保存] をクリックします。

   エッジ MTA リレーサーバのリストに新しいエントリが表示されます。

   1 つ以上のエントリを削除するには、エントリを選択して [削除] をクリックします。

内部ドメイン

内部ドメインリストを設定すると、メッセージが受信または送信のどちらであるかを Deep Discovery Email Inspector で特定できるようになります。

送信者アドレスのドメインが内部ドメインリストに存在する場合、Deep Discovery Email Inspector ではその送信者からのメッセージが送信メッセージと見なされ、メッセージの方向に基づいたポリシーが適用されます。

注意

内部ドメインリストにエントリを追加しない場合、Deep Discovery Email Inspector では初期設定ですべてのメッセージが受信メッセージと見なされます。

内部ドメインを追加する

最大 1024 件の内部ドメインを追加できます。

手順

1. [管理] > [メール設定] > [内部ドメイン] の順に選択します。
2. [追加] をクリックします。
3. ドメインを入力します。ドメインのプレフィックスとしてワイルドカード文字 (*) を使用できます。

   たとえば、example.com、sub.example.com、または*.example.com のように入力します。

4. ドメインの追加情報を入力します。
5. (オプション) 備考を入力します。
6. (オプション) さらにドメインを追加するには、[さらに追加] をクリックします。
7. [保存] をクリックします。
8. (オプション) [許可された受信者のドメインを含む] を選択し、[制限および除外] 画面で内部ドメインとして指定した受信者のドメインを設定します。

   詳細については、323 ページの「制限と除外を設定する」を参照してください。
9. [保存] をクリックします。

   ドメインの追加後、次の操作を実行できます。

   - 選択したエントリを削除するには、[削除] をクリックします。
   - すべてのエントリを CSV ファイルでダウンロードするには、[エクスポート] をクリックします。

内部ドメインをインポートする

正しく書式設定された CSV ファイルから内部ドメインをインポートできます。

手順

1. [管理] > [メール設定] > [内部ドメイン] の順に選択します。
2. [インポート] をクリックします。
3. [ファイルの選択] をクリックして、インポートするファイルを指定します。
4. 次のいずれかのオプションを選択します。

   - 現在のリストにマージする:インポートされたエントリを既存の内部ドメインリストに追加します。

- 現在のリストを上書きする:すべてのエントリを CSV ファイル内のエントリで置き換えます。

5. [インポート] をクリックします。

   インポートしたエントリがリストに表示されます。

アドレスの変更

MTA モードの Deep Discovery Email Inspector では、アドレスの変更を設定して次の処理を行うことができます。

- メッセージのエンベロープやヘッダの送信者または受信者のアドレスを書き換える
- メールアドレスのドメインを書き換える

注意

- Deep Discovery Email Inspector は、メールアドレスを変更してからポリシーの一致やメッセージ配信を行います。
- Deep Discovery Email Inspector は、アドレスの変更処理についてイベントログを生成しません。

アドレスの書き換えを設定する

Deep Discovery Email Inspector でアドレスの書き換えを設定して、メールメッセージの受信者または送信者のアドレスを配信前に変更します。アドレスの書き換え機能を使用すると、たとえば、特定のメッセージを別のメールホストに再ルーティングしたり、あるユーザ名を別のユーザ名にマッピングしたりできます。

注意

- Deep Discovery Email Inspector は、メールメッセージを検索し、書き換えられたメールアドレスに基づいてポリシールールを適用します。
- Deep Discovery Email Inspector は、メールアドレスを変更する前に、メールの送信、送信者フィルタ、および送信者の認証を行います。

メールアドレス全体またはアドレスのドメイン部分のみを置き換えるように書き換えルールを設定できます。次の図にいくつかの例を示します。

元のアドレス	新しいアドレス
test@example.com	myname@mydomain.com
test1@example.com	test2@example.com
test@test.com	test@example.com

手順

1. [管理] > [メール設定] > [アドレスの変更] の順に選択します。

   [アドレスの書き換え] 画面が表示されます。

2. [アドレスの書き換えを有効にする] を選択して、この機能を有効にします。
3. 一致させる送信者アドレスと受信者アドレスの場所を選択します。
4. アドレスの書き換えルールを 1 つ以上設定します。次のいずれかを実行します。
   - ファイルからルールをインポートするには、[インポート] をクリックし、ルール設定を含む CSV ファイルを選択します。
   - ルールを手動で追加するには、次の手順を実行します。
     a. 元のメールアドレスを入力します。
     b. 元のメールアドレスを置き換える新しいメールアドレスを入力します。
     c. ルールを適用するアドレスの種類 ([送信者]、[受信者]、または [送信者と受信者]) を選択します。
     d. [追加] をクリックします。

   ルールを 1 つ以上設定したら、次の操作を実行できます。
   - 選択したエントリを削除するには、[削除] をクリックします。
   - 選択したエントリを CSV ファイルにエクスポートするには、[エクスポート] をクリックします。

5. [保存] をクリックします。

メールドメインの書き換えを設定する

アドレスのドメインを書き換えたりアドレスをマスカレードしたりすることで、メールアドレスのドメイン情報を変更し、メールゲートウェイ (Deep Discovery Email Inspector) の背後にあるドメイン内のホストを隠すことができます。アドレスのドメインを書き換えると、メールメッセージが個々のエンドポイントではなくゲートウェイから発信されているように見せることができます。

注意

- Deep Discovery Email Inspector は、メールメッセージを検索し、書き換えられたメールアドレスに基づいてポリシールールを適用します。
- Deep Discovery Email Inspector は、メールアドレスを変更する前に、メールの送信、送信者フィルタ、および送信者の認証を行います。

手順

1. [管理] > [メール設定] > [アドレスの変更] の順に選択し、[ドメインの書き換え] をクリックします。
2. [ドメインの書き換えを有効にする] を選択して、この機能を有効にします。
3. 一致させる送信者アドレスと受信者アドレスの場所を選択します。
4. (オプション) [ユーザ名の除外] で、ドメインの書き換えをバイパスするメールアドレスのユーザ名を 1 つ以上入力します。

   注意

   ユーザ名の除外は、ドメインの除外よりも優先されます。

5. [設定] で、ドメインの書き換えリストと除外リストを設定します。

   ドメイン名を入力し、[書き換えリストに追加] または [除外リストに追加] をクリックします。

6. [保存] をクリックします。

Transport Layer Security (TLS)

TLS (Transport Layer Security) はインターネット上のホスト間で安全な通信チャネルを提供して、伝送中のデータのプライバシーと整合性を確保します。

2 台のホスト (Deep Discovery Email Inspector アプライアンスおよびメールリレー) によって、次の手順で TLS セッションが確立されます。

1. 暗号化リストを送信することによって、送信元ホストが送信先ホストとの安全な接続を要求します。
2. 2 台のホストが接続を確立します。
3. 送信先ホストは 1 つの暗号化を選択し、認証局 (CA) によって署名されたデジタル証明書で応答します。
4. 送信元ホストは信頼される CA 証明書を使用して ID を確認し、公開鍵を使用してメッセージを暗号化することによりセッションキーを生成します。
5. 送信先ホストは対応する秘密鍵を使用してメッセージを復号します。
6. 送信元ホストの ID は、送信先ホストが秘密鍵を使用してメッセージを復号すると、確認されます。
7. TLS セッションが確立され、ホスト間で渡されるメールメッセージが暗号化されます。

ヒント

初期設定では、Deep Discovery Email Inspector は TLS またはメール暗号化を適用しません。また、メールリレーホストの ID を確認しません。受信メールメッセージを暗号化するには、Deep Discovery Email Inspector で TLS を有効化します。

TLS 環境に Deep Discovery Email Inspector を配置する

Deep Discovery Email Inspector で送受信されるメッセージに対して TLS 設定を有効にします。

手順

1. 前提条件を見直します。

   336 ページの「TLS を使用するための前提条件」を参照してください。

2. 着信 TLS を有効にします。

   337 ページの「受信メッセージに対して TLS を設定する」を参照してください。

3. 送信 TLS を有効にします。

   344 ページの「送信メッセージに対して TLS を設定する」を参照してください。

TLS を使用するための前提条件

TLS インフラストラクチャを確立するためには、組織に専用の認証局 (以下、CA) を構築するか、外部 CA によって発行された証明書が必要です。秘密鍵と証明書署名要求は、ネットワーク内の各 SMTP サーバで生成される必要があります。証明書署名要求は、CA が署名する必要があります。

デジタル証明書を入手する

デジタル証明書を入手するには、次のいずれかの処理を実行します。

- 管理コンソールで証明書署名要求 (CSR) を作成し、CA に証明書の署名を要求して、署名された証明書を Deep Discovery Email Inspector にインポートします。
- 管理コンソールで自己署名証明書を作成します。
- CA に公開鍵と秘密鍵のペアおよび証明書を申請し、証明書と鍵ファイルを Deep Discovery Email Inspector にインポートします。

Deep Discovery Email Inspector で証明書署名要求を設定して証明書を管理するには、427 ページの「証明書の管理」を参照してください。

TLS を設定する

管理コンソールを使用して、Deep Discovery Email Inspector で送受信されるメッセージに対して TLS 設定を有効にします。Deep Discovery Email

Inspector が SMTP サーバとして動作する場合は、受信メッセージに TLS を設定します。Deep Discovery Email Inspector が SMTP クライアントとして動作する場合は、送信メッセージに TLS を設定します。

受信メッセージ

Deep Discovery Email Inspector がアップストリーム MTA からメールメッセージを受信する SMTP サーバとして動作する場合は、Deep Discovery Email Inspector で受信するメッセージに TLS を設定します。

次の表は、[受信メッセージ] 画面で実行できるタスクを示しています。

タスク	説明
TLS の設定の追加	[追加] をクリックします。 詳細については、337 ページの「受信メッセージに対して TLS を設定する」を参照してください。
TLS の設定の編集	IP アドレスまたはドメインをクリックします。 詳細については、337 ページの「受信メッセージに対して TLS を設定する」を参照してください。
TLS の設定のインポート	[インポート] をクリックします。 詳細については、339 ページの「TLS の設定をインポートする」を参照してください。
TLS の設定のエクスポート	エントリを 1 つ以上選択して、[エクスポート] をクリックします。すべてのエントリをカンマ区切り値 (CSV) ファイルにエクスポートするには、[すべてエクスポート] をクリックします。 注意 TLS の設定をエクスポートする場合、初期設定のエントリ (アスタリスク「*」で示される) も含めてファイルにエクスポートされます。
TLS の設定の削除	エントリを 1 つ以上選択して、[削除] をクリックします。

受信メッセージに対して TLS を設定する

手順

1. [管理] > [メール設定] > [TLS] の順に選択します。

   [受信メッセージ] 画面が表示されます。

2. 次のいずれかを実行します。

   - [追加] をクリックして新しいエントリを作成します。
   - エントリをクリックします。

3. ステータスオプションを選択します。

4. 対象とするメール送信者の IP アドレス、サブネット、またはドメインを指定します。

   注意

   初期設定のエントリの IP アドレスまたはドメインの設定は変更できません。

5. セキュリティレベルを選択します。

セキュリティレベル	説明
なし	Deep Discovery Email Inspector は指定された IP アドレスまたはドメインに対して TLS を使用しません。
透過的	Deep Discovery Email Inspector は指定された IP アドレスまたはドメインに対する TLS のサポートを宣言し、クライアントは TLS 接続を開始するかどうかを選択できます。
必須	Deep Discovery Email Inspector は指定された IP アドレスまたはドメインに対する通信に TLS を要求します。Deep Discovery Email Inspector とクライアント間の通信は暗号化されます。
検証	Deep Discovery Email Inspector はクライアントに、指定された IP アドレスまたはドメインに対する TLS 接続の開始と、クライアントを識別するために自身の証明書を Deep Discovery Email Inspector に送信することを要求します。

6. 暗号グレードオプションを選択します。

注意

セキュリティレベルに [なし] を選択した場合、このフィールドは有効になりません。

暗号グレード	説明
中	Deep Discovery Email Inspector とクライアント間の通信に、「中」および「強」の暗号化の暗号スイートが使用されます。
高	Deep Discovery Email Inspector とクライアント間の通信に、「強」の暗号化の暗号スイートが使用されます。

7. [保存] をクリックします。

TLS の設定をインポートする

注意

初期設定のエントリ (アスタリスク「*」を使用) をインポートファイルに含めて、設定をアップデートできます。

手順

1. [管理] > [メール設定] > [TLS] の順に選択します。

   [受信メッセージ] 画面が表示されます。

2. [インポート] をクリックします。
3. [選択] をクリックします。
4. IP アドレスまたはドメインのリストを含むカンマ区切り値 (CSV) ファイルを選択します。

   新しいエントリが表に表示されます。

送信メッセージ

Deep Discovery Email Inspector がダウンストリーム MTA にメールメッセージを送信する SMTP クライアントとして動作する場合は、Deep Discovery Email Inspector から送信するメッセージに TLS を設定します。

次の表は、[送信メッセージ] 画面で実行できるタスクを示しています。

タスク	説明
TLS の設定の追加	[追加] をクリックします。 詳細については、344 ページの「送信メッセージに対して TLS を設定する」を参照してください。
TLS の設定の編集	IP アドレスまたはドメインをクリックします。 詳細については、344 ページの「送信メッセージに対して TLS を設定する」を参照してください。
TLS の設定のインポート	[インポート] をクリックします。 詳細については、346 ページの「TLS の設定をインポートする」を参照してください。
TLS の設定のエクスポート	すべてのエントリをカンマ区切り値 (CSV) ファイルにエクスポートするには、[すべてエクスポート] をクリックします。 **注意** TLS の設定をエクスポートする場合、初期設定のエントリ (アスタリスク「*」で示される) も含めてファイルにエクスポートされます。
TLS の設定の削除	エントリを 1 つ以上選択して、[削除] をクリックします。

SMTP の DANE

Deep Discovery Email Inspector は DANE (名前付きエンティティの DNS ベースの認証) をサポートしており、SMTP サーバ ID を検証することで送信メッセージを保護します。

送信メッセージのセキュリティレベルには、[DANE] または [DANE のみ] を指定できます。詳細については、344 ページの「送信メッセージに対して TLS を設定する」を参照してください。

次の表は、DNS レコードと TLSA レコード、および検証結果に基づいて送信メッセージに実行される処理を示しています。

表 8-11. DANE のみ

MX レコード	A レコード	TLSA	証明書検証	DANE 検証	処理
Secure	Secure	Secure	成功	成功	配信
Secure	Secure	Secure	失敗	失敗	遅延 (サーバ証明書が信頼されていない)
Secure	Secure	Insecure	該当なし	失敗	遅延 (DNSSEC に対応していない送信先)
Secure	Secure	NXDOMAIN	該当なし	失敗	遅延 (TLSA レコードなし)
Secure	Secure	Bogus	該当なし	失敗	遅延 (TLSA 検索エラー)
Secure	Insecure	該当なし	該当なし	失敗	遅延 (DNSSEC に対応していない送信先)
Secure	Bogus	該当なし	該当なし	失敗	遅延 (ホスト名またはドメイン名が見つからない)
Insecure	Secure	Secure	成功	失敗	遅延 (DNSSEC に対応していない送信先)

MX レコード	A レコード	TLSA	証明書検証	DANE 検証	処理
Insecure	Secure	Secure	失敗	失敗	遅延 (DNSSEC に対応していない送信先)
Insecure	Secure	Insecure	該当なし	失敗	遅延 (DNSSEC に対応していない送信先)
Insecure	Secure	NXDOMAIN	該当なし	失敗	遅延 (DNSSEC に対応していない送信先)
Insecure	Secure	Bogus	該当なし	失敗	遅延 (DNSSEC に対応していない送信先)
Insecure	Insecure	該当なし	該当なし	失敗	遅延 (DNSSEC に対応していない送信先)
Insecure	Bogus	該当なし	該当なし	失敗	遅延 (ホスト名またはドメイン名が見つからない)
Bogus	該当なし	該当なし	該当なし	失敗	遅延 (ホスト名またはドメイン名が見つからない)

表 8-12. DANE

MX レコード	A レコード	TLSA	証明書検証	DANE 検証	処理
Secure	Secure	Secure	成功	成功	配信
Secure	Secure	Secure	失敗	失敗	遅延 (サーバ証明書が信頼されていない)
Secure	Secure	Insecure	該当なし	失敗	透過的 TLS に戻る
Secure	Secure	NXDOMAIN	該当なし	失敗	透過的 TLS に戻る
Secure	Secure	Bogus	該当なし	失敗	遅延 (TLSA 検索エラー)
Secure	Insecure	該当なし	該当なし	失敗	透過的 TLS に戻る
Secure	Bogus	該当なし	該当なし	失敗	遅延 (ホスト名またはドメイン名が見つからない)
Insecure	Secure	Secure	成功	失敗	透過的 TLS に戻る
Insecure	Secure	Secure	失敗	失敗	遅延 (サーバ証明書が信頼されていない)
Insecure	Secure	Insecure	該当なし	失敗	透過的 TLS に戻る
Insecure	Secure	NXDOMAIN	該当なし	失敗	透過的 TLS に戻る
Insecure	Secure	Bogus	該当なし	失敗	遅延 (TLSA 検索エラー)

MX レコード	A レコード	TLSA	証明書検証	DANE 検証	処理
Insecure	Insecure	該当なし	該当なし	失敗	透過的 TLS に戻る
Insecure	Bogus	該当なし	該当なし	失敗	遅延 (ホスト名またはドメイン名が見つからない)
Bogus	該当なし	該当なし	該当なし	失敗	遅延 (ホスト名またはドメイン名が見つからない)

送信メッセージに対して TLS を設定する

手順

1. [管理] > [メール設定] > [TLS] の順に選択します。
2. [送信メッセージ] をクリックします。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを作成します。
   - エントリをクリックします。
4. ステータスオプションを選択します。
5. 対象とするメッセージ受信者のドメインを指定します。

   注意
   初期設定のエントリのドメイン設定は変更できません。

6. セキュリティレベルを選択します。

セキュリティレベル	説明
なし	Deep Discovery Email Inspector は指定された IP アドレスまたはドメインに対して TLS を使用しません。
透過的	Deep Discovery Email Inspector は指定された IP アドレスまたはドメインに対する TLS のサポートを宣言し、メールサーバは TLS 接続を開始するかどうかを選択できます。
必須	Deep Discovery Email Inspector は指定された IP アドレスまたはドメインに対する通信に TLS を要求します。Deep Discovery Email Inspector とメールサーバ間の通信は暗号化されます。
検証	Deep Discovery Email Inspector はメールサーバに、指定された IP アドレスまたはドメインに対する TLS 接続の開始を要求します。Deep Discovery Email Inspector はクライアントを識別するために自身の証明書をメールサーバに送信します。
DANE	Deep Discovery Email Inspector は最初に DANE を使用してメールメッセージを検証します。DANE 検証が失敗した場合、Deep Discovery Email Inspector はエラーの状態に基づいて、透過的 TLS を使用した接続の保護に戻る、メッセージを遅延キューに追加する、またはメッセージを拒否する、のいずれかを実行します。 詳細については、340 ページの「SMTP の DANE」を参照してください。
DANE のみ	Deep Discovery Email Inspector は DANE を使用してメールメッセージを検証します。DANE 検証が失敗した場合、Deep Discovery Email Inspector はエラーの状態に応じて、メッセージを遅延キューに追加するかメッセージを拒否します。 詳細については、340 ページの「SMTP の DANE」を参照してください。

7. 暗号グレードオプションを選択します。

注意

セキュリティレベルに [なし] を選択した場合、このフィールドは有効になりません。

暗号グレード	説明
中	Deep Discovery Email Inspector と SMTP サーバ間の通信に、「中」および「強」の暗号化の暗号スイートが使用されます。
高	Deep Discovery Email Inspector と SMTP サーバ間の通信に、「強」の暗号化の暗号スイートが使用されます。

8. [保存] をクリックします。

TLS の設定をインポートする

注意

初期設定のエントリ (アスタリスク「*」を使用) をインポートファイルに含めて、設定をアップデートできます。

手順

1. [管理] > [メール設定] > [TLS] の順に選択します。
2. [送信メッセージ] をクリックします。
3. [インポート] をクリックします。
4. [選択] をクリックします。
5. ドメインのリストを含むカンマ区切り値 (CSV) ファイルを選択します。

   新しいエントリが表に表示されます。

統合製品/サービス

Deep Discovery Email Inspector は、次の製品やサービスと統合されます。

- 347 ページの「Trend Vision One」
- 350 ページの「Apex Central」
- 356 ページの「Deep Discovery Director」
- 362 ページの「補助製品/サービス」

- 361 ページの「脅威インテリジェンスの共有」
- 389 ページの「LDAP」
- 392 ページの「SAML 統合」
- 402 ページの「ログ設定」
- 405 ページの「SFTP」
- 406 ページの「Email Encryption」

トレンドマイクロの統合製品

シームレスな統合を実現するために、Deep Discovery Email Inspector と統合するトレンドマイクロ製品は、必須または推奨バージョンを使用してください。

表 8-13. Deep Discovery Email Inspector と統合できるトレンドマイクロ製品およびサービス

製品/サービス	バージョン
Trend Vision One	
Deep Discovery Director - オンプレミスバージョン	• 5.3
Deep Discovery Analyzer	• 7.0 • 6.9
Apex Central	• 2019
Smart Protection Server	• 3.3 • 3.2
TippingPoint Security Management System (SMS)	• 5.4 • 5.3

Trend Vision One

Trend Vision One は検出と対応をエンドポイントを超えて拡張し、より広範な可視性と専門家によるセキュリティ分析を提供することで、より多くの脅

威の検出と早期の迅速な対応を実現します。Trend Vision One により、効果的に脅威に対応し、侵害の重大度と範囲を最小限に抑えることができます。

Deep Discovery Email Inspector は Trend Vision One と統合され、ハイブリッド環境における連携したセキュリティ分析を行うために次のタスクを実行します。

- 不審オブジェクトおよび除外リストを Trend Vision One と同期する
- 分析レポートを内部仮想アナライザから Trend Vision One にアップロードする
- 検出ログを Trend Vision One に転送する

注意

Deep Discovery Email Inspector を Trend Vision One、Deep Discovery Director 3.0 以降、および Trend Micro Apex Central に登録すると、Deep Discovery Email Inspector は次の優先順位で不審オブジェクトおよび除外リストを統合製品と同期します。Trend Vision One、Deep Discovery Director、Apex Central。

Deep Discovery Email Inspector を Trend Vision One と統合する

Deep Discovery Email Inspector は、Trend Vision One と直接統合するか Service Gateway を介して統合できます。

重要

統合設定を行う前に、サポート窓口までお問い合せのうえ、最新の HotFix または Patch を適用してください。

手順

1. Trend Vision One コンソールで、[Point Product Connection] > [Product Connector] の順に選択します。
2. [接続] をクリックします。
3. [製品名] フィールドで、[Deep Discovery Email Inspector] を選択します。

4. リンクをクリックして登録トークンを生成します。
5. Deep Discovery Email Inspector 管理コンソールで使用するために登録トークンをコピーします。
6. [保存] をクリックします。
7. Deep Discovery Email Inspector 管理コンソールで、[管理] > [統合製品/サービス] の順に選択し、[Trend Vision One] をクリックします。
8. Trend Vision One の Product Connector から取得した登録トークンを貼り付けます。
9. Service Gateway を介して Deep Discovery Email Inspector を Trend Vision One と統合するには、次の操作を実行します。
    a. Trend Vision One コンソールで、[Workflow and Automation] > [Service Gateway Management] の順に選択します。使用可能な場合は [Service Gateway Management 2.0] タブをクリックします。
    b. 配置している既存の Service Gateway がない場合は、Service Gateway をインストールします。

       配置手順の詳細については、Service Gateway 仮想アプライアンスの配置に関するオンラインヘルプを参照してください。
    c. Service Gateway の名前をクリックします。
    d. [サービスを管理] をクリックします。
    e. インストールアイコンをクリックしてインストールした 後、[転送プロキシ] サービスを有効にします。
    f. Service Gateway の IP アドレスを記録します。これは Deep Discovery Email Inspector コンソールでの接続設定に必要になります。
    g. Deep Discovery Email Inspector 管理コンソールで、[管理] > [統合製品/サービス] の順に選択し、[Trend Vision One] をクリックします。
    h. [Service Gateway の接続を有効にする] を選択します。
    i. Service Gateway の IPv4 または IPv6 アドレスを指定します。
10. 検出ログを Trend Vision One に送信するには、[検出ログを Trend Vision One に転送する] を選択します。

11. [登録] をクリックします。
12. [接続テスト] をクリックして確認します。

Deep Discovery Email Inspector を Trend Vision One から登録解除する

重要

- Deep Discovery Email Inspector を Trend Vision One から登録解除すると、Trend Vision One から取得した不審オブジェクトリスト内の項目がクリアされます。
- Deep Discovery Email Inspector を Trend Vision One から登録解除した後、再度 Trend Vision One に登録するには、新しい登録トークンを取得する必要があります。

手順

1. [管理] > [統合製品/サービス] の順に選択します。

   [Trend Vision One] タブが表示されます。
2. [登録解除] をクリックします。

   警告画面が表示されます。
3. [登録解除] をクリックして確認します。

Apex Central

Apex Central は、ウイルス対策プログラムおよびコンテンツセキュリティプログラムを、その物理的な場所やプラットフォームにかかわらず一元管理するためのソフトウェア管理ソリューションです。このアプリケーションによって、企業のウイルス対策ポリシーおよびコンテンツセキュリティポリシーの管理が簡素化されます。

注意

Deep Discovery Email Inspector と Apex Central サーバの両方を同じネットワークセグメント内に配置してください。Deep Discovery Email Inspector が Apex Central と同じネットワークセグメントにない場合は、Deep Discovery Email Inspector のポート転送を設定してください。

Apex Central の機能の詳細については、351 ページの「Apex Central の機能」を参照してください。

Deep Discovery Email Inspector で [管理] > [統合製品/サービス] > [Apex Central] タブの順に選択して、次の作業を行います。

- Apex Central サーバに登録します。

  詳細については、353 ページの「Apex Central に登録する」を参照してください。

- Deep Discovery Email Inspector と Apex Central 間の接続ステータスを確認します。

- Apex Central サーバから登録解除します。

  詳細については、355 ページの「Apex Central から登録解除する」を参照してください。

- 不審オブジェクトを Apex Central と同期します。

注意

Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降と Apex Central の両方に登録すると、Deep Discovery Email Inspector は不審オブジェクトリストと除外リストを Deep Discovery Director からのみ同期します。同期のステータスは Deep Discovery Director 管理コンソールで確認できます。

Apex Central の機能

Apex Central には次の機能があります。

表 8-14. Apex Central の機能

機能	APEX CENTRAL の画面
ログデータの集計	ログ集約の設定
不審オブジェクトデータの集計	不審オブジェクト
レポート	• 1 回限りのレポート: 1 回限りのレポート • 予約レポート: 予約レポート
通知	イベント通知
シングルサインオン (SSO)	製品
製品コンポーネントのアップデート	製品
除外	仮想アナライザのオブジェクト

詳細については、「Trend Micro Apex Central 管理者ガイド」を参照してください。

Apex Central のコンポーネント

表 8-15. Apex Central のコンポーネント

コンポーネント	説明
Apex Central サーバ	Apex Central アプリケーションのインストール先コンピュータ。このサーバに Web ベースの Apex Central 製品コンソールが配置されます。
MCP (Management Communication Protocol) エージェント	Apex Central による製品の管理を可能にする、Deep Discovery Email Inspector とともにインストールされるアプリケーション。このエージェントは、Apex Central サーバからコマンドを受信し、それらを Deep Discovery Email Inspector に適用します。また製品からログを収集して、それらを Apex Central に送信します。Apex Central エージェントは Apex Central サーバとは直接通信しません。代わりに、コミュニケータと呼ばれるコンポーネントとやり取りします。
エンティティ	Apex Central コンソールのディレクトリツリーに表示される管理下の製品 (Deep Discovery Email Inspector など)。ディレクトリツリーには管理下のエンティティがすべて 含まれます。

Apex Central に登録する

手順

1. [管理] > [統合製品/サービス] > [Apex Central] の順に選択します。
2. [一般] を設定します。
   - 登録ステータスを確認します。
   - Apex Central の製品ディレクトリで Deep Discovery Email Inspector を識別する名前を入力します。

   ヒント

   ホスト名を使用するか一意で意味のある名前を指定すれば、Deep Discovery Email Inspector を簡単に見分けることができます。
3. [サーバ設定] を設定します。

オプション	説明
サーバアドレス	Apex Central のサーバ FQDN または IP アドレスを入力します。
ポート番号	MCP エージェントで Apex Central との通信に使用するポート番号を入力します。 Apex Central のセキュリティを中または高に設定している場合は、[HTTPS を使用する] を選択します。 中: Apex Central と管理下の製品の MCP エージェントとの間で HTTPS および HTTP 通信を許可します。 高: Apex Central と管理下の製品の MCP エージェントとの間で HTTPS 通信のみを許可します。
ユーザ名とパスワード	ネットワークで認証が必要な場合は、Apex Central で使用する IIS サーバのログオンアカウント情報を入力します。
システムのプロキシ設定を使用	オプションで [システムのプロキシ設定を使用] を選択します。 詳細については、417 ページの「プロキシの設定」を参照してください。

4. (オプション) [Apex Central からの受信接続] を設定します。
   a. NAT デバイスを使用するには、[NAT デバイス経由で接続を受信する] を選択します。
   b. NAT の IP アドレスを入力します。
   c. ポート番号を入力します。
5. (オプション) [不審オブジェクトの同期] で次の操作を実行します。
   a. [不審オブジェクトを Apex Central と同期する] を選択します。
   b. API キーを入力します。

   
   注意
   Apex Central の API キーは、ログオンして取得してください。

   Deep Discovery Email Inspector は、不審オブジェクトのリストを 20 秒ごとに Apex Central と同期し、前回の同期時刻を表示します。

注意

- 不審オブジェクトを同期できるのは 1 つのソースのみです。Deep Discovery Email Inspector で Apex Central との同期を有効にしている場合は、その他の外部ソースから不審オブジェクトを受信することはありません。
- Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降と Apex Central の両方に登録すると、Deep Discovery Email Inspector は不審オブジェクトリストと除外リストを Deep Discovery Director からのみ同期します。同期のステータスは Deep Discovery Director 管理コンソールで確認できます。
- Deep Discovery Director から登録解除した Deep Discovery Email Inspector がまだ Apex Central に登録されている場合は、再度設定を行って、不審オブジェクトを Apex Central と同期する必要があります。
- 外部サンドボックスを使用している場合は、このオプションを選択する前に、不審オブジェクトを Apex Central に送信するように外部サンドボックスが設定されていることを確認してください。

6. [保存] をクリックします。

Deep Discovery Email Inspector が Apex Central に登録されます。

登録を確認するには、Apex Central で [ディレクトリ] > [製品] の順に選択します。

Apex Central から登録解除する

手順

1. [管理] > [統合製品/サービス] > [Apex Central] の順に選択します。
2. [一般] で [登録解除] をクリックします。

注意

Deep Discovery Email Inspector を Apex Central から登録解除するには、このオプションを使用します。登録解除した Deep Discovery Email Inspector は別の Apex Central に登録できます。

Deep Discovery Email Inspector が Apex Central から登録解除されます。

結果を確認するには、Apex Central で [ディレクトリ] > [製品] の順に選択します。

Deep Discovery Director

Trend Micro Deep Discovery Director (以下、Deep Discovery Director) は、Deep Discovery 製品へのアップデート、アップグレード、および仮想アナライザイメージの配信と、Deep Discovery 製品の設定の複製およびログの集約を一元管理する管理ソリューションです。さまざまな組織上およびインフラストラクチャ上の要求に対応するため、Deep Discovery Director には Distributed Mode や Consolidated Mode などの柔軟な配信オプションが用意されています。

詳細については、「Deep Discovery Director 管理者ガイド」を参照してください。

Deep Discovery Email Inspector では、Deep Discovery Director 5.0 以降のバージョンとの統合がサポートされます。

[Deep Discovery Director] 画面には、次の情報が表示されます。

表 8-16. [Deep Discovery Director] のフィールド

フィールド	情報
ステータス	次のアプライアンスのステータスが表示されます。 • 登録されていません:アプライアンスは Deep Discovery Director に登録されていません。 • 登録しています:アプライアンスは Deep Discovery Director に登録されています。 • 登録済み	接続:アプライアンスは Deep Discovery Director に登録され、接続されています。 • 登録済み	接続できません:アプライアンスは Deep Discovery Director に登録されていますが、接続できません。Deep Discovery Director のネットワーク設定が有効であることを確認してください。 • 登録済み	信頼されていないフィンガープリント:アプライアンスは Deep Discovery Director に登録されていますが、接続が中断されました。接続を回復するには、新しいフィンガープリントの有効性を確認して信頼してください。 • 登録を解除しています:アプライアンスは Deep Discovery Director から登録解除されています。
前回の接続	アプライアンスが前回 Deep Discovery Director に接続した時間です。
ホスト名	アプライアンスのホスト名です。
サーバアドレス	Deep Discovery Director サーバのアドレスです。
ポート	Deep Discovery Director のポートです。
API キー	Deep Discovery Director の API キーです。
フィンガープリント (SHA-256)	Deep Discovery Director のフィンガープリントです。
システムのプロキシ設定を使用	システムのプロキシ設定を使用して Deep Discovery Director に接続する場合に選択します。

Deep Discovery Director への登録に関する注意事項

Deep Discovery Director に登録して統合する際は、次のことを考慮してください。

- Deep Discovery Director を統合して仮想アナライザイメージを配信するには、追加のディスク容量が必要です。Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降に登録したら、空きディスク容量の合計が 20%未満になった場合はログを削除するように Deep Discovery Email Inspector を設定します。
- Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降と Apex Central の両方に登録すると、Deep Discovery Email Inspector は不審オブジェクトリストと除外リストを Deep Discovery Director からのみ同期します。同期のステータスは Deep Discovery Director 管理コンソールで確認できます。
- Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降に登録すると、Deep Discovery Director によってエンドユーザメール隔離設定の一元管理が行われます。登録に成功した Deep Discovery Email Inspector では、次の処理が行われます。
  - YARA ルールの設定を Deep Discovery Director から同期し、既存の YARA ルールの設定を上書きする
  - エンドユーザメール隔離の設定を Deep Discovery Director から取得し、管理コンソールでの手動による設定を防止する
  - エンドユーザメール隔離通知の送信を停止する
  - エンドユーザメール隔離コンソールのアクセスを無効にする

詳細については、「Deep Discovery Director 管理者ガイド」を参照してください。

Deep Discovery Director に登録する

次の手順は、Deep Discovery Director への登録方法を示しています。すでに登録している Deep Discovery 製品の接続設定を変更するには、まず登録解除する必要があります。

手順

1. [管理] > [統合製品/サービス] > [Deep Discovery Director] の順に選択します。
2. [接続設定] を設定します。

オプション	説明
サーバアドレス	Deep Discovery Director のサーバアドレスを入力します。
ポート	Deep Discovery Director サーバのポート番号を入力します。 初期設定のポート番号は 443 です。
API キー	Deep Discovery Director の API キーを入力します。 **注意** この情報は Deep Discovery Director の管理コンソールの [ヘルプ] 画面で確認できます。

3. (オプション) Deep Discovery Email Inspector に設定したプロキシ設定を Deep Discovery Director との接続に使用する場合は、[プロキシサーバを使用して接続する] を選択します。

   注意

   この設定は、Deep Discovery Director への登録後に変更できます。

   この設定を Deep Discovery Director から登録解除せずに更新するには、[設定のアップデート] をクリックします。

4. [登録] をクリックします。

   [ステータス] が [登録済み | 接続] に変更されます。

注意

Deep Discovery Director のフィンガープリントを 変更すると、接続が中断され、[信頼する] ボタンが表示されます。接続を回復させるには、Deep Discovery Director のフィンガープリントが 有効であることを確認してから [信頼する] をクリックします。

登録が完了したら、[接続テスト] ボタンが表示されます。[接続テスト] クリックして、Deep Discovery Director への接続をテストします。

重要

Deep Discovery Director を統合して仮想アナライザイメージを配信するには、追加のディスク容量が必要です。Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降に登録したら、空きディスク容量の合計が 20%未満になった場合はログを削除するように Deep Discovery Email Inspector を設定します。

詳細については、448 ページの「ストレージ管理を設定する」を参照してください。

Deep Discovery Director から登録解除する

Deep Discovery Director から登録解除するか、別の Deep Discovery Director に登録し直す場合は事前に、次の手順を実行してください。

手順

1. [管理] > [統合製品/サービス] > [Deep Discovery Director] の順に選択します。
2. [登録解除] をクリックします。

   [ステータス] が [登録されていません] に変更されます。

脅威インテリジェンスの共有

Deep Discovery Email Inspector では、HTTP または HTTPS Web サービスを介して、不審 URL などの脅威インテリジェンスデータを Blue Coat ProxySG デバイスなど他の製品やサービスと共有できます。

注意

Deep Discovery Email Inspector が Apex Central に登録されている場合、Apex Central から同期したユーザ指定不審オブジェクトは共有する脅威インテリジェンスデータに含まれません。

脅威インテリジェンスの共有を設定する

手順

1. Deep Discovery Email Inspector 管理コンソールで、[管理] > [統合製品/サービス] > [脅威インテリジェンスの共有] の順に選択します。
2. [[脅威インテリジェンスの共有] を有効にすると、統合製品/サービスで Deep Discovery Email Inspector の情報を取得できるようになります] を選択します。
3. [条件] で、脅威インテリジェンスのデータファイルに含めるオブジェクトのリスクレベルを選択します。
4. (オプション) 初期設定で、脅威インテリジェンスのデータは HTTPS Web サービス経由で共有されます。HTTP Web サービスを有効にしてデータを共有することもできます。[サーバ設定] で [HTTP を使用して情報を共有 (HTTPS に追加)] を選択して、HTTP ポート番号を指定します。
5. (オプション) [予約設定] で、[予約ファイルを生成] に [有効] を選択してスケジュールを設定します。
6. [保存] をクリックします。
7. [生成] をクリックします。

注意

ファイルが生成されたら、URL をクリックし、脅威インテリジェンスのデータファイルをダウンロードして内容を確認できます。

8. Blue Coat ProxySG デバイスなどの統合製品/サービスを設定して、Deep Discovery Email Inspector から脅威インテリジェンスのデータを取得します。詳細については、統合製品/サービスのドキュメントを参照してください。

補助製品/サービス

脅威を効果的に検出してネットワーク侵入前に阻止するため、仮想アナライザの不審オブジェクトリストを補助製品やサービスに配信できます。

Deep Discovery Email Inspector は、次のソリューションと連携します。

表 8-17. Deep Discovery Email Inspector と連携するソリューション

名前	バージョン
Trend Micro TippingPoint Security Management System (SMS)	SMS 5.3 または 5.4
Check Point Open Platform for Security (OPSEC)	Check Point R80.10
IBM Security Network Protection (XGS)	XGS 5.2
Palo Alto Panorama	PAN-OS 7.0.1
Palo Alto Firewall	PAN-OS 4.1.0

注意

- Deep Discovery Email Inspector が一度にサポートするのは付随する 1 つの製品/サービスのみです。
- Deep Discovery Email Inspector は、ユーザ指定の不審オブジェクトをサポート対象の補助製品やサービスと同期しません。
- 有効な場合、Deep Discovery Email Inspector は選択された不審オブジェクトの種類のリストを 10 分ごとに配信します。

Trend Micro TippingPoint Security Management System (SMS)

Deep Discovery Email Inspector と Apex Central の両方から不審オブジェクトを Trend Micro TippingPoint SMS に送信できます。Deep Discovery Email Inspector では各不審オブジェクトに次のオプション情報を含めて送信します。

- リスクレベル:各不審オブジェクトの重大度
- 製品名:トレンドマイクロ Deep Discovery Email Inspector (設定不可)
- アプライアンスのホスト名:トレンドマイクロ Deep Discovery Email Inspector のホスト名 (設定不可)

Trend Micro TippingPoint Security Management System (SMS) は、レピュテーションフィルタを使用して、レピュテーショングループ全体にブロック、許可、または通知の処理を適用します。レピュテーションフィルタの詳細については、Trend Micro TippingPoint のドキュメントを参照してください。

Trend Micro TippingPoint Security Management System (SMS) の設定

手順

1. Deep Discovery Email Inspector 管理コンソールで、[管理] > [統合製品/サービス] > [補助製品/サービス] の順に選択します。
2. [Trend Micro TippingPoint Security Management System (SMS)] を選択します。
3. [オブジェクトの配信] で [有効] を選択します。
4. [サーバ設定] で次の情報を入力します。
   - サーバ名

     注意

     サーバ名は、補助製品の完全修飾ドメイン名または IPv4 アドレスである必要があります。

   - ユーザ名: 既存の認証情報

- パスワード: 既存の認証情報

表 8-18. 有効な文字セット

	ユーザ名	パスワード
最小文字数	1 文字	1 文字
最大文字数	15 文字	15 文字

5. (オプション) [接続テスト] をクリックします。
6. Deep Discovery Email Inspector からこの製品/サービスにオブジェクト情報を送信するには、次の条件を設定します。
   - オブジェクトの種類:
     - 不審オブジェクト
       - IPv4 アドレス
       - ドメイン

     注意
     オブジェクトを少なくとも 1 つ選択する必要があります。
   - リスクレベル:
     - 高のみ
     - 高および中
     - 高、中、および低
7. [保存] をクリックします。

次の表は、Deep Discovery Email Inspector のデータ列と TippingPoint のレピュテーションデータベースのタグのカテゴリとのマッピングを示しています。

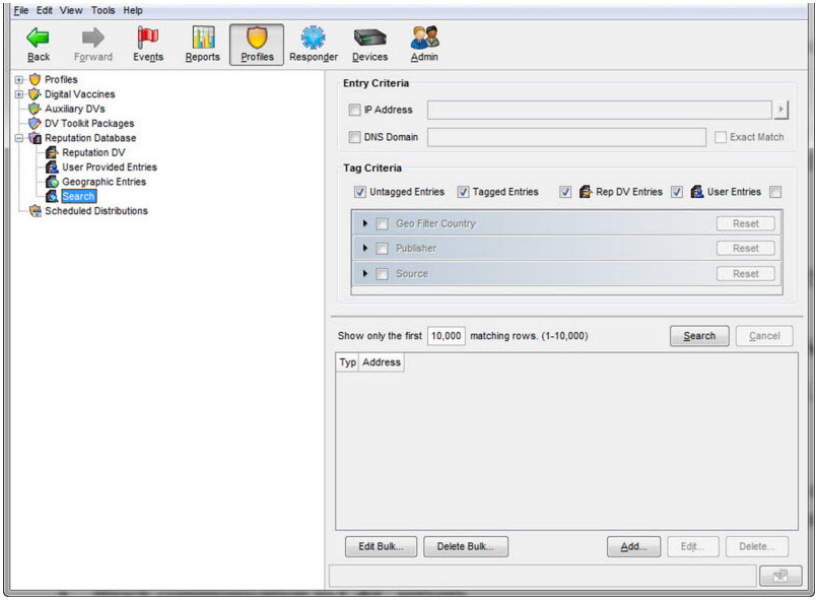
表 8-19. レピュテーションデータベースに追加されるタグのカテゴリ

列	タグのカテゴリ
製品名	Trend Micro Publisher

列	タグのカテゴリ
アプライアンスのホスト名	Trend Micro Source
オブジェクトの種類	Trend Micro Detection Category
リスクレベル	Trend Micro Severity

8. (オプション) 配信された不審オブジェクトを TippingPoint SMS で表示するには、次の手順を実行します。

   a. [Profile] タブで [Reputation Database] > [Search] の順に選択します。



   b. [Entry Criteria] 画面で検索パラメータを入力し、[Search] をクリックします。

   Deep Discovery Email Inspector から配信された不審オブジェクトが表示されます。

Check Point OPSEC (Open Platform for Security)

Check Point OPSEC (Open Platform for Security) は、オープンかつ拡張可能な管理フレームワークを通じてネットワークのセキュリティを管理します。

Deep Discovery Email Inspector は、SAM (Suspicious Activities Monitoring) API を介して OPSEC と統合されます。

SAM API を実装した SAM クライアント (Deep Discovery Email Inspector) は、Check Point ファイアウォールとの通信を行い、SAM サーバとして機能します。Deep Discovery Email Inspector は、SAM API を使用して、特定の接続に対して指定した処理を実行するようファイアウォールに要求します。

たとえば、Deep Discovery Email Inspector は、不正なコマンドを発行しているクライアントやログオンに繰り返し失敗しているクライアントとの接続をブロックするよう Check Point OPSEC に求める場合があります。

Check Point OPSEC (Open Platform for Security) の設定

手順

1. Deep Discovery Email Inspector 管理コンソールで、[管理] > [統合製品/サービス] > [補助製品/サービス] の順に選択します。
2. [Check Point OPSEC (Open Platform for Security)] を選択します。
3. [オブジェクトの配信] で [有効] を選択します。
4. [サーバ設定] で接続の種類を選択します。

> **注意**
>
> ネットワーク設定で、Deep Discovery Email Inspector から Check Point のアプライアンスへの接続が許可されていることを確認します。
>
> Deep Discovery Email Inspector から Check Point のアプライアンスへの接続は、Check Point で設定された保護された接続ポートまたは通常の接続ポートが使用されます。また Deep Discovery Email Inspector では、ポート 18210 を介して Check Point のアプライアンスから証明書を取得します。

[保護された接続] を選択した場合、[OPSEC アプリケーション名] 設定と [SIC ワンタイムパスワード] 設定が表示されます。

5. サーバ名を入力します。

注意

サーバ名は、補助製品の完全修飾ドメイン名または IPv4 アドレスである必要があります。

6. [保護された接続] を選択した場合は、[OPSEC アプリケーション名] と [SIC ワンタイムパスワード] を入力します。

   詳細については、377 ページの「保護された接続を設定する」を参照してください。

注意

Check Point のアプライアンスでワンタイムパスワードがリセットされた場合、新しいワンタイムパスワードはその前のワンタイムパスワードとは別のものにする必要があります。

7. ポート番号を入力します。

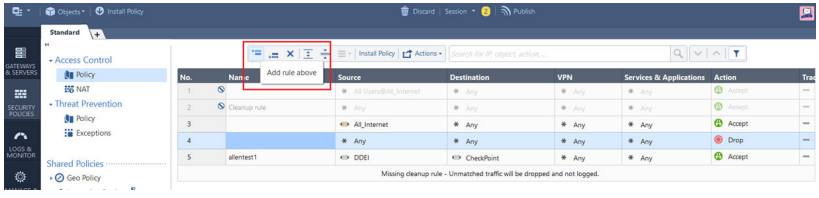
注意

このポート番号は、セキュリティゲートウェイに設定されているポート番号と同じである必要があります。詳細については、375 ページの「セキュリティゲートウェイを事前設定する」を参照してください。

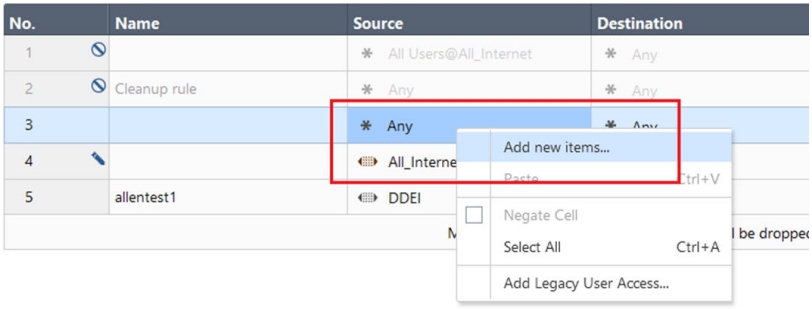
8. (オプション) [接続テスト] をクリックします。
9. Deep Discovery Email Inspector からこの製品/サービスにオブジェクト情報を送信するには、次の条件を設定します。
   - オブジェクトの種類:
     - 不審オブジェクト
       - IPv4 アドレス
   - リスクレベル:

- 高のみ
- 高および中
- 高、中、および低

10. [保存] をクリックします。
11. Check Point のファイアウォールアプライアンスでセキュリティゲートウェイを事前設定します。詳細については、375 ページの「セキュリティゲートウェイを事前設定する」を参照してください。
12. SmartConsole に移動して次の操作を実行し、Deep Discovery Email Inspector から不審オブジェクトが配信されるようにアプライアンスを設定します。
    a. [SECURITY POLICIES] タブで、[Access Control] > [Policy] の順に選択します。

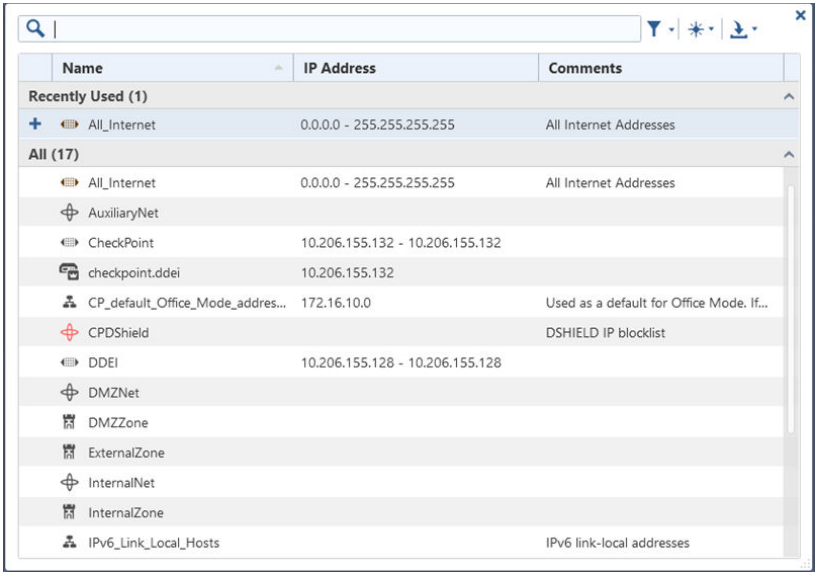


    b. ルールを追加するには、[Add rule above] アイコン ( ) をクリックします。
    c. 新しいポリシーを設定するには、処理を右クリックします。
    d. 処理を [Accept] に変更します。
    e. 送信元を右クリックします。

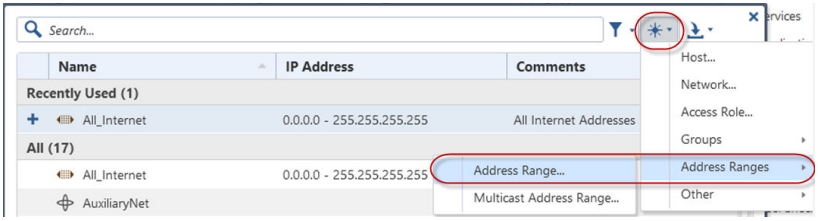


f. [Add new items...] を選択します。

次の画面が表示されます。

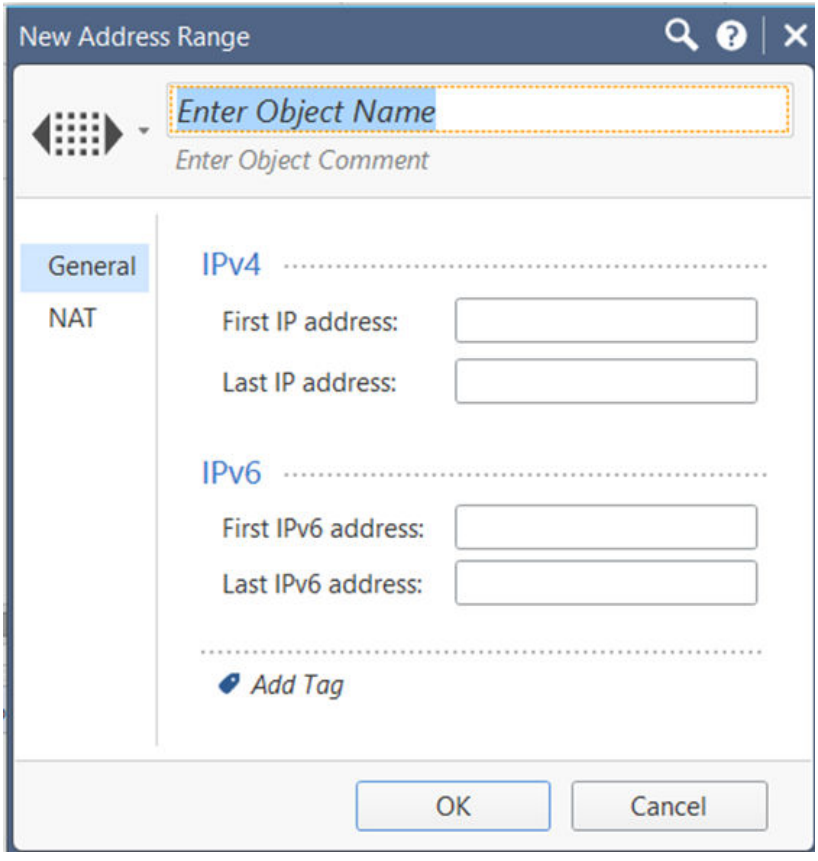


g. 新しいアイコン ( ) をクリックします。



h. [Address Ranges] > [Address Range...] の順に選択します。

[New Address Range] 画面が表示されます。



i. [Enter Object Name] フィールドに「`DDEI`」と入力します。

j. [First IP address] には、Deep Discovery Email Inspector の IP アドレスを入力します。

k. [Last IP address] には、Deep Discovery Email Inspector の IP アドレスを入力します。

l. [OK] をクリックします。

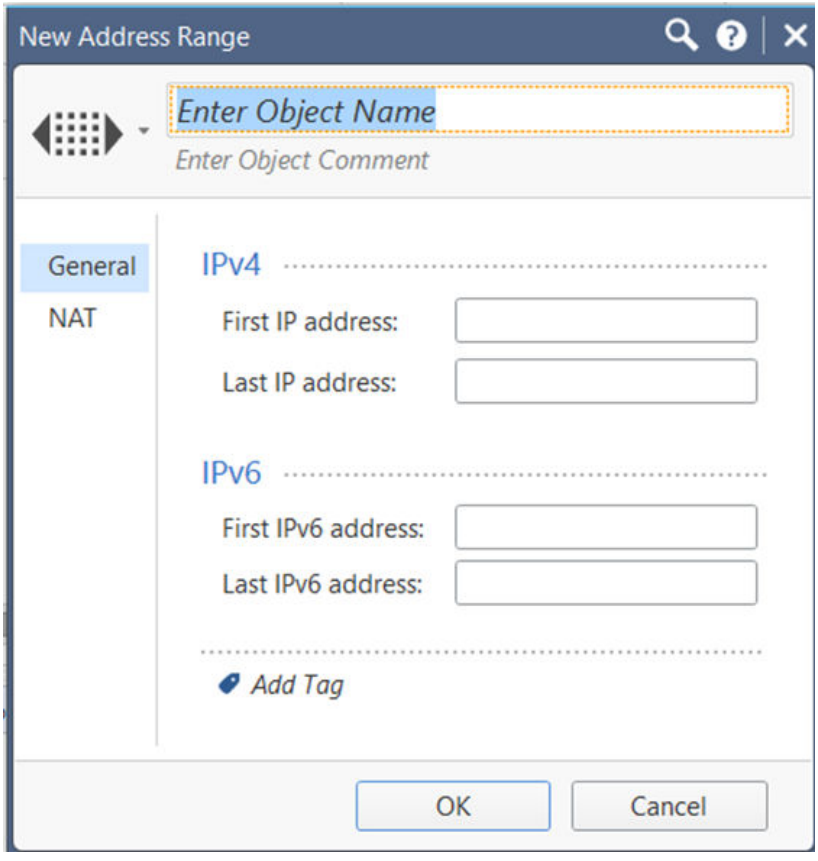
m. 送信先を右クリックします。

n. [Add new items...] を選択します。

o. 新しいアイコン ( ) をクリックします。

p. [Address Ranges] > [Address Range...] の順に選択します。

[New Address Range] 画面が表示されます。



q. [Enter Object Name] フィールドに「`CheckPoint`」と入力します。

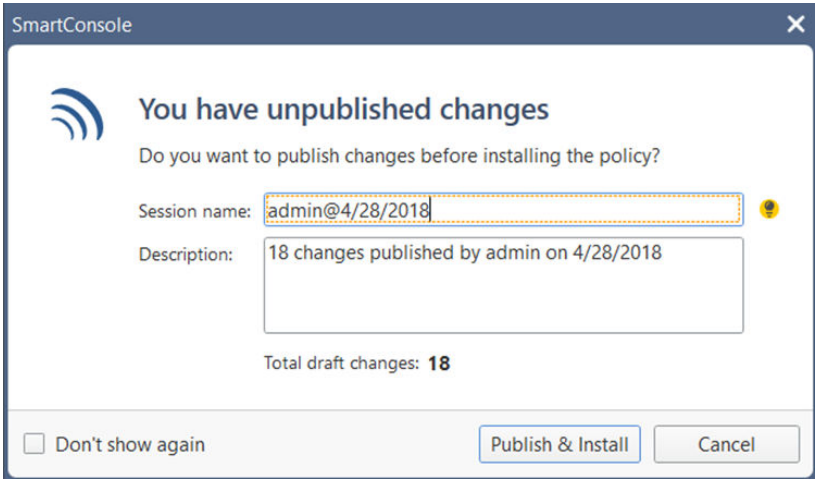
r. [First IP address] には、CheckPoint の IP アドレスを入力します。

s. [Last IP address] には、CheckPoint の IP アドレスを入力します。

t. [OK] をクリックします。

u. [Install Policy] をクリックします。

次の画面が表示されます。



v. [Publish & Install] をクリックします。

ゲートウェイがインストールされます。

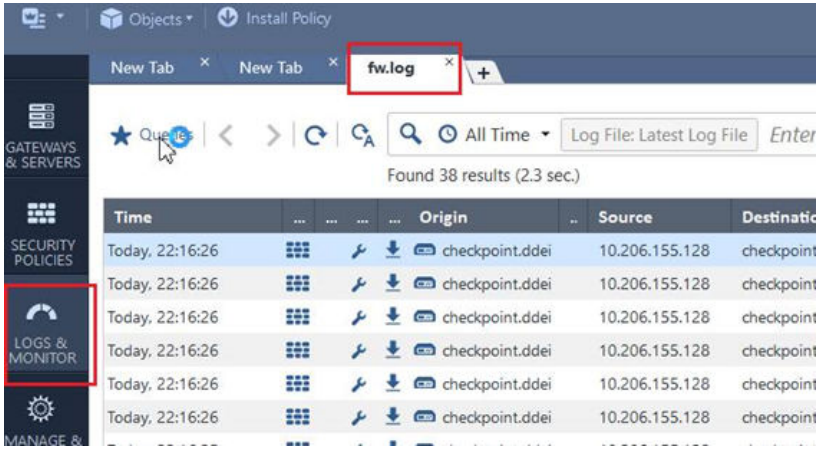
w. [Install] をクリックします。

Check Point のアプライアンスで、Deep Discovery Email Inspector からの不審オブジェクトの受信が有効になります。

13. Deep Discovery Email Inspector の管理コンソールで次の条件を設定して、不審オブジェクトの情報を Deep Discovery Email Inspector からこの製品/サービスに送信します。
    - オブジェクトの種類:
        - 不審オブジェクト
            - IPv4 アドレス
    - リスクレベル:
        - 高のみ
        - 高および中
        - 高、中、および低
14. [詳細設定] で、次の処理のいずれかをクリックします。

- 拒否: パケットが拒否され、パケットが拒否された通信先に通知が送信されます。
- 破棄: パケットは破棄されますが、通信先には通知が送信されません。
- 通知: 定義されたアクティビティについて 通知が送信されますが、そのアクティビティはブロックされません 。

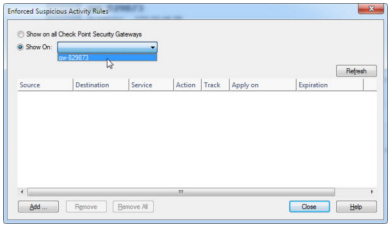
15. [保存] をクリックします。
16. (オプション) [配信] をクリックして、不審オブジェクトを Check Point のアプライアンスにただちに配信します。
17. Deep Discovery Email Inspector から配信された不審オブジェクトを Check Point の SmartView Monitor で表示するには、次の手順を実行します。
    a. Check Point SmartConsole で、[Logs & Monitor] に移動します。
    b. 新しいタブを追加します。



    c. [Tunnels & User Monitoring] をクリックして、SmartView Monitor を開きます。
    d. [Launch Menu] アイコンをクリックして 、[Tools] > [Suspicious Activity Rules] の順にクリックします。

[Enforced Suspicious Activity Rules] 画面が開きます。

e. [Show On] で目的のアプライアンス名を選択します。



f. [Refresh] をクリックします。

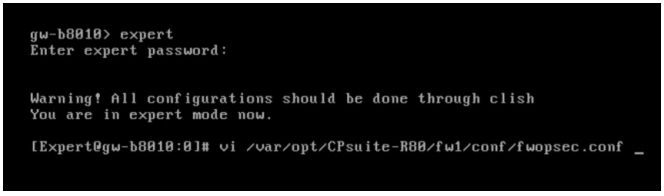
Deep Discovery Email Inspector から配信された不審オブジェクトが表示されます。

セキュリティゲートウェイを事前設定する

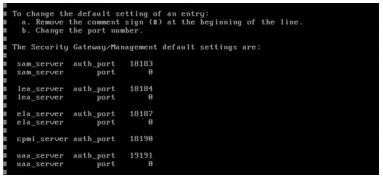
手順

1. Check Point のアプライアンスにログオンします。

2. (オプション) expert モードのパスワードを設定します。
3. パスワードを入力して expert モードに入ります。



4. vi エディタを使用して/var/opt/CPsuite-R80/fw1/conf/fwopsec.conf を開きます。



注意

初期設定のイメージは参照のみを目的としています。実際のファイルの内容は異なる場合があります。

5. fwopsec.conf で、次のいずれかのオプションを使用して SAM の通信モードポートを設定します。

   - 保護された接続 (初期設定ポート)
     - fwopsec.conf の変更は必要ありません。初期設定ポートの 18183 が sam_server auth_port 設定に使用されます。

       注意

       Deep Discovery Email Inspector の [管理] > [統合製品/サービス] > [補助製品/サービス] で、[Check Point Open Platform for Security (OPSEC)] の [ポート] が同じ 18183 に設定されていることを確認してください。

   - 保護された接続 (ユーザ指定ポート)
     - fwopsec.conf で、sam_server auth_port: 18183 のコメント記号 (#) を削除してポート番号を変更します。

注意

`fwopsec.conf` と、Deep Discovery Email Inspector の [管理] > [統合製品/サービス] > [補助製品/サービス] にある [Check Point Open Platform for Security (OPSEC)] の [ポート] に同じポート番号を指定します。

- 通常の接続 (ユーザ指定ポート)
  - `fwopsec.conf` で、`sam_server port: 0` のコメント記号 (#) を削除してポート番号を変更します。

注意

`fwopsec.conf` と、Deep Discovery Email Inspector の [管理] > [統合製品/サービス] > [補助製品/サービス] にある [Check Point Open Platform for Security (OPSEC)] の [ポート] に同じポート番号を指定します。

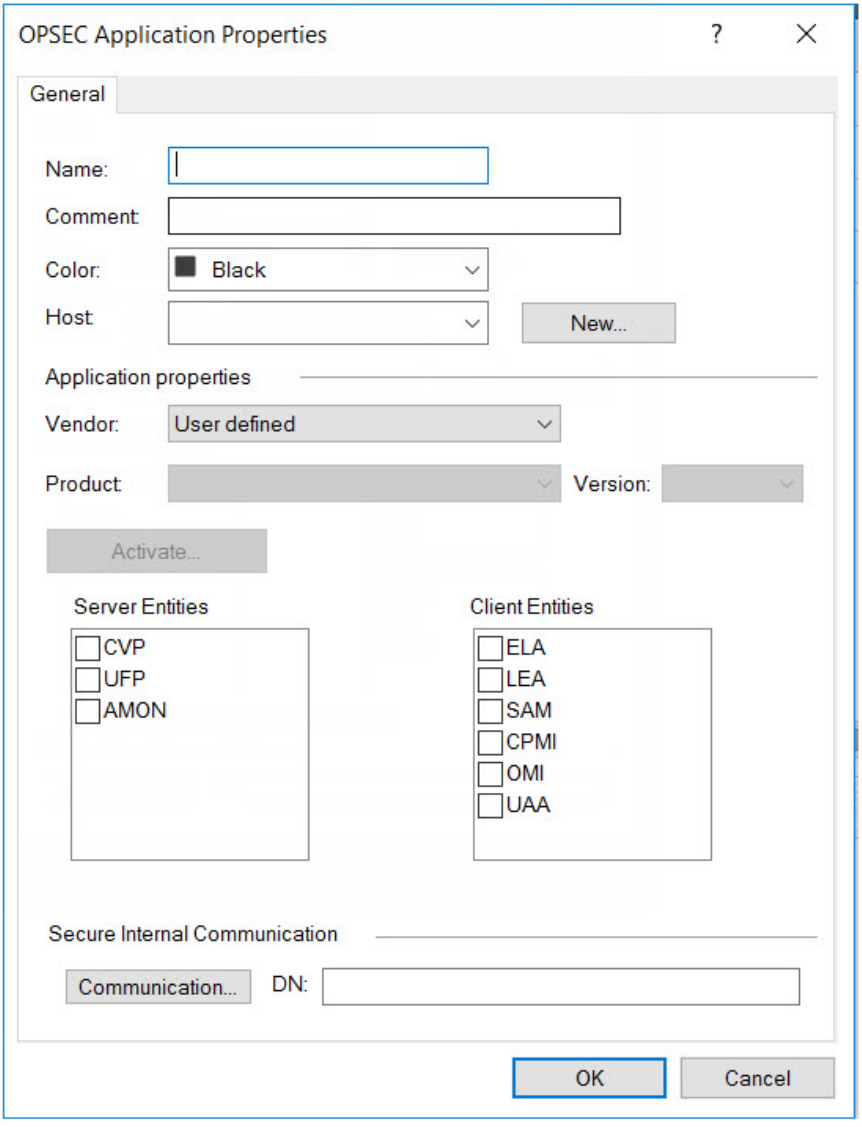
6. `fwopsec.conf` ファイルに変更を行った場合は、`fwopsec.conf` ファイルを保存して Check Point アプライアンスを再起動します。

保護された接続を設定する

手順

1. Check Point SmartConsole を開き、メインメニューアイコン () をクリックします。
2. [New object] > [More object types] > [Server] > [OPSEC Application] > [New Application...] の順に選択します。

[OPSEC Application Properties] 画面が表示されます。



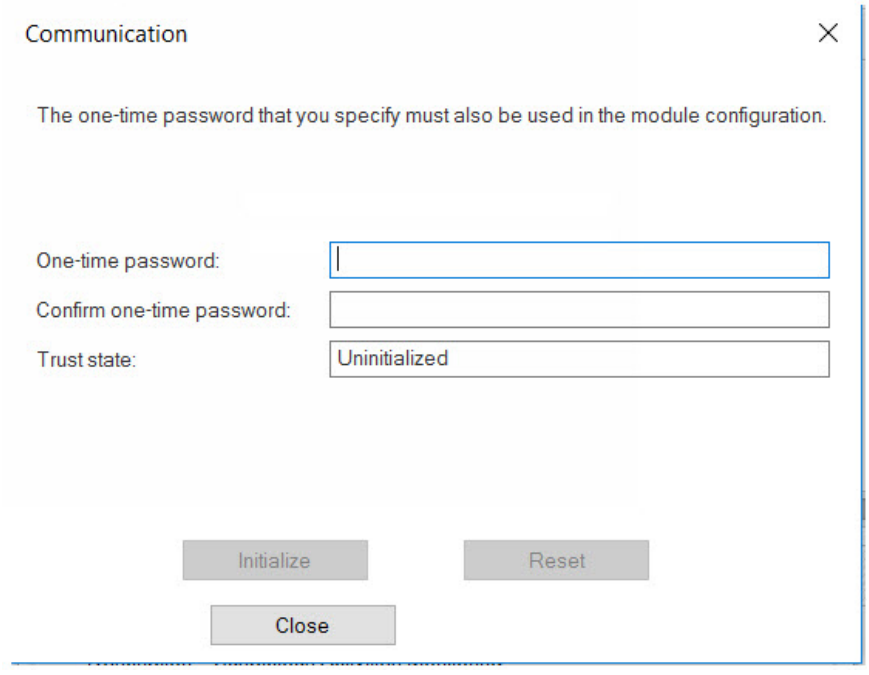
3. [Name] に名前を入力します。

注意

- Deep Discovery Email Inspector では、この名前を [OPSEC application name] に使用します。
- アプリケーション名は 100 文字以下で入力してください。英文字で始まり、英文字、ピリオド、アンダースコア、またはダッシュのみが使用されている必要があります。

4. [Host] でホストを選択します。
5. [Client Entities] で [SAM] を選択します。
6. [Communication...] をクリックします。

[Communication] 画面が表示されます。



7. [One-time password] にパスワードを入力し、同じパスワードを [Confirm one-time password] に入力します。

注意

Deep Discovery Email Inspector では、このパスワードを [SIC one-time password] に使用します。

注意

Check Point のアプライアンスでワンタイムパスワードがリセットされた場合、新しいワンタイムパスワードには、以前とは異なるものを使用する必要があります

8. [Initialize] をクリックします。

   [Trust state] が [Initialized but trust not established] になります。

9. ユーザ定義をインストールします。

   a. メイン画面の [Check Point SmartConsole] で、  をクリックし、[Install database...] を選択します。

      [Install database] 画面が表示されます。

   b. インストールするコンポーネントを選択し、[OK] をクリックします。

      ユーザ定義のインストールが開始されます。

IBM Security Network Protection

IBM Security Network Protection (XGS) の提供する Web サービス API を使用すると、Deep Discovery Email Inspector などのサードパーティ製アプリケーションから不審オブジェクトおよび C&C コールバックアドレスを直接送信できます。IBM XGS では次の機能を実行できます。

- 不正プログラムに感染したホストの隔離
- C&C サーバへの通信のブロック
- 不正プログラムの配信が検出された URL へのアクセスのブロック

Deep Discovery Email Inspector を IBM XGS と統合するには、次のことを実行するように汎用エージェントを設定します。

- 特定のスキーマに従ったアラートの許可
- 一般的な ATP 変換ポリシーに基づく隔離ルールの作成

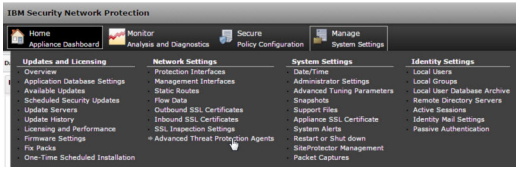
ATP 変換ポリシーにより、IBM XGS に対してメッセージの複数のカテゴリを使用してブロックやアラートなどの異なる処理を実行できます。

IBM Security Network Protection の設定

手順

1. IBM XGS のコンソールで次の手順を実行して、汎用エージェントを設定します。

   a. [Manage System Settings] > [Network Settings] > [Advanced Threat Protection Agents] の順に選択します。

   [Advanced Threat Protection Agents] 画面が開きます。

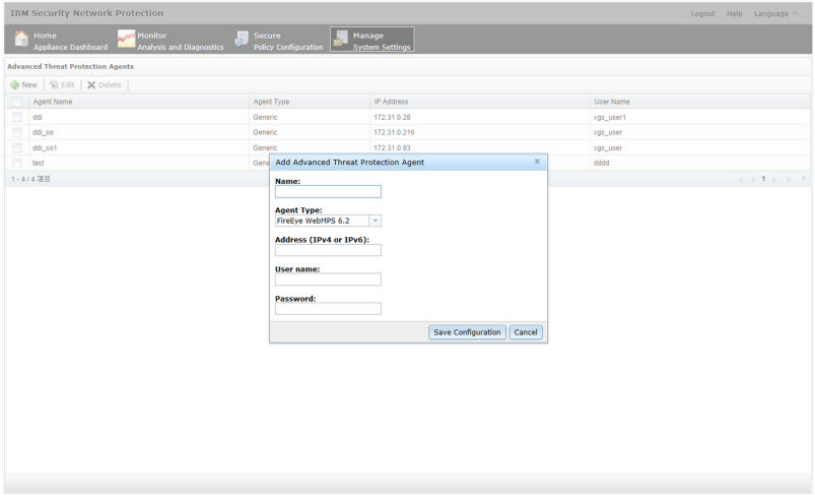
   b. [New] をクリックします。

   c. 次の情報を入力します。

      - Name:名前を入力します
      - Agent Type:[Generic] を選択します
      - Address:Deep Discovery Email Inspector 管理ポートの IPv4 または IPv6 形式の IP アドレス
      - ユーザ名: 既存の認証情報
      - パスワード: 既存の認証情報

      表 8-20. 有効な文字セット

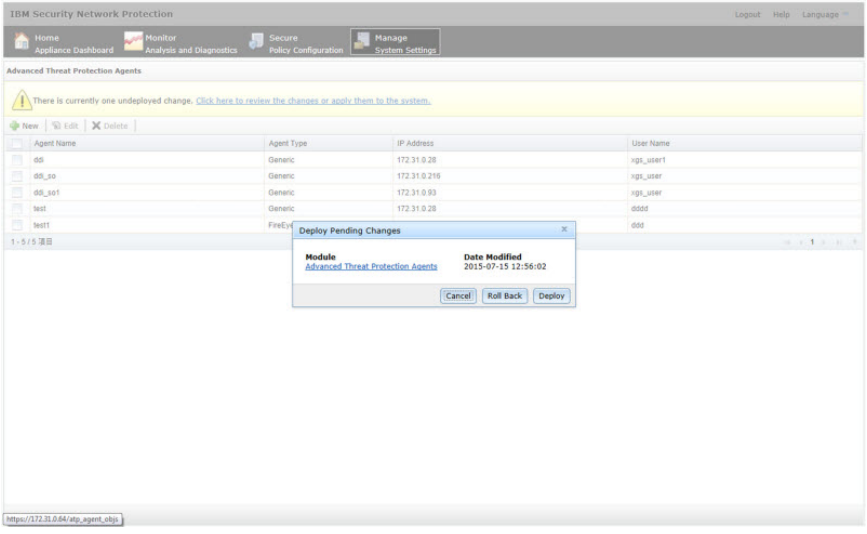
	ユーザ名	パスワード
最小文字数	1 文字	1 文字
最大文字数	15 文字	15 文字



2. [Save Confirmation] をクリックします。

   [Deploy Pending Changes] 画面が開きます。

3. IBM XGS に変更を適用するには、[Deploy] をクリックします。



新しいエージェントが [Advanced Threat Protection Agents] リストに表示されます。

4. Deep Discovery Email Inspector 管理コンソールで、[管理] > [統合製品/サービス] > [補助製品/サービス] の順に選択します。
5. [Configuring IBM Security Network Protection (XGS)] を選択します。
6. [オブジェクトの配信] で [有効] を選択します。
7. [サーバ設定] で次の情報を入力します。
   - サーバ名

     注意
     サーバ名は、補助製品の完全修飾ドメイン名または IPv4 アドレスである必要があります。
   - ユーザ名: 既存の認証情報
   - パスワード: 既存の認証情報

   表 8-21. 有効な文字セット

	ユーザ名	パスワード
最小文字数	1 文字	1 文字
最大文字数	15 文字	15 文字

8. (オプション) [接続テスト] をクリックします。
9. Deep Discovery Email Inspector からこの製品/サービスにオブジェクト情報を送信するには、次の条件を設定します。
   - オブジェクトの種類:
     - 不審オブジェクト
       - IPv4 アドレス
       - URL

注意

オブジェクトを少なくとも 1 つ選択する必要があります。

- リスクレベル:
  - 高のみ
  - 高および中
  - 高、中、および低

10. [保存] をクリックします。
11. (オプション) IBM XGS のコンソールで [Secure Policy Configuration] > [Security Policies] > [Active Quarantine Rules] の順に選択して、Deep Discovery Email Inspector から IBM XGS に送信された不審オブジェクトおよび C&C コールバックアドレスを表示します。

注意

リスクレベルの低い不審オブジェクトは、IBM XGS の [Active Quarantine Rules] には表示されません。Deep Discovery Email Inspector から送信された不審オブジェクトをすべて表示するには、[Security Policy Configuration] > [Advanced Threat Policy] の順に選択し、次のように設定します。

- Agent Type:Generic
- Alert Type:Reputation
- Alert Severity:Low

Deep Discovery Email Inspector から配信された不審オブジェクトおよび C&C コールバックアドレスが表示されます。

Palo Alto Panorama または Firewall

Palo Alto Firewall は、ポート番号、プロトコル、暗号化方式 (SSL や SSH)、または秘匿技術に関係なくアプリケーションを識別して制御します。Panorama™はポリシーやデバイスを一元管理するシステムで、管理者による Palo Alto Firewall の制御を可能にします。

Deep Discovery Email Inspector では、一致条件として Palo Alto Firewall または Palo Alto Panorama の URL カテゴリに IPv4、ドメイン、および URL の不審オブジェクトを送信でき、これによって例外ベースの動作が可能になります。

ポリシーで URL カテゴリを使用するには、次のように設定します。

- Active Directory 内の複数のグループに属するユーザについて、一般的なセキュリティポリシーに対する例外を特定して許可します。

  例:すべてのユーザには不正プログラムやハッキングサイトへのアクセスを拒否しますが、セキュリティグループに属するユーザには許可します。

- ストリーミングメディアカテゴリへのアクセスを許可しますが、サービスの品質ポリシーを適用して帯域幅の使用量を制御します。

- リスクレベルの高い URL カテゴリでのファイルのダウンロードとアップロードを防止します。

  例:未知のサイトへのアクセスは許可しますが、未知のサイトからの実行可能ファイルのアップロードとダウンロードは防止して、不正プログラムの伝播を防ぎます。

- 金融およびショッピングカテゴリへの暗号化アクセスを許可し、その他すべての URL カテゴリへのトラフィックを復号して検査する、SSL 復号ポリシーを適用します。

Palo Alto Panorama および Firewall を設定する

手順

1. Deep Discovery Email Inspector 管理コンソールで、[管理] > [統合製品/サービス] > [補助製品/サービス] の順に選択します。
2. [Palo Alto Panorama または Firewall] を選択します。

3. [オブジェクトの配信] で [有効] を選択します。
4. [サーバ設定] で次の情報を入力します。
   - サーバ名

     注意

     サーバ名は、補助製品の完全修飾ドメイン名または IPv4 アドレスである必要があります。
   - サーバの種類
   - ユーザ名: 既存の認証情報
   - パスワード: 既存の認証情報

   表 8-22. 有効な文字セット

	ユーザ名	パスワード
最小文字数	1 文字	1 文字
最大文字数	15 文字	15 文字

5. (オプション) [接続テスト] をクリックします。
6. Deep Discovery Email Inspector からこの製品/サービスにオブジェクト情報を送信するには、次の条件を設定します。
   - オブジェクトの種類:
     - 不審オブジェクト
       - URL
       - IPv4 アドレス
       - ドメイン

     注意

     オブジェクトを少なくとも 1 つ選択する必要があります。
   - リスクレベル:

- 高のみ
- 高および中
- 高、中、および低

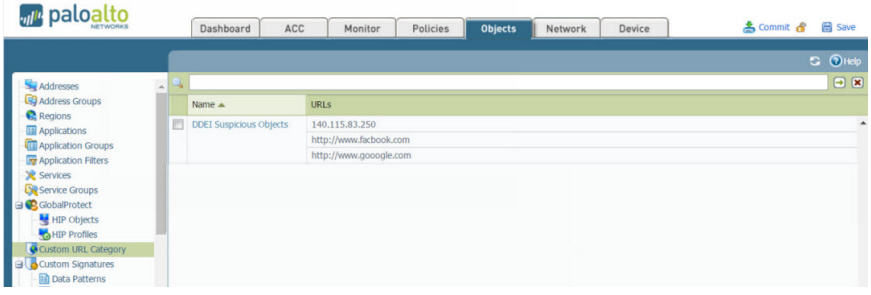
7. (オプション) [詳細設定] で URL カテゴリ名をカスタマイズします。

   URL カテゴリ名は、次の文字を使用して 1〜31 文字で作成します。

   - 大文字 (A〜Z)
   - 小文字 (a〜z)
   - 数字 (0〜9)
   - 特殊文字: - _
   - スペース

8. [保存] をクリックします。

9. (オプション) Palo Alto 製品のコンソールで Deep Discovery Email Inspector から送信された不審オブジェクトを表示するには、[Objects] > [Custom URL Category] (または [Objects] > [Custom Objects] > [URL Category]) の順に選択します。



   Deep Discovery Email Inspector から配信された不審オブジェクトが表示されます。

LDAP

Deep Discovery Email Inspector は、ユーザグループ定義と管理者権限に対応する LDAP サーバと統合されます。

Deep Discovery Email Inspector では、次の種類のディレクトリサーバがサポートされます。

- Windows Server 2016 および 2019 上の Microsoft Active Directory
- Windows Server 2016 および 2019 上の Microsoft Active Directory グローバルカタログ
- IBM Domino 9 および 10
- OpenLDAP

次の表は、[LDAP] 画面で実行できるタスクを示しています。

タスク	説明
LDAP サーバの追加	[追加] をクリックして新しいディレクトリサーバを追加します。 Deep Discovery Email Inspector は、最大 10 個のディレクトリサーバをサポートしています。 詳細については、390 ページの「LDAP サーバを設定する」を参照してください。
LDAP サーバの編集	サーバ名をクリックして設定を編集します。 詳細については、390 ページの「LDAP サーバを設定する」を参照してください。
LDAP サーバの有効化または無効化	[ステータス] 列のボタンを切り替えて、以下を実行します。 • 設定画面で有効にするよう選択した LDAP サーバを有効にします。 • プライマリおよびセカンダリ両方の LDAP サーバを無効にします。
ディレクトリ情報の同期	[すべてを 同期] をクリックして、ディレクトリ情報をすべての LDAP サーバと同期します。
ディレクトリサーバの削除	[削除] をクリックして、選択したエントリを 1 つ以上削除します。

LDAP サーバを設定する

手順

1. サーバ管理者から LDAP との統合設定に必要な情報を取得します。
2. [管理] > [統合製品/サービス] > [LDAP] の順に選択します。
3. 次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを追加します。
   - 名前をクリックしてサーバ設定を変更します。
4. サーバの種類を選択します。
5. プライマリサーバとセカンダリサーバのいずれかまたは両方を有効にするように選択します。
6. サーバを設定します (サーバアドレス、アクセスプロトコル、およびポート番号)。

   注意

   次の初期設定のポートを使用することをお勧めします。

   - Microsoft Active Directory、Domino、または OpenLDAP の場合:
     - SSL: 636
     - STARTTLS: 389
   - Microsoft Active Directory グローバルカタログの場合:
     - SSL: 3269
     - STARTTLS: 3268
7. LDAP サーバの管理設定を行います。

   次の表に、サポートされる LDAP サーバの種類それぞれに推奨される設定を示します。

LDAP サーバの種類	ユーザアカウント (例)	基本識別名 (例)	認証方法
Active Directory	user1@example.com (UPN)	dc=example, dc=com	• 簡易 • 詳細 (Kerberos 使用)
Active Directory グローバルカタログ	user1@example.com (UPN)	dc=example, dc=com dc=example1, dc=com (固有のドメインが複数存在する場合)	• 簡易 • 詳細 (Kerberos 使用)
OpenLDAP	cn=manager, dc=test1, dc=com	dc=test1, dc=com	簡易
IBM Domino	user1/example	なし	簡易

a. 基本識別名を入力します。

b. メールアドレス属性オプションを選択して、アドレス情報に基づいてポリシー設定を適用します。

c. ユーザ名を入力します。

d. パスワードを入力します。

e. (オプション) 組織で CA 証明書を使用する場合は、[CA 証明書を使用] を選択し、[選択] をクリックして CA 証明書ファイルを指定します。

f. [認証方法] セクションで、[簡易] または [詳細] を選択します。

Active Directory の場合は [詳細] を選択し、必要な設定を行います。

8. (オプション) [接続テスト] をクリックして、LDAP サーバへの接続を確認します。

9. [保存] をクリックします。

SAML 統合

SAML (Security Assertion Markup Language) は、当事者間でのユーザ ID 情報のセキュアなやり取りを可能にするオープンな認証標準です。SAML はシングルサインオン (SSO) をサポートしており、1 回のユーザログインによって複数のアプリケーションとサーバにわたる 操作が可能になります。Deep Discovery Email Inspector で SAML の設定を行うと、組織のポータルにサインインするユーザは、既存の Deep Discovery Email Inspector アカウントなしで Deep Discovery Email Inspector にシームレスにサインインできるようになります。

SAML シングルサインオンでは、SAML メタデータファイルを使用することで、ID プロバイダ (IdP) とサービスプロバイダ (SP) 間の信頼関係が確立されます。ID プロバイダのディレクトリサーバにはユーザ ID 情報が保存されています。サービスプロバイダ (この場合は Deep Discovery Email Inspector) は、ID プロバイダのユーザ ID 情報を使用してユーザの認証と認可を行います。

Deep Discovery Email Inspector は、シングルサインオンに対応する次の ID プロバイダをサポートしています。

- Microsoft Active Directory フェデレーションサービス (AD FS) 4.0 または 5.0
- Okta
- 組織の環境に Deep Discovery Email Inspector のシングルサインオンの設定を行うには、次の手順を実行します。

  1. Deep Discovery Email Inspector の管理コンソールにアクセスして、サービスプロバイダのメタデータファイルを取得します。

     詳細については、393 ページの「サービスプロバイダのメタデータと証明書」を参照してください。

  2. ID プロバイダで次の操作を実行します。

     a. シングルサインオンに必要な設定を行います。

     b. フェデレーションメタデータファイルを 取得します。

     詳細については、397 ページの「Active Directory フェデレーションサービス (AD FS) を設定する」および 395 ページの「Okta を設定する」を参照してください。

3. Deep Discovery Email Inspector で、次の手順を実行します。

   a. ID プロバイダのフェデレーションメタデータファイルをインポートします。

      詳細については、394 ページの「ID プロバイダを設定する」を参照してください。

   b. SAML ユーザグループを作成します。

      詳細については、440 ページの「SAML グループ」を参照してください。

サービスプロバイダのメタデータと証明書

Deep Discovery Email Inspector からサービスプロバイダメタデータを取得して、ID プロバイダに提供します。

[SAML 認証] 画面の [サービスプロバイダ] セクションに、次のサービスプロバイダ情報が表示されます。

- エンティティ ID: サービスプロバイダのアプリケーションを識別します。
- シングルサインオン URL: SAML アサーションの受信と解析を行うエンドポイント URL です (「Assertion Consumer Service」と呼ばれることもあります)。
- シングルサインアウト URL: SAML ログアウトプロセスを開始するエンドポイント URL です。
- 証明書: X.509 形式の暗号化証明書 (検証証明書) です。

[サービスプロバイダ] セクションでは、次の項目をクリックできます。

- メタデータのダウンロード: Deep Discovery Email Inspector のメタデータファイルをダウンロードします。メタデータファイルは、Active Directory フェデレーションサービス (AD FS) の ID プロバイダにインポートできます。
- 証明書のダウンロード: Deep Discovery Email Inspector の証明書ファイルをダウンロードします。証明書ファイルは、Okta の ID プロバイダにインポートできます。
- 証明書の更新: 新しい証明書を Deep Discovery Email Inspector にアップロードします。

Deep Discovery Email Inspector では、X.509 PEM 形式の証明書がサポートされます。

ID プロバイダを設定する

注意

- ID プロバイダを追加する前に、フェデレーションメタデータファイルを ID プロバイダから取得します。
- Deep Discovery Email Inspector では、管理コンソールとエンドユーザメール隔離コンソールに 2 つずつ、最大で 4 つの ID プロバイダを追加できます。

手順

1. [管理] > [統合製品/サービス] > [SAML 認証] の順に選択します。
2. [ID プロバイダ] セクションで、次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを追加します。
   - ID プロバイダ名をクリックして設定を変更します。
3. ステータスオプションを選択して、ID プロバイダの設定を有効または無効にします。
4. ID プロバイダのわかりやすい名前を入力します。
5. 説明を入力します。
6. [選択] をクリックし、ID プロバイダから取得したフェデレーションメタデータファイルを選択します。

   フェデレーションメタデータファイルをインポートした後、ID プロバイダ情報が表示されます。
7. [保存] をクリックします。

Okta を設定する

Okta は、複数の標準に準拠した OAuth 2.0 認証サーバを使用してクラウド ID 管理ソリューションを組織に提供し、シングルサインオンプロバイダとして Deep Discovery Email Inspector へのユーザアクセス管理を可能にします。

ここでは Okta を SAML (2.0) ID プロバイダとして設定し、Deep Discovery Email Inspector で使用する方法について説明します。

Okta の設定を開始する前に、次のことを確認してください。

- サインインプロセスを処理して Deep Discovery Email Inspector 管理コンソールに認証資格情報を提供する、Okta の有効なライセンスを購入している。
- Deep Discovery Email Inspector の管理者として管理コンソールにログオンしている。

手順

1. 管理者権限のあるユーザとして Okta にログインします。
2. 画面右上にある [Admin] をクリックし、 [Applications] > [Applications] の順に選択します。
3. [Add Application] をクリックし、[Create New App] をクリックします。

   [Create a New Application Integration] 画面が表示されます。
4. [Platform] に [Web] を、[Sign on method] に [SAML 2.0] を選択し、[Create] をクリックします。
5. [General Settings] 画面の [App name] に、「Deep Discovery Email Inspector」など Deep Discovery Email Inspector の名前を入力し、[Next] をクリックします。
6. [Configure SAML] 画面で、次を指定します。
   a. [Single sign on URL] フィールドに Deep Discovery Email Inspector のアドレスを入力します。
   b. [Use this for Recipient URL and Destination URL] を選択します。
   c. ご使用のサイトに基づいて、[Audience URI (SP Entity ID)] にオーディエンス URI を指定します。

d. [Assertion Encryption] で [Encrypted] を選択します。

e. [Encryption Certificate] で [Browse files] をクリックし、Deep Discovery Email Inspector から取得した証明書ファイルを選択します。

詳細については、393 ページの「サービスプロバイダのメタデータと証明書」を参照してください。

f. (オプション) Deep Discovery Email Inspector でエンドユーザメール隔離コンソールにアクセスするため、[ATTRIBUTE STATEMENTS (OPTIONAL)] セクションに次の情報を指定します。

- Name: Deep Discovery Email Inspector で設定されている値

注意

ID プロバイダのメールアドレスと Deep Discovery Email Inspector には、同じ要求の値を指定してください。

- Value: 指定した属性の名前

g. [Group Attribute Statements (Optional)] セクションで、次のように指定します。

- Name: DDEI_GROUP
- Filter: Matches regex ^(.*)*$

h. [Next] をクリックします。

7. [Feedback] 画面で [I'm an Okta customer adding an internal app] をクリックし、[This is an internal app that we have created] を選択して、[Finish] をクリックします。

新しく作成した Deep Discovery Email Inspector アプリケーションの [Sign On] タブが表示されます。

8. [Identity Provider Metadata] をクリックし、Okta からメタデータファイルをダウンロードします。

注意

このメタデータファイルを Deep Discovery Email Inspector にインポートします。

9. アプリケーションをグループに割り当て、人をグループに追加します。

   a. [Directory] > [Groups] の順に選択します。

   b. アプリケーションを割り当てるグループをクリックし、[Manage Apps] をクリックします。

      [Assign Applications] 画面が表示されます。

   c. 追加した Deep Discovery Email Inspector を探し、[Assign] をクリックします。

   d. [Manage People] をクリックします。

      [Add People to Groups] 画面が表示されます。

   e. Deep Discovery Email Inspector へのアクセスを許可するユーザを指定し、Deep Discovery Email Inspector グループに追加します。

   f. アプリケーションがユーザとグループに割り当てられていることを確認します。

      アプリケーションをグループに割り当てると、グループ内のすべてのユーザにアプリケーションが自動的に割り当てられます。

   g. 上記手順を繰り返し、必要に応じて他のグループにアプリケーションを割り当てます。

   これで、Okta を使用したシングルサインオンを設定し、必要な SAML グループを Deep Discovery Email Inspector 管理コンソールで作成できます。

Active Directory フェデレーションサービス (AD FS) を設定する

ここでは、Active Directory フェデレーションサービス (AD FS) を使用してフェデレーションサーバを設定し、Deep Discovery Email Inspector と連動させる方法について説明します。

注意

Deep Discovery Email Inspector では、AD FS 4.0 および 5.0 を使用したフェデレーションサーバへの接続がサポートされます。

Active Directory フェデレーションサービス (AD FS) は、Windows Server や Active Directory の技術に関連した要求対応の ID 管理ソリューションを提供します。AD FS では、WS-Trust、WS-Federation、および SAML (Security Assertion Markup Language) の各プロトコルがサポートされます。

AD FS の設定を開始する前に、次のことを確認してください。

- フェデレーションサーバとして 機能する、AD FS 4.0 または AD FS 5.0 を搭載した Windows Server がある。
- Deep Discovery Email Inspector の管理者として管理コンソールにログオンしている。
- Deep Discovery Email Inspector からメタデータファイルを取得している。

手順

1. [スタート] > [すべてのプログラム] > [管理ツール] の順に選択し、AD FS 管理コンソールを開きます。
2. 左側のナビゲーションで [AD FS] をクリックし、右側の [操作] 領域にある [証明書利用者信頼の追加] をクリックします。
3. [証明書利用者信頼の追加ウィザード] 画面の各タブで設定を行います。
   a. [ようこそ] タブで [要求に対応する] を選択し、[開始] をクリックします。
   b. [データ ソースの選択] タブで [証明書利用者についてのデータをファイルからインポートする] を選択し、[参照] をクリックして、Deep Discovery Email Inspector から取得するメタデータファイルを選択します。次に [次へ] をクリックします。
   c. [表示名の指定] タブで、「Deep Discovery Email Inspector」など Deep Discovery Email Inspector の表示名を指定し、[次へ] をクリックします。

d. [アクセス制御ポリシーの選択] タブで、[すべてのユーザーを許可] または [特定のグループを許可] を選択します。[特定のグループを許可] を選択する場合は、[ポリシー] でグループを 1 つ以上選択します。次に [次へ] をクリックします。

e. [信頼の追加の準備完了] タブで [次へ] をクリックします。

f. [完了] タブで [ウィザードの終了時にこの証明書利用者信頼の [要求規則の編集] ダイアログを開く] チェックボックスをオンにし、[閉じる] をクリックします。

[要求規則の編集] 画面が表示されます。

4. [発行変換規則] タブで [規則の追加] をクリックします。

5. [変換要求規則の追加ウィザード] 画面の各タブを設定し、以下の表に示す LDAP 属性の要求規則を設定します。

a. [規則の種類の選択] タブで、[要求規則テンプレート] ドロップダウンリストから [LDAP 属性を要求として送信] を選択し、[次へ] をクリックします。

b. [要求規則の構成] タブの [要求規則名] に要求規則の名前を入力し、[属性ストア] ドロップダウンリストから [Active Directory] を選択します。

c. LDAP 属性に [User-Principal-Name] を選択し、属性の出力方向の要求の種類として [名前 ID] を指定します。

d. [OK] をクリックします。

表 8-23. LDAP 属性

Web コンソール	LDAP 属性	出力方向の要求の種類	必須
管理	User-Principal-Name	名前 ID	はい
エンドユーザメール隔離	User-Principal-Name	名前 ID	はい
エンドユーザメール隔離	E-Mail-Addresses	<ユーザ指定値> 例: EUQ_Email	いいえ

Web コンソール	LDAP 属性	出力方向の要求の種類	必須
エンドユーザメール隔離	Proxy-Addresses	<ユーザ指定値> 例: EUQ_PROXY_Email	いいえ

6. 手順 3d で許可した Active Directory グループごとに設定を行い、要件に基づいて設定をカスタマイズします。

注意

出力方向の要求の種類が「`DDEI_GROUP`」に設定されていることを確認してください。

---

a. [規則の追加] をクリックします。

[変換要求規則の追加ウィザード] 画面が表示されます。

b. [規則の種類の選択] タブで、[要求規則テンプレート] ドロップダウンリストから [グループ メンバーシップを要求として送信] を選択し、[次へ] をクリックします。

[要求規則の構成] タブが表示されます。

c. [要求規則名] に Active Directory グループの名前を入力します。

d. [ユーザーのグループ] で [参照] をクリックし、Active Directory グループを選択します。

e. [出力方向の要求の種類] に「`DDEI_GROUP`」と入力します。

f. [出力方向の要求の値] に Active Directory グループの名前を入力します。

g. [適用]→[OK] の順にクリックします。

表 8-24. グループメンバーシップの規則

要求規則名	ユーザー グループ	出力方向の要求の種類	出力方向の要求の値
<ユーザ指定の規則名>	<AD FS のユーザグループ名>	DDEI_GROUP	<ユーザ指定値>  注意 この値は、Deep Discovery Email Inspector で設定する SAML グループ名と同じである必要があります。

7. [適用]→[OK] の順にクリックします。

AD FS を介したシングルサインオンについてエンドポイントを設定する

Active Directory フェデレーションサービス (AD FS) を介したシングルサインオンを使用して Deep Discovery Email Inspector にアクセスするには、Deep Discovery Email Inspector とフェデレーションサーバの 両方を信頼するように各エンドポイントの Web ブラウザを設定します。

Web ブラウザの設定は、手動でもグループポリシーを介しても実行できます。

Windows 10 を実行するエンドポイントでの手順を以下に示します。この手順は、Windows のバージョンによって異なる可能性があります。

手順

1. エンドポイントで、[スタート] メニューから [コントロール パネル] を開きます。
2. [ネットワークとインターネット] > [インターネット オプション] の順にクリックします。

   [インターネットのプロパティ] 画面が表示されます。
3. [セキュリティ] タブをクリックします。
4. [ローカル イントラネット] を選択し、[サイト] をクリックします。
5. [詳細設定] をクリックします。
6. [この Web サイトをゾーンに追加する] フィールドにアカウントフェデレーションサーバの FQDN または IP アドレスを入力し、[追加] をクリックします。
7. 手順 6 を繰り返して、Deep Discovery Email Inspector の FQDN または IP アドレスを [Web サイト] リストに追加します。
8. [閉じる] をクリックします。
9. [OK] をクリックします。
10. [OK] をクリックします。

ログ設定

Deep Discovery Email Inspector では、コンポーネントのアップデートやアプライアンスの再起動など、システムイベントをまとめたシステムログが保存されます。[管理] > [統合製品/サービス] > [Syslog] の順に選択して、Syslog サーバにログを送信するように Deep Discovery Email Inspector を設定します。

Deep Discovery Email Inspector では、ログをデータベースに保存した後、最大 3 つの Syslog サーバに送信できます。Syslog サーバを有効にした後に保存されたログのみが、その Syslog サーバに送信されます。それ以前のログは送信されません。

次の表は、[ログ設定] 画面で実行できるタスクを示しています。

タスク	説明
サーバのプロファイルの追加	[追加] をクリックして新しい Syslog サーバのプロファイルを作成します。 詳細については、403 ページの「Syslog サーバを追加する」を参照してください。
既存のサーバのプロファイルの編集	サーバのプロファイル名をクリックして、設定を表示または変更します。 詳細については、404 ページの「Syslog サーバのプロファイルを編集する」を参照してください。
既存のサーバのプロファイルの削除	1 つ以上のサーバプロファイルを選択して [削除] をクリックすると、選択したエントリが表から削除されます。

Syslog サーバを追加する

手順

1. [管理] > [統合製品/サービス] > [Syslog] の順に選択します。

   [ログ設定] 画面が表示されます。

2. [追加] をクリックします。

   [Syslog サーバのプロファイルの追加] の設定が表示されます。

3. Syslog サーバのプロファイル名を入力します。
4. Syslog サーバのホスト名または IP アドレスを入力します。
5. ポート番号を入力します。
6. ログコンテンツを Syslog サーバに転送する際に使用するプロトコルを選択します。

   - TCP
   - UDP
   - SSL

7. Syslog サーバにイベントログを送信する形式を選択します。
   - CEF: Common Event Format (CEF) は、HP ArcSight によって開発されたオープンなログ管理標準です。CEF は、標準のプレフィックス、およびキー/値のペアとして形式化された変数拡張から構成されます。
   - LEEF: Log Event Extended Format (LEEF) は、IBM Security QRadar のカスタマイズされたイベント形式です。LEEF は、LEEF ヘッダ、イベント属性、およびオプションの Syslog ヘッダから構成されます。
   - TMEF: Trend Micro Event Format (TMEF) は、トレンドマイクロ製品でイベント情報のレポートに使用される、トレンドマイクロによって開発されカスタマイズされたイベント形式です。
8. ログに記録するデータの範囲を選択します。
   - 検出
   - アラート
   - 仮想アナライザの分析ログ
   - システムイベント
   - メッセージ追跡
   - 送信者フィルタ /認証
   - MTA イベント
   - Time-of-Click プロテクション
9. [保存] をクリックします。

Syslog サーバのプロファイルを編集する

手順

1. [管理] > [統合製品/サービス] > [Syslog] の順に選択します。

   [ログ設定] 画面が表示されます。
2. Syslog サーバのプロファイルのハイパーリンクをクリックします。

[Syslog サーバのプロファイルの編集] 画面が表示されます。

3. 必要な変更を行います。
4. [保存] をクリックします。

SFTP

仮想アナライザの検出情報をセキュアな FTP (SFTP) サーバに送信するように Deep Discovery Email Inspector を設定できます。

手順

1. [管理] > [統合製品/サービス] > [SFTP] の順に選択します。
2. [検出情報を SFTP サーバに送信] を選択します。
3. 次の設定を行います。

フィールド	説明
認証方法	ドロップダウンリストからオプションを選択します。
IP アドレス/ドメイン	サーバの IP アドレスまたはドメイン名を入力します。
ポート番号	ポート番号を入力します。
ユーザ名	SFTP サーバにアクセスするユーザ名を入力します。
パスワード	SFTP サーバにアクセスするユーザアカウントのパスワードを入力します。
パス	ファイルをアップロードする SFTP サーバ上のディレクトリを指定します。
暗号化	アップロード用に ZIP ファイルを暗号化するためのパスワードを入力します。
証明書	[選択] をクリックしてアップロードする証明書を指定します。

フィールド	説明
パスフレーズ	証明書を保護するためのパスフレーズを入力します。

4. [条件] で、次の検出情報を SFTP サーバに送信することを選択します。
   - 安全なメールメッセージのための調査パッケージ
   - データタイプ (脅威サンプル、元のメールメッセージ、またはレポート)
5. [保存] をクリックします。

Email Encryption

Email Encryption により、Deep Discovery Email Inspector はトレンドマイクロの ID ベース暗号化 (IBE) を使用してメッセージを暗号化します。たとえば、暗号化および復号を行うドメインとして a.com が登録されており、user1@a.com が個人情報を含むメッセージを user2@b.com に送信する場合、Deep Discovery Email Inspector は user2@b.com に送信されるメッセージを暗号化します。個人情報を含むメッセージを暗号化するようにポリシールールを設定できます。

注意

日本語版では Email Encryption 機能をご利用いただけません。

ヒント

Email Encryption を使用する場合、システム時間を NTP サーバと同期して標準の日時データを確認するよう Deep Discovery Email Inspector を設定しておくことをお勧めします。

注意

Deep Discovery Email Inspector を Deep Discovery Director 5.1 以降に登録すると、Deep Discovery Director によって Email Encryption の設定の一元管理が行われます。登録された Deep Discovery Email Inspector は、登録済みメールドメインを含む Email Encryption の設定を Deep Discovery Director から取得し、管理コンソールでの手動による設定を防止します。

重要

Email Encryption が有効な場合、Deep Discovery Email Inspector が暗号化および復号するメールメッセージの数によってはシステムのパフォーマンスが低下することがあります。組織に大量のメールメッセージが存在する場合は、次のことをお勧めします。

- コンテンツフィルタルールを 使用してポリシーを設定し、特定の送信メールメッセージを暗号化する
- メールの暗号化および復号を行う専用の Deep Discovery Email Inspector アプライアンスを設定する

パフォーマンスに応じたサイズの設定については、トレンドマイクロのテクニカルサポートにお問い合わせください。

Deep Discovery Email Inspector で Email Encryption を設定するには、次の操作を実行します。

1. Trend Micro Email Encryption サーバにドメインを 1 つ以上登録します。

   詳細については、408 ページの「Email Encryption のドメインを登録する」を参照してください。

2. メッセージ署名のための初期設定の送信者アドレスを設定します。

   詳細については、410 ページの「メッセージ署名のための初期設定のメール ID を設定する」を参照してください。

3. (オプション) Email Encryption の除外を設定します。

   詳細については、173 ページの「Email Encryption の除外を設定する」を参照してください。

4. [メッセージの暗号化] 処理を指定して、コンテンツフィルタルールまたは情報漏えい対策ルールを設定します。

   詳細については、118 ページの「コンテンツフィルタルールを 設定する」および 124 ページの「情報漏えい対策ルールを設定する」を参照してください。

Email Encryption のドメインを登録する

Email Encryption を機能させるには、1 つ以上のドメインを Trend Micro Email Encryption サーバに登録する必要があります。

注意

- ゲートウェイモジュールの製品ライセンスの有効期限が切れている場合、Deep Discovery Email Inspector では、[Email Encryption] 画面の設定ができなくなり、指定したドメイン所有者のメールアドレスが Trend Micro Email Encryption サーバから削除されます。
- ドメインを初めて Trend Micro Email Encryption サーバに登録する際、Deep Discovery Email Inspector もサーバに登録されます。
- Trend Micro Email Encryption サーバに登録されているドメインを再登録することはできません。
- Trend Micro Email Encryption サーバには最大 300 件のドメインを追加および登録できます。

手順

1. [管理] > [統合製品/サービス] > [Email Encryption] の順に選択します。
2. [ドメインリスト] セクションで、ドメインの登録手順を確認します。
3. [追加] をクリックします。
4. [ドメインの追加] 画面で、次の手順を実行します。
   a. 初めてドメインを追加する場合は、ドメインの所有権を検証する鍵ファイルをトレンドマイクロから受け取るメールアドレスを指定します。

注意

最初のドメインの Trend Micro Email Encryption サーバへの登録が正常に行われた後、[アプライアンス情報] セクションでメールアドレスを更新できます。

b. 入力オプションを選択して次のいずれかを実行し、ドメインを [選択したドメイン] リストに追加します。

- テキストフィールドにドメイン名を入力し、<Enter> キーを押します。
- リストからドメインを選択します。

c. [保存] をクリックします。

注意

- 一度に追加できるドメインは最大 10 件です。
- ドメインとそのサブドメインは一意のエントリとして扱われます。サブドメインは個別にドメインリストに追加する必要があります。
- ワイルドカードを使用してサブドメインを含めることはできません。
- LDAP グループ (「LDAP」で始まるエントリ) をドメインリストに追加することはできません。

5. 自身がドメインリスト内のドメインの登録された所有者である場合は、トレンドマイクロから送信される確認メッセージに返信します。

   トレンドマイクロは、次のメールアドレスにメッセージを送信してドメインの所有権を検証します。

   - postmaster@<domain>
   - webmaster@<domain>
   - ドメインの WHOIS 検索で返されたメールアドレス

6. ドメインが承認されると、トレンドマイクロは指定されたメールアドレスに鍵ファイルを送信します。鍵ファイルをアップロードするには、次の操作を実行します。

a. [ドメインリスト] セクションで、[鍵ファイルのインポート] をクリックします。

b. [ファイルの選択] をクリックし、鍵ファイルを選択します。

c. [インポート] をクリックします。

注意

トレンドマイクロは追加された各ドメインの鍵ファイルを指定されたメールアドレスに送信します。3 営業日以内にドメインの鍵ファイルを含むメッセージを受け取らなかった場合は、販売代理店にお問い合わせください。

ヒント

ドメインを登録したら、[削除] をクリックしてリストからドメインを削除できます。削除したドメインをリストに追加するには、ドメインの登録手順を再度実行する必要があります。

7. ドメインを初めて Trend Micro Email Encryption サーバに登録する場合は、[アプライアンス 情報] にゲートウェイ ID 情報が表示されていることを確認します。

メッセージ署名のための初期設定のメール ID を設定する

初期設定の送信者アドレスは、ドメインリストに存在しない送信者ドメインから送信されたメッセージを Deep Discovery Email Inspector が暗号化する場合に使用されます。これらのメッセージは初期設定の送信者アドレスで署名されます。

手順

1. [管理] > [統合製品/サービス] > [Email Encryption] の順に選択します。
2. [メッセージ署名の初期設定メール ID] で、初期設定の送信者アドレスを入力します。

3. [保存] をクリックします。

システム設定

この項の内容は次のとおりです。

ネットワーク設定

この画面を使用して、ホスト名の設定、Deep Discovery Email Inspector アプライアンスの IPv4 アドレスや IPv6 アドレスの設定、および他のネットワーク設定を行います。

ネットワークを設定する

ネットワークの初期設定は、コマンドラインインタフェース (CLI) を使用して行います。ネットワークインタフェースの 設定を変更するには、管理コンソールを使用します。

手順

1. [管理] > [システム 設定] > [ネットワーク]の順に選択します。
2. ホスト名を指定します。
3. ネットワークを設定します。

オプション	説明

IP アドレスとサブネットマスク/プレフィックス長	管理ネットワーク、カスタムネットワーク、およびメールネットワークのネットワークインタフェースの IP 設定を指定します。
	• 管理ネットワーク: 管理ネットワークは、管理コンソール、SSH 接続、およびトレンドマイクロのアップデートを処理します。メールトラフィックは管理ネットワークを通過します。初期設定で、メールをルーティングするのは管理ネットワークのみです。管理ポート (eth0) のみを使用します。
	• カスタムネットワーク: カスタムネットワークは、サンドボックス分析を処理します。不正なサンプルが他のネットワークに影響を及ぼさないよう、このネットワークは接続制限のない隔離されたネットワークである必要があります。メールネットワークが設定されていない、任意の使用可能なネットワークインタフェース (eth1、eth2、eth3) を使用します。
	• メールネットワーク: メールネットワークは、メールのルーティングと監視を処理します。カスタムネットワークが設定されていないネットワークインタフェースを使用します。
	  • (オプション) BCC モードまたは MTA モードでは、任意の使用可能なネットワークインタフェース (eth1、eth2、eth3) を使用します。
	  • SPAN/TAP モードでは、eth2 または eth3 のネットワークインタフェースを使用します。
	注意
	動作モードの設定については、414 ページの「動作モード」を参照してください。

ゲートウェイ/DNS	ゲートウェイや DNS 設定など、すべてのインタフェースに影響を与える全般的なネットワーク設定を指定します。

4. [保存] をクリックします。

NIC チーミングを設定する

NIC (ネットワークインタフェースカード) チームとは、ソフトウェアベースの仮想ネットワークインタフェースであり、ネットワークインタフェースカードで障害が発生した場合でも、その機能を保持して正常に稼動させ続けることができます (フォールトトレランス)。Deep Discovery Email Inspector では、1 つ以上のネットワークインタフェースカードを 1 つの NIC チームにグループ化できます。

注意

- Deep Discovery Email Inspector がサポートする NIC チーミングのモードは、アクティブ/バックアップのみです。
- 管理ポートは常に eth0 インタフェースにバインドされます。eth0 インタフェースとともにグループ化する場合は、もう一方のネットワークインタフェースがバックアップインタフェースとして 機能します。
- SPAN/TAP モードで使用するには、NIC チーミングに選択していないネットワークインタフェースカードが 3 つ以上必要になります。

手順

1. [管理] > [システム設定] > [NIC チーミング] の順に選択します。
2. [NIC チーミング] セクションで、次の操作を実行します。
   a. [ステータスの切り替え] ボタンで NIC チームを有効にします。
   b. NIC チームに追加するネットワークインタフェースカードを 1 つ以上選択します。

注意

- 1 つの NIC チームにグループ化できるネットワークインタフェースカードは 2 つまでです。
- 1 つのネットワークインタフェースカードは 1 つの NIC チームにのみ属することができます。

3. [保存] をクリックします。

   システムが自動的に再起動します。この処理には時間がかかることがあります。処理が完了すると、管理コンソールに再度アクセスできるようになります。

動作モード

Deep Discovery Email Inspector は、メール転送エージェント (MTA モード) またはアウトオブバンドアプライアンス (BCC モードまたは SPAN/TAP モード) として動作できます。

詳細については、「Deep Discovery Email Inspector インストールガイド」を参照してください。

動作モードを設定するには、[管理] > [システム設定] > [操作モード] の順に選択します。

注意

内部 Postfix サーバを使用してメール通知を BCC または SPAN/TAP モードで送信することはできません。

外部 SMTP サーバの指定の詳細については、419 ページの「通知 SMTP サーバを設定する」を参照してください。

表 8-25. 動作モード

モード	説明
MTA モード (初期設定)	メールトラフィックフロー内のインライン MTA として、不正なメールメッセージをブロックしてネットワークを危険から守ります。受信者には安全なメールメッセージが配信されます。
BCC モード	ネットワーク上の脅威を監視するアウトオブバンドアプライアンスとして、ミラーリングされたトラフィックをアップストリーム MTA から受信します。複製されたすべてのメールメッセージは、配信されずに破棄されます。

モード	説明
SPAN/TAP モード	ネットワーク上の脅威を監視するアウトオブバンドアプライアンスとして、ミラーリングされたトラフィックを SPAN/TAP デバイスから受信します。複製されたすべてのメールメッセージは、配信されずに破棄されます。 [SPAN/TAP モード] を選択する場合は、少なくとも 1 つの監視ルールを追加する必要があります。詳細については、416 ページの「SPAN/TAP モードの監視ルール」を参照してください。 注意 Microsoft Hyper-V にインストールされた Deep Discovery Email Inspector 仮想アプライアンスでは、SPAN/TAP モードはサポートされません。 Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。

次の表は、各動作モードで使用可能な機能を示しています。

機能/サービス	MTA モード	BCC モード	SPAN/TAP モード
メッセージの変更 (タグ、スタンプ、削除、駆除、URL の書き換え、X-Header の追加、ファイルのサニタイズ、メッセージの暗号化など)	あり	なし	なし
メッセージの通知	あり	なし	あり (外部 SMTP サーバを使用)
メッセージの配信	あり	なし	なし
メッセージの隔離	あり	なし	なし
メッセージのアーカイブ	あり	なし	なし
DKIM 署名	あり	なし	なし
エンドユーザメール隔離	あり	なし	なし

機能/サービス	MTA モード	BCC モード	SPAN/TAP モード
送信者の認証 (SPF、DKIM、DMARC)	あり	なし	なし
Email Reputation Services (ERS)	あり	なし	なし
送信者フィルタ	あり	なし	なし
アラート	あり	あり	あり
アラート通知とレポート	あり	あり (外部 SMTP サーバを使用)	あり (外部 SMTP サーバを使用)
キューの管理	あり	あり	あり
Deep Discovery Director の統合	あり	あり	あり

SPAN/TAP モードの監視ルール

SPAN/TAP モードを選択している場合、最大 10 件の監視ルールを追加できます。Deep Discovery Email Inspector でネットワーク上の脅威を監視する SMTP トラフィックを指定します。

監視ルールを追加する

手順

1. [管理] > [システム設定] > [操作モード] の順に選択します。
2. [ルールの追加] をクリックします。

   [SPAN/TAP モードルールの追加] 画面が表示されます。
3. 監視する [送信元 IP アドレス]、[送信先 IP アドレス]、および [SMTP ポート] を入力します。

注意

フィールドが空白の場合、そのオプションのすべての SMTP トラフィックが監視対象になります。

たとえば、[送信元 IP アドレス] が空白の場合、すべての送信元からの SMTP トラフィックが監視対象になります。

4. [追加] をクリックします。

監視ルールを編集する

手順

1. [管理] > [システム設定] > [操作モード] の順に選択します。
2. 監視ルールを選択して、[編集] をクリックします。

   [SPAN/TAP モードルールの編集] 画面が表示されます。
3. 変更を行います。
4. [編集] をクリックします。

監視ルールを削除する

手順

1. [管理] > [システム設定] > [操作モード] の順に選択します。
2. 監視ルールを選択して、[削除] をクリックします。

プロキシの設定

プロキシの設定は次のものに影響します。

- ソフトウェア安全性評価サービス
- コミュニティファイルレピュテーション
- コンポーネントのアップデート

- 製品ライセンスの登録
- スクリプトアナライザエンジン
- Web レピュテーションクエリ
- Web 検査サービス
- Time-of-Click プロテクション
- 機械学習型検索エンジン

手順

1. [管理] > [システム設定] > [プロキシ] の順に選択します。

   [プロキシ] 画面が表示されます。

2. プロキシサーバを設定します。

オプション	説明
チェックボックス	[プロキシサーバを使用してインターネットに接続する] をオンにします。
種類	プロキシのプロトコルを選択します。 • HTTP • SOCKS4 • SOCKS5
サーバアドレス	プロキシサーバホスト名または IP アドレスを指定します。
ポート番号	プロキシサーバがインターネットへの接続に使用するポートを指定します。
ユーザ名	(オプション)プロキシサーバにアクセスするための管理ユーザ名を指定します。
パスワード	(オプション)対応するパスワードを指定します。

3. [保存] をクリックします。

通知 SMTP サーバを設定する

Deep Discovery Email Inspector は、SMTP サーバの設定を使用してアラート通知とレポートを送信します。

SMTP トラフィックの処理の詳細については、316 ページの「メール設定」を参照してください。

手順

1. [管理] > [システム設定] > [SMTP] の順に選択します。
2. [送信者のメールアドレス] を入力します。
3. SMTP サーバの設定を指定します。

オプション	説明
内部 Postfix サーバ	Deep Discovery Email Inspector に埋め込まれた Postfix サーバを SMTP サーバとして使用する場合は、このオプションを選択します。 注意 内部 Postfix は BCC モードおよび SPAN/TAP モードでの動作中は使用できません。
外部 SMTP サーバ	Microsoft Exchange などのスタンドアロン SMTP サーバを指定する場合は、このオプションを選択します。
サーバアドレス	外部 SMTP サーバのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。
ポート番号	外部 SMTP サーバのポート番号を入力します。
接続のセキュリティ	接続に必要な場合はセキュリティプロトコルを選択します。

オプション	説明
SMTP サーバの接続に認証を使用	SMTP サーバの接続に認証が必要な場合は、このオプションを選択します。 注意 • ユーザ名とパスワードを正しく設定してください。認証試行の失敗が最大回数に達すると、外部 SMTP サーバで Deep Discovery Email Inspector からの接続が拒否されることがあります。 • [接続テスト] をクリックすることで、Deep Discovery Email Inspector から外部 SMTP サーバへの接続は確認されますが、SMTP サーバ認証は検証されません。
ユーザ名	認証に使用するユーザ名を入力します。 注意 このオプションは、[SMTP サーバの接続に認証を使用] が選択されている場合のみ使用できます。
パスワード	認証に使用するパスワードを入力します。 注意 このオプションは、[SMTP サーバの接続に認証を使用] が選択されている場合のみ使用できます。

4. [保存] をクリックします。
5. (オプション) 外部 SMTP サーバへの接続をテストするには、次の手順を実行します。
   a. [接続テスト] をクリックします。
   b. 受信者のメールアドレスを入力します。
   c. [OK] をクリックします。

注意

Deep Discovery Email Inspector から受信者にテストメールメッセージは送信されません。

システム時刻を設定する

NTP (Network Time Protocol) はインターネット内のコンピュータのシステム時計を同期します。NTP の設定を行ってサーバの時計を NTP サーバと同期するか、システム時刻を手動で設定します。

手順

1. [管理] > [システム設定] > [時間] の順に選択します。
2. システム時刻を設定します。
   - NTP サーバと同期するには、[アプライアンスの時間を NTP サーバと同期する] を選択して NTP サーバのドメイン名または IP アドレスを指定します。
   - システム時刻を手動で設定するには、[時間を手動で設定] を選択してから、日付と時刻を選択するか、タイムゾーンを選択します。
   - 日付と時刻を別の形式で表示するには、[日時の形式] ドロップダウンリストから形式を選択します。
3. [保存] をクリックします。

SNMP

SNMP (Simple Network Management Protocol) は、管理者の注意を必要とする状況についてネットワークに接続されたデバイスを監視するためのプロトコルです。

SNMP トラップは、このプロトコルをサポートする管理コンソールを使用するネットワーク管理者に対して通知を送信する手段です。

Deep Discovery Email Inspector で [管理] > [システム設定] > [SNMP] タブの順に選択して、次の作業を行います。

- トラップメッセージを送信するようアプライアンスを設定する

  詳細については、422 ページの「トラップメッセージを設定する」を参照してください。

- マネージャ要求を待機するようアプライアンスを設定する

  詳細については、424 ページの「マネージャ要求を設定する」を参照してください。

トラップメッセージを設定する

SNMP トラップメッセージは、管理者の注意を必要とするイベントの発生時に SNMP サーバに送信される通知メッセージです。

手順

1. [管理] > [システム設定] > [SNMP] の順に選択します。
2. [トラップメッセージ] セクションで、[SNMP トラップメッセージの送信] を選択します。
3. トラップメッセージの設定を指定します。

オプション	説明
マネージャサーバのアドレス	マネージャサーバのアドレスを指定します。

オプション	説明
SNMP バージョン	次の SNMP のバージョンを選択します。 • SNMPv1/SNMPv2c • SNMPv3 SNMPv3 を使用する場合は、SNMP サーバを次のように設定します。 Deep Discovery Email Inspector ビルド 3190 (以降) の場合: • コンテキスト名: `""` (初期設定のコンテキスト) • コンテキストエンジン ID: `<Auto>` • (オプション) 認証プロトコル: `SHA` • (オプション) プライバシープロトコル: `AES` Deep Discovery Email Inspector ビルド 3189 (以前) の場合: • コンテキスト名: `""` (初期設定のコンテキスト) • コンテキストエンジン ID: `<Auto>` • (オプション) 認証プロトコル: `HMAC-MD5` • (オプション) プライバシープロトコル: `CBC-DES`
コミュニティ名	コミュニティ名を指定します。
セキュリティモデル	注意 このフィールドは SNMPv3 でのみ使用できます。 次のセキュリティモデルを選択します。 • 認証またはプライバシーなし • 認証 • プライバシーにより認証
ユーザ名	注意 このフィールドは SNMPv3 でのみ使用できます。 ユーザ名を指定します。

オプション	説明
パスワード	注意 このフィールドは SNMPv3 でのみ使用できます。 パスワードを指定します。
プライバシーパスフレーズ	注意 このフィールドは SNMPv3 でのみ使用できます。 プライバシーパスフレーズを指定します。

4. [保存] をクリックします。
5. (オプション) [MIB をダウンロード] をクリックして、MIB (Management Information Database) ファイルをダウンロードします。
   - MIB ファイルを開くと、SNMP プロトコルを使用して監視および管理できるすべてのネットワークオブジェクトを確認できます。また MIB ファイルは、SNMP プロトコルをサポートする管理コンソールにインポートできます。
   - Deep Discovery Email Inspector でサポートされる SNMP オブジェクト ID (OID) のリストについては、527 ページの SNMP オブジェクト ID を参照してください。

マネージャ要求を設定する

SNMP マネージャでは、SNMP プロトコルのコマンドを使用して Deep Discovery Email Inspector のシステム情報を要求できます。

手順

1. [管理] > [システム設定] > [SNMP] の順に選択します。
2. [マネージャ要求] で、[SNMP マネージャからの要求を待機] を選択します。
3. マネージャ要求の設定を指定します。

オプション	説明
デバイスの位置	アプライアンスの場所を指定します。
管理者の連絡先	アプライアンスの管理者の連絡先を指定します。
SNMP バージョン	次の SNMP のバージョンを選択します。 • SNMPv1/SNMPv2c • SNMPv3 SNMPv3 を使用する場合は、SNMP サーバを次のように設定します。 Deep Discovery Email Inspector ビルド 3190 (以降) の場合: • コンテキスト名: `""` (初期設定のコンテキスト) • コンテキストエンジン ID: `<Auto>` • (オプション) 認証プロトコル: `SHA` • (オプション) プライバシープロトコル: `AES` Deep Discovery Email Inspector ビルド 3189 (以前) の場合: • コンテキスト名: `""` (初期設定のコンテキスト) • コンテキストエンジン ID: `<Auto>` • (オプション) 認証プロトコル: `HMAC-MD5` • (オプション) プライバシープロトコル: `CBC-DES`
許可するコミュニティ名	コミュニティ名を 5 つまで指定します。
セキュリティモデル	**注意** このフィールドは SNMPv3 でのみ使用できます。 次のセキュリティモデルを選択します。 • 認証またはプライバシーなし • 認証 • プライバシーにより認証

オプション	説明
ユーザ名	注意 このフィールドは SNMPv3 でのみ使用できます。 ユーザ名を指定します。
パスワード	注意 このフィールドは SNMPv3 でのみ使用できます。 パスワードを指定します。
プライバシーパスフレーズ	注意 このフィールドは SNMPv3 でのみ使用できます。 プライバシーパスフレーズを指定します。
信頼されるマネージャサーバのアドレス	信頼されるマネージャサーバのアドレスを 5 件まで指定します。

4. [保存] をクリックします。
5. (オプション) [MIB をダウンロード] をクリックして、MIB (Management Information Database) ファイルをダウンロードします。
   - MIB ファイルを開くと、SNMP プロトコルを使用して監視および管理できるすべてのネットワークオブジェクトを確認できます。また MIB ファイルは、SNMP プロトコルをサポートする管理コンソールにインポートできます。
   - Deep Discovery Email Inspector でサポートされる SNMP オブジェクト ID (OID) のリストについては、527 ページの SNMP オブジェクト ID を参照してください。

セッションタイムアウトを設定する

Deep Discovery Email Inspector では、一定期間操作を実行していないユーザを管理コンソールから自動的にログアウトします。初期設定のセッションタイムアウト期間は 30 分です。

セッションタイムアウトを設定するには、[管理] > [システム設定] > [セッションタイムアウト] の順に選択し、ドロップダウンリストからオプションを 選択します。

証明書の管理

デジタル証明書とは、サーバまたは Web サイトとクライアントを安全に接続するために使われる電子ドキュメントです。有効な信頼済み証明書は、信頼済みのサーバまたは Web サイトに接続していることをクライアントに保証し、中間者攻撃からネットワークを保護するのに役立ちます。

証明書は、認証局 (CA) の検証プロセスを経て信頼済みとなります。認証局そのものは通常は第三者機関であり、サーバまたは Web サイトとクライアントの両者に信頼されています。

Deep Discovery Email Inspector で証明書を管理することにより、Transport Layer Security (TLS) 環境での安全なコンソールアクセスと SMTP 通信が可能になります。

TLS の詳細については、335 ページの「Transport Layer Security (TLS)」を参照してください。

SMTP 証明書と HTTPS 証明書

SMTP 証明書と HTTPS 証明書は、メッセージ転送エージェント (MTA) などの他のエンティティに対して Deep Discovery Email Inspector を識別します。その信頼性を証明するため、SMTP 証明書または HTTPS 証明書とともに秘密鍵が Deep Discovery Email Inspector に格納されます。

Deep Discovery Email Inspector で証明書を管理することにより、次のサービスの安全な接続が可能になります。

- SMTP クライアント通信
- SMTP サーバ通信

- エンドユーザメール隔離コンソールアクセス
- 管理コンソールアクセス

次の表は、[SMTP 証明書と HTTPS 証明書] 画面で実行できるタスクを示しています。

タスク	説明
自己署名証明書の作成	[追加] をクリックします。 詳細については、428 ページの「証明書署名要求を設定する」を参照してください。
証明書署名要求の作成	[追加] をクリックします。 詳細については、430 ページの「自己署名証明書を設定する」を参照してください。
証明書名の変更と詳細情報の表示	IP アドレスまたはドメインをクリックします。 詳細については、428 ページの「証明書署名要求を設定する」または 430 ページの「自己署名証明書を設定する」を参照してください。
証明書のインポート	[インポート] をクリックします。 詳細については、431 ページの「証明書をインポートする」を参照してください。
証明書のエクスポート	証明書を選択し、[エクスポート] をクリックします。 詳細については、431 ページの「証明書をエクスポートする」を参照してください。
証明書の割り当て	証明書を選択し、[割り当て] をクリックします。 詳細については、431 ページの「証明書を割り当てる」を参照してください。
証明書の削除	証明書を 1 つ以上選択して [削除] をクリックし、 [はい] をクリックして削除を確定します。

証明書署名要求を設定する

手順

1. [管理] > [システム 設定] > [証明書の管理] の順に選択します。

   [SMTP 証明書と HTTPS 証明書] 画面が表示されます。

2. 次のいずれかを実行します。

   - [追加] をクリックして新しいエントリを作成します。
   - 名前をクリックして詳細情報を表示し、名前のみを変更します。

3. 証明書の名前を入力します。
4. [サブジェクトの別名] フィールドに、生成した証明書に関連付けるドメイン名を 1 つ以上入力します。
5. [種類] ドロップダウンリストから、[証明書署名要求] を選択します。
6. 必要なフィールドを設定します。

フィールド	説明
鍵長	証明書の鍵のサイズを選択します。
国コード	会社が存在する国を選択します。
都道府県	会社が存在する都道府県を入力します。
市区町村	会社が存在する市区町村を入力します。
組織	会社名を入力します。
組織単位	会社内の部署名を入力します。
一般名	一般名 (サーバの FQDN など) を入力します。
メールアドレス	自身のメールアドレスを入力します。

7. [追加] をクリックします。
8. 認証局 (CA) に要求を送信できるように、証明書署名要求の内容をコピーして保存します。
9. [閉じる] をクリックします。

自己署名証明書を設定する

手順

1. [管理] > [システム設定] > [証明書の管理] の順に選択します。

   [SMTP 証明書と HTTPS 証明書] 画面が表示されます。

2. 次のいずれかを実行します。
   - [追加] をクリックして新しいエントリを作成します。
   - 名前をクリックして詳細情報を表示し、名前のみを変更します。
3. 証明書の名前を入力します。
4. [サブジェクトの別名] フィールドに、生成した証明書に関連付けるドメイン名を 1 つ以上入力します。
5. [種類] ドロップダウンリストから、[自己署名証明書] を選択します。
6. 必要なフィールドを設定します。

フィールド	説明
鍵長	証明書の鍵のサイズを選択します。
国コード	会社が存在する国を選択します。
都道府県	会社が存在する都道府県を入力します。
市区町村	会社が存在する市区町村を入力します。
組織	会社名を入力します。
組織単位	会社内の部署名を入力します。
一般名	一般名 (サーバの FQDN など) を入力します。
メールアドレス	自身のメールアドレスを入力します。
有効日数	証明書の有効日数を入力します。

7. [追加] をクリックします。

証明書をインポートする

フィンガープリントを変更したり別の認証局を指定したりする場合は、新しい証明書をインポートします。

手順

1. [管理] > [システム設定] > [証明書の管理] の順に選択します。

   [SMTP 証明書と HTTPS 証明書] 画面が表示されます。

2. [インポート] をクリックします。
3. 証明書ファイルを選択します。
4. (オプション) 秘密鍵ファイルを選択し、パスワードを入力します。
5. [インポート] をクリックします。

証明書をエクスポートする

手順

1. [管理] > [システム設定] > [証明書の管理] の順に選択します。

   [SMTP 証明書と HTTPS 証明書] 画面が表示されます。

2. 証明書を選択し、[エクスポート] をクリックします。
3. (オプション) [秘密鍵ファイルのエクスポート] を選択し、パスワードを入力します。
4. [エクスポート] をクリックします。

証明書を割り当てる

証明書をインポートするか自己署名証明書を作成したら、その証明書をサービスに割り当てて使用します。

手順

1. [管理] > [システム設定] > [証明書の管理] の順に選択します。

   [SMTP 証明書と HTTPS 証明書] 画面が表示されます。

2. 証明書を選択し、[割り当て] をクリックします。

3. 選択した 1 つ以上のサービスを [利用可能なサービス] リストから [選択されたサービス] リストに移動します。

4. [割り当て] をクリックします。

信頼する CA 証明書

信頼する認証局 (CA) 証明書は、Deep Discovery Email Inspector に提示されるリモート証明書を検証します。CA 証明書には、証明書信頼リスト (CTL) の階層を形成する依存関係があります。この階層をたどって証明書をルート CA に結び付け、その信頼性を検証します。

次の表は、[信頼する CA 証明書] 画面で実行できるタスクを示しています。

タスク	説明
証明書の情報の表示	名前をクリックします。
証明書のインポート	[インポート] をクリックします。 詳細については、433 ページの「証明書をインポートする」を参照してください。
証明書のエクスポート	証明書を 1 つ以上選択し、[エクスポート] をクリックします。 **注意** エクスポートする証明書を複数選択した場合、Deep Discovery Email Inspector は、選択した証明書を同じ証明書ファイルにエクスポートします。
証明書の削除	証明書を 1 つ以上選択して [削除] をクリックし、 [はい] をクリックして削除を確定します。

証明書をインポートする

フィンガープリントを変更したり別の認証局を指定したりする場合は、新しい証明書をインポートします。

注意

複数の CA 証明書を同時にインポートする場合は、それらを同じファイルに保存してインポートします。

手順

1. [管理] > [システム設定] > [証明書の管理] の順に選択します。
2. [信頼する CA 証明書] をクリックします。
3. [インポート] をクリックします。
4. 証明書ファイルを選択します。

   Deep Discovery Email Inspector によってファイルがインポートされます。

接続のセキュリティを設定する

Deep Discovery Email Inspector が Web コンソールや SMTP の接続に使用するセキュリティプロトコルを選択できます。

手順

1. [管理] > [システム設定] > [接続のセキュリティ] の順に選択します。
2. 接続の種類 ([Web コンソール] および [SMTP]) に対するセキュリティプロトコルを選択します。

注意

接続の種類が SMTP の場合は、[TLS] 画面で、受信および送信メッセージに Transport Layer Security (TLS) を設定できます。

詳細については、336 ページの「TLS を設定する」を参照してください。

3. [保存] をクリックします。

アカウント/連絡先

Deep Discovery Email Inspector では、役割ベースの管理を使用して、管理タスクを実行する管理コンソールへのアクセスを付与および制御します。

役割ベースの管理を使用するには、カスタムアカウントを作成して、各アカウントに特定の役割を割り当てます。役割は管理コンソールへのアクセスレベルを定義します。

カスタムアカウントを作成して管理コンソールの特定の権限を割り当てることにより、アカウントユーザに特定タスクの実行に必要なツールと権限のみを表示するようにできます。

管理コンソールへのアクセスについてセキュリティを強化するため、Deep Discovery Email Inspector では、ログオンに 5 回失敗したアカウントを自動的にロックします。そのアカウントを使用して管理コンソールに再度ログオンするには、10 分待つか、管理者にアカウントをロック解除するよう求めることができます。

連絡先管理の一部として、連絡先リストの受信者のリストを設定することもできます。連絡先リストは初期設定でアラート通知やレポートの送信に使用されます。

アカウントを管理する

Deep Discovery Email Inspector には初期設定の管理者アカウント (「admin」) があり、このアカウントには管理上の完全なアクセス権があります。

初期設定の管理者アカウントは、次のタスクを実行できます。

- 新しい管理者アカウントを追加する
- アカウントをロックまたはロック解除する

管理者の役割を割り当てられたアカウントは、追加のアカウントを作成し、そのアカウントに管理者またはオペレータの役割を割り当てることができます。管理者はタスクを別の管理者およびオペレータに委任して、Deep Discovery Email Inspector の管理におけるボトルネックを削減できます。

管理者アカウントでは、既存のアカウントを編集または削除することもできます。

アカウントの役割の分類

役割	説明
管理者	メニュー項目に含まれるすべての機能と設定にアクセスできます。 • [ダッシュボード] • [検出] • [ポリシー] • [アラート/レポート] • [ログ] • [管理] • [ヘルプ]
調査者	メニュー項目に含まれる特定の機能と設定を表示できますが、管理に関する修正はできません。 • [ダッシュボード] • [検出] • [アラート/レポート] > [レポート] > [生成されたレポート] • [アラート/レポート] > [アラート] > [実行されたアラート] • [ログ] • [ヘルプ]

役割	説明
オペレータ	メニュー項目に含まれる特定の機能と設定を表示できますが、管理に関する修正はできません。 • [ダッシュボード] • [検出] (メッセージ本文へのアクセスなし) • [アラート/レポート] > [レポート] > [生成されたレポート] • [アラート/レポート] > [アラート] > [実行されたアラート] • [ログ] • [ヘルプ]

ローカルユーザアカウントを追加する

手順

1. [管理] > [アカウント/連絡先] > [アカウント] の順に選択します。
2. [追加] をクリックします。

   [アカウントの追加] 画面が表示されます。
3. このアカウントの [ステータス] を切り替えます。
4. [種類] ドロップダウンリストから [ローカルユーザ] を選択します。
5. アカウントユーザ名とパスワードを指定します。
6. アカウントの [役割] を選択します。役割はアカウントのアクセスレベルを決定します。

   435 ページの「アカウントの役割の分類」を参照してください。
7. [保存] をクリックします。

   新しいアカウントが [アカウント] リストに追加されます。

Active Directory のユーザアカウントまたはグループを追加する

注意

Active Directory のユーザアカウントまたはグループを追加する前に、Microsoft Active Directory を設定する必要があります。

詳細については、389 ページの「LDAP」を参照してください。

手順

1. [管理] > [アカウント/連絡先] > [アカウント] の順に選択します。
2. [追加] をクリックします。

   [アカウントの追加] 画面が表示されます。
3. このアカウントの [ステータス] を切り替えます。
4. アカウントの [種類] に [LDAP ユーザまたはグループ] を選択します。
5. ユーザまたはグループの名前を入力して [検索] をクリックし、LDAP サーバの一致するユーザアカウントまたはグループを検索します。

   一致するユーザアカウントとグループが結果に表示されます。

   注意

   ユーザアカウントが表示されない場合は、次の理由が考えられます。

   - ユーザアカウントのユーザプリンシパル名 (UPN) が LDAP サーバで指定されていない
   - ユーザアカウントが LDAP サーバで無効になっている
6. 追加する LDAP のユーザアカウントまたはグループを選択します。
7. アカウントの [役割] を選択します。役割はアカウントのアクセスレベルを決定します。

   435 ページの「アカウントの役割の分類」を参照してください。
8. [保存] をクリックします。

新しいアカウントが [アカウント] リストに追加されます。

アカウントを編集する

アカウントの権限を変更して、役割の見直しやその他の組織的変更に応じて設定を調整します。

手順

1. [管理] > [アカウント/連絡先] > [アカウント] の順に選択します。
2. アカウント名をクリックします。
3. 必要な変更を行います。
4. [保存] をクリックします。

アカウントを削除する

アカウントを削除して、役割の見直しやその他の組織的変更に応じて設定を調整します。

注意

削除できるのはカスタムアカウントのみです。Deep Discovery Email Inspector の初期設定の管理者アカウントは削除できません。

手順

1. [管理] > [アカウント/連絡先] > [アカウント] の順に選択します。
2. 削除するアカウントを選択します。
3. [削除] をクリックします。
4. 確認メッセージが表示されたら、[OK] をクリックして続行します。

ロックされたアカウントをロック解除する

Deep Discovery Email Inspector では、ログオンに 5 回失敗したアカウントを自動的にロックします。管理者アカウントを使用して、アカウントを手動でロック解除できます。

注意

アカウントがロックされた場合、ユーザは 10 分経過すれば再度ログインできるようになります。アカウントのロックは Deep Discovery Email Inspector によって解除されます。10 分経過してもユーザが再度ログインしなければ、アカウントはロックされたままになります。

手順

1. [管理] > [アカウント/連絡先] > [アカウント] の順に選択します。
2. ロックされたアカウントを選択します。
3. [ロック解除] をクリックします。

パスワードを変更する

注意

次のパスワードは管理コンソールでは変更できません。

- Microsoft Active Directory アカウント
- Trend Micro Apex Central のシングルサインオン (SSO) アカウント
- SAML SSO アカウント

手順

1. 管理コンソールのバナーで、アカウント名をクリックします。

   [パスワードの変更] 画面が表示されます。
2. パスワードを設定します。

- 現在のパスワード
- 新しいパスワード
- パスワードの確認入力

3. [保存] をクリックします。

SAML グループ

Deep Discovery Email Inspector と ID プロバイダの間で信頼関係が確立されると、Deep Discovery Email Inspector は ID プロバイダのディレクトリサーバ上にあるユーザ ID にアクセスできるようになります。ただし、Deep Discovery Email Inspector でユーザ ID 情報を使用してユーザの認証および認可を実際に行うには、グループ、役割、および要求を使用してアカウントの種類と SAML グループを設定する必要があります。

Deep Discovery Email Inspector で ID プロバイダの SAML アカウントをユーザの役割にマッピングする設定の概要を次に示します。

1. ユーザアカウントを作成します。
   a. ユーザアカウントを作成します。
   b. ユーザグループを作成し、ユーザアカウントをグループに割り当てます。

   詳細については、ID プロバイダに付属のドキュメントを参照してください。
2. Deep Discovery Email Inspector で、指定した役割と要求を持つ SAML グループを作成します。

   詳細については、440 ページの「SAML グループを設定する」を参照してください。

SAML グループを設定する

Deep Discovery Email Inspector で SAML グループを設定して、ID プロバイダのユーザグループにマッピングします。

手順

1. [管理] > [アカウント/連絡先] > [SAML] の順に選択します。
2. 次のいずれかを実行します。
   - [追加] をクリックして SAML グループを作成します。
   - SAML グループの名前をクリックして設定を行います。
3. ステータスオプションを選択して、SAML グループを有効または無効にします。
4. クレーム値を入力します。

   重要

   クレーム値は、ID プロバイダによって送信される応答内でユーザの役割を識別します。ID プロバイダのユーザグループと Deep Discovery Email Inspector には、同じクレーム値を指定してください。
5. (オプション) SAML グループの説明を入力します。
6. SAML グループの役割および関連付けられた権限を選択します。
   - 管理者: 送信されたオブジェクト、分析結果、および製品設定にフルアクセスできます。
   - 調査者: 送信されたオブジェクト、分析結果、および製品設定に読み取り専用でアクセスできますが、オブジェクトの送信と調査パッケージのダウンロードが可能です (送信されたオブジェクトを含む)。
   - オペレータ: 送信されたオブジェクト、分析結果、および製品設定に読み取り専用でアクセスできます。
   - エンドユーザメール隔離: エンドユーザメール隔離コンソールにのみフルアクセスできます。
7. [保存] をクリックします。

連絡先を管理する

アラート通知やレポートの送信先メールアドレスを入力します。

詳細については、204 ページの「レポートを予約する」および 181 ページの「アラート通知を設定する」を参照してください。

システムのメンテナンス

[システムのメンテナンス] 画面に移動して、次の操作を実行します。

- 442 ページの「設定のバックアップと復元」
- 448 ページの「ストレージ管理を設定する」
- 451 ページの「デバッグログ」
- 452 ページの「ネットワーク接続をテストする」

設定のバックアップと復元

Deep Discovery Email Inspector の設定をバックアップするには、管理コンソールから設定をエクスポートします。システム障害が発生した場合は、以前バックアップした設定ファイルをインポートして、その設定を復元できます。

重要

Deep Discovery Email Inspector で復元できるのは、ライセンスのステータスに互換性があり、ファームウェアバージョン、ハードウェアモデル、およびロケールが同じ別の Deep Discovery Email Inspector サーバの設定のみです。たとえば、バージョン 3.2 以前のバージョンを実行しているサーバからバックアップした設定ファイルで、バージョン 5.1 を実行しているサーバを復元することはできません。

ライセンスの互換性の詳細については、443 ページの「ライセンスの互換性」を参照してください。

注意

設定のエクスポート/インポートを行う際はデータベースがロックされます。そのため、データベースアクセスに依存する Deep Discovery Email Inspector のすべての処理が機能しません。

推奨事項:

- 各インポート操作の前には、現在の設定をバックアップしてください。
- Deep Discovery Email Inspector がアイドル状態のときに操作を実行してください。インポートとエクスポートは Deep Discovery Email Inspector のパフォーマンスに影響します。

設定をバックアップして、Deep Discovery Email Inspector アプライアンスの設定のコピーを作成し、別の Deep Discovery Email Inspector アプライアンスで設定を復元したり、後からバックアップした設定に戻したりします。複数の Deep Discovery Email Inspector アプライアンス間で同じ設定ファイルを各アプライアンスに復元することにより、設定を複製します。

ライセンスの互換性

次の表は、製品ライセンスの互換性について説明しています。復元できるのは、ライセンスに互換性があり、ファームウェアバージョン、ハードウェアモデル、およびロケールが同じ別の Deep Discovery Email Inspector サーバからバックアップした設定ファイルのみです。

表 8-26. ライセンスの互換性

ライセンスのアクティベーション	高度な脅威対策 + ゲートウェイモジュール	ゲートウェイモジュールのみ	高度な脅威対策のみ
高度な脅威対策 + ゲートウェイモジュール	互換性あり	互換性あり	互換性あり
ゲートウェイモジュールのみ	互換性なし	互換性あり	互換性なし
高度な脅威対策のみ	互換性なし	互換性なし	互換性あり

バックアップの推奨事項

設定をエクスポートして、次を実行することをお勧めします。

- バックアップを作成する

  Deep Discovery Email Inspector が重大な問題から回復できない場合、デバイスを復元してから設定のバックアップをインポートすると、自動的に障害が発生する前の設定に戻されます。

- 複数のデバイスで設定を複製する

  ネットワーク上に複数のデバイスがある場合、ほとんどの設定は個別に行う必要はありません。

設定をバックアップする

エクスポート中は、次のことは行わないでください。

- 他の管理コンソール画面へのアクセスや設定の変更
- データベースの操作
- デバイス上またはデバイスが属するグループのサービスの開始/停止
- 他のインポートまたはエクスポートタスクの開始

次の表に示す画面とタブの設定をバックアップできます。

表 8-27. バックアップされる設定

画面	タブ
[ダッシュボード]	すべてのウィジェットの設定のみ
[ポリシー] > [ポリシー管理]	[ポリシーリスト]
	[コンテンツフィルタルール]
	[情報漏えい対策ルール]
	[スパムメール対策ルール]
	[脅威対策ルール]
[ポリシー] > [ポリシーオブジェクト]	[通知]
	[置換ファイル]
	[リダイレクトページ]
	[アーカイブサーバ]
	[データ識別子]
	[情報漏えい対策テンプレート]

画面	タブ
[ポリシー] > [除外]	[メッセージ]
	[オブジェクト] (ローカルオブジェクトの除外のみ)
	[URL キーワード]
	[グレーメールの除外]
	[Email Encryption の除外]
[アラート/レポート] > [アラート]	[ルール]
[アラート/レポート] > [レポート]	[スケジュール]
[管理] > [コンポーネントのアップデート]	[スケジュール]
	[ソース]
[管理] > [システム設定]	[操作モード]
	[プロキシ]
	[SMTP]
	[時間] (日時の形式と NTP サーバ設定のみ)
	[SNMP]
	[セッションタイムアウト]
	[証明書の管理]
	[接続のセキュリティ]
[管理] > [メール設定]	[ネットワーク接続]
	[メッセージ配信]
	[制限および除外]
	[SMTP グリーティング]
	[エッジ MTA リレーサーバ]

画面	タブ
	[内部ドメイン]
[管理] > [統合製品/サービス]	[Syslog]
	[LDAP]
	[SFTP]
[管理] > [検索/分析]	[設定] ([サブミッションフィルタ]、[URL サブミッションフィルタ]、および [タイムアウト設定] セクションのみ)
	[ファイルパスワード]
	[Smart Protection]
	[スマートフィードバック]
	[YARA ルール]
	[Time-of-Click プロテクション]
	[ビジネスメール詐欺からの保護]
	[URL 検索]
[管理] > [送信者フィルタ/認証]	[承認済み送信者]
	[ブロックする送信者]
	[ディレクトリハーベスト攻撃 (DHA) からの保護]
	[メールレピュテーション]
	[バウンスメール攻撃からの保護]
	[SMTP トラフィックスロットリング]
	[SPF]
	[DKIM 認証]
	[DKIM 署名]

画面	タブ
	[DMARC]
[管理] > [エンドユーザメール隔離]	[ユーザ隔離アクセス]
	[エンドユーザメール隔離通知]
[管理] > [システムメンテナンス]	[ストレージの管理]
[管理] > [アカウント/連絡先]	[アカウント]
	[連絡先]

手順

1. [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択します。
2. [設定のバックアップ] の横にある [エクスポート] をクリックします。

   Web ブラウザで、ファイルの保存先を選択する画面が表示されます。
3. ファイルの保存先を選択して、設定ファイルをローカルストレージに保存します。

設定を復元する

Deep Discovery Email Inspector の設定を復元すると、メッセージ配信設定などの元の設定とルールが、インポートされた設定に置き換えられます。

インポート中は、次のことは行わないでください。

- 他の管理コンソールへのアクセスや設定の変更
- データベースの操作
- デバイス上またはデバイスが属するグループのサービスの開始/停止
- 他のインポートまたはエクスポートタスクの開始

注意

復元できる設定については、444 ページの「設定をバックアップする」を参照してください。

手順

1. [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択します。
2. [設定ファイルの復元] にある [ファイルを選択] または [参照] をクリックしてファイルを選択します。
3. [復元] をクリックします。

   すべてのサービスが再起動します。復元する設定およびルールによっては時間がかかる場合があります。

ストレージ管理を設定する

[ストレージの管理] では、隔離フォルダのサイズやシステムに 保存するログデータの量を制御できます。隔離フォルダの現在の使用状況も確認できます。

手順

1. [管理] > [システムのメンテナンス] > [ストレージの管理] の順に選択します。
2. グローバル隔離設定を指定します。
   - グローバル隔離フォルダのサイズ : グローバル隔離フォルダのサイズを GB 単位で指定します。

注意

グローバル隔離フォルダのサイズは Deep Discovery Email Inspector アプライアンスのバージョンに応じて次のように設定します。

- Deep Discovery Email Inspector 7100/7200/7300: 1〜100 の間で指定する必要があります。
- Deep Discovery Email Inspector 9100/9200: 1〜400 の間で指定する必要があります。

- グローバル隔離のディスク空き容量が次の値以下である場合にメッセージの添付ファイル、リンク、および分析レポートを削除: ファイルを自動的に削除するための隔離ディスク空き容量のしきい値を指定します。

注意

しきい値は 10〜50 の間で設定する必要があります。

Deep Discovery Email Inspector は指定された割合にさらに 10%を足した容量のデータを削除します。

3. エンドユーザメール隔離 (EUQ) の設定を指定します。
   - すべてのデータの削除 (メッセージおよび承認済み送信者を含む): [削除] をクリックして、エンドユーザメール隔離データベースのすべてのデータを削除します。
   - エンドユーザメール隔離フォルダのサイズ : 隔離フォルダのサイズを GB 単位で指定します。
   - エンドユーザメール隔離のディスク空き容量が次の値以下である場合にメッセージの添付ファイル、リンク、および分析レポートを削除: ファイルを自動的に削除するためのエンドユーザメール隔離のディスク空き容量のしきい値を指定します。

注意

しきい値は 10～50 の間で設定する必要があります。

Deep Discovery Email Inspector は指定された割合にさらに 10%を足した容量のデータを削除します。

- 隔離メッセージの最長保存期間: 隔離されたスパムメールメッセージを保存する日数を指定します。

注意

日数は 1～60 の間で指定する必要があります。

4. ログ設定を指定します。
   - 次の日数を経過したログを削除: ログを保持する日数を指定します。

注意

日数は 3～366 の間で指定する必要があります。

   - 空きディスク容量の合計が次の値以下である場合にログを削除する: ログを自動的に削除するためのディスク空き容量のしきい値を指定します。

注意

しきい値は 10～50 の間で設定する必要があります。

Deep Discovery Email Inspector は指定された割合にさらに 10%を足した容量のデータを削除します。

重要

Deep Discovery Director を統合して仮想アナライザイメージを配信するには、追加のディスク容量が必要です。Deep Discovery Email Inspector を Deep Discovery Director 5.0 以降に登録したら、空きディスク容量の合計が 20%未満になった場合はログを削除するように Deep Discovery Email Inspector を設定します。

5. [保存] をクリックします。

Deep Discovery Email Inspector を電源オフまたは再起動する

[電源オフ/再起動] 画面には、Deep Discovery Email Inspector アプライアンスと関連サービスの電源オフや再起動を行うためのオプションがあります。

手順

1. [管理] > [システムのメンテナンス] > [電源オフ/再起動] の順に選択します。
2. 次のいずれかを実行します。
   - Deep Discovery Email Inspector アプライアンスをシャットダウンするには、[電源オフ] をクリックします。
   - Deep Discovery Email Inspector を再起動するには、[再起動] をクリックします。
3. [OK] をクリックして確認します。

デバッグログ

Deep Discovery Email Inspector により作成されるデバッグログには、問題のトラブルシューティングに 役立つ情報が含まれています。

デバッグログをエクスポートする

問題をトラブルシューティングするには、デバッグログをエクスポートして、テクニカルサポートに情報を提供します。

手順

1. [管理] > [システムのメンテナンス] > [デバッグログ] の順に選択します。
2. エクスポートするログの日数を選択します。
3. [エクスポート] をクリックします。

4. エクスポートが完了するまで待ちます。エクスポートに要する時間は、データ量によって異なります。

ログレベルを設定する

ログレベルを設定して、問題のトラブルシューティングに 役立つ情報を保存します。

手順

1. [管理] > [システムのメンテナンス] > [デバッグログ] の順に選択します。
2. ログレベルを選択します。
   - デバッグ
   - エラー
3. [保存] をクリックします。

ネットワーク接続をテストする

[ネットワークサービス診断] 画面を使用して、内部仮想アナライザや他のネットワークサービスに対するネットワーク接続をテストできます。

手順

1. [管理] > [システムメンテナンス] > [ネットワークサービス診断] の順に選択します。
2. 有効なサービスを 1 つ以上選択して、[テスト] をクリックします。

> **注意**
>
> [Smart Protection Server] オプションは、[Smart Protection] 画面の設定で有効にできます。
>
> 詳細については、262 ページの「Smart Protection を設定する」を参照してください。

接続テストが完了するまで待ちます。テストに要する時間はネットワーク環境や選択したサービスの数に応じて異なります。接続テストの結果は [結果] 列に表示されます。

ライセンス

[ライセンス] 画面には、ライセンス情報が表示され、Deep Discovery Email Inspector の機能セットに対する有効なアクティベーションコードを入力できます。

- 高度な脅威対策
- ゲートウェイモジュール

次の表は、各機能セットで使用可能な機能またはサービスを示しています。

機能/サービス	高度な脅威対策	ゲートウェイモジュール
補助製品/サービスの統合	あり	あり
コミュニティファイルレピュテーション	あり	あり
ファイルパスワードアナライザ	あり	なし
内部仮想アナライザ	あり	なし
Office マクロの検索	あり	あり
機械学習型検索	あり	あり
Time-of-Click プロテクション	あり	あり
脅威インテリジェンスの共有	あり	あり
Web サービス API	あり	あり
YARA ルール	あり	なし
スパムメール対策/グレーメール対策	なし	あり

機能/サービス	高度な脅威対策	ゲートウェイモジュール
コンテンツフィルタ	なし	あり
情報漏えい対策	なし	あり
DKIM 署名	なし	あり
Email Reputation Services (ERS)	なし	あり
エンドユーザメール隔離	なし	あり
送信者フィルタ	なし	あり

注意

アップデート、不審オブジェクトの検出、およびソーシャルエンジニアリング攻撃からの保護など、表に記載されていないその他の機能は両方の機能セットで使用できます。

サポート契約

サポート契約は、お客さまの組織とトレンドマイクロ間の契約で、適用される料金の支払いと引き換えにお客さまがテクニカルサポートおよび製品のアップデートを受ける権利が規定されます。トレンドマイクロ製品の購入時に、製品とともにお客さまに渡される使用許諾契約にその製品のサポート契約の条件が記載されています。

通常はサポート契約の有効期限の 90 日前に、サポート終了が迫っていることを知らせるメッセージが表示されます。サポート契約は、販売店、トレンドマイクロの営業担当、または次のトレンドマイクロのオンライン登録の URL からサポートの更新料をお支払いいただくことでアップデートできます。

https://clp.trendmicro.com/fullregistration?T=TM

アクティベーションコード

有効なアクティベーションコードを使用して製品を使用できるようにします。製品は、アクティベーションが完了するまで操作できません。アクティベーションコードは、次のような 37 文字 (ハイフンを含む) の文字列です。

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

アクティベーションコードではなくレジストレーションキーを 取得している場合は、レジストレーションキーを使用して、次の Web サイトで製品を登録します。

https://clp.trendmicro.com/fullregistration?T=TM

レジストレーションキーはハイフンを 含んだ 22 文字のキーで、次のように表示されます。

xx-xxxx-xxxx-xxxx-xxxx

登録後、アクティベーションコードがメールで 送付されます。

製品ライセンスのステータス

サポート契約の更新が必要になったとき、製品ライセンスのステータスは最初に製品を取得したときのステータスから変更されます。一部のステータスでは、すべての製品機能を維持するために操作が必要な場合があります。製品ライセンスをアクティベートせずに 製品を体験することができます。

ステータス	説明
体験版	限定された体験期間にすべての 機能を使用できます。体験期間はサポート契約に基づきます。
非アクティベート	テクニカルサポートを受けたり、コンポーネントをアップデートすることができません。製品ライセンスがアクティベートされるまで、すべてのメールメッセージは調査されずに配信されます。
アクティベート済み	ライセンス期間内は、すべての機能とコンポーネントのアップデートを使用できます。利用可能なテクニカルサポートはサポート契約に基づきます。

ステータス	説明
有効期限切れ	ライセンスの有効期限が終了しています。猶予期間を過ぎると、製品の機能が制限されます。 • 体験版ライセンスでは、コンポーネントのアップデートと検索を使用できなくなります。 • 製品版ライセンスでは、テクニカルサポートとコンポーネントのアップデートを使用できなくなります。検索では期限切れのコンポーネントが使用されます。  警告! 期限切れのコンポーネントは、製品の検出機能を大幅に低下させます。

製品ライセンスを表示する

製品ライセンスのステータスは、[ライセンス] 画面で確認します。

手順

1. [管理] > [ライセンス] の順に選択します。

   次の表は、ライセンス情報の詳細を示しています。

フィールド	説明
ステータス	製品ライセンスの現在の状態です。製品ライセンスのステータスの詳細については、455 ページの「製品ライセンスのステータス」を参照してください。
種類	ライセンスには、製品版と体験版があります。使用可能なライセンスの種類はサポート契約で定められます。
有効期限	ライセンスの有効期限が終了する日付です。

フィールド	説明
アクティベーションコード	アクティベーションコードは、次のような 37 文字 (ハイフンを含む) の文字列です。 xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx 詳細については、454 ページの「アクティベーションコード」を参照してください。

2. [ライセンスの詳細] で次の手順を実行します。
   - [詳細情報の表示] をクリックしてトレンドマイクロの Web サイトを表示します。
   - [表示更新] をクリックして、ライセンスの有効期限を手動で同期します。

製品ライセンスをアクティベートまたは更新する

手順

1. [管理] > [ライセンス] の順に選択します。
2. [新しいアクティベーションコード] をクリックします。

   [アクティベーションコード] 画面が表示されます。
3. 新しいアクティベーションコードを指定します。
4. ライセンスを初めてアクティベートする場合は、使用許諾契約書を読んで、[使用許諾契約書の条件を読み、同意します。] を選択します。
5. [保存] をクリックします。

   Deep Discovery Email Inspector コンポーネントがアクティベートされます。
6. 製品ライセンスを表示します。

   456 ページの「製品ライセンスを表示する」を参照してください。

Deep Discovery Email Inspector について

ファームウェアのバージョン、API キー、およびその他の製品情報を表示するには、[ヘルプ]→[バージョン情報] 画面を使用します。

注意

ハードウェアモデル 7300 で、管理コンソールにハードウェアモデルの正しい情報を表示するには、HotFix (ビルド 1394) をダウンロードしてインストールします。

詳細については、https://success.trendmicro.com/dcx/s/solution/000291496?language=ja を参照してください。

第 9 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/dcx/s/?language=ja

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/ 駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/dcx/s/threat?language=ja

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの 送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録

付録

付録 A

コマンドラインインタフェースの使用

この付録の内容は次のとおりです。

CLI を使用する

コマンドラインインタフェース (CLI) を使用して、次のタスクを実行します。

- デバイスの IP アドレスやホスト名の初期設定
- デバイスの再起動
- デバイスのステータスの表示
- デバイスのデバッグとトラブルシューティング

注意

HyperTerminal の使用時はキーボードのスクロールロックを有効にしないでください。スクロールロックが有効な場合、データを入力できません。

CLI を開始する

サーバに直接接続するか、SSH を使用して接続し、CLI にログオンします。

手順

- サーバに直接接続するには
  a. モニタまたはキーボードをサーバに接続します。
  b. CLI にログオンします。

注意

初期設定のアカウント情報は次のとおりです。

- ユーザ名:`admin`
- パスワード:`ddei`

- SSH サービスが有効な場合は、次の手順を実行し、SSH を使用して接続します。
  a. 使用しているコンピュータから Deep Discovery Email Inspector の IP アドレスに Ping を実行できることを確認します。

b. SSH クライアントを使用して、Deep Discovery Email Inspector の IP アドレスと TCP ポート 22 に接続します。

注意

初期設定の IP アドレス/サブネットマスクは `192.168.252.1/255.255.0.0` です。

コマンドラインインタフェースのコマンド

Deep Discovery Email Inspector の CLI コマンドは、標準コマンドと特権コマンドの 2 つのカテゴリに分類されます。標準コマンドは、システム情報を取得したり単純なタスクを実行したりするための基本コマンドです。特権コマンドは、設定のフルコントロールと、高度な監視およびデバッグ機能を提供します。特権コマンドは、`enable` コマンドとパスワードによって保護されています。

特権モードを開始する

警告!

シェル環境に入るのは、サポートプロバイダからデバッグ操作の指示があった場合のみです。

手順

1. CLI にログオンします。

   468 ページの「CLI を開始する」を参照してください。

2. プロンプトで「`enable`」と入力して <Enter> キーを押し、特権モードに切り替えます。

3. 初期設定パスワードの「`trend#1`」を入力し、<Enter> キーを押します。

   プロンプトが>から#に変更されます。

CLI コマンドリファレンス

次の表では、CLI コマンドについて説明します。

注意

CLI コマンドの実行には特権モードが必要です。詳細については、469 ページの「特権モードを開始する」を参照してください。

configure product management-port

表 A-1. configure product management-port

管理ポートの IP アドレスを設定します。	
構文: `configure product management-port [ipv4 | ipv6] <ip> <mask>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <ip>: インタフェースの IP アドレス <mask>: NIC のネットワークマスク
例:	
管理ポートの IPv4 アドレスを設定するには: `configure product management-port ipv4 192.168.10.21 255.255.255.0`	

configure product operation-mode

表 A-2. configure product operation-mode

Deep Discovery Email Inspector の動作モードを設定します。 **注意** Microsoft Hyper-V にインストールされた Deep Discovery Email Inspector 仮想アプライアンスでは、SPAN/TAP モードはサポートされません。 Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。
構文: `configure product operation-mode [BCC | MTA | TAP]`

表示	特権
パラメータ	BCC: BCC モードで配置します MTA: MTA モードで配置します TAP: SPAN/TAP モードで配置します
例:	
BCC モードで配置するには: `configure product operation-mode BCC`	

configure network basic

表 A-3. configure network basic

ホスト名、IP アドレス、サブネットマスク、ゲートウェイ、および DNS など、ネットワークの基本設定を行います。
構文: `configure network basic`

表示	特権
パラメータ	なし

例:

```
***Network Configuration***

Specify value for each item and press ENTER.Settings apply to the
management port (Eth0) and require a restart.

Host name: mail.com

IPv4 address: 10.64.70.151

Subnet mask: 255.255.254.0

IPv4 gateway: 10.64.70.1

Preferred IPv4 DNS: 10.64.1.55

Alternate IPv4 DNS: 10.64.1.54

IPv6 address:

Prefix length:

IPv6 gateway:

Preferred IPv6 DNS:

Alternate IPv6 DNS:

Confirm changes and restart (Y/N):
```

configure network dns

表 A-4. configure network dns

Deep Discovery Email Inspector デバイスの DNS を設定します。	
構文: `configure network dns [ipv4 | ipv6] <dns1> <dns2>`	
表示	特権

パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <dns1>: プライマリ DNS サーバ <dns2>: セカンダリ DNS サーバ  注意 プライマリとセカンダリの DNS 値は、空白で区切ります。
例:	
プライマリ DNS に IP アドレス 192.168.10.21 を設定するには: `configure network dns ipv4 192.168.10.21`	
プライマリおよびセカンダリ DNS に次の値を設定するには: • プライマリ DNS: `192.168.10.21` • セカンダリ DNS: `192.168.10.22` `configure network dns ipv4 192.168.10.21 192.168.10.22`	

configure network hostname

表 A-5. configure network hostname

Deep Discovery Email Inspector デバイスのホスト名を設定します。	
構文: `configure network hostname <hostname>`	
表示	特権
パラメータ	<hostname>: Deep Discovery Email Inspector デバイスのホスト名または完全修飾ドメイン名
例:	
Deep Discovery Email Inspector デバイスのホスト名を test.host.com に変更するには: `configure network hostname test.example.com`	

configure network interface

表 A-6. configure network interface

ネットワークインタフェースカード (NIC) の IP アドレスを設定します。	
構文: `configure network interface [ipv4 | ipv6] <interface> <ip> <mask>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <interface>: NIC 名 <ip>: インタフェースの IP アドレス <mask>: NIC のネットワークマスク
例:	
NIC に次の値を設定するには: • インタフェース: `eth0` • IPv4 アドレス: `192.168.10.10` • IPv4 サブネットマスク: `255.255.255.0` `configure network interface ipv4 eth0 192.168.10.10 255.255.255.0`	

configure network teaming reinit

表 A-7. configure network teaming reinit

ネットワークインタフェースカード (NIC) チーミングを無効にして、ネットワークカードの設定を復元します。	
構文: `configure network teaming reinit`	
表示	特権
パラメータ	なし

例:
NIC チーミングを無効にするには: `configure network teaming reinit`

configure network route add

表 A-8. configure network route add

新しいルートエントリを追加します。	
構文: `configure network route add [ipv4 | ipv6] <ip_prefixlen> <via> <dev>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <ip_prefixlen>: IP_Address/Prefixlen 形式の送信先ネットワーク ID <via>: 次のホップの IP アドレス <dev>: デバイス名
例:	
新しいルートエントリを追加するには: `configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1`	

configure network route default

表 A-9. configure network route default

初期設定のルートを設定します。	
構文: `configure network route default [ipv4 | ipv6] <gateway>`	
表示	特権

パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <gateway>: 初期設定のゲートウェイの IP アドレス
例:	
Deep Discovery Email Inspector アプライアンスの初期設定のルートを設定するには: `configure network route default ipv4 192.168.10.1`	

configure network route del

表 A-10. configure network route del

ルートを削除します。	
構文: `configure network route del [ipv4 | ipv6] <ip_prefixlen> <via> <dev>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <ip_prefixlen>: IP_Address/Prefixlen 形式の送信先ネットワーク ID <via>: 次のホップの IPv4 アドレス <dev>: デバイス名
例:	
Deep Discovery Email Inspector アプライアンスのルートを削除するには: `configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1`	

configure network route del default/default ipv6

表 A-11. configure network route del default/default ipv6

初期設定の IPv6 ゲートウェイを削除します。

構文: `configure network route del default ipv6 <gateway> <device>`	
表示	特権
パラメータ	gateway: 初期設定のゲートウェイの IPv6 アドレス device: IPv6 初期設定ゲートウェイに対してリンクローカル
例: デバイス eth0 上の初期設定 IPv6 ゲートウェイ fe80::20c:29ff:fe75:b579 を削除するには:`configure network route del default ipv6 fe80::20c:29ff:fe75:b579 eth0`	

configure service nscd disable

表 A-12. configure service nscd disable

システムの起動時にネームサービスキャッシュデーモン (nscd) を無効にします。	
構文: `configure service nscd disable`	
表示	特権
パラメータ	なし
例: システムの起動時にネームサービスキャッシュデーモン (nscd) を無効にするには: `configure service nscd disable`	

configure service nscd enable

表 A-13. configure service nscd enable

システムの起動時にネームサービスキャッシュデーモン (nscd) を有効にします。	
構文: `configure service nscd enable`	
表示	特権

パラメータ	なし
例:	
システムの起動時にネームサービスキャッシュデーモン (nscd) を有効にするには: `configure service nscd enable`	

configure service ssh disable

表 A-14. configure service ssh disable

すべてのネットワークインタフェースカード (NIC) で SSH を無効にします。	
構文: `configure service ssh disable`	
表示	特権
パラメータ	なし
例:	
すべての NIC で SSH を無効にするには: `configure service ssh disable`	

configure service ssh enable

表 A-15. configure service ssh enable

特定の 1 つのネットワークインタフェースカード (NIC) で SSH を有効にします。	
構文: `configure service ssh enable`	
表示	特権
パラメータ	なし
例:	
SSH を有効にするには: `configure service ssh enable`	

configure service ssh port

表 A-16. configure service ssh port

SSH サービスポートを変更します。	
構文: `configure service ssh port <port>`	
表示	特権
パラメータ	<port>: SSH サービスポート番号
例: SSH サービスポートを 56743 に変更するには: `configure service ssh port 56743`	

configure service ntp

表 A-17. configure service ntp

Deep Discovery Email Inspector のシステム時刻を NTP サーバと同期します。	
構文: `configure service ntp [enable | disable | server-address <address>]`	
表示	特権
パラメータ	enable: NTP を有効にします disable: NTP を無効にします server-address: NTP サーバのアドレスを設定します <address>: NTP サーバの FQDN または IP アドレスを指定します
例:	
NTP サーバのアドレスを 192.168.10.21 に設定するには: `configure service ntp server-address 192.168.10.21`	
NTP サーバとの同期を有効にするには: `configure service ntp enable`	

configure system date

表 A-18. configure system date

日時を設定して、CMOS にそのデータを保存します。	
構文: `configure system date <date> <time>`	
表示	特権
パラメータ	<date>:yyyy-mm-dd の形式で時刻を設定します。 <time>:hh:mm:ss の形式で時刻を設定します。
例:	
日付を 2010 年 8 月 12 日、時刻を午後 3 時 40 分に設定するには: `configure system date 2010-08-12 15:40:00`	

configure system password enable

表 A-19. configure system password enable

特権モードを開始するためのパスワードを変更します。	
構文: `configure system password enable`	
表示	特権
パラメータ	なし
例:	
特権モードを開始するためのパスワードを変更するには: `configure system password enable`	

configure system timezone

表 A-20. configure system timezone

Deep Discovery Email Inspector で使用するタイムゾーンを設定します。

構文: `configure system timezone <region> <city>`	
表示	特権
パラメータ	<region>: 地域名 <city>: 都市名
例:	
次の場所のタイムゾーンを使用するように Deep Discovery Email Inspector アプライアンスを設定するには: 地域: America 都市: New York `configure system timezone America New_York`	

表 A-21. タイムゾーン設定の例

地域/国	都市
Africa	Cairo
	Harare
	Nairobi
America	Anchorage
	Bogota
	Buenos_Aires
	Caracas
	Chicago
	Chihuahua
	Denver
	Godthab
	Lima

地域/国	都市
	Los_Angeles
	Mexico_City
	New_York
	Noronha
	Phoenix
	Santiago
	St_Johns
	Tegucigalpa
Asia	Almaty
	Baghdad
	Baku
	Bangkok
	Calcutta
	Colombo
	Dhaka
	Hong_Kong
	Irkutsk
	Jerusalem
	Kabul
	Karachi
	Katmandu
	Krasnoyarsk
	Kuala_Lumpur

地域/国	都市
	Kuwait
	Magadan
	Manila
	Muscat
	Rangoon
	Seoul
	Shanghai
Asia (続き)	Singapore
	Taipei
	Tehran
	Tokyo
	Yakutsk
Atlantic	Azores
Australia	Adelaide
	Brisbane
	Darwin
	Hobart
	Melbourne
	Perth
Europe	Amsterdam
	Athens
	Belgrade
	Berlin

地域/国	都市
	Brussels
	Bucharest
	Dublin
	Moscow
	Paris
Pacific	Auckland
	Fiji
	Guam
	Honolulu
	Kwajalein
	Midway
US	Alaska
	Arizona
	Central
	East-Indiana
	Eastern
	Hawaii
	Mountain
	Pacific

enable

表 A-22. enable

特権モードを開始して、特権コマンドを入力できるようにします。

構文: `enable`	
表示	標準
パラメータ	なし
例:	
特権モードを開始するには: `enable`	

exit

表 A-23. exit

特権モードを終了します。 特権モードではないセッションを終了します。	
構文: `exit`	
表示	標準
パラメータ	なし
例:	
特権モードを終了する、または特権モードではないセッションを終了するには: `exit`	

help

表 A-24. help

CLI のヘルプ情報を表示します。	
構文: `help`	
表示	標準

パラメータ	なし
例:	
CLI のヘルプ情報を表示するには: `help`	

history

表 A-25. history

現在のセッションのコマンドライン履歴を表示します。	
構文: `history [limit]`	
表示	標準
パラメータ	[limit]: 現在のセッションの履歴リストのサイズを指定します。 「0」を指定すると、セッションのすべてのコマンドが維持されます。
例:	
履歴リストのサイズに 6 コマンドを指定するには: `history 6`	

logout

表 A-26. logout

現在の CLI セッションからログアウトします。	
構文: `logout`	
表示	標準
パラメータ	なし
例:	

現在のセッションからログアウトするには: `logout`

ping

表 A-27. ping

指定したホストに Ping を実行します。	
構文: `ping [-c num_echos] [-i interval] <dest>`	
表示	標準
パラメータ	[-c num_echos]: 送信するエコー要求の数を指定します。初期設定値は 5 です。 [-i interval]: パケットの送信間隔を秒単位で指定します。初期設定値は 1 です。 <dest>: 送信先のホスト名または IP アドレスを指定します。
例:	
IP アドレス 192.168.1.1 に Ping を実行するには: `ping 192.168.1.1`	
ホスト remote.host.com に Ping を実行するには: `ping remote.host.com`	

ping6

表 A-28. ping6

インタフェース eth0 を介して指定した IPv6 ホストに ping を実行します。	
構文: `ping6 [-c num_echos] [-i interval] <dest>`	
表示	標準

パラメータ	[-c num_echos]: 送信するエコー要求の数を指定します。初期設定値は 5 です。 [-i interval]: パケットの送信間隔を秒単位で指定します。初期設定値は 1 です。 <dest>: 送信先のホスト名または IP アドレスを指定します。
例:	
IPv6 アドレス fe80::21a:a5ff:fec1:1060 に ping を実行するには: `ping6 fe80::21a:a5ff:fec1:1060`	
ホスト remote.host.com に ping を実行するには: `ping6 remote.host.com`	

start task postfix drop

表 A-29. start task postfix drop

指定したメッセージまたはメールメッセージキュー内のすべてのメッセージを 削除します。	
構文: `start task postfix drop { <mail_id> | all }`	
表示	特権
パラメータ	<mail_id>: Postfix キューから削除するメッセージの ID を指定します。
例:	
メールメッセージキューからメールメッセージ D10D4478A5 を削除するには: `start task postfix drop D10D4478A5`	
メールメッセージキューからすべてのメールメッセージを 削除するには: `start task postfix drop all`	

start task postfix flush

表 A-30. start task postfix flush

キューにあるすべてのメールメッセージを 配信します。	
構文: `start task postfix flush`	
表示	特権
パラメータ	なし
例:	
キューにあるすべてのメールメッセージを 配信するには: `start task postfix flush`	

start task postfix queue

表 A-31. start task postfix queue

Postfix のキューにあるすべてのメールメッセージを 表示します。	
構文: `start task postfix queue`	
表示	特権
パラメータ	なし
例:	
Postfix のキューにあるすべてのメールメッセージを 表示するには: `start task postfix queue`	

start service nscd

表 A-32. start service nscd

ネームサービスキャッシュデーモン (nscd) を起動します。

構文: `start service nscd`	
表示	特権
パラメータ	なし
例:	
ネームサービスキャッシュデーモン (nscd) を起動するには: `start service nscd`	

start service postfix

表 A-33. start service postfix

Postfix メールシステムを開始します。	
構文: `start service postfix`	
表示	特権
パラメータ	なし
例:	
Postfix メールシステムを開始するには: `start service postfix`	

start service product

表 A-34. start service product

製品サービスシステムを開始します。	
構文: `start service product`	
表示	特権
パラメータ	なし

例:
製品サービスシステムを開始するには: `start service product`

start service ssh

表 A-35. start service ssh

ssh サービスシステムを開始します。	
構文: `start service ssh`	
表示	特権
パラメータ	なし
例:	
ssh サービスシステムを開始するには: `start ssh service`	

stop process core

表 A-36. stop process core

実行中のプロセスを停止してコアファイルを生成します。	
構文: `stop process core <pid>`	
表示	特権
パラメータ	<pid>: プロセス ID です
例:	
ID 33 のプロセスを中止するには: `stop process core 33`	

stop service nscd

表 A-37. stop service nscd

ネームサービスキャッシュデーモン (nscd) を停止します。	
構文: `stop service nscd`	
表示	特権
パラメータ	なし
例:	
ネームサービスキャッシュデーモンを停止するには: `stop service nscd`	

stop service postfix

表 A-38. stop service postfix

Postfix メールシステムを停止します。	
構文: `stop service postfix`	
表示	特権
パラメータ	なし
例:	
Postfix メールシステムを停止するには: `stop service postfix`	

stop service product

表 A-39. stop service product

製品サービスシステムを停止します。

構文: `stop service product`	
表示	特権
パラメータ	なし
例:	
製品サービスシステムを停止するには: `stop service product`	

stop service ssh

表 A-40. stop service ssh

ssh サービスシステムを停止します。	
構文: `stop service ssh`	
表示	特権
パラメータ	なし
例:	
ssh サービスシステムを停止するには: `stop ssh service`	

reboot

表 A-41. reboot

Deep Discovery Email Inspector アプライアンスを即時にまたは指定時間の経過後に再起動します。	
構文: `reboot [time]`	
表示	特権

パラメータ	[time]: Deep Discovery Email Inspector アプライアンスを再起動するまでの時間を分単位で指定します。
例:	
Deep Discovery Email Inspector アプライアンスを即時に再起動するには: `reboot`	
Deep Discovery Email Inspector アプライアンスを 5 分後に再起動するには: `reboot 5`	

resolve

表 A-42. resolve

ホスト名から IPv4 アドレスを解決したり、IPv4 アドレスからホスト名を解決したりします。	
構文: `resolve <dest>`	
表示	特権
パラメータ	<dest>: 解決する IPv4 アドレスまたはホスト名を指定します。
例:	
IP アドレス 192.168.10.1 からホスト名を解決するには: `resolve 192.168.10.1`	
ホスト名 parent.host.com から IP アドレスを解決するには: `resolve parent.host.com`	

show storage statistic

表 A-43. show storage statistic

ファイルシステムのディスク領域使用率を表示します。
構文: `show storage statistic [partition]`

表示	標準
パラメータ	[partition]: パーティションを指定します。このパラメータはオプションです。
例:	
Deep Discovery Email Inspector アプライアンスのファイルシステムのディスク領域使用率を表示するには: `show storage statistic`	

show network

表 A-44. show network

Deep Discovery Email Inspector のさまざまなネットワーク設定を表示します。	
構文: `show network [arp <address> | connections | dns | dns ipv6| hostname | interface | route | route ipv4 | route default ipv4 | route default ipv6]`	
表示	標準

パラメータ	arp: 指定したアドレスに対してアドレス解決プロトコル (ARP) で返された値を表示します。 <address>: アドレス解決プロトコル (ARP) で解決される FQDN または IP アドレスです。 connections: Deep Discovery Email Inspector アプライアンスの現在のネットワーク接続を表示します。 dns: Deep Discovery Email Inspector アプライアンスの DNS の IP アドレスを表示します。 dns ipv6: IPv6 のシステム DNS 設定を表示します。 hostname: Deep Discovery Email Inspector アプライアンスのホスト名を表示します。 interface: ネットワークインタフェースカード (NIC) のステータスと設定を表示します。 route: IP アドレスのルーティングテーブルを表示します。 route ipv4: システムの IPv4 ルーティングテーブルを表示します。 route default ipv4: 初期設定の IPv4 ルーティングテーブルを表示します。 route default ipv6: 初期設定の IPv6 ルーティングテーブルを表示します。
例:	
アドレス「10.2.23.41」に対する ARP の情報を表示するには: `show network arp 10.2.23.41`	
Deep Discovery Email Inspector アプライアンスの現在のネットワーク接続を表示するには: `show network connections`	
DNS 設定を表示するには: `show network dns`	
IPv6 のシステム DNS 設定を表示するには: `show network dns ipv6`	

Deep Discovery Email Inspector アプライアンスのホスト名を表示するには: `show network hostname`
NIC のステータスと設定を表示するには: `show network interface`
IP アドレスのルーティングテーブルを 表示するには: `show network route`
システムの IPv4 ルーティングテーブルを 表示するには: `show network route ipv4`
システムの初期設定の IPv4 ゲートウェイを表示するには: `show network route default ipv4`
システムの初期設定の IPv6 ゲートウェイを表示するには: `show network route default ipv6`

show kernel

表 A-45. show kernel

Deep Discovery Email Inspector アプライアンスの OS カーネル情報を表示します。	
構文: `show kernel {messages | modules | parameters | iostat}`	
表示	標準
パラメータ	messages: カーネルメッセージを表示します。 modules: カーネルモジュールを表示します。 parameters: カーネルパラメータを表示します。 iostat: デバイスとパーティションの CPU 統計および I/O 統計を表示します。
例:	

OS カーネルのメッセージを表示するには: `show kernel messages`
OS カーネルのモジュールを表示するには: `show kernel modules`
OS カーネルのパラメータを表示するには: `show kernel parameters`
CPU 統計および I/O 統計を表示するには: `show kernel iostat`

show service

表 A-46. show service

Deep Discovery Email Inspector サービスのステータスを表示します。	
構文: `show service [ntp <enabled | server-address> | ssh | nscd]`	
表示	標準
パラメータ	nscd: ネームサービスキャッシュデーモン (nscd) のステータスを表示します。 ntp enabled: システムの NTP サービスのステータスを表示します。 ntp server-address: システムの NTP サービスのサーバアドレスを表示します。 ssh: SSH のステータスを表示します。
例:	
ネームサービスキャッシュデーモン (nscd) のステータスを表示するには: `show service nscd`	
NTP サービスのステータスを表示するには: `show service ntp`	

SSH のステータスを表示するには: `show service ssh`

show memory

表 A-47. show memory

デバイスのシステムメモリ情報を表示します。	
構文: `show memory [vm | statistic]`	
表示	標準
パラメータ	vm:仮想メモリの統計を表示します。 statistic: システムメモリの統計を表示します。
例:	
仮想メモリの統計を表示するには: `show memory vm`	
システムメモリの統計を表示するには: `show memory statistic`	

show process

表 A-48. showprocess

現在実行中のプロセスのステータスを表示します。	
構文: `show process [top | stack | itrace | trace] [pid]`	
表示	標準

パラメータ	top: 現在実行中のプロセスとシステム関連プロセスのステータスを表示します。 stack: 実行プロセスのスタックトレースの印刷 itrace: ライブラリコールのトレース trace: システムコールとシグナルのトレース pid: プロセス ID 番号
例:	

現在実行中のプロセスのステータスを表示するには:
`show process`
プロセス 1233 のスタックトレースを表示するには:
`show process stack 1233`
プロセス 1233 のシステムコールを表示するには:
`show process trace 1233`
プロセス 1233 のライブラリコールを表示するには:
`show process itrace 1233`	

show product-info

表 A-49. show product-info

製品情報を表示します。	
構文: `show product-info [management-port | operation-mode | service-status | version`	
表示	標準

パラメータ	management-port: 管理ポートの IP アドレスとサブネットマスクを表示します。 operation-mode: Deep Discovery Email Inspector の操作モードを表示します。 service-status: サービスのステータスを表示します。 version: 製品バージョンを表示します。
例:	
管理ポートの IP アドレスとサブネットマスクを表示するには: `show product-info management-port` 操作モードを表示するには: `show product-info operation-mode` サービスのステータスを表示するには: `show-product-info service-status` Deep Discovery Email Inspector のビルドバージョンを表示するには: `show product-info version`	

show system

表 A-50. show system

さまざまなシステム設定を表示します。	
構文: `show system [date | timezone [continent | city | country]| uptime | version]`	
表示	標準

パラメータ	date: 現在の日付と時刻を表示します。 timezone: タイムゾーン設定を表示します。オプションで次のタイムゾーン情報を指定できます。 • continent: システムの大陸を表示 • city: システムの都市を表示 • country: システムの国/地域を表示 uptime: Deep Discovery Email Inspector アプライアンスの稼働時間を表示します。 version: Deep Discovery Email Inspector アプライアンスのバージョン番号を表示します。
例:	
Deep Discovery Email Inspector アプライアンスの現在の日時を表示するには: `show system date`	
タイムゾーン設定を表示するには: `show system timezone`	
Deep Discovery Email Inspector アプライアンスの大陸を表示するには: `show system timezone continent`	
Deep Discovery Email Inspector アプライアンスの都市を表示するには: `show system timezone city`	
Deep Discovery Email Inspector アプライアンスの国/地域を表示するには: `show system timezone country`	
Deep Discovery Email Inspector の稼働時間を表示するには: `show system uptime`	
Deep Discovery Email Inspector アプライアンスのバージョン番号を表示するには: `show system version`	

shutdown

表 A-51. shutdown

Deep Discovery Email Inspector アプライアンスを即時にまたは指定時間の経過後にシャットダウンします。	
構文: `shutdown [time]`	
表示	特権
パラメータ	[time]: Deep Discovery Email Inspector アプライアンスを指定した分数の経過後にシャットダウンします。
例:	
Deep Discovery Email Inspector アプライアンスを即時にシャットダウンするには: `shutdown`	
Deep Discovery Email Inspector アプライアンスを 5 分後にシャットダウンするには: `shutdown 5`	

traceroute

表 A-52. traceroute

指定した送信先への追跡ルートを表示します。	
構文: `traceroute [-h hops] <dest>`	
表示	標準
パラメータ	[-h hops]: 送信先までの最大ホップ数を指定します。最少数は 6 です。 <dest>: トレースするリモートシステムを指定します。
例:	
最大 6 ホップまでの IP アドレス 172.10.10.1 へのルートを表示するには: `traceroute 172.10.10.1`	

最大 30 ホップまでの IP アドレス 172.10.10.1 へのルートを表示するには:

```
traceroute -h 30 172.10.10.1
```

付録 B

通知のメッセージトークン

メールメッセージの通知をカスタマイズするには、メッセージトークンを追加します。

この章の内容は次のとおりです。

受信者通知メッセージトークン

Deep Discovery Email Inspector では、検出された脅威がメールメッセージに含まれていることを知らせる受信者通知を送信します。メールメッセージの処理後、検出されたリスクレベルに基づいて受信者通知が送信されます。メッセージトークンを使用して受信者通知をカスタマイズするには、次の表を使用します。

注意

受信者通知の設定の詳細については、135 ページの「受信者通知を設定する」を参照してください。

表 B-1. メッセージトークン

トークン	説明	例
%Action%	処理されたメッセージに対して実行する操作	• ブロックして隔離 • 添付ファイルの削除、ブロックページへのリンクのリダイレクト、およびタグ付け • 添付ファイルの削除、警告ページへのリンクのリダイレクト、およびタグ付け • 放置およびタグ付け • 放置および処理なし
%AttachmentNames%	検出された添付ファイルの上位 10 件	important.doc
%ConsoleURL%	Deep Discovery Email Inspector 管理コンソールの URL。	https://192.168.252.1/loginPage.ddei
%DateTime%	アラートが実行された日付と時刻	2014-03-21 03:34:09
%DeviceIP%	Deep Discovery Email Inspector アプライアンスの IP アドレス	123.123.123.123
%DeviceName%	Deep Discovery Email Inspector アプライアンスのホスト名	example.com

トークン	説明	例
%Risk%	メールメッセージのリスクレベル	• 高 • 中 • 低 • 未評価
%Sender%	送信中のメールアドレス	senderemail@example.com
%Subject%	メールメッセージの件名	夢の仕事!
%ThreatNames%	検出された脅威の上位 10 件	スパムメール/グレーメール

アラート通知のメッセージトークン

次の表は、アラート通知に使用できるトークンについて説明しています。メッセージトークンを使用してアラート通知をカスタマイズするには、次の表を参照してください。

注意

すべてのアラート通知にすべてのメッセージトークンを使用できるわけではありません。アラートのパラメータの仕様を確認してから、メッセージトークンを使用してください。詳細については、183 ページの「アラート通知パラメータ」を参照してください。

表 B-2. メッセージトークン

トークン	説明	備考
%Account%	Deep Discovery Email Inspector でロックされているアカウントのユーザ名	対象: • システム: アカウントのロック 例: • JohnDoe • テスト

トークン	説明	備考
%Action%	処理されたメッセージに対して実行する操作	対象: • ポリシー: 受信者への通知 例: • ポリシー: 受信者への通知 • 放置およびタグ付け
%AveSandboxProc%	過去 1 時間にメッセージの処理待ちおよび分析にかかった平均時間 (分単位)	対象: • システム: 仮想アナライザの処理時間の超過 例: • 3 • 2
%ComponentList%	コンポーネントのリスト	対象: • システム: コンポーネントのアップデート/ロールバック成功 • システム: コンポーネントのアップデート/ロールバック失敗 例: • ネットワークコンテンツ検査エンジン/ 0x48000204/ 9.862.1107 • ネットワークコンテンツ検査エンジン/ 0x48000204/ 不明
%ConsoleURL%	Deep Discovery Email Inspector 管理コンソールの URL。	対象: • すべて 例: • https://192.168.252.1/loginPage.ddei

トークン	説明	備考
%CPUThreshold%	許容される最大 CPU 使用率 (%)。これを超えるとアラート通知が送信されます。	対象: • システム: CPU 使用率の超過 例: • 95 • 85
%CPUUsage%	合計 CPU 使用率 (%)	対象: • システム: CPU 使用率の超過 例: • 80 • 65
%DateTime%	Deep Discovery Email Inspector でメールメッセージを受信した日付と時刻	対象: • すべて 例: • 2014-03-21 03:34:09 • 2014/06/15 11:31:22
%DaysBeforeExpirationATD%	高度な脅威対策の製品ライセンスの有効期限までの日数	対象: • システム: ライセンス有効期限 例: • 4 • 123
%DaysBeforeExpirationSEG%	ゲートウェイモジュールの製品ライセンスの有効期限までの日数	対象: • システム: ライセンス有効期限 例: • 4 • 123

トークン	説明	備考
%DeferredQueue%	遅延キューで処理を待機しているメールメッセージ件数	対象: • システム: メッセージ遅延キュー長の超過 例: • 100
%DeliveryQueue%	配信キューで処理を待機しているメールメッセージ件数	対象: • システム: メッセージ配信キュー長の超過 例: • 100 • 600
%DetectionCount%	指定された期間内に不審な特徴が検出されたメッセージの件数	対象: • システム: 検出の急増 例: • 50 • 200
%DetectionThreshold%	不審な特徴が検出されたメッセージの最大件数。この件数を超えるとアラート通知が送信されます。	対象: • システム: 検出の急増 例: • 50 • 40
%DeviceIP%	Deep Discovery Email Inspector アプライアンスの IP アドレス	対象: • すべて 例: • 123.123.123.123
%DeviceName%	Deep Discovery Email Inspector アプライアンスのホスト名	対象: • すべて

トークン	説明	備考
		例: • example.com
%DiagnosisTip%	問題の解決方法についての推奨事項	対象: • システム: 接続の問題
%DiskSpace%	最小空きディスク容量 (GB)。この容量を下回るとアラート通知が送信されます。	対象: • システム: ディスク空き容量の低下 • システム: 隔離ディスク空き容量の低下 例: • 2 • 30
%ExpirationDateATD%	高度な脅威対策の製品ライセンスの有効期限	対象: • システム: ライセンス有効期限 例: • 2014-03-21 03:34:09 • 2014/06/15 11:31:22
%ExpirationDateSEG%	ゲートウェイモジュールの製品ライセンスの有効期限	対象: • システム: ライセンス有効期限 例: • 2014-03-21 03:34:09 • 2014/06/15 11:31:22
%Interval%	メッセージ処理ボリュームを確認する頻度 (分単位)	対象: • システム: 検出の急増 • システム: 処理の急増 例:

トークン	説明	備考
		• 15 • 10
%LicenseStatusATD%	高度な脅威対策の製品ライセンスの現在のステータス	対象: • システム: ライセンス有効期限 例: • 体験版 • アクティベーション未完了 • アクティベート済み • 期限切れ • 更新猶予期間 詳細については、455 ページの「製品ライセンスのステータス」を参照してください。
%LicenseStatusSEG%	ゲートウェイモジュールの製品ライセンスの現在のステータス	対象: • システム: ライセンス有効期限 例: • 体験版 • アクティベーション未完了 • アクティベート済み • 期限切れ • 更新猶予期間 詳細については、455 ページの「製品ライセンスのステータス」を参照してください。
%LicenseTypeATD%	高度な脅威対策の製品ライセンスの種類	対象: • システム: ライセンス有効期限

トークン	説明	備考
		例: • 製品版 • 体験版
%LicenseTypeSEG%	ゲートウェイモジュールの製品ライセンスの種類	対象: • システム: ライセンス有効期限 例: • 製品版 • 体験版
%MemoryThreshold%	許容される最大メモリ使用率 (%)。これを超えるとアラート通知が送信されます。	対象: • システム: メモリ使用率の超過 例: 90
%MemoryUsage%	合計メモリ使用率 (%)	対象: • システム: メモリ使用率の超過 例: 90

%MessageList%	検出されたメッセージのリスト。これにはリスクレベル、脅威の名前、実行された処理、メッセージ ID、受信者、送信者、件名、最も危険性の高い添付ファイル上位 3 件の詳細、およびメッセージの受信日時が含まれます。
	このトークンは次のアラート通知に対して、検出された脅威の名前も提供します。
	• セキュリティ: 不審メッセージの検出
		対象:
		• セキュリティ: 不審メッセージの検出
		• セキュリティ: 高リスクのウォッチリスト対象受信者
		• システム: 隔離されたメッセージ
		• セキュリティ: 情報漏えい対策イベント
		例:
		`==========`
		`Risk: High (Suspicious`

トークン	説明	備考
	• セキュリティ: 高リスクのウォッチリスト対象受信者 • システム: 隔離されたメッセージ • セキュリティ: 情報漏えい対策イベント	File) Action: Action set to 'pass' Threat Name: EMERGING-THREAT_GENERIC.ERS|VAN_DROPPER.UMXX Message ID: <E1fk6FQ-00073X-Ns@funimo.com> Recipients: relay@njrelay.itlab.trendmicro.com Sender: aliconwamonic@yahoo.com Subject: Our Order#6501732 Attachment: 65017832.xls (Excel 95 or 97 spreadsheet), Company Profile.ZIP(ZIP archive) Detected: 2018-07-30 19:41:23 ========== ========== Risk: Medium (Malicious URL) Action: Quarantined Threat Name: LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS Message ID: <20180903210849.3B4D93A06C9@ddei155.localdomain> Recipients: bvt@ddei.com Sender: test@test.com Subject: Te_%*s'<>?|\@~$%^&#$!`~(=-+<>;:.){[]}(`)+=-_t"ddd, Attachment: (Link only) Detected: 2018-09-03 21:

トークン	説明	備考
		08:51 ================ ================ Message ID: <5C32BC03.9090201@test.com> Recipients: test@test.com;test@test1.com Sender: test@test.com Subject: 1033 Attachment: (Link only) DLP templates (Data identifiers): templateName (China: Mobile Phone Number) Detected: 2019-02-25 01:07:42 ================
%MTAList%	到達不能な MTA のリスト。各 MTA は IP アドレスとポート番号で表示されます。	対象: • システム: 到達不能なリレー MTA 例: • [1.1.1.1]:99 • [7.7.7.7]:77
%ProcessingCount%	指定された期間に処理されたメッセージの合計件数	対象: • システム: 処理の急増 例: • 50 • 200
%ProcessingThreshold%	指定された時間枠内で処理されたメッセージの最大件数。この件数を超えるとアラート通知が送信されます。	対象: • システム: 処理の急増 例:

トークン	説明	備考
		• 100 • 40
%QueueThreshold%	配信キュー内メッセージの最大件数。この件数を超えるとアラート通知が送信されます。	対象: • システム: メッセージ配信キュー長の超過 例: • 100 • 40
%SandboxProcThreshold%	平均のサンドボックス処理に割り当てられる最大時間。この時間を超えるとアラート通知が送信されます。	対象: • システム: 仮想アナライザの処理時間の超過 例: • 15 • 30
%SandboxQueue%	仮想アナライザによる分析を待機しているサンドボックスキュー内のメールメッセージ件数	対象: • システム: 仮想アナライザの送信キュー長の超過 例: • 30 • 75
%SandboxQueueThreshold%	サンドボックスキュー内メッセージの最大件数。この件数を超えるとアラート通知が送信されます。	対象: • システム: 仮想アナライザの送信キュー長の超過 例: • 100 • 75
%ServiceList%	接続の問題によって影響を受けるサービスのリスト	対象: • システム: 接続の問題

トークン	説明	備考
		例: • 内部仮想アナライザネットワーク (eth1、プロキシなし)
%ServiceName%	停止した Deep Discovery Email Inspector サービス 対象: • システム: サービス停止	対象: • システム: サービス停止 例: • 検索機能
%TotalMessages%	DKIM 署名に失敗したメッセージの総数	対象: • システム: DKIM 署名失敗 例 • 10 • 25

付録 C

接続とポート

サービスのアドレスとポート

Deep Discovery Email Inspector では、新しい脅威に関する情報を取得し、既存のトレンドマイクロ製品を管理するために、複数のトレンドマイクロサービスにアクセスします。次の表は、各サービスについての説明と、ご利用の地域での製品バージョンを入手するために必要なアドレスとポートの情報を示しています。

表 C-1. サービスのアドレスとポート

サービス	説明	アドレスとポート
アップデートサーバ	パターンファイルなどの製品コンポーネントのアップデートを提供します。コンポーネントのアップデートを定期的にリリースします。	http://ddei50-p.activeupdate.trendmicro.co.jp:80/activeupdate/japan https://ddei50-p.activeupdate.trendmicro.co.jp:443/activeupdate/japan
CSSS (ソフトウェア安全性評価サービス)	ファイルの安全性を確認します。CSSS を使用すると誤検出が減少し、計算時間や計算リソースが節約されます。	https://grid-global.trendmicro.com:443
コミュニティファイルレピュテーション	検出したファイルの出現率を判断します。出現率とは、あるファイルが一定期間内にトレンドマイクロのセンサで検出された回数を示す統計的概念です。	ddei510-jp-census.trendmicro.com:80
コミュニティドメイン/IP レピュテーションサービス	検出されたドメインと IP アドレスの出現率を判断します。出現率とは、あるドメインまたは IP アドレスが一定期間内にトレンドマイクロのセンサで検出された回数を示す統計的概念です。	ddei510-jp-domaincensus.trendmicro.com:80
サポート契約ポータル	お客さま情報、申し込み、製品やサービスのライセンスを管理します。	licenseupdate.trendmicro.com:80 clp.trendmicro.com:443
動的な URL 検索	URL のリアルタイム分析を実行して、ゼロデイ攻撃を検出します。	ddei5-0-jp.url.trendmicro.com:80

サービス	説明	アドレスとポート
プロキシ接続テスト	このリモートファイルへの接続を確立して、プロキシの設定を確認します。	http://www.msftncsi.com/ncsi.txt
機械学習型検索エンジン	不正プログラムモデリングの使用により、機械学習型検索では、サンプルを不正プログラムモデルと比較して可能性スコアを割り当て、ファイルに含まれる潜在的な不正プログラムの種類を判別します。	ddei51-jp-f.trx.trendmicro.com:443
スマートフィードバック	保護された脅威情報を Trend Micro Smart Protection Network と共有し、トレンドマイクロが新しい脅威を迅速に特定し、対処できるようにします。トレンドマイクロスマートフィードバックには、製品名、ID、バージョンなどの製品情報に加えて、ファイルタイプ、SHA-1 ハッシュ値、URL、IP アドレス、ドメインなどの検出情報も含まれる場合があります。	ddei500-jp.fbs25.trendmicro.com:443
Time-of-Click プロテクション	ユーザがクリックしたときに URL を書き換えて分析することにより、メールメッセージ内の不明な URL を検出して、リンクベースの不正プログラムとフィッシング攻撃からユーザを保護します。	ddei5-0-ctp.trendmicro.com:443
Threat Connect	環境内で検出された不審オブジェクトと Trend Micro Smart Protection Network の脅威データを関連付けます。生成されるインテリジェンスレポートを使用すれば、潜在的な脅威について調べ、攻撃プロファイルに適した対応ができます。	ddei5jp-threatconnect.trendmicro.com:443

サービス	説明	アドレスとポート
Trend Vision One	検出と対応をエンドポイントを超えて拡張し、より広範な可視性と専門家によるセキュリティ分析を提供することで、より多くの脅威の検出と早期の迅速な対応を実現します。Trend Vision One により、効果的に脅威に対応し、侵害の重大度と範囲を最小限に抑えることができます。	`*.xdr.trendmicro.com:443` `*.xdr.trendmicro.co.jp:443`
Web 検査サービス	Web レピュテーションサービスの補助サービスで、脅威結果の詳細なレベルと包括的な脅威名を提供します。 この脅威名と重大度は、積極的な処理とより集約的な検索を実行するためのフィルタ条件として使用できます。	`ddei5-0-jp-wis.trendmicro.com:443`

Web レピュテーションサービス	Web ドメインの信頼性を追跡します。Web サイトの新しさ、場所の変更履歴、不正プログラム動作分析で検出された不審活動の兆候などの要素に基づいて、レピュテーションスコアを割り当てます。	`ddei5-0-jp.url.trendmicro.com:80`
		`ddei5-0-jp-backup.url.trendmicro.com:80`
		`ddei5-0-usbx-jp.url.trendmicro.com:80` (内部仮想アナライザで使用)
		`ddei5-0-usbx-jp-backup.url.trendmicro.com:80` (内部仮想アナライザで使用)

アプライアンスで使用されるポート

次の表は、Deep Discovery Email Inspector で使用されるポートとその目的を示しています。

表 C-2. Deep Discovery Email Inspector で使用されるポート

ポート	プロトコル	機能	目的
22	TCP	インバウンド	エンドポイントは SSH 経由で Deep Discovery Email Inspector に接続します。
25	TCP	インバウンド	MTA とメールサーバは、Deep Discovery Email Inspector に SMTP 経由で接続します。
53	TCP/UDP	アウトバウンド	次のことを実行します。 • DNS を解決します。 • 送信者の認証 (SPF、DKIM、DMARC) のクエリを実行します。
80	TCP	待機およびアウトバウンド	他のコンピュータやトレンドマイクロの統合製品およびホステッドサービスに接続します。 • サポート契約ポータルに接続して製品ライセンスを管理します。 • コミュニティファイルレピュテーションサービスのクエリを実行します。 • コミュニティドメイン/IP レピュテーションサービスのクエリを実行します。 • Trend Micro Smart Protection Network を使用して Web レピュテーションサービスに対してクエリを実行します。 • イメージアップロードツールを使用して Deep Discovery Email Inspector に仮想アナライザイメージをアップロードします。 • Deep Discovery Email Inspector が HTTP 経由で登録されている場合、Trend Micro Apex Central と通信します。

ポート	プロトコル	機能	目的
123	UDP	アウトバウンド	NTP サーバに接続して時間を同期します。
161	UDP	インバウンド	このポートは SNMP マネージャからの要求を待機するために使用されます。
162	UDP	アウトバウンド	SNMP マネージャに接続して SNMP トラップメッセージを送信します。

ポート	プロトコル	機能	目的
443	TCP	待機およびアウトバウンド	次のことを実行します。 • 機械学習型検索エンジンに対してクエリを実行します。 • Web 検査サービスのクエリを実行します。 • コンピュータを使用して HTTPS 経由で管理コンソールにアクセスします。 • Trend Micro Apex Central と通信します。 • Trend Micro Smart Protection Network に接続して Web レピュテーションサービスのクエリを実行します。 • トレンドマイクロ Threat Connect に接続します。 • スマートフィードバックに保護された脅威情報を送信します。 • アップデートサーバに接続してコンポーネントをアップデートします。 • フィードバックサーバに製品の使用に関する情報を送信します。 • CSSS (Certified Safe Software Service) を使用してファイルの安全性を確認します。 • オンプレミスバージョンの Deep Discovery Director と通信します。 • 脅威インテリジェンス情報と除外リストを他の製品と共有します。
4459	TCP	待機およびアウトバウンド	エンドポイントはこのポートを通じて Deep Discovery Email Inspector のエンドユーザメール隔離の管理コンソールに接続します。

ポート	プロトコル	機能	目的
5274	TCP	アウトバウンド	Deep Discovery Email Inspector では、このポートを初期設定のポートとして使用し、Smart Protection Server に接続して Web レピュテーションサービスを利用します。
ユーザ指定	適用外	アウトバウンド	次のことを実行します。 • Syslog サーバにログを送信します。 • 脅威インテリジェンスを統合製品/サービスと共有します。 • 検出ログを SFTP サーバにアップロードします。 • Check Point Open Platform for Security (OPSEC) と通信します。 • サードパーティ認証や LDAP クエリのために LDAP サーバに接続します。

付録 D

SNMP オブジェクト ID

この付録の内容は次のとおりです。

SNMP クエリオブジェクト

表 D-1. memTotalSwap

項目	説明
OID	.1.3.6.1.4.1.2021.4.3
オブジェクト名	memTotalSwap
説明	このホストに設定されているスワップ領域の合計サイズ。

表 D-2. memAvailSwap

項目	説明
OID	.1.3.6.1.4.1.2021.4.4
オブジェクト名	memAvailSwap
説明	現在未使用または使用可能なスワップ領域のサイズ。

表 D-3. memTotalReal

項目	説明
OID	.1.3.6.1.4.1.2021.4.5
オブジェクト名	memTotalReal
説明	このホストにインストールされている実メモリ/物理メモリの合計サイズ。

表 D-4. memAvailReal

項目	説明
OID	.1.3.6.1.4.1.2021.4.6
オブジェクト名	memAvailReal
説明	現在未使用または使用可能な実メモリ/物理メモリのサイズ。

表 D-5. memTotalFree

項目	説明
OID	.1.3.6.1.4.1.2021.4.11
オブジェクト名	memTotalFree
説明	このホストの空きメモリまたは使用可能メモリの合計サイズ。この値は一般に、実メモリとスワップ領域または仮想メモリの合計になります。

表 D-6. memMinimumSwap

項目	説明
OID	.1.3.6.1.4.1.2021.4.12
オブジェクト名	memMinimumSwap
説明	このホストの通常動作中に維持するスワップ領域の最小空きサイズまたは最小使用可能サイズ。「memAvailSwap(4)」によりこの値が指定レベルを下回っていることが報告されると、「memSwapError(100)」が 1 に設定され、「memSwapErrorMsg(101)」でエラーメッセージが使用可能になります。

表 D-7. memShared

項目	説明
OID	.1.3.6.1.4.1.2021.4.13
オブジェクト名	memShared
説明	現在共有メモリに割り当てられている実メモリまたは仮想メモリの合計サイズ。この目的のために特別に予約されたメモリが基礎となる OS で明示的に識別されないホストでは、このオブジェクトは実装されません。

表 D-8. memBuffer

項目	説明
OID	.1.3.6.1.4.1.2021.4.14
オブジェクト名	memBuffer

項目	説明
説明	現在メモリバッファに割り当てられている実メモリまたは仮想メモリの合計サイズ。この目的のために特別に予約されたメモリが基礎となる OS で明示的に識別されないホストでは、このオブジェクトは実装されません。

表 D-9. memCached

項目	説明
OID	.1.3.6.1.4.1.2021.4.15
オブジェクト名	memCached
説明	現在キャッシュメモリに割り当てられている実メモリまたは仮想メモリの合計サイズ。この目的のために予約されたメモリが基礎となる OS で明示的に識別されないホストでは、このオブジェクトは実装されません。

表 D-10. memSwapError

項目	説明
OID	.1.3.6.1.4.1.2021.4.100
オブジェクト名	memSwapError
説明	「memAvailSwap(4)」により報告された使用可能なスワップ領域のサイズが「memMinimumSwap(12)」に指定された最小レベルを下回っているかどうかを示します。

表 D-11. memSwapErrorMsg

項目	説明
OID	.1.3.6.1.4.1.2021.4.101
オブジェクト名	memSwapErrorMsg
説明	「memAvailSwap(4)」により報告された使用可能なスワップ領域のサイズが「memMinimumSwap(12)」に指定された最小レベルを下回っているかどうかを説明します。

表 D-12. dskIndex

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.1
オブジェクト名	dskIndex
説明	ディスク MIB 用の整数の参照番号 (行番号)。

表 D-13. dskPath

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.2
オブジェクト名	dskPath
説明	ディスクのマウントパス。

表 D-14. dskDevice

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.3
オブジェクト名	dskDevice
説明	パーティション用デバイスのパス。

表 D-15. dskMinimum

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.4
オブジェクト名	dskMinimum
説明	ディスク残量 (MB) がこの値を下回るとエラーが実行されます。このオブジェクトまたは dskMinPercent がエージェントの snmpd.conf ファイルを介して設定されます。

表 D-16. dskMinPercent

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.5

項目	説明
オブジェクト名	dskMinPercent
説明	ディスク残量がこの割合を下回るとエラーが実行されます。このオブジェクトまたは dskMinimum がエージェントの snmpd.conf ファイルを介して設定されます。

表 D-17. dskTotal

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.6
オブジェクト名	dskTotal
説明	ディスク/パーティションの合計サイズ (KB)。

表 D-18. dskAvail

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.7
オブジェクト名	dskAvail
説明	使用可能なディスク容量。

表 D-19. dskUsed

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.8
オブジェクト名	dskUsed
説明	使用しているディスク容量。

表 D-20. dskPercent

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.9
オブジェクト名	dskPercent
説明	ディスクで使用されている容量の割合。

表 D-21. dskPercentNode

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.10
オブジェクト名	dskPercentNode
説明	ディスクで使用されている inode の割合。

表 D-22. dskErrorFlag

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.100
オブジェクト名	dskErrorFlag
説明	ディスクまたはパーティションの最小容量が設定値を下回っているかどうかを示すエラーフラグ。

表 D-23. dskErrorMsg

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.101
オブジェクト名	dskErrorMsg
説明	警告とディスク残量を示すエラーメッセージ。

表 D-24. ssSwapIn

項目	説明
OID	.1.3.6.1.4.1.2021.11.3
オブジェクト名	ssSwapIn
説明	過去 1 分間にディスクからスワップインされたメモリの平均値。

表 D-25. ssSwapOut

項目	説明
OID	.1.3.6.1.4.1.2021.11.4
オブジェクト名	ssSwapOut

項目	説明
説明	過去 1 分間にディスクにスワップアウトされたメモリの平均値。

表 D-26. ssIOSent

項目	説明
OID	.1.3.6.1.4.1.2021.11.5
オブジェクト名	ssIOSent
説明	過去 1 分間にディスクまたは他のブロックデバイスに書き込まれたデータの平均値。このオブジェクトは非推奨となっています。代わりに、任意の時間を対象に同じメトリックを計算する「ssIORawSent(57)」を使用することをお勧めします。

表 D-27. ssIOReceive

項目	説明
OID	.1.3.6.1.4.1.2021.11.6
オブジェクト名	ssIOReceive
説明	過去 1 分間にディスクまたは他のブロックデバイスから読み取られたデータの平均値。このオブジェクトは非推奨となっています。代わりに、任意の時間を対象に同じメトリックを計算する「ssIORawReceived(58)」を使用することをお勧めします。

表 D-28. ssSysInterrupts

項目	説明
OID	.1.3.6.1.4.1.2021.11.7
オブジェクト名	ssSysInterrupts
説明	過去 1 分間に処理された平均割り込み率 (クロックを含む)。このオブジェクトは非推奨となっています。代わりに、任意の時間を対象に同じメトリックを計算する「ssRawInterrupts(59)」を使用することをお勧めします。

表 D-29. ssSysContext

項目	説明
OID	.1.3.6.1.4.1.2021.11.8
オブジェクト名	ssSysContext
説明	過去 1 分間の平均コンテキストスイッチ率。このオブジェクトは非推奨となっています。代わりに、任意の時間を対象に同じメトリックを計算する「ssRawContext(60)」を使用することをお勧めします。

表 D-30. ssCpuUser

項目	説明
OID	.1.3.6.1.4.1.2021.11.9
オブジェクト名	ssCpuUser
説明	過去 1 分間にユーザレベルコードの処理に費やされた CPU 時間の割合。このオブジェクトは非推奨となっています。代わりに、任意の時間を対象に同じメトリックを計算する「ssCpuRawUser(50)」を使用することをお勧めします。

表 D-31. ssCpuSystem

項目	説明
OID	.1.3.6.1.4.1.2021.11.10
オブジェクト名	ssCpuSystem
説明	過去 1 分間にシステムレベルコードの処理に費やされた CPU 時間の割合。このオブジェクトは非推奨となっています。代わりに、任意の時間を対象に同じメトリックを計算する「ssCpuRawSystem(52)」を使用することをお勧めします。

表 D-32. ssCpuIdle

項目	説明
OID	.1.3.6.1.4.1.2021.11.11
オブジェクト名	ssCpuIdle

項目	説明
説明	過去 1 分間にアイドル状態であった CPU 時間の割合。このオブジェクトは非推奨となっています。代わりに、任意の時間を対象に同じメトリックを計算する「ssCpuRawIdle(53)」を使用することをお勧めします。

表 D-33. ssCpuRawUser

項目	説明
OID	.1.3.6.1.4.1.2021.11.50
オブジェクト名	ssCpuRawUser
説明	ユーザレベルコードの処理に費やされたチック数 (通常は 1/100 秒)。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。

表 D-34. ssCpuRawNice

項目	説明
OID	.1.3.6.1.4.1.2021.11.51
オブジェクト名	ssCpuRawNice
説明	優先度低下コードの処理に費やされたチック数 (通常は 1/100 秒)。この特別な CPU メトリックが、OS 上で計測されないホストではこのオブジェクトは実装されません。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。

表 D-35. ssCpuRawSystem

項目	説明
OID	.1.3.6.1.4.1.2021.11.52
オブジェクト名	ssCpuRawSystem

項目	説明
説明	システムレベルコードの処理に費やされたチック数 (通常は 1/100 秒)。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。このオブジェクトは「ssCpuRawWait(54)」カウンタや「ssCpuRawKernel(55)」カウンタと組み合わせて導入されることがあるため、全体的な行カウンタを合計する場合は注意が必要です。

表 D-36. ssCpuRawIdle

項目	説明
OID	.1.3.6.1.4.1.2021.11.53
オブジェクト名	ssCpuRawIdle
説明	アイドル状態であったチック数 (通常は 1/100 秒)。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。

表 D-37. ssCpuRawWait

項目	説明
OID	.1.3.6.1.4.1.2021.11.54
オブジェクト名	ssCpuRawWait
説明	IO を待機していたチック数 (通常は 1/100 秒)。この特別な CPU メトリックが、OS 上で計測されないホストではこのオブジェクトは実装されません。この時間は「ssCpuRawSystem(52)」カウンタに含まれることもあります。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。

表 D-38. ssCpuRawKernel

項目	説明
OID	.1.3.6.1.4.1.2021.11.55
オブジェクト名	ssCpuRawKernel

項目	説明
説明	カーネルレベルコードの処理に費やされたチック数 (通常は 1/100 秒)。この特別な CPU メトリックが、OS 上で計測されないホストではこのオブジェクトは実装されません。この時間は「ssCpuRawSystem(52)」カウンタに含まれることもあります。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。

表 D-39. ssCpuRawInterrupt

項目	説明
OID	.1.3.6.1.4.1.2021.11.56
オブジェクト名	ssCpuRawInterrupt
説明	ハードウェアの割り込みの処理に費やされたチック数 (通常は 1/100 秒)。この特別な CPU メトリックが、OS 上で計測されないホストではこのオブジェクトは実装されません。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。

表 D-40. ssIORawSent

項目	説明
OID	.1.3.6.1.4.1.2021.11.57
オブジェクト名	ssIORawSent
説明	ブロックデバイスに送信されたブロックの数。

表 D-41. ssIORawReceived

項目	説明
OID	.1.3.6.1.4.1.2021.11.58
オブジェクト名	ssIORawReceived
説明	ブロックデバイスから受信したブロックの数。

表 D-42. ssRawInterrupts

項目	説明
OID	.1.3.6.1.4.1.2021.11.59
オブジェクト名	ssRawInterrupts
説明	処理された割り込みの数。

表 D-43. ssRawContexts

項目	説明
OID	.1.3.6.1.4.1.2021.11.60
オブジェクト名	ssRawContexts
説明	コンテキストスイッチの数。

表 D-44. ssCpuRawSoftIRQ

項目	説明
OID	.1.3.6.1.4.1.2021.11.61
オブジェクト名	ssCpuRawSoftIRQ
説明	ソフトウェアの割り込みの処理に費やされたチック数 (通常は 1/100 秒)。この特別な CPU メトリックが、OS 上で計測されないホストではこのオブジェクトは実装されません。マルチプロセッサシステムでは「ssCpuRaw」カウンタはすべての CPU を対象に累計されるため、通常合計は N*100 (N はプロセッサ数) になります。

表 D-45. ssRawSwapIn

項目	説明
OID	.1.3.6.1.4.1.2021.11.62
オブジェクト名	ssRawSwapIn
説明	スワップインされたブロックの数。

表 D-46. ssRawSwapOut

項目	説明
OID	.1.3.6.1.4.1.2021.11.63
オブジェクト名	ssRawSwapOut
説明	スワップアウトされたブロックの数。

表 D-47. productVersion

項目	説明
OID	.1.3.6.1.4.1.6101.3004.1.1
オブジェクト名	productVersion
説明	Deep Discovery Email Inspector のバージョンを返します。

表 D-48. productBuild

項目	説明
OID	.1.3.6.1.4.1.6101.3004.1.2
オブジェクト名	productBuild
説明	Deep Discovery Email Inspector のビルド番号を返します。

表 D-49. productHotfix

項目	説明
OID	.1.3.6.1.4.1.6101.3004.1.3
オブジェクト名	productHotfix
説明	Deep Discovery Email Inspector の HotFix 番号を返します。

表 D-50. patternIndex

項目	説明
OID	.1.3.6.1.4.1.6101.3004.2.1.1
オブジェクト名	patternIndex

項目	説明
説明	パターンファイルのインデックスを返します。

表 D-51. patternID

項目	説明
OID	.1.3.6.1.4.1.6101.3004.2.1.2
オブジェクト名	patternID
説明	パターンファイルの ID を返します。

表 D-52. patternName

項目	説明
OID	.1.3.6.1.4.1.6101.3004.2.1.3
オブジェクト名	patternName
説明	パターンファイルの名前を返します。

表 D-53. patternVersion

項目	説明
OID	.1.3.6.1.4.1.6101.3004.2.1.4
オブジェクト名	patternVersion
説明	パターンファイルのバージョンを返します。

表 D-54. deliveryQueue

項目	説明
OID	.1.3.6.1.4.1.6101.3004.3.1
オブジェクト名	deliveryQueue
説明	配信キューの数を返します。

表 D-55. virtualAnalyzerQueue

項目	説明
OID	.1.3.6.1.4.1.6101.3004.3.2
オブジェクト名	virtualAnalyzerQueue
説明	仮想アナライザのキューの数を返します。

表 D-56. deferredQueue

項目	説明
OID	.1.3.6.1.4.1.6101.3004.3.3
オブジェクト名	deferredQueue
説明	遅延キューの数を返します。

表 D-57. ifIndex

項目	説明
OID	.1.3.6.1.4.1.6101.3004.4.1.1
オブジェクト名	ifIndex
説明	インタフェースのインデックスを返します。

表 D-58. ifDescr

項目	説明
OID	.1.3.6.1.4.1.6101.3004.4.1.2
オブジェクト名	ifDescr
説明	インタフェースの説明を返します。

表 D-59. ifReceiveThroughput

項目	説明
OID	.1.3.6.1.4.1.6101.3004.4.1.3
オブジェクト名	ifReceiveThroughput

項目	説明
説明	インタフェース受信スループットを返します。

表 D-60. ifTransmitThroughput

項目	説明
OID	.1.3.6.1.4.1.6101.3004.4.1.4
オブジェクト名	ifTransmitThroughput
説明	インタフェース送信スループットを返します。

SNMP トラップ

表 D-61. coldStart

項目	説明
OID	.1.3.6.1.6.3.1.1.5.1.0
オブジェクト名	coldStart
説明	通知の送信元アプリケーションをサポートしている SNMP エンティティが自身を再初期化していることと、その設定が変更されている可能性があることを意味します。

表 D-62. linkDown

項目	説明
OID	.1.3.6.1.6.3.1.1.5.3.0
オブジェクト名	linkDown
説明	エージェントの役割を担う SNMP エンティティで、そのいずれかの通信リンクの ifOperStatus オブジェクトが、(notPresent 以外の) 他の状態から切断状態に移行しようとしていることが検出されたこと意味します。他の状態は ifOperStatus の値によって示されます。

表 D-63. linkUp

項目	説明
OID	.1.3.6.1.6.3.1.1.5.4.0
オブジェクト名	linkUp
説明	エージェントの役割を担う SNMP エンティティで、そのいずれかの通信リンクの ifOperStatus オブジェクトが、切断状態から (notPresent 以外の) 他の状態に移行しようとしていることが検出されたこと意味します。他の状態は ifOperStatus の値によって示されます。

表 D-64. nsNotifyShutdown

項目	説明
OID	.1.3.6.1.4.1.8072.4.0.2
オブジェクト名	nsNotifyShutdown
説明	エージェントがシャットダウン中であることを示します。

表 D-65. vaStoppedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.1
オブジェクト名	vaStoppedNotification
説明	仮想アナライザが使用できないことを示します。

表 D-66. serviceStoppedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.2
オブジェクト名	serviceStoppedNotification
説明	サービスが停止して再起動できないことを示します。

表 D-67. unreachableMTANotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.3
オブジェクト名	unreachableMTANotification
説明	ドメインのリレー MTA に到達できないことを示します。

表 D-68. suspiciousMsgNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.4
オブジェクト名	suspiciousMsgNotification
説明	1 件以上のメールメッセージで脅威が検出されたことを示します。

表 D-69. watchlistNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.5
オブジェクト名	watchlistNotification
説明	脅威が検出された 1 件以上のメールメッセージがウォッチリストの受信者に送信されたことを示します。

表 D-70. deliveryQueueNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.6
オブジェクト名	deliveryQueueNotification
説明	配信キュー内のメールメッセージ数がしきい値の上限に達したことを示します。

表 D-71. cpuUsageNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.7

項目	説明
オブジェクト名	cpuUsageNotification
説明	CPU 使用率のレベルがしきい値の上限に達したことを示します。

表 D-72. vaQueueNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.8
オブジェクト名	vaQueueNotification
説明	仮想アナライザキュー内のメールメッセージ数がしきい値の上限に達したことを示します。

表 D-73. vaProcessTimeNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.9
オブジェクト名	vaProcessTimeNotification
説明	仮想アナライザの平均処理時間がしきい値の上限を上回っていることを示します。

表 D-74. diskSpaceNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.10
オブジェクト名	diskSpaceNotification
説明	使用可能なディスク容量がしきい値の下限を下回っていることを示します。

表 D-75. updateFailedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.11
オブジェクト名	updateFailedNotification

項目	説明
説明	コンポーネントのアップデートに失敗したことを示します。

表 D-76. updateSuccessNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.12
オブジェクト名	updateSuccessNotification
説明	コンポーネントのアップデートに成功したことを示します。

表 D-77. ntpFailedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.13
オブジェクト名	ntpFailedNotification
説明	NTP サーバとの時間の同期に失敗したことを示します。

表 D-78. vaProcessTimeoutNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.14
オブジェクト名	vaProcessTimeoutNotification
説明	分析結果を出力せずに分析処理がタイムアウトしたことを示します。

表 D-79. quarantineDiskSpaceNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.15
オブジェクト名	quarantineDiskSpaceNotification
説明	隔離ファイル用の使用可能なディスク容量がしきい値の下限に達したことを示します。

表 D-80. msgQuarantinedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.16
オブジェクト名	msgQuarantinedNotification
説明	1 件以上のメールメッセージが隔離されたことを示します。

表 D-81. memUsageNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.17
オブジェクト名	memUsageNotification
説明	メモリ使用率のレベルがしきい値の上限に達したことを示します。

表 D-82. deferredQueueNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.18
オブジェクト名	deferredQueueNotification
説明	遅延キュー内のメールメッセージ数がしきい値の上限に達したことを示します。

表 D-83. spamQuarantineSpaceNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.19
オブジェクト名	spamQuarantineSpaceNotification
説明	スパムメール隔離ファイル用の使用可能なディスク容量がしきい値の下限に達したことを示します。

表 D-84. accountLockedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.20
オブジェクト名	accountLockedNotification
説明	アカウントがロックされていることを示す通知です。

表 D-85. failedDKIMSignNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.21
オブジェクト名	failedDKIMSignNotification
説明	DKIM 署名に失敗したメッセージ数がしきい値の上限に達したことを示します。

表 D-86. connectionIssueNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.22
オブジェクト名	connectionIssueNotification
説明	アプライアンスが必要なリソースへの接続を確立できないことを示す通知です。

表 D-87. dataLossPreventionNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.23
オブジェクト名	dataLossPreventionNotification
説明	選択したテンプレートのメッセージ数がしきい値の下限に達したことを示す通知です。

表 D-88. encryptionExceptionNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.0.24
オブジェクト名	encryptionExceptionNotification
説明	Deep Discovery Email Inspector が暗号化または復号できなかったメッセージ数がしきい値の上限に達したことを示す通知です。

表 D-89. vaStoppedMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.1
オブジェクト名	vaStoppedMsg
説明	仮想アナライザが使用できないことを示すメッセージです。

表 D-90. serviceStoppedMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.2
オブジェクト名	serviceStoppedMsg
説明	サービスが停止して再起動できないことを示すメッセージです。

表 D-91. unreachableMTAMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.3
オブジェクト名	unreachableMTAMsg
説明	ドメインのリレー MTA に到達できないことを示すメッセージです。

表 D-92. suspiciousMsgMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.4

項目	説明
オブジェクト名	suspiciousMsgMsg
説明	1 件以上のメールメッセージで脅威が検出されたことを示すメッセージです。

表 D-93. watchlistMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.5
オブジェクト名	watchlistMsg
説明	脅威が検出された 1 件以上のメールメッセージがウォッチリストの受信者に送信されたことを示すメッセージです。

表 D-94. deliveryQueueMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.6
オブジェクト名	deliveryQueueMsg
説明	配信キュー内のメールメッセージ数がしきい値の上限に達したことを示すメッセージです。

表 D-95. cpuUsageMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.7
オブジェクト名	cpuUsageMsg
説明	CPU 使用率のレベルがしきい値の上限に達したことを示すメッセージです。

表 D-96. vaQueueMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.8
オブジェクト名	vaQueueMsg

項目	説明
説明	仮想アナライザキュー内のメールメッセージ数がしきい値の上限に達したことを示すメッセージです。

表 D-97. vaProcessTimeMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.9
オブジェクト名	vaProcessTimeMsg
説明	仮想アナライザの平均処理時間がしきい値の上限を上回っていることを示すメッセージです。

表 D-98. diskSpaceMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.10
オブジェクト名	diskSpaceMsg
説明	使用可能なディスク容量がしきい値の下限を下回っていることを示すメッセージです。

表 D-99. updateFailedMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.11
オブジェクト名	updateFailedMsg
説明	コンポーネントのアップデートに失敗したことを示すメッセージです。

表 D-100. updateSuccessMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.12
オブジェクト名	updateSuccessMsg

項目	説明
説明	コンポーネントのアップデートに成功したことを示すメッセージです。

表 D-101. ntpFailedMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.13
オブジェクト名	ntpFailedMsg
説明	NTP サーバとの時間の同期に失敗したことを示すメッセージです。

表 D-102. vaProcessTimeoutMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.14
オブジェクト名	vaProcessTimeoutMsg
説明	分析結果を出力せずに分析処理がタイムアウトしたことを示すメッセージです。

表 D-103. quarantineDiskSpaceMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.15
オブジェクト名	quarantineDiskSpaceMsg
説明	隔離ファイル用の使用可能なディスク容量がしきい値の下限に達したことを示すメッセージです。

表 D-104. msgQuarantinedMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.16
オブジェクト名	msgQuarantinedMsg

項目	説明
説明	1 件以上のメールメッセージが隔離されたことを示すメッセージです。

表 D-105. memUsageMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.17
オブジェクト名	memUsageMsg
説明	メモリ使用率のレベルがしきい値の上限に達したことを示すメッセージです。

表 D-106. deferredQueueMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.18
オブジェクト名	deferredQueueMsg
説明	遅延キュー内のメールメッセージ数がしきい値の上限に達したことを示すメッセージです。

表 D-107. spamQuarantineSpaceMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.19
オブジェクト名	spamQuarantineSpaceMsg
説明	スパムメール隔離ファイル用の使用可能なディスク容量がしきい値の下限に達したことを示すメッセージです。

表 D-108. accountLockedMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.20
オブジェクト名	accountLockedMsg
説明	アカウントがロックされていることを示すメッセージです。

表 D-109. failedDKIMSignMsg

項目	説明
OID	1.3.6.1.4.1.6101.3004.5.1.21
オブジェクト名	failedDKIMSignMsg
説明	DKIM 署名に失敗したメッセージ数がしきい値の上限に達したことを示すメッセージです。

表 D-110. connectionIssueMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.22
オブジェクト名	connectionIssueMsg
説明	アプライアンスが必要なリソースへの接続を確立できないことを示すメッセージです。

表 D-111. dataLossPreventionMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.23
オブジェクト名	dataLossPreventionMsg
説明	情報漏えい対策イベントの検出されたメッセージ数が指定したしきい値に達したことを示すメッセージです。

表 D-112. encryptionExceptionMsg

項目	説明
OID	.1.3.6.1.4.1.6101.3004.5.1.24
オブジェクト名	encryptionExceptionMsg
説明	Deep Discovery Email Inspector が暗号化または復号できなかったメッセージ数がしきい値の上限に達したことを示すメッセージです。

登録オブジェクト

OID	説明
.1.3.6.1.4.1.2021	UC Davis
.1.3.6.1.4.1.6101	Trend Micro, Inc.
.1.3.6.1.6.3.1.1.5.1	SNMPv2-MIB MIB
.1.3.6.1.4.1.8072	NET-SNMP-AGENT-MIB
.1.3.6.1.4.1.6101.999	TMCM
.1.3.6.1.4.1.6101.3001	TMTM
.1.3.6.1.4.1.6101.3004	DeepDiscoveryEmailInspector

付録 E

Deep Discovery Email Inspector での IPv6 のサポート

この付録の内容は、IPv6 アドレスをサポートする環境に Deep Discovery Email Inspector を配置する場合に必要となります。ここでは、Deep Discovery Email Inspector での IPv6 のサポート範囲について説明します。

Deep Discovery Email Inspector では、読者に IPv6 の概念と、IPv6 アドレスをサポートするネットワークの設定に関する知識があることを想定しています。

Deep Discovery Email Inspector では、バージョン 2.1 から IPv6 がサポートされています。それより前の Deep Discovery Email Inspector では、IPv6 アドレスはサポートされません。IPv6 のサポートは、Deep Discovery Email Inspector のインストール後またはアップグレード後に自動的に有効になります。

IPv6 がサポートされる Deep Discovery Email Inspector の機能は次のとおりです。

- メールメッセージの処理 (受信および配信)
- 管理コンソールと CLI のアクセス
- SMTP 通知
- SPAN/TAP モード
- Syslog サーバ

- 送信者フィルタ設定 (承認済み送信者、メールレピュテーション、ディレクトリハーベスト攻撃 (DHA) からの保護、バウンスメール攻撃からの保護、SMTP トラフィックスロットリング)
- 送信者の認証設定 (SPF のみ)
- エッジリレー MTA サーバ

IPv6 アドレスを設定する

CLI および管理コンソールで IPv6 アドレスを設定できます。設定のガイドラインは次のとおりです。

- Deep Discovery Email Inspector では標準表記の IPv6 アドレスを使用できます。

  例:

  ```
  2001:0db7:85a3:0000:0000:8a2e:0370:7334
  ```

  ```
  2001:db7:85a3:0:0:8a2e:370:7334
  ```

  ```
  2001:db7:85a3::8a2e:370:7334
  ```

  ```
  ::ffff:192.0.2.128
  ```

  注意

  Deep Discovery Email Inspector ではリンクローカルの IPv6 アドレスは使用できません。

- IPv6 アドレスが URL に含まれている場合は、そのアドレスを角カッコ ([]) で囲みます。

設定可能な IPv6 アドレス

IPv6 アドレスは管理コンソールおよび CLI で設定できます。

管理コンソールの IPv6 アドレス

IPv6 アドレスは、次の管理コンソール画面で設定できます。

- [管理] > [システム設定] > [ネットワーク]
- [管理] > [システム設定] > [SMTP]
- [管理] > [メール設定] > [ネットワーク接続]
- [管理] > [メール設定] > [メッセージ配信]
- [管理] > [メール設定] > [制限および除外]

- [管理] > [統合製品/サービス] > [Syslog]
- [管理] > [システム設定] > [操作モード] (SPAN/TAP モードルール)
- [管理] > [送信者フィルタ/認証] > [承認済み送信者]
- [管理] > [メール設定] > [エッジ MTA リレーサーバ]

CLI の IPv6 アドレス

IPv6 アドレスは、次の CLI コマンドを使用して設定できます。

- 470 ページの「configure product management-port」
- 471 ページの「configure network basic」
- 472 ページの「configure network dns」
- 474 ページの「configure network interface」
- 475 ページの「configure network route add」
- 475 ページの「configure network route default」
- 476 ページの「configure network route del」

付録 F

システムイベントログ

次の表は、Deep Discovery Email Inspector のシステムイベントログを示しています。

表 F-1. システムイベントログ

ID	ログの種類	メッセージ
11001	Update (アップデートイベント)	Product Updates: {USER} installed hot fix {VERSION} from {IP}
11002	Update (アップデートイベント)	Product Updates: {USER} rolled back hot fix {VERSION} from {IP}
11003	Update (アップデートイベント)	Product Updates: Appliance firmware upgraded by {USER} from {IP}
12001	Update (アップデートイベント)	Deep Discovery Director: Hotfix update successful
12002	Update (アップデートイベント)	Deep Discovery Director: Firmware update successful

ID	ログの種類	メッセージ
12003	Update (アップデートイベント)	Deep Discovery Director: Virtual Analyzer image import successful
12004	Update (アップデートイベント)	Deep Discovery Director: Configuration update successful
12005	Update (アップデートイベント)	Deep Discovery Director: Unregistered by Deep Discovery Director administrator
12101	Update (アップデートイベント)	Deep Discovery Director: Suspicious object synchronization with Apex Central disabled
12201	Update (アップデートイベント)	Deep Discovery Director: End-User Quarantine configuration disabled
130xx	Update (アップデートイベント)	ActiveUpdate: {COMPONENT} downloaded manually by {USER} from {IP}
131xx	Update (アップデートイベント)	ActiveUpdate: {COMPONENT} unsuccessfully downloaded manually by {USER} from {IP}
132xx	Update (アップデートイベント)	ActiveUpdate: {COMPONENT} downloaded by scheduled update
133xx	Update (アップデートイベント)	ActiveUpdate: {COMPONENT} unsuccessfully downloaded by scheduled update
134xx	Update (アップデートイベント)	ActiveUpdate: {COMPONENT} rolled back to version {VERSION} by {USER} from {IP}
135xx	Update (アップデートイベント)	ActiveUpdate: {COMPONENT} unsuccessfully rolled back by {USER} from {IP}

ID	ログの種類	メッセージ
136xx	Update (アップデートイベント)	ActiveUpdate Exception - Apply {COMPONENT} {VERSION} to local scanner failed
20101	Audit (監査ログ)	System started
20102	Audit (監査ログ)	System stopped
20201	Audit (監査ログ)	Service started
20202	Audit (監査ログ)	Service stopped
20301	Audit (監査ログ)	License: {NAME} license expired, grace period ends on {DATE}
20302	Audit (監査ログ)	License: {NAME} license expired
20303	Audit (監査ログ)	License: {NAME} license updated
20401	Audit (監査ログ)	System Maintenance: Device powered off by {USER} from {IP}
20402	Audit (監査ログ)	System Maintenance: Device restarted by {USER} from {IP}
20501	Audit (監査ログ)	Logon: 'admin' logged on from {HOST} via SSH
20502	Audit (監査ログ)	Logon: Attempted logon with user name ('admin') from {HOST} via SSH
20503	Audit (監査ログ)	Logon: 'root' logged on from {HOST} with token {NAME} via SSH
20504	Audit (監査ログ)	Logon: Attempted logon with user name ('root') from {HOST} via SSH

ID	ログの種類	メッセージ
20505	Audit (監査ログ)	Logon: 'admin' logged off from {HOST} via SSH
20506	Audit (監査ログ)	Logon: 'root' logged off from {HOST} with token {NAME} via SSH
20507	Audit (監査ログ)	Logon: Attempted logon with user name {USER} from {HOST} via SSH
30101	Audit (監査ログ)	Active update source setting was changed
30102	Audit (監査ログ)	Active update schedule setting was changed
30201	Audit (監査ログ)	System Settings: Host name saved as {NAME} by {USER} from {IP}
30202	Audit (監査ログ)	System Settings: {INTERFACE} IPv4 address and subnet mask were saved as {SUBNET} by {USER} from {IP}
30203	Audit (監査ログ)	System Settings: {INTERFACE} IPv6 address and prefix length were saved as {IP}/{LENGTH} by {USER} from {IP}
30204	Audit (監査ログ)	System Settings: {INTERFACE} IPv4 gateway saved as {GATEWAY} by {USER} from {IP}
30205	Audit (監査ログ)	System Settings: {INTERFACE} IPv6 gateway saved as {GATEWAY} by {USER} from {IP}
30206	Audit (監査ログ)	System Settings: {INTERFACE} primary IPv4 DNS server saved as {IP} and secondary IPv4 DNS server saved as {IP} by {USER} from {IP}
30207	Audit (監査ログ)	System Settings: {INTERFACE} primary IPv6 DNS server saved as {IP} and secondary IPv6 DNS server saved as {IP} by {USER} from {IP}
30208	Audit (監査ログ)	System Settings: {INTERFACE} IPv4 address and subnet mask deleted by {USER} from {IP}
30209	Audit (監査ログ)	System Settings: NIC teaming settings changed by {USER} from {IP}

ID	ログの種類	メッセージ
30301	Audit (監査ログ)	System Settings: Operation mode saved as {MODE} by {USER} from {IP}
30401	Audit (監査ログ)	System Settings: Proxy settings modified by {USER} from {IP}
30402	Audit (監査ログ)	System Settings: Proxy settings unsuccessfully modified by {USER} from {IP}
30501	Audit (監査ログ)	System Settings: SMTP server settings modified by {USER} from {IP}
30601	Audit (監査ログ)	System Settings: System time zone saved as {ZONE} by {USER} from {IP}
30602	Audit (監査ログ)	System Settings: NTP server synchronization enabled by {USER} from {IP}
30603	Audit (監査ログ)	System Settings: NTP server synchronization disabled by {USER} from {IP}
30604	Audit (監査ログ)	System Settings: System time saved as {TIME} by {USER} from {IP}
30605	Audit (監査ログ)	System Settings: Database time zone saved as {ZONE} by {USER} from {IP}
30606	Audit (監査ログ)	System Settings: NTP server saved as {NAME} by {USER} from {IP}
30701	Audit (監査ログ)	System Settings: SNMP settings modified by {USER} from {IP}
30702	Audit (監査ログ)	System Settings: SNMP MIB files downloaded by {USER} from {IP}
30703	Audit (監査ログ)	System settings: Session timeout setting modified by {USER} from {IP}
30704	Audit (監査ログ)	System Settings: SSL settings modified by {USER} from {IP}
30705	Audit (監査ログ)	System Settings: {USER} added certificate signing request {NAME} from {IP}

ID	ログの種類	メッセージ
30706	Audit (監査ログ)	System Settings: {USER} added self-signed certificate {NAME} from {IP}
30707	Audit (監査ログ)	System Settings: {USER} deleted certificate {NAME} from {IP}
30708	Audit (監査ログ)	System Settings: {USER} imported certificate {NAME} from {IP}
30709	Audit (監査ログ)	System Settings: {USER} changed certificate name from {NAME} to {NAME} from {IP}
30710	Audit (監査ログ)	System Settings: {USER} assigned certificate {NAME} to {SERVICE} from {IP}
30711	Audit (監査ログ)	System Settings: {USER} deleted trusted CA certificate {NAME} from {IP}
30712	Audit (監査ログ)	System Settings: {USER} imported trusted CA certificate {NAME} from {IP}
30801	Audit (監査ログ)	Mail Settings: SMTP Connection setting saved by {USER} from {IP}
30802	Audit (監査ログ)	Mail Settings: TLS certificate uploaded by {USER} from {IP}
30803	Audit (監査ログ)	Mail Settings: TLS certificate downloaded by {USER} from {IP}
30901	Audit (監査ログ)	Mail Settings: Delivery profiles exported by {USER} from {IP}
30902	Audit (監査ログ)	Mail Settings: Delivery profiles unsuccessfully exported by {USER} from {IP}
30903	Audit (監査ログ)	Mail Settings: Delivery profiles imported by {USER} from {IP}
30904	Audit (監査ログ)	Mail Settings: Mail Settings: Delivery profiles unsuccessfully imported due to maximum entries (256) exceeded
30905	Audit (監査ログ)	Mail Settings: Delivery profiles unsuccessfully imported by {USER} from {IP}

ID	ログの種類	メッセージ
30906	Audit (監査ログ)	Mail Settings: Delivery profile added by {USER} from {IP}
30907	Audit (監査ログ)	Mail Settings: Delivery profile modified by {USER} from {IP}
30908	Audit (監査ログ)	Mail Settings: Delivery profile deleted by {USER} from {IP}
31001	Audit (監査ログ)	Mail Settings: Mail settings modified by {USER} from {IP}
31101	Audit (監査ログ)	Mail Settings: SMTP server greeting saved by {USER} from {IP}
31102	Audit (監査ログ)	Mail Settings: Internal domain settings modified by {USER} from {IP}
31103	Audit (監査ログ)	Mail Settings: Internal domains imported by {USER} from {IP}
31103	Audit (監査ログ)	Mail Settings: Internal domain {NAME} added through a policy by {USER} from {IP}
31104	Audit (監査ログ)	Mail Settings: Address Rewriting settings modified by {USER} from {IP}
31105	Audit (監査ログ)	Mail Settings: Domain Rewriting settings modified by {USER} from {IP}
31106	Audit (監査ログ)	Mail Settings: {USER} added IP address or domain {NAME} from {IP} for incoming messages
31107	Audit (監査ログ)	Mail Settings: {USER} updated IP address or domain {NAME} from {IP} for incoming messages
31108	Audit (監査ログ)	Mail Settings: {USER} deleted one or more IP addresses or domains from {IP} for incoming messages
31109	Audit (監査ログ)	Mail Settings: {USER} imported one or more IP addresses or domains from {IP} for incoming messages
31110	Audit (監査ログ)	Mail Settings: {USER} enabled IP address or domain {NAME} from {IP} for incoming messages

ID	ログの種類	メッセージ
31111	Audit (監査ログ)	Mail Settings: {USER} disabled IP address or domain {NAME} from {IP} for incoming messages
31112	Audit (監査ログ)	Mail Settings: {USER} added domain {NAME} from {IP} for outgoing messages
31113	Audit (監査ログ)	Mail Settings: {USER} updated domain {NAME} from {IP} for outgoing messages
31114	Audit (監査ログ)	Mail Settings: {USER} deleted one or more domains from {IP} for outgoing messages
31115	Audit (監査ログ)	Mail Settings: {USER} imported one or more domains from {IP} for outgoing messages
31116	Audit (監査ログ)	Mail Settings: {USER} enabled domain {NAME} from {IP} for outgoing messages
31117	Audit (監査ログ)	Mail Settings: {USER} disabled domain {NAME} from {IP} for outgoing messages
31201	Audit (監査ログ)	Log Settings: {NAME} syslog server profile created by {USER} from {IP}
31202	Audit (監査ログ)	Log Settings: {NAME} syslog server profile deleted by {USER} from {IP}
31203	Audit (監査ログ)	Log Settings: {NAME} syslog server profile modified by {USER} from {IP}
31204	Audit (監査ログ)	Log Settings: {NAME} enabled by {USER} from {IP}
31205	Audit (監査ログ)	Log Settings: {NAME} disabled by {USER} from {IP}
31206	Audit (監査ログ)	Integrated Products/Services: {USER} synchronized data for all LDAP servers from {IP}
31207	Audit (監査ログ)	Integrated Products/Services: {USER} enabled LDAP server {NAME} from {IP} Log Settings: {NAME} disabled by {USER} from {IP}

ID	ログの種類	メッセージ
31208	Audit (監査ログ)	Integrated Products/Services: {USER} disabled LDAP server {NAME} from {IP}
31301	Audit (監査ログ)	Integrated Products/Services: SFTP Upload settings modified by {USER} from {IP}
31402	Audit (監査ログ)	Integrated Products/Services: {USER} added LDAP server {NAME} from {IP}
31403	Audit (監査ログ)	Integrated Products/Services: {USER} modified LDAP server {NAME} from {IP}
31404	Audit (監査ログ)	Integrated Products/Services: {USER} deleted LDAP server {NAME} from {IP}
31405	Audit (監査ログ)	Integrated Products/Services: {USER} synchronized data for LDAP server {NAME} from {IP}
31406	Audit (監査ログ)	Integrated Products/Services: {USER} synchronized data for all LDAP servers from {IP}
31407	Audit (監査ログ)	Integrated Products/Services: {USER} enabled LDAP server {NAME} from {IP}
31408	Audit (監査ログ)	Integrated Products/Services: {USER} disabled LDAP server {NAME} from {IP}
31501	Audit (監査ログ)	Integrated Products/Services: Threat Intelligent Sharing settings modified by {USER} from {IP}
31502	Audit (監査ログ)	Integrated Products/Services: {USER} generate suspicious objects list from {IP}
31601	Audit (監査ログ)	Integrated Products/Services: Auxiliary Products/Services settings modified by {USER} from {IP}
31602	Audit (監査ログ)	Integrated Products/Services: {USER} clicked Auxiliary Products/Services > Distribute Now from {IP}
31701	Audit (監査ログ)	Systems Settings: Apex Central settings modified by {USER} from {IP}
31702	Audit (監査ログ)	System Settings: Suspicious object synchronization enabled by {USER} from {IP}

ID	ログの種類	メッセージ
31703	Audit (監査ログ)	System Settings: Suspicious object synchronization disabled by {USER} from {IP}
31801	Audit (監査ログ)	System Settings: Proxy settings for Deep Discovery Director modified by {USER} by {IP}
31802	Audit (監査ログ)	System Settings: Registered to Deep Discovery Director by {USER} from {IP}
31803	Audit (監査ログ)	System Settings: Unregistered from Deep Discovery Director by {USER} from {IP}
31804	Audit (監査ログ)	System Settings: Deep Discovery Director fingerprint trusted by {USER} from {IP}
31901	Audit (監査ログ)	Scanning / Analysis: Image imported by {USER} from {IP}
31902	Audit (監査ログ)	Scanning / Analysis: Image deleted by {USER} from {IP}
31903	Audit (監査ログ)	Scanning / Analysis: Number of instances for each Virtual Analyzer image modified by {USER} from {IP}
32001	Audit (監査ログ)	Scanning / Analysis: Virtual Analyzer settings modified by {USER} from {IP}
32101	Audit (監査ログ)	Scanning / Analysis: {PRODUCT NAME} registered to the external Virtual Analyzer
32102	Audit (監査ログ)	Scanning / Analysis: Unable to register to the external Virtual Analyzer
32103	Audit (監査ログ)	Scanning / Analysis: {PRODUCT NAME} unregistered from the external Virtual Analyzer
32104	Audit (監査ログ)	Scanning / Analysis: Virtual Analyzer external integration settings modified by {USER} from ''%s''
32201	Audit (監査ログ)	Scanning / Analysis: File Passwords setting was modified by {USER} from {IP}
32301	Audit (監査ログ)	Scanning / Analysis: Smart Protection settings modified by {USER} from {IP}

ID	ログの種類	メッセージ
32401	Audit (監査ログ)	Scanning / Analysis: Smart Feedback settings modified by {USER} from {IP}
32501	Audit (監査ログ)	Scanning / Analysis: {USER} added YARA rule {NAME} from {IP}
32502	Audit (監査ログ)	Scanning / Analysis: {USER} modified YARA rule {NAME} from {IP}
32503	Audit (監査ログ)	Scanning / Analysis: {USER} deleted YARA rule {NAME} from {IP}
32504	Audit (監査ログ)	Scanning / Analysis: {USER} modified status for YARA rule {NAME} from {IP}
32510	Audit (監査ログ)	Scanning / Analysis: Time-of-Click settings modified by {USER} from {IP}
32520	Audit (監査ログ)	Scanning / Analysis: High-Profile Users settings modified by {USER} from {IP}
32521	Audit (監査ログ)	Scanning / Analysis: Internal Domains settings modified by {USER} from {IP}
32522	Audit (監査ログ)	Scanning / Analysis: Approved Senders settings modified by {USER} from {IP}
32523	Audit (監査ログ)	Scanning / Analysis: Cousin Domains settings modified by {USER} from {IP}
32530	Audit (監査ログ)	Scanning / Analysis: URL Scanning setting modified by {USER} from {IP}
32601	Audit (監査ログ)	System Maintenance: Configuration imported by {USER} from {IP}
32602	Audit (監査ログ)	System Maintenance: Configuration unsuccessfully imported by {USER} from {IP}
32603	Audit (監査ログ)	System Maintenance: Configuration exported by {USER} from {IP}
32604	Audit (監査ログ)	System Maintenance: Configuration unsuccessfully exported by {USER} from {IP}

ID	ログの種類	メッセージ
32701	Audit (監査ログ)	System Maintenance: Data purge started automatically
32702	Audit (監査ログ)	System Maintenance: Data purge completed ({MIN} min {SEC} s)
32703	Audit (監査ログ)	System Maintenance: Storage maintenance setting modified by {USER} from {IP}
32801	Audit (監査ログ)	System Maintenance: System log level setting modified by {USER} from {IP}
32901	Audit (監査ログ)	Accounts / Contacts: {USER} created the account {NAME} from {IP}
32902	Audit (監査ログ)	Accounts / Contacts: {USER} deleted the account {NAME} from {IP}
32903	Audit (監査ログ)	Accounts / Contacts: {USER} modified the account {NAME} from {IP}
32904	Audit (監査ログ)	Accounts / Contacts: {USER} unlocked the account {NAME} from {IP}
33001	Audit (監査ログ)	Logon: {USER} logged on as {ROLE} role from {IP}
33002	Audit (監査ログ)	Logon: {USER} logged off from {IP}
33003	Audit (監査ログ)	Logon: Attempted logon with an invalid user name ({USER}) or password from {IP}
33004	Audit (監査ログ)	Logon: Attempted logon with a disabled user name ({USER}) from {IP}
33005	Audit (監査ログ)	Logon: Attempted logon with a locked user name {NAME} from {IP}
33006	Audit (監査ログ)	Logon: Unlocked user name {NAME} from {IP}
33007	Audit (監査ログ)	RDQA Logon: ''{USER}'' logged on as {NAME} role from {IP}

ID	ログの種類	メッセージ
33008	Audit (監査ログ)	RDQA Logon: ''{USER}'' logged off
33009	Audit (監査ログ)	RDQA Logon: Attempted logon with an invalid user name ''{USER}'' or password from {IP}
33010	Audit (監査ログ)	RDQA Logon: Attempted logon with a disabled user name ''{USER}'' from {IP}
33011	Audit (監査ログ)	RDQA Logon: Attempted logon with a locked user name ''{USER}'' from {IP}
33012	Audit (監査ログ)	RDQA Logon: Unlocked user name ''{USER}'' from {IP}
33101	Audit (監査ログ)	Accounts / Contacts: Contacts for alert notifications and reports modified by {USER} from {IP}
33201	Audit (監査ログ)	Accounts / Contacts: {USER} modified the password for {NAME} from {IP}
33202	Audit (監査ログ)	Accounts / Contacts: {USER} added SAML group {NAME} from {IP}
33203	Audit (監査ログ)	Accounts / Contacts: {USER} modified SAML group {NAME} from {IP}
33204	Audit (監査ログ)	Accounts / Contacts: {USER} deleted SAML group {NAME} from {IP}
33205	Audit (監査ログ)	Accounts / Contacts: {USER} enabled SAML group {NAME} from {IP}
33206	Audit (監査ログ)	Accounts / Contacts: {USER} disabled SAML group {NAME} from {IP}
33301	Audit (監査ログ)	License: {NAME} license activated by {USER} from {IP}
33302	Audit (監査ログ)	License: Attempted to activate {NAME} license using an invalid Activation Code by {USER} from {IP}
33303	Audit (監査ログ)	License: {NAME} license updated by {USER} from {IP}

ID	ログの種類	メッセージ
33401	Audit (監査ログ)	Policy: Policy setting changed by {USER} from {IP}
33402	Audit (監査ログ)	Policy: {USER} added policy {NAME} from {IP}
33403	Audit (監査ログ)	Policy: {USER} modified policy {NAME} from {IP}
33404	Audit (監査ログ)	Policy: {USER} imported policies from {IP}
33405	Audit (監査ログ)	Policy: {USER} deleted policy {NAME} from {IP}
33406	Audit (監査ログ)	Policy: {USER} copied policy {NAME} from {IP}
33407	Audit (監査ログ)	Policy: {USER} enabled policy {NAME} from {IP}
33408	Audit (監査ログ)	Policy: {USER} disabled policy {NAME} from {IP}
33409	Audit (監査ログ)	Policy: {USER} modified priority setting of policy {NAME} from {PRIORITY} to {PRIORITY} from {IP}
33410	Audit (監査ログ)	Policy: {USER} added content filtering rule {NAME} from {IP}
33411	Audit (監査ログ)	Policy: {USER} updated content filtering rule {NAME} from {IP}
33412	Audit (監査ログ)	Policy: {USER} copied content filtering rule {NAME} from {IP}
33413	Audit (監査ログ)	Policy: {USER} deleted content filtering rule {NAME} from {IP}
33414	Audit (監査ログ)	Policy: {USER} added antispam rule {NAME} from {IP}
33415	Audit (監査ログ)	Policy: {USER} updated antispam rule {NAME} from {IP}

ID	ログの種類	メッセージ
33416	Audit (監査ログ)	Policy: {USER} copied antispam rule {NAME} from {IP}
33417	Audit (監査ログ)	Policy: {USER} deleted antispam rule {NAME} from {IP}
33418	Audit (監査ログ)	Policy: {USER} added advanced threat protection rule {NAME} from {IP}
33419	Audit (監査ログ)	Policy: {USER} updated advanced threat protection rule {NAME} from {IP}
33420	Audit (監査ログ)	Policy: {USER} copied advanced threat protection rule {NAME} from {IP}
33421	Audit (監査ログ)	Policy: {USER} deleted advanced threat protection rule {NAME} from {IP}
33422	Audit (監査ログ)	Policy: {USER} added policy notification {NAME} from {IP}
33423	Audit (監査ログ)	Policy: {USER} modified policy notification {NAME} from {IP}
33424	Audit (監査ログ)	Policy: {USER} deleted some policy notifications from {IP}
33425	Audit (監査ログ)	Policy: {USER} copied policy notification {NAME} from {IP}
33426	Audit (監査ログ)	Policy: {USER} added archive server {NAME} from {IP}
33427	Audit (監査ログ)	Policy: {USER} modified archive server {NAME} from {IP}
33428	Audit (監査ログ)	Policy: {USER} deleted some archive servers from {IP}
33429	Audit (監査ログ)	Policy: {USER} added DLP rule {NAME} from {IP}
33430	Audit (監査ログ)	Policy: '{USER} updated DLP rule {NAME} from {IP}

ID	ログの種類	メッセージ
33431	Audit (監査ログ)	Policy: {USER} copied DLP rule {NAME} from {IP}
33432	Audit (監査ログ)	Policy: {USER} deleted DLP rule {NAME} from {IP}
33433	Audit (監査ログ)	Policy Objects: {USER} added expression {NAME} from {IP}
33434	Audit (監査ログ)	Policy Objects: {USER} updated expression {NAME} from {IP}
33435	Audit (監査ログ)	Policy Objects: {USER} copied expression {NAME} from {IP}
33436	Audit (監査ログ)	Policy Objects: {USER} deleted expression {NAME} from {IP}
33437	Audit (監査ログ)	Policy Objects: {USER} imported expression file from {IP}
33438	Audit (監査ログ)	Policy Objects: {USER} added file attribute {NAME} from {IP}
33439	Audit (監査ログ)	Policy Objects: {USER} updated file attribute {NAME} from {IP}
33440	Audit (監査ログ)	Policy Objects: {USER} copied file attribute {NAME} from {IP}
33441	Audit (監査ログ)	Policy Objects: {USER} deleted file attribute {NAME} from {IP}
33442	Audit (監査ログ)	Policy Objects: {USER} imported file attribute file from {IP}
33443	Audit (監査ログ)	Policy Objects: {USER} added keyword list {NAME} from {IP}
33444	Audit (監査ログ)	Policy Objects: {USER} updated keyword list {NAME} from {IP}
33445	Audit (監査ログ)	Policy Objects: {USER} copied keyword list {NAME} from {IP}

ID	ログの種類	メッセージ
33446	Audit (監査ログ)	Policy Objects: {USER} deleted keyword list {NAME}from {IP}
33447	Audit (監査ログ)	Policy Objects: {USER} imported keyword list file from {IP}
33448	Audit (監査ログ)	Policy Objects: {USER} added template {NAME} from {IP}
33449	Audit (監査ログ)	Policy Objects: {USER} updated template {NAME} from {IP}
33450	Audit (監査ログ)	Policy Objects: {USER} copied template {NAME} from {IP}
33451	Audit (監査ログ)	Policy Objects: {USER} deleted template {NAME} from {IP}
33452	Audit (監査ログ)	Policy Objects: {USER} imported template file from {IP}
33453	Audit (監査ログ)	Policy Objects: {USER} added policy stamp {NAME} from {IP}
33454	Audit (監査ログ)	Policy Objects: {USER} modified policy stamp {NAME} from {IP}
33455	Audit (監査ログ)	Policy Objects: {USER} deleted some policy stamps from {IP}
33456	Audit (監査ログ)	Policy Objects: {USER} enabled policy stamp {NAME} from {IP}
33457	Audit (監査ログ)	Policy Objects: {USER} disabled policy stamp {NAME} from {IP}
33458	Audit (監査ログ)	Policy Objects: {USER} added address group {NAME} from {IP}
33459	Audit (監査ログ)	Policy Objects: {USER} deleted address group {NAME} from {IP}
33460	Audit (監査ログ)	Policy Objects: {USER} updated address group {NAME} from {IP}

ID	ログの種類	メッセージ
33501	Audit (監査ログ)	Policy: Policy exception settings modified by {USER} from {IP}
33502	Audit (監査ログ)	Policy: Graymail exception settings modified by {USER} from {IP}
33601	Audit (監査ログ)	Alerts: Alert rule settings modified by {USER} from {IP}
33701	Audit (監査ログ)	Report: Report settings changed by {USER} from {IP}
33801	Audit (監査ログ)	Detected Messages: Message {NAME} downloaded by {USER} from {IP}
33802	Audit (監査ログ)	Detected Messages: Investigation package {NAME} downloaded by {USER} from {IP}
33803	Audit (監査ログ)	Detected Messages: Screenshot of message {NAME} viewed by {USER} from {IP}
33804	Audit (監査ログ)	Detected Messages: Virtual Analyzer report of message {NAME} viewed by {USER} from {IP}
33901	Audit (監査ログ)	Quarantine: MsgID {ID} released by {USER} from {IP}
33902	Audit (監査ログ)	Quarantine: MsgID {ID} deleted by {USER} from {IP}
33903	Audit (監査ログ)	Quarantine: Resumed processing message {ID} by {USER} from {IP}
33904	Audit (監査ログ)	Quarantine: Message {ID} unlocked and reprocessed by {USER} from {IP}
34001	Audit (監査ログ)	Unable to distribute suspicious objects to Check Point OPSEC.Verify that the Check Point OPSEC settings are correct and that no network problem exists.
34002	Audit (監査ログ)	Unable to distribute suspicious objects to Trend Micro TippingPoint SMS.Verify that the Trend Micro TippingPoint SMS settings are correct and that no network problem exists.

ID	ログの種類	メッセージ
34003	Audit (監査ログ)	Unable to distribute suspicious objects to IBM Security Network Protection XGS.Verify that the IBM Security Network Protection XGS settings are correct and that no network problem exists.
34004	Audit (監査ログ)	Unable to distribute suspicious objects to Palo Alto Panorama or Firewalls.Verify that the Palo Alto Panorama or Firewalls settings are correct and that no network problem exists.
34005	Audit (監査ログ)	Unable to generate suspicious objects list.Verify that the Threat Intelligence Sharing settings are correct.
34101	Audit (監査ログ)	End-User Quarantine: EUQ settings modified by {USER} from {IP}
34102	Audit (監査ログ)	End-User Quarantine: User Quarantine Access settings modified by {USER} from {IP}
34103	Audit (監査ログ)	End-User Quarantine: EUQ Digest settings modified by {USER} from {IP}
34201	Audit (監査ログ)	Sender Filtering: Approved Senders list modified by {USER} from {IP}
34202	Audit (監査ログ)	Sender Filtering: ERS settings modified by {USER} from {IP}
34203	Audit (監査ログ)	Sender Filtering: DHA protection settings modified by {USER} from {IP}
34204	Audit (監査ログ)	Sender Filtering: Bounced attack protection settings modified by {USER} from {IP}
34205	Audit (監査ログ)	Sender Filtering: SMTP traffic throttling settings modified by {USER} from {IP}
34206	Audit (監査ログ)	Sender Filtering: Blocked Senders list modified by {USER} from {IP}
34207	Audit (監査ログ)	Sender Filtering: Some Blocked Senders list entries moved to Approved Senders list by {USER} from {IP}
34208	Audit (監査ログ)	Sender Filtering: SPF settings modified by {USER} from {IP}

ID	ログの種類	メッセージ
34209	Audit (監査ログ)	Sender Filtering: DKIM Authentication settings modified by {USER} from {IP}
34210	Audit (監査ログ)	Sender Filtering: DKIM Signatures settings modified by {USER} from {IP}
34211	Audit (監査ログ)	Sender Filtering: DMARC settings modified by {USER} from {IP}
35001	Audit (監査ログ)	Message Queues: Messages deleted by {USER} from {IP}
35002	Audit (監査ログ)	Message Queues: Messages delivered by {USER} from {IP}
35003	Audit (監査ログ)	Message Queues: All messages delivered by {USER} from {IP}
35004	Audit (監査ログ)	Message Tracking: Investigation package {NAME} downloaded by {USER} from {IP}
35005	Audit (監査ログ)	Email Submissions: Message submitted by {USER} from {IP}
35006	Audit (監査ログ)	Message Queues: Messages rerouted by to {IP} by {USER} from {IP}
35007	Audit (監査ログ)	Message Queues: All messages rerouted by to {IP} by {USER} from {IP}
35008	Audit (監査ログ)	Message Queues: All messages deleted by {USER} from {IP}
35011	Audit (監査ログ)	Integrated Products/Services: Registered to Email Encryption server by {USER} from {IP}
35012	Audit (監査ログ)	Integrated Products/Services: Domain {DOMAIN} added to Email Encryption server by {USER} from {IP}
35013	Audit (監査ログ)	Integrated Products/Services: Domain {DOMAIN} deleted from Email Encryption server by {USER} from {IP}
35014	Audit (監査ログ)	Integrated Products/Services: Key file uploaded to Email Encryption server for domain {DOMAIN} by {USER} from {IP}

ID	ログの種類	メッセージ
35016	Audit (監査ログ)	Integrated Products/Services: Default sender modified to {SENDER} for Email Encryption by {USER} from {IP}
35017	Audit (監査ログ)	Integrated Products/Services: Email address modified to {EMAIL} for Email Encryption by {USER} from {IP}
35021	Audit (監査ログ)	Integrated Products/Services: {USER} added identity provider server {NAME} from {IP}
35022	Audit (監査ログ)	Integrated Products/Services: {USER} modified identity provider server {NAME} from {IP}
35023	Audit (監査ログ)	Integrated Products/Services: {USER} deleted identity provider server {NAME} from {IP}
35024	Audit (監査ログ)	Integrated Products/Services: {USER} enabled identity provider server {NAME} from {IP}
35025	Audit (監査ログ)	Integrated Products/Services: {USER} disabled identity provider server {NAME} from {IP}
35026	Audit (監査ログ)	Integrated Products/Services: {USER} updated certificate for management console from {IP}
35027	Audit (監査ログ)	Integrated Products/Services: {USER} updated certificate for EUQ console from {IP}
35028	Audit (監査ログ)	Logon: {USER} logged on via identity provider server {NAME} as {ROLE} from {IP}
35029	Audit (監査ログ)	Logon: {USER} logged off via identity provider server {NAME} from {IP}
41001	エンドユーザメール隔離ログ	EUQ: {USER} logged on from {IP}
41002	エンドユーザメール隔離ログ	EUQ: {USER} logged off from {IP}
41003	エンドユーザメール隔離ログ	EUQ: MsgID {ID} released by {USER} from {IP}

ID	ログの種類	メッセージ
41004	エンドユーザメール隔離ログ	EUQ: MsgID {ID} deleted by {USER} from {IP}
41005	エンドユーザメール隔離ログ	EUQ: Approved Senders list modified by {USER} from {IP}
41006	エンドユーザメール隔離ログ	EUQ: {USER} logged on via identity provider server {NAME} from {IP}
41007	エンドユーザメール隔離ログ	EUQ: {USER} logged off via identity provider server {NAME} from {IP}

付録 G

送信者の認証のエラーコード

ここでは、送信者の各認証プロトコルのエラーコードについて説明します。

Sender Policy Framework (SPF) のエラーコード

表 G-1. SPF エラーコードの分類

エラータイプ	エラーコード
無効な SPF レコード	3〜25、27~32
SPF レコードなし	2
内部エラー	-99、1、26

表 G-2. SPF エラーコード

エラーコード	内容
-99	内部エラー
1	メモリ不足
2	SPF レコードなし
3	構文エラー
4	修飾子にプレフィックスが含まれています
5	無効な文字が見つかりました

エラーコード	内容
6	不明なメカニズムが見つかりました
7	無効なオプションが見つかりました
8	CIDR の長さが無効です
9	必要なオプションがありません
10	内部エラー
11	エスケープ文字%が無効です
12	マクロ変数が無効です
13	サブドメインの切り捨ての長さが大きすぎます
14	区切り文字が無効です
15	オプションの文字列が長すぎます
16	必要以上のメカニズムがあります
17	必要以上の修飾子があります
18	メカニズムで必要以上の DNS 検索が使用されています
19	IPv4 アドレスが無効です
20	IPv6 アドレスが無効です
21	メカニズムのプレフィックスが無効です
22	SPF の結果が不明です
23	変数が初期化されていません
24	修飾子が見つかりません
25	必要な設定が行われていません
26	DNS 検索に失敗しました
27	ホスト名または形式が無効です
28	ホスト名の TLD が無効か見つかりません

エラーコード	内容
29	"all:"の後のメカニズムを無視します
30	インクルードの再帰的クエリが None を返す場合、SPF の結果は permerror です
31	再帰的インクルード
32	複数の SPF または TXT レコードが見つかりました
51	IP アドレスが 0.0.0.0 です
52	from および ehlo パラメータが null です
53	none のルールに一致しました
54	neutral のルールに一致しました
55	softfail のルールに一致しました
56	fail のルールに一致しました
57	temperror のルールに一致しました
58	permerror のルールに一致しました

DomainKeys Identified Mail (DKIM) のエラーコード

表 G-3. DKIM エラーコードの分類

エラータイプ	エラーコード
無効な DKIM レコード	1、23~24、116、34、36、38、40、41、42、43、46、108、111
DKIM レコードなし	22、103、104
無効な DKIM 署名	2~5、7〜21、25〜27、31〜33、44〜45、102、105
DKIM 署名の不一致	28、37、101
内部エラー	-1、6、39、107、112~115、およびその他すべて

表 G-4. DKIM エラーコード

エラーコード	内容	結果
-1	内部エラー	PermError
0	成功	Pass
1	サポートされないバージョンです	Fail
2	ドメインが無効です (d=/i=)	PermError
3	署名の有効期限が切れています	Fail
4	今後の署名	Fail
5	x= < t=	Fail
6	廃止	Fail
7	ヘッダの c=値が無効です	Neutral
8	本文の c=値が無効です	Neutral
9	a=値がありません	PermError
10	a=値が無効です	Neutral
11	h=値がありません	PermError
12	l=値が無効です	Neutral
13	q=値が無効です	Neutral
14	q=オプションが無効です	Neutral
15	d=値がありません	PermError
16	d=値が空です	Neutral
17	s=値がありません	PermError
18	s=値が空です	Neutral
19	b=値がありません	PermError
20	b=値が空です	Neutral

エラーコード	内容	結果
21	b=値が破損しています	PermError
22	DNS で鍵が見つかりません	None
23	DNS 応答が不正です	Neutral
24	DNS 応答に失敗しました	TempError
25	bh=値がありません	PermError
26	bh=値が空です	Neutral
27	bh=値が不正です	PermError
28	署名が一致しません	Fail
29	未承認のサブドメインです	TempError
30	複数のレコードが返されました	TempError
31	h=値が空です	Neutral
32	h=値の必要なエントリがありません	Neutral
33	l=値が本文のサイズを超過しています	Neutral
34	必要な署名を満たしていません	Neutral
35	鍵のバージョンが不明です	Neutral
36	鍵のハッシュが不明です	Neutral
37	署名と鍵のハッシュが一致しません	PermError
38	メールの鍵ではありません	Neutral
39	廃止	Fail
40	鍵の種類がありません	Neutral
41	鍵の種類が不明です	Neutral
42	鍵が失効しました	PermError
43	解読不能な鍵です	PermError

エラーコード	内容	結果
44	v=タグがありません	PermError
45	v=タグが空です	Fail
46	鍵のビット数が不足しています	PermError
101	署名が不正です	Fail
102	使用できる署名がありません	Fail
103	公開鍵が見つかりません	None
104	検証するドメイン鍵がありません	None
105	構文エラー	Fail
106	リソースが使用できません	Fail
107	内部エラー	Fail
108	鍵が失効しました	Fail
109	関数のパラメータが無効です	Fail
110	関数が実装されていません	Fail
111	鍵を取得できません	Fail
112	コールバック要求が拒否されました	Fail
113	コールバック結果が無効です	Fail
114	コールバックがタイムアウトしました	Fail
115	コールバックがタイムアウトしました	Fail
116	複数の DNS 応答があります	Fail

Domain-based Message Authentication, Reporting & Conformance (DMARC) のエラーコード

表 G-5. DMARC エラーコードの分類

エラータイプ	エラーコード
無効な DMARC レコード	2〜5、11
DMARC レコードなし	1、6、9、10、12
認証失敗	13
アライメントチェック失敗	21
内部エラー	7、8

表 G-6. DMARC エラーコード

エラーコード	内容
0	成功
1	データなし
2	NULL コンテキストを受信しました
3	v=値が無効です
4	p=値が無効です
5	p=値がありません
6	ドメインが見つかりません
7	メモリを割り当てることができません
8	マクロではありません
9	DMARC レコードなし
10	ドメインが存在しません
11	回復可能な DNS エラーです
12	未定義の TLD タイプです
13	From:ドメインが使用できません

エラーコード	内容
14	カスタムポリシーの DMARC レコードが見つかりません
15	ポリシー設定に基づいてメッセージを許可します
16	ポリシー設定に基づいてメッセージを拒否します
17	ポリシー設定に基づいてメッセージを隔離します
18	ポリシー設定に基づいてメッセージを監視し、レポートを生成します
19	ドメインポリシー ('p') を適用します
20	サブドメインポリシー ('sp') を適用します
21	アライメントチェック失敗

付録 H

用語集

用語	定義
アップデートサーバ	パターンファイルなどの製品コンポーネントのアップデートを提供します。コンポーネントのアップデートを定期的にリリースします。
高度な脅威検索エンジン 高度な脅威検索エンジン (64 ビット)	高度な脅威検索エンジンは、ウイルス、不正プログラム、および Java や Flash などのソフトウェアの脆弱性悪用からシステムを保護します。トレンドマイクロのウイルス検索エンジンと統合されており、シグネチャベースの検出、動作ベースの検出、および積極的なヒューリスティック検出を行います。
影響を受ける受信者	不正または不審なメールメッセージの受信者。

用語	定義
アラート	事前定義された条件を実行するイベントまたは一連のイベントの発生。 アラートには次の重大度レベルがあります。 • 重大なアラート ただちに対応が必要なイベントに関するメッセージ。 • 重要なアラート ただちに対応する必要はないが、監視が必要なイベントに関するメッセージ。 • 情報アラート ほとんど無害なイベントに関するメッセージ。
アーカイブ	移動または保存のために連結、圧縮、または暗号された、1 つ以上のファイルで構成されるファイル。 「圧縮ファイル」と呼ばれることもあります。
アーカイブファイルのパスワード	アーカイブを復号するために使用するパスワード。
攻撃の発生元	不審メッセージをルーティングするパブリック IP アドレスを持つ最初のメールサーバ。たとえば、不審メッセージが IP1 (送信者) から IP2 (MTA: 225.237.59.52)、IP3 (会社のメールゲートウェイ) を経て IP4 (受信者) にルーティングされた場合は、225.237.59.52 (IP2) が攻撃の発生元として識別されます。攻撃の発生元を判別することで、地域の攻撃パターンまたは同じメールサーバが関係する攻撃パターンを特定できます。
攻撃者	有害な活動を行う、または行う意図がある個人、グループ、組織、または政府。

用語	定義
認証	人またはプロセスの ID の確認。認証により、デジタルデータ伝送が目的の受信者に対してのみ行われるようになります。また認証によって、メッセージとその送信元 (場所や送信者) の受信者側での整合性も保証されます。 認証の最も簡単な形式では、特定のアカウントにアクセスするためのユーザ名とパスワードを求められます。その他の認証プロトコルには、データ暗号標準 (DES) アルゴリズムなどの秘密鍵暗号やデジタル署名を使用する公開鍵システムがあります。
ボット	インターネットに接続されたコンピュータに感染し、攻撃者がリモートで制御できるようにするプログラム。ボットに制御されているコンピュータは、感染したコンピュータのネットワークの一部となり、攻撃者に攻撃されて不正な活動が行われます。
ボットネット	ボットネット (「ボットネットワーク」の短縮形) は、ハイジャックされたゾンビコンピュータのネットワークで、攻撃者によりリモートで制御されます。攻撃者はこのネットワークを使用してスパムメールを送信したり、DoS (サービス拒否) 攻撃を開始し、ネットワークを別のサイバー犯罪に貸し出すこともあります。標的にされたコンピュータのうち 1 台が感染されると、多くの場合、攻撃者はそのコンピュータを支配下に置き、ボットネットに追加することができます。
BCC モード	Deep Discovery Email Inspector の動作モード。アウトオブバンドアプライアンスとして動作します。このモードでは、アップストリームメールサーバから受信した、ミラーリングされたメールトラフィックをユーザに気付かれないように監視し、検出された脅威についてセキュリティ管理者に通知します。
コールバックアドレス	検索または分析中にオブジェクトが要求する (「コールバック」する) 外部 IP アドレス、ホスト名、または URL。C&C サーバに接続された不正プログラムは、多くの場合、有害な活動を実行するために C&C サーバに要求を送信します。 オブジェクトが要求するホスト名または IP アドレスは「コールバックホスト」と呼ばれることがあります。オブジェクトが要求する URL は「コールバック URL」と呼ばれることがあります。
コマンド&コントロール (C&C) サーバ	ボットネットの一元管理サーバまたは危険にさらされているデバイスが参加しているネットワーク全体の一元管理サーバであり、不正プログラムの拡散やホストの感染を目的として不正なボットが利用します。

用語	定義
感染 MTA	感染 MTA は通常、サードパーティによるオープンメールリレーです。メールリレーでは既知のユーザの送信元や送信先を確認しないため、攻撃者は感染 MTA を使用して、検出されずに不正なメールメッセージまたはスパムメールを送信できます。
CSSS (ソフトウェア安全性評価サービス)	ファイルの安全性を確認します。CSSS を使用すると誤検出が減少し、計算時間や計算リソースが節約されます。
コミュニケータ	Apex Central システムの通信の中核です。コミュニケータは、Apex Central Management Infrastructure に属しています。Apex Central サーバから Deep Discovery Email Inspector へのコマンド、および Deep Discovery Email Inspector から Apex Central サーバへのステータスレポートはすべてこのコンポーネントを経由します。
データポート	ネットワーク上で使用可能なリソースにアクセスするハードウェアポート。
検出	検出されたイベント、ファイル、またはネットワークアドレス。検出には、異常、不要、不審、不明、および不正な動作と接続が含まれます。
イベント	システムまたはネットワーク内の観測可能かつ測定可能な事象。
誤検出	危険性が高いと判断されたが、実際は無害な検出。
ファイル送信ルール	仮想アナライザキュー内のファイル数を削減するための一連の基準と条件。ファイル送信ルールは、検出タイプ、検出ルール、およびファイルプロパティに基づいてファイルをチェックします。
IntelliTrap	自動実行型のリアルタイム圧縮ファイルをブロックし、それらを他の不正プログラムの特性に対応付けて、ネットワークにウイルスが侵入する危険性を軽減できるトレンドマイクロのユーティリティ。
IntelliTrap 除外パターンファイル	IntelliTrap 除外パターンファイルには、IntelliTrap 機能による検索実行時の誤検出を減らすため、自動実行型の安全な圧縮ファイルの検出ルーチンが含まれます。
IntelliTrap パターンファイル	IntelliTrap パターンファイルには、一般に難読化された不正プログラムやその他の潜在的な脅威として知られる自動実行型圧縮ファイルタイプの検出ルーチンが含まれます。
ログ	システムまたはネットワーク内で発生したイベントの正式な記録。

用語	定義
管理コンソール	製品を管理するための Web ベースのユーザインタフェース。
管理ポート	管理ネットワークに接続するハードウェアポート。
メッセージ ID	デジタルメッセージの一意の ID。通常は、メールメッセージで使用されるグローバルに一意の ID のことを指します。メッセージ ID は、特定の形式 (メールアドレスのサブセット) を使用して、グローバルで一意にする必要があります。多くのメッセージシステムで使用されている共通の手法は、タイム/日付スタンプをローカルホストのドメイン名と一緒に使用する方法です。
メッセージスタンプ	メールメッセージの先頭または末尾に追加されるテキスト。
メッセージタグ	メールメッセージの件名行に追加されるテキスト。
MTA モード	Deep Discovery Email Inspector の動作モード。Deep Discovery Email Inspector は、メールトラフィックフロー内でメール転送エージェント (MTA) として動作できます。インライン MTA として、不正なメールメッセージをブロックしてネットワークを直接危険から守ります。
通知	エンドポイントまたはネットワーク内のイベントにより通知されるメッセージ。
許可された送信者	Deep Discovery Email Inspector によって安全であると承認されたメール送信者。
リレーされたメールの許可された送信者	エンドポイントは、単一のエンドポイントの IP アドレスまたは IP アドレス範囲の任意のエンドポイントに基づいて、アプライアンスへの接続を許可または拒否されます。
ポート番号	次の用語には、コンテキストに応じて複数の定義があります。 • ハードウェア リムーバブルデバイス、ケーブル、またはその他の外部機器に接続するためのエンドポイント上のソケット。 • TCP/IP ネットワーク 複数のソフトウェアアプリケーションがハードウェアリソースを並行して使用できるようにするアクセスチャネル。
レポート	選択可能な条件に基づいて生成されるデータのコンパイル。ユーザに必要な情報を提供するために使用されます。

用語	定義
サンプル	仮想アナライザに送信される潜在的に不正なファイルまたは URL。仮想アナライザは、ファイルを開くかサンプル内のリンクにアクセスしてリスクレベルを分析します。サンプルの分析中に追加のリンクやファイルを検出した場合は、それらも分析します。 例: ユーザが複数のファイルを含むアーカイブを仮想アナライザに送信すると、仮想アナライザは、アーカイブとすべての 暗号されたファイルを分析します。
サンドボックスイメージ	仮想アナライザでサンドボックスインスタンスの配信に使用されるテンプレート。サンドボックスイメージには、OS、インストール済みのソフトウェア、および特定のコンピュータ環境に必要なその他の設定が含まれます。
サンドボックスインスタンス	サンドボックスイメージに基づく単一の仮想マシン。
スクリプトアナライザエンジン スクリプトアナライザパターンファイル (Deep Discovery)	スクリプトアナライザパターンファイル (Deep Discovery) は、不正コードを識別するために Web ページスクリプトの解析時に使用されます。
スマートフィードバック	保護された脅威情報を Trend Micro Smart Protection Network と共有し、トレンドマイクロが新しい脅威を迅速に特定し、対処できるようにします。トレンドマイクロスマートフィードバックには、製品名、ID、バージョンなどの製品情報に加えて、ファイルタイプ、SHA-1 ハッシュ値、URL、IP アドレス、ドメインなどの検出情報も含まれる場合があります。
Trend Micro Smart Protection Network	グローバルな脅威インテリジェンスをすべての トレンドマイクロ製品およびサービスに配信して、新しい脅威を迅速かつ正確に特定します。深く広がる Trend Micro Smart Protection Network のクラウドデータマイニングフレームワークにより、トレンドマイクロでは脅威データの検索対象か所が増え、より効果的に新しい脅威に対応でき、データを保存場所に関係なく保護できます。
ソーシャルエンジニアリング	人間を心理的に操って、操作を実行させたり、機密情報を漏えいさせたりする攻撃形式です。情報収集、不正行為、またはシステムアクセスを目的とする信用詐欺の一種ですが、従来の詐欺とは異なり、多くの場合、より複雑な詐欺計画における多くの手順の 1 つです。

用語	定義
送信元 IP	メールの送信者に最も近いメールサーバの IP アドレス。 例: ゲートウェイメールサーバ、感染メールサーバ、メールリレー機能を持つボットネット
SPAN/TAP モード	Deep Discovery Email Inspector の動作モード。アウトオブバンドアプライアンスとして動作します。このモードでは、スイッチまたはネットワークタップから受信した、ミラーリングされたメールトラフィックをユーザに気付かれないように監視し、検出された脅威についてセキュリティ管理者に通知します。
スピアフィッシング	標的型攻撃の一種で、攻撃者は既知または正規の団体に見せかけたメールメッセージを送信し、標的となる個人から個人情報を取得します。スピアフィッシングでは、標的となるネットワークを危険にさらしかねないメッセージが読まれる機会が著しく増加します。多くの場合、スピアフィッシングのメールでは、正規のドキュメントに見せかけた添付ファイルを使用します。メールでのファイル共有は、大企業や政府機関では当たり前に行われているためです。
スパイウェアパターンファイル	スパイウェアパターンファイルは、メッセージや添付ファイルに含まれるスパイウェアおよびグレーウェアを特定します。
Threat Connect	環境内で検出された不審オブジェクトとトレンドマイクロ Smart Protection Network の脅威データを関連付けます。生成されるインテリジェンスレポートを使用すれば、潜在的な脅威について調べ、攻撃プロファイルに適した対応ができます。
脅威ナレッジベース	脅威ナレッジベースは、脅威の相関分析に関する情報を提供します。
実際のファイルタイプ	そのファイルの拡張子とは関係なく、ファイル内に実際に保存されているデータの種類。 例: テキストファイルには HTML、CSV、または TXT の拡張子が付く可能性がありますが、実際のファイルタイプは同じです。
検索できないアーカイブ	カスタム定義のパスワードリストやヒューリスティックに取得されたパスワードを使用しても抽出および検索できない、パスワード保護されたアーカイブ。
ビューアカウント	検出およびシステム情報を表示できるが、管理コンソール上のほとんどの画面にはアクセスできないアカウント。

用語	定義
仮想アナライザ	サンプルの管理および分析に使用する、隔離された仮想環境。仮想アナライザではサンプルの動作や特徴を監視して、そのサンプルにリスクレベルを割り当てます。
仮想アナライザセンサ	仮想アナライザセンサは、不正プログラムの実行と検出、および仮想アナライザでの動作の記録に使用されるユーティリティ群です。
ウイルスパターンファイル	トレンドマイクロのウイルス検索エンジンは、ヒューリスティック検出、シグネチャベースの検出、および動作ベースの検出によってウイルスや不正プログラムからシステムを保護します。トレンドマイクロは、新しい脅威の検出ルーチンが使用可能になるとウイルスパターンファイルをただちにアップデートします。
Web レピュテーションサービス	Web ドメインの信頼性を追跡します。Web サイトの新しさ、場所の変更履歴、不正プログラム動作分析で検出された不審な活動の兆候などの要素に基づいて、レピュテーションスコアを割り当てます。
ウィジェットフレームワーク	ウィジェットフレームワークは、Deep Discovery Email Inspector ウィジェットのテンプレートを提供します。

索引

アルファベット

あ

か

さ

た

な

は

ま

や

ら

わ