Deep Discovery™ Analyzer 7.1

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/jp/solution/000207383

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、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバ

P/N: APEM79309_210806_JP_R1 (2022/07)

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 Analyzer 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 Analyzer 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 3 章：ダッシュボード

第 4 章：仮想アナライザ

第 5 章：アラートとレポート

第 6 章：管理

はじめに

本書について

このガイドには、製品の設定とサービスレベルに関する情報が記載されています。

ドキュメント

Deep Discovery Analyzer 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 Analyzer を設定して管理する方法の詳細な手順、および Deep Discovery Analyzer 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 Analyzer の導入計画とインストールの要件および手順、さらに事前設定コンソールを使用して初期設定とシステムタスクを実行する方法についての情報が含まれています。
Syslog コンテンツマッピングガイド	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。 Syslog コンテンツマッピングガイドには、ログの管理基準や、Deep Discovery Analyzer の Syslog イベントを実装するための構文に関する情報が記載されています。
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 Analyzer 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 Analyzer 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 Analyzer のコンポーネントと機能、Deep Discovery Analyzer 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/jp/technical-support

対象読者

この Deep Discovery Analyzer 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
- データベース管理
- ウイルス対策とコンテンツのセキュリティ保護

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

表記規則	説明
 ヒント	推奨事項
 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

用語

用語	説明
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。
アクティブなプライマリアプライアンス	すべての管理タスクを実行するクラスタ化されたアプライアンスです。すべての設定を保持し、パフォーマンス向上のためにセカンダリアプライアンスに送信を割り当てます。
管理者	Deep Discovery Analyzer の管理担当者です。
クラスタリング	複数のスタンドアロン Deep Discovery Analyzer アプライアンスを配置および設定して 1 つのクラスタを形成することで、フォールトトレランス、パフォーマンスの向上、またはそれらの両方を実現できます。
カスタムポート	サンドボックス分析専用の隔離されたネットワークに Deep Discovery Analyzer を接続するハードウェアポートです。
ダッシュボード	ウィジェットが表示される UI 画面です。

用語	説明
高可用性クラスタ	高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。
負荷分散クラスタ	負荷分散クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。
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。
パッシブなプライマリアプライアンス	アクティブなプライマリアプライアンスでエラーが発生し回復できない状態になるまでスタンバイしているクラスタ化されたアプライアンスです。高可用性を提供します。
役割ベースの管理	管理者がユーザアカウントを設定して管理コンソールへのアクセスを制御する方法を効率化します。
サンドボックスイメージ	設定とインストールが不要の、すぐに使用できるソフトウェアパッケージ (OS とアプリケーションのセット) です。仮想アナライザは OVA (Open Virtual Appliance) 形式のイメージファイルのみをサポートします。
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。
セカンダリアプライアンス	パフォーマンスの向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理するクラスタ化されたアプライアンスです。

用語	説明
スタンドアロンアプライアンス	どのクラスタにも属さないアプライアンスです。クラスタ化されたアプライアンスは、アプライアンスをクラスタからデタッチすることでスタンドアロンアプライアンスに戻すことができます。
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。
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。
ウィジェット	目的の選択したデータセットを表示するためのカスタマイズ可能な画面です。
YARA	YARA ルールは、環境に固有の標的型攻撃およびセキュリティ脅威を特定するためのカスタマイズ可能な不正プログラム検出パターンです。

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、Deep Discovery Analyzer 7.1 およびこのリリースの新機能について説明します。

Deep Discovery Analyzer について

Deep Discovery Analyzer は、トレンドマイクロやサードパーティのセキュリティ製品において標的型攻撃に対する保護を強化する、カスタムサンドボックスによるサンプル分析サーバです。トレンドマイクロのメールセキュリティ製品や Web セキュリティ製品と統合することができ、他の製品のサンドボックス分析を補完および一元管理するためにも使用できます。Deep Discovery Analyzer 内に作成可能なカスタムサンドボックス環境は、対象となるデスクトップソフトウェア設定と正確に一致するため、検出の精度が向上し、誤検出が減少します。

また Deep Discovery Analyzer には、任意のサードパーティ製品との統合を可能にする Web サービス API や、脅威を調査するための手動送信機能も用意されています。

新機能

表 1-1. Deep Discovery Analyzer 7.1 の新機能

機能/強化点	詳細
Trend Micro Vision One の統合	Service Gateway を介した Trend Micro Vision One との統合により、ハイブリッド環境における共同でのセキュリティ分析が可能になります。
メールでの送信	メールでの送信機能により、許可された送信者ドメインおよび SMTP サーバからのメールメッセージを受信して分析できるようになります。
仮想アナライザの機能強化	内部仮想アナライザが強化され、次の機能が追加されます。 • Windows 10 October 2020 Update イメージのサポート • SHA-256 オブジェクトの除外の種類 • 分析レポートの TLSH 情報

機能/強化点	詳細
監査ログの機能強化	ユーザが次のことを実行すると監査ログが生成されます。 • 調査パッケージまたは分析レポートの表示またはダウンロード • 送信のエントリの削除
システムログの機能強化	ICAP 事前検索のログを Syslog サーバに送信するオプションが提供されます。
運用レポートの機能強化	運用レポートが強化され、ICAP 事前検索のログが含まれるようになります。
インタフェース管理の機能強化	インタフェース管理の機能が強化され、トラブルシューティングを容易にするため、インタフェースの MAC アドレスが含まれるようになります。

サンプルの送信のフィルタと削除	[送信] 画面に次のものが含まれます。
	• 選択したサンプルと関連する分析データを削除するオプション ([完了] タブと [失敗] タブ)
	• 次の詳細検索フィルタ ([完了] タブ):
	  • MITRE ATT&CK™ Tactics
	  • MITRE ATT&CK™ Techniques
	  • 著しい特性

SNMP クエリの機能強化	SNMP クエリの機能が強化され、リアルタイムのアプリケーションイベントまたは指定した時間範囲内のイベントが含まれるようになります。
YARA ルールの機能強化	YARA ルールの機能が強化され、4.1.0 の公式な仕様がサポートされるようになります。
Deep Discovery Analyzer 6.9 および 7.0 からのインラインでの移行	ハードウェアモデルが 1100 および 1200 の場合、Deep Discovery Analyzer 6.9 または 7.0 の設定を 7.1 に自動的に移行できます。

機能と利点

Deep Discovery Analyzer には次の機能があります。

一元化されたサービスとしてのサンドボックスの有効化

メール、ネットワーク、エンドポイント、およびその他のサンプルソースの遅延のない処理を可能するスケーラブルなソリューションにより、最適なパフォーマンスを実現します。

カスタムサンドボックス

ご使用の環境について攻撃者が想定するデスクトップソフトウェア設定に合わせた環境でサンドボックスシミュレーションと分析を行い、誤検出の可能性を低減しながら最適な検出を実現します。

幅広いファイル分析範囲

複数の検出エンジンとサンドボックスを使用して、Windows 実行可能ファイル、Microsoft Office や PDF のドキュメント、Web コンテンツ、および圧縮ファイルなど広範囲にわたるファイルタイプを検査します。

YARA ルール

Deep Discovery Analyzer では YARA ルールを使用して不正プログラムを特定します。YARA ルールは、環境に固有の標的型攻撃およびセキュリティ脅威を特定するためのカスタマイズ可能な不正プログラム検出パターンです。

ドキュメントのセキュリティホール悪用の検出

専用の検出機能とサンドボックスを使用して、通常一般的な Office 文書や他のファイル形式で配信される不正プログラムやセキュリティホール悪用を検出します。

自動 URL 分析

統合製品により自動的に送信された URL のページ検索とサンドボックス分析を実行します。

詳細レポート

一元化されたダッシュボードやレポートを介して、サンプルの活動や C&C 通信の詳細など、詳しい分析結果を得られます。

アラート通知

アラート通知は、Deep Discovery Analyzer の状態をただちに知らせる機能です。

クラスタ化配置

複数のスタンドアロン Deep Discovery Analyzer アプライアンスを配置および設定して 1 つのクラスタを形成することで、フォールトトレランス、パフォーマンスの向上、またはそれらの両方を実現できます。

トレンドマイクロ製品との統合

トレンドマイクロ製品との統合があらかじめサポートされており、Deep Discovery Analyzer のサンドボックス機能をトレンドマイクロのメールセキュリティ製品や Web セキュリティ製品でも使用できます。

サンプルの送信

Deep Discovery Analyzer では、次のいずれかの方法でサンプルを送信できます。

- 統合セキュリティ製品の Web サービス API

- 管理コンソールでの手動操作
- 許可された送信者ドメインおよび SMTP サーバからのメール

Connected Threat Defense

仮想アナライザによって生成された、不審オブジェクトや IOC (Indicators of Compromise) 検出情報を、他のトレンドマイクロのソリューションやサードパーティのセキュリティ製品と自動的に共有、脅威への迅速な対応を実現します。

ICAP の統合

Deep Discovery Analyzer では、ICAP (Internet Content Adaptation Protocol) クライアントとの統合がサポートされます。統合後は、Deep Discovery Analyzer で次の機能を実行できるようになります。

- ICAP クライアントから送信されたサンプルを ICAP サーバとして分析する
- 指定したネットワーク動作 (URL アクセス/ファイルのアップロード/ファイルのダウンロード) がブロックされた場合に、ユーザ設定ページをエンドユーザに表示する
- ICAP クライアントリストを設定することで、サンプルを送信できる ICAP クライアントを制御する
- 選択した MIME コンテントタイプに基づいてファイルの検索をバイパスする
- 実際のファイルタイプに基づいてファイルの検索をバイパスする
- RESPMOD モードでの URL 検索をバイパスする
- さまざまな検索モジュールを使用してサンプルを検索する
- 仮想アナライザが処理できるファイルタイプに基づいてサンプル送信をフィルタする

第 2 章

基本設定

この章では、Deep Discovery Analyzer を導入し、その初期設定を行う方法について説明します。

事前設定コンソール

事前設定コンソールは、ネットワーク設定、高可用性の詳細の表示、リモートホストの Ping、および事前設定コンソールのパスワードの変更に使用する Bash ベースの (UNIX シェル) インタフェースです。

詳細については、「Deep Discovery Analyzer インストールガイド」を参照してください。

管理コンソール

Deep Discovery Analyzer 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。

次のいずれかの Web ブラウザを使用して、管理ネットワーク上の任意のコンピュータから管理コンソールを開きます。

- Microsoft Internet Explorer 11
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

注意

Web ブラウザの JavaScript が有効になっていることを確認してください。

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>/pages/login.php`

Deep Discovery Analyzer 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。

- 29 ページの「ローカルアカウントを使用したログオン」
- 30 ページの「シングルサインオンによるログオン」

ローカルアカウントを使用したログオン

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: `Admin1234!`

   注意

   お使いのアカウントに応じて、[ユーザ名] フィールドに次のいずれかの情報を入力します。

   - ユーザ名
   - ユーザプリンシパル名 (UPN)
   - メールアドレス

2. (オプション) [セッションタイムアウトの延長を有効にする] を選択し、ログオンセッションのセッションタイムアウトを延長します。初期設定のセッションタイムアウトは 10 分です。

   セッションタイムアウトの設定を変更するには、[管理] > [システム設定] の順に選択し、[セッションタイムアウト] タブをクリックします。

3. [ログオン] をクリックします。
4. 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。

シングルサインオンによるログオン

Deep Discovery Analyzer 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 Analyzer の管理コンソールにアクセスできます。

詳細については、210 ページの「[SAML 認証] タブ」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 Analyzer の管理コンソールにアクセスします。

管理コンソールナビゲーション

管理コンソールは、次の要素で構成されます。

表 2-1. 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、次のものが含まれています。 • 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、40 ページの「ダッシュボードの概要」を参照してください。 • 管理コンソールに現在ログオンしているユーザの名前。 • [パスワードの変更] リンク。クリックすると、現在のユーザパスワードを変更できます。 • [ログオフ] リンク。クリックすると、現在のコンソールセッションが終了し、ログオン画面に戻ります。 • 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。
メインメニューバー	メインメニューバーには、製品の設定を行うためのいくつかのメニュー項目が含まれます。[ダッシュボード] などの一部のメニュー項目は、クリックすると対応する画面が開きます。その他のメニュー項目は、クリックするかマウスを重ねると、サブメニュー項目が表示されます。サブメニュー項目をクリックすると、対応する画面が開きます。
スクロールアップボタンと矢印ボタン	すべてのコンテンツが画面に表示されない場合は、[上にスクロール] オプションを使用します。[上にスクロール] ボタンの横に、画面の下のバーを展開/縮小する矢印ボタンがあります。
コンテキスト依存のヘルプ	[ヘルプ] を使用して、現在表示されている画面の詳細を知ることができます。

パスワードの変更

管理コンソールへのアクセスに現在使用しているアカウントのパスワードを変更できます。管理コンソールのバナーで、右上隅にあるアカウント名をクリックし、[パスワードの変更] を選択します。

表示されるフィールドに現在のパスワードと新しいパスワードを 2 回入力してから、[保存] をクリックします。

導入タスク

手順

1. 有効なアクティベーションコードを使用して、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、282 ページの「ライセンス」を参照してください。

2. Deep Discovery Analyzer のホスト名と IP アドレスを指定します。詳細については、226 ページの「[ネットワーク] タブ」を参照してください。

3. Deep Discovery Analyzer がプロキシサーバ経由で管理ネットワークに接続する場合は、プロキシ設定を行います。詳細については、230 ページの「[プロキシ] タブ」を参照してください。

4. 日付と時刻を設定して、Deep Discovery Analyzer の機能が予定どおりに動作するようにします。詳細については、233 ページの「[時間] タブ」を参照してください。

5. SMTP を設定して、メールで通知を送信できるようにします。詳細については、232 ページの「[SMTP] タブ」を参照してください。

6. サンドボックスインスタンスを仮想アナライザにインポートします。詳細については、104 ページの「イメージをインポートする」を参照してください。

7. 仮想アナライザのネットワーク設定を実行して、サンドボックスインスタンスが外部接続先に接続できるようにします。詳細については、127 ページの「外部接続を有効にする」を参照してください。

8. (オプション) 高可用性または負荷分散クラスタで使用する追加の Deep Discovery Analyzer アプライアンスを配置および設定します。詳細については、239 ページの「[クラスタ] タブ」を参照してください。

9. Deep Discovery Analyzer と統合するために、サポートされているトレンドマイクロ製品を設定します。詳細については、33 ページの「トレンドマイクロ製品との統合」を参照してください。

10. オブジェクトを送信するすべての送信元に重みとタイムアウト値を設定する事で、送信元間で使用する仮想アナライザのリソースの割り当てを

調整します。詳細については、131 ページの「[送信元] 画面」を参照してください。

トレンドマイクロ製品との統合

Deep Discovery Analyzer は、次のトレンドマイクロ製品と連携します。

サンドボックス分析

Deep Discovery Analyzer にサンドボックス分析用のサンプルを送信できる製品は、次のとおりです。

注意

サンプルはすべて、Deep Discovery Analyzer 管理コンソールの [仮想アナライザ] > [送信] にある [送信] 画面に表示されます。Deep Discovery Analyzer の管理者および調査者は、この画面から手動でサンプルを送信することもできます。

- Apex One as a Service
- Apex One 2019
- Deep Discovery Inspector 3.7 以降
- Deep Discovery Web Inspector 2.5 以降 (日本語版はリリースされていません)
- Deep Discovery Email Inspector 2.5 以降
- InterScan for Microsoft Exchange 11.0 以降
- InterScan for IBM Domino 5.6 SP1 Patch1 HF4666 以降
- InterScan Messaging Security Virtual Appliance (IMSVA) 8.2 SP2 以降
- InterScan Messaging Security Suite (IMSS) 7.5 Windows 版以降
- InterScan Web Security Virtual Appliance (IWSVA) 6.5 以降
- InterScan Web Security Suite (IWSS) 6.5

- InterScan Messaging Security Suite (IMSS) 9.1 Linux 版以降
- Deep Security 10.0 以降
- ウイルスバスター Corp. XG 以降
- Trend Micro TippingPoint Security Management System 5.0 以降
- InterScan Web Security 3.1 以降

統合する製品の管理コンソールで、適切な画面に移動し、次の情報を指定します。どの画面にアクセスするかについては、製品ドキュメントを参照してください。

- API キー。Deep Discovery Analyzer 管理コンソールの [ヘルプ] > [バージョン情報] から入手できます。
- 仮想 IP アドレス。IP アドレスがわからない場合は、Deep Discovery Analyzer 管理コンソールへのアクセスに使用した URL を確認します。IP アドレスはこの URL に含まれています。
- Deep Discovery Analyzer の IPv4 または IPv6 仮想アドレス。高可用性設定で Deep Discovery Analyzer を使用する場合は、統合製品に設定用の固定 IP アドレスを提供するために仮想 IP アドレスが使用されます。Deep Discovery Analyzer 管理コンソールの [管理] > [システム設定] > [高可用性] から入手できます。
- Deep Discovery Analyzer の SSL ポート 443。この値は固定です。

重要

統合製品に登録した後、Deep Discovery Analyzer の API キーを変更した場合は、Deep Discovery Analyzer を統合製品から削除して再度追加します。

注意

統合する製品によっては、Deep Discovery Analyzer と正しく統合するための追加情報が必要になる場合があります。詳細については、製品ドキュメントを参照してください。

(オプション) Deep Discovery Analyzer 管理コンソールで統合製品の重みの値を確認および変更して、仮想アナライザのリソース割り当てを調整します。詳細については、131 ページの「[送信元] 画面」を参照してください。

不審オブジェクトのリスト

Deep Discovery Analyzer から不審オブジェクトのリストを取得する製品は次のとおりです。

- 最新の HotFix を適用した Apex Central 2019
- Deep Discovery Email Inspector 2.5 以降
- Deep Discovery Inspector 3.7 以降
- 最新の Patch を適用したスタンドアロンの Smart Protection Server 2.6
- ウイルスバスター Corp.統合 Smart Protection Server 10.6 SP2 Patch1～ウイルスバスター Corp.統合 Smart Protection Server 11 SP1
- InterScan Web Security Virtual Appliance (IWSVA) 6.x 以降
- InterScan Web Security Suite (IWSS) 6.5
- InterScan Web Security 3.1 以降

統合する製品の管理コンソールで、適切な画面に移動し、次の情報を指定します。どの画面にアクセスするかについては、製品ドキュメントを参照してください。

- API キー。Deep Discovery Analyzer 管理コンソールの [ヘルプ] > [バージョン情報] から入手できます。
- Deep Discovery Analyzer の IPv4 または IPv6 アドレス。IP アドレスがわからない場合は、Deep Discovery Analyzer 管理コンソールへのアクセスに使用した URL を確認します。IP アドレスはこの URL に含まれています。

- Deep Discovery Analyzer の IPv4 または IPv6 仮想アドレス。高可用性設定で Deep Discovery Analyzer を使用する場合は、統合製品に設定用の固定 IP アドレスを提供するために仮想 IP アドレスが使用されます。Deep Discovery Analyzer 管理コンソールの [管理] > [システム設定] > [高可用性] から入手できます。
- Deep Discovery Analyzer の SSL ポート 443。この値は固定です。
- Deep Discovery Analyzer ユーザのログオン認証情報。詳細については、262 ページの「[アカウント] タブ」を参照してください。

重要

統合製品に登録した後、Deep Discovery Analyzer の API キーを変更した場合は、Deep Discovery Analyzer を統合製品から削除して再度追加します。

注意

統合する製品によっては、Deep Discovery Analyzer と正しく統合するための追加情報が必要になる場合があります。詳細については、製品ドキュメントを参照してください。

除外設定

Deep Discovery Analyzer に除外設定を送信する製品は次のとおりです。

- 最新の HotFix を適用した Apex Central 2019

統合する製品の管理コンソールで、適切な画面に移動し、次の情報を指定します。どの画面にアクセスするかについては、製品ドキュメントを参照してください。

- Deep Discovery Analyzer の IPv4 または IPv6 アドレス。IP アドレスがわからない場合は、Deep Discovery Analyzer 管理コンソールへのアクセスに使用した URL を確認します。IP アドレスはこの URL に含まれています。
- Deep Discovery Analyzer の IPv4 または IPv6 仮想アドレス。高可用性設定で Deep Discovery Analyzer を使用する場合は、統合製品に設定用の固定 IP アドレスを提供するために仮想 IP アドレスが使用されます。Deep

Discovery Analyzer 管理コンソールの [管理] > [システム設定] > [高可用性] から入手できます。

- Deep Discovery Analyzer の SSL ポート 443。この値は固定です。
- Deep Discovery Analyzer ユーザのログオン認証情報。詳細については、262 ページの「[アカウント] タブ」を参照してください。

重要

統合製品に登録した後、Deep Discovery Analyzer の API キーを変更すると、Deep Discovery Analyzer を統合製品から削除して再度追加する必要が生じます。

注意

統合する製品によっては、Deep Discovery Analyzer と正しく統合するための追加情報が必要になる場合があります。詳細については、製品ドキュメントを参照してください。

第 3 章

ダッシュボード

この章では、Deep Discovery Analyzer のダッシュボードについて説明します。

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、40 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、42 ページの「ウィジェット」を参照してください。

注意

新しいウィジェットを使用できるときは、[ウィジェットの追加] ボタンに星が表示されます。

[タブのスライドショーの再生] をクリックすると、ダッシュボードのスライドショーが表示されます。

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。

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	ダッシュボードの最上部にあるプラスアイコン ( ) をクリックします。[新規タブ] 画面が表示されます。 詳細については、41 ページの「[新規タブ] 画面」を参照してください。
タブの設定の編集	[タブ設定] をクリックします。[新規タブ] 画面と同様の画面が開き、設定を編集できます。
タブの移動	ドラッグアンドドロップを使用して、タブの位置を変更します。
タブの削除	タブタイトルの横にある削除アイコン ( ) をクリックします。タブを削除すると、タブ内のすべてのウィジェットも削除されます。

[新規タブ] 画面

[新規タブ] 画面は、ダッシュボード上部にあるプラスアイコン ( ) をクリックすると表示されます。

この画面には、次のオプションが含まれます。

表 3-1. [新規タブ] のタスク

タスク	手順
タイトル	タブの名前を入力します。
レイアウト	使用可能なレイアウトから選択します。
スライドショー	[このタブをスライドショーに含める] にチェックを入れると、作成したタブがスライドショーに含まれます。
更新間隔	ダッシュボードのスライドショー再生中にこのタブを表示する秒数を入力します。
自動調整	[オン] または [オフ] を選択します。この機能は、1 つの列に 1 つのウィジェットが存在する場合にのみ動作します。単一のウィジェットの高さを最も高い列に合わせるよう調整するには、[オン] を選択します。

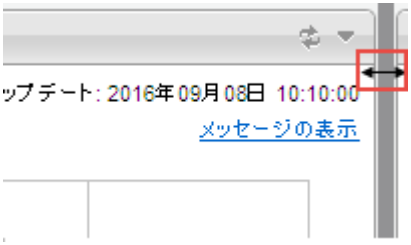
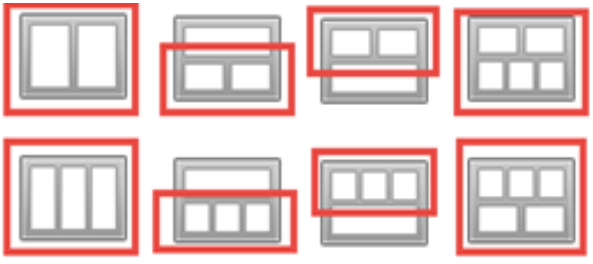
ウィジェット

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。

タスク	手順
ウィジェットの追加	タブを開き、右上隅にある [ウィジェットの追加] をクリックします。[ウィジェットの追加] 画面が表示されます。詳細については、43 ページの「ダッシュボードにウィジェットを追加する」を参照してください。
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。 ウィジェットの更新頻度を設定したり、ウィジェットデータを自動的に更新したりするには、設定の更新アイコン ( ) をクリックします。
ウィジェットの削除	ウィジェットを閉じるには、削除アイコン ( ) をクリックします。この操作により、ウィジェットがそのタブから削除されますが、そのウィジェットを含む他のタブや [ウィジェットの追加] 画面内のウィジェットリストからは削除されません。
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。
ノードの変更	使用可能な場合は、ウィジェット上部の [ノード] ドロップダウンボックスをクリックしてノードを変更します。
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。

タスク	手順
ウィジェットのサイズ変更	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ます。次の画像のように太い縦線と矢印が表示されたら、カーソルをクリックしたままの状態で左または右に移動します。  複数列のタブ内にある任意のウィジェットのサイズを変更できます (赤い四角)。これらのタブは次のレイアウトのいずれかになります。 

ダッシュボードにウィジェットを追加する

[ウィジェットの追加] 画面は、ダッシュボードのタブからウィジェットを追加する際に表示されます。

次のいずれかを実行します。

手順

- 表示されるウィジェットを減らすには、左側のカテゴリをクリックします。
- ウィジェットを検索するには、上部の検索テキストボックスにウィジェット名を入力します。
- ページごとのウィジェット数を変更するには、[レコード] ドロップダウンメニューで数字を選択します。
- [詳細] ビューと [概要] ビューを切り替えるには、右上の表示アイコン ( ) をクリックします。
- ダッシュボードに追加するウィジェットを選択するには、ウィジェットのタイトルの横にあるチェックボックスを選択します。
- 選択したウィジェットを追加するには、[追加] をクリックします。

[概要] タブ

[概要] タブのウィジェットでは、Deep Discovery Analyzer によって検出された脅威を、種類や件数、分析時に検出された不審オブジェクトの数、特定期間内のサンプルの送信数、および仮想アナライザに送信されたサンプルの総数に基づいて把握できます。

脅威の種類

このウィジェットは、指定期間内にすべての送信で検出された脅威の種類、件数、およびリスクレベルを示します。

初期設定の期間は [過去 24 時間] です。この期間は必要に応じて変更できます。

[リスク高]、[リスク中]、[リスク低]、または [合計] の数字をクリックすると [送信] 画面が開き、詳細情報が表示されます。

不審オブジェクト

このウィジェットは、指定された期間に不審オブジェクトのリストに追加されたオブジェクトの数 (IP アドレス、ドメイン、URL、およびファイル) をグラフにします。

初期設定の期間は [過去 24 時間] です。この期間は必要に応じて変更できます。

[不審オブジェクトの表示] をクリックして [不審オブジェクト] 画面に移動し、詳細情報を表示します。

詳細については、90 ページの「生成された不審オブジェクトリスト」を参照してください。

送信の時間別推移

このウィジェットは、特定期間内に仮想アナライザに送信されたサンプル数をグラフで示します。

初期設定の期間は [過去 24 時間] です。この期間は必要に応じて変更できます。

[送信の表示] をクリックして [送信] 画面に移動し、詳細情報を表示します。

詳細については、51 ページの「送信」を参照してください。

仮想アナライザの概要

このウィジェットは、仮想アナライザに送信されたサンプルの総数、およびこれらのサンプルのうちリスクが含まれるものの数を示します。

初期設定の期間は [過去 24 時間] です。この期間は必要に応じて変更できます。

サンプルの総数、または [リスク高]、[リスク中]、[リスク低] のサンプル数をクリックし、[送信] 画面に移動して、詳細情報を表示します。

詳細については、51 ページの「送信」を参照してください。

[システムステータス] タブ

[システムステータス] タブでウィジェットを表示すると、仮想アナライザのステータス、キューにあるサンプル、およびハードウェアのステータスに基づいて Deep Discovery Analyzer の全体的なパフォーマンスを把握できます。

仮想アナライザのステータス

このウィジェットには、1 つまたはすべてのノード上の仮想アナライザのステータスとイメージごとのインスタンス数が表示されます。

ノードの種類に応じて、ウィジェットの情報には次のいずれかが含まれます。

- 単一のノード、またはクラスタ内すべてのノード: キュー内のサンプル数と処理中のサンプル数
- クラスタ内のプライマリノードまたはセカンダリノード: 仮想アナライザの前処理のキュー内にある URL 数と処理中のサンプル数

注意

- Deep Discovery Analyzer をスタンドアロンアプライアンスとし配置する場合、[ノード] ドロップダウンリストは使用できません。
- Deep Discovery Analyzer がクラスタ内のプライマリアプライアンスであるか ICAP 統合が有効な場合、表示される仮想アナライザのインスタンス数が、設定された仮想アナライザのインスタンス数と一致しないことがあります。

  設定された仮想アナライザのインスタンス数を確認するには、103 ページの「[イメージ] タブ」を参照してください。

[仮想アナライザの管理] をクリックして、[サンドボックス管理] 画面に移動します。詳細については、101 ページの「サンドボックス管理」を参照してください。

[すべてのノードで正常ステータス] は、すべてのノードがエラーなしで動作していることを示します。

1 つ以上のノードでステータスにエラーが表示される場合は、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックして、エラーの詳細情報を表示します。

キュー内のサンプル

このウィジェットには、仮想アナライザのキューにあるサンプルの数が表示されます。赤線は仮想アナライザで 5 分以内に分析できるサンプルの推定数を表しています。

[キューの表示] をクリックし、[送信] 画面の [処理待ち] タブに移動して、詳細情報を表示します。

詳細については、51 ページの「送信」を参照してください。

ハードウェアステータス

このウィジェットには、主要なハードウェアコンポーネントのリアルタイムの使用率が表示されます。

仮想アナライザの平均処理時間

このウィジェットには、指定期間内の仮想アナライザの平均処理時間が表示されます。

このウィジェットには、次のデータが比較表示されます。

- 仮想アナライザの分析時間: 仮想アナライザが分析処理を開始してから完了するまでの、仮想アナライザ内のサンプルによって使用された平均時間
- 合計処理時間: Deep Discovery Analyzer がサンプルを受信してから最終的な分析結果を生成するまでの、Deep Discovery Analyzer 内のサンプルによって使用された平均合計時間

初期設定の期間は [過去 4 時間] です。この期間は必要に応じて変更できます。

[仮想アナライザの管理] をクリックして、[イメージ] タブに移動します。

詳細については、103 ページの「[イメージ] タブ」を参照してください。

第 4 章

仮想アナライザ

この章では、仮想アナライザについて説明します。

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。

仮想アナライザは Threat Connect と連携して動作します。Threat Connect は、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るトレンドマイクロのサービスです。

送信

[仮想アナライザ] > [送信] にある [送信] 画面には、仮想アナライザによって処理されるサンプルのリストが含まれます。サンプルは、許可された送信者ドメインや SMTP サーバからのメールメッセージを介して統合製品によって自動的に送信されるか、Deep Discovery Analyzer の管理者または調査者によって手動で送信されるファイルおよび URL です。

[送信] 画面では、サンプルが次のタブにまとめられています。

- 完了: 仮想アナライザが分析したサンプル
- 処理中: 仮想アナライザが現在分析しているサンプル
- 処理待ち: 分析を保留しているサンプル
- 失敗: 分析プロセスを実行したが、エラーのため分析結果がないサンプル

  注意

  [失敗] タブにリストされているサンプルは、ウィジェットに表示されるサンプル数に含まれません。

- ICAP 事前検索:統合 ICAP クライアントから受信したリスク高のサンプル

各タブには、送信されたサンプルの基本情報をまとめた表が表示されます。表内に表示する列をカスタマイズするには、歯車アイコン ( ) をクリックし、表示する列を選択して、[適用] をクリックします。

表のデータを更新するには、[表示更新] をクリックします。

次の表は、表示されるすべての列について説明しています。表示される列は、選択するタブによって異なります。

表 4-1. [送信] の列

列	情報
オブジェクト情報	

列	情報
送信	サンプルが送信された日時 この列は [完了]、[処理中]、[処理待ち]、および [失敗] タブにのみ表示されます。
ファイル名	次のいずれかの情報が表示されます。 • サンプルのファイル名 • リスクレベルの最も高い子オブジェクトのファイル名 • (リスクが検出されない場合) 任意の子オブジェクトのファイル名 **注意** ファイルサイズが 0 または小さすぎて分析できない場合は「NONAMEFL」
サンプルパッケージ	アーカイブされたファイルサンプルのコピー **注意** 送信されたサンプルがファイルの場合にのみダウンロードできます。クリックすると、ファイルサンプルがアーカイブファイルとしてダウンロードされます。アーカイブのパスワードは `virus` です。 この列は [失敗] タブにのみ表示されます。
送信元	• サンプルを送信したトレンドマイクロ製品の名前 • サンプルがメールメッセージを介して送信された場合は「メールでの送信」 • サンプルが手動で送信された場合は「手動での送信」 • サンプルが ICAP クライアントから送信された場合は「ICAP クライアント」 この列は [完了]、[処理中]、[処理待ち]、および [失敗] タブにのみ表示されます。

列	情報
送信元名	• サンプルを送信した製品のホスト名 • 手動で送信された場合はデータなし (ダッシュで示されます) • ICAP クライアントまたは SMTP サーバの IP アドレス
SHA-1	サンプルの SHA-1 値
SHA-256	サンプルの SHA-256 値 この列は [完了] タブと [ICAP 事前検索] タブにのみ表示されます。
オブジェクトの種類	ファイルまたは URL この列は [完了]、[処理中]、[処理待ち]、および [失敗] タブにのみ表示されます。
検出	サンプルが検出された日時 この列は [ICAP 事前検索] タブにのみ表示されます。
ICAP モード	サンプルの検出時に ICAP クライアントにより報告されたモード 指定可能な値: • REQMOD:ICAP 要求の変更方法 • RESPMOD:ICAP 応答の変更方法 この列は [ICAP 事前検索] タブにのみ表示されます。
分析情報	

列	情報
リスクレベル	仮想アナライザは、静的な分析および動作シミュレーションを実行してサンプルの特徴を識別します。分析時、仮想アナライザではコンテキストで特徴を評価し、評価の累計に基づいてサンプルのリスクレベルを割り当てます。 • 赤色のアイコン (): 高リスク。このオブジェクトは通常不正プログラムと関連付けられる極めて不審な特性を示しました。 例: • 不正プログラムのシグネチャ、既知のエクスプロイトコード • 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 • 黄色のアイコン (): 低リスク。このオブジェクトは無害である可能性の高い多少不審な特性を示しました。 • 緑色のアイコン (): リスクなし。このオブジェクトは不審な特性を示しませんでした。 • 灰色のアイコン (): 未分析。 仮想アナライザがファイルを分析しなかった理由として考えられることについては、87 ページの「分析失敗の原因として考えられる理由」を参照してください。 **注意** サンプルが複数のインスタンスによって処理された場合、最も高いリスクレベルのアイコンが表示されます。たとえば、あるインスタンスのリスクレベルが黄色で、別のインスタンスのリスクレベルが赤色の場合、赤色のアイコンが表示されます。アイコンにマウスを重ねると、リスクレベルの詳細が表示されます。 この列は [完了] タブにのみ表示されます。

列	情報
完了日時	サンプル分析が完了した日付と時刻 この列は [完了] タブにのみ表示されます。
ファイルの種類	• オブジェクトのファイルタイプ • アーカイブのファイルタイプ/最高リスクの子オブジェクトのファイルタイプ • アーカイブのファイルタイプ/リスクがない場合は任意の子オブジェクトのファイルタイプ 注意 ファイルサイズが 0 または小さすぎて分析対象のファイルタイプを特定できない場合は「Empty」または「UNKNOWN」 この列は [完了] タブと [ICAP 事前検索] タブにのみ表示されます。
脅威	トレンドマイクロのパターンファイルとその他のコンポーネントによって検出された脅威の名前 この列は [完了] タブと [ICAP 事前検索] タブにのみ表示されます。 注意 [ICAP 事前検索] タブでは、脅威名がわからない場合 (Web 検査サービスで URL に対する脅威名が表示されない場合など)、[未定義の脅威] と表示されます。
脅威の種類	トレンドマイクロのパターンファイルとその他のコンポーネントによって検出された脅威の種類 この列は [完了] タブにのみ表示されます。
経過時間	処理が開始してから経過した時間 この列は [処理中] タブにのみ表示されます。

列	情報
処理元	オブジェクトを処理しているノードの IP アドレス (Deep Discovery Analyzer が負荷分散クラスタで設定されている場合) この列は [完了] および [処理中] タブにのみ表示されます。 **注意** インタラクティブモードを有効にしてサンプルを分析している場合、[処理中] 画面では次のタスクを実行できます。 ・ 現在のステータスを確認する ([アクセスを準備しています]、[アクセス可能]、[完了しています]、または [完了]) ・ このフィールドをクリックして詳細情報を表示する (インタラクティブモードでの分析方法や VNC アクセスの IP アドレスとポート情報など) ・ [分析の停止] をクリックしてサンプル分析を終了する
優先度	サンプルに割り当てられた優先度 この列は [処理待ち] タブにのみ表示されます。
処理待ち時間	仮想アナライザがサンプルをキューに追加してから経過した時間 この列は [処理待ち] タブにのみ表示されます。
エラー	分析が失敗した理由 この列は [失敗] タブにのみ表示されます。
子ファイル	サンプル内で検出された子ファイルの数 数字をクリックすると、子ファイルの詳細な検出情報が表示されます。詳細については、83 ページの「子ファイルの検出情報を表示する」を参照してください。 この列は [ICAP 事前検索] タブにのみ表示されます。
検出元	オブジェクトを処理した検出モジュールの名前 この列は [ICAP 事前検索] タブにのみ表示されます。

列	情報
YARA ルールファイル	一致する YARA ルールを含む YARA ルールファイルの名前 子ファイルが検出された場合、リンクをクリックすると YARA 検出の詳細な情報が表示されます。 この列は [完了] タブにのみ表示されます。 **注意** • 子ファイルに対する一致は見つかったが、親ファイルに対する一致は見つからなかった場合、このフィールドには、一致する YARA ルールを含む任意の YARA ルールファイルの名前が表示されます。 • 親ファイルに対する一致、または子ファイルのないファイルに対する一致が見つかった場合、このフィールドには、一致する YARA ルールを含む YARA ルールファイルの名前が表示されます。
YARA ルール名	一致する YARA ルールの名前。 この列は [完了] タブと [ICAP 事前検索] タブに表示されます。
イベント情報	
イベントのログ記録日時	• 他のトレンドマイクロ製品によって送信されたサンプルの場合、その製品がサンプルを送信した日時 • 手動で送信されたサンプルと ICAP クライアントにより送信されたサンプルの場合、Deep Discovery Analyzer がサンプルを受信した日時
送信元/送信者	サンプルの送信元 • ネットワークトラフィックの IP アドレス • メールでの送信のメールアドレス • 手動で送信された場合はデータなし (ダッシュで示されます)

列	情報
送信先/受信者	サンプルの送信先 • ネットワークトラフィックの IP アドレスまたはメールのメールアドレス • サンプルが手動で送信されたか、メールメッセージを介して送信された場合はデータなし (ダッシュで示されます)
プロトコル	• メールの場合は SMTP、ネットワークトラフィックの場合は HTTP など、サンプルの送信に使用されたプロトコル • 手動で送信された場合はデータなし (ダッシュで示されます) この列は [完了]、[処理中]、[処理待ち]、および [失敗] タブにのみ表示されます。
URL	サンプルの URL 注意 管理コンソールを使用して送信された場合は、Deep Discovery Analyzer が URL を正規化している場合があります。
メールの件名	サンプルのメールの件名 この列は [完了]、[処理中]、[処理待ち]、および [失敗] タブにのみ表示されます。
メッセージ ID	サンプルのメッセージ ID この列は [完了]、[処理中]、[処理待ち]、および [失敗] タブにのみ表示されます。
送信元 IP	ICAP クライアントにより送信された X-Client-IP ICAP ヘッダに基づく、サンプルの送信元の IP アドレス この列は [ICAP 事前検索] タブにのみ表示されます。
送信先 IP	ICAP クライアントにより送信された X-Server-IP ICAP ヘッダに基づく、サンプルの送信先の IP アドレス この列は [ICAP 事前検索] タブにのみ表示されます。

列	情報
送信元ユーザ	ICAP クライアントにより送信された X-Authenticated-User ICAP ヘッダに基づく、サンプルが検出された時点でログオンしていたユーザ この列は [ICAP 事前検索] タブにのみ表示されます。
Threat Connect	Threat Connect へのリンクを表示します この列は [ICAP 事前検索] タブにのみ表示されます。

ICAP での送信

Deep Discovery Analyzer では、ICAP (Internet Content Adaptation Protocol) クライアントとの統合がサポートされます。

ICAP 事前検索

ICAP クライアントが分析用にサンプルを送信すると、Deep Discovery Analyzer は次のリソースを使用して事前検索を行い、既知の脅威と受信したサンプルを比較します。

- ファイル検索用の高度な脅威検索エンジン (ATSE)
- YARA ルール
- 不審オブジェクトおよびユーザ指定の不審オブジェクトリスト
- 機械学習型検索エンジン
- URL 検索用の Web レピュテーションサービス (WRS)
- Deep Discovery Analyzer キャッシュ

事前検索の結果に応じて、Deep Discovery Analyzer は次の処理を行います。

結果	処理
サンプルが既知の安全なファイル/URL である場合	• 分析用に送信された元の HTTP リクエストやレスポンスを ICAP クライアントに返します。

結果	処理
サンプルが既存のレコードと一致しない場合	• 分析用に送信された元の HTTP リクエストやレスポンスを ICAP クライアントに返します。 • 仮想アナライザに送信されたサンプルとして処理し、[送信] キューに送ります。このサンプルは [ICAP 事前検索] タブには表示されません。 • 今後の送信の参考として、サンプルを Deep Discovery Analyzer データベースに追加します。 **注意** 送信されたサンプルのファイルタイプを仮想アナライザがサポートしていない場合、Deep Discovery Analyzer はそのサンプルを [送信] キューに送ることも、Deep Discovery Analyzer データベースに追加することもしません。
サンプルが既知の不正な脅威と一致する場合	• `403 Forbidden` メッセージを応答として ICAP クライアントに返します。 • サンプルをログ記録し、サンプルの詳細を [ICAP 事前検索] タブに表示します。

注意

[送信] 画面に [ICAP 事前検索] タブを表示するには、[管理] > [統合製品/サービス] > [ICAP] で設定を有効にします。このタブは初期設定で非表示になっています。

詳細については、203 ページの「[ICAP] タブ」を参照してください。

ICAP ヘッダの応答

ICAP クライアントから送信される各サンプルに対して、Deep Discovery Analyzer は ICAP ヘッダを返します。

次に例を示します。

```
ICAP/1.0 200 OK
Server: Deep Discovery Analyzer 6.8 Build 1165
ISTag: "12.300.1011"
```

```
X-Virus-ID: TROJ_FRS.0NA103DD20,TROJ_FRS.0NA104DD20
X-Infection-Found: Type=0; Resolution=2; Threat=TROJ_FRS.0NA103
DD20,TROJ_FRS.0NA104DD20;
X-Response-Desc: URL: No risk rating from WRS; FILE: Detected b
y ATSE
Encapsulated: res-hdr=0, res-body=86
Date: Thu, 16 Apr 2020 07:38:01 GMT
```

次の表は、ICAP ヘッダの詳細を示しています。

ICAP ヘッダ	値	例

ICAP/1.0	ICAP のステータスコード
	例:
	• 204: ICAP クライアントが 204 ステータスコード受け入れ、キャッシュされているコンテンツを使用する場合
	• 200:
	  • ICAP クライアントが 204 ステータスコードを受け入れない場合
	  • ICAP クライアントがキャッシュに保存するにはコンテンツが大きすぎます。Deep Discovery Analyzer から、`200 OK` とともに HTTP コンテンツが返されます。
	  • 脅威が検出されています。Deep Discovery Analyzer から、`200 OK` とともに ICAP ヘッダと HTTP 403 Forbidden が返されます。
	ステータスコードの詳細については、RFC ドキュメントを参照してください。
		ICAP 1.0 200 OK
		ICAP 1.0 204 No Content

Server	Deep Discovery Analyzer のバージョンとビルド番号	Server: Deep Discovery Analyzer 6.8 Build 1165

ICAP ヘッダ	値	例
ISTag	Deep Discovery コンポーネント (Linux、64 ビット) の高度な脅威検索エンジンのバージョン Deep Discovery Analyzer の以前の応答をキャッシュしている可能性のある ICAP クライアントで、その有効期限が切れていないかどうかを確認するために使用されます。	ISTag: "12.300.1011"
Encapsulated	メッセージの本文のカプセル化の開始位置に相対する、カプセル化された各セクションの開始位置のオフセット	Encapsulated: req-hdr=0, req-body=86
Date	Deep Discovery Analyzer クロックにより提供される、RFC 1123 準拠の日付/時刻文字列として指定された日時の値	Date: Thu, 16 Apr 2020 07:38:01 GMT

ICAP ヘッダの詳細については、次のサイトを参照してください。

http://www.icap-forum.org/

次の表は、Deep Discovery Analyzer によって返される追加のヘッダを示しています。

注意

設定が有効な場合、Deep Discovery Analyzer は常に X-Response-Desc ヘッダを返します。また、ICAP クライアントから受信したサンプルの事前検索で既知の脅威が検出された場合のみ X-Virus-ID および X-Infection-Found ヘッダを返します。

ICAP ヘッダ	値	例
X-Virus-ID	検出されたウイルスまたはリスクの名前を含む 1 行の US-ASCII テキスト	X-Virus-ID: TSPY_ONLINEG.MCS
X-Infection-Found	感染の種類と解決策の数値コード、およびリスクの説明	X-Infection-Found: Type=0; Resolution=2; Threat=TSPY_ONLINEG.MCS;

ICAP ヘッダ	値	例
X-Response-Desc	Deep Discovery Analyzer で URL またはファイルサンプルが不正または安全と見なされた理由	X-Response-Desc: URL: No risk rating from WRS; FILE: Detected by ATSE

注意

これらのヘッダを有効にしたり、他の ICAP 設定を行ったりするには、[管理] > [統合製品/サービス] > [ICAP] の順に選択します。

詳細については、205 ページの「ICAP を設定する」を参照してください。

X-Response-Desc ヘッダは事前検索の結果に応じて異なります。次の表は、X-Response-Desc ヘッダの詳細を示しています。

表 4-2. X-Response-Desc ヘッダ: URL

X-Response-Desc ヘッダ	説明
No risk rating from WRS	Web レピュテーションサービスで検出され、安全と見なされています。
Match found in URL exception list	除外リストのエントリに一致しており、[除外] 画面に表示されます。
No risk rating from VA	仮想アナライザで検出され、安全と見なされています。
Bypass URL scanning in RESPMOD mode	[ICAP] 画面で [RESPMOD モードでの URL 検索のバイパス] を選択すると、Deep Discovery Analyzer は RESPMOD モードで URL を検索しません。
Invalid URL	形式が無効として検出されています。
Unable to analyze URL in VA	この URL は仮想アナライザでサポートされていません。
Detected by WRS	Web レピュテーションサービスで検出され、不正と見なされています。
Detected by suspicious objects list	不審オブジェクトリストのエントリに一致しています。
Detected by user-defined suspicious objects list	ユーザ指定の不審オブジェクトリストのエントリに一致しています。

X-RESPONSE-DESC ヘッダ	説明
Detected by VA cache	仮想アナライザですでに分析され、不正と見なされています。
URL submitted to VA	事前検索の結果がありません。URL のサンプルを仮想アナライザに送信して分析します。

表 4-3. X-Response-Desc ヘッダ: File

X-RESPONSE-DESC ヘッダ	説明
Match found in file exception list	除外リストのエントリに一致しており、[除外] 画面に表示されます。
No risk rating from VA	仮想アナライザで検出され、安全と見なされています。
Unsupported file type in VA	次のいずれかの原因により、仮想アナライザで分析されません。 • 仮想アナライザでサポートされていないファイルタイプである サポートされているファイルタイプの詳細については、116 ページの「[送信設定] タブ」を参照してください。 • パスワード保護されているため、仮想アナライザで抽出して分析できない • その他
Bypass MIME content-type scanning	[MIME コンテントタイプの除外を有効にする] を選択し、そのコンテントタイプが除外リストにある場合、Deep Discovery Analyzer ではこのファイルが検索されません。
Maximum file size exceeded	ファイルサイズが最大値 (60MB) を超えています。
Bypass true file type scanning	[MIME コンテントタイプの検証を有効にする] を選択し、そのファイルタイプが除外リストにある場合、Deep Discovery Analyzer ではこのファイルが検索されません。
Detected by ATSE	Deep Discovery の高度な脅威検索エンジンで検出されています。
Detected by YARA rule	YARA ルールに一致しています。

X-Response-Desc ヘッダ	説明
Detected by suspicious objects list	不審オブジェクトリストのエントリに一致しています。
Detected by user-defined suspicious objects list	ユーザ指定の不審オブジェクトリストのエントリに一致しています。
Detected by Predictive Machine Learning engine	機械学習型検索エンジンで検出されています。
Detected by VA cache	仮想アナライザですでに分析され、不正と見なされています。
File submitted to VA	事前検索の結果がありません。ファイルのサンプルを仮想アナライザに送信して分析します。
Detected as password-protected file. Block sample without scanning	[ICAP] 画面で [検索せずにサンプルをパスワード保護されたファイルとして分類する] を選択している場合、パスワード保護されているファイルは検索なしでブロックされます。
Detected as password-protected file. Block non-malicious sample that cannot be extracted	[ICAP] 画面で [ファイルを抽出できない場合のみ、既知のリスクを含まないサンプルをパスワード保護されたファイルとして分類する] を選択している場合、パスワード保護されたファイルが抽出できないが、すべての ICAP 事前検索モジュールによる検索でリスクなしと判定されると、この結果がヘッダで返されます。

次のヘッダの例では、ファイルと URL が安全と見なされています。

```
ICAP/1.0 204 No Content
Server: Deep Discovery Analyzer 6.8 Build 1165
ISTag: "12.300.1011"
X-Response-Desc: URL: No risk rating from WRS; FILE: No risk ra
ting from VA
Date: Thu, 16 Apr 2020 07:32:30 GMT
```

次のヘッダの例では、ファイルが高度な脅威検索エンジンで検出されているため、Deep Discovery Analyzer から `HTTP/1.1 403 Forbidden` ステータスコードが返されています。この URL は検索されません。

注意

管理コンソールでリダイレクトページを設定している場合は、HTTP 403 Forbidden ヘッダに続き、Deep Discovery Analyzer からリダイレクトページのコンテンツが送信されます。

```
ICAP/1.0 200 OK
Server: Deep Discovery Analyzer 6.8 Build 1165
ISTag: "12.300.1011"
X-Virus-ID: TROJ_FRS.0NA103DD20,TROJ_FRS.0NA104DD20
X-Infection-Found: Type=0; Resolution=2; Threat=TROJ_FRS.0NA103
DD20,TROJ_FRS.0NA104DD20;
X-Response-Desc: URL: Bypass URL scanning in RESPMOD mode; FILE
: Detected by ATSE
Encapsulated: res-hdr=0, res-body=86
Date: Thu, 16 Apr 2020 07:38:01 GMT

HTTP/1.1 403 Forbidden
```

次のヘッダの例では、URL は安全と見なされ、ファイルの検出情報がありません。このファイルのサンプルは自動的に Deep Discovery Analyzer に送信され、分析されます。

```
ICAP/1.0 204 No Content
Server: Deep Discovery Analyzer 6.8 Build 1165
ISTag: "12.300.1011"
X-Response-Desc: URL: No risk rating from WRS; FILE: File submi
tted to VA
Date: Thu, 16 Apr 2020 07:22:41 GMT
```

送信のタスク

次の表は、[送信] のすべてのタスクのリストです。

表 4-4. [送信] のタスク

タスク	手順
オブジェクトの送信	完了したら、[送信する] をクリックし、[処理中] または [処理待ち] タブのステータスを確認します。分析されたサンプルは、[完了] タブに表示されます。 詳細については、73 ページの「オブジェクトを送信する」を参照してください。 一度に複数のファイルを手動で送信するには、Manual Submission Tool を使用します。76 ページの「オブジェクトを手動で送信する」を参照してください。
再分析	1 つ以上のサンプルを選択して [再分析] をクリックすることで、次の操作を実行します。 ・ 既存の分析結果を削除します。 ・ サンプルをキューに再送信します。 ・ キャッシュされたデータを無視して、サンプルを再分析します。 このオプションは [完了] および [失敗] タブにのみ表示されます。 詳細については、71 ページの「サンプルを再分析する」を参照してください。
すべてエクスポート	すべての表示された送信を CSV ファイルにエクスポートします。 このオプションは [完了]、[失敗]、および [ICAP 事前検索]タブにのみ表示されます。
削除	1 つ以上のエントリ (最大 50) を選択して [削除] をクリックすると、選択したサンプルとすべての関連する分析データが削除されます。 このオプションは [完了]、[処理待ち]、および [失敗] タブにのみ表示されます。
詳細情報画面	[完了] タブで、行の任意の場所をクリックすると、送信されたサンプルの詳細情報が表示されます。行の下にある新しいセクションに、詳細が表示されます。 詳細については、80 ページの「詳細情報画面」を参照してください。

タスク	手順
オブジェクトの優先度設定	キューの先頭にオブジェクトを移動するには、[処理待ち] タブでオブジェクトを選択して [優先度設定] をクリックします。

タスク	手順
データフィルタ	表内のエントリが多すぎる場合、データフィルタを使用してエントリを限定します。それぞれのタブで異なるデータフィルタを使用できます。 [完了] タブのみで使用可能なデータフィルタ: • リスクレベル: [リスクレベル] 列に基づいてフィルタを実行します。 • イベントのログ記録日時: [イベントのログ記録日時] 列に基づいてフィルタを実行します。すべての期間は、Deep Discovery Analyzer が使用する時間を示します。期間が選択されていない場合、初期設定の [24 時間以内] が使用されます。 [処理中] タブのみで使用可能なデータフィルタ: • 種類: すべてのエントリ、またはインタラクティブモードを有効にして処理したサンプルを表示できます。 [失敗] タブのみで使用可能なデータフィルタ: • エラー:[エラー] 列に基づいてフィルタを実行します。 • 送信: [送信] 列に基づいてフィルタを実行します。すべての期間は、Deep Discovery Analyzer が使用する時間を示します。期間が選択されていない場合、初期設定の [24 時間以内] が使用されます。 [ICAP 事前検索] タブのみで使用可能なデータフィルタ: • 検出:[検出] 列に基づいてフィルタを実行します。すべての期間は、Deep Discovery Analyzer が使用する時間を示します。期間が選択されていない場合、初期設定の [24 時間以内] が使用されます。 次のオプションはすべてのタブで使用できます。 • すべてのタブに検索ボックスがあります。検索する文字を入力して <Enter> キーを押します。Deep Discovery Analyzer は、現在のタブ内のファイル名と URL のみを対象に一致を検索します。[完了] タブで検索を実行すると、子ファイル名も一致の対象になります。 • [詳細] リンクは、1 つ以上の列で指定された情報に従ってエントリを絞り込みます。詳細については、70 ページの「詳細フィルタを適用する」を参照してください。

タスク	手順
列のカスタマイズ	表内に表示する列をカスタマイズするには、歯車アイコン ( ) をクリックし、表示する列を選択して、[適用] をクリックします。 Deep Discovery Analyzer では、ユーザアカウントの列の設定を保存し、次回ユーザが [送信] 画面にアクセスした際、選択された列を表内に表示します。
レコードコントロールとページ区切りコントロール	画面の最下部にあるパネルには、サンプルの合計数が表示されます。すべてのサンプル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サンプルを表示します。

詳細フィルタを適用する

手順

1. [詳細] をクリックします。

   フィルタバーが表示されます。

2. [フィルタ] ドロップダウンボックスで属性を選択します。

3. 選択した属性に応じて必要な情報を指定します。

4. 属性を追加するには+をクリックします。

   属性を削除するには×をクリックします。最後のフィルタは削除できません。

5. [適用] をクリックすると、フィルタが現在の表にただちに適用されます。

   適用後は次のオプションが使用可能になります。

   - 編集: 現在のフィルタを編集します
   - クリア: 適用したフィルタを削除します
   - 保存: フィルタの変更を保存したり、フィルタを新しい名前で保存したりします

注意

- フィルタは作成したタブ内に保存されます。ただし Deep Discovery Analyzer では、異なるタブ内に存在する場合でも、重複したフィルタ名を使用することはできません。
- 検索テキストボックスの▾をクリックすると、現在のタブに保存されているすべてのフィルタが表示されます。保存されたフィルタを選択すると、そのフィルタが現在の表にただちに適用されます。
- 保存されたフィルタを削除するには✖をクリックします。

6. [キャンセル] をクリックすると、現在のフィルタが破棄されます。

サンプルを再分析する

次の目的で、選択したサンプルを再分析できます。

- 既存の分析結果を削除します。
- サンプルをキューに再送信します。
- キャッシュされたデータを無視して、サンプルを再分析します。

注意

インタラクティブモードを有効にしてサンプルを再分析することもできます。

手順

1. [仮想アナライザ] > [送信] の順に選択します。
2. サンプルを 1 つ以上選択して、[再分析] をクリックします。
3. (オプション) 前回のサンプル分析で検出された不審オブジェクトを削除するには、[関連する不審オブジェクトの削除] を選択します。
4. (オプション) サンプル分析のために仮想アナライザへの VNC アクセスを可能にするには、[このサンプル分析に対してインタラクティブモードを有効にする] を選択し、次の設定を行います。

a. Windows イメージを選択します。

b. タイムアウト期間を選択します。

注意

- サンプルが正常に送信されると、タイムアウトのカウントダウンタイマが開始されます。タイムアウト期間が終了した場合、分析が進行中であっても VNC アクセスは終了されます。たとえば、サンプルの送信に 30 分のタイムアウト期間を設定し、VNC セッションを 5 分後に開始する場合、セッションの残り時間は 25 分になります。
- タイムアウトのカウントダウンはアーカイブ内の各ファイルに対して個別に開始されるため、アーカイブファイルの実際のタイムアウト期間は指定した設定よりも長くなることがあります。

c. VNC クライアントを使用してイメージにアクセスする場合、仮想アナライザにより自動的に分析を開始するには、[自動] 分析方法を選択します。VNC セッションの開始後に手動で分析を開始するには、[手動] を選択します。

注意

- インタラクティブモードは、URL リストの送信や、再分析用に複数のサンプルが選択されている場合は使用できません。
- Deep Discovery Analyzer 管理者は、ポート範囲や VNC アクセス用のセキュリティパスワードなど、詳細なインタラクティブモード設定を行うことができます。

  詳細については、129 ページの「[インタラクティブモード設定] タブ」を参照してください。

5. [続行] をクリックします。

オブジェクトを送信する

手順

1. [仮想アナライザ] > [送信] の順に選択します。
2. [オブジェクトの送信] をクリックします。

   [オブジェクトの送信] 画面が表示されます。
3. 単一のファイルを送信するには、[ファイル] を選択します。
   a. アップロードするサンプルを参照して選択します。
   b. (オプション) ポータブル実行可能ファイルのサンプルの場合、必要に応じてコマンドパラメータを指定します。
   c. (オプション) [優先度設定] を選択して、送信されたオブジェクトをキューの先頭に配置します。
   d. (オプション) サンプル分析のために仮想アナライザへの VNC アクセスを可能にするには、[このサンプル分析に対してインタラクティブモードを有効にする] を選択し、次の設定を行います。
      i. イメージを選択します。
      ii. タイムアウト期間を選択します。

      注意

      サンプルが正常に送信されると、タイムアウトのカウントダウンタイマが開始されます。タイムアウト期間が終了した場合、分析が進行中であっても VNC アクセスは終了されます。たとえば、サンプルの送信に 30 分のタイムアウト期間を設定し、VNC セッションを 5 分後に開始する場合、セッションの残り時間は 25 分になります。

      iii. VNC クライアントを使用してイメージにアクセスする場合、仮想アナライザにより自動的に分析を開始するには、[自動] 分析方法を選択します。VNC セッションの開始後に手動で分析を開始するには、[手動] を選択します。

注意

- インタラクティブモードは、URL リストの送信や、送信用に複数のサンプルが選択されている場合は使用できません。
- Deep Discovery Analyzer 管理者は、ポート範囲や VNC アクセス用のセキュリティパスワードなど、詳細なインタラクティブモード設定を行うことができます。

  詳細については、129 ページの「[インタラクティブモード設定] タブ」を参照してください。

e. [送信する] をクリックします。

注意

- サンプルの送信後は、[処理中] タブで VNC アクセス情報および分析ステータスを確認できます。実行中の仮想アナライザイメージに対して VNC セッションを開始するには、VNC アクセス情報を使用します。
- アーカイブの場合、仮想アナライザはアーカイブ内のファイルの分析結果を 1 つのレポートにマージします。

4. 単一の URL を送信するには、[URL] を選択します。

   a. 単一の URL を指定します。

   b. (オプション) [URL プレフィルタに送信] を選択して、送信された URL を URL プレフィルタに送信します。URL プレフィルタで安全が確認された URL は、検索と分析のために仮想アナライザに送信されません。

   c. (オプション) [優先度設定] を選択して、送信されたオブジェクトをキューの先頭に配置します。

   d. [送信する] をクリックします。

注意

送信前に、Deep Discovery Analyzer は次のすべてを正規化します。

- URL ドメインの Punycode
- URL パスとクエリ文字列の URL エンコーディング

5. 複数の URL を送信するには、[URL リスト] を選択します。

   a. URL リストファイルを参照して選択します。

注意

URL リストは、最大 1,000 件の URL を含む CSV または TXT ファイルです。CSV ファイルの場合、最初の列に URL を指定してください。URL リストファイルでは 1 行に 1 つの URL を指定し、UTF-8 エンコーディングを使用する必要があります。

送信前に、Deep Discovery Analyzer は次のすべてを正規化します。

- URL ドメインの Punycode
- URL パスとクエリ文字列の URL エンコーディング

1,000 件の URL の分析には数時間かかることがあります。

   b. (オプション) [URL プレフィルタに送信] を選択して、送信された URL を URL プレフィルタに送信します。URL プレフィルタで安全が確認された URL は、検索と分析のために仮想アナライザに送信されません。

   c. (オプション) [優先度設定] を選択して、送信されたオブジェクトをキューの先頭に配置します。

   d. [送信する] をクリックします。

6. 特定のファイルを特定のパスに配置することが必要なアプリケーションをアップロードするには、[バンドルファイル] を選択します。

   a. アーカイブファイルを参照して選択します。

> **注意**
> アーカイブの場合、仮想アナライザはアーカイブ内のファイルの分析結果を 1 つのレポートにマージします。

b. アーカイブ内のどのファイルを実行するかを指定します。

c. (オプション) ポータブル実行可能ファイルのサンプルの場合、必要に応じてコマンドパラメータを指定します。

d. (オプション) [優先度設定] を選択して、送信されたオブジェクトをキューの先頭に配置します。

e. ファイルの解凍先を指定します。

- アーカイブ内のすべてのファイルを単一のフォルダに解凍するには、[解凍先のパス] テキストボックスに完全なパスを指定します。
- アーカイブ内の特定のファイルを別のパスに解凍するには、その [ファイル名] と完全な [パス] を次のセクションに指定します。
  - 新しいファイルを指定するには + をクリックします。
  - エントリを削除するには × をクリックします。

f. ファイル名で使用される文字エンコードを指定します。

g. [送信する] をクリックします。

> **注意**
> 一度に複数のファイルを手動で送信するには、Manual Submission Tool を使用します。詳細については、76 ページの「オブジェクトを手動で送信する」を参照してください。

オブジェクトを手動で送信する

Manual Submission Tool を使用して、ユーザのコンピュータ上の場所から Deep Discovery Analyzer にサンプルをリモートで送信できます。この機能で

は複数のサンプルを一度に送信できます。これらのサンプルは [送信] キューに追加されます。

Manual Submission Tool では、Microsoft Windows OS に加えて次の Linux ディストリビューションがサポートされます。

- CentOS/RedHat 5.x (32 ビットおよび 64 ビット)
- CentOS/RedHat 6.x (32 ビットおよび 64 ビット)
- CentOS/RedHat 7.x (32 ビットおよび 64 ビット)
- Ubuntu 12.04 (32 ビット)

重要

`glibc.i686` および `zlib.i686` を 64 ビット Linux ディストリビューションにインストールする必要があります。

オブジェクトを手動で送信する (Windows)

手順

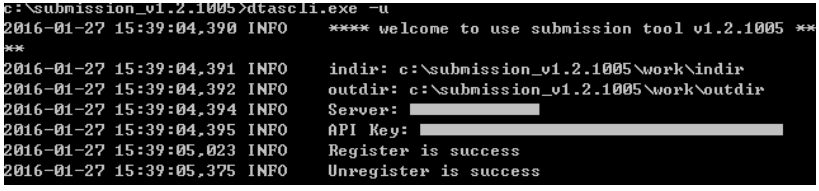
1. Manual Submission Tool がインストールされていない場合は、インストールします。詳細については、281 ページの「Manual Submission Tool」を参照してください。
2. Manual Submission Tool パッケージのフォルダに移動し、`work` フォルダを開いて、すべてのサンプルファイルまたは URL リストファイルを `indir` フォルダに配置します。
3. `cmd.exe` を実行し、ディレクトリをツールパッケージのフォルダに変更 (`cd`) します。
4. アップロードするオブジェクトの種類に応じて、次のいずれかを実行します。

ヒント

ヘルプを表示するには、`dtascli.exe` を実行します。

- ファイル: `dtascli.exe -u` を実行して、`work/indir` フォルダ内のすべてのファイルを仮想アナライザにアップロードします。

  `dtascli.exe -u` の実行後、`cmd.exe` によって、`work/indir` フォルダからアップロードしたすべてのファイルを示す次のような画面が表示されます。



- URL リスト: `dtascli.exe -u --url` を実行して、`work/indir` フォルダ内の `url.txt` ファイルを仮想アナライザにアップロードします。

  `dtascli.exe -u --url` の実行後、`cmd.exe` によって、`work/indir` フォルダからアップロードしたすべてのファイルを示す次のような画面が表示されます。

注意

URL リストには「`URL.txt`」という名前を使用する必要があります。

送信前に、Deep Discovery Analyzer は次のすべてを正規化します。

- URL ドメインの Punycode
- URL パスとクエリ文字列の URL エンコーディング

5. ファイルを仮想アナライザにアップロードした後、それらが管理コンソールで分析されていることを確認します。[仮想アナライザ] > [送信] をクリックしてファイルの場所を確認します。

   ファイルは送信後、分析前は [処理中] タブまたは [処理待ち] タブに表示されます。分析されたサンプルは、[完了] タブに表示されます。分析中にエラーが発生したサンプルは、[失敗] タブに表示されます。

オブジェクトを手動で送信する (Linux)

手順

1. Manual Submission Tool がインストールされていない場合は、インストールします。詳細については、281 ページの「Manual Submission Tool」を参照してください。
2. Manual Submission Tool パッケージのフォルダに移動し、`work` フォルダを開いて、すべてのサンプルファイルまたは URL リストファイルを `indir` フォルダに配置します。
3. ターミナルを開き、ディレクトリをツールパッケージのフォルダに変更 (`cd`) します。
4. `chmod +x dtascli` を実行します。
5. アップロードするオブジェクトの種類に応じて、次のいずれかを実行します。

   ヒント

   ヘルプを表示するには、`./dtascli` を実行します。

   - ファイル: `./dtascli -u` を実行して、`work/indir` フォルダ内のすべてのファイルを仮想アナライザにアップロードします。

     `./dtascli -u` の実行後、`terminal` によって、`work/indir` フォルダからアップロードしたすべてのファイルが表示されます。

   - URL リスト: `./dtascli -u --url` を実行して、`work/indir` フォルダ内の `url.txt` ファイルを仮想アナライザにアップロードします。

`./dtascli -u --url` の実行後、`terminal` によって、`work/indir` フォルダからアップロードしたすべてのファイルが表示されます。

注意

URL リストには「`URL.txt`」という名前を使用する必要があります。

送信前に、Deep Discovery Analyzer は次のすべてを正規化します。

- URL ドメインの Punycode
- URL パスとクエリ文字列の URL エンコーディング

6. ファイルを仮想アナライザにアップロードした後、それらが管理コンソールで分析されていることを確認します。[仮想アナライザ] > [送信] をクリックしてファイルの場所を確認します。

   ファイルは送信後、分析前は [処理中] タブまたは [処理待ち] タブに表示されます。分析されたサンプルは、[完了] タブに表示されます。分析中にエラーが発生したサンプルは、[失敗] タブに表示されます。

詳細情報画面

[完了] タブで、行の任意の場所をクリックすると、送信されたサンプルの詳細情報が表示されます。行の下にある新しいセクションに、詳細が表示されます。

この画面には、次のフィールドが表示されます。

<table>
<tr><th rowspan="2">フィールド名</th><th colspan="2">情報</th></tr>
<tr><th>ファイル/メールメッセージのサンプル</th><th>URL のサンプル</th></tr>
<tr><td>送信の詳細</td><td>未加工ログから抽出された基本データフィールド (ログの日時、ファイル名、およびタイプなど)</td><td>未加工ログから抽出された基本データフィールド (ログの日時、URL、送信元 IP アドレスとポート番号、および送信先 IP アドレスとポート番号など)

注意
Deep Discovery Analyzer が URL を正規化している場合があります。</td></tr>
<tr><td></td><td colspan="2">• サンプルの ID (SHA-1)
• 送信されたサンプルに含まれるか、そのサンプルから生成された子ファイル (存在する場合)
• サンプルを処理したノードの IP アドレス
• 未加工ログのデータフィールドをすべて表示する [未加工のログ] リンク
• ネットワーク共有で実行された検索に対する検索処理</td></tr>
</table>

フィールド名	情報	
	ファイル/メールメッセージのサンプル	URL のサンプル

著しい特性	• サンプルが示す著しい特性のカテゴリ。次のいずれかまたはすべてが該当します。
	  • セキュリティ製品への耐性、自己保護
	  • 自動実行や他システムの再設定
	  • 詐欺、ソーシャルエンジニアリング
	  • ファイルのドロップ、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
	  • 不正な形式、不完全、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
	  • 不審ネットワークやメッセージングアクティビティ
	• 数字のリンク。クリックすると、実際の著しい特性が表示されます。	

その他の送信ログ	その他のログの送信について次の情報を示す表 • ログの日時 • プロトコル • 方向 • 送信元 IP • 感染元ホスト名 • 送信先 IP • 感染先ホスト名	
MITRE ATT&CK™ Framework	検出された MITRE ATT&CK™の Tactics と Techniques のリスト。リンクをクリックすると、MITRE の Web サイトで詳細情報を確認できます。	

フィールド名	情報	
	ファイル/メールメッセージのサンプル	URL のサンプル
レポート	PDF アイコン () はダウンロード可能な PDF レポートにリンクし、HTML アイコン () はインタラクティブな HTML レポートにリンクします。 **注意** リンクがクリックできない場合、シミュレーション中にエラーが発生したことを意味します。リンクにマウスを重ねると、エラーの詳細が表示されます。	
調査パッケージ	ダウンロードして追加の調査を実行できる、パスワードによって保護された調査パッケージへの [ダウンロード] リンク 詳細については、84 ページの「調査パッケージ」を参照してください。	
グローバルインテリジェンス	トレンドマイクロ Threat Connect を表示する [Threat Connect で表示] リンク このページには、サンプルの詳細情報が含まれます。	

子ファイルの検出情報を表示する

送信されたサンプル内の子ファイルの詳細な検出情報を表示できます。

手順

1. [仮想アナライザ] > [送信] の順に選択します。
2. [ICAP 事前検索] タブをクリックします。
3. [子ファイル] 列の数字をクリックします。

   [検出された子ファイル] 画面が表示されます。

   次の表は、画面の詳細を示しています。

フィールド	説明
ファイル名	子ファイルの名前
ファイルの種類	子ファイルのファイルタイプ
脅威	トレンドマイクロのパターンファイルとその他のコンポーネントによって検出された脅威の名前
SHA-1	子ファイルの SHA-1 値
SHA-256	子ファイルの SHA-256 値
YARA ルール名	一致した YARA ルールの名前
YARA ルールファイル	一致する YARA ルールを含む YARA ルールファイルの名前

調査パッケージ

調査パッケージを使用することで、管理者と調査者は、仮想アナライザで分析されたサンプルから生成された脅威データを検査して解釈できるようになります。調査パッケージには、影響を受けたホストまたはネットワークで識別された IOC (Indicators of Compromise) を説明する OpenIOC 形式のファイルが含まれています。

次の表は、調査パッケージに含まれる一部のファイルを示しています。

表 4-5. 調査パッケージの内容

調査パッケージ内のパス	説明
¥%SHA1%	ルートレベルにある各フォルダは、その名前に SHA-1 ハッシュ値を持ち、1 つのオブジェクトと関連付けられています。この種類のフォルダは、最初のオブジェクトがアーカイブファイルまたはメールメッセージである場合にのみ複数存在します。
¥%SHA1%¥%imageID%	オブジェクトを分析したサンドボックスイメージと関連付けられています。

調査パッケージ内のパス	説明
¥%SHA1%¥%imageID%¥drop¥droplist	分析時に生成または変更されたファイルのリストが含まれます。
¥%SHA1%¥%imageID%¥memory¥image.bin	メモリでプロセスが開始された後の未加工のメモリダンプが含まれます。
¥%SHA1%¥%imageID%¥pcap¥%SHA1%.pcap	ペイロードの抽出に使用できる、取得されたネットワークデータが含まれます。ネットワークデータが生成されなかった場合、このファイルは存在しません。
¥%SHA1%¥%imageID%¥report¥report.xml	特定のイメージの単一のオブジェクトに対する最終分析レポートが含まれます。
¥%SHA1%¥%imageID%¥report¥so.xml	分析時に検出されたすべての不審オブジェクトのリストが含まれます。分析時に不審オブジェクトが検出されなかった場合、このファイルは空です。
¥%SHA1%¥%imageID%¥report¥SHA1.ioc	攻撃者の戦術、手法、および手順、またはその他の侵害の証拠を識別する技術特性が含まれます。
¥%SHA1%¥%imageID%¥screenshot¥%SHA1%-%N%.png	分析時に発生した UI イベントのスクリーンショットです。分析時に UI イベントが発生しなかった場合、このファイルは存在しません。
¥common	すべてのサンプルに共通するファイルを含みます。
¥common¥drop¥%%%	分析時に生成または変更されます。
¥common¥sample¥%SHA1%	送信されたサンプルです。
¥common¥sample¥extracted¥%SHA1%	分析時にサンプルから抽出されます。
¥%SHA1%.report.xml	すべてのオブジェクトの最終分析レポートです。
¥%SHA1%¥%imageID%¥extrainfo	オブジェクトを分析したサンドボックスイメージに関連するファイルが含まれます。

調査パッケージ内のパス	説明
¥%SHA1%¥%imageID%¥extrainfo ¥extra_info.xml	オブジェクトを分析したサンドボックスイメージに関する詳細情報が含まれます。
¥%SHA1%¥%imageID%¥strings	オブジェクトを分析したサンドボックスイメージに関連するファイルが含まれます。
¥%SHA1%¥%imageID%¥strings¥ %SHA1%.string	サンドボックスイメージでの分析中にオブジェクトから取得した文字列ダンプが含まれます。
¥%SHA1%.ioc	IOC ファイル。
¥%SHA1%_ioc.stix	STIX IOC ファイル。
¥%SHA1%_so.stix	STIX SO ファイル。
¥%SHA1%_so_stix2.json	STIX2 SO ファイル。
¥%SHA1%_ioc_stix2.json	STIX2 IOC ファイル。

調査パッケージのデータの保持

Deep Discovery Analyzer では、調査パッケージのデータを最大 100 日間保持できますが、ストレージの制限によっては期間が短縮される可能性があります。

注意

調査パッケージのデータの可用性を確保するため、データは外部サーバにバックアップすることをお勧めします。詳細については、273 ページの「データのバックアップ」を参照してください。

次の例は、データの保持期間がストレージの制限にどのように影響を受けるかを示しています。

トレンドマイクロが実施したテストによると、調査パッケージのデータの平均サイズは 8MB です。Deep Discovery Analyzer で 1 日に 8,000 のサンプルを分析すると、結果として生成される調査パッケージのデータは 64,000MB になります。

クラスタモードの Deep Discovery Analyzer では、1 日あたりに使用されるディスク容量は、クラスタ内のアプライアンスの数を乗じたものとなります。

分析失敗の原因として考えられる理由

[リスクレベル] 列に灰色のアイコン () が表示される場合、仮想アナライザはサンプルを分析していません。次の表は、分析の失敗の原因として考えられる理由と実行できる対応策を示しています。

表 4-6. 分析失敗の原因として考えられる理由

理由	対応策
仮想アナライザがこのファイル形式をサポートしていないか、ファイルが空です。	[仮想アナライザ] > [サンドボックス管理] > [送信設定] タブで、サポートされるファイルタイプのリストを確認してください。
使用可能なサンドボックスイメージはこのファイル形式をサポートしていません。	[仮想アナライザ] > [サンドボックス管理] > [イメージ] タブで、サンドボックスイメージの情報を確認してください。
URL が 2,083 文字の制限を超えています。	URL が 2,083 文字を超えていないことを確認してください。
仮想アナライザはこの暗号または圧縮の形式をサポートしていません。	[仮想アナライザ] > [サンドボックス管理] > [ファイルパスワード] タブで、パスワードリストを確認してください。
仮想アナライザはこのファイル形式をサポートしていません。	現在のサンドボックスイメージでサポートされていないファイルタイプです。[仮想アナライザ] > [サンドボックス管理] > [イメージ] タブで、サンドボックスイメージの情報を確認してください。
仮想アナライザからインターネットにアクセスできません。	管理ネットワークのインターネット接続を確認してください。

理由	対応策
macOS 向けサンドボックスで予期しないエラーが発生しました。	テクニカルサポートにお問い合わせください。
タイムアウト期間が経過する前に macOS 向けサンドボックスが分析結果を返しませんでした。	分析用にオブジェクトを再送信してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。
macOS 向けサンドボックスへの接続を確立できません。	管理ネットワークのインターネット接続を確認してください。
URL が無効です。	指定した URL の形式が有効であることを確認してください。
解凍後のファイルサイズの合計が制限値を超えています。	抽出されたサンプルの合計ファイルサイズが指定された制限を超えていないことを確認してください。
分析用にアーカイブファイルが展開されました。子ファイルの検索に失敗しました。	子ファイルの検索結果を参照してください。
仮想アナライザでオブジェクトを分析できません。使用可能なディスク空き容量が不足しています。	分析を実行するのに十分なディスク容量があることを確認してください。
仮想アナライザでタイムアウト期間内にオブジェクトを分析できません。	分析用にオブジェクトを再送信してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。

理由	対応策
仮想アナライザでオブジェクトを分析できません。オブジェクトで必要な依存関係が見つかりません。	アプリケーションの実行に必要なファイルがありません。[バンドルファイル] オプションを使用して、オブジェクトの分析に必要なファイルをアップロードしてください。
仮想アナライザでオブジェクトを分析できません。分析中にオブジェクトがクラッシュします。	分析用にオブジェクトを再送信してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。
仮想アナライザでオブジェクトを分析できません。正しいコマンドライン引数を指定してオブジェクトを実行する必要があります。	必要なコマンドラインパラメータを指定してオブジェクトを再送信してください。
仮想アナライザでオブジェクトを分析できません。Office のライセンスの有効期限が切れています。	有効な Microsoft Office のライセンスを使用してイメージを再インポートしてください。
予期しないエラーが発生しました。分析用にサンプルを再送信してください。	分析用にオブジェクトを再送信してください。問題が解決しない場合は、テクニカルサポートにお問い合わせください。
macOS 向けサンドボックスのライセンスの有効期限が切れています。	テクニカルサポートにお問い合わせください。
ユーザにより分析がキャンセルされました。	インタラクティブモードでユーザがサンプル分析を中止しました。分析用にオブジェクトを再送信してください。

理由	対応策
仮想アナライザでタイムアウト期間内にオブジェクトを分析できません。	インタラクティブモードでサンプルがタイムアウト期間内に分析されず、仮想アナライザから-45 の評価が返されています。分析用にオブジェクトを再送信し、タイムアウト値を長く設定して、インタラクティブモードでタイムアウト期間内にサンプル分析を開始してください。

不審オブジェクト

不審オブジェクトとは、システムを危険にさらす、またはデータ損失を引き起こす可能性のあるオブジェクトです。Deep Discovery Analyzer は、不審 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。

注意

- 不審オブジェクトを Trend Micro Vision One または Deep Discovery Director から同期するように Deep Discovery Analyzer を設定できます。

  詳細については、191 ページの「Trend Micro Vision One」または 195 ページの「Deep Discovery Director に登録する」を参照してください。

- Deep Discovery Analyzer を Deep Discovery Director と Apex Central の両方と統合すると、Deep Discovery Analyzer は不審オブジェクトリストを Deep Discovery Director にのみアップロードします。

  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。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 Analyzer を Trend Micro Vision One、Deep Discovery Director、および Apex Central と統合すると、Deep Discovery Analyzer は不審オブジェクトリストを Trend Micro Vision One にのみアップロードします。

生成された不審オブジェクトリスト

次の表は、Deep Discovery Analyzer で検出され、生成された不審オブジェクトリストに追加される不審オブジェクトを示しています。

フィールド	説明
前回の検出	仮想アナライザが送信されたサンプルから最後にオブジェクトを検出した日時
失効日	仮想アナライザが [不審オブジェクト] タブからオブジェクトを削除する日時
リスクレベル	不審オブジェクトの種類によって、異なるリスク評価が表示されます。 • IP アドレスまたはドメイン: 通常表示されるリスクレベルは [高] または [中] です (次に示すリスクレベルの説明を参照してください)。これは、リスクが [高] および [中] の IP アドレスとドメインのみが不審オブジェクトと見なされることを意味します。 • URL: 表示されるリスクレベルは [高] または [中] です。 • SHA-1: 表示されるリスクレベルは常に [高] です。 リスクレベルの説明を次に示します。 • 高: 不正であることがわかっているか、リスクの高い接続に関与しています。 • 中: レピュテーションサービスにとって不明な IP アドレス、ドメイン、または URL です。
種類	IP アドレス、ドメイン、URL、または SHA-1
オブジェクト	ファイルの IP アドレス、ドメイン、URL、または SHA-1 ハッシュ値
最新の関連サンプル	オブジェクトが最後に見つかったサンプルの SHA-1 ハッシュ値。
関連する送信	オブジェクトが見つかったサンプルの合計数。 値をクリックすると、[送信] 画面が開き、SHA-1 ハッシュ値が検索条件として表示されます。

次の表は、[生成された不審オブジェクト] タブで実行できるタスクを示しています。

表 4-7. 不審オブジェクトのタスク

タスク	手順
エクスポート/すべてエクスポート	1 つ以上のオブジェクトを選択し、[エクスポート] をクリックすると、それらのオブジェクトが CSV ファイルに保存されます。 すべてのオブジェクトを CSV ファイルに保存するには、[すべてエクスポート] をクリックします。
除外設定に追加	無害と思われる 1 つ以上のオブジェクトを選択し、[除外設定に追加] をクリックします。オブジェクトが [除外] タブに移動します。
失効期限なし	常に不審オブジェクトとしてフラグを設定する 1 つ以上のオブジェクトを選択し、[失効期限なし] をクリックします。
すぐに失効	[不審オブジェクト] から削除する 1 つ以上のオブジェクトを選択し、[すぐに失効] をクリックします。その後同じオブジェクトが検出された場合、そのオブジェクトは再度 [不審オブジェクト] に追加されます。
データフィルタ	表内のエントリが多すぎる場合、次の作業を実行してエントリを限定します。 • [表示] ドロップダウンボックスからオブジェクトの種類を選択します。 • [検索列] ドロップダウンボックスから列名を選択した後、その横にある [検索キーワード] テキストボックスに文字を入力します。入力すると、入力した文字に一致するエントリが表示されます。Deep Discovery Analyzer は、表内の選択列のみを対象に一致を検索します。
レコードコントロールとページ区切りコントロール	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。

同期された不審オブジェクトリスト

次の表は、Deep Discovery Analyzer が Deep Discovery Director または Trend Micro Vision One から同期する不審オブジェクトを示しています。

フィールド	説明
オブジェクト	ファイルの IP アドレス、ドメイン、URL、または SHA-1 ハッシュ値
種類	IP アドレス、ドメイン、URL、または SHA-1
ソース	不審オブジェクトを追加した送信元 (Deep Discovery Director または Trend Micro Vision One)
リスクレベル	不審オブジェクトの種類によって、異なるリスク評価が表示されます。 • IP アドレスまたはドメイン: 通常表示されるリスクレベルは [高] または [中] です (次に示すリスクレベルの説明を参照してください)。これは、リスクが [高] および [中] の IP アドレスとドメインのみが不審オブジェクトと見なされることを意味します。 • URL: 表示されるリスクレベルは [高] または [中] です。 • SHA-1: 表示されるリスクレベルは常に [高] です。 リスクレベルの説明を次に示します。 • 高: 不正であることがわかっているか、リスクの高い接続に関与しています。 • 中: レピュテーションサービスにとって不明な IP アドレス、ドメイン、または URL です。
失効日	仮想アナライザが [不審オブジェクト] タブからオブジェクトを削除する日時
前回の同期	オブジェクトが前回 Deep Discovery Director または Trend Micro Vision One から同期された日時

次の表は、[同期された不審オブジェクト] タブで実行できるタスクを示しています。

タスク	手順
エクスポート/すべてエクスポート	1 つ以上のオブジェクトを選択し、[エクスポート] をクリックすると、それらのオブジェクトが CSV ファイルに保存されます。 すべてのオブジェクトを CSV ファイルに保存するには、[すべてエクスポート] をクリックします。

タスク	手順
データフィルタ	表内のエントリが多すぎる場合、次の作業を実行してエントリを限定します。 • [種類] ドロップダウンリストからオブジェクトの種類を選択します。 • [検索キーワード] テキストボックスにキーワードを入力します。
レコードコントロールとページ区切りコントロール	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。

ユーザ指定の不審オブジェクトリスト

[ユーザ指定の不審オブジェクト] タブでは、STIX (Structured Threat Information eXpression) 形式を使用して、不審オブジェクトを Deep Discovery Analyzer に手動で追加できます。

次の列は、[ユーザ指定の不審オブジェクト] タブに表示されるオブジェクトに関する情報を示しています。

表 4-8. ユーザ指定の不審オブジェクトの列

列の名前	情報
追加日	不審オブジェクトが追加された日時
種類	IP アドレス、ドメイン、URL、ファイルの SHA-1、またはファイルの SHA-256
オブジェクト	ファイルの IP アドレス、ドメイン、URL、SHA-1 または SHA-256 ハッシュ値 表示された値を変更するには、[編集] をクリックします。
アップデート元	不審オブジェクトを追加した送信元 (Deep Discovery Director、ローカル、または Trend Micro Vision One)

Deep Discovery Analyzer では、バージョン 1.2、1.1.1、および 1.0.1 の仕様でフォーマットされた STIX ファイルをインポートできます。1.0.1 の仕様は仮想アナライザの出力にのみ使用できます。

STIX ファイルには複数のオブジェクトを含めることができます。ただし、Deep Discovery Analyzer では次のサポートされる STIX インジケータのみをインポートします。

- インジケータ - ファイルハッシュウォッチリスト (SHA-1 および SHA-256)
- インジケータ - URL ウォッチリスト
- インジケータ - ドメインウォッチリスト
- インジケータ - IP ウォッチリスト

STIX インジケータでは次のプロパティ属性を使用できます。

- `@condition` は `Equals` である必要があります
- `@apply_condition` は `ANY` である必要があります

ユーザ指定の不審オブジェクトリストを管理する

手順

1. [仮想アナライザ] > [不審オブジェクト] の順に選択し、[ユーザ指定の不審オブジェクト] タブをクリックします。
2. 単一のオブジェクトを指定するには、次の手順を実行します。

   a. [追加] をクリックします。

      [オブジェクトの追加] 画面が表示されます。

   b. オブジェクトの種類を選択します。

      - IP アドレス: IP アドレスまたは IP アドレスの範囲 (ハイフン区切り) を入力します

- ドメイン: ドメイン名を入力します

  注意

  ワイルドカードは、ドメイン名のプレフィックスでのみ使用でき、「.」記号で接続する必要があります。ドメインごとに 1 つのワイルドカードのみを使用します。たとえば、「*.com」は「example.com」または「example1.com」に一致します。

- URL: URL を入力します

  注意

  Deep Discovery Analyzer では、HTTP と HTTPS の両方がサポートされます。

  ワイルドカードは、ドメイン名のプレフィックスでのみ使用できます。URL のドメイン部分で使用されているワイルドカードは、「.」記号で接続する必要があります。URL ごとに 1 つのワイルドカードのみを使用します。たとえば、「http://*.com」は「example.com」または「example1.com」に一致します。

  ワイルドカードは、URL の任意の URI 部分に一致します。たとえば、「http://example.com/*abc」は「http://example.com/test.abc」に一致します。

- SHA-1: ファイルの SHA-1 ハッシュ値を入力します
- SHA-256: ファイルの SHA-256 ハッシュ値を入力します

c. [追加] をクリックします。

注意

[ユーザ指定の不審オブジェクト] リストには最大 25,000 件のオブジェクトを追加できます。

3. STIX ファイルを使用して複数のオブジェクトを追加するには、次の手順を実行します。

   a. [STIX からリストをインポート] をクリックします。

   b. 有効な STIX ファイルを指定します。

c. [インポート] をクリックします。

注意

Deep Discovery Analyzer では、バージョン 1.2、1.1.1、および 1.0.1 の仕様でフォーマットされた STIX ファイルをインポートできます。1.0.1 の仕様は仮想アナライザの出力にのみ使用できます。

STIX ファイルには複数のオブジェクトを含めることができます。ただし、Deep Discovery Analyzer では次のサポートされる STIX インジケータのみをインポートします。

- インジケータ - ファイルハッシュウォッチリスト (SHA-1 および SHA-256)
- インジケータ - URL ウォッチリスト
- インジケータ - ドメインウォッチリスト
- インジケータ - IP ウォッチリスト

STIX インジケータでは次のプロパティ属性を使用できます。

- `@condition` は `Equals` である必要があります
- `@apply_condition` は `ANY` である必要があります

4. リスト内のオブジェクトを削除するには、次の手順を実行します。
   - 1 つ以上のオブジェクトを選択し、[削除] をクリックすると、選択したオブジェクトが削除されます。
   - リストのすべてのオブジェクトを削除するには、[すべて削除] をクリックします。

除外

例外リスト内のオブジェクトは安全であると自動的に見なされ、不審オブジェクトリストには追加されません。信頼できるオブジェクトを手動で追加するか、[仮想アナライザ] > [不審オブジェクト] 画面に移動し、無害と思われる不審オブジェクトを選択します。

次の表では、例外リスト内のオブジェクトについて説明します。

表 4-9. [除外] の列

列の名前	情報
追加日	仮想アナライザが [除外] タブにオブジェクトを追加した日時
種類	オブジェクトの種類 ([IP アドレス]、[ドメイン]、[URL]、[SHA-1]、または [SHA-256])
オブジェクト	ファイルの IP アドレス、ドメイン、URL、SHA-1 または SHA-256 ハッシュ値
送信元	除外設定を追加した送信元 (Trend Micro Vision One、Apex Central、Deep Discovery Director、またはローカル)
備考	オブジェクトに関する注意事項。 注意事項を編集するには、リンクをクリックします。

除外のタスク

次の表は、[除外] タブのすべてのタスクのリストです。

表 4-10. 除外のタスク

タスク	手順
追加	1. オブジェクトを追加するには、[追加] をクリックします。 [除外設定の追加] 画面が表示されます。 2. [IP アドレス]、[ドメイン]、[URL]、[SHA-1]、または [SHA-256] の除外基準を指定します。 • IP アドレスの場合は、タイプに [IP アドレス] を選択して IP アドレスまたは IP アドレスの範囲 (ハイフン区切り) を入力します。 • ドメインの場合は、タイプに [ドメイン] を選択してドメインを入力します。

タスク	手順
	注意 ワイルドカードは、ドメイン名のプレフィックスでのみ使用できます。ワイルドカードがプレフィックスで使用されている場合は、「. 」で接続する必要があります。1 つのドメインで 1 つのワイルドカードのみを使用できます。たとえば、「*.com」は「example.com」または「example1.com」に一致します。 • URL の場合は、タイプに [URL] を選択して URL を入力します。 注意 • ワイルドカードは、ドメイン名のプレフィックスでのみ使用できます。ワイルドカードが URL のドメイン部分で使用されている場合は、「. 」で接続する必要があります。1 つの URL で 1 つのワイルドカードのみを使用できます。たとえば、「http://*.com」は「example.com」または「example1.com」に一致します。 • 未割り当てのワイルドカードが URL の URI 部分で使用されている場合は、すべての部分に一致します。たとえば、「http://example.com/*abc」は「http://example.com/test.abc」に一致します。 • Deep Discovery Analyzer では HTTP と HTTPS の両方を使用できます。 • ファイルの場合は、タイプに [SHA-1] または [SHA-256] を選択してハッシュ値を入力します。 • 備考: オブジェクトに関する注意事項を入力します。 • さらに追加: さらにオブジェクトを追加するには、このボタンをクリックします。オブジェクトの種類を選択し、次のフィールドにオブジェクトを入力した後、注意事項を入力し、[リストに追加] をクリックします。 3. (オプション) オブジェクトに関する注意事項を入力します。

タスク	手順
	4. さらにオブジェクトを追加するには、[さらに追加] をクリックします。 a. [IP アドレス]、[ドメイン]、[URL]、[SHA-1]、または [SHA-256] の除外基準を指定します。 b. [リストに追加] をクリックします。 5. 追加するすべてのオブジェクトを定義したら、[追加] をクリックします。  注意 Deep Discovery Analyzer では最大 25,000 件の除外オブジェクトを追加できます。
インポート	正しく書式設定された CSV ファイルからオブジェクトを追加するには、[インポート] をクリックします。表示された新しいウィンドウで、次の作業を実行します。 • 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。  重要 • インポートを実行すると現在の除外リストが上書きされます。ただし、統合製品から取得したオブジェクトは変更されません。現在の除外リストのコピーを保存するには、インポート処理を開始する前にリストをエクスポートします。 • 1 つの CSV ファイルで最大 25,000 件の除外オブジェクトをインポートできます。
削除/すべて削除	削除する 1 つ以上のオブジェクトを選択した後、[削除] をクリックします。

タスク	手順
	すべてのオブジェクトを削除するには、[すべて削除] をクリックします。
エクスポート/すべてエクスポート	1 つ以上のオブジェクトを選択し、[エクスポート] をクリックすると、それらのオブジェクトが CSV ファイルに保存されます。 すべてのオブジェクトを CSV ファイルに保存するには、[すべてエクスポート] をクリックします。
データフィルタ	表内のエントリが多すぎる場合、次の作業を実行してエントリを限定します。 ・ [表示] ドロップダウンボックスからオブジェクトの種類を選択します。 ・ [検索列] ドロップダウンボックスから列名を選択した後、その横にある [検索キーワード] テキストボックスに文字を入力します。入力すると、入力した文字に一致するエントリが表示されます。Deep Discovery Analyzer は、表内の選択列のみを対象に一致を検索します。
レコードコントロールとページ区切りコントロール	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。

サンドボックス管理

[サンドボックス管理] 画面には、次のものが含まれています。

注意

仮想アナライザにイメージが含まれていない場合、[サンドボックス管理] をクリックすると [イメージ] タブが表示されます。

[ステータス] タブ

[ステータス] タブには次の情報が表示されます。

- 仮想アナライザ全体のステータス。キュー内にあるサンプルおよび現在処理中のサンプルの数も含まれます。

  仮想アナライザのステータスの一覧は、次の表のとおりです。

  表 4-11. 仮想アナライザのステータス

ステータス	説明
初期化されていません	仮想アナライザが初期化されていません。
イメージがありません	イメージが仮想アナライザにインポートされていません。
無効	仮想アナライザは一時的に使用できません。
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。
イメージをインポートしています...	1 つ以上のイメージをインポートしています。
イメージを削除しています...	1 つ以上のイメージを削除しています。
設定しています...	サンドボックスを設定しています。
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。
実行中	サンドボックスが動作中です
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。
修復不能なエラー	エラーから回復できません。詳細については、トレンドマイクロ サポートセンターにお問い合わせください。
Deep Discovery Director からイメージを配信しています...	Deep Discovery Director からイメージを配信しています。

- インポートされたイメージのステータス

表 4-12. イメージ情報

ステータス	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。

[イメージ] タブ

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。

[イメージ] 画面で次の情報を確認できます。

- イメージに設定されたインスタンス数
- 使用中のインスタンス数

次の表は、[イメージ] 画面で実行できるタスクを示しています。

タスク	説明
イメージのインポート	[インポート] をクリックして、新しい仮想アナライザイメージをアップロードします。 詳細については、104 ページの「イメージをインポートする」を参照してください。 注意 Linux イメージでは、CentOS 7.8 (64 ビット) のみがサポートされます。
イメージのエクスポート	イメージを選択して、[エクスポート] をクリックします。
イメージ名またはサンドボックスのインスタンス数の変更	イメージを選択して、[変更] をクリックします。 詳細については、107 ページの「サンドボックスインスタンスを変更する」を参照してください。
プラットフォーム別のエントリの表示	[プラットフォーム] ドロップダウンリストからオプションを選択します。

イメージをインポートする

最大 4 つのイメージをアップロードできます (1 つの Linux イメージと 3 つの Windows イメージ)。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。

仮想アナライザは最大 30GB の OVA ファイルをサポートします。

重要

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。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[イメージ] タブをクリックします。

   [イメージ] 画面が表示されます。

2. [インポート] をクリックします。

   [イメージのインポート] 画面が表示されます。

3. [プラットフォーム] オプションを選択します。

4. イメージソースを選択して、適切な設定を行います。

   a. 最大 50 文字でイメージ名を入力します。このイメージ名は後から変更できません。

   b. イメージに割り当てるインスタンス数を選択します。

   c. OVA ファイルの URL またはネットワーク共有パスを入力します。

   d. (オプション) [プロキシサーバを使用して接続する] を選択します。

   e. (オプション) 認証が必要な場合は、ログオンアカウント情報を入力します。

5. [インポート] をクリックします。

   インポート処理を開始する前に、仮想アナライザで OVA ファイルが検証されます。

注意

- [HTTP/HTTPS または FTP サーバ] を選択すると、Deep Discovery Analyzer でイメージがダウンロードされてから、仮想アナライザにインポートされます。この処理は、ダウンロードが完了する前のみキャンセルできます。
- Deep Discovery Analyzer では、インポート元として HTTP/1.0 以降に準拠した HTTP サーバへの接続がサポートされます。

トレンドマイクロ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する

仮想アナライザは 1～30GB までの OVA ファイルをサポートします。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[イメージ] タブをクリックします。
2. [インポート] をクリックします。
3. [プラットフォーム] オプションを選択します。
4. [送信元] で [イメージアップロードツール] を選択します。
5. [ダウンロード] をクリックし、イメージアップロードツールをダウンロードします。
6. ファイル `VirtualAnalyzerImageImportTool.exe` を開きます。
7. Deep Discovery Analyzer の IP アドレスを入力します。

   イメージのアップロード後、Deep Discovery Analyzer がただちにインスタンスを配信します。インスタンスの配信が完了するまで待ちます。

イメージのアップロードプロセスは、次の理由によって、停止するか失敗と見なされることがあります。

- 接続が確立されていないか、製品がビジー状態の可能性がある。
- アプライアンスへの接続が中断された
- 接続がタイムアウトした
- メモリの割り当てが失敗した
- Windows のソケット初期化が失敗した
- イメージファイルが壊れている
- イメージのアップロードが完了しなかった

- イメージのアップロードがキャンセルされた

サンドボックスインスタンスを変更する

最大 4 つのイメージをアップロードできます (1 つの Linux イメージと 3 つの Windows イメージ)。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。

重要

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、仮想アナライザはすべての分析を停止して、すべてのサンプルをキューに保持します。イメージが追加された場合は、すべてのインスタンスが自動的に再配布されます。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[イメージ] タブをクリックします。

   [イメージ] 画面が表示されます。

2. [変更] をクリックします。

   [サンドボックスインスタンスの変更] 画面が表示されます。

3. (オプション) イメージの名前を変更します。

4. イメージに割り当てられたインスタンスを変更します。

5. [設定] をクリックします。

   次の確認メッセージが表示されます。

6. [OK] をクリックします。

   仮想アナライザでサンドボックスインスタンスが設定されます。処理が完了するまで、この画面から移動せずに待機します。

注意

設定が失敗すると、以前の設定にロールバックされてエラーメッセージが表示されます。

[YARA ルール] タブ

仮想アナライザでは YARA ルールを使用して不正プログラムを特定します。YARA ルールは、環境に固有の標的型攻撃およびセキュリティ脅威を特定するためのカスタマイズ可能な不正プログラム検出パターンです。Deep Discovery Analyzer では、YARA ルールファイルの数にかかわらず最大 5,000 の YARA ルールがサポートされます。

次の列は、YARA ルールファイルに関する情報を示しています。

表 4-13. [YARA ルール] の列

列の名前	情報
ファイル名	YARA ルールファイルの名前
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
追加日	YARA ルールファイルが追加された日時

次の表は、[YARA ルール] タブのすべてのタスクのリストです。

表 4-14. [YARA ルール] のタスク

タスク	手順
追加	YARA ルールファイルと分析対象のファイルタイプを参照して選択します。詳細については、111 ページの「YARA ルールファイルを管理する」を参照してください。
削除	削除する YARA ルールファイルを 1 つ以上選択して、[削除] をクリックします。

タスク	手順
エクスポート	1 つの YARA ルールファイルを選択し、[エクスポート] をクリックして YARA ルールファイルのコピーをダウンロードします。
編集	編集する YARA ルールファイルの [ファイル名] をクリックします。 詳細については、111 ページの「YARA ルールファイルを管理する」を参照してください。
レコードコントロールとページ区切りコントロール	画面の最下部にあるパネルに YARA ルールファイルの合計数が表示されます。すべてのサンプル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サンプルを表示します。

YARA ルールファイルを作成する

Deep Discovery Analyzer では、バージョン 4.1.0 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/v4.1.0/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 4-15. 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 Analyzer 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 ルールファイルを管理する

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[YARA ルール] タブに移動します。
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 YARA ルールを追加します。

     追加する前に 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方法の詳細については、109 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。
   - 既存の YARA ルールファイルの [ファイル名] をクリックして、その設定を編集します。
3. [ファイルの選択] をクリックし、追加する YARA ルールファイルを参照して選択します。
4. [分析対象ファイル] で、次のいずれかを実行します。
   - [ファイルタイプを指定してください] を選択し、仮想アナライザがこの YARA ルールファイルに関連付けるファイルタイプを選択して追加します。

     カスタムファイルタイプを追加するには、[新しいファイルタイプ] フィールドにファイル拡張子を入力して、<Enter> キーを押します。リストの [ユーザ指定のファイルタイプ] セクションの下に、新しいファイルタイプが表示されます。

     重要

     新しいファイルタイプを Deep Discovery Analyzer に永続的に保存するには、[保存] をクリックします。
   - この YARA ルールファイルの対象としてすべてのファイルタイプを関連付ける場合は、[すべてのファイルタイプ] を選択します。

注意

すべてのファイルタイプを分析すると、意図しない検出が行われ、システムのパフォーマンスが低下することがあります。YARA ルールファイルの対象となる特定のファイルタイプの分析を行うことをお勧めします。

5. [保存] をクリックします。

   YARA ルールファイルの追加後、次の操作を実行できます。

   - 選択した YARA ルールファイルのコピーをダウンロードするには、[エクスポート] をクリックします。
   - 1 つ以上の選択した YARA ルールファイルを削除するには、[削除] をクリックします。

[ファイルパスワード] タブ

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 Analyzer 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 Analyzer 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 Analyzer 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`
- `egg`
- `rar`

- zip

Deep Discovery Analyzer 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
- odt
- ods
- pdf
- ppt
- pptx
- xls
- xlsx

リストされたいずれのパスワードを使用してもファイルを抽出できない場合は、サポートされていないファイルタイプというエラーが表示され、アーカイブファイルがキューから削除されます。

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 Analyzer 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 Analyzer 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
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、114 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。
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。
すべてのパスワードのエクスポート	[すべてエクスポート] 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。

ファイルのパスワードを追加する

Deep Discovery Analyzer は最大 100 個のパスワードをサポートします。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[ファイルパスワード] タブをクリックします。
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 Analyzer では、最大 100 件のパスワードを追加できます。

注意

ファイルからパスワードをインポートすると、Deep Discovery Analyzer の既存のパスワードが置き換えられます。パスワードをインポートする前に、エクスポート機能を使用して既存のパスワードをバックアップすることをお勧めします。

手順

1. [サンドボックス管理] > [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 Analyzer 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。

[送信設定] タブ

[仮想アナライザ] > [サンドボックス管理] の [送信設定] タブを使用して、仮想アナライザで処理するファイルタイプを表示または指定します。

トレンドマイクロでは、拡張子ではなく実際のファイルタイプによってファイルを識別します。サンプルファイルの拡張子は参照用に提供されます。

注意

仮想アナライザ設定パターンファイルのアップデートには、新しいファイルタイプサポートの追加が含まれることもあります。アップデート後、新しいファイルタイプは [分析対象] リストに配置されます。

表 4-16. 仮想アナライザのファイルタイプ: Windows

表示されるファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
bat	Microsoft Windows バッチファイル	.bat
cmd	Microsoft Windows コマンドスクリプトファイル	.cmd
cell	Hancom Hancell 表計算ファイル	.cell
chm	コンパイル済み HTML (CHM) ヘルプファイル	.chm
csv	カンマ区切り値 (CSV) ファイル	.csv
class	Java クラスファイル	.class .cla
com	Microsoft Windows 実行可能ファイル	.com
dll	AMD 64 ビット DLL ファイル Microsoft Windows 16 ビット DLL ファイル Microsoft Windows 32 ビット DLL ファイル	.dll .ocx .drv
doc	Microsoft Word 1.0 ドキュメント Microsoft Word 2.0 ドキュメント	.doc .dot

表示されるファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
docx	Microsoft Office Word ドキュメント (Word 2007 以降) マクロが有効な Microsoft Office Word ドキュメント (Word 2007 以降)	.docx .dotx .docm .dotm
elf	Executable and Linkable Format (ELF) ファイル **注意** CentOS 7.8 (64 ビット) イメージの仮想アナライザ分析でのみ使用。	.elf

表示されるファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
exe	AMD 64 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 DIET DOS EXE ファイル GNU UPX 圧縮 EXE ファイル IBM OS/2 EXE ファイル LZEXE DOS 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 Microsoft Windows 16 ビット EXE ファイル Microsoft Windows 32 ビット EXE ファイル MIPS EXE ファイル MSIL ポータブル実行可能ファイル 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 WWPACK 圧縮実行可能ファイル	.cpl .exe .sys .crt .scr
gul	JungUm Global ドキュメント	.gul
hta	HTML アプリケーションファイル	.hta

表示されるファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
html	Hypertext Markup Language (HTML) ファイル	.htm .html
hwp	Hancom Hangul Word Processor (HWP) ドキュメント	.hwp
hwpx	Hancom Hangul Word Processor (2014 以降) (HWPX) ドキュメント	.hwpx
iqy	Microsoft Excel Web クエリファイル	.iqy
jar	Java アプレット Java アプリケーション 注意 仮想アナライザは Java ライブラリをサポートしていません。	.jar
js	JavaScript ファイル	.js
jse	JavaScript エンコードスクリプトファイル	.jse
jtd	JustSystems 一太郎ドキュメント	.jtd
lnk	Microsoft Windows Shell Binary Link ショートカット Microsoft Windows 95/NT ショートカット	.lnk
mht mhtml	Web ページのアーカイブファイル	.mht .mhtml
mov	Apple QuickTime メディア	.mov
odt	OpenDocument テキスト	.odt
odp	OpenDocument プレゼンテーション	.odp
ods	OpenDocument スプレッドシート	.ods
pdf	Adobe Portable Document Format (PDF)	.pdf

表示されるファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
ppt	Microsoft PowerPoint プレゼンテーション	.ppt .pps
pptx	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 PowerPoint プレゼンテーション (PowerPoint 2007 以降)	.pptx .ppsx
ps1	Microsoft Windows PowerShell スクリプトファイル	.ps1
pub	Microsoft Office Publisher ファイル (Publisher 2016)	.pub
rtf	Microsoft リッチテキストフォーマット (RTF) ドキュメント	.rtf
shell	シェルスクリプトファイル **注意** CentOS 7.8 (64 ビット) イメージの仮想アナライザ分析でのみ使用。	.sh
slk	Microsoft シンボリックリンク形式	.slk
svg	スケーラブルベクターグラフィックスファイル	.svg
swf	Adobe Shockwave Flash ファイル	.swf
vbe	Visual Basic エンコードスクリプトファイル	.vbe
vbs	Visual Basic スクリプトファイル	.vbs
wsf	Microsoft Windows スクリプトファイル	.wsf
xls	Microsoft Excel スプレッドシート	.xls .xla .xlt .xlm

表示されるファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
xlsx	Microsoft Office Excel スプレッドシート (Excel 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)	.xlsx .xlsb .xltx .xlsm .xlam .xltm
xml	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 Microsoft PowerPoint 2003 XML プレゼンテーション	.xml
xht xhtml	Extensible Hypertext Markup Language (XHTML)	.xht .xhtml
url	インターネットショートカットファイル	.url

注意

次のファイルについて、拡張子とファイルの種類が一致しない場合、仮想アナライザは分析を実行しません。

- bat
- cmd
- csv
- hta
- htm
- html
- iqy
- js
- jse
- mht
- mhtml
- ps1
- slk
- svg
- url
- vbe
- vbs
- wsf
- xht
- xhtml
- xls

表 4-17. 仮想アナライザのファイルタイプ: Linux

表示されるファイルタイプ	完全なファイルタイプ	ファイル拡張子の例
elf	ELF 実行可能ファイル	該当なし
sh	シェルスクリプト	.sh

仮想アナライザは、パスワード保護されていない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。

注意

仮想アナライザで分析できるパスワード保護されたアーカイブファイルのリストについては、112 ページの「[ファイルパスワード] タブ」を参照してください。

表 4-18. 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
ARK	Google Android アプリケーションパッケージ (APK)	.apk
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

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
CRX	Chrome 拡張形式 (CRX)	.crx
EGG	ALZip アーカイブ	.egg
GZIP	GNU ZIP アーカイブ	.gzip .gz
ISO	ISO イメージ	.iso
LHA	LHARC 圧縮アーカイブ	.lha .lharc
LZW	Lempel-Ziv-Welch (LZW) Compressed Amiga アーカイブ	.lzh
MACBIN	Apple MacBinary ファイル	.bin.macbin
MIME	Multipurpose Internet Mail Extensions (MIME) Base64 ファイル	.eml .email
MSG	Microsoft Outlook アイテム	.msg
MSI	Microsoft のインストーラパッケージ	.msi
MSCOMP	Microsoft 圧縮ファイル	.arc
RAR	Roshal Archive (RAR) アーカイブ	.rar
SIS	Symbian インストールファイル	.sis
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

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
UUCODE	Uuencode ファイル	.uue
WIM	Microsoft Windows イメージ (WIM)	.wim
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 Analyzer が自動的に 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。

注意

Deep Discovery Analyzer では、JAR および CLASS ファイルは、macOS 向けサンドボックスと内部仮想アナライザの両方に送信されて分析されます。

表 4-19. 仮想アナライザのファイルタイプ: Mac

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
JAR	Java アプレット Java アプリケーション **注意** 仮想アナライザは Java ライブラリをサポートしていません。	.jar
CLASS	Java クラスファイル	.class .cla
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

[送信設定] タブのタスク

手順

1. ファイルタイプを [分析対象] リストに移動するには、次の手順を実行します。
   a. [分析対象外] リスト内で 1 つ以上のファイルタイプを選択します。
   b. [>] をクリックします。
   c. [保存] をクリックします。
2. ファイルタイプを [分析対象外] リストに移動するには、次の手順を実行します。
   a. [分析対象] リスト内で 1 つ以上のファイルタイプを選択します。
   b. [<] をクリックします。
   c. [保存] をクリックします。
3. 初期設定に戻すには、[初期設定に戻す] をクリックします。

[ネットワーク接続] タブ

[ネットワーク接続] タブを使用して、サンドボックスインスタンスから外部接続先への接続方法を指定します。

外部接続は初期設定では無効です。外部接続は、管理ネットワークから隔離された環境を使用して有効にすることをお勧めします。このような環境には、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を使用することもできます。

外部接続を有効にすると、サンプル処理中に、インターネットやリモートホストを巻き込む不正な活動が実際に発生してしまいますのでご注意ください。

外部接続を有効にする

仮想アナライザが設定されると、サンプル分析が一時停止して設定が無効になります。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[ネットワーク接続] タブをクリックします。

   [ネットワーク接続] 画面が表示されます。

2. [外部接続の有効化] を選択します。

   設定パネルが表示されます。

3. サンドボックスインスタンスで使用する接続の種類を選択します。

   - カスタム: 任意のユーザ定義ネットワークです。

     重要
     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。

   - 管理ネットワーク: 初期設定の社内イントラネットです。

     警告!
     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。

4. [カスタム] を選択した場合は、次を設定します。

   - ネットワークアダプタ: 接続された状態のアダプタを選択します。
   - IP アドレス: IPv4 のアドレスを入力します。
   - サブネットマスク
   - ゲートウェイ

- DNS

5. サンドボックスでネットワーク接続にプロキシサーバが必要な場合は、[専用のプロキシサーバを使用する] を選択して次を指定します。
   - サーバアドレス
   - ポート番号
   - ユーザ名: このオプションは、[プロキシサーバへの接続に認証を使用] が有効な場合のみ使用できます。
   - パスワード: このオプションは、[プロキシサーバへの接続に認証を使用] が有効な場合のみ使用できます。
6. [保存] をクリックします。

インターネット接続をテストする

外部接続を有効にして設定を保存したら、インターネット接続を確認します。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[ネットワーク接続] タブをクリックします。
2. [インターネット接続のテスト] をクリックします。

> **注意**
> 外部接続が有効でないか設定が保存されていない場合、[インターネット接続のテスト] は無効になります。

[検索設定] タブ

[仮想アナライザ] > [サンドボックス管理] の [検索設定] タブでは、仮想アナライザが Trend Micro Vision One または Deep Discovery Director から同期した不審オブジェクトを使用してサンプルを分析するように設定できます。

注意

この検索設定を有効にするには、Deep Discovery Analyzer が Trend Micro Vision One または Deep Discovery Director から不審オブジェクトを同期するように設定する必要もあります。

詳細については、191 ページの「Trend Micro Vision One」または 195 ページの「Deep Discovery Director に登録する」を参照してください。

[インタラクティブモード設定] タブ

VNC アクセスの詳細な設定を行うことができます。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[インタラクティブモード設定] タブをクリックします。
2. パスワードは 8 文字以上で、アルファベットの大文字と小文字、数字、および特殊文字を組み合わせて入力してください。

   パスワードを設定しない場合、このフィールドは空のままにします。

   注意

   指定したパスワードを忘れた場合は、リセットする必要があります。
3. ポート範囲を指定します。

   注意

   開始ポート番号は 5900～6100 の間で指定する必要があります。
4. [保存] をクリックします。

[スマートフィードバック] タブ

Deep Discovery Analyzer 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、Trend Micro Smart

Protection Network に脅威情報を送信します。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。

- 製品の ID とバージョン
- 詐欺サイトまたは脅威の発信源である可能性のある 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、および仮想アナライザのログ)
- 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. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[スマートフィードバック] タブをクリックします。
2. スマートフィードバックを設定します。
   a. トレンドマイクロに匿名の脅威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。
   b. トレンドマイクロにリスク高のファイルを送信してさらに調査するには、[不審なファイルをトレンドマイクロに送信します] を選択します。

[macOS 向けサンドボックス] タブ

[macOS 向けサンドボックス] を有効にすると、解析のために、macOS の潜在的な脅威を Deep Discovery Analyzer からトレンドマイクロの macOS 向けサンドボックスサービスに送信できます。

macOS 向けサンドボックスを有効にする

macOS 向けサンドボックスを有効にする前に、Deep Discovery Analyzer からインターネットに接続できることを確認します。

注意

macOS 向けサンドボックス設定は、クラスタ環境ではプライマリアプライアンスから同期されません。各セカンダリアプライアンスの管理コンソール上で macOS 向けサンドボックス設定を有効にしてください。

重要

Deep Discovery Analyzer のライセンスの有効期限が切れると、macOS 向けサンドボックス設定は自動的に無効になります。

手順

1. [仮想アナライザ] > [サンドボックス管理] の順に選択し、[macOS 向けサンドボックス] タブをクリックします。
2. [macOS の潜在的な脅威を Sandbox as a Service に送信して分析] を選択します。
3. [保存] をクリックします。

[送信元] 画面

[仮想アナライザ] > [送信元] にある [送信元] 画面を使用して、分析のために Deep Discovery Analyzer にオブジェクトを送信するすべての送信元間で、仮

想アナライザのリソースの割り当てを調整します。仮想アナライザは、より高い重みが設定された送信元による送信の処理により多くのリソースを使用します。

次の列は、送信元、平均処理時間、送信の合計数、および送信元に割り当てられたリソース合計に関する情報を示します。重みの調整や送信元の削除に関する列もあります。

表 4-20. [送信元] 画面の列

列の名前	情報/処理
送信元	オブジェクトを送信するトレンドマイクロ製品の名前
ホスト名	• オブジェクトを送信した統合セキュリティ製品のホスト名 • メールまたは手動による送信の場合はデータなし (ダッシュで示されます) • ICAP クライアントの IP アドレス • ネットワーク共有の名前
前回の送信	仮想アナライザが最後に送信を受信した日付と時刻
平均処理時間	仮想アナライザが送信されたオブジェクトを処理するためにかかる平均時間
送信 (%)	トレンドマイクロ製品によって送信されたオブジェクトの数
重み	トレンドマイクロ製品の重みの設定。 リソースの割り当てを再計算するための値を 1〜100 の数値で指定します。
リソース合計に対する割合 (%)	トレンドマイクロ製品に割り当てられた仮想アナライザのリソース合計に対する割合
タイムアウト	トレンドマイクロ製品に割り当てられたタイムアウト期間。 タイムアウト期間は 0〜10000 の分単位で指定してください。値 0 はタイムアウトが無効であることを意味します。過去 24 時間にタイムアウト期間の影響を受けたサンプル数が [件数] 列にまとめられます。

列の名前	情報/処理
処理	Deep Discovery Analyzer からトレンドマイクロ製品を削除します。 削除した製品から検索や分析またはクエリ分析結果のために新しいオブジェクトを送信することはできませんが、キュー内の既存のオブジェクトは処理され、分析結果が保存されます。 **注意** 製品を再統合するには、33 ページの「トレンドマイクロ製品およびサービスとの統合」を参照してください。

ネットワーク共有

Deep Discovery Analyzer は、ネットワーク共有の検索機能を使用してネットワーク共有上のファイルを検索し、不正な可能性があるファイルを検出して、ネットワーク環境への拡散を防止します。

次の表は、[ネットワーク共有] 画面の詳細を示しています。

フィールド	説明
共有名	ネットワーク共有の名前
説明	ネットワーク共有に関する追加情報
プロトコル	ネットワーク共有のアクセスプロトコル (CIFS または NFS)
サーバアドレス	ネットワーク共有のサーバの IP アドレスまたは完全修飾ドメイン名 (FQDN)
パス	ネットワーク共有のファイルパス
予約検索	ネットワーク共有の予約検索設定

フィールド	説明
検索結果	前回のネットワーク共有の検索結果。数字をクリックすると詳細な検索結果が表示されます。 注意 検索が進行中の場合、検索結果は 10 秒ごとに自動的に更新されます。
検索ステータス	前回のネットワーク共有の検索ステータス 検索が進行中の場合は、[停止] をクリックすると検索タスクを終了できます。
手動検索	[検索] をクリックして手動検索を開始します。
ネットワークステータス	ネットワーク共有の接続ステータス ([アクセス可能] または [アクセス不可])
ステータス	ネットワーク共有の検索設定の有効/無効を切り替えます。 注意 ネットワーク共有の検索設定を無効にすると、手動検索機能と予約検索設定が無効になります。

次の表は、[ネットワーク共有] 画面で実行できるタスクを示しています。

表 4-21. ネットワーク共有: タスク

タスク	説明
ネットワーク共有の追加	[追加] をクリックしてネットワーク共有を追加します。 詳細については、136 ページの「ネットワーク共有を設定する」を参照してください。 ヒント ネットワーク共有を追加したら、[送信元] 画面にアクセスして、関連するサンプルの送信を確認したり、仮想アナライザのリソース割り当ての重みの値 (初期設定は 4) を調整したりできます。

タスク	説明
ネットワーク共有への接続のテスト	ネットワーク共有名をクリックし、[接続テスト] をクリックします。[ネットワーク共有] 画面の [ネットワークステータス] フィールドでテスト結果を確認します。
ネットワーク共有の編集	ネットワーク共有名をクリックして設定を編集します。 詳細については、136 ページの「ネットワーク共有を設定する」を参照してください。 注意 検索が進行中のネットワーク共有の設定を編集することはできません。
ネットワーク共有の削除	エントリを 1 つ以上選択して [削除] をクリックし、[OK] をクリックして確認します。
検索の停止	検索の進行中に、[検索ステータス] フィールドの [停止] をクリックします。
手動検索の開始	[手動検索] フィールドの [検索] をクリックして、検索を開始します。
ネットワーク共有設定の有効化/無効化	[ステータス] フィールドの切り替えスイッチをクリックして、ネットワーク共有設定を有効または無効にします。
検索結果の表示	[検索結果] フィールドで、次の操作を実行します。 • 検索済み: 数字をクリックして、成功した検索についての情報を [送信] 画面に表示します。 • 失敗: 数字をクリックして、[失敗した検索] 画面に情報を表示します。 詳細については、140 ページの「失敗した検索を表示する」を参照してください。

ネットワーク共有を設定する

手順

1. [仮想アナライザ] > [ネットワーク共有] 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ネットワーク共有を設定します。
   - ネットワーク共有名をクリックして設定を変更します。
3. ネットワーク共有の一般設定を行います。

フィールド	説明
ステータス	ネットワーク共有設定を有効または無効にするオプションを選択します。
共有名	ネットワーク共有のわかりやすい名前を入力します。
説明	ネットワーク共有の追加情報を入力します。
プロトコル	ドロップダウンリストからアクセスプロトコルを選択します。
サーバアドレス	ネットワーク共有サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。 **注意** Deep Discovery Analyzer がサンプル分析を実行してサーバアドレスを正しく表示できるように、共有サーバが UTF-8 エンコーディングを使用していることを確認してください。
パス	ネットワーク共有パスを入力します (例: /Users/Shares/Website)。
ユーザ名	ネットワーク共有にアクセスするユーザ名を入力します。 ドメインユーザについては、ユーザ名を `domain_name\user_name` の形式で入力します。

フィールド	説明
パスワード	ネットワーク共有にアクセスするパスワードを入力します。

4. Deep Discovery Analyzer が検索用にファイルをフィルタするために使用するファイル名パターンを設定します。次の操作を実行します。

   a. 対象リストまたは除外リストに基づいてファイルを一致させることを選択します。

   注意

   ファイル名の一致に両方のリストを使用することを選択した場合は、除外リストが優先されます。

   b. 選択したリストに対して 1 つ以上のファイル名パターンを入力します。

   注意

   - ファイル名パターンでは大文字小文字は区別されません。
   - Deep Discovery Analyzer では、ファイル名パターンに次のワイルドカードがサポートされます。
     - `*`: すべてに一致
     - `?`: 任意の 1 文字に一致
     - `[seq]`: `seq` 内の任意の文字に一致
     - `[!seq]`: `seq` に含まれない任意の文字に一致
   - リストには最大 10 個のファイル名パターンを設定できます。
   - 同じファイル名パターンを対象リストと除外リストの両方に設定することはできません。
   - Deep Discovery Analyzer により、選択したファイル名パターンリストに一致するファイルが検索されます。

5. 検索処理を指定します。

処理	説明
検索後にファイルを移動しない	検索後にファイルを元のフォルダに残すには、このオプションを選択します。これが初期設定です。 注意 output_ddan 出力フォルダを自動的に作成するには、[分析レポートを出力フォルダにコピー] オプションを選択します。
ファイルを移動する	検索後に指定した出力フォルダにファイルを移動するには、このオプションを選択します。 ネットワーク共有と同じアクセス認証情報を使用して出力パスにアクセスするには [ネットワーク共有の認証情報を継承する] を選択します。そうでない場合は、出力パスのアクセス認証情報を指定します。 注意 • 出力パスとネットワーク共有パスを同じにすることはできません。 • 指定したフォルダで読み取り書き込み権限が設定されていることを確認します。 • 出力パス内のファイルは検索から除外されます。
検索後に選択したリスクレベルのファイルを削除する	検索後に選択したリスクレベルのファイルを削除するには、このオプションを選択します。 注意 output_ddan 出力フォルダを自動的に作成するには、[分析レポートを出力フォルダにコピー] オプションを選択します。

Deep Discovery Analyzer では、生成される次のファイルが、検索から除外される出力フォルダに保存されます。

- レポートファイル (ファイル命名規則は `id_filename_report.zip`)

- 検索したファイルの元のファイルパス情報を含むレポートメタデータファイル (ファイル命名規則は `id_filename.meta`)

6. 検索方法を選択します。

注意

検索後にファイルを移動するオプションを選択した場合、この設定は適用されません。

- クイック検索: 前回の検索以降に変更されたファイルのみを検索するには、このオプションを選択します。これが初期設定です。
- フル検索: すべてのファイルを検索するには、このオプションを選択します。

注意

- 初回のクイック検索ではフル検索が実行され、その後のクイック検索では変更されたファイルのみが検索されます。
- [フル検索] から [クイック検索] に切り替えると、前回のフル検索の完了後に変更されたファイルのみが検索されます。

7. その他の検索設定を指定します。

- 検出ファイルの名前を変更: 検出されたファイルの名前を変更し、不正なファイルが誤って実行されることを防ぐには、このオプションを選択します。

  検出されたファイルの名前は `id_<original filename>.vir` 形式に変更されます。

  たとえば、元のファイル名が `test` の場合、変更後のファイル名は `56_test.vir` になります。

- 分析レポートを出力フォルダにコピー: 分析レポートのコピーを出力フォルダに作成するには、このオプションを選択します。

注意

検索設定を有効にする場合は、ネットワーク共有で読み取り書き込み権限が設定されていることを確認してください。

8. 予約検索を設定します。次の操作を実行します。
   a. ボタンをクリックして、予約検索の有効/無効を切り替えます。
   b. スケジュールオプションを選択して、必要な設定を行います。

   注意

   フル検索を選択した場合に設定できるのは、毎週または毎月のスケジュールのみです。

9. (オプション) [接続テスト] をクリックして、ネットワーク共有への接続をテストします。
10. [保存] をクリックします。

ヒント

ネットワーク共有を追加したら、[送信元] 画面にアクセスして、関連するサンプルの送信を確認したり、仮想アナライザのリソース割り当ての重みの値 (初期設定は 4) を調整したりできます。

失敗した検索を表示する

Deep Discovery Analyzer が検索できなかったファイルのリストは、[失敗した検索] 画面で確認できます。

注意

Deep Discovery Analyzer は、次の予約検索または手動検索でファイルの検索を再度試行します。

[失敗した検索] 画面を表示するには、[仮想アナライザ] > [ネットワーク共有] の順に選択し、[検索結果] フィールドの [失敗] の横にある数字をクリックします。

検索機能やフィルタエントリ (ファイル名、パス、ネットワーク共有名、エラーの種類、またはイベントのログ記録日時) を使用できます

次の表は、[失敗した検索] 画面の詳細を示しています。

フィールド	説明
ファイル名	Deep Discovery Analyzer が検索できなかったファイルの名前を表示します
共有名	ネットワーク共有の名前を表示します
パス	ネットワーク共有のファイルパスを表示します
エラーの種類	検索エラーの種類を表示します
イベントのログ記録日時	イベントが検出された日時を表示します

第 5 章

アラートとレポート

この章では、[アラート] と [レポート] の機能について説明します。

アラート

[アラート] 画面には、次のものが含まれています。

- [アラートの送信] タブ
- [ルール] タブ

[アラートの送信] タブ

[アラート/レポート] > [アラート] の [アラートの送信] タブには、Deep Discovery Analyzer で生成されたすべてのアラート通知が表示されます。アラート通知は、Deep Discovery Analyzer の状態をただちに知らせる機能です。

次の列は、Deep Discovery Analyzer で作成されるアラート通知に関する情報を示しています。

表 5-1. [アラートの送信] の列

列の名前	情報
実行日時	アラート通知が実行された日付と時刻。
レベル	実行されたアラート通知のレベル。 • 重大: ただちに対応が必要なイベント • 重要: 監視が必要なイベント • 情報: 限定的な観察が必要なイベント
ルール	アラート通知を実行したルール。
影響を受けるアプライアンス	該当する場合は、ホスト名、アラート通知の内容によって影響を受けるアプライアンスの IPv4 および IPv6 アドレス。
詳細	クリックすると、アラート通知の受信者、件名、およびメッセージのリストを含むアラート通知の詳細を表示できます。

[ルール] タブ

[アラート/レポート] > [アラート] の [ルール] タブには、Deep Discovery Analyzer で使用されているすべてのアラート通知ルールが表示されます。

次の列は、Deep Discovery Analyzer で使用されるアラート通知ルールに関する情報を示しています。

表 5-2. [ルール] の列

列の名前	情報
アラートレベル	アラート通知ルールのレベル。 • 重大: ただちに対応が必要なイベント • 重要: 監視が必要なイベント • 情報: 限定的な観察が必要なイベント
ルール	アラート通知を実行したルール。
条件	アラートルールの説明。
アラートの実行間隔	しきい値に達したかしきい値を超えた場合にアラート通知を送信する間隔。
ステータス	クリックしてルールの有効/無効を切り替えます。

各アラートを実行するしきい値を設定できます。詳細については、149 ページの「ルールを変更する」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 Analyzer では、サンドボックスおよびアプライアンスの機能不全は重大な問題と見なされます。

表 5-3. 重大なアラート

名前	条件 (初期設定)	アラートの実行間隔 (初期設定)
Virtual Analyzer Stopped (仮想アナライザの停止)	Virtual Analyzer encountered an error and was unable to recover. Analysis has stopped. (仮想アナライザでエラーが発生し、回復できませんでした。分析は中止されました。)	即時

名前	条件 (初期設定)	アラートの実行間隔 (初期設定)
Passive Primary Appliance Activated (パッシブなプライマリアプライアンスのアクティベート)	The active primary appliance encountered an error and was unable to recover. The passive primary appliance took over the active role. (アクティブなプライマリアプライアンスでエラーが発生し、回復できませんでした。パッシブなプライマリアプライアンスがアクティブの役割を引き継ぎました。)	即時
License Expiration (ライセンス有効期限)	License is about to expire or has expired. (ライセンスの有効期限が近づいているか切れています。)	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 Analyzer では、不審オブジェクトの検出、ハードウェア容量の変更、特定のサンドボックスキューのアクティビティ、コンポーネントのアップデート、およびアカウントとクラスタリングの問題は重要な問題と見なされます。

表 5-4. 重要なアラート

名前	条件 (初期設定)	アラートの実行間隔 (初期設定)
Account Locked (アカウントのロック)	An account was locked because of multiple unsuccessful logon attempts. (ログオンに複数回失敗したためアカウントがロックされました。)	即時
Long Virtual Analyzer Queue (仮想アナライザのキュー長超過)	The number of Virtual Analyzer submissions has exceeded the threshold of 100. (仮想アナライザの送信数がしきい値の 100 を超過しました。)	30 分ごとに 1 回

名前	条件 (初期設定)	アラートの実行間隔 (初期設定)
Component Update Unsuccessful (コンポーネントのアップデート失敗)	A component update was unsuccessful. (コンポーネントのアップデートに失敗しました。)	30 分ごとに 1 回
High CPU UsageCPU (使用率の超過)	The average CPU usage in the last 5 minutes has exceeded the threshold of 90%. (過去 5 分間の平均 CPU 使用率がしきい値の 90%を超過しました。)	30 分ごとに 1 回
High Memory Usage (メモリ使用率の超過)	The average memory usage in the last 5 minutes has exceeded the threshold of 90%. (過去 5 分間の平均メモリ使用率がしきい値の 90%を超過しました。)	30 分ごとに 1 回
High Disk Usage (ディスク使用量の超過)	Disk usage has exceeded the threshold of 85%. (ディスク使用量がしきい値の 85%を超過しました。)	30 分ごとに 1 回
Secondary Appliance Unresponsive (セカンダリアプライアンスの応答なし)	A secondary appliance in the cluster encountered an error and was unable to recover. (クラスタ内のセカンダリアプライアンスでエラーが発生し、回復できませんでした。)	即時
High Availability Suspended (高可用性の一時停止)	The passive primary appliance encountered an error and was unable to recover. High availability was suspended. (パッシブなプライマリアプライアンスでエラーが発生し、回復できませんでした。高可用性は一時停止されました。)	30 分ごとに 1 回
New High-Risk Objects Identified (新しいリスク高オブジェクトの特定)	The number of new high-risk objects identified during the last 30 minutes has reached the threshold of 10. (過去 30 分間に識別された新しいリスク高オブジェクトの数がしきい値の 10 に達しました。)	即時

名前	条件 (初期設定)	アラートの実行間隔 (初期設定)
Connection Issue (接続の問題)	Unable to establish connection to a required resource. (必要なリソースへの接続を確立することができません。)	30 分ごとに 1 回
Long Virtual Analyzer Processing Time (仮想アナライザの処理時間の超過)	The Virtual Analyzer processing time has exceeded the threshold of 30 minutes. (仮想アナライザの処理時間がしきい値の 30 分を超過しました。)	30 分ごとに 1 回
Network Share Inaccessible (ネットワーク共有アクセス不可)	A network share is inaccessible. (ネットワーク共有にアクセスできません。)	30 分ごとに 1 回

注意

システムで長期間にわたり高 CPU 使用率またはメモリ使用率が頻繁に発生する場合は、サンドボックスインスタンスの数を減らすことを検討してください。

詳細については、107 ページの「サンドボックスインスタンスを変更する」を参照してください。

情報アラート

次の表は、限定的な観察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。Deep Discovery Analyzer では、高可用性の復元、および Syslog サーバとバックアップサーバにアクセスできない状態は情報イベントと見なされます。

表 5-5. 情報アラート

名前	条件 (初期設定)	アラートの実行間隔 (初期設定)
Syslog Server InaccessibleSyslog (サーバにアクセスできない)	The syslog server was inaccessible. Logs were not sent to the server.Syslog (サーバにアクセスできませんでした。ログがサーバに送信されませんでした。)	30 分ごとに 1 回
Backup Server Inaccessible (バックアップサーバにアクセスできない)	The backup server was inaccessible. Logs and objects were not backed up. (バックアップサーバにアクセスできませんでした。ログとオブジェクトがバックアップされませんでした。)	30 分ごとに 1 回
High Availability Restored (高可用性の復元)	The passive primary appliance recovered from an error and high availability was restored. (パッシブなプライマリアプライアンスがエラーから回復し、高可用性が復元されました。)	即時

ルールを変更する

始める前に

SMTP サーバを設定して通知を送信します。詳細については、232 ページの「[SMTP] タブ」を参照してください。

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。一部のルールには、オブジェクト件数、送信件数、または期間などの追加のパラメータがあります。すべての重大および重要なアラートについて、通知の受信者を 1 つ以上追加することをお勧めします。

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。

   [ルール] 画面が表示されます。

2. [ルール] 列のアラートルール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. ルールの設定を変更します。

   注意

   詳細については、150 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。

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。一部のルールには、オブジェクト件数、送信件数、または期間などの追加のパラメータがあります。

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、167 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 5-6. 仮想アナライザの停止

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔が表示されます。変更できません。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-7. パッシブなプライマリアプライアンスのアクティベート

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔が表示されます。変更できません。
件名	実行されたアラート通知の件名を指定します。
メッセージ	実行されたアラート通知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。 • %ProductName% • %ProductShortName% • %ActiveApplianceName% • %ActiveApplianceIP% • %PassiveApplianceName% • %PasssiveApplianceIP% • %DateTime% • %ConsoleURL%

表 5-8. ライセンス有効期限

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
件名	実行されたアラート通知の件名を指定します。
メッセージ	実行されたアラート通知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。 • %ProductName% • %ProductShortName% • %LicenseStatus% • %ExpirationDate% • %DaysBeforeExpiration% • %DateTime% • %ConsoleURL%
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。

表 5-9. ネットワーク共有アクセス不可

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔が表示されます。変更できません。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL% • %NetworkShare%
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。

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、167 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 5-10. アカウントのロック

パラメータ	説明
ステータス	このアラートを有効または無効にします。 **ヒント** Apex Central からシングルサインオンを使用して管理コンソールにアクセスしている場合は、Apex Central でパスワードの設定を確認してから再度ログオンしてください。
アラートレベル	このアラートのレベルを表示します。変更できません。

パラメータ	説明
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔が表示されます。変更できません。
件名	実行されたアラート通知の件名を指定します。
メッセージ	実行されたアラート通知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。 • %ProductName% • %ProductShortName% • %LockedAccount% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-11. 仮想アナライザのキュー長超過

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
送信	アラートを実行する送信のしきい値を指定します。 ヒント 仮想アナライザで 5 分以内に分析できるサンプルの推定数を表示するには、[キュー内のサンプル] ウィジェット内の赤線を参照してください。詳細については、47 ページの「キュー内のサンプル」を参照してください。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %SandboxQueueThreshold% • %SandboxQueue% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-12. コンポーネントのアップデート失敗

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %ComponentList% • %UpdateError% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-13. CPU 使用率の超過

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
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	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
確認の実行間隔	次の確認を実行するまで待機する時間を指定します。
期間	各確認の期間を指定します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %CPUThreshold% • %CPUUsage% • %CheckingInterval% • %CheckingDuration% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-14. メモリ使用率の超過

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
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指定します。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
確認の実行間隔	次の確認を実行するまで待機する時間を指定します。
期間	各確認の期間を指定します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %MemThreshold% • %MemUsage% • %CheckingInterval% • %CheckingDuration% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-15. ディスク使用量の超過

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
ディスクの使用状況	アラートを実行するディスク使用率のしきい値を指定します。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
確認の実行間隔	次の確認を実行するまで待機する時間を指定します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %DiskThreshold% • %DiskUsage% • %FreeDiskSpace% • %CheckingInterval% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-16. セカンダリアプライアンスの応答なし

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔が表示されます。変更できません。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %ApplianceError% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-17. 高可用性の一時停止

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %ActiveApplianceName% • %ActiveApplianceIP% • %PassiveApplianceName% • %PasssiveApplianceIP% • %DateTime% • %ConsoleURL%

表 5-18. 新しいリスク高オブジェクトの特定

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
オブジェクト	アラートを実行するオブジェクトのしきい値を指定します。 注意 低いしきい値を指定すると、アラートが頻繁に生成される可能性がありますが、各アラートは検出の一意のセットを対象とします。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔が表示されます。変更できません。

パラメータ	説明
期間	アラートを実行する期間のしきい値を指定します。 注意 低いしきい値を指定すると、アラートが頻繁に生成される可能性がありますが、各アラートは検出の一意のセットを対象とします。
件名	実行されたアラート通知の件名を指定します。
メッセージ	実行されたアラート通知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。 • %ProductName% • %ProductShortName% • %HighRiskThreshold% • %TimeRange% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-19. 接続の問題

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
監視対象サービス	このアラートで監視するサービスを選択します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %ServiceList% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-20. 仮想アナライザの処理時間の超過

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
処理時間	アラートを実行する処理時間のしきい値を指定します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %SandboxProcessTimeThreshold% • %SampleList% • %TotalSampleNumber% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-21. ネットワーク共有アクセス不可

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %ActiveApplianceName% • %ActiveApplianceIP% • %DateTime% • %ConsoleURL% • %NetworkShare%
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。

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、167 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 5-22. Syslog サーバにアクセスできない

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
件名	実行されたアラート通知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通知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。 • %ProductName% • %ProductShortName% • %SyslogServer% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-23. バックアップサーバにアクセスできない

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔を選択します。
件名	実行されたアラート通知の件名を指定します。
メッセージ	実行されたアラート通知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。 • %ProductName% • %ProductShortName% • %BackupServer% • %ApplianceName% • %ApplianceIP% • %DateTime% • %ConsoleURL%

表 5-24. 高可用性の復元

パラメータ	説明
ステータス	このアラートを有効または無効にします。
アラートレベル	このアラートのレベルを表示します。変更できません。
アラートの実行間隔	ルール条件が満たされたときにこのアラートを送信する間隔が表示されます。変更できません。
件名	実行されたアラート通知の件名を指定します。
メッセージ	実行されたアラート通知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。 • %ProductName% • %ProductShortName% • %ActiveApplianceName% • %ActiveApplianceIP% • %PassiveApplianceName% • %PasssiveApplianceIP% • %DateTime% • %ConsoleURL%

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できるアラートルールについて、また、そのトークンによりアラート通知に含まれる情報については、こ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、150 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 5-25. メッセージトークン

トークン	説明	対象
%ActiveApplianceIP%	Deep Discovery Analyzer のアクティブなプライマリアプライアンスの IP アドレス 例: • 123.123.123.123 | 2001:0:3238:DFE1:63::FEFB	高可用性の復元 高可用性の一時停止 パッシブなプライマリアプライアンスのアクティベート
%ActiveApplianceName%	Deep Discovery Analyzer のアクティブなプライマリアプライアンスのホスト名 例: • •	高可用性の復元 高可用性の一時停止 パッシブなプライマリアプライアンスのアクティベート
%ApplianceError%	アプライアンスで発生したエラー 例: • 接続なし • 無効な API キー • 互換性がないソフトウェアバージョン	セカンダリアプライアンスの応答なし
%ApplianceIP%	Deep Discovery Analyzer アプライアンスの IP アドレス 例: • 123.123.123.123 | 2001:0:3238:DFE1:63::FEFB	すべて • 高可用性の復元 • 高可用性の一時停止 • パッシブなプライマリアプライアンスのアクティベート

トークン	説明	対象
%ApplianceName%	Deep Discovery Analyzer アプライアンスのホスト名 例: • •	すべて • 高可用性の復元 • 高可用性の一時停止 • パッシブなプライマリアプライアンスのアクティベート
%BackupServer%	バックアップサーバのホスト名または IP アドレス 例: • my.example.com • 123.123.123.123 • 2001:0:3238:DFE1:63::FEFB	バックアップサーバにアクセスできない
%ComponentList%	コンポーネントのリスト 例: • 高度な脅威検索エンジン • 不正プログラムパターンファイル (Deep Discovery) • IntelliTrap 除外パターンファイル • IntelliTrap パターンファイル	コンポーネントのアップデート失敗
%ConsoleURL%	Deep Discovery Analyzer 管理コンソールの URL 例: • https://192.168.85.69/ | https://[2001:0:3238:DFE1:63::FEFB]/	すべて

トークン	説明	対象
%CPUThreshold%	過去 5 分間に許容される平均 CPU 使用率 (%)。この値を超えるとアラート通知が送信されます。 例: • 80%	CPU 使用率の超過
%CPUUsage%	過去 5 分間の合計 CPU 使用率 (%) 例: • 80%	CPU 使用率の超過
%DateTime%	アラートが発生した日付と時刻 例: • 2014-03-21 03:34:09	すべて
%DaysBeforeExpiration%	製品ライセンスの有効期限までの日数 例: • 4	ライセンス有効期限
%DiskThreshold%	許容されるディスク使用率 (%)。この値を超えるとアラート通知が送信されます。 例: • 85%	ディスク使用量の超過
%DiskUsage%	合計ディスク使用率 (%) 例: • 85%	ディスク使用量の超過
%ExpirationDate%	製品ライセンスの有効期限日時 例: • 2014-03-21 03:34:09	ライセンス有効期限

トークン	説明	対象
%FreeDiskSpace%	使用可能なディスク容量 (GB) 例: • 50GB	ディスク使用量の超過
%HighRiskThreshold%	指定された期間内に識別された新しいリスク高オブジェクトの最大件数。この件数を超えるとアラート通知が送信されます。 例: • 10	新しいリスク高オブジェクトの特定
%LicenseStatus%	製品ライセンスの現在の状態 例: • アクティベート済み	ライセンス有効期限
%LockedAccount%	ロックされたアカウント 例: • ゲスト	アカウントのロック
%MemThreshold%	過去 5 分間に許容される平均メモリ使用率 (%)。この値を超えるとアラート通知が送信されます。 例: • 90%	メモリ使用率の超過
%MemUsage%	過去 5 分間の合計メモリ使用率 (%) 例: • 90%	メモリ使用率の超過
%NetworkShare%	ネットワーク共有フォルダ情報 例: 共有名: test | サーバアドレス: 123.123.123.123 | プロトコル: CIFS	ネットワーク共有アクセス不可

トークン	説明	対象
%PasssiveApplianceIP%	Deep Discovery Analyzer のパッシブなプライマリアプライアンスの IPv4 アドレス 例: • 123.123.123.123	高可用性の復元 高可用性の一時停止 パッシブなプライマリアプライアンスのアクティベート
%PassiveApplianceName%	Deep Discovery Analyzer のパッシブなプライマリアプライアンスのホスト名 例: • •	高可用性の復元 高可用性の一時停止 パッシブなプライマリアプライアンスのアクティベート
%ProductName%	製品名 例: • Deep Discovery Analyzer	すべて
%ProductShortName%	短縮された製品名 例: • DDAn	すべて
%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送信件数 例: • 100	仮想アナライザのキュー長超過
%SandboxQueueThreshold%	サンドボックスキュー内送信の最大件数。この件数を超えるとアラート通知が送信されます。 例: • 30	仮想アナライザのキュー長超過

トークン	説明	対象
%SyslogServer%	Syslog サーバのホスト名または IP アドレス 例: • my.example.com • 123.123.123.123 • 2001:0:3238:DFE1:63::FEFB	Syslog サーバにアクセスできない
%TimeRange%	新しいリスク高オブジェクトの観察期間。この期間を超えるとアラート通知が送信されます。 例: • 5 分 • 30 分 • 1 時間 • 12 時間 • 24 時間	新しいリスク高オブジェクトの特定
%UpdateError%	アップデートエラーのリスト 例: • ダウンロードできません: 高度な脅威検索エンジン • アップデートできません: Deep Discovery 用不正プログラムパターンファイル • アップデートできません: IntelliTrap 除外パターンファイル。アプライアンスは仮想アナライザのインスタンスの設定中、またはシャットダウン中です。	コンポーネントのアップデート失敗

トークン	説明	対象
%ServiceList%	問題によって影響を受けるサービス 例: • 内部仮想アナライザネットワーク (eth1、プロキシなし)	接続の問題
%SandboxProcessTimeThreshold%	サンプルの処理に費やされる最大時間。この時間を超えるとアラート通知が送信されます。	仮想アナライザの処理時間の超過のアラート
%SampleList%	問題によって影響を受けたサンプル	仮想アナライザの処理時間の超過のアラート
%TotalSampleNumber%	問題によって影響を受けたサンプルの合計数	仮想アナライザの処理時間の超過のアラート
%CheckingDuration%	各確認の実行に要する時間	CPU 使用率の超過 メモリ使用率の超過
%CheckingInterval%	次の確認を実行するまでの時間	CPU 使用率の超過 メモリ使用率の超過 ディスク使用量の超過
%DiagnosisTip%	問題の解決方法についての推奨事項	接続の問題

レポート

Deep Discovery Analyzer のすべてのレポートは、使用可能なレポートテンプレートに基づいて生成されます。

[生成されたレポート] タブ

[アラート/レポート] > [レポート] の [生成されたレポート] タブには、Deep Discovery Analyzer によって生成されたすべてのレポートが表示されます。

生成されたレポートは、管理コンソールにリンクとして表示されるだけでなく、メールの添付ファイルとしても使用できます。レポートを生成する前に、1 人以上のメール受信者への送信を選択できます。

生成されたレポートのタスク

[生成されたレポート] 画面には、次のオプションが含まれます。

表 5-26. [生成されたレポート] のタスク

タスク	手順
レポートの生成	175 ページの「レポートを生成する」を参照してください。
レポートのダウンロード	レポートをダウンロードするには、表内の最終列に移動してアイコンをクリックします。生成されたレポートは、PDF 形式のファイルとして使用できます。
レポートの送信	レポートを選択して、[レポートの送信] をクリックします。一度に送信できるレポートは 1 つのみです。
削除	レポートを 1 つ以上選択して、[削除] をクリックします。
列データの並べ替え	列タイトルをクリックすると、その下にあるデータを並べ替えることができます。
レコードコントロールとページ区切りコントロール	画面の最下部にあるパネルにレポートの合計数が表示されます。すべてのレポー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レポートを表示します。

レポートを生成する

手順

1. [アラート/レポート] > [レポート] > [生成されたレポート] の順に選択します。

   [生成されたレポート] 画面が表示されます。

2. [新規生成] をクリックします。

   [レポートの生成] 画面が表示されます。

3. レポートを設定します。

オプション	説明
テンプレート	使用可能なレポートテンプレートを選択します。
説明	説明を 500 文字以内で入力します。
範囲	選択したレポートテンプレートに基づいて対象とする日付を指定します。 • 日次レポート: 現在より前の日付を選択します。レポートの対象期間は各日の 00:00:00 から 23:59:59 までになります。 • 週次レポート: レポートの対象期間が終了する曜日を選択します。たとえば、水曜日を選択すると、レポートの対象期間は特定週の水曜日の 23:59:59 からさかのぼって前週の木曜日の 00:00:00 までになります。 • 月次レポート: レポートの対象期間が終了する日付を選択します。たとえば、10 日を選択すると、レポートの対象期間は特定月の 10 日の 23:59:59 からさかのぼって前月の 11 日の 00:00:00 までになります。
形式	レポートのファイル形式は PDF のみです。
すべての連絡先に送信	生成されたレポートをすべての連絡先に送信するには、このチェックボックスをオンにします。
受信者	ドロップダウンリストから連絡先を選択するか、メールアドレスを入力して <Enter> キーを押します。 最大で 100 個のメールアドレスを入力できます。入力は一度に 1 つずつ行います。 **注意** メールアドレスごとに <Enter> キーを押します。複数のメールアドレスをカンマで区切って入力することはできません。 受信者を指定する前に、[管理] > [システム設定] > [SMTP] で SMTP を設定します。

オプション	説明
	注意 Deep Discovery Analyzer は、[送信] がクリックされてから約 5 分後にレポートを生成します。

4. [生成] をクリックします。

[スケジュール] タブ

[アラート/レポート] > [レポート] の [スケジュール] タブには、レポートテンプレートから作成されたすべての予約レポートが表示されます。それぞれの予約レポートには、使用されるテンプレートや実際のスケジュールなどのレポートの設定が含まれます。

注意

生成されたレポートはこの画面に表示されません。レポートを表示するには、[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。

このタブには、次のオプションが含まれます。

表 5-27. [スケジュール] のタスク

タスク	手順
スケジュールの追加	新規予約レポートを追加するには、[スケジュールの追加] をクリックします。これにより [レポートスケジュールの追加] 画面が開きます。ここで予約レポートの設定を指定します。詳細については、178 ページの「[レポートスケジュールの追加] 画面」を参照してください。
編集	予約レポートの設定を編集するには、予約レポートを選択し、[編集] をクリックします。これにより [レポートスケジュールの編集] 画面が開きます。ここには [レポートスケジュールの追加] 画面と同じ設定が表示されます。詳細については、178 ページの「[レポートスケジュールの追加] 画面」を参照してください。 一度に編集できる予約レポートは 1 つのみです。

タスク	手順
削除	削除する予約レポートを 1 つ以上選択して、[削除] をクリックします。
列データの並べ替え	列タイトルをクリックすると、その下にあるデータを並べ替えることができます。
レコードコントロールとページ区切りコントロール	画面の最下部にあるパネルに予約レポートの合計数が表示されます。すべての予約レポー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予約レポートを表示します。

[レポートスケジュールの追加] 画面

[レポートスケジュールの追加] 画面は、予約レポートを追加するときに表示されます。予約レポートには、Deep Discovery Analyzer が定期レポートの生成時に使用する設定が含まれます。

この画面には、次のオプションが含まれます。

表 5-28. [レポートスケジュールの追加] 画面のタスク

フィールド	手順
テンプレート	テンプレートを選択します。
説明	説明を入力します。

フィールド	手順
生成時刻	選択したテンプレートに従って予約を設定します。 日次レポートのテンプレートの場合は、レポートを生成する時間を設定します。レポートの対象範囲は、毎日 00:00:00〜23:59:59 で、指定した時間にレポートの生成が開始されます。 週次レポートのテンプレートの場合は、開始曜日を選択して、レポートを生成する時間を設定します。たとえば水曜日を選択した場合、レポートの対象範囲は、各週の水曜日の 00:00:00 から翌週の火曜日の 23:59:59 までになります。このレポートは、範囲開始の翌週の水曜日の指定した時間に生成が開始されます。 月次レポートのテンプレートの場合は、月内の日付を選択して、レポートを生成する時間を設定します。たとえば 10 日を選択した場合、レポートの対象範囲は、各月の 10 日の 00:00:00 から翌月の 9 日の 23:59:59 までになります。このレポートは、範囲開始の翌月の 10 日の指定した時間に生成が開始されます。 **注意** 29 日、30 日または 31 日にレポートが生成されるように設定すると、これらの日付がない月には、Deep Discovery Analyzer によって翌月の 1 日の指定時間にレポートの生成が開始されます。
形式	レポートのファイル形式は PDF のみです。
すべての連絡先に送信	生成されたレポートをすべての連絡先に送信するには、このチェックボックスをオンにします。
受信者	ドロップダウンリストから連絡先を選択するか、レポートの送信先とする有効なメールアドレスを入力して <Enter> キーを押します。最大で 100 個のメールアドレスを入力できます。入力は一度に 1 つずつ行います。カンマで区切って複数のメールアドレスを入力することはできません。 受信者を指定する前に、[管理] > [システム設定] にある [SMTP] タブで SMTP 設定を指定していることを確認します。

[カスタマイズ] タブ

[アラート/レポート] > [レポート] の [カスタマイズ] タブを使用すると、Deep Discovery Analyzer のレポートの項目をカスタマイズできます。

この画面には、次のオプションが含まれます。

表 5-29. [表紙ページ]

オプション	タスク	表示領域
タイトル	タイトルを 40 文字以内で入力します。	レポートの表紙

表 5-30. [メールメッセージ]

オプション	タスク	表示領域
ヘッダロゴ	ロゴの場所を参照します。 イメージの要件は次のとおりです。 • 寸法: 180 x 60 ピクセル • 最大ファイルサイズ: 30KB • ファイルの種類: BMP、GIF、JPG、または PNG	通知
区切りの色	初期設定の色を変更するには、ボックスをクリックし、カラーピッカーを使用して新しい値を指定します。	通知
フッタロゴ	ロゴの場所を参照します。 イメージの要件は次のとおりです。 • 寸法: 100 x 40 ピクセル • 最大ファイルサイズ: 30KB • ファイルの種類: BMP、GIF、JPG、または PNG	通知
フッタテキスト	フッタを 60 文字以内で入力します。	通知

第 6 章

管理

この章では、[管理] の機能について説明します。

アップデート

[管理] > [アップデート] 画面を使用して、コンポーネントと製品のアップデートを設定します。

コンポーネントの使用およびアップデートにはアクティベーションコードが必要です。詳細については、282 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] タブ

[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 6-1. 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 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。
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。
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、最新の不正プログラムや複合的な脅威による攻撃を Deep Discovery Analyzer で識別できるようにするための情報が含まれます。トレンドマイクロでは、1 週間に数回、また特に有害なウイルス/不正プログラムの検出後は随時、新しいバージョンのパターンファイルを作成およびリリースしています。
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。

コンポーネント	説明
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。
信頼済み証明書情報	信頼済み証明書情報には、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。
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。
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 (Windows および Linux 用)。

この画面には、次のオプションが含まれます。

オプション	タスク
今すぐアップデート	1 つ以上のコンポーネントを選択して [今すぐアップデート] をクリックすると、選択したコンポーネントがアップデートされます。
ロールバック	1 つ以上のコンポーネントを選択して [ロールバック] をクリックすると、選択したコンポーネントが以前のバージョンに戻ります。
バージョン情報の同期	アップデート元からコンポーネントのバージョンを取得して、アップデートが必要なコンポーネントを確認する場合にクリックします。 [アップデート元のバージョン] 列に表示されているバージョンが現在のバージョンよりも大きい場合、対象のコンポーネントをアップデートしてください。Deep Discovery Analyzer では、アップデートが利用可能なコンポーネントのバージョン番号が赤色で表示されます。

[コンポーネントのアップデート設定] タブ

[コンポーネントのアップデート設定] タブでは、自動アップデートおよびアップデート元を設定できます。

設定	説明
自動アップデート	[アップデートを自動的に確認] を選択すると、アップデートが 15 分ごとに確認されるようになります。特定の時間間隔でアップデートを実行するように指定することもできます。
アップデート元	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。 • トレンドマイクロから直接コンポーネントをダウンロードするには、[トレンドマイクロのアップデートサーバ] を選択します。Deep Discovery Analyzer がインターネットに接続されていることを確認してください。 アップデートサーバを認証するには、[HTTPS 認証を有効にする] を選択します。

設定	説明
	注意 [HTTPS 認証を有効にする] を選択し、ネットワーク上 (セキュアゲートウェイなど) で HTTPS 復号を有効にする場合は、アップデートサーバの URL を承認済みリストに含めることをお勧めします。 • 別のアップデート元を指定するには、[その他のアップデートサーバ] を選択します。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。 [システムプロキシを使用する] を選択すると、[管理]→[システム設定]→[プロキシ] 画面で指定したシステムのプロキシ設定を使用してアップデート元に接続できます。 その他のアップデートサーバから入手したアップデートパッケージの整合性を確認するには、[コンポーネントアップデートパッケージの整合性の確認を有効にする] を選択します。このオプションを選択する場合は、Deep Discovery Analyzer のアップデートサーバに、コンポーネントアップデートパッケージの整合性を確認するためのシグネチャファイルがあることを確認してください。 アップデート元のセットアップに支援が必要な場合は、テクニカルサポートにお問い合わせください。 注意 • IPv6 アドレスが URL の一部である場合は、アドレスを角カッコ ([]) で囲みます。 • Deep Discovery Analyzer からアップデート元への接続にプロキシサーバが必要な場合は、プロキシ設定が正しいことを確認します。詳細については、230 ページの「[プロキシ] タブ」を参照してください。 • Trend Micro Vision One を Deep Discovery Analyzer のアップデート元として設定することもできます。これを行うには、Trend Micro Vision One でアップデートを有効にして必要な設定を行います。Deep Discovery Analyzer はこの設定を Service Gateway 経由で取得できます。 詳細については、Trend Micro Vision One のドキュメントを参照してください。

[HotFix/Patch] タブ

[HotFix/Patch] 画面を使用して、HotFix および Patch を Deep Discovery Analyzer に適用します。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 6-2. HotFix/Patch

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。
Patch	Patch は、複数のプログラムの問題を解決する HotFix と Critical Patch をまとめたものです。トレンドマイクロでは定期的に Patch を配布しています。

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 HotFix および Patch 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

HotFix/Patch のインストール

高可用性クラスタ設定で Deep Discovery Analyzer を使用する場合は、次のタスクを実行します。

1. パッシブなプライマリアプライアンスをデタッチします。
2. アクティブなプライマリアプライアンスで、次に説明するメインタスクを実行します。
3. パッシブなプライマリアプライアンスで、次に説明するメインタスクを実行します。
4. パッシブなプライマリアプライアンスをクラスタに再度追加します。

手順

1. 管理コンソールのログオンページで [セッションタイムアウトの延長を有効にする] を選択し、有効なユーザ名とパスワードを使用してログオンします。
2. [管理] > [アップデート] > [HotFix/Patch] の順に選択します。
3. [アップデートファイル] 横の [ファイルを選択] をクリックして、製品のアップデートファイルを選択します。
4. [インストール] をクリックします。

   重要

   アップグレードが完了するまで、ブラウザを閉じたり、表示を更新したり、別のページに移動したり、管理コンソールでタスクを実行したり、アプライアンスの電源をオフにしたりしないでください。

   アップデートが完了すると、Deep Discovery Analyzer が自動的に再起動します。
5. 管理コンソールにログオンします。
6. [管理] > [アップデート] > [HotFix/Patch] 画面に戻ります。

7. 適用した HotFix/Patch が最新のアップデートとして表示されることを [履歴] で確認します。

HotFix/Patch のロールバック

高可用性クラスタ設定で Deep Discovery Analyzer を使用する場合は、次のタスクを実行します。

1. パッシブなプライマリアプライアンスをデタッチします。
2. アクティブなプライマリアプライアンスで、次に説明するメインタスクを実行します。
3. パッシブなプライマリアプライアンスで、次に説明するメインタスクを実行します。
4. パッシブなプライマリアプライアンスをクラスタに再度追加します。

Deep Discovery Analyzer には、アップデートを取り消し、製品をアップデート前の状態に戻すためのロールバック機能があります。特定の HotFix/Patch の適用後に製品に問題が発生した場合は、この機能を使用します。

注意

ロールバックプロセスでは Deep Discovery Analyzer が自動的に再起動されるため、ロールバック前に管理コンソール上のすべてのタスクを完了してください。

手順

1. [管理] > [アップデート] > [HotFix/Patch] の順に選択します。
2. [履歴] で [ロールバック] をクリックします。

   ロールバックが完了すると、Deep Discovery Analyzer が自動的に再起動します。
3. 管理コンソールにログオンします。
4. [管理] > [アップデート] > [HotFix/Patch] 画面に戻ります。

5. ロールバックした HotFix/Patch が [履歴] に表示されないことを確認します。

[ファームウェア] タブ

[ファームウェア] タブを使用して、Deep Discovery Analyzer にアップグレードを適用します。トレンドマイクロ各アップグレードには Readme ファイルが用意されています。アップグレードを適用する前に付属する Readme ファイルを読み、機能情報やインストール手順について確認してください。

注意

ハードウェアモデル 1100 および 1200 にファームウェアのアップデートを適用すると、Deep Discovery Analyzer によって、Deep Discovery Analyzer 6.9 または 7.0 の設定が自動的に 7.1 に移行されます。

高可用性クラスタ設定で Deep Discovery Analyzer を使用する場合は、次のタスクを実行します。

1. パッシブなプライマリアプライアンスをデタッチします。
2. アクティブなプライマリアプライアンスで、次に説明するメインタスクを実行します。
3. パッシブなプライマリアプライアンスで、次に説明するメインタスクを実行します。
4. パッシブなプライマリアプライアンスをクラスタに再度追加します。

アップグレードをインストールするには、次の手順を実行します。

手順

1. 管理コンソールのログオンページで [セッションタイムアウトの延長を有効にする] を選択し、有効なユーザ名とパスワードを使用してログオンします。
2. [管理] > [アップデート] に移動して、[ファームウェア] タブをクリックします。

3. [アップデートファイル] 横の [ファイルを選択] をクリックして、ファームウェアのアップグレードファイルを選択します。

4. [適用] をクリックします。

重要

アップグレードが完了するまで、ブラウザを閉じたり、表示を更新したり、別のページに移動したり、管理コンソールでタスクを実行したり、アプライアンスの電源をオフにしたりしないでください。

アップグレードが完了すると、Deep Discovery Analyzer が自動的に再起動します。

5. ブラウザのキャッシュをクリアしてから、管理コンソールにアクセスします。

統合製品/サービス

[管理] > [統合製品/サービス] にある [統合製品/サービス] 画面には次のタブがあります。

- 191 ページの「Trend Micro Vision One」
- 192 ページの「[Deep Discovery Director] タブ」
- 197 ページの「[Smart Protection] タブ」
- 203 ページの「[ICAP] タブ」
- 209 ページの「[Microsoft Active Directory] タブ」
- 210 ページの「[SAML 認証] タブ」
- 221 ページの「メールでの送信」
- 223 ページの「[Syslog] タブ」

Trend Micro Vision One

Trend Micro 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。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 Analyzer は Service Gateway を介して Trend Micro Vision One と統合され、ハイブリッド環境で共同してセキュリティ分析を行うために次の処理を実行します。

- 不審オブジェクト (同期対象のものとユーザ指定のもの) および例外を Vision One と同期する
- 内部仮想アナライザにより生成された新しい不審オブジェクトを Vision One にアップロードする

注意

Deep Discovery Analyzer は、内部仮想アナライザにより生成された既存の不審オブジェクトを Vision One にアップロードしません。

Service Gateway の設定と同期ステータスの表示は [Trend Micro Vision One] タブで行います。

Service Gateway を設定する

注意

- 事前に Trend Micro Vision One 管理者から必要な Service Gateway の設定 (サーバアドレスや API キーなど) を入手し、さらに Trend Micro Vision One で [不審オブジェクトリストの同期] 機能が有効になっていることを確認してください。
- Trend Micro Vision One と統合されている場合、Deep Discovery Analyzer は常に不審オブジェクトリストと除外リストを Trend Micro Vision One と同期します。

手順

1. [管理] > [統合製品/サービス] の順に選択します。

   [Trend Micro Vision One] タブが表示されます。

2. [Service Gateway を有効にする] をクリックします。

3. Service Gateway のアドレスを入力します。

4. API キーを入力します。

5. (オプション) Trend Micro Vision One 接続で使用するように Deep Discovery Analyzer のプロキシ設定が指定されている場合は、[プロキシサーバを使用して接続する] を選択します。

6. (オプション) 組織で CA 証明書を使用する場合は、[証明書を使用する] を選択し、[選択] をクリックして証明書ファイルを指定します。

7. [保存] をクリックします。

8. (オプション) [接続テスト] をクリックして、Service Gateway 経由での Trend Micro Vision One への接続をテストします。

[Deep Discovery Director] タブ

Trend Micro Deep Discovery Director (以下、Deep Discovery Director) は、侵害の兆候 (IOC) に関する情報を提供し、製品のアップデート、製品のアップグレード、設定の複製、および仮想アナライザイメージの Deep Discovery Analyzer への配信を一元管理する管理ソリューションです。

次のバージョンの Deep Discovery Director と統合されます。

- 5.2 以上

高可用性クラスタに設定された Deep Discovery Analyzer アプライアンスにアップデートまたはアップグレードを配信すると、一時的に次のような状態になります。

- 高可用性アプライアンスが接続解除され、高可用性が一時停止される

- 管理コンソールへのアクセスが制限され、情報画面が表示される

アップデートまたはアップグレードが完了すると、接続解除されたアプライアンスが自動的に再接続され、高可用性が復元します。

重要

- アップデートまたはアップグレードを配信する前に、アプライアンスでタスクが実行されていないことを確認してください。
- アップグレード中はアプライアンスをデタッチしないでください。
- アプライアンスのアップグレードに失敗するか、[アプライアンスをアップグレードしています] 画面が 2 時間以上表示され続ける場合は、Deep Discovery Director でエラーを確認してください。エラーを解決するには、一時的にアプライアンスをデタッチします。デタッチしたアプライアンスでアップグレードを続行します。アップグレード後、アプライアンスを手動で再度アタッチして高可用性を復元します。

仮想アナライザのイメージや設定をプライマリアプライアンスに配信または複製するには Deep Discovery Director 管理コンソールを使用しますが、この操作をセカンダリアプライアンスに対して実行する必要ありません。これはセカンダリアプライアンスが、仮想アナライザのイメージや設定をプライマリアプライアンスと自動同期するように設定されているためです。

Deep Discovery Director との統合により、次のことが可能になります。

- Deep Discovery Director への内部仮想アナライザにより生成された不審オブジェクトのアップロード
- 生成された不審オブジェクトとユーザ指定の不審オブジェクトの同期
- Deep Discovery Director 5.3 からの Linux イメージの配信
- Deep Discovery Director からの次の項目のダウンロード
  - 除外設定
  - 不審オブジェクト
  - YARA ルールファイル
  - ファイルパスワード (5.2 以上のオンプレミスバージョンの Deep Discovery Director)

注意

- Deep Discovery Analyzer を Deep Discovery Director に登録すると、Deep Discovery Analyzer 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。
- Deep Discovery Analyzer を Deep Discovery Director に登録すると、Deep Discovery Analyzer は Deep Discovery Director から自動的にファイルのパスワードを同期し、既存のファイルのパスワードを上書きします。ファイルのパスワードは Deep Discovery Director 管理コンソールでのみ変更できます。
- Deep Discovery Analyzer を Deep Discovery Director と Apex Central の両方に登録すると、Deep Discovery Analyzer は Deep Discovery Director からのみ除外リストを同期して、仮想アナライザの不審オブジェクトを Deep Discovery Director にのみアップロードします。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。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] 画面には、次の情報が表示されます。

表 6-3. [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。
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。

フィールド	情報
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。
不審オブジェクトを Deep Discovery Director から同期する	不審オブジェクトを Deep Discovery Director から同期するには、このオプションを選択します。

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] で次の操作を実行します。
   a. [サーバアドレス] に Deep Discovery Director のサーバアドレスを入力します。
   b. [ポート] に Deep Discovery Director 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。
   c. [API キー] に 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 Analyzer 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、[システムプロキシを使用] 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. (オプション) 不審オブジェクトを Deep Discovery Director から同期するには、[不審オブジェクトを Deep Discovery Director から同期する] を選択します。

注意

- 同期された不審オブジェクトのリストは、[同期された不審オブジェクト] 画面で表示できます。
- 同期された不審オブジェクトリストを ICAP 事前検索や仮想アナライザでの分析に使用するには、[ICAP] および [検索設定] 画面で必要な検索設定を行います。

  詳細については、205 ページの「ICAP を設定する」および 128 ページの「[検索設定] タブ」を参照してください。

5. [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。
- Deep Discovery Analyzer を負荷分散クラスタで使用している場合は、プライマリアプライアンスの登録によって自動的にすべてのセカンダリアプライアンスが登録されます。

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] に変わります。

注意

Deep Discovery Analyzer を Deep Discovery Director から登録解除すると、Deep Discovery Analyzer により、すべての同期された不審オブジェクトが自動的に削除されます。

[Smart Protection] タブ

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 Analyzer 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 Analyzer 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 Analyzer 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 6-4. 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	HTTPS	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、201 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、201 ページの「Smart Protection Server 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 Analyzer 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 Analyzer 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。
2. Deep Discovery Analyzer 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、201 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] > [統合製品/サービス] > [Smart Protection] の順に選択します。
2. [有効] を選択します。
3. [アップデート元] を選択します。
   - Trend Micro Smart Protection Network

     トレンドマイクロ Smart Protection Network は、Smart Protection テクノロジを統合するトレンドマイクロ製品にレピュテーションサー

ビスを提供する、グローバルなクラウドベースのインフラストラクチャです。Deep Discovery Analyzer は、HTTPS を使用して Trend Micro Smart Protection Network に接続します。Smart Protection Server を設定しない場合は、このオプションを選択します。

- Smart Protection Server

  Smart Protection Server は次のことを実行します。

  - Trend Micro Smart Protection Network と同じ Web レピュテーションサービスを提供します。
  - これらのサービスをグローバルな Trend Micro Smart Protection Network にリレーしてネットワーク効率を最適化します。
  - Deep Discovery Analyzer からグローバルサービスに接続するためのリバースプロキシとして機能します。

  トレンドマイクロ製品の管理者は、このサーバの設定と管理を行う必要があります。すでにサーバを設定している場合は、このオプションを選択します。

4. [Smart Protection Server] を選択する場合は、次の設定を行います。

   a. Smart Protection Server 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。

      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。

      ヒント

      Trend Micro Vision One を Deep Discovery Analyzer のローカルの Smart Protection Server として機能させることもできます。この場合は Service Gateway のアドレスを指定します。

      ---

   b. (オプション) Smart Protection Server 接続で使用するように Deep Discovery Analyzer のプロキシ設定が指定されている場合は、[プロキシサーバを使用して接続する] を選択します。

注意

プロキシ設定を無効にすると、Smart Protection Server は Deep Discovery Analyzer に直接接続を行います。

c. (オプション) 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指定します。

d. (オプション) 組織で証明書失効リストを使用する場合は、[CRL (証明書失効リスト) を使用] を選択し、[参照] をクリックして証明書失効リストを指定します。

重要

Deep Discovery Analyzer では、Smart Protection Server 3.3 を使用している場合のみグローバルサービスへの接続をサポートします。

注意

Smart Protection ソースに [Smart Protection Server] を選択する場合、次のサービスと、それぞれの接続を確認する機能が有効になります。

- CSSS (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
- 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

5. [保存] をクリックします。

[ICAP] タブ

Deep Discovery Analyzer では、ICAP (Internet Content Adaptation Protocol) クライアントとの統合がサポートされます。ICAP クライアントは、分析のためにサンプルを Deep Discovery Analyzer に送信するプロキシサーバまたはネットワークストレージとして使用できます。ICAP クライアントは、Deep

Discovery Analyzer からの分析結果に基づいてサンプルに処理 (許可またはブロック) を実行します。

ICAP の統合後は、Deep Discovery Analyzer で次の機能を実行できるようになります。

- ICAP クライアントから送信されたサンプルを ICAP サーバとして分析する
- 指定したネットワーク動作 (URL アクセス/ファイルのアップロード/ファイルのダウンロード) がブロックされた場合に、ユーザ設定ページをエンドユーザに表示する
- ICAP クライアントリストを設定することで、サンプルを送信できる ICAP クライアントを制御する
- 選択した MIME コンテントタイプに基づいてファイルの検索をバイパスする
- 実際のファイルタイプに基づいてファイルの検索をバイパスする
- RESPMOD モードでの URL 検索をバイパスする
- さまざまな検索モジュールを使用してサンプルを検索する
- 仮想アナライザが処理できるファイルタイプに基づいてサンプル送信をフィルタする

Deep Discovery Analyzer は、次の ICAP の仕様をサポートしています。

プロトコル	ICAP モード	ICAP URL
ICAP	REQMOD	icap://<Deep Discovery Analyzer の IP アドレス>:1344/request
	RESPMOD	icap:// <Deep Discovery Analyzer の IP アドレス>:1344/response
ICAPS	REQMOD	icaps://<Deep Discovery Analyzer の IP アドレス>:11344/request
	RESPMOD	icaps://<Deep Discovery Analyzer の IP アドレス>:11344/response

ICAP には次のモードがあります。

- REQMOD (要求変更モード): URL やアップロードされたファイルを含め、HTTP 要求本文の内容を確認します。
- RESPMOD (応答変更モード): URL やダウンロードされたファイルを含め、HTTP 応答本文の内容を確認します。

Deep Discovery Analyzer との完全な互換性を確保するため、ICAP クライアントで要求変更モードと応答変更モードの両方を設定します。

ICAP を設定する

注意

ICAP の統合が有効な場合、Deep Discovery Analyzer は自動的に仮想アナライザのスループットを調節して、システムリソースの消費を抑えます。

手順

1. [管理] > [統合製品/サービス] > [ICAP] の順に選択します。
2. [ICAP を有効にする] を選択します。
3. [ICAP ポート番号] を入力します。

   初期設定値は 1344 です。
4. 安全な接続で ICAP クライアントに接続するには、[SSL 経由の ICAP を有効にする] を選択して、次の情報を指定します。
   - ICAPS ポート番号: 初期設定値は 11344 です
   - 証明書: 証明書には base64 エンコーディングを使用する必要があります
   - 秘密鍵: 秘密鍵には base64 エンコーディングを使用する必要があります

     重要

     暗号化された秘密鍵のみがサポートされます。

- パスフレーズ
- パスフレーズの確認入力

5. (オプション) [ヘッダ設定] セクションで、Deep Discovery Analyzer での ICAP ヘッダの処理方法を指定します。

   a. [Deep Discovery Analyzer からの ICAP ヘッダ] で、Deep Discovery Analyzer から ICAP クライアントに送信する ICAP ヘッダを選択します。

      詳細については、60 ページの「ICAP ヘッダの応答」を参照してください。

   b. [ICAP クライアントからの ICAP ヘッダ] で、Deep Discovery Analyzer が ICAP クライアントからヘッダを受信したときに保存する ICAP ヘッダを選択します。

6. (オプション) [検索設定] で、次のオプションを 1 つ以上選択します。

   - RESPMOD モードでの URL 検索のバイパス
   - YARA ルールを使用したサンプルの検索
   - 選択された不審オブジェクトリストを使用したサンプルの検索

     注意

     - 生成された不審オブジェクトリスト内の不審オブジェクトは Deep Discovery Analyzer の内部仮想アナライザによって追加されたものであるのに対し、同期された不審オブジェクトリスト内の不審オブジェクトは Deep Discovery Director から取得されたものです。
     - [同期された不審オブジェクトリスト] を選択した場合は、Deep Discovery Analyzer を Trend Micro Vision One と統合するか、Deep Discovery Director からの不審オブジェクトの同期を有効にする必要もあります。

       詳細については、195 ページの「Deep Discovery Director に登録する」を参照してください。

   - ユーザ指定の不審オブジェクトリストを使用したサンプルの検索

- 機械学習型検索エンジンを使用したサンプルの検索
- パスワード保護されたサンプルの分類

7. (オプション) [コンテンツ設定] で次の操作を実行します。

   a. [MIME コンテントタイプの除外を有効にする] を選択し、選択または指定した MIME コンテントタイプに基づいて検索からファイルを除外します。

   b. 送信されたサンプルの実際のファイルタイプを Deep Discovery Analyzer で検証するには、[MIME コンテントタイプの検証を有効にする] を選択します。

   注意

   - [MIME コンテントタイプの検証を有効にする] の設定は、[MIME コンテントタイプの除外を有効にする] を選択した場合にのみ適用されます。
   - このオプションを選択しても、Deep Discovery Analyzer では次のいずれかでサンプルの ICAP 事前検索が引き続き実行されます。
     - HTTP 圧縮
     - ICAP プレビューモードでの一部の MIME コンテントタイプ
     - カスタム MIME コンテントタイプ
     - 事前定義された一部の MIME コンテントタイプ

     サポートされていないファイルタイプのサンプルは、ICAP 事前検索の実行後、検索のために仮想アナライザに送信されることはありません。

8. (オプション) [ユーザ通知ページ] で [次のイベントに対して ICAP クライアントがネットワークトラフィックをブロックする場合はユーザ通知ページを使用する] を選択し、ページコンテンツを含むファイルを指定します。

注意

この設定により、特定のイベントに対して ICAP クライアントがネットワークトラフィックをブロックする場合は常に、Deep Discovery Analyzer でカスタムページを表示できるようになります。ただし、ICAP クライアントがこの設定を上書きする場合があります。設定が有効でもカスタムページが表示されない場合は、ICAP クライアントの設定と競合していないか確認してください。

Deep Discovery Analyzer では、次のイベントに対するカスタムページがサポートされます。

- URL アクセス
- ファイルのアップロード
- ファイルのダウンロード

注意

任意のテキストエディタを使用してページを作成し、プレーンテキストとして保存します。書式設定には HTML タグを使用できます。ファイルは 5MB 未満となるようにしてください。

9. (オプション) [ICAP クライアントリスト] で次の操作を実行します。

   a. 許可する [最大接続数] を指定します。

      初期設定値は `1000` です。

   b. [次の ICAP クライアントからのみ検索要求を受け入れる] を選択し、送信を特定のクライアントのみに限定します。

      - 新しい IP アドレスまたは IP アドレス範囲を追加するには、[追加] をクリックします。
      - 既存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。

      注意

      初期設定では、すべての ICAP クライアントが Deep Discovery Analyzer にサンプルを送信できます。

10. [保存] をクリックします。
11. ICAP の統合が Deep Discovery Analyzer で正しく機能していることを確認します。

    リスク高のサンプルの場合:

    - Deep Discovery Analyzer は ICAP クライアントに「HTTP 403 Forbidden」メッセージを返します。
    - [ユーザ通知ページ] 設定が有効な場合、Deep Discovery Analyzer はアップロードされたページをメッセージの一部に含めます。
    - X-Virus-ID ヘッダと X-Infection-Found ICAP ヘッダが有効な場合、Deep Discovery Analyzer はこれらのヘッダをメッセージ内に含めます。

    リスクのないサンプルの場合:

    - Deep Discovery Analyzer は ICAP クライアントから受信した元のメッセージを返します。
    - ICAP クライアントが ICAP の「204 No Content」をサポートしている場合は、元のメッセージを含めずに「204 No Content」応答を返します。

[Microsoft Active Directory] タブ

Deep Discovery Analyzer では、Microsoft Active Directory サーバとの統合がサポートされます。統合後は、Microsoft Active Directory アカウントを Deep Discovery Analyzer ユーザとして追加できるようになります。

Microsoft Active Directory を設定する

注意

Deep Discovery Analyzer では、Microsoft Active Directory 2012、2016、および 2019 との統合のみがサポートされます。

手順

1. [管理] > [統合製品/サービス] > [Microsoft Active Directory] の順に選択します。
2. [Microsoft Active Directory サーバを使用] を選択します。
3. サーバの種類を指定します。
4. プライマリ Microsoft Active Directory サーバについて、次の情報を指定します。
   - サーバアドレス
   - アクセスプロトコル
   - ポート番号
5. (オプション) [セカンダリサーバを有効にする] を選択します。

   プライマリ Microsoft Active Directory サーバにアクセスできなくなるとセカンダリサーバがバックアップとして機能します。
6. プライマリ Microsoft Active Directory サーバについて、次の情報を指定します。
   - 基本識別名
   - ユーザ名
   - パスワード
7. (オプション) プライマリサーバで証明書が必要な場合は、[CA 証明書を使用] を選択して必要な証明書を指定します。
8. (オプション) [接続テスト] をクリックして、プライマリ Microsoft Active Directory サーバへの接続をテストします。
9. [保存] をクリックします。

[SAML 認証] タブ

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 Analyzer 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 Analyzer アカウントなしで Deep Discovery Analyzer 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 Analyzer) 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 Analyzer 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
- Deep Discovery Director 5.3

組織の環境に Deep Discovery Analyzer 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 Analyzer 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。

   Deep Discovery Analyzer で証明書を更新することもできます。

   詳細については、212 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、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。

3. Deep Discovery Analyzer 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、213 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。

サービスプロバイダのメタデータと証明書

Deep Discovery Analyzer 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 Analyzer 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 Analyzer 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 Analyzer にアップロードします。

Deep Discovery Analyzer 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 Analyzer では、AD FS と Okta に 1 つずつ、最大で 2 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。

   注意

   Deep Discovery Analyzer では、[ログオン] 画面のドロップダウンリストに名前が表示されます。

   詳細については、30 ページの「シングルサインオンによるログオン」を参照してください。
5. 説明を入力します。
6. [選択] または [アップデート] 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 Analyzer 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 Analyzer 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 Analyzer 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 Analyzer 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 Analyzer」など Deep Discovery Analyzer 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 Analyzer 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 Analyzer 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、212 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. [Group Attribute Statements (Optional)] セクションで、次のように指定します。

- Name: DDAN_groups
- Filter: 正規表現^(.*)*$に一致

g. [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 Analyzer 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 Analyzer 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 Analyzer 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 Analyzer へのアクセスを許可するユーザを指定し、Deep Discovery Analyzer 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 Analyzer 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 Analyzer と連動させる方法について説明します。

注意

Deep Discovery Analyzer 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 Analyzer 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 Analyzer からメタデータファイルを取得している。
- 各エンドポイントで Web ブラウザが Deep Discovery Analyzer およびフェデレーションサーバを信頼するように設定されている。

  詳細については、220 ページの「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」を参照してください。

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 Analyzer 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 Analyzer」など Deep Discovery Analyzer 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、[ポリシー] でグループを 1 つ以上選択します。[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] タブで、[要求規則名] テキストボックスに要求規則名を指定し、[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、その属性の出力方向の要求の種類に [名前 ID] を指定します。

d. [OK] をクリックします。

表 6-5. LDAP 属性

要求規則名	LDAP 属性	出力方向の要求の種類
<ユーザ指定の規則名>	User-Principal-Name	**名前 ID**

6. 手順 3d で許可した、Deep Discovery Analyzer へのアクセス権を付与する Active Directory グループごとに設定を行います。

注意

- 次の手順は、Active Directory グループごとに [グループ メンバーシップを要求として送信] 規則を使用して設定する方法を示しています。子グループに属するユーザと、その子グループに関連付けられた親グループにアクセス権を付与する場合、子グループと親グループそれぞれに規則を作成する必要があります。
- 要件に基づいて設定をカスタマイズするには、[カスタム規則を使用して要求を送信] オプションを使用することをお勧めします。
- 出力方向の要求の種類を DDAN_groups に設定していることを確認します。

詳細については、https://success.trendmicro.com/jp/solution/000262468 を参照してください。

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] で、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「`DDAN_groups`」と入力します。

f. [出力方向の要求の値] で、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 6-6. 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>	DDAN_groups	<AD FS のユーザグループ名>

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 Analyzer にアクセスするには、Deep Discovery Analyzer 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 Analyzer 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。

メールでの送信

管理コンソールや Manual Submission Tool を使用してオブジェクトを送信できることに加えて、メールでの送信機能を有効にすると、不審なメールメッセージと添付ファイルを分析のために Deep Discovery Analyzer に送信できるようになります。

メールでの送信プロセスの概要は次のとおりです。

1. ユーザが不審な添付ファイルが含まれるメールメッセージを Deep Discovery Analyzer に送信します。
2. Deep Discovery Analyzer がそのメールメッセージを受信し、メールの内容と添付ファイルを検索します。
3. 分析の完了後、Deep Discovery Analyzer は次の項目を含むメール通知をユーザに送信します。
   - 分析結果のサマリー
   - 詳細な分析レポート

メールでの送信を設定する

手順

1. [管理] > [統合製品/サービス] の順に選択し、[メールでの送信] タブをクリックします。
2. [メールでの送信を有効にする] を選択します。

注意

メールでの送信機能を無効にすると、仮想アナライザで現在処理中のサンプルについて、分析結果を含むメール通知が Deep Discovery Analyzer から送信されなくなります。

3. [一般] セクションで、Deep Discovery Analyzer がメールメッセージの受信と分析結果通知の送信に使用するメールアドレスを指定します。初期設定は `911@ddan.com` です。
4. [メール送信者] セクションで、Deep Discovery Analyzer への分析用メールメッセージの送信を許可するユーザドメインと SMTP サーバを指定します。
   - 許可されたドメイン: ドメインを入力して <Enter> キーを押します。最大 5 件のドメインを追加できます。
   - 許可された SMTP サーバ: SMTP サーバアドレスを入力して <Enter> キーを押します。最大 5 件のサーバアドレスを指定できます。

     Deep Discovery Analyzer で、SMTP サーバの次の設定を行います。
     - ポート: サーバのポート番号を入力します。初期設定は 25 です。この設定は必須です。
     - SSL/TLS: [SSL/TLS を有効にする] を選択して、サーバへの安全な接続を確立します。次に、必要な証明書ファイルと秘密鍵ファイル、およびパスフレーズを選択します。
5. [メール通知] セクションで、Deep Discovery Analyzer が分析結果を含むメール通知の送信に使用する SMTP サーバを設定します。
   a. 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。
   b. SMTP サーバで使用するポート番号を入力します。
   c. 接続に使用するセキュリティの種類を選択します。
   d. サーバで認証が必要な場合は、[SMTP サーバの認証を使用する] を選択してユーザ名とパスワードを指定します。
   e. (オプション) [接続テスト] をクリックして、SMTP サーバへの接続をテストします。

6. メール通知テンプレートのメールの件名とメッセージの内容を指定します。

   ヒント

   通知メールでは、「%RiskLevel%」トークンと「%Subject%」トークンを使用できます。

7. [保存] をクリックします。

[Syslog] タブ

Deep Discovery Analyzer には、次の概要を提供するシステムログが保持されます。

- 仮想アナライザの分析ログ
- 統合製品検出ログ
- ICAP 事前検索ログ
- システムイベント
- アラートイベント

[管理] > [統合製品/サービス] > [Syslog] タブで、Deep Discovery Analyzer から複数の Syslog サーバにログを送信するように設定します。

Syslog を設定する

Deep Discovery Analyzer では、ログをデータベースに保存した後、複数の Syslog サーバに転送できます。

注意

- Deep Discovery Analyzer では、最大 3 件の Syslog サーバを設定してログを転送できます。
- 転送されるのは、この設定を有効にした後に保存されたログのみです。

手順

1. [管理] > [統合製品/サービス] > [Syslog] の順に選択します。

   [Syslog 設定] 画面が表示されます。

2. 次のいずれかを実行します。

   - 新しい Syslog サーバを追加するには、[追加] をクリックします。
   - 既存の Syslog サーバの詳細を更新するには、その Syslog サーバの名前をクリックします。

3. 表示される画面で、プロファイルの [ステータス] を指定します。

4. Syslog サーバの [プロファイル名] と [サーバアドレス] を入力します。

5. ポート番号を入力します。

   注意

   次の初期設定の Syslog ポートを使用することをお勧めします。

   - UDP: 514
   - TCP: 601
   - SSL: 443

6. ログコンテンツの Syslog サーバへの転送時に使用するプロトコルを選択します。

   - UDP
   - TCP
   - SSL

7. イベントログの Syslog サーバへの送信時に使用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. Syslog サーバに送信するログの範囲を選択します。
   - 仮想アナライザの分析ログ
   - 統合製品検出ログ
   - ICAP 事前検索ログ
   - システムイベントログ
   - アラートイベントログ
9. (オプション) Syslog サーバへの送信から除外するログを選択します。
10. [保存] をクリックします。

システム設定

[管理] > [システム設定] にある[システム設定] 画面には次のタブがあります。

- 226 ページの「[ネットワーク] タブ」
- 230 ページの「[プロキシ] タブ」
- 232 ページの「[SMTP] タブ」
- 233 ページの「[時間] タブ」
- 234 ページの「[SNMP] タブ」
- 238 ページの「[パスワードポリシー] タブ」
- 238 ページの「[セッションタイムアウト] タブ」

- 239 ページの「[クラスタ] タブ」
- 256 ページの「[高可用性] タブ」
- 257 ページの「[HTTPS 証明書] タブ」

[ネットワーク] タブ

この画面を使用して、Deep Discovery Analyzer アプライアンスのホスト名、IPv4 アドレス、および IPv6 アドレスと、TLS 1.2 の適用を含めたその他のネットワーク設定を行います。

IPv4 アドレスは必須で、初期設定は `192.168.252.2` です。IPv4 アドレスは、すべての配置タスクを完了した後すぐに変更してください。

Deep Discovery Analyzer は、Trend Micro Smart Protection Network、アップデートサーバ、Threat Connect などのトレンドマイクロがホストするサービスにアクセスするときには、指定された IP アドレスを使用してインターネットに接続します。IP アドレスによって、管理コンソールにアクセスするための URL も決まります。

[常に TLS 1.2 を使用する] を選択すると、Deep Discovery Analyzer での受信および送信接続のデータセキュリティを強化できます。

注意

- Payment Card Industry Data Security Standard (PCI-DSS) v3.2 に準拠するには、アプライアンスはすべての受信および送信接続に TLS 1.2 のみを使用する必要があります。
- このオプションを設定する前に、Deep Discovery Analyzer アプライアンスが高可用性クラスタで使用されていないことを確認します。[管理] > [システム設定] > [クラスタ] で、クラスタからパッシブなプライマリアプライアンスをデタッチしてください。
- 統合製品およびサービスが TLS 1.2 をサポートする最新バージョンを使用していることを確認してください。詳細については、329 ページの統合製品/サービスでの TLS 1.2 のサポートを参照してください。
- 次の製品/サービスが TLS 1.2 を使用するように設定されていることを確認します。
  - [管理] > [アップデート] > [コンポーネントのアップデート設定] のアップデートサーバは、HTTPS を使用する必要があります。
  - [管理] > [統合製品/サービス] > [ICAP] の ICAP 設定は、SSL 経由の ICAP を使用する必要があります。
  - [管理] > [統合製品/サービス] > [Syslog] の Syslog サーバは、SSL を使用する必要があります。
  - [管理] > [システム設定] > [SMTP] の SMTP サーバは、SSL/TLS または STARTTLS を使用する必要があります。

次の表は、設定の制限を示しています。

表 6-7. 設定の制限

フィールド	制限事項
ホスト名	高可用性を使用している場合は変更できません。
IPv4 アドレス	• IPv4 仮想アドレスとは異なる必要があります。 • IPv4 仮想アドレスと同じネットワークセグメント内に存在している必要があります。

フィールド	制限事項
IPv6 アドレス	• IPv6 仮想アドレスとは異なる必要があります。 • IPv6 仮想アドレスと同じネットワークセグメント内に存在している必要があります。 • IPv6 仮想アドレスが設定されている場合は削除できません。 • 高可用性を使用している場合は追加または削除できません。

[ネットワークインタフェース] タブ

[ネットワークインタフェース] 画面では次の操作を実行できます。

- ネットワークインタフェースのステータスを確認する。
- ポートを設定する。

  詳細については、228 ページの「ポートを設定する」を参照してください。
- NIC チーミングを設定する。

  詳細については、229 ページの「NIC チーミングを設定する」を参照してください。

ポートを設定する

手順

1. [管理] > [システム設定] > [ネットワークインタフェース] の順に選択します。
2. [ポートリスト] セクションの設定を行います。
   - 選択したインタフェースで [管理ポート] を設定するには、ドロップダウンリストからオプションを選択します。Deep Discovery Analyzer の初期設定では、eth0 インタフェースが管理ポートに使用されます。

- サンドボックス分析に使用するインタフェースのポートを設定するには、[編集] をクリックします。
- 高可用性ポートの詳細情報を表示するには、[詳細の表示] をクリックします。

3. [保存] をクリックします。
4. ネットワークサービスを再起動するように求められたら、[はい] をクリックします。

   ネットワークサービスが再起動します。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。

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 Analyzer では、最大 2 つの NIC チームがサポートされます。1 つの NIC チームには、2 つのネットワークインタフェースカードをグループ化する必要があります。

手順

1. [管理] > [システム設定] > [ネットワークインタフェース] 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. 接続モード ([アクティブ/バックアップ] または [LACP]) を選択します。

注意

[LACP] を選択した場合は、LACP (Link Aggregation Control Protocol) を使用した通信を有効にするため、ターゲットスイッチでも必要な設定を行う必要があります。

たとえば NIC チームに管理ポートが含まれており、LACP を使用した管理ポートとして機能する場合、ターゲットスイッチで必要な設定が行われるまで、Deep Discovery Analyzer はそのスイッチへの通信を確立できません。

c. 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 2 つ選択します。

注意

- 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。
- NIC チームに管理ポート (`eth0`) とネットワークポート (`eth1`) が含まれる場合、この NIC チームは管理ポートとして機能します。この NIC チームを無効にすると、`eth0` または `eth1` のいずれかが管理ポートになります。

3. [保存] をクリックします。
4. ネットワークサービスを再起動するように求められたら、[はい] をクリックします。

   ネットワークサービスが再起動します。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。

[プロキシ] タブ

Deep Discovery Analyzer がプロキシサーバ経由でインターネットまたは管理ネットワークに接続する場合は、プロキシ設定を行います。

次の設定を行います。

表 6-8. [プロキシ] タブのタスク

タスク	手順
HTTP プロキシサーバを使用する	プロキシ設定を有効化するにはこのオプションを選択します。
サーバ名または IP アドレス	プロキシサーバのホスト名、IPv4 アドレス、または IPv6 アドレスを入力します。 管理コンソールでは、ホスト名にダブルバイトでエンコードされた文字は使用できません。ホスト名にこのような文字が含まれる場合は、代わりに IP アドレスを入力してください。
ポート番号	Deep Discovery Analyzer がプロキシサーバの接続に使用するポート番号を入力します。
プロキシサーバへの接続に認証を使用	プロキシ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。Deep Discovery Analyzer では次の認証方法がサポートされます。 • 認証なし • 基本認証 • ダイジェスト認証 • NTLMv1 認証
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、[プロキシサーバへの接続に認証を使用] が有効な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、[プロキシサーバへの接続に認証を使用] が有効な場合のみ使用できます。

[SMTP] タブ

Deep Discovery Analyzer では、メールで通知を送信するときに SMTP 設定を使用します。

手順

1. [管理] > [システム設定] の順に選択し、[SMTP] タブをクリックします。
2. 次の情報を指定します。

   表 6-9. [SMTP] タブのタスク

フィールド	手順
サーバアドレス	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。 管理コンソールでは、ホスト名にダブルバイトでエンコードされた文字は使用できません。ホスト名にこのような文字が含まれる場合は、代わりに IP アドレスを入力してください。
ポート番号	SMTP サーバで使用するポート番号を入力します。
接続のセキュリティ	接続に使用するセキュリティの種類を指定します。 指定できる値は「なし」、「STARTTLS」、または「SSL/TLS」です。
送信者のメールアドレス	送信者のメールアドレスを入力します。
SMTP サーバの接続に認証を使用	サーバで認証が必要な場合は、[SMTP サーバの接続に認証を使用] を選択してユーザ名とパスワードを指定します。 警告! SMTP サーバ上の有効なユーザ名とパスワードを指定してください。ユーザ名とパスワードが正しくない場合、一部の SMTP サーバにおいて、Deep Discovery Analyzer サーバからの通信が拒否されることがあります。

3. (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 Analyzer 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。

4. [保存] をクリックします。

[時間] タブ

インストール後すぐに日付と時間を設定します。

手順

1. [管理] > [システム設定] の順に選択し、[時間] タブをクリックします。

   [時間] 画面が表示されます。

2. [日時の設定] をクリックします。

   設定パネルが表示されます。

3. 次の方式のいずれかを選択して、適切な設定を行います。

   - [NTP サーバに接続] を選択し、NTP 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。
   - [手動で設定] を選択し、時間を設定します。

4. [保存] をクリックします。

5. [タイムゾーンの設定] をクリックします。

   設定パネルが表示されます。

6. 適切なタイムゾーンを選択します。

注意

適用可能な場合は、夏時間 (DST) が使用されます。

7. [保存] をクリックします。
8. [形式の設定] をクリックします。

   設定パネルが表示されます。
9. 希望の日時の形式を選択します。
10. [保存] をクリックします。

[SNMP] タブ

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 Analyzer 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、234 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、236 ページの「SNMP 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。
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。 • 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) MD5 認証プロトコル: `HMAC-MD5` • (オプション) DES 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	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	ユーザ名を指定します。
パスワード	パスワードを指定します。
プライバシーパスフレーズ	プライバシーパスフレーズを指定します。

注意

最初に同じ SNMP のバージョン、コミュニティ名、セキュリティモデル、ユーザ名、パスワード、およびプライバシーパスフレーズを使用して SNMP サーバを設定してからアプライアンスを設定します。

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 Analyzer 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、297 ページの SNMP オブジェクト ID を参照してください。

SNMP 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 Analyzer 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。

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。 • 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) MD5 認証プロトコル: `HMAC-MD5` • (オプション) DES 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	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	ユーザ名を指定します。
パスワード	パスワードを指定します。
プライバシーパスフレーズ	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 32 個まで指定します。

注意

最初に同じ SNMP のバージョン、コミュニティ名、セキュリティモデル、ユーザ名、パスワード、およびプライバシーパスフレーズを使用して SNMP サーバを設定してからアプライアンスを設定します。

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 Analyzer 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、297 ページの SNMP オブジェクト ID を参照してください。

[パスワードポリシー] タブ

強力なパスワードを要求することをお勧めします。通常、強力なパスワードには、大文字、小文字、数字および記号を組み合わせ、長さは 8 文字以上にします。

強力なパスワードが求められる場合は、ユーザが新しいパスワードを送信すると、パスワードポリシーによってそのパスワードが社内で設定された要件に合致するかどうかが判定されます。

パスワードポリシーが厳重であると、覚えておくのが困難なパスワードの選択をユーザに強制するために、組織内のコストが増加する場合があります。ユーザはパスワードを忘れた場合にヘルプデスクに問い合わせたり、パスワードを記録したりするので、脅威に対する脆弱性が増加します。このため、パスワードポリシーを設定する場合は、セキュリティ強度の必要性とユーザにとって遵守が容易なポリシーにすることのバランスをとる必要があります。

[セッションタイムアウト] タブ

管理コンソールの [ログオン] 画面で、初期設定または延長セッションのタイムアウトを選択できます。

初期設定のセッションタイムアウトは 10 分で、延長セッションのタイムアウトは 1 日です。これらの値は、必要に応じて変更できます。新しい値は次回のログオン時に有効になります。

[クラスタ] タブ

複数のスタンドアロン Deep Discovery Analyzer アプライアンスを配置および設定して 1 つのクラスタを形成することで、フォールトトレランス、パフォーマンスの向上、またはそれらの両方を実現できます。

ご使用環境の要件と使用可能な Deep Discovery Analyzer アプライアンスの数に応じて、次のクラスタ設定を使用できます。

表 6-10. クラスタ設定

クラスタ設定	説明
高可用性クラスタ	高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。
負荷分散クラスタ	負荷分散クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。 注意 Deep Discovery Analyzer のすべての機能が負荷分散環境で正しく動作するように、プライマリアプライアンスとセカンダリアプライアンスが互いに通信できることを確認してください。

クラスタ設定	説明
負荷分散機能を備えた高可用性クラスタ	負荷分散機能を備えた高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして、その他の追加のアプライアンスがセカンダリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスとして役割を引き継ぎます。セカンダリアプライアンスはパフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。

詳細については、「Deep Discovery Analyzer インストールガイド」を参照してください。

次の表は、使用可能な設定モードと関連付けられたアプライアンスの動作を示しています。

表 6-11. クラスタ設定モード

設定モード	説明
プライマリ (アクティブ)	• 管理コンソールに完全にアクセスできます。 • すべての設定を保持します。
プライマリ (パッシブ)	• 管理コンソールにアクセスできません。 • アクティブなプライマリアプライアンスの設定に基づいて自動的に設定されます。 • スタンバイ状態 • アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、アクティブなプライマリアプライアンスとして役割を引き継ぎます。 • 送信を処理しません。

設定モード	説明

セカンダリ	• アクティブなプライマリアプライアンスの設定に基づいて自動的に設定されます。
	• IP アドレスまたは仮想 IP アドレスを使用してアクティブなプライマリアプライアンスを特定します。
	• パフォーマンス向上のため、アクティブなプライマリアプライアンスによって割り当てられた送信を処理します。
	• 管理コンソールには設定可能な設定を含む画面のみが表示されます。アクセス可能な画面は次のとおりです。
	  • [仮想アナライザ] > [サンドボックス管理] > [ネットワーク接続]
	  • [仮想アナライザ] > [サンドボックス管理] > [macOS 向けサンドボックス]
	  • [管理] > [アップデート] > [HotFix/Patch]
	  • [管理] > [アップデート] > [ファームウェア]
	  • [管理] > [統合製品/サービス] > [SAML 認証]
	  • [管理] > [システム設定] > [ネットワーク]
	  • [管理] > [システム設定] > [ネットワークインタフェース]
	  • [管理] > [システム設定] > [HTTPS 証明書]
	  • [管理] > [システム設定] > [クラスタ]
	  • [管理] > [アカウント/連絡先] > [アカウント]
	  • [管理] > [システムログ]
	  • [管理] > [システムメンテナンス] > [ネットワークサービス診断]
	  • [管理] > [システムメンテナンス] > [電源オフ/再起動]
	  • [管理] > [システムメンテナンス] > [デバッグ]
	  • [管理] > [ライセンス]

注意

負荷分散クラスタまたは負荷分散を行う高可用性クラスタを使用する環境では、Deep Discovery Analyzer はアクティブなプライマリアプライアンス上で仮想アナライザのスループットを自動的に調節して、システムリソースの消費を抑えます。

[ノード] リスト

[ノード] リストはアクティブなプライマリアプライアンスに表示されます。

[ノード] リストには、次の情報が含まれます。

表 6-12. [ノード] リストの列

列	説明
ステータス	アプライアンスの接続ステータス。ステータスアイコンの上にマウスを重ねると詳細が表示されます。
モード	アプライアンスのクラスタモード。
管理 IP アドレス	アプライアンスの管理 IP アドレス。
ホスト名	アプライアンスのホスト名。
前回の接続	アプライアンスがアクティブなプライマリアプライアンスに最後に接続した日時。 **注意** アプライアンスがパッシブなプライマリアプライアンスである場合、データはありません (ダッシュで表示)。
詳細	アプライアンスの動作ステータスの詳細情報。 • スタンドアロンアプライアンスの場合: • スタンドアロンアプライアンス: アプライアンスはスタンドアロンアプライアンスです。 • パッシブなプライマリアプライアンスの場合:

列	説明
	• 完全同期: パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスと完全に同期されています。 • n%同期しています: パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスから設定を同期しています。 • 同期エラー: パッシブなプライマリアプライアンスからアクティブなプライマリアプライアンスに接続できません。アプライアンスが eth3 を使用して直接接続されており、eth3 がサンドボックス分析に使用されていないことを確認してください。 ヒント このフィールドには、接続の遅延とスループットの情報も表示されます。 • セカンダリアプライアンスの場合: • 一致しないコンポーネントバージョン: アクティブなプライマリアプライアンスとセカンダリアプライアンスの 1 つ以上のコンポーネントのバージョンが異なります。すべてのアプライアンスで同じコンポーネントのバージョンを使用してください。 • 接続なし: アクティブなプライマリアプライアンスが、過去 10 秒間にセカンダリアプライアンスから接続ステータスに関する情報を受信しませんでした。セカンダリアプライアンスの電源がオンになっており、アクティブなプライマリアプライアンスにネットワーク経由で接続できることを確認してください。 • 無効な API キー: セカンダリアプライアンスが無効な API キーで設定されています。セカンダリアプライアンスの [アクティブなプライマリ API キー] を確認してください。 • 互換性がないソフトウェアバージョン: アクティブなプライマリアプライアンスとセカンダリアプライアンスのファームウェア、HotFix、および Patch のバージョンが異なります。すべてのアプライアンスで同じファームウェア、HotFix、および Patch のバージョンを使用してください。

列	説明
	• 予期しないエラー: 予期しないエラーが発生しました。問題が解決しない場合は、テクニカルサポートにお問い合わせください。
処理	アプライアンスモードとステータスに応じて実行可能な処理。 • アクティブなプライマリアプライアンスの場合: • スワップ: プライマリアプライアンスの役割をスワップします。現在のパッシブなプライマリアプライアンスをプライマリモード (アクティブ) に設定し、現在のアクティブなプライマリアプライアンスをプライマリモード (パッシブ) に設定します。パッシブなプライマリアプライアンスがアクティブなプライマリアプライアンスからすべての設定を同期したときに表示されます。詳細については、249 ページの「アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスをスワップする」を参照してください。 • パッシブなプライマリアプライアンスの場合: • デタッチ: パッシブなプライマリアプライアンスをデタッチします。高可用性が無効になり、パッシブなプライマリアプライアンスがスタンドアロンアプライアンスとして使用可能になります。パッシブなプライマリアプライアンスがアクティブなプライマリアプライアンスからすべての設定を同期したときに表示されます。詳細については、249 ページの「クラスタからパッシブなプライマリアプライアンスをデタッチする」を参照してください。 • 削除: アクセスできないパッシブなプライマリアプライアンスを削除します。高可用性を無効にします。アクティブなプライマリアプライアンスが eth3 経由でパッシブなプライマリアプライアンスに接続できない場合に表示されます。詳細については、250 ページの「クラスタからパッシブなプライマリアプライアンスを削除する」を参照してください。 • セカンダリアプライアンスの場合: • 削除: アクセスできないセカンダリアプライアンスを削除します。オブジェクトの処理能力に影響します。セカンダリアプライアンスは 10 秒ごとにアクティブなプライマリアプライアンスへの接続を試行します。アクティブなプライマリアプライアンスがセカンダリアプライア

列	説明
	ンスから 1 分間接続ステータスに関する情報を受信しない場合に表示されます。詳細については、253 ページの「クラスタからセカンダリアプライアンスを削除する」を参照してください。

[更新] をクリックして、[ノード] リスト内の情報を更新します。

クラスタにパッシブなプライマリアプライアンスを追加する

次の表は、パッシブなプライマリアプライアンスをクラスタに追加する前に、アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスの両方が満たす必要のある要件を示しています。

表 6-13. 高可用性クラスタリングの要件

要件	説明
ハードウェアモデル	ハードウェアモデル (1100 または 1200) が同じである必要があります。

要件	説明

物理的な接続	eth3 を使用して相互に直接接続することをお勧めします。
	
	重要
	高可用性を使用する場合、eth3 は、2 つの同一のアプライアンスを接続するために使用します。管理ポート、外部ネットワーク接続、NIC チーム内のメンバーポートなど、その他の目的で使用することはできません。
	
	注意
	異なるデータセンター内に配置されているなど、アクティブなプライマリアプライアンスがパッシブなプライマリアプライアンスに直接接続されていない場合は、次の要件を満たす必要があります。
	• アプライアンスが Deep Discovery Analyzer 1100 または 1200 である
	• アプライアンス間の接続が次の条件を満たしている
	  • ネットワークの遅延が 15 ミリ秒未満
	  • パケット損失率が 0.000001%未満
	  • ネットワーク帯域幅が 240Mbps より大きい

ファームウェア、HotFix、および Patch のバージョン	同じである必要があります。
ホスト名	異なる必要があります。
IP アドレス	対称的である必要があります。 • アクティブなプライマリアプライアンスで IPv4 アドレスのみが設定されている場合、パッシブなプライマリアプライアンスで IPv4 アドレスと IPv6 アドレスの両方を設定することはできません。 • アクティブなプライマリアプライアンスで IPv4 アドレスと IPv6 アドレスが設定されている場合、パッシブなプライマリアプライアンスで IPv4 アドレスのみを設定することはできません。

要件	説明
ネットワークセグメント	同じネットワークセグメント内に存在している必要があります。
仮想 IP アドレス	アクティブなプライマリアプライアンスで設定されている必要があります。
管理ポート	同じネットワークポートを使用する必要があります。
仮想アナライザ用の外部接続ポート	同じネットワークポートを使用する必要があります。
NIC チーミング	設定されている場合、同じ NIC チーミングポートと接続の種類を使用する必要があります。

高可用性クラスタでは、1 つのアプライアンスがアクティブなプライマリアプライアンスとして、もう 1 つのアプライアンスがパッシブなプライマリアプライアンスとして機能します。アクティブなプライマリアプライアンスでエラーが発生し回復できない場合、パッシブなプライマリアプライアンスは新しいアクティブなプライマリアプライアンスとして役割を自動的に引き継ぎます。

注意

- ネットワークに Trend Micro Apex Central が設定されている場合は、プライマリアプライアンス (高可用性クラスタの場合、仮想 IP アドレス) を Apex Central に登録してください。
- 高可用性を使用する場合は、仮想 IP アドレスを使用して登録してください。

手順

1. 「Deep Discovery Analyzer インストールガイド」の説明に従って、インストールおよび配置タスクを実行します。
2. パッシブなプライマリアプライアンスを設定します。
   a. パッシブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
   b. [プライマリモード (パッシブ)] を選択します。

c. [アクティブなプライマリ IP アドレス] にアクティブなプライマリアプライアンスの IPv4 アドレスまたは IPv6 アドレスを入力します。

d. [接続テスト] をクリックします。

e. [保存] をクリックします。

アプライアンスのスタンバイ画面にリダイレクトされます。

- パッシブなプライマリアプライアンスで実行していたオブジェクトの処理は停止されます。
- パッシブなプライマリアプライアンスはアクティブなプライマリアプライアンスからすべての設定を同期します。同期が完了するまでの時間はアプライアンスモデルによって異なります。

重要

アプライアンスの同期中は次のタスクを実行できません。

- アクティブなプライマリアプライアンスとしての役割の引き継ぎ
- 別のモードへの切り替え

- パッシブなプライマリアプライアンスの管理コンソールにアクセスすることはできません。アプライアンスの管理と同期ステータスの監視は、アクティブなプライマリアプライアンスの管理コンソールから実行してください。
- 高可用性クラスタへの Deep Discovery Analyzer の配置後は、次の設定を変更することはできません。
  - NIC チーミング
  - 管理ポート
  - 外部ネットワーク接続

アクティブなプライマリアプライアンスとパッシブなプライマリアプライアンスをスワップする

プライマリアドレスをスワップすると、現在のパッシブなプライマリアプライアンスがプライマリモード (アクティブ) に設定され、現在のアクティブなプライマリアプライアンスがプライマリモード (パッシブ) に設定されます。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
2. [スワップ] をクリックして、プライマリアプライアンスをスワップします。

クラスタからパッシブなプライマリアプライアンスをデタッチする

パッシブなプライマリアプライアンスをデタッチすると、高可用性が無効になり、アプライアンスをスタンドアロンアプライアンスとして使用できるようになります。パッシブなプライマリアプライアンスがデタッチされると、ノードリストに表示されなくなります。

製品をアップデートまたはアップグレードするには、パッシブなプライマリアプライアンスをデタッチします。

重要

パッシブなプライマリアプライアンスをデタッチしても、アプライアンスの設定はリセットされません。スタンドアロンアプライアンスとして使用する場合は、アプライアンスを再インストールすることをお勧めします。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。

2. [デタッチ] をクリックして、クラスタからパッシブなプライマリアプライアンスをデタッチします。

クラスタからパッシブなプライマリアプライアンスを削除する

切断されたまたは異常な状態のパッシブなプライマリアプライアンスをクラスタから削除すると、ノードリスト内の混乱が緩和されます。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
2. ノードリストのパッシブなプライマリアプライアンスの横に [削除] が表示されるまで待機します。
3. [削除] をクリックして、クラスタからパッシブなプライマリアプライアンスを削除します。

注意

パッシブなプライマリアプライアンスは、アクティブなプライマリアプライアンスに再接続されると自動的にクラスタに再結合されます。

クラスタにセカンダリアプライアンスを追加する

セカンダリアプライアンスのファームウェア、HotFix、および Patch のバージョンがアクティブなプライマリアプライアンスと同じであることを確認します。

アプライアンスのファームウェア、HotFix、および Patch のバージョンを表示するには、284 ページの「バージョン情報」を参照してください。

必要に応じてアプライアンスのファームウェア、HotFix、および Patch のバージョンをアップデートまたはアップグレードします。詳細については、182 ページの「アップデート」を参照してください。

注意

- ネットワークに Trend Micro Apex Central が設定されている場合は、プライマリアプライアンス (高可用性クラスタの場合、仮想 IP アドレス) を Apex Central に登録してください。
- 高可用性を使用する場合は、仮想 IP アドレスを使用して登録してください。

手順

1. 「Deep Discovery Analyzer インストールガイド」の説明に従って、インストールおよび配置タスクを実行します。
2. セカンダリアプライアンスを設定します。
   a. セカンダリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
   b. [セカンダリモード] を選択します。
   c. [アクティブなプライマリ IP アドレス] にアクティブなプライマリアプライアンスの IPv4 アドレスまたは IPv6 アドレスを入力します。

      注意

      高可用性を使用している場合は、IPv4 仮想アドレスまたは IPv6 仮想アドレスを入力してください。

   d. [アクティブなプライマリ API キー] にアクティブなプライマリアプライアンスの API キーを入力します。
   e. [接続テスト] をクリックします。

      ヒント

      セカンダリアプライアンスでは、アクティブなプライマリアプライアンスへの接続をいつでもテストできます。接続の問題について詳細情報を確認するには、[接続テスト] をクリックします。

   f. [保存] をクリックします。
3. (オプション) セカンダリアプライアンスで追加の設定を実行します。

a. サンドボックスのネットワーク接続を設定します。

詳細については、127 ページの「外部接続を有効にする」を参照してください。

注意

アクティブなプライマリアプライアンスの外部ネットワーク接続設定を使用することをお勧めします。

b. [macOS 向けサンドボックス] を設定します。

詳細については、131 ページの「[macOS 向けサンドボックス] タブ」を参照してください。

c. アプライアンスのネットワークを設定します。

詳細については、226 ページの「[ネットワーク] タブ」を参照してください。

d. アカウントを追加します。

詳細については、262 ページの「[アカウント] タブ」を参照してください。

注意

セカンダリアプライアンスは、アクティブなプライマリアプライアンスのサンドボックス割り当ての割合に基づいてサンドボックスインスタンスを自動的に配信します。次の表は、設定の例を示しています。

表 6-14. 2 つのイメージを使用した設定例

アプライアンスの種類	Deep Discovery Analyzer ハードウェアモデル	インスタンスの最大数 (合計)	Windows 7 インスタンスの数	Windows 8.1 インスタンスの数
プライマリアプライアンス	1200 または 1100	60	40	20
セカンダリアプライアンス	1200 または 1100	60	40	20

クラスタからセカンダリアプライアンスを削除する

クラスタから切断されたセカンダリアプライアンスを削除すると、アクティブなプライマリアプライアンスのノードリストやウィジェットの混雑が緩和されます。

手順

1. アクティブなプライマリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
2. ノードリストのセカンダリアプライアンスの横に [削除] が表示されるまで待機します。

注意

セカンダリアプライアンスは 10 秒ごとにアクティブなプライマリアプライアンスへの接続を試行します。アクティブなプライマリアプライアンスが 1 分以内に接続ステータスに関するメッセージを受信しない場合、[ノード] リストのセカンダリアプライアンスの横に [削除] が表示されます。

セカンダリアプライアンスは、アクティブなプライマリアプライアンスに再接続されると自動的にクラスタに再結合されます。

3. [削除] をクリックして、クラスタからセカンダリアプライアンスを削除します。

   セカンダリアプライアンスがアクティブなプライマリアプライアンスのノードリストとウィジェットから削除されます。

アクティブなプライマリアプライアンスをセカンダリアプライアンスで置き換える

アクティブなプライマリアプライアンスが応答を停止しているか復元できず、さらにパッシブなプライマリアプライアンスも配置されていない場合は、同じクラスタ内のセカンダリアプライアンスで置き換えることができます。

ヒント

トレンドマイクロ 高可用性のため、パッシブなプライマリアプライアンスを配置することをお勧めします。詳細については、245 ページの「クラスタにパッシブなプライマリアプライアンスを追加する」を参照してください。

重要

応答を停止したときにアクティブなプライマリアプライアンスで分析されていた送信には結果は表示されません。

手順

1. アクティブなプライマリアプライアンスの電源をオフにします。
2. 同じクラスタからセカンダリアプライアンスを選択し、新しいアクティブなプライマリアプライアンスとして設定します。
   a. セカンダリアプライアンスの管理コンソールで、[管理] > [システム設定] の順に選択し、[クラスタ] タブをクリックします。
   b. [プライマリモード (アクティブ)] を選択します。
   c. [保存] をクリックします。
3. 新しいアクティブなプライマリアプライアンスの IP アドレスを設定します。

詳細については、226 ページの「[ネットワーク] タブ」を参照してください。

注意

元のアクティブなプライマリアプライアンスと同じ IP アドレスを使用することをお勧めします。これにより、セカンダリアプライアンスと統合製品を再設定せずに接続できます。

4. 新しいアクティブなプライマリアプライアンス上で設定を確認します。

注意

設定がセカンダリアプライアンスに適用されるまで最大 1 日かかります。

高可用性クラスタのアプライアンスを移動する

重要

高可用性クラスタのアプライアンスを別の場所に移動する場合は、常にパッシブノードの電源を最初にオフにし、電源を投入する際は最後にオンにします。

手順

1. パッシブなプライマリアプライアンスの電源をオフにします。
2. [管理] > [システムメンテナンス] > [電源オフ/再起動] タブでアクティブなプライマリアプライアンスの電源をオフにします。
3. 両方のアプライアンスを新しい場所に移動します。
4. eth0 を使用して各アプライアンスを管理ネットワークに接続します。
5. eth3 を使用して両方のアプライアンスを相互に直接接続します。
6. アクティブなプライマリアプライアンスの電源をオンにします。
7. パッシブなプライマリアプライアンスの電源をオンにします。

高可用性クラスタの IP セグメントを変更する

管理コンソールでは、同じネットワークセグメントにある場合のみ仮想 IP アドレスと管理 IP アドレスを変更できます。ただし、IP アドレスを別のネットワークセグメントに移動する必要がある場合は、ノードをデタッチし、再設定してから、再度セットアップする必要があります。

手順

1. パッシブなプライマリアプライアンスをデタッチします。
2. アクティブなプライマリアプライアンスの UI で、仮想 IP アドレスを削除し、新しいネットワークセグメントの IP アドレスに一致するように管理 IP アドレスと仮想 IP アドレスを設定します。
3. パッシブなプライマリアプライアンスの UI で、新しいネットワークセグメントの IP アドレスに一致するように管理 IP アドレスを設定します。
4. パッシブなプライマリアプライアンスをクラスタに再度追加します。

[高可用性] タブ

高可用性設定でアプライアンスを使用する場合は、IPv4 および IPv6 仮想アドレスを指定します。IPv4 および IPv6 仮想アドレスは、統合製品に設定用の固定 IP アドレスを提供するとともに、管理コンソールにアクセスする URL を特定するために使用されます。

仮想 IP アドレスにはアプライアンスの元の IP アドレスを使用することをお勧めします。そうすることで、統合製品で設定を変更することなく引き続き Deep Discovery Analyzer にオブジェクトを送信できます。

[仮想アナライザ用の外部接続が使用できなくなった場合、パッシブなプライマリアプライアンスに切り替える] オプションを選択すると、仮想アナライザ用の外部接続が使用できなくなった場合に自動的にパッシブなプライマリアプライアンスに切り替えることができます。

次の表は、設定の制限を示しています。

表 6-15. 高可用性使用時の設定上の制限

フィールド	制限事項
IPv4 仮想アドレス	• 別のホストでは使用できません。 • IPv4 アドレスとは異なる必要があります。 • IPv4 アドレスと同じネットワークセグメント内に存在している必要があります。
IPv6 仮想アドレス	• 別のホストでは使用できません。 • IPv6 アドレスとは異なる必要があります。 • IPv6 アドレスと同じネットワークセグメント内に存在している必要があります。 • リンクローカルにすることはできません。 • IPv6 アドレスが設定されている場合にのみ設定できます。

[HTTPS 証明書] タブ

Deep Discovery Analyzer で HTTPS 証明書を更新して、ネットワーク通信のセキュリティを強化できます。

現在の証明書情報を確認するには、[管理] > [システム設定] の順に選択し、[HTTPS 証明書] タブをクリックします。

次の表は、[詳細] セクションの各フィールドを示しています。

表 6-16. HTTPS 証明書の詳細

項目	説明
バージョン	証明書のバージョン番号
シリアル番号	証明書の一意の識別番号

項目	説明
署名アルゴリズム	署名を作成するために使用するアルゴリズム
発行元	情報を確認して証明書を発行したエンティティ
発効日	証明書が最初に有効になった日付
失効日	証明書の有効期限
件名	識別される個人またはエンティティ
サブジェクトの別名	証明書に関連付けられたユーザ指定の追加のドメイン名
公開鍵	暗号化に使用される 2048 ビット以上の公開鍵

[HTTPS 証明書] 画面では次の各タスクを実行できます。

- 証明書署名要求 (CSR) を生成して、証明機関 (CA) の新しい証明書を申請する。

  詳細については、259 ページの「証明書署名要求を生成する」を参照してください。

- 新しい証明書をインポートして、Deep Discovery Analyzer の既存の証明書を置換する。

  詳細については、261 ページの「証明書をインポートして置換する」を参照してください。

証明書署名要求を生成する

Deep Discovery Analyzer で証明書署名要求 (CSR) を生成して、証明機関 (CA) の新しい証明書を申請できます。

注意

Deep Discovery Analyzer では、X.509 PEM 形式の証明書がサポートされます。

手順

1. [管理] > [システム設定] の順に選択し、[HTTPS 証明書] タブをクリックします。
2. [証明書署名要求の生成] をクリックします。
3. 証明書署名要求を設定します。

   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
一般名 (CN)	ドメイン名またはサーバのホスト名を指定します。
サブジェクトの別名	生成した証明書に関連付けるドメイン名を 1 つ以上指定します。
組織 (O)	会社名を指定します。
組織単位 (OU)	会社内の部署名を指定します。
国 (C)	会社が存在する国を示す 2 文字のコードを指定します。
都道府県 (ST)	会社が存在する都道府県を指定します。
市区町村 (L)	会社が存在する市区町村を指定します。
メールアドレス	自身のメールアドレスを指定します。
キーのタイプとサイズ	次のいずれかのオプションを選択します。 • RSA (2048 ビット) • RSA (4096 ビット)

4. [生成してダウンロード] をクリックします。

   証明書署名要求が生成されると、該当の.csr ファイルが自動的にダウンロードされます。

証明書をインポートして置換する

重要

証明書をインポートすると、Deep Discovery Analyzer の既存の証明書が置換されます。

注意

- Web ブラウザのセキュリティを強化するには、Deep Discovery Analyzer の初期設定の証明書を置換することをお勧めします。
- Deep Discovery Analyzer では、X.509 PEM 形式の証明書がサポートされます。

手順

1. [管理] > [システム設定] の順に選択し、[HTTPS 証明書] タブをクリックします。
2. [証明書をインポートして置換] をクリックします。
3. 証明書ファイルを選択します。
4. [インポートして置換] をクリックします。

   このプロセスが完了すると、[HTTPS 証明書] 画面に新しい証明書の情報が表示されます。

アカウント/連絡先

[管理] > [アカウント/連絡先] 画面には、次のタブがあります。

- 262 ページの「[アカウント] タブ」
- 266 ページの「[SAML] タブ」
- 268 ページの「[連絡先] タブ」

[アカウント] タブ

[アカウント] タブは、ユーザアカウントの作成および管理に使用します。

注意

- クラスタ環境では、セカンダリ Deep Discovery Analyzer アプライアンスは、初期設定の管理者アカウント (admin) を除くすべてのローカルユーザアカウントをアクティブなプライマリアプライアンスから同期します。
- 同期したアカウントでセカンダリアプライアンスの管理コンソールにログインすると、アカウントのパスワードを変更するように求められます。

手順

1. [管理] > [アカウント/連絡先] の順に選択します。
2. [アカウント] タブをクリックします。
3. 次のオプションを使用してユーザアカウントを管理します。
   - 新しいユーザアカウントを追加するには、[追加] をクリックします。

     [アカウントの追加] 画面が開きます。詳細については、263 ページの「ユーザアカウントを設定する」を参照してください。
   - アカウントを削除するには、1 つ以上のユーザアカウントを選択して [削除] をクリックします。

     重要

     - Deep Discovery Analyzer の初期設定の管理者アカウントは削除できません。
     - ログオンしているアカウントは削除できません。
   - アカウントを手動でロック解除するには、アカウントを選択して [ロック解除] をクリックします。

     Deep Discovery Analyzer には、ユーザが 5 回連続して誤ったパスワードを入力した場合にアカウントをロックするセキュリティ機能があります。この機能は無効にできません。ロックされたアカウン

トは 10 分後に自動的にロック解除されます。管理者はロックされたアカウントを手動でロック解除できます。

一度にロック解除できるユーザアカウントは 1 つのみです。

4. 既存のアカウントを変更するには、アカウントのユーザ名をクリックします。

   [アカウントの編集] 画面が開きます。詳細については、263 ページの「ユーザアカウントを設定する」を参照してください。

5. 表内のエントリが多い場合は、次のオプションを使用してユーザアカウントリストを管理します。

   - 特定の種類のアカウントのみを表示するには、[種類] ドロップダウンからアカウントの種類を選択します。
   - 名前をアルファベット順に並べ替えるには、[名前] 列をクリックします。
   - エントリを絞り込むには、[検索] テキストボックスにいくつかの文字を入力します。入力すると、入力した文字に一致するエントリが表示されます。Deep Discovery Analyzer は、現在のページのすべてのセルを対象に一致を検索します。
   - 画面の最下部にあるパネルには、ユーザアカウントの合計数が表示されます。すべてのユーザアカウン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アカウントを表示します。

ユーザアカウントを設定する

手順

1. [管理] > [アカウント/連絡先] の順に選択して、[アカウント] タブに移動します。
2. 次のいずれかを実行します。
   - [追加] をクリックして、新しいユーザアカウントを作成します。

- 既存のユーザアカウント名をクリックして、その設定を変更します。

3. ローカルアカウントを追加するには、アカウントの [種類] に [ローカルユーザ] を選択し、次の情報を入力します。

   - 名前:アカウント所有者の名前。
   - ユーザ名:最大 40 文字まで入力できます。

     注意

     新規アカウントの作成と管理コンソールのログオンプロセスでは、ユーザ名の大文字と小文字は区別されません。

   - パスワード:パスワードは 8 文字以上で、アルファベットの大文字と小文字、数字、および特殊文字を組み合わせて入力してください。

     注意

     - より複雑なパスワード要件を設定するには、[管理] > [システム設定] > [パスワードポリシー] タブでグローバルパスワードポリシーを設定します。パスワードポリシーが画面に表示され、ユーザアカウントを追加するにはこのポリシーの条件を満たす必要があります。
     - ユーザのパスワード入力時に入力の誤りが許容される再試行数を超えた場合、Deep Discovery Analyzer はそのユーザアカウントを無効に設定します (ロック)。このようなアカウントは [アカウント] 画面でロック解除できます。

   - パスワードの確認入力:パスワードを再度入力します。
   - (オプション) 説明:最大 40 文字まで入力できます。

     注意

     新しいローカルユーザアカウントで管理コンソールに初めてログインすると、アカウントのパスワードを変更するように求められます。

4. Active Directory ユーザを追加するには、アカウントの [種類] に [Active Directory ユーザ] を選択し、次の情報を入力します。

- ユーザの名前またはグループ:ユーザプリンシパル名 (UPN) またはユーザグループ名を指定します。

  注意

  特定のユーザ名またはグループを簡単に見つけるには、テキストボックスにいくつかの文字を入力し、[検索] をクリックします。

- (オプション) 説明:最大 40 文字まで入力できます。

5. ローカルアカウントのパスワードを変更するには、[パスワードの変更] を選択し、必要なフィールドを設定します。

   注意

   - 管理者としてログインしている場合は、新しいパスワードを 2 回入力することでローカルユーザアカウントのパスワードを変更できます。ローカルユーザアカウントの元のパスワードを入力する必要はありません。
   - ローカルユーザアカウントのパスワードが管理者により変更された場合、ユーザはログイン時に再度アカウントのパスワードを変更するように求められます。

6. このユーザアカウントの役割と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の再分析、オブジェクトの送信、および調査パッケージ (送信されたオブジェクトを含む) のダウンロードを実行でき、分析結果と製品設定に読み取り専用でアクセスできます。
   - 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。

7. (オプション) [連絡先に追加] を選択してユーザアカウントを [連絡先] リストに追加し、次の情報を入力します。

注意

連絡先は初期設定でメールアラート通知を受信します。

- メールアドレス
- (オプション) 電話番号

8. [保存] をクリックします。

[SAML] タブ

Deep Discovery Analyzer と ID プロバイダの間で信頼関係が確立されると、Deep Discovery Analyzer 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 Analyzer 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 Analyzer 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 Analyzer 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、267 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 Analyzer 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] の順に選択し、[SAML] タブをクリックします。
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. SAML グループを有効または無効にするステータスオプションを選択します。
4. 要求値として Deep Discovery Analyzer のグループ名を入力します。

   重要

   [SAML] 画面で新しい SAML グループを設定する場合、要求値の大文字と小文字は区別されません。シングルサインオンプロセスでも、SAML グループのマッピングでは大文字と小文字が区別されません。
5. (オプション) SAML グループの説明を入力します。
6. SAML グループの役割と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の再分析、オブジェクトの送信、および調査パッケージ (送信されたオブジェクトを含む) のダウンロードを実行でき、分析結果と製品設定に読み取り専用でアクセスできます。
   - 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。

7. [保存] をクリックします。

> **注意**
> ログオンしているアカウントがある SAML グループは削除できません。

[連絡先] タブ

[管理] > [アカウント/連絡先] の [連絡先] タブにて、ログで収集するデータを必要とする連絡先のリストを管理します。

この画面には、次のオプションが含まれます。

表 6-17. [連絡先] のタスク

タスク	手順
連絡先の追加	新規アカウントを追加するには、[連絡先の追加] をクリックします。これにより [連絡先の追加] 画面が開きます。ここで連絡先の詳細を指定します。詳細については、269 ページの「[連絡先の追加] 画面」を参照してください。
編集	連絡先の詳細を編集するには、連絡先を選択し、[編集] をクリックします。これにより [連絡先の編集] 画面が開きます。ここには [連絡先の追加] 画面と同じ設定が表示されます。詳細については、269 ページの「[連絡先の追加] 画面」を参照してください。 一度に編集できる連絡先は 1 つのみです。
削除	削除する連絡先を 1 つ以上選択して、[削除] をクリックします。
列データの並べ替え	列タイトルをクリックすると、その下にあるデータを並べ替えることができます。
検索	表に含まれるエントリが多い場合は、[検索] テキストボックスにいくつかの文字を入力してエントリを絞り込みます。入力すると、入力した文字に一致するエントリが表示されます。Deep Discovery Analyzer は、表内のすべてのセルを対象に一致を検索します。

タスク	手順
レコードコントロールとページ区切りコントロール	画面の最下部にあるパネルには、連絡先の合計数が表示されます。すべての連絡先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連絡先を表示します。

[連絡先の追加] 画面

[連絡先の追加] 画面は、[連絡先] タブから [連絡先の追加] をクリックしたときに表示されます。

この画面には、次のオプションが含まれます。

表 6-18. [連絡先の追加] 画面

フィールド	詳細
名前	連絡先の名前を入力します。
メールアドレス	連絡先のメールアドレスを入力します。
電話番号	(オプション) 連絡先の電話番号を入力します。
説明	(オプション) 説明を 40 文字以内で入力します。

システムログ

Deep Discovery Analyzer には、ユーザアクセス、コンポーネントのアップデート、設定の変更、および管理コンソールで行われたその他の設定変更についての概要を提供するシステムログが保持されます。

Deep Discovery Analyzer では、これらのシステムログがアプライアンスのハードドライブに保存されます。

システムログのクエリ

手順

1. [管理] > [システムログ] の順に選択します。
2. 種類を選択します。
   - すべて
   - システム設定
   - アカウントのログオン/ログオフ
   - システムアップデート
3. 期間を選択するか、カレンダーおよびスライダを使用してカスタムの範囲を指定します。
4. (オプション) [ユーザ名] フィールドにキーワードを入力して拡大鏡アイコンをクリックすると、キーワードが含まれるユーザ名のシステムログのみが表示されます。
5. [すべてエクスポート] をクリックして、システムログを.csv ファイルにエクスポートします。

システムメンテナンス

[管理] > [システムメンテナンス] 画面には、次のタブがあります。

- 271 ページの「[バックアップ] タブ」
- 275 ページの「[復元] タブ」
- 277 ページの[ネットワークサービス診断] タブ
- 278 ページの「[電源オフ/再起動] タブ」
- 278 ページの「[デバッグ] タブ」

[バックアップ] タブ

[バックアップ] タブには次のセクションがあります。

- 271 ページの「設定のバックアップ」
- 273 ページの「データのバックアップ」
- 274 ページの「データバックアップステータス」

注意

クラスタ内のプライマリノードとセカンダリノードの両方でデータをバックアップするように Deep Discovery Analyzer を設定している場合、[データバックアップステータス] セクションは [データバックアップ] 画面に表示されます。

詳細については、276 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。

設定のバックアップ

Deep Discovery Analyzer では、ほとんどの設定のバックアップファイルをエクスポートできます。

設定のバックアップファイルをダウンロードするには、[エクスポート] をクリックします。

次の表は、バックアップされる設定を含む画面およびタブを示しています。

表 6-19. バックアップされる設定

画面	タブ
ダッシュボード	ウィジェット設定のみ
[仮想アナライザ] > [送信]	カスタム列と詳細フィルタの設定
[仮想アナライザ] > [不審オブジェクト]	ユーザ指定の不審オブジェクト
[仮想アナライザ] > [除外]	該当なし

画面	タブ
[仮想アナライザ] > [サンドボックス管理]	ファイルパスワード
	送信設定 (ファイルタイプフィルタ設定)
	検索設定
	インタラクティブモード設定
	スマートフィードバック
	macOS 向けサンドボックス
	YARA ルール
[仮想アナライザ] > [ネットワーク共有]	該当なし
[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
	カスタマイズ
[管理] > [アップデート]	コンポーネントのアップデート設定
[管理] > [統合製品/サービス]	Smart Protection
	ICAP
	Microsoft Active Directory
	メールでの送信
	Syslog

画面	タブ
[管理] > [システム設定]	ネットワーク (セキュアプロトコル設定)
	プロキシ
	SMTP
	時間 (タイムゾーンと形式)
	SNMP
	パスワードポリシー
	セッションタイムアウト
[管理] > [アカウント/連絡先]	アカウント
	SAML
	連絡先
[管理] > [システムメンテナンス]	データのバックアップ
	ストレージ管理

データのバックアップ

Deep Discovery Analyzer は、送信レコード、分析の結果、およびオブジェクトを [ストレージ管理] 画面で指定されたリモートサーバに自動的にエクスポートします。

調査パッケージのデータは、利用可能な保存領域に基づいて定期的に削除されます。データの可用性を確保するため、データは外部サーバにバックアップすることをお勧めします。詳細については、86 ページの「調査パッケージのデータの保持」を参照してください。

手順

1. [管理] > [システムメンテナンス] 画面で、[バックアップ] タブをクリックします。
2. [リモートサーバに自動的にバックアップ] を選択します。

3. サーバの種類を選択します。
   - [SFTP サーバ]
   - [FTP サーバ]
4. 次の情報を入力します。
   a. [ホスト名または IP アドレス]: バックアップサーバのホスト名、IPv4 アドレス、または IPv6 アドレス。
   b. [ポート番号]: バックアップサーバのポート番号。
   c. (オプション) [フォルダ]: バックアップフォルダのパス。初期設定の値はルートフォルダです。
   d. [ユーザ名]: 認証に使用するユーザ名。
   e. [パスワード]: 認証に使用するパスワード。
5. [サーバ接続のテスト] をクリックして、プライマリバックアップサーバへの接続を確認します。
6. バックアップするデータの範囲を選択します。
   - [すべての送信]
   - [リスク高、中、および低]
   - [リスク高のファイルのみ]
7. [保存] をクリックします。

データバックアップステータス

クラスタ内のプライマリノードとセカンダリノードの両方でデータをバックアップするように Deep Discovery Analyzer を設定している場合、セカンダリノードのデータバックアップステータスを [データバックアップ] 画面で確認できます。

クラスタノードでのデータバックアップ設定の詳細については、276 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。

次の表は、[データバックアップステータス] セクションの詳細を示しています。

フィールド	説明
モード	アプライアンスに関連付けられているクラスタ設定モードが表示されます。
IP アドレス	アプライアンスの IP アドレスが表示されます。
ホスト名	アプライアンスのホスト名が表示されます。
前回のバックアップ	データバックアップステータス、またはアプライアンスのデータがプライマリノードから最後に更新された時刻が表示されます。

[復元] タブ

[復元] タブでは、バックアップファイルから設定を復元します。

設定のバックアップファイルの作成方法については、271 ページの「[バックアップ] タブ」を参照してください。

重要

Deep Discovery Analyzer のライセンスがアクティベートされていない場合、[macOS 向けサンドボックス] の設定は復元されません。

手順

1. [バックアップファイル] 横のボックスまたは [参照] をクリックします。
2. バックアップファイルを選択します。
3. 次のいずれかの復元オプションを選択します。
   - すべての設定を復元
   - ネットワーク共有設定を除くすべての設定を復元
   - ネットワーク共有設定のみを復元

4. [復元] をクリックします。

ストレージ管理を設定する

[ストレージ管理] 画面を使用して、分析結果を保存するクラスタノードを指定し、Deep Discovery Analyzer によって保存されるログの量を制御できます。

手順

1. [管理] > [システムメンテナンス] の順に選択し、[ストレージ管理] タブをクリックします。
2. [分析結果] セクションで、分析結果を保存するノードの場所を選択します。
   - プライマリノード: プライマリノードとセカンダリノードの両方で分析されたサンプルに対するすべての分析結果をプライマリノードに保存するには、このオプションを選択します。

     注意

     このオプションを選択すると、プライマリノードでのストレージの使用率が増加する可能性があります。
   - プライマリノードとセカンダリノード: サンプルを検索したノードに分析結果を保存するには、このオプションを選択します。たとえば、セカンダリノードで分析されたサンプルの結果はこのノード自体に保存され、プライマリノードには送信されません。

     注意

     セカンダリノードのデータバックアップステータスは、[データバックアップ] 画面で確認できます。
3. [検出ログ] セクションで、次の設定を行います。
   - 次の日数を経過したログを削除する: ログを保持する日数を指定します。

注意

日数は 1～100 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未満である場合にログを削除する: ログを自動的に削除するディスク容量のしきい値を指定し、削除するログの種類を選択します。すべてのログを削除することも、検出リスクに基づいてログの削除の優先度を設定することもできます。

注意

- しきい値は 10～90 の間で設定する必要があります。
- Deep Discovery Analyzer 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。
- [無害なサンプル検出のログを削除してから、不正なサンプル検出のログを削除する] を選択すると、ログが 1 つずつチェックされてから削除されるため、システムのパフォーマンスが低下することがあります。

4. [保存] をクリックします。

[ネットワークサービス診断] タブ

[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. 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。

   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。

[電源オフ/再起動] タブ

管理コンソールで、Deep Discovery Analyzer アプライアンスの電源をオフにしたり、再起動したりできます。

- 電源オフ: すべてのアクティブなタスクが停止され、アプライアンスがシャットダウンします。
- 再起動: すべてのアクティブなタスクが停止され、アプライアンスが再起動します。

アプライアンスの電源をオフにしたり再起動したりすると、次のことに影響します。

- 仮想アナライザのオブジェクト分析: 統合製品は、アプライアンスが使用できない間、オブジェクトをキューに入れたり、送信をスキップする可能性があります。
- すべてのユーザによって開始されたアクティブな設定タスク: すべてのアクティブなタスクが完了したことを確認してから、処理を続行することをお勧めします。

[デバッグ] タブ

[デバッグ] タブを使用すると、トラブルシューティング用にデバッグログを生成したり、デバッグログを設定したりできます。

手順

1. デバッグログに出力するイベントのデバッグレベルを指定します。
   a. [デバッグレベルの設定] セクションで、次のイベントに割り当てられている初期設定のデバッグレベルを確認します。
      - 仮想アナライザセンサ
      - 仮想アナライザ
      - 検索フロー
      - クラスタ

- 通知
- Apex Central
- SNMP
- Deep Discovery Director
- 製品の統合
- 運用レポート
- ICAP サーバ
- 管理コンソール
- ネットワーク共有
- その他

b. デバッグレベルをカスタマイズするには、現在割り当てられているレベルをクリックして別の値を選択します。

c. [保存] をクリックします。

d. すべてのデバッグレベルを初期設定値に戻すには、[初期設定に戻す] をクリックします。

2. デバッグログを収集します。

a. [ログ収集] セクションで、ログの収集タスクを実行するアプライアンスを特定します。

アクティブなプライマリアプライアンスでは、常にアクティブなプライマリアプライアンスが最初のエントリとして表示されます。

パッシブなプライマリアプライアンスでは、簡単に見分けられるように、パッシブなプライマリアプライアンスのホスト名が表示されます。

b. 選択したアプライアンスで [デバッグログの収集] をクリックします。

c. タスクが完了するまで待ちます。

d. [デバッグログのダウンロード] をクリックして、デバッグログを保存します。

注意

パッシブなプライマリアプライアンスのデバッグログは、アクティブなプライマリアプライアンスの管理コンソールで確認できます。

セカンダリアプライアンスのデバッグログは、セカンダリアプライアンスの管理コンソールで確認できます。

ツール

[管理] > [ツール] 画面にて、Deep Discovery Analyzer の専用ツールを表示およびダウンロードします。

この画面に表示される各ツールには、次の 2 つのオプションがあります。

- [ユーザガイド]: ツールの使用手順が記載された、オンラインヘルプの関連するページにリンクします。
- [ダウンロード]: ツールが含まれるダウンロードセンター内の関連するページにリンクします。

Virtual Analyzer Image Preparation Tool

仮想アナライザにイメージをインポートする前に、Virtual Analyzer Image Preparation Tool を使用します。Virtual Analyzer Image Preparation Tool は、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、さらに必要なアプリケーションが揃っているかどうかを確認します。

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://appweb.trendmicro.com/ecs/default.aspx

Manual Submission Tool

Manual Submission Tool を使用して、ユーザのコンピュータ上の場所から Deep Discovery Analyzer にサンプルをリモートで送信できます。この機能では複数のサンプルを一度に送信できます。これらのサンプルは [送信] キューに追加されます。

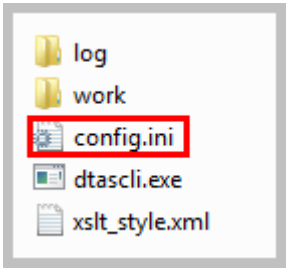
次の手順に従って、Manual Submission Tool をダウンロード、設定、および使用してください。

手順

1. Manual Submission Tool で使用する次の情報を記録します。
   a. API キー。Deep Discovery Analyzer 管理コンソールの [ヘルプ] [バージョン情報] から入手できます。
   b. Deep Discovery Analyzer の IP アドレス。IP アドレスがわからない場合は、Deep Discovery Analyzer 管理コンソールへのアクセスに使用した URL を確認します。IP アドレスはこの URL に含まれています。
2. [管理] > [ツール] で、Manual Submission Tool の [ダウンロード] リンクをクリックします。

   トレンドマイクロ のソフトウェアダウンロードセンターの画面が開きます。
3. 最新バージョンの横にあるダウンロードアイコンをクリックします。

   異なるダウンロードオプションを示す画面が表示されます。
4. [Use HTTP Download] をクリックします。
5. ツールパッケージを解凍します。
6. ツールの解凍先フォルダで、`config.ini` を開きます。



7. Host の横に Deep Discovery Analyzer の IP アドレスを入力します。ApiKey の横に Deep Discovery Analyzer の API キーを入力します。config.ini を保存します。

```
[DTAS]
Host = 10.100.100.100
ApiKey = YZ12A345-B67C-890D-1E23-F45G678HIJKL
[Header]
X-DTAS-ProtocolVersion = 1.1
X-DTAS-ProductName = DTASSubmisstionTool
X-DTAS-ClientHostname = DTASSubmisstionTool01
```

8. サンプルを送信します。詳細については、76 ページの「オブジェクトを手動で送信する」を参照してください。

ライセンス

[管理] > [ライセンス] 画面にて、Deep Discovery Analyzer のサポート契約情報の表示、アクティベート、およびサポート契約の更新を行います。

Deep Discovery Analyzer のサポート契約では、購入日から 1 年間、製品アップデート (トレンドマイクロのアップデートを含む) および基本的なテクニカルサポートを受けることができます。このライセンスによって分析のための脅威サンプルのアップロード、および仮想アナライザからの Trend Micro Threat Connect へのアクセスも実行できます。さらに、分析のために、トレンドマイクロのクラウドサンドボックスにサンプルを送信することもできます。

最初の 1 年が終了すると、サポート契約は年ベースで更新する必要があり、その際はトレンドマイクロの最新の料金が適用されます。

サポート契約は、お客さまの組織とトレンドマイクロの間の契約です。この契約では、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。

サポート契約には有効期限があります。ソフトウェアの使用権にはありません。サポート契約の有効期限が満了すると、トレンドマイクロからテクニカルサポートを受ける権利、および Trend Micro Threat Connect にアクセスする権利が無効になります。

通常、サポート契約の有効期限の 90 日前に、お客さまに契約の中止が保留中であることを警告するメール通知の送信が開始されます。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サポート契約ポータルからメンテナンス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://olr.trendmicro.com/registration/jp/ja/login.aspx

[ライセンス] 画面には、次の情報およびオプションが含まれます。

表 6-20. 製品詳細

フィールド	詳細
製品名	製品の名前が表示されます。
ファームウェアのバージョン	製品の完全なビルド番号が表示されます。
使用許諾契約	[トレンドマイクロ使用許諾契約] へのリンクが表示されます。リンクをクリックすると、使用許諾契約を表示または印刷できます。

表 6-21. ライセンスの詳細

フィールド	詳細
アクティベーションコード	ここにアクティベーションコードが表示されます。サポート契約の有効期限が満了した場合は、トレンドマイクロから新しいアクティベーションコードを入手してください。サポート契約を更新するには、[新しいアクティベーションコード] をクリックして、新しいアクティベーションコードを入力します。 [ライセンス] 画面が再表示され、サポート契約の有効期限までの残余日数が表示されます。
ステータス	[アクティベート済み]、[アクティベーション未完了]、[猶予期間]、[有効期限切れ]、または [体験版の有効期限終了] のいずれかが表示されます。 トレンドマイクロの Web サイトでライセンス情報の詳細を表示するには、[詳細情報をオンラインで確認] をクリックします。たとえばサポート契約の更新後など、ステータスの変更後に正しいステータスが画面に表示されない場合は、[更新] をクリックしてください。
種類	• 製品版: すべての製品機能へのアクセスを提供します • 体験版: すべての製品機能へのアクセスを提供します
有効期限	サポート契約の有効期限が表示されます。サポートサービスの継続をご希望される場合は、有効期限の満了前にサポート契約を更新してください。

バージョン情報

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

API キーは、トレンドマイクロ製品で Deep Discovery Analyzer への登録およびサンプルの送信に使用されます。サポートされる製品およびバージョンについては、33 ページの「トレンドマイクロ製品との統合」を参照してください。

第 7 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/jp/technical-support

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/jp/virus-and-threat-help

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

サービスのアドレスとポート

Deep Discovery Analyzer 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 A-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。	ddan70-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。	grid-global.trendmicro.com:443/ws/level-0/files
Sandbox as a Service (macOS 向け)	macOS の潜在的な脅威を分析するホステッドサービスです。	ddaaas.trendmicro.com:443

サービス	説明	アドレスとポート
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。	ddan710-jp-domaincensus.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。	ddan710-jp-census.trendmicro.com:443
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:443/ollu/license_update.aspx
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。	ddan7-0-jp-t0.url.trendmicro.com:443 ddan7-0-jp-t0-backup.url.trendmicro.com:443
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。	ddan70-jp-f.trx.trendmicro.com:443
スマートフィードバック	匿名の脅威データベースを 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。	ddan700-jp.fbs25.trendmicro.com:443

サービス	説明	アドレスとポート
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。	ddan70jp-threatconnect.trendmicro.com: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。	ddan7-0-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。	ddan7-0-jp.url.trendmicro.com:443 ddan7-0-jp-backup.url.trendmicro.com:443

付録 B

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 B-1. system

項目	説明
OID	.1.3.6.1.2.1.1
オブジェクト名	system
説明	システム

表 B-2. sysDescr

項目	説明
OID	.1.3.6.1.2.1.1.1
オブジェクト名	sysDescr
説明	エンティティのテキスト形式の説明。この値には、システムのハードウェアの種類、ソフトウェアの OS、およびネットワーキングソフトウェアの完全な名前とバージョン ID が、印刷可能な ASCII 文字のみで含まれる必要があります。

表 B-3. sysObjectID

項目	説明
OID	.1.3.6.1.2.1.1.2
オブジェクト名	sysObjectID
説明	エンティティに含まれるネットワーク管理サブシステムのベンダの認証 ID。この値は SMI エンタープライズサブツリー (1.3.6.1.4.1) 内に割り当てられ、これにより管理対象が「どのようなデバイスであるか」を簡単かつ明確に判断できます。たとえば「Flintstones, Inc.」というベンダにサブツリー 1.3.6.1.4.1.424242 が割り当てられている場合、その「Fred Router」に ID 1.3.6.1.4.1.424242.1.1 を割り当てることができます。

表 B-4. sysUpTime

項目	説明
OID	.1.3.6.1.2.1.1.3
オブジェクト名	sysUpTime
説明	システムのネットワーク管理部分が最後に再初期化されてからの経過時間 (1/100 秒単位)。

表 B-5. sysContact

項目	説明
OID	.1.3.6.1.2.1.1.4
オブジェクト名	sysContact
説明	この管理対象ノードの連絡先担当者のテキスト形式の ID、およびこの担当者への連絡方法に関する情報。連絡先情報が不明な場合、この値はゼロ長の文字列になります。

表 B-6. sysName

項目	説明
OID	.1.3.6.1.2.1.1.5
オブジェクト名	sysName
説明	この管理対象ノードに管理用に割り当てられた名前。慣例により、これにはノードの完全修飾ドメイン名を使用します。名前が不明な場合、この値はゼロ長の文字列になります。

表 B-7. sysLocation

項目	説明
OID	.1.3.6.1.2.1.1.6
オブジェクト名	sysLocation
説明	このノードの物理的な場所 (「3 階の電話置き場」など)。場所が不明な場合、この値はゼロ長の文字列になります。

表 B-8. sysServices

項目	説明
OID	.1.3.6.1.2.1.1.7
オブジェクト名	sysServices
説明	このエンティティが提供する可能性がある一連のサービスを示す値。これは合計値で、初期値はゼロになります。次に、このノードがトランザクションを実行する 1〜7 までの範囲のレイヤ (L) ごとに、2 を (L - 1) 乗した数が合計に追加されます。たとえば、ルーティング機能のみを実行するノードの値は、4 (2^(3-1)) になります。それに対して、アプリケーションサービスを提供するホストノードの値は、72 (2^(4-1) + 2^(7-1)) になります。インターネットプロトコルスイートの場合は、次に従って値を計算する必要があります。 レイヤの機能 1 物理 (例: リピータ) 2 データリンク/サブネットワーク (例: ブリッジ) 3 インターネット (例: IP 対応) 4 エンドツーエンド (例: TCP 対応) 7 アプリケーション (例: SMTP 対応) OSI プロトコルを含むシステムでは、レイヤ 5 とレイヤ 6 も考慮される場合があります。

表 B-9. sysORLastChange

項目	説明
OID	.1.3.6.1.2.1.1.8
オブジェクト名	sysORLastChange
説明	sysORID の任意のインスタンスの状態または値が直近に変化した時の sysUpTime の値。

表 B-10. interfaces

項目	説明
OID	.1.3.6.1.2.1.2
オブジェクト名	interfaces
説明	インタフェース

表 B-11. ifNumber

項目	説明
OID	.1.3.6.1.2.1.2.1
オブジェクト名	ifNumber
説明	このシステムに存在するネットワークインタフェースの数 (現在の状態は影響しません)。

表 B-12. ifTable

項目	説明
OID	.1.3.6.1.2.1.2.2
オブジェクト名	ifTable
説明	インタフェースエントリのリスト。エントリの数は、ifNumber の値によって決まります。

表 B-13. memIndex

項目	説明
OID	.1.3.6.1.4.1.2021.4.1
オブジェクト名	memIndex
説明	ダミーのインデックス。常に整数 0 を返します。

表 B-14. memErrorName

項目	説明
OID	.1.3.6.1.4.1.2021.4.2
オブジェクト名	memErrorName
説明	ダミーの名前。常に「swap」という文字列を返します。

表 B-15. 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 B-16. 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 B-17. 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 B-18. memAvailReal

項目	説明
OID	.1.3.6.1.4.1.2021.4.6

項目	説明
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 B-19. 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 B-20. 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 B-21. 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 B-22. memBuffer

項目	説明
OID	.1.3.6.1.4.1.2021.4.14
オブジェクト名	memBuffer
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 B-23. 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 B-24. 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 B-25. memSwapErrorMsg

項目	説明
OID	.1.3.6.1.4.1.2021.4.101
オブジェクト名	memSwapErrorMsg

項目	説明
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 B-26. 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 B-27. 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 B-28. 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 B-29. dskMinimum

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.4
オブジェクト名	dskMinimum

項目	説明
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 B-30. dskMinPercent

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.5
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 B-31. 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 B-32. 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 B-33. dskUsed

項目	説明
OID	.1.3.6.1.4.1.2021.9.1.8
オブジェクト名	dskUsed

項目	説明
説明	使用しているディスク容量。

表 B-34. 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 B-35. 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 B-36. 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 B-37. 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 B-38. laTable

項目	説明
OID	.1.3.6.1.4.1.2021.10
オブジェクト名	laTable
説明	ロードアベレージの情報

表 B-39. ssSwapIn

項目	説明
OID	.1.3.6.1.4.1.2021.11.1
オブジェクト名	ssIndex
説明	ダミーのインデックス。常に整数 0 を返します。

表 B-40. ssSwapIn

項目	説明
OID	.1.3.6.1.4.1.2021.11.2
オブジェクト名	ssErrorName
説明	ダミーの名前。常に「systemStats」という文字列を返します。

表 B-41. 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 B-42. 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 B-43. 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 B-44. 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 B-45. 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 B-46. 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 B-47. 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 B-48. 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 B-49. 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 B-50. 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 B-51. 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 B-52. 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 B-53. 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 B-54. 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 B-55. 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 B-56. 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 B-57. 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 B-58. 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 B-59. 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 B-60. 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 B-61. 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 B-62. 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 B-63. 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 B-64. ssCpuRawSteal

項目	説明
OID	.1.3.6.1.4.1.2021.11.64
オブジェクト名	ssCpuRawSteal
説明	CPU により仮想 CPU (ゲスト) の実行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 B-65. ssCpuRawGuest

項目	説明
OID	.1.3.6.1.4.1.2021.11.65
オブジェクト名	ssCpuRawGuest
説明	CPU により仮想 CPU (ゲスト) の実行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 B-66. ssCpuRawGuestNice

項目	説明
OID	.1.3.6.1.4.1.2021.11.66
オブジェクト名	ssCpuRawGuestNice
説明	CPU により仮想 CPU (ゲスト) の実行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 B-67. productVersion

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.1.1
オブジェクト名	productVersion
説明	Deep Discovery Analyzer のバージョンを返します。

表 B-68. productBuild

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.1.2
オブジェクト名	productBuild
説明	Deep Discovery Analyzer のビルド番号を返します。

表 B-69. productHotfix

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.1.3
オブジェクト名	productHotfix
説明	Deep Discovery Analyzer の HotFix 番号を返します。

表 B-70. componentTable

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.2
オブジェクト名	componentTable
説明	一連のコンポーネント情報を含む表。

表 B-71. componentIndex

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.2.1.1
オブジェクト名	componentIndex
説明	コンポーネントのインデックスを返します。

表 B-72. componentID

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.2.1.2
オブジェクト名	componentID
説明	コンポーネントの ID を返します。

表 B-73. componentName

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.2.1.3
オブジェクト名	componentName
説明	コンポーネントの名前を返します。

表 B-74. componentVersion

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.2.1.4
オブジェクト名	componentVersion

項目	説明
説明	コンポーネントのバージョンを返します。

表 B-75. throughputTable

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.3
オブジェクト名	throughputTable
説明	一連のスループット情報を含む表。

表 B-76. ifIndex

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.3.1.1
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 B-77. ifDescr

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.3.1.2
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 B-78. ifReceiveThroughput

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.3.1.3
オブジェクト名	ifReceiveThroughput
説明	インタフェース受信スループットを返します。

表 B-79. ifTransmitThroughput

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.3.1.4
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。

表 B-80. numberInQueue

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.1
オブジェクト名	numberInQueue
説明	キュー内のサンプルの数を返します。

表 B-81. numberInProcessing

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.2
オブジェクト名	numberInProcessing
説明	現在処理中のサンプルの数を返します。

表 B-82. suspiciousObjectIP

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.3.1
オブジェクト名	suspiciousObjectIP
説明	不審オブジェクト (IP アドレス) の数を返します。

表 B-83. suspiciousObjectDomain

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.3.2
オブジェクト名	suspiciousObjectDomain

項目	説明
説明	不審オブジェクト (ドメイン) の数を返します。

表 B-84. suspiciousObjectURL

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.3.3
オブジェクト名	suspiciousObjectURL
説明	不審オブジェクト (URL) の数を返します。

表 B-85. suspiciousObjectSha1

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.3.4
オブジェクト名	suspiciousObjectSha1
説明	不審オブジェクト (SHA1) の数を返します。

表 B-86. vaUtilization

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.4
オブジェクト名	vaUtilization
説明	仮想アナライザの使用率情報を返します。

表 B-87. numberCompleted

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.5
オブジェクト名	numberCompleted
説明	過去 24 時間に処理が完了したサンプルの数を返します。

表 B-88. numberIcapPreScanned

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.6
オブジェクト名	numberIcapPreScanned
説明	過去 24 時間に ICAP 事前検索によって処理されたサンプルの数を返します。

表 B-89. numberSubmissionHigh

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.7.1
オブジェクト名	numberSubmissionHigh
説明	過去 24 時間にリスク高と分析された送信の数を返します。

表 B-90. numberSubmissionMedium

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.7.2
オブジェクト名	numberSubmissionMedium
説明	過去 24 時間にリスク中と分析された送信の数を返します。

表 B-91. numberSubmissionLow

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.7.3
オブジェクト名	numberSubmissionLow
説明	過去 24 時間にリスク低と分析された送信の数を返します。

表 B-92. numberSubmissionNo

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.7.4

項目	説明
オブジェクト名	numberSubmissionNo
説明	過去 24 時間にリスクなしと分析された送信の数を返します。

表 B-93. numberSubmissionNot

項目	説明
OID	.1.3.6.1.4.1.6101.3005.1.4.7.5
オブジェクト名	numberSubmissionNot
説明	過去 24 時間に仮想アナライザによって分析されなかった送信の数を返します。

SNMP トラップ

表 B-94. 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 B-95. 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

項目	説明
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 B-96. 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 B-97. 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 B-98. accountLockedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.1
オブジェクト名	accountLockedNotification
説明	ログオンに複数回失敗してアカウントがロックされた場合に発信されます。

表 B-99. vaStoppedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.2
オブジェクト名	vaStoppedNotification
説明	仮想アナライザがエラーから回復できない場合に発信されます。

表 B-100. vaLongQueueNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.3
オブジェクト名	vaLongQueueNotification
説明	仮想アナライザの送信数がしきい値を上回った場合に発信されます。

表 B-101. compUpdateErrorNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.4
オブジェクト名	compUpdateErrorNotification
説明	コンポーネントのアップデートに失敗した場合に発信されます。

表 B-102. highCpuNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.5
オブジェクト名	highCpuNotification
説明	過去 5 分間の平均 CPU 使用率がしきい値を上回った場合に発信されます。

表 B-103. highMemNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.6
オブジェクト名	highMemNotification
説明	過去 5 分間の平均メモリ使用率がしきい値を上回った場合に発信されます。

表 B-104. highDiskNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.7
オブジェクト名	highDiskNotification
説明	ディスク使用率がしきい値を上回った場合に発信されます。

表 B-105. secondaryDownNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.8
オブジェクト名	secondaryDownNotification
説明	セカンダリアプライアンスがエラーから回復できない場合に発信されます。

表 B-106. haPassiveActivatedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.9
オブジェクト名	haPassiveActivatedNotification
説明	アクティブなプライマリアプライアンスがエラーから回復できず、パッシブなプライマリアプライアンスがアクティブな役割を引き継いだ場合に発信されます。

表 B-107. haSuspendedNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.10
オブジェクト名	haSuspendedNotification
説明	パッシブなプライマリアプライアンスがエラーから回復できず、高可用性が一時停止された場合に発信されます。

表 B-108. syslogErrorNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.11
オブジェクト名	syslogErrorNotification
説明	Syslog サーバにアクセスできない場合に発信されます。

表 B-109. backupErrorNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.12
オブジェクト名	backupErrorNotification
説明	バックアップサーバにアクセスできない場合に発信されます。

表 B-110. haRestoredNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.13
オブジェクト名	haRestoredNotification
説明	パッシブなプライマリアプライアンスが回復し、高可用性が復元された場合に発信されます。

表 B-111. vaHighRiskNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.14
オブジェクト名	vaHighRiskNotification
説明	前回の TimeRange 内で識別された新しいリスク高オブジェクトの数がしきい値に達した場合に発信されます。

表 B-112. vaConnectionFailureNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.15
オブジェクト名	vaConnectionFailureNotification
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場合に発信されます。

表 B-113. vaLongProcessTimeNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.16
オブジェクト名	vaLongProcessTimeNotification
説明	仮想アナライザの送信処理時間がしきい値を上回った場合に発信されます。

表 B-114. licenseExpireNotification

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.17
オブジェクト名	licenseExpireNotification
説明	ライセンスの有効期限が近づいているか切れている場合に発信されます。

表 B-115. networkShareInaccessible

項目	説明
OID	.1.3.6.1.4.1.6101.3005.2.1.0.18
オブジェクト名	networkShareInaccessible
説明	アプライアンスがネットワーク共有サーバへの接続を確立できない場合に発信されます。

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

付録 C

統合製品/サービスでの TLS 1.2 のサポート

セキュアプロトコルオプションが有効な場合、次の統合製品/サービスでは TLS 1.2 が使用されます。詳細については、226 ページの「[ネットワーク] タブ」を参照してください。

- Active Directory
- SSL 経由のメールでの送信
- SSL 経由の ICAP
- HTTPS を使用したイメージのアップロード
- 内部仮想アナライザサービス
- 管理コンソールアクセス
- SMTP
- SSL による Syslog
- トレンドマイクロのアップデート
- トレンドマイクロのソフトウェア安全性評価サービス
- トレンドマイクロのコミュニティドメイン/IP レピュテーションサービス

- トレンドマイクロのコミュニティファイルレピュテーションサービス
- トレンドマイクロのサポート契約ポータル
- Trend Micro Deep Discovery Director
- トレンドマイクロの機械学習型検索エンジン
- トレンドマイクロの動的な URL 検索
- トレンドマイクロスマートフィードバック
- Trend Micro Smart Protection Server 3.3 以降
- トレンドマイクロの Web 検査サービス
- トレンドマイクロの Web レピュテーションサービス
- Trend Micro Vision One
- Web サービス

索引

か

さ