Deep Discovery™ Director（統合モード）5.3

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

著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

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、およびスマスキャは、トレンドマイクロ株式会社の登録商標です。

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、
各社の商標または登録商標です。

Copyright © 2021 Trend Micro Incorporated. All rights reserved.

P/N: APEM59259/210318_JP (2021/08)

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 Director 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 Director 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

本書について

本書について 15
ドキュメント 16
対象読者 17
ドキュメントの表記規則 17
トレンドマイクロについて 17

第 1 章：はじめに

Deep Discovery Director (統合モード) について 20
新機能 20
機能と利点 21

第 2 章：インストール

システム要件 28
推奨されるシステム要件 28
Deep Discovery Director をインストールする 29
ネットワークを設定する 31
管理コンソールにログオンする 32
統合ソリューションの導入の概要 32
配信前チェックリスト 33

第 3 章：ダッシュボード

ダッシュボードの概要 38
タブ 38
タブのタスク 38
ウィジェット 39
ウィジェットのタスク 39

Deep Discovery Inspector のウィジェット 43
脅威検出状況の概要 44
影響を受けたホストの上位 45
検索されたプロトコル別トラフィック 45
脅威のグラフィック地図 - C&C 通信 46
YARA ルールでのネットワーク検出の上位 46

Deep Discovery Email Inspector のウィジェット 46
メールメッセージの検出のサマリー 47
メールメッセージの高度な脅威インジケータ 47
メールメッセージの攻撃元 48
YARA ルールでのメールメッセージ検出の上位 48

第 4 章：検出

[検出] 画面について 50
ホストの重大度 51
メールメッセージのリスクレベル 54
メールメッセージの脅威の種類の分類 57
相関データを使用した詳細分析をサポートするプロトコル 58

影響を受けたホスト 60
表示オプションと検索フィルタ 61
[影響を受けたホスト] を表示する 63
[影響を受けたホスト] - [ホストの詳細] を表示する 68
[影響を受けたホスト] - [検出の詳細] を表示する 71
[影響を受けたホスト] の詳細検索フィルタ 84

ネットワーク検出 102
表示オプションと検索フィルタ 102
[ネットワーク検出] を表示する 104
[ネットワーク検出] - [検出の詳細] を表示する 108
[ネットワーク検出] の詳細検索フィルタ 121

メールメッセージ 131
表示オプションと検索フィルタ 132
[メールメッセージ] を表示する 133
[メールメッセージ] - [検出の詳細] を表示する 135
[メールメッセージ] の詳細検索フィルタ 140

隔離メッセージ 147
表示オプションと検索フィルタ 147
[隔離メッセージ] を表示する 151
[隔離メッセージ] - [検出の詳細] を表示する 152
[隔離メッセージ] の詳細検索フィルタ 157
隔離されたメッセージを管理する 159
相関イベント 160
表示オプションと検索フィルタ 160
[相関イベント] を表示する 161
[相関イベント] - [相関データ] を表示する 162
[相関イベント] - [検出の詳細] を表示する 185
無視ルール 196
無視ルールのタスク 196

第 5 章：脅威インテリジェンス

製品インテリジェンス 200
同期された不審オブジェクト 200
C&C コールバックアドレス 205
カスタムインテリジェンス 208
YARA ルール 209
STIX 215
ユーザ指定の不審オブジェクト 217
除外 226
フィード管理 229
インテリジェンスフィードを追加する 230
インテリジェンスフィードを編集する 232
インテリジェンスフィードを削除する 232
共有設定 233
TAXII 1.x 233
TAXII 2.0 234
OpenDXL 234
Web サービス 235
補助製品/サービス 237

第 6 章：アプライアンス

ディレクトリ 262
ディレクトリのタスク 262
ディレクトリのその他のタスク 265

計画 269
計画のタスク 271
アプライアンスのステータス 272
計画のその他のタスク 273

リポジトリ 281
HotFix/Critical Patch/ファームウェア 281
仮想アナライザイメージ 282
アップロードセンター 284

ファイルパスワード 286
ユーザ指定のパスワード 286
ヒューリスティック検出されたパスワード 290

ネットワーク資産 290
ドメインの除外 291
優先ウォッチリスト 293
登録済みドメイン 295
登録済みサービス 297
ネットワークグループ 300
分析 305

Email Encryption 305
ドメインリスト 306
ID 309

ログ 310
メールメッセージ追跡 310
MTA 317
メッセージキュー 318

エンドユーザメール隔離 322
エンドユーザメール隔離の設定 322
エンドユーザメール隔離通知 325
エンドユーザメール隔離コンソール 327

第 7 章：アラート

アラートについて 334
トークン変数 334
実行されたアラート 339
組み込みルール 340
組み込みルールを編集する 341
カスタムルール 343
カスタムルールを追加する 344
カスタムルールのその他のタスク 346

第 8 章：レポート

レポートについて 348
生成されたレポート 348
生成されたレポートを表示する 349
生成されたレポートを削除する 349
スケジュール 349
スケジュールを表示する 350
スケジュールを追加する 351
スケジュールを編集する 353
スケジュールを削除する 353
手動 353
手動レポートを生成する 354
カスタマイズ 355
レポートをカスタマイズする 355

第 9 章：管理

アップデート 358
コンポーネント 358
HotFix/Patch 359
ファームウェア 362
統合製品/サービス 363
Apex Central 363
Microsoft Active Directory 365

SAML 認証 367
Syslog 379
Trend Micro Vision One 381
ステータス 382
接続済みソース 382
ネットワーク分析 383
オンプレミス固有の画面 384
Software as a Service 固有の画面 386
システム設定 390
ネットワーク 390
プロキシ 394
SMTP 395
SNMP 396
帯域幅 400
時間 401
証明書 402
セッションタイムアウト 404
アカウント管理 405
アカウント 405
役割 412
システムログ 415
システムログのクエリを実行する 417
システムのメンテナンス 418
システムステータス 419
ストレージ 419
バックアップ 421
復元 425
電源オフ/再起動 429
ライセンス 429

第 10 章：トラブルシューティング

トラブルシューティング 434

第 11 章：テクニカルサポート

トラブルシューティングのリソース 436
サポートポータルの利用 436
脅威データベース 436
製品サポート情報 437
サポートサービスについて 437
トレンドマイクロへのウイルス解析依頼 437
メールレピュテーションについて 438
ファイルレピュテーションについて 438
Web レピュテーションについて 439
その他のリソース 439
最新版ダウンロード 439
脅威解析・サポートセンター TrendLabs (トレンドラボ) 439

付録

付録 A：サービスのアドレスとポート

サービスのアドレスとポート 444
Deep Discovery Director (統合モード) で使用されるポート .. 445

付録 B：Deep Discovery Director で複製される設定

Deep Discovery Analyzer 6.8 で複製される設定 450
Deep Discovery Analyzer 6.9 で複製される設定 451
Deep Discovery Analyzer 7.0 で複製される設定 453
Deep Discovery Inspector 5.6 で複製される設定 455
Deep Discovery Inspector 5.7 で複製される設定 457
Deep Discovery Inspector 5.8 で複製される設定 460
Deep Discovery Web Inspector 2.5 で複製される設定 463
Deep Discovery Web Inspector 2.6 で複製される設定 464
Deep Discovery Director (Standalone Network Analytics モード) 5.2 で複製される設定 466

Deep Discovery Director (Standalone Network Analytics モード) 5.3 で複製される設定 467

はじめに

本書について

Trend Micro Deep Discovery Director (統合モード) 管理者ガイドをお読みいただきありがとうございます。このガイドには、製品の設定に関する情報が記載されています。

ドキュメント

Deep Discovery Director (統合モード) 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	管理者ガイドには、Deep Discovery Director (統合モード) を設定して管理する方法の詳細な手順、および Deep Discovery Director (統合モード) の概念や機能に関する説明が記載されています。
Syslog コンテンツマッピングガイド	Syslog コンテンツマッピングガイドには、ログの管理基準や、Deep Discovery Director (統合モード) 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。
Automation API Guide	Deep Discovery Director (統合モード) オートメーション API の使用方法を説明する PDF ドキュメントです。
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 Director (統合モード) 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 Director (統合モード) のコンポーネントと機能、Deep Discovery Director (統合モード) を設定するために必要な手順が説明されています。
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 Director (統合モード) 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

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

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

トレンドマイクロについて

トレンドマイクロは、サイバーセキュリティにおける世界的企業として、安全にデジタル情報をやり取りできる環境の実現に向けて継続的に取り組んで

います。個人消費者、企業、および政府機関向けの革新的ソリューションである XGen セキュリティ戦略を巧みに利用することで、つながるセキュリティをデータセンター、クラウドワークロード、ネットワーク、およびエンドポイントにもたらします。

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

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

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

第 1 章

はじめに

この章では、Trend Micro™ Deep Discovery™ Director (統合モード) 5.3 および このリリースの新機能について説明します。

Deep Discovery Director (統合モード) について

Trend Micro Deep Discovery Director は、以下を可能にする管理ソリューションです。

- HotFix、Critical Patch、ファームウェア、および仮想アナライザイメージの配信の一元管理
- 設定の複製
- ログの集計
- リアルタイムでの脅威の検出監視と相関分析
- 脅威インテリジェンスの管理と共有

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

Deep Discovery Director は、Deep Discovery Analyzer、Deep Discovery Email Inspector、Deep Discovery Inspector、および Deep Discovery Director - Network Analytics と統合できます。

新機能

表 1-1. Deep Discovery Director (統合モード) 5.3 の新機能

機能/強化点	詳細
Linux ベースの仮想アナライザイメージのサポート	Linux ベースの仮想アナライザイメージを管理下の Deep Discovery アプライアンスに配信できるようになります。
ネットワーク資産の一元化された設定	ネットワーク資産の設定を管理下の Deep Discovery Inspector および Deep Discovery Director - Network Analytics アプライアンスに同期できるようになります。
不審オブジェクトのネットワーク分析アラート	ユーザ指定の不審オブジェクトについて相関イベントが検出された場合、アラート通知を送信できるようになります。

機能/強化点	詳細
管理コンソールナビゲーションの強化	[ドメインの除外]、[優先ウォッチリスト]、[登録済みドメイン]、[ネットワークグループ]、および[登録済みサービス]のネットワーク分析の設定が、[アプライアンス] > [ネットワーク資産]の下に移動します。 ネットワーク分析のステータス情報とデータソースの設定画面は、[管理] > [ネットワーク分析]の下に残ります。

機能と利点

Deep Discovery Director (統合モード) には次の機能があります。

機能または利点	詳細
Trend Micro Vision One の統合	Trend Micro Vision One との統合により、Deep Discovery アプライアンスのアクティビティデータを Trend Micro Vision One に送信したり、Trend Micro Vision One が Network Analytics の相関データにアクセスしたりできます。
MITRE ATT&CK™ Framework Tactics と Techniques の情報	Deep Discovery Director (統合モード) の検出の詳細と分析レポートに、MITRE ATT&CK™ Framework Tactics と Techniques の情報が含まれます。
高度な脅威分析	Deep Discovery Director (Standalone Network Analytics モード)または Deep Discovery Director - Network Analytics as a Service で動作する複数の Deep Discovery Director (Internal Network Analytics バージョン)サーバとの統合により、相関データを使用した高度な脅威分析が可能です。
Deep Discovery Inspector のログの集約	Deep Discovery Inspector の検出ログを集約します。Deep Discovery Director (統合モード) の管理コンソールでは、直感的に使用できるさまざまな方法で脅威をリアルタイムに視認して分析できます。このため、セキュリティ担当者は、実際のリスクに集中してフォレンジック分析を詳細に行い、封じ込めや修正の措置をただちにとることができます。

機能または利点	詳細
Deep Discovery Email Inspector のログの集約	Deep Discovery Email Inspector の検出、メールメッセージ追跡、および MTA のログを集約します。Deep Discovery Director (統合モード) の管理コンソールでは、Deep Discovery Email Inspector ユーザが使い慣れた直感的に使用できるさまざまな方法で脅威をリアルタイムに視認して分析できます。
製品インテリジェンス	登録済みの Deep Discovery アプライアンスで検出された不審オブジェクトや C&C コールバックアドレスを一元管理します。
カスタムインテリジェンス	登録済みのアプライアンスに YARA ルールを配信したり、STIX (Structured Threat Information eXpression) 1.x および 2.0 形式で脅威インテリジェンスをインポートしたりできます。ネットワークで検出されていないユーザ指定の不審オブジェクトを追加したり、無害と思われる対象の除外を追加したりすることもできます。
フィードの管理	脅威情報のインテリジェンスフィードを登録および監視して、製品やカスタムインテリジェンスの補完として使用できます。
脅威インテリジェンスの共有	TAXII (1.x、2.0)、OpenDXL、および HTTP または HTTPS Web サービスを使用して、脅威インテリジェンスデータを他の製品またはサービスと共有できます。
補助製品とサービス	脅威を効果的に検出してネットワーク侵入前に阻止するため、脅威インテリジェンスのデータを補助製品やサービスに配信できます。
ファイルパスワードの同期	ファイルパスワードを設定して、登録済みの Deep Discovery Analyzer および Deep Discovery Email Inspector アプライアンスと同期できます。
Email Encryption の管理	Email Encryption の機能に関連する設定を行い、登録済みの Deep Discovery Email Inspector アプライアンスと同期できます。 **注意** 日本語版では Email Encryption 機能をご利用いただけません。
ダッシュボード	管理者は [ダッシュボード] 画面や Deep Discovery アプライアンスのウィジェットを使用して、ネットワークの整合性、システム脅威データ、メールメッセージの検出、およびセキュリティ情報を表示できます。

機能または利点	詳細
検出	[検出] 画面から、さまざまな検出カテゴリに関するリアルタイムの情報にアクセスできます。
アプライアンスのログ	[ログ] 画面から、メールメッセージ追跡、MTA、および メッセージキューのログなど、Deep Discovery アプライアンス関連のログを検索できます。
Syslog	[Syslog] 画面では、不審オブジェクトのリストや、検出およびアプライアンスに関連する CEF および LEEF 形式のログを最大 3 つの Syslog サーバに送信できます。
システムアラート	実行されたアラートの詳細を管理コンソールで直接表示できます。カスタムルールを作成して、特定の脅威に対するアラートを生成できます。
レポート	予約および手動による [ネットワークセキュリティ] および [メールセキュリティ] レポートを生成できます。
Simple Network Management Protocol	SNMP (Simple Network Management Protocol) がサポートされます。これにより、管理者に SNMP トラップメッセージを送信して注意が必要なイベントについて通知したり、システム情報やステータスアップデートに対する SNMP マネージャからの要求を待機したりすることができます。
役割ベースのアクセス制御	組み込みの役割を使用して、管理コンソールの各画面と機能へのアクセスを制御することができます。役割をカスタマイズすると、表示および管理可能なアプライアンスや表示可能なメールメッセージの検出を制御できます。
ストレージの設定	Deep Discovery Director (統合モード) のパーティションに使用可能なディスク容量を追加して、保存可能なログやリポジトリのファイル数を増やすことができます。
ディレクトリ	[ディレクトリ] には、Deep Discovery Director (統合モード) に登録された Deep Discovery のアプライアンスについての情報が表示されます。
計画	対象アプライアンスへの配信の範囲とスケジュールを指定できます。

機能または利点	詳細
リポジトリ	[リポジトリ] 画面には、すべてのアップデート、アップグレードパッケージおよびサーバでホストされる仮想アナライザイメージファイルが表示されます。ファイルはここでアップロードおよび削除します。
コンポーネントのアップデート	Deep Discovery Director (統合モード) ではコンポーネントを使用して、検出についての関連情報を表示します。
アップデート	[アップデート] 画面では、HotFix、Patch、およびファームウェアのアップグレードを Deep Discovery Director (統合モード) にインストールできます。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。
Microsoft Active Directory との統合	Deep Discovery Director (統合モード) の管理コンソールへのアクセスに Active Directory アカウントを使用することができます。
SAML によるシングルサインオン (SSO) のサポート	Okta および Active Directory フェデレーションサービス (AD FS) の ID プロバイダを使用した SAML (Security Assertion Markup Language) 認証標準がサポートされ、ユーザは組織のポータルにサインインすることで、Deep Discovery Director (統合モード) コンソールにシングルサインオンできるようになります。
システムログ	Deep Discovery Director (統合モード) には、ユーザアクセス、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。
[隔離メッセージ] 画面	機能強化された [検出] セクションから隔離メールメッセージにアクセスできます。
メールメッセージキューの管理	登録済みの Deep Discovery Email Inspector アプライアンスのメールキューを管理できます。
エンドユーザメール隔離	Deep Discovery Director (統合モード) には、スパムメールの管理を強化するエンドユーザメール隔離 (EUQ) 機能があります。
Trend Micro Apex Central™の統合	Deep Discovery Director (統合モード) はエンドポイント分析レポートを取得する目的で Apex Central と統合され、より多くのデータを Deep Discovery Director - Network Analytics as a Service に提供することで詳細かつ高度な脅威分析を可能にします。

機能または利点	詳細
Web API アクセス	Web API を介したシステムへのアクセスのみを許可するユーザアカウントを作成できるようになります。Web API を使用すると、特定の脅威インテリジェンス関連のタスクを自動化できます。

第 2 章

インストール

この章では、Deep Discovery Director (統合モード) をインストールするための要件と手順について説明します。

システム要件

システム要件については、次の Web サイトを参照してください。

https://www.go-tm.jp/ddd

注意

システム要件に記載されている OS の種類やハードディスク容量などは、OS のサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

推奨されるシステム要件

Deep Discovery Director (統合モード) での検出ログおよびアプライアンスログの集約が必要な Deep Discovery アプライアンスの数に応じて、CPU、メモリ、およびハードディスクの要件は異なります。

注意

ハードディスクの要件は、180 日間の検出ログのストレージを基準として計算されます。検出ログの保持期間が長いほど、必要なディスク容量は増えます。

DDI1100/DDEI7100 アプライアンスの数	CPU (コア数)	メモリ (GB)	ハードディスク (GB)
5	4	16	600
15	8	28	1200
25	12	40	1800

Deep Discovery Director をインストールする

重要

Deep Discovery Director (統合モード) では、レガシー BIOS (Basic Input/Output System) または UEFI (Unified Extensible Firmware Interface) でのインストールがサポートされます。

- インストール後に設定を変更すると、Deep Discovery Director (統合モード) を起動できなくなります。
- 設定を変更するには、Deep Discovery Director (統合モード) を再インストールする必要があります。

手順

1. 次の最小限の仕様を満たすカスタム仮想マシンを作成します。
   - 仮想マシンのハードウェアバージョン: 8
   - ゲスト OS: CentOS Linux 6/7 (64 ビット) または Red Hat Enterprise Linux 7 (64 ビット)
   - CPU: 1 仮想ソケット 2 コア
   - メモリ: 10GB
   - ネットワークインタフェースカード: 1 枚、E1000 または VMXNET 3 アダプタを装備

     重要

     - Deep Discovery Director (統合モード) では、VMXNET 2 (拡張) アダプタはサポートされません。
     - ポートバインディングのため、すべてのネットワークインタフェースカードで同じ種類のアダプタを指定します。
   - SCSI コントローラ: LSI Logic パラレル
   - ハードディスク: 150GB

2. 仮想マシンコンソールを開き、仮想マシンの電源を入れます。
3. 仮想マシンの CD/DVD デバイスを Deep Discovery Director の ISO イメージファイルに接続し、仮想マシンを CD/DVD ドライブから起動します。

   Deep Discovery Director (統合モード) のインストール画面が表示されます。
4. [Install software] を選択します。

   [Install Deep Discovery Director Software] 画面が表示されます。
5. [Install in consolidated mode] を選択します。

   [Install in Consolidated Mode] 画面が表示されます。
6. 次のインストールオプションのいずれかを選択します。

   - Install base version: Deep Discovery ファミリのすべてのアプライアンスを管理できます。Internal Network Analytics はありませんが、Deep Discovery Director - Network Analytics as a Service に登録できます。
   - Install no log receiving capability version: Deep Discovery ファミリのすべてのアプライアンスを管理できますが、Internal Network Analytics もログ受信機能もありません。

   注意

   このオプションは後から変更できません。オプションを変更するには、Deep Discovery Director (統合モード) を再インストールする必要があります。

   [ディスクの選択] 画面が表示されます。
7. [続行] をクリックします。

   [ハードウェアプロファイル] 画面が表示されます。
8. [続行] をクリックします。

   [ディスク容量の設定] 画面が表示されます。

9. (オプション) ディスク容量の設定を変更し、[続行] をクリックします。

   [ディスクの再パーティション] 確認メッセージが表示されます。

10. [続行] をクリックします。

    インストールが開始されます。

ネットワークを設定する

手順

1. 事前設定コンソールにログオンします。

   初期設定の認証情報は次のとおりです。

   - ユーザ名: admin
   - パスワード: admin

   [Main Menu] 画面が表示されます。

2. [Configure network settings] を選択し、<Enter> キーを押します。

   [Configure network settings] 画面が表示されます。

3. 次の必要な設定を行います。

   - IPv4 アドレス (IPv4 address)
   - サブネットマスク (Subnet mask)
   - IPv4 ゲートウェイ (IPv4 gateway)
   - DNS サーバ 1 (DNS server 1)

注意

事前設定コンソールでは IPv4 のみ設定できます。IPv6 とポートバインディングを設定するには、管理コンソールの [ネットワーク] 画面を使用します。

4. <Tab> キーを押して [Save] に移動し、<Enter> キーを押します。

   設定が正常に保存されると、[Main Menu] 画面が表示されます。

管理コンソールにログオンする

手順

1. ブラウザ画面を開き、事前設定コンソールで指定したサーバアドレスに接続します。

   管理コンソールのログオン画面が表示されます。

2. 次の初期設定のアカウント情報を入力します。

   - ユーザ名: admin
   - パスワード: admin

   重要

   管理コンソールに初めてログオンした場合は、ただちにパスワードを変更することをお勧めします。

3. [ログオン] をクリックします。

   管理コンソールが表示されます。

統合ソリューションの導入の概要

統合ソリューションの一部である Deep Discovery Director - Network Analytics as a Service は、一定期間に検出された脅威イベントを関連付け、ネットワーク内で脅威がどのように始まり進化するのかを特定することで高度な脅威分析を提供します。

この統合ソリューションには、次の 3 つのトレンドマイクロ製品が必要です。

- Deep Discovery Director - Network Analytics as a Service

  Deep Discovery Inspector により検出された脅威について、相関データおよび高度な脅威分析を提供します。

- Deep Discovery Inspector

  データの関連付けおよび高度な脅威分析のために使用される、ネットワークメタデータおよび検出ログを提供します。

- Deep Discovery Director (統合モード)

  この統合ソリューションのサービスは Deep Discovery Director (統合モード) のコンソールを使用して配信および管理されます。Deep Discovery Director (統合モード) から、相関データおよび分析結果が表示される [相関データ] 画面にアクセスすることもできます。

配信前チェックリスト

Deep Discovery Director - Network Analytics as a Service は、Deep Discovery Director (統合モード) および Deep Discovery Inspector と統合されたクラウドベースソリューションです。

このサービスは Deep Discovery Director (統合モード) コンソールを使用してライセンス認証および管理されます。サービスで提供される詳細分析データは、Deep Discovery Director (統合モード) コンソールからアクセスする [相関データ] 画面に表示されます。

ライセンスをアクティベートすると、Deep Discovery Director (統合モード) コンソール上で、接続済みソースとして使用する Deep Discovery Inspector アプライアンスを選択できます。この接続済みソースを使用して、詳細分析の関連付けのためのデータが収集されます。

接続済みソースとして使用するすべての Deep Discovery Inspector アプライアンスは、Deep Discovery Director (統合モード) アプライアンスに登録する必要があります。

各 Deep Discovery Director (統合モード) アプライアンスは、単一のサービスのみを管理できます。各サービスは、1 台以上の統合された Deep Discovery Inspector アプライアンスを接続済みデータソースとして使用できます。

ネットワーク分析ソリューションの一部として、[相関データ] 画面から、Apex Central によって提供されるエンドポイント分析レポートにアクセスできます。エンドポイント分析レポートを取得するには、Apex Central で Deep Discovery Director (統合モード) をアプライアンスとして追加する必要があります。

表 2-1. 配信前チェックリスト

要件	詳細
Deep Discovery Director (統合モード) 5.0 以降	管理やアクセスに利用します。
Deep Discovery Inspector 5.5 以降	関連付けと詳細分析のために使用するネットワークメタデータおよび検出ログを提供します。
Deep Discovery Director - Network Analytics as a Service のアクティベーションコードの取得	トレンドマイクロから取得します。
Deep Discovery Director (統合モード) での前提条件となる設定の完了	Deep Discovery Director - Network Analytics as a Service を配信する前に、Deep Discovery Director (統合モード) ライセンスがアクティベート済みであることと、基本設定が完了していることを確認します。 Deep Discovery Director (統合モード) の設定には、次のものを含める必要があります。 • ネットワーク • プロキシ (使用する場合) • SMTP サーバ (アラートに使用) • NTP の日時 • 証明書 • 自動バックアップ設定

要件	詳細
Deep Discovery Inspector の Deep Discovery Director (統合モード) への登録	詳細分析と関連付けのための検出ログを送信するすべての Deep Discovery Inspector アプライアンスは、Deep Discovery Director (統合モード) アプライアンスに登録する必要があります。 これは、Deep Discovery Inspector コンソールから実行します。
Apex Central で Deep Discovery Director (統合モード) をアプライアンスとして追加	エンドポイント分析レポートを取得するには、Apex Central に Deep Discovery Director (統合モード) をアプライアンスとして追加する必要があります。 これは、Apex Central 管理コンソールから実行します。
インターネットに接続可能なコンピュータ	サービスの配信に使用する Deep Discovery Director (統合モード) 管理コンソールへのアクセスに使用します。

第 3 章

ダッシュボード

[ダッシュボード] 画面に表示される情報については、次の項目を参照してください。

ダッシュボードの概要

ネットワークの整合性をダッシュボードで監視します。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。

使用可能なウィジェットで Deep Discovery Director (統合モード) のダッシュボードをカスタマイズできます。これにより、ネットワークに関する正確なシステムステータスと脅威の情報を必要なときに取得できます。

タブ

タブはウィジェットを含めるコンテナです。

ダッシュボードでは最大 30 個のタブを使用できます。ダッシュボードの各タブには、最大 8 個のウィジェットを含めることができます。

タブのタスク

タスク	手順
タブの追加	ダッシュボード上部のプラス記号のアイコンをクリックします。
タブの名前の変更	1. 名前を変更するタブを選択します。 2. タブタイトルの横にあるメニューアイコンをクリックし、[名前の変更] を選択します。 3. 最大 64 文字で名前を入力します。
タブの移動	タブのタイトルをドラッグアンドドロップして位置を変更します。
タブの削除	1. 削除するタブを選択します。 2. タブタイトルの横にあるメニューアイコンをクリックし、[削除] 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主要なコンポーネントです。ウィジェットには見やすいグラフが表示されるため、脅威を追跡し、1 つ以上のソースから収集したログと関連付けることができます。

各ウィジェットをカスタマイズして、ネットワークの状態と脆弱性を明確に示すスナップショットを提供できます。

ウィジェットのタスク

タスク	手順
ダッシュボードへのウィジェットの追加	ダッシュボードにウィジェットを追加するには、次のいずれかを実行します。 ・ ウィジェットを追加するタブを選択し、タブタイトルの横にあるメニューアイコンをクリックして、[ウィジェットの追加] を選択します。 ・ ウィジェットを追加するタブを選択し、画面の右上隅にある歯車のアイコンをクリックして、[ウィジェットの追加] を選択します。 ・ 新しく作成したタブで、[ウィジェットを追加してください] 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、41 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。
新規ウィジェットの作成	新しいカスタムウィジェットを作成して、関心のある情報を追跡および監視します。 詳細については、42 ページの「ウィジェットを作成する」を参照してください。

タスク	手順
ウィジェットの表示の更新	ウィジェットの右上隅にあるメニューアイコンをクリックして、更新アイコンを選択します。 **注意** ウィジェットの表示は自動的に更新されます。ウィジェットごとに異なる更新間隔を設定できます。
ウィジェットの編集	ウィジェットの右上隅にあるメニューアイコンをクリックして、編集アイコンを選択します。[ウィジェットの編集] ダイアログが表示されます。 詳細については、42 ページの「ウィジェットを編集する」を参照してください。 **注意** ウィジェットの種類に応じて設定内容は異なります。
ウィジェットの削除	ウィジェットの右上隅にあるメニューアイコンをクリックして、削除アイコンを選択します。 **注意** ウィジェットは、[ウィジェットの追加] 画面からも削除できます。[ウィジェットの追加] 画面から削除する場合は、ダッシュボード上のすべてのインスタンスに影響し、削除したウィジェットを復元することはできません。
ウィジェットの移動	ウィジェットのタイトルをドラッグアンドドロップして位置を変更します。
ウィジェットのサイズ変更	ウィジェットの右下隅のサイズ変更アイコンをドラッグしてサイズを変更します。

ダッシュボードにウィジェットを追加する

手順

1. [ダッシュボード] 画面で、次のいずれかを実行します。

   - ウィジェットを追加するタブを選択し、タブタイトルの横にあるメニューアイコンをクリックして、[ウィジェットの追加] を選択します。
   - ウィジェットを追加するタブを選択し、画面の右上隅にある歯車のアイコンをクリックして、[ウィジェットの追加] を選択します。
   - 新しく作成したタブで、[ウィジェットを追加してください] 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。

2. 追加するウィジェットを探すには、次のいずれかを実行します。

   - ドロップダウンリストからカテゴリを選択して、表示するウィジェットの数を減らします。
   - 画面上部にある検索テキストボックスにウィジェット名またはウィジェット名の一部を入力して、ウィジェットを検索します。

   ヒント

   カスタムウィジェットを作成して、ダッシュボードに追加することもできます。詳細については、42 ページの「ウィジェットを作成する」を参照してください。

3. ダッシュボードに追加するウィジェットを選択します。ダッシュボードの各タブには、最大 8 個のウィジェットを含めることができます。

4. [追加] をクリックします。

   選択したウィジェットがダッシュボードに追加されます。

ウィジェットを作成する

手順

1. [ダッシュボード] 画面を表示して、いずれかのタブを選択します。
2. 画面の右上隅にある歯車のアイコンをクリックして、[新規ウィジェットの作成] を選択します。

   [新規ウィジェットの作成] 画面が表示されます。
3. 次の設定を行います。
   a. ウィジェットの一意の名前を入力します。
   b. ウィジェットに使用するフィルタを選択します。[ネットワーク検出] および [メールメッセージ] の保存された検索条件のみを選択できます。
   c. ウィジェットの説明を入力します。
   d. グラフの種類を選択し、表示するデータを設定します。

   注意
   - グラフの種類に応じて設定内容は異なります。
   - サンプルのグラフは、選択した期間に関係なく、過去 24 時間のデータのみを使用して作成されます。
4. [保存] をクリックします。

   ウィジェットが作成され、[ウィジェットの追加] 画面に追加されます。

ウィジェットを編集する

手順

1. [ダッシュボード] 画面に移動し、編集するウィジェットを含むタブを選択します。

2. ウィジェットの右上隅にあるメニューアイコンをクリックして、編集アイコンを選択します。

   [ウィジェットの編集] ダイアログが表示されます。

3. ウィジェットを設定します。

   注意

   - ウィジェットの種類に応じて設定内容は異なります。
   - ダイアログには、グラフのサンプルは表示されません。

4. [OK (成功)] をクリックします。

Deep Discovery Inspector のウィジェット

Deep Discovery Director (統合モード) には、次の Deep Discovery Inspector のウィジェットが含まれています。

表 3-1. Deep Discovery Inspector のウィジェット

ウィジェット	説明
脅威検出状況の概要	このウィジェットには、6 つの主要なメトリックについての実行可能な情報と、対応する検出ログのリンクが表示されます。
影響を受けたホストの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間で重大度が最も高かったホストが、重大度別に表示されます。
検索されたプロトコル別トラフィック	このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間のプロトコル別の総トラフィック量が表示されます。
脅威のグラフィック地図 - C&C 通信	このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間に C&C 通信が検出され、影響を受けたホストが仮想世界地図上にグラフィカル表示されます。

脅威検出状況の概要

このウィジェットには、6 つの主要なメトリックについての実行可能な情報と、対応する検出ログのリンクが表示されます。

表 3-2. 脅威検出状況の概要

メトリック	ソース	説明
標的型攻撃の検出	影響を受けたホスト	• 影響を受けたホストの数を表示します。 • 事前設定された検索フィルタ [標的型攻撃の検出] に関連付けられています。 値をクリックすると、[影響を受けたホスト] 画面に詳細が表示されます。
C&C 通信の検出	影響を受けたホスト	• 影響を受けたホストの数を表示します。 • 事前設定された検索フィルタ [C&C 通信の検出] に関連付けられています。 値をクリックすると、[影響を受けたホスト] 画面に詳細が表示されます。
内部活動の検出	影響を受けたホスト	• 影響を受けたホストの数を表示します。 • 事前設定された検索フィルタ [内部活動の検出] に関連付けられています。 値をクリックすると、[影響を受けたホスト] 画面に詳細が表示されます。
ランサムウェア	ネットワーク検出	• 検出数を表示します。 • 事前設定された検索フィルタ [ランサムウェア] に関連付けられています。 値をクリックすると、[ネットワーク検出] 画面に詳細が表示されます。

メトリック	ソース	説明
潜在的な脅威	ネットワーク検出	• 検出数を表示します。 • 事前設定された検索フィルタ [潜在的な脅威] に関連付けられています。 値をクリックすると、[ネットワーク検出] 画面に詳細が表示されます。
メールによる脅威	ネットワーク検出	• 検出数を表示します。 • 事前設定された検索フィルタ [メールによる脅威] に関連付けられています。 値をクリックすると、[ネットワーク検出] 画面に詳細が表示されます。

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

影響を受けたホストの上位

このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間で重大度が最も高かったホストが、重大度別に表示されます。

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

検索されたプロトコル別トラフィック

このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間のプロトコル別の総トラフィック量が表示されます。

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

脅威のグラフィック地図 - C&C 通信

このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間に C&C 通信が検出され、影響を受けたホストが仮想世界地図上にグラフィカル表示されます。

[脅威のグラフィック地図 - C&C 通信] には、影響を受けたホストの所在地が赤色の円で表示されます。

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

YARA ルールでのネットワーク検出の上位

このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間で、ネットワーク検出において検出数が最も多かった YARA ルールファイルが表示されます。

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

Deep Discovery Email Inspector のウィジェット

Deep Discovery Director (統合モード) には、次の Deep Discovery Email Inspector のウィジェットが含まれています。

表 3-3. Deep Discovery Email Inspector のウィジェット

ウィジェット	説明
メールメッセージの検出のサマリー	このウィジェットには、さまざまな脅威の種類の検出数が表示されます。

ウィジェット	説明
メールメッセージの高度な脅威インジケータ	このウィジェットには、すべてのメールメッセージで検出された高度な脅威インジケータの種類、量、およびリスクレベルが表示されます。
メールメッセージの攻撃元	このウィジェットには、不審なメールトラフィックをルーティングしたすべてのソース MTA がインタラクティブなマップに表示されます。

メールメッセージの検出のサマリー

このウィジェットには、さまざまな脅威の種類の検出数が表示されます。

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

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

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

メールメッセージの高度な脅威インジケータ

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

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

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

注意

[ウィジェットの編集] ダイアログで [表示データ] ドロップダウンリストから [使用不可] を選択すると、[使用不可] リスクレベルの検出が表示されます。

メールメッセージの攻撃元

このウィジェットには、不審なメールトラフィックをルーティングしたすべてのソース MTA がインタラクティブなマップに表示されます。

攻撃の発生元とは、不審メッセージをルーティングするパブリック IP アドレスを持つ最初の MTA です。たとえば、不審メッセージが IP1 (送信者)→IP2 (MTA: 203.0.113.1)→IP3 (会社のメールゲートウェイ)→IP4 (受信者) とルーティングされた場合は、203.0.113.1 (IP2) が攻撃の発生元として識別されます。攻撃の発生元を判別することで、地域の攻撃パターンまたは同じメールサーバが関係する攻撃パターンを特定できます。

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

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

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

YARA ルールでのメールメッセージ検出の上位

このウィジェットには、過去 1 時間、24 時間、7 日間、14 日間、30 日間、または 90 日間で、メールメッセージにおいて検出数が最も多かった YARA ルールファイルが表示されます。

初期設定の期間は [過去 24 時間] です。

ウィジェットの右上隅にあるメニューアイコンをクリックし、編集アイコンを選択してウィジェットを設定します。

第 4 章

検出

[検出] 画面に表示される情報については、次の項目を参照してください。

[検出] 画面について

[検出] 画面では、次の検出カテゴリに関するリアルタイムの情報にアクセスできます。

表 4-1. [検出]

検出のカテゴリ	説明
影響を受けたホスト	標的型攻撃の 1 つ以上の段階に関係しているホスト。 詳細については、60 ページの「影響を受けたホスト」を参照してください。 ホストの重大度の詳細については、51 ページの「ホストの重大度」を参照してください。
ネットワーク検出	グローバルインテリジェンス、ユーザ定義リスト、およびその他のソースを含む、すべてのイベントログからの検出と一致するホスト。 詳細については、102 ページの「ネットワーク検出」を参照してください。
メールメッセージ	不正または不審なコンテンツ、埋め込みリンク、添付ファイル、あるいはソーシャルエンジニアリング攻撃に関連した特徴が含まれるメールメッセージ。 詳細については、131 ページの「メールメッセージ」を参照してください。 メールメッセージのリスクレベルの詳細については、54 ページの「メールメッセージのリスクレベル」を参照してください。 メールメッセージの脅威の種類の分類の詳細については、57 ページの「メールメッセージの脅威の種類の分類」を参照してください。

検出のカテゴリ	説明
隔離メッセージ	特定のポリシー条件に一致したために隔離されたメールメッセージ。 詳細については、147 ページの「隔離メッセージ」を参照してください。 隔離の理由の詳細については、152 ページの「隔離の理由」を参照してください。
相関イベント	ネットワーク内の複数の検出の相関データから得られた、1 つ以上の攻撃パターンを示すイベント。 詳細については、160 ページの「相関イベント」を参照してください。 **注意** Deep Discovery Director - Network Analytics で相関データを提供するプロトコルや、相関データが表示されない場合の理由については、次を参照してください。 • 58 ページの「相関データを使用した詳細分析をサポートするプロトコル」 • 59 ページの「相関が検出されない理由」

ホストの重大度

ホストの重大度とは、トレンドマイクロ製品およびサービスによって判断されたホストに対する影響を指します。

イベントセキュリティよりもさらに詳しく調査することで、ホストの重大度の数値スケールは、最も脆弱なホストを明らかにし、優先度を設定して迅速に対応することを可能にします。

ホストの重大度は、ホストに影響するイベントの重大度の集約と相関分析に基づいています。複数のイベントが 1 つのホストに影響しており、関係が検

出されなかった場合、そのホストの重大度は、それらのイベントのうち最も高いイベントの重大度に基づきます。ただし、イベントに相関性が検出された場合、ホストの重大度のレベルはそれに従って高くなります。

例: あるホストに影響を与える 5 つのイベントのうち、最も高いリスクレベルが「中」だとします。イベント間に相関性がない場合、そのホストの重大度レベルは、最も高いリスクレベルの「中」に基づきます。ただし、イベントに相関性がある場合、ホストの重大度のレベルは検出された相関性に基づいて高くなります。

ホストの重大度スケールは、複数の検出テクノロジからの脅威データベースを統合し、全体的な重大度の判断を容易にします。この情報と、関連する脅威応答ポリシーに基づいて、応答に優先度を設定できます。

表 4-2. ホストの重大度スケール

カテゴリ	レベル	説明
重大 (Critical) 侵害されていることを明確に示す動作がホストから検出されています。	10	ホストが次のような侵害の証拠を示します。 • 情報送出 • 複数の感染ホスト/サーバ
	9	ホストが次のような APT による侵害の兆候を示します。 • 既知の APT に関連付けられた IP アドレスへの接続 • 既知の APT に関連付けられた URL へのアクセス • 既知の APT に関連付けられたダウンロードファイル • 内部活動の証拠
	8	ホストは次を示している可能性があります。 • 重大度が高のネットワークイベント • Web レピュテーションサービスにより検出された C&C サーバへの接続 • 仮想アナライザにより高リスクと評価されたダウンロードファイル

カテゴリ	レベル	説明
メジャー (Major) 既知の不正な動作または攻撃の対象となり、侵害された可能性を示す動作がホストから検出されています。	7	ホストは次を示している可能性があります。 • 不正プログラムのダウンロード。ユーザが関与した証拠はありません。 • セキュリティホール悪用の検出
	6	ホストは次を示している可能性があります。 • Web レピュテーションサービスにより検出された危険なサイトへの接続
	5	ホストは次を示している可能性があります。 • 中～低リスクの不正と思われるダウンロードされたファイル。ユーザが関与した証拠はありません。
	4	ホストは次を示している可能性があります。 • 重大度が中のネットワークイベント • 仮想アナライザにより中リスクと評価されたダウンロードファイル
マイナー (Minor) 無害の可能性もあれば脅威を示している可能性もある、異常または不審動作がホストから検出されています。	3	ホストは次を示している可能性があります。 • ログオン試行の連続した失敗または異常な使用パターン • パックされた実行可能ファイルまたは不審ファイルのダウンロードまたは拡散 • IRC、TOR、またはトンネリングソフトウェアを実行している証拠
	2	ホストは次を示している可能性があります。 • 重大度が低のネットワークイベント • 危険な URL を含むメールメッセージを受信した証拠 • 仮想アナライザにより低リスクと評価されたダウンロードファイル

カテゴリ	レベル	説明
軽微 (Trivial) ホストは正常な動作を示していますが、これは無害の可能性もあれば、将来不正なアクティビティとして識別される脅威を示している可能性もあります。	1	ホストは次を示している可能性があります。 • 重大度が情報のネットワークイベント • Web レピュテーションサービスにより検出された未テストまたは新規ドメインとして評価されたサイトへの接続 • P2P などの要注意アプリケーションを実行している証拠

メールメッセージのリスクレベル

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

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

表 4-3. メールメッセージのリスク定義

リスクレベル	説明
高	リスク高のメールメッセージは次のとおりです。 • 仮想アナライザにリスク高として検出された未知の脅威の添付ファイル • YARA ルールに基づきリスク高として検出された添付ファイル • 不審ファイルの一致に基づきリスク高として検出された添付ファイル • 機械学習型検索およびメール不正プログラム脅威検索により検出された添付ファイル • ビジネスメール詐欺 • 仮想アナライザにリスク高として検出されたリンク • 不審 URL の一致に基づきリスク高として検出されたリンク
中	リスク中のメールメッセージは次のとおりです。 • 既知の不正プログラム • 既知のフィッシング脅威 • 既知の危険なリンク • YARA ルールに基づきリスク中として検出された添付ファイル • 不審 URL の一致に基づきリスク中として検出されたリンク

リスクレベル	説明
低	リスク低のメールメッセージは次のとおりです。 • 既知の極めて不審な、または不審なリンク (アグレッシブモード) • 仮想アナライザにリスク低として検出されたリンク • 仮想アナライザにリスク低として検出された添付ファイル • YARA ルールに基づきリスク低として検出された添付ファイル • 不審 URL の一致に基づきリスク低として検出されたリンク • ソーシャルエンジニアリング攻撃 • ビジネスメール詐欺 (BEC)
リスクなし	リスクのないメールメッセージ: • 不審な添付ファイルやリンクは含まれない • 既知の極めて不審な、または不審なリンクを含む (標準モード) • ポリシー除外条件に一致する

リスクレベル	説明

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

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

メールメッセージの脅威の種類の分類

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

表 4-4. メールメッセージの脅威の種類

脅威の種類	分類
標的型不正プログラム	上司や同僚など、ユーザがメールメッセージの送信元として予期する相手から送信されたかのように見せかける不正プログラム

脅威の種類	分類
不正プログラム	コンピュータシステムに対する妨害、制御、盗難、データ喪失、スパイ、または無許可のアクセスを目的として攻撃者によって使用される不正なソフトウェア
不正 URL	既知の不正な Web サイトにリンクする、メールメッセージに埋め込まれたハイパーリンク
不審ファイル	不正な特徴を示すファイル **重要** 不審ファイルは十分に注意して処理してください。
不審 URL	未知の不正な Web サイトにリンクする、メールメッセージに埋め込まれたハイパーリンク
フィッシング	ユーザを正規の Web サイトになりすましたサイトに誘導することで、個人情報を漏えいさせようとするメールメッセージ
スパムメール/グレーメール	受信者の意向を無視して複数の個人に無差別に送り付けられる、主に商品の宣伝を目的としたメールメッセージ グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールのことを指す
コンテンツ違反	私信やサイズの大きな添付ファイルなど、不適切だと思われるコンテンツ

相関データを使用した詳細分析をサポートするプロトコル

Deep Discovery Director - Network Analytics では、次のプロトコルの相関データが提供されます。

- HTTP

- HTTPS
- SSL
- FTP/FTP データ
- RDP
- SMB/SMB2
- KRB5
- SMTP

相関が検出されない理由

Deep Discovery Director - Network Analytics で相関が検出されない場合、次のような理由があります。

- 致命的エラーの原因となる無効なデータを受信しました。再度実行してください。
- セッションが無効です。Deep Discovery Director に再ログインして、再度実行してください。
- 相関の検出中に無効なパラメータが検出されました。エラーが解決された後、再度実行してください。
- 相関の検出中にクライアントエラーが発生しました。エラーが解決された後、再度実行してください。
- 相関の検出中に無効な応答がありました。エラーが解決された後、再度実行してください。
- 相関の検出中に内部エラーが発生しました。エラーが解決された後、再度実行してください。
- 選択したインシデントは安全なサーバのリストにあるクライアントで発生しているため、相関を得られませんでした。
- 選択したイベントのプロトコルはサポートされていないため、相関を得られませんでした。

- 現在、選択したインシデントには相関が検出されていません。システムが相関の検出を実行中です。
- 選択したインシデントには相関が検出されていません。相関の検出はこれ以上試行されません。
- 選択したイベントが見つからなかったため、相関を得られませんでした。
- 選択した不審オブジェクトはドメインの除外リストに含まれているため、相関を得られませんでした。
- 致命的エラーの原因となる無効なデータを受信しました。再度実行してください。
- データがないため、相関グラフはレンダリングされませんでした。

影響を受けたホスト

[影響を受けたホスト] 画面には、標的型攻撃の 1 つ以上の段階に関係しているホストに関する情報が表示されます。

イベントセキュリティよりもさらに詳しく調査することで、ホストの重大度の数値スケールは、最も脆弱なホストを明らかにし、優先度を設定して迅速に対応することを可能にします。ホストの重大度スケールの詳細については、51 ページの「ホストの重大度」を参照してください。

次のビューで、影響を受けたホストに関するさまざまな情報にアクセスできます。

1. [影響を受けたホスト] ビュー:
   - 攻撃段階ごとに影響を受けたホストの概要を表示します。
   - IP アドレスをクリックすると、[ホストの詳細] ビューが表示されます。

     初期設定では、[IP アドレス] および [ホスト名] 別に [影響を受けたホスト] ビューから検索できます。
2. [ホストの詳細] ビュー:

- ホストイベントの詳細を時系列で表示します。
- [詳細] 列のアイコンをクリックすると、[検出の詳細] ビューが表示されます。
- 初期設定では、[ピアホスト] の IP アドレスとホスト名で [影響を受けたホスト] - [ホストの詳細] 画面から検索できます。

3. [検出の詳細] ビュー:
   - 検出された各脅威の詳細を表示します。
   - 検索やその他のフィルタ条件と設定に応じて、異なる情報パネルへのアクセスを提供します。

表示オプションと検索フィルタ

表示をカスタマイズするには、次の表示オプションと検索フィルタを適用してください。

表 4-5. 表示オプションと検索フィルタ: [影響を受けたホスト]

フィルタオプション	説明	
検出の重大度	フィルタオプションには、次の検出の重大度設定が含まれます。	
	高	重大度が高の検出を表示します
	中	重大度が中の検出を表示します
	低	重大度が低の検出を表示します
	情報	情報検出を表示します
	すべての検出の重大度レベル	すべての検出を表示します

フィルタオプション	説明
期間	過去 24 時間
	過去 7 日間
	過去 14 日間
	過去 30 日間
	過去 60 日間
	カスタム範囲
データソース	データソースとして含めるアプライアンスを選択します。
列のカスタマイズ	列を表示したり非表示にして表示をカスタマイズします
基本検索	IP アドレスまたはホスト名を検索します。 注意 基本検索フィールドにキーワードを入力してホストの部分一致を検索します。大文字と小文字は区別されません。

保存された検索条件	保存された検索条件で検索します。
	• [影響を受けたホスト] ビューには、次の組み込みの保存された検索条件が含まれています。
	  • 標的型攻撃の検出
	  • C&C 通信の検出
	  • 内部活動の検出
	• [ホストの詳細] ビューには、次の事前設定された検索条件が含まれています。
	  • 脅威
	  • 既知の脅威
	  • 潜在的な脅威
	  • ランサムウェア
	  • YARA ルール検出

フィルタオプション	説明
詳細検索	ユーザ定義の条件セットによる検索を行います。 各セットには次のものが 1 つ以上含まれます。 • 属性 • 演算子 • 関連付けられた値 詳細については、84 ページの「[影響を受けたホスト] の詳細検索フィルタ」を参照してください。

[影響を受けたホスト] を表示する

手順

1. [検出] > [影響を受けたホスト] の順に選択します。

   [影響を受けたホスト] 画面が表示されます。

2. ドロップダウンコントロールを使用して検出の重大度を選択します。
3. 期間を選択します。
4. データソースとして含めるアプライアンスを選択します。
5. (オプション) [詳細] の横にある [その他] アイコンをクリックして [列のカスタマイズ] を選択し、非表示または表示にする列を選択します。次に [適用] をクリックして、変更した [影響を受けたホスト] 画面に戻ります。

   表 4-6. [ホスト情報] の列

列の名前	事前選択済み	説明
IP アドレス	X	影響を受けたホストの IP アドレス。
ホスト名	X	ホストのコンピュータ名。
MAC アドレス		ネットワークノードの MAC アドレス。

列の名前	事前選択済み	説明
ネットワークグループ	X	IP アドレス/ホストが割り当てられたネットワークグループ。
ホストの重大度	X	トレンドマイクロ製品およびサービスによって集計された検出から判断されたホストの重大度。 ホストの重大度レベルの詳細については、51 ページの「ホストの重大度」を参照してください。
最も注目すべき脅威	X	検出の重大度が最も高い脅威の説明。
前回の検出	X	タイムスタンプに基づく最新の検出。

注意

初期設定の [IP アドレス]、[ホストの重大度]、および [前回の検出] 列は削除できません。

表 4-7. [重要な統計] の列

列の名前	事前選択済み	説明
標的型攻撃		標的となるシステムからデータを抜き取ることを目的とする脅威。 詳細については、66 ページの「APT 攻撃シーケンス」を参照してください。

表 4-8. [攻撃段階] の列

列の名前	事前選択済み	説明
情報収集	X	攻撃者は、ソーシャルメディア Web サイトなどのパブリックな情報源を使用してターゲットとなる個人を特定して調査し、カスタマイズされた攻撃の準備をします。

列の名前	事前選択済み	説明
初期侵入	X	最初にセキュリティを破るのは、通常、メールやインスタントメッセージ、ドライブバイダウンロードなどのソーシャルエンジニアリングにより配信されるゼロデイ不正プログラムです。バックドアが作成されて、ネットワークへの侵入が可能になります。または、Web サイトのセキュリティホールの攻撃やネットワークの直接ハッキングが行われる場合もあります。
C&C 通信	X	C&C 通信は通常、攻撃の全体を通じて使用されます。これにより、攻撃者は使用している不正プログラムに対する指示および制御を行うことができ、感染したコンピュータを攻撃してネットワーク内を動き回り、データを抜き出すことができます。
内部活動	X	ネットワーク内に侵入すると、攻撃者はさらにコンピュータを感染させて資格情報を採取し、権限レベルを上げて持続的に制御を行います。
情報探索	X	ポート検索など、いくつかの手法を使用して、注目に値するサーバや興味深いデータを格納するサービスを特定します。
情報送出	X	機密情報を収集したら、そのデータを内部ステージングサーバに送り、そこでデータを攻撃者の制御の下で外部の場所へ送信するためにチャンク化して圧縮し、さらに多くの場合、暗号化します。
不明な攻撃段階	X	攻撃段階と関連付けられていないルールによって発生した検出です。

6. 基本の検索を実行するには、検索テキストボックスに IP アドレスまたはホスト名を入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

初期設定では、[IP アドレス] および [ホスト名] 別に [影響を受けたホスト] が検索されます。

7. 保存された検索条件を実行するには、[保存された検索条件] アイコンをクリックし、保存された検索条件を選択します。

   Deep Discovery Director (統合モード) には、次の保存された検索条件が組み込みで用意されています。

   表 4-9. 組み込みの保存された検索条件

名前	フィルタオプション
標的型攻撃の検出	標的型攻撃に関連する注意すべきイベント
C&C 通信の検出	C&C 通信に関連する注意すべきイベント
内部活動の検出	内部活動に関連する注意すべきイベント

8. 詳細検索フィルタを作成して適用するには、[詳細] をクリックします。

   詳細については、84 ページの「[影響を受けたホスト] の詳細検索フィルタ」を参照してください。

9. (オプション) [詳細] の横にある [詳細] アイコンをクリックして [エクスポート] を選択し、使用する区切り記号を選択します。次に [OK] をクリックし、選択した区切り記号で、影響を受けたホストの現在のフィルタ済みリストを CSV ファイルにエクスポートしてダウンロードします。

APT 攻撃シーケンス

標的型攻撃および APT (標的型サイバー攻撃) とは、企業や政府機関に侵入して内部システム、データ、およびその他の資産にアクセスするためにカスタマイズして作成される、狙いを定めた攻撃です。攻撃はそれぞれ標的に合わせてカスタマイズされますが、組織の内部に潜入して作戦を実行するために、一定のライフサイクルをたどります。

標的型攻撃では、APT ライフサイクルは主に 6 段階の連続プロセスをたどります。

表 4-10. APT 攻撃シーケンス

段階	説明
情報収集 (Intelligence Gathering)	ソーシャルメディア Web サイトなどのパブリックな情報源を使用してターゲットとなる個人を特定して調査し、カスタマイズされた攻撃の準備をします。
初期侵入 (Point of Entry)	最初にセキュリティを破るのは、通常、メールやインスタントメッセージ、ドライブバイダウンロードなどのソーシャルエンジニアリングにより配信されるゼロデイ不正プログラムです。 バックドアが作成されて、ネットワークへの侵入が可能になります。または、Web サイトのセキュリティホールの攻撃やネットワークの直接ハッキングが行われる場合もあります。
C&C 通信 (Command & Control (C&C) Communication)	使用している不正プログラムに対する指示および制御を行うために攻撃全体を通じて使用される通信です。 C&C 通信により、攻撃者は感染したコンピュータを攻撃してネットワーク内を動き回り、データを抜き出すことができます。
内部活動 (Lateral Movement)	さらにコンピュータを感染させる攻撃です。 ネットワーク内に侵入すると、攻撃者は資格情報を採取し、権限レベルを上げ、最初の標的を超えて持続的に制御を行います。
情報探索 (Asset/Data Discovery)	ポート検索など、いくつかの手法を使用して、注目に値するサーバや興味深いデータを格納するサービスを特定します。
情報送出 (Data Exfiltration)	外部の場所へ無認可のデータを送信します。 機密情報を収集したら、そのデータを内部ステージングサーバに送り、そこでデータを攻撃者の制御の下で外部の場所へ送信するためにチャンク化して圧縮し、さらに多くの場合、暗号化します。

Deep Discovery Director (統合モード) は、APT および標的型攻撃の検出を目的として構築されています。そして、高度な不正プログラムまたは攻撃者の活動を示す可能性がある不正なコンテンツ、通信、および動作を、攻撃シーケンスのすべての段階で識別します。

[影響を受けたホスト] - [ホストの詳細] を表示する

手順

1. [検出] > [影響を受けたホスト] の順に選択し、任意の検出リンクをクリックします。

   ホストの詳細が表示されます。

2. ドロップダウンコントロールを使用して検出の重大度を選択します。

3. 期間を選択します。

4. データソースとして含めるアプライアンスを選択します。

5. (オプション) [詳細] の横にある [詳細] アイコンをクリックして [列のカスタマイズ] を選択し、非表示または表示にする列を選択します。次に [適用] をクリックして、変更した [ホストの詳細] 画面に戻ります。

   表 4-11. [一般] の列

列の名前	事前選択済み
タイムスタンプ	X
詳細	X
データソース	X
送信元ホスト	
送信先ホスト	
注目すべきホスト	
注目すべきネットワークグループ	
ピアホスト	X
ピアネットワークグループ	
ピア IP の国/地域	
ユーザアカウント	

注意

初期設定の [タイムスタンプ]、[詳細]、および [脅威の詳細] 列は削除できません。

表 4-12. [メール] の列

列の名前	事前選択済み
送信者	
受信者	
メールの件名	

表 4-13. [検出情報] の列

列の名前	事前選択済み
脅威の詳細	X
検出名	X
脅威 (仮想アナライザ)	
レファレンス/参照情報	
検出の種類	
プロトコル	X
Transport Layer Security (TLS)	
検出の重大度	X
攻撃段階	X
Tactics	X
URL カテゴリ	
方向	X
顕著なオブジェクト	X
YARA ルールファイル名	

6. 基本の検索を実行するには、検索テキストボックスに IP アドレスまたはホスト名を入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

   初期設定では、[ピアホスト] の IP アドレスとホスト名で [影響を受けたホスト] - [ホストの詳細] 画面が検索できます。

7. 保存された検索条件を実行するには、[保存された検索条件] アイコンをクリックし、保存された検索条件を選択します。

   Deep Discovery Director (統合モード) には、次の保存された検索条件が組み込みで用意されています。

   表 4-14. 組み込みの保存された検索条件

名前	フィルタオプション
脅威	検出の種類のオプションは次のとおりです。 • 不正なコンテンツ • 不正な動作 • 不審動作 • セキュリティホール悪用 • グレーウェア • 不正な URL
既知の脅威	ファイル検出の種類: 既知の不正プログラム

潜在的な脅威	• 仮想アナライザの結果: 分析結果あり
	• ファイル検出の種類のオプションは次のとおりです。
	  • 極めて不審なファイル
	  • ヒューリスティック検出

ランサムウェア	検出名のオプションは次のとおりです。 • ランサムウェア関連の検出
YARA ルール検出	YARA ルールファイル名: YARA ルールファイル名あり

8. 詳細検索フィルタを作成して適用するには、[詳細] をクリックします。

詳細については、90 ページの「[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタについて」を参照してください。

9. [エクスポート] をクリックして、ホストの詳細の現在のフィルタ済みリストをエクスポートします。

   [エクスポート] ダイアログが表示されます。

10. フィルタを確認し、使用する区切り文字を選択します。

11. [OK (成功)] をクリックすると、選択した区切り文字で、ホストの詳細の現在のフィルタ済みリストが CSV ファイルにエクスポートされ、ダウンロードされます。

[影響を受けたホスト] - [検出の詳細] を表示する

手順

1. 任意のイベントの [影響を受けたホスト] の検出の詳細を表示するには、[影響を受けたホスト] - [ホストの詳細] 画面の [詳細] 列のアイコンをクリックします。

   そのイベントの検出の詳細が表示されます。

2. [接続の詳細] 画面では、次の操作を実行できます。

   - [Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。
   - [ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - パケットキャプチャが有効で、検出がパケットキャプチャルールに一致した場合、[ダウンロード] をクリックしてから [PCAP ファイル] を選択すると、PCAP ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

     PCAP ファイルの「pkt_comment」フィールドにあるコメント「Detected Packet」は、検出の原因となったパケットを示しています。

- [ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、パケットキャプチャファイル、および接続の詳細を含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。感染ファイルおよび PCAP ファイルはお客さまの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

3. [ファイル分析結果] セクションでは、次の操作を実行できます。

   - [仮想アナライザレポートの表示] をクリックすると、仮想アナライザレポートを表示できます。
   - [ダウンロード] をクリックしてから [仮想アナライザレポート] を選択すると、仮想アナライザレポートをダウンロードできます。
   - [ダウンロード] をクリックしてから [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - [ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - [ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。検出されたファイルはユーザの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

4. [不審オブジェクトおよび関連するファイル分析結果] には、不審オブジェクトと分析された関連ファイル情報が表示されます。

[影響を受けたホスト] - [検出の詳細]

Deep Discovery Inspector では、検出された脅威ごとに詳細情報がログに記録されます。[検出の詳細] 画面には、検索やその他のフィルタ条件と設定に応じて、次の情報が表示されます。

[影響を受けたホスト] - [検出の詳細] - [接続の詳細]

[影響を受けたホスト] - [検出の詳細] 画面の [接続の詳細] には、次の情報を含めることができます。

- 74 ページの「[影響を受けたホスト] - [検出の詳細] - [検出情報]」
- 76 ページの「[影響を受けたホスト] - [検出の詳細] - [接続の概要]」
- 77 ページの「[影響を受けたホスト] - [検出の詳細] - [プロトコル情報]」
- 78 ページの「[影響を受けたホスト] - [検出の詳細] - [ファイル情報]」
- 78 ページの「[影響を受けたホスト] - [検出の詳細] - [追加情報]」

[Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。

[ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

パケットキャプチャが有効で、検出がパケットキャプチャルールに一致した場合、[ダウンロード] をクリックしてから [PCAP ファイル] を選択すると、PCAP ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。PCAP ファイルの「pkt_comment」フィールドにあるコメント「Detected Packet」は、検出の原因となったパケットを示しています。

[ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイルとパケットキャプチャファイルを含むパスワード保護された ZIP アーカイブがダウンロードされます。

重要

- 不審ファイルおよび PCAP ファイルは常に注意して扱う必要があります。感染ファイルおよび PCAP ファイルはお客さまの責任で抽出してください。ファイルは隔離された環境で分析することをお勧めします。
- zip アーカイブのパスワードは「virus」です。

[影響を受けたホスト] - [検出の詳細] - [検出情報]

[検出情報] セクションには、次の情報が表示されます。

- 検出されたアクティビティ
- 攻撃段階
- 相関分析ルール ID (ICID)
- 検出名
- 検出ルール ID

ヒント

検出ルールの番号をクリックすると、そのルールの詳細を脅威データベースで参照できます。

- 検出の重大度
- 検出の種類
- イベントクラス
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

ヒント

Tactics または Techniques 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。

重要

Deep Discovery Director (統合モード) に表示される MITRE の情報は、バージョン 6 の ATT&CK™に基づくものです。別のバージョンの ATT&CK™を使用する製品に表示される情報とは異なる場合があります。

© ATT&CK™は、MITRE Corporation の商標です。

- 顕著なオブジェクト
- プロトコル
- 参照
- 標的型攻撃
- 前回の検出
- 脅威
- 脅威の詳細
- タイムスタンプ
- URL カテゴリ
- 仮想アナライザのリスクレベル

注意

特定の相関関係のあるインシデントの追加情報が表示される場合もあります。

表 4-15. 検出の種類

検出の種類	説明
相関関係のあるインシデント	連続して発生した、またはしきい値に達したアクティビティのパターンを定義するイベント/検出

検出の種類	説明
要注意アプリケーション	次の理由により要注意と見なされるピアツーピア、インスタントメッセンジャー、およびストリーミングメディアアプリケーション • ネットワークパフォーマンスに影響する • セキュリティリスクを発生させる • 従業員の注意を散漫にさせる
セキュリティホール悪用	情報に対するネットワークおよびファイルベースのアクセス試行
グレーウェア	さまざまな種類および信頼度レベルのアドウェア/グレーウェアの検出
不正な動作	すでに不正であることが明確なため詳細な相関分析が不要な動作には次のものがあります。 • 明確に識別された不正プログラムによる通信 • 既知の不正な接続先 • 不正な動作パターンや文字列
不正なコンテンツ	シグネチャによる検出
不正な URL	不正な処理を実行しようとする Web サイト
不審動作	危険な可能性があり、相関分析を確認する必要がある動作には次のものがあります。 • 異常な動作 • 擬似データ • 不審な動作、不正な動作パターンや文字列

[影響を受けたホスト] - [検出の詳細] - [接続の概要]

[接続の概要] セクションには、次の情報が表示されます。

- イベントの方向やその他の情報を含むグラフィカル表示。図の [クライアント] は接続を開始したホストを表します。
- ホストの詳細には、次の情報が含まれます。

- ホスト名
- IP アドレスとポート
- 前回のログオンユーザ
- MAC アドレス
- ネットワークグループ
- ネットワークゾーン
- OS

[影響を受けたホスト] - [検出の詳細] - [プロトコル情報]

[プロトコル情報] セクションには、次の情報が表示されます。

- ボットのコマンド
- ボットの URL
- 証明書の情報
  - 発行先
    - 一般名
    - 組織
    - 組織単位
  - 発行者
    - 一般名
    - 組織
    - 組織単位
- ドメイン名
- ホスト名
- HTTP リファラ

- ICMP コード
- ICMP タイプ
- IRC チャネル名
- IRC ニックネーム
- メッセージ ID
- プロトコル
- クエリ対象ドメイン
- 受信者
- 送信者
- SNI ホスト名
- 件名
- ターゲット共有
- Transport Layer Security (TLS)
- URL
- ユーザエージェント
- ユーザ名

[影響を受けたホスト] - [検出の詳細] - [ファイル情報]

[ファイル情報] セクションには、次の情報が表示されます。

- ファイル名
- SHA-1
- SHA-256
- ファイルサイズ

[影響を受けたホスト] - [検出の詳細] - [追加情報]

[追加情報] セクションには、次の情報が表示されます。

- 接続の中断の試行
- 検出元
- Mitigation
- フィンガープリント
  - JA3 ハッシュ値
  - JA3S ハッシュ値
- VLAN ID

[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果]

[影響を受けたホスト] - [検出の詳細] 画面の [ファイル分析結果] セクションには、次の情報が含まれます。

- 80 ページの「[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果] - [ファイル情報]」
- 81 ページの「[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果] - [YARA 検出]」
- 81 ページの「[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果] - [著しい特性]」

[仮想アナライザレポートの表示] をクリックすると、仮想アナライザレポートを表示できます。

[ダウンロード] をクリックしてから [仮想アナライザレポート] を選択すると、仮想アナライザレポートをダウンロードできます。

ヒント

仮想アナライザレポートの表示またはダウンロードは、その他のオプションより時間がかかる場合があります。仮想アナライザレポートの表示またはダウンロードに時間がかかる点についてご了承ください。

[ダウンロード] をクリックしてから [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。検出されたファイルはユーザの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

[ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

[ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果] - [ファイル情報]

[検出の詳細] 画面の [ファイル分析結果] - [ファイル情報] セクションには、次の情報が表示されます。

- 子ファイル
  - ファイル名/URL
  - ファイルサイズ (バイト)
  - 種類
  - SHA-1
  - SHA-256
- ファイル名
- ファイルサイズ
- ファイルの種類
- MD5
- SHA-1
- SHA-256
- MITRE ATT&CK™ Framework

- Tactics
- Techniques

ヒント

Tactics または Techniques 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。

重要

Deep Discovery Director (統合モード) に表示される MITRE の情報は、バージョン 6 の ATT&CK™に基づくものです。別のバージョンの ATT&CK™を使用する製品に表示される情報とは異なる場合があります。

© ATT&CK™は、MITRE Corporation の商標です。

- 脅威
- 仮想アナライザのリスクレベル

[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果] - [YARA 検出]

[検出の詳細] 画面の [ファイル分析結果] - [YARA 検出] セクションには、次の情報が表示されます。

- YARA ルールファイル
- YARA ルール

[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果] - [著しい特性]

[検出の詳細] 画面の [ファイル分析結果] - [著しい特性] セクションには、一般に不正プログラムに関連付けられる特性が表示されます。特性は次のカテゴリに分類されます。

- セキュリティ違反、自己保存
- 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
- 不正な形式またはその他の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
- その他の著しい特性

[影響を受けたホスト] - [検出の詳細] - [不審オブジェクトおよび関連するファイル分析結果]

[影響を受けたホスト] - [検出の詳細] 画面の [不審オブジェクトおよび関連するファイル分析結果] には、次の情報が表示されます。

[影響を受けたホスト] - [検出の詳細] - [不審オブジェクト情報]

[不審オブジェクト情報] セクションには、次の情報が表示されます。

- 分析された関連ファイル
- 不審オブジェクト
- 種類
- 仮想アナライザのリスクレベル

[影響を受けたホスト] - [検出の詳細] - [分析された関連ファイル情報]

[検出の詳細] 画面の [分析された関連ファイル情報] セクションには、次の情報が表示されます。

- 子ファイル
  - ファイル名
  - ファイルサイズ (バイト)
  - ファイルの種類

- SHA-1
- ファイル名
- ファイルサイズ
- ファイルの種類
- MD5
- SHA-1
- SHA-256
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

ヒント

Tactics または Techniques 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。

重要

Deep Discovery Director (統合モード) に表示される MITRE の情報は、バージョン 6 の ATT&CK™に基づくものです。別のバージョンの ATT&CK™を使用する製品に表示される情報とは異なる場合があります。

© ATT&CK™は、MITRE Corporation の商標です。

- 脅威
- 仮想アナライザのリスクレベル

YARA 検出

- YARA ルールファイル
- YARA ルール

一般的に不正プログラムの特性は、次のカテゴリに分類されます。

- 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
- 不正な形式またはその他の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
- その他の著しい特性

[影響を受けたホスト] の詳細検索フィルタ

詳細検索フィルタを使用して、次の画面に表示される検出についてカスタマイズされた検索を作成および適用します。

- 影響を受けたホスト

  詳細については、84 ページの「[影響を受けたホスト] の詳細検索フィルタについて」を参照してください。

- 影響を受けたホスト - ホストの詳細

  詳細については、90 ページの「[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタについて」を参照してください。

[影響を受けたホスト] の詳細検索フィルタについて

特定のデータを表示するには、次のオプションの属性および演算子を選択して、関連付けられた値を入力してください。

表 4-16. 検索フィルタの条件: [影響を受けたホスト]

属性	演算子	処理
ホスト名	次の値を含む/次の値を含まない/次の値で始まる/等しい	値を入力
IP アドレス	次の値を含む/次の値を含まない/等しい	値を入力
	範囲内/範囲外	範囲を入力
MAC アドレス	次のいずれかの値を含む/次のいずれの値も含まない	値を入力
ネットワークグループ	次の値を含む/次の値を含まない/等しい	値を入力
重要なイベント	次のいずれかの値を含む	次を 1 つ以上選択します。 • 標的型攻撃 • C&C 通信 • 内部活動

詳細については、次を参照してください。

[影響を受けたホスト] の詳細検索フィルタを追加する

手順

1. [影響を受けたホスト] の詳細検索フィルタを作成するには、[検出] > [影響を受けたホスト] の順に選択し、[詳細] をクリックします。
2. 属性および関連付けられた演算子を選択します。
3. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

ヒント

キーワードを入力して、部分一致を検索します。

詳細については、84 ページの「[影響を受けたホスト] の詳細検索フィルタについて」を参照してください。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

4. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
5. [適用] をクリックします。

   [影響を受けたホスト] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
6. 検索を保存するには、次の操作を実行します。
   a. [保存] アイコンをクリックし、[名前を付けて保存] を選択します。

      [名前を付けて保存] ダイアログが表示されます。
   b. 名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

      新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

      注意

      保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。
7. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

[影響を受けたホスト] の保存された検索条件を編集する

手順

1. [影響を受けたホスト] の保存された検索条件を編集するには、[検出] > [影響を受けたホスト] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. 編集する保存された検索条件を選択します。
3. 保存された検索条件を編集するには、次のいずれかを実行します。
   - 画面右側にある編集アイコンをクリックします。
   - [詳細] をクリックします。
4. 属性および関連付けられた演算子を選択します。
5. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

   ヒント

   キーワードを入力して、部分一致を検索します。

   詳細については、84 ページの「[影響を受けたホスト] の詳細検索フィルタについて」を参照してください。

   注意

   値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。
6. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
7. [適用] をクリックします。

   [影響を受けたホスト] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。

8. 編集した検索条件を保存するには、[保存] アイコンをクリックして、次のいずれかを実行します。

   - 編集した検索条件を同じ名前で保存するには、[保存] を選択します。
   - 編集した検索条件を新しい名前で保存するには、[名前を付けて保存] を選択し、次を実行します。

   a. 表示される [名前を付けて保存] ダイアログに名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

      新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

   注意

   保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。

9. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

[影響を受けたホスト] の保存された検索条件を削除する

手順

1. [影響を受けたホスト] の保存された検索条件を削除するには、[検出] > [影響を受けたホスト] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. 削除する保存された検索条件の横にある削除アイコンをクリックします。

   注意

   組み込みフィルタは削除できません。

[影響を受けたホスト] の保存された検索条件をインポートする

手順

1. [影響を受けたホスト] の 1 つ以上の保存された検索条件をインポートするには、[検出] > [影響を受けたホスト] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. [保存された検索条件] ドロップダウンメニュー上部の [インポート] をクリックします。

   [保存された検索条件のインポート] ダイアログが表示されます。
3. [選択] をクリックして、保存された検索条件を含むファイルを指定します。

   ファイルがアップロードされ、検証されます。
4. [インポート] をクリックします。

   注意

   インポートするものと同じ名前の既存の保存された検索条件は上書きされます。

   インポート済みの保存された検索条件が [保存された検索条件] ドロップダウンメニューに表示されます。

[影響を受けたホスト] の保存された検索条件をエクスポートする

手順

1. [影響を受けたホスト] の 1 つ以上の保存された検索条件をエクスポートするには、[検出] > [影響を受けたホスト] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. [保存された検索条件] ドロップダウンメニュー上部の [エクスポート] をクリックします。

   [保存された検索条件のエクスポート] ダイアログが表示されます。

3. 保存された検索条件を個別に選択してエクスポートするか、列上部にあるチェックボックスをオンにして、保存された検索条件をすべてエクスポートします。初期設定では、すべての保存された検索条件が選択され、エクスポートされます。

   注意

   組み込みフィルタはエクスポートできません。

4. [エクスポート] をクリックします。

   保存された検索条件のファイルのダウンロードが開始されます。

[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタについて

特定のデータを表示するには、次のオプションの属性および演算子を選択して、関連付けられた値を入力してください。

表 4-17. 検索フィルタの条件: [影響を受けたホスト] - [ホストの詳細]

属性	演算子	処理
ピアホスト	次の値を含む/次の値を含まない/次の値で始まる/等しい	値を入力
ピア IP アドレス	次の値を含む/次の値を含まない/等しい	値を入力
	範囲内/範囲外	範囲を入力
ピア MAC アドレス	次のいずれかの値を含む/次のいずれの値も含まない	値を入力
ピアネットワークグループ	次の値を含む/次の値を含まない/等しい	値を入力
ピア IP の国/地域	次のいずれかの値を含む/次のいずれの値も含まない	ピア IP の国または地域を 1 つ以上選択

属性	演算子	処理
ユーザアカウント	ユーザアカウントあり/ユーザアカウントなし	
	次の値を含む/次の値を含まない	値を入力
プロトコル	次のいずれかの値を含む/次のいずれの値も含まない	プロトコルを 1 つ以上選択
Transport Layer Security (TLS)	等しい	次のいずれかを選択します。 • Over SSL/TLS • Over SSL/TLS でない
方向	等しい	次のいずれかを選択します。 • 内部 • 外部
脅威/検出/参照	次の値を含む/次の値を含まない/次の値で始まる/次の値と等しい	値を入力
検出ルール ID	次のいずれかの値を含む/次のいずれの値も含まない	値を入力
YARA ルールファイル名	YARA ルールファイル名あり/YARA ルールファイル名なし	
	次の値を含む/次の値を含まない/次の値と等しい	値を入力
相関分析ルール ID (ICID)	次のいずれかの値を含む/次のいずれの値も含まない	値を入力

属性	演算子	処理
検出の種類	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • 不正なコンテンツ • 不正な動作 • 不審動作 • セキュリティホール悪用 • グレーウェア • 不正な URL • 要注意アプリケーション • 相関関係のあるインシデント
攻撃段階	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • 情報収集 • 初期侵入 • C&C 通信 • 内部活動 • 情報探索 • 情報送出 • 不明な攻撃段階

属性	演算子	処理
Tactics	Tactics あり/Tactics なし	
	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • Initial Access • Execution • Persistence • Privilege Escalation • Defense Evasion • Credential Access • Discovery • Lateral Movement • Collection • Exfiltration • Command and Control • Impact

属性	演算子	処理
URL カテゴリ	次のいずれかの値を含む/次のいずれの値も含まない	URL カテゴリを 1 つ以上選択します。 • アドウェア • C&C サーバ • 不正プログラム配信 • コインマイナー • 違法または禁止されたコンテンツ • 不正ドメイン • 不正プログラムによる外部アクセス • フィッシング • プロキシ回避システム/匿名化ソフトウェア • ランサムウェア • 詐欺サイト • スパイウェア
C&C リストのソース	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • グローバルインテリジェンス • 仮想アナライザ • ユーザ指定 • 関連ルール
C&C コールバックアドレス	次の値を含む/次の値を含まない/次の値と等しい	値を入力

属性	演算子	処理
C&C リスクレベル	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 ・ 低 ・ 中 ・ 高
仮想アナライザの結果	分析結果あり/分析結果なし	
PCAP ファイル	PCAP ファイルあり/PCAP ファイルなし	
標的型攻撃への関連	等しい	次のいずれかを選択します。 ・ はい ・ いいえ
ファイル検出の種類	次のいずれかの値を含む	次を 1 つ以上選択します。 ・ 極めて不審なファイル ・ ヒューリスティック検出 ・ 不正なコンテンツ
ファイルパス/ファイル名	ファイル名あり/ファイル名なし	
	次の値を含む/次の値を含まない/等しい	値を入力
SHA-1	ファイルの SHA-1 あり/ファイルの SHA-1 なし/	
	次の値を含む/次の値を含まない	値を入力
SHA-256	ファイルの SHA-256 あり/ファイルの SHA-256 なし	
	次の値を含む/次の値を含まない	値を入力

属性	演算子	処理
ドメイン/URL	ネットワークオブジェクトあり/ネットワークオブジェクトなし	
	次の値を含む/次の値を含まない/次の値と等しい	値を入力
不審オブジェクト/拒否リストエンティティ/ユーザ指定の不審オブジェクト	次の値を含む/次の値を含まない/次の値で始まる/等しい	値を入力
送信者 (メール)	送信者あり/送信者なし	
	次の値を含む/次の値を含まない/次の値と等しい	値を入力
受信者 (メール)	受信者あり/受信者なし	
	次の値を含む/次の値を含まない/次の値と等しい	値を入力
メッセージ ID (メール)	メッセージ ID あり/メッセージ ID なし	
	次の値を含む/次の値を含まない	値を入力
件名 (メール)	件名あり/件名なし	
	次の値を含む/次の値を含まない	値を入力

詳細については、次を参照してください。

[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタを追加する

手順

1. [検出] > [影響を受けたホスト] の順に選択します。
2. [影響を受けたホスト] - [ホストの詳細] を表示するには、次のいずれかを実行します。

- 影響を受けたホストに関連付けられている検出リンクをクリック
- 影響を受けたホストの IP アドレスをクリック

ホストの詳細が表示されます。

3. [詳細] をクリックします。
4. 属性および関連付けられた演算子を選択します。
5. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

ヒント

キーワードを入力して、部分一致を検索します。

詳細については、90 ページの「[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタについて」を参照してください。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

---

6. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
7. [適用] をクリックします。

   [影響を受けたホスト] - [ホストの詳細] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
8. 検索を保存するには、次の操作を実行します。
   a. [保存] アイコンをクリックし、[名前を付けて保存] を選択します。

      [名前を付けて保存] ダイアログが表示されます。
   b. 名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

注意

保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。

9. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

[影響を受けたホスト] — [ホストの詳細] の保存された検索条件を編集する

手順

1. [検出] > [影響を受けたホスト] の順に選択します。
2. [影響を受けたホスト] - [ホストの詳細] を表示するには、次のいずれかを実行します。
   - 影響を受けたホストに関連付けられている検出リンクをクリック
   - 影響を受けたホストの IP アドレスをクリック

   ホストの詳細が表示されます。
3. [保存された検索条件] アイコンをクリックします。
4. 編集する保存された検索条件を選択します。
5. 保存された検索条件を編集するには、次のいずれかを実行します。
   - 画面右側にある編集アイコンをクリックします。
   - [詳細] をクリックします。
6. 属性および関連付けられた演算子を選択します。
7. 次のいずれかを実行して、処理を指定します。

- テキストボックスに値を入力します。
- ドロップダウンリストから値を選択します。

ヒント

キーワードを入力して、部分一致を検索します。

詳細については、90 ページの「[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタについて」を参照してください。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

8. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
9. [適用] をクリックします。

   [影響を受けたホスト] - [ホストの詳細] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
10. 編集した検索条件を保存するには、[保存] アイコンをクリックして、次のいずれかを実行します。
    - 編集した検索条件を同じ名前で保存するには、[保存] を選択します。
    - 編集した検索条件を新しい名前で保存するには、[名前を付けて保存] を選択し、次を実行します。

    a. 表示される [名前を付けて保存] ダイアログに名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

       新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

       注意

       保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。

11. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

[影響を受けたホスト] - [ホストの詳細] の保存された検索条件を削除する

手順

1. [検出] > [影響を受けたホスト] の順に選択します。
2. [影響を受けたホスト] - [ホストの詳細] を表示するには、次のいずれかを実行します。
   - 影響を受けたホストに関連付けられている検出リンクをクリック
   - 影響を受けたホストの IP アドレスをクリック

   ホストの詳細が表示されます。
3. [保存された検索条件] アイコンをクリックします。
4. 削除する保存された検索条件の横にある削除アイコンをクリックします。

   注意

   組み込みフィルタは削除できません。

[影響を受けたホスト] – [ホストの詳細] の保存された検索条件のインポート

手順

1. [検出] > [影響を受けたホスト] の順に選択し、任意の検出リンクをクリックします。
2. [保存された検索条件] アイコンをクリックします。

3. [インポート] をクリックします。

   [保存された検索条件のインポート] ダイアログが表示されます。

4. [選択] をクリックして、保存された検索条件を含むファイルを指定します。

   ファイルがアップロードされ、検証されます。

5. [インポート] をクリックします。

   注意

   - Deep Discovery Director (統合モード) の [影響を受けたホスト] - [ホストの詳細] 画面で作成された、保存された検索条件のみをインポートできます。
   - インポートするものと同じ名前の既存の保存された検索条件は上書きされます。

   インポート済みの保存された検索条件が [保存された検索条件] ドロップダウンメニューに表示されます。

[影響を受けたホスト] – [ホストの詳細] の保存された検索条件のエクスポート

手順

1. [検出] > [影響を受けたホスト] の順に選択し、任意の検出リンクをクリックします。
2. [保存された検索条件] アイコンをクリックします。
3. [エクスポート] をクリックします。

   [保存された検索条件のエクスポート] ダイアログが表示されます。

4. 保存された検索条件を個別に選択してエクスポートするか、列上部にあるチェックボックスをオンにして、保存された検索条件をすべてエクスポートします。初期設定では、すべての保存された検索条件が選択され、エクスポートされます。

注意

組み込みフィルタはエクスポートできません。

5. [エクスポート] をクリックします。

   保存された検索条件のファイルのダウンロードが開始されます。

ネットワーク検出

[ネットワーク検出] 画面には、ユーザが指定した期間内にイベントが発生したホストのリストが表示されます。グローバルインテリジェンス、ユーザ定義のリスト、およびその他のソースからの検出が表示されます。

初期設定では、[送信元ホスト]、[送信先ホスト]、および [注目すべきホスト] で [ネットワーク検出] が検索されます。

表示オプションと検索フィルタ

表示をカスタマイズするには、次の表示オプションと検索フィルタを適用してください。

表 4-18. 表示オプションと検索フィルタ: [ネットワーク検出]

フィルタオプション	説明	
検出の重大度	フィルタオプションには、次の検出の重大度設定が含まれます。	
	高	重大度が高の検出を表示します
	中	重大度が中の検出を表示します
	低	重大度が低の検出を表示します
	情報	情報検出を表示します
	すべての検出の重大度レベル	すべての検出を表示します

フィルタオプション	説明
期間	過去 24 時間
	過去 7 日間
	過去 14 日間
	過去 30 日間
	過去 60 日間
	カスタム範囲
データソース	データソースとして含めるアプライアンスを選択します。
列のカスタマイズ	列を表示したり非表示にして表示をカスタマイズします
基本検索	IP アドレスまたはホスト名を検索します。 注意 基本検索フィールドにキーワードを入力してホストの部分一致を検索します。大文字と小文字は区別されません。
保存された検索条件	保存された検索条件で検索します。 [ネットワーク検出] ビューには、次の事前設定された検索条件が含まれています。 • 脅威 • 既知の脅威 • 潜在的な脅威 • メールによる脅威 • ランサムウェア • YARA ルール検出

フィルタオプション	説明
詳細検索	ユーザ定義の条件セットによる検索を行います。 各セットには次のものが 1 つ以上含まれます。 • 属性 • 演算子 • 関連付けられた値 詳細については、121 ページの「[ネットワーク検出] の詳細検索フィルタ」を参照してください。

[ネットワーク検出] を表示する

手順

1. [検出] > [ネットワーク検出] の順に選択します。
2. ドロップダウンコントロールを使用して検出の重大度を選択します。
3. 期間を選択します。
4. データソースとして含めるアプライアンスを選択します。
5. (オプション) [詳細] の横にある [その他] アイコンをクリックして [列のカスタマイズ] を選択し、非表示または表示にする列を選択します。次に [適用] をクリックして、変更した [ネットワーク検出] 画面に戻ります。

表 4-19. [一般] の列

列の名前	事前選択済み
タイムスタンプ	X
データソース	X
詳細	X
送信元ホスト	X
送信先ホスト	X

列の名前	事前選択済み
注目すべきホスト	X
注目すべきネットワークグループ	
ピアホスト	
ピアネットワークグループ	
ピア IP の国/地域	
ユーザアカウント	

注意

初期設定の [タイムスタンプ] 列と [詳細] 列は削除できません。

表 4-20. [メール] の列

列の名前	事前選択済み
送信者	
受信者	
メールの件名	

表 4-21. [検出情報] の列

列の名前	事前選択済み
脅威の詳細	X
検出名	X
脅威 (仮想アナライザ)	
参照	
検出の種類	
プロトコル	X
Transport Layer Security (TLS)	

列の名前	事前選択済み
検出の重大度	X
攻撃段階	X
Tactics	X
URL カテゴリ	
方向	
顕著なオブジェクト	X
YARA ルールファイル名	

注意

初期設定の [脅威の詳細] 列は削除できません。

6. 基本の検索を実行するには、検索テキストボックスに IP アドレスまたはホスト名を入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

   初期設定では、[送信元ホスト]、[送信先ホスト]、および [注目すべきホスト] で [ネットワーク検出] が検索されます。

7. 保存された検索条件を実行するには、[保存された検索条件] アイコンをクリックし、保存された検索条件を選択します。

   Deep Discovery Director (統合モード) には、次の保存された検索条件が組み込みで用意されています。

表 4-22. 組み込みの保存された検索条件

名前	フィルタオプション
脅威	検出の種類のオプションは次のとおりです。 • 不正なコンテンツ • 不正な動作 • 不審動作 • セキュリティホール悪用 • グレーウェア • 不正な URL
既知の脅威	ファイル検出の種類: 既知の不正プログラム

潜在的な脅威	• 仮想アナライザの結果: 分析結果あり
	• ファイル検出の種類のオプションは次のとおりです。
	  • 極めて不審なファイル
	  • ヒューリスティック検出

メールによる脅威	プロトコルのオプションは次のとおりです。 • IMAP4 • POP3 • SMTP
ランサムウェア	検出名のオプションは次のとおりです。 • ランサムウェア関連の検出
YARA ルール検出	YARA ルールファイル名: YARA ルールファイル名あり

8. 詳細検索フィルタを作成して適用するには、[詳細] をクリックします。

詳細については、121 ページの「[ネットワーク検出] の詳細検索フィルタ」を参照してください。

9. (オプション) [詳細] の横にある [詳細] アイコンをクリックして [エクスポート] を選択し、使用する区切り記号を選択します。次に [OK] をクリックし、選択した区切り記号で、ネットワーク検出の現在のフィルタ済みリストを CSV ファイルにエクスポートしてダウンロードします。

[ネットワーク検出] - [検出の詳細] を表示する

手順

1. 任意のイベントの [ネットワーク検出] の検出の詳細を表示するには、[ネットワーク検出] 画面の [詳細] 列のアイコンをクリックします。

   そのイベントの検出の詳細が表示されます。

2. [接続の詳細] 画面では、次の操作を実行できます。

   - [Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。
   - [ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - パケットキャプチャが有効で、検出がパケットキャプチャルールに一致した場合、[ダウンロード] をクリックしてから [PCAP ファイル] を選択すると、PCAP ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

     PCAP ファイルの「pkt_comment」フィールドにあるコメント「Detected Packet」は、検出の原因となったパケットを示しています。
   - [ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、パケットキャプチャファイル、および接続の詳細を含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。感染ファイルおよび PCAP ファイルはお客さまの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

3. [ファイル分析結果] セクションでは、次の操作を実行できます。
   - [仮想アナライザレポートの表示] をクリックすると、仮想アナライザレポートを表示できます。
   - [ダウンロード] をクリックしてから [仮想アナライザレポート] を選択すると、仮想アナライザレポートをダウンロードできます。
   - [ダウンロード] をクリックしてから [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - [ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - [ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。検出されたファイルはユーザの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

4. [不審オブジェクトおよび関連するファイル分析結果] には、不審オブジェクトと分析された関連ファイル情報が表示されます。

[ネットワーク検出] - [検出の詳細]

Deep Discovery Inspector では、検出された脅威ごとに詳細情報がログに記録されます。[検出の詳細] 画面には、検索やその他のフィルタ条件と設定に応じて、次の情報が表示されます。

[ネットワーク検出] - [検出の詳細] - [接続の詳細]

[ネットワーク検出] - [検出の詳細] 画面の [接続の詳細] には、次の情報を含めることができます。

- 111 ページの「[ネットワーク検出] - [検出の詳細] - [検出情報]」
- 113 ページの「[ネットワーク検出] - [検出の詳細] - [接続の概要]」
- 114 ページの「[ネットワーク検出] - [検出の詳細] - [プロトコル情報]」
- 115 ページの「[ネットワーク検出] - [検出の詳細] - [ファイル情報]」
- 115 ページの「[ネットワーク検出] - [検出の詳細] - [追加情報]」

[Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。

[ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

パケットキャプチャが有効で、検出がパケットキャプチャルールに一致した場合、[ダウンロード] をクリックしてから [PCAP ファイル] を選択すると、PCAP ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。PCAP ファイルの「pkt_comment」フィールドにあるコメント「Detected Packet」は、検出の原因となったパケットを示しています。

[ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイルとパケットキャプチャファイルを含むパスワード保護された ZIP アーカイブがダウンロードされます。

重要

- 不審ファイルおよび PCAP ファイルは常に注意して扱う必要があります。感染ファイルおよび PCAP ファイルはお客さまの責任で抽出してください。ファイルは隔離された環境で分析することをお勧めします。
- zip アーカイブのパスワードは「virus」です。

[ネットワーク検出] - [検出の詳細] - [検出情報]

[検出情報] セクションには、次の情報が表示されます。

- 検出されたアクティビティ
- 攻撃段階
- 相関分析ルール ID (ICID)
- 検出名
- 検出ルール ID
- 検出の重大度
- 検出の種類
- イベントクラス
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

ヒント

Tactics または Techniques 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。

重要

Deep Discovery Director (統合モード) に表示される MITRE の情報は、バージョン 6 の ATT&CK™に基づくものです。別のバージョンの ATT&CK™を使用する製品に表示される情報とは異なる場合があります。

© ATT&CK™は、MITRE Corporation の商標です。

- 顕著なオブジェクト
- プロトコル
- 参照
- 標的型攻撃
- 前回の検出
- 脅威
- 脅威の詳細
- タイムスタンプ
- URL カテゴリ
- 仮想アナライザのリスクレベル

注意

特定の相関関係のあるインシデントの追加情報が表示される場合もあります。

表 4-23. 検出の種類

検出の種類	説明
相関関係のあるインシデント	連続して発生した、またはしきい値に達したアクティビティのパターンを定義するイベント/検出
要注意アプリケーション	次の理由により要注意と見なされるピアツーピア、インスタントメッセンジャー、およびストリーミングメディアアプリケーション • ネットワークパフォーマンスに影響する • セキュリティリスクを発生させる • 従業員の注意を散漫にさせる
セキュリティホール悪用	情報に対するネットワークおよびファイルベースのアクセス試行

検出の種類	説明
グレーウェア	さまざまな種類および信頼度レベルのアドウェア/グレーウェアの検出
不正な動作	すでに不正であることが明確なため詳細な相関分析が不要な動作には次のものがあります。 • 明確に識別された不正プログラムによる通信 • 既知の不正な接続先 • 不正な動作パターンや文字列
不正なコンテンツ	シグネチャによる検出
不正な URL	不正な処理を実行しようとする Web サイト
不審動作	危険な可能性があり、相関分析を確認する必要がある動作には次のものがあります。 • 異常な動作 • 擬似データ • 不審な動作、不正な動作パターンや文字列

[ネットワーク検出] - [検出の詳細] - [接続の概要]

[接続の概要] セクションには、次の情報が表示されます。

- イベントの方向やその他の情報を含むグラフィカル表示。図の [クライアント] は接続を開始したホストを表します。
- ホストの詳細には、次の情報が含まれます。
  - ホスト名
  - IP アドレスとポート
  - 前回のログオンユーザ
  - MAC アドレス
  - ネットワークグループ
  - ネットワークゾーン

- OS

[ネットワーク検出] - [検出の詳細] - [プロトコル情報]

[プロトコル情報] セクションには、次の情報が表示されます。

- ボットのコマンド
- ボットの URL
- 証明書の情報
  - 発行先
    - 一般名
    - 組織
    - 組織単位
  - 発行者
    - 一般名
    - 組織
    - 組織単位
- ドメイン名
- ホスト名
- HTTP リファラ
- ICMP コード
- ICMP タイプ
- IRC チャネル名
- IRC ニックネーム
- メッセージ ID
- プロトコル

- クエリ対象ドメイン
- 受信者
- 送信者
- SNI ホスト名
- 件名
- ターゲット共有
- Transport Layer Security (TLS)
- URL
- ユーザエージェント
- ユーザ名

[ネットワーク検出] - [検出の詳細] - [ファイル情報]

[ファイル情報] セクションには、次の情報が表示されます。

- ファイル名
- SHA-1
- SHA-256
- ファイルサイズ

[ネットワーク検出] - [検出の詳細] - [追加情報]

[追加情報] セクションには、次の情報が表示されます。

- 接続の中断の試行
- 検出元
- Mitigation
- フィンガープリント
  - JA3 ハッシュ値

  - JA3S ハッシュ値
- VLAN ID

[ネットワーク検出] - [検出の詳細] - [ファイル分析結果]

[ネットワーク検出] - [検出の詳細] 画面の [ファイル分析結果] には、次の情報が含まれます。

- 117 ページの「[ネットワーク検出] - [検出の詳細] - [ファイル分析結果] - [ファイル情報]」
- 118 ページの「[ネットワーク検出] - [検出の詳細] - [ファイル分析結果] - [YARA ルール検出]」
- 118 ページの「[ネットワーク検出] - [検出の詳細] - [ファイル分析結果] - [著しい特性]」

[仮想アナライザレポートの表示] をクリックすると、仮想アナライザレポートを表示できます。

[ダウンロード] をクリックしてから [仮想アナライザレポート] を選択すると、仮想アナライザレポートをダウンロードできます。

ヒント

仮想アナライザレポートの表示またはダウンロードは、その他のオプションより時間がかかる場合があります。仮想アナライザレポートの表示またはダウンロードに時間がかかる点についてご了承ください。

[ダウンロード] をクリックしてから [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。検出されたファイルはユーザの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

[ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

[ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

[ネットワーク検出] - [検出の詳細] - [ファイル分析結果] - [ファイル情報]

[検出の詳細] 画面の [ファイル分析結果] - [ファイル情報] セクションには、次の情報が表示されます。

- 子オブジェクト
  - ファイル名/URL
  - ファイルサイズ (バイト)
  - 種類
  - SHA-1
  - SHA-256
- ファイル名
- ファイルサイズ
- ファイルの種類
- MD5
- SHA-1
- SHA-256
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

ヒント

Tactics または Techniques 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。

重要

Deep Discovery Director (統合モード) に表示される MITRE の情報は、バージョン 6 の ATT&CK™に基づくものです。別のバージョンの ATT&CK™を使用する製品に表示される情報とは異なる場合があります。

© ATT&CK™は、MITRE Corporation の商標です。

- 脅威
- 仮想アナライザのリスクレベル

[ネットワーク検出] - [検出の詳細] - [ファイル分析結果] - [YARA ルール検出]

[検出の詳細] 画面の [ファイル分析結果] - [YARA 検出] セクションには、次の情報が表示されます。

- YARA ルールファイル
- YARA ルール

[ネットワーク検出] - [検出の詳細] - [ファイル分析結果] - [著しい特性]

[検出の詳細] 画面の [ファイル分析結果] - [著しい特性] には、一般に不正プログラムに関連付けられる特性が表示されます。特性は次のカテゴリに分類されます。

- セキュリティ違反、自己保存
- 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
- 不正な形式またはその他の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
- その他の著しい特性

[ネットワーク検出] - [検出の詳細] - [不審オブジェクトおよび関連するファイル分析結果]

[ネットワーク検出] - [検出の詳細] 画面の [不審オブジェクトおよび関連するファイル分析結果] には、次の情報が含まれます。

[ネットワーク検出] - [検出の詳細] - [不審オブジェクト情報]

[不審オブジェクト情報] セクションには、次の情報が表示されます。

- 分析された関連ファイル
- 仮想アナライザのリスクレベル
- 不審オブジェクト
- 種類

[ネットワーク検出] - [検出の詳細] - [分析された関連ファイル情報]

[検出の詳細] 画面の [分析された関連ファイル情報] セクションには、次の情報が表示されます。

- 子オブジェクト
  - ファイル名
  - ファイルサイズ (バイト)
  - 種類
  - SHA-1
  - SHA-256
- ファイル名

- ファイルサイズ
- ファイルの種類
- MD5
- SHA-1
- SHA-256
- MITRE ATT&CK™ Framework
  - Tactics
  - Techniques

ヒント

Tactics または Techniques 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。

重要

Deep Discovery Director (統合モード) に表示される MITRE の情報は、バージョン 6 の ATT&CK™に基づくものです。別のバージョンの ATT&CK™を使用する製品に表示される情報とは異なる場合があります。

© ATT&CK™は、MITRE Corporation の商標です。

- 脅威
- 仮想アナライザのリスクレベル

YARA 検出

- YARA ルールファイル
- YARA ルール

一般的に不正プログラムの特性は、次のカテゴリに分類されます。

- 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
- 不正な形式またはその他の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
- その他の著しい特性

[ネットワーク検出] の詳細検索フィルタ

特定のデータを表示するには、次のオプションの属性および演算子を選択して、関連付けられた値を入力してください。

表 4-24. 検索条件: [ネットワーク検出]

属性	演算子	処理
ホスト名	次の値を含む/次の値を含まない/次の値で始まる/等しい	値を入力
注目すべきホスト	次の値を含む/次の値を含まない/次の値で始まる/等しい	値を入力
ピアホスト	次の値を含む/次の値を含まない/次の値で始まる/等しい	値を入力
IP アドレス	次の値を含む/次の値を含まない/等しい	値を入力
	範囲内/範囲外	範囲を入力
注目すべき IP アドレス	次の値を含む/次の値を含まない/等しい	値を入力
	範囲内/範囲外	範囲を入力

属性	演算子	処理
ピア IP アドレス	次の値を含む/次の値を含まない/等しい	値を入力
	範囲内/範囲外	範囲を入力
ピア IP の国/地域	次のいずれかの値を含む/次のいずれの値も含まない	ピア IP の国または地域を 1 つ以上選択
MAC アドレス	次のいずれかの値を含む/次のいずれの値も含まない	値を入力
ネットワークグループ	次の値を含む/次の値を含まない/等しい	値を入力
ユーザアカウント	ユーザアカウントあり/ユーザアカウントなし	
	次の値を含む/次の値を含まない	値を入力
プロトコル	次のいずれかの値を含む/次のいずれの値も含まない	プロトコルを 1 つ以上選択
Transport Layer Security (TLS)	等しい	次のいずれかを選択します。 • Over SSL/TLS • Over SSL/TLS でない
方向	等しい	次のいずれかを選択します。 • 内部 • 外部
脅威/検出/参照	次の値を含む/次の値を含まない/等しい	値を入力
検出ルール ID	次のいずれかの値を含む/次のいずれの値も含まない	範囲を入力
YARA ルールファイル名	YARA ルールファイル名あり/YARA ルールファイル名なし	
	次の値を含む/次の値を含まない/次の値と等しい	値を入力

属性	演算子	処理
相関分析ルール ID (ICID)	次のいずれかの値を含む/次のいずれの値も含まない	値を入力
検出の種類	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • 不正なコンテンツ • 不正な動作 • 不審動作 • セキュリティホール悪用 • グレーウェア • 不正な URL • 要注意アプリケーション • 相関関係のあるインシデント
攻撃段階	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • 情報収集 • 初期侵入 • C&C 通信 • 内部活動 • 情報探索 • 情報送出 • 不明な攻撃段階

属性	演算子	処理
Tactics	Tactics あり/Tactics なし	
	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • Initial Access • Execution • Persistence • Privilege Escalation • Defense Evasion • Credential Access • Discovery • Lateral Movement • Collection • Exfiltration • Command and Control • Impact
URL カテゴリ	次のいずれかの値を含む/次のいずれの値も含まない	URL カテゴリを 1 つ以上選択
C&C リストのソース	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 • グローバルインテリジェンス • 仮想アナライザ • ユーザ指定 • 関連ルール
C&C コールバックアドレス	次の値を含む/次の値を含まない	値を入力

属性	演算子	処理
C&C リスクレベル	次のいずれかの値を含む/次のいずれの値も含まない	次を 1 つ以上選択します。 ・ 低 ・ 中 ・ 高 ・ 不明
仮想アナライザの結果	分析結果あり/分析結果なし	
PCAP ファイル	PCAP ファイルあり/PCAP ファイルなし	
標的型攻撃への関連	等しい	次のいずれかを選択します。 ・ はい ・ いいえ
ファイル検出の種類	次のいずれかの値を含む	次を 1 つ以上選択します。 ・ 極めて不審なファイル ・ ヒューリスティック検出 ・ 不正なコンテンツ
ファイルパス/ファイル名	ファイル名あり/ファイル名なし	
	次の値を含む/次の値を含まない/等しい	値を入力
SHA-1	ファイルの SHA-1 あり/ファイルの SHA-1 なし/	
	次の値を含む/次の値を含まない	値を入力
SHA-256	ファイルの SHA-256 あり/ファイルの SHA-256 なし	
	次の値を含む/次の値を含まない	値を入力
ドメイン/URL	次の値を含む/次の値を含まない/等しい	値を入力

属性	演算子	処理
不審オブジェクト/拒否リストエンティティ/ユーザ指定の不審オブジェクト	次の値を含む/次の値を含まない/次の値で始まる/等しい	値を入力
送信者 (メール)	送信者あり/送信者なし	
	等しい/次の値を含む/次の値を含まない	値を入力
受信者 (メール)	受信者あり/受信者なし	
	等しい/次の値を含む/次の値を含まない	値を入力
メッセージ ID (メール)	メッセージ ID あり/メッセージ ID なし	
	次の値を含む/次の値を含まない	値を入力
件名 (メール)	件名あり/件名なし	
	次の値を含む/次の値を含まない	値を入力

詳細については、次を参照してください。

[ネットワーク検出] の詳細検索フィルタを追加する

手順

1. [ネットワーク検出] の詳細検索フィルタを作成するには、[検出] > [ネットワーク検出] の順に選択し、[詳細] をクリックします。
2. 属性および関連付けられた演算子を選択します。
3. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

ヒント

キーワードを入力して、部分一致を検索します。

詳細については、121 ページの「[ネットワーク検出] の詳細検索フィルタ」を参照してください。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

4. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
5. [適用] をクリックします。

   [ネットワーク検出] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
6. 検索を保存するには、次の操作を実行します。
   a. [保存] アイコンをクリックし、[名前を付けて保存] を選択します。

      [名前を付けて保存] ダイアログが表示されます。
   b. 名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

      新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

      注意

      保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。
7. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

[ネットワーク検出] の保存された検索条件を編集する

手順

1. [ネットワーク検出] の保存された検索条件を編集するには、[検出] > [ネットワーク検出] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. 編集する保存された検索条件を選択します。
3. 保存された検索条件を編集するには、次のいずれかを実行します。
   - 画面右側にある編集アイコンをクリックします。
   - [詳細] をクリックします。
4. 属性および関連付けられた演算子を選択します。
5. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

   ヒント

   キーワードを入力して、部分一致を検索します。

   詳細については、121 ページの「[ネットワーク検出] の詳細検索フィルタ」を参照してください。

   注意

   値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。
6. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
7. [適用] をクリックします。

   [ネットワーク検出] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。

8. 編集した検索条件を保存するには、[保存] アイコンをクリックして、次のいずれかを実行します。

   - 編集した検索条件を同じ名前で保存するには、[保存] を選択します。
   - 編集した検索条件を新しい名前で保存するには、[名前を付けて保存] を選択し、次を実行します。

   a. 表示される [名前を付けて保存] ダイアログに名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

      新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

   注意

   保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。

9. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

[ネットワーク検出] の保存された検索条件を削除する

手順

1. [ネットワーク検出] の保存された検索条件を削除するには、[検出] > [ネットワーク検出] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. 削除する保存された検索条件の横にある削除アイコンをクリックします。

注意

組み込みフィルタは削除できません。

[ネットワーク検出] の保存された検索条件をインポートする

手順

1. [ネットワーク検出] の 1 つ以上の保存された検索条件をインポートするには、[検出] > [ネットワーク検出] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. [保存された検索条件] ドロップダウンメニュー上部の [インポート] をクリックします。

   [保存された検索条件のインポート] ダイアログが表示されます。
3. [選択] をクリックして、保存された検索条件を含むファイルを指定します。

   ファイルがアップロードされ、検証されます。
4. [インポート] をクリックします。

   注意

   インポートするものと同じ名前の既存の保存された検索条件は上書きされます。

   インポート済みの保存された検索条件が [保存された検索条件] ドロップダウンメニューに表示されます。

[ネットワーク検出] の保存された検索条件をエクスポートする

手順

1. [ネットワーク検出] の 1 つ以上の保存された検索条件をエクスポートするには、[検出] > [ネットワーク検出] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. [保存された検索条件] ドロップダウンメニュー上部の [エクスポート] をクリックします。

[保存された検索条件のエクスポート] ダイアログが表示されます。

3. 保存された検索条件を個別に選択してエクスポートするか、列上部にあるチェックボックスをオンにして、保存された検索条件をすべてエクスポートします。初期設定では、すべての保存された検索条件が選択され、エクスポートされます。

   注意

   組み込みフィルタはエクスポートできません。

4. [エクスポート] をクリックします。

   保存された検索条件のファイルのダウンロードが開始されます。

メールメッセージ

[メールメッセージ] 画面には、不正または不審なコンテンツ、埋め込みリンク、添付ファイル、またはソーシャルエンジニアリング攻撃に関連した特徴が含まれるために検出されたメールメッセージのリストが表示されます。Deep Discovery Email Inspector は、調査結果に基づいて、各メールメッセージにリスク評価を割り当てます。

検出されたメールメッセージにクエリを実行すると、以下のことが可能になります。

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

表示オプションと検索フィルタ

表示をカスタマイズするには、次の表示オプションと検索フィルタを適用してください。

表 4-25. 表示オプションと検索フィルタ: [メールメッセージ]

フィルタオプション	説明	
リスクレベル	フィルタオプションには、次のリスクレベル設定が含まれます。	
	高	高リスクのメールメッセージを表示します
	中	中リスクのメールメッセージを表示します
	低	低リスクのメールメッセージを表示します
	使用不可	スパムメール/グレーメールメッセージ、およびコンテンツ違反により検出されたメールメッセージを表示します
	すべて	すべてのメールメッセージを表示します
期間	過去 24 時間	
	過去 7 日間	
	過去 14 日間	
	過去 30 日間	
	過去 60 日間	
	カスタム範囲	
監視対象ドメイン	メールメッセージを表示するドメインを選択します	
基本検索	基本検索フィールドにキーワードを入力して、送信者、メールヘッダ (from)、受信者、またはメールヘッダ (to) の部分一致を検索します。大文字と小文字は区別されません。	
保存された検索条件	保存された検索条件で検索します。	

フィルタオプション	説明
詳細検索	ユーザ定義の条件セットによる検索を行います。 各セットには次のものが 1 つ以上含まれます。 • 属性 • 演算子 • 関連付けられた値
列のカスタマイズ	列を表示したり非表示にして表示をカスタマイズします

[メールメッセージ] を表示する

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

手順

1. [検出] > [メールメッセージ] の順に選択します。

   [メールメッセージ] 画面が表示されます。

2. ドロップダウンコントロールを使用してリスクレベルを選択します。
3. 期間を選択します。
4. 表示するメールメッセージのドメインを選択します。
5. (オプション) [詳細] の横にある [その他] アイコンをクリックして [列のカスタマイズ] を選択し、非表示または表示にする列を選択します。次に [適用] をクリックして、変更した [メールメッセージ] 画面に戻ります。
6. 基本の検索を実行するには、検索テキストボックスにキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

Deep Discovery Director (統合モード) の初期設定では、メールメッセージを [受信者]、[メールヘッダ (To)]、[送信者]、[メールヘッダ (From)] で検索できます。

7. 保存された検索条件を実行するには、[保存された検索条件] アイコンをクリックし、保存された検索条件を選択します。

   Deep Discovery Director (統合モード) には初期設定で、次の保存された検索条件が組み込みで用意されています。

   表 4-26. 組み込みの保存された検索条件

名前	フィルタオプション
仮想アナライザの結果あり	検出元: 仮想アナライザ
不審メッセージの特定	[脅威の種類] のオプションは次のとおりです。 • 標的型不正プログラム • 不正プログラム • 不正な URL • 不審ファイル • 不審 URL • フィッシング
スパムメール/グレーメール	脅威の種類: スパムメール/グレーメール
コンテンツ違反	脅威の種類: コンテンツ違反
パスワード保護された添付ファイル	パスワード保護された添付ファイルあり
YARA ルール検出	YARA ルールファイル名: YARA ルールファイル名あり

8. 詳細検索フィルタを作成して適用するには、[詳細] をクリックします。

   詳細については、140 ページの「[メールメッセージ] の詳細検索フィルタ」を参照してください。

9. (オプション) [詳細] の横にある [詳細] アイコンをクリックして [エクスポート] を選択し、使用する区切り記号を選択します。次に [OK] をク

リックし、選択した区切り記号で、メールメッセージの現在のフィルタ済みリストを CSV ファイルにエクスポートしてダウンロードします。

[メールメッセージ] - [検出の詳細] を表示する

手順

1. メールメッセージの検索の詳細を表示するには、[メールメッセージ] 画面の [詳細] 列の下にあるアイコンをクリックします。

   メールメッセージの詳細が表示されます。

2. [メッセージの詳細] セクションでは、次の操作を実行できます。

   - [仮想アナライザレポートの表示] をクリックすると、分析レポートが HTML 形式で表示されます。
   - [Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。
   - [スクリーンショットの表示] をクリックすると、メールメッセージが画像として安全に表示されます。
   - [ダウンロード] をクリックして [検出の詳細] を選択すると、検出の詳細が CSV ファイルでダウンロードされます。
   - [ダウンロード] をクリックして [検出されたメッセージ] を選択すると、検出されたメールメッセージを含むパスワード保護された ZIP アーカイブがダウンロードされます。
   - [ダウンロード] をクリックして [仮想アナライザレポート] を選択すると、仮想アナライザレポートが PDF 形式でダウンロードされます。
   - [ダウンロード] をクリックして [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブがダウンロードされます。
   - [ダウンロード] をクリックして [すべて] を選択すると、検出の詳細、検出されたメッセージ、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブがダウンロードされます。

重要

不審ファイルは常に注意して扱う必要があります。アーカイブはユーザの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

3. [概要]、[メッセージ]、[添付ファイル]、[リンク]、[メッセージの特徴]、[内容のキーワード/式の一致]、[情報漏えい対策イベント]、および [メールヘッダ] セクションでメールメッセージに関する詳細および情報を表示します。

[メールメッセージ] - [検出の詳細]

Deep Discovery Email Inspector では、検出されたメールメッセージごとに詳細情報がログに記録されます。[検出の詳細] 画面には、検索やその他のフィルタ条件と設定に応じて、次の情報が表示されます。

[メールメッセージ] - [検出の詳細] - [概要]

メールメッセージのメッセージ ID、受信者、前回の検出時刻、および送信者と送信元の IP アドレスを表示して、メッセージの送信元やその他のトラッキング情報を確認します。

メールメッセージが違反したポリシールールについての情報を取得します。

[概要] セクションには、次の情報が表示されます。

- リスクレベル
- タイムスタンプ
- 脅威の種類
- メッセージ ID
- メールの件名
- 送信元 IP
- 送信者 IP

- 送信者
- 受信者
- メールヘッダ (from)
- メールヘッダ (to)
- 方向
- 処理
- ポリシー
- ルール

[メールメッセージ] - [検出の詳細] - [メッセージ]

検索エンジン名と、スパムメールまたはグレーメールとして検出されたメールメッセージのカテゴリを表示します。

[メッセージ] セクションには、次の情報が表示されます。

- 検出元
- カテゴリ
- 脅威名

[メールメッセージ] - [検出の詳細] - [添付ファイル]

メールメッセージに添付されたファイルについて情報を取得します。この情報にはファイル名、パスワード、ファイルタイプ、リスクレベル、SHA-1 値、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。

[添付ファイル] セクションには、次の情報が表示されます。

- ファイル名
- パスワード
- ファイルの種類

- サイズ (バイト数)
- リスクレベル
- SHA-1
- SHA-256
- 検出元
- 脅威/データ識別子

[メールメッセージ] - [検出の詳細] - [YARA ルール検出]

関連付けられた YARA ルールファイル内の一致する YARA ルールに基づいて検出されたファイルについて情報を取得します。

[YARA ルール検出] セクションには、次の情報が表示されます。

- ファイル名
- ソースファイル名
- YARA ルール名
- YARA ルールファイル名
- SHA-1
- SHA-256

[メールメッセージ] - [検出の詳細] - [リンク]

メールメッセージに埋め込まれた不審 URL について情報を取得します。この情報には URL、サイトのカテゴリ、リスクレベル、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。

[リンク] セクションには、次の情報が表示されます。

- URL
- 抽出元

- サイトカテゴリ
- リスクレベル
- 検出元
- 脅威名

[メールメッセージ] - [検出の詳細] - [メッセージの特徴]

[メッセージの特徴] セクションには、次の情報が表示されます。

- 検出
- 詳細

[メールメッセージ] - [検出の詳細] - [内容のキーワード/式の一致]

メールメッセージ内の一致した内容のキーワードまたは式について情報を取得します。

[内容のキーワード/式の一致] セクションには、次の情報が表示されます。

- データ識別子
- 場所

[メールメッセージ] - [検出の詳細] - [情報漏えい対策イベント]

メールメッセージ内の一致したデータ識別子と情報漏えい対策テンプレートについて情報を取得します。

[情報漏えい対策イベント] セクションには、次の情報が表示されます。

- 情報漏えい対策テンプレート
- データ識別子
- 場所

[メールメッセージ] - [検出の詳細] - [メールヘッダ]

メールメッセージのヘッダの内容を表示します。この情報は、ローカルメールクライアントでヘッダを表示する場合と同じです。

[メールメッセージ] の詳細検索フィルタ

特定のデータを表示するには、次のオプションの属性および演算子を選択して、関連付けられた値を入力してください。

表 4-27. 検索条件: [メールメッセージ]

属性	演算子	処理
送信者	次の値と等しい/次の値を含む/次の値を含まない	値を入力
受信者	次の値と等しい/次の値を含む/次の値を含まない	値を入力
メールヘッダ (From)	差出人あり/差出人なし	
	次の値と等しい/次の値を含む/次の値を含まない	値を入力
メールヘッダ (To)	次の値と等しい/次の値を含む/次の値を含まない	値を入力
送信元 IP	次の値を含む/次の値を含まない/次の値と等しい	値を入力
	範囲内/範囲外	範囲を入力
送信元 IP の国/地域	次のいずれかの値を含む/次のいずれの値も含まない	送信元 IP の国または地域を 1 つ以上選択
送信者 IP	次の値を含む/次の値を含まない/次の値と等しい	値を入力
	範囲内/範囲外	範囲を入力
送信者 IP の国/地域	次のいずれかの値を含む/次のいずれの値も含まない	送信元 IP の国または地域を 1 つ以上選択

属性	演算子	処理
メッセージ ID	次の値を含む/次の値を含まない	値を入力
件名	件名あり/件名なし	
	次の値と等しい/次の値を含む/次の値を含まない	値を入力
方向	等しい	方向を選択
URL	URL あり/URL なし	
	次の値と等しい/次の値に部分的に一致する/次の値を含む/次の値を含まない	値を入力
ファイル名	ファイル名あり/ファイル名なし	
	次の値と等しい/次の値を含む/次の値を含まない	値を入力
パスワード保護された添付ファイルあり	はい/いいえ	
SHA-1	次の値を含む/次の値を含まない/次の値と等しい	値を入力
SHA-256	次の値を含む/次の値を含まない/次の値と等しい	値を入力
脅威名	次の値を含む/次の値を含まない/次の値と等しい/次の値で始まる	値を入力
脅威の種類	次のいずれかの値を含む/次のいずれの値も含まない	脅威の種類を 1 つ以上選択
検出元	次のいずれかの値を含む/次のいずれの値も含まない	検出元を 1 つ以上選択
不審オブジェクト	次の値を含む/次の値を含まない/次の値と等しい/次の値で始まる	値を入力
ポリシー	次の値と等しい/次の値を含む/次の値を含まない	値を入力

属性	演算子	処理
ポリシールール	次の値と等しい/次の値を含む/次の値を含まない	値を入力
YARA ルールファイル名	YARA ルールファイル名あり/YARA ルールファイル名なし	
	次の値を含む/次の値を含まない/次の値と等しい	値を入力
データ識別子	次の値と等しい/次の値を含む/次の値を含まない	値を入力
情報漏えい対策テンプレート	次の値と等しい/次の値を含む/次の値を含まない	値を入力
手動によるメールの送信	はい/いいえ	
処理	次のいずれかの値を含む/次のいずれの値も含まない	処理を 1 つ以上選択

詳細については、次を参照してください。

[メールメッセージ] の詳細検索フィルタを追加する

手順

1. [メールメッセージ] の詳細検索フィルタを作成するには、[検出] > [メールメッセージ] の順に選択し、[詳細] をクリックします。
2. 属性および関連付けられた演算子を選択します。
3. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

   ヒント
   キーワードを入力して、部分一致を検索します。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

4. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
5. [適用] をクリックします。

   [メールメッセージ] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
6. 検索を保存するには、次の操作を実行します。
   a. [保存] アイコンをクリックし、[名前を付けて保存] を選択します。

      [名前を付けて保存] ダイアログが表示されます。
   b. 名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

      新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

      注意

      保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。
7. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

[メールメッセージ] の保存された検索条件を編集する

手順

1. [メールメッセージ] の保存された検索条件を編集するには、[検出] > [メールメッセージ] の順に選択し、[保存された検索条件] アイコンをクリックします。

2. 編集する保存された検索条件を選択します。
3. 保存された検索条件を編集するには、次のいずれかを実行します。
   - 画面右側にある編集アイコンをクリックします。
   - [詳細] をクリックします。
4. 属性および関連付けられた演算子を選択します。
5. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

ヒント

キーワードを入力して、部分一致を検索します。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

6. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
7. [適用] をクリックします。

   [メールメッセージ] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
8. 編集した検索条件を保存するには、[保存] アイコンをクリックして、次のいずれかを実行します。
   - 編集した検索条件を同じ名前で保存するには、[保存] を選択します。
   - 編集した検索条件を新しい名前で保存するには、[名前を付けて保存] を選択し、次を実行します。

   a. 表示される [名前を付けて保存] ダイアログに名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

注意

保存された検索条件には、作成した検索フィルタと、現在のカスタマイズされた列の設定が含まれます。

9. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

メールメッセージの保存された検索条件を削除する

手順

1. [メールメッセージ] の保存された検索条件を削除するには、[検出] > [メールメッセージ] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. 削除する保存された検索条件の横にある削除アイコンをクリックします。

注意

組み込みフィルタは削除できません。

[メールメッセージ] の保存された検索条件をインポートする

手順

1. [メールメッセージ] の保存された検索条件を 1 つ以上インポートするには、[検出] > [メールメッセージ] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. [保存された検索条件] ドロップダウンメニュー上部の [インポート] をクリックします。

[保存された検索条件のインポート] ダイアログが表示されます。

3. [選択] をクリックして、保存された検索条件を含むファイルを指定します。

   ファイルがアップロードされ、検証されます。

4. [インポート] をクリックします。

   注意

   インポートするものと同じ名前の既存の保存された検索条件は上書きされます。

   インポート済みの保存された検索条件が [保存された検索条件] ドロップダウンメニューに表示されます。

[メールメッセージ] の保存された検索条件をエクスポートする

手順

1. [メールメッセージ] の保存された検索条件を 1 つ以上エクスポートするには、[検出] > [メールメッセージ] の順に選択し、[保存された検索条件] アイコンをクリックします。
2. [保存された検索条件] ドロップダウンメニュー上部の [エクスポート] をクリックします。

   [保存された検索条件のエクスポート] ダイアログが表示されます。

3. 保存された検索条件を個別に選択してエクスポートするか、列上部にあるチェックボックスをオンにして、保存された検索条件をすべてエクスポートします。初期設定では、すべての保存された検索条件が選択され、エクスポートされます。

   注意

   組み込みフィルタはエクスポートできません。

4. [エクスポート] をクリックします。

   保存された検索条件のファイルのダウンロードが開始されます。

隔離メッセージ

[隔離メッセージ] 画面には、特定のポリシー条件に一致したために Deep Discovery Email Inspector によって隔離されたメールメッセージのリストが表示されます。メールメッセージの詳細を確認してから、メールメッセージを削除するか、隔離解除して本来の受信者に配信するか、または処理を再開するかを決定してください。

表示オプションと検索フィルタ

表示をカスタマイズするには、次の表示オプションと検索フィルタを適用してください。

表 4-28. 表示オプションと検索フィルタ: [隔離メッセージ]

フィルタオプション	説明	
リスクレベル	フィルタオプションには、次のリスクレベル設定が含まれます。	
	高	高リスクのメールメッセージを表示します
	中	中リスクのメールメッセージを表示します
	低	低リスクのメールメッセージを表示します
	使用不可	スパムメール/グレーメールメッセージ、およびコンテンツ違反により検出されたメールメッセージを表示します
	未評価	メール形式が無効であるか、検索不能な添付ファイルまたはリンクを含むメールメッセージを表示します
	すべて	すべてのメールメッセージを表示します

フィルタオプション	説明
期間	過去 24 時間
	過去 7 日間
	過去 14 日間
	過去 30 日間
	過去 60 日間
	カスタム範囲
監視対象ドメイン	メールメッセージを表示するドメインを選択します

フィルタオプション	説明	
隔離の理由	フィルタオプションには、次の隔離の理由が含まれます。	
	すべて	すべてのメールメッセージを表示します
	コンテンツ違反	内容がコンテンツフィルタルールに一致するメッセージ
	情報漏えい対策イベント	情報漏えい対策ポリシー違反を含むメッセージ
	不正な形式	開いて処理できないメッセージ
	スパムメール検出	スパムメール/グレーメールとして検出されたメッセージ
	脅威の検出	不正プログラムを含むことが検出されたメッセージ
	不明	不明な脅威を含むメッセージ
	検索不能	検索できないメッセージ
	復号に失敗	復号できないメッセージ。
	暗号化に失敗	暗号化できないメッセージ。
	仮想アナライザのエラー	処理のタイムアウトなど、仮想アナライザの予期しないエラーにより分析されなかったメッセージ
	仮想アナライザのタイムアウト	仮想アナライザの処理のタイムアウトにより分析されなかったメッセージ

フィルタオプション	説明	
脅威の種類	フィルタオプションには、次の脅威の種類の分類が含まれます。	
	すべて	すべてのメールメッセージを表示します
	標的型不正プログラム	上司や同僚など、ユーザがメールメッセージの送信元として予期する相手から送信されたかのように見せかける不正プログラム
	不正プログラム	コンピュータシステムに対する妨害、制御、盗難、データ喪失、スパイ、または無許可のアクセスを目的として攻撃者によって使用される不正なソフトウェア
	不正な URL	既知の不正な Web サイトにリンクする、メールメッセージに埋め込まれたハイパーリンク
	不審ファイル	不正な特徴を示すファイル
	不審 URL	未知の不正な Web サイトにリンクする、メールメッセージに埋め込まれたハイパーリンク
	フィッシング	ユーザを正規の Web サイトになりすましたサイトに誘導することで、個人情報を漏えいさせようとするメールメッセージ
	スパムメール/グレーメール	受信者の意向を無視して複数の個人に無差別に送り付けられる、主に商品の宣伝を目的としたメールメッセージ グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールのことを指す
	コンテンツ違反	私信やサイズの大きな添付ファイルなど、不適切だと思われるコンテンツ
	情報漏えい対策イベント	データを喪失させる可能性があるポリシー違反

フィルタオプション	説明
基本検索	基本検索フィールドにキーワードを入力して送信者または受信者の部分一致を検索します。大文字と小文字は区別されません。
詳細検索	ユーザ定義の条件セットによる検索を行います。 各セットには次のものが 1 つ以上含まれます。 • 属性 • 関連付けられた値

[隔離メッセージ] を表示する

手順

1. [検出] > [隔離メッセージ] の順に選択します。

   [隔離メッセージ] 画面が表示されます。

2. ドロップダウンコントロールを使用してリスクレベルを選択します。
3. 期間を選択します。
4. 表示するメールメッセージのドメインを選択します。
5. ドロップダウンコントロールを使用して隔離の理由を選択します。
6. ドロップダウンコントロールを使用して脅威の種類を選択します。
7. 基本の検索を実行するには、検索テキストボックスにキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

   Deep Discovery Director (統合モード) の初期設定では、隔離メッセージを [受信者]、[メールヘッダ (To)]、[送信者]、[メールヘッダ (From)] で検索できます。

8. 詳細検索フィルタを作成して適用するには、[詳細] をクリックします。

詳細については、157 ページの「[隔離メッセージ] の詳細検索フィルタ」を参照してください。

隔離の理由

次の表は、[隔離メッセージ] 画面に表示される隔離の理由の詳細を示しています。

表 4-29. 隔離の理由

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

[隔離メッセージ] - [検出の詳細] を表示する

手順

1. 隔離メッセージの検出の詳細を表示するには、[隔離メッセージ] 画面の [詳細] 列の下にあるアイコンをクリックします。

隔離メッセージの詳細が表示されます。

2. [メッセージの詳細] セクションでは、次の操作を実行できます。

   - [仮想アナライザレポートの表示] をクリックすると、分析レポートが HTML 形式で表示されます。
   - [Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。
   - [スクリーンショットの表示] をクリックすると、メールメッセージが画像として安全に表示されます。
   - [ダウンロード] をクリックして [検出の詳細] を選択すると、検出の詳細が CSV ファイルでダウンロードされます。
   - [ダウンロード] をクリックして [検出されたメッセージ] を選択すると、検出されたメールメッセージを含むパスワード保護された ZIP アーカイブがダウンロードされます。
   - [ダウンロード] をクリックして [仮想アナライザレポート] を選択すると、仮想アナライザレポートが PDF 形式でダウンロードされます。
   - [ダウンロード] をクリックして [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブがダウンロードされます。
   - [ダウンロード] をクリックして [すべて] を選択すると、検出の詳細、検出されたメッセージ、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブがダウンロードされます。

   重要

   不審ファイルは常に注意して扱う必要があります。アーカイブはユーザの責任で抽出してください。

   zip アーカイブのパスワードは「virus」です。

3. [概要]、[メッセージ]、[添付ファイル]、[リンク]、[メッセージの特徴]、[内容のキーワード/式の一致]、[情報漏えい対策イベント]、および [メー

ルヘッダ] セクションで隔離メッセージに関する詳細および情報を表示します。

[隔離メッセージ] - [検出の詳細]

[検出の詳細] 画面には、検索やその他のフィルタ条件と設定に応じて、次の情報が表示されます。

[隔離メッセージ] - [検出の詳細] - [概要]

隔離メッセージのメッセージ ID、受信者、前回の検出時刻、および送信者と送信元の IP アドレスを表示して、メッセージの送信元やその他のトラッキング情報を確認します。

隔離メッセージが違反したポリシールールについての情報を取得します。

[概要] セクションには、次の情報が表示されます。

- リスクレベル
- タイムスタンプ
- 脅威の種類
- メッセージ ID
- メールの件名
- 送信元 IP
- 送信者 IP
- 送信者
- 受信者
- メールヘッダ (from)
- メールヘッダ (to)
- 方向

- 処理
- ポリシー
- ルール

[隔離メッセージ] - [検出の詳細] - [メッセージ]

[メッセージ] セクションには、次の情報が表示されます。

- 検出元
- カテゴリ
- 脅威名

[隔離メッセージ] - [検出の詳細] - [添付ファイル]

隔離メッセージに添付されたファイルについて情報を取得します。この情報にはファイル名、パスワード、ファイルタイプ、リスクレベル、SHA-1 値、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。

[添付ファイル] セクションには、次の情報が表示されます。

- ファイル名
- パスワード
- ファイルの種類
- サイズ (バイト数)
- リスクレベル
- SHA-1
- SHA-256
- 検出元
- 脅威/データ識別子

[隔離メッセージ] - [検出の詳細] - [YARA ルール検出]

関連付けられた YARA ルールファイル内の一致する YARA ルールに基づいて検出されたファイルについて情報を取得します。

[YARA ルール検出] セクションには、次の情報が表示されます。

- ファイル名
- ソースファイル名
- YARA ルール名
- YARA ルールファイル名
- SHA-1
- SHA-256

[隔離メッセージ] - [検出の詳細] - [リンク]

隔離メッセージに埋め込まれた不審 URL について情報を取得します。この情報には URL、サイトのカテゴリ、リスクレベル、脅威を特定した検索エンジン、および検出された脅威の名前などがあります。

[リンク] セクションには、次の情報が表示されます。

- URL
- 抽出元
- サイトカテゴリ
- リスクレベル
- 検出元
- 脅威名

[隔離メッセージ] - [検出の詳細] - [メッセージの特徴]

[メッセージの特徴] セクションには、次の情報が表示されます。

- 検出
- 詳細

[隔離メッセージ] - [検出の詳細] - [内容のキーワード/式の一致]

隔離メッセージ内の一致した内容のキーワードまたは式について情報を取得します。

[内容のキーワード/式の一致] セクションには、次の情報が表示されます。

- データ識別子
- 場所

[隔離メッセージ] - [検出の詳細] - [情報漏えい対策イベント]

隔離メッセージ内の一致したデータ識別子と情報漏えい対策テンプレートについて情報を取得します。

[情報漏えい対策イベント] セクションには、次の情報が表示されます。

- 情報漏えい対策テンプレート
- データ識別子
- 場所

[隔離メッセージ] - [検出の詳細] - [メールヘッダ]

隔離メッセージのヘッダの内容を表示します。この情報は、ローカルメールクライアントでヘッダを表示する場合と同じです。

[隔離メッセージ] の詳細検索フィルタ

詳細検索フィルタを使用して、カスタマイズされた検索を作成および適用します。

詳細については、次を参照してください。

- 158 ページの「[隔離メッセージ] の詳細検索フィルタを追加する」

特定のデータを表示するには、次のオプションの属性を選択して、処理を入力してください。

表 4-30. 検索条件: [隔離メッセージ]

属性	処理
送信者	値を入力
受信者	値を入力
送信元 IP	値を入力
送信者 IP	値を入力
メールヘッダ (From)	値を入力
メールヘッダ (To)	値を入力
メッセージ ID	値を入力
件名	値を入力
脅威名	値を入力
手動によるメールの送信	[はい] または [いいえ] を選択

[隔離メッセージ] の詳細検索フィルタを追加する

手順

1. [隔離メッセージ] の詳細検索フィルタを作成するには、[検出] > [隔離メッセージ] の順に選択し、[詳細] をクリックします。
2. 属性および関連付けられた演算子を選択します。
3. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

4. (オプション) [および] をクリックして、検索フィルタに別の条件セットを含めます。
5. [適用] をクリックします。

   [隔離メッセージ] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
6. (オプション) 保存された検索条件のドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

隔離されたメッセージを管理する

手順

1. [検出] > [隔離メッセージ] の順に選択します。

   [隔離メッセージ] 画面が表示されます。
2. メールメッセージを 1 つ以上選択し、次のいずれかをクリックします。
   - 隔離解除: 選択したメッセージを再処理せずに目的の受信者に直接配信します。
   - 再開: 選択したメッセージの処理を続行します。

     注意

     Deep Discovery Email Inspector では、スパムメール検出、コンテンツ違反、または情報漏えい対策イベントにより隔離されたメッセージの処理のみを続行できます。
   - 削除: 選択したメッセージを削除します。削除したメッセージを復元することはできません。

   選択した処理は、選択したメッセージを保管している Deep Discovery Email Inspector アプライアンスにタスクとしてただちに送信されます。

相関イベント

[相関イベント] 画面には、ネットワーク内の複数の検出の相関データから得られた、1 つ以上の攻撃パターンを示すイベントのリストが表示されます。

表示オプションと検索フィルタ

表示をカスタマイズするには、次の表示オプションと検索フィルタを適用してください。

表 4-31. 表示オプションと検索フィルタ: [相関イベント]

フィルタオプション	説明	
重大度	フィルタオプションには、次の重大度設定が含まれます。	
	高	重大度が高のイベントを表示します
	中	重大度が中のイベントを表示します
	低	重大度が低のイベントを表示します
	すべて	すべてのイベントを表示します
期間	過去 24 時間	
	過去 7 日間	
	過去 14 日間	
	過去 30 日間	
	過去 60 日間	
	カスタム範囲	

フィルタオプション	説明	
攻撃パターン	フィルタオプションには、次の攻撃パターンが含まれます。	
	すべての攻撃パターン	すべてのイベントを表示します
	ブルートフォース攻撃	[ブルートフォース攻撃] の攻撃パターンを持つイベントを表示します
	C&C コールバック	[C&C コールバック] の攻撃パターンを持つイベントを表示します
	情報送出	[情報送出] の攻撃パターンを持つイベントを表示します
	内部活動	[内部活動] の攻撃パターンを持つイベントを表示します
	不正転送	[不正転送] の攻撃パターンを持つイベントを表示します
	その他の不正な活動	[その他の不正な活動] の攻撃パターンを持つイベントを表示します
	脆弱性の悪用	[脆弱性の悪用] の攻撃パターンを持つイベントを表示します
基本検索	注目すべき IP アドレスを検索します。	

[相関イベント] を表示する

手順

1. [検出] > [相関イベント] の順に選択します。

   [相関イベント] 画面が表示されます。

2. ドロップダウンコントロールを使用して重大度を選択します。
3. ドロップダウンコントロールを使用して攻撃パターンを選択します。

4. 期間を選択します。

5. 基本の検索を実行するには、検索テキストボックスに IP アドレスまたはホスト名を入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

[相関イベント] - [相関データ] を表示する

手順

1. 相関データを表示するには、[相関イベント] 画面の [詳細] の下にある [相関データ] アイコン ( ) をクリックします。

   注意

   相関データが利用できない場合、[相関データ] アイコンはグレーアウトされています。

2. 不正な活動の詳細分析が、次の各セクションに表示されます。

   - 概要

     重大度、検出された内部ホストと侵害の兆候 (IOC) の数、および割り当てられている攻撃パターンが表示され、相関データの不正な活動の概要が示されます。

   - 相関グラフ

     Deep Discovery Director で選択した相関イベントとその他の関連イベントとの相関関係が時間の経過に従って表示されます。

   - トランザクションと IOC の詳細

     相関グラフに示された各トランザクションと、検出された侵害の兆候 (IOC) それぞれの詳細が表示されます。トランザクションは、最も古いものを先頭にして順番に表示されます。IOC は、最初に検出された最も古いものを先頭にして順番に表示されます。

ヒント

- [相関データ] 画面の情報は動的に作成されます。この画面に表示される相関数、およびホスト間の相互処理や不正な活動についての詳細は、時間の経過とともに変化する可能性があります。特定の検出の相関データに後からアクセスすると、分析の詳細が追加されているかどうかを確認できます。
- Deep Discovery Director (統合モード) が、Deep Discovery Director (Standalone Network Analytics モード) で動作する複数の Deep Discovery Director (Internal Network Analytics バージョン) サーバと統合されている場合、1 つの相関イベントに対して複数の相関データセットが存在する可能性があります。Network Analytics サーバの表示名と IP アドレスをクリックし、目的のサーバを選択して、各 Deep Discovery Director (Standalone Network Analytics モード) サーバによって生成された相関データを切り替えます。

3. [相関データ] 画面に表示される情報を詳細分析に使用する方法については、163 ページの「相関データ情報を分析する」を参照してください。

相関データ情報を分析する

[相関データ] 画面に表示される情報を詳細分析に使用する方法については、次の項目を参照してください。

[相関データ] 画面の概要

[相関データ] 画面は、主に次の部分で構成されます。

- 概要
- 相関グラフ
- トランザクションと IOC の詳細

概要

[概要] には、重大度、検出された内部ホストと侵害の兆候 (IOC) の数、および攻撃パターンが表示され、相関イベントの不正な活動の概要が示されます。

この相関イベントの相関データをエクスポートするには、[エクスポート] をクリックして、[印刷対応] または [CSV] を選択します。

ヘルプアイコン (?) をクリックして [チュートリアル] を選択すると、[相関データ] 画面の各セクションを順番に説明するチュートリアルが表示されます。[次へ] と [戻る] を使用してチュートリアルを移動するか、[スキップ] をクリックしてただちに終了します。

[概要] は、折りたたみアイコン (^) と展開アイコン (v) をクリックすることで、折りたたみや展開が可能です。

164 ページの「[概要] を確認する」を参照してください。

相関グラフ

[相関グラフ] には、Deep Discovery Director で選択した相関イベントや不審オブジェクトとその他の関連イベントとの相関関係が時間の経過に従って表示されます。

再生バーの横にあるフィルタアイコン (▼) をクリックして、詳細検索フィルタの表示/非表示を切り替えます。

168 ページの「[相関グラフ] を使用した分析」を参照してください。

トランザクションと IOC の詳細

[トランザクションと IOC の詳細] には、相関グラフに示された各トランザクションと、検出された侵害の兆候 (IOC) それぞれの詳細が表示されます。

トランザクションは、最も古いものを先頭にして順番に表示されます。一覧に表示されるトランザクションは、1 日分の場合も、数か月分にわたる場合もあり、Deep Discovery Director - Network Analytics で検出された相関によって異なります。IOC は、最初に検出された最も古いものを先頭にして順番に表示されます。

[トランザクションと IOC の詳細] は、折りたたみアイコン (>) と展開アイコン (<) をクリックすることで、折りたたみや展開が可能です。

183 ページの「[トランザクションと IOC の詳細] を使用した分析」を参照してください。

[概要] を確認する

[概要] には、重大度、検出された内部ホストと侵害の兆候 (IOC) の数、および攻撃パターンが表示され、相関イベントの不正な活動の概要が示されます。

手順

1. 重大度、検出数、攻撃パターン、および活動の概要を確認します。

重大度	Deep Discovery Director - Network Analytics によってイベントや関連する相関に割り当てられた重大度。 Deep Discovery Director - Network Analytics では、独自の分析を含め、多くの要素を使用して重大度の割り当てを行います。
内部ホストと侵害の兆候の検出数	検出数を使用すると、相関イベントの範囲をすばやく決定できます。
攻撃パターン	Deep Discovery Director で選択した相関イベントまたは不審オブジェクトの攻撃パターン。

活動の概要	活動の概要は攻撃パターン別に分類され、次の情報を提供します。 • 活動が検出されたプロトコル。 • 検出された不審オブジェクト (SO) と侵害の兆候 (IOC) の数。 • 不審または不正な活動に関与したホスト。 活動は、内部ホストと外部サーバ間で行われることも、内部ホスト間の内部活動であることもあります。 内部ホストは、[ネットワークグループ] リストによって定義されます。 **注意** • 相関データの正確な分析を行うには、内部のネットワークやホストを [ネットワークグループ] リストに指定することが重要です。 • プライベートネットワークは初期設定で信頼済みと見なされ、内部で「信頼済み」として設定されます。非プライベート IP アドレスのみを [ネットワークグループ] リストに追加する必要があります。 • ラベルが [トリガイベント] の活動は、この相関イベントの焦点であり、この活動には [相関イベント] 画面の [注目すべきホスト] にある IP アドレスが含まれます。 • 不審な活動に関与した追加のホスト。 • 不審オブジェクトの相関データを表示する際の追加の不審オブジェクト。

2. (オプション) 個々の概要項目に対して、次のいずれかの操作を行います。

項目	操作
内部ホストの検出番号	検出番号をクリックし、[クリップボードにコピー] アイコン () をクリックしてリスト全体をクリップボードにコピーするか、[フォーカス] アイコン () をクリックして [相関グラフ] 内の項目に焦点を当てます。
侵害の兆候の検出番号	検出番号をクリックし、[クリップボードにコピー] アイコン () をクリックして、値をクリップボードにコピーします。

項目	操作
攻撃パターン	攻撃パターンにカーソルを合わせると、その攻撃パターンに関連する活動のみが概要で強調表示されます。
IP アドレスとドメイン	三角アイコン ( ) にカーソルを合わせ、次のいずれかを選択します。 • フォーカス: [相関グラフ] 内の項目に焦点を当てます。 • クリップボードにコピー: クリップボードに値をコピーします。 • ネットワーク検出イベントの表示: このオブジェクトに一致するフィルタが適用された新しいブラウザタブで [ネットワーク検出] 画面を開きます。 • Threat Connect: このオブジェクトに対するクエリが含まれた新しいブラウザタブで [Trend Micro Threat Connect] を開きます。 • DomainTools (WHOIS): IP アドレスまたはドメインに対するクエリが含まれた新しいブラウザタブで [DomainTools] を開きます。 • VirusTotal: このオブジェクトに対するクエリが含まれた新しいブラウザタブで [VirusTotal] を開きます。

3. (オプション) [エクスポート] をクリックし、次のいずれかのオプションを選択して、この相関イベントの相関データをエクスポートします。

   - 印刷対応: システムの印刷ダイアログを表示します。設定を変更して、[印刷] をクリックします。
   - CSV: 区切り記号を選択し、[エクスポート] をクリックして、選択した区切り記号で、この相関イベントの相関データを CSV ファイルにエクスポートしてダウンロードします。

   注意

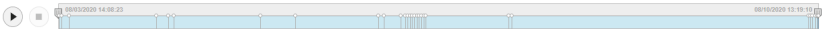
   詳細検索フィルタが適用されている場合、エクスポートは現在フィルタ済みの相関データに制限されます。

[相関グラフ] を使用した分析

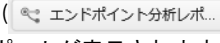
[相関グラフ] には、Deep Discovery Director で選択したトリガイベントとその他の関連イベントとの相関関係が時間の経過に従って表示されます。

手順

- メイン画面で最初の分析を実行します。

[相関グラフ] の要素
 図 4-1. 再生バー/タイムスライダ 再生バーをクリックすると、相関イベントのタイムラインが表示されます。Deep Discovery Director - Network Analytics により、最も古い相関イベントから最新の相関までが連続して描画されます。 タイムラインのスライダを使用して、選択した期間の相関イベントを表示します。このグラフには、選択した期間の相関のみが表示されます。 • 期間を調整するには、タイムラインの左側および右側にあるグラブバーをクリックして、目的の位置にドラッグします。 • 期間全体を移動するには、現在の期間の内側をクリックして、左方向または右方向にドラッグします。 • グラフに表示される相関 (および結果として得られるトランザクションの詳細) は、選択した期間に見つかったイベントデータに応じて異なります。
再生バーの横にあるフィルタアイコン ( ) をクリックして、詳細検索フィルタの表示/非表示を切り替えます。 詳細検索フィルタを使用して、カスタマイズされた検索を作成および適用します。 詳細については、173 ページの「[相関グラフ] の詳細検索フィルタ」を参照してください。

[相関グラフ] の要素
相関ライン 各相関グラフには、送信元と送信先の不正または不審な活動を相互に関連付ける、1 つ以上の相関ラインが含まれます。 ・ 各相関ラインは 2 台のホスト間の 1 つ以上のトランザクションを表しています。 ・ ラインの太さは、ホスト間で発生したトランザクションの数に比例します。 ・ 相関ラインは、内部ホストと外部サーバ間、または 2 台の内部ホスト間 (内部活動) で形成されます。 ・ 各相関ラインには、ホスト間のトランザクションに使用されたプロトコルがラベル付けされています。相関ライン内の矢印は、送信元から送信先へのトランザクションの方向を示しています。 メール送信者が関係する相関ラインは、[不審なメール活動] としてラベル付けされています。

[相関グラフ] の要素
内部ホスト • 内部ホストは IP アドレスによって識別されます。判明している場合、そのホスト名とログオンユーザも表示されます。 関連情報を示すアイコンが内部ホストの横に表示される場合があります。たとえば、内部ホストが優先ウォッチリストまたは登録済みサービスリストに含まれている場合、それを示すアイコンがグラフに表示されます。 • 内部ホストや外部サーバの横にある下向きの三角アイコン ( ) の上にマウスカーソルを合わせると、そのホストに対して実行できる追加処理のリストが表示されます。 • クリップボードにコピー: クリップボードに値をコピーします。 • ネットワーク検出イベントの表示: このオブジェクトに一致するフィルタが適用された新しいブラウザタブで [ネットワーク検出] 画面を開きます。 • Deep Discovery Director は、優先ウォッチリストに含まれるホスト、およびトリガイベントの注目すべき IP を持つホストのエンドポイント分析レポートを取得しようとします。レポートが存在する場合、アイコンが内部ホストの下に表示されます。[エンドポイント分析レポート] アイコン () をクリックすると、Apex Central により提供されるレポートが表示されます。 **注意** • 相関グラフで [エンドポイント分析レポート] アイコンを利用できるようにするには、Deep Discovery Director を Apex Central と統合する必要があります。 詳細については、365 ページの「Apex Central を設定する」を参照してください。

[相関グラフ] の要素
外部サーバ • 外部サーバは IP アドレスによって識別されます。判明している場合、そのドメイン名も表示されます。 メール送信者はメールアドレスによって識別され、常に外部サーバ側の上部に表示されます。 外部ホストに関連する他の情報が表示される場合もあります。 • 外部サーバの横にある下向きの三角アイコン ( ) の上にマウスカーソルを合わせると、そのホストに対して実行できる追加処理のリストが表示されます。 ◦ クリップボードにコピー: クリップボードに値をコピーします。 ◦ ネットワーク検出イベントの表示: このオブジェクトに一致するフィルタが適用された新しいブラウザタブで [ネットワーク検出] 画面を開きます。 ◦ Threat Connect: このオブジェクトに対するクエリが含まれた新しいブラウザタブで [Trend Micro Threat Connect] を開きます。 ◦ DomainTools (WHOIS): IP アドレスまたはドメインに対するクエリが含まれた新しいブラウザタブで [DomainTools] を開きます。 ◦ VirusTotal: このオブジェクトに対するクエリが含まれた新しいブラウザタブで [VirusTotal] を開きます。
特殊なアイコン 相関グラフの要素についての情報を提供する追加アイコンです。 • 優先ウォッチリストアイコン: • エンドポイント分析レポートアイコン: エンドポイント分析レポ... Deep Discovery Director は、優先ウォッチリストに含まれるホスト、およびトリガイベントの注目すべき IP を持つホストのエンドポイント分析レポートを取得しようとします。レポートが存在する場合、アイコンが内部ホストの下に表示されます。 Deep Discovery Director (統合モード) は、Apex One と統合された Apex Central からレポートを取得します。Apex One には Endpoint Sensor 機能があります。 レポートの取得にはいくつかのステータスがあります。

[相関グラフ] の要素
凡例 相関グラフで使用されるアイコンやラインのリストを次に示します。 • 注目すべきホストの相関ラインの色 • グラフ内のホストの優先ウォッチリストへの登録有無 (優先ウォッチリストアイコン) • グラフ内のホストのサービス登録状況 (サービス名のアイコン)   図 4-2. 凡例
注目すべきホスト この相関イベントの焦点を表します。 相互処理は一般に内部ホストと外部サーバ間で行われ、送信元と送信先を結びつける黄色の線で識別されます。 注意 Deep Discovery Director で不審オブジェクトの検出を選択しても、[注目すべきホスト] の相関は通常生成されません。

[相関グラフ] の要素
活動の凡例 グラフに表示される内部ホストや外部サーバの主な活動を識別します。 • 活動は個々の相関グラフによって異なります。 • ブルートフォース攻撃、C&C コールバック、情報送出、内部活動、不正転送、その他の不正活動、脆弱性の悪用などに類似する活動が含まれる可能性があります。 • 一部の活動は Deep Discovery Inspector のログの「検出の種類」に対応します。
関与状況アイコン 対応する活動列のアイコンの表示を確認することで、内部ホストや外部サーバが関与した活動を判別できます。 内部ホストや外部サーバにカーソルを合わせると、関与している活動が青色で強調表示されます。

[相関グラフ] の詳細検索フィルタ

詳細検索フィルタを使用して、カスタマイズされた検索を作成および適用します。

次の表は、詳細検索フィルタで使用可能な操作の概要を示しています。

操作	説明
パネル表示の切り替え	再生バーの横にあるフィルタアイコン ( ) をクリックして、詳細検索フィルタの表示/非表示を切り替えます。
保存された検索条件フィルタの適用	詳細検索フィルタパネルを表示した状態で、[保存された検索条件] ドロップダウンリスト ( ) をクリックし、保存された詳細検索フィルタを選択して [相関グラフ] に適用します。
詳細検索フィルタの追加	詳細検索フィルタパネルを表示した状態で、[相関グラフ] に適用する詳細検索フィルタを追加します。 詳細については、174 ページの「[相関グラフ] の詳細検索フィルタを追加する」を参照してください。

操作	説明
詳細検索フィルタの保存	フィルタを適用して詳細検索フィルタパネルを非表示にした状態で、[保存] アイコン ( ) をクリックし、[保存] または [名前を付けて保存] を選択して詳細検索フィルタを保存します。
詳細検索フィルタの編集	フィルタを適用して詳細検索フィルタパネルを非表示にした状態で、[編集] アイコン ( ) をクリックし、詳細検索フィルタパネルを表示して検索条件を編集します。 [保存] ボタン ( ) をクリックし、[保存] を選択して詳細検索フィルタを保存します。
フィルタのクリア	詳細検索フィルタを適用した状態で、[クリア] アイコン ( ) をクリックして詳細検索フィルタをクリアします。

[相関グラフ] の詳細検索フィルタを追加する

手順

1. [相関グラフ] の詳細検索フィルタを作成するには、[検出] > [相関イベント] の順に選択し、[詳細] の下にある [相関データ] アイコン ( ) をクリックします。
2. 再生バーの横にあるフィルタアイコン ( ) をクリックして、詳細検索フィルタを表示します。
3. 属性および関連付けられた演算子を選択します。
4. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

ヒント

キーワードを入力して、部分一致を検索します。

詳細については、121 ページの「[ネットワーク検出] の詳細検索フィルタ」を参照してください。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

5. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
6. [適用] をクリックします。

   [相関グラフ] が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットは [相関グラフ] の上に表示されます。
7. [保存] ボタン ( ) をクリックし、[名前を付けて保存] を選択します。

   [名前を付けて保存] ダイアログが表示されます。
8. 名前を入力し、必要に応じて説明を入力して、[保存] をクリックします。

   新しく保存された検索条件の名前が、保存された検索条件のリストに追加されます。

[エンドポイント分析レポート] - ステータスの詳細

[エンドポイント分析レポート] のアイコンには、次のステータスが表示されます。

表 4-32. [エンドポイント分析レポート] - ステータスの詳細

アイコン	メッセージ	説明
	次の日時にレポートが取得されました: <日付 + 時間>。	新しいデータを含むレポートが取得され、開く準備も整っています。
		既存のデータを含むレポートが取得され、開く準備が整っています。
		既存データの取得は保留中です。

アイコン	メッセージ	説明
	このホストに関する相関レポートはありません。	このホストに関する新しいデータを含む相関レポートはありません。既存のレポートもありません。
	最新の相関レポートを取得できません。[エラーコード]	クリックすると既存のレポートが開きます。
	相関レポートを取得できません。[エラーコード]	取得するデータがありません。
	エンドポイント分析レポートを取得しています。しばらくお待ちください。	取得するレポートがあります。
	レポートの取得に失敗しました。レポートの取得を再度試みています。[エラーコード]	Deep Discovery Director がレポートの取得を再度試みています。

次の表は、表示されるエラーコードとその問題の解決方法を示しています。

表 4-33. エラーコードの説明と解決方法

エラーコード	説明	解決方法
4	エンドポイント分析レポートの取得がタイムアウトしました。	Deep Discovery Director (統合モード) 、Deep Discovery Director - Network Analytics as a Service、および Apex Central 間の接続に問題がないことを確認します。
11352		
11356		
11351	Apex Central で予期しないエラーが発生しました。	Apex Central が正常に機能していることを確認します。
11353	Endpoint Sensor ライセンスが無効です。	Apex Central で Endpoint Sensor ライセンスのステータスが正常であることを確認します。

エラーコード	説明	解決方法
11354	Apex Central が対象エンドポイントを見つけられませんでした。	Endpoint Sensor およびセキュリティエージェントのインストールが Apex Central で有効になっていることを確認します。
11355	エンドポイントの OS がサポートされていません。	解決方法はありません。エンドポイント分析レポートは、Windows OS を実行するエンドポイントでのみ生成されます。

エンドポイント分析レポート

エンドポイント分析レポートの生成に使用された条件は、画面上部に表示されます。

ヒント

タイトルバーの下矢印アイコンをクリックすると、条件を表示または非表示にできます。

エンドポイント分析レポートには次のタブがあります。

- 177 ページの「分析チェーン」
- 182 ページの「オブジェクトの詳細」

分析チェーン

[分析チェーン] タブには、原因分析が表示され、さらに調査に役立つ可能性のある追加情報が強調表示されます。

情報	説明
対象エンドポイント	原因分析チェーンの起点となるエンドポイントの詳細が表示されます。

情報	説明
最初に確認されたオブジェクト	一致したオブジェクトを作成した可能性が最も高いオブジェクトです。 これは多くの場合、標的型攻撃の侵入ポイントになります。 オブジェクトにマウスカーソルを重ねて 🔍 をクリックすると、原因分析内のオブジェクトを特定できます。
一致したオブジェクト	調査条件に一致するオブジェクトまたはオブジェクトのリストが表示されます。 オブジェクトにマウスカーソルを重ねて 🔍 をクリックすると、原因分析内のオブジェクトを特定できます。
注意が必要なオブジェクト	既存のトレンドマイクロインテリジェンスに基づいて、チェーン内の不正な可能性のあるオブジェクトが強調表示されます。 値はチェーン内の一意の再評価対象オブジェクトの数を示します。 値にカーソルを合わせると、再評価対象オブジェクトのリストが表示されます。 オブジェクトにマウスカーソルを重ねて 🔍 をクリックすると、原因分析内のオブジェクトを特定できます。
原因分析領域	原因分析マップが表示されます。

原因分析領域には、イベントに関与するオブジェクトの分析が視覚的に表示されます。

注意

原因分析チェーンのノード数が表示可能な数を超えた場合は、主要な原因分析チェーンのみが表示されます。

領域を移動するには、領域をクリックして目的の方向にドラッグします。この領域には、次のナビゲーションオプションがあります。

アイコン	説明
	原因分析には、1 つ以上の一致する原因分析チェーンが含まれることがあります。 選択したエンドポイントのその他の原因分析チェーンを表示するには、ドロップダウンをクリックします。
	クリックすると全画面表示になります。 再度クリックすると元に戻ります。
	クリックすると表示が拡大または縮小します。
	マウスカーソルを重ねると、原因分析チェーンに表示される記号の説明が表示されます。

原因分析領域のオブジェクトにマウスカーソルを重ねると、詳細が表示されます。オブジェクトをクリックすると、次のタブとともにサイドパネルが表示されます。

- [プロファイル] タブには、選択したオブジェクトの種類の詳細が表示されます。

  オブジェクトによっては、一部の詳細のみ表示されたり、実行時に表示できる詳細がないことがあります。

  [一致したオブジェクト] および [注意が必要なオブジェクト] では、このタブに次のオプションも表示されます。

- 不審オブジェクトリストに追加: オブジェクトを [ユーザ指定の不審オブジェクト] リストに追加します。リストに追加できるのは、次のオブジェクトの種類です。
  - IP アドレス
  - URL
  - SHA-1
  - ドメイン

- [関連するオブジェクト] タブには、一致したオブジェクトのすべての依存関係が表示されます。

  これらは、一致したオブジェクトを実行するために必要なオブジェクトです。このタブには次の詳細が表示されます。

プロパティ	説明
処理	オブジェクトによって実行された処理。
ログの日時	記録された処理の日時。
評価	トレンドマイクロインテリジェンスに基づいてオブジェクトに割り当てられた評価。
送信先パス	オブジェクトの送信先。

[関連するオブジェクト] タブを管理するには、次のオプションを使用します。

- ドロップダウンで処理を指定して、オブジェクトをフィルタできます。ドロップダウンをクリックすると、選択可能なすべての処理が表示されます。
- [詳細の表示] をクリックすると、オブジェクトに関する詳細が表示されます。

Root Cause Analysis のアイコン

分析チェーンでは、次のアイコンを使用してオブジェクトの種類が表示されます。

アイコン	名前	説明
	最初に確認されたオブジェクト	一致するオブジェクトを作成した可能性が最も高いオブジェクトを表します
	一致条件	調査条件に一致するオブジェクトを表します
	通常のオブジェクト	脅威をもたらさないことが確認されたオブジェクトを表します これらは通常、一般的なシステムファイルです。
	未評価のオブジェクト	まだ評価されていないオブジェクトを表します
	不審オブジェクト	既知の脅威に類似する挙動を示すオブジェクトを表します
	不正なオブジェクト	既知の脅威に一致するオブジェクトを表します
	システム領域感染型ウイルス	システムのスタートアップ時に起動するオブジェクトです
	ブラウザ	Web ページを表示する機能を備えたオブジェクトです。これは通常、Web ブラウザです
	メールクライアント	メールメッセージを送受信できるオブジェクトです。これは通常、メールクライアントまたはサーバです
	メールメッセージ	Cloud App Security 統合のメールの関連付け機能を使用して特定されたオブジェクトです
	ファイル	ディスク上のファイルであるオブジェクトです
	ネットワーク	ネットワーク接続またはインターネットに関連するオブジェクトです

アイコン	名前	説明
	プロセス	実行時のプロセスであるオブジェクトです
	レジストリ	レジストリキー、エントリ、またはデータであるオブジェクトです
	イベント	オブジェクトにより実行されたアクションを示します
	関連付け	2 つのオブジェクト間の関係を示します

オブジェクトの詳細

[オブジェクトの詳細] タブには、情報が表形式で表示されます。また、オブジェクトが次のタブにまとめられています。

- オブジェクト: 親プロセス別にまとめられた、一致したオブジェクトの実行に関与したオブジェクト。▶をクリックするとリストが展開します。
- 注意が必要なオブジェクト: 既存のトレンドマイクロインテリジェンスに基づいて不正な可能性があるチェーン内のオブジェクト。
- ファイルイベント: ファイルであるチェーン内のオブジェクト。
- レジストリイベント: レジストリキー、データ、およびエントリであるチェーン内のオブジェクト。
- IP アドレス/DNS イベント: IP アドレスまたは DNS イベントであるオブジェクト。

この表には次の詳細が表示されます。

列	説明
記録済みオブジェクト	記録済みオブジェクトの名前。 オブジェクト名をクリックすると、さらに詳細が表示されます。
PID	記録済みオブジェクトのプロセス ID。

列	説明
記録済み	オブジェクトがチェーンに含められた日時。
活動	オブジェクトによって実行された処理。 オブジェクト名をクリックすると、さらに詳細が表示されます。
オブジェクトレピュテーション	トレンドマイクロインテリジェンスに基づいてオブジェクトに割り当てられた評価。

次のオプションを使用して表を管理します。

- [オブジェクト] タブでフィルタアイコン ( ) をクリックし、指定した条件に応じて表をフィルタします。
- [注意が必要なオブジェクト]、[ファイルイベント]、[レジストリイベント]、および [IP アドレス/DNS イベント] タブで表を並び替えるには、[記録済み] および [オブジェクトレピュテーション] 列をクリックします。

[トランザクションと IOC の詳細] を使用した分析

[トランザクションと IOC の詳細] セクションには、[相関グラフ] セクションのトランザクションと IOC に関する情報が表示されます。

最も古いトランザクションが先頭に表示されます。IOC は、まず最も高いリスクレベル順に表示され、次に最初に検出された時間順に表示されます。

手順

- トランザクションのリストと IOC のリストをスクロールして、分析に役立つ情報を特定します。
- [相関グラフ] セクションの相関ラインをクリックすると概要が表示され、[トランザクションと IOC の詳細] セクションに表示されるトランザクションと IOC を、選択した相関ラインに直接関係するものだけに制限できます。

> **ヒント**
>
> フィルタを削除するには、[相関グラフ] セクションの空白部分をクリックします。

- [相関グラフ] セクションで内部ホスト、外部サーバ、またはメール送信者をクリックすると、選択した内部ホスト、外部サーバ、またはメール送信者の詳細が [トランザクションと IOC の詳細] セクションに表示されます。

ヒント

[トランザクションと IOC の詳細] セクションを通常の状態に戻すには、[相関グラフ] セクションの空白部分をクリックします。

- [トランザクションと IOC の詳細] セクションの項目に対して、次のいずれかの操作を行います。

項目	操作
IP アドレス、ドメイン、URL、およびハッシュ値	三角アイコン ( ) にカーソルを合わせ、次のいずれかを選択します。 **注意** 画面上の項目の場所によっては、すべての操作が利用できるとは限りません。 • フォーカス: [相関グラフ] 内の項目に焦点を当てます。 • クリップボードにコピー: クリップボードに値をコピーします。 • ネットワーク検出イベントの表示: このオブジェクトに一致するフィルタが適用された新しいブラウザタブで [ネットワーク検出] 画面を開きます。 • Threat Connect: このオブジェクトに対するクエリが含まれた新しいブラウザタブで [Trend Micro Threat Connect] を開きます。 • DomainTools (WHOIS): IP アドレスまたはドメインに対するクエリが含まれた新しいブラウザタブで [DomainTools] を開きます。 • VirusTotal: このオブジェクトに対するクエリが含まれた新しいブラウザタブで [VirusTotal] を開きます。

項目	操作
Deep Discovery Inspector のルール	ハイパーリンクが設定されているルールをクリックすると、そのルールに関する Trend Micro の脅威データベース画面が新しいブラウザタブで開きます。

[相関イベント] - [検出の詳細] を表示する

手順

1. イベントの検索の詳細を表示するには、[相関イベント] 画面の [詳細] 列にある [詳細] アイコンをクリックします。

   注意

   次の理由により、[詳細] アイコンが表示されないことがあります。

   - 関連する検出ログが削除されている
   - 現在のユーザアカウントの役割では、関連する検出があるアプライアンスを表示および管理できない
   - 関連する検出があるアプライアンスが [非管理対象] グループに移動された
   - 関連する検出があるアプライアンスが Deep Discovery Director (統合モード) から登録解除された

   そのイベントの検出の詳細が表示されます。

2. [接続の詳細] 画面では、次の操作を実行できます。
   - [Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。
   - [ダウンロード] をクリックしてから [接続の詳細] を選択すると、接続の詳細を CSV ファイルでダウンロードできます。
   - [ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

- パケットキャプチャが有効で、検出がパケットキャプチャルールに一致した場合、[ダウンロード] をクリックしてから [PCAP ファイル] を選択すると、PCAP ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

  PCAP ファイルの「pkt_comment」フィールドにあるコメント「Detected Packet」は、検出の原因となったパケットを示しています。

- [ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、パケットキャプチャファイル、および接続の詳細を含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。感染ファイルおよび PCAP ファイルはお客さまの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

---

3. [ファイル分析結果] セクションでは、次の操作を実行できます。

   - [仮想アナライザレポートの表示] をクリックすると、仮想アナライザレポートを表示できます。
   - [ダウンロード] をクリックしてから [仮想アナライザレポート] を選択すると、仮想アナライザレポートをダウンロードできます。
   - [ダウンロード] をクリックしてから [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - [ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。
   - [ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。検出されたファイルはユーザの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

4. [不審オブジェクトおよび関連するファイル分析結果] には、不審オブジェクトと分析された関連ファイル情報が表示されます。

[相関イベント] - [検出の詳細]

Deep Discovery Inspector では、検出された脅威ごとに詳細情報がログに記録されます。[検出の詳細] 画面には、検索やその他のフィルタ条件と設定に応じて、次の情報が表示されます。

- 187 ページの「[相関イベント] - [検出の詳細] - [接続の詳細]」
- 192 ページの「[相関イベント] - [検出の詳細] - [ファイル分析結果]」
- 194 ページの「[相関イベント] - [検出の詳細] - [不審オブジェクトおよび関連するファイル分析結果]」

[相関イベント] - [検出の詳細] - [接続の詳細]

[相関イベント] - [検出の詳細] 画面の [接続の詳細] には、次の情報を含めることができます。

- 188 ページの「[相関イベント] - [検出の詳細] - [検出情報]」
- 190 ページの「[相関イベント] - [検出の詳細] - [接続の概要]」
- 191 ページの「[相関イベント] - [検出の詳細] - [プロトコル情報]」
- 191 ページの「[相関イベント] - [検出の詳細] - [ファイル情報]」
- 192 ページの「[相関イベント] - [検出の詳細] - [追加情報]」

[Threat Connect で表示] をクリックすると、Threat Connect に接続して脅威に関する現在の情報を検索できます。

[ダウンロード] をクリックしてから [接続の詳細] を選択すると、接続の詳細を CSV ファイルでダウンロードできます。

[ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

パケットキャプチャが有効で、検出がパケットキャプチャルールに一致した場合、[ダウンロード] をクリックしてから [PCAP ファイル] を選択すると、PCAP ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。PCAP ファイルの「pkt_comment」フィールドにあるコメント「Detected Packet」は、検出の原因となったパケットを示しています。

[ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、パケットキャプチャファイル、および接続の詳細を含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

- 不審ファイルおよび PCAP ファイルは常に注意して扱う必要があります。感染ファイルおよび PCAP ファイルはお客さまの責任で抽出してください。ファイルは隔離された環境で分析することをお勧めします。
- zip アーカイブのパスワードは「virus」です。

[相関イベント] - [検出の詳細] - [検出情報]

[検出情報] セクションには、次の情報が表示されます。

- 検出されたアクティビティ
- 攻撃段階
- 相関分析ルール ID (ICID)
- 検出名
- 検出ルール ID
- 検出の重大度
- イベントクラス
- 顕著なオブジェクト

- プロトコル
- 参照
- 標的型攻撃
- 前回の検出
- 脅威
- 脅威の詳細
- 検出の種類
- タイムスタンプ
- URL カテゴリ
- 仮想アナライザのリスクレベル

注意

特定の相関関係のあるインシデントの追加情報が表示される場合もあります。

表 4-34. 検出の種類

検出の種類	説明
相関関係のあるインシデント	連続して発生した、またはしきい値に達したアクティビティのパターンを定義するイベント/検出
要注意アプリケーション	次の理由により要注意と見なされるピアツーピア、インスタントメッセンジャー、およびストリーミングメディアアプリケーション • ネットワークパフォーマンスに影響する • セキュリティリスクを発生させる • 従業員の注意を散漫にさせる
セキュリティホール悪用	情報に対するネットワークおよびファイルベースのアクセス試行
グレーウェア	さまざまな種類および信頼度レベルのアドウェア/グレーウェアの検出

検出の種類	説明
不正な動作	すでに不正であることが明確なため詳細な相関分析が不要な動作には次のものがあります。 • 明確に識別された不正プログラムによる通信 • 既知の不正な接続先 • 不正な動作パターンや文字列
不正なコンテンツ	シグネチャによる検出
不正な URL	不正な処理を実行しようとする Web サイト
不審動作	危険な可能性があり、相関分析を確認する必要がある動作には次のものがあります。 • 異常な動作 • 擬似データ • 不審な動作、不正な動作パターンや文字列

[相関イベント] - [検出の詳細] - [接続の概要]

[接続の概要] セクションには、次の情報が表示されます。

- イベントの方向やその他の情報を含むグラフィカル表示。図の [クライアント] は接続を開始したホストを表します。
- ホストの詳細には、次の情報が含まれます。
  - ホスト名
  - IP アドレスとポート
  - 前回のログオンユーザ
  - MAC アドレス
  - ネットワークグループ
  - ネットワークゾーン
  - OS

[相関イベント] - [検出の詳細] - [プロトコル情報]

[プロトコル情報] セクションには、次の情報が表示されます。

- ボットのコマンド
- ボットの URL
- ドメイン名
- ホスト名
- HTTP リファラ
- ICMP コード
- ICMP タイプ
- IRC チャネル名
- IRC ニックネーム
- メッセージ ID
- プロトコル
- クエリ対象ドメイン
- 受信者
- 送信者
- 件名
- ターゲット共有
- Transport Layer Security (TLS)
- URL
- ユーザエージェント
- ユーザ名

[相関イベント] - [検出の詳細] - [ファイル情報]

[ファイル情報] セクションには、次の情報が表示されます。

- ファイル名
- SHA-1
- SHA-256
- ファイルサイズ

[相関イベント] - [検出の詳細] - [追加情報]

[追加情報] セクションには、次の情報が表示されます。

- 接続の中断の試行
- 検出元
- Mitigation
- VLAN ID

[相関イベント] - [検出の詳細] - [ファイル分析結果]

[相関イベント] - [検出の詳細] 画面の [ファイル分析結果] には、次の情報が表示されます。

- 193 ページの「[相関イベント] - [検出の詳細] - [ファイル分析結果] - [ファイル情報]」
- 194 ページの「[相関イベント] - [検出の詳細] - [ファイル分析結果] - [著しい特性]」

[仮想アナライザレポートの表示] をクリックすると、仮想アナライザレポートを表示できます。

[ダウンロード] をクリックしてから [仮想アナライザレポート] を選択すると、仮想アナライザレポートをダウンロードできます。

ヒント

仮想アナライザレポートの表示またはダウンロードは、その他のオプションより時間がかかる場合があります。仮想アナライザレポートの表示またはダウンロードに時間がかかる点についてご了承ください。

[ダウンロード] をクリックしてから [調査パッケージ] を選択すると、調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

重要

不審ファイルは常に注意して扱う必要があります。検出されたファイルはユーザの責任で抽出してください。

zip アーカイブのパスワードは「virus」です。

[ダウンロード] をクリックしてから [感染ファイル] を選択すると、感染ファイルを含むパスワード保護された ZIP アーカイブをダウンロードできます。

[ダウンロード] をクリックしてから [すべて] を選択すると、感染ファイル、仮想アナライザレポート、および調査パッケージを含むパスワード保護された ZIP アーカイブをダウンロードできます。

[相関イベント] - [検出の詳細] - [ファイル分析結果] - [ファイル情報]

[検出の詳細] 画面の [ファイル分析結果] - [ファイル情報] セクションには、次の情報が表示されます。

- 子オブジェクト
  - ファイル名/URL
  - ファイルサイズ (バイト)
  - 種類
  - SHA-1
  - SHA-256
- ファイル名
- ファイルサイズ
- ファイルの種類
- MD5

- SHA-1
- SHA-256
- 脅威
- 仮想アナライザのリスクレベル

[相関イベント] - [検出の詳細] - [ファイル分析結果] - [著しい特性]

[検出の詳細] 画面の [ファイル分析結果] - [著しい特性] には、一般に不正プログラムに関連付けられる特性が表示されます。特性は次のカテゴリに分類されます。

- セキュリティ違反、自己保存
- 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
- 不正な形式またはその他の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
- その他の著しい特性

[相関イベント] - [検出の詳細] - [不審オブジェクトおよび関連するファイル分析結果]

[相関イベント] - [検出の詳細] 画面の [不審オブジェクトおよび関連するファイル分析結果] には、次の情報が表示されます。

- 195 ページの「[相関イベント] - [検出の詳細] - [不審オブジェクト情報]」
- 195 ページの「[相関イベント] - [検出の詳細] - [分析された関連ファイル情報]」

[相関イベント] - [検出の詳細] - [不審オブジェクト情報]

[不審オブジェクト情報] セクションには、次の情報が表示されます。

- 分析された関連ファイル
- 仮想アナライザのリスクレベル
- 不審オブジェクト
- 種類

[相関イベント] - [検出の詳細] - [分析された関連ファイル情報]

[検出の詳細] 画面の [分析された関連ファイル情報] セクションには、次の情報が表示されます。

- 子オブジェクト
  - ファイル名
  - ファイルサイズ (バイト)
  - 種類
  - SHA-1
  - SHA-256
- ファイル名
- ファイルサイズ
- ファイルの種類
- MD5
- SHA-1
- SHA-256
- 脅威
- 仮想アナライザのリスクレベル

一般的に不正プログラムの特性は、次のカテゴリに分類されます。

- 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
- 不正な形式またはその他の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
- その他の著しい特性

無視ルール

[無視ルール] 機能を使用すると、特定の検出ログを管理コンソールで非表示にして、情報を表示する際にその検出ログを無視することができます。

無視ルールのタスク

タスク	手順
無視ルールの作成	[ネットワーク検出] または [メールメッセージ] の [詳細検索] フィルタを使用します。 詳細については、197 ページの「無視ルールを作成する」を参照してください。
ルールの詳細表示	[条件] または [説明] 列の任意のテキストの上にマウスカーソルを重ねると、無視ルールの詳細が表示されます。
ルールの削除	削除する無視ルールを 1 つ以上選択して、[削除] をクリックします。

タスク	手順
ルールのステータスの切り替え	[ステータス] 列で切り替えスイッチをクリックします。 重要 初期設定では、無視ルールは無効になっています。ルールを有効にすると、一致する検出ログが管理コンソールで非表示になり、情報を表示する際に無視されます。

無視ルールを作成する

手順

1. 無視ルールを作成するには、[検出] > [ネットワーク検出] または [検出] > [メールメッセージ] の順に選択し、[詳細] をクリックします。
2. 属性および関連付けられた演算子を選択します。
3. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

   ヒント
   キーワードを入力して、部分一致を検索します。

   注意
   値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。
4. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
5. [無視ルールの作成] をクリックします。

   [無視ルールの作成] ダイアログが表示されます。

6. ルールの名前を入力します。
7. (オプション) ルールの説明を入力します。
8. [保存] をクリックします。

   無視ルールが作成され、[検出] > [無視ルール] 画面から有効にできるようになります。

第 5 章

脅威インテリジェンス

次の項目では、脅威インテリジェンスと関連タスクについて説明しています。

製品インテリジェンス

Deep Discovery Director (統合モード) では、管理下のアプライアンスで検出された脅威インテリジェンスを一元管理します。

同期された不審オブジェクト

[同期された不審オブジェクト] 画面には、仮想アナライザで検出された不審オブジェクトのリストが表示されます。

検出された不審オブジェクトは、[オブジェクト]、[種類]、[リスクレベル]、[同期元]、[失効日時]、および [検出] で並び替えることができます。

同期された不審オブジェクトを表示する

同期された不審オブジェクトを表示することで、そのリスクを理解し、関連する検出を確認して、不審オブジェクトの相対的な出現率を評価できます。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [同期された不審オブジェクト] の順に選択します。

   [同期された不審オブジェクト] 画面が表示されます。

2. 検出の種類のドロップダウンをクリックして、次のいずれかを選択します。

   - すべて (初期設定)
   - IP アドレス
   - URL
   - SHA-1
   - ドメイン

3. 検索を実行するには、検索テキストボックスに IP アドレス、ドメイン、URL、または SHA-1 ハッシュ値を入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

4. (オプション) [ネットワーク検出] または [メールメッセージ] の列の数字をクリックすると、フィルタが適用された [ネットワーク検出] または [メールメッセージ] 画面が表示されます。

   注意

   [ネットワーク検出] の数字には、Deep Discovery Inspector アプライアンスからの検出のみが含まれます。[メールメッセージ] の数字には、Deep Discovery Email Inspector アプライアンスからのメールメッセージのみが含まれます。

5. (オプション) 検出関連の表示を設定するには、列タイトルの [ネットワーク検出] または [メールメッセージ] アイコンの上にマウスカーソルを重ね、[表示設定] を選択します。

   a. 期間を選択します。

   b. データソースとして含めるアプライアンスと、メールメッセージを表示するドメインを選択します。

      注意

      期間、データソース、および監視対象ドメインのフィルタは、[検出] の件数にのみ影響します。

   c. [適用] をクリックします。

6. (オプション) 列のタイトルをクリックして、同期された不審オブジェクトのリストを並び替えます。

同期された不審オブジェクトをエクスポートする

[同期された不審オブジェクト] リストは、CSV 形式でエクスポートして表示できます。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [同期された不審オブジェクト] の順に選択します。

   [同期された不審オブジェクト] 画面が表示されます。

2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。

   詳細については、200 ページの「同期された不審オブジェクトを表示する」を参照してください。

3. [エクスポート] をクリックして、同期された不審オブジェクトの現在のフィルタ済みリストをエクスポートします。

   [エクスポート] ダイアログが表示されます。

4. フィルタを確認し、使用する区切り文字を選択します。

   - カンマ
   - セミコロン
   - スペース
   - タブ

5. [エクスポート] をクリックすると、選択した区切り文字で、同期された不審オブジェクトの現在のフィルタ済みリストが CSV ファイルにエクスポートされ、ダウンロードされます。

同期された不審オブジェクトを除外設定に移動する

無害と思われるオブジェクトは、[除外] リストに移動できます。除外設定は安全と見なされ、今後仮想アナライザで検出されても [同期された不審オブジェクト] リストには追加されません。

注意

新しく登録した Deep Discovery アプライアンスでは、脅威インテリジェンスの同期中、オブジェクトが [除外] と [同期された不審オブジェクト] の両方のリストに表示されることがあります。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [同期された不審オブジェクト] の順に選択します。

   [同期された不審オブジェクト] 画面が表示されます。

2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。

   詳細については、200 ページの「同期された不審オブジェクトを表示する」を参照してください。

3. 無害と思われるオブジェクトを 1 つ以上選択し、[除外に移動] をクリックします。

   [除外に移動] ダイアログが表示されます。

4. [移動] をクリックして、選択したオブジェクトを [除外] リストに移動します。

同期された不審オブジェクトを失効させる

オブジェクトを失効させると、[同期された不審オブジェクト] リストから削除されます。その後、同じオブジェクトが仮想アナライザで検出された場合は、再度 [同期された不審オブジェクト] リストに追加されます。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [同期された不審オブジェクト] の順に選択します。

   [同期された不審オブジェクト] 画面が表示されます。

2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。

   詳細については、200 ページの「同期された不審オブジェクトを表示する」を参照してください。

3. [同期された不審オブジェクト] から削除するオブジェクトを 1 つ以上選択し、[すぐに失効] をクリックします。

   [すぐに失効] ダイアログが表示されます。

4. [失効] をクリックすると、選択したオブジェクトが [同期された不審オブジェクト] リストから削除されます。

同期された不審オブジェクトを失効期限なしに設定する

有害と思われるオブジェクトを失効期限なしに設定すると、[同期された不審オブジェクト] リストから削除されないようになります。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [同期された不審オブジェクト] の順に選択します。

   [同期された不審オブジェクト] 画面が表示されます。

2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。

   詳細については、200 ページの「同期された不審オブジェクトを表示する」を参照してください。

3. 有害と思われるオブジェクトを 1 つ以上選択し、[失効期限なし] をクリックします。

   [失効期限なし] ダイアログが表示されます。

4. [失効期限なし] をクリックすると、選択したオブジェクトが失効期限なしに設定され、[同期された不審オブジェクト] リストから削除されないようになります。

失効日を設定する

初期設定では、同期された不審オブジェクトの有効期限は 21 日です。新しく同期された不審オブジェクトの有効期限を短く設定することができます。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [同期された不審オブジェクト] の順に選択します。

[同期された不審オブジェクト] 画面が表示されます。

2. [失効日時] 列の上にある歯車のアイコンをクリックします。

   [失効日の設定] ダイアログが表示されます。

3. [新しく同期した不審オブジェクトが失効するまでの期間:] を選択し、ドロップダウンリストから日数を選択します。

4. [保存] をクリックします。

C&C コールバックアドレス

[C&C コールバックアドレス] 画面には、Deep Discovery Inspector の検索エンジンパターンファイルおよびルールの一致により識別される C&C コールバックアドレスのリストが表示されます。

C&C コールバックアドレスの検出は、[コールバックアドレス]、[C&C リスクレベル]、[種類]、[同期元]、[最新のコールバック]、および [コールバック] で並び替えることができます。

[C&C コールバックアドレス] を表示する

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [C&C コールバックアドレス] の順に選択します。

   [C&C コールバックアドレス] 画面が表示されます。

2. 検出の種類のドロップダウンをクリックして、次のいずれかを選択します。

   - すべて (初期設定)
   - IP アドレス
   - URL
   - ドメイン

3. 表示を設定するには、[コールバック] 列のタイトルの上にマウスカーソルを重ね、[表示設定] を選択します。

   [表示設定] ダイアログが表示されます。

4. 期間を選択します。

5. データソースとして含めるアプライアンスを選択します。

   注意

   期間とデータソースのフィルタは、[コールバック] の件数にのみ影響します。

6. 部分一致検索を実行するには、検索テキストボックスにキーワードを入力して (大文字小文字は区別されません)、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

7. (オプション) [コールバック] 列の数字をクリックすると、フィルタが適用された [ネットワーク検出] 画面が表示されます。

8. (オプション) 列のタイトルをクリックして、C&C コールバックアドレスのリストを並び替えます。

C&C コールバックアドレスをエクスポートする

[C&C コールバックアドレス] リストは、CSV 形式でエクスポートして表示できます。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [C&C コールバックアドレス] の順に選択します。

   [C&C コールバックアドレス] 画面が表示されます。

2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。詳細については、205 ページの「[C&C コールバックアドレス] を表示する」を参照してください。

3. [エクスポート] をクリックして、C&C コールバックアドレスの現在のフィルタ済みリストをエクスポートします。

   [エクスポート] が表示されます。

4. フィルタを確認し、使用する区切り文字を選択します。

   - カンマ
   - セミコロン
   - スペース
   - タブ

5. [エクスポート] をクリックすると、選択した区切り文字で C&C コールバックアドレスの現在のフィルタ済みリストが CSV ファイルにエクスポートされ、ダウンロードされます。

C&C コールバックアドレスをユーザ指定の不審オブジェクトにコピーする

有害と思われる C&C コールバックアドレスを、[ユーザ指定の不審オブジェクト] リストにコピーできます。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [C&C コールバックアドレス] の順に選択します。

   [C&C コールバックアドレス] 画面が表示されます。

2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。詳細については、205 ページの「[C&C コールバックアドレス] を表示する」を参照してください。

3. 有害と思われる 1 つ以上の C&C コールバックアドレスを選択し、[ユーザ指定の不審オブジェクトにコピー] をクリックします。

   [ユーザ指定の不審オブジェクトにコピー] ダイアログが表示されます。

4. [コピー] をクリックして、選択した C&C コールバックアドレスを [ユーザ指定の不審オブジェクト] リストにコピーします。

C&C コールバックアドレスを除外設定にコピーする

無害と思われる C&C コールバックアドレスは、[除外] リストにコピーできます。

手順

1. [脅威インテリジェンス] > [製品インテリジェンス] > [C&C コールバックアドレス] の順に選択します。

   [C&C コールバックアドレス] 画面が表示されます。

2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。詳細については、205 ページの「[C&C コールバックアドレス] を表示する」を参照してください。

3. 無害と思われる 1 つ以上の C&C コールバックアドレスを選択し、[除外にコピー] をクリックします。

   [除外にコピー] ダイアログが表示されます。

4. [コピー] をクリックして、選択した C&C コールバックアドレスを [除外] リストにコピーします。

カスタムインテリジェンス

Deep Discovery 製品では、さまざまな方法により、まだ識別されていない不審オブジェクトからネットワークを保護します。

- 209 ページの「YARA ルール」
- 215 ページの「STIX」
- 217 ページの「ユーザ指定の不審オブジェクト」

Deep Discovery Director (統合モード) では、SHA-1 ハッシュ値、IP アドレス、ドメイン、または URL に基づいて [同期された不審オブジェクト] リストからオブジェクトを除外できます。

- 226 ページの「除外」

YARA ルール

Deep Discovery 製品では、YARA ルールを使用して不正プログラムを特定します。YARA ルールはカスタマイズ可能な不正プログラム検出パターンであり、標的型攻撃や環境に固有のセキュリティ脅威を特定します。

Deep Discovery Director (統合モード) 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。

次の表は、YARA ルールファイルについての情報を示しています。

表 5-1. YARA ルール

列	説明
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。
リスクレベル	YARA ルールのリスクレベル。 **注意** これらのリスクレベルは、Deep Discovery Email Inspector のみで使用されます。
説明	YARA ルールファイルの説明。
前回のアップデート	YARA ルールファイルが最後にアップデートされた日時。
アップデート実行元	YARA ルールファイルを最後にアップデートしたアカウント。

列	説明
ネットワーク検出	数字をクリックすると、フィルタが適用された [ネットワーク検出] 画面に詳細が表示されます。この数字には、Deep Discovery Inspector アプライアンスからの検出のみが含まれます。
メールメッセージ	数字をクリックすると、フィルタが適用された [メールメッセージ] 画面に詳細が表示されます。この数字には、Deep Discovery Email Inspector アプライアンスからのメールメッセージのみが含まれます。

YARA ルールファイルを作成する

Deep Discovery Director (統合モード) では、バージョン 3.10.0 の公式な仕様に準拠する YARA ルールファイルをサポートしています。YARA ルールは、任意のテキストエディタを使用して作成可能なプレーンテキストファイルに保存されます。

YARA ルールの記述の詳細については、次のサイトを参照してください。

https://yara.readthedocs.io/en/v3.10.0/writingrules.html

不正プログラムを検出するために仮想アナライザに追加する YARA ルールファイルは、次の特定の要件を満たしている必要があります。

- ファイル名が一意であること
- ファイルコンテンツが空でないこと

次の例は単純な YARA ルールを示しています。

```
rule NumberOne
{
meta:
desc = "Sonala"
weight = 10
strings:
$a = {6A 40 68 00 30 00 00 6A 14 8D 91}
$b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
$c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
condition:
$a or $b or $c
}
```

次の表に、YARA ルールを構成する各要素とその使用方法を示します。

表 5-2. 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** • この値は Deep Discovery 製品によって割り当てられたリスクレベルには対応しません。 • この値は Deep Discovery Email Inspector では無視されます。
strings:	「文字列」セクションの開始位置を示します。文字列は、不正プログラムを検出するための主要な手段です。
$a / $b / $c	不正プログラムの検出に使用する文字列です。$文字で開始し、1 つ以上の英数字やアンダースコアが続きます。
condition:	「条件」セクションの開始位置を示します。条件は、文字列をどのように使用して不正プログラムを検出するかを決定します。
$a or $b or $c	条件はルールの論理を定義するブール演算式です。送信されたオブジェクトがルールを満たすかどうかを判断するための条件を示します。条件には、通常のブール演算子 (and、or、not) に加えて関係演算子 (>=、<=、<、>、==、!=) を指定できます。数式には算術演算子 (+、-、*、\、%) およびビット演算子 (&、|、<<、>>、~、^) を使用できます。

YARA ルールファイルを追加する

管理下のアプライアンスの YARA ルールは、Deep Discovery Director (統合モード) と同期すると上書きされます。YARA ルールが失われないようにするには、管理下のアプライアンスからエクスポートして、Deep Discovery Director (統合モード) に追加します。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [YARA ルール] の順に選択します。

   [YARA ルール] 画面が表示されます。

2. [追加] をクリックします。

   [YARA ルールファイルの追加] ダイアログが表示されます。

3. [選択] をクリックして、追加する YARA ルールファイルを指定します。

4. この YARA ルールファイルに固有の仮想アナライザの処理を行うファイルタイプを指定するには、ファイルタイプを選択するか、入力して検索し、<Enter> キーを押します。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仮想アナライザで処理する場合は、[すべてのファイルタイプ] を選択します。

   注意

   - YARA ルールの対象となるファイルタイプのみ指定することをお勧めします。[すべてのファイルタイプ] オプションには、仮想アナライザでサポートされないファイルタイプも含まれます。このようなファイルタイプは、Deep Discovery Email Inspector のみで使用されます。
   - 仮想アナライザでサポートされないファイルタイプは、カスタムファイルタイプとして追加できます。カスタムファイルタイプは、Deep Discovery Email Inspector のみで使用されます。

5. ファイルの YARA ルールのリスクレベルを選択します。

注意

これらのリスクレベルは、Deep Discovery Email Inspector のみで使用されます。

6. (オプション) YARA ルールファイルの説明を入力します。
7. [追加] をクリックします。

   YARA ルールファイルが [YARA ルール] リストに表示されます。登録済みのアプライアンスは、更新された [YARA ルール] リストを次回の同期で受信します。

YARA ルールファイルを編集する

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [YARA ルール] の順に選択します。

   [YARA ルール] 画面が表示されます。
2. 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。

   [YARA ルールファイルの編集] ダイアログが表示されます。
3. 設定を変更します。
4. [保存] をクリックします。

YARA ルールファイルをエクスポートする

YARA ルールファイルをエクスポートして、YARA に互換性のある他の製品で使用できます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [YARA ルール] の順に選択します。

[YARA ルール] 画面が表示されます。

2. 次のいずれかを実行して、YARA ルールファイルをエクスポートします。

   - すべての YARA ルールファイルをエクスポートするには、YARA ルールファイルを選択せずに [エクスポート] をクリックします。
   - 特定の YARA ルールファイルをエクスポートするには、エクスポートする YARA ルールファイルを選択して、[選択したファイルのエクスポート] をクリックします。

   Deep Discovery Director (統合モード) で、YARA ルールファイルの ZIP アーカイブが作成されます。

   注意

   YARA ルールファイルのインポート時に使用していた元のエンコード方式にかかわらず、エクスポートされた YARA ルールファイルでは、常に UTF-8 エンコーディングが使用されます。

3. ZIP アーカイブをダウンロードして保存します。

YARA ルールファイルを削除する

使用していない YARA ルールファイルを削除して使用中のルール数を減らし、データベースのディスク空き容量を増やします。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [YARA ルール] の順に選択します。

   [YARA ルール] 画面が表示されます。

2. 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。

YARA ルールファイルが [YARA ルール] リストから削除されます。登録済みのアプライアンスは、更新された [YARA ルール] リストを次回の同期で受信します。

STIX

Deep Discovery Director (統合モード) では、STIX (Structured Threat Information eXpression) 形式を使用して、オブジェクトを [ユーザ指定の不審オブジェクト] リストにインポートできます。

次の表は、STIX ファイルについての情報を示しています。

表 5-3. STIX

列	説明
ファイル名	STIX ファイルの名前
説明	STIX ファイルの説明
バージョン	STIX ファイルのバージョン
インポート済み	STIX ファイルがインポートされた日時
インポート実行元	STIX ファイルをインポートした Deep Discovery Director (統合モード) アカウントまたは TAXII クライアントの IP アドレス

オブジェクトを STIX からインポートする

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [STIX] の順に選択します。

   [STIX] 画面が表示されます。

2. [インポート] をクリックします。

   [STIX からのオブジェクトのインポート] ダイアログが表示されます。

3. [選択] をクリックして、インポートする STIX ファイルを指定します。
4. (オプション) STIX ファイルの説明を入力します。
5. [インポート] をクリックします。

注意

- IP アドレス、ドメイン、URL、ファイルの SHA-1 ハッシュ値、およびファイルの SHA-256 ハッシュ値のみが [ユーザ指定の不審オブジェクト] リストに追加されます。
- STIX 1.x を使用する場合、`Confidence` が `Medium`、`Low`、`None`、または `Unknown` でない `Indicator` のみが [ユーザ指定の不審オブジェクト] リストに追加されます。
- STIX 2.0 を使用する場合、`"anomalous-activity"`、`"anonymization"`、`"benign"`、または`"compromised"`としてラベル付けされておらず、失効していない`"indicator"`タイプのオブジェクトのみが [ユーザ指定の不審オブジェクト] リストに追加されます。
- STIX ファイルとオブジェクト情報は、脅威インテリジェンスの一部として共有できます。

オブジェクトが [ユーザ指定の不審オブジェクト] リストに表示されます。登録済みのアプライアンスは、更新された [ユーザ指定の不審オブジェクト] リストを次回の同期で受信します。

STIX ファイルをエクスポートする

STIX ファイルをエクスポートして、STIX に互換性のある他の製品で使用できます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [STIX] の順に選択します。

   [STIX] 画面が表示されます。

2. 次のいずれかを実行して、STIX ファイルをエクスポートします。

   - すべての STIX ファイルをエクスポートするには、STIX ファイルを選択せずに [エクスポート] をクリックします。
   - 特定の STIX ファイルをエクスポートするには、エクスポートする STIX ファイルを選択して、[選択したファイルのエクスポート] をクリックします。

   Deep Discovery Director (統合モード) で、STIX ファイルの ZIP アーカイブが作成されます。

STIX ファイルを削除する

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [STIX] の順に選択します。

   [STIX] 画面が表示されます。

2. 削除する STIX ファイルを 1 つ以上選択して、[削除] をクリックします。

   STIX ファイルが [STIX] リストから削除されます。

   注意

   STIX ファイルを削除しても、インポート済みのオブジェクトに影響はありません。

ユーザ指定の不審オブジェクト

[ユーザ指定の不審オブジェクト] リストには、Deep Discovery 製品の仮想アナライザではまだ検出されていない、不審ファイルの SHA-1 ハッシュ値、不審ファイルの SHA-256 ハッシュ値、IP アドレス、URL、およびドメインオブジェクトを定義できます。サポート対象の Deep Discovery 製品は、このリス

トに定義されたオブジェクトに処理を実行し、未知の脅威が拡散しないよう防止できます。

[ユーザ指定の不審オブジェクト] を表示する

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. 検出の種類のドロップダウンをクリックして、次のいずれかを選択します。

   - すべて (初期設定)
   - IP アドレス
   - URL
   - SHA-1
   - SHA-256
   - ドメイン

3. 検索を実行するには、検索テキストボックスに IP アドレス、ドメイン、URL、SHA-1 ハッシュ値、SHA-256 ハッシュ値、または説明のキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

4. (オプション) [ネットワーク検出] または [メールメッセージ] の列の数字をクリックすると、フィルタが適用された [ネットワーク検出] または [メールメッセージ] 画面が表示されます。

   注意

   [ネットワーク検出] の数字には、Deep Discovery Inspector アプライアンスからの検出のみが含まれます。[メールメッセージ] の数字には、Deep Discovery Email Inspector アプライアンスからのメールメッセージのみが含まれます。

5. (オプション) 表示を設定するには、列タイトルの [ネットワーク検出] または [メールメッセージ] アイコンの上にマウスカーソルを重ね、[表示設定] を選択します。

   a. 期間を選択します。

   b. データソースとして含めるアプライアンスと、メールメッセージを表示するドメインを選択します。

   注意

   期間、データソース、および監視対象ドメインのフィルタは、[検出] の件数にのみ影響します。

6. (オプション) 列のタイトルをクリックして、ユーザ指定の不審オブジェクトのリストを並び替えます。

[ユーザ指定の不審オブジェクト] - [相関データ] を表示する

Deep Discovery Director - Network Analytics は透過的ソリューションであり、相関データを使用した詳細な脅威分析を提供します。不審オブジェクトに相関データがある場合は、Deep Discovery Director からそのデータにアクセスできます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。
2. 相関データを表示するには、[詳細] の下にある [相関データ] アイコン () をクリックします。

注意

- 相関データが利用できない場合、[相関データ] アイコンはグレーアウトされています。
- Deep Discovery Director - Network Analytics では、不審オブジェクトが失効期限なしに設定されている場合であっても、不審オブジェクトの相関データを限られた期間のみ保管します。
- 相関データの収集元にする Deep Discovery Inspector アプライアンスは、接続済みソースとして有効にする必要があります。

[相関データ] 画面が表示されます。

3. 不正な活動の詳細分析が、次の各セクションに表示されます。

- 概要

  重大度、検出された内部ホストと侵害の兆候 (IOC) の数、および割り当てられている攻撃パターンが表示され、相関データの不正な活動の概要が示されます。

- 相関グラフ

  Deep Discovery Director で選択した相関イベントとその他の関連イベントとの相関関係が時間の経過に従って表示されます。

- トランザクションと IOC の詳細

  相関グラフに示された各トランザクションと、検出された侵害の兆候 (IOC) それぞれの詳細が表示されます。トランザクションは、最も古いものを先頭にして順番に表示されます。IOC は、最初に検出された最も古いものを先頭にして順番に表示されます。

ヒント

[相関データ] 画面の情報は動的に作成されます。この画面に表示される相関数、およびホスト間の相互処理や不正な活動についての詳細は、時間の経過とともに変化する可能性があります。特定の検出の相関データに後からアクセスすると、分析の詳細が追加されているかどうかを確認できます。

4. [相関データ] 画面に表示される情報を詳細分析に使用する方法については、163 ページの「相関データ情報を分析する」を参照してください。

ユーザ指定の不審オブジェクトを追加する

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [追加] をクリックします。

   [オブジェクトの追加] ダイアログが表示されます。

3. 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。

     注意

     IPv4 および IPv6 アドレスとサブネットマスクのビットがサポートされます。

   - URL: URL を入力します。

     注意

     HTTP および HTTPS の URL がサポートされます。

   - 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。
   - ドメイン: ドメイン名を入力します。

> **注意**
>
> ドメインのプレフィックスでは、「.」で連結した 1 文字のワイルドカード (*) がサポートされます。

4. (オプション) オブジェクトの説明を入力します。
5. [追加] をクリックします。

   オブジェクトが [ユーザ指定の不審オブジェクト] リストに表示されます。登録済みのアプライアンスは、更新された [ユーザ指定の不審オブジェクト] リストを次回の同期で受信します。

> **ヒント**
>
> オブジェクトは、[製品インテリジェンス] から追加することもできます。
>
> 詳細については、207 ページの「C&C コールバックアドレスをユーザ指定の不審オブジェクトにコピーする」を参照してください。

ユーザ指定の不審オブジェクトを編集する

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。
2. 編集するオブジェクトをクリックします。

   [オブジェクトの編集] ダイアログが表示されます。
3. 設定を変更します。

> **注意**
>
> オブジェクトの種類は変更できません。

4. [保存] をクリックします。

ユーザ指定の不審オブジェクトをインポートする

Deep Discovery Director (統合モード) では、CSV ファイルからオブジェクトをインポートできます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [インポート] をクリックします。

   [CSV からのオブジェクトのインポート] ダイアログが表示されます。

3. [選択] をクリックして、インポートする CSV ファイルを指定します。

   ヒント

   CSV ファイルを初めてインポートする場合は、[サンプル CSV のダウンロード] をクリックしてファイルを保存します。CSV ファイルにオブジェクトを正しい書式設定で入力して (CSV ファイル内の説明を参照)、ファイルを保存し、[選択] をクリックして CSV ファイルを指定します。

4. CSV ファイルで使用されている区切り記号を選択します。

5. [インポート] をクリックします。

   オブジェクトが [ユーザ指定の不審オブジェクト] リストに表示されます。登録済みのアプライアンスは、新しいオブジェクトの情報を次回の同期で受信します。

ユーザ指定の不審オブジェクトをエクスポートする

[ユーザ指定の不審オブジェクト] リストは、CSV 形式でエクスポートして表示できます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。
2. (オプション) 必要に応じてフィルタや検索キーワードを適用します。

   詳細については、218 ページの「[ユーザ指定の不審オブジェクト] を表示する」を参照してください。
3. [エクスポート] をクリックして、ユーザ指定の不審オブジェクトの現在のフィルタ済みリストをエクスポートします。

   [エクスポート] ダイアログが表示されます。
4. フィルタを確認し、使用する区切り文字を選択します。
   - カンマ
   - セミコロン
   - スペース
   - タブ
5. [エクスポート] をクリックすると、選択した区切り文字で、ユーザ指定の不審オブジェクトの現在のフィルタ済みリストが CSV ファイルにエクスポートされ、ダウンロードされます。

ユーザ指定の不審オブジェクトを削除する

使用していないユーザ指定の不審オブジェクトを削除して、オブジェクトの数を減らします。オブジェクトが最大数に達している場合、オブジェクトを追加またはインポートすると、最も古いオブジェクトが上書きされます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. 削除するオブジェクトを 1 つ以上選択して、[削除] をクリックします。

   オブジェクトが [ユーザ指定の不審オブジェクト] リストから削除されます。登録済みのアプライアンスは、更新された [ユーザ指定の不審オブジェクト] リストを次回の同期で受信します。

失効日を設定する

初期設定では、ユーザ指定の不審オブジェクトは失効期限なしに設定されます。既存および新しく追加されたユーザ指定の不審オブジェクトを、自動的に失効するように設定できます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [ユーザ指定の不審オブジェクト] の順に選択します。
2. 検出列の上にある歯車のアイコンをクリックします。

   [失効日の設定] ダイアログが表示されます。
3. [既存および新しく追加されたユーザ指定の不審オブジェクトが失効するまでの期間:] を選択し、ドロップダウンリストから日数を選択します。
4. [保存] をクリックします。

   失効日の設定は既存のオブジェクトにはただちに適用され、新しく追加されるオブジェクトには追加時に適用されます。

注意

- 指定した日数アップデートされないオブジェクトはただちに削除されます。削除されたオブジェクトを復元することはできません。
- 失効日の設定を無効にすると、すべての既存オブジェクトは失効期限なしに設定されます。

除外

無害と思われるオブジェクトは、[除外] リストに追加できます。除外設定は安全とみなされ、今後仮想アナライザで検出されても [同期された不審オブジェクト] リストには追加されません。

注意

新しく登録した Deep Discovery アプライアンスでは、脅威インテリジェンスの同期中、オブジェクトが [除外] と [同期された不審オブジェクト] の両方のリストに表示されることがあります。

[除外] を表示する

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [除外] の順に選択します。

   [除外] 画面が表示されます。

2. 検出の種類のドロップダウンをクリックして、次のいずれかを選択します。
   - すべて (初期設定)
   - IP アドレス
   - URL
   - SHA-1
   - ドメイン
3. 検索を実行するには、検索テキストボックスに IP アドレス、ドメイン、URL、SHA-1 ハッシュ値、または説明のキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。
4. (オプション) 列のタイトルをクリックして、除外設定のリストを並び替えます。

除外設定を追加する

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [除外] の順に選択します。

   [除外] 画面が表示されます。

2. [追加] をクリックします。

   [除外の追加] ダイアログが表示されます。

3. 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。

     注意

     IPv4 および IPv6 アドレスとサブネットマスクのビットがサポートされます。

   - URL: URL を入力します。

     注意

     HTTP および HTTPS の URL がサポートされます。

   - SHA-1: ファイルの SHA-1 ハッシュ値を入力します。
   - ドメイン: ドメイン名を入力します。

     注意

     ドメインのプレフィックスでは、「.」で連結した 1 文字のワイルドカード (*) がサポートされます。

4. (オプション) オブジェクトの説明を入力します。
5. [追加] をクリックします。

オブジェクトが [除外] リストに表示されます。登録済みのアプライアンスは、更新された [除外] リストを次回の同期で受信します。

ヒント

除外設定は、[製品インテリジェンス] から追加することもできます。詳細については、次の項目を参照してください。

- 202 ページの「同期された不審オブジェクトを除外設定に移動する」
- 208 ページの「C&C コールバックアドレスを除外設定にコピーする」

除外設定をインポートする

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [除外] の順に選択します。

   [除外] 画面が表示されます。

2. [インポート] をクリックします。

   [CSV からのオブジェクトのインポート] ダイアログが表示されます。

3. [選択] をクリックして、インポートする CSV ファイルを指定します。

   ヒント

   CSV ファイルを初めてインポートする場合は、[サンプル CSV のダウンロード] をクリックしてファイルを保存します。CSV ファイルにオブジェクトを正しい書式設定で入力して (CSV ファイル内の説明を参照)、ファイルを保存し、[選択] をクリックして CSV ファイルを指定します。

4. [インポート] をクリックします。

   オブジェクトが [除外] リストに表示されます。登録済みのアプライアンスは、新しいオブジェクトの情報を次回の同期で受信します。

除外設定を削除する

使用していない除外設定を削除して、オブジェクトの数を減らします。オブジェクトが最大数に達している場合、オブジェクトを追加またはインポートすると、最も古いオブジェクトが上書きされます。

手順

1. [脅威インテリジェンス] > [カスタムインテリジェンス] > [除外] の順に選択します。

   [除外] 画面が表示されます。

2. 削除するオブジェクトを 1 つ以上選択して、[削除] をクリックします。

   オブジェクトが [除外] リストから削除されます。登録済みのアプライアンスは、更新された [除外] リストを次回の同期で受信します。

フィード管理

Deep Discovery Director (統合モード) では、脅威情報のインテリジェンスフィードを登録および監視して、製品やカスタムインテリジェンスの補完として使用できます。

次の表は、インテリジェンスフィードについての情報を示しています。

表 5-4. インテリジェンスフィード

列	説明
フィード名	インテリジェンスフィードの名前。
TAXII バージョン	インテリジェンスフィードの TAXII バージョン。
API ルート	インテリジェンスフィードの API ルート。
コレクション	インテリジェンスフィードから選択したコレクション。
ポーリング間隔	インテリジェンスフィードをポーリングして情報を確認する頻度。

列	説明
前回のポーリング	インテリジェンスフィードを最後にポーリングした日時。
ステータス	クリックしてインテリジェンスフィードのポーリングの有効/無効を切り替えます。

インテリジェンスフィードを追加する

手順

1. [脅威インテリジェンス] > [フィード管理] の順に選択します。

   [フィード管理] 画面が表示されます。

2. [追加] をクリックします。

   [インテリジェンスフィードの追加] 画面が表示されます。

3. インテリジェンスフィードを有効にします。

4. インテリジェンスフィードの名前を入力します。

5. インテリジェンスフィードのサーババージョンを選択します。

   注意

   インテリジェンスフィードが追加されたら、サーババージョンを変更することはできません。

6. インテリジェンスフィードのディスカバリ URL を入力します。

7. (オプション) サーバでサーバ証明書を使用する場合は、[サーバ証明書を使用] を選択し、[選択] をクリックして、サーバ証明書ファイルを指定します。

8. (オプション) サーバで認証情報が必要な場合は、[認証情報の設定、認証情報の指定] を選択し、認証に使用するユーザ名とパスワードを入力します。

9. (オプション) サーバでクライアント認証が必要な場合は、[サーバでクライアント認証を要求] を選択し、[選択] をクリックして、クライアント証明書ファイルを指定します。
10. (オプション) クライアント証明書のパスフレーズを入力します。
11. [ディスカバー] をクリックし、使用可能なコレクションを探して選択します。
12. インテリジェンスフィードをポーリングして情報確認の実行間隔を選択します。
13. ポーリング時に過去の情報を取得するためにさかのぼる期間を選択します。
14. [追加] をクリックします。

    インテリジェンスフィードが [フィード管理] リストに表示されます。IP アドレス、ドメイン、URL、SHA-1 ハッシュ値、および SHA-256 ハッシュ値を含むポーリングされた情報が [ユーザ指定の不審オブジェクト] リストに追加されます。登録済みのアプライアンスは、更新された [ユーザ指定の不審オブジェクト] リストを次回の同期で受信します。

注意

- TAXII 1.x を使用する場合、`Confidence` が `Medium`、`Low`、`None`、または `Unknown` でない `Indicator` のみが [ユーザ指定の不審オブジェクト] リストに追加されます。
- TAXII 2.0 を使用する場合、`"anomalous-activity"`、`"anonymization"`、`"benign"`、または`"compromised"`としてラベル付けされておらず、失効していない`"indicator"`タイプのオブジェクトのみが [ユーザ指定の不審オブジェクト] リストに追加されます。
- TAXII 2.0 を使用する場合、サーバの互換性を確保するための特定の仕様が存在します。詳細については、次のサイトを参照してください。

  http://docs.oasis-open.org/cti/taxii/v2.0/cs01/taxii-v2.0-cs01.html

インテリジェンスフィードを編集する

手順

1. [脅威インテリジェンス] > [フィード管理] の順に選択します。

   [フィード管理] 画面が表示されます。

2. 編集するインテリジェンスフィードのフィード名をクリックします。

   [インテリジェンスフィードの編集] 画面が表示されます。

3. 設定を変更します。

   注意

   インテリジェンスフィードが追加されたら、サーババージョンを変更することはできません。

4. [保存] をクリックします。

インテリジェンスフィードを削除する

手順

1. [脅威インテリジェンス] > [フィード管理] の順に選択します。

   [フィード管理] 画面が表示されます。

2. 削除するインテリジェンスフィードを 1 つ以上選択して、[削除] をクリックします。

   インテリジェンスフィードが [フィード管理] リストから削除されます。インテリジェンスフィードから取得した STIX ファイルや、[STIX] リストに追加された STIX ファイルは削除されます。STIX ファイルを削除しても、インポート済みのオブジェクトに影響はありません。

共有設定

Deep Discovery Director (統合モード) では、さまざまな方法で脅威インテリジェンスデータを他の製品やサービスと共有できます。

TAXII 1.x

Deep Discovery Director (統合モード) では、TAXII 1.x を使用して脅威インテリジェンスデータを他の製品またはサービスと共有できます。

TAXII 1.x を設定する

手順

1. [脅威インテリジェンス] > [共有設定] > [TAXII 1.x] の順に選択します。

   [TAXII 1.x] 画面が表示されます。

2. [TAXII 1.x サーバを有効にして、脅威インテリジェンスの統合製品/サービスとの連携を許可する] を選択します。

3. 認証に使用するユーザ名とパスワードを入力します。

4. 脅威インテリジェンスのデータファイルに含めるオブジェクトのリスクレベルを選択します。

5. [保存] をクリックします。

6. (オプション) [生成] をクリックします。

7. Deep Discovery Director (統合モード) では脅威情報が 10 分おきに自動生成されます。Deep Discovery Director (統合モード) の脅威情報のディスカバリ URL を登録および監視する統合製品/サービスを設定します。詳細については、統合製品/サービスのドキュメントを参照してください。

TAXII 2.0

Deep Discovery Director (統合モード) では、TAXII 2.0 を使用して脅威インテリジェンスデータを他の製品またはサービスと共有できます。

TAXII 2.0 を設定する

手順

1. [脅威インテリジェンス] > [共有設定] > [TAXII 2.0] の順に選択します。

   [TAXII 2.0] 画面が表示されます。

2. [TAXII 2.0 サーバを有効にして、脅威インテリジェンスの統合製品/サービスとの連携を許可する] を選択します。

3. 認証に使用するユーザ名とパスワードを入力します。

4. 脅威インテリジェンスのデータファイルに含めるオブジェクトのリスクレベルを選択します。

5. [保存] をクリックします。

6. (オプション) [生成] をクリックします。

7. Deep Discovery Director (統合モード) では脅威情報が 10 分おきに自動生成されます。Deep Discovery Director (統合モード) の脅威情報のディスカバリ URL を登録および監視する統合製品/サービスを設定します。詳細については、統合製品/サービスのドキュメントを参照してください。

OpenDXL

Deep Discovery Director (統合モード) では、脅威インテリジェンスのデータを OpenDXL クライアント、サービス、およびブローカーに配信できます。

OpenDXL を設定する

手順

1. [脅威インテリジェンス] > [共有設定] > [OpenDXL] の順に選択します。

   [OpenDXL] 画面が表示されます。

2. [OpenDXL クライアント/サービス/ブローカーにオブジェクトを配信する] を選択します。
3. サーバのアドレスを入力します。
4. ポート番号を入力します。
5. [選択] をクリックし、認証に使用するサーバ証明書、クライアント証明書、およびキーファイルを指定します。
6. (オプション) [接続テスト] をクリックします。
7. 脅威インテリジェンスのデータに含めるオブジェクトを選択します。
8. 脅威インテリジェンスのデータに含めるオブジェクトのリスクレベルを選択します。
9. オブジェクト配信の実行間隔を選択します。
10. [保存] をクリックします。
11. (オプション) [配信] をクリックして、不審オブジェクトおよび C&C コールバックアドレスをこの OpenDXL クライアント/サービス/ブローカーに配信します。

Web サービス

Deep Discovery Director (統合モード) では、HTTP または HTTPS Web サービスを介して、脅威インテリジェンスデータを Blue Coat ProxySG デバイスなど他の製品やサービスと共有できます。

Web サービスを設定する

手順

1. [脅威インテリジェンス] > [共有設定] > [Web サービス] の順に選択します。

   [Web サービス] 画面が表示されます。

2. [Web サービスを有効にして、統合製品/サービスに Deep Discovery Director の情報の取得を許可する] を選択します。

3. (オプション) 初期設定で、脅威インテリジェンスのデータは HTTPS Web サービス経由でのみ共有されます。HTTP を介したデータの共有を追加で有効にするには、[HTTP を使用して情報を共有 (HTTPS に追加)] 選択し、HTTP サーバのポート番号を指定します。

4. 脅威インテリジェンスのデータファイルに含めるオブジェクトを選択します。

5. 脅威インテリジェンスのデータファイルに含めるオブジェクトのリスクレベルを選択します。

   生成されるファイル内の次のカテゴリにオブジェクトが表示されます。

   表 5-5. 生成されるファイル内のオブジェクトカテゴリ

オブジェクト	生成されるファイル内のカテゴリ
同期された不審オブジェクト	DDD_so_list
ユーザ指定の不審オブジェクト	DDD_so_list
C&C コールバックアドレス	DDD_cnc_callback_addresses_list
統合製品から Web レピュテーションサービスにより検出された不正 URL	DDD_wrs_list

6. オブジェクト共有の実行間隔を選択します。

7. [保存] をクリックします。

8. (オプション) [生成] をクリックします。

注意

ファイルが生成されたら、URL をクリックし、脅威インテリジェンスのデータファイルをダウンロードして内容を確認できます。

9. Blue Coat ProxySG デバイスなどの統合製品/サービスを設定して、Deep Discovery Director (統合モード) から脅威インテリジェンスのデータを取得します。詳細については、統合製品/サービスのドキュメントを参照してください。

補助製品/サービス

脅威を効果的に検出してネットワーク侵入前に阻止するため、脅威インテリジェンスのデータを補助製品やサービスに配信できます。

Deep Discovery Director (統合モード) は、次のソリューションと連携します。

表 5-6. サポート対象のソリューション

名前	バージョン
Trend Micro TippingPoint Security Management System (SMS)	SMS 4.6.0 以降
Check Point Open Platform for Security (OPSEC)	Check Point R80.10 以降
IBM Security Network Protection (XGS)	XGS 5.2 以降
Palo Alto Panorama	PAN-OS 7.0.1 以降
Palo Alto Firewalls	PAN-OS 4.1.0 以降

Trend Micro TippingPoint Security Management System (SMS)

Deep Discovery Director (統合モード) では、同期された不審オブジェクト、ユーザ指定の不審オブジェクト、および C&C コールバックアドレスを Trend Micro TippingPoint Security Management System (SMS) に送信できます。

注意

次の操作を実行すると、Trend Micro TippingPoint Security Management System (SMS) から不審オブジェクトが削除されます。

- 同期された不審オブジェクトを除外設定に移動する
- 同期された不審オブジェクトを失効させる
- ユーザ指定の不審オブジェクトを削除する

Deep Discovery Director (統合モード) では、C&C コールバックアドレスと不審オブジェクトのそれぞれに、次のオプション情報を含めて送信します。

- Trend Micro Severity: 各不審オブジェクトまたは C&C コールバック試行の重大度
- Trend Micro Publisher: トレンドマイクロ Deep Discovery Director (統合モード) の製品名
- Trend Micro Source: Deep Discovery Director (統合モード) のホスト名
- Trend Micro Detection Category: 不審オブジェクトまたは C&C コールバック試行
- Reputation Entries TTL: C&C コールバックアドレスまたは不審オブジェクトの有効期間 (TTL)

注意

SMS 5.1 以上でのみサポートされます。

Trend Micro TippingPoint Security Management System (SMS) を設定する

手順

1. Deep Discovery Director (統合モード) の管理コンソールで、[脅威インテリジェンス] > [共有設定] > [補助製品/サービス] の順に選択します。

   [補助製品/サービス] 画面が表示されます。

2. [補助製品/サービスにオブジェクトを配信する] を選択します。
3. [Trend Micro TippingPoint Security Management System (SMS)] を選択します。
4. サーバのアドレスを入力します。

   注意

   サーバのアドレスは、補助製品/サービスの IPv4 アドレスまたは完全修飾ドメイン名である必要があります。

5. 認証に使用するユーザ名とパスワードを入力します。
6. (オプション) [接続テスト] をクリックします。
7. Deep Discovery Director (統合モード) からこの補助製品/サービスにオブジェクト情報を送信するには、次の条件を設定します。
   - オブジェクトの種類:
     - C&C コールバックアドレス
       - IPv4 アドレス
       - ドメイン
       - URL

       注意

       SMS 5.0 以上でのみサポートされます。

     - 不審オブジェクト
       - IPv4 アドレス
       - ドメイン
       - URL

       注意

       SMS 5.0 以上でのみサポートされます。

- リスクレベル:
  - 高のみ
  - 高および中
  - 高、中、および低

8. オブジェクト情報の配信の実行間隔を選択します。
9. [保存] をクリックします。

   次のタグのカテゴリが TippingPoint SMS Reputation Database に表示されます。

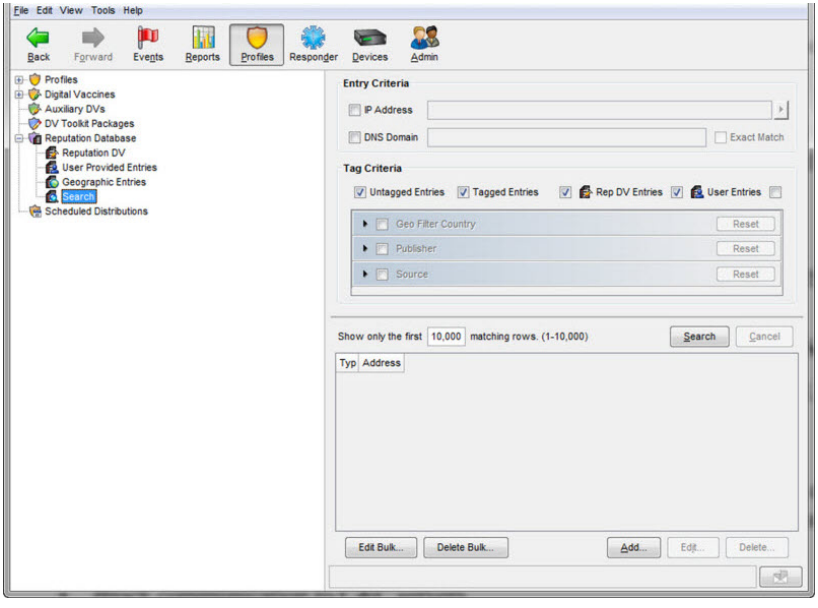
タグのカテゴリ	値
Trend Micro Source	Deep Discovery Director (統合モード) のホスト名
Trend Micro Severity	指定可能な値: • 高 • 中 • 低
Trend Micro Publisher	Deep Discovery Director (統合モード) の製品名
Trend Micro Detection Category	脅威の検出の種類
Reputation Entries TTL	YYYY-MM-DD hh:mm:ss TZ 形式のタイムスタンプで表示される有効期間 (TTL) 注意 SMS 5.1 以上でのみサポートされます。

10. (オプション) 配信された C&C コールバックアドレスおよび不審オブジェクトを TippingPoint SMS で表示するには、次の手順を実行します。

    a. 次のタグのカテゴリが TippingPoint SMS クライアントの [Tag Categories] リストに含まれていることを確認します。

- Trend Micro Severity
- Trend Micro Source
- Trend Micro Publisher
- Trend Micro Detection Category

b. [Profile] タブで [Reputation Database] > [Search] の順に選択します。



c. [Entry Criteria] 画面で検索パラメータを入力し、[Search] をクリックします。

Deep Discovery Director (統合モード) から配信された不審オブジェクトおよび C&C コールバックアドレスが表示されます。

Check Point OPSEC (Open Platform for Security)

Check Point OPSEC (Open Platform for Security) は、オープンかつ拡張可能な管理フレームワークを通じてネットワークのセキュリティを管理します。

Deep Discovery Director (統合モード) は、SAM (Suspicious Activities Monitoring) API を介して Check Point OPSEC と統合されます。

SAM API を実装した SAM クライアント (Deep Discovery Director (統合モード)) は、Check Point ファイアウォールとの通信を行い、SAM サーバとして機能します。Deep Discovery Director (統合モード) は、SAM API を使用して、特定の接続に対して指定した処理を実行するよう Check Point ファイアウォールに要求します。

たとえば、Deep Discovery Director (統合モード) は、不正なコマンドを発行しているクライアントやログオンに繰り返し失敗しているクライアントとの接続をブロックするよう Check Point OPSEC に求める場合があります。

Check Point OPSEC (Open Platform for Security) を設定する

手順

1. Deep Discovery Director (統合モード) の管理コンソールで、[脅威インテリジェンス] > [共有設定] > [補助製品/サービス] の順に選択します。

   [補助製品/サービス] 画面が表示されます。

2. [補助製品/サービスにオブジェクトを配信する] を選択します。

3. [Check Point Open Platform for Security (OPSEC)] を選択します。

4. [有効にする場合必ずお読みください] をクリックします。

   [有効にする場合必ずお読みください] ダイアログが表示されます。

5. [有効にする場合必ずお読みください] を読み、同意できる場合は同意します。

   重要

   この補助製品/サービスとの連携を有効にするには、[有効にする場合必ずお読みください] に同意する必要があります。

6. 接続の種類を選択します。

注意

ネットワーク設定で、Deep Discovery Director (統合モード) から Check Point のアプライアンスへの接続が許可されていることを確認します。

Deep Discovery Director (統合モード) から Check Point のアプライアンスへの接続には、Check Point のアプライアンスで設定された保護された接続ポートまたは通常の接続ポートが使用されます。また Deep Discovery Director (統合モード) では、ポート 18210 を介して Check Point のアプライアンスから証明書を取得します。

7. サーバのアドレスを入力します。

注意

サーバのアドレスは、補助製品/サービスの IPv4 アドレスまたは解決可能なホスト名である必要があります。

8. ポート番号を入力します。

注意

このポート番号は、セキュリティゲートウェイに設定されているポート番号と同じである必要があります。詳細については、248 ページの「セキュリティゲートウェイを事前設定する」を参照してください。

9. [保護された接続] を選択した場合は、[OPSEC アプリケーション名] と [SIC ワンタイムパスワード] を入力します。

   詳細については、250 ページの「保護された接続を設定する」を参照してください。

注意

Check Point のアプライアンスでワンタイムパスワードがリセットされた場合、新しいワンタイムパスワードはその前のワンタイムパスワードとは別のものにする必要があります。

10. (オプション) [接続テスト] をクリックします。
11. Check Point のファイアウォールアプライアンスでセキュリティゲートウェイを事前設定します。詳細については、248 ページの「セキュリティゲートウェイを事前設定する」を参照してください。

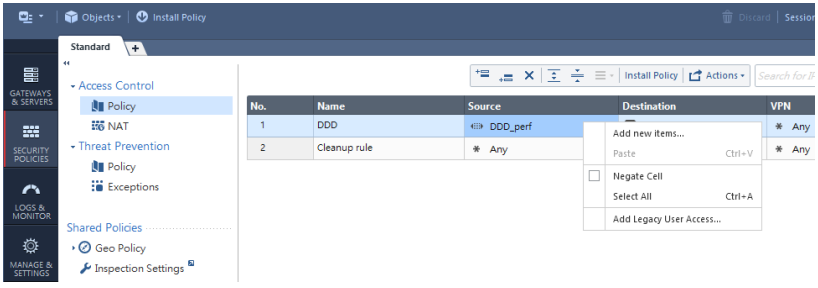
12. Check Point SmartConsole で次の操作を実行し、Deep Discovery Director (統合モード) から不審オブジェクトおよび C&C コールバックアドレスが配信されるように Check Point のアプライアンスを設定します。

    a. 左側のペインで [Security Policies] をクリックします。

    b. [Standard] タブの [Access Control] で、[Policy] をクリックします。

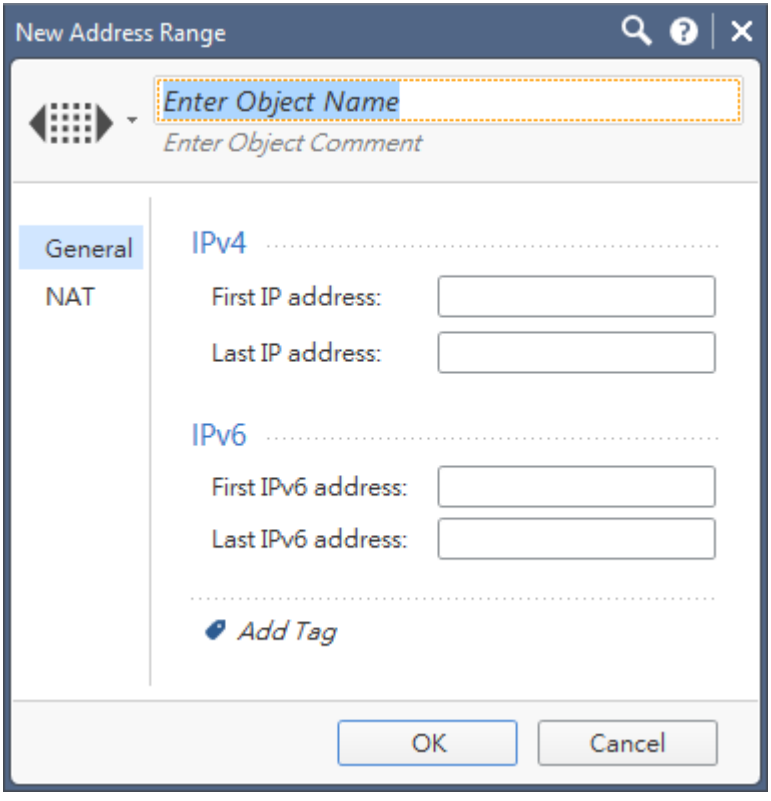
    c. ルールを追加するには、下記の [Add rule above] アイコンをクリックします。

    d. 送信元を右クリックし、[Add new items...] を選択します。

    e. 下記の [New] アイコンをクリックし、[Address Ranges] > [Address Range...] の順に選択します。

[New Address Range] 画面が表示されます。



f. 名前を「DDD」と入力します。

g. [First IP address] に、Deep Discovery Director (統合モード) の IP アドレスを入力します。

h. [Last IP address] に、Deep Discovery Director (統合モード) の IP アドレスを入力します。

i. [OK (成功)] をクリックします。

DDD という名前の項目が作成され、送信元として自動的に選択されます。

j. 送信先を右クリックし、Check Point のアプライアンスを選択します。

k. 処理を右クリックし、[Accept] を選択します。

l. [Install Policy] をクリックします。

Check Point SmartConsole に、ポリシーをインストールする前に変更を公開するよう求めるメッセージが表示されます。

m. [Publish & Install] をクリックします。

[Install Policy] ダイアログが表示されます。

n. [Install] をクリックします。

Check Point のアプライアンスで、Deep Discovery Director (統合モード) からの不審オブジェクトおよび C&C コールバックアドレスの受信が有効になります。

13. Deep Discovery Director (統合モード) の管理コンソールで次の条件を設定して、不審オブジェクトおよび C&C コールバックアドレスの情報を Deep Discovery Director (統合モード) からこのインライン製品/サービスに送信します。

- オブジェクトの種類:
  - C&C コールバックアドレス
    - IPv4 アドレス
  - 不審オブジェクト
    - IPv4 アドレス
- リスクレベル:
  - 高のみ
  - 高および中
  - 高、中、および低

14. [詳細設定] で、次の処理のいずれかをクリックします。

- 拒否: パケットが拒否され、パケットが拒否された通信先に通知が送信されます。
- 破棄: パケットは破棄されますが、通信先には通知が送信されません。
- 通知: 定義された活動について通知が送信されますが、その活動はブロックされません。

15. オブジェクト情報の配信の実行間隔を選択します。
16. [保存] をクリックします。

    [配信] オプションが表示されます。
17. (オプション) [配信] をクリックして、不審オブジェクトおよび C&C コールバックアドレスを Check Point のアプライアンスにただちに配信します。
18. Deep Discovery Director (統合モード) から配信された不審オブジェクトおよび C&C コールバックアドレスを Check Point SmartConsole で表示するには、次の手順を実行します。

    a. 左側のペインで [Logs & Monitor] をクリックします。

    b. 下記のアイコンをクリックして新しいタブを作成します。

    c. 新しいタブで、[Tunnel & User Monitoring] をクリックします。

    [SmartView Monitor] 画面が表示されます。

    d. [SmartView Monitor] 画面で [Launch Menu] アイコンをクリックし、[Tools] > [Suspicious Activity Rules...] の順に選択します。

    [Enforced Suspicious Activity Rules] ダイアログが表示されます。

    e. [Show On] で Check Point のアプライアンスを選択します。

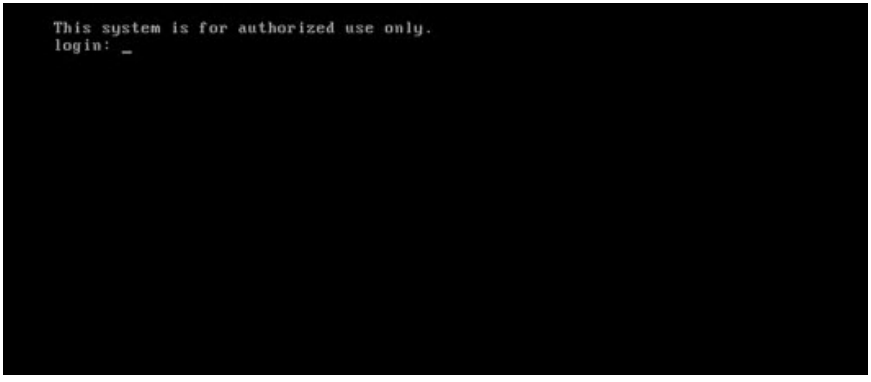
    f. [Refresh] をクリックします。

    Deep Discovery Director (統合モード) から配信された不審オブジェクトおよび C&C コールバックアドレスが表示されます。

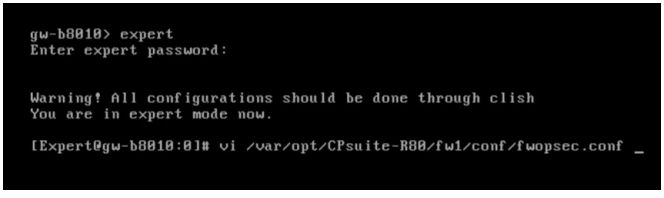
セキュリティゲートウェイを事前設定する

手順

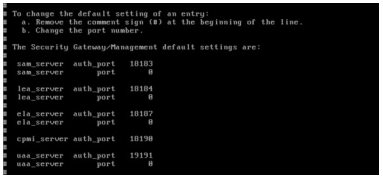
1. Check Point のアプライアンスにログオンします。



2. (オプション) expert モードのパスワードを設定します。
3. パスワードを入力して expert モードに入ります。



4. vi エディタを使用して/var/opt/CPsuite-R80/fw1/conf/fwopsec.conf を開きます。



注意

初期設定のイメージは参照のみを目的としています。実際のファイルの内容は異なる場合があります。

5. `fwopsec.conf` で、次のいずれかのオプションを使用して SAM の通信モードポートを設定します。

   - 保護された接続 (初期設定ポート)
     - `fwopsec.conf` の変更は必要ありません。初期設定ポートの 18183 が sam_server auth_port 設定に使用されます。

       注意

       Deep Discovery Director (統合モード) の [脅威インテリジェンス] > [共有設定] > [補助製品/サービス] で、[Check Point Open Platform for Security (OPSEC)] の [ポート] が同じ 18183 に設定されていることを確認してください。

   - 保護された接続 (ユーザ指定ポート)
     - `fwopsec.conf` で、`sam_server auth_port: 18183` のコメント記号 (#) を削除してポート番号を変更します。

       注意

       `fwopsec.conf` と、Deep Discovery Director (統合モード) の [脅威インテリジェンス] > [共有設定] > [補助製品/サービス] にある [Check Point Open Platform for Security (OPSEC)] の [ポート] に同じポート番号を指定します。

   - 通常の接続 (ユーザ指定ポート)
     - `fwopsec.conf` で、`sam_server port: 0` のコメント記号 (#) を削除してポート番号を変更します。

       注意

       `fwopsec.conf` と、Deep Discovery Director (統合モード) の [脅威インテリジェンス] > [共有設定] > [補助製品/サービス] にある [Check Point Open Platform for Security (OPSEC)] の [ポート] に同じポート番号を指定します。

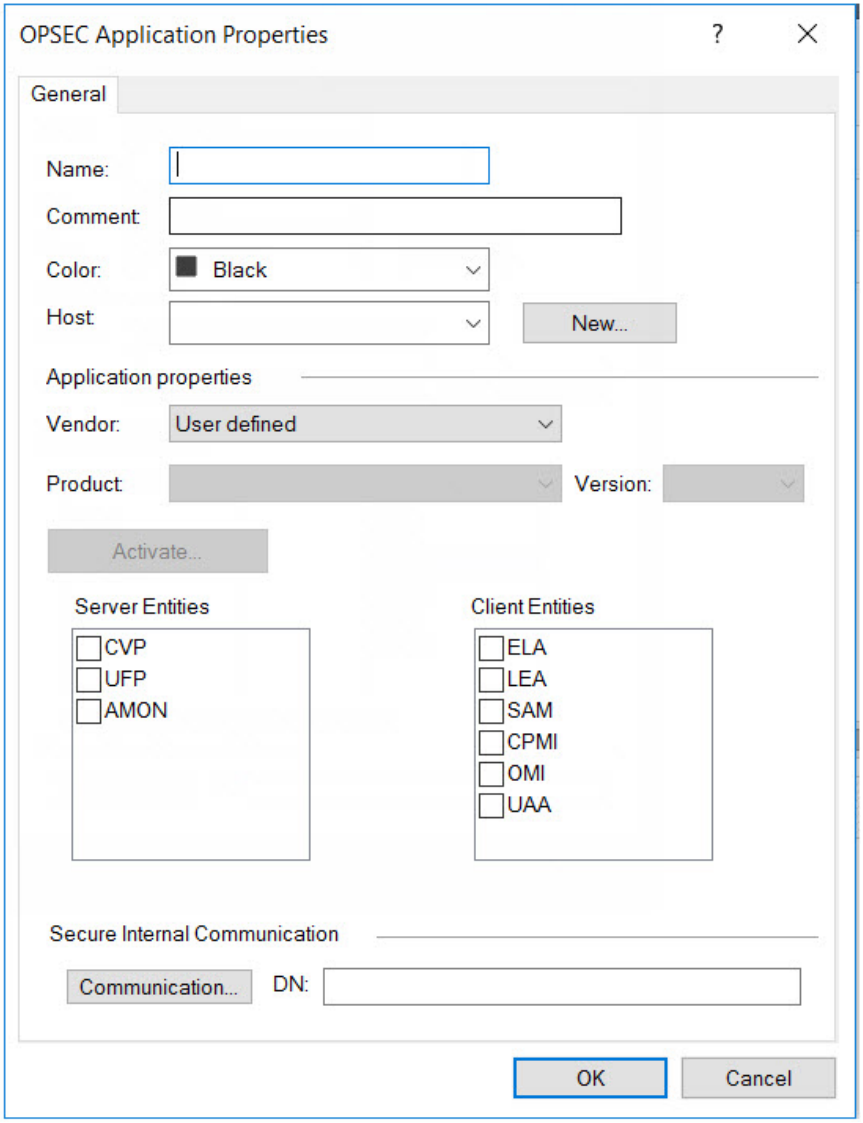
6. `fwopsec.conf` ファイルに変更を行った場合は、`fwopsec.conf` ファイルを保存して Check Point アプライアンスを再起動します。

保護された接続を設定する

手順

1. Check Point SmartConsole を開き、メインメニューアイコン ( ) をクリックします。
2. [New object] > [More object types] > [Server] > [OPSEC Application] > [New Application...] の順に選択します。

[OPSEC Application Properties] 画面が表示されます。



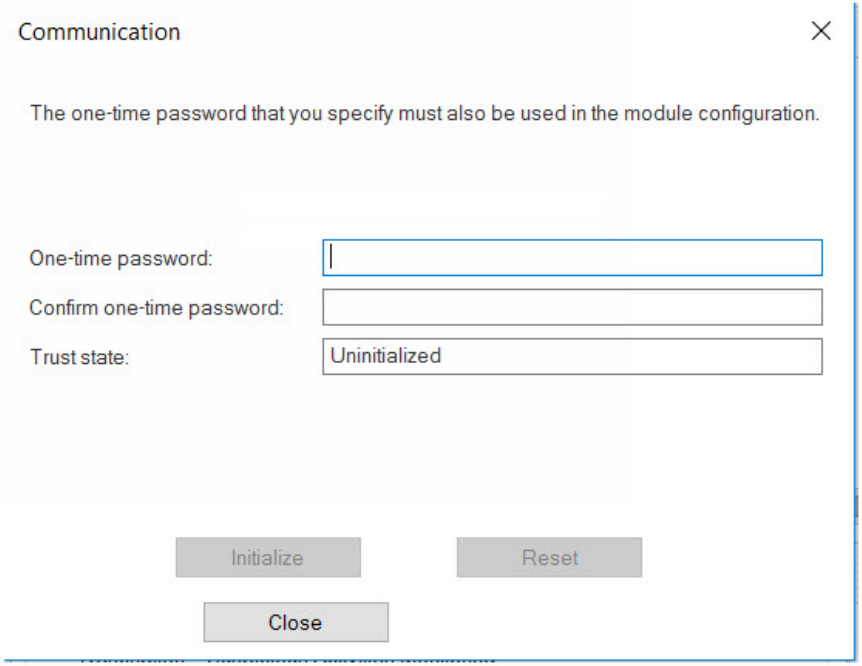
3. [Name] に名前を入力します。

注意

- Deep Discovery Director (統合モード) では、この名前を [OPSEC application name] に使用します。
- アプリケーション名は 100 文字以下で入力してください。英文字で始まり、英文字、ピリオド、アンダースコア、またはダッシュのみが使用されている必要があります。

4. [Host] でホストを選択します。
5. [Client Entities] で [SAM] を選択します。
6. [Communication...] をクリックします。

   [Communication] 画面が表示されます。



7. [One-time password] にパスワードを入力し、同じパスワードを [Confirm one-time password] に入力します。

   注意

   Deep Discovery Director (統合モード) では、このパスワードを [SIC one-time password] に使用します。

   注意

   Check Point のアプライアンスでワンタイムパスワードがリセットされた場合、新しいワンタイムパスワードには、以前とは異なるものを使用する必要があります

8. [Initialize] をクリックします。

   [Trust state] が [Initialized but trust not established] になります。

9. ユーザ定義をインストールします。

   a. メイン画面の [Check Point SmartConsole] で、 をクリックし、[Install database...] を選択します。

      [Install database] 画面が表示されます。

   b. インストールするコンポーネントを選択し、[OK] をクリックします。

      ユーザ定義のインストールが開始されます。

IBM Security Network Protection (XGS)

IBM Security Network Protection (XGS) の提供する Web サービス API を使用すると、Deep Discovery Director (統合モード) などのサードパーティ製アプリケーションから不審オブジェクトおよび C&C コールバックアドレスを直接送信できます。IBM XGS では次の機能を実行できます。

- 不正プログラムに感染したホストの隔離
- C&C サーバへの通信のブロック

- 不正プログラムの配信が検出された URL へのアクセスのブロック

Deep Discovery Director (統合モード) を IBM XGS と統合するには、次のことを実行するように汎用エージェントを設定します。

- 特定のスキーマに従ったアラートの許可
- 一般的な ATP 変換ポリシーに基づく隔離ルールの作成

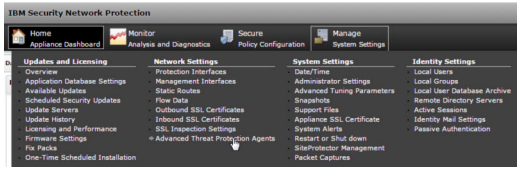
ATP 変換ポリシーにより、IBM XGS に対してメッセージの複数のカテゴリを使用してブロックやアラートなどの異なる処理を実行できます。

IBM Security Network Protection (XGS) を設定する

手順

1. IBM XGS のコンソールで次の手順を実行して、汎用エージェントを設定します。

   a. [Manage System Settings] > [Network Settings] > [Advanced Threat Protection Agents] の順に選択します。

   [Advanced Threat Protection Agents] 画面が開きます。

   b. [New] をクリックします。

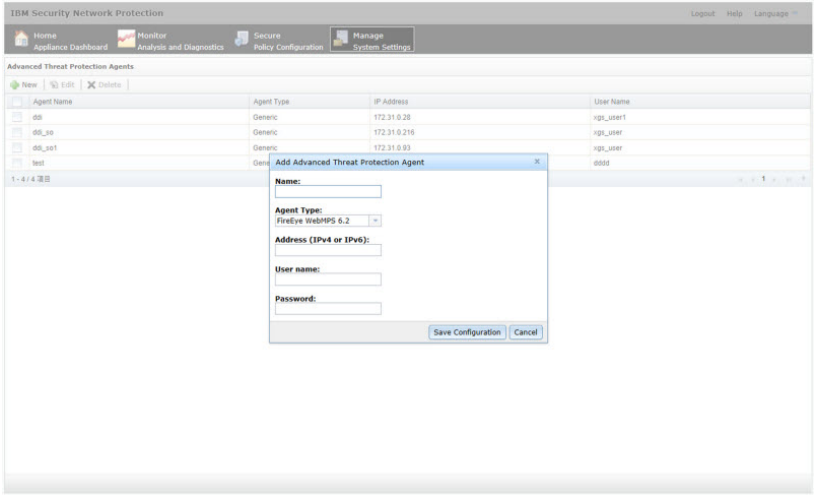
   c. 次の情報を入力します。

      - Name: 名前を入力
      - Agent Type: [Generic] を選択
      - Address: Deep Discovery Director (統合モード) 管理ポートの IPv4 または IPv6 形式の IP アドレス

- User name: 既存の認証情報
- Password: 既存の認証情報

表 5-7. 有効な文字セット

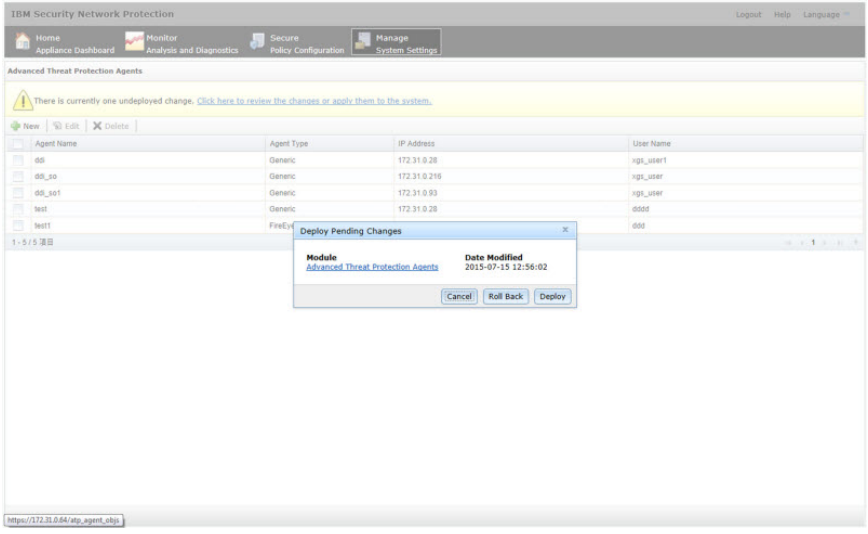
	ユーザ名	パスワード
最小文字数	1 文字	1 文字
最大文字数	15 文字	15 文字



2. [Save Confirmation] をクリックします。

   [Deploy Pending Changes] 画面が開きます。

3. IBM XGS に変更を適用するには、[Deploy] をクリックします。



新しいエージェントが [Advanced Threat Protection Agents] リストに表示されます。

4. Deep Discovery Director (統合モード) の管理コンソールで、[脅威インテリジェンス] > [共有設定] > [補助製品/サービス] の順に選択します。

   [補助製品/サービス] 画面が表示されます。

5. [補助製品/サービスにオブジェクトを配信する] を選択します。

6. [IBM Security Network Protection (XGS)] を選択します。

7. [有効にする場合必ずお読みください] をクリックします。

   [有効にする場合必ずお読みください] ダイアログが表示されます。

8. [有効にする場合必ずお読みください] を読み、同意できる場合は同意します。

重要

この補助製品/サービスとの連携を有効にするには、[有効にする場合必ずお読みください] に同意する必要があります。

9. サーバのアドレスを入力します。

注意

サーバのアドレスは、補助製品/サービスの IPv4 アドレスまたは完全修飾ドメイン名である必要があります。

10. 認証に使用するユーザ名とパスワードを入力します。
11. (オプション) [接続テスト] をクリックします。
12. Deep Discovery Director (統合モード) からこの補助製品/サービスにオブジェクト情報を送信するには、次の条件を設定します。
    - オブジェクトの種類:
      - C&C コールバックアドレス
        - IPv4 アドレス
        - URL
      - 不審オブジェクト
        - IPv4 アドレス
        - URL
    - リスクレベル:
      - 高のみ
      - 高および中
      - 高、中、および低
13. オブジェクト情報の配信の実行間隔を選択します。
14. [保存] をクリックします。
15. (オプション) IBM XGS のコンソールで [Secure Policy Configuration] > [Security Policies] > [Active Quarantine Rules] の順に選択して、Deep Discovery Director (統合モード) から IBM XGS に送信された不審オブジェクトおよび C&C コールバックアドレスを表示します。

注意

リスクレベルの低い不審オブジェクトは、IBM XGS の [Active Quarantine Rules] には表示されません。Deep Discovery Director (統合モード) から送信された不審オブジェクトをすべて表示するには、[Security Policy Configuration] > [Advanced Threat Policy] の順に選択し、次のように設定します。

- Agent Type: Generic
- Alert Type: Reputation
- Alert Severity: Low

Deep Discovery Director (統合モード) から配信された不審オブジェクトおよび C&C コールバックアドレスが表示されます。

Palo Alto Panorama または Firewalls

Palo Alto Firewalls は、ポート番号、プロトコル、暗号化方式 (SSL や SSH)、または秘匿技術に関係なくアプリケーションを識別して制御します。

Deep Discovery Director (統合モード) は、例外ベースの動作を可能にする一致する条件として、Palo Alto Firewall または Palo Alto Panorama™の URL カテゴリにダウンロード可能な IPv4、ドメイン、および URL の不審オブジェクトを生成します。

ポリシーで URL カテゴリを使用するには、次のように設定します。

- Active Directory 内の複数のグループに属するユーザについて、一般的なセキュリティポリシーに対する例外を特定して許可します。

  例: すべてのユーザには不正プログラムやハッキングサイトへのアクセスを拒否しますが、セキュリティグループに属するユーザには許可します。

- ストリーミングメディアカテゴリへのアクセスを許可しますが、サービスの品質ポリシーを適用して帯域幅の使用量を制御します。
- リスクレベルの高い URL カテゴリでのファイルのダウンロードとアップロードを防止します。

  例: 未知のサイトへのアクセスは許可しますが、未知のサイトからの実行可能ファイルのアップロードとダウンロードは防止して、不正プログラムの伝播を防ぎます。
- 金融およびショッピングカテゴリへの暗号化アクセスを許可し、その他すべての URL カテゴリへのトラフィックを復号して検査する、SSL 復号ポリシーを適用します。

Palo Alto Panorama または Firewall を設定する

手順

1. Deep Discovery Director (統合モード) の管理コンソールで、[脅威インテリジェンス] > [共有設定] > [補助製品/サービス] の順に選択します。

   [補助製品/サービス] 画面が表示されます。
2. [補助製品/サービスにオブジェクトを配信する] を選択します。
3. [Palo Alto Panorama または Firewall] を選択します。
4. [有効にする場合必ずお読みください] をクリックします。

   [有効にする場合必ずお読みください] ダイアログが表示されます。
5. [有効にする場合必ずお読みください] を読み、同意できる場合は同意します。

   重要

   この補助製品/サービスとの連携を有効にするには、[有効にする場合必ずお読みください] に同意する必要があります。
6. (オプション) 初期設定で、脅威インテリジェンスのデータは HTTPS 経由で共有されます。HTTP を使用して共有することもできます。[サーバ設

定] で [HTTP を使用して情報を共有する] を選択して、ポート番号を指定します。

7. [条件] で、脅威インテリジェンスのデータファイルに含めるオブジェクトのリスクレベルを選択します。
8. オブジェクト情報の配信の実行間隔を選択します。
9. [保存] をクリックします。
10. (オプション) [生成] をクリックします。

注意

ファイルが生成されたら、URL をクリックし、脅威インテリジェンスのデータファイルをダウンロードして内容を確認できます。

11. Palo Alto Firewall または Palo Alto Panorama™を設定して、Deep Discovery Director (統合モード) から脅威インテリジェンスのデータを取得します。詳細については、統合製品/サービスのドキュメントを参照してください。

第 6 章

アプライアンス

アプライアンスの管理、計画に関連するタスクの実行、リポジトリの管理、ファイルパスワードの管理、ネットワーク資産の設定、Email Encryption の設定、アプライアンスのログの表示、およびエンドユーザ隔離の設定の方法については、次の項目を参照してください。

ディレクトリ

[ディレクトリ] には、Deep Discovery Director (統合モード) に登録された Deep Discovery アプライアンスについての情報が表示されます。

- 左側のペイン: アプライアンスツリーにグループ (フォルダごとに表示) およびアプライアンス (表示名で識別、最初はホスト名と同一) が表示されます。

  注意

  アプライアンスのアイコンに表示される感嘆符のアイコンは、このアプライアンスとの接続が切断されていることを示します。

- 右側のペイン: 配信計画、アプライアンス、アップデートファイル、仮想アナライザイメージなどの情報が表示されます。

新規インストールの場合、[ディレクトリ] は空白で、次の初期設定のグループのみが表示されます。

- 管理対象: このグループに属するアプライアンスは、計画情報、アップデート、および仮想アナライザイメージを Deep Discovery Director から受信できます。アプライアンスは、互換性のある他のアプライアンスとの間で設定を複製することもできます。
- 非管理対象: このグループに属するアプライアンスは、配信計画の情報、アップデート、または仮想アナライザイメージを受信したり、その設定を複製したりすることはできません。

アプライアンスは、各管理コンソールで Deep Discovery Director (統合モード) に登録できます。新しく登録したアプライアンスは、まず非管理対象グループに表示されますが、いつでも管理対象グループに移動できます。

ディレクトリのタスク

[ディレクトリ] は主に、グループやアプライアンス、およびそれらのオブジェクトに関連付けられた計画についての情報の表示に使われます。左側のペインでオブジェクトを選択すると、右側のペインに情報が表示されます。

次の表は、オブジェクトの種類と、各オブジェクトについて表示される情報を示しています。

表 6-1. ディレクトリのオブジェクトの種類

オブジェクト	表示される情報
アプライアンス	• 計画: アプライアンスに配信された、または配信される計画 • アプライアンス: IP アドレス、仮想 IP アドレス、ホスト名、表示名などの識別子、脅威インテリジェンスの同期時刻、ファイルパスワードの同期時刻、およびその他の情報 **注意** Deep Discovery Analyzer のクラスタについて、Deep Discovery Director (統合モード) では次の項目も表示されます。 • アクティ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についての情報 (高可用性クラスタおよび負荷分散クラスタ) • パッシブなプライマリアプライアンス: パッシブなプライマリアプライアンスについての情報 (高可用性クラスタ) • セカンダリアプライアンス: セカンダリアプライアンスについての情報 (負荷分散クラスタ) Deep Discovery Director - Network Analytics サーバについて、Deep Discovery Director (統合モード) ではライセンスステータスと接続済みのデータソースも表示されます。 • アップデート: インストール済みのすべてのアップデートのビルド番号とインストール時刻、さらにアプライアンスの設定の複製元と複製日時についての情報 • 仮想アナライザ: アプライアンスの仮想アナライザ設定についての情報 (種類、内部仮想アナライザの最大イメージおよびインスタンス、配信済みのイメージおよびインスタンスなど) **注意** Deep Discovery Analyzer のアクティブなプライマリアプライアンスについては、[すべてのノード] をクリックすると、クラスタ内のすべてのノードで使用中のインスタンスの合計数が表示されます。

オブジェクト	表示される情報
グループ	グループに関連するアプライアンスや計画の概要 (ステータスや接続情報など)

ディレクトリのその他のタスク

次の操作を実行することもできます。

表 6-2. ディレクトリのその他のタスク

操作	説明
グループの追加	アプライアンスを場所別または部門別などで整理しやすくするために、グループを追加します。 グループを追加するには 1. グループ名の横にあるメニューアイコンをクリックし、[追加] を選択します。 2. テキストボックスに、最大 256 文字で名前を入力します。
グループまたはアプライアンスの名前の編集	グループまたはアプライアンスの名前を編集するには 1. グループ名またはアプライアンス名の横にあるメニューアイコンをクリックし、[編集] を選択します。 2. テキストボックスに、最大 256 文字で名前を入力します。
脅威インテリジェンスの同期	アプライアンスが Deep Discovery Director (統合モード) から脅威インテリジェンスを同期するように設定します。 脅威インテリジェンスを同期するには、アプライアンス名の横にあるメニューアイコンをクリックし、[脅威インテリジェンスの同期] を選択します。 **注意** アプライアンスは Deep Discovery Director (統合モード) から脅威インテリジェンスを自動的に同期します。脅威インテリジェンスの同期には時間がかかります。可能であれば、この操作は実行しないでください。

操作	説明
ファイルパスワードの同期	アプライアンスが Deep Discovery Director (統合モード) からファイルパスワードを同期するように設定します。 ファイルパスワードを同期するには、アプライアンス名の横にあるメニューアイコンをクリックし、[ファイルパスワードの同期] を選択します。 **注意** Deep Discovery Director (統合モード) からファイルパスワードを自動的に同期するよう、登録済みアプライアンスを設定できます。
ネットワーク資産設定の同期	アプライアンスが Deep Discovery Director (統合モード) からネットワーク資産設定を同期するように設定します。 ネットワーク資産設定を同期するには、アプライアンス名の横にあるメニューアイコンをクリックし、[ネットワーク資産設定の同期] を選択します。 **注意** Deep Discovery Director (統合モード) からネットワーク資産設定を自動的に同期するよう、登録済みアプライアンスを設定できます。
グループまたはアプライアンスの移動	グループまたはアプライアンスを別のグループに移動するには 1. グループ名またはアプライアンス名の横にあるメニューアイコンをクリックし、[移動] を選択します。 2. 画面で新しいフォルダを選択し、[移動] をクリックします。 次の場合、この機能は無効になります。 • 関連する 1 つ以上の計画の配信が保留中または実行中の場合。 • アプライアンスツリーが特定の Deep Discovery アプライアンスでフィルタされている場合。この機能を有効にするには、表示を [すべて] に変更します。

操作	説明
グループの削除	空のグループや使用されていないグループを削除して、[ディレクトリ] を簡素化します。 グループを削除するには、グループ名の横にあるメニューアイコンをクリックし、[削除] を選択します。 警告! グループを削除すると、そのグループに関連する計画がキャンセルされ、アプライアンスが [非管理対象] グループに移動します。削除できるのは、未完了の計画のないグループのみです。 次の場合、この機能は無効になります。 • 関連する 1 つ以上の計画の配信が保留中または実行中の場合。 • アプライアンスツリーが特定の Deep Discovery アプライアンスでフィルタされている場合。この機能を有効にするには、表示を [すべて] に変更します。

操作	説明
アプライアンスの削除	アプライアンスを削除するには、表示名の横にあるメニューアイコンをクリックし、[削除] を選択します。 アプライアンスツリーが特定の Deep Discovery アプライアンスでフィルタされている場合、この機能は無効になります。この機能を有効にするには、表示を [すべて] に変更します。 警告! • アプライアンスを削除すると、Deep Discovery Director (統合モード) から登録解除され、すべての接続が停止し、関連する計画はすべてキャンセルされます。 • Deep Discovery Inspector アプライアンスを削除すると、Deep Discovery Director - Network Analytics から自動的に登録解除され、その Deep Discovery Inspector アプライアンスが提供するデータから得られた相関イベントは利用できなくなります。 Deep Discovery Inspector アプライアンスを Deep Discovery Director に再登録しても、Deep Discovery Director - Network Analytics には自動的に再登録されません。すべての機能を復元するには、Deep Discovery Inspector アプライアンスの管理コンソールに移動して、元々登録されていた Deep Discovery Director - Network Analytics サーバに Deep Discovery Inspector アプライアンスを再登録します。
表示の切り替え	カスタムビューを切り替えるには、[ビュー] の横にある名前をクリックして、切り替え後に表示するビューを選択します。

操作	説明
列のカスタマイズ	列をカスタマイズして新しいカスタムビューを保存し、すべての情報を見やすく整理します。 カスタムビューを作成するには 1. [ビュー] の横にある名前をクリックし、[列のカスタマイズ] を選択します。 2. 一意のカスタムビュー名を入力します。 3. カスタムビューに含める列の組み合わせを選択します。 4. [適用] をクリックします。 ヒント 列の順序はドラッグアンドドロップ操作で並び替えることができます。
カスタムビューの編集	カスタムビューを編集するには 1. [ビュー] の横にある名前をクリックし、ビューの横にある (鉛筆) アイコンを選択します。 2. (オプション) カスタムビューの名前を編集します。 3. 列の組み合わせを編集します。 4. [適用] をクリックします。
カスタムビューの削除	カスタムビューを削除するには、[ビュー] の横にある名前をクリックし、ビューの横にある (ゴミ箱) アイコンを選択します。

計画

配信の範囲とスケジュールを指定して、対象アプライアンスへの配信計画を設定できます。

各計画は、対象アプライアンスの特定のセットに対して作成され、ユーザが指定した期間に 1 回だけ配信されます。配信する計画は、対象アプライアンスの製品および言語に一致する必要があります。

計画が配信されると、必要なファイルをいつダウンロードするか、計画をいつ実行するかについて、Deep Discovery Director (統合モード) から対象アプライアンスに指示が送信されます。計画がただちに配信されない場合、アプライアンスはスケジュールの次の要素に従って、ファイルをダウンロードし、計画を実行します。

- 配信開始
- ダウンロード期間
- 実行開始

重要

すべての時刻はアプライアンスのローカル時間に基づきます。

[計画] 画面には、作成されたすべての計画と次の情報が一覧表示されます。

表 6-3. 計画

項目	説明
名前	計画の作成時に指定します。
種類	対象に配信する計画の種類。Deep Discovery Director (統合モード) では現在、次の種類の計画がサポートされています。 • HotFix/Critical Patch/ファームウェア • 仮想アナライザのイメージ • 設定の複製

項目	説明
ステータス	計画のステータスは次のいずれかになります。 • 進行中: 指定された時刻に配信が開始され、1 つ以上のアプライアンスが計画を実行しました。 • 保留中: 配信が開始されていないか、Deep Discovery Director (統合モード) から計画情報を受信したアプライアンスがありません。 • 完了: 指定された時刻に配信が開始され、すべてのアプライアンスが正常に計画を実行しました。 • 失敗: 指定された時刻に配信が開始されなかったか、1 つ以上のアプライアンスが計画を実行できませんでした。
スケジュール	計画の配信と実行がスケジュールされている日時。次のいずれかが表示されます。 • カスタム: 計画の配信、必要なファイルのダウンロード、および計画の実行は、スケジュールに従って実行されます。すべての時刻はアプライアンスのローカル時間に基づきます。 • 即時: 計画がただちに配信され、アプライアンスは必要なファイルをダウンロードした後すぐに計画を実行します。すべての時刻はサーバのローカル時間に基づきます。
配信開始	配信開始の日付と時刻。
説明	計画の作成時に指定します。
作成者	計画を作成したユーザアカウント。

ヒント

リストの表示は、(フィルタ) ボタンをクリックし、表示されるドロップダウンリストや検索ボックスを使用してフィルタできます。

計画のタスク

計画名をクリックすると、その計画の詳細画面が表示されます。

表 6-4. 計画のタスク

タスク	説明
計画情報	計画の配信のステータスと予約、ファイルの詳細、およびその他の関連情報
アプライアンス情報	ホスト名、アプライアンスのステータス、配信開始日時と完了日時、およびアプライアンスの Directory 上のパス 詳細については、272 ページの「アプライアンスのステータス」を参照してください。

アプライアンスのステータス

Deep Discovery Director (統合モード) では、次のいずれかのアプライアンスのステータスが表示されます。

表 6-5. アプライアンスのステータス

ステータス	説明
保留中	アプライアンスは Deep Discovery Director (統合モード) から計画情報を受信していません。
進行中	次のいずれかの状況が考えられます。 • アプライアンスは計画情報の受信を確認し、ファイルのダウンロードを開始しています。 • アプライアンスは計画情報の受信を確認し、計画の実行を開始しています。 • アプライアンスは計画の実行に必要なファイルをダウンロードしています。 • アプライアンスはファイルをダウンロードし、計画を実行しています。
一時停止	アプライアンスはファイルのダウンロードを一時停止しており、指定されたダウンロード期間に再開します。
完了	アプライアンスは計画を正常に実行しました。

ステータス	説明
失敗	次のいずれかの状況が考えられます。 • アプライアンスは計画を実行できませんでした。 • アプライアンスは計画情報に一致しないタスクを実行しています。
到達不能	次のいずれかの状況が考えられます。 • アプライアンスは Deep Discovery Director (統合モード) から登録解除されています。 • アプライアンスは Deep Discovery Director (統合モード) から削除されています。
キャンセル済み	次のいずれかの状況が考えられます。 • アプライアンスが Deep Discovery Director (統合モード) から計画情報を受信する前に、計画が手動でキャンセルされました。 • アプライアンスでファイルのダウンロード中、または計画の実行中に、計画が手動でキャンセルされました。 • アプライアンスがファイルのダウンロードを一時停止している間に、計画が手動でキャンセルされました。

計画のその他のタスク

次のタスクを実行することもできます。

表 6-6. その他のタスク

タスク	説明
追加	次のいずれかの種類の計画を Deep Discovery Director (統合モード) に追加します。 • HotFix/Critical Patch/ファームウェア 詳細については、275 ページの「HotFix/Critical Patch/ファームウェアの配信計画を追加する」を参照してください。 • 仮想アナライザのイメージ 詳細については、276 ページの「仮想アナライザイメージの配信計画を追加する」を参照してください。 • 設定の複製 詳細については、279 ページの「設定の複製計画を追加する」を参照してください。 重要 Deep Discovery Director (統合モード) では、ライセンスのステータスが [アクティベート未完了] または [有効期限切れ] の場合、新しい計画を作成できません。既存の計画は、通常どおりに配信および実行されます。
編集	ステータスが [保留中] の計画名をクリックし、[編集] をクリックします。 注意 未配信の計画のみを編集できます。
計画のキャンセル	ステータスが次のいずれかの計画名をクリックし、[計画のキャンセル] をクリックします。 • 保留中 • 進行中 • 一時停止
コピー	リストで計画を選択し、[コピー] をクリックします。

タスク	説明
計画の作成	ステータスが [失敗] の計画をクリックし、[計画の作成] をクリックします。配信に失敗した計画の設定に基づいて新しい計画が作成されます。
削除	ステータスが [保留中] の計画をリストで選択し、[削除] をクリックします。

HotFix/Critical Patch/ファームウェアの配信計画を追加する

互換性のあるアプライアンスに製品のアップデートやアップグレードを配信するには、この種類の計画を使用します。

手順

1. [アプライアンス] > [計画] の順に選択し、[追加] をクリックします。

   [計画の追加] 画面が表示されます。

2. 最大 256 文字で計画の名前を入力します。
3. 種類に [HotFix/Critical Patch/ファームウェア] を選択します。
4. (オプション) 説明を入力します。
5. [HotFix/Critical Patch/ファームウェア] のリストからファイルを選択します。

   注意

   Deep Discovery Director (統合モード) では、リポジトリで使用可能なファイルのリストが表示されます。ファイルが製品および対象アプライアンスの言語と一致することを確認します。

6. 対象アプライアンスを選択します。Deep Discovery Director (統合モード) では、互換性のあるアプライアンスのみが表示されます。

   注意

   アップデートをインストールすると、対象アプライアンスが自動的に再起動します。

7. スケジュールを指定します。
   - カスタム: 指定したとおりに計画の配信、ファイルのダウンロード、および計画の実行を行います。
     - 配信開始: 計画を配信する日付です。

       注意

       計画は常に選択した日付の午前 0 時 (00:00) に配信されます。

     - ダウンロード期間: 計画の実行に必要なファイルをアプライアンスがダウンロードできる期間です。

       注意

       - ダウンロード期間が午後 8 時から午前 4 時に設定されている場合、アプライアンスはファイルのダウンロードを、翌日の午後 8 時ではなく、計画が配信された直後の午前 0 時頃に開始します。
       - ダウンロード期間を午後 8 時から午後 11 時 59 分に (またはもう少し時間に余裕を持たせて) 設定すると、アプライアンスが計画配信直後の午前 0 時頃にファイルをダウンロードするのを防ぐことができます。

     - 実行開始: 計画を実行する日時です。

       ヒント

       [スケジュールの予約] を選択すると、予期しないタイミングで計画が実行されるのを防ぐことができます。

   - 即時: 計画の保存直後に開始します。
8. [保存] をクリックします。

仮想アナライザイメージの配信計画を追加する

互換性のあるアプライアンスに仮想アナライザイメージを配信するには、この種類の計画を使用します。

次の表は、互換性のあるアプライアンスの要件を示しています。

表 6-7. 互換性のあるアプライアンスの要件

要件	説明
ライセンス	• ステータス: アクティベート済み • 種類: 製品版
仮想アナライザ	• ステータス: 有効 **注意** 仮想アナライザイメージは、仮想アナライザのステータスが無効の Deep Discovery Inspector アプライアンスに配信できます。Deep Discovery Inspector では、仮想アナライザイメージの配信後、仮想アナライザを自動的に有効にします。 • 種類: 内部
Deep Discovery Director (統合モード)	• Deep Discovery Director (統合モード) 1.1 以降と統合済み • Deep Discovery Director (統合モード) へ登録済み • 管理対象グループ内に存在

手順

1. [アプライアンス] > [計画] の順に選択し、[追加] をクリックします。

   [計画の追加] 画面が表示されます。

2. 最大 256 文字で計画の名前を入力します。
3. 種類に [仮想アナライザのイメージ] を選択します。
4. (オプション) 説明を入力します。
5. [仮想アナライザのイメージ] のリストから製品を選択します。
6. イメージの最大値を選択します。
7. リストから OS の種類の組み合わせを選択します。

8. インスタンスの最大値を選択します。
9. [選択] をクリックします。

   [仮想アナライザイメージ] ダイアログが表示されます。

   注意

   Deep Discovery Director (統合モード) では、リポジトリで使用可能な仮想アナライザイメージのリストが表示されます。

10. 配信する仮想アナライザイメージの設定を選択し、[保存] をクリックします。

    重要

    - 対象アプライアンスに現在配信されている設定は、ここで選択した設定に置き換えられます。
    - 対象アプライアンスに現在配信されているイメージを保持するには、そのイメージを仮想アナライザイメージの最終的な設定のひとつとして選択します。対象アプライアンスでは、選択されたイメージが同一のものであるかどうか、配信が必要であるかどうかを自動的に判別します。

11. (オプション) イメージに割り当てられたインスタンス数を変更します。
12. 対象アプライアンスを選択します。Deep Discovery Director (統合モード) では、互換性のあるアプライアンスのみが表示されます。

    注意

    Deep Discovery Analyzer のセカンダリアプライアンスは表示されません。これは、仮想アナライザのイメージと設定がプライマリアプライアンスから自動的に同期されるためです。仮想アナライザイメージを Deep Discovery Analyzer のセカンダリアプライアンスに配信するには、対応するプライマリアプライアンスを選択します。

13. スケジュールを指定します。
    - カスタム: 指定したとおりに計画の配信、ファイルのダウンロード、および計画の実行を行います。

- 配信開始: 計画を配信する日付です。

  注意

  計画は常に選択した日付の午前 0 時 (00:00) に配信されます。

- ダウンロード期間: 計画の実行に必要なファイルをアプライアンスがダウンロードできる期間です。

  注意

  - ダウンロード期間が午後 8 時から午前 4 時に設定されている場合、アプライアンスはファイルのダウンロードを、翌日の午後 8 時ではなく、計画が配信された直後の午前 0 時頃に開始します。
  - ダウンロード期間を午後 8 時から午後 11 時 59 分に (またはもう少し時間に余裕を持たせて) 設定すると、アプライアンスが計画配信直後の午前 0 時頃にファイルをダウンロードするのを防ぐことができます。

- 実行開始: 計画を実行する日時です。

  ヒント

  [スケジュールの予約] を選択すると、予期しないタイミングで計画が実行されるのを防ぐことができます。

- 即時: 計画の保存直後に開始します。

14. [保存] をクリックします。

設定の複製計画を追加する

1 つのアプライアンスの設定を互換性のある複数のアプライアンスに複製するには、この種類の計画を使用します。

各 Deep Discovery 製品では、さまざまな組み合わせの設定の複製がサポートされます。詳細については、449 ページの Deep Discovery Director で複製される設定を参照してください。

手順

1. [アプライアンス] > [計画] の順に選択し、[追加] をクリックします。

   [計画の追加] 画面が表示されます。

2. 最大 256 文字で計画の名前を入力します。
3. 種類に [設定の複製] を選択します。
4. (オプション) 説明を入力します。
5. [複製元] のリストから複製元を選択します。

   ヒント

   [表示] ドロップダウンリストから製品を選択し、選択した製品のアプライアンスのみが表示されるようにします。

6. 対象アプライアンスを選択します。Deep Discovery Director (統合モード) では、互換性のあるアプライアンスのみが表示されます。
7. スケジュールを指定します。
   - カスタム: 指定したとおりに計画の配信、ファイルのダウンロード、および計画の実行を行います。
     - 配信開始: 計画を配信する日付です。

       注意

       計画は常に選択した日付の午前 0 時 (00:00) に配信されます。

     - ダウンロード期間: 計画の実行に必要なファイルをアプライアンスがダウンロードできる期間です。

注意

- ダウンロード期間が午後 8 時から午前 4 時に設定されている場合、アプライアンスはファイルのダウンロードを、翌日の午後 8 時ではなく、計画が配信された直後の午前 0 時頃に開始します。
- ダウンロード期間を午後 8 時から午後 11 時 59 分に (またはもう少し時間に余裕を持たせて) 設定すると、アプライアンスが計画配信直後の午前 0 時頃にファイルをダウンロードするのを防ぐことができます。

- 実行開始: 計画を実行する日時です。

ヒント

[スケジュールの予約] を選択すると、予期しないタイミングで計画が実行されるのを防ぐことができます。

- 即時: 計画の保存直後に開始します。

8. [保存] をクリックします。

リポジトリ

[リポジトリ] 画面には、すべてのアップデート、アップグレードパッケージおよびサーバでホストされる仮想アナライザイメージファイルが表示されます。ファイルはここでアップロードおよび削除します。

HotFix/Critical Patch/ファームウェア

[アプライアンス] > [リポジトリ] > [HotFix/Critical Patch/ファームウェア] にある [HotFix/Critical Patch/ファームウェア] 画面を使用して、アップロード済みのアップデートファイルの表示、未使用のアップデートファイルの削除、および配信する新しいアップデートファイルのアップロードを実行します。

フィルタを使用すると、アップデートまたはアップグレードファイルの種類、製品、言語、ファイルの名前またはバージョンで対象ファイルを検索できます。

ファイルを削除するには、リストからファイルを選択して [削除] をクリックします。

HotFix/Critical Patch/ファームウェアのファイルをアップロードする

Deep Discovery Director (統合モード) では、1 回のファイルアップロードセッションで最大 5 つのファイルを同時にアップロードできます。

重要

管理コンソールのブラウザまたはタブを閉じると、実行中のすべてのアップロードがキャンセルされます。

手順

1. [アプライアンス] > [リポジトリ] > [HotFix/Critical Patch/ファームウェア] の順に選択します。
2. [アップロード] をクリックします。
3. [選択] をクリックして、有効な TAR ファイルを選択します。
4. (オプション) 検証のため、選択したファイルの 64 文字の SHA-256 ハッシュ値を入力するか貼り付けます。
5. (オプション) 説明を入力します。
6. [アップロード] をクリックします。

仮想アナライザイメージ

[アプライアンス] > [リポジトリ] > [仮想アナライザイメージ] にある [仮想アナライザイメージ] 画面を使用して、アップロード済みのイメージファイルの

表示、未使用のイメージファイルの削除、および配信する新しいイメージファイルのアップロードを実行します。

ファイルを削除するには、リストからファイルを選択して [削除] をクリックします。

重要

Deep Discovery Director (統合モード) でアップロードおよび配信できるのは、Virtual Analyzer Image Preparation Tool を使用して TAR 形式で圧縮した仮想アナライザイメージのみです。

詳細については、https://appweb.trendmicro.com/ecs/default.aspx を参照してください。

仮想アナライザのイメージをアップロードする

Deep Discovery Director (統合モード) では、SFTP またはネットワークフォルダを使用して、最大 3 つの仮想アナライザイメージファイルを連続してアップロードできます。アップロードセッション用の SFTP またはネットワークサーバへの接続はバックグラウンドで開かれるため、アップロードの完了を待つ間、ユーザは画面を移動して別のタスクを実行することができます。

手順

1. [アプライアンス] > [リポジトリ] > [仮想アナライザイメージ] 順に選択します。
2. [アップロード] をクリックします。
3. リストからアップロード元を選択します。
   - SFTP
   - ネットワークフォルダ
4. サーバの詳細を入力します。
   - SFTP: サーバの IP アドレスまたは完全修飾ドメイン名、ポート番号、ユーザ名、およびパスワードを入力します。

- ネットワークフォルダ: ユーザ名とパスワードを入力します。

注意

Deep Discovery Director (統合モード) では、サーバ情報とログオンアカウント情報が自動的に保存されます。

5. 1 つ以上の仮想アナライザイメージファイルの詳細を入力します。
   a. ファイルパスを入力します。
   b. 一意のイメージ名を入力します。
   c. (オプション) 説明を入力します。
6. [アップロード] をクリックします。

アップロードセンター

アップロードセンターのパネルを使用して、アップロード中およびアップロード済みのファイルに関する情報を表示できます。パネルを切り替えるには、画面の右上隅にある上矢印と引き出しのアイコンをクリックします。パネルは次の 2 つのタブに分かれています。

- 284 ページの「アップロード中のファイル」
- 285 ページの「アップロード履歴」

アップロード中のファイル

このタブには Deep Discovery Director (統合モード) にアップロードしているファイルの情報が表示されます。

ファイルのアップロードをキャンセルするには、アップロードの横にある [x] をクリックします。

ファイルのアップロードは次の段階に従って実行されます。

表 6-8. ファイルのアップロードの段階

段階	説明
1: 計算中	ファイルのアップロードが有効であることを確認するため、ファイルのアップロードの最初の部分が検証されています。
2: リポジトリへのアップロード中	ファイルがリポジトリにアップロードされています。SFTP サーバおよびネットワークフォルダのすべてのファイルのアップロードは、任意のユーザがキャンセルできます。
3: 処理中	ファイルがリポジトリにアップロードされ、完全性が検証されています。この段階でファイルのアップロードをキャンセルすることはできません。

ファイルのアップロードについては次の情報が表示されます。

表 6-9. ファイルのアップロードについての情報

情報	説明
ファイル名	ファイル名です。
(X KB / MB / GB)	ファイルサイズです。KB、MB、GB の単位で表示されます。
残り時間	ファイルサイズとアップロード速度から推定される、ファイルのアップロードが完了するまでの時間です。
(X KB/秒 / MB/秒 / GB/秒)	アップロード速度です。KB/秒、MB/秒、GB/秒の単位で表示されます。

アップロード履歴

このタブには Deep Discovery Director (統合モード) にアップロードされたファイルの情報が表示されます。

アップロードの履歴をクリアするには、[すべてクリア] をクリックします。

アップロード済みのファイルについて、次の情報が表示されます。

表 6-10. アップロード済みのファイルに関する情報

情報	説明
ステータス	次のステータスのいずれかになります。 • 成功: ファイルのアップロードに成功しました。 • 失敗: ファイルのアップロードに失敗しました。 • キャンセル済み: ファイルのアップロードがキャンセルされました。
ファイル名	ファイル名です。

ファイルパスワード

不審ファイルは十分に注意して処理してください。このようなファイルをネットワーク経由で転送する場合は、パスワード保護されたアーカイブファイルやパスワード保護された文書ファイルに追加して開かれないようにすることをお勧めします。

[登録済みアプライアンスに同期] の切り替えスイッチをクリックして、すべての登録済みの Deep Discovery Analyzer および Deep Discovery Email Inspector アプライアンスに対する [ファイルパスワード] 設定の同期を有効または無効にします。

注意

- [ユーザ指定のパスワード] リストは、登録済みの Deep Discovery Analyzer および Deep Discovery Email Inspector アプライアンスに同期されます。
- [ヒューリスティック検出されたパスワード] の設定は、Deep Discovery Email Inspector アプライアンスのみに同期されます。

ユーザ指定のパスワード

[ユーザ指定のパスワード] 画面には、ユーザ指定のパスワードのリストが表示されます。登録済みの Deep Discovery Analyzer および Deep Discovery Email Inspector アプライアンス上の仮想アナライザは、このリストを使用し

てファイルを抽出したりパスワード保護された文書を開いたりします。パフォーマンス向上のため、よく使用されるパスワードを上位に配置します。

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。

パスワードを追加する

手順

1. [アプライアンス] > [ファイルパスワード] > [ユーザ指定のパスワード] の順に選択します。
2. [追加] をクリックします。

   [パスワードの追加] ダイアログが表示されます。
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) 手順 2〜3 を繰り返して、さらにパスワードを追加します。

   注意

   [ユーザ指定のパスワード] リストには、最大 100 個のパスワードを追加できます。
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、行の右側にある [X] ボタンをクリックします。

7. [保存] をクリックします。

パスワードを編集する

手順

1. [アプライアンス] > [ファイルパスワード] > [ユーザ指定のパスワード] の順に選択します。
2. 編集するパスワードをクリックします。

   パスワードが編集可能なテキストボックスに変わります。
3. パスワードを編集します。
4. (オプション) 手順 2～3 を繰り返して、さらにパスワードを編集します。
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、行の右側にある [X] ボタンをクリックします。
7. [保存] をクリックします。

パスワードをインポートする

手順

1. [アプライアンス] > [ファイルパスワード] > [ユーザ指定のパスワード] の順に選択します。
2. [インポート] をクリックします。

   [パスワードのインポート] ダイアログが表示されます。
3. [選択] をクリックして、インポートする TXT ファイルを指定します。

注意

TXT ファイルを初めてインポートする場合は、[サンプルファイルのダウンロード] をクリックしてファイルを保存します。TXT ファイルに項目を正しい書式設定で入力して、ファイルを保存し、[選択] をクリックして TXT ファイルを指定します。

4. [次へ] をクリックします。

   ファイル内のエントリを Deep Discovery Director (統合モード) が確認し、無効または重複するパスワードを検出します。

5. [インポート] をクリックします。

   パスワードが [ユーザ指定のパスワード] リストに追加されます。

6. [保存] をクリックします。

パスワードをエクスポートする

手順

1. [アプライアンス] > [ファイルパスワード] > [ユーザ指定のパスワード] の順に選択します。
2. [エクスポート] をクリックします。

   ファイルのダウンロードが開始されます。

パスワードを削除する

手順

1. [アプライアンス] > [ファイルパスワード] > [ユーザ指定のパスワード] の順に選択します。
2. 行の右側にある [X] ボタンをクリックします。

注意

さらにパスワードを削除するには、この手順を繰り返します。

3. [保存] をクリックします。

ヒューリスティック検出されたパスワード

Deep Discovery Email Inspector アプライアンスでは、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 Director (統合モード) では、ヒューリスティック検出されたパスワードとタイムアウト設定を登録済み Deep Discovery Email Inspector アプライアンスと同期できます。

[ヒューリスティック検出されたパスワード] 画面を使用して、同期とタイムアウトを設定します。

ヒューリスティック検出されたパスワードを同期する

手順

1. [アプライアンス] > [ファイルパスワード] > [ヒューリスティック検出されたパスワード] の順に選択します。
2. [ヒューリスティック検出されたパスワードの同期] を選択します。
3. Password Analyzer とヒューリスティック検出されたパスワードがタイムアウトするまでの時間 (分数) を変更します。
4. [保存] をクリックします。

ネットワーク資産

ネットワーク資産の設定は、Deep Discovery Inspector 製品がネットワークコンテンツ相関エンジン用に監視するネットワークのプロファイルを定義およ

び確立し、Deep Discovery Director - Network Analytics を最大限活用するのに役立ちます。

[登録済み製品に同期] の切り替えスイッチをクリックして、すべてのサポートされる登録済みの Deep Discovery Inspector および Deep Discovery Director - Network Analytics 製品に対する [ネットワーク資産] 設定の同期を有効または無効にします。

注意

- [ドメインの除外]、[優先ウォッチリスト]、[ネットワークグループ]、および [登録済みサービス] のリストは Deep Discovery Director - Network Analytics 製品に同期されます。
- [登録済みドメイン]、[ネットワークグループ]、および [登録済みサービス] のリストは Deep Discovery Inspector 製品に同期されます。
- 同期すると、製品の既存の設定が上書きされます。

ドメインの除外

[ドメインの除外] リストには、安全であると見なすドメインを追加します。リストに追加したドメイン、およびそれらとの相互処理は、[相関イベント] 画面に含まれなくなります。このリストからドメインを削除すると、そのドメインと、過去および今後のイベントにおいて関連する相互処理が含まれるようになります。

次の表は、[ドメインの除外] 画面で使用可能な操作の概要を示しています。

操作	説明
追加	リストに項目を追加します。 詳細については、292 ページの「ドメインの除外を追加する」を参照してください。
インポート	インポートして既存のリストを上書きします。 詳細については、292 ページの「ドメインの除外リストをインポートする」を参照してください。
すべてエクスポート	現在のリストをエクスポートします。

操作	説明
削除	1 つ以上の選択した項目を削除します。

ドメインの除外を追加する

手順

1. [アプライアンス] > [ネットワーク資産] > [ドメインの除外] の順に選択します。

   [ドメインの除外] 画面が表示されます。

2. [追加] をクリックします。

   [ドメインの除外の追加] ダイアログが表示されます。

3. ドメイン名を入力します。

   注意

   ドメインのプレフィックスでは、「.」で連結した 1 文字のワイルドカード (*) がサポートされます。

4. [追加] をクリックします。

   項目が [ドメインの除外] リストに表示されます。

ドメインの除外リストをインポートする

リストをインポートすると、既存のリストが上書きされます。リストをインポートする前に、既存のリストをエクスポートしておくことをお勧めします。

手順

1. [アプライアンス] > [ネットワーク資産] > [ドメインの除外] の順に選択します。

   [ドメインの除外] 画面が表示されます。

2. [インポート] をクリックします。

   [CSV からのドメインの除外のインポート] ダイアログが表示されます。

3. [選択] をクリックして、インポートする CSV ファイルを指定します。

   ヒント

   CSV ファイルを初めてインポートする場合は、[サンプル CSV のダウンロード] をクリックしてファイルを保存します。CSV ファイルに項目を正しい書式設定で入力して (CSV ファイル内の説明を参照)、ファイルを保存し、[選択] をクリックして CSV ファイルを指定します。

4. [インポート] をクリックします。

   項目が [ドメインの除外] リストに表示されます。

優先ウォッチリスト

自身の環境内でイベント追跡とインシデントレポートにおいて優先度が高いと見なすサーバを追加します。

次の表は、[優先ウォッチリスト] 画面で使用可能な操作の概要を示しています。

操作	説明
追加	リストに項目を追加します。 詳細については、294 ページの「優先ウォッチリストに項目を追加する」を参照してください。
インポート	インポートして既存のリストを上書きします。 詳細については、294 ページの「優先ウォッチリストをインポートする」を参照してください。
すべてエクスポート	現在のリストをエクスポートします。
削除	1 つ以上の選択した項目を削除します。

優先ウォッチリストに項目を追加する

手順

1. [アプライアンス] > [ネットワーク資産] > [優先ウォッチリスト] の順に選択します。

   [優先ウォッチリスト] 画面が表示されます。

2. [追加] をクリックします。

   [優先ウォッチリストアイテムの追加] ダイアログが表示されます。

3. IP アドレスを入力します。

   注意

   単一の IPv4 アドレスと IPv6 アドレス、およびアドレス範囲がサポートされます。サブネットマスクはオプションです。

4. [追加] をクリックします。

   項目が [優先ウォッチリスト] リストに表示されます。

優先ウォッチリストをインポートする

リストをインポートすると、既存のリストが上書きされます。リストをインポートする前に、既存のリストをエクスポートしておくことをお勧めします。

手順

1. [アプライアンス] > [ネットワーク資産] > [優先ウォッチリスト] の順に選択します。

   [優先ウォッチリスト] 画面が表示されます。

2. [インポート] をクリックします。

   [CSV からの優先ウォッチリストのインポート] ダイアログが表示されます。

3. [選択] をクリックして、インポートする CSV ファイルを指定します。

ヒント

CSV ファイルを初めてインポートする場合は、[サンプル CSV のダウンロード] をクリックしてファイルを保存します。CSV ファイルに項目を正しい書式設定で入力して (CSV ファイル内の説明を参照)、ファイルを保存し、[選択] をクリックして CSV ファイルを指定します。

4. [インポート] をクリックします。

   項目が [優先ウォッチリスト] リストに表示されます。

登録済みドメイン

企業で社内用に使用されているドメイン、または信頼できると見なされるドメインを追加します。信頼されたドメインを指定することで、許可されていないドメインの検出が可能になります。

次の表は、[登録済みドメイン] 画面で使用可能な操作の概要を示しています。

操作	説明
追加	リストに項目を 1 つ以上追加します。 詳細については、296 ページの「登録済みドメインの追加」を参照してください。
インポート	インポートして既存のリストを上書きします。 詳細については、296 ページの「登録済みドメインリストをインポートする」を参照してください。
すべてエクスポート	現在のリストをエクスポートします。
削除	1 つ以上の選択した項目を削除します。

登録済みドメインの追加

手順

1. [アプライアンス] > [ネットワーク資産] > [登録済みドメイン] の順に選択します。

   [登録済みドメイン] 画面が表示されます。

2. [追加] をクリックします。

   [登録済みドメインの追加] ダイアログが表示されます。

3. ドメイン名を入力します。

   注意

   ドメインを複数追加するには、ドメインを 1 つ入力するごとに <Enter> キーを押します。ワイルドカードはサポートされません。

4. (オプション) 説明を入力します。

5. [追加] をクリックします。

   項目が [登録済みドメイン] リストに表示されます。

登録済みドメインリストをインポートする

リストをインポートすると、既存のリストが上書きされます。リストをインポートする前に、既存のリストをエクスポートしておくことをお勧めします。

手順

1. [アプライアンス] > [ネットワーク資産] > [登録済みドメイン] の順に選択します。

   [登録済みドメイン] 画面が表示されます。

2. [インポート] をクリックします。

[CSV、XML からの登録済みドメインのインポート] ダイアログが表示されます。

3. [選択] をクリックして、インポートする CSV または XML ファイルを指定します。

ヒント

- CSV ファイルを初めてインポートする場合は、[サンプル CSV のダウンロード] をクリックしてファイルを保存します。CSV ファイルに項目を正しい書式設定で入力して (CSV ファイル内の説明を参照)、ファイルを保存し、[選択] をクリックして CSV ファイルを指定します。
- Deep Discovery Inspector 5.5 以降からエクスポートした XML ファイルから項目をインポートできます。

---

4. 使用する区切り記号を選択します。
5. [インポート] をクリックします。

   項目が [登録済みドメイン] リストに表示されます。

登録済みサービス

組織で社内用に使用されている、または信頼できると見なされる、特定サービスの専用サーバを追加します。ネットワーク内の信頼するサービスを特定しておくと、不正なアプリケーションやサービスの検出に役立ちます。

次の表は、[登録済みサービス] 画面で使用可能な操作の概要を示しています。

操作	説明
追加	リストに項目を追加します。 詳細については、298 ページの「登録済みサービスの追加」を参照してください。
インポート	インポートして既存のリストを上書きします。 詳細については、299 ページの「登録済みサービスリストをインポートする」を参照してください。

操作	説明
すべてエクスポート	現在のリストをエクスポートします。
削除	1 つ以上の選択した項目を削除します。

登録済みサービスの追加

手順

1. [アプライアンス] > [ネットワーク資産] > [登録済みサービス] の順に選択します。

   [登録済みサービス] 画面が表示されます。

2. [追加] をクリックします。

   [登録済みサービスの追加] ダイアログが表示されます。

3. [種類] から項目を 1 つ以上選択します。

4. IP アドレスを入力します。

   注意

   - 単一の IPv4 アドレスと IPv6 アドレス、およびアドレス範囲がサポートされます。サブネットマスクはオプションです。
   - IP アドレスまたは IP アドレスの範囲はクラス D またはクラス E に属することはできません。
   - IP アドレスまたは IP アドレスの範囲をループバックアドレスにすることはできません。
   - IP アドレスまたは IP アドレスの範囲を複数追加するには、IP アドレスまたは IP アドレスの範囲を 1 つ入力するごとに <Enter> キーを押します。ワイルドカードはサポートされません。

5. (オプション) 説明を入力します。

6. [追加] をクリックします。

項目が [登録済みサービス] リストに表示されます。

登録済みサービスリストをインポートする

リストをインポートすると、既存のリストが上書きされます。リストをインポートする前に、既存のリストをエクスポートしておくことをお勧めします。

手順

1. [アプライアンス] > [ネットワーク資産] > [登録済みサービス] の順に選択します。

   [登録済みサービス] 画面が表示されます。

2. [インポート] をクリックします。

   [CSV,XML からの登録済みサービスのインポート] ダイアログが表示されます。

3. [選択] をクリックして、インポートする CSV または XML ファイルを指定します。

   ヒント

   - CSV ファイルを初めてインポートする場合は、[サンプル CSV のダウンロード] をクリックしてファイルを保存します。CSV ファイルに項目を正しい書式設定で入力して (CSV ファイル内の説明を参照)、ファイルを保存し、[選択] をクリックして CSV ファイルを指定します。
   - Deep Discovery Inspector 5.5 以降からエクスポートした XML ファイルから項目をインポートできます。

   注意

   256 文字を超える説明は切り捨てられます。

4. 使用する区切り記号を選択します。
5. [インポート] をクリックします。

項目が [登録済みサービス] リストに表示されます。

ネットワークグループ

IP アドレスまたは IP アドレスの範囲を追加して監視対象ネットワークのグループを構築します。これにより Deep Discovery 製品では、攻撃元がネットワークの内部または外部のいずれであるかを判断できるようになります。

次の表は、[ネットワークグループ] 画面で使用可能な操作の概要を示しています。

操作	説明
追加	リストに項目を 1 つ以上追加します。 詳細については、301 ページの「ネットワークグループを追加する」を参照してください。
サブグループの追加	サブグループを既存のグループに追加するには、グループ名の横にあるメニューアイコンをクリックし、[サブグループの追加] を選択します。 詳細については、302 ページの「サブグループを追加する」を参照してください。 **注意** 最大 3 件のサブグループのレイヤを追加できます。
インポート	インポートして既存のリストを上書きします。 詳細については、304 ページの「ネットワークグループリストをインポートする」を参照してください。
すべてエクスポート	現在のリストをエクスポートします。
削除	グループを削除するには、グループ名の横にあるメニューアイコンをクリックし、[削除] を選択します。

ネットワークグループを追加する

手順

1. [アプライアンス] > [ネットワーク資産] > [ネットワークグループ] の順に選択します。

   [ネットワークグループ] 画面が表示されます。

2. [追加] をクリックします。

   [新しいグループの追加] ダイアログが表示されます。

3. グループ名を入力します。

   注意

   IP アドレスの属するネットワークを識別しやすくするためにグループに名前を付けてください。例: 「Finance network」、「IT network」、「Administration」 などを使用します。

4. IP アドレスまたは IP アドレスの範囲を入力します。

   注意

   - グループごとに最大 1,000 個の IP アドレスまたは IP アドレスの範囲を追加できます。
   - IP アドレスまたは IP アドレスの範囲はクラス D またはクラス E に属することはできません。
   - IP アドレスまたは IP アドレスの範囲をループバックアドレスにすることはできません。

   a. IP アドレスの範囲を指定するには、ダッシュを使用します。

      [監視対象ネットワークグループ] 画面では、IPv4 と IPv6 がサポートされます。

      - IPv4 の例: `192.168.1.0-192.168.1.255`
      - IPv6 の例: `2620:1005::123-2620:1005::460`

b. IP アドレスのサブネットマスク/プレフィックスを指定するには、スラッシュを使用します。

- IPv4 サブネットマスクの例: `192.168.1.0/24`
- IPv6 サブネットプレフィックスの例: `fd00:1:1111:200::1000/116`

5. IP アドレスまたは IP アドレスの範囲を [信頼する] または [信頼しない] として設定するかどうかを選択します。
6. [監視対象 IP アドレス] の横にある [追加] をクリックします。

   IP アドレスまたは IP アドレスの範囲が下の表に追加されます。
7. (オプション) 手順 4〜6 を繰り返して、このグループに IP アドレスまたは IP アドレスの範囲を追加します。
8. [追加] をクリックします。

   項目が [ネットワークグループ] リストに表示されます。

サブグループを追加する

最大 3 件のサブグループのレイヤを追加できます。

手順

1. [アプライアンス] > [ネットワーク資産] > [ネットワークグループ] の順に選択します。

   [ネットワークグループ] 画面が表示されます。
2. グループ名の横にあるメニューアイコンをクリックし、[サブグループの追加] を選択します。

   [新しいサブグループの追加] ダイアログが表示され、親グループの IP アドレスの範囲が表示されます。
3. グループ名を入力します。

注意

IP アドレスの属するネットワークを識別しやすくするためにグループに名前を付けてください。例: 「Finance network」、「IT network」、「Administration」 などを使用します。

4. IP アドレスまたは IP アドレスの範囲を入力します。

注意

- 追加する IP アドレスは親グループの IP アドレスの範囲内に収める必要があります。
- グループごとに最大 1,000 個の IP アドレスまたは IP アドレスの範囲を追加できます。
- IP アドレスまたは IP アドレスの範囲はクラス D またはクラス E に属することはできません。
- IP アドレスまたは IP アドレスの範囲をループバックアドレスにすることはできません。

a. IP アドレスの範囲を指定するには、ダッシュを使用します。

[監視対象ネットワークグループ] 画面では、IPv4 と IPv6 がサポートされます。

- IPv4 の例: `192.168.1.0-192.168.1.255`
- IPv6 の例: `2620:1005::123-2620:1005::460`

b. IP アドレスのサブネットマスク/プレフィックスを指定するには、スラッシュを使用します。

- IPv4 サブネットマスクの例: `192.168.1.0/24`
- IPv6 サブネットプレフィックスの例: `fd00:1:1111:200::1000/116`

5. IP アドレスまたは IP アドレスの範囲を [信頼する] または [信頼しない] として設定するかどうかを選択します。

6. [監視対象 IP アドレス] の横にある [追加] をクリックします。

IP アドレスまたは IP アドレスの範囲が下の表に追加されます。

7. (オプション) 手順 4〜6 を繰り返して、このグループに IP アドレスまたは IP アドレスの範囲を追加します。
8. [追加] をクリックします。

   項目が [ネットワークグループ] リストに表示されます。

ネットワークグループリストをインポートする

リストをインポートすると、既存のリストが上書きされます。リストをインポートする前に、既存のリストをエクスポートしておくことをお勧めします。

手順

1. [アプライアンス] > [ネットワーク資産] > [ネットワークグループ] の順に選択します。

   [ネットワークグループ] 画面が表示されます。
2. [インポート] をクリックします。

   [JSON、XML からのネットワークグループのインポート] ダイアログが表示されます。
3. [選択] をクリックして、インポートする JSON または XML ファイルを指定します。

   ヒント

   - JSON ファイルを初めてインポートする場合は、[サンプル JSON のダウンロード] をクリックしてファイルを保存します。JSON ファイルに項目を正しい書式設定で入力して (JSON ファイル内の説明を参照)、ファイルを保存し、[選択] をクリックして JSON ファイルを指定します。
   - Deep Discovery Inspector 5.5 以降からエクスポートした XML ファイルから項目をインポートできます。
4. [インポート] をクリックします。

項目が [ネットワークグループ] リストに表示されます。

分析

検出を分析し、検出されたドメインとサービスを選択して、登録済みドメインと登録済みサービスのリストに追加してください。

登録済みドメインと登録済みサービスへの検出の追加

手順

1. [アプライアンス] > [ネットワーク資産] > [分析] の順に選択します。

   [分析] 画面が表示されます。

2. [検出の分析] をクリックします。

   [登録済みドメインと登録済みサービスへの検出の追加] ダイアログが表示されます。

3. ネットワークの設定を確認し、ドメインとサービスを選択して、[登録済みドメイン] と [登録済みサービス] のリストに追加します。

4. (オプション) 選択したドメインとサービスの説明を入力します。

5. [追加] をクリックします。

   項目が [登録済みドメイン] と [登録済みサービス] のリストに追加されます。

Email Encryption

Email Encryption により、Deep Discovery Email Inspector アプライアンスはトレンドマイクロの ID ベース暗号化 (IBE) を使用してメッセージを暗号化します。たとえば、暗号化および復号を行うドメインとして aa.com が登録されており、user1@aa.com が個人情報を含むメッセージを user2@bb.com に送信

する場合、Deep Discovery Email Inspector は user2@bb.com に送信されるメッセージを暗号化します。

ヒント

Email Encryption を使用する場合、システム時間を NTP サーバと同期して標準の日時データを確認するよう Deep Discovery Email Inspector アプライアンスを設定しておくことをお勧めします。

注意

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

[登録済みアプライアンスに同期] の切り替えスイッチをクリックして、すべての登録済みの Deep Discovery Email Inspector アプライアンスに対する [Email Encryption] 設定の同期を有効または無効にします。

ドメインリスト

Email Encryption を機能させるには、1 つ以上のドメインを Trend Micro Email Encryption サーバに登録する必要があります。

注意

- Trend Micro Email Encryption サーバに登録されているドメインを再登録することはできません。
- Trend Micro Email Encryption サーバには最大 300 件のドメインを追加および登録できます。

[ドメインリスト] 画面には、次の情報が表示されます。

表 6-11. [ドメインリスト] の列

列	情報
ドメイン	ドメイン名。
追加日	ドメインが追加された日時。

列	情報
前回のアップデート	ドメインの登録ステータスが最後にアップデートされた日時。
登録のステータス	ドメインの登録ステータスは次のいずれかになります。 • 保留中: ドメインの検証とキーファイルのインポートを待機しています • 完了
ドメイン:	使用中のドメインの数/許可されるドメインの最大数。

ドメインを登録する

手順

1. [アプライアンス] > [Email Encryption] > [ドメインリスト] の順に選択します。
2. [追加] をクリックします。

   [ドメインの追加] ダイアログが表示されます。
3. トレンドマイクロからキーファイルを受信するメールアドレスを指定します。

   注意

   - 追加した各ドメインにキーファイルが送信されます。ドメインの登録プロセスを完了するには、キーファイルを Deep Discovery Director (統合モード) にインポートする必要があります。
   - 最初のドメインの Trend Micro Email Encryption サーバへの登録が正常に行われた後、[ID] 画面でメールアドレスを変更できます。
4. ドメインを選択するか、入力して検索するか、またはドメインを入力して <Enter> キーを押します。

注意

- 一度に最大 10 個のドメインを追加できます。
- ドメインとそのサブドメインは一意のエントリとして扱われます。サブドメインは個別にドメインリストに追加する必要があります。
- ワイルドカードを使用してサブドメインを含めることはできません。
- LDAP グループ (「LDAP」で始まるエントリ) をドメインリストに追加することはできません。

5. [追加] をクリックします。

   指定したドメインが [ドメインリスト] 画面に追加されます。

6. 確認のメールメッセージに返信して、ドメインの所有権を確認します。

   確認のメールメッセージは次のメールアドレスに送信されます。

   - `webmaster@yourdomain`
   - `postmaster@yourdomain`
   - ドメインの WHOIS 検索で返されたメールアドレス

7. ドメインの所有権が確認されると、手順 3 で指定したメールアドレスにキーファイルが送信されます。

注意

トレンドマイクロは追加された各ドメインのキーファイルを指定されたメールアドレスに送信します。3 営業日以内にドメインのキーファイルを含むメッセージを受け取らなかった場合は、販売代理店にお問い合わせください。

8. [キーファイルのインポート] をクリックします。

   [キーファイルのインポート] ダイアログが表示されます。

9. [ファイルの選択] をクリックして、インポートするキーファイルを指定します。

10. [インポート] をクリックします。

11. ドメインを初めて Trend Micro Email Encryption サーバに登録する場合は、[ID] 画面にゲートウェイ ID 情報が表示されていることを確認します。

ドメインを削除する

手順

1. [アプライアンス] > [Email Encryption] > [ドメインリスト] の順に選択します。
2. 削除するドメインを 1 つ以上選択して、[削除] をクリックします。

注意

削除したドメインをドメインリストに再び追加するには、ドメインの登録手順を再度実行する必要があります。

ID

メールメッセージに署名するための初期設定の ID を設定したり、アプライアンスのゲートウェイ ID を表示したり、キーファイルを受信するためのメールアドレスを設定したりするには、[ID] 画面を使用します。

[初期設定の ID] セクションで指定する送信者アドレスは、[ドメインリスト] に含まれないドメインのメッセージに署名するために使用されます。

[アプライアンス情報] セクションで指定するメールアドレスは、検証済みのドメインのキーファイルを受信するために使用されます。このメールアドレスは、最初のドメインが Trend Micro Email Encryption サーバに正常に登録された後に変更できます。

ID を設定する

手順

1. [アプライアンス] > [Email Encryption] > [ID] の順に選択します。
2. [初期設定の ID] セクションで、送信者アドレスを指定します。

   注意
   正常に登録されているドメインのメールアドレスのみを使用できます。

3. [アプライアンス情報] セクションで、検証済みのドメインのキーファイルを受信するためのメールアドレスを指定します。

   注意
   このメールアドレスは、最初のドメインがトレンドマイクロ Email Encryption サーバに正常に登録された後に変更できます。

4. [保存] をクリックします。

ログ

[ログ] 画面には、Deep Discovery Director (統合モード) に登録された Deep Discovery アプライアンスのさまざまなログが表示されます。

メールメッセージ追跡

ブロックされたメッセージや配信されたメッセージなど、Deep Discovery Email Inspector を通過したメールメッセージを追跡します。Deep Discovery Email Inspector は送信者、受信者、および実施されたポリシー処理などのメッセージの詳細をログに記録します。

メールメッセージ追跡ログは、メールメッセージが Deep Discovery Email Inspector によって受信または送信されたかどうかを示します。メールメッ

セージ追跡ログは、Deep Discovery Email Inspector がメールメッセージを調査している証拠にもなります。

表示オプションと検索フィルタ

表示をカスタマイズするには、次の表示オプションと検索フィルタを適用してください。

表 6-12. 表示オプションと検索フィルタ: [メールメッセージ追跡]

フィルタオプション	説明	
リスクレベル	フィルタオプションには、次のリスクレベル設定が含まれます。	
	高	リスク高のメールメッセージを表示します
	中	リスク中のメールメッセージを表示します
	低	リスク低のメールメッセージを表示します
	リスクなし	リスクのないメールメッセージを表示します
	未評価	検索できなかったメールメッセージを表示します
	使用不可	スパムメール/グレーメールメッセージ、およびコンテンツ違反により検出されたメールメッセージを表示します
	すべて	すべてのメールメッセージを表示します
期間	過去 24 時間	
	過去 7 日間	
	過去 14 日間	
	過去 30 日間	
	過去 60 日間	
	カスタム範囲	

フィルタオプション	説明
監視対象ドメイン	表示するメールメッセージのドメインを選択します。
基本検索	基本検索フィールドにキーワードを入力して、送信者、メールヘッダ (from)、受信者、またはメールヘッダ (to) の部分一致を検索します。大文字と小文字は区別されません。
詳細検索	ユーザ定義の条件セットによる検索を行います。 各セットには次のものが 1 つ以上含まれます。 • 属性 • 演算子 • 関連付けられた値

メールメッセージ追跡ログを表示する

手順

1. [アプライアンス] > [ログ] > [メールメッセージ追跡] の順に選択します。

   [メールメッセージ追跡] 画面が表示されます。

2. ドロップダウンコントロールを使用してリスクレベルを選択します。
3. 期間を選択します。
4. 表示するメールメッセージのドメインを選択します。
5. 基本の検索を実行するには、検索テキストボックスにキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

   Deep Discovery Director (統合モード) の初期設定では、メールメッセージを [受信者]、[メールヘッダ (To)]、[送信者]、[メールヘッダ (From)] で検索できます。

6. 詳細検索フィルタを作成して適用するには、[詳細] をクリックします。

   詳細については、315 ページの「[メールメッセージ追跡] の詳細検索フィルタ」を参照してください。

7. 左端の列にある矢印アイコンをクリックして、メールメッセージの詳細情報を表示します。

フィールド	説明
メッセージ ID	メールメッセージの一意の ID。
送信元 IP	メールメッセージの送信者に最も近い MTA の IP アドレス。
送信者 IP	メールメッセージの送信者の IP アドレス。

フィールド	説明

処理履歴	メールメッセージが Deep Discovery Email Inspector でどのように処理されたかを表示します。処理には次のものがあります。
	• 処理を「放置」に設定
	  • メールメッセージに [放置] ポリシー処理が適用されました。
	  • ユーザによってメールメッセージのコピーが配信されました。これは [添付ファイルの削除、ブロックページへのリンクのリダイレクト、およびタグ付け] と [添付ファイルの削除、警告ページへのリンクのリダイレクト、およびタグ付け] のポリシーが元のメールメッセージに適用されている場合にのみ適用されます。
	• 削除 (理由): コンテンツフィルタルール、脅威対策ルール、または情報漏えい対策ポリシー違反に基づいて、あるいは [隔離] からメールメッセージが削除されました。
	• 配信済み: メールメッセージが配信されました。
	• 未分析: 指定された理由により仮想アナライザで分析を完了できませんでした。
	• 処理完了: 分析が完了し、メールメッセージが破棄されました。これは、BCC モードおよび SPAN/TAP モードの最終ステータスです。
	• 隔離 (理由): メールメッセージが Deep Discovery Email Inspector のポリシーに従って隔離されました。BCC モードおよび SPAN/TAP モードでは、メールメッセージは隔離されません。
	• 配信のためにキューに配置: メールメッセージの配信が保留されています。BCC モードおよび SPAN/TAP モードでは、このステータスのメールメッセージはキューに入れられ破棄されます。
	• 受信: メールメッセージが Deep Discovery Email Inspector によって受信されました。
	• 分析のために送信: メールメッセージが分析のため仮想アナライザに送信されました。
	• 削除 (コンテンツフィルタ/情報漏えい対策イベント/脅威): メールメッセージから添付ファイルが削除され、配信処理が開始されました。

次のいずれかを実行します。

- 隔離メッセージ:
  - 検出の詳細で表示
  - 隔離で表示
- 隔離されていないメッセージ (高/中/低のリスクレベル):

  検出の詳細で表示

8. (オプション) [エクスポート] アイコンをクリックし、使用する区切り記号を選択します。次に [OK] をクリックし、選択した区切り記号で、メールメッセージ追跡ログの現在のフィルタ済みリストを CSV ファイルにエクスポートしてダウンロードします。

[メールメッセージ追跡] の詳細検索フィルタ

詳細検索フィルタを使用して、カスタマイズされた検索を作成および適用します。

詳細については、316 ページの「[メールメッセージ追跡] の詳細検索フィルタを追加する」を参照してください。

特定のデータを表示するには、次のオプションの属性および演算子を選択して、関連付けられた値を入力してください。

表 6-13. 検索条件: [メールメッセージ追跡]

属性	演算子	処理
送信者	次の値と等しい/次の値を含む/次の値を含まない	値を入力
受信者	次の値と等しい/次の値を含む/次の値を含まない	値を入力
メールヘッダ (From)	差出人あり/差出人なし	
	次の値と等しい/次の値を含む/次の値を含まない	値を入力

属性	演算子	処理
メールヘッダ (To)	次の値と等しい/次の値を含む/次の値を含まない	値を入力
メッセージ ID	次の値を含む/次の値を含まない	値を入力
件名	次の値を含む/次の値を含まない/次の値と等しい	値を入力
方向	等しい	方向を選択
送信元 IP	次の値を含む/次の値を含まない/次の値と等しい	値を入力
	範囲内/範囲外	範囲を入力
送信者 IP	次の値を含む/次の値を含まない/次の値と等しい	値を入力
	範囲内/範囲外	範囲を入力
最新のステータス	次のいずれかの値を含む/次のいずれの値も含まない	ステータスを 1 つ以上選択

[メールメッセージ追跡] の詳細検索フィルタを追加する

手順

1. [メールメッセージ追跡] の詳細検索フィルタを作成するには、[アプライアンス] > [ログ] > [メールメッセージ追跡] の順に選択し、[詳細] をクリックします。
2. 属性および関連付けられた演算子を選択します。
3. 次のいずれかを実行して、処理を指定します。
   - テキストボックスに値を入力します。
   - ドロップダウンリストから値を選択します。

ヒント

キーワードを入力して、部分一致を検索します。

注意

値の入力後に <Enter> キーを押すと、複数の条件エントリを追加できます。

4. (オプション) [および] または [または] をクリックして、検索フィルタに別の条件セットを含めます。
5. [適用] をクリックします。

   [メールメッセージ追跡] 画面が更新され、検索条件によってフィルタされたデータが表示されます。すべての検索条件セットのサマリーが表示されます。
6. (オプション) [リスクレベル] ドロップダウンリストの横にある右矢印アイコンをクリックして、詳細検索機能を閉じます。

MTA

ネットワーク上の Postfix と SMTP の活動について、接続の詳細を参照できます。

MTA ログのクエリを実行する

手順

1. [アプライアンス] > [ログ] > [MTA] の順に選択します。

   [MTA] 画面が表示されます。
2. 期間を選択します。
3. どのアプライアンスの MTA ログにクエリを実行するのかを選択します。
4. 検索テキストボックスに説明のキーワードを入力し、[クエリ] をクリックします。

Deep Discovery Director (統合モード) により、選択したアプライアンスに対して一致する MTA ログのクエリが実行されます。この処理には数分かかることがあります。

注意

初期設定では、結果はまず [データソース] を基準に並び替えられ、次に [タイムスタンプ] を基準に並び替えられます。

5. (オプション) [エクスポート] アイコンをクリックし、使用する区切り記号を選択します。次に [OK] をクリックし、選択した区切り記号で、MTA ログの現在のフィルタ済みリストを CSV ファイルにエクスポートしてダウンロードします。

メッセージキュー

登録済み Deep Discovery Email Inspector アプライアンスのメールキューにクエリを実行して管理します。

Deep Discovery Email Inspector が受信したメールメッセージは、次のいずれかのメッセージキューに保存されます。

- 受信: 処理と配信を待機するメールメッセージが保存されます。
- アクティブ: 処理が開始されたメールメッセージが保存されます。
- 遅延: 処理後に配信できないメールメッセージが保存されます。

メッセージキューのログを表示して、メッセージがメッセージキューに追加された日時を確認できます。詳細については、319 ページの「メッセージキューログのクエリを実行する」を参照してください。

クエリを実行したメッセージを選択して、処理を実行できます。詳細については、321 ページの「メッセージキューを管理する」を参照してください。

次の表は、[メッセージキュー] 画面の詳細を示しています。

フィールド	説明
受信	メッセージを受信した日時
種類	メッセージキューの種類
メッセージ ID	メールメッセージの一意の ID
送信者	送信者のメールアドレス
受信者	メッセージ受信者のメールアドレス
件名	メッセージの件名
サイズ (バイト)	メッセージのバイト単位のサイズ
アーカイブ/MTA サーバ	Deep Discovery Email Inspector がメッセージを送信するアーカイブサーバまたは MTA サーバのアドレス
メッセージの種類	メッセージの種類
前回の配信ステータス	前回の配信処理の実行ステータス
データソース	メッセージを保管している Deep Discovery Email Inspector アプライアンス

メッセージキューログのクエリを実行する

手順

1. [アプライアンス] > [ログ] > [メッセージキュー] の順に選択します。

   [メッセージキュー] 画面が表示されます。

2. 基本的または詳細なクエリを実行します。

   - 基本的なクエリ:

     a. クエリの対象とするメッセージキューの種類を選択します。

     b. クエリの対象とするメッセージの種類を選択します。

c. どのアプライアンスのメッセージキューログにクエリを実行するのかを選択します。

d. 検索テキストボックスに受信者のキーワードを入力し、[クエリ] をクリックします。

- 詳細なクエリ:

a. [詳細] をクリックします。

b. クエリの対象とするメッセージキューの種類を選択します。

c. クエリの対象とするメッセージの種類を選択します。

d. どのアプライアンスのメッセージキューログにクエリを実行するのかを選択します。

e. 属性を選択します。

- 送信者: 送信者のメールアドレス。
- 受信者: 受信者のメールアドレス。
- メッセージ ID: メールメッセージの一意の ID。
- 件名: メッセージの件名。
- アーカイブ/MTA サーバ: メールメッセージの送信先であったアーカイブまたは MTA サーバ。

f. テキストボックスに値を入力します。

g. (オプション) [および] をクリックして、クエリに別の条件セットを含めます。

h. [クエリ] をクリックします。

Deep Discovery Director (統合モード) により、選択したアプライアンスに対して一致するメッセージキューログのクエリが実行されます。この処理には数分かかることがあります。

注意

- 初期設定では、結果は [受信] を基準に並び替えられます。
- クエリを実行した各 Deep Discovery Email Inspector アプライアンスから返されるメッセージキューログは、最新の 10,000 件のみです。

メッセージキューを管理する

手順

1. [アプライアンス] > [ログ] > [メッセージキュー] の順に選択します。

   [メッセージキュー] 画面が表示されます。

2. メッセージにクエリを実行します。
3. メッセージを 1 つ以上選択し、次のいずれかをクリックします。
   - 配信: 選択したメッセージを再処理せずに目的の受信者に直接配信します。

     注意

     この処理は遅延メッセージにのみ実行できます。

   - 再ルーティング: 選択したメッセージをアーカイブ/MTA サーバに再ルーティングします。

     注意

     この処理は受信および遅延メッセージにのみ実行できます。

   - 削除: 選択したメッセージを削除します。削除したメッセージを復元することはできません。
   - 選択した処理は、選択したメッセージを保管している Deep Discovery Email Inspector アプライアンスにタスクとしてただちに送信されます。

- ダイアログにタスクのステータスが表示されます。すべてのタスクが正常に送信されると、ダイアログが自動的に閉じます。

エンドユーザメール隔離

Deep Discovery Director (統合モード) には、スパムメールの管理を強化するエンドユーザメール隔離 (EUQ) 機能があります。スパムメールと判定されたメッセージは隔離され、エンドユーザがメッセージを再確認、削除、および隔離解除して配信することができます。

インライン処理リンクを含むエンドユーザメール隔離通知を自動的に送信するように Deep Discovery Director (統合モード) を設定できます。

Web ベースのエンドユーザメール隔離コンソールを使用することで、ユーザは各自の個人アカウントおよび、自分が所属する配布リストのスパムメールの隔離方法を管理したり、送信者を承認済み送信者リストに追加したりできます。

エンドユーザメール隔離の設定

この画面を使用して、エンドユーザメール隔離を設定します。

エンドユーザメール隔離を設定する

手順

1. [アプライアンス] > [エンドユーザメール隔離] > [エンドユーザメール隔離の設定] の順に選択します。

   [エンドユーザメール隔離の設定] 画面が表示されます。

2. [エンドユーザメール隔離を有効にする] を選択します。

3. 認証方法を選択します。

- EUQ 認証に Active Directory を使用する: Active Directory のアカウント認証情報に基づいてユーザを認証します。このオプションを選択する場合は、次の設定を指定できます。
  - すべてのグループに対するエンドユーザメール隔離コンソールへのアクセス: 設定した Microsoft Active Directory サーバ上のすべての Active Directory グループに対してエンドユーザメール隔離コンソールのアクセスを有効にするには、このオプションを選択します。
  - 指定したグループに対するエンドユーザメール隔離コンソールへのアクセス: 指定した Active Directory グループに対してエンドユーザメール隔離コンソールのアクセスを有効にするには、このオプションを選択します。

    テキストボックスにキーワードを入力し、[クエリ] をクリックしてユーザグループを検索します。[利用可能なグループ] リストでグループ名をクリックして、[選択したグループ] リストに追加します。

注意

この方法は、Microsoft Active Directory が設定済みの場合にのみ使用できます。

詳細については、365 ページの「Microsoft Active Directory」を参照してください。

- EUQ 認証に ID プロバイダを使用する: 設定された ID プロバイダに基づいてユーザを認証します。このオプションを選択する場合は、次の設定を指定できます。
  - 任意の設定済み ID プロバイダによって認証されたすべてのユーザ: 任意の設定済み ID プロバイダによって認証されたすべてのユーザに対してエンドユーザメール隔離コンソールのアクセスを有効にします。
  - クレーム値が指定された SAML グループユーザ: クレーム値が指定された SAML グループユーザに対してエンドユーザメール隔離コンソールのアクセスを有効にします。

大文字と小文字を区別してクレーム値を入力し、<Enter> キーを押します。

注意

この方法は、SAML 認証が設定済みの場合にのみ使用できます。

詳細については、367 ページの「SAML 認証」を参照してください。

- EUQ 認証に SMTP サーバを使用する: メールアカウント認証情報に基づいてユーザを認証します。[追加] をクリックして [SMTP サーバの追加] ダイアログを開き、SMTP サーバの設定を指定します。

4. [エンドユーザメール隔離コンソールのアクセスを有効にする] を選択し、ユーザがエンドユーザメール隔離コンソールにアクセスできるようにします。
5. (オプション) [配布リスト EUQ の管理を有効にする] をオンにすると、ユーザは自分が所属する配布リストのスパムメール隔離を管理できます。
6. (オプション) [隔離解除したメッセージを再処理せずに直接配信する] をオンにすると、隔離されたメッセージを検索せずに隔離解除し、ユーザが受信者に直接配信できます。

注意

このオプションを無効にすると、隔離解除されたメッセージの処理が Deep Discovery Email Inspector で続行されます。検索結果に応じて、メッセージは再度隔離されることがあります。

7. (オプション) [ユーザ 1 人あたりの承認済み送信者の最大数] ドロップダウンリストで、エンドユーザメール隔離コンソールで追加できる承認済み送信者のメールアドレスの最大数を選択します。
8. [保存] をクリックします。

Deep Discovery Director (統合モード) により、エンドユーザメール隔離機能と Web ベースのエンドユーザメール隔離コンソールが設定されます。この URL をクリックしたり、URL をコピーしてユーザに送信したりすることで、エンドユーザメール隔離コンソールにアクセスできるようになります。

詳細については、327 ページの「エンドユーザメール隔離コンソール」を参照してください。

エンドユーザメール隔離通知

エンドユーザメール隔離通知は、スパムメールとして検出され、一時的に隔離されているメールメッセージについてユーザに知らせるために Deep Discovery Director (統合モード) から送信される通知です。

注意

- 認証に Active Directory を使用している場合、Deep Discovery Director (統合モード) はユーザグループ (または配布リスト) にエンドユーザメール隔離通知を送信しません。
- 認証に ID プロバイダを使用する場合、エンドユーザメール隔離通知を [すべてのユーザ] または [指定された Active Directory グループのメンバー] に送信するように Deep Discovery Director (統合モード) を設定できます。テキストボックスにキーワードを入力し、[クエリ] をクリックしてユーザグループを検索します。[利用可能なグループ] リストでグループ名をクリックして、[選択したグループ] リストに追加します。
- 認証に 1 つ以上の SMTP サーバを使用しており、検出されたメッセージが配布リストに送信される場合、Deep Discovery Director (統合モード) は配布リストにエンドユーザメール隔離通知を送信します。

エンドユーザメール隔離通知では、次の情報が提供されます。

- 新規のスパムメール数: 最後の通知が送信されて以降にスパムメールと特定された新しいメールメッセージの数
- 新規のスパムメール合計サイズ: 最後の通知が送信されて以降の新しいメールメッセージの合計サイズ
- メッセージ: スパムメールと特定された新しいメールメッセージの概要
  - 受信: メールメッセージを受信した日時
  - 送信者: 送信者のメールアドレス

- メールの件名: メールの件名
- 処理: 隔離されたメッセージに処理を適用できるリンク

> **注意**
> インライン処理リンクは、[エンドユーザメール隔離 (EUQ) 通知] 画面でこの機能を有効にしている場合にのみ表示されます。

エンドユーザメール隔離通知を設定する

手順

1. [アプライアンス] > [エンドユーザメール隔離] > [エンドユーザメール隔離 (EUQ) 通知] の順に選択します。

   [エンドユーザメール隔離 (EUQ) 通知] 画面が表示されます。

2. [エンドユーザメール隔離 (EUQ) 通知を有効にする] を選択します。
3. [通知の頻度] ドロップダウンリストから、Deep Discovery Director (統合モード) がエンドユーザメール隔離通知を送信するまで待機する時間数を選択します。
4. エンドユーザメール隔離通知からユーザが処理を適用できるようにするには、[有効] を選択します。
5. (オプション) 通知テンプレートを変更します。使用可能なトークンが右側に表示されます。トークンをクリックすると、テキストカーソルの位置に挿入できます。
6. [保存] をクリックします。

インライン処理

エンドユーザメール隔離通知にインライン処理リンクを含めるように Deep Discovery Director (統合モード) を設定できます。ユーザはエンドユーザメール隔離通知のリンクをクリックすることで、エンドユーザメール隔離コンソールにアクセスすることなく隔離メッセージを管理できます。

インライン処理リンクを使用すると、隔離されたメッセージに対して次の処理を実行できます。

- 削除: メッセージとすべての関連する添付ファイルを削除します。
- 隔離解除: メッセージを目的の受信者に配信します。
- 隔離解除して送信者を承認: メッセージを目的の受信者に配信し、送信者のメールアドレスを承認済み送信者リストに追加します。

重要

隔離解除したメッセージを再処理せずに目的の受信者に直接配信するには、[エンドユーザメール隔離の設定] 画面で [隔離解除したメッセージを再処理せずに直接配信する] を選択する必要があります。そうしない場合、隔離解除されたメッセージの処理が Deep Discovery Email Inspector で続行されます。

詳細については、322 ページの「エンドユーザメール隔離を設定する」を参照してください。

注意

通知は転送しないことをお勧めします。

エンドユーザメール隔離コンソール

エンドユーザメール隔離を有効にする際は、Deep Discovery Director (統合モード) のエンドユーザメール隔離コンソールで次のタスクを実行できます。

- ユーザ各自の個人アカウントのスパムメール隔離の管理
- 承認済み送信者リストへの送信者の追加
- ユーザが所属する Active Directory の配布リストのスパムメール隔離の管理

注意

エンドユーザメール隔離コンソールは、[エンドユーザメール隔離の設定] 画面で有効にしておく必要があります。

詳細については、322 ページの「エンドユーザメール隔離の設定」を参照してください。

エンドユーザメール隔離コンソールにアクセスする

隔離されたスパムメールメッセージを管理し、メールアドレスを [承認済み送信者リスト] に追加するには、エンドユーザメール隔離コンソールにアクセスします。

手順

1. Web ブラウザに、Deep Discovery Director (統合モード) サーバの IP アドレスとポート番号 `4459` を入力します。

   `https://<サーバの IP アドレス>:4459`

2. ログオンアカウント情報を入力します。

   次の表は、使用する認証方法に応じたログオンユーザ名の形式を示しています。

認証方法	ログオン名形式
Active Directory	**ユーザプリンシパル名** 例: `user@example.com`
SMTP	**有効なメールアドレス**

3. [ログオン] をクリックします。

   [隔離メッセージ] 画面が表示されます。

隔離メッセージ

エンドユーザメール隔離コンソールの [隔離メッセージ] 画面には、Deep Discovery Email Inspector によってスパムと特定され、一時的に隔離された

メールメッセージのリストが表示されます。メールメッセージの詳細を表示してから、メールメッセージを隔離解除するか、メールメッセージを隔離解除して送信者のメールアドレスを [承認済み送信者リスト] に追加するか、またはメールメッセージを削除するかを決定してください。

エンドユーザメール隔離コンソールの [隔離メッセージ] 画面には、次の情報が表示されます。

表 6-14. [隔離メッセージ] の列

列	情報
詳細	このアイコンをクリックすると、サイズ、メッセージ ID、添付ファイル名、メッセージ表示 (メッセージの最初の 2KB 分) など、メールメッセージに関する詳細が表示されます。
送信者	送信者のメールアドレス。
受信者	受信者のメールアドレス。
メールの件名	メールの件名。
検出	メールメッセージを検出した日時。

隔離メッセージを表示および管理する

Deep Discovery Email Inspector によってスパムと特定され、一時的に隔離されたメールメッセージのリストを表示します。

手順

1. エンドユーザメール隔離コンソールにアクセスします。

   [隔離メッセージ] 画面が表示されます。

   注意

   初期設定では、メールメッセージは [検出] を基準に並び替えられます。

2. (オプション) 期間を選択します。
3. メールメッセージを 1 つ以上選択し、次のいずれかをクリックします。

- 隔離解除: 選択したメールメッセージを目的の受信者に配信します。
- 隔離解除して送信者を承認: 選択したメッセージを隔離解除し、送信者のメールアドレスを [承認済み送信者リスト] に追加します。
- 削除: 選択したメッセージを削除します。削除したメッセージを復元することはできません。

注意

隔離解除したメッセージを再処理せずに目的の受信者に直接配信するには、[エンドユーザメール隔離の設定] 画面で [隔離解除したメッセージを再処理せずに直接配信する] を選択する必要があります。そうしない場合、隔離解除されたメッセージの処理が Deep Discovery Email Inspector で続行されます。

選択した処理は、選択したメッセージを保管している Deep Discovery Email Inspector アプライアンスにタスクとしてただちに送信されます。

承認済み送信者

[承認済み送信者] 画面には、Deep Discovery Email Inspector の送信者フィルタ設定と送信者の認証設定をバイパスする信頼された送信者のリストが表示されます。

注意

Deep Discovery Email Inspector は Trend Micro Email Reputation Services (ERS) を使用して、承認済み送信者からの受信 SMTP トラフィックを引き続き確認しますが、トラフィックをブロックすることはありません。

承認済み送信者を追加する

安全と見なす送信者のメールアドレスを追加して、スパムメールの誤検出を減らすことができます。

手順

1. エンドユーザメール隔離コンソールにアクセスし、[承認済み送信者] タブをクリックします。

   [承認済み送信者] 画面が表示されます。

2. テキストボックスにメールアドレスを入力し、[追加] をクリックします。

3. [保存] をクリックします。

配布リスト隔離

[配布リスト隔離] 画面には、Deep Discovery Email Inspector によりスパムメール/グレーメールと見なされた、自分が所属する配布リスト宛ての隔離メールメッセージのリストが表示されます。

配布リスト隔離メッセージのクエリを実行する

手順

1. エンドユーザメール隔離コンソールにアクセスし、[配布リスト隔離] タブをクリックします。

   [配布リスト隔離] 画面が表示されます。

2. 期間を選択します。

3. 検索テキストボックスにメールグループアドレス全体を入力し、[クエリ] をクリックします。

   Deep Discovery Director (統合モード) により、Deep Discovery Email Inspector アプライアンスに対して一致する隔離メールメッセージのクエリが実行されます。この処理には数分かかることがあります。

   注意

   初期設定では、結果は [検出] を基準に並び替えられます。

配布リスト隔離を管理する

手順

1. エンドユーザメール隔離コンソールにアクセスし、[配布リスト隔離] タブをクリックします。

   [配布リスト隔離] 画面が表示されます。

2. メッセージにクエリを実行します。

3. メールメッセージを 1 つ以上選択し、次のいずれかをクリックします。

   - 隔離解除: 選択したメールメッセージを目的の受信者に配信します。
   - 削除: 選択したメッセージを削除します。削除したメッセージを復元することはできません。

   注意

   隔離解除したメッセージを再処理せずに目的の受信者に直接配信するには、[エンドユーザメール隔離の設定] 画面で [隔離解除したメッセージを再処理せずに直接配信する] を選択する必要があります。そうしない場合、隔離解除されたメッセージの処理が Deep Discovery Email Inspector で続行されます。

   選択した処理は、選択したメッセージを保管している Deep Discovery Email Inspector アプライアンスにタスクとしてただちに送信されます。

第 7 章

アラート

次の項目では、アラート通知とその設定方法について説明します。

アラートについて

Deep Discovery Director (統合モード) では、さまざまなイベントを監視し、それらのイベントについてユーザに知らせるアラートを生成できます。

トークン変数

次の表は、アラート通知の件名をカスタマイズするために使用できるトークン変数を示しています。

注意

すべてのトークンがすべてのアラートで使用可能なわけではありません。

表 7-1. 件名のトークン

トークン	説明
%AlertLevel%	アラート通知のレベル。
%AlertName%	アラート通知の名前。
%AlertType%	アラート通知の種類。
%HostName%	Deep Discovery Director (統合モード) のホスト名。
%ProductShortName%	Deep Discovery Director (統合モード) の略称。

次の表は、アラート通知のメッセージ本文で使用されるトークン変数を示しています。

注意

アラート通知のメッセージ本文は変更できません。

表 7-2. メッセージ本文のトークン

トークン	説明
%LoopStart% %LoopEnd%	この 2 つのトークンの間にあるテキストが、すべてのシステムエラーが表示されるまで繰り返されます。
%IssueDescription%	システムエラーの説明。
%Recommendation%	システムエラーの解決方法に関する推奨事項。
%DateTime%	アラートが実行された日時。
%ConsoleURL%	Deep Discovery Director (統合モード) 管理コンソールの URL。
%DataBaseUsage%	データベースパーティションの合計使用率。
%FreeDataBaseSpace%	データベースパーティションの空き容量。
%YaraRulesPage%	Deep Discovery Director (統合モード) 管理コンソールの [YARA ルール] 画面の URL。
%STIXPage%	Deep Discovery Director (統合モード) 管理コンソールの [STIX] 画面の URL。
%LicenseLoopStart% %LicenseLoopEnd%	この 2 つのトークンの間にあるテキストが、すべてのライセンス項目が表示されるまで繰り返されます。
%LicenseDescription%	ライセンスの説明。
%LicenseType%	ライセンスの種類。
%LicenseStatus%	ライセンスのステータス。
%ExpirationDate%	ライセンスの有効期限。
%DaysBeforeExpiration%	ライセンスの有効期限までの日数。
%LicensePageURL%	Deep Discovery Director (統合モード) 管理コンソールの [ライセンス] 画面の URL。

トークン	説明
%ServiceLoopStart% %ServiceLoopEnd%	この 2 つのトークンの間にあるテキストが、すべての停止されたサービスが表示されるまで繰り返されます。
%ServiceID%	停止されたサービスの ID。
%TriggerTime%	サービスが停止された日時。
%HighRiskLevelDetections%	検出された相関イベントの数。
%AlertConsole%	Deep Discovery Director (統合モード) 管理コンソールのルールページの URL。
%LastDetectedTime%	前回の検出日時。
%CorrelatedEventsPage%	Deep Discovery Director (統合モード) 管理コンソールの [相関イベント] 画面の URL。
%AttachmentHint%	添付ファイルについてのヒント。
%TotalDetections%	合計検出数。
%HighRiskLevelDetections%	リスクレベルに高が割り当てられたメールメッセージの数。
%MediumRiskLevelDetections%	リスクレベルに中が割り当てられたメールメッセージの数。
%LowRiskLevelDetections%	リスクレベルに低が割り当てられたメールメッセージの数。
%UnavailableRiskLevelDetections%	リスクレベルに使用不可が割り当てられたメールメッセージの数。
%EmailMessagePage%	Deep Discovery Director (統合モード) 管理コンソールの [メールメッセージ] 画面の URL。
%HighSeverityDetections%	重大度レベルに高が割り当てられたネットワーク検出の数。

トークン	説明
%MediumSeverityDetections%	重大度レベルに中が割り当てられたネットワーク検出の数。
%LowSeverityDetections%	重大度レベルに低が割り当てられたネットワーク検出の数。
%InformationalSeverityDetections%	重大度レベルに情報が割り当てられたネットワーク検出の数。
%NetworkDetectionPage%	Deep Discovery Director (統合モード) 管理コンソールの [ネットワーク検出] 画面の URL。
%SuccessLoopStart% %SuccessLoopEnd%	この 2 つのトークンの間にあるテキストが、すべての完了した計画が表示されるまで繰り返されます。
%CompletedPlanName%	完了した計画の名前。
%Detail_page_URL%	Deep Discovery Director (統合モード) 管理コンソールの計画の [詳細] 画面の URL。
%CompletedPlanType%	完了した計画の種類。
%CompletedDateTime%	計画が完了した日時。
%FailedLoopStart% FailedLoopEnd	この 2 つのトークンの間にあるテキストが、すべての失敗した計画が表示されるまで繰り返されます。
%UnsuccessfulPlanName%	失敗した計画の名前。
%UnsuccessfulPlanType%	失敗した計画の種類。
%ApplianceUnsuccessfulNumber%	計画の実行に失敗したアプライアンスの数。

トークン	説明
%ApplianceUnreachableNumber%	到達不能であったアプライアンスの数。
%ApplianceCanceledNumber%	計画がキャンセルされたアプライアンスの数。
%LogPartitionUsage%	ログパーティションの合計使用率。
%FreeLogPartitionSpace%	ログパーティションの空き容量。
%LogPartitionSpaceThreshold%	ディスク空き容量の低下のしきい値。
%StoragePage%	Deep Discovery Director (統合モード) 管理コンソールの [ストレージ] 画面の URL。
%RepositoryUsage%	リポジトリの合計使用率。
%FreeRepositorySpace%	リポジトリの空き容量。
%PageURL%	Deep Discovery Director (統合モード) 管理コンソールの [リポジトリ] 画面の URL。
%FileUploadLoopStart% %FileUploadLoopEnd%	この 2 つのトークンの間にあるテキストが、すべてのファイルアップロードの結果が表示されるまで繰り返されます。
%FileName%	アップロードされたファイルの名前。
%FileType%	アップロードされたファイルの種類。
%UploadResult%	アップロードの結果。
%UploadDateTime%	ファイルがアップロードされた日時。
%RepositoryURL%	Deep Discovery Director (統合モード) 管理コンソールの [リポジトリ] 画面の URL。

トークン	説明
%PlanPageURL%	Deep Discovery Director (統合モード) 管理コンソールの [計画] 画面の URL。

実行されたアラート

[実行されたアラート] 画面には、次の情報が表示されます。

表 7-3. [実行されたアラート] の列

列	情報
実行日時	アラートが実行された日時。
アラートレベル	アラートは次のいずれかのレベルに分類できます。 • 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
種類	アラートを実行するルールの種類は、次のいずれかになります。 • システム: 組み込みのシステム関連のルール • メールセキュリティ: メールセキュリティ関連のルール • ネットワークセキュリティ: ネットワークセキュリティ関連のルール • カスタム: ユーザ指定のカスタムルール • ネットワーク分析: Network Analytics 関連のルール
ルール	アラートを実行したルール。
条件	ルールの条件の概要。 カスタムルールでは、このルールの条件として使用される詳細検索フィルタが表示されます。

列	情報
イベント	実行されたアラートの発生数。数字をクリックすると、[ネットワーク検出] または [メールメッセージ] 画面に詳細が表示されます。 注意 [ネットワーク検出] または [メールメッセージ] 画面に表示されるレコード数が、[実行されたアラート] 画面に表示されるイベント数と異なる場合があります。これは、関連する検出ログが削除されたか、関連する検出があるアプライアンスで次の操作が実行されたためです。 • [非管理対象] グループに移動 • Deep Discovery Director (統合モード) から削除 • Deep Discovery Director (統合モード) から登録解除
詳細	アイコンをクリックすると、アラートの受信者、件名、およびメッセージのリストを含むアラートの詳細が表示されます。

ヒント

リストの表示は、(フィルタ) ボタンをクリックし、表示されるドロップダウンリストや検索ボックスを使用してフィルタできます。

組み込みルール

[組み込みルール] 画面には、次の情報が表示されます。

表 7-4. [組み込みルール] の列

列	情報
アラートレベル	アラートは次のいずれかのレベルに分類できます。 • 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
種類	アラートを実行するルールの種類は、次のいずれかになります。 • システム: 組み込みのシステム関連のルール • メールセキュリティ: メールセキュリティ関連のルール • ネットワークセキュリティ: ネットワークセキュリティ関連のルール • ネットワーク分析: Network Analytics 関連のルール
ルール	アラートを実行するルール。 ルールを編集するには、[ルール] 列のいずれかのリンクをクリックします。
条件	ルールの条件の概要。
アラートの実行間隔	ルール条件を満たしたとき、または超過したときにアラートを生成する間隔。
前回の実行日時	アラートが最後に実行された日時。
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。

組み込みルールを編集する

ルールを編集して、アラートの生成頻度、条件、および受信者を変更します。

注意

- 初期設定で有効化されている組み込みルールでは、有効なメールアドレスを持つすべての連絡先にアラートを送信するように設定されています。
- 条件を変更できるのは、[メールセキュリティ] のルールのみです。

手順

1. [アラート] > [組み込みルール] の順に選択します。

   [組み込みルール] 画面が表示されます。

2. [ルール] 列で、編集するルールの名前をクリックします。

   [ルールの編集] 画面が表示されます。

3. ルールのステータスを切り替えます。

4. アラートを生成する頻度を設定します。

   - 確認頻度: ルール条件の確認の実行間隔を選択します。
   - アラートの実行間隔: ルール条件を満たしたとき、または超過したときにアラートを生成する間隔を選択します。

   注意

   - 間隔が短いとアラートの生成回数は多くなります。間隔を長くすることで、不要なアラートの生成を軽減することができます。
   - システムルールを設定すると、ルール条件が継続的に確認されます。変更できるのは [アラートの実行間隔] のみです。
   - セキュリティおよびカスタムルールを設定すると、ルール条件を満たすか超過したときに、ただちにアラートが生成されます。変更できるのは [確認頻度] のみです。

5. [メールセキュリティ] アラートの場合、次の項目を設定します。

   - 受信者のウォッチリスト: メールアドレスを入力して <Enter> キーを押し、指定したメールアドレスを受信者のウォッチリストに追加します。

- しきい値: 検出数のしきい値を指定します。
- リスクレベル: リスクレベルを選択し、[適用] をクリックします。

6. (オプション) [すべてのアカウントに送信] をオンまたはオフにします。

注意

この設定は、[受信者] フィールドと組み合わせて使用できます。

7. (オプション) 連絡先を選択するか、入力して検索するか、またはメールアドレスを入力して、<Enter> キーを押します。

   連絡先またはアカウントが受信者に追加されます。

8. (オプション) 件名行を変更します。使用可能なトークンが右側に表示されます。トークンをクリックすると、テキストカーソルの位置に挿入できます。

   詳細については、334 ページの「トークン変数」を参照してください。

9. [保存] をクリックします。

ヒント

[初期設定に戻す] をクリックすると、このルールが初期設定値に戻ります。

カスタムルール

[カスタムルール] 画面には、次の情報が表示されます。

表 7-5. [カスタムルール] の列

列	情報
アラートレベル	アラートは次のいずれかのレベルに分類できます。 • 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
種類	アラートを実行するルールの種類は、次のいずれかになります。 • メールセキュリティ: メールセキュリティ関連のルール • ネットワークセキュリティ: ネットワークセキュリティ関連のルール
ルール	アラートを実行するルール。 ルールを編集するには、[ルール] 列のいずれかのリンクをクリックします。
条件	このルールの条件として使用される詳細検索フィルタ。
確認頻度	ルール条件を確認する頻度。
前回の実行日時	アラートが最後に実行された日時。
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。

カスタムルールを追加する

保存された検索条件フィルタに基づくカスタムルールを追加して、特定の脅威に対するアラートを生成します。

注意

最大 500 個のカスタムルールを追加できます。

手順

1. [アラート] > [カスタムルール] の順に選択し、[ルールの追加] をクリックします。

[ルールの追加] 画面が表示されます。

2. ルールのステータスを切り替えます。
3. ルールの名前を入力します。
4. ルールに割り当てるアラートレベルを選択します。
5. [フィルタの選択] をクリックし、ルールの条件として使用する [ネットワーク検出] または [メールメッセージ] の保存された検索条件を選択して、[適用] をクリックします。

重要

ルールの作成後は、選択したフィルタに変更を行っても適用されません。

6. 次のいずれかを実行します。
   - [ネットワーク検出] の保存された検索条件の場合、ルールのデータソースとして含めるアプライアンスを選択します。
   - [メールメッセージ] の保存された検索条件の場合、ルールに含めるメールメッセージのドメインを選択します。
7. ルール条件の確認の実行間隔を選択します。

注意

- 間隔が短いとアラートの生成回数は多くなります。間隔を長くすることで、不要なアラートの生成を軽減することができます。
- カスタムルールを設定すると、ルール条件を満たすか超過したときに、ただちにアラートが生成されます。変更できるのは [確認頻度] のみです。

8. しきい値を指定します。
9. (オプション) ルールの説明を入力します。
10. (オプション) [すべてのアカウントに送信] をオンまたはオフにします。

注意

この設定は、[受信者] フィールドと組み合わせて使用できます。

11. (オプション) 連絡先を選択するか、入力して検索するか、またはメールアドレスを入力して、<Enter> キーを押します。

    連絡先またはアカウントが受信者に追加されます。

12. (オプション) 件名行を変更します。使用可能なトークンが右側に表示されます。トークンをクリックすると、テキストカーソルの位置に挿入できます。

    詳細については、334 ページの「トークン変数」を参照してください。

13. [保存] をクリックします。

カスタムルールのその他のタスク

次のタスクを実行することもできます。

表 7-6. その他のタスク

タスク	説明
ルールの編集	ルール名をクリックして [ルールの編集] 画面を開き、ルールを編集します。 **注意** 条件として使用されている詳細検索フィルタは変更できません。
ルールの削除	削除するルールを 1 つ以上選択して、[削除] をクリックします。
ルールのステータスの切り替え	[ステータス] 列で切り替えスイッチをクリックすると、ルールを有効または無効にできます。

第 8 章

レポート

Deep Discovery Director (統合モード) の予約レポートおよび手動レポートの生成およびアクセス方法については、次の項目を参照してください。

レポートについて

Deep Discovery Director (統合モード) に用意されているレポートを使用すると、複雑な脅威のシナリオを理解し、応答に優先順位を設定して、封じ込めや軽減策を計画することが容易になります。

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。

レポートは、手動または日次、週次、あるいは月次のスケジュールで生成されます。

生成されたレポート

[生成されたレポート] 画面には、次の情報が表示されます。

表 8-1. [生成されたレポート] の列

列	情報
名前	レポートの名前。
種類	レポートの種類は次のいずれかになります。 • メールセキュリティ: Deep Discovery Email Inspector アプライアンスのデータから生成されるレポート • ネットワークセキュリティ: Deep Discovery Inspector アプライアンスのデータから生成されるレポート
実行間隔	レポートの生成頻度は次のいずれかになります。 • 日次 • 週次 • 月次 • 手動
生成	レポートが生成された日時。

列	情報
ダウンロード	アイコンをクリックしてレポートをダウンロードします。

生成されたレポートを表示する

手順

1. [レポート] > [生成されたレポート] の順に選択します。
2. レポートの種類を選択します。
3. 実行間隔を選択します。
4. 期間を選択します。
5. 検索を実行するには、検索テキストボックスにレポート名のキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。
6. (オプション) 列のタイトルをクリックしてリストを並び替えます。
7. [ダウンロード] 列のアイコンをクリックし、PDF 形式でレポートをダウンロードして保存します。

生成されたレポートを削除する

手順

1. [レポート] > [生成されたレポート] の順に選択します。
2. 削除するレポートを 1 つ以上選択して、[削除] をクリックします。

スケジュール

[スケジュール] 画面には、次の情報が表示されます。

表 8-2. [スケジュール] の列

	情報
名前	レポートの名前。
種類	レポートの種類は次のいずれかになります。 • メールセキュリティ: Deep Discovery Email Inspector アプライアンスのデータから生成されるレポート • ネットワークセキュリティ: Deep Discovery Inspector アプライアンスのデータから生成されるレポート
実行間隔	レポートの生成頻度は次のいずれかになります。 • 日次 • 週次 • 月次
説明	レポートの説明。
前回のアップデート	レポートのスケジュールが最後にアップデートされた日時。
最終生成日	レポートが最後に生成された日時。

スケジュールを表示する

手順

1. [レポート] > [スケジュール] の順に選択します。
2. [フィルタ] ボタンをクリックします。

   フィルタのドロップダウンリストと検索ボックスが表示されます。
3. レポートの種類を選択します。
4. 実行間隔を選択します。
5. 検索を実行するには、検索テキストボックスにレポート名のキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。

6. (オプション) 列のタイトルをクリックしてリストを並び替えます。

スケジュールを追加する

手順

1. [レポート] > [スケジュール] の順に選択します。
2. [スケジュールの追加] をクリックします。

   [スケジュールの追加] 画面が表示されます。
3. レポートの種類を選択します。
4. レポートの名前を入力します。
5. 次のいずれかを実行します。
   - [ネットワークセキュリティ] レポートの場合、データソースとして含めるアプライアンスを選択します。
   - [メールセキュリティ] レポートの場合、含めるメールメッセージのドメインを選択します。
6. (オプション) レポートの説明を入力します。
7. (オプション) レポートの表紙上に表示されるメモを入力します。
8. レポート生成の実行間隔を選択します。
   - [日次]: レポートが生成される時刻を選択または入力します。
   - [週次]: レポートが生成される曜日と時刻を選択します。
   - [月次]: 次のいずれかを実行します。
     - [1 か月レポートの場合、毎月 1 日の次の時刻に生成] を選択し、レポートが生成される時刻を選択または入力します。レポート期間は前月の 1 か月間 (1 日～31 日) です。
     - [30 日レポートの場合、次の日に月を開始] を選択し、レポートが生成される日時を選択します。レポート期間は指定した日付以前の 30 日間です (15 日～15 日など)。

> **注意**
>
> 指定した日付 (29、30、または 31) が存在しない場合、レポートは現在の月の最終日に作成されます。

9. レポートの内容を選択します。
   - [ネットワークセキュリティ] レポートの場合:
     a. レポートに含めるホストを選択します。
        - すべてのホストを含める場合は、[すべての監視対象ホスト] を選択します。
        - 特定のホストのみを含める場合は、[フィルタされたホスト] を選択し、[フィルタの選択] をクリックして、条件に [影響を受けたホスト] の保存された検索条件を使用するよう選択し、[適用] をクリックします。
     b. レポートに含める上位のホストの数を選択します。
   - [メールセキュリティ] レポートの場合:
     a. レポートに詳細情報を含めるかどうかを選択します。
     b. レポートに受信または送信メッセージのどちらかのみを含めるか、受信および送信メッセージの両方を含めるかを選択します。
10. (オプション) [すべてのアカウントに送信] をオンまたはオフにします。

> **注意**
>
> この設定は、[受信者] フィールドと組み合わせて使用できます。

11. (オプション) アカウントを選択するか、入力して検索するか、またはメールアドレスを入力して <Enter> キーを押します。

    アカウントまたはメールアドレスが受信者に追加されます。
12. (オプション) 件名行を変更します。使用可能なトークンが右側に表示されます。トークンをクリックすると、テキストカーソルの位置に挿入できます。

13. [保存] をクリックします。

スケジュールを編集する

手順

1. [レポート] > [スケジュール] の順に選択します。
2. 編集するレポートの名前をクリックします。

   [編集スケジュール] 画面が表示されます。
3. 設定を変更します。
4. [保存] をクリックします。

スケジュールを削除する

手順

1. [レポート] > [スケジュール] の順に選択します。
2. 削除するスケジュールを 1 つ以上選択して、[削除] をクリックします。

手動

必要に応じて 1 回限りのレポートを生成します。手動レポートはただちに生成され、生成直後に表示可能になります。

手動レポートを生成する

手順

1. [レポート] > [手動] の順に選択します。
2. レポートの種類を選択します。
3. レポートの名前を入力します。
4. 次のいずれかを実行します。
   - [ネットワークセキュリティ] レポートの場合、データソースとして含めるアプライアンスを選択します。
   - [メールセキュリティ] レポートの場合、含めるメールメッセージのドメインを選択します。
5. (オプション) レポートの表紙上に表示されるメモを入力します。
6. レポートの期間を選択します。
7. レポートの内容を選択します。
   - [ネットワークセキュリティ] レポートの場合:
     a. レポートに含めるホストを選択します。
        - すべてのホストを含める場合は、[すべての監視対象ホスト] を選択します。
        - 特定のホストのみを含める場合は、[フィルタされたホスト] を選択し、[フィルタの選択] をクリックして、条件に [影響を受けたホスト] の保存された検索条件を使用するよう選択し、[適用] をクリックします。

     b. レポートに含める上位のホストの数を選択します。
   - [メールセキュリティ] レポートの場合:
     a. レポートに詳細情報を含めるかどうかを選択します。
     b. レポートに受信または送信メッセージのどちらかのみを含めるか、受信および送信メッセージの両方を含めるかを選択します。

8. (オプション) [すべてのアカウントに送信] をオンまたはオフにします。

   注意

   この設定は、[受信者] フィールドと組み合わせて使用できます。

9. (オプション) アカウントを選択するか、入力して検索するか、またはメールアドレスを入力して <Enter> キーを押します。

   アカウントまたはメールアドレスが受信者に追加されます。

10. (オプション) 件名行を変更します。使用可能なトークンが右側に表示されます。トークンをクリックすると、テキストカーソルの位置に挿入できます。

11. [生成] をクリックします。

    新しい手動レポートが [生成されたレポート] 画面に表示されます。

カスタマイズ

[カスタマイズ] 画面を使用して、レポートの表紙オプションを設定します。

レポートをカスタマイズする

手順

1. [レポート] > [カスタマイズ] の順に選択します。
2. 会社名を入力します。
3. 会社のロゴを表示するには、[会社のロゴの表示] を選択し、[ファイルの選択] をクリックしてイメージファイルを指定します。

   注意

   イメージファイルは JPEG または PNG 形式で、ファイルサイズは 200KB 以内で指定する必要があります。

4. (オプション) レポートの表紙ページにトレンドマイクロのロゴを表示させないようにするには、[トレンドマイクロのロゴを表示する] チェックボックスをオフにします。
5. [保存] をクリックします。

第 9 章

管理

Deep Discovery Director (統合モード) の管理方法については、次の項目を参照してください。

アップデート

[管理] > [アップデート] にある [アップデート] 画面を使用して、コンポーネントをアップデートしたり、HotFix、Patch、およびファームウェアのアップグレードを Deep Discovery Director (統合モード) にインストールしたりします。

コンポーネント

Deep Discovery Director (統合モード) ではコンポーネントを使用して、検出についての関連情報を表示します。トレンドマイクロでは、最新の脅威に対応するためにコンポーネントの新しいバージョンを高い頻度で作成しています。

Deep Discovery Director (統合モード) では、[コンポーネント] 画面が開かれるたびに新しいコンポーネントが入手可能かどうかを自動的に確認します。

コンポーネントをアップデートする

コンポーネントはいつでも手動でアップデートできます。

手順

1. [管理] > [アップデート] > [コンポーネント] の順に選択します。

   [コンポーネント] 画面が表示されます。

2. [すべてアップデート] をクリックします。

コンポーネントのアップデートを設定する

コンポーネントを自動的にアップデートするように Deep Discovery Director (統合モード) を設定します。

手順

1. [管理] > [アップデート] > [コンポーネント] の順に選択します。

   [コンポーネント] 画面が表示されます。

2. [設定] をクリックします。

   [コンポーネントのアップデート設定] 画面が表示されます。

3. アップデートのダウンロード元を選択します。

   - トレンドマイクロのアップデートサーバ: トレンドマイクロのアップデートサーバは、最新コンポーネントを取得する初期設定のアップデート元です。
   - その他のアップデートサーバ: 別のアップデート元を指定する場合は、このオプションを選択します。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。

4. [アップデートを自動的に確認] を選択します。

5. 数時間おきにアップデートするか、毎日指定した時刻にアップデートするかを選択します。

   ヒント

   アップデートの頻度は 2 時間間隔で設定することをお勧めします。

6. [保存] をクリックします。

HotFix/Patch

[管理] > [アップデート] > [HotFix/Patch] にある [HotFix/Patch] 画面を使用して、Deep Discovery Director (統合モード) の HotFix と Patch をインストールします。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 9-1. 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。
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。

https://downloadcenter.trendmicro.com/

HotFix/Patch をインストールする

手順

1. HotFix や Patch などのアップデート用ファイルを入手します。
2. [管理] > [アップデート] > [HotFix/Patch] の順に選択します。

   [HotFix/Patch] 画面が表示されます。
3. [ファイルの選択] 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. [アップロード] をクリックします。
5. [インストール] をクリックします。

重要

- インストールした一部のアップデートはロールバックできません。
- アップデートが完了するまで、ブラウザの終了、表示の更新、別のページへの移動、管理コンソールでタスクの実行、アプライアンスの電源をオフなどを行わないでください。

アップデートの完了に必要な場合、Deep Discovery Director (統合モード) はアップデートをインストールした後、自動的に再起動します。

6. 管理コンソールにログオンします。
7. [管理] > [アップデート] 画面に戻ります。
8. 適用した HotFix/Patch が最新のアップデートとして [履歴] に表示されることを確認します。

HotFix/Patch をロールバックする

Deep Discovery Director (統合モード) 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

ロールバックの完了に必要な場合、Deep Discovery Director (統合モード) は HotFix または Patch をロールバックした後、自動的に再起動します。ロールバックを実行する前に、管理コンソールのすべてのタスクが完了していることを確認してください。

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。

   ロールバックの完了に必要な場合、Deep Discovery Director (統合モード) は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. HotFix または Patch のロールバックが、[履歴] 画面の最新のエントリに表示されていることを確認します。

ファームウェア

[管理] > [アップデート] > [ファームウェア] にある [ファームウェア] 画面を使用して、Deep Discovery Director (統合モード) のアップグレードをインストールします。トレンドマイクロの各アップグレードには Readme ファイルが用意されています。アップグレードをインストールする前に付属する 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。

ファームウェアのアップグレードをインストールする

手順

1. [管理] > [アップデート] > [ファームウェア] の順に選択します。

   [ファームウェア] 画面が表示されます。
2. [ファイルの選択] 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。
3. [アップロード] をクリックします。
4. [インストール] をクリックします。

重要

- Deep Discovery Director (統合モード) では、ライセンスのステータスが [アクティベート未完了] または [有効期限切れ] の場合、ファームウェアのアップグレードをインストールできません。
- インストールしたファームウェアのアップグレードはロールバックできません。
- 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、サーバ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 Director (統合モード) 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] > [ファームウェア] 画面に戻ります。
7. ファームウェアのバージョンが正しいことを確認します。

統合製品/サービス

Deep Discovery Director (統合モード) は、他の製品やサービスと統合されます。

Apex Central

Apex Central は、ウイルス対策プログラムおよびコンテンツセキュリティプログラムを、その物理的な場所やプラットフォームにかかわらず一元管理するためのソフトウェア管理ソリューションです。このアプリケーションによって、企業のウイルス対策ポリシーおよびコンテンツセキュリティポリシーの管理が簡素化されます。

重要

- Deep Discovery Director (統合モード) はエンドポイント分析レポートを取得する目的で Apex Central と統合され、より多くのデータを Deep Discovery Director - Network Analytics に提供することで詳細かつ高度な脅威分析を可能にします。
- Deep Discovery アプライアンスの管理と脅威インテリジェンスの共有は、Deep Discovery Director (統合モード) により継続して行われます。

[Apex Central] 画面には、次の情報が表示されます。

フィールド	情報
サーバの種類	Deep Discovery Director (統合モード) は Apex Central のオンプレミスバージョンまたは Software as a Service バージョンと統合できます。 **注意** プロキシ設定が有効な場合、Deep Discovery Director (統合モード) ではプロキシサーバを使用して Apex Central as a Service に接続します。
ステータス	[Apex Central に接続されています]、[Apex Central に接続されていません]、または [N/A] のいずれかが表示されます。
前回の接続	Deep Discovery Director (統合モード) が Apex Central に最後に接続した日時が表示されます。
Endpoint Sensor ライセンス	[アクティベートされています] または [アクティベートされていません] のいずれかが表示されます。
Apex Central サーバアドレス	Apex Central のサーバアドレス。
ポート	Apex Central のポート。
アプリケーション ID	Apex Central 管理コンソールで Deep Discovery Director (統合モード) 用に生成されたアプリケーション ID。
API キー	Apex Central 管理コンソールで Deep Discovery Director (統合モード) 用に生成された API キー。

Apex Central を設定する

手順

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

   [Apex Central] 画面が表示されます。

2. [Apex Central からエンドポイント分析レポートを取得します] を選択します。

   重要

   - Apex Central 管理コンソールで、[運用管理] > [設定] > [オートメーション API のアクセス設定] の順に選択し、Deep Discovery Director (統合モード) をアプリケーションとして追加します。
   - この機能を有効にするには、Apex Central で Endpoint Sensor を設定する必要があります。

3. [サーバの種類] を選択します。
4. Apex Central サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
5. Apex Central サーバのポートを入力します。
6. Apex Central 管理コンソールで Deep Discovery Director (統合モード) 用に生成されたアプリケーション ID を入力します。
7. Apex Central 管理コンソールで Deep Discovery Director (統合モード) 用に生成された API キーを入力します。
8. (オプション) [接続テスト] をクリックします。
9. [保存] をクリックします。

Microsoft Active Directory

[Microsoft Active Directory] 画面を使用して、Microsoft Active Directory サーバを Deep Discovery Director (統合モード) と統合します。その後、Deep

Discovery Director (統合モード) で、管理コンソールにアクセス可能なアカウントのリストに Active Directory アカウントを追加できます。

Microsoft Active Directory を設定する

手順

1. サーバ管理者から Microsoft Active Directory との統合設定に必要な情報を取得します。
2. [管理] > [統合製品/サービス] > [Microsoft Active Directory] の順に選択します。
3. 統合するサーバの種類を選択します。
   - Microsoft Active Directory
   - Microsoft Active Directory グローバルカタログ
4. サーバのアドレスを入力します。
5. 暗号化方式を入力します。
   - SSL
   - STARTTLS
6. ポート番号を入力します。

注意

次の初期設定のポートを使用することをお勧めします。

- Microsoft Active Directory の場合:
  - SSL: 636
  - STARTTLS: 389
- Microsoft Active Directory グローバルカタログの場合:
  - SSL: 3269
  - STARTTLS: 3268

7. 基本識別名を入力します。
8. ユーザ名を入力します。
9. パスワードを入力します。
10. (オプション) [接続テスト] をクリックして、Microsoft Active Directory サーバへの接続を確認します。
11. (オプション) 組織で CA 証明書を使用する場合は、[CA 証明書を使用] を選択し、[選択] をクリックして CA 証明書ファイルを指定します。
12. [保存] をクリックします。

SAML 認証

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 Director (統合モード) 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 Director (統合モード) アカウントなしで Deep Discovery Director (統合モード) 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 Director (統合モード)) 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 Director (統合モード) は、シングルサインオンに対応する次の ID プロバイダをサポートしています。

- Microsoft Active Directory フェデレーションサービス (AD FS) 4.0 または 5.0
- Okta

組織の環境に Deep Discovery Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) で証明書を更新することもできます。

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. 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 Director (統合モード) で、次の手順を実行します。

   a. ID プロバイダのメタデータファイルをインポートします。

   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 Director (統合モード) 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 Director (統合モード) 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 (ADFS) にインポートできます。

  注意

  ID プロバイダにメタデータファイルをインポートした後に Deep Discovery Director (統合モード) の完全修飾ドメイン名を変更した場合、再度メタデータファイルをダウンロードして ID プロバイダにインポートする必要があります。

- 証明書のダウンロード: Deep Discovery Director (統合モード) の証明書ファイルをダウンロードします。
- アップデート: 新しい証明書を Deep Discovery Director (統合モード) にアップロードします。証明書は次の仕様を満たしている必要があります。
  - X.509 PEM 形式である。
  - パスワードまたはパスフレーズで保護されていない。
  - プライベート CA または CA チェーンの証明書に [AIA (authority information access)] と [CRL 配布点] が含まれている。

ID プロバイダの設定

注意

- ID プロバイダを追加する前に、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 Director (統合モード) 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。

- 表の上にあるドロップダウンボックスから、ID プロバイダを追加または表示するには [カスタム ID プロバイダ] を、Vision One 用に使用されている内部 ID プロバイダを表示するには [内部 ID プロバイダ] を選択します。

  注意

  このドロップダウンボックスは、Deep Discovery Director (統合モード) が Vision One に統合されている場合にのみ表示されます。

- [追加] をクリックして新しいエントリを追加します。
- ID プロバイダのサービス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 Director (統合モード) では、[ログオン] 画面のドロップダウンリストにサービス名が表示されます。

5. 説明を入力します。
6. [選択] をクリックし、ID プロバイダから取得したメタデータファイルを選択します。

   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 Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) 」など Deep Discovery Director (統合モード) 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. Deep Discovery Director (統合モード) の [Single sign on URL] を入力します。

      注意

      Deep Discovery Director (統合モード) のシングルサインオン URL を取得するには、Deep Discovery Director (統合モード) 管理コンソールで [管理] > [統合製品/サービス] > [SAML 統合] の順に選択し、[サービスプロバイダ] セクションの [シングルサインオン URL] をコピーします。

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. [Name ID format] に「`EmailAddress`」と入力します。

e. [Group Attribute Statements (Optional)] セクションで、次のように指定します。

- Name: `DDD_GROUP`
- Filter: Matches `^(.*)*$`

f. [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 Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) へのアクセスを許可するユーザを指定し、Deep Discovery Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) と連動させる方法について説明します。

注意

Deep Discovery Director (統合モード) 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 Director (統合モード) 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 Director (統合モード) からメタデータファイルを取得している。
- Windows 統合認証がフェデレーションサーバで有効になっている。

  詳細については、376 ページの「AD FS で Windows 統合認証を有効にする」を参照してください。
- 各エンドポイントで Web ブラウザが Deep Discovery Director (統合モード) 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、378 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 Director (統合モード) 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 Director (統合モード) 」など Deep Discovery Director (統合モード) 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] を選択し、[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。

6. [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。

7. [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 [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。

b. [要求規則名] で、Active Directory グループの名前を入力します。

c. [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。

d. [出力方向の要求の種類] に「`DDD_GROUP`」と入力します。

e. [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。

f. [適用]、[OK] の順にクリックします。

8. シングルサインオン URL を収集し、AD FS 用の ID プロバイダメタデータをエクスポートします。

a. AD FS 管理コンソールで、[AD FS] > [サービス] > [エンドポイント] の順に選択します。

b. 右側のペインの [エンドポイント] > [メタデータ] の下にある [フェデレーション メタデータ] 行で、URL パスをコピーします。

c. コピーした URL に AD FS コンピュータのホスト名を追加します。

例: `https://hostname/FederationMetadata/2007-06/FederationMetadata.xml`

d. ID プロバイダのメタデータを取得するには、前の手順で取得した完全な URL に Web ブラウザを使用して移動します。

e. ID プロバイダのメタデータファイルを XML ファイルとして保存します。

注意

このメタデータファイルを Deep Discovery Director (統合モード) にインポートします。

AD FS で Windows 統合認証を有効にする

Windows 統合認証 (WIA) を使用すると、エンドポイントへのサインオンに使用したドメインアカウント情報を使用して Deep Discovery Director (統合モード) にシングルサインオンできるようになります。

手順

1. AD FS 4.0 または AD FS 5.0 がインストールされている Windows Server にログオンします。

2. [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。
3. 左側のナビゲーションで [AD FS] > [サービス] > [認証方法] を選択し、右側の [操作] 領域にある [プライマリ認証方法の編集] をクリックします。
4. [プライマリ] タブの [イントラネット] で、[Windows 認証] が有効になっていることを確認します。
5. [OK] をクリックします。
6. [ドメイン コントローラー] にログオンします。
7. [スタート] > [すべてのプログラム] > [管理ツール] > [グループ ポリシーの管理] の順に選択します。
8. [ユーザーの構成] > [ポリシー] > [管理用テンプレート] > [Windows コンポーネント] > [Internet Explorer] > [インターネット コントロール パネル] > [セキュリティ ページ] の順に選択します。
9. [サイトとゾーンの割り当て一覧] をダブルクリックして設定を行います。
10. [有効] を選択します。
11. [オプション] で [表示] をクリックします。
12. Deep Discovery Director (統合モード) 管理コンソールの URL を [値の名前] に追加し、[値] を「1」に設定します。
13. [OK] をクリックします。

    Deep Discovery Director (統合モード) 管理コンソールの URL が [イントラネット ゾーン] に追加されます。
14. [ユーザーの構成] > [ポリシー] > [管理用テンプレート] > [Windows コンポーネント] > [Internet Explorer] > [インターネット コントロール パネル] > [セキュリティ ページ] > [イントラネット ゾーン] の順に選択します。
15. [ログオンのオプション] をダブルクリックして設定を行います。
16. [有効] を選択します。
17. [オプション] で、[現在のユーザー名とパスワードで自動的にログオンする] をクリックします。

18. [OK] をクリックします。

    これにより、現在のユーザ名とパスワードを使用して、Web ブラウザから Deep Discovery Director (統合モード) 管理コンソールに自動的にログオンできるようになります。

19. 更新されたグループポリシーをエンドポイントに配信します。

    注意

    グループポリシーの配信が Windows ファイアウォールによってブロックされる場合は、配信を許可するインバウンドルールを追加し、エンドポイントの管理者コマンドプロンプトで `gpudate /force` を実行して、エンドポイントに新しいファイアウォールポリシーを受け入れるように強制します。

    ドメインアカウント情報を使用してエンドポイントにサインオンしたユーザは、Deep Discovery Director (統合モード) にシングルサインオンできるようになります。

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 Director (統合モード) にアクセスするには、Deep Discovery Director (統合モード) 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 Director (統合モード) 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。

Syslog

[Syslog] 画面を使用して、Deep Discovery Director (統合モード) から最大 3 つの Syslog サーバに不審オブジェクトのリストと Deep Discovery アプライアンスのログを送信するように設定します。

Syslog サーバプロファイルを追加する

手順

1. [管理] > [統合製品/サービス] > [Syslog] の順に選択し、[追加] をクリックします。

   [Syslog サーバのプロファイルの追加] ダイアログが表示されます。
2. サーバプロファイルのステータスを選択します。
3. Syslog サーバの一意のプロファイル名を入力します。

4. Syslog サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
5. (オプション) ポート番号を変更します。

   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。

   - SSL/TLS: 6514
   - TCP: 601
   - UDP: 514

6. ログコンテンツを Syslog サーバに転送する際に使用するプロトコルを選択します。
7. Syslog サーバに送信するデータの範囲を選択します。
8. [保存] をクリックします。

Syslog のその他のタスク

次のタスクを実行することもできます。

タスク	説明
Syslog サーバプロファイルの編集	サーバプロファイル名をクリックして [Syslog サーバのプロファイルの編集] ダイアログを開き、次の操作を実行します。 • ステータスの切り替え • プロファイル名の変更 • サーバアドレスの変更 • ポート番号の変更 • プロトコルの変更 **注意** サーバアドレスまたはプロトコルを変更すると、すべての不審オブジェクトリストが再送信されます。

タスク	説明
Syslog サーバプロファイルの削除	削除する Syslog サーバプロファイルを 1 つ以上選択して、[削除] をクリックします。 **注意** キューにある検出とアプライアンスのログは破棄され、削除された Syslog サーバには送信されません。
Syslog サーバプロファイルのステータスの切り替え	[ステータス] 列で切り替えスイッチをクリックすると、Syslog サーバプロファイルを有効または無効にできます。 **注意** サーバのプロファイルを無効にすると、キューにある検出とアプライアンスのログは破棄されます。

Trend Micro Vision One

Trend Micro Vision One は、環境内のネイティブセンサから収集したアクティビティデータに最も効果的な AI と専門家の分析を適用し、発生するアラートが忠実度の高いものに絞られるようにします。Trend Micro Smart Protection Network™のグローバルな脅威インテリジェンスと、脅威の専門家が継続的に更新する検出ルールを組み合わせることで、AI および分析モデルの能力を他にはない方法で最大限に活用できます。

Trend Micro Vision One は、メール、エンドポイント、サーバ、クラウドワークロード、およびネットワーク全体からデータを収集して相互に関連付けます。これにより、他では実現が困難なまたは不可能な可視性と分析が可能になります。

より多くのコンテキストを集めることで、それ自体は無害に見えるイベントが突然、重要な意味のある侵害の兆候になることがあり、影響をすばやく封じ込めて、重大度と範囲を最小限に抑えることができます。

重要

- Trend Micro Vision One にアクティビティデータを送信するには、Deep Discovery アプライアンスを Deep Discovery Director (統合モード) に登録する必要があります。
- [Trend Micro Vision One] 画面を利用するには、Deep Discovery Director - Network Analytics as a Service ライセンスをアクティベートする必要があります。

ステータス

[管理] > [Trend Micro Vision One] > [ステータス] にある [ステータス] 画面を使用して、Deep Discovery Director (統合モード) の Trend Micro Vision One の統合ステータスを確認します。

[ステータス] 画面には、次の情報およびオプションが含まれます。

フィールド	詳細
ステータス	[登録済み | 接続済み]、[登録済み | 接続なし]、または [未登録] のいずれかが表示されます。 **注意** プロキシ設定が有効な場合、Deep Discovery Director (統合モード) ではプロキシサーバを使用して Trend Micro Vision One に接続します。
前回の接続	Deep Discovery Director (統合モード) が最後に Trend Micro Vision One に接続した日時。
Network Analytics as a Service	Deep Discovery Director - Network Analytics as a Service が Trend Micro Vision One に登録されている場合、[Trend Micro Vision One に登録済み] と表示されます。

接続済みソース

[管理] > [Trend Micro Vision One] > [接続済みソース] にある [接続済みソース] 画面を使用して、アクティビティデータを Trend Micro Vision One に送信

する Deep Discovery Inspector アプライアンスを表示し、Deep Discovery Inspector アプライアンスが Trend Micro Vision One への接続にそれぞれのプロキシ設定を使用するかどうかを設定します。

[接続済みソース] 画面には、次の情報が表示されます。

表 9-2. [接続済みソース] の列

列	情報
表示名	Deep Discovery Inspector アプライアンスの表示名。
ステータス	[登録済み] または [未登録] のいずれかが表示されます。
前回送信されたデータ	Deep Discovery Inspector アプライアンスが Trend Micro Vision One に最後にデータを送信した日時。
ホスト名	Deep Discovery Inspector アプライアンスのホスト名。
IP アドレス	Deep Discovery Inspector アプライアンスの IP アドレス。
バージョン	Deep Discovery Inspector アプライアンスのバージョン。

ネットワーク分析

Deep Discovery Director - Network Analytics の提供する高度な脅威分析には、Deep Discovery Director (統合モード) で選択した検出とその他の関連イベントとのデータの関連付けが時間の経過に従って表示されます。

Deep Discovery Director - Network Analytics は、Deep Discovery Director (統合モード) および Deep Discovery Inspector と統合された透過的ソリューションであり、ネットワークを脅かすサイバー脅威やサイバー攻撃に対する高度な保護を提供します。

[管理] > [ネットワーク分析] にある [ネットワーク分析] 画面を使用して、Deep Discovery Director - Network Analytics のステータスを表示したり、データソースを設定したりします。

設定を追加して Deep Discovery Director - Network Analytics を最大限活用するには、[アプライアンス] > [ネットワーク資産] の順に選択します。

詳細については、290 ページの「ネットワーク資産」を参照してください。

注意

Deep Discovery Director (統合モード) は、Deep Discovery Director - Network Analytics のオンプレミスバージョンまたは SaaS (Software as a Service) バージョンとのみ統合できます。Deep Discovery Director (統合モード) と統合するバージョンに応じて、使用可能な管理コンソール画面がわずかに異なります。

オンプレミス固有の画面

Deep Discovery Director (統合モード) を Deep Discovery Director (Standalone Network Analytics モード)で動作する Deep Discovery Director (Internal Network Analytics バージョン)サーバと統合すると、管理コンソールに次の設定画面が表示されます。

サーバ情報

[管理] > [ネットワーク分析] > [サーバ情報] にある [サーバ情報] 画面を使用して、登録済みのすべての Deep Discovery Director - Network Analytics サーバのステータスと基本情報を表示します。

データソース

[管理] > [ネットワーク分析] > [データソース] にある [データソース] 画面を使用して、Deep Discovery Director (統合モード) による高度な脅威分析のデータの取得元となる Deep Discovery Inspector アプライアンスを表示および設定します。

[データソース] 画面には、次の情報が表示されます。

表 9-3. [データソース] の列

列	情報
表示名	Deep Discovery Inspector アプライアンスの表示名。
ホスト名	Deep Discovery Inspector アプライアンスのホスト名。

列	情報
IP アドレス	Deep Discovery Inspector アプライアンスの IP アドレス。
接続済み Network Analytics	接続済みの Deep Discovery Director - Network Analytics サーバの表示名。
接続ステータス	Deep Discovery Director - Network Analytics サーバの接続ステータス。
バージョン	Deep Discovery Inspector アプライアンスのバージョン。
アプライアンスのプロキシの設定	Deep Discovery Inspector アプライアンスのプロキシの設定が使用されているかどうかに応じて、[有効] または [無効] のいずれかが表示されます。
帯域幅	Deep Discovery Inspector アプライアンスによって使用されている帯域幅。
最終同期日	データが Deep Discovery Inspector アプライアンスと最後に同期された日時。
接続テスト	Deep Discovery Inspector アプライアンスが Deep Discovery Director - Network Analytics as a Service への接続を確立した日時。 Deep Discovery Inspector アプライアンスから Deep Discovery Director - Network Analytics as a Service への接続を試みるには、[接続テスト] をクリックします。

データソースを設定する

手順

1. [管理] > [ネットワーク分析] > [データソース] の順に選択します。

   [データソース] 画面が表示されます。

2. アプライアンスを 1 つ以上選択して、[設定] をクリックします。

3. 次のいずれかを選択します。

   - 個別: 各 Deep Discovery Inspector アプライアンスを個別に設定します。
   - 一括: 選択したすべての Deep Discovery Inspector アプライアンスをまとめて設定します。

   [データソースの設定] ダイアログが表示されます。

4. データソースを設定します。

   - 個別:

     a. 各 Deep Discovery Inspector アプライアンスの接続先の Network Analytics サーバを選択します。

     b. 各 Deep Discovery Inspector アプライアンスのプロキシ設定を使用するかどうか選択します。

   - 一括:

     a. 現在の接続をすべて保持するか、すべての Deep Discovery Inspector アプライアンスの接続先の Network Analytics サーバを指定するかを選択します。

     b. すべての Deep Discovery Inspector アプライアンスのプロキシ設定を保持するか、有効にするか、または無効にするかを選択します。

5. [保存] をクリックします。

   すべての設定がすべてのアプライアンスにただちに適用されます。以前の設定が適用されるまで、追加の設定は実行できません。

Software as a Service 固有の画面

Deep Discovery Director (統合モード) を Deep Discovery Director - Network Analytics as a Service と統合すると、管理コンソールに次の設定画面が表示されます。

ステータス

[管理] > [ネットワーク分析] > [ステータス] にある [ステータス] 画面を使用して、Deep Discovery Director (統合モード) の登録と Deep Discovery Director - Network Analytics as a Service への接続ステータスの表示および接続テストを行います。また、不審オブジェクトと除外が Deep Discovery Director - Network Analytics as a Service と同期された日時を表示します。

[ステータス] 画面には、次の情報およびオプションが含まれます。

フィールド	詳細
ステータス	[登録済み | 接続済み]、[登録済み | 接続なし]、または [未登録] のいずれかが表示されます。 Deep Discovery Director (統合モード) が自動的に Deep Discovery Director - Network Analytics as a Service に接続できなかった場合、[再試行] ハイパーリンクが表示されます。 注意 プロキシ設定が有効な場合、Deep Discovery Director (統合モード) ではプロキシサーバを使用して Deep Discovery Director - Network Analytics as a Service に接続します。
前回の接続	Deep Discovery Director (統合モード) が Deep Discovery Director - Network Analytics as a Service に最後に接続した日時。
帯域幅	使用可能な帯域幅。使用可能な帯域幅は、Deep Discovery Director - Network Analytics as a Service のライセンスによって決まります。
データ保持	相関データが保持される日数。この数値は、Deep Discovery Director - Network Analytics as a Service のライセンスによって決まります。
接続テスト	Deep Discovery Director - Network Analytics as a Service への接続を試みるには、[接続テスト] をクリックします。
同期された不審オブジェクト	同期された不審オブジェクトが Deep Discovery Director - Network Analytics as a Service と最後に同期された日時。
ユーザ指定の不審オブジェクト	ユーザ指定の不審オブジェクトが Deep Discovery Director - Network Analytics as a Service と最後に同期された日時。

フィールド	詳細
除外	除外が Deep Discovery Director - Network Analytics as a Service と最後に同期された日時。

接続済みソース

[管理] > [ネットワーク分析] > [接続済みソース] にある [接続済みソース] 画面を使用して、Deep Discovery Director - Network Analytics as a Service による高度な脅威分析のデータの取得元となる Deep Discovery Inspector アプライアンスを表示および設定します。

[接続済みソース] 画面には、次の情報が表示されます。

表 9-4. [接続済みソース] の列

列	情報
ステータス	切り替えスイッチをクリックすると、Deep Discovery Inspector アプライアンスをデータソースとして有効または無効にできます。
表示名	Deep Discovery Inspector アプライアンスの表示名。
ホスト名	Deep Discovery Inspector アプライアンスのホスト名。
IP アドレス	Deep Discovery Inspector アプライアンスの IP アドレス。
バージョン	Deep Discovery Inspector アプライアンスのバージョン。
アプライアンスのプロキシの設定	Deep Discovery Inspector アプライアンスのプロキシの設定が使用されているかどうかに応じて、[有効] または [無効] のいずれかが表示されます。
帯域幅	Deep Discovery Inspector アプライアンスによって使用されている帯域幅。

列	情報
最終同期日	データが Deep Discovery Inspector アプライアンスと最後に同期された日時。
接続テスト	Deep Discovery Inspector アプライアンスが Deep Discovery Director - Network Analytics as a Service への接続を確立した日時。 Deep Discovery Inspector アプライアンスから Deep Discovery Director - Network Analytics as a Service への接続を試みるには、[接続テスト] をクリックします。

接続済みソースを設定する

手順

1. [管理] > [ネットワーク分析] > [接続済みソース] の順に選択します。

   [接続済みソース] 画面が表示されます。

2. アプライアンスを 1 つ以上選択して、[設定] をクリックします。

   [接続済みソースの設定] ダイアログが表示されます。

3. [ステータス] 列で切り替えスイッチをクリックすると、Deep Discovery Inspector アプライアンスをデータソースとして有効または無効にできます。

   重要

   - 有効にできる Deep Discovery Inspector アプライアンスの数に制限はありませんが、[帯域幅] の合計は、使用可能な [帯域幅の容量] 以下になるようにしてください。
   - 使用可能な帯域幅は、Deep Discovery Director - Network Analytics as a Service のライセンスによって決まります。

4. Deep Discovery Inspector アプライアンスのプロキシの設定を使用するかどうか選択します。

5. [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、次の項目があります。

ネットワーク

この画面を使用して、Deep Discovery Director (統合モード) アプライアンスのホスト名または完全修飾ドメイン名、IP アドレス、およびその他のネットワーク設定を行います。

IP 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。

注意

事前設定コンソールを使用してネットワーク設定を変更することもできます。

詳細については、31 ページの「ネットワークを設定する」を参照してください。

重要

- Deep Discovery Director (統合モード) 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。
- IP アドレスを変更すると次のようになります。
  - 登録済みの Deep Discovery アプライアンスは、アップデートされた IP アドレスで再登録する必要があります。
  - Deep Discovery Director (統合モード) の脅威インテリジェンスの共有 URL を使用する製品とサービスは、アップデートされた URL を使用するように設定する必要があります。
  - Deep Discovery と統合する製品とサービスは、アップデートされた IP アドレスを使用するように設定する必要があります。
  - Web API を使用して Deep Discovery Director (統合モード) にアクセスする製品とサービスは、アップデートされた IP アドレスを使用するように設定する必要があります。

ホスト名を ID として使用する

Deep Discovery Director (統合モード) では、サーバの識別に IP アドレスではなくホスト名を使用できます。

この機能を選択すると、アプライアンスはホスト名を使用して Deep Discovery Director (統合モード) に接続し、計画の実行に必要なファイルをダウンロードします。

重要

- ホスト名はネットワーク内で解決可能である必要があります。
- ホスト名を変更すると次の影響があります。
  - 登録済みの Deep Discovery アプライアンスは、アップデートされたホスト名で再登録する必要があります。
  - Deep Discovery Director (統合モード) の脅威インテリジェンスの共有 URL を使用する製品とサービスは、アップデートされた URL を使用するように設定する必要があります。
  - Deep Discovery と統合する製品とサービスは、アップデートされたホスト名を使用するように設定する必要があります。
  - Web API を使用して Deep Discovery Director (統合モード) にアクセスする製品とサービスは、アップデートされたホスト名を使用するように設定する必要があります。

手順

1. [この Deep Discovery Director の識別に IP アドレスではなくホスト名を使用する] を選択します。
2. IP アドレスやその他のネットワーク設定を行います。
3. [保存] をクリックします。

ポートバインディングを設定する

Deep Discovery Director (統合モード) では、サービスをセカンドネットワークポートにバインディングできます。

この機能を選択すると、すべての接続が eth1 経由で脅威インテリジェンスフィード、ライセンスアップデートサーバ、およびアップデートサーバに転送されます。

注意

この機能は事前設定コンソールからは設定できません。

手順

1. [サービスのバインド先] で、サービスをバインドする [eth0 (管理) と eth1] を選択します。

   重要

   この機能を使用するには、2 つ以上のネットワークインタフェースカードを取り付けて設定する必要があります。そうでない場合、この機能は [ネットワーク] 画面に表示されません。

   既存の [eth0 (管理)] の下に、セカンドネットワークポートのネットワーク設定を行うための新しい [eth1] が表示されます。

2. セカンドネットワークポートの IP アドレスやその他のネットワーク設定を行います。

3. [保存] をクリックします。

IPv4 と IPv6 のデュアルスタックを使用する

Deep Discovery Director (統合モード) では、IPv6 プロトコルで通信するネットワーク環境での動作を可能にする、IPv4 と IPv6 のデュアルスタック設定がサポートされます。

手順

1. [種類] に [IPv4 および IPv6 (デュアルスタック)] を選択します。

   IPv6 の設定を行う新しいセクションが、既存の IPv4 と DNS の設定の間に表示されます。

2. IPv6 の設定を行います。

3. [保存] をクリックします。

プロキシ

プロキシサーバを使用してインターネットに接続するよう Deep Discovery Director (統合モード) を設定できます。プロキシサーバを使用して、次の機能/サービスに接続することもできます。

- Trend Micro Vision One
- Deep Discovery Director - Network Analytics as a Service
- Apex Central as a Service
- Threat Connect
- Trend Micro Email Encryption サーバ
- 脅威インテリジェンスフィード
- ライセンスアップデートサーバ
- アップデートサーバ

注意

ポートバインディングが設定されている場合、eth1 のみでプロキシ設定を使用します。

手順

1. [管理] > [システム設定] > [プロキシ] の順に選択します。

   [プロキシ] 画面が表示されます。

2. [プロキシサーバを使用してインターネットに接続する] をオンにします。
3. プロキシサーバの IPv4 アドレスまたは完全修飾ドメイン名を入力します。
4. ポート番号を入力します。初期設定のポート番号は [80] です。
5. (オプション) プロキシサーバで認証が必要な場合は、[認証情報の指定] を選択し、認証に使用するユーザ名とパスワードを入力します。

6. (オプション) [接続テスト] をクリックして、プロキシサーバへの接続を確認します。
7. [保存] をクリックします。

SMTP

[管理] > [システム設定] > [SMTP] にある [SMTP] 画面を使用すると、SMTP サーバを使用してアラート通知をメールで送信できます。

手順

1. [管理] > [システム設定] > [SMTP] の順に選択します。

   [SMTP] 画面が表示されます。
2. [SMTP サーバを使用する] を選択します。
3. SMTP サーバの IPv4 アドレスまたは完全修飾ドメイン名を入力します。
4. SMTP サーバとの接続に使用するセキュリティプロトコルを選択します。
5. (オプション) ポート番号を変更します。
6. 送信者のメールアドレスを入力します。
7. (オプション) SMTP 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、認証に使用するユーザ名とパスワードを入力します。

   警告!

   ユーザ名とパスワードが有効であることを確認します。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 Director (統合モード) からの通信が拒否されることがあります。
8. (オプション) Deep Discovery Director (統合モード) で、指定した SMTP サーバとの通信とメールの送信が可能であることを確認します。

   a. [テストメッセージの送信] をクリックします。

[テストメッセージの送信] ダイアログが表示されます。

b. 有効なメールアドレスを 1 つ以上入力して、[送信] をクリックします。

SMTP サーバとの通信が可能な場合、指定されたメールアドレスに、事前定義された件名とメッセージでメールが送信されます。

c. メールアカウントでメールの受信を確認します。

SNMP

SNMP (Simple Network Management Protocol) は、管理者の注意を必要とする状況についてネットワークに接続されたデバイスを監視するためのプロトコルです。

SNMP トラップは、このプロトコルをサポートする管理コンソールを使用するネットワーク管理者に対して通知を送信する手段です。

[管理] > [システム設定] > [SNMP] 画面の順に選択して、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に Deep Discovery Director (統合モード) を設定する。

  詳細については、396 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に Deep Discovery Director (統合モード) を設定する。

  詳細については、398 ページの「マネージャ要求を設定する」を参照してください。

トラップメッセージを設定する

SNMP トラップメッセージは、管理者の注意を必要とするイベントの発生時に SNMP サーバに送信される通知メッセージです。

手順

1. [管理] > [システム設定] > [SNMP] の順に選択します。
2. [トラップメッセージ] セクションで、[SNMP トラップメッセージの送信] を選択します。
3. トラップメッセージの設定を指定します。

オプション	説明
マネージャサーバのアドレス	マネージャサーバのアドレスを指定します。
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) 認証プロトコル: `HMAC-SHA` • (オプション) プライバシープロトコル: `CBC-AES-128`
コミュニティ名	コミュニティ名を指定します。
セキュリティモデル	注意 このフィールドは SNMPv3 でのみ使用できます。 次のセキュリティモデルを選択します。 • 認証またはプライバシーなし • 認証 • プライバシーにより認証

オプション	説明
ユーザ名	注意 このフィールドは SNMPv3 でのみ使用できます。 ユーザ名を指定します。
パスワード	注意 このフィールドは SNMPv3 でのみ使用できます。 パスワードを指定します。
プライバシーパスフレーズ	注意 このフィールドは SNMPv3 でのみ使用できます。 プライバシーパスフレーズを指定します。

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。

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 Director (統合モード) のシステム情報を要求できます。

手順

1. [管理] > [システム設定] > [SNMP] の順に選択します。

2. [マネージャ要求] で、[SNMP マネージャからの要求を待機] を選択します。
3. マネージャ要求の設定を指定します。

オプション	説明
デバイスの位置	アプライアンスの場所を指定します。
管理者の連絡先	アプライアンスの管理者の連絡先を指定します。
SNMP バージョン	次の SNMP のバージョンを選択します。 • SNMPv1/SNMPv2c • SNMPv3 SNMPv3 を使用する場合は、SNMP サーバを次のように設定します。 • コンテキスト名: `""` (初期設定のコンテキスト) • コンテキストエンジン ID: `<Auto>` • (オプション) 認証プロトコル: `HMAC-SHA` • (オプション) プライバシープロトコル: `CBC-AES-128`
許可するコミュニティ名	コミュニティ名を 5 つまで指定します。
セキュリティモデル	**注意** このフィールドは SNMPv3 でのみ使用できます。 次のセキュリティモデルを選択します。 • 認証またはプライバシーなし • 認証 • プライバシーにより認証

オプション	説明
ユーザ名	注意 このフィールドは SNMPv3 でのみ使用できます。 ユーザ名を指定します。
パスワード	注意 このフィールドは SNMPv3 でのみ使用できます。 パスワードを指定します。
プライバシーパスフレーズ	注意 このフィールドは SNMPv3 でのみ使用できます。 プライバシーパスフレーズを指定します。
信頼されるマネージャサーバのアドレス	信頼されるマネージャサーバのアドレスを 32 個まで指定します。

4. [保存] をクリックします。
5. (オプション) [MIB をダウンロード] をクリックして、MIB (Management Information Database) ファイルをダウンロードします。

   MIB ファイルを開くと、SNMP プロトコルを使用して監視および管理できるすべてのネットワークオブジェクトを確認できます。また MIB ファイルは、SNMP プロトコルをサポートする管理コンソールにインポートできます。

帯域幅

[管理] > [システム設定] > [帯域幅] にある [帯域幅] 画面を使用して、帯域幅使用率のスロットリングの設定を有効にします。帯域幅使用率のスロットリングを設定することで、ファイルのダウンロードやアップロードがネットワークやインターネット接続に与える影響を管理できます。

詳細については、401 ページの「帯域幅使用率のスロットリングを設定する」を参照してください。

帯域幅使用率のスロットリングを設定する

手順

1. [管理] > [システム設定] > [帯域幅] の順に選択します。

   [帯域幅] 画面が表示されます。

2. [帯域幅スロットリングの有効化] を選択します。

3. Deep Discovery Director (統合モード) からアプライアンスにファイルをダウンロードする際の、1 接続あたりの速度制限値を入力します。アプライアンスはそれぞれ 1 つの接続を確立します。

4. 接続の最大数を入力します。

5. [保存] をクリックします。

時間

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] > [時間] の順に選択します。

   [時間] 画面が表示されます。

2. 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 サーバの完全修飾ドメイン名または IP 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。

3. 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。

4. 日時の形式を選択します。
5. [保存] をクリックします。

証明書

デジタル証明書とは、サーバまたは Web サイトとクライアントを安全に接続するために使われる電子ドキュメントです。有効な信頼済み証明書は、信頼済みのサーバまたは Web サイトに接続していることをクライアントに保証し、中間者攻撃からネットワークを保護するのに役立ちます。

証明書は、認証局 (CA) の検証プロセスを経て信頼済みとなります。認証局そのものは通常は第三者機関であり、サーバまたは Web サイトとクライアントの両者に信頼されています。

最初のインストール時、Deep Discovery Director (統合モード) は自己署名 SSL 証明書を作成し、これを使用して他の Deep Discovery アプライアンスやローカルリポジトリと安全に通信を行います。この場合、Deep Discovery Director (統合モード) は自らの認証局としても機能します。

自社の認証局を指定したいユーザは、その認証局が署名した証明書を Deep Discovery Director (統合モード) にインポートできます。

重要

信頼されていない証明書や期限切れの証明書を使用して Deep Discovery Director (統合モード) サーバの管理コンソールにアクセスすると、Web ブラウザにセキュリティの警告が表示されます。

信頼されていない証明書や期限切れの証明書が Deep Discovery Director (統合モード) サーバと Deep Discovery アプライアンスとの通信に影響を与えることはありません。信頼されていない証明書や期限切れの証明書を使用する Deep Discovery Director (統合モード) サーバであっても、Deep Discovery アプライアンスに計画を配信でき、アプライアンスは計画の実行に必要なファイルをそのサーバから継続してダウンロードできます。

証明書をインポートする

Deep Discovery Director (統合モード) では、証明書を使用してクライアントと安全に接続します。フィンガープリントを変更したり別の認証局を指定したりする場合は、新しい証明書をインポートします。

警告!

- 新しい証明書をインポートする前に、その証明書が Web ブラウザで受け入れられることを確認します。Web ブラウザで受け入れられない証明書をインポートすると、管理コンソールにアクセスできなくなります。
- 証明書をインポートするとサービスが再起動します。リポジトリや Deep Discovery アプライアンスへの既存の接続が中断され、クライアントは新しいフィンガープリントを信頼して接続を回復することが必要になります。

手順

1. [管理] > [システム設定] > [証明書] の順に選択します。

   [証明書] 画面が表示されます。

2. [証明書をインポートして置換] をクリックし、証明書を選択して、[開く] をクリックします。

   証明書がただちにインポートされます。

証明書署名要求を生成する

Deep Discovery Director (統合モード) 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 Director (統合モード) 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] > [証明書] の順に選択します。
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。

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入力します。
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 つ以上入力します。
組織 (O)	会社名を入力します。
組織単位 (OU)	会社内の部署名を入力します。
国 (C)	会社が存在する国を示す 2 文字のコードを入力します。
都道府県 (ST)	会社が存在する都道府県を入力します。
市区町村 (L)	会社が存在する市区町村を入力します。
メールアドレス	自身のメールアドレスを入力します。
鍵の種類とサイズ	証明書の鍵の種類とサイズを選択します。

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。

セッションタイムアウト

操作を実行していないユーザをログアウトするまでの時間を選択します。初期設定値は [15 分] です。

アカウント管理

Deep Discovery Director (統合モード) では、役割ベースの管理を使用して、管理コンソールへのアクセスを付与および制御します。この機能を使用することで、管理コンソールの特定の権限をアカウントに割り当て、そのアカウントに特定タスクの実行に必要なツールと権限のみを表示します。

アカウントにはそれぞれ特定の役割が割り当てられます。役割は管理コンソールへのアクセスレベルを定義します。

アカウント

[管理] > [アカウント管理] > [アカウント] にある [アカウント] 画面を使用して、ユーザアカウントを作成および管理します。ユーザは、初期設定の管理者アカウントではなく、ユーザアカウントを使用して管理コンソールにアクセスできます。

Deep Discovery Director (統合モード) では、次の方法でユーザアカウントを作成できます。

- 406 ページの「ローカルユーザアカウントを追加する」
- 407 ページの「Active Directory のユーザアカウントまたはグループを追加する」

  注意

  この方法は、Microsoft Active Directory が設定済みの場合にのみ使用できます。

  詳細については、365 ページの「Microsoft Active Directory」を参照してください。

- 409 ページの「SAML グループを追加する」

  注意

  この方法は、SAML 認証が設定済みの場合にのみ使用できます。

  詳細については、367 ページの「SAML 認証」を参照してください。

ローカルユーザアカウントを追加する

手順

1. [管理] > [アカウント管理] > [アカウント] の順に選択し、[追加] をクリックします。

   [アカウントの追加] 画面が表示されます。

2. アカウントの [ステータス] を切り替えます。

3. アカウントの [種類] に [ローカルユーザ] を選択します。

4. 有効なユーザ名を入力します。

5. 有効なパスワードを入力します。

   重要

   - ユーザは、管理コンソールに初めてログオンしたときにパスワードを変更する必要があります。
   - 統合するためにローカルユーザアカウントの認証情報を使用する製品は、管理者に割り当てられたパスワードが変更されるまで統合できません。

6. 確認用にパスワードを再度入力します。

   ヒント

   (パスワードを表示) アイコンをクリックすると、パスワードが表示され、この手順が省略されます。

7. (オプション) Deep Discovery Director (統合モード) から送信されるアラートの受信に使用する有効なメールアドレスを入力します。

8. アカウントの [役割] を選択します。役割はアカウントのアクセスレベルを決定します。

   詳細については、412 ページの「役割」を参照してください。

9. [このアカウントに Web API を介したシステムへのアクセスを許可する] を選択し、このアカウントの資格情報および権限キーで Web API を介してシステムにアクセスすることを許可します。

   a. 権限キーの有効期限が切れるまでの日数を選択します。

   b. [このアカウントに管理コンソールへのログオンを許可する] を選択し、このアカウントの資格情報で管理コンソールにログオンすることを許可します。このオプションを無効にすると、このアカウントは Web API を介してのみシステムにアクセスできるようになります。

10. (オプション) アカウントの説明を入力します。

11. [保存] をクリックします。

    [このアカウントに Web API を介したシステムへのアクセスを許可する] を選択した場合、権限キーを含むダイアログが表示されます。

Active Directory のユーザアカウントまたはグループを追加する

Microsoft Active Directory でユーザアカウントとグループを管理してる場合は、そのユーザアカウントとグループを使用して Deep Discovery Director (統合モード) にアクセスできます。

注意

- Active Directory のユーザアカウントまたはグループを追加する前に、Microsoft Active Directory を設定する必要があります。

  詳細については、365 ページの「Microsoft Active Directory」を参照してください。

- Deep Discovery Director (統合モード) では、Microsoft Active Directory のユーザアカウントとグループが 24 時間ごとに同期されます。Active Directory サーバから削除されたユーザアカウントまたはグループは、Active Directory サーバとの同期後に Deep Discovery Director (統合モード) から削除されます。

- Microsoft Active Directory ユーザが 1 つ以上のグループに属している場合、そのユーザの Deep Discovery Director (統合モード) でのアクセスレベルは、ユーザの Deep Discovery Director (統合モード) アカウントまたは所属グループに割り当てられているアクセスレベルのうち最も高いレベルになります。

手順

1. [管理] > [アカウント管理] > [アカウント] の順に選択し、[追加] をクリックします。

   [アカウントの追加] 画面が表示されます。

2. アカウントの [ステータス] を切り替えます。

3. アカウントの [種類] に [LDAP ユーザまたはグループ] を選択します。

4. ユーザまたはグループの名前を入力して [検索] をクリックし、LDAP サーバの一致するユーザアカウントまたはグループを検索します。

   一致するユーザアカウントとグループが結果に表示されます。

   注意

   ユーザアカウントが表示されない場合は、次の理由が考えられます。

   - ユーザアカウントのユーザプリンシパル名 (UPN) が LDAP サーバで指定されていない
   - ユーザアカウントが LDAP サーバで無効になっている

5. 追加する LDAP のユーザアカウントまたはグループを選択します。

注意

Deep Discovery Director (統合モード) では、ユーザアカウントまたはグループの LDAP のメールアドレスが使用されます。

6. アカウントの [役割] を選択します。役割はアカウントのアクセスレベルを決定します。

   詳細については、412 ページの「役割」を参照してください。

7. (オプション) アカウントの説明を入力します。
8. [保存] をクリックします。

SAML グループを追加する

手順

1. [管理] > [アカウント管理] > [アカウント] の順に選択し、[追加] をクリックします。

   [アカウントの追加] 画面が表示されます。

2. アカウントの [ステータス] を切り替えます。
3. アカウントの [種類] に [SAML グループ] を選択します。
4. 要求の値を入力します。

注意

要求の値は、ADFS 要求発行ポリシー規則の出力方向の要求の値、または Okta のグループ名です。

5. アカウントの [役割] を選択します。役割はアカウントのアクセスレベルを決定します。

   詳細については、412 ページの「役割」を参照してください。

6. (オプション) アカウントの説明を入力します。
7. [保存] をクリックします。

アカウントのその他のタスク

次のタスクを実行することもできます。

表 9-5. その他のタスク

タスク	説明
アカウントの編集	ユーザ名をクリックして [アカウントの編集] 画面を開き、次の操作を実行します。 • アカウントのステータスの切り替え • パスワードの変更 • メールアドレスの変更 • 役割の変更 • Web API アクセスの有効化/無効化 • 説明の変更 注意 • Microsoft Active Directory アカウントのパスワードとメールアドレスは、管理コンソールでは変更できません。 • 管理コンソールに現在ログオンしていてアカウントが無効になったユーザは、自動的にログオフします。 • 管理コンソールに現在ログオンしていて役割が変更されたユーザは、自動的にログオフします。

タスク	説明
アカウントの削除	削除するユーザアカウントを 1 つ以上選択して、[削除] をクリックします。 注意 ・ 組み込みの管理者の役割を使用するローカルユーザアカウントが 1 つ以上必要です。 ・ ログオンしているアカウントは削除できません。 ・ 管理コンソールに現在ログオンしているユーザは、自動的にログオフします。
Web API アクセスのステータスの表示	Web API アクセスをアクティベートしたアカウントに対し、[新しい権限キーの生成] アイコンをクリックして新しい権限キーを生成します。
アカウントのロック状態の表示	Deep Discovery Director (統合モード) には、ユーザが 3 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。この方法でロックされたアカウントは、管理者アカウントであっても、10 分後に自動的にロック解除されます。 注意 Microsoft Active Directory アカウントがロックされることはありません。
アカウントのステータスの切り替え	[ステータス] 列で切り替えスイッチをクリックすると、ユーザアカウントを有効または無効にできます。 注意 ・ 組み込みの管理者の役割を使用するローカルユーザアカウントを 1 つ以上有効にする必要があります。 ・ 管理コンソールに現在ログオンしていてアカウントが無効になったユーザは、自動的にログオフします。

役割

[管理] > [アカウント管理] > [役割] にある [役割] 画面を使用して、ユーザの役割を作成および管理します。ユーザに役割を割り当てて、その活動を、役割の遂行に必要な活動のみに制限します。

Deep Discovery Director (統合モード) には、次の組み込みの役割が用意されています。この役割は削除できません。

役割	説明
Administrator	管理コンソールのすべての機能に対して完全なアクセス権があります。
Investigator	調査パッケージや PCAP データのダウンロード操作を除き、管理コンソールのすべての機能に対して読み取り専用のアクセス権があります。
Operator	管理コンソールのすべての機能に対して読み取り専用のアクセス権があります。

Deep Discovery Director (統合モード) では、ユーザの役割をカスタマイズできます。新しい役割を作成して管理コンソールへのアクセスを制限したり、ユーザが特定のアプライアンスを表示および管理しないように制限したりできます。

役割を追加する

手順

1. [管理] > [アカウント管理] > [役割] の順に選択し、[追加] をクリックします。

   [役割の追加] 画面が表示されます。

2. 役割名を入力します。
3. 役割の [権限] を選択します。
4. この役割で表示および管理できるアプライアンスを選択します。

5. メールメッセージの検出を表示するドメインを選択します。

   注意

   ドメインを指定する前に、ドメインを追加する必要があります。詳細については、413 ページの「ドメインを管理する」を参照してください。

6. アカウントを選択するか、入力して検索し、<Enter> キーを押します。その後、[追加] をクリックして、選択したアカウントをこの役割に追加します。

   注意

   追加したアカウントは、その他すべての役割から削除されます。

7. (オプション) 役割の説明を入力します。

8. [保存] をクリックします。

ドメインを管理する

Deep Discovery Email Inspector との統合では、役割ごとにどのアプライアンスを表示および管理できるのかをきめ細かく制御するだけでなく、役割ごとにどのメールメッセージを表示できるのかを制御することも必要です。この要件に対応するため、Deep Discovery Director (統合モード) はドメインを使用してメールメッセージを分類する機能を備えています。

手順

1. [管理] > [アカウント管理] > [役割] の順に選択します。

   [役割] 画面が表示されます。

2. 次のいずれかを実行します。

   - [追加] をクリックすると、[役割の追加] 画面が開きます。
   - 役割名をクリックすると、[役割の編集] 画面が開きます。

3. [ドメインアクセス] セクションで、[ドメインの管理] をクリックします。

[ドメインの管理] ダイアログが表示されます。

4. 左側のテキストボックスにドメインを入力し、[追加] をクリックしてリストにドメインを追加します。

   注意

   ドメインのプレフィックスでは、「.」で連結した 1 文字のワイルドカード (*) がサポートされます。

5. リストから 1 つ以上のドメインを選択し、[削除] をクリックすると、選択したドメインが削除されます。
6. (オプション) ドメインを検索するには、右側の検索テキストボックスにキーワードを入力して、<Enter> キーを押すか、虫眼鏡アイコンをクリックします。
7. [閉じる] をクリックします。

役割のその他のタスク

次のタスクを実行することもできます。

表 9-6. その他のタスク

タスク	説明
役割の編集	役割名をクリックして [役割の編集] 画面を開き、次の操作を実行します。 • 役割名の変更 • 権限の変更 • この役割で表示および管理できるアプライアンスの変更 • この役割へのアカウントの追加 • 説明の変更 注意 • 組み込み済みの役割の名前、権限、アプライアンスのアクセス権、および説明は変更できません。 • 管理コンソールに現在ログオンしていてアプライアンスのアクセス権が変更されたユーザは、自動的にログオフします。 • 管理コンソールに現在ログオンしていて役割が変更されたユーザは、自動的にログオフします。
役割の削除	削除するユーザの役割を 1 つ以上選択して、[削除] をクリックします。 注意 • 組み込みの役割は削除できません。 • 1 つ以上のアカウントで使用中の役割は削除できません。

システムログ

[管理] > [システムログ] にある [システムログ] 画面を使用して、システムログの表示、クエリ、およびエクスポートを行います。

Deep Discovery Director (統合モード) には、ユーザアクセス、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 Director (統合モード) 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。

データベースから情報を収集するには、システムログのクエリを実行します。クエリで問い合わせたシステムログは、CSV 形式でエクスポートして表示できます。

詳細については、417 ページの「システムログのクエリを実行する」を参照してください。

次の表は、システムログに関連するすべての情報を示しています。

表 9-7. [システムログ] の情報

列	説明
ログの日時	イベントが発生した日付と時刻
イベント ID	イベントの識別子 処理にはそれぞれ独自のイベント ID があります。例: • 20001 説明: User logged on • 20002 説明: User logged off
種類	次のいずれかの種類が表示されます。 • アカウントのログオン/ログオフ • Apex Central 統合 • 外部 Web サービス • メッセージの操作 • システム • アップデート

列	説明
レベル	次のいずれかのレベルが表示されます。 • 情報 • 警告 • エラー
結果	次のいずれかの結果が表示されます。 • 成功 • 失敗
ソース	送信元別の活動 次の送信元についての情報が表示されます。 • **ユーザ名** **例:** johnadmin • **システム** **例:** SYSTEM
IP アドレス	イベントに関係する IP アドレス
説明	イベントの詳細

システムログのクエリを実行する

システムログに数百または数千のエントリが存在する場合、そこから特定のエントリを探すのは困難です。フィルタや検索ボックスを使用すると、表示されるエントリの数を減らすことができます。

手順

1. [管理] > [システムログ] の順に選択します。

   [システムログ] 画面が表示されます。

2. [フィルタ] ボタンをクリックします。

   フィルタのドロップダウンリストと検索ボックスが表示されます。

3. 次のいずれかの処理を実行します。

   - ログの種類を選択します。
   - ログレベルを選択します。
   - ログの結果を選択します。
   - 期間を選択するか、カレンダーおよび時計を使用してカスタム期間を指定します。
   - イベント ID、送信元、または説明のキーワードを検索ボックスに入力して <Enter> キーを押すと、イベント ID、送信元、または説明にキーワードが含まれるシステムログのみが表示されます。

   画面がただちに更新されます。

4. (オプション) [エクスポート] をクリックして、現在フィルタ済みのシステムログをエクスポートします。

   [エクスポート] ダイアログが表示されます。

5. システムログのフィルタを確認し、使用する区切り文字を選択します。

6. [OK (成功)] をクリックすると、選択した区切り文字で、現在のフィルタ済みのシステムログが CSV ファイルにエクスポートされ、ダウンロードされます。

注意

エクスポートしたシステムログはログ ID の順に並べられます。ログ ID は、ログの日時と一致する連続した数字です。

システムのメンテナンス

[管理] > [システムのメンテナンス] にある [システムのメンテナンス] 画面には、次のタブがあります。

システムステータス

[システムステータス] 画面には、主要なハードウェアコンポーネントの使用状況が表示されます。

ストレージ

[管理] > [システムのメンテナンス] > [ストレージ] にある [ストレージ] 画面を使用して、Deep Discovery Director (統合モード) でデータベースエントリ、システムログ、および検出ログを保存する期間やディスク使用率を設定します。

[データベースストレージ] で、次の設定を行います。

- X 日より古いデータベースエントリを削除します。: データベースエントリを保存する日数を入力します。指定した値よりも古いエントリは自動的に削除されます。

  ヒント

  ここでデータベースエントリとは、Deep Discovery Director (統合モード) の計画を指します。

- X 日より古いシステムログを削除します。: システムログを保存する日数を入力します。指定した値よりも古いログは自動的に削除されます。
- *X* 日より古い検出ログを削除します。: 検出ログを保存する日数を入力します。指定した値よりも古いログは自動的に削除されます。

  ヒント

  - ここでの検出ログとは、Deep Discovery Inspector および Deep Discovery Email Inspector に関連する検出の詳細を指します。

- *x* 日より古い生成されたレポートを削除します。: 生成されたレポートを保存する日数を入力します。指定した値よりも古いレポートは自動的に削除されます。

注意

上記の設定に加えて、Deep Discovery Director (統合モード) ではシステムログを自動的に削除し、データベースのディスク空き容量を 200MB 以上確保します。このしきい値は変更できません。

[ディスク使用率] には、ディスク使用率とパーティションの合計サイズについての情報が表示されます。任意の使用可能な容量を任意のパーティションに追加できます。新しいディスクを追加して、パーティションのサイズを増やすこともできます。

ディスク容量を設定する

Deep Discovery Director (統合モード) のパーティションに使用可能なディスク容量を追加すると、保存できるログやリポジトリのファイル数が増えます。

手順

1. [管理] > [システムのメンテナンス] > [ストレージ] の順に選択し、[容量の設定] をクリックします。

   [ディスク容量の設定] ダイアログが表示されます。

2. (オプション) Deep Discovery Director (統合モード) にさらにディスクを追加するには、次の操作を実行します。

   a. [ディスクの追加] をクリックします。

      ディスクの選択ダイアログが表示されます。

   b. ディスクを 1 つ以上選択して、Deep Discovery Director (統合モード) のディスク容量の設定に追加します。

      重要

      サイズが 1024MB を超える未フォーマットのディスクのみが表示されます。

   c. [追加] をクリックします。

警告!

追加したディスクは削除できません。

選択したディスクがフォーマットされ、使用可能なディスク容量が [ディスク容量の設定] ダイアログに追加されます。

3. 使用可能な容量をパーティションに追加するには、次のいずれかを実行します。

   - [すべての空き容量をこのパーティションに追加してください] を選択します。
   - [追加] に値を入力します。

注意

- [空き容量] と [合計] の値が自動的に更新されます。
- 使用可能なすべての容量をパーティション間で配分する必要はありません。

4. [適用] をクリックします。

   指定した容量がパーティションに追加されます。

バックアップ

[管理] > [システムのメンテナンス] > [バックアップ] にある [バックアップ] 画面では、ほとんどの設定やデータベースについて、バックアップファイルをエクスポートしたり自動バックアップを設定したりすることができます。

- 423 ページの「設定とデータベースのバックアップをエクスポートする」
- 424 ページの「自動バックアップを設定する」

次の表は、バックアップの対象となる設定の画面名と要素を示しています。

表 9-8. バックアップされる設定

画面		要素
[脅威インテリジェンス] > [製品インテリジェンス]	同期された不審オブジェクト	オブジェクト
	C&C コールバックアドレス	オブジェクト
[脅威インテリジェンス] > [カスタムインテリジェンス]	YARA ルール	YARA ルール
	STIX	STIX
	ユーザ指定の不審オブジェクト	オブジェクト
	除外	オブジェクト
[脅威インテリジェンス] > [フィードの管理]		すべての設定
[脅威インテリジェンス] > [共有設定]	TAXII 1.x	すべての設定
	TAXII 2.0	すべての設定
	OpenDXL	すべての設定
	Web サービス	すべての設定
	補助製品/サービス	すべての設定
[アプライアンス] > [ディレクトリ]		グループ構造のアプライアンスツリー
		登録済みアプライアンスとアプライアンスの詳細
[アプライアンス] > [計画]		すべての計画
[アラート]	実行されたアラート	実行されたアラートのすべてのレコード
	組み込みルール	すべてのルール設定
	カスタムルール	すべてのルール設定
[レポート]	スケジュール	すべてのスケジュール
	カスタマイズ	すべての設定

画面		要素
[管理] > [統合製品/サービス]	Microsoft Active Directory	Microsoft Active Directory サーバの設定
	Syslog	Syslog サーバのすべてのプロファイル
[管理] > [ネットワーク分析]	接続済みソース	すべての設定
[管理] > [システム設定]	プロキシ	プロキシ設定
	帯域幅	帯域幅使用率のスロットリングの設定
	時間	時刻設定
	証明書	証明書
	セッションタイムアウト	セッションタイムアウト値
[管理] > [アカウント管理]	アカウント	すべてのユーザアカウント
	役割	すべての役割
[管理] > [システムログ]		すべてのシステムログ
[管理] > [システムのメンテナンス]	ストレージ	ストレージの設定値
	バックアップ	自動バックアップ設定
[管理] > [ライセンス]		アクティベーションコード
[ヘルプ]		API キー

設定とデータベースのバックアップをエクスポートする

Deep Discovery Director (統合モード) では、ほとんどの設定とデータベースのバックアップファイルをエクスポートできます。バックアップファイルを使用して、Deep Discovery Director (統合モード) を以前の時点に復元します。アクティブなサーバが応答せず復元できない場合は、バックアップファイルを使用して別のサーバに設定を復元し、ダウンタイムを最小限に抑えます。

手順

1. [管理] > [システムのメンテナンス] > [バックアップ] の順に選択します。

   [バックアップ] 画面が表示されます。

2. [設定とデータベースのバックアップ] の [エクスポート] をクリックします。

   アクティブなサーバで、設定とデータベースのバックアップファイルがエクスポートされます。

3. バックアップファイルをダウンロードして保存します。

自動バックアップを設定する

Deep Discovery Director (統合モード) では、設定やデータベースの自動バックアップを作成して任意の SFTP サーバにアップロードできます。バックアップファイルは 5 つまで作成されます。6 つ目のバックアップファイルを作成する際は最も古いファイルが削除され、バックアップファイルは常に 5 つに維持されます。

手順

1. [管理] > [システムのメンテナンス] > [バックアップ] の順に選択します。

   [バックアップ] 画面が表示されます。

2. [自動バックアップ] で [SFTP サーバに自動的にバックアップする] を選択します。

3. SFTP サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

4. ポート番号を入力します。初期設定のポート番号は 22 です。

5. SFTP サーバで使用するフォルダパスを入力します。

6. SFTP サーバへのログオンに使用するユーザ名とパスワードを入力します。

7. ドロップダウンリストと時計ツールを使用して、バックアップの頻度を指定します。

8. [保存] をクリックします。

復元

[管理] > [システムのメンテナンス] > [復元] にある [復元] 画面を使用して、バックアップファイルから設定とデータベースを復元します。アクティブな Deep Discovery Director (統合モード) サーバが応答しない、または復元できない場合は、設定とデータベースのバックアップファイルを別のサーバで使用して設定を復元し、ダウンタイムを最小限に抑えることができます。

- 425 ページの「設定とデータベースのバックアップを復元する」
- 426 ページの「アクティブなサーバを別のサーバと置き換える」

注意

設定とデータベースのバックアップをエクスポートする方法の詳細については、423 ページの「設定とデータベースのバックアップをエクスポートする」を参照してください。

設定とデータベースのバックアップを復元する

設定とデータベースのバックアップを使用して、Deep Discovery Director (統合モード) を以前の時点に復元できます。

アクティブな Deep Discovery Director (統合モード) が応答しない、または復元できない場合は、設定とデータベースのバックアップを別のサーバで使用して操作を復元し、ダウンタイムを最小限に抑えることができます。

詳細については、426 ページの「アクティブなサーバを別のサーバと置き換える」を参照してください。

手順

1. [管理] > [システムのメンテナンス] > [復元] の順に選択します。

   [復元] 画面が表示されます。

2. [ファイルの選択] をクリックして、バックアップファイルを選択します。
3. [アップロード] をクリックします。

   バックアップファイルがアップロードされると、Deep Discovery Director (統合モード) にバックアップファイルの情報が表示されます。
4. [復元] をクリックします。

   Deep Discovery Director (統合モード) に確認メッセージが表示されます。
5. [OK] をクリックします。

   Deep Discovery Director (統合モード) でバックアップファイルから設定とデータベースが復元され、サーバが再起動します。
6. (オプション) 以前アップロードしたすべてのアップデート、アップグレード、および仮想アナライザイメージファイルをリポジトリに再アップロードして、リポジトリを復元します。

   重要

   アップデート、アップグレード、および仮想アナライザイメージファイルはバックアップファイルに含まれないため、自動的には復元されません。ファイルがリポジトリに再アップロードされない場合、アプライアンスでは計画をダウンロードして実行することができません。
7. (オプション) ネットワークアドレスを設定します。

   サーバで操作を再開する準備が整いました。

アクティブなサーバを別のサーバと置き換える

Deep Discovery Director (統合モード) サーバが応答しない、または復元できない場合、別のサーバに置き換えることができます。

ホストコンピュータのハードウェア、ホストコンピュータのソフトウェア、および置換先サーバの Deep Discovery Director (統合モード) のバージョンとビルドはアクティブサーバと同じである必要があります。

手順

1. アクティブサーバの設定とデータベースをバックアップします。

   a. アクティブサーバの管理コンソールで、[管理] > [システムのメンテナンス] > [バックアップ] の順に選択します。

   b. [設定とデータベースのバックアップ] で [エクスポート] をクリックします。

      アクティブなサーバで、設定とデータベースのバックアップファイルがエクスポートされます。

   c. バックアップファイルをダウンロードして保存します。

2. 置換先サーバに Deep Discovery Director (統合モード) をインストールします。

3. 置換先サーバに一時的なネットワークアドレスを設定します。

   重要

   IP アドレスが競合しないよう、一時的なネットワークアドレスがアクティブサーバのネットワークアドレスと異なることを確認してください。

4. 置換先サーバの管理コンソールにログオンします。

5. 置換先サーバで設定とデータベースを復元します。

   a. 置換先サーバの管理コンソールで、[管理] > [システムのメンテナンス] > [復元] の順に選択します。

   b. [ファイルの選択] をクリックして、バックアップファイルを選択します。

   c. [アップロード] をクリックします。

      バックアップファイルがアップロードされると、Deep Discovery Director (統合モード) にバックアップファイルの情報が表示されます。

   d. [復元] をクリックします。

Deep Discovery Director (統合モード) に確認メッセージが表示されます。

e. [OK] をクリックします。

Deep Discovery Director (統合モード) でバックアップファイルから設定とデータベースが復元され、サーバが再起動します。

6. 以前アップロードしたすべてのアップデート、アップグレード、および仮想アナライザイメージファイルをリポジトリに再アップロードして、リポジトリを復元します。

重要

アップデート、アップグレード、および仮想アナライザイメージファイルはバックアップファイルに含まれないため、自動的には復元されません。ファイルがリポジトリに再アップロードされない場合、アプライアンスでは計画をダウンロードして実行することができません。

7. アクティブサーバの電源をオフにします。

a. アクティブサーバの管理コンソールで、[管理] > [システムのメンテナンス] > [電源オフ/再起動] の順に選択します。

b. [電源オフ] をクリックします。

アクティブサーバがすべてのサービスを停止して、シャットダウンします。

警告!

置換先サーバはアクティブサーバのネットワークアドレスを使用するように設定されます。アクティブサーバの電源を入れたままにしておくと、IP アドレスの競合が発生します。

8. アクティブサーバのネットワークアドレスを使用するように置換先サーバを設定します。

この作業により、新しいアクティブサーバとして置換先サーバでサービスを再開する準備が整いました。

電源オフ/再起動

[管理] > [システムのメンテナンス] > [電源オフ/再起動] にある [電源オフ/再起動] 画面を使用して、サーバの電源オフや再起動を実行します。

- 電源オフ: すべてのアクティブなタスクが停止され、サーバ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、サーバが再起動します。

統合製品は、Deep Discovery Director を使用できない間、データをキューに入れる可能性があります。

ライセンス

[管理] > [ライセンス] にある [ライセンス] 画面を使用して、Deep Discovery Director (統合モード) および Deep Discovery Director - Network Analytics as a Service 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。

[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 9-9. [ライセンス] の詳細

フィールド	詳細
ステータス	[アクティベート済み]、[アクティベート未完了]、または [有効期限切れ] のいずれかが表示されます。 **重要** • Deep Discovery Director (統合モード) では、ライセンスのステータスが [アクティベート未完了] または [有効期限切れ] の場合、新しい計画を作成できません。既存の計画は、通常どおりに配信および実行されます。 • Deep Discovery Director (統合モード) では、ライセンスのステータスが [アクティベート未完了] または [有効期限切れ] の場合、コンポーネントをアップデートできません。 • Deep Discovery Director - Network Analytics as a Service では、ライセンスのステータスが [アクティベート未完了] または [有効期限切れ] の場合、相関イベントを表示できません。 • ライセンスの有効期限が切れた後、相関イベントとデータは Deep Discovery Director - Network Analytics as a Service から削除され、復元できなくなります。 [詳細の表示] をクリックすると、トレンドマイクロの Web サイトにライセンス情報の詳細が表示されます。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、[表示の更新] をクリックします。 **注意** • プロキシ設定が有効な場合、Deep Discovery Director (統合モード) ではプロキシサーバを使用してライセンスアップデートサーバに接続します。 • Deep Discovery Director - Network Analytics as a Service ライセンスのステータスの表示を更新するには、Deep Discovery Director (統合モード) ライセンスのステータスが [アクティベート済み] になっている必要があります。

フィールド	詳細
種類	• 製品版: すべての製品機能を利用できます • 体験版: すべての製品機能を利用できます
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。[更新手順の表示] をクリックすると、トレンドマイクロの Web サイトに手順が表示されます。
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、更新された有効期限が示されます。 **ヒント** Deep Discovery Director (統合モード) は、Deep Discovery 製品のいずれかのアクティベーションコードでアクティベートできます。 **注意** Deep Discovery Director - Network Analytics as a Service ライセンスの契約を更新するには、Deep Discovery Director (統合モード) ライセンスのステータスが [アクティベート済み] になっている必要があります。

第 10 章

トラブルシューティング

Deep Discovery Director (統合モード) で利用可能なトラブルシューティングの一般的なオプションについて説明します。

トラブルシューティング

[トラブルシューティング] 画面を開くには、`https://<アプライアンスの IP アドレス>/troubleshooting` にアクセスします。

ログ

Deep Discovery Director (統合モード) では、さまざまな内部サービスに対するデバッグログが生成され、保存されます。オフラインで表示してトラブルシューティングを実行するには、デバッグログをエクスポートします。

1. (オプション) さまざまなサービスで生成されるデバッグログのレベルを変更し、[適用] をクリックします。
2. [デバッグログファイルのエクスポート] をクリックして、[デバッグログファイルのエクスポート] ダイアログを表示します。
3. エクスポートするデバッグログファイルを選択し、[エクスポート] をクリックします。

   ログファイルの収集とダウンロード用アーカイブファイルの作成が開始されます。

(オプション) [初期設定に戻す] をクリックすると、すべての設定が初期設定値に戻ります。

クラッシュダンプの削除

Deep Discovery Director (統合モード) では、プロセスのクラッシュ時にダンプファイルが生成され、保存されます。

プロセスのクラッシュダンプファイルを手動で削除してディスクの空き容量を増やすには、[削除] をクリックします。

脅威インテリジェンス

統合処理のタイムアウトまでの時間、処理のバッチサイズ (Check Point のみ)、URL からクエリ文字列を削除するかどうか (Palo Alto のみ) など、脅威インテリジェンスの共有設定を変更して、[保存] をクリックします。

第 11 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

ここでは、Deep Discovery Director (統合モード) で使用されるサービスのアドレスとポートについて説明します。Deep Discovery Director (統合モード) がサービスに接続して最適な状態で動作できるように、プロキシおよびファイアウォールを設定します。

サービスのアドレスとポート

Deep Discovery Director (統合モード) 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。

注意

すべてのサービスは TLS 1.2 以上の HTTPS を使用して接続します。ご利用の環境に中継機器がある場合は、その機器が TLS 1.2 以上をサポートしていることを確認してください。

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	備考
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。	ddd53-p.activeupdate.trendmicro.co.jp:443/activeupdate/japan	製品のバージョンに関連
サポート契約ポータル	お客さま情報、申し込み、製品やサービスのライセンスを管理します。	licenseupdate.trendmicro.com:80	
Deep Discovery Director - Network Analytics as a Service	履歴ネットワークデータに基づくネットワーク検出や、その他の関連イベント発生の時間別推移について高度な脅威分析を提供するホステッドサービスです。	api.nacloud.trendmicro.com:443 api.eu.nacloud.trendmicro.com:443 api.jp.nacloud.trendmicro.com:443 api.sg.nacloud.trendmicro.com:443 api.us.nacloud.trendmicro.com:443	製品の地域に関連

サービス	説明	アドレスとポート	備考
Email Encryption	個人情報の安全な配信のため、ID ベース暗号化 (IBE) を使用して、登録されたドメインのメールメッセージを暗号化および復号します。	root.ibe-ta.com:80 public.ibe-ta.com:80 ppconfig.ibe-ta.com:80	
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。	ddd53jp-threatconnect.trendmicro.com:443	製品のバージョンに関連
Trend Micro Vision One	検出と対応をエンドポイントを超えて拡張し、より広範な可視性と専門家によるセキュリティ分析を提供することで、より多くの脅威の検出と早期の迅速な対応を実現します。Trend Micro Vision One により、効果的に脅威に対応し、侵害の重大度と範囲を最小限に抑えることができます。	*.xdr.trendmicro.co.jp:443	製品バージョンと地域に関連

Deep Discovery Director (統合モード) で使用されるポート

次の項目は、Deep Discovery Director (統合モード) で使用されるポートとその目的を示しています。

表 A-2. Deep Discovery Director (統合モード) で使用されるポート

ポート	プロトコル	機能	目的
22	TCP	インバウンドおよびアウトバウンド	次のことを実行します。 • 事前設定コンソールに接続します。 • 仮想アナライザイメージを SFTP サーバからダウンロードします。 • 設定とデータを SFTP サーバにバックアップします。
25	TCP	アウトバウンド	このポートを使用して SMTP 経由でアラート通知を送信します。
53	TCP/UDP	アウトバウンド	このポートは DNS による名前解決用に使用されます。
80	TCP	アウトバウンド	他のコンピュータやトレンドマイクロの統合製品およびホステッドサービスに接続します。 具体的には次のことを実行します。 • Customer Licensing Portal に接続します。 • プロキシサーバに接続します。 • Email Encryption サービスに接続します。
123	UDP	アウトバウンド	このポートを使用して NTP サーバに接続し、時間を同期します。
139	TCP	アウトバウンド	このポートを使用して仮想アナライザイメージをネットワークフォルダからダウンロードします。
161	UDP	インバウンド	このポートを SNMP エージェントの待機およびプロトコル変換に使用します。

ポート	プロトコル	機能	目的
162	UDP	インバウンドおよびアウトバウンド	次のことを実行します。 • SNMP エージェントの待機およびプロトコル変換を行います。 • SNMP トラップ通知を送信します。
443	TCP	インバウンドおよびアウトバウンド	次のことを実行します。 • コンピュータを使用して HTTPS 経由で管理コンソールにアクセスします。 • TAXII 1.x および 2.0 クライアントの要求を待機します。 • 脅威インテリジェンスデータについて統合製品またはサービスの要求を待機します。 • 脅威インテリジェンスデータについて補助製品またはサービスの要求を待機します。 • 脅威インテリジェンスを共有するために補助製品またはサービスと通信します。 • Deep Discovery アプライアンスと通信します。 • Deep Discovery Director - Network Analytics as a Service と通信します。 • アップデートサーバと通信します。 • Trend Micro Apex Central と通信します。 • Trend Micro Vision One と通信します。
445	TCP/UDP	アウトバウンド	このポートを使用して仮想アナライザイメージをネットワークフォルダからダウンロードします。

ポート	プロトコル	機能	目的
601	TCP	アウトバウンド	このポートを使用してログを Syslog サーバに送信します。
636	TCP	アウトバウンド	このポートを使用して Microsoft Active Directory からユーザ情報を取得します。
4459	TCP	インバウンド	このポートを使用して、HTTPS 経由でコンピュータを使用してエンドユーザメール隔離コンソールにアクセスします。
6514	TCP	インバウンドおよびアウトバウンド	このポートを使用して、TCP 経由で SSL 暗号化を使用して Syslog サーバにログを送信します。
8080	TCP	インバウンド	このポートを使用して脅威インテリジェンスを他の製品と共有します。
8883	TCP	アウトバウンド	このポートを使用して脅威インテリジェンスデータを OpenDXL クライアント、サービス、およびブローカーに配信します。
18183	TCP	アウトバウンド	このポートを使用して脅威インテリジェンスデータを Check Point Open Platform for Security に配信します。

付録 B

Deep Discovery Director で複製される設定

ここでは、Deep Discovery のアプライアンスとバージョンごとに Deep Discovery Director (統合モード) で複製される設定のリストを示します。

注意

日本ではリリースされていない製品またはバージョンについての内容が含まれることがあります。

Deep Discovery Analyzer 6.8 で複製される設定

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-1. Deep Discovery Analyzer 6.8 で複製される設定

画面		要素
[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	フィルタ設定
	[不審オブジェクト] > [ユーザ指定の不審オブジェクト]	ユーザ指定の不審オブジェクト
	除外	除外設定リスト
[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	パスワードリスト
	送信設定	ファイルタイプフィルタ設定
	スマートフィードバック	スマートフィードバック設定
	macOS 向けサンドボックス	macOS 向けサンドボックス設定
	YARA ルール	すべての YARA ルール
[アラート/レポート] > [アラート]	ルール	すべてのアラート通知ルール設定
[アラート/レポート] > [レポート]	スケジュール	すべての予約レポート
	カスタマイズ	レポートのカスタマイズ設定
[管理] > [アップデート] > [コンポーネントのアップデート設定]		コンポーネントのアップデート設定

画面		要素
[管理] > [統合製品/サービス]	Smart Protection	Smart Protection 設定
	ICAP	ICAP 設定
	Microsoft Active Directory	Microsoft Active Directory 設定
	ログ設定	ログ設定
[管理] > [システム設定]	ネットワーク	TLS 設定
	プロキシ	プロキシ設定
	SMTP	SMTP 設定
	時間	時刻設定
	SNMP	SNMP 設定
	パスワードポリシー	パスワードポリシー設定
	セッションタイムアウト	セッションタイムアウト値
[管理] > [アカウント/連絡先]	アカウント	すべてのユーザアカウント
	連絡先	すべての連絡先
[管理] > [システムメンテナンス] > [バックアップ]		自動バックアップ設定

Deep Discovery Analyzer 6.9 で複製される設定

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-2. Deep Discovery Analyzer 6.9 で複製される設定

画面	要素
[ダッシュボード]	ウィジェット設定のみ

画面		要素
[仮想アナライザ]	送信	フィルタ設定
	[不審オブジェクト] > [ユーザ指定の不審オブジェクト]	ユーザ指定の不審オブジェクト
	除外	除外設定リスト
[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	パスワードリスト
	送信設定	ファイルタイプフィルタ設定
	スマートフィードバック	スマートフィードバック設定
	macOS 向けサンドボックス	macOS 向けサンドボックス設定
	YARA ルール	すべての YARA ルール
[アラート/レポート] > [アラート]	ルール	すべてのアラート通知ルール設定
[アラート/レポート] > [レポート]	スケジュール	すべての予約レポート
	カスタマイズ	レポートのカスタマイズ設定
[管理] > [アップデート] > [コンポーネントのアップデート設定]		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	Smart Protection 設定
	ICAP	ICAP 設定
	Microsoft Active Directory	Microsoft Active Directory 設定
	ログ設定	ログ設定

画面		要素
[管理] > [システム設定]	ネットワーク	TLS 設定
	プロキシ	プロキシ設定
	SMTP	SMTP 設定
	時間	時刻設定
	SNMP	SNMP 設定
	パスワードポリシー	パスワードポリシー設定
	セッションタイムアウト	セッションタイムアウト値
[管理] > [アカウント/連絡先]	アカウント	すべてのユーザアカウント
	SAML	すべての SAML グループ
	連絡先	すべての連絡先
[管理] > [システムメンテナンス] > [バックアップ]		自動バックアップ設定

Deep Discovery Analyzer 7.0 で複製される設定

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-3. Deep Discovery Analyzer 7.0 で複製される設定

画面		要素
[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	フィルタ設定
	[不審オブジェクト] > [ユーザ指定の不審オブジェクト]	ユーザ指定の不審オブジェクト
	除外	除外設定リスト

画面		要素
[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	パスワードリスト
	送信設定	ファイルタイプフィルタ設定
	検索設定	すべての設定
	インタラクティブモード設定	すべての設定
	スマートフィードバック	スマートフィードバック設定
	macOS 向けサンドボックス	macOS 向けサンドボックス設定
	YARA ルール	すべての YARA ルール
[アラート/レポート] > [アラート]	ルール	すべてのアラート通知ルール設定
[アラート/レポート] > [レポート]	スケジュール	すべての予約レポート
	カスタマイズ	レポートのカスタマイズ設定
[管理] > [アップデート] > [コンポーネントのアップデート設定]		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	Smart Protection 設定
	ICAP	ICAP 設定
	Microsoft Active Directory	Microsoft Active Directory 設定
	ログ設定	ログ設定

画面		要素
[管理] > [システム設定]	ネットワーク	TLS 設定
	プロキシ	プロキシ設定
	SMTP	SMTP 設定
	時間	時刻設定
	SNMP	SNMP 設定
	パスワードポリシー	パスワードポリシー設定
	セッションタイムアウト	セッションタイムアウト値
[管理] > [アカウント/連絡先]	アカウント	すべてのユーザアカウント
	SAML	すべての SAML グループ
	連絡先	すべての連絡先
[管理] > [システムメンテナンス] > [バックアップ]		自動バックアップ設定

Deep Discovery Inspector 5.6 で複製される設定

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-4. Deep Discovery Inspector 5.6 で複製される設定

画面		要素
[検出]	影響を受けたホスト	[保存された検索条件] のみ
	[影響を受けたホスト] - [ホストの詳細]	
	すべての検出	
[レポート]	スケジュール	すべての設定
	カスタマイズ	

画面		要素
[管理] > [アップデート] > [コンポーネントのアップデート]	予約アップデート	すべての設定
	アップデート元	すべての設定
[管理] > [通知]	[通知設定] > [脅威の検出]	すべての設定
	[通知設定] > [高リスクホストの検出]	
	[通知設定] > [不審ホストの検出]	
	[通知設定] > [高ネットワークトラフィック]	
	[通知設定] > [分析されていないサンプルの検出]	
	[通知設定] > [仮想アナライザによる検出]	
	[通知設定] > [拒否リスト]	
	[通知設定] > [Retro Scan による検出]	
	[配信オプション] > [メール設定]	
[管理] > [監視/検索]	ホスト/ポート	すべての設定
	脅威の検出	
	Web レピュテーション	
	アプリケーションフィルタ	
	拒否リスト/許可リスト	
	検出ルール	
	除外	
	パケットキャプチャ	

画面		要素
[管理] > [仮想アナライザ]	セットアップ	内部仮想アナライザプロキシ設定と macOS 向けサンドボックス設定のみ
	ファイル送信	すべての設定
	[内部仮想アナライザ] > [サンドボックス管理] > [パスワード]	
[管理] > [ネットワークグループとエンドポイント]	ネットワークグループ	すべての設定
	登録済みドメイン	
	登録済みサービス	
[管理] > [統合製品/サービス]	脅威インテリジェンスの共有	すべての設定
	Microsoft Active Directory	
	Syslog	
[管理] > [システム設定]	ネットワーク	[セキュアプロトコル] 設定のみ
	プロキシ	すべての設定
	SNMP	
	時間	
	セッションタイムアウト	
[管理] > [アカウント]		すべての設定
[管理] > [システムのメンテナンス] > [ストレージ管理]		[ファイルサイズの設定] のみ

Deep Discovery Inspector 5.7 で複製される設定

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-5. Deep Discovery Inspector 5.7 で複製される設定

画面		要素
[検出]	影響を受けたホスト	[保存された検索条件] のみ
	[影響を受けたホスト] - [ホストの詳細]	
	すべての検出	
[レポート]	スケジュール	すべての設定
	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]	予約アップデート	すべての設定
	アップデート元	すべての設定
[管理] > [通知]	[通知設定] > [脅威の検出]	すべての設定
	[通知設定] > [高リスクホストの検出]	
	[通知設定] > [不審ホストの検出]	
	[通知設定] > [高ネットワークトラフィック]	
	[通知設定] > [分析されていないサンプルの検出]	
	[通知設定] > [仮想アナライザによる検出]	
	[通知設定] > [拒否リスト]	
	[通知設定] > [Retro Scan による検出]	
	[配信オプション] > [メール設定]	

画面		要素
[管理] > [監視/検索]	ホスト/ポート	すべての設定
	脅威の検出	
	Web レピュテーション	
	アプリケーションフィルタ	
	拒否リスト/許可リスト	
	検出ルール	
	検出の除外	
	パケットキャプチャ	
[管理] > [仮想アナライザ]	セットアップ	内部仮想アナライザプロキシ設定と macOS 向けサンドボックス設定のみ
	ファイル送信	すべての設定
	[内部仮想アナライザ] > [サンドボックス管理] > [パスワード]	
[管理] > [ネットワークグループとエンドポイント]	ネットワークグループ	すべての設定
	登録済みドメイン	
	登録済みサービス	
[管理] > [統合製品/サービス]	脅威インテリジェンスの共有	すべての設定
	Microsoft Active Directory	
	Syslog	

画面		要素
[管理] > [システム設定]	ネットワーク	[セキュアプロトコル] 設定のみ
	プロキシ	すべての設定
	SMTP	
	SNMP	
	時間	
	セッションタイムアウト	
[管理] > [アカウント]		すべての設定
[管理] > [システムのメンテナンス] > [ストレージ管理]		[ファイルサイズの設定] のみ

Deep Discovery Inspector 5.8 で複製される設定

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-6. Deep Discovery Inspector 5.8 で複製される設定

画面		要素
[検出]	影響を受けたホスト	[保存された検索条件] のみ
	[影響を受けたホスト] - [ホストの詳細]	
	すべての検出	
[レポート]	スケジュール	すべての設定
	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]	予約アップデート	すべての設定
	アップデート元	すべての設定

画面		要素
[管理] > [通知]	[通知設定] > [脅威の検出]	すべての設定
	[通知設定] > [高リスクホストの検出]	
	[通知設定] > [不審ホストの検出]	
	[通知設定] > [高ネットワークトラフィック]	
	[通知設定] > [分析されていないサンプルの検出]	
	[通知設定] > [仮想アナライザによる検出]	
	[通知設定] > [拒否リスト]	
	[通知設定] > [Retro Scan による検出]	
	[配信オプション] > [メール設定]	
[管理] > [監視/検索]	ホスト/ポート	すべての設定
	脅威の検出	
	Web レピュテーション	
	アプリケーションフィルタ	
	拒否リスト/許可リスト	
	検出ルール	
	検出の除外	
	パケットキャプチャ	

画面		要素
[管理] > [仮想アナライザ]	セットアップ	内部仮想アナライザプロキシ設定と macOS 向けサンドボックス設定のみ
	ファイル送信	すべての設定
	[内部仮想アナライザ] > [サンドボックス管理] > [パスワード]	
[管理] > [ネットワークグループとエンドポイント]	ネットワークグループ	すべての設定
	登録済みドメイン	
	登録済みサービス	
[管理] > [統合製品/サービス]	脅威インテリジェンスの共有	すべての設定
	Microsoft Active Directory	
	Syslog	
[管理] > [システム設定]	ネットワーク	[セキュアプロトコル] 設定のみ
	プロキシ	すべての設定
	SMTP	
	SNMP	
	時間	
	セッションタイムアウト	
[管理] > [アカウント]		すべての設定
[管理] > [システムのメンテナンス] > [ストレージ管理]		[ファイルサイズの設定] のみ

Deep Discovery Web Inspector 2.5 で複製される設定

注意

Deep Discovery Web Inspector の日本語版はリリースされていません。

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-7. Deep Discovery Web Inspector 2.5 で複製される設定

画面		要素
[Dashboard]		すべての設定
[Policy]	Policy	すべてのポリシールールとポリシーのグローバル設定
	Decryption Rules	すべての HTTPS 復号ルール (以前の HTTPS 検査ルール)
	Digital Certificates	信頼済み証明書、信頼されていない証明書、無効な証明書のストア内のすべての証明書、および証明書の除外
	HTTPS Tunnels	すべてのドメイントンネル
	Intelligent Decryption	すべてのカスタムのパターンファイルと除外
[Policy] > [User Defined Settings]	Network Objects	すべてのネットワークオブジェクト
	Domain Objects	すべてのドメインオブジェクト
	Approved/Blocked Lists	承認済みリストとブロックリスト
	Notifications	すべての通知設定

画面		要素
[Alerts / Reports]	[Alerts] > [Rules]	すべてのアラートルール
	[Reports] > [Schedules]	すべての予約レポート
[Administration]	[Component Updates] > [Schedules]	すべてのスケジュール設定
	[System Settings] > [X-Header Handling]	すべての設定
[Administration] > [Active Directory Services]	Active Directory	すべての設定
	Authentication Policy	すべての設定
	Global Authentication Settings	すべての設定 注意 Kerberos キーテーブル情報はバックアップされません。

Deep Discovery Web Inspector 2.6 で複製される設定

注意

Deep Discovery Web Inspector の日本語版はリリースされていません。

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-8. Deep Discovery Web Inspector 2.6 で複製される設定

画面	要素
[Dashboard]	すべての設定

画面		要素
[Policy]	Policy	すべてのポリシールールとポリシーのグローバル設定
	Decryption Rules	すべての HTTPS 復号ルール (以前の HTTPS 検査ルール)
	Digital Certificates	信頼済み証明書、信頼されていない証明書、無効な証明書のストア内のすべての証明書、および証明書の除外
	HTTPS Tunnels	すべてのドメイントンネル
	Intelligent Decryption	すべてのカスタムのパターンファイルと除外
[Policy] > [User Defined Settings]	Network Objects	すべてのネットワークオブジェクト
	Domain Objects	すべてのドメインオブジェクト
	Approved/Blocked Lists	承認済みリストとブロックリスト
	Notifications	すべての通知設定
[Alerts / Reports]	[Alerts] > [Rules]	すべてのアラートルール
	[Reports] > [Schedules]	すべての予約レポート
[Administration]	[Component Updates] > [Schedules]	すべてのスケジュール設定
	[System Settings] > [X-Header Handling]	すべての設定

画面		要素
[Administration] > [Active Directory Services]	Active Directory	すべての設定
	Authentication Policy	すべての設定
	Global Authentication Settings	すべての設定 **注意** Kerberos キーテーブル情報はバックアップされません。

Deep Discovery Director (Standalone Network Analytics モード) 5.2 で複製される設定

注意

Deep Discovery Director（Standalone Network Analytics モード）の日本語版はリリースされていません。

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-9. Deep Discovery Director (Standalone Network Analytics モード) 5.2 で複製される設定

画面		要素
[管理] > [統合製品/サービス] > [Microsoft Active Directory]		すべての設定
[管理] > [システム設定]	プロキシ	すべての設定
	SMTP	すべての設定
	SNMP	すべての設定
	時間	手動で設定した日時を除くすべての設定
	セッションタイムアウト	すべての設定

画面	要素
[管理] > [アカウント管理]	すべての設定

Deep Discovery Director (Standalone Network Analytics モード) 5.3 で複製される設定

注意

Deep Discovery Director（Standalone Network Analytics モード）の日本語版はリリースされていません。

次の表は、複製の対象となる設定の画面名と要素を示しています。

表 B-10. Deep Discovery Director (Standalone Network Analytics モード) 5.3 で複製される設定

画面		要素
[管理] > [統合製品/サービス] > [Microsoft Active Directory]		すべての設定
[管理] > [システム設定]	プロキシ	すべての設定
	SMTP	すべての設定
	SNMP	すべての設定
	時間	手動で設定した日時を除くすべての設定
	セッションタイムアウト	すべての設定
[管理] > [アカウント管理]		すべての設定