Deep Discovery™ Inspector 6.8

管理者ガイド

※注意事項

複数年契約について

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

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

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

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

法人向け製品のサポートについて

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

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

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、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

先得、Trend Micro One、Workforce One、Security Go、Dock 365、TrendConnect、TREND MICRO FORUM、トレンドマイクロ知恵袋、Trend Cloud One、Trend Service One、および Accelerating You 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 © 2024 Trend Micro Incorporated. All rights reserved.

P/N: APEM69959/241023

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

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

重要

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

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

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

目次

第 1 章：はじめに

Deep Discovery Inspector について 2

新機能 2

機能と利点 3

- 脅威の管理機能 3
- APT 攻撃シーケンス 4
- ホストの重大度 5
- 高度な脅威検索エンジン 8
- 仮想アナライザ 8

第 2 章：開始する

事前設定コンソール 12

基本設定のタスク 12

管理コンソール 13

- 管理コンソールの要件 14
- 管理コンソールを開く 15
- 管理コンソールのアカウントのパスワード 16
  - 管理者アカウントパスワードの変更 17
  - 閲覧者アカウントパスワードの変更 18
- シングルサインオンによるログオン 19

ネットワーク 19

- アプライアンス IP の設定 19
  - ネットワークの形式ルール 22
- ネットワークインタフェースのポートの管理 24

第 3 章：ダッシュボード

ダッシュボードの概要 28

タブ 28

- タブのタスク 29

タブの追加/変更 29
タブの移動 30
タブを閉じる/タブの削除 30
ウィジェット 31
ウィジェットのタスク 31
ダッシュボードへのウィジェットの追加 32
Deep Discovery Inspector のウィジェットについて 33
Deep Discovery Inspector のウィジェット 34
Deep Discovery Inspector の初期設定ウィジェットのタブ 37
概要 37
脅威検出状況の概要 37
影響を受けたホストの上位 39
脅威の概要 39
検索された不正なネットワークトラフィック 39
検索されたプロトコル別トラフィック 40
脅威の監視 40
脅威のグラフィック地図 40
[脅威のグラフィック地図] での情報の表示 41
過去 30 日間の監視対象のネットワークトラフィック 41
仮想アナライザのステータス 42
仮想アナライザで検出されたホストの上位 42
仮想アナライザで分析された不正なサイトの上位 43
不審ファイルの上位 43
仮想アナライザ 44
傾向の上位 46
要注意アプリケーションの上位 46
検出された不正 URL の上位 46
システムステータス 47
CPU 使用率 47
ディスクの使用状況 47
メモリ使用率 47
オプションのウィジェット 47
検索されたすべてのトラフィック 48
不正なリアルタイムネットワークトラフィック 48

リアルタイム検索されたトラフィック 49
セキュリティホールを悪用されたホストの上位 49
グレーウェアに感染したホストの上位 49
検出された不正コンテンツ の上位 50
不正プログラムに感染したホストの上位 50
検出された不審動作の上位 50

第 4 章：検出

[検出] 画面について 54
影響を受けたホスト 55
表示オプションと検索フィルタ 55
影響を受けたホストの表示 58
[影響を受けたホスト] - [ホストの詳細] の表示 61
[影響を受けたホスト] - [検出の詳細] の表示 65
[影響を受けたホスト] - [検出の詳細] 67
接続の詳細 67
[影響を受けたホスト] - [検出の詳細] - [ファイル分析結果] 73
[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] 76
[影響を受けたホスト] - [検出の詳細] - [不審オブジェクト情報] 76
[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] 77
軽減策の提案 78
影響を受けたホストの詳細検索フィルタ 78
影響を受けたホストの詳細検索フィルタについて 79
影響を受けたホストの詳細検索フィルタの追加 ... 81
[影響を受けたホスト] の保存された検索条件の編集 82
[影響を受けたホスト] の保存された検索条件の削除 84
[影響を受けたホスト] の保存された検索条件のインポート 84
[影響を受けたホスト] の保存された検索条件のエクスポート 85

[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 86
[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタの追加 92
[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編集 94
[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削除 96
[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 96
[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 97
C&C コールバックアドレス 98
C&C コールバックアドレスの表示 98
仮想アナライザ不審オブジェクト 99
ユーザ指定の不審オブジェクト 101
Retro Scan 102
Retro Scan と Trend Micro Smart Protection Network 103
Retro Scan の有効化 104
Retro Scan 画面 104
Retro Scan レポートの詳細画面 105
Retro Scan の無効化 106
Retro Scan の無効化 107
すべての検出 107
表示オプションと検索フィルタ 107
すべての検出の表示 109
[すべての検出] - [検出の詳細] の表示 113
[すべての検出] - [検出の詳細] 115
[すべての検出] - [検出の詳細] - [接続の詳細] 115
[すべての検出] - [検出の詳細] - [検出情報] 117
[すべての検出] - [検出の詳細] - [接続の概要] 119
[すべての検出] - [検出の詳細] - [プロトコル情報] 120
[すべての検出] - [検出の詳細] - [ファイル情報] 121

[すべての検出] - [検出の詳細] - [追加情報] 121
[すべての検出] - [検出の詳細] - [ファイル分析結果] 122
[すべての検出] - [検出の詳細] - [ファイル分析結果] - [ファイル情報] 123
[すべての検出] - [検出の詳細] - [ファイル分析結果] - [YARA 検出] 124
[すべての検出] - [検出の詳細] - [ファイル分析結果] - [著しい特性] 124
[すべての検出] - [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] 124
[すべての検出] - [検出の詳細] - [不審オブジェクト情報] 125
[すべての検出] - [検出の詳細] - [分析された関連ファイル情報] 125
[すべての検出] - [検出の詳細] - [軽減策の提案] ... 126
すべての検出の詳細検索フィルタ 127
すべての検出の詳細検索フィルタの追加 133
[すべての検出] の保存された検索条件の編集 135
すべての検出の保存された検索条件の削除 137
すべての検出の保存された検索条件のインポート 137
すべての検出の保存された検索条件のエクスポート . 138

第 5 章：レポート

レポートについて 142
予約レポート 144
スケジュール 145
レポートのスケジュールの設定 146
レポートのスケジュールの削除 147
手動レポート 148
手動レポートの生成 149
手動レポートの削除 150
カスタマイズ 151
レポートのカスタマイズ 151

第 6 章：管理

アップデート 154
コンポーネントのアップデート 154
アップデートするコンポーネント 154
コンポーネントのアップデート方法 156
コンポーネントのアップデートタスク 157
手動アップデート 158
手動アップデートの実行 158
予約アップデートの設定 159
アップデート元 159
アップデート元の設定 160
製品のアップデート 160
HotFix/Patch 161
HotFix または Patch の適用 162
HotFix または Patch のロールバック 164
Service Pack/バージョンアップグレード 165
Service Pack またはバージョンアップグレードの適用 165
ブラウザのキャッシュのクリア 167
通知 168
脅威の検出の通知 169
高リスクホストの検出の通知 171
高リスクホストの検出通知の除外リストへの追加 174
不審ホストの検出の通知 174
高ネットワークトラフィックの通知 176
分析されていないサンプルの検出の通知 178
仮想アナライザによる検出の通知 180
拒否リストに基づく検出の通知 182
Retro Scan による検出の通知 183
トンネリングされたドメインの超過の通知 184
低ネットワークトラフィックの通知 185
配信オプション 187
メール通知の設定 187
監視/検索 188
ホスト/ポート 188
ホストとポートの設定 189

脅威の検出 190
脅威の検出設定 190
Smart Protection 192
Smart Protection Server について 194
Smart Protection Server の設定 195
Smart Protection Server リストの管理 195
Web レピュテーション 196
Web レピュテーションの設定 197
アプリケーションフィルタ 200
アプリケーションフィルタの設定 200
拒否リスト/許可リスト 201
拒否リスト/許可リストの形式ルール 202
拒否リストと許可リストの設定 206
拒否リストと許可リストの設定 207
拒否リスト/許可リストをインポートするための形式ルール 209
カスタム拒否リスト/許可リストのエクスポート 209
カスタム拒否リスト/許可リストのインポート 210
検出ルール 212
検出ルールの設定 212
パケットキャプチャ 213
パケットキャプチャルールの追加 214
検出の除外設定 215
TLS トラフィックインスペクション 219
インスペクション設定 220
トンネリングされたドメインの設定 221
証明書の管理 221
信頼済み CA 証明書 222
署名証明書 223
復号ポリシー 224
仮想アナライザ 228
仮想アナライザの種類 228
内部仮想アナライザの設定 229
外部仮想アナライザの設定 231
Sandbox as a Service の設定 231
Trend Vision One — Sandbox Analysis の設定 232

ファイル送信 233
ソフトウェア安全性評価サービス 234
ファイル送信ルール 234
ファイル送信ルールの種類と条件 235
ファイル送信ルール画面 239
ファイル送信ルールの追加 240
内部仮想アナライザ 242
サンドボックス管理 243
仮想アナライザのステータス 243
仮想アナライザイメージ 244
Image Preparation Tool 244
イメージをインポートする 244
トレンドマイクロ仮想アナライザイメージアップロードツールを使用してイメージをアップロードする 247
インスタンスの変更 248
インスタンスの変更 248
インスタンスの削除 249
アーカイブのパスワード 249
アーカイブのパスワードの追加 250
macOS 向けサンドボックス 251
YARA ルール 251
YARA ルールファイルの作成 252
YARA ルールファイルの追加 254
YARA ルールファイルの編集 255
YARA ルールファイルの削除 255
YARA ルールファイルのエクスポート 256
ネットワークグループとエンドポイント 256
ネットワークグループの追加 257
登録済みドメインの追加 259
登録済みサービスの追加 261
Trend Vision One からのネットワークグループとエンドポイントの同期 264
設定のインポート/エクスポート 265
統合製品/サービス 266
トレンドマイクロの統合製品とサービス 266

Trend Vision One 267
Trend Vision One への直接接続 268
Service Gateway をプロキシとして使用した Trend Vision One への接続 270
Network Inventory を使用して Deep Discovery Inspector を Trend Vision One から切断します 271
Service Gateway の接続 272
Service Gateway のサービス 274
有効な Service Gateway のサービスの表示 274
Smart Protection Services 274
コンポーネントサービスのアップデート 276
Service Gateway を切断する 276
Apex Central 277
Apex Central のコンポーネント 278
Apex Central への登録 278
Apex Central からの登録解除 280
Apex Central との接続の管理 281
Deep Discovery Director 281
Deep Discovery Director に接続する 282
Deep Discovery Director から登録解除する 284
Threat Investigation Center 284
Threat Investigation Center の統合 285
TXOne OT Defense Console 286
TXOne OT Defense Console の設定 286
脅威インテリジェンスの共有 287
脅威インテリジェンスの共有設定 288
インライン製品とサービス 289
Trend Micro TippingPoint Security Management System (SMS) 290
Trend Micro TippingPoint Security Management System (SMS) の設定 291
Check Point OPSEC (Open Platform for Security) 294
Check Point OPSEC (Open Platform for Security) の設定 295
セキュリティゲートウェイの事前設定 303
保護された接続を設定する 305
IBM Security Network Protection 309
IBM Security Network Protection の設定 310

Palo Alto Panorama または Firewall 314
Palo Alto Panorama または Firewall の設定 315
SAML 認証 319
サービスプロバイダのメタデータと証明書 320
ID プロバイダの設定 321
Okta の設定 322
Active Directory フェデレーションサービスを設定する 324
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 327
Microsoft Active Directory 328
Microsoft Active Directory との統合を設定する 329
Syslog 330
Syslog サーバの追加 331
システム設定 333
ネットワーク 334
ネットワークインタフェース 334
データポートと管理ポート 335
インラインポート 335
プロキシ 336
プロキシサーバの設定 336
SMTP 337
SMTP を設定する 337
SNMP 338
SNMP トラップのモードの設定 339
SNMP エージェントのモードの設定 340
HTTPS 証明書 341
HTTPS 証明書の生成 341
HTTPS 証明書のインポート 343
時間 343
時刻オプションの設定 344
セッションタイムアウト 344
セッションタイムアウトの設定 344
アカウント 345
アカウントについて 346
ユーザの役割とメニュー項目の権限 347
ローカルアカウントの追加 350

Active Directory アカウントの追加 351
SAML アカウントの追加 353
アカウントの編集 354
アカウントパスワードのリセット 356
アカウントの削除 357
アカウントのロック解除 357
システムログ 358
システムログのクエリ 358
システムのメンテナンス 360
ストレージ管理 360
ストレージ管理の実行 361
製品データベースの管理の実行 362
ファイルサイズの設定 362
バックアップ/復元 362
ファイルの設定のバックアップ 364
ファイルの設定をインポートする 364
初期設定の復元 366
電源オフ/再起動 367
Deep Discovery Inspector の再起動 367
Deep Discovery Inspector の電源オフ 368
ライセンス 368
アクティベーションコード 368
製品バージョン 369
Deep Discovery Inspector のライセンスの有効期限 369
ライセンスのアクティベートまたは更新 370

第 7 章：トラブルシューティング

よくある質問 (FAQ) 374
FAQ - アプライアンスの復元 374
FAQ - 設定 375
FAQ - 検出 375
FAQ - 設置 375
FAQ - アップグレード 376
FAQ - 仮想アナライザイメージ 376

トラブルシューティング 377
管理コンソールの応答が遅くなります 377
検出 378
[すべての検出] 画面に検出が表示されません 378
[すべての検出] クエリでの [登録されていないサービス] サーバの表示 379
不明な IP アドレスが画面に表示されます 379
既知の安全なオブジェクトに不正のフラグが付けられます 380
[データベースが破損しています。] アラートが表示されます 380
仮想アナライザ 380
OVA をアップロードできません 380
仮想アナライザがファイルの送信に応答しません 381
仮想アナライザのイメージ 382
インストールメディアが起動しません 382
[Found New Hardware] ウィザード 382
イメージによるブルースクリーンの表示 383
ネットワークサービスに接続できない 383
診断 384
インライン導入と TLS インスペクション 385
ネットワーク接続の問題 385
TLS 接続の問題 387

第 8 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 390
サポートポータルの利用 390
脅威データベース 390
製品サポート情報 390
サポートサービスについて 391
トレンドマイクロへのウイルス解析依頼 391
メールレピュテーションについて 392
ファイルレピュテーションについて 392
Web レピュテーションについて 392
その他のリソース 393
最新版ダウンロード 393

脅威解析・サポートセンター TrendLabs (トレンドラボ) 393

付録

付録 A：仮想アナライザがサポートするファイルタイプ

付録 B：Deep Discovery Director および Trend Vision One で複製される設定

付録 C：統合製品/サービスでの TLS のサポート

付録 D：サービスのアドレスとポート

索引

索引 417

はじめに

本書について

次の項目を参照してください。

- 2 ページの「ドキュメント」
- 3 ページの「対象読者」
- 3 ページの「ドキュメントの表記規則」

ドキュメント

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

表 1. 製品ドキュメント

ドキュメント	説明
管理者ガイド	管理者ガイドには、Deep Discovery Inspector を設定して管理する方法の詳細な手順、および Deep Discovery Inspector の概念や機能に関する説明が記載されています。
AWS 配信ガイド	AWS 配信ガイドには、Deep Discovery Inspector の AWS への導入の計画、実施、およびトラブルシューティングに関する要件および手順についての情報が含まれています。
インライン (LAN バイパス) ネットワークインタフェースカード インストールガイド	インライン (LAN バイパス) ネットワークインタフェースカードインストールガイドには、追加のバイパスネットワークインタフェースカードを、サポートされる Deep Discovery Inspector アプライアンスにインストールするための要件と手順に関する情報が記載されています。
インストールガイド	インストールガイドには、Deep Discovery Inspector の導入計画とインストールの要件および手順、さらに事前設定コンソールを使用して初期設定とシステムタスクを実行する方法についての情報が含まれています。
Syslog コンテンツマッピングガイド	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 Inspector の Syslog イベントを実装するための構文に関する情報が記載されています。
クイックスタートガイド	クイックスタートガイドには、Deep Discovery Inspector をネットワークに接続して初期設定を実行するための手順がわかりやすく説明されています。
Readme	Readme には、オンラインヘルプや印刷されたドキュメントには記載されていない最新の製品情報が含まれています。新機能、既知の問題、および製品リリースの履歴に関する情報を確認できます。
オンラインヘルプ	Deep Discovery Inspector 管理コンソールからアクセスできる Web ベースのドキュメントです。 オンラインヘルプには、Deep Discovery Inspector のコンポーネントと機能、Deep Discovery Inspector を設定するために必要な手順が説明されています。

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

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。

https://www.trendmicro.com/ja_jp/business/products/downloads.html?clk=left_nav&clkval=all_download&regs=jp

対象読者

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

- ネットワークトポロジ
- データベース管理
- ウイルス対策とコンテンツのセキュリティ保護

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

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記規則	説明
注意	設定上の注意

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

第 1 章

はじめに

製品の機能およびセキュリティテクノロジについては、次の項目を参照してください。

- 2 ページの「Deep Discovery Inspector について」
- 3 ページの「機能と利点」
- 3 ページの「脅威の管理機能」
- 4 ページの「APT 攻撃シーケンス」
- 5 ページの「ホストの重大度」
- 8 ページの「高度な脅威検索エンジン」
- 8 ページの「仮想アナライザ」

Deep Discovery Inspector について

Deep Discovery Inspector は第 3 世代の脅威管理ソリューションで、標的型攻撃や高度な脅威の可視性、洞察、および制御を強化するよう設計されています。Deep Discovery Inspector は、重要なセキュリティ情報、警告、およびレポートを IT 管理者に提供します。

Deep Discovery Inspector は、世界中の主要な 1,000 の組織と政府機関の要件を満たすために開発されました。グローバルインテリジェンスと検索テクノロジを統合することで、従来のシグネチャベースの脅威だけでなくヒューリスティック分析を必要とするより高度な脅威を検出します。

新機能

次の表は、Deep Discovery Inspector6.8 の新機能を説明しています。

機能	詳細
Trend Vision One との情報の共有	Deep Discovery Inspector から Trend Vision One に次の情報を送信できるようになります。 • TCP テレメトリ
Trend Vision One の Sandbox Analysis との統合	Trend Vision One コンソールから [サンドボックスに送信] をオンにして Deep Discovery Inspector を有効にし、不審ファイルやその他のオブジェクトを Trend Vision One の Sandbox Analysis アプリに送信して分析します。結果は、Trend Vision One — Sandbox Analysis で確認できます。
SNMPv3 のサポート	Deep Discovery Inspector で SNMPv3 がサポートされるようになります。
新しい Deep Discover Inspector モデル	新しい Deep Discovery Inspector 40G モデルでは、1 つのアプライアンスで最大 40Gpbs の帯域幅がサポートされます。
仮想アナライザの強化	仮想アナライザで次のイメージがサポートされるようになります。 • Windows 10 22H2 • Windows 11 23H2

機能と利点

Deep Discovery Inspector は洗練された検出機能により、多数の高度な検出エンジンを使用し、さまざまなネットワークプロトコルを介してカスタムおよびシグネチャベースの検出についての詳細な情報を提供します。Deep Discovery Inspector は、標的型攻撃や高度な脅威を検出し、自動化されたプロセスにより標的型攻撃に対処します。

Deep Discovery Inspector には次の機能があります。

- 3 ページの「脅威の管理機能」
- 4 ページの「APT 攻撃シーケンス」
- 5 ページの「ホストの重大度」
- 8 ページの「高度な脅威検索エンジン」
- 8 ページの「仮想アナライザ」

脅威の管理機能

Deep Discovery Inspector は、脅威をリアルタイムに検出および特定し、企業データに対する攻撃の検出、防止、封じ込めに必要となる徹底的な分析と実行可能なインテリジェンスを提供します。

表 1-1. 脅威の管理機能

機能	説明
APT および標的型攻撃の検出の強化	Deep Discovery Inspector の検出エンジンでは、カスタムサンドボックス分析をはじめとして、APT および標的型攻撃の検出機能が強化されています。新しい検出ルールおよび相関分析のためのルールが、攻撃シーケンスの段階にまたがって不正なコンテンツ、通信、および動作を検出します。
可視性、分析、および処理	Deep Discovery Inspector 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	説明
大容量のプラットフォーム	Deep Discovery Inspector の特長である高性能アーキテクチャは、大規模な組織の、容量における厳しく多様な要件を満たします。 Deep Discovery Inspector の機能はあらゆる規模の企業で役立ち、特に標的型攻撃のリスクを軽減する必要がある大規模組織には必要不可欠です。

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 1-2. 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。

段階	説明
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 Inspector 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。

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 1-3. 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
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

カテゴリ	レベル	説明
	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
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

高度な脅威検索エンジン

高度な脅威検索エンジン (ATSE: Advanced Threat Scan Engine) は、シグネチャファイルベースの検索とルールベースのヒューリスティック検索を組み合わせて使用し、ドキュメントのセキュリティホールや標的型攻撃で使用されるその他の脅威を検出します。

主な機能は次のとおりです。

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

仮想アナライザ

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

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

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

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

第 2 章

開始する

Deep Discovery Inspector 管理コンソールおよびアプライアンスの基本的な設定については、次の項目を参照してください。

- 12 ページの「事前設定コンソール」
- 12 ページの「基本設定のタスク」
- 13 ページの「管理コンソール」
- 19 ページの「ネットワーク」

事前設定コンソール

Deep Discovery Inspector の事前設定コンソールは、Deep Discovery Inspector 管理コンソールにアクセスするために必要なネットワーク設定とシステム設定を行うための端末通信プログラムです。

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

基本設定のタスク

次の設定によって脅威の検出をカスタマイズします。

設定の詳細については、次の各手順の項目を参照してください。

ヒント

以下の各手順についてセットアップガイドを画面に表示するには、管理コンソールで [ヘルプ] > [セットアップガイド] の順に選択します。

手順

1. [監視対象ネットワークグループ] を追加します。

   詳細については、257 ページの「ネットワークグループの追加」を参照してください。

2. [登録済みドメイン] を設定します。

   詳細については、259 ページの「登録済みドメインの追加」を参照してください。

3. [登録済みサービス] を設定します。

   詳細については、261 ページの「登録済みサービスの追加」を参照してください。

4. (オプション) [プロキシ設定] を行います。

   詳細については、336 ページの「プロキシサーバの設定」を参照してください。

5. コンポーネントをアップデートします。

   詳細については、158 ページの「手動アップデートの実行」を参照してください。

6. (オプション) [TLS トラフィックインスペクション] を設定します。

   詳細については、220 ページの「インスペクション設定」を参照してください。

管理コンソール

Deep Discovery Inspector にはオンライン管理コンソールが組み込まれており、これを使用して、システムのステータスの表示、脅威検出とログの設定と表示、レポートの実行、Deep Discovery Inspector の管理、コンポーネントの更新、およびヘルプの閲覧を行うことができます。

管理コンソールには、次のユーザインタフェース要素が含まれています。

番号	UI 要素	説明
1.	アカウント名および基本的なユーザアカウント操作	基本的なユーザアカウント操作は、管理コンソール画面の右上隅のアカウント名の下に配置され、次のオプションが含まれます。 • パスワードの変更 注意 ローカルアカウント以外のパスワードは、管理コンソールでは変更できません。 • ログオフ
2.	一目でわかるアプライアンス情報	一目でわかるアプライアンス情報には、次のものが含まれます。 • タイムゾーン • アプライアンスの完全修飾ドメイン名/IP アドレス • ネットワークトラフィック • 復号されたトラフィック (TLS トラフィックインスペクションが有効な場合)
3.	メイン画面のタブ	管理コンソールには次のタブがあります。 • ダッシュボード • 検出数 • レポート • 管理 • ヘルプ

管理コンソールの要件

Deep Discovery Inspector の管理コンソールでは、次の Web ブラウザがサポートされます。

- Google Chrome

- Mozilla Firefox
- Microsoft Edge

推奨解像度: 1280 * 800 もしくはそれ以上

管理コンソールを開く

手順

1. 管理コンソールにアクセスする端末で、サポートされるブラウザを開きます。
2. インターネットのセキュリティレベルを [中] に設定し、ActiveX のバイナリビヘイビアとスクリプトビヘイビアを有効にして、ツールチップおよびレポートが表示されるようにします。
3. 管理コンソールの IP アドレスを入力します。
   - 初期設定の Deep Discovery Inspector の IP アドレスを使用している場合は、次のように入力します。

     ```
     https://192.168.252.1/index.html
     ```

     注意

     URL では、大文字/小文字が区別されます。
   - 一意の IP アドレスを使用している場合は、その IP アドレスを入力します。
4. 次の初期設定のユーザ名を入力します。

   ```
   admin
   ```
5. 次の初期設定のパスワードを入力します。

   ```
   admin
   ```
6. [ログオン] をクリックします。

重要

Deep Discovery Inspector アプライアンスの IP アドレスを変更した場合は、ブラウザのブックマークを更新して新しい IP アドレスが反映されるようにします。

7. 初期設定のパスワードを変更します。

   16 ページの「管理コンソールのアカウントのパスワード」を参照してください。

8. システム時刻を設定します。

   344 ページの「時刻オプションの設定」を参照してください。

9. Deep Discovery Inspector をアクティベートします。

   370 ページの「ライセンスのアクティベートまたは更新」を参照してください。

管理コンソールのアカウントのパスワード

注意

ローカルアカウント以外のパスワードは、管理コンソールでは変更できません。

Deep Discovery Inspector では、ユーザアカウントごとに管理コンソールへのアクセス権が付与されます。あらかじめ組み込まれている管理者アカウントでは、最大 127 件のローカルアカウントを作成できます。管理コンソールにアクセスするには、各ユーザアカウントでログオンパスワードが必要です。

管理コンソールのパスワードでは、次のルールに従って作成されたパスワードを使用できます。

- 文字数が 8〜32 文字
- 少なくとも 1 つの大文字 (A〜Z)
- 少なくとも 1 つの小文字 (a〜z)
- 少なくとも 1 つの数字 (0〜9)

- 少なくとも 1 つの特殊文字: ` ~ !@ # $ % ^ & * ( ) - _ + = [ ] { } \ | < > , . / ? : ; ' "

強固なパスワードを作成するために、次のガイドラインに従ってください。

- 辞書にある単語は避ける
- 意図的に入れ替えた単語のスペルを使用する
- 句や結合した単語を使用する
- 大文字と小文字の両方を使用する

管理者アカウントパスワードの変更

注意

ローカルアカウント以外のパスワードは、管理コンソールでは変更できません。

システム管理者アカウントの初期設定の管理コンソールパスワードは `admin` です。

ヒント

セキュリティを強化するために、Deep Discovery Inspector のパスワードは定期的に変更してください。

ヒント

管理者パスワードは、[アカウント] 画面でもリセットできます。

手順

1. Deep Discovery Inspector のメイン画面の右上隅で、自分のアカウント名のドロップダウンメニューを開きます。

2. [パスワードの変更] をクリックします。

3. 現在のパスワードを入力します。
4. 新しいパスワードを入力して、確認用に再度入力します。
5. [保存] をクリックします。

   Deep Discovery Inspector から自動的にログオフされます。
6. 新しいパスワードで Deep Discovery Inspector にログオンします。

閲覧者アカウントパスワードの変更

注意

ローカルアカウント以外のパスワードは、管理コンソールでは変更できません。

新しい閲覧者アカウントの作成時に、初期設定の管理コンソールパスワードが生成されます。

新規ユーザは管理者からこの初期設定のパスワードを取得して、初回ログオン後、アカウントパスワードを変更する必要があります。

ヒント

セキュリティを強化するために、Deep Discovery Inspector のパスワードは定期的に変更してください。

手順

1. Deep Discovery Inspector のメイン画面の右上隅で、自分のアカウント名のドロップダウンメニューを開きます。
2. [パスワードの変更] をクリックします。
3. 現在のパスワードを入力します。
4. 新しいパスワードを入力して、確認用に再度入力します。
5. [保存] をクリックします。

Deep Discovery Inspector から自動的にログオフされます。

6. 新しいパスワードで Deep Discovery Inspector にログオンします。

シングルサインオンによるログオン

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

詳細については、319 ページの「SAML 認証」を参照してください。

手順

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

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

ネットワーク

[管理] > [システム設定] > [ネットワーク] の順に選択して、Deep Discovery Inspector アプライアンスのネットワーク設定を管理します。

Deep Discovery Inspector では、管理ポートといくつかのデータポートを使用します。[管理] > [システム設定] > [ネットワークインタフェース] の順に選択して、これらのポートのステータスを確認します。

アプライアンス IP の設定

手順

1. [管理] > [システム設定] > [ネットワーク] の順に選択します。
2. [ホスト名または完全修飾ドメイン名] で、ホスト名または完全修飾ドメイン名を指定します。

注意

SAML 認証を使用している場合、[ホスト名または完全修飾ドメイン名] にはドメイン名を含める必要があります。[ホスト名または完全修飾ドメイン名] を変更すると、SAML 認証に影響します。

3. (オプション) このアプライアンスの識別に IP アドレスではなくホスト名を使用する場合にこのオプションを選択します。

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。

4. [IPv4 タイプ] を選択します。
   - 静的 IP アドレス
   - 動的 IP アドレス (DHCP)

注意

Deep Discovery Inspector では、管理ポートから管理コンソールにアクセスできるようにするために、専用の IP アドレスが必要です。ネットワークで DHCP サーバから Deep Discovery Inspector に IP アドレスを動的に割り当てるには、[動的 IP アドレス (DHCP)] を選択します。そうでない場合は、[静的 IP アドレス] を選択します。

5. [静的 IP アドレス] を選択した場合は、次を指定します。
   a. IPv4 アドレス: Deep Discovery Inspector 専用の数値アドレス
   b. IPv4 サブネットマスク: Deep Discovery Inspector の IP アドレスが含まれるネットワークのサブネットマスク
   c. IPv4 ゲートウェイ: ネットワークゲートウェイの IP アドレス
   d. IPv4 DNS サーバ 1: ホスト名を IP アドレスに解決するプライマリサーバの IP アドレス
   e. IPv4 DNS サーバ 2 (オプション): ホスト名を IP アドレスに解決するセカンダリサーバの IP アドレス

6. (オプション) IPv6 アドレスを設定します。
   a. [IPv6 アドレスを有効にする] を選択します。

      IPv6 アドレス設定が表示されます。

   b. 次の IPv6 アドレス設定を指定します。

      - IPv6 アドレス: Deep Discovery Inspector 専用の英数字アドレス
      - IPv6 サブネットプレフィックス長: Deep Discovery Inspector の IP アドレスが含まれるネットワークのプレフィックス長
      - IPv6 ゲートウェイ: ネットワークゲートウェイの IP アドレス
      - (オプション) IPv6 DNS サーバ: ホスト名を IP アドレスに解決するサーバの IP アドレス
7. (オプション) [常に TLS 1.2 以上を使用する] を有効にします。

重要

[常に TLS 1.2 以上を使用する] を有効または無効に変更した場合、アプライアンスを再起動する必要があります。

このオプションを有効にすると、Deep Discovery Inspector は、TLS 1.2 以上をサポートしない製品/サービスに接続できなくなります。

注意

Payment Card Industry Data Security Standard (PCI-DSS) v3.2 に準拠するには、アプライアンスはすべての受信および送信接続に TLS 1.2 以上を使用する必要があります。

統合製品およびサービスが TLS 1.2 以上をサポートする最新バージョンを使用していることを確認してください。詳細については、407 ページの統合製品/サービスでの TLS のサポートを参照してください。

次の製品/サービスが TLS 1.2 以上を使用するように設定されていることを確認します。

- [管理] > [アップデート] > [コンポーネントのアップデート] > [アップデート元] のアップデートサーバは、HTTPS を使用する必要があります。
- [管理] > [統合製品/サービス] > [Apex Central] の Apex Central サーバアドレスは、HTTPS を使用する必要があります。
- [管理] > [統合製品/サービス] > [Syslog] の Syslog サーバは、SSL を使用する必要があります。
- [管理] > [システム設定] > [SMTP] の SMTP サーバは、SSL/TLS または STARTTLS を使用する必要があります。
- [管理] > [統合製品/サービス] > [脅威インテリジェンスの共有] の脅威インテリジェンスの共有サービスは、HTTPS のみを使用する ([HTTP を使用して情報を共有] を無効にする) 必要があります。

8. [保存] をクリックします。

ネットワークの形式ルール

[管理] > [システム設定] > [ネットワーク] の順に選択します。

Deep Discovery Inspector のネットワーク設定には、次の形式ルールが適用されます。

表 2-1. ネットワーク設定の形式ルール

形式の設定	説明
アプライアンスのホスト名の形式	ホスト名には英数字とダッシュ (「A〜Z」、「a〜z」、「0〜9」、「-」) を含めることができます。
動的 IP アドレス	ネットワーク上の DHCP サーバから動的 IP サーバを取得します。それに従って事前設定コンソールが変更されていることを確認してください。詳細については、「Deep Discovery Inspector 6.8 インストールガイド」を参照してください。
静的 IP アドレスの形式	**注意** この IP アドレスにはブロードキャストまたはネットワークアドレスを指定できません。 IP アドレスは、次の形式で指定する必要があります。XXX.XXX.XXX.XXX。ここで、X は 0〜255 の 10 進数値です。 IPv4 アドレスを次のいずれかの形式で指定することはできません。 • AAA.XXX.XXX.XXX。ここで、AAA は 223〜240 の数値です (マルチキャストアドレス)。 • 0.0.0.0 (ローカルホスト名) • 255.255.255.255 (ブロードキャストアドレス) • 127.0.0.1 (ループバックアドレス) IPv6 アドレスを次のいずれかの形式で指定することはできません。 • ff00::/8 (マルチキャストアドレス) • fe80::/10 (リンクローカルアドレス) • ::0 (ユニキャストルートアドレス) • ::1/128 (ループバックアドレス)

形式の設定	説明
サブネットマスクの形式	注意 このサブネットマスクにはブロードキャストまたはネットワークアドレスを指定できません。 2 進形式のサブネットマスクは、1 の連続で始まり、0 の連続で終わります。 IPv4 アドレスのサブネットマスクの例: • 255.255.255.0 の 2 進形式は 11111111.11111111.11111111.00000000 です。
サブネットプレフィックスの形式	IPv6 アドレスは、ビットのグループをコロンで区切った 16 進数のグループに変換します。IPv6 アドレスの左側の上位ビットはネットワークを指定し、残りの部分はそのネットワークの特定のアドレスを指定します。あるネットワークのすべてのアドレスの先頭の N ビットは同じで、「プレフィックス」と呼ばれます。 プレフィックスのビットの長さは「/N」のように示します。 IPv6 アドレスのサブネットプレフィックスの例: • 2001:db8::/32 の場合、プレフィックスは/32 で 32 ビットの長さとなります。 この例では、すべてのアドレスで最初の 32 ビットが 2001:db8 となることを示します。
デフォルトゲートウェイアドレスの形式	ゲートウェイは、IP アドレスと同じサブネットに指定する必要があります。
DNS	IPv4 または IPv6 アドレス

ネットワークインタフェースのポートの管理

手順

1. [管理] > [システム設定] > [ネットワークインタフェース] の順に選択します。
2. 各ポートのステータスを確認します。

3. (オプション) VLAN タグを使用している場合は、[各ストリームの VLAN タグを確認して接続を区別する] を選択して TCP 接続を区別します。

   注意

   このオプションを有効にすると、TCP 接続を区別するために、さらに各ストリームの VLAN ID が確認されます。

4. (オプション) SSL インスペクション製品を使用している場合は、Deep Discovery Inspector が復号された SSL トラフィックを特定する方法を指定します。

   a. 行の先頭にある右向き矢印 ( ) をクリックして、[インタフェース] パネルを開きます。

   b. [インタフェース] パネルで、[SSL 識別] チェックボックスをオンにします。

      [SSL 識別] をオンにすると、[条件の編集] オプションが表示されます。

   c. [条件の編集] をクリックします。

      [復号された SSL トラフィックの特定] 画面が表示されます。

   d. 復号された SSL トラフィックで使用される [マーカ VLAN タグ] または [TCP ポート] を設定します。

   e. [OK] をクリックします。

   f. 復号された SSL トラフィックを受信するインタフェースごとに前述の手順を繰り返します。

5. (オプション) カプセル化されたリモートミラーリング経由でトラフィックを受信する場合は、Deep Discovery Inspector で受信ポートを設定します。

   a. 行の先頭にある右向き矢印 ( ) をクリックして、[インタフェース] パネルを開きます。

b. [インタフェース] パネルで、[カプセル化されたリモートミラーリング] チェックボックスをオンにします。

c. [カプセル化されたリモートミラーリング] の横にあるテキストボックスに、IPv4 アドレスを入力します。

d. カプセル化されミラーリングされたトラフィックを受信するインタフェースごとに前述の手順を繰り返します。

6. [保存] をクリックします。

第 3 章

ダッシュボード

[ダッシュボード] タブ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。

- 28 ページの「ダッシュボードの概要」
- 28 ページの「タブ」
- 31 ページの「ウィジェット」
- 33 ページの「Deep Discovery Inspector のウィジェットについて」
- 34 ページの「Deep Discovery Inspector のウィジェット」
- 37 ページの「Deep Discovery Inspector の初期設定ウィジェットのタブ」
- 47 ページの「オプションのウィジェット」

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で、部分的に独立したダッシュボードが提供されます。ユーザアカウントのダッシュボードを変更すると、他のユーザアカウントのダッシュボードに影響します。

使用可能なウィジェットで Deep Discovery Inspector 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。

Deep Discovery Inspector のダッシュボードには次の情報が表示されます。ダッシュボードのウィジェットはカスタマイズでき、ユーザによる選択が可能です。

- システムデータとステータス
- 脅威データと分析
- 概要グラフ

さらにダッシュボードでは、Deep Discovery Inspector で検索したネットワークトラフィックの量をリアルタイムで監視します。

ダッシュボードには、次のユーザインタフェース要素が含まれています。

- 28 ページの「タブ」
- 31 ページの「ウィジェット」

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 20 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

表 3-1. 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。詳細については、29 ページの「タブの追加/変更」を参照してください。
タブ設定の編集	[タブ設定] をクリックします。詳細については、29 ページの「タブの追加/変更」を参照してください。
タブの移動	タブをドラッグアンドドロップして位置を変更します。詳細については、30 ページの「タブの移動」を参照してください。
タブを閉じる/タブの削除	初期設定のタブは閉じることはできますが、削除することはできません。 カスタマイズしたタブは削除することはできますが、閉じることはできません。 重要 タブを削除すると、そのタブに含まれているすべてのウィジェットが削除されます。 詳細については、30 ページの「タブを閉じる/タブの削除」を参照してください。

タブの追加/変更

手順

1. 新しいタブを追加する、または既存のタブを変更するには、次のいずれかの手順を実行します。
   - 新しいタブを追加するには、[ダッシュボード] 画面を表示して、「+」アイコンのタブをクリックします。

     [新規タブ] 画面が表示されます。
   - 既存のタブを変更するには、[ダッシュボード] > [タブ設定] の順に選択します。

[タブ設定] 画面が表示されます。

2. タブのタイトル、レイアウト、および自動調整オプションを変更します。

   注意
   自動調整機能は、選択したレイアウトとタブに追加されるウィジェットの数に影響を受けます。Deep Discovery Inspector で自動調整が機能するのは、自動調整が有効であり、行ごとに 1 つになるようにウィジェットが配置されている場合のみです。

3. [保存] をクリックします。

   更新されたタブが [ダッシュボード] 画面に表示されます。

タブの移動

手順

1. [ダッシュボード] を選択します。
2. タブをクリックして目的の位置にドラッグします。

   注意
   タブに含まれるウィジェットはすべてタブとともに移動します。

タブを閉じる/タブの削除

ダッシュボードで、閉じるまたは削除するタブを選択します。

- 初期設定のタブは閉じることはできますが、削除することはできません。
- カスタマイズしたタブは削除することはできますが、閉じることはできません。

重要

タブを削除すると、そのタブに含まれているすべてのウィジェットが削除されます。

手順

1. タブを閉じる、または削除するには、タブのタイトルの横にある アイコンをクリックします。
   - 初期設定のタブが閉じ、表示されなくなります。
   - カスタマイズしたタブは削除されます。

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。詳細については、31 ページの「ウィジェットのタスク」を参照してください。

ウィジェットのタスク

表 3-2. ウィジェットのタスク

タスク	手順
閉じる	ウィジェットを閉じて表示から削除します。
編集	• ウィジェットの名前を変更します。 • 表示オプションを変更します。 • データオプションを変更します。
エクスポート	ウィジェットデータに関する情報を含む.csv ファイルをダウンロードします。

タスク	手順
ヘルプ	ウィジェット、ウィジェットデータ、および設定、または編集可能なオプションについての情報を表示します。
更新	最新の情報を画面に表示します。 注意 ウィジェットの表示は自動的に更新されます。更新間隔はウィジェットごとに異なります。

ダッシュボードへのウィジェットの追加

手順

1. [ダッシュボード] 画面を表示して [ウィジェットの追加] をクリックします。
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。
   - 左側のナビゲーションパネルのカテゴリをクリックして、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。
3. (オプション) ページあたりのウィジェット数を変更するには、[レコード] ドロップダウンメニューから数字を選択します。
4. (オプション) 詳細表示と概要表示を切り替えるには、ページ上部にある表示アイコンをクリックします。
5. ウィジェットを選択するには、ウィジェットのタイトルの横にあるチェックボックスをオンにします。
6. [追加] をクリックします。

   ウィジェットがタブに追加されます。

Deep Discovery Inspector のウィジェットについて

Deep Discovery Inspector では、管理者がシステム脅威データをさまざまなウィジェットに表示できます。

初期設定では、ウィジェットは 5 つのタブに表示されます。

表 3-3. 初期設定のタブ

タブ	説明
概要	このタブには、優先的に注意する必要のあるホストとその他の実行可能な詳細情報を表示するウィジェットが含まれます。詳細については、37 ページの「概要」を参照してください。
脅威の監視	このタブには、脅威データをリアルタイムで表示するウィジェットが含まれます。これにより、管理者は影響を受けたホストを特定し、ネットワークの脅威の分布を確認できます。詳細については、40 ページの「脅威の監視」を参照してください。
仮想アナライザのステータス	このタブには、最も不審なファイル、仮想アナライザが検出したホストの上位、仮想アナライザで分析された不正なサイトの上位、および仮想アナライザのステータスと検出を表示するウィジェットが含まれます。詳細については、42 ページの「仮想アナライザのステータス」を参照してください。
傾向の上位	このタブには、事前定義済みの 8 種類の脅威の概要情報を表示するウィジェットが含まれます。詳細については、46 ページの「傾向の上位」を参照してください。
システムステータス	このタブには、Deep Discovery Inspector の基本ステータス(CPU 使用率、ディスク使用量、メモリ使用率など) を表示するウィジェットが含まれます。詳細については、47 ページの「システムステータス」を参照してください。

オプションで表示されていないウィジェットを任意のウィジェットタブに追加できます。詳細については、32 ページの「ダッシュボードへのウィジェットの追加」を参照してください。

脅威データを表示するウィジェットについては、117 ページの「[すべての検出] - [検出の詳細] - [検出情報]」で、表示される脅威の種類のリストを参照してください。

Deep Discovery Inspector のウィジェット

Deep Discovery Inspector には次のウィジェットがあります。

表 3-4. 概要ウィジェット

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、または 30 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。
脅威の概要	このウィジェットには、過去 24 時間、7 日間、または 30 日間以内に検出された各種の脅威数が表示されます。
検索された不正なネットワークトラフィック	このウィジェットには、Deep Discovery Inspector によって検出された、リアルタイム検索された不正トラフィックの総量が、HTTP、SMTP、およびその他のトラフィック別に時間単位で表示されます。
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、または 30 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。

表 3-5. 脅威の監視ウィジェット

ウィジェット	説明
脅威のグラフィック地図	このウィジェットには、過去 1 時間、本日、過去 7 日間、または過去 30 日間に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。
過去 30 日間の監視対象のネットワークトラフィック	このウィジェットには、過去 30 日間に Deep Discovery Inspector が監視したネットワークトラフィックのスループットが表示されます。

表 3-6. 仮想アナライザのステータスのウィジェット

ウィジェット	説明
仮想アナライザで検出されたホストの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間に脅威の影響を受けて仮想アナライザで分析された上位のホストが、検出数に基づいて表示されます。

ウィジェット	説明
仮想アナライザで分析された不正なサイトの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間に仮想アナライザで分析された上位の不正なサイトが、検出数および影響を受けたホスト数別に表示されます。
不審ファイルの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間に仮想アナライザで分析された上位の不審ファイルが、検出数および影響を受けたホスト数別に表示されます。
仮想アナライザ	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間の仮想アナライザの脅威の分析結果を含む、仮想アナライザのステータスが表示されます。

表 3-7. 傾向の上位ウィジェット

ウィジェット	説明
要注意アプリケーションの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最も多く検出された要注意アプリケーションが表示されます。
検出された不正 URL の上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最も多く検出された不正 URL が表示されます。

表 3-8. システムステータス関連のウィジェット

ウィジェット	説明
CPU 使用率	このウィジェットには、Deep Discovery Inspector で使用されている CPU ごとの CPU 使用率がリアルタイムで表示されます。 CPU 使用率が 85%以下の場合、インジケータの色が緑色になります。CPU 使用率が 85～95%では黄色に変わり、95%を超えると赤色になります。
ディスク使用率	このウィジェットには、すべてのディスクの使用量がリアルタイムで表示されます。使用されているディスク容量は緑色で表示されます (GB 単位)。使用可能なディスク容量は青色で表示されます (GB 単位)。

ウィジェット	説明
メモリ使用率	このウィジェットには、メモリの使用量がリアルタイムで表示されます。使用されているメモリ容量は緑色で表示されます (GB 単位)。使用可能なメモリ容量は青色で表示されます (GB 単位)。 メモリ使用率の情報は、事前設定コンソールでも参照可能です。

表 3-9. オプションのウィジェット

ウィジェット	説明
検索されたすべてのトラフィック	このウィジェットには、過去 24 時間に検索されたトラフィックの総量が、HTTP、SMTP、およびその他のトラフィック別に秒単位で表示されます。
検索された不正なネットワークトラフィック	このウィジェットには、Deep Discovery Inspector によって検出されたリアルタイムの不正なトラフィックの総量が、HTTP、SMTP、およびその他のトラフィック別に秒単位で表示されます。
リアルタイム検索されたトラフィック	このウィジェットには、Deep Discovery Inspector によって検索されたリアルタイムのトラフィックの総量が、HTTP、SMTP、およびその他のトラフィック別に秒単位で表示されます。
セキュリティホールを悪用されたホストの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最も多くセキュリティホールが悪用されたホストが表示されます。
グレーウェアに感染したホストの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最もグレーウェアに感染したホストが表示されます。
検出された不正コンテンツの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最も多く検出された脅威が表示されます。
不正プログラムに感染したホストの上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最も不正プログラムの影響を受けたホストが表示されます。
検出された不審動作の上位	このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最も多く検出された不審動作が表示されます。

オプションのウィジェットを任意のウィジェットタブに追加できます。

Deep Discovery Inspector の初期設定ウィジェットのタブ

概要

[概要] タブには、優先的に注意する必要のあるホストとその他の実行可能な詳細情報を表示するウィジェットが含まれます。

初期設定では、このタブには次のウィジェットが表示されます。

- 37 ページの「脅威検出状況の概要」
- 39 ページの「影響を受けたホストの上位」
- 39 ページの「脅威の概要」
- 39 ページの「検索された不正なネットワークトラフィック」
- 40 ページの「検索されたプロトコル別トラフィック」

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 3-10. 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 [標的型攻撃が検出されたホスト] 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。

メトリック	ソース	説明
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 通信が検出されたホスト] 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 [内部活動が検出されたホスト] 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	すべての検出	• 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、[すべての検出] 画面に詳細が表示されます。
潜在的な脅威	すべての検出	• 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、[すべての検出] 画面に詳細が表示されます。
メールによる脅威	すべての検出	• 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、[すべての検出] 画面に詳細が表示されます。

この時間の初期設定は [過去 24 時間] です。

ウィジェットのタイトルを変更するには、[編集] をクリックします。

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、または 30 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。

[編集] をクリックすると、影響を受けたホストの総表示数を変更できます (最大 20 件)。

ホストの重大度スケールの詳細については、5 ページの「ホストの重大度」を参照してください。

脅威の概要

このウィジェットには、過去 24 時間、7 日間、または 30 日間以内の脅威の総数が表示されます。情報は、時間と脅威の総数を関連付けてグラフで表示されます。脅威の種類は色で区別されます。

時間範囲は左上のドロップダウンで変更できます。

バーをクリックすると、当該期間の [検出の種類: 不正な動作] フィルタが適用された [すべての検出] 画面が表示されます。

グラフに表示される脅威の種類をフィルタするには、[編集] をクリックします。

検索された不正なネットワークトラフィック

このウィジェットには、Deep Discovery Inspector によって検出された、リアルタイム検索された不正トラフィックの総量が、HTTP、SMTP、およびその他のトラフィック別に時間単位で表示されます。このデータには、次のトラフィックの種類別にフィルタを適用できます。

- すべてのトラフィック
- HTTP
- SMTP
- その他

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、または 30 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。

[編集] をクリックすると、データの表示形式を棒グラフ、円グラフ、または折れ線グラフから選択できます。表示するプロトコルは最大 10 種類まで選択できます。

脅威の監視

[脅威の監視] タブには、脅威データをリアルタイムで表示するウィジェットが含まれます。これにより、管理者は影響を受けたホストを特定し、ネットワークの脅威の分布を確認できます。

初期設定では、このタブには次のウィジェットが表示されます。

- 40 ページの「脅威のグラフィック地図」
- 41 ページの「過去 30 日間の監視対象のネットワークトラフィック」

脅威のグラフィック地図

[脅威のグラフィック地図] ウィジェットは、影響を受けたホストの仮想世界地図上のグラフィカル表示です。選択した期間内に世界各国で影響を受けたホストが、次のカテゴリに応じて表示されます。

- 不正プログラムの送信元
- ネットワークのセキュリティホール悪用元
- ドキュメントのセキュリティホール悪用元
- 不正なメールの送信元
- 不正プログラムのコールバック (C&C) 送信先

[脅威のグラフィック地図] 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、Deep Discovery Inspector の所在地が赤色のピンポイントで表示されます。

[脅威のグラフィック地図] での情報の表示

手順

1. 次のいずれかの期間を選択します。
   - 過去 1 時間
   - 本日
   - 過去 7 日間
   - 過去 30 日間
2. 位置を変更します。
   a. [脅威のグラフィック地図] で [編集] アイコンをクリックします。

      編集画面が表示されます。

   b. 編集画面で、位置を選択します。

   c. [適用] をクリックします。

      [脅威のグラフィック地図] が更新され、新しい位置が表示されます。
3. 任意の場所をクリックすると、関連情報がポップアップ画面に表示されます。

   注意

   右側のペインには、影響を受けたホストの情報が国別に整理されて表示されます。
4. ポップアップ画面の脅威のイベント総数をクリックします。

   脅威、国、および期間に関連する、すべての脅威の詳細を示した表が表示されます。
5. この表で [表示] をクリックすると、検出の詳細が表示されます。

過去 30 日間の監視対象のネットワークトラフィック

このウィジェットには、過去 30 日間に Deep Discovery Inspector が監視したトラフィックの総量がグラフで表示されます。これには復号された TLS トラ

フィックも含まれます。グラフの上にマウスを重ねると、トラフィックのサイズと種類が表示されます。Deep Discovery Inspector が帯域幅の最大容量を超過、または超過しそうな場合は、帯域幅の最大容量を示す赤色の線が表示されます。

タイムラインのセクションでマウスをクリックしてドラッグし、リリースすると、表示を拡大できます。表示をリセットするには、[リセット] をクリックします。

このウィジェットを確認することで、ネットワークトラフィックを検索するのに十分な帯域幅が Deep Discovery Inspector にあるかどうか、過去 30 日間分を評価することが出来ます。

仮想アナライザのステータス

仮想アナライザのウィジェットは、Deep Discovery Inspector で検出され、仮想アナライザで分析されたすべての APT (標的型サイバー攻撃) を表示します。

初期設定では、このタブには次のウィジェットが表示されます。

- 42 ページの「仮想アナライザで検出されたホストの上位」
- 43 ページの「仮想アナライザで分析された不正なサイトの上位」
- 43 ページの「不審ファイルの上位」
- 44 ページの「仮想アナライザ」

この概要データを使用して、ネットワークに影響を与えている脅威のファイルタイプ、影響を受けたホスト、およびネットワークアクセスを試行する不正サイトを詳細に把握できます。

仮想アナライザで検出されたホストの上位

このウィジェットには、脅威の影響を受けて仮想アナライザで分析されたホストの上位が、検出数に基づいて表示されます。

過去 1 時間、24 時間、7 日間、または 30 日間以内に攻撃を受けたホストおよび検出された攻撃の種類が表示されるため、ユーザ (通常はシステム管理者またはネットワーク管理者) は適切な処理 (ネットワークアクセスのブロック、IP アドレスに応じたコンピュータの隔離) を行い、影響を受けたホストの不正な動作を防止できます。

バーをクリックすると、当該ホストの選択した期間の [フィルタされた検出] 画面が表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。影響を受けたホストの総表示数も設定できます (最大 20 件)。

仮想アナライザで分析された不正なサイトの上位

このウィジェットには、仮想アナライザで分析された不正なサイトの上位が、影響を受けたホスト別の検出数で表示されます。Trend Micro Smart Protection Network と組み合わせた場合、Deep Discovery Inspector は接続先のセキュリティレベルを問い合わせます。

過去 1 時間、24 時間、7 日間、または 30 日間以内にシステムホストに対して攻撃を仕掛けた不正サイトの上位が表示されるため、ユーザ (通常はシステム管理者またはネットワーク管理者) は適切な処理 (プロキシまたは DNS サーバによる、これらの不正な接続先へのネットワークアクセスのブロック) を行い、影響を受けたホストの不正な動作を防止できます。

選択した期間内に検出された不正なサイトはすべて表に表示されます。

行をクリックすると、当該不正サイトの選択した期間の [フィルタされた検出] 画面が表示されます。

不審ファイルの上位

このウィジェットには、仮想アナライザで分析された不審ファイルの上位と、次の情報が表示されます。

- Deep Discovery Inspector で検出されたファイル数
- 不審ファイルの影響を受けたホスト。

過去 1 時間、24 時間、7 日間、30 日間にホストに影響を及ぼした不審ファイルがグラフィカルな形式で表示されるため、ユーザ (通常はシステム管理者またはネットワーク管理者) は、メールの受信拒否リストへの追加、HTTP サーバまたは FTP サーバの変更、システムファイルの修正、レジストリキーの作成などの適切な処置を実施し、影響を受けたホストの不正な動作を削除します。

影響を受けたホストについて、次のデータが収集されます。

表 3-11. [不審ファイルの上位] のデータ

列の名前	説明
ファイル名/SHA-1	不審ファイル名または SHA-1
検出	特定の期間内に Deep Discovery Inspector で検出されたイベント
影響を受けたホスト	不審ファイルの影響を受けたすべてのホスト
不正プログラム名	既知の不正プログラムの名前
重大度	不審ファイルの脅威レベル

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。表示する不審ファイルの総数も設定できます (最大 20 件)。

パスワード保護された.zip アーカイブ内の不審ファイルをダウンロードするには、ファイル名の横にあるダウンロードアイコン ( ) をクリックします。

行をクリックすると、当該不正ファイルの選択した期間の [フィルタされた検出] 画面が表示されます。

仮想アナライザ

このウィジェットは、仮想アナライザで分析するファイルに関する情報を表示します。

このウィジェットは次の目的に使用します。

- 仮想アナライザに関する情報を知る
- 仮想アナライザによる分析全体の結果を表示する

ウィジェットを使用して次の処理を実行することもできます。

- [期間] (過去 30 日間、7 日間、24 時間、または 1 時間) の指定に基づいて情報をフィルタする
- グラフのセクションにマウスを重ねて不正または不正でないと分析されたファイルの割合を表示する

このウィジェットには次の情報をまとめた表が表示されます。

仮想アナライザの種類	表示される情報
内部	• 分析モジュール: 内部 • 仮想アナライザのステータス: 有効 • 前回分析されたファイル: 最後に検索したファイル名または SHA-1 • 前回のファイル分析日 • 分析待ちファイル数 • 1 時間あたりの分析ファイル数
外部	• 分析モジュール: 外部 • 前回分析されたファイル: 最後に検索したファイル名または SHA-1 • 前回のファイル分析日 • 分析待ちファイル数 • 1 時間あたりの分析ファイル数
Sandbox as a Service	• 分析モジュール: Sandbox as a Service • 仮想アナライザのステータス: 有効 • 前回分析されたファイル: 最後に検索したファイル名または SHA-1 • 前回のファイル分析日 • 分析待ちファイル数 • 1 時間あたりの分析ファイル数
Trend Vision One — Sandbox Analysis	• 分析モジュール: Trend Vision One — Sandbox Analysis • 仮想アナライザのステータス: 有効 • 前回分析されたファイル: 最後に検索したファイル名または SHA-1 • 前回のファイル分析日 • 分析待ちファイル数 • 1 時間あたりの分析ファイル数

傾向の上位

[傾向の上位] タブには、さまざまな視点から見た脅威の概要情報が表示されます。この脅威データを使用して、最も危険なホストや最も大きな損害をもたらす脅威を特定し、適切な処置を実施できます。Deep Discovery Inspector の複数のウィジェットは、特定の期間内に最も影響を受けたホストと最も大きな損害をもたらした脅威を特定します。ウィジェットごとに、詳細な脅威のログをエクスポートして詳細に分析できます。

初期設定では、このタブには次のウィジェットが表示されます。

- 46 ページの「要注意アプリケーションの上位」
- 46 ページの「検出された不正 URL の上位」

要注意アプリケーションの上位

このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内の要注意アプリケーションが表示されます。

バーをクリックすると、[プロトコル] と [検出の種類: 要注意アプリケーション] のフィルタが適用された [すべての検出] 画面が表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。表示する要注意アプリケーションの総数も設定できます (最大 20 件)。

検出された不正 URL の上位

このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内に最も多く検出された不正 URL が表示されます。

初期設定では、選択した期間内のすべての検出が、URL と総検出数を含む表に表示されます。

行をクリックすると、[IP アドレス/ドメイン/URL] と [検出の種類: 不正 URL] のフィルタが適用された [すべての検出] 画面が表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。表示するホストの総数も設定できます (最大 20 件)。

システムステータス

[システムステータス] タブは、Deep Discovery Inspector のリソース状況を管理者に通知します。リソースが不足している場合、システム障害が発生する可能性があります。これらのウィジェットには、Deep Discovery Inspector のすべてのリソースがそのキャパシティ内で動作していることを確認するために、リアルタイムでシステムリソースデータが表示されます。

初期設定では、このタブには次のウィジェットが表示されます。

- 47 ページの「CPU 使用率」
- 47 ページの「ディスクの使用状況」
- 47 ページの「メモリ使用率」

CPU 使用率

このウィジェットには、各 CPU の使用率が表示されます。

ディスクの使用状況

このウィジェットには、アプライアンスで使用可能なディスク容量が表示されます。

メモリ使用率

このウィジェットには、アプライアンスで使用可能なメモリ容量が表示されます。

オプションのウィジェット

初期設定では、次のウィジェットは、Deep Discovery Inspector 6.8 では表示されませんが、任意のウィジェットタブに追加できます。

- 48 ページの「検索されたすべてのトラフィック」
- 48 ページの「不正なリアルタイムネットワークトラフィック」
- 49 ページの「リアルタイム検索されたトラフィック」
- 49 ページの「セキュリティホールを悪用されたホストの上位」

- 49 ページの「グレーウェアに感染したホストの上位」
- 50 ページの「検出された不正コンテンツ の上位」
- 50 ページの「不正プログラムに感染したホストの上位」
- 50 ページの「検出された不審動作の上位」

検索されたすべてのトラフィック

このウィジェットには、過去 24 時間に検索されたすべてのトラフィックが表示され、トラフィックの種類別にフィルタを適用できます。

- すべてのトラフィック
- HTTP
- SMTP
- その他

不正なリアルタイムネットワークトラフィック

このウィジェットには、Deep Discovery Inspector で検出されたすべての不正トラフィックが折れ線グラフで表示されます。次のトラフィックの種類別にフィルタを適用できます。

- すべてのトラフィック
- HTTP
- SMTP
- その他

トラフィックサイズは、右から左方向へのタイムスケールを使用して、秒単位で表示されます。グラフ上の折れ線にマウスを重ねると、トラフィックサイズが表示されます。

[編集] をクリックすると、データの表示をトラフィックサイズまたはパーセントで切り替えることができます。検索されたすべてのトラフィックデータの表示/非表示を切り替えることもできます。

リアルタイム検索されたトラフィック

このウィジェットには、リアルタイムの HTTP、SMTP、またはその他のトラフィックに関するすべての情報に基づいて、検索されたトラフィックが折れ線グラフで表示されます。タイムスケールは右から左方向に秒単位で移動します。グラフ上の折れ線にマウスを重ねると、トラフィックサイズが表示されます。

セキュリティホールを悪用されたホストの上位

このウィジェットでは、過去 1 時間、24 時間、7 日間、または 30 日間以内にセキュリティホールを悪用された、ホストの上位が表示されます。初期設定では、選択した期間内にセキュリティホールを悪用されたすべてのホストが、セキュリティホールを悪用されたホストの上位の IP アドレスと総検出数を示す表に表示されます。

行をクリックすると、当該ホストの [検出の種類: 攻撃コード] フィルタが適用された [ホストの詳細] 画面が表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。セキュリティホールを悪用されたホストの総表示数も設定できます (最大 20 件)。

グレーウェアに感染したホストの上位

このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内にネットワーク上で最も多く検出されたグレーウェアが表示されます。

注意

このウィジェットには、重大度「高」として分類された脅威を持つホストのみが表示されます。

初期設定では、選択した期間内に検出されたグレーウェアがすべて表に表示されます。

行をクリックすると、当該ホストの [検出の種類: グレーウェア] フィルタが適用された [ホストの詳細] 画面が表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。グレーウェアに感染したホストの総表示数も設定できます (最大 20 件)。

検出された不正コンテンツ の上位

このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内にネットワーク上で最も多く検出された既知の不正プログラムが表示されます。

初期設定では、選択した期間内に検出された既知の不正プログラムがすべて表に表示されます。

行をクリックすると、[脅威/検出/参照] フィルタが適用された [すべての検出] 画面が表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。セキュリティホールを悪用されたホストの総表示数も設定できます (最大 20 件)。

不正プログラムに感染したホストの上位

このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内にネットワーク上で最も不正プログラムに感染したホストが表示されます。

初期設定では、選択した期間内に不正プログラムに感染したすべてのホストが、それらのホストの IP アドレスと総検出数を示す表に表示されます。

行をクリックすると、当該ホストの [検出の種類: 不正な動作] フィルタが適用された [ホストの詳細] 画面が表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。不正プログラムに感染したホストの総表示数も設定できます (最大 20 件)。

検出された不審動作の上位

このウィジェットには、過去 1 時間、24 時間、7 日間、または 30 日間以内にネットワーク上で最も多く検出された不審動作が表示されます。

初期設定では、選択した期間内のすべての不審動作が、不審動作の上位の説明と総検出数を含む表に表示されます。

行をクリックすると、[脅威/検出/参照] フィルタが適用された [すべての検出] 画面に重要度の高い検出のみが表示されます。

[編集] をクリックすると、データの表示形式を図、グラフ、または表から選択できます。表示する不審動作の総数も設定できます (最大 20 件)。

第 4 章

検出

[検出] タブ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。

- 54 ページの「[検出] 画面について」
- 55 ページの「影響を受けたホスト」
- 98 ページの「C&C コールバックアドレス」
- 99 ページの「仮想アナライザ不審オブジェクト」
- 101 ページの「ユーザ指定の不審オブジェクト」
- 102 ページの「Retro Scan」
- 107 ページの「すべての検出」

[検出] 画面について

図 4-1. 検出のカテゴリ

[検出] タブでは、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。

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、55 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、5 ページの「ホストの重大度」を参照してください。
C&C コールバックアドレス	既知の C&C アドレスへのコールバック試行を行ったアドレス 詳細については、98 ページの「C&C コールバックアドレス」を参照してください。
仮想アナライザ不審オブジェクト	仮想アナライザによって特定された、または外部ソースから取得された不審オブジェクト 詳細については、99 ページの「仮想アナライザ不審オブジェクト」を参照してください。
ユーザ指定の不審オブジェクト	外部ソースから取得された不審オブジェクトと除外 詳細については、101 ページの「ユーザ指定の不審オブジェクト」を参照してください。
Retro Scan	クラウドベースのサービスで、ネットワーク内での C&C サーバへのコールバック回数や、関連するその他のアクティビティについての Web アクセス履歴ログを検索します。 詳細については、102 ページの「Retro Scan」を参照してください。
すべての検出	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、107 ページの「すべての検出」を参照してください。

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、5 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。
   - [ホストの詳細] ビューへのアクセスを提供します。

     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] ビューが検索されます。
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。
   - [検出の詳細] ビューへのアクセスを提供します。

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

標的型攻撃の検出の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 4-1. 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。	
	高のみ	重大度が高の検出のみを表示します。
		重大度が高および中の検出を表示します。
		重大度が高、中、および低の検出を表示します。
	すべて	情報検出を含むすべての検出を表示します。
期間	過去 1 時間	
	過去 24 時間 (初期設定)	
	過去 7 日間	
	過去 30 日間	
	カスタム範囲 現在の日付から過去 31 日間のカスタム範囲を指定します。	
列のカスタマイズ	オプションの列を表示します。	

フィルタオプション	説明
基本検索	IP アドレスまたはホスト名を検索します。 ヒント 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。

事前設定された検索フィルタ	事前設定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、次の事前設定された検索フィルタが含まれています。
	  • 標的型攻撃が検出されたホスト
	  • C&C 通信が検出されたホスト
	  • 内部活動が検出されたホスト
	• [影響を受けたホスト] – [ホストの詳細] ビューには、次の事前設定された検索フィルタが含まれています。
	  • 脅威
	  • 既知の脅威
	  • 潜在的な脅威
	  • ランサムウェア

詳細検索フィルタ	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、78 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の表示

手順

1. [検出] > [影響を受けたホスト] の順に選択します。
2. 検出の重大度を設定するには、[検出の重大度] スライダを目的のレベルにドラッグします。
3. 期間を選択します。
4. [列のカスタマイズ] をクリックして表示するオプションの列を 1 つ以上選択し、[適用] をクリックして、変更された [影響を受けたホスト] 画面に戻ります。

図 4-2. 列のカスタマイズ

表 4-2. [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 (Media Access Control) アドレス。
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。 ホストの重大度の詳細については、5 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 4-3. [重要な統計] 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、4 ページの「APT 攻撃シーケンス」を参照してください。

表 4-4. [攻撃段階] の列

列	事前選択済み	説明
情報収集 (Intelligence Gathering)	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。
初期侵入 (Point of Entry)	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。

列	事前選択済み	説明
内部活動 (Lateral Movement)	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 (Asset/Data Discovery)	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 (Data Exfiltration)	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。

5. 基本検索を実行するには、次のいずれかを実行します。

   - 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、<Enter> キーを押します。
   - 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。

6. 保存された検索条件を実行するには、[検出] > [影響を受けたホスト] の順に選択して、検索ボックスのドロップダウンメニューを開き、保存された検索条件をクリックします。

   次の事前設定された検索条件が用意されています。

   表 4-5. 事前設定された検索条件

名前	フィルタオプション
標的型攻撃が検出されたホスト	標的型攻撃に関連する注意すべきイベント
C&C 通信が検出されたホスト	C&C 通信に関連する注意すべきイベント

名前	フィルタオプション
内部活動が検出されたホスト	内部活動に関連する注意すべきイベント

7. 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、78 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。

8. [エクスポート] をクリックします。

   次のファイルがダウンロードされます。

   - affected_host.csv

[影響を受けたホスト] - [ホストの詳細] の表示

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。

   図 4-3. [影響を受けたホスト] - [ホストの詳細]

3. 検出の重大度を設定するには、[検出の重大度] スライダをドラッグします。
4. 期間を選択します。
5. 表示する列を選択するには、[列のカスタマイズ] をクリックします。列を 1 つ以上選択し [適用] をクリックして、変更された [影響を受けたホスト] 画面に戻ります。

表 4-6. [影響を受けたホスト] - [ホストの詳細] の列

列	事前選択済み
ステータス	X
タイムスタンプ	X
送信元ホスト	
送信先ホスト	
注目すべきホスト	
ピアホスト	X
送信者	
受信者	
メールの件名	
ユーザアカウント	
脅威の詳細	X
検出名	X
検出の種類	
プロトコル	X
検出の重大度	X
攻撃段階	X
方向	X
顕著なオブジェクト	X

注意

初期設定の [タイムスタンプ] 列と [脅威の詳細] 列は削除できません。

6. (オプション) [表示されている検出を解決済みに設定] をクリックすると、現在画面に表示されているすべての検出を解決済みに設定できます。

[ステータス] 列で アイコンが に変更されます。

注意

表示されているすべての検出を解決済みに設定した後、検出を未解決に変更する場合は個別に変更します。

7. 基本検索を実行するには、次のいずれかを実行します。
   - 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、<Enter> キーを押します。
   - 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 [ホストの詳細] 画面が検索できます。
8. 影響を受けたピアホストに、次のいずれかのマークを付けます。
   - ネットワークグループ
   - 登録済みドメイン
   - 登録済みサービス

   次のいずれかを実行してドロップダウンメニューを開き、ホストにマークを付けます。
   - IP アドレスの横にある アイコンをクリックします。
   - [ピアホスト] 列の アイコンをクリックします。
9. 保存された検索条件を実行するには、検索ボックスのドロップダウンメニューを開き、保存された検索条件をクリックします。

   [影響を受けたホスト] - [ホストの詳細] 画面に、次の事前設定された検索条件が表示されます。

表 4-7. 事前設定された検索条件

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

10. 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、86 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。

11. [エクスポート] をクリックします。

    次のファイルを含む zip アーカイブがダウンロードされます。

    - threats.csv
    - malicious_urls.csv
    - application_filters.csv
    - correlated_incidents.csv

[影響を受けたホスト] - [検出の詳細] の表示

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] - [検出の詳細] 画面の [詳細] 列の下で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。

   図 4-4. [影響を受けたホスト] - [検出の詳細]

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。
   - [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。
   - 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。

     パケットキャプチャの詳細については、213 ページの「パケットキャプチャ」を参照してください。
   - [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。
5. [軽減策の提案] には、脅威の説明、ホストに対する影響、およびその脅威から保護するための推奨処理が表示されます。

[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。

- 67 ページの「接続の詳細」
- 73 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]」
- 76 ページの「[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]」
- 78 ページの「軽減策の提案」

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] セクションには、次の情報が含まれます。

- 69 ページの「[影響を受けたホスト] - [検出の詳細] - [検出情報]」
- 71 ページの「[影響を受けたホスト] - [検出の詳細] - [接続の概要]」
- 71 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]」
- 73 ページの「[影響を受けたホスト] - [検出の詳細] - [ファイル情報]」
- 73 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 [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。

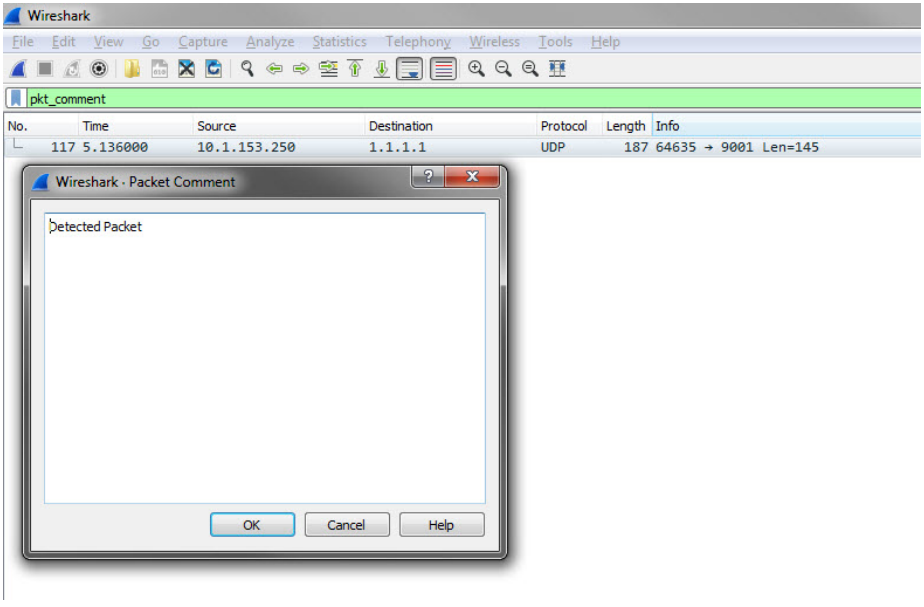


図 4-5. 検出されるパケット例

パケットキャプチャの詳細については、213 ページの「パケットキャプチャ」を参照してください。

[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。

[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。

© 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 4-8. 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
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

検出の種類	説明
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。

- 74 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]」
- 75 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]」
- 76 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。

© 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] セクションには、次の情報が含まれます。

- 76 ページの「[影響を受けたホスト] - [検出の詳細] - [不審オブジェクト情報]」
- 77 ページの「[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]」

[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。

- 有効期限
- 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。

© 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

軽減策の提案

[軽減策の提案] セクションには、次の情報が表示されます。

- 詳細情報
- 詳細な説明
- 影響
- 一次処理

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] ビュー

  詳細については、79 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] ビュー

  詳細については、86 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

各詳細検索フィルタには次を含めます。

- 最大 20 件の条件セット
- 各テキストベースの値フィールドに最大 1024 文字

最大 50 件の詳細検索フィルタを保存できます。

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 4-9. 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	値を入力
IP アドレス	次の値を含む/次の値を含まない 範囲内/範囲外	値を入力 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。 • すべてのグループ • 初期設定

属性	演算子	処理
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
登録済みサービス	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。 • Active Directory • 認証サーバ - Kerberos • コンテンツ管理サーバ • データベースサーバ • DNS • ドメインコントローラ • ファイルサーバ • FTP • HTTP プロキシ • Radius サーバ • セキュリティ監査サーバ • SMTP • SMTP オープンリレー • ソフトウェアアップデートサーバ • Web サーバ

詳細については、次を参照してください。

- 81 ページの「影響を受けたホストの詳細検索フィルタの追加」
- 82 ページの「[影響を受けたホスト] の保存された検索条件の編集」
- 84 ページの「[影響を受けたホスト] の保存された検索条件のインポート」

影響を受けたホストの詳細検索フィルタの追加

手順

1. 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. [フィルタ] ドロップダウンメニューを開き、[注目すべきホスト] 属性および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。
   - ドロップダウンメニューから処理を選択します。

   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、79 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

   複数の条件エントリを追加するにはカンマで区切ります。
4. (オプション) 検索フィルタに他の条件セットを含めるには、[新規追加] をクリックします。

   各詳細検索フィルタには次を含めます。
   - 最大 20 件の条件セット
   - 各テキストベースの値フィールドに最大 1024 文字

   最大 50 件の詳細検索フィルタを保存できます。
5. [検索] 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. (オプション) 検索を保存するには、次を実行します。

   a. [保存] アイコンをクリックし、[名前を付けて保存...] をクリックします。

      [保存された検索条件] 画面が開きます。

   b. 名前を入力して、[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) 詳細検索機能を終了して前の画面に戻るには、[キャンセル] をクリックします。

[影響を受けたホスト] の保存された検索条件の編集

手順

1. [影響を受けたホスト] で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] ドロップダウンメニューを開きます。
2. 編集する保存された検索条件を選択し、 アイコンをクリックします。
3. 属性および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。
   - ドロップダウンメニューから処理を選択します。

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、79 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

複数の条件エントリを追加するにはカンマで区切ります。

5. (オプション) 他の条件セットを含めるには、[新規追加] をクリックします。

   各詳細検索フィルタには次を含めます。

   - 最大 20 件の条件セット
   - 各テキストベースの値フィールドに最大 1024 文字

6. [検索] 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。

7. (オプション) 編集した検索を保存するには、[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。

   - 編集した検索を同じ名前で保存するには、[保存] をクリックします。
   - 編集した検索を新しい名前で保存するには、次を実行します。

   a. [名前を付けて保存...] をクリックします。

      [保存された検索条件] 画面が開きます。

   b. 名前を入力して、[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。

8. (オプション) 詳細検索機能を終了するには、次のいずれかを実行します。
   - 元の画面に戻るには、[キャンセル] をクリックします。
   - 基本検索を実行するには、保存された検索条件をクリックします。

[影響を受けたホスト] の保存された検索条件の削除

重要

保存された検索条件を削除すると、その検索に関連付けられているレポートスケジュールも削除されます。ただし、生成されたレポートは削除されません。

手順

1. 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] ドロップダウンメニューを開きます。
2. 削除する検索の横にある [削除] アイコンをクリックします。

注意

事前設定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のインポート

手順

1. 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] の順に選択して、[保存された検索条件] ドロップダウンメニューを開きます。

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をインポート] 画面が表示されます。

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

   ファイルがアップロードされ、検証されます。初期設定では、すべての有効な保存された検索条件が選択され、インポートされます。

   Deep Discovery Inspector では、現在の製品バージョンと互換性のない保存された検索条件は無効になります。

4. (オプション) 保存された検索条件の名前をインポート前に変更するには、保存された検索条件の名前にマウスを重ねて編集アイコンをクリックします。

   注意

   保存された検索条件の名前が重複している場合は、インポート前に名前を変更する必要があります。名前が重複している保存された検索条件は赤いボックスで強調表示されます。

5. 保存された検索条件の横にあるチェックボックスでインポート対象を個別に選択するか、列上部にあるチェックボックスですべての保存された検索条件を選択します。

6. [インポート] をクリックします。

   インポートした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のエクスポート

手順

1. 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] の順に選択して、[保存された検索条件] ドロップダウンメニューを開きます。

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] 画面が表示されます。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。

3. 保存された検索条件の横にあるチェックボックスでインポート対象を個別に選択するか、列上部にあるチェックボックスですべての保存された検索条件を選択します。

   注意

   Deep Discovery Inspector では初期設定されている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 4-10. 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	例
ホスト名	次の値を含む/次の値を含まない	値を入力	computer.example.com
IP アドレス	次の値を含む/次の値を含まない 範囲内/範囲外	値を入力 範囲を入力	10.1.1.2
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	AA:AA:AA:AA:AA:AA

属性	演算子	処理	例
ネットワークグループ	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。 • すべてのグループ • 初期設定	
登録済みサービス	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。 • Active Directory • 認証サーバ - Kerberos • コンテンツ管理サーバ • データベースサーバ • DNS • ドメインコントローラ • ファイルサーバ • FTP • HTTP プロキシ • Radius サーバ • セキュリティ監査サーバ • SMTP • SMTP オープンリレー • ソフトウェアアップデートサーバ • Web サーバ	
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	次を 1 つ以上選択します。 • すべてのプロトコル • 検索したいプロトコル • その他	
Transport Layer Security (TLS)	Over SSL/TLS Over SSL/TLS を使用しない		

属性	演算子	処理	例
方向	等しい	次のいずれかを選択します。 • 内部 • 外部	
ステータス	等しい	次のいずれかを選択します。 • 解決済み • 未解決	
脅威/検出/参照	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	VAN_RANSOMWARE.UMXX
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	707-710、721-727
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	707-710、721-727
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	

属性	演算子	処理	例
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	
YARA ルールファイル/YARA ルール	次の値を含む/次の値と等しい	値を入力	myYARAFile
	YARA 検出あり		
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	
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	computer.example.com
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。 • 高 • 中 • 低	
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		

属性	演算子	処理	例
標的型攻撃に関連している	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 • 既知の不正プログラム	
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	値を入力	myFile
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	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145
SHA-256	ファイルの SHA-256 あり/ファイルの SHA-256 なし		

属性	演算子	処理	例
	次の値を含む/次の値を含まない	値を入力	8b7df143d91c716ecfa5fc1730022f6b421b05cedee8fd52b1fc65a96030ad52
IP アドレス/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	10.1.1.2
不審オブジェクト/拒否リストのエンティティ	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	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145
メールアドレス	メールアドレスあり/メールアドレスなし		example@example.com
	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		

属性	演算子	処理	例
	次の値を含む/次の値を含まない	値を入力	950124.162336@example.com
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	mySubject

詳細については、次を参照してください。

- 92 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の追加」
- 94 ページの「[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編集」
- 96 ページの「[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」

[影響を受けたホスト] - [ホストの詳細] の詳細検索フィルタの追加

手順

1. [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作成するには、[検出] > [影響を受けたホスト] の順に選択し、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. [詳細] をクリックします。
3. [フィルタ] ドロップダウンメニューを開き、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。

- ドロップダウンメニューから処理を選択します。

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、79 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

複数の条件エントリを追加するにはカンマで区切ります。

5. (オプション) 検索フィルタに他の条件セットを含めるには、[新規追加] をクリックします。

   各詳細検索フィルタには次を含めます。

   - 最大 20 件の条件セット
   - 各テキストベースの値フィールドに最大 1024 文字

   最大 50 件の詳細検索フィルタを保存できます。

6. [検索] 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。

7. (オプション) 検索を保存するには、次を実行します。

   a. [保存] アイコンをクリックし、[名前を付けて保存...] をクリックします。

      [保存された検索条件] 画面が開きます。

   b. 名前を入力して、[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。

8. (オプション) 詳細検索機能を終了するには、[キャンセル] をクリックします。

[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編集

手順

1. [影響を受けたホスト] - [ホストの詳細] で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、検出リンクをクリックします。
2. [保存された検索条件] ドロップダウンメニューを開きます。
3. 編集する保存された検索条件を選択します。
4. 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。
   - アイコンをクリックします。
   - [詳細] をクリックします。
5. 属性および関連付けられた演算子を選択します。
6. 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。
   - ドロップダウンメニューから処理を選択します。

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、79 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

複数の条件エントリを追加するにはカンマで区切ります。

7. (オプション) 検索フィルタに他の条件セットを含めるには、[新規追加] をクリックします。

注意

各詳細検索フィルタには次を含めます。

- 最大 20 件の条件セット
- 各テキストベースの値フィールドに最大 1024 文字

最大 50 件の詳細検索フィルタを保存できます。

8. [検索] 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。

9. (オプション) 編集した検索を保存するには、[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。

   - 編集した検索を同じ名前で保存するには、[保存] をクリックします。

     編集した検索が元の名前で保存されます。

   - 編集した検索を新しい名前で保存するには、次を実行します。

   a. [名前を付けて保存...] をクリックします。

      [保存された検索条件] 画面が開きます。

   b. 名前を入力して、[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。

10. (オプション) 詳細検索機能を終了するには、次のいずれかを実行します。
    - 元の画面に戻るには、[キャンセル] をクリックします。
    - 基本検索を実行するには、保存された検索条件をクリックします。

[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削除

手順

1. [影響を受けたホスト] 画面から [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
2. 保存された検索条件を削除するには、[保存された検索条件] ドロップダウンメニューを開きます。
3. 削除する検索の横にある [削除] アイコンをクリックします。

注意

事前設定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. 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] の順に選択して、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] ドロップダウンメニューを開きます。
3. [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をインポート] 画面が表示されます。

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

   ファイルがアップロードされ、検証されます。初期設定では、すべての有効な保存された検索条件が選択され、インポートされます。

   Deep Discovery Inspector では、現在の製品バージョンと互換性のない保存された検索条件は無効になります。

5. (オプション) 保存された検索条件の名前をインポート前に変更するには、保存された検索条件の名前にマウスを重ねて編集アイコンをクリックします。

   注意

   保存された検索条件の名前が重複している場合は、インポート前に名前を変更する必要があります。名前が重複している保存された検索条件は赤いボックスで強調表示されます。

6. 保存された検索条件の横にあるチェックボックスをオンにして個別に選択するか、列上部にあるチェックボックスをオンにしてすべての検索を選択します。

7. [インポート] をクリックします。

   インポートした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. 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] の順に選択して、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] ドロップダウンメニューを開きます。

3. [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] 画面が表示されます。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。

4. 保存された検索条件の横にあるチェックボックスでエクスポート対象を個別に選択するか、列上部にあるチェックボックスですべての保存された検索条件を選択します。

> **注意**
> Deep Discovery Inspector では事前設定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。

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、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]、[最新のコールバック]、または [コールバック] によって並べ替えることができます。

図 4-6. C&C コールバックアドレス

C&C コールバックアドレスの表示

手順

1. [検出] > [C&C コールバックアドレス] の順に選択します。
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/ドメイン

- URL

3. (オプション) コールバックアドレスを拒否リストまたは許可リストにコピーします。
   a. コールバックアドレスの検出を選択します。
   b. [拒否リストにコピー] または [許可リストにコピー] をクリックします。

      拒否リストまたは許可リストにコピーする画面が表示されます。
   c. オプションを指定して [保存] をクリックします。

      リストをリロードするように求める通知が表示されます。
   d. [リロード] をクリックします。
4. (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 [すべての検出] 画面が表示されます。
5. (オプション) C&C コールバックアドレスのリストを並べ替えるには、列のタイトルをクリックします。

注意

一度に並べ替えることができる列は 1 つのみです。

- コールバックアドレス : 英数字の昇順/降順
- C&C リスクレベル : アルファベットの昇順/降順
- 種類 : アルファベットの昇順/降順
- 最新のコールバック : 最も古い/最新の日付
- コールバック : 数字の昇順/降順

仮想アナライザ不審オブジェクト

[仮想アナライザ不審オブジェクト] 画面 ([検出] > [仮想アナライザ不審オブジェクト]) には、仮想アナライザによって特定された、または外部ソースから同期された不審ファイル、IP アドレス、URL、およびドメインのリストが表示されます。

次の表は、[仮想アナライザ不審オブジェクト] 画面で実行可能な操作を示しています。

操作	説明
オブジェクトデータのフィルタ	検索フィールドまたはオブジェクトの種類のリストを使用してオブジェクトをフィルタします。 ヒント 検索フィールドでは大文字小文字は区別されず、部分一致が有効になります。
指定期間内の検出数の表示	期間を指定して、すべてのオブジェクトについて選択した期間内の検出数を表示します。 重要 • この表には、選択した期間に関係なくすべての仮想アナライザ不審オブジェクトが含まれます。 • 選択した期間に仮想アナライザ不審オブジェクトが検出されなかった場合、その総検出数は「0」と表示されます。
仮想アナライザ不審オブジェクトの管理	1 つまたは複数の仮想アナライザ不審オブジェクトを管理します。オプションには次のものがあります。 • オブジェクトを拒否リストに移動: 1 つ以上のオブジェクトを選択して [拒否リストに移動] をクリックし、選択したオブジェクトを拒否リストに移動します。 • オブジェクトを許可リストに移動: 1 つ以上のオブジェクトを選択して [許可リストに移動] をクリックし、選択したオブジェクトを許可リストに移動します。 • オブジェクトを削除: 1 つ以上のオブジェクトを選択して [削除] をクリックし、選択したオブジェクトを削除します。
検出の詳細の表示	[検出数] 列の数字をクリックすると、フィルタが適用された [すべての検出] 画面が表示されます。

操作	説明
リストの並べ替え	仮想アナライザ不審オブジェクトのリストを並べ替えるには、任意の列タイトルをクリックします。 注意 一度に並べ替えることができる列は 1 つのみです。

ユーザ指定の不審オブジェクト

異なるソースからの入力に基づいて不審オブジェクト情報を統合します。

[ユーザ指定の不審オブジェクト] 画面 ([検出] > [ユーザ指定の不審オブジェクト]) には、ユーザ指定の不審オブジェクトリストと除外リストがあります。

「不審オブジェクト」とは、不正であることがわかっているか、不正な可能性のあるドメイン、ファイルの SHA-1、ファイルの SHA-256、IP アドレス、または URL のことを指します。「除外」には、安全と見なされるオブジェクトが含まれます。

注意

Deep Discovery Inspector は、Trend Vision One、Deep Discovery Director、および Apex Central からユーザ指定の不審オブジェクトリストと除外リストを取得します。

次の表は、[ユーザ指定の不審オブジェクト] 画面で実行可能な操作を示しています。

操作	説明
ユーザ指定の不審オブジェクトリストの表示	[不審オブジェクト] タブをクリックして、ユーザ指定の不審オブジェクトリストを表示します。
除外リストの表示	[除外] タブをクリックして、除外リストを表示します。

操作	説明
オブジェクトデータのフィルタ	検索フィールドまたはオブジェクトの種類のリストを使用してオブジェクトをフィルタします。 ヒント 検索フィールドでは大文字小文字は区別されず、部分一致が有効になります。
リストの並べ替え	ユーザ指定の不審オブジェクトリストまたは除外リストを並べ替えるには、任意の列タイトルをクリックします。 注意 一度に並べ替えることができる列は 1 つのみです。
すべての同期されたデータのエクスポート	すべての同期された不審オブジェクトデータを CSV ファイルにエクスポートするには、[不審オブジェクト] タブで [すべてエクスポート] をクリックします。 すべての同期された除外データを CSV ファイルにエクスポートするには、[除外] タブで [すべてエクスポート] をクリックします。

Retro Scan

クラウドベースサービスの Retro Scan は、ネットワーク内の C&C サーバへのコールバック試行とその他の関連アクティビティについて Web アクセスの履歴ログを検索します。Web アクセスログには、ごく最近になって発見された、未検出および未ブロックの C&C サーバへの接続が含まれている場合があります。そのようなログを調査することは、攻撃によってネットワークが影響を受けているかどうかを判断するための、フォレンジック調査の重要な要素です。

Retro Scan は、Trend Micro Smart Protection Network に次のログ情報を保存します。

- Deep Discovery Inspector の監視対象エンドポイントの IP アドレス
- エンドポイントによってアクセスされた URL

- このサーバの GUID

その後、Retro Scan は保存されたログエントリを定期的に検索し、次のリストの C&C サーバへのコールバック回数を確認します。

- トレンドマイクロのグローバルインテリジェンスリスト: トレンドマイクロは、複数のソースからのリストをコンパイルして、各 C&C コールバックアドレスのリスクレベルを評価しています。C&C リストは、毎日アップデートされ、グローバルインテリジェンスを使用している製品に配信されます。
- ユーザ指定リスト: また、Retro Scan は、ユーザ専用の C&C サーバリストと照合してログを検索できます。アドレスは、テキストファイルで保存する必要があります。

重要

Deep Discovery Inspector の [Retro Scan] 画面には、トレンドマイクロのグローバルインテリジェンスリストを使用した検索に関する情報のみが表示されます。

Retro Scan と Trend Micro Smart Protection Network

C&C 通信は一般に大規模なボットネットに関連付けられますが、標的型攻撃の重要なコンポーネントでもあります。標的型攻撃は、通常、危険にさらされているホストと攻撃者の間の C&C 通信を介して、リモートで画策されます。不正プログラムは C&C サーバにコールバックしてダウンロードや命令を追加しますが、攻撃者は危険にさらされているホストにアクセスするために、このような不正プログラムを使用できます。

標的型攻撃の C&C 関連のトラフィックは、通常、特定するのは困難です。攻撃者は、アドレスを変更およびリダイレクトし、正規のサイトを使用して、企業のネットワーク内の C&C サーバの設定さえ行います。さらに、大半のセキュリティテクノロジは、その時点で不正であることが判明しているアドレスの検出とブロックにのみ重点を置いています。レピュテーションスコアは常に変化するため、このことが問題となります。現在、安全と見なされているアドレスが、1 時間後または翌日には不正となる場合も多々あります。

この問題に対処するため、Retro Scan は Trend Micro Smart Protection Network を統合して脅威を検出します。このクラウドベースの保護システム

は、高度な脅威調査とお客さまからのインテリジェンスを組み合わせ、より強力な保護を提供し、標的型攻撃の影響を最小限に抑えます。

Retro Scan は Web アクセスログの履歴を調べるため、アドレスがどの時点で不正として特定されたかに関係なく、不審接続を検出するために役立ちます。

Retro Scan の有効化

Retro Scan は、Deep Discovery Inspector とは独立して機能し、初期設定では無効になっています。

手順

1. [管理] > [監視/検索] > [Web レピュテーション] の順に選択します。
2. [Web レピュテーションを有効にする] をオンにします。
3. [Smart Protection の設定] で、[Trend Micro Smart Protection Network] を設定します。
4. [Retro Scan を有効にする] をオンにします。

   [サービスと使用条件] ウィンドウが表示されます。
5. 情報を読み、[同意する] をクリックします。
6. [保存] をクリックします。

Retro Scan が有効になった後、Deep Discovery Inspector は Retro Scan のスキャンレポートを定期的に確認します。スキャンレポートが使用可能な場合は、[Retro Scan] 画面に概要情報を表示します。

Retro Scan 画面

[Retro Scan] 画面には、次の情報が表示されます。

- 最新検索の日時
- Retro Scan レポートリポジトリへのリンク

注意

リンクをクリックすると、レポートリポジトリが新しいブラウザタブで開きます。

- すべての検索結果の概要

列	説明
生成されたレポート	スキャンレポートが完了した日時
感染ホスト	検索期間に C&C コールバックアドレスへの接続が試行されたホストの数
コールバック試行	スキャン期間にログ内で見つかった C&C コールバック試行の数

注意

数値をクリックすると特定のレポートの詳細が表示されます。詳細については、105 ページの「Retro Scan レポートの詳細画面」を参照してください。

また、[Retro Scan] 画面では、概要情報を.csv ファイルにエクスポートすることもできます。

Retro Scan レポートの詳細画面

[Retro Scan] 画面の [コールバック回数] 列で数値をクリックすると、新しい画面が開き次の情報が表示されます。

- コールバック回数
- Retro Scan レポートへのリンク

注意

リンクをクリックすると、オンラインバージョンのレポートが新しいブラウザタブで開きます。

- 標準スキャンレポートの概要

列	説明
試行されたコールバック	各 C&C コールバック試行の日時
監視対象ネットワークグループ	危険にさらされているホストが属する監視対象ネットワークグループ
感染ホスト	危険にさらされているホストの名前
IP アドレス	危険にさらされているホストの IP アドレス
コールバックアドレス	C&C サーバの URL または IP アドレス
関連する不正プログラムファミリ	C&C コールバックアドレスに関連付けられた不正プログラムファミリ
関連する攻撃者グループ	C&C コールバックアドレスに関連付けられた攻撃者グループ

Retro Scan の無効化

次のいずれかを実行すると、Retro Scan は自動的に無効になります。

- Web レピュテーションを無効にします

  URL をブロックするために他のセキュリティ製品を使用している場合、または Deep Discovery Inspector をサンドボックス分析専用として使用している場合のみ、オプションとして Web レピュテーションを無効にします。

- Smart Protection ソースをローカル Smart Protection Server に変更します

  Retro Scan は、Trend Micro Smart Protection Network の Web レピュテーションテクノロジへのクエリに基づいています。Retro Scan は、ローカル Smart Protection サーバにクエリするためにログを保存したりスキャンしたりできません。

Retro Scan の無効化

警告!

Retro Scan を無効にすると、Deep Discovery Inspector によって受信され表示されていたすべての Retro Scan 検出ログが削除されます。

手順

1. Retro Scan サービスを無効にするには、[管理] > [監視/検索] > [Web レピュテーション] の順に選択します。
2. [Smart Protection の設定] で、[Retro Scan を有効にする] をオフにします。
3. 確認メッセージ画面で、[OK] をクリックして Retro Scan を無効にし、すべての Retro Scan 検出ログを削除します。

すべての検出

[すべての検出] 画面には、ユーザ定義の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] 別に Deep Discovery Inspector によって [すべての検出] 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 4-11. 表示オプションと検索フィルタ:すべての検出

フィルタオプション	説明
重大度別のフィルタ	フィルタオプションには、次の重大度設定が含まれます。

フィルタオプション	説明	
	高のみ	重大度が高の検出のみを表示します。
		重大度が高および中の検出を表示します。
		重大度が高、中、および低の検出を表示します。
	すべて	情報を含むすべての検出を表示します。
期間	過去 1 時間 過去 24 時間 (初期設定) 過去 7 日間 過去 30 日間 カスタム範囲 現在の日付から過去 31 日間のカスタム範囲を指定します。	
列のカスタマイズ	オプションの列を表示します。	
基本検索	IP アドレスまたはホスト名を検索します。 ヒント 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。	

フィルタオプション	説明
事前設定された検索フィルタ	事前設定された検索条件で検索します。 [すべての検出] ビューには、次の事前設定された検索フィルタが含まれています。 • 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
詳細検索フィルタ	次を含む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、127 ページの「すべての検出の詳細検索フィルタ」を参照してください。

すべての検出の表示

手順

1. [検出] > [すべての検出] の順に選択します。
2. 検出の重大度を設定するには、[検出の重大度] スライダをドラッグします。
3. 期間を選択します。
4. 表示する列を選択するには、[列のカスタマイズ] をクリックします。列を 1 つ以上選択し [適用] をクリックして、変更された [すべての検出] 画面に戻ります。

表 4-12. [すべての検出] の列

列	事前選択済み
ステータス	X
タイムスタンプ	X
送信元ホスト	X
送信先ホスト	X
注目すべきホスト	X
ピアホスト	
送信者	
受信者	
メールの件名	
ユーザアカウント	
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)	
検出の重大度	X
攻撃段階	X
方向	
顕著なオブジェクト	X

注意

初期設定の [タイムスタンプ] 列と [脅威の詳細] 列は削除できません。

初期設定の [詳細] 列は削除できないため、[列のカスタマイズ] オプションには表示されません。

5. (オプション) [表示されている検出を解決済みに設定] をクリックすると、現在画面に表示されているすべての検出を解決済みに設定できます。

   [ステータス] 列で アイコンが に変更されます。

注意

表示されているすべての検出を解決済みに設定した後、検出を未解決に変更する場合は個別に変更します。

6. 基本検索を実行するには、次のいずれかを実行します。

   - 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、<Enter> キーを押します。
   - 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] 別に [すべての検出] が検索されます。

図 4-7. すべての検出の基本検索

7. 保存された検索条件を実行するには、[検出][すべての検出] の順に選択して、検索ボックスのドロップダウンメニューを開き、保存された検索条件をクリックします。

   次の事前設定された検索条件が用意されています。

   表 4-13. 事前設定された検索条件

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

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、127 ページの「すべての検出の詳細検索フィルタ」を参照してください。

9. [エクスポート] をクリックします。

   次のファイルを含む zip フォルダがダウンロードされます。

   - threats.csv
   - malicious_urls.csv
   - application_filters.csv
   - correlated_incidents.csv

[すべての検出] - [検出の詳細] の表示

手順

1. 任意のイベントの [すべての検出] の詳細を表示するには、[すべての検出] 画面の [詳細] 列の下で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。

   図 4-8. [すべての検出] - [検出の詳細]

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。
   - [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。
   - 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。

パケットキャプチャの詳細については、213 ページの「パケットキャプチャ」を参照してください。

- [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。
5. [軽減策の提案] には、脅威の説明、ホストに対する影響、およびその脅威から保護するための推奨処理が表示されます。

[すべての検出] - [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。

- 115 ページの「[すべての検出] - [検出の詳細] - [接続の詳細]」
- 122 ページの「[すべての検出] - [検出の詳細] - [ファイル分析結果]」
- 124 ページの「[すべての検出] - [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]」
- 126 ページの「[すべての検出] - [検出の詳細] - [軽減策の提案]」

[すべての検出] - [検出の詳細] - [接続の詳細]

[すべての検出] - [検出の詳細] 画面の [接続の詳細] セクションには、次の情報が含まれます。

- 117 ページの「[すべての検出] - [検出の詳細] - [検出情報]」
- 119 ページの「[すべての検出] - [検出の詳細] - [接続の概要]」
- 120 ページの「[すべての検出] - [検出の詳細] - [プロトコル情報]」
- 121 ページの「[すべての検出] - [検出の詳細] - [ファイル情報]」
- 121 ページの「[すべての検出] - [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 [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。

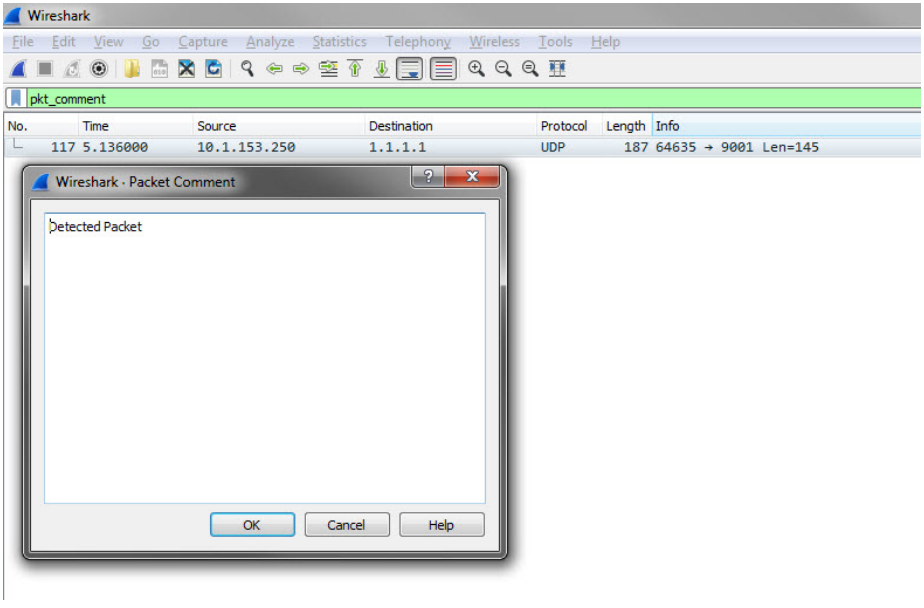


図 4-9. 検出されるパケット例

パケットキャプチャの詳細については、213 ページの「パケットキャプチャ」を参照してください。

[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。

[すべての検出] - [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

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。

© 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 4-14. 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

[すべての検出] - [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

[すべての検出] - [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
- その他

[すべての検出] - [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

[すべての検出] - [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

[すべての検出] - [検出の詳細] - [ファイル分析結果]

[すべての検出] - [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。

- 123 ページの「[すべての検出] - [検出の詳細] - [ファイル分析結果] - [ファイル情報]」
- 124 ページの「[すべての検出] - [検出の詳細] - [ファイル分析結果] - [YARA 検出]」
- 124 ページの「[すべての検出] - [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。

[すべての検出] - [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。

© 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

[すべての検出] - [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

[すべての検出] - [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] 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

[すべての検出] - [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]

[すべての検出] - [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] セクションには、次の情報が含まれます。

- 125 ページの「[すべての検出] - [検出の詳細] - [不審オブジェクト情報]」

- 125 ページの「[すべての検出] - [検出の詳細] - [分析された関連ファイル情報]」

[すべての検出] - [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。

- 有効期限
- 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

[すべての検出] - [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。

© 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

[すべての検出] - [検出の詳細] - [軽減策の提案]

[軽減策の提案] セクションには、次の情報が表示されます。

- 詳細情報
- 詳細な説明
- 影響
- 一次処理

すべての検出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。

注意

各詳細検索フィルタには次を含めます。

- 最大 20 件の条件セット
- 各テキストベースの値フィールドに最大 1024 文字

最大 50 件の詳細検索フィルタを保存できます。

詳細については、次を参照してください。

- 133 ページの「すべての検出の詳細検索フィルタの追加」
- 135 ページの「[すべての検出] の保存された検索条件の編集」
- 137 ページの「すべての検出の保存された検索条件のインポート」

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 4-15. 検索フィルタの条件: すべての検出

属性	演算子	処理	例
ホスト名	次の値を含む/次の値を含まない	値を入力	computer.example.com

属性	演算子	処理	例
IP アドレス	次の値を含む/次の値を含まない 範囲内/範囲外	値を入力 範囲を入力	10.1.1.2
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	AA:AA:AA:AA:AA:AA
ネットワークグループ	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。 • すべてのグループ • 初期設定	
登録済みサービス	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。 • Active Directory • 認証サーバ - Kerberos • コンテンツ管理サーバ • データベースサーバ • DNS • ドメインコントローラ • ファイルサーバ • FTP • HTTP プロキシ • Radius サーバ • セキュリティ監査サーバ • SMTP • SMTP オープンリレー • ソフトウェアアップデートサーバ • Web サーバ	

属性	演算子	処理	例
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	次を 1 つ以上選択します。 • すべてのプロトコル • 検索したいプロトコル • その他	
Transport Layer Security (TLS)	Over SSL/TLS Over SSL/TLS を使用しない		
方向	等しい	次のいずれかを選択します。 • 内部 • 外部	
ステータス	等しい	次のいずれかを選択します。 • 解決済み • 未解決	
脅威/検出/参照	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	VAN_RANSOMWARE.UMXX
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	707-710、721-727
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	707-710、721-727

属性	演算子	処理	例
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	
YARA ルールファイル/YARA ルール	次の値を含む/次の値と等しい	値を入力	myYARAFile
	YARA 検出あり		
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	

属性	演算子	処理	例
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	computer.example.com
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。 • 高 • 中 • 低	
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		
標的型攻撃に関連している	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 • 既知の不正プログラム	
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	値を入力	myFile
SHA-1	ファイルの SHA-1 あり/ファイルの SHA-1 なし		

属性	演算子	処理	例
	次の値を含む/次の値を含まない	値を入力	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145
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	8b7df143d91c716ecfa5fc1730022f6b421b05ceedee8fd52b1fc65a96030ad52
IP アドレス/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	10.1.1.2
不審オブジェクト/拒否リストのエンティティ	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	5bf1fd927dfb8679496a2e6cf00cbe50c1c87145

属性	演算子	処理	例
メールアドレス	メールアドレスあり/メールアドレスなし		example@example.com
	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	950124.162336@example.com
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	mySubject

すべての検出の詳細検索フィルタの追加

手順

1. 詳細検索フィルタを作成するには、[検出] > [すべての検出] の順に選択し、[詳細] をクリックします。
2. [フィルタ] ドロップダウンメニューを開き、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。
   - ドロップダウンメニューから処理を選択します。

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、127 ページの「すべての検出の詳細検索フィルタ」を参照してください。

注意

複数の条件エントリを追加するにはカンマで区切ります。

4. (オプション) 検索フィルタに他の条件セットを含めるには、[新規追加] をクリックします。

   各詳細検索フィルタには次を含めます。

   - 最大 20 件の条件セット
   - 各テキストベースの値フィールドに最大 1024 文字

   最大 50 件の詳細検索フィルタを保存できます。

5. [検索] をクリックします。

   [すべての検出] 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. (オプション) 検索を保存するには、次を実行します。

   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。

      [保存された検索条件] 画面が開きます。

   b. 名前を入力して、[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ともに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) 詳細検索機能を終了するには、[キャンセル] をクリックします。

[すべての検出] の保存された検索条件の編集

手順

1. [すべての検出] で保存された検索条件を編集するには、[検出] > [すべての検出] の順に選択し、[保存された検索条件] ドロップダウンメニューを開きます。
2. 編集する保存された検索条件を選択し、 アイコンをクリックします。
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。
   - ドロップダウンメニューから処理を選択します。

   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、127 ページの「すべての検出の詳細検索フィルタ」で「検索フィルタの条件: すべての検出」の表を参照してください。

   注意

   複数の条件エントリを追加するにはカンマで区切ります。
5. (オプション) 検索フィルタに他の条件セットを含めるには、[新規追加] をクリックします。

注意

各詳細検索フィルタには次を含めます。

- 最大 20 件の条件セット
- 各テキストベースの値フィールドに最大 1024 文字

最大 50 件の詳細検索フィルタを保存できます。

6. [検索] をクリックします。

   [すべての検出] 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。

7. (オプション) 編集した検索を保存するには、[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。

   - 編集した検索を同じ名前で保存するには、[保存] をクリックします。

     編集した検索が元の名前で保存されます。

   - 編集した検索を新しい名前で保存するには、次を実行します。

   a. [名前を付けて保存...] をクリックします。

      [保存された検索条件] 画面が開きます。

   b. 名前を入力して、[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。

8. (オプション) 詳細検索機能を終了するには、次のいずれかを実行します。

   - 元の画面に戻るには、[キャンセル] をクリックします。
   - 基本検索を実行するには、保存された検索条件をクリックします。

すべての検出の保存された検索条件の削除

手順

1. 保存された検索条件を削除するには、[検出] > [すべての検出] の順に選択し、[保存された検索条件] ドロップダウンメニューを開きます。

2. 削除する検索の横にある [フィルタの削除] アイコンをクリックします。

注意

事前設定フィルタは削除できません。

すべての検出の保存された検索条件のインポート

手順

1. 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] > [すべての検出] の順に選択して、[保存された検索条件] ドロップダウンメニューを開きます。

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をインポート] 画面が表示されます。

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

   ファイルがアップロードされ、検証されます。初期設定では、すべての有効な保存された検索条件が選択され、インポートされます。

   Deep Discovery Inspector では、現在の製品バージョンと互換性のない保存された検索条件は無効になります。

4. (オプション) 保存された検索条件の名前をインポート前に変更するには、保存された検索条件の名前にマウスを重ねて編集アイコンをクリックします。

注意

保存された検索条件の名前が重複している場合は、インポート前に名前を変更する必要があります。名前が重複している保存された検索条件は赤いボックスで強調表示されます。

5. 保存された検索条件の横にあるチェックボックスでインポート対象を個別に選択するか、列上部にあるチェックボックスですべての保存された検索条件を選択します。
6. [インポート] をクリックします。

   インポートした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。

すべての検出の保存された検索条件のエクスポート

手順

1. 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] > [すべての検出] の順に選択して、[保存された検索条件] ドロップダウンメニューを開きます。
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] 画面が表示されます。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。
3. 保存された検索条件の横にあるチェックボックスをオンにして個別に選択するか、列上部にあるチェックボックスをオンにしてすべての検索を選択します。

   注意

   Deep Discovery Inspector では初期設定されている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。

第 5 章

レポート

Deep Discovery Inspector 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。

- 142 ページの「レポートについて」
- 144 ページの「予約レポート」
- 145 ページの「スケジュール」
- 146 ページの「レポートのスケジュールの設定」
- 147 ページの「レポートのスケジュールの削除」
- 148 ページの「手動レポート」
- 149 ページの「手動レポートの生成」
- 150 ページの「手動レポートの削除」
- 151 ページの「カスタマイズ」
- 151 ページの「レポートのカスタマイズ」

レポートについて

Deep Discovery Inspector には、脅威データベースに簡単にアクセスするためのレポートテンプレートが用意されています。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。

表 5-1. Deep Discovery Inspector のレポート

レポートの種類と形式	目次

詳細レポート
次の形式のファイルを含む圧縮アーカイブ:
1. PDF ファイル
2. CSV ファイル
	• 検出の概要
	  • 仮想アナライザの概要
	  • カスタム拒否リストのイベントの概要
	• 重大度の高いホスト
	• 重大度の高いホストの詳細
	• 仮想アナライザの結果の詳細
	• 拒否リストの検出結果
	• 不正プログラムの脅威タイプ別統計
	  • 不正なサイトにアクセスしたホストのトップ 20
	  • 不正なコンテンツの統計
	• 情報検出
	• 要注意アプリケーションの使用
	• 推奨事項
	• 用語集
	• 付録 A: レポート範囲

レポートの種類と形式	目次

管理レポート
PDF
	• 概要
	• ビジネスリスク
	• 影響を受けたエンドポイント
	• 感染原因
	• 使用された検出テクノロジ
	• 不正プログラムの脅威タイプ別統計
	• 仮想アナライザの統計
	• 要注意アプリケーション
	• 拒否リストのエンティティ
	• 潜在的な影響
	• 推奨事項
	• 付録
	  • 付録 A: レポート範囲
	  • 付録 B: 最も影響を受けるホストのサマリー

ホストの重大度レポート
PDF
	• 概要
	• 影響を受けたホスト
	• C&C 通信
	• 潜在的な脅威
	• 既知の脅威
	• 内部活動
	• 付録
	  • 付録 A: レポート範囲
	  • 付録 B: 影響を受けたホストの重大度

概要レポート PDF	• 概要 • 検出状況 • 推奨事項 • 付録 A: レポート範囲

レポートの種類と形式	目次

脅威の検出レポート
PDF
	• 概要
	  • 仮想アナライザのみで検出された脅威のトップ 10
	  • 仮想アナライザによって検出された脅威のトップ 10
	  • 検出された既知の不正プログラムの種類
	  • 感染経路
	  • グループごとの攻撃元トップ 10
	  • 複数グループ攻撃トップ 10
	  • 攻撃元のトップ 10
	  • 脅威の種類のトップ 10
	  • 脅威の動向
	  • 仮想アナライザの統計
	• 付録
	  • 付録 A: レポート範囲
	  • 付録 B: 推奨事項

予約レポート

[予約レポート] 画面では、ユーザが予約した日次、週次、および月次レポートがカレンダに表示されます。

表 5-2. カレンダのアイコン

アイコン	実行間隔	ユーザ	目的
D	日次	管理者	脅威ステータスの追跡
W	週次	企業幹部	組織のセキュリティ状況の概要の把握
M	月次	企業幹部	組織のセキュリティ状況の概要の把握

カレンダの選択した日付ごとの予約レポートのリストから、以前のレポートにアクセスできます。レポートをクリックして開くか、または保存します。

スケジュール

[スケジュール] 画面を使用すると、次の操作を実行できます。

- 予約レポートの属性の確認
- レポートのスケジュールの追加、変更、および削除

表 5-3. 列の名前: [スケジュール] タブ

列	説明
実行間隔	次を含む一般的なレポートの期間: • 日次 • 週次 • 月次
名前	カスタマイズされた、または初期設定のレポート名
種類	次を含むレポートの種類: • 詳細 • 企業幹部 • ホストの重大度 • 概要 • 脅威の検出
範囲	含まれるホスト: • すべての監視対象ホスト • フィルタされたホスト
通知	通知オプションのステータス • オン: 有効 • オフ: 無効
期間	レポートの対象となる期間
作成者	レポートを予約したユーザアカウント名

レポートのスケジュールの設定

日次、週次、および月次のレポートの作成スケジュールを設定できます。

手順

1. [レポート] > [スケジュール] タブで [追加] をクリックします。[スケジュールの追加] 画面が開きます。

2. (オプション) レポート名を入力します。

3. [スケジュール] で、レポートの実行間隔を選択します。

   表 5-4. レポートの実行間隔

実行間隔	オプション	説明
日次		00:00〜23:59
週次	開始する曜日:	初期設定: 日曜日 設定可能: 日曜日〜土曜日
月次	開始する日:	初期設定: 1 日 設定可能: 1〜31

   [次のレポート期間] には、レポートの期間が表示されます。

4. レポートの種類を選択します。

   利用可能なレポートの詳細については、142 ページの「レポートについて」を参照してください。

   選択したレポートの [目次] が表示されます。

5. レポート範囲を選択するには、次のいずれかをクリックします。

   - すべての監視対象ホスト
   - フィルタされたホスト

注意

選択可能な保存されたフィルタには、事前設定された [影響を受けたホスト] の保存された検索条件と、カスタムの保存された検索条件があります。

6. (オプション) [生成されたレポートをメール受信者に送信する] を選択します。

   メール受信者のリストを編集するには、[管理] > [通知] > [配信オプション] > [メールの設定] の順に選択します。

7. [保存] をクリックします。

8. レポートのスケジュールを変更するには、レポート名をクリックして、手順 2〜7 を実行します。

注意

レポートのスケジュールは、そのスケジュールを作成したユーザアカウントのみが編集できます。ただし、誰でも任意のレポートスケジュールを削除することができます。

レポートのスケジュールの削除

手順

1. [レポート] > [スケジュール] タブで、削除するレポートのスケジュールを選択します。
2. [削除] をクリックします。

注意

これによりレポートのスケジュールが削除されます。レポートは削除されません。

重要

アカウントが削除されると、そのアカウントで作成されたレポートのスケジュールも削除されます。ただし、生成されたレポートは削除されません。

検索が削除されると、その検索に関連付けられたレポートのスケジュールも削除されます。ただし、生成されたレポートは削除されません。

以前生成された予約レポートを削除する方法については、360 ページの「ストレージ管理」を参照してください。

手動レポート

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] 画面で次の操作を実行できます。

- 生成された手動レポートの属性の確認
- 手動レポートの追加、ダウンロード、および削除

表 5-5. 列の名前: [手動レポート] タブ

列	説明
生成	レポートの生成日時
名前	カスタマイズされた、または初期設定のレポート名
種類	次を含むレポートの種類: • 詳細 • 企業幹部 • ホストの重大度 • 概要 • 脅威の検出レポート
範囲	含まれるホスト: • すべての監視対象ホスト • フィルタされたホスト

列	説明
期間	レポートの対象となる期間
作成者	レポートを生成したユーザアカウント名
ダウンロード	生成されたレポートを保存するか開きます。

注意

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。手動レポートではメール通知は送信されません。

手動レポートの生成

手順

1. [レポート] > [手動レポート] の順に選択します。
2. [追加] をクリックします。

   [手動レポートの追加] 画面が開きます。
3. レポートの期間を選択します。オプションは次のとおりです。
   - 次の事前設定された期間をクリックします。
     - 過去 7 日間
     - 過去 2 週間
     - 過去 4 週間
   - カレンダをクリックして日付範囲を選択します。

   注意

   事前設定された期間をクリックすると、正確な日付が [開始]/[終了] に自動的に追加されます。
4. レポートの種類を選択します。

利用可能なレポートの詳細については、142 ページの「レポートについて」を参照してください。

選択したレポートの [目次] が表示されます。

5. レポート範囲を選択するには、次のいずれかをクリックします。
   - すべての監視対象ホスト
   - フィルタされたホスト

   [影響を受けたホスト] で保存された検索条件を選択します。

   注意

   選択可能な保存された検索条件には、事前設定された [影響を受けたホスト] の保存された検索条件と、カスタムの保存された検索条件があります。アプリケーションの保存された検索条件をレポートに設定するには、[検出] > [影響を受けたホスト] > [詳細] の順に選択し、ホストの属性および関連付けられた条件を選択します。

6. [生成] をクリックしてレポートを作成します。

   新しい手動レポートがリストに表示されます。

手動レポートの削除

重要

この手順では、Deep Discovery Inspector からレポートを削除します。一度削除されたレポートは復元できません。

任意のユーザが任意のレポートを削除できます。

手順

1. [レポート] > [手動レポート] タブで、削除するレポートを選択します。
2. [削除] をクリックします。

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。詳細については、151 ページの「レポートのカスタマイズ」を参照してください。

レポートのカスタマイズ

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、[表示する] をクリックし、画像を参照して選択します。

   重要

   画像ファイルは、JPG または PNG 形式である必要があります。最大ファイルサイズは 200KB です。

4. (オプション) [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。

   注意

   [トレンドマイクロのロゴを表示する] は初期設定ではオンになっています。

5. [保存] をクリックします。

第 6 章

管理

Deep Discovery Inspector の管理方法については、次の項目を参照してください。

- 154 ページの「アップデート」
- 168 ページの「通知」
- 188 ページの「監視/検索」
- 228 ページの「仮想アナライザ」
- 256 ページの「ネットワークグループとエンドポイント」
- 266 ページの「統合製品/サービス」
- 346 ページの「アカウントについて」
- 333 ページの「システム設定」
- 358 ページの「システムログ」
- 360 ページの「システムのメンテナンス」
- 368 ページの「ライセンス」

アップデート

[アップデート] 画面を使用して、コンポーネントと製品のアップデート設定を行います。

コンポーネントのアップデート

ネットワークの脅威を検索および検出するために使用する、製品コンポーネントをダウンロードして配信します。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。

アップデートするコンポーネント

ネットワークの保護を支援するために、Deep Discovery Inspector では次の表に示すコンポーネントを使用します。

表 6-1. Deep Discovery Inspector のコンポーネント

コンポーネント	説明
APT (標的型サイバー攻撃) 情報パターンファイル	APT (標的型サイバー攻撃) 情報パターンファイルには、APT に関する詳細情報が記載されています。
高度な脅威相関パターンファイル	高度な脅威相関パターンファイルには、既知の脅威には関係のないファイル機能のリストが含まれます。
高度な脅威検索エンジン (Deep Discovery、Linux、64 ビット)	高度な脅威検索エンジンは、ウイルス、不正プログラム、および Java や Flash などのソフトウェアの脆弱性悪用からシステムを保護します。トレンドマイクロのウイルス検索エンジンと統合されており、シグネチャベースの検出、動作ベースの検出、および積極的なヒューリスティック検出を行います。
C&C 識別パターンファイル	C&C 識別パターンファイルには、既知の C&C サーバおよびコールバックアドレスのリストが含まれています。
一般的な脅威ファミリ情報パターンファイル	一般的な脅威ファミリ情報パターンファイルには、検出に使用するための共通の脅威ファミリ名が記載されています。
一般的な脆弱性および漏えいの情報パターンファイル	一般的な脆弱性および漏えいの情報パターンファイルには、検出に使用するための共通の脆弱性/感染に関する参照情報が記載されています。

コンポーネント	説明
CI クエリハンドラ	CI クエリハンドラは、CI エンジンにより特定された動作を処理して機械学習型検索エンジンにレポートを送信します。
不正プログラムパターンファイル (Deep Discovery)	トレンドマイクロのウイルス検索エンジンは、ヒューリスティック検出、シグネチャベースの検出、および動作ベースの検出によってウイルスや不正プログラムからシステムを保護します。トレンドマイクロは、新しい脅威の検出ルーチンが使用可能になるとウイルスパターンファイルをただちにアップデートします。
IntelliTrap 除外パターンファイル	IntelliTrap 除外パターンファイルには、IntelliTrap 機能による検索実行時の誤検出を減らすため、自動実行型の安全な圧縮ファイルの検出ルーチンが含まれます。
IntelliTrap パターンファイル	IntelliTrap パターンファイルには、一般に難読化された不正プログラムやその他の潜在的な脅威として知られる自動実行型圧縮ファイルタイプの検出ルーチンが含まれます。
ネットワークコンテンツ相関パターンファイル	ネットワークコンテンツ相関パターンファイルは、トレンドマイクロによって定義された検出ルールを実装します。
ネットワークコンテンツ検査エンジン (5.14、カーネルモード、64 ビット、Conf: 6500)	ネットワークコンテンツ検査エンジンは、ネットワーク検索を実行するために使用されます。
ネットワークコンテンツ検査エンジン (Linux、ユーザモード、64 ビット)	ネットワークコンテンツ検査エンジンは、ネットワーク検索を実行するために使用されます。
ネットワークコンテンツ検査パターンファイル	ネットワークコンテンツ検査パターンファイルは、ネットワーク検索を実行するためにネットワークコンテンツ検査エンジンによって使用されます。
スクリプトアナライザ共通パターンファイル	スクリプトアナライザパターンファイル (Deep Discovery) は、不正コードを識別するために Web ページスクリプトの解析時に使用されます。

コンポーネント	説明
スパイウェア/グレーウェアパターンファイル	スパイウェア/グレーウェアパターンファイルは、アドウェアやスパイウェアまたはグレーウェアなど、特定タイプの潜在的に望ましくないファイルおよびプログラムの存在を示すビットとバイトの一意のパターンを特定します。
脅威相関分析パターンファイル	脅威相関分析パターンファイルは、脅威の相関分析の実行時に Deep Discovery Inspector によって使用されます。
脅威ナレッジベース (JP)	脅威ナレッジベースは、脅威の相関分析に関する情報を提供します。
トレンドマイクロ インテリジェンスエージェント v.2 (Deep Discovery Inspector、Linux、64 ビット)	トレンドマイクロ インテリジェンスエージェント v.2 は、検出の追加情報を取得します。
信頼済み証明書情報パターンファイル	信頼済み証明書情報パターンファイルには、PE シグネチャを検証するための信頼済み証明書情報が記載されています。
仮想アナライザ設定パターンファイル	仮想アナライザ設定パターンファイルには、サポートされる脅威の種類やファイルタイプなど、仮想アナライザの設定情報が含まれます。
仮想アナライザセンサ	仮想アナライザセンサは、不正プログラムの実行と検出、および仮想アナライザでの動作の記録に使用されるユーティリティ群です。

コンポーネントのアップデート方法

次のいずれかの方法を使用してコンポーネントをアップデートします。

表 6-2. アップデート方法

方法	説明
手動アップデート	新しいコンポーネントが利用可能かどうかを確認するには、管理コンソールで [管理] > [アップデート] > [コンポーネントのアップデート] の順に選択します。詳細については、158 ページの「手動アップデート」を参照してください。 注意 Deep Discovery Inspector のすべてのコンポーネントがアップデートされます。コンポーネントを個別にアップデートすることはできません。 Deep Discovery Inspector コンポーネントをアップデートするには、[管理] > [アップデート] > [コンポーネントのアップデート] > [アップデート元] の順に選択します。詳細については、159 ページの「アップデート元」を参照してください。
予約アップデート	予約アップデートを設定するには、[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] の順に選択します。Deep Discovery Inspector が指定した頻度で自動的にアップデート元を確認します。詳細については、159 ページの「予約アップデートの設定」を参照してください。

コンポーネントのアップデートタスク

すべてのコンポーネントをアップデートするには、次の手順を確認してください。

- 336 ページの「プロキシ」
- 158 ページの「手動アップデート」
- 159 ページの「予約アップデートの設定」
- 159 ページの「アップデート元」
- 165 ページの「Service Pack/バージョンアップグレード」

手動アップデート

Deep Discovery Inspector では、手動でコンポーネントをアップデートできます。この機能は、大規模感染の際、またはスケジュールの固定によってアップデートが届かない場合に使用します。

[手動] 画面には、次の詳細が表示されます。

表 6-3. [手動アップデート] 画面の詳細

詳細	説明
コンポーネント	コンポーネント名
現在のバージョン	製品で現在使用されている各コンポーネントのバージョン番号
最新バージョン	サーバで利用可能な最新バージョン
前回の更新	前回の更新日時

手動アップデートの実行

手順

1. [管理] > [アップデート] > [コンポーネントのアップデート] > [手動] の順に選択します。
2. Deep Discovery Inspector では、アップデートの必要なコンポーネントが自動的に確認されます。

   アップデートの必要なコンポーネントは赤色で表示されます。
3. [アップデート] ボタンをクリックします。

   Deep Discovery Inspector のコンポーネントがアップデートされます。アップデートが完了したら、次のメッセージが表示されます。

   すべてのコンポーネントは最新です。

予約アップデートの設定

予約アップデートを設定して、Deep Discovery Inspector のコンポーネントを最新の状態に保ちます。

手順

1. [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] の順に選択します。
2. [予約アップデートを有効にする] を選択します。
3. アップデートスケジュールを [時]、[日]、または [週] で選択し、日付または時刻を指定します。

   ヒント

   アップデートスケジュールは 2 時間間隔で設定することをお勧めします。
4. [保存] をクリックします。

アップデート元

Deep Discovery Inspector は、初期設定のアップデート元であるトレンドマイクロのアップデートサーバからコンポーネントをダウンロードします。組織内の別のアップデート元からコンポーネントをダウンロードするように Deep Discovery Inspector を設定できます。

トレンドマイクロのアップデートサーバまたは Trend Micro Apex Central をアップデート元として使用する場合、Deep Discovery Inspector は常に TLS 1.2 を使用して接続し、パッケージの整合性を確認します。

トレンドマイクロのアップデートサーバをアップデート元として使用する場合、Deep Discovery Inspector は HTTPS サーバ認証のチェックを行います。

[その他のアップデートサーバ] をアップデート元として使用する場合は、[管理] > [システム設定] > [ネットワーク] で [常に TLS 1.2 以上を使用する] を有効にして、TLS 接続を使用する必要があります。

注意

Deep Discovery Inspector は、Trend Micro Apex Central から直接コンポーネントをダウンロードするように設定できます。Apex Central サーバをアップデート元として指定する方法の詳細については、「Trend Micro Apex Central 管理者ガイド」を参照してください。

アップデート元の設定

手順

1. [管理] > [アップデート] > [コンポーネントのアップデート] > [アップデート元] の順に選択します。
2. [アップデートのダウンロード元] で、次のいずれかのアップデート元を選択します。
   - 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: その他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。アップデート元は「http://」または「https://」で始まる必要があります。

     例:

     - `http://activeupdate.example.com`
     - `https://activeupdate.example.com`

   注意

   アップデート元を UNC パス形式で指定することはできません。
3. (オプション) [失敗したアップデートを再試行] を有効にして、[再試行回数] と [再試行間隔] を指定します。

製品のアップデート

製品のアップデートには、次のものが含まれます。

- HotFix/Patch
- Service Pack/バージョンアップグレード

Deep Discovery Inspector をアップグレードするには、次のいずれかを実行します。

- 管理コンソールからファームウェアをアップグレードするか、Deep Discovery Director を設定してアップグレードを管理します。

  ファームウェアをアップグレードすると、既存のアプリケーションファイルが更新され、機能が向上します。

  詳細については、165 ページの「Service Pack/バージョンアップグレード」および 281 ページの「Deep Discovery Director」を参照してください。

- アプライアンス設定をバックアップ/復元します。

  アプライアンス設定をバックアップまたは復元すると、必要に応じて以前の設定の一部を維持できます。

  ただし、データおよびログはバックアップ/復元できません。新しい機能もインストールされません。既存の設定は暗号化ファイルにエクスポートすることでバックアップし、この暗号化ファイルをインポートすることで復元できます。Deep Discovery Inspector は、製品出荷時の初期設定を復元することでもリセットできます。

  詳細については、362 ページの「バックアップ/復元」を参照してください。

HotFix/Patch

トレンドマイクロからの製品リリース後、各種問題への対応や製品パフォーマンスの向上のために、HotFix や Patch が配布されることがあります。

表 6-4. HotFix/Patch

システムアップデート	説明
Hotfix	HotFix は、お客さまから報告された問題に対する回避策や解決方法です。固有の問題に対応するものであるため、すべてのお客さまに配布されるものではありません。Windows 版以外の HotFix の場合、HotFix の適用では、一般的にプログラムデーモンを停止し、HotFix ファイルをコピーしてインストール内の対象ファイルを上書きし、デーモンを再起動する必要があります。
Critical Patch	至急対策の必要がある問題のみを修正する目的で一般公開されるプログラムです。特定の問題を修正するプログラムであるため、基本的に、他の修正は含まれませんが、同時期に発見された問題に対する複数の修正が含まれる場合があります。一般公開時期に応じて、後述の Patch に統合されます。問題発生条件に合致するすべてのお客さまに適用を推奨いたします。Windows 以外の Patch には、通常、セットアップスクリプトが含まれています。
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。Windows 以外の Patch には、通常、セットアップスクリプトが含まれています。

これらを利用できるようになると、ベンダやサポートプロバイダから連絡がある場合があります。新しい Critical Patch、Patch、および Service Pack のリリースについては、次のトレンドマイクロの Web サイトで確認してください。

https://www.trendmicro.com/ja_jp/business/products/downloads.html?clk=left_nav&clkval=all_download&regs=jp

HotFix または Patch の適用

次の手順は手動アップグレードの場合にのみ適用されます。Deep Discovery Director を使用したアップグレードの詳細については、Deep Discovery Director の製品ドキュメントを参照してください。

手順

1. HotFix/Patch ファイルをコンピュータの任意のフォルダに保存します。

警告!

HotFix/Patch ファイルの適用時の問題を回避するため、HotFix/Patch ファイルは元の名前を使用して保存してください。

2. ファイルを保存したコンピュータで管理コンソールにアクセスし、ログオンします。
3. [管理] > [アップデート] > [製品のアップデート] > [HotFix/Patch] の順に選択します。
4. HotFix/Patch ファイルを参照して見つけます。
5. [アップロード] をクリックします。

警告!

ファイルのアップロードで問題が発生しないよう、ブラウザを閉じたり他の画面に移動したりしないでください。

6. アップロードが正常に完了したら、[アップロードしたシステムアップデートの詳細] を確認します。

   ここには、アップロードした HotFix/Patch のビルド番号と、再起動が必要かどうかが示されます。

注意

アップデートの適用後は、管理コンソールのログオン画面が表示されます。

7. 再起動が必要な場合、管理コンソールでのすべてのタスクを終了してから先に進んでください。
8. [続行] をクリックして、HotFix/Patch を適用します。

警告!

HotFix/Patch の適用で問題が発生しないよう、ブラウザを閉じたり他の画面に移動したりしないでください。

注意

システムアップデートの適用で問題が発生した場合は、再起動が必要かどうかを [HotFix/Patch] 画面またはシステムログの詳細情報で確認します。

9. 再起動が必要な場合:
   a. 管理コンソールにログオンします。
   b. [管理] > [システムログ] の順に選択して、HotFix/Patch の適用中に発生した問題について確認します。
   c. [HotFix/Patch] 画面に戻ります。
10. ブラウザのキャッシュをクリアします。詳細については、167 ページの「ブラウザのキャッシュのクリア」を参照してください。
11. 適用した HotFix/Patch が最新のアップデートとして表示されることを [履歴] で確認します。

    適用したシステムアップデートは、[HotFix/Patch] 画面に表示されます。この画面には、これまで適用またはロールバックしたすべての HotFix/Patch が一覧表示されます。

HotFix または Patch のロールバック

Deep Discovery Inspector 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。

ロールバックできるのは最新の HotFix/Patch のみです。ロールバック後、他の既存の HotFix/Patch をロールバックすることはできません。ロールバック機能は、新しい HotFix/Patch が適用された場合にのみ再度利用できるようになります。

注意

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

手順

1. [管理] > [アップデート] > [製品のアップデート] > [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。
3. ロールバック結果を、[HotFix/Patch] 画面の最初の行で確認します。

Service Pack/バージョンアップグレード

トレンドマイクロでは、パフォーマンスの強化を図ったり新しいバージョンにアップグレードしたりするために、Deep Discovery Inspector の新しいファームウェアをリリースすることがあります。

Deep Discovery Inspector6.6、6.7、および 6.7 Service Pack1 をバージョン 6.8 にアップグレードできます。

アップグレード後は、Deep Discovery Inspector で既存のデータ、ログ、および設定が維持されます。

次の表は、Deep Discovery Inspector で使用可能なシステムアップグレードの種類を示しています。

システムアップグレード	説明
Service Pack	Service Pack は、HotFix、Patch、および機能拡張を組み合わせたもので、製品のアップグレードに相当します。Windows 以外の Service Pack には、セットアッププログラムおよびセットアップスクリプトが含まれています。
バージョンアップグレード	ファームウェアをアップグレードすると、既存のアプリケーションファイルが更新され、機能が向上します。

Service Pack またはバージョンアップグレードの適用

次の手順は手動アップグレードの場合にのみ適用されます。Deep Discovery Director を使用したアップグレードの詳細については、Deep Discovery Director の製品ドキュメントを参照してください。

手順

1. アプライアンスの設定をバックアップします。詳細については、362 ページの「バックアップ/復元」を参照してください。
2. Deep Discovery Inspector を Apex Central に登録している場合は、Apex Central の登録の詳細情報を記録してください。

   注意

   Service Pack/バージョンアップグレードの適用後、Deep Discovery Inspector によって製品の現在の設定が移行されるため、設定を再度指定する必要はありません。ファームウェアのアップデートが完了すると、Deep Discovery Inspector は自動的に Apex Central に再登録されます。

3. Deep Discovery Inspector のファームウェアイメージは、トレンドマイクロの Web サイトからダウンロードしてください。
4. このイメージをコンピュータの任意のフォルダに保存します。
5. [管理] > [アップデート] > [製品のアップデート] > [Service Pack/バージョンアップグレード] の順に選択します。
6. ファームウェアイメージを保存したフォルダを参照します。

   ヒント

   イメージファイルの拡張子は「`.R.tar`」です。

7. [アップロード] をクリックします。

   警告!

   次の手順を実行すると、Deep Discovery Inspector が再起動します。続行する前に、すべての製品コンソールタスクを完了していることを確認してください。

8. [OK] をクリックします。

   ファームウェアがアップグレードされ、Deep Discovery Inspector が再起動します。

9. アップグレードの進行状況の画面が読み込まれるまで 5 分間待ちます。オプションとして、ブラウザの [更新] をクリックすると、アップグレードの進行状況の画面が表示されます。

10. 管理コンソールで [ログオン] 画面が読み込まれるまで待ちます。

11. ブラウザのキャッシュをクリアします。詳細については、167 ページの「ブラウザのキャッシュのクリア」を参照してください。

12. 管理コンソールにログオンします。

13. Deep Discovery Inspector を Apex Central に登録している場合は、製品を再登録します。詳細については、278 ページの「Apex Central への登録」を参照してください。

ブラウザのキャッシュのクリア

手順

1. Chrome の場合:
   a. ブラウザで、[設定] に移動します。
   b. [詳細設定を表示...] をクリックします。
   c. [プライバシー] の [閲覧履歴データの消去...] をクリックします。
   d. [Cookie と他のサイトやプラグインのデータ] および [キャッシュされた画像とファイル] を選択します。
   e. [閲覧履歴データを消去する] をクリックします。
2. Mozilla Firefox の場合:
   a. [オプション] > [プライバシー] の順に選択します。
   b. [最近の履歴を消去] をクリックします。
   c. [Cookies] および [キャッシュ] を選択します。
   d. [今すぐ消去] をクリックします。
3. Microsoft Edge の場合:

a. 「ハブ」アイコンをクリックします。

b. 「履歴」アイコンをクリックします。

c. [すべての履歴をクリア] をクリックします。

d. [Cookie と保存済みの Web サイトデータ] と [キャッシュされたデータとファイル] を選択します。

e. [クリア] をクリックします。

通知

Deep Discovery Inspector は、しきい値ベースのネットワークイベントが発生した場合にメール通知を送信できます。

次の表は、Deep Discovery Inspector で使用可能な通知を示しています。

イベント	説明
脅威の検出	脅威の検出数が指定したしきい値に達しました。 詳細については、169 ページの「脅威の検出の通知」を参照してください。
高リスクホストの検出	Deep Discovery Inspector により、ネットワーク上の高リスクホストが確認されました。 詳細については、171 ページの「高リスクホストの検出の通知」を参照してください。
不審ホストの検出	不審ホストの数が指定したしきい値に達しました。 詳細については、174 ページの「不審ホストの検出の通知」を参照してください。
高ネットワークトラフィック	ネットワークトラフィックが指定したしきい値に達しました。 詳細については、176 ページの「高ネットワークトラフィックの通知」を参照してください。
分析されていないサンプルの検出	仮想アナライザでサンプルを分析できませんでした。 詳細については、178 ページの「分析されていないサンプルの検出の通知」を参照してください。

イベント	説明
仮想アナライザによる検出	仮想アナライザがサンプル内の不正なコンテンツを検出しました。 詳細については、180 ページの「仮想アナライザによる検出の通知」を参照してください。
拒否リストに基づく検出	ユーザ定義の拒否リスト内のオブジェクトへの一致が検出されました。 詳細については、182 ページの「拒否リストに基づく検出の通知」を参照してください。
Retro Scan による検出	Retro Scan が、トレンドマイクロのグローバルインテリジェンスリストで、C&C サーバへのコールバック回数の履歴を検出しました。 詳細については、183 ページの「Retro Scan による検出の通知」を参照してください。
トンネリングされたドメインの超過	トンネリングされたドメインのリストが指定したしきい値を超えています。 詳細については、184 ページの「トンネリングされたドメインの超過の通知」を参照してください。
低ネットワークトラフィック	指定したポートのネットワークトラフィックが設定したしきい値を下回っています。 詳細については、185 ページの「低ネットワークトラフィックの通知」を参照してください。

脅威の検出の通知

Deep Discovery Inspector は、検出数が指定したしきい値に達した場合に通知を送信できます。この通知では、脅威の種類ごとに検出数が示されます。

手順

1. [管理] > [通知] > [通知設定] > [脅威の検出] の順に選択します。
2. [脅威の検出数が次の場合に、管理者に通知する] を選択します。
3. 送信トラフィックと受信トラフィックのしきい値を指定します。

- 送信トラフィック: 監視対象ネットワークの検出
- 受信トラフィック: ネットワーク外部からの検出

4. 検出する脅威の種類を選択します。
5. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。
6. (オプション) 初期設定の件名とメッセージ本文を変更します。

重要

- メッセージの件名は 256 文字以内で指定してください。
- メッセージ本文は 4,096 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__LOOP_END__	メッセージトークンのループの終了
__LOOP_RISKS_COUNT__	検出数
__LOOP_RISKS_DIRECTION__	ネットワークトラフィックの方向
__LOOP_RISKS_NAME__	検出の種類
__LOOP_RISKS_THRESHOLD__	検出しきい値

メッセージトークン	説明
__LOOP_START__	メッセージトークンのループの開始
__TIMESTAMP__	通知の日時

重要

次のトークンは、メッセージトークンのループ内で必要に応じて繰り返されます。

- __LOOP_RISKS_COUNT__
- __LOOP_RISKS_DIRECTION__
- __LOOP_RISKS_NAME__
- __LOOP_RISKS_THRESHOLD__

7. [保存] をクリックします。

高リスクホストの検出の通知

Deep Discovery Inspector は、高リスクホストを検出した場合に通知を送信できます。ホストは、重大度の高いイベントが検出された場合に高リスクと見なされます。

手順

1. 監視対象ネットワークグループを 1 つ以上追加します。

   詳細については、257 ページの「ネットワークグループの追加」を参照してください。

2. [管理] > [通知] > [通知設定] > [高リスクホストの検出] の順に選択します。
3. [検出された高リスクホストを管理者に通知する] を選択します。
4. 送信間隔を指定します。

- 設定された間隔で通知を 1 つにまとめて送信します。
- 検出のたびにただちに送信します。

ヒント

パフォーマンスを向上させるには、通知をまとめて送信することをお勧めします。

5. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。

6. (オプション) 初期設定の件名とメッセージ本文を変更します。

注意

- メッセージ本文は 4,096 文字以内で指定してください。
- メッセージの件名は 256 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__AFFECTED_HOST__	影響を受けたホスト
__BEHAVIOR__	不審動作の説明
__DATE__	脅威の検出日時
__DIRECTION__	ネットワークトラフィックの方向
__DST_ACCOUNT__	送信先アカウント

メッセージトークン	説明
__DST_GROUP__	送信先グループ
__DST_IP_ADDR__	送信先 IP
__DST_MAC_ADDR__	送信先 MAC アドレス
__DST_PORT__	送信先ポート
__DST_ZONE__	送信先ゾーン
__HOSTNAME__	ホスト名
__HOST_IP__	危険性の高いホストの IP アドレス
__INCIDENT_COUNT__	高リスクホストの数
__LOG_QUERY_URL__	管理コンソールの [すべての検出] 画面へのリンク
__NETWORK_PROTOCOL__	ネットワークプロトコル
__SRC_ACCOUNT__	送信元アカウント
__SRC_GROUP__	送信元グループ
__SRC_IP_ADDR__	送信元 IP アドレス
__SRC_MAC_ADDR__	送信元 MAC アドレス

メッセージトークン	説明
__SRC_PORT__	送信元ポート
__SRC_ZONE__	送信元ゾーン
__TIMESTAMP__	通知の日時

7. [保存] をクリックします。

高リスクホストの検出通知の除外リストへの追加

手順

1. [管理] > [通知] > [通知設定] > [高リスクホストの検出通知] > [検索除外リスト] の順に選択します。

   [検索除外リスト] 画面が表示されます。

2. 通知から除外するホスト名を入力します。
3. IP アドレスまたはアドレス範囲を入力します。
4. [追加] をクリックします。

   IP アドレスまたはアドレス範囲が [定義済み IP アドレス] リストに表示されます。

不審ホストの検出の通知

Deep Discovery Inspector は、不審ホストを検出した場合に通知を送信できます。ホストは、関連する検出数が設定したしきい値に達した場合に不審と見なされます。この通知には、検出数が増加した原因を判別するために役立つ情報が含まれます。

手順

1. [管理] > [通知] > [通知設定] > [不審ホストの検出] の順に選択します。
2. [IP アドレスごとの検出数が次の場合に、管理者に通知する] を選択します。
3. 検出数のしきい値を指定します。

ヒント

初期設定の値を使用することをお勧めします。

4. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。

5. (オプション) 初期設定の件名とメッセージ本文を変更します。

注意

- メッセージ本文は 4,096 文字以内で指定してください。
- メッセージの件名は 256 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__LOOP_END__	メッセージトークンのループの終了
__LOOP_HOST_IP__	ホストの IP アドレス
__LOOP_INCIDENT_NUMBER__	インシデント数

メッセージトークン	説明
__LOOP_INCIDENT_THRESHOLD__	インシデントのしきい値
__LOOP_START__	メッセージトークンのループの開始
__TIMESTAMP__	通知の日時

注意

次のトークンは、メッセージトークンのループ内で必要に応じて繰り返されます。

- __LOOP_HOST_IP__
- __LOOP_INCIDENT_NUMBER__
- __LOOP_INCIDENT_THRESHOLD__

6. [保存] をクリックします。

高ネットワークトラフィックの通知

Deep Discovery Inspector は、ネットワークトラフィックが指定したしきい値に達した場合に通知を送信できます。アクティビティの増加は、ネットワーク上での攻撃を示す可能性があります。

手順

1. [管理] > [通知] > [通知設定] > [高ネットワークトラフィック] の順に選択します。
2. [ネットワークトラフィックが設定されたしきい値を越えた場合に、管理者に通知する] を選択します。
3. 次のいずれかを実行します。

- [自動検出] をクリックして、Deep Discovery Inspector が通常のトラフィックのしきい値を定義できるようにします。
- 手動で 1 時間ごとのトラフィックしきい値を指定します。

注意

ネットワークトラフィック量は最も近い整数に切り上げられます。たとえば、1.2GB は 2GB として、2.6GB は 3GB として表示されます。

4. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。

5. (オプション) 初期設定の件名とメッセージ本文を変更します。

注意

- メッセージ本文は 4,096 文字以内で指定してください。
- メッセージの件名は 256 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__TIMESTAMP__	通知の日時
__TRAFFIC_END_TIME__	トラフィック監視の終了日時
__TRAFFIC_START_TIME__	トラフィック監視の開始日時
__TRAFFIC_THRESHOLD__	ネットワークトラフィックのしきい値

6. [保存] をクリックします。

分析されていないサンプルの検出の通知

Deep Discovery Inspector は、仮想アナライザでサンプルを分析できない場合に通知を送信できます。この通知は、各サンプル、分析時間、ファイルのダウンロードで使用された URL に関する情報を提供します。

手順

1. [管理] > [通知] > [通知設定] > [分析されていないサンプルの検出] の順に選択します。
2. [分析されていないサンプルの検出を管理者に通知する] を選択します。
3. 送信間隔を指定します。

   ヒント

   初期設定の値を使用することをお勧めします。

4. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。

5. (オプション) 初期設定の件名とメッセージ本文を変更します。

   注意

   - メッセージ本文は 4,096 文字以内で指定してください。
   - メッセージの件名は 256 文字以内で指定してください。

   通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__IP_ADDRESS__	Deep Discovery Inspector の IP アドレス

メッセージトークン	説明
__LOOP_END__	メッセージトークンのループの終了
__LOOP_SAMPLE_FILE_ANALYZETIME__	サンプルの分析日時
__LOOP_SAMPLE_FILE_DOWNLOADURL__	サンプルのダウンロード URL
__LOOP_SAMPLE_FILE_SHA1__	SHA-1
__LOOP_SAMPLE_FILE_SIZE__	ファイルサイズ
__LOOP_SAMPLE_FILE_TYPE__	ファイルの種類
__LOOP_START__	メッセージトークンのループの開始
__TIMESTAMP__	通知の日時
__TOTAL_FAILED_COUNT__	分析されていないサンプルの数

注意

次のトークンは、メッセージトークンのループ内で必要に応じて繰り返されます。

- __LOOP_SAMPLE_FILE_ANALYZETIME__
- __LOOP_SAMPLE_FILE_DOWNLOADURL__
- __LOOP_SAMPLE_FILE_SHA1__
- __LOOP_SAMPLE_FILE_SIZE__
- __LOOP_SAMPLE_FILE_TYPE__

6. [保存] をクリックします。

仮想アナライザによる検出の通知

Deep Discovery Inspector は、どのパターンファイルにも一致しないファイルが、指定期間内に仮想アナライザによって不正と判定された場合に通知を送信できます。

不審ファイルとは、次の条件を満たしているものです。

- 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: [極めて不審なファイル] または [ヒューリスティック検出]
- 仮想アナライザのリスクレベル: 高、中、または低

手順

1. [管理] > [通知] > [通知設定] > [仮想アナライザによる検出] の順に選択します。
2. [仮想アナライザによって検出された不正なコンテンツ (または脅威) についてのみ管理者に通知する] を選択します。
3. 送信間隔を指定します。
   - 設定された間隔で通知をまとめて送信します。

1 時間から 24 時間までの値を選択します。

- 検出のたびにただちに送信します。

ヒント

パフォーマンスを向上させるには、通知をまとめて送信することをお勧めします。

4. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。

5. (オプション) 初期設定の件名とメッセージ本文を変更します。

注意

- メッセージ本文は 4,096 文字以内で指定してください。
- メッセージの件名は 256 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

変数	説明
__DETECTION_DETAIL__	仮想アナライザによる検出の詳細
__HTTPURL__	Deep Discovery Inspector の管理コンソールの URL
__TIMESTAMP__	通知の日時
__XHOURS__	通知の送信間隔

6. [保存] をクリックします。

拒否リストに基づく検出の通知

Deep Discovery Inspector は、指定した期間内に拒否リスト内のオブジェクトに一致する脅威を検出した場合に通知を送信できます。

手順

1. [管理] > [通知] > [通知設定] > [拒否リストの検出] の順に選択します。
2. [拒否リストに一致する不正コンテンツを管理者に通知する] を選択します。
3. 送信間隔を指定します。

   1 時間から 24 時間までの値を選択します。

   ヒント

   初期設定の値を使用することをお勧めします。

4. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。

5. (オプション) 初期設定の件名とメッセージ本文を変更します。

   注意

   - メッセージ本文は 4,096 文字以内で指定してください。
   - メッセージの件名は 256 文字以内で指定してください。

   通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__HTTPURL__	Deep Discovery Inspector の管理コンソールの URL
__TIMESTAMP__	通知の日時

メッセージトークン	説明
__XHOURS__	通知の送信間隔

6. [保存] をクリックします。

Retro Scan による検出の通知

Deep Discovery Inspector は、Retro Scan がトレンドマイクロのグローバルインテリジェンスリストに含まれる C&C サーバへのコールバックの履歴を検出した場合に通知を送信できます。

手順

1. [管理] > [通知] > [通知設定] > [Retro Scan による検出] の順に選択します。
2. [既知の C&C サーバへの過去のコールバック試行回数が確認された場合に管理者に通知する] を選択します。
3. 送信間隔を指定します。

   1 日から 30 日までの値を選択します。

   ヒント

   初期設定の値を使用することをお勧めします。

4. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。

5. (オプション) 初期設定の件名とメッセージ本文を変更します。

   注意

   - メッセージ本文は 4,096 文字以内で指定してください。
   - メッセージの件名は 256 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__HTTPURL__	Deep Discovery Inspector の管理コンソールの URL
__RETRO_SCAN_COMPROMISED_HOST_NUM__	危険にさらされているホストの数
__RETRO_SCAN_C_AND_C_CALLBACK_NUM__	検出された C&C コールバック回数
__TIMESTAMP__	Retro Scan レポートの実行日時

6. [保存] をクリックします。

トンネリングされたドメインの超過の通知

Deep Discovery Inspector は、トンネリングされたドメインのリストが指定したしきい値を超えた場合に通知を送信できます。

重要

トンネリングされたドメインの超過の通知は、Deep Discovery Inspector がインラインモードの場合のみ使用できます。

手順

1. [管理] > [通知] > [通知設定] > [トンネリングされたドメインの超過] の順に選択します。
2. [トンネリングされたドメインのリストが指定したしきい値を超えた場合に、管理者に通知する] を選択します。
3. [しきい値] に 1〜10,000 の値を指定します。
4. [通知の頻度] を指定します。
5. (オプション) 通知の受信者を設定します。

詳細については、187 ページの「メール通知の設定」を参照してください。

6. (オプション) 初期設定の件名とメッセージ本文を変更します。

注意

- メッセージ本文は 4,096 文字以内で指定してください。
- メッセージの件名は 256 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__TIMESTAMP__	通知の日時
__CURRENTNUMBER__	トンネリングされたドメインのリスト内の項目数
__THRESHOLDNUMBER__	トンネリングされたドメインの指定されたしきい値
__CONSOLEURL__	Deep Discovery Inspector の管理コンソールの URL

7. [保存] をクリックします。

低ネットワークトラフィックの通知

Deep Discovery Inspector は、指定したポートのネットワークトラフィックが設定したしきい値を下回る場合に通知を送信できます。

重要

Deep Discovery Inspector がインラインモードの場合、低トラフィックの通知は使用できません。

手順

1. [管理] > [通知] > [通知設定] > [低ネットワークトラフィック] の順に選択します。
2. [ネットワークトラフィックが指定したしきい値を下回った場合は管理者に通知する] を選択します。
3. 次の設定を行います。
   - しきい値: 1〜10,000 の値を指定します。
   - 管理対象ポート: Deep Discovery Inspector が低ネットワークトラフィックについて監視するポートを選択します。
   - 通知の頻度: 低ネットワークトラフィックが検出された場合に通知を受信する頻度を指定します。
4. (オプション) 通知の受信者を設定します。

   詳細については、187 ページの「メール通知の設定」を参照してください。
5. (オプション) 初期設定の件名とメッセージ本文を変更します。

注意

- メッセージ本文は 4,096 文字以内で指定してください。
- メッセージの件名は 256 文字以内で指定してください。

通知をカスタマイズする場合は、次のメッセージトークンのいずれかを使用できます。

メッセージトークン	説明
__LOOP_CURRENTNUMBER__	管理対象ポートのネットワークトラフィック
__LOOP_END__	管理対象ポートリストの終わり

メッセージトークン	説明
__LOOP_PORTNUMBER__	管理対象ポート
__LOOP_START__	管理対象ポートリストの始まり
__THRESHOLDNUMBER__	ネットワークトラフィックのしきい値
__TIMESTAMP__	通知の日時

6. [保存] をクリックします。

配信オプション

[メール設定] 画面を使用して、すべての通知について次の項目を設定します。

- 受信者のメールアドレス
- 通知期間ごとの最大通知数:
- 通知期間

メール通知の設定

[管理] > [システム設定] > [SMTP] で、SMTP サーバを設定します。

手順

1. [管理] > [通知] > [配信オプション] > [メール設定] の順に選択します。
2. 通知受信者のメールアドレスを 1 つ以上入力します。
   複数のアドレスはセミコロン (;) で区切ります。
3. 指定期間内に送信できる通知の最大数を入力します。

ヒント
初期設定の値を使用することをお勧めします。

4. 通知期間 (分) を入力します。

   それぞれの期間で通知の合計数がカウントされます。合計数が指定した通知の最大数を超えると、次の期間まで通知は送信されません。

ヒント
初期設定の値を使用することをお勧めします。

5. [保存] をクリックします。

監視/検索

[監視/検索] 設定では、次の Deep Discovery Inspector のネットワーク検出機能についてフィルタと除外項目を指定します。

- 188 ページの「ホスト/ポート」
- 190 ページの「脅威の検出」
- 196 ページの「Web レピュテーション」

  詳細については、192 ページの「Smart Protection」を参照してください。
- 200 ページの「アプリケーションフィルタ」
- 201 ページの「拒否リスト/許可リスト」
- 212 ページの「検出ルール」
- 213 ページの「パケットキャプチャ」
- 215 ページの「検出の除外設定」

ホスト/ポート

[ホスト/ポート] を設定すると、Deep Discovery Inspector で監視するネットワークトラフィックを指定できます。ネットワーク内のすべてのトラフィック、またはネットワーク内の指定されたセグメントを通過するトラフィックを検索します。

Deep Discovery Inspector では、初期設定ですべてのネットワークトラフィックが監視されます。

ネットワークの一部を経由する特定のトラフィックを監視することで、脅威およびイベントに関連する検出の数を大幅に減らすことができます。たとえば、送受信されるメールトラフィックを検索するには、[特定の IP 範囲とポートを監視する] を選択して、次の設定でルールを追加します。

- 送信元 IP: すべて
- 送信先 IP: すべて
- 送信先ポート: 25

ヒント

初期設定を使用して、すべてのネットワークトラフィックを設定することをお勧めします。

ホストとポートの設定

手順

1. [管理] > [監視/検索] > [ホスト/ポート] の順に選択します。
2. ネットワーク上のすべてのトラフィックを監視するには、[すべての IP 範囲とポートを監視する] を選択します。
3. ネットワーク上の特定のトラフィックを監視するには、[特定の IP 範囲とポートを監視する] を選択し、次のように設定します。
   a. [ネットワーク監視リスト] の下の [追加] をクリックします。

      [IP 範囲とポートを指定する] 画面が表示されます。
   b. [送信元 IP] を指定します。
   c. [送信先 IP] を指定します。
   d. [ポート] を指定します。
   e. [追加] をクリックします。

      [ネットワーク監視リスト] に新しいエントリが表示されます。

注意

[送信元 IP] または [送信先 IP] が [すべての IP 範囲とポートを監視する] の場合、反転したストリームによって開始されるトラフィックも検索されます。

ヒント

特定の IP アドレスでは、サブネットプレフィックス「/32」が必要です。

脅威の検出

次の機能を有効または無効にします。

- 脅威の検出: 既知および潜在的な脅威の両方を検出します。この機能は初期設定で有効になっています。
- Outbreak Containment Service: Deep Discovery Inspector が検出情報をログに記録したり、ネットワークトラフィックをブロックしたりすることを可能にします。

脅威の検出設定

手順

1. [管理] > [監視/検索] > [脅威の検出] の順に選択します。
2. [すべての脅威の検出を有効にする] を選択します。
3. [脅威の検出] で、[脅威の検出を有効にする] を選択します。
4. (オプション) [MARS (Mobile App Reputation Service) サーバクエリを有効にする] を選択します。

   このサービスは高度なサンドボックス環境であり、モバイルアプリの実行時の動作を分析して個人情報の漏えい、再パックされたモバイルアプリ、サードパーティの広告 SDK、脆弱性、およびアプリのカテゴリを検出します。

注意

MARS サービスは、Deep Discovery Inspector がモバイルデバイスに関する検出情報を解析のために MARS サーバに送信することを可能にします。

5. [Outbreak Containment Service] で、次のいずれかの方法を選択します。
   - 大規模感染検出を有効にする: 大規模感染検出機能を有効にしますが、トラフィックはブロックしません。
   - 大規模感染検出とトラフィックのブロックを有効にする: 大規模感染検出機能を有効にし、かつトラフィックをブロックします。

   Outbreak Containment Service は、大規模感染を引き起こす可能性のある既知の不正プログラムと不明の不正プログラムの両方を検出します。
6. Trend Micro Smart Protection Network に保護された脅威データベースを送信するには、[スマートフィードバックを有効にする (推奨)] をクリックします。

   スマートフィードバックを有効にすると、保護された脅威データベースが Trend Micro Smart Protection Network に送信され、トレンドマイクロは新しい脅威を迅速に識別して対応できるようになります。

   次のファイルタイプの情報をフィードバックに含めることができます。
   - class
   - cmd
   - hta
   - jar
   - js
   - lnk
   - mach-o
   - mov
   - ps1

- svg
- swf
- vbe
- vbs
- wsf

フィードバックには、製品名/製品 ID とバージョン情報のほかに、ファイルの種類、SHA-1、URL、IP アドレス、およびドメインなどの検出情報が含まれます。

7. [保存] をクリックします。

Smart Protection

トレンドマイクロの Smart Protection テクノロジは、ファイルレピュテーションサービスと Web レピュテーションサービスを提供する、次世代のクラウドベースの保護ソリューションです。Web レピュテーションサービスを統合することにより、Deep Discovery Inspector では、ユーザがアクセスしようとする Web サイトのレピュテーションデータを取得できます。Deep Discovery Inspector は、詐欺サイトや脅威の既知の発信源であることが Smart Protection テクノロジによって確認された URL をログに記録し、レポートを生成するためにログをアップロードします。

注意

Deep Discovery Inspector では、Smart Protection テクノロジに含まれているファイルレピュテーションサービスは使用しません。

Deep Discovery Inspector は、Smart Protection ソースに接続して Web レピュテーションデータを取得します。

レピュテーションサービスは、Trend Micro Smart Protection Network と Smart Protection Server によって提供されます。次の表では、2 つのソースを比較します。

注意

Smart Protection Server のサポートされるバージョンの詳細については、266 ページの「トレンドマイクロの統合製品とサービス」を参照してください。

表 6-5. Smart Protection ソース

比較基準	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
目的	Smart Protection テクノロジを統合するトレンドマイクロ製品にファイルレピュテーションサービスと Web レピュテーションサービスを提供する、グローバルなインターネットベースのインフラストラクチャです。	企業ネットワーク内にファイルレピュテーションサービスや Web レピュテーションサービスを配置して、効率を最適化します。 さらに Smart Protection Server は次のものを提供します。 • ソフトウェア安全性評価サービス • コミュニティドメイン/IP レピュテーションサービス • コミュニティファイルレピュテーション • モバイルアプリレピュテーションサービス • 機械学習型検索エンジン • Web 検査サービス • Web レピュテーションサービス
管理	トレンドマイクロがホストおよび管理します。	トレンドマイクロ製品の管理者がインストールおよび管理します。
接続プロトコル	HTTPS	HTTPS

比較基準	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
使用方法	Smart Protection Server をインストールしない場合に使用します。 Trend Micro Smart Protection Network をソースとして設定する方法については、197 ページの「Web レピュテーションの設定」を参照してください。	プライマリソースとして使用し、Trend Micro Smart Protection Network を代替ソースとして使用します。 Smart Protection Server の導入時の設定方法や、ソースとしての設定方法については、195 ページの「Smart Protection Server の設定」を参照してください。

Smart Protection Server について

留意点	説明
配置	別のトレンドマイクロ製品で使用するために Smart Protection Server をインストールしたことがある場合は、同じサーバを Deep Discovery Inspector でも使用できます。複数のトレンドマイクロ製品からクエリを同時に送信できますが、クエリの量が増加すると、Smart Protection Server に対する負荷が過剰になる場合もあります。Smart Protection Server が、異なる製品から送信されたクエリを処理できることを確認してください。規模のガイドラインや推奨事項については、サポートプロバイダにお問い合わせください。
IP アドレス	Smart Protection Server と VMware ESX/ESXi サーバ (Smart Protection Server のホスト) には、一意の IP アドレスが必要です。VMware ESX/ESXi サーバと Deep Discovery Inspector の IP アドレスをチェックし、これらの IP アドレスが Smart Protection Server に割り当てられていないことを確認してください。
インストール	インストールの手順と要件については、次の URL から「Trend Micro Smart Protection Server インストールガイド」をダウンロードしてご確認ください。https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

Smart Protection Server の設定

手順

1. VMware ESX/ESXi サーバに Smart Protection Server (スタンドアロン) をインストールします。
2. Deep Discovery Inspector 管理コンソールから Smart Protection Server を設定します。

   詳細については、197 ページの「Web レピュテーションの設定」の手順 3 以降を参照してください。

注意

- Smart Protection Server では Trend Micro Smart Protection Network のデータベース全体を複製できないため、一部の URL のレピュテーションデータが含まれないことがあります。また更新頻度が低いと、古くなったレピュテーションデータが Smart Protection Server から返される場合があります。
- このオプションを有効にすることで、レピュテーションデータの精度と関連性が向上します。
- このオプションを無効にすると、データを取得するための時間と帯域幅を節約できます。

Smart Protection Server リストの管理

複数の Smart Protection Server が追加され、フェイルオーバーが発生すると、Deep Discovery Inspector はフェイルオーバーサーバの Web レピュテーションサービスのみを使用し、他のサービスは使用しなくなります。

手順

1. [管理] > [監視/検索] > [Web レピュテーション] > [Smart Protection Server のリスト] の順に選択します。
2. Smart Protection Server との接続ステータスを確認するには、[接続テスト] をクリックします。

3. サーバの設定を変更するには、次の手順に従ってください。
   a. サーバのアドレスをクリックします。
   b. 表示された画面で、サーバの IP アドレス、説明、および設定を変更します。
   c. 新しい IP アドレスを指定した場合は、[接続テスト] をクリックして接続を確認します。
   d. [OK] をクリックします。
4. リストからサーバを削除するには、サーバを選択して [削除] をクリックします。
5. サーバの使用順序を変更するには、[順序] 列のアイコンをクリックします。
6. [保存] をクリックします。

Web レピュテーション

Deep Discovery Inspector は、Trend Micro Smart Protection Network と統合されています。これは、ユーザがアクセスしようとしている Web サイトの評価を判断するクラウドベースのインフラストラクチャです。Deep Discovery Inspector は、Smart Protection テクノロジによって詐欺サイトや脅威の既知の発信源であることが確認された URL をログに記録します。

注意

[検出] > [すべての検出] から、Web レピュテーションログに対してクエリを実行できます。

Smart Protection テクノロジの詳細と Smart Protection Server (スタンドアロン) の設定方法については、192 ページの「Smart Protection」を参照してください。

Web レピュテーションの設定

手順

1. [管理] > [監視/検索] > [Web レピュテーション] の順に選択します。
2. [Web レピュテーションを有効にする] をオンにします。
3. [Smart Protection ソース] を選択します。
   - Trend Micro Smart Protection Network

     Trend Micro Smart Protection Network は、Smart Protection テクノロジを統合するトレンドマイクロ製品にレピュテーションサービスを提供する、グローバルなクラウドベースのインフラストラクチャです。Deep Discovery Inspector は、HTTP を使用して Trend Micro Smart Protection Network に接続します。Smart Protection Server を設定しない場合は、このオプションを選択します。

     重要

     このオプションを選択すると、ネットワーク内の C&C サーバへのコールバック試行とその他の関連アクティビティについて Web アクセスの履歴ログを検索する、クラウドベースサービスの Retro Scan を有効にできます。Web アクセスログには、ごく最近になって発見された、未検出および未ブロックの C&C サーバへの接続が含まれている場合があります。そのようなログを調査することは、フォレンジック調査において重要で、攻撃によってネットワークが影響を受けているかどうかを判断するために役立ちます。

     手順 4 で Retro Scan を有効にすることをお勧めします。

   - Smart Protection Server

     Smart Protection Server (スタンドアロン) は次のことを実行します。

     - Trend Micro Smart Protection Network と同じ Web レピュテーションサービス、CSSS (ソフトウェア安全性評価サービス)、Mobile App Reputation Service (MARS)、およびコミュニティファイルレピュテーションを提供します。

- これらのサービスをグローバルな Trend Micro Smart Protection Network にリレーしてネットワーク効率を最適化します。

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

重要

このオプションを選択すると、Retro Scan が無効になり、それまでの Retro Scan の検出ログはすべて削除されます。

4. (オプション) Retro Scan を有効にします。

   詳細については、104 ページの「Retro Scan の有効化」を参照してください。

5. Smart Protection Server を選択するには、[Smart Protection Server のリスト] を設定します。

   a. Smart Protection Server の名前または IP アドレスを入力します。

      Smart Protection Server のコンソールで、[Smart Protection] > [レピュテーションサービス] > [Web レピュテーション] の順に選択して、この IP アドレスを取得します。

      IP アドレスは画面にリストされている URL に含まれています。

   b. (オプション) [接続テスト] をクリックします。

   c. サーバの説明を入力します。

   d. Smart Protection Server を定期的にアップデートします。

      Smart Protection Server のコンソールで、[アップデート] > [Program] > [自動アップデート] の順に選択し、[予約アップデートを有効にする] をクリックします。

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

注意

プロキシ設定を無効にすると、プロキシサーバ経由で接続されている Smart Protection Server に対し直接接続を行います。プロキシ設定が無効な場合、[プロキシ接続] 列のステータスは [なし] と表示されます。

注意

プロキシサーバで次のポートを設定して、Smart Protection Server への接続を許可します。

- 5275
- 443

f. [追加] をクリックします。

この Smart Protection Server が [Smart Protection Server のリスト] に追加されます。

g. (オプション) 別のサーバを追加します。

注意

最大 10 件のサーバを追加できます。複数のサーバを設定する場合、Deep Discovery Inspector は、リストに表示される順番でこれらのサーバに接続します。

ヒント

フェイルオーバーの目的で複数の Smart Protection Server をインストールすることをお勧めします。Deep Discovery Inspector がサーバに接続できない場合は、Smart Protection Server のリストにある他のサーバへの接続が試行されます。

h. [順序] 列の下の矢印でサーバの優先度を設定できます。

6. 大量の Web レピュテーション検出をフィルタ処理するには、[スパムメールとアドウェアの検出を除外し、検出量を削減する] をオンにします。

ほとんどの Web レピュテーション検出はスパムメールやアドウェアに関連しています。スパムメールとアドウェアの検出を除外すると、検出量を削減できます。

7. [保存] をクリックします。

アプリケーションフィルタ

アプリケーションフィルタは、セキュリティリスクを迅速に特定し、不正コードの拡散を防ぐために役立つ情報を提供します。

次のアプリケーションの検出を有効にします。

表 6-6. アプリケーションの種類

アプリケーション	説明
インスタントメッセージング	ネットワークに接続中のユーザ間で通信を行い、情報やファイルを共有します。
P2P トラフィック	コンピュータ間でファイルを共有します。
ストリーミングメディア	オーディオビジュアルコンテンツをダウンロードしながら再生します。

アプリケーションフィルタの設定

手順

1. [管理] > [監視/検索] > [アプリケーションフィルタ] の順に選択します。
2. [インスタントメッセージング] の検出を有効にします。
   a. [インスタントメッセージング] チェックボックスをオンにします。
   b. 検出するインスタントメッセージアプリケーションを選択します。

ヒント

複数のアプリケーションを選択するには <Ctrl> キーを使用します。

c. >> アイコンをクリックして、選択したアプリケーションを [選択したインスタントメッセージングアプリケーション] に移動します。

3. [P2P トラフィック] の検出を有効にします。
   a. [P2P トラフィック] チェックボックスをオンにします。
   b. 検出する P2P アプリケーションを選択します。

ヒント

複数のアプリケーションを選択するには <Ctrl> キーを使用します。

   c. >> アイコンをクリックして、選択したアプリケーションを [選択した P2P アプリケーション] に移動します。
4. [ストリーミングメディア] の検出を有効にします。
   a. [ストリーミングメディア] チェックボックスをオンにします。
   b. 検出するストリーミングメディアアプリケーションを選択します。

ヒント

複数のアプリケーションを選択するには <Ctrl> キーを使用します。

   c. >> アイコンをクリックして、アプリケーションを [選択したストリーミングメディアアプリケーション] に移動します。
5. [保存] をクリックします。

拒否リスト/許可リスト

[拒否リスト] および [許可リスト] にアクセスするには、[管理] > [監視/検索] > [拒否リスト/許可リスト] の順に選択します。

[拒否リスト/許可リスト] 画面には、[拒否リスト]、[許可リスト]、および [インポート/エクスポート] のタブが含まれています。

表 6-7. [拒否リスト/許可リスト] のタブ

タブ	説明
拒否リスト	Deep Discovery Inspector では、[拒否リスト] のエンティティへの接続を管理できます。[拒否リスト] エンティティに対して、次の処理を設定できます。 • 監視 • 監視およびリセット
許可リスト	Deep Discovery Inspector は、[許可リスト] のエンティティへの接続を許可します。 ヒント [許可リスト] を使用して、[拒否リスト] による誤検知の数を減少させます。
インポート/エクスポート	[拒否リスト] または [許可リスト] のエンティティをインポートまたはエクスポートします。

拒否リスト/許可リストの形式ルール

Deep Discovery Inspector の拒否リストおよび許可リストには、次の形式ルールが適用されます。

[管理] > [監視/検索] > [拒否リスト/許可リスト] の順に選択します。

表 6-8. 拒否リスト/許可リストの形式ルール

形式ルール	説明
IP アドレス	構文 • 単一の IP: IP アドレスは、次の形式で指定する必要があります。XXX.XXX.XXX.XXX。ここで、X は 0〜255 の整数です。 IPv4 の例: 192.168.1.1 IPv6 の例: fd00:1:1111:200::1000 • IP 範囲: IP アドレスは、次の形式で指定する必要があります。XXX.XXX.XXX.XXX-XXX.XXX.XXX.XXX。ここで、X は 0〜255 の整数です。 IPv4 の例: 192.168.1.0-192.168.1.255 IPv6 の例: fd00:1:1111:200::1000-fd00:1:1111:200::1fff • サブネット: IP アドレスは、次の形式で指定する必要があります。XXX.XXX.XXX.XXX/<Mask Bit>。ここで、X は 0〜255 の整数で、<Mask Bit>は 1〜32 の整数です。 IPv4 の例: 192.168.1.0/24 IPv6 の例: fd00:1:1111:200::1000/116
	IP アドレスのエンティティの最大数 拒否/許可リストには、[IP アドレス] のエンティティを最大 10,000 件まで追加できます。

形式ルール	説明
ドメイン	サポートされる文字 各ドメイン名は 1 文字以上にする必要があります。 Deep Discovery Inspector では、ドメイン名に次の文字を使用できます。 ASCII • 0x2D (-)、0x2E (.) • 0x30 (0)〜0x39 (9) • 0x41 (A)〜0x5A (Z) • 0x61 (a)〜0x7A (z) UTF-8 文字 (ASCII コード>=0x80) 注意 UTF8 以外の文字は Punycode に変換されます。
	最大長 各ドメイン名の最大長: 63 文字 ドメインの最大長: 255 文字
	ワイルドカード (*) ワイルドカードは、ドメイン名のプレフィックスでのみ使用できます。ワイルドカードがプレフィックスで使用されている場合は、「.」で接続する必要があります。1 つのドメインで 1 つのワイルドカードのみを使用できます。 ドメインのマッチングでは大文字小文字が区別されます。
	ドメインのエンティティの最大数 拒否リスト/許可リストには、最大 10,000 件の [ドメイン] のエンティティを追加できます。

形式ルール	説明
URL	構文 [http:// | https://]<Domain>[:<Port>][/<URI-prefix>] • [http:// | https://] 割り当てられていない場合、初期設定は「http://」です。 「http://:」と「https://」の両方に一致させるには、ルールを複数作成します。 • <Domain> DNS のドメイン拒否リストの構文に準じます。 • [:<Port>] (オプション) 割り当てられていない場合、初期設定は HTTP で「:80」(ポート 80)、HTTPS で「:443」(ポート 443) です。 特定のポートに 1〜65,535 の整数を割り当てるか、ワイルドカード (*) を使用してすべてのポートに割り当てます。 • [/<URI-prefix>] (オプション) 割り当てられていない場合、初期設定は、すべてのパスに一致するワイルドカードです。 パスのない URL に一致させるには、「/」と「/*」を使用します。 例: `www.abc.com/*`は、`www.abc.com` に一致します。 [/<URI-prefix>] は、常にプレフィックスマッチングとして適用されます。1 つのプレフィックスで 1 つのワイルドカードのみを使用できます。 URI マッチングでは大文字小文字は区別されません。
	URL エンティティの最大数 拒否リスト/許可リストには、最大 10,000 件の [URL] のエンティティを追加できます。

形式ルール	説明
SHA-1	構文 Deep Discovery Inspector は、SHA-1 ルール用に次の文字をサポートしています。 ASCII • 0x30 (0)〜0x39 (9) • 0x41 (A)〜0x46 (F) • 0x61 (a)〜0x66 (f)
	最大長 SHA-1 ルールの最大長: 40
	SHA-1 エンティティの最大数 拒否リスト/許可リストには、[SHA-1] のエンティティを最大 10,000 件まで追加できます。

拒否リストと許可リストの設定

[拒否リスト] および [許可リスト] 画面で、次の機能を設定します。

- 表示
- 追加
- 削除
- ステータス
- 編集
- 優先度 ([拒否リスト] のみ)

さらに、[検索] を使用して、さまざまなエンティティをクエリできます。

変更を保存してすべてのアップデートを適用するには、[リロード] をクリックします。

拒否リストと許可リストの設定

手順

1. [表示] を設定して、次の拒否リスト/許可リストのエンティティのいずれかを表示します。
   - ファイル
   - IP アドレス
   - URL
   - ドメイン

   (オプション) [許可リスト] では [すべて] を選択することもできます。
2. [追加] をクリックして、[拒否リストへの項目の追加]/[許可リストへの項目の追加] 画面を開きます。
   a. [種類] として [ファイル]、[IP アドレス]、[URL]、または [ドメイン] を選択します。
   b. 適切なテキストボックスに値を入力します。

リストの種類	名前の種類
ファイル	SHA-1
IP アドレス	IP アドレス
URL	URL
ドメイン	ドメイン

   注意
   ファイルの最大サイズを設定するには、[管理] > [システムのメンテナンス] > [ストレージ管理] の順に選択します。

   c. ([拒否リスト] のみ) 新しいエンティティへの接続を管理するための [処理] を設定します。

リストの種類	処理
ファイル	監視のみ
IP アドレス	• 監視のみ • 監視およびリセット
URL	• 監視のみ • 監視およびリセット
ドメイン	• 監視のみ • 監視およびリセット

d. (オプション) コメントを追加します。

3. [拒否リスト] または [許可リスト] のエンティティを削除するには、[削除] をクリックします。

   削除されたエンティティはデータベースから削除されます。

4. [拒否リスト] または [許可リスト] のエンティティのステータスを有効または無効にします。

5. [種類]、[IP アドレス]/[SHA-1]、コメント、および [処理] ([拒否リスト] のみ) を編集するには、[拒否リスト] または [許可リスト] のエンティティをクリックします。

6. (オプション: [拒否リスト] のみ) [拒否リストのエンティティ] の優先度を変更するには、優先度の数の横にあるアイコンをクリックします。

   [優先度] の数は、[拒否リストのエンティティ] が検出に一致する順序を示しています。優先度の数字は連続し、番号順になっています。小さな数字ほど先に一致します。

7. さまざまな拒否/許可リストのエンティティをクエリするには、IP アドレス、SHA-1、ドメイン、または URL を指定します。

注意

SHA-1 エンティティを検索するには、正確な値を入力します。IP アドレス、ドメイン、または URL のエンティティの場合、Deep Discovery Inspector は部分的な値に一致させます。

8. すべてのアップデートを適用して変更を保持するには、[リロード] をクリックします。

注意

最適なパフォーマンスを得るには、[拒否リスト/許可リスト] をアップデートするときに [リロード] ボタンを使用します。

拒否リスト/許可リストをインポートするための形式ルール

Deep Discovery Inspector の拒否リストおよび許可リストのインポートには、次の形式ルールが適用されます。

[管理] > [監視/検索] > [拒否リスト/許可リスト] > [インポート/エクスポート] の順に選択します。

表 6-9. 拒否リスト/許可リストをインポートするための形式ルール

形式ルール	説明
コメント	コメントは 64 文字までです。
重複するファイル	重複するファイルをインポートできます。
CSV 形式	Deep Discovery Inspector は、標準の.csv 形式のみサポートします。カンマ区切りと UTF-8 エンコーディングを使用します。

他のすべての拒否リスト/許可リストの形式ルールについては、202 ページの「拒否リスト/許可リストの形式ルール」を参照してください。

カスタム拒否リスト/許可リストのエクスポート

手順

1. [管理] > [監視/検索] > [拒否リスト/許可リスト] > [インポート/エクスポート] の順に選択します。
2. [インポート/エクスポート] タブを選択します。

3. 拒否リストをエクスポートするには、[インポート/エクスポート] 画面から [拒否リスト] を選択し、[エクスポート] をクリックします。

   Deep Discovery Inspector は、すべてのカスタム許可リストを含む.csv ファイルをエクスポートします。

4. 許可リストをエクスポートするには、[インポート/エクスポート] 画面から [許可リスト] を選択し、[エクスポート] をクリックします。

   Deep Discovery Inspector は、すべてのカスタム拒否リストを含む.csv ファイルをエクスポートします。

カスタム拒否リスト/許可リストのインポート

手順

1. [管理] > [監視/検索] > [拒否リスト/許可リスト] > [インポート/エクスポート] の順に選択します。
2. [インポート/エクスポート] タブを選択します。
3. (オプション) .csv ファイルを準備します。

   次のいずれかを実行します。

   - カスタム拒否リストを準備します。

     次のフィールドを含む.csv ファイルを準備します。[ステータス]、[優先度]、[拒否リストのエンティティ]、[ソースの種類]、[種類]、[処理]、[コメント]、および[最終更新日]

   - カスタム許可リストを準備します。

     次のフィールドを含む.csv ファイルを準備します。[ステータス]、[許可リストのエンティティ]、[ソースの種類]、[種類]、[コメント]、および[最終更新日]

   ステータス

   - 0:無効
   - 1:有効

ソースの種類

- 0:ユーザ指定
- 1:仮想アナライザ
- 2:C&C コールバック

処理 (拒否リストのみ)

- 0:監視
- 1:監視およびリセット

注意

[ステータス]、[ソースの種類]、および [処理] に値を入力しない場合は、次のように初期設定値が適用されます。

- ステータス:`1`
- ソースの種類:`0`
- 処理:`0`

4. 参照してファイルを選択します。

   ファイル形式は「,」によって区切られ、UTF-8 によってエンコーディングされます。

注意

.csv ファイル、種類、および許可リストのエンティティのフィールドには、有効なエンティティを入力する必要があります。[種類] として [ファイル]、[IP アドレス]、[URL]、または [ドメイン] を選択します。

[ステータス] と [処理] の場合は、`0` と `1` のみが有効な値です。[ソースの種類] の場合は、`0`、`1`、および `2` のみが有効な値です。他の値を使用した場合は、インポートの試行時にエラーが返されます。

5. [インポート] をクリックします。

現在選択されているリストは上書きされます。

検出ルール

検出ルールを有効または無効にして、脅威の検出をカスタマイズします。

確実性レベル、概要、技術的な詳細情報など、検出ルールの詳細については脅威データベースにアクセスしてください。脅威データベースにアクセスするには、管理コンソールで [ヘルプ] > [脅威データベース] の順に選択し、[Network Content Inspection Rules] を参照するか特定のルールの番号を検索します。

検出ルールの設定

手順

1. [管理] > [監視/検索] > [検出ルール] の順に選択します。
2. (オプション) [エクスポート] をクリックすると、現在の検出ルールの設定を含むファイルをダウンロードできます。
3. (オプション) [インポート] をクリックすると、検出ルールの設定を含むファイルをインポートして、すべての検出ルールの設定を置換できます。
4. (オプション) [現在] 列のアイコンをクリックして特定のルールの設定を変更したら、[変更の保存] をクリックします。
5. (オプション) [すべてのルールの設定変更] ドロップダウンメニューで次のいずれかのオプションを選択したら、[変更の保存] をクリックします。
   - [初期設定状態]: 初期設定の検出ルールを使用する場合に選択します。

     注意

     トレンドマイクロは初期設定を使用することをお勧めします。
   - [有効]: すべての検出ルールを有効にする場合に選択します。
   - [無効]: すべての検出ルールを無効にする場合に選択します。

6. (オプション) [ID] 列で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に表示できます。

パケットキャプチャ

注意

Deep Discovery Inspector が Trend Vision One に接続されている場合、この設定は使用できません。

Deep Discovery Inspector は、検出されたトラフィックだけでなく、検出時の接続に関係していたクライアントまたはサーバに関連するトラフィックも取得します。

この機能は慎重に使用することをお勧めします。ネットワークパケットのキャプチャは、処理能力とディスク容量の消費を増大させる可能性があります。

次の表は、[パケットキャプチャ] 画面で実行可能な操作を示しています。

操作	説明
パケットキャプチャの有効化	[パケットキャプチャの有効化] を選択すると、特定の検出にリンクしている TCP/UDP パケットを取得できます。 警告! この機能を有効にするには、アプライアンスを再起動する必要があります。
パケットキャプチャルールの追加	[追加] をクリックして、新しいパケットキャプチャルールを作成します。 詳細については、214 ページの「パケットキャプチャルールの追加」を参照してください。
パケットキャプチャルールの削除	リストからパケットキャプチャルールを 1 つ以上選択して、[削除] をクリックします。
パケットキャプチャルールのインポート	[インポート] をクリックして、他の Deep Discovery Inspector アプライアンスのパケットキャプチャルールをインポートします。

操作	説明
パケットキャプチャルールのエクスポート	[エクスポート] をクリックして、お使いの Deep Discovery Inspector アプライアンスのすべてのパケットキャプチャルールをダウンロードします。

ヒント

- 指定した検出のパケットキャプチャファイルは、[検出の詳細] 画面で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。詳細については、115 ページの「[すべての検出] - [検出の詳細] - [接続の詳細]」および 67 ページの「接続の詳細」を参照してください。

パケットキャプチャルールの追加

手順

1. [管理] > [監視/検索] > [パケットキャプチャ] の順に選択します。
2. [追加] をクリックします。

   新しい画面が表示されます。
3. [有効] を選択します。
4. ルールの優先度を指定します。
5. (オプション) [説明] を入力します。
6. IP アドレスまたは IP アドレスの範囲を 1 つ以上入力します。

   注意

   指定したアドレスまたはアドレス範囲内の検出条件のパケットのみが取得されます。

   IP アドレスまたは IP アドレス範囲は最大 50 エントリまで追加できます。

7. [検出条件] で、何も行わずにすべての検出に対してルールを適用するか、[特定条件の追加] をクリックします。
8. [特定条件の追加] をクリックした場合は、条件を指定します。
   - 検出の種類
   - 検出ルール ID
   - 脅威/検出/参照

   注意
   [次の値を含む] および [次の値を含まない] は部分的な文字列に一致します。[等しい] は部分的な文字列には一致しません。

   - 重大度

   注意
   条件を追加するには [+] をクリックします。条件を削除するには [-] をクリックします。

   最大 10 の条件を追加できます。
9. パケットが条件に一致した場合に実行する処理を選択します。
   - 取得する
   - 取得しない
10. [追加] をクリックします。

検出の除外設定

検出の除外には、除外の条件のリストが含まれます。有効にした条件に一致する検出はログに記録されません。

検出の除外設定

重要

Deep Discovery Inspector が Network Inventory に接続され、Network Inventory から管理されている場合、検出の除外設定を使用することはできません。

手順

1. [管理] > [監視/検索] > [検出の除外設定] の順に選択します。
2. (オプション) 検出の除外を追加します。
   a. [追加] をクリックします。

      [除外設定の追加] 画面が表示されます。
   b. [ステータス] を選択します。
      - 有効: 検出の除外を有効にします。
      - 無効: 検出の除外を無効にします。
   a. (オプション) [説明] に検出の除外の説明を入力します。
   b. [除外設定の条件] に検出の除外の条件を指定します。条件を追加するには、[+] をクリックします。

      複数の値を指定するには、`<Tab>` キーまたは `<Enter>` キーで区切ります。

      部分的な文字列に一致させるには contains 演算子、完全な文字列に一致させるには in 演算子、ドメイン名に一致させるには end with 演算子を使用します。Deep Discovery Inspector では、文字列の一致で大文字と小文字は区別されません。

      例:

      - ホスト名 - 次のいずれかの値を含む - `abc,DEF`

        この条件は、「abc」または「def」と完全に一致する (大文字と小文字は区別しない) ホスト名と一致します。

- 「abc」は一致
- 「deF」は一致
- 「abcxyz」は一致しない
- 「xyzdEf」は一致しない

- ホスト名 - 次の値を含む - `abc,DEF`

  この条件は、名前の一部に「abc」または「def」を含む (大文字と小文字は区別しない) ホスト名と一致します。

  - 「abc」は一致
  - 「deF」は一致
  - 「abcxyz」は一致
  - 「xyzdEf」は一致

- ドメイン - 次で終わる - `trendmicro.com`

  この条件は、「trendmicro.com」で終わる (大文字と小文字は区別しない) ドメインと一致します。

  - 「www.trendmicro.com」は一致
  - 「www.NOTrendmicro.com」は一致
  - 「www.trendmicro.com.tw」は一致しない

c. [追加] をクリックします。

   [除外設定の追加] 画面が閉じます。

d. [保存] をクリックします。

3. (オプション) 検出の除外設定を 1 つ以上削除します。

   a. 削除する検出の除外の横にあるチェックボックスをオンにします。

   b. [削除] をクリックします。

   c. [保存] をクリックします。

4. (オプション) [すべてエクスポート] をクリックして、すべての検出の除外の条件を含むファイルを保存します。

5. (オプション) 検出の除外をインポートします。

警告!

検出の除外設定をインポートすると、現在のすべての検出の除外設定が置換されます。

[すべてエクスポート] 機能を使用して、現在の検出の除外設定のバックアップを作成することをお勧めします。

   a. [インポート] をクリックします。

      [除外設定にインポート] 画面が表示されます。

   b. 検出の除外の条件を含むファイルを選択します。

   c. [インポートして置換] をクリックします。

6. (オプション) 検出の除外を編集します。

   a. 編集する項目の横にある [編集] 列のアイコンをクリックします。

      [除外設定の編集] 画面が表示されます。

   b. 検出の除外を編集します。

   c. [保存] をクリックします。

      [除外設定の編集] 画面が閉じます。

   d. [保存] をクリックします。

7. (オプション) 検出の除外を有効または無効にします。

   a. [ステータス] 列のアイコンをクリックしてステータスを切り替えます。

   b. [保存] をクリックします。

TLS トラフィックインスペクション

重要

TLS トラフィックインスペクションを使用するには、Deep Discovery Inspector アプライアンスでインライン導入がサポートされる必要があります。詳細については、「インストールガイド」を参照してください。

インライン導入した Deep Discovery Inspector で TLS トラフィックインスペクションを使用して、TLS トラフィックの復号と検査を行います。TLS トラフィックインスペクションでは、IPv4、VLAN、および TLS がサポートされます。Deep Discovery Inspector をインライン導入して TLS トラフィックインスペクションを有効にしない場合、インラインポートを流れるトラフィックは検査されません。

Deep Discovery Inspector のインライン導入とアウトオブバンド導入は同時にサポートされません。トラフィックを検査するには、TLS トラフィックインスペクションを有効にしてインラインポートを使用するか、TLS トラフィックインスペクションを無効にしてトラフィックをデータポートにミラーリングする必要があります。

Deep Discovery Inspector にはトラフィックをブロックする機能はありません。Deep Discovery Inspector ではトラフィックの検査のみ行うことができます。

次の画面を使用して、TLS トラフィックインスペクションを設定します。

- TLS トラフィックインスペクションの一般的な設定を行うには、[インスペクション設定] 画面を使用します。

  詳細については、220 ページの「インスペクション設定」を参照してください。

- TLS トラフィックインスペクションの証明書を設定するには、[証明書の管理] 画面を使用します。

  注意

  TLS トラフィックインスペクションには信頼済み CA 証明書と署名証明書を設定する必要があります。

詳細については、221 ページの「証明書の管理」を参照してください。

- TLS トラフィックインスペクションの復号ポリシーを設定するには、[復号ポリシー] 画面を使用します。

  詳細については、224 ページの「復号ポリシー」を参照してください。

Deep Discovery Inspector によって復号された TLS トラフィックの量は、「一目でわかるアプライアンス情報」または [過去 30 日間の監視対象のネットワークトラフィック] ウィジェットで確認できます。詳細については、41 ページの「過去 30 日間の監視対象のネットワークトラフィック」および 13 ページの「管理コンソール」を参照してください。

注意

TLS トラフィックインスペクションが有効な場合、Deep Discovery Inspector で検索されたトラフィックとは、インラインポートを流れ、Deep Discovery Inspector によって復号されたトラフィックのことを指します。

インスペクション設定

[インスペクション設定] 画面では、次の項目を設定できます。

設定	説明
TLS トラフィックインスペクションを有効にする	有効/無効を切り替えます。 有効にすると、Deep Discovery Inspector はインラインアプライアンスとして暗号化された送信トラフィックを監視します。 この設定を有効にするには、復号ポリシーを設定しておく必要があります。詳細については、224 ページの「復号ポリシー」を参照してください。

設定	説明
ドメイントンネリングを有効にする	有効 (初期設定) /無効を切り替えます。 Deep Discovery Inspector で検査できない TLS 接続が、トンネリングされたドメインのリストに表示されます。 有効にすると、Deep Discovery Inspector では以降の 24 時間、トンネリングされたドメインのリスト内の、クライアントとドメインのペア間の新しい接続が検査されなくなります。 ドメインまたは URL への TLS 接続の検査が失敗しても、そのドメインまたは URL が信頼される場合は、[復号ポリシー] 画面の [ドメインオブジェクト] で、そのドメインまたは URL を [除外] として設定できます。

トンネリングされたドメインの設定

Deep Discovery Inspector が復号と検査を試みた TLS トラフィックのドメインのリストを確認するには、[管理] > [監視/検索] > [TLS トラフィックインスペクション] > [インスペクション設定] の順に選択し、[トンネリングされたドメインの設定] をクリックします。

特定のドメインの TLS トラフィックを復号しない場合は、[復号ポリシー] 画面で、[ドメインの除外に移動] をクリックするか、そのドメインを [ドメインオブジェクト] > [除外] リストに追加します。

ヒント

すべてのサブドメインをドメインの除外に含めるには、[復号ポリシー] 画面でドメインを指定して、ワイルドカード文字 (*) を使用します。

証明書の管理

TLS トラフィックインスペクションを実行するには、信頼済み CA 証明書と署名証明書を設定する必要があります。詳細については、次の項目を参照してください。

- 222 ページの「信頼済み CA 証明書」
- 223 ページの「署名証明書」

信頼済み CA 証明書

TLS トラフィックを検査する際、Deep Discovery Inspector はクライアントに代わってプロキシのように動作し、サーバ証明書を確認します。Deep Discovery Inspector がサーバを確認するには、信頼済み CA 証明書をインポートする必要があります。信頼済み CA 証明書をインポートしないと、Deep Discovery Inspector はサーバを信頼せず、サーバに接続しません。

信頼済み CA 証明書を管理するには、[管理] > [監視/検索] > [TLS トラフィックインスペクション] > [証明書の管理] > [信頼済み CA 証明書] の順に選択します。Deep Discovery Inspector で TLS トラフィックを復号するには、1 つの有効な信頼済み CA 証明書が必要です。

Deep Discovery Inspector では、次の形式の信頼済み証明書のみがサポートされます。

- PEM
- DER
- PKCS#7

注意

Deep Discovery Inspector のバックアップと復元の操作、および Deep Discovery Director の設定の複製では、信頼済み証明書の設定がサポートされます。

[信頼済み CA 証明書] 画面では、次の操作を実行できます。

操作	説明
追加	新しい証明書を追加します。
削除	選択した証明書を削除します。
インポート	新しい証明書をインポートします。

操作	説明
すべてエクスポート	すべての証明書をエクスポートします。
表示更新	証明書のリストを更新します。
サブジェクトの検索	証明書のサブジェクトに基づいてリストを検索します。

署名証明書

TLS トラフィックインスペクションが有効な場合、クライアントは Deep Discovery Inspector 経由でサーバに接続されます。クライアントで Deep Discovery Inspector を信頼するには、署名証明書をインポートする必要があります。

Deep Discovery Inspector が TLS トラフィックの復号に使用する署名証明書を管理するには、[管理] > [監視/検索] > [TLS トラフィックインスペクション] > [証明書の管理] > [署名証明書] の順に選択します。

重要

Deep Discovery Inspector のバックアップと復元の操作、および Deep Discovery Director の設定の複製では、署名証明書の設定はサポートされません。

署名証明書を設定するには、次のいずれかの操作を行います。

- Deep Discovery Inspector からダウンロードした証明書を直接インポートする
  1. [証明書のダウンロード] をクリックして、Deep Discovery Inspector の自己生成証明書をダウンロードします。
  2. 証明書をクライアントにインポートします。
- 証明書署名要求 (CSR) を使用する
  1. [CSR の生成] をクリックし、署名証明書を生成してダウンロードします。
  2. ユーザの秘密鍵と証明書を使用して CSR に署名し、署名証明書を生成します。

3. [証明書をインポートして置換] をクリックして、生成した署名証明書を Deep Discovery Inspector にインポートします。
4. クライアントで、CSR の署名に使用したユーザの証明書をインポートします。

秘密鍵と署名証明書を置換ではなく削除するには、アプライアンスを初期設定にリセットする必要があります。詳細については、366 ページの「初期設定の復元」を参照してください。

復号ポリシー

[管理] > [監視/検索] > [TLS トラフィックインスペクション] > [復号ポリシー] の順に選択し、復号するトラフィックおよび復号から除外するトラフィックを指定します。

[復号ポリシー] 画面では次の操作を実行できます。

セクション	復号または除外	操作または設定	説明
すべて	すべて	ポリシーのインポート	ポリシーをインポートします。
すべて	すべて	ポリシーのエクスポート	ポリシーをエクスポートして、バックアップを作成するか別のアプライアンスで使用します。
すべて	すべて	保存	現在のポリシー設定を保存します。
クライアントの IP アドレス	復号する	追加	復号するクライアント IP アドレスを追加します。
クライアントの IP アドレス	復号する	インポート	復号するクライアント IP アドレスをインポートします。
クライアントの IP アドレス	復号する	すべてエクスポート	復号リスト内のすべてのクライアント IP アドレスをエクスポートします。

セクション	復号または除外	操作または設定	説明
クライアントの IP アドレス	復号する	削除	選択したクライアント IP アドレスを復号リストから削除します。
クライアントの IP アドレス	復号する	IP または説明の検索	復号リスト内の指定したクライアント IP アドレスまたは説明を検索します。
クライアントの IP アドレス	除外	追加	除外するクライアント IP アドレスを追加します。
クライアントの IP アドレス	除外	インポート	除外するクライアント IP アドレスをインポートします。
クライアントの IP アドレス	除外	すべてエクスポート	除外対象のすべてのクライアント IP アドレスをエクスポートします。
クライアントの IP アドレス	除外	削除	選択したクライアント IP アドレスを除外から削除します。
クライアントの IP アドレス	除外	IP または説明の検索	除外対象の指定したクライアント IP アドレスまたは説明を検索します。
サーバポート	復号する	• 任意 • カスタム	任意のサーバポートへの接続を復号するには [任意] を選択し、特定のサーバポートへの接続を復号するには [カスタム] を選択してポートを指定します。

セクション	復号または除外	操作または設定	説明
サーバドメインカテゴリ **注意** Smart Protection Server を使用する際、[サーバドメインカテゴリ] は無効になっています。詳細については、197 ページの「Web レピュテーションの設定」を参照してください。	• 復号する • 復号しない	• 任意 • なし • カスタム	復号するまたは復号しないサーバドメインカテゴリを選択します。
ドメインオブジェクト	復号する	任意	ドメインへの任意の接続を復号する場合に選択します。
ドメインオブジェクト	復号する	なし	ドメインに基づいていずれの接続も復号しない場合に選択します。

セクション	復号または除外	操作または設定	説明
ドメインオブジェクト	復号する	カスタム	ドメインに基づいて復号する接続を指定する場合に選択します。 次の操作を行えます。 • [追加] を選択して、ドメイン名または IP アドレスを追加する • [削除] を選択して、指定したドメインをリストから削除する • [インポート] を選択して、ドメインの IP アドレスとドメイン名のリストをインポートする • [すべてエクスポート] を選択して、リスト内のすべてのドメインをエクスポートする • [ドメインの検索] を選択して、リスト内のドメインを検索する
ドメインオブジェクト	除外	追加	ドメイン名または IP アドレスを追加します。
ドメインオブジェクト	除外	削除	選択したドメインをリストから削除します。

セクション	復号または除外	操作または設定	説明
ドメインオブジェクト	除外	インポート	ドメインの IP アドレスとドメイン名のリストをインポートします。
ドメインオブジェクト	除外	すべてエクスポート	リスト内のすべてのドメインをエクスポートします。
ドメインオブジェクト	除外	ドメインの検索	リスト内のドメインを検索します。

仮想アナライザ

仮想アナライザは、ネットワークを危険にさらすことなくサンプルを管理および分析するための隔離された仮想環境を提供します。システムイメージを使用してサンプルの動作や特徴を監視し、そのサンプルにリスクレベルを割り当てます。

Deep Discovery Inspector は、他の Trend Micro 製品に組み込まれたものも含め、内部仮想アナライザと外部仮想アナライザの両方を使用できます。

仮想アナライザへのファイルの送信を有効にすると、最大ストレージファイルサイズが 15MB に増大するため、ファイルの破棄を最小限に抑えられます。Deep Discovery Inspector では、サイズが [ファイルサイズの設定] 画面で設定した値を超えるとファイルが破棄されます。

この最大ストレージファイルサイズを変更するには、[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] の順に選択します。

仮想アナライザの種類

重要

[内部仮想アナライザ] および [Sandbox as a Service] を利用できるかどうかは、お使いのモデルとライセンスによって異なります。

次の表に、Deep Discovery Inspector がファイルを送信できる仮想アナライザの種類を示します。

種類	説明
内部	Deep Discovery Inspector に組み込まれている仮想アナライザ。
外部	他の Trend Micro 製品の仮想アナライザ。 サポートされる外部仮想アナライザ製品の詳細については、266 ページの「トレンドマイクロの統合製品とサービス」を参照してください。
Sandbox as a Service	Trend Micro が提供するクラウドベースのサンドボックスサービス
Trend Vision One — Sandbox Analysis	Trend Vision One で提供されるサンドボックスサービス。 Sandbox Analysis の詳細については、Trend Vision One のオンラインヘルプを参照してください。https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-sandbox-analysis

内部仮想アナライザの設定

重要

この種類の仮想アナライザを利用できるかどうかは、お使いの Deep Discovery Inspector モデルとライセンスによって異なります。

手順

1. [管理] > [仮想アナライザ] > [セットアップ] の順に選択します。
2. [仮想アナライザにファイルを送信する] を選択します。
3. [仮想アナライザ] メニューで [内部] を選択します。
4. 選択した仮想アナライザの設定を指定します。
   a. ネットワークの種類を選択します。

      使用可能な脅威データについてトレンドマイクロのクラウドベースサービス (Web レピュテーションサービスなど) にクエリを実行するには、インターネット接続が必要です。ネットワークの種類によって、仮想アナライザのインターネット接続性が決まります。

      次の表に、使用可能なネットワークの種類を示します。

ネットワークの種類	説明
カスタムネットワーク (推奨)	仮想アナライザトラフィック専用のポートを設定します。 外部ネットワークに接続できるポートを指定します。ポートが競合していないことを確認します。 **警告!** カスタムネットワーク内の不正なサンプルが他のネットワーク内のホストに影響を及ぼさないよう、カスタムネットワークは管理ネットワークや他の内部ネットワークから独立している必要があります。
管理ネットワーク	仮想アナライザは、Deep Discovery Inspector 管理ポートを使用してインターネットに接続します。
ネットワークなし	仮想アナライザはインターネットに接続せず、分析エンジンに依存します。

b. 内部仮想アナライザ専用のプロキシを設定します。

プロキシを設定するには、ネットワークの種類に [管理ネットワーク] または [カスタムネットワーク] を選択します。

1. [プロキシ設定] で、[専用のプロキシ設定を使用する] を選択します。
2. [サーバアドレス] で、プロキシサーバの IP アドレス、ホスト名、または完全修飾ドメイン名を入力します。

   仮想アナライザでは、HTTP プロキシサーバおよび HTTPS プロキシサーバがサポートされます。
3. ポート番号を入力します。
4. プロキシで認証が必要な場合は、プロキシサーバの認証資格情報を入力します。

c. [接続のテスト] をクリックします。

5. [保存] をクリックします。

6. 内部仮想アナライザがインターネットに接続できることを確認するには、[インターネット接続のテスト] をクリックします。

ヒント

設定を変更するたびにインターネット接続をテストすることをお勧めします。

7. macOS に影響を及ぼす可能性のあるサンプルを分析する場合は、[内部仮想アナライザ] > [macOS 向けサンドボックス] の順に選択し、[macOS の潜在的な脅威を Trend Micro Sandbox as a Service に送信して分析] をオンにします。

外部仮想アナライザの設定

手順

1. [管理] > [仮想アナライザ] > [セットアップ] の順に選択します。
2. [仮想アナライザにファイルを送信する] を選択します。
3. [仮想アナライザ] メニューで [外部] を選択します。
4. 選択した仮想アナライザの設定を指定します。
   a. 外部仮想アナライザの IP アドレスおよびポート番号を入力します。
   b. 外部仮想アナライザから API キーを入力します。
      外部仮想アナライザから API キーを取得できます。
   c. [接続のテスト] をクリックします。
5. [保存] をクリックします。

Sandbox as a Service の設定

重要

この種類の仮想アナライザを利用できるかどうかは、お使いの Deep Discovery Inspector モデルとライセンスによって異なります。

手順

1. [管理] > [仮想アナライザ] > [セットアップ] の順に選択します。
2. [仮想アナライザにファイルを送信する] を選択します。
3. [仮想アナライザ] メニューで [Sandbox as a Service] を選択します。
4. 初期設定では、[Sandbox as a Service] を選択するとプロキシ設定が有効になります。プロキシを設定していない場合でも、Deep Discovery Inspector は Sandbox as a Service に接続します。
   a. [接続のテスト] をクリックします。
5. [保存] をクリックします。

Trend Vision One — Sandbox Analysis の設定

重要

- 次の手順は、2024 年 11 月現在のものです。詳細については、Trend Vision One のドキュメントを参照してください。
- [サンドボックスに送信] は有料の機能であり、有効にするにはクレジットを割り当てる必要があります。

手順

1. Deep Discovery Inspector アプライアンスを Trend Vision One に接続します。

   詳細については、267 ページの「Trend Vision One」を参照してください。

2. Trend Vision One コンソールで、[Network Security] > [Network Inventory] > [Deep Discovery Inspector] の順に選択します。
3. サポートされているアプライアンスで [サンドボックスに送信] を設定します。
   a. サポートされている Deep Discovery Inspector アプライアンスを 1 つ以上選択します。
   b. [サンドボックスの設定] > [サンドボックスに送信をオンにする] の順にクリックします。
   c. クレジットの要件を確認して、[有効にする] をクリックします。

Trend Vision One は、Sandbox Analysis を仮想アナライザとして使用するように Deep Discovery Inspector アプライアンスを設定します。

重要

[サンドボックスに送信] が有効になっている場合:

- [管理] > [仮想アナライザ] > [セットアップ] で仮想アナライザを選択できません。
- [管理] > [仮想アナライザ] > [セットアップ] の [プロキシ設定] が自動的に有効化されます。

ファイル送信

仮想アナライザキュー内のファイルの数を削減するために、ソフトウェア安全性評価サービス (CSSS) を有効にし、ファイル送信ルールを設定します。

Deep Discovery Inspector は、次の設定に基づいてファイルを送信します。

- 送信の一般設定: 初期設定では、仮想アナライザにファイルを送信する前に、Deep Discovery Inspector が CSSS に照合してファイルを確認します。
- ファイル送信ルール: Deep Discovery Inspector は、設定されたルール条件に従って、仮想アナライザに送信されたすべてのファイルを確認します。

ソフトウェア安全性評価サービス

Certified Safe Software Service (CSSS) は、安全なファイルをまとめたトレンドマイクロのクラウドデータベースです。Deep Discovery Inspector は、トレンドマイクロのデータセンターに対してクエリを実行して、送信されたファイルをデータベースと照合して確認します。

CSSS を有効にすると、安全なファイルが仮想アナライザキューに送信されることが防止されます。次のような利点があります。

- 計算時間とリソースの節約
- 誤検出数の減少

ヒント

ソフトウェア安全評価サービスは、初期設定で有効になっています。初期設定の値を使用することをお勧めします。

ファイル送信ルール

Deep Discovery Inspector を使用して、仮想アナライザキューのファイル数を削減するファイル送信ルールを作成できます。不審ファイルのみが分析されるようにするために、ファイル送信ルールは検出タイプ、検出ルール、およびファイルプロパティに基づいてファイルを確認します。

ファイル送信ルールには、次の要素が含まれます。

- ステータス: [有効] または [無効]
- 優先度: リスト全体の中のルールの位置
- 条件: 指定された処理が実行される前に、ファイルが満たしている必要がある条件のセット
- 処理: [ファイルを送信する] または [ファイルを送信しない]

Deep Discovery Inspector は、一致するまで、リスト内の各ルールに対してファイルを照合します。ルールを追加しない場合、Deep Discovery Inspector は次のデフォルトルールを使用します。

表 6-10. 初期設定の送信ルールの要素

ルールの種類	条件	処理
基本	不正なコンテンツ	ファイルを送信しない
基本	検出の種類なし AND CHM / JAR / JAVA Applet / LNK / Mach-O / WIN_EXE	ファイルを送信する
基本	検出の種類なし AND HTTP AND *.vbs / *.vbe / *.ps1 / *.hta / *.wsf	ファイルを送信する
基本	検出の種類なし AND SMTP AND *.vbs / *.vbe / *.ps1 / *.hta / *.wsf / *.js / *.jse / *.bat / *.cmd / *.html / *.htm	ファイルを送信する
基本	検出の種類なし AND SMTP AND SWF	ファイルを送信する
詳細	ルール 28/29/40/52	ファイルを送信しない
基本	ヒューリスティック検出/極めて不審なファイル	ファイルを送信する

ファイル送信ルールの種類と条件

Deep Discovery Inspector には、2 種類のファイル送信ルールがあります。ルールの種類ごとに特定の条件セットが必要です。

- 基本: 検出タイプとその他のプロパティに基づいてファイルを確認します。
- 詳細: 検出ルールとその他のプロパティに基づいてファイルを確認します。

基本または詳細のファイル送信ルールの作成時には、次のオプションの条件を選択します。

1. プロトコル
    - Common Internet File System (CIFS)
    - File Transfer Protocol (FTP)

- Hypertext Transfer Protocol (HTTP)
- Instant Messaging (IM)
- Internet Message Access Protocol (IMAP)
- Post Office Protocol 3 (POP3)
- Simple Mail Transfer Protocol (SMTP)

2. ファイルの種類

オプション	ファイルの種類	ファイル拡張子の例
7zip	7-zip アーカイブ	.7z
ALZ	ALZip 圧縮ファイル	.alz
BZIP2	BZIP2 アーカイブ	.bz2
CHM	コンパイル済み HTML (CHM) ヘルプファイル	.chm
EGG	ALZip アーカイブファイル	.egg
ELF	Executable and Linkable Format バイナリファイル	.elf
JAR	Java アーカイブ	.jar
Java Applet	Java クラスファイル	.class
LNK	Microsoft Windows Shell Binary Link ショートカット Microsoft Windows 95/NT ショートカット	.lnk
Mach-O	Mach-O x86/x64	ほとんどの実行可能ファイルに拡張子なし
Mac OS X Installer Package	Mac OS X インストーラパッケージ	.pkg

オプション	ファイルの種類	ファイル拡張子の例
OFFICE	Microsoft Office ファイル	.doc .docx .ppt .pptx .xls .xlsx
OpenDocument	OpenDocument ファイル	.odt .odp .ods
PDF	Adobe Portable Document Format (PDF)	.pdf
RAR	RAR アーカイブ	.rar
SWF	Adobe Shockwave Flash ファイル	.swf
TAR	TAR アーカイブ	.tar
WIN_EXE	Windows 実行可能ファイル	.exe
ZIP	PKWARE PKZIP アーカイブ (ZIP)	.zip

注意

Mac OS X インストーラパッケージをサブミットするには、[ファイルの種類] オプションで [Mac OS X Installer Package] を選択し、[ファイル拡張子] オプションで `pkg` を指定する必要があります。

3. ファイル拡張子

   ファイル拡張子を 1 つ以上入力します。エントリを複数入力する場合は、カンマ (,) で区切ってください。

4. ファイルサイズ

[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] で指定した最大ファイルサイズ以下の値を入力します。

5. 方向
   - 内部ホスト: 監視対象ネットワーク内のホスト
   - 外部ホスト: ネットワーク外部のホスト
6. 送信元/送信先 IP
   - すべて
   - 指定の IP アドレス
   - 監視対象ネットワークグループからの IP アドレス
7. URL

   URL を 20 件まで入力します。エントリを複数入力する場合は、カンマ (,) で区切ってください。

   構文: [http://]<Domain>[:<Port>][/<URI-prefix>]

   - [http://]

     許可して無視されます。

   - <Domain>

     ワイルドカード (*) は、プレフィックスでのみ使用できます。ワイルドカードがプレフィックスで使用されている場合は、「.」で接続する必要があります。1 つのドメインで 1 つのワイルドカードのみを使用できます。

   - [:<Port>]

     (オプション) 割り当てられていない場合、初期設定は「:80」 (ポート 80) です。

     特定のポートに 1～65,535 の整数を割り当てるか、ワイルドカード (*) を使用してすべてのポートに割り当てます。

   - [/<URI-prefix>]

     (オプション) 割り当てられていない場合、初期設定は、すべてのパスに一致するワイルドカードです。

パスのない URL に一致させるには、「/」と「/*」を使用します。

例: `www.abc.com/*`は、`www.abc.com` に一致します。

[/<URI-prefix>] は、常にプレフィックスマッチングとして適用されます。1 つのプレフィックスで 1 つのワイルドカードのみを使用できます。

URI マッチングでは大文字小文字は区別されません。

ヒント

URL の条件を追加する場合は、[プロトコル] にも新しい条件を追加することをお勧めします。たとえば、[HTTP] やメールに関するプロトコルを追加します。

ファイル送信ルール画面

[ファイル送信ルール] 画面で次の処理を実行できます。

- 追加: 最大 1,000 件ルールを追加できます。
- インポート: Deep Discovery Inspector アプライアンスからエクスポートされたルールをインポートします。

注意

インポートすると既存のすべてのルールが置き換えられます。インポートする前に既存のすべてのルールのバックアップを作成することをお勧めします。

- エクスポート: バックアップするために、またはその他の Deep Discovery Inspector アプライアンスにインポートするためにルールをエクスポートします。

注意

Deep Discovery Inspector はルールを.dat ファイルにエクスポートします。

- リセット: すべてのユーザ定義ルールを削除し、デフォルトルールを保持します。
- 編集: ルールを有効または無効にしたり、ルールコンポーネントを編集したりします。

ファイル送信ルールの追加

Deep Discovery Inspector は最大 1,000 件のルールをサポートします。

手順

1. [管理] > [仮想アナライザ] > [ファイル送信] の順に選択します。
2. [ファイル送信ルール] の [追加] をクリックします。

   [新規送信ルール] 画面が表示されます。
3. [送信ルールを有効にする] を選択します。
4. [条件] で、次のいずれかを選択します。
   - 基本: 検出タイプとその他のプロパティに基づいてファイルを確認します。
   - 詳細: 検出ルールとその他のプロパティに基づいてファイルを確認します。
5. (オプション) [基本] を選択した場合は、次の検出タイプも 1 つ以上選択します。
   - 検出ルールに一致しない: Deep Discovery Inspector の検出ルールをトリガしないファイル

     注意

     特定の条件を満たすが、検出数のないファイルを検索する場合は、このオプションを選択します。
   - 次のいずれか:

注意

検出の種類を少なくとも 1 つ選択してください。

- 不正なコンテンツ: シグネチャベースの方法によって検出された不正ファイル
- ヒューリスティック検出: ヒューリスティック分析によって検出された不審ファイル
- 極めて不審なファイル: 検出ルールによって検出された、極めて不審な動作を示すファイル

6. (オプション) [詳細] を選択した場合は、[選択] をクリックして検出ルールを 1 つ以上選択します。

   Deep Discovery Inspector の検出ルールの詳細については、[管理] > [監視/検索] > [検出ルール] の順に選択して確認してください。

7. (オプション) [新規条件] をクリックします。
8. 次の条件のいずれかを選択して、適切な設定を行います。
   - プロトコル: プロトコルを 1 つ以上選択します。
   - ファイルの種類: 検出の種類を 1 つ以上選択します。
   - ファイル拡張子: ファイル拡張子を 1 つ以上入力します。エントリを複数入力する場合は、カンマ (,) で区切ってください。
   - ファイルサイズ: [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] で指定した最大ファイルサイズ以下の値を入力します。
   - 方向:
     - 内部ホスト
     - 外部ホスト
   - 送信元/送信先 IP: 送信元と送信先の両方について、[選択] をクリックし、次のいずれかを選択します。
     - すべて

- 指定の IP アドレス
- 監視対象ネットワークグループから選択します。

- URL: URL を 20 件まで入力します。エントリを複数入力する場合は、カンマ (,) で区切ってください。

ヒント

URL の条件を追加する場合は、[プロトコル] にも新しい条件を追加することをお勧めします。たとえば、[HTTP] やメールに関するプロトコルを追加します。

9. ファイルが設定された条件を満たす場合に、Deep Discovery Inspector が実行する処理を選択します。
10. ルールの優先度を指定します。1 からルールの合計数までの数値を入力します。
11. [追加] をクリックします。

内部仮想アナライザ

一部の Deep Discovery Inspector モデルは、いつでも有効にできる内部仮想アナライザを搭載しています。

Deep Discovery Inspector を使用する前に、イメージをインポートして内部仮想アナライザを設定します。

注意

外部仮想アナライザまたは Sandbox as a Service には、[内部仮想アナライザ] の設定は適用されません。外部分析モジュールの詳細については、適用可能な製品の管理者ガイドを参照してください。

[内部仮想アナライザ] には次の画面があります。

- サンドボックス管理
- YARA ルール

サンドボックス管理

[サンドボックス管理] 画面には次のタブがあります。

- ステータス
- イメージ
- パスワード
- macOS 向けサンドボックス

注意

外部仮想アナライザまたは Sandbox as a Service には、[サンドボックス管理] の設定は適用されません。外部分析モジュールの詳細については、適用可能な製品の管理者ガイドを参照してください。

仮想アナライザのステータス

[ステータス] タブは、次の情報を提供します。

1. 仮想アナライザの現在の全体的なステータス
   - 初期化しています...
   - 開始しています...
   - 設定しています...
   - イメージをインポートしています...
   - 停止しています...
   - 中止されました
   - 実行中
   - アクティブなイメージがありません
   - 無効
2. 配信されたインスタンス数、状態 (アイドルまたはビジー)、使用率情報を含む各イメージのステータス

仮想アナライザイメージ

初期設定では仮想アナライザにイメージは含まれていません。仮想アナライザでサンプルを分析できるようにするには、イメージを準備してアップロードする必要があります。

仮想アナライザでファイルを分析できるようにするには、1〜30GB までのカスタム OVA ファイルをインポートします。

Deep Discovery Inspector は最大 2 件のイメージをサポートします。Deep Discovery Inspector アプライアンスのハードウェア仕様に応じて、配置可能なインスタンスの合計数が決まります。

Image Preparation Tool

初期設定では、仮想アナライザにイメージは含まれていません。サンプルを分析するには、少なくとも 1 つのイメージを OVA (Open Virtual Appliance) 形式で準備してアップロードする必要があります。

既存の VirtualBox または VMware イメージを使用するか、VirtualBox を使用して新しいイメージを作成できます。詳細については、「Virtual Analyzer Image Preparation Tool ユーザガイド」 (https://appweb.trendmicro.com/ecs/default.aspx) の第 2 章と第 3 章を参照してください。

アップロードする前に、Virtual Analyzer Image Preparation Tool を使用してイメージを検証および設定します。詳細については、「Virtual Analyzer Image Preparation Tool ユーザガイド」の第 4 章を参照してください。

ご使用の製品のハードウェア仕様に応じて、アップロード可能なイメージ数、およびイメージごとに配信可能なインスタンス数が決まります。

イメージをインポートする

イメージがインポートまたは削除された場合、またはインスタンスが変更された場合、Deep Discovery Inspector はすべての分析を停止して、すべてのサンプルを仮想アナライザキューに保持します。イメージがインポートされた場合は、すべてのインスタンスが自動的に再配置されます。

注意

Windows OS およびその他の Microsoft 製品は、Microsoft および Microsoft チャネルパートナーとは別途利用可能です。

重要

トレンドマイクロでは、Deep Discovery Inspector 内で作成する仮想アプライアンスまたはサンドボックス上でのインストールに必要な Microsoft Windows OS またはサードパーティ製品は提供しません。OS およびその他のアプリケーションのインストールメディア、またサンドボックスを作成するのに必要な適切なライセンス権限をお客様にて準備する必要があります。

手順

1. [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [サンドボックス管理] > [イメージ] の順に選択します。
2. [インポート] をクリックします。

   [イメージのインポート] 画面が表示されます。
3. 次のイメージソースのいずれかを選択して、適切な設定を行います。

送信元	手順
ローカルまたはネットワークフォルダ	a. 最大 260 文字でイメージの名前を入力します。 注意 Trend Micro Cloud Sandbox という名前は予約されているため使用できません。 b. [接続] をクリックします。 c. 接続されたら、トレンドマイクロ仮想アナライザイメージアップロードツールを使用してイメージをアップロードします。 詳細については、247 ページの「トレンドマイクロ仮想アナライザイメージアップロードツールを使用してイメージをアップロードする」を参照してください。 注意 イメージのアップロードおよびインポート後、Deep Discovery Inspector がただちにインスタンスを配信します。配信が完了するまでお待ちください。

送信元	手順
HTTP または FTP サーバ	a. 最大 260 文字でイメージの名前を入力します。 注意 Trend Micro Cloud Sandbox という名前は予約されているため使用できません。 b. HTTP または FTP の URL を入力します。 c. (オプション) 認証が必要な場合はログオン認証情報を入力するか、または [匿名でログオン] を選択します。 注意 [匿名でログオン] は、サーバがこの機能をサポートしている場合のみ選択します。 d. [インポート] をクリックします。

トレンドマイクロ仮想アナライザイメージアップロードツールを使用してイメージをアップロードする

仮想アナライザは 1～30GB までの OVA ファイルをサポートします。

手順

1. インポートする前に、コンピュータと Deep Discovery Inspector の接続が確立されていることを確認します。

   [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [サンドボックス管理] > [ステータス] の順に選択し、接続ステータスを確認します。

2. [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [サンドボックス管理] > [イメージ] の順に選択し、[インポート] をクリックします。
3. [送信元] には、[ローカルまたはネットワークフォルダ] を選択します。
4. Deep Discovery Inspector に接続します。
5. [イメージアップロードツールのダウンロード] をクリックします。

6. ファイル `VirtualAnalyzerImageImportTool.exe` を開きます。
7. Deep Discovery Inspector の IP アドレスを入力します。

   イメージのアップロードおよびインポート後、Deep Discovery Inspector がただちにインスタンスを配信します。インスタンスの配信が完了するまでお待ちください。

イメージのインポートプロセスは、次の理由によって、停止するか失敗と見なされることがあります。

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

インスタンスの変更

イメージがインポートまたは削除された場合、またはインスタンスが変更された場合、Deep Discovery Inspector はすべての分析を停止して、すべてのサンプルを仮想アナライザキューに保持します。イメージがインポートされた場合は、すべてのインスタンスが自動的に再配置されます。

インスタンスの変更

手順

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

   [インスタンスの変更] 画面が表示されます。

3. 各イメージのインスタンス数を指定します。

注意

各イメージにはインスタンスが少なくとも 1 つ必要です。

4. [保存] をクリックします。

インスタンスの削除

手順

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

   [インスタンスの変更] 画面が表示されます。
3. インスタンスを削除するには、イメージのインスタンス数の左にあるマイナス記号のアイコンをクリックします。

注意

各イメージにはインスタンスが少なくとも 1 つ必要です。

4. [保存] をクリックします。

アーカイブのパスワード

不審ファイルは常に注意して扱う必要があります。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に追加することをお勧めします。

仮想アナライザはユーザ指定のパスワードを使用して、アーカイブファイルからファイルを抽出します。

この機能を使用するには、次の条件で基本ファイル送信ルールを追加し、有効にします。

- 検出の種類: 検出数のないファイル

- ファイルの種類: リストされたパスワードで復号される選択可能なファイルの種類

詳細については、240 ページの「ファイル送信ルールの追加」を参照してください。

指定されたいずれのパスワードを使用しても暗号化されたファイルを抽出できない場合は、「Unsupported file type」(ファイルタイプがサポートされていません) というステータスが表示され、アーカイブファイルがキューから削除されます。

注意

パスワードは、最初の暗号化レイヤでのみ使用できます。SMTP 添付ファイルの復号はサポートされていません。

Deep Discovery Inspector は、アーカイブファイルのパスワードを暗号化なしのテキストとして保存します。

アーカイブのパスワードの追加

Deep Discovery Inspector は最大 5 件のパスワードをサポートします。

この機能を使用するには、次の条件で基本ファイル送信ルールを追加し、有効にします。

- 検出の種類: 検出数のないファイル
- ファイルの種類: リストされたパスワードで復号される選択可能なファイルの種類

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最初にリストします。

手順

1. [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [サンドボックス管理] > [パスワード] の順に選択します。
2. [アーカイブファイルのパスワード] でパスワードを入力します。
3. (オプション) [パスワードの追加...] をクリックして、別のパスワードを入力します。

4. [保存] をクリックします。

macOS 向けサンドボックス

macOS 向けサンドボックス設定を有効にすると、Deep Discovery Inspector は macOS の潜在的な脅威を Sandbox as a Service に送信して分析します。

macOS 向けサンドボックスを有効にするには、[管理] > [仮想アナライザ] > [内部仮想アナライザ] > [サンドボックス管理] > [macOS 向けサンドボックス] の順に選択し、[macOS の潜在的な脅威を Snadbox as a Service に送信して分析] を有効にします。

[ネットワークサービス診断] 画面で、サービスの接続を確認します。詳細については、383 ページの「ネットワークサービスに接続できない」を参照してください。

重要

Deep Discovery Inspector のアクティベーションコードを置き換えると、macOS 向けサンドボックスは自動的に無効になります。Deep Discovery Inspector のアクティベーションコードを置き換えたら、macOS 向けサンドボックスを再度有効にしてください。

YARA ルール

重要

- Deep Discovery Inspector を Deep Discovery Director に登録すると、Deep Discovery Inspector は自動的に YARA ルールの設定を Deep Discovery Director から同期し、既存の YARA ルールの設定を上書きします。
- [YARA ルール] のすべての設定は、内部仮想アナライザに送信されたオブジェクトにのみ適用されます。

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 Inspector では、YARA ルールを使用して不正プログラムを特定します。

Deep Discovery Inspector では、YARA ルールファイルの数に関係なく、最大 5,000 の有効な YARA ルールがサポートされます。YARA ルールの表の右上隅にある [使用中のルール] フィールドには、システムで現在有効な YARA ルールの数が表示されます。

Deep Discovery Director と統合されている場合、すべての YARA ルールは Deep Discovery Director で集中管理されるため、ユーザは YARA ルールを Deep Discovery Director 管理コンソールで管理する必要があります。詳細については、「Deep Discovery Director 管理者ガイド」を参照してください。

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。

フィールド	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。
分析対象のファイル	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。
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。

YARA ルールファイルの作成

Deep Discovery Inspector では、バージョン 4.1.0 の公式な仕様に準拠する YARA ルールファイルをサポートしています。YARA ルールは、任意のテキストエディタを使用して作成可能なプレーンテキストファイルに保存されます。

YARA ルールの記述の詳細については、次のサイトを参照してください。

https://yara.readthedocs.io/en/v4.1.0/writingrules.html

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

- ファイル名が一意であること
- ファイルコンテンツが空でないこと

次の例は単純な YARA ルールを示しています。

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

次の表に、YARA ルールを構成する各要素とその使用方法を示します。

表 6-11. YARA ルールの構成要素と使用方法

要素	使用方法
rule	YARA ルールの名前です。一意である必要があり、スペースを含めることはできません。
meta:	「メタ」セクションの開始位置を示します。メタセクション内の要素は検出に影響しません。
desc	ルールについて説明するオプションの要素です。
weight	ルールの条件が一致した場合にリスクレベルを判断するオプションの要素です。1〜10 で指定する必要があります。 • 1〜9 = リスク低 • 10 = リスク高 注意 weight の値は、Deep Discovery Inspector によって割り当てられるリスクレベルに対応しません。
strings:	「文字列」セクションの開始位置を示します。文字列は、不正プログラムを検出するための主要な手段です。

要素	使用方法
$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 ルールファイルの追加

Deep Discovery Director 5.0 以降と統合されている場合、すべての YARA ルールは Deep Discovery Director で集中管理されるため、ユーザは YARA ルールを Deep Discovery Director 管理コンソールで管理する必要があります。詳細については、「Deep Discovery Director 管理者ガイド」を参照してください。

手順

1. [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [YARA ルール] の順に選択します。
2. [追加] をクリックして YARA ルールファイルを追加します。

   [YARA ルールファイルの追加] 画面が表示されます。
3. 表示された新しい画面で、次の設定を行います。
   a. ルールファイル: 追加する YARA ルールファイルを参照して選択します。
   b. 分析対象のファイル: この YARA ルールファイルに固有の、仮想アナライザで処理するファイルタイプを選択します。

注意

すべてのファイルタイプを分析すると、意図しない検出が行われる可能性があります。YARA ルールファイルの対象となる特定のファイルタイプの分析を行うことをお勧めします。

4. 追加する YARA ルールファイルと分析対象のファイルタイプを選択したら、[追加] をクリックします。

   追加する前に仮想アナライザで YARA ルールファイルが検証されます。

YARA ルールファイルの編集

手順

1. [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [YARA ルール] の順に選択します。
2. 編集する YARA ルールファイルの名前をクリックします。

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

YARA ルールファイルの削除

手順

1. [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [YARA ルール] の順に選択します。
2. 削除する YARA ルールファイルを 1 つ以上選択します。
3. [削除] をクリックします。

YARA ルールファイルのエクスポート

手順

1. [管理] > [仮想アナライザ] > [内部仮想アナライザ] > [YARA ルール] の順に選択します。
2. エクスポートする YARA ルールファイルを選択します。

   注意
   一度にエクスポートできる YARA ルールファイルは 1 つのみです。

3. [ファイルのエクスポート] をクリックします。

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とエンドポイント] には、ネットワークグループ、登録済みドメイン、および登録済みサービスが含まれます。

Deep Discovery Inspector がネットワークコンテンツ相関分析エンジン用に監視するネットワークのプロファイルは、ネットワーク設定によって定義および確立されます。

詳細については、次の項目を参照してください。

- 257 ページの「ネットワークグループの追加」
- 259 ページの「登録済みドメインの追加」
- 261 ページの「登録済みサービスの追加」
- 264 ページの「Trend Vision One からのネットワークグループとエンドポイントの同期」
- 265 ページの「設定のインポート/エクスポート」

注意

Deep Discovery Director でネットワークグループとエンドポイントを管理している場合、Deep Discovery Inspector ではその設定が無効になります。Deep Discovery Director 管理コンソールに移動して、ネットワークグループとエンドポイントを設定してください。Deep Discovery Director では初期設定で [登録済み製品に同期] が無効になっており、ネットワークグループとエンドポイントは Deep Discovery Inspector に同期されません。

Deep Discovery Director で [登録済み製品に同期] が有効な場合、ネットワークグループとエンドポイントは Deep Discovery Inspector に同期されます。Deep Discovery Director で [登録済み製品に同期] が無効な場合、ネットワークグループとエンドポイントは Deep Discovery Inspector に同期されません。

ネットワークグループの追加

攻撃がネットワークの内部、外部のどちらから来たのかを Deep Discovery Inspector が判断できるようにするには、IP アドレスを使用して、監視対象となるネットワークのグループを作成します。

注意

Deep Discovery Director でネットワークグループとエンドポイントを管理している場合、Deep Discovery Inspector ではその設定が無効になります。Deep Discovery Director 管理コンソールに移動して、ネットワークグループとエンドポイントを設定してください。

手順

1. [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] > [監視対象ネットワークグループ] の順に選択します。
2. [追加] をクリックします。

   [ネットワークグループ] 画面が表示されます。
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. テキストボックスに IP アドレスの範囲 (最高 1,000 個の IP アドレス範囲) を入力します。

注意

IP アドレスの範囲には、クラス D またはクラス E のアドレス (224.0.0.0-255.255.255.255) を含めることはできません。

Deep Discovery Inspector には、初期設定のネットワークグループが用意されています。このネットワークグループには、プライベートネットワークについて、Internet Assigned Numbers Authority (IANA) により予約されている次の IP アドレスブロックが含まれます。

- IPv4: `10.0.0.0 - 10.255.255.255`
- IPv4: `172.16.0.0 - 172.31.255.255`
- IPv4: `192.168.0.0 - 192.168.255.255`
- IPv6: `fe80::-febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff`
- IPv6: `fc00::-fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`
- IPv6: `fec0::-feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`

ヒント

新しいネットワークグループは、[初期設定] ネットワークグループを編集して作成します。

a. [初期設定] をクリックして編集し、新しいネットワークグループを追加します。

b. 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`

c. 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`

注意

最大 3 件のサブグループのレイヤを追加できます。

5. [ネットワークゾーン] を選択します。

注意

[信頼する] はセキュリティで保護されたネットワークであることを意味し、[信頼できない] はセキュリティがある程度不審なネットワークであることを意味します。

6. [追加] をクリックします。
7. [保存] をクリックします。

登録済みドメインの追加

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。

ネットワークプロファイルの正確性を維持するために、10000 件までの信頼されたドメインのみを追加します。

Deep Discovery Inspector では、登録済みドメインのサフィックスマッチングがサポートされます。たとえば、`domain.com` を追加すると、`one.domain.com` と `two.domain.com` も追加されます。

注意

Deep Discovery Director でネットワークグループとエンドポイントを管理している場合、Deep Discovery Inspector ではその設定が無効になります。Deep Discovery Director 管理コンソールに移動して、ネットワークグループとエンドポイントを設定してください。

手順

1. [管理] > [ネットワークグループとエンドポイント] > [登録済みドメイン] の順に選択します。
2. (オプション) 追加する登録済みドメインを指定します。
   a. [追加] をクリックします。

      [登録済みドメインの追加] 画面が表示されます。
   b. [ドメイン] にドメインを 1 つ以上入力します。複数入力する場合はスペースで区切ります。
   c. (オプション) [説明] にドメインの説明を入力します。

      説明は 256 文字以内で入力できます。
3. (オプション) 検出を分析して、追加する登録済みドメインを選択します。
   a. [分析] をクリックします。

      検出が分析されます。分析後、検出されたネットワーク上のサービスとドメインのリストが表示されます。
   b. 追加する各項目のチェックボックスをオンにします。
   c. (オプション) [説明] 列に、選択した各項目の説明を入力します。
   d. [保存] をクリックします。
   e. ブラウザでページの表示を更新します。

      ドメインがリストに表示されます。
4. (オプション) ドメインを編集するには、リスト内のドメインをクリックします。

登録済みサービスの追加

社内利用を目的とするサービス、または信頼できると見なされる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されたサービスを指定することで、許可されていないアプリケーションやサービスの検出が可能になります。

信頼されたサービスのみを追加することで、ネットワークプロファイルの正確性が維持されます。

注意

最大 10,000 件の登録済みサービスを追加できます。各サービスに複数の専用サーバ (IP アドレス) を指定できます。

サービスと IP アドレスの組み合わせごとに 1 つのエントリが追加され、合計 10,000 件の登録済みサービスがカウントされます。たとえば、[サービス] に `DNS`、[IP アドレス] に `10.2.1.1` と `10.2.1.2` を指定すると、2 件の登録済みサービスが追加されます。

注意

Deep Discovery Director でネットワークグループとエンドポイントを管理している場合、Deep Discovery Inspector ではその設定が無効になります。Deep Discovery Director 管理コンソールに移動して、ネットワークグループとエンドポイントを設定してください。

手順

1. [管理] > [ネットワークグループとエンドポイント] > [登録済みサービス] の順に選択します。
2. (オプション) 追加する登録済みサービスを指定します。
   a. [追加] をクリックします。

      [登録済みサービスの追加] 画面が表示されます。

   b. [サービス] でサービスを 1 つ以上選択します。

表 6-12. サービスの種類

サービス	ネットワークサーバの説明
Active Directory	ディレクトリサービスを提供し、ユーザアカウントとパスワードを保存します。 ドメインコントローラと同じサーバを設定します。
認証サーバ — Kerberos	Kerberos 認証を提供します。
コンテンツ管理サーバ	コンテンツを管理します。
データベースサーバ	データベースサーバとして使用されます。
DNS	DNS サーバとして使用されます。
ドメインコントローラ	セキュリティ認証要求に応答し、ドメインリソースへのホストのアクセスを許可します。 Active Directory と同じサーバを設定します。
ファイルサーバ	共有ファイルアクセスの場所を提供します。
FTP	FTP サーバとして使用されます。
HTTP プロキシ	HTTP プロキシサーバとして使用されます。
Radius サーバ	Radius 認証サーバとして使用されます。
セキュリティ監査サーバ	脆弱性および安全性の低い設定を検出します。
SMTP	SMTP サーバとして使用されます。
SMTP オープンリレー	SMTP オープンリレーサーバとして使用されます。
ソフトウェアアップデートサーバ	次の目的で使用されます。 • Windows Server Update Services (WSUS) を実行します。 • リモート配信を実行します。

サービス	ネットワークサーバの説明
Web サーバ	Web サーバとして使用されます。

c. [IP アドレス] に IP アドレスを 1 つ以上入力します。複数入力する場合はスペースで区切ります。

[登録済みサービスの追加] 画面では、IPv4 と IPv6 がサポートされます。単一の IP アドレス、IP アドレス範囲、または CIDR 形式で複数の IP アドレスまたは範囲を指定できます。次の例を参照してください。

- 単一の IP アドレス: `10.0.0.5`
- IP アドレス範囲: `10.0.0.0-10.255.255.255`
- CIDR 形式: `10.0.0.0/8`

複数のサービスと IP アドレスを指定する場合、サービスと IP アドレスの組み合わせごとに 1 つの登録済みサービスが追加されます。たとえば、[サービス] に `DNS` と `SMTP`、[IP アドレス] に `10.2.1.1` と `10.2.1.2` を指定すると、次の 4 件の登録済みサービスが追加されます。

- DNS: 10.2.1.1
- DNS: 10.2.1.2
- SMTP: 10.2.1.1
- SMTP: 10.2.1.2

d. (オプション) [説明] にサービスの説明を入力します。

説明は 256 文字以内で入力できます。

3. (オプション) 検出を分析して、追加する登録済みサービスを選択します。

a. [分析] をクリックします。

検出が分析されます。分析後、検出されたネットワーク上のサービスとドメインのリストが表示されます。

b. 追加する各項目のチェックボックスをオンにします。

c. (オプション) [説明] 列に、選択した各項目の説明を入力します。

d. [保存] をクリックします。

e. ブラウザでページの表示を更新します。

サービスがリストに表示されます。

4. (オプション) サービスを編集するには、リスト内の IP アドレスをクリックします。

Trend Vision One からのネットワークグループとエンドポイントの同期

Trend Vision One では、ネットワークエンドポイントを定義して、すべての登録済み Deep Discovery Inspector アプライアンスに同期できます。

手順

1. Trend Vision One コンソールで、[Network Inventory] > [ネットワークリソース] の順に選択します。
2. 利用可能なリストを使用して、ネットワークトポロジを定義します。

重要

Trend Vision One では、次のリストを登録済み Deep Discovery Inspector アプライアンスに同期します。

- 信頼するドメインのリスト
- ネットワークグループのリスト
- 信頼するサービスソースのリスト

3. [すべてを登録済みアプライアンスに同期] をクリックします。

警告!

Trend Vision One からネットワークエンドポイントを同期すると、Deep Discovery Inspector アプライアンスの既存のリストが上書きされます。

設定のインポート/エクスポート

Deep Discovery Inspector アプライアンス (アプライアンス 1) から別のアプライアンス (アプライアンス 2) にネットワーク設定を複製するには、設定をファイルにエクスポートして、そのファイルを複製先のアプライアンスにインポートします。

初期設定のファイル名は `cav.xml` ですが、必要に応じて変更できます。

注意

ネットワーク設定に加えて Deep Discovery Inspector の設定を複製するには、362 ページの「バックアップ/復元」を参照してください。

注意

Deep Discovery Director でネットワークグループとエンドポイントを管理している場合、Deep Discovery Inspector ではそのすべての設定がエクスポートを除いて無効になります。Deep Discovery Director 管理コンソールに移動して、ネットワークグループとエンドポイントを設定してください。

手順

1. アプライアンス 1 で、[管理] > [監視/検索] > [ネットワークグループとエンドポイント] > [インポート/エクスポート] の順に選択します。
2. [設定のエクスポート] で、[エクスポート] をクリックします。

   `cav.xml` ファイルを開くか保存するよう求めるメッセージが表示されます。
3. [保存] をクリックしてファイルの保存先を参照し、もう一度 [保存] をクリックします。

4. アプライアンス 2 で、[管理] > [監視/検索] > [ネットワークグループとエンドポイント] > [インポート/エクスポート] の順に選択します。
5. [設定のエクスポート] で、[エクスポート] をクリックします。

   cav.xml ファイルを開くか保存するよう求めるメッセージが表示されます。
6. [保存] をクリックしてファイルの保存先を参照し、もう一度 [保存] をクリックします。

   これにより、現在のネットワーク設定がバックアップされます。
7. [設定のインポート] で、[参照] をクリックします。
8. cav.xml ファイルを選択し、[開く] をクリックします。
9. [インポート] をクリックします。

注意

インポート中、cav.xml 内の 256 文字を超える説明は切り捨てられます。

統合製品/サービス

Deep Discovery Inspector は、トレンドマイクロの他の製品やサービスと統合されています。

トレンドマイクロの統合製品とサービス

次の表は、Deep Discovery Inspector6.8 に統合されている Trend Micro の製品とサービスを示しています。

注意

Deep Discovery Inspector 40G は、Deep Discovery Director に関連する機能をサポートしていません。

製品/サービス	バージョン
Apex Central	2019 HF6658
Deep Discovery Analyzer	• 7.5 • 7.6
Deep Discovery Director - Network Analytics (日本における本製品のリリースはいたしません。)	5.3
Deep Discovery Director - Network Analytics as a Service	なし
Deep Discovery Director - オンプレミスバージョン	5.3
Service Gateway	なし
Smart Protection Server	3.3 Patch 11
Threat Investigation Center	なし
Trend Micro TXOne OT Defense Console	1.5
Trend Vision One	なし

Trend Vision One

利用可能ないずれかの方法で、Deep Discovery Inspector を Trend Vision One に接続します。

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

次の表は、Deep Discovery Inspector を Trend Vision One に接続するために利用可能な方法を示しています。

方法	説明
直接接続	お使いの Deep Discovery Inspector アプライアンスを、Network Inventory アプリを使用して接続します。 詳細については、268 ページの「Trend Vision One への直接接続」を参照してください。 **注意** Network Analytics as a Service に関連する情報が Network Inventory アプリに表示されます。
Service Gateway をプロキシとして使用	お使いの Deep Discovery Inspector アプライアンスを、Service Gateway をプロキシに使用して接続します。 詳細については、270 ページの「Service Gateway をプロキシとして使用した Trend Vision One への接続」を参照してください。
Deep Discovery Director	Deep Discovery Director を Trend Vision One に接続すると、すべての管理下の Deep Discovery Inspector アプライアンスが自動的に接続されます。 詳細については、Trend Micro Vision One のオンラインヘルプを参照してください。 **重要** Deep Discovery Inspector がすでに Trend Vision One に接続されている場合は、Deep Discovery Director に接続できません。

Trend Vision One への直接接続

Network Inventory アプリを使用して、導入された Deep Discovery Inspector アプライアンスを Trend Vision One に接続します。

Network Inventory では、Deep Discovery Inspector 5.7 Service Pack 3 以降との接続がサポートされます。お使いのアプライアンスで以前のバージョン (5.7 Service Pack 2 から前) を使用している場合は、最新バージョンにアップグレードしてから Network Inventory に接続してください。

重要

次の手順は、2024 年 11 月現在のものです。詳細については、Trend Vision One のドキュメントを参照してください。https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-xdr-help/ConnectingDeployedDDIDirectly

手順

1. Network Analytics as a Service を使用する場合は、Deep Discovery Director - Network Analytics から切断します。
2. Trend Vision One コンソールで、Network Security Operations > Network Inventory > [Deep Discovery Inspector Appliances] の順に選択します。
3. [アプライアンスを接続] をクリックします。
4. [製品] で [Deployed Deep Discovery Inspector] を選択します。
5. [6.7 以降]を選択します。
6. 接続方法のリストから、[直接接続] を選択します。
7. Deep Discovery Inspector アプライアンスの IP アドレスまたは完全修飾ドメイン名を指定します。

   アクセスできるのは、企業ネットワーク内のアプライアンスまたは直接接続できるアプライアンスのみです。
8. [Go] をクリックします。

   Deep Discovery Inspector アプライアンスのコンソールが表示されます。
9. Deep Discovery Inspector コンソールで、管理者アカウントを使用してサインインします。
10. (オプション) パスワードを変更します。
11. [Trend Micro Vision One に登録します] ダイアログで、[続行] をクリックして処理を確認します。
12. Trend Vision One コンソールで、Network Security Operations > Network Inventory > [Deep Discovery Inspector Appliances] の順に選択して、接続ステータスを確認します。

注意

Deep Discovery Inspector が Trend Vision One に接続すると、Deep Discovery Inspector によって「Trend Vision One 管理者」および「Trend Vision One 閲覧者」アカウントが自動的に作成されます。

Service Gateway をプロキシとして使用した Trend Vision One への接続

Service Gateway をプロキシとして使用し、導入した Deep Discovery Inspector アプライアンスを Trend Vision One に接続します。

重要

次の手順は、2024 年 11 月現在のものです。詳細については、Trend Vision One のドキュメントを参照してください。https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-xdr-help/ConnectingDeployedDDI

手順

1. Network Analytics as a Service を使用する場合は、Deep Discovery Director - Network Analytics から切断します。
2. Service Gateway で転送プロキシサービスが設定されていることを確認します。

   詳細については、https://docs.trendmicro.com/ja-jp/documentation/article/trend-vision-one-forwardproxyservice で転送プロキシサービスを参照してください。
3. Trend Vision One コンソールで、Network Security Operations > Network Inventory > [Deep Discovery Inspector Appliances] の順に選択します。
4. [アプライアンスを接続] をクリックします。
5. [製品] で [Deployed Deep Discovery Inspector] を選択します。
6. [6.7 以降] を選択します。
7. 接続方法のリストから、[Service Gateway をプロキシとして使用して接続] を選択します。

8. リストから [Service Gateway] を選択します。
9. Deep Discovery Inspector アプライアンスの IP アドレスまたは完全修飾ドメイン名を指定します。

   アクセスできるのは、企業ネットワーク内のアプライアンスまたは直接接続できるアプライアンスのみです。
10. [Go] をクリックします。

    Deep Discovery Inspector アプライアンスのコンソールが表示されます。
11. Deep Discovery Inspector コンソールで、管理者アカウントを使用してサインインします。
12. (オプション) パスワードを変更します。
13. [Trend Micro Vision One に登録します] ダイアログで、[続行] をクリックして処理を確認します。
14. Trend Vision One コンソールで、Network Security Operations > Network Inventory > [Deep Discovery Inspector Appliances] の順に選択して、接続ステータスを確認します。

注意

Deep Discovery Inspector が Trend Vision One に接続すると、Deep Discovery Inspector によって「Trend Vision One 管理者」および「Trend Vision One 閲覧者」アカウントが自動的に作成されます。

Network Inventory を使用して Deep Discovery Inspector を Trend Vision One から切断します

ヒント

Deep Discovery Inspector を Deep Discovery Director から切断する必要がある場合は、284 ページの「Deep Discovery Director から登録解除する」を参照してください。

Trend Vision One から Deep Discovery Inspector を切断すると、Deep Discovery Inspector と統合されている Network Analytics および Service Gateway アプライアンスのバインドが解除されます。

手順

1. Trend Vision One コンソールで、Network Security Operations > Network Inventory > [Deep Discovery Inspector Appliances] の順に選択します。
2. Network Inventory のリストで目的の Deep Discovery Inspector アプライアンスを見つけ、行の右側にある削除ボタン ( ) をクリックします。
3. [Disconnect] をクリックします。

ヒント

Deep Discovery Inspector の Trend Vision One への再接続の詳細については、268 ページの「Trend Vision One への直接接続」 を参照してください。

Service Gateway の接続

Service Gateway をサービスソースとして使用するように、Trend Vision One に直接接続する Deep Discovery Inspector アプライアンスを設定します。

Service Gateway は、企業ネットワーク内の Trend Vision One から Deep Discovery Inspector アプライアンスへの接続を可能にし、より多くのサービスを提供します。

手順

1. Trend Vision One で、Service Gateway を 1 つ以上設定します。

   詳細については、Trend Micro Vision One のオンラインヘルプを参照してください。
2. Service Gateway に次のサービスがインストールされていることを確認します。
   - ActiveUpdate

- Smart Protection Services
- 不審オブジェクトリストの同期

詳細については、Trend Micro Vision One のオンラインヘルプを参照してください。

3. Service Gateway への接続を設定します。

重要

次の手順は、2024 年 11 月現在のものです。詳細については、Trend Vision One のドキュメントを参照してください。https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-xdr-help/ConnectingNetworkSensorsServiceGateway

---

a. Trend Vision One コンソールで、次の場所に移動します。Network Security Operations > Network Inventory > [Deep Discovery Inspector Appliances]。

b. 接続されているアプライアンスを 1 つ以上選択します。

c. [接続設定を設定]をクリックします。

[アプライアンスの接続設定] パネルが表示されます。

d. アプライアンスで [直接接続] 方式を使用している場合は、 [Service Gateway をサービスソースとして使用] を選択し、ソースとして使用するサービスゲートウェイを選択します。

e. Deep Discovery Inspector アプライアンスのバージョンが 6.7 以降の場合は、 [テスト接続]をクリックします。

ステータスが [成功] の場合、Deep Discovery Inspector 6.7 以降のアプライアンスに設定を適用できます。

Deep Discovery Inspector の以前のバージョンでは、ステータスが [未テスト]と表示されます。他のすべてのアプライアンスが [失敗] のステータスを返した場合でも、設定を適用できます。

f. [適用] をクリックして、ステータスが [成功] または [未テスト]のすべての Deep Discovery Inspector アプライアンスに設定を適用します。

Service Gateway のサービス

ヒント

Service Gateway でのサービスの管理の詳細については、Trend Micro Vision One のオンラインヘルプを参照してください。

有効なサービスを設定または表示するには、次の項目を参照してください。

- 274 ページの「有効な Service Gateway のサービスの表示」
- 274 ページの「Smart Protection Services」
- 276 ページの「コンポーネントサービスのアップデート」

有効な Service Gateway のサービスの表示

手順

1. Deep Discovery Inspector 管理コンソールで、[管理] > [統合製品/サービス] > Trend Vision One の順に選択します。
2. [Service Gateway] セクションで、有効なサービスを確認します。

Smart Protection Services

重要

次の手順は、2024 年 11 月現在のものです。詳細については、Trend Vision One のドキュメントを参照してください。https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-xdr-help/ManagingServicesSG

手順

1. Trend Vision One コンソールで、[Workflow and Automation] > [Service Gateway Management] の順に選択します。
2. 管理する Service Gateway の名前をクリックします。

   Service Gateway の画面が表示されます。
3. Smart Protection サービスを設定します。
   a. [サービスを管理] をクリックします。
   b. [サービスを管理] パネルで、[Smart Protection Services] を見つけます。
   c. インストールアイコン ( ) をクリックします。

   注意

   - サービスを有効にすると、Deep Discovery Inspector は自動的に Service Gateway の Smart Protection Server をプライマリ Smart Protection Server に設定します。
   - サービスを無効にすると、Deep Discovery Inspector は自動的に Smart Protection Server を以前の設定にします。

   Deep Discovery Inspector は Smart Protection Server を自動的に設定します。

   ヒント

   Service Gateway でのサービスの管理の詳細については、Trend Micro Vision One のオンラインヘルプを参照してください。

コンポーネントサービスのアップデート

重要

次の手順は、2024 年 11 月現在のものです。詳細については、Trend Vision One のドキュメントを参照してください。https://docs.trendmicro.com/ja-jp/enterprise/trend-micro-xdr-help/ManagingServicesSG

手順

1. Trend Vision One コンソールで、[Workflow and Automation] > [Service Gateway Management] の順に選択します。
2. 管理する Service Gateway の名前をクリックします。

   Service Gateway の画面が表示されます。
3. アップデートサービスを設定します。
   a. [サービスを管理] をクリックします。
   b. [サービスを管理] パネルで、[ActiveUpdate Service] を見つけます。
   c. インストールアイコン ( ) をクリックします。

Deep Discovery Inspector は、Service Gateway のアップデートサーバをアップデート元として自動的に設定します。

Service Gateway を切断する

手順

1. Trend Vision One コンソールで、Network Security Operations > Network Inventory > [Deep Discovery Inspector Appliances] の順に選択します。
2. 接続されているアプライアンスを 1 つ以上選択します。
3. [接続設定を設定]をクリックします。
4. アプライアンスで [直接接続] 方式を使用している場合は、[初期設定をサービスソースとして使用] を選択します。

5. [適用] をクリックします。

重要

Deep Discovery Inspector は、Service Gateway を介した不審オブジェクトデータの共有を停止します。

Apex Central

Trend Micro Apex Central は、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を容易にするソフトウェア管理ソリューションです。Apex Central には次の機能があります。

- 次の項目の一元管理
  - 不審オブジェクト、ユーザ定義リスト、および除外リスト
  - Deep Discovery Inspector の複数のシステムステータス
  - 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 (プログラムの物理的な場所やプラットフォームにかかわらない)
- Deep Discovery Inspector の複数ログの統合

Apex Central を使用した製品管理の詳細については、「Trend Micro Apex Central 管理者ガイド」を参照してください。

次の内容を実行するには、Deep Discovery Inspector の管理コンソールで [Apex Central] 画面を使用します。

- Deep Discovery Inspector を Apex Central サーバに登録できるかどうかの確認
- Apex Central サーバへの登録
- Deep Discovery Inspector と Apex Central 間の接続ステータスの確認
- Apex Central との最新の接続ステータスの確認
- Apex Central サーバからの登録解除
- 不審オブジェクトの Apex Central との同期

注意

Deep Discovery Inspector と Apex Central サーバの両方を同じネットワークセグメント内に配置してください。Deep Discovery Inspector が Apex Central と同じネットワークセグメントにない場合は、Deep Discovery Inspector のポート転送を設定します。

詳細については、278 ページの「Apex Central への登録」を参照してください。

Apex Central のコンポーネント

表 6-13. Apex Central のコンポーネント

コンポーネント	説明
Apex Central サーバ	Apex Central がインストールされているアプライアンス Web ベースの Apex Central 管理コンソールをホストします。
エンティティ	Apex Central コンソールのディレクトリツリーに表示される管理下の製品 (Deep Discovery Inspector など) ディレクトリツリーには管理下のエンティティがすべて含まれます。

Apex Central への登録

手順

1. [管理] > [統合製品/サービス] > [Apex Central] の順に選択します。
2. [接続設定] にある Apex Central の製品ディレクトリで、Deep Discovery Inspector を識別する名前を入力します。

   注意

   一意で意味のある名前を指定すれば、Deep Discovery Inspector を簡単に見分けることができます。

3. [Apex Central サーバ設定] で、次の操作を実行します。
   a. Apex Central 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。

b. Deep Discovery Inspector で Apex Central との通信に使用するポート番号を入力します。

c. (オプション) Apex Central のセキュリティを次のレベルに設定している場合は、[HTTPS を使用して接続する] を選択します。

- 中: Apex Central と Deep Discovery Inspector との間で HTTPS および HTTP 通信を許可します。
- 高: Apex Central と Deep Discovery Inspector との間で HTTPS 通信のみを許可します。

d. (オプション) ネットワークで認証が必要な場合は、IIS (Internet Information Services) サーバの [ユーザ名] と [パスワード] を入力します。

4. (オプション) NAT デバイスを使用する場合は、[双方向通信ポート転送を有効にする] を選択し、NAT デバイスの [IP アドレス] と [ポート] 番号を入力します。

注意

- Deep Discovery Inspector ではポート転送 IP アドレスおよびポート転送ポート番号を使用して Apex Central と双方向通信を行います。
- NAT デバイスの設定はオプションで、ネットワーク環境によって異なります。

5. プロキシ設定を Deep Discovery Inspector に設定済みであり、その設定を Apex Central との接続でも使用する場合は、[プロキシサーバを使用して接続する] を選択します。

6. (オプション) [不審オブジェクトの同期] で次の操作を実行します。

a. [不審オブジェクトを Apex Central と同期する] を選択します。

重要

不審オブジェクトを同期できるのは 1 つのソースのみです。Deep Discovery Inspector で Apex Central との同期を有効にしている場合は、その他の外部ソースから不審オブジェクトを受信することはありません。

このオプションを選択する前に、外部サンドボックスが、不審オブジェクトを Apex Central に送信するように設定されていることを確認します。

b. API キーを入力します。

注意

API キーを取得するには、Apex Central にログオンします。

Deep Discovery Inspector は、不審オブジェクトのリストを 20 秒ごとに Apex Central と同期し、前回の同期時刻を表示します。

7. [接続テスト] をクリックして、Deep Discovery Inspector から Apex Central サーバに接続できることを確認します。
8. 接続が正常に確立された場合は、[登録] をクリックします。

Apex Central からの登録解除

手順

1. [管理] > [統合製品/サービス] > [Apex Central] の順に選択します。
2. [接続ステータス] で [登録解除] をクリックします。

注意

Deep Discovery Inspector を Apex Central から登録解除するか別の Apex Central に登録するには、このオプションを使用します。

Apex Central との接続の管理

手順

1. [管理] > [統合製品/サービス] > [Apex Central] の順に選択します。
2. [接続ステータス] で次の処理を実行します。
   a. 製品が Apex Central に接続可能であることを確認します。
   b. 製品が接続されていない場合は、ただちに接続を復元してください。
   c. 接続ステータスをチェックして、Deep Discovery Inspector および Apex Central サーバ間の前回の通信を確認します。
3. 登録後に変更を行い、Apex Central サーバをアップデートするには、[設定のアップデート] をクリックします。
4. Deep Discovery Inspector の管理を別の Apex Central サーバで行うには、[登録解除] をクリックし、Deep Discovery Inspector を新しい Apex Central サーバに登録します。

   詳細については、278 ページの「Apex Central への登録」を参照してください。

Deep Discovery Director

Trend Micro Deep Discovery Director (以下、Deep Discovery Director) は、Deep Discovery 製品へのアップデート、アップグレード、および仮想アナライザイメージの配信と、Deep Discovery 製品の設定の複製およびログの集約を一元管理する管理ソリューションです。さまざまな組織上およびインフラストラクチャ上の要求に対応するため、Deep Discovery Director には Distributed Mode や Consolidated Mode などの柔軟な配信オプションが用意されています。

さらに Deep Discovery Inspector では、Deep Discovery Director との間で脅威インテリジェンスを供給および取得することにより、脅威インテリジェンスの共有サービスおよび検出機能が強化されます。

Deep Discovery Director の統合の詳細については、「Deep Discovery Director 管理者ガイド」および次の項を参照してください。

- 282 ページの「Deep Discovery Director に接続する」
- 284 ページの「Deep Discovery Director から登録解除する」
- 403 ページの Deep Discovery Director および Trend Vision One で複製される設定

Deep Discovery Director に接続する

重要

Deep Discovery Inspector がすでに Trend Vision One に接続されている場合、Deep Discovery Director に接続することはできません。

次の手順は、Deep Discovery Director への登録方法を示しています。すでに登録している Deep Discovery 製品の接続設定を変更するには、まず登録解除する必要があります。

クラウドバージョンの Deep Discovery Director は Trend Vision One と統合されています。[管理] > [統合製品/サービス] > Trend Vision One で接続ステータスを確認してください。

手順

1. [管理] > [統合製品/サービス] > [Deep Discovery Director] > [管理サーバ] の順に選択します。
2. [接続設定] で、Deep Discovery Director マネジメントサーバの [サーバアドレス] を入力します。
3. [接続設定] で、Deep Discovery Director の [ポート] 番号を入力します。
4. [接続設定] で、Deep Discovery Director マネジメントサーバの [API キー] を入力します。

注意

この情報は Deep Discovery Director の管理コンソールの [ヘルプ] 画面で確認できます。

5. (オプション) Deep Discovery Inspector に設定したプロキシ設定を Deep Discovery Director との接続に使用する場合は、[システムのプロキシ設定を使用] を選択します。

ヒント

この設定は、Deep Discovery Director への登録後に変更できます。

この設定を Deep Discovery Director から登録解除せずに更新するには、[設定のアップデート] をクリックします。

6. [登録] をクリックします。

[ステータス] が [登録済み | 接続] に変更されます。

注意

Deep Discovery Director のフィンガープリントを変更すると、接続が中断され、[信頼する] ボタンが表示されます。接続を回復させるには、Deep Discovery Director のフィンガープリントが有効であることを確認してから [信頼する] をクリックします。

登録が完了したら、[接続テスト] ボタンが表示されます。[接続テスト] クリックして、Deep Discovery Director への接続をテストします。

注意

Deep Discovery Director - Network Analytics as a Service (以下、DDD - NAaaS) への登録については、Deep Discovery Director のドキュメントを参照してください。

Deep Discovery Inspector は、DDD - NAaaS と Deep Discovery Director - Network Analytics (以下、DDD - NA) の両方に同時に登録することはできません。DDD - NA に登録している Deep Discovery Inspector を DDD - NAaaS に登録する場合は、まず DDD - NA から登録解除する必要があります。

Deep Discovery Inspector を DDD - NAaaS に登録すると、DDD - NAaaS の情報が [管理サーバ] タブに表示されます。

Deep Discovery Director から登録解除する

Deep Discovery Director から登録解除するか、別の Deep Discovery Director に登録し直す場合は事前に、次の手順を実行してください。

手順

1. [管理] > [統合製品/サービス] > [Deep Discovery Director] の順に選択します。
2. [登録解除] をクリックします。

注意

Deep Discovery Director を登録解除すると、Deep Discovery Director - Network Analytics および Deep Discovery Director - Network Analytics as a Service も登録解除されます。

Threat Investigation Center

Trend Micro Threat Investigation Center は、ビッグデータの収集、集約、形式化、および関連付けを行うスケーラブルなサービスです。ビッグデータを実行可能なインテリジェンスに変換し、可視化およびレポートを提供します。

Threat Investigation Center は、Windows イベントログをサポートするだけでなく、Advanced Threat Assessment Service、Deep Discovery Email Inspector、Deep Discovery Inspector、Deep Security、Apex Central、および Endpoint Sensor など複数のトレンドマイクロ製品やサービスと連携します。Deep Discovery Inspector から Threat Investigation Center に接続して利用するには、別途監視サービスのご契約が必要となります。

Threat Investigation Center の統合

次の手順に従い、組み込みエージェントを介して Threat Investigation Center を統合します。

Threat Investigation Center で追加の手順の実行が必要になる場合があります。詳細については、Threat Investigation Center のドキュメントを参照してください。

手順

1. Deep Discovery Inspector 管理コンソールを開き、[管理] > [統合製品/サービス] > [Threat Investigation Center] の順に選択します。

   [Threat Investigation Center] ウィンドウが表示されます。

2. [追加] をクリックします。

   [Threat Investigation Center サーバの追加] ウィンドウが表示されます。

3. [有効] を選択します。

4. [サーバアドレス] で、Threat Investigation Center の HTTPS ログサーバアドレスを入力します。

5. (オプション) [ファイルの取得] を有効にします。

   注意

   ファイルの取得が有効な場合、Threat Investigation Center は調査パッケージとパケットキャプチャのファイルを Deep Discovery Inspector から収集します。Deep Discovery Inspector が Threat Investigation Center に登録されている場合に、この機能を利用できます。

6. (オプション) [CA 証明書を使用] を有効にしてから [選択] をクリックすると、Threat Investigation Center の CA 証明書を選択できます。

   注意

   CA 証明書の使用はオプションです。Threat Investigation Center サーバと Deep Discovery Inspector の間に中間者アプライアンスが存在する場合は、証明書が必要となります。

7. (オプション) [システムのプロキシ設定を使用] を有効にします。

   注意

   [管理] > [システム設定] > [プロキシ] で、システムのプロキシを設定します。

8. (オプション) [接続のテスト] をクリックして、Threat Investigation Center サーバへの接続を確認します。
9. [保存] をクリックします。

TXOne OT Defense Console

Trend Micro TXOne OT Defense Console は、産業用ネットワーク向けの安全で分散化されたサポートを提供し、運用技術 (OT) 環境のサイバー脅威を一元的かつ継続的に監視することで、途切れることのない製品ラインの稼働を実現します。

TXOne OT Defense Console の設定

手順

1. Deep Discovery Inspector 管理コンソールで、[管理] > [統合製品/サービス] > [TXOne OT Defense Console] の順に選択します。
2. [TXOne OT Defense Console にオブジェクトを配信する] を有効にします。
3. 次の情報を入力します。

- サーバアドレス

注意

サーバアドレスは、TXOne OT Defense Console 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。

- API キー: 既存の認証情報
- API シークレット: 既存の認証情報

4. (オプション) [接続テスト] をクリックします。
5. (オプション) [オブジェクトの配信] で、新しい [実行間隔] を選択します。
6. Deep Discovery Inspector から TXOne OT Defense Console 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:
     - 不審オブジェクト
       - IPv4 アドレス
       - SHA1
   - リスクレベル:
     - 高のみ
     - 高および中
     - 高、中、および低
7. [保存] をクリックします。

脅威インテリジェンスの共有

Deep Discovery Inspector では、HTTP または HTTPS Web サービスを介して、不審 URL などの脅威インテリジェンスデータを Blue Coat ProxySG デバイスなど他の製品やサービスと共有できます。

脅威インテリジェンスの共有設定

手順

1. Deep Discovery Inspector 管理コンソールで、[管理] > [統合製品/サービス] > [脅威インテリジェンスの共有] の順に選択します。
2. [脅威インテリジェンスの共有] を有効にすると、統合製品/サービスで Deep Discovery Inspector の情報を取得できるようになります] を選択します。
3. [条件] で、脅威インテリジェンスのデータファイルに含めるオブジェクトを選択します。

注意

共有 URL オブジェクトは最大 997 文字まで入力できます。

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 6-14. 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
仮想アナライザで特定された不審 URL	DDI_va_suspicious_objects
拒否リスト内の URL	DDI_custom_defense_denylists
Apex Central または Deep Discovery Director のユーザ指定の不審オブジェクトリスト内の URL	DDI_control_manager_denylists
Web レピュテーションサービスで検出された不正 URL	DDI_wrs_malicious_urls
C&C コールバック URL	DDI_aggressive_rule_urls

オブジェクト	生成されるファイル内のカテゴリ
次のいずれかのファイルの送信元 URL: • 仮想アナライザで特定された不審ファイル • 拒否リスト内のファイル • Apex Central または Deep Discovery Director のユーザ指定の不審オブジェクトリスト内のファイル	DDI_aggressive_rule_urls
不正ファイルの送信元 URL	DDI_aggressive_rule_urls

4. [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。
5. (オプション) 初期設定で、脅威インテリジェンスのデータは HTTPS Web サービス経由で共有されます。HTTP Web サービスを有効にしてデータを共有することもできます。[サーバ設定] で [HTTP を使用して情報を共有 (HTTPS に追加)] を選択して、HTTP ポート番号を指定します。
6. [保存] をクリックします。
7. [生成] をクリックします。

注意

ファイルが生成されたら、URL をクリックし、脅威インテリジェンスのデータファイルをダウンロードして内容を確認できます。

8. Blue Coat ProxySG デバイスなどの統合製品/サービスを設定して、Deep Discovery Inspector から脅威インテリジェンスのデータを取得します。詳細については、統合製品/サービスのドキュメントを参照してください。

インライン製品とサービス

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、仮想アナライザ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インラインの製品やサービスに配信できます。

Deep Discovery Inspector は、次のインラインソリューションと連携します。

表 6-15. サポート対象のインラインソリューション

名前	バージョン
Trend Micro TippingPoint Security Management System (SMS)	5.5
Check Point Open Platform for Security (OPSEC)	Check Point R81
IBM Security Network Protection (XGS)	XGS 5.5
Palo Alto Panorama または Firewall	• PAN-OS 10.2 • Panorama 10.2

注意

Deep Discovery Inspector が一度にサポートするのは 1 つの製品/サービスのみです。

Trend Micro TippingPoint Security Management System (SMS)

Deep Discovery Inspector と Apex Central の両方から不審オブジェクトと 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。Deep Discovery Inspector では各不審オブジェクトおよび C&C コールバックアドレス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: Trend MicroDeep Discovery Inspector の製品名
- Trend Micro Source: Deep Discovery Inspector 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

Trend Micro TippingPoint Security Management System (SMS) は、レピュテーションフィルタを使用して、レピュテーショングループ全体にブロック、許可、または通知の処理を適用します。レピュテーションフィルタの詳細については、Trend Micro TippingPoint のドキュメントを参照してください。

Trend Micro TippingPoint Security Management System (SMS) の設定

手順

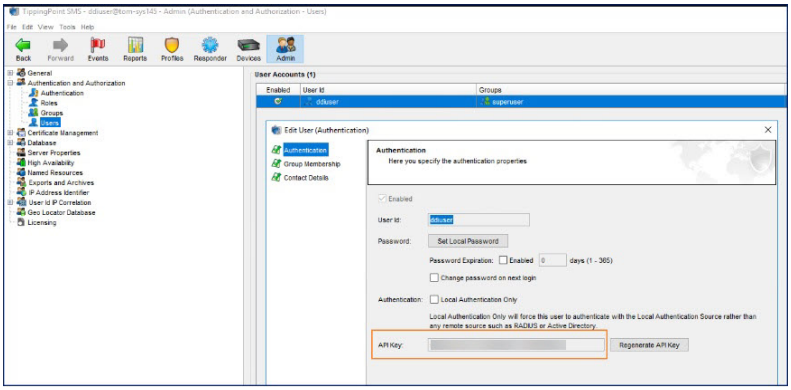
1. [管理] > [統合製品/サービス] > [インライン製品/サービス] の順に選択します。
2. [Trend Micro TippingPoint Security Management System (SMS)] を選択します。
3. [サーバ情報] で登録方法を選択します。
   - API キー (推奨)
   - ユーザ名/パスワード
4. すべての必要な情報を指定します。

重要

- サーバアドレスは、インライン製品の 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。
- ユーザ名とパスワードには最大 15 文字まで指定できます。

ヒント

API キーは TippingPoint SMS のコンソールで確認できます。



5. (オプション) [接続テスト] をクリックします。
6. [オブジェクトの配信] で [有効] をクリックします。
7. (オプション) 新しいオブジェクトの配信間隔を指定します。
8. [条件] で、Deep Discovery Inspector から Trend Micro TippingPoint Security Management System に送信するオブジェクトの種類とリスクレベルを指定します。

オブジェクトの種類	リスクレベル
C&C コールバックアドレスと不審オブジェクト • IPv4 アドレス • ドメイン • URL **重要** Trend Micro TippingPoint Security Management System 5.0 以上でのみサポートされます。	• 高のみ • 高および中 • 高、中、および低

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 Inspector のホスト名
Trend Micro Severity	指定可能な値: • 高 • 中 • 低

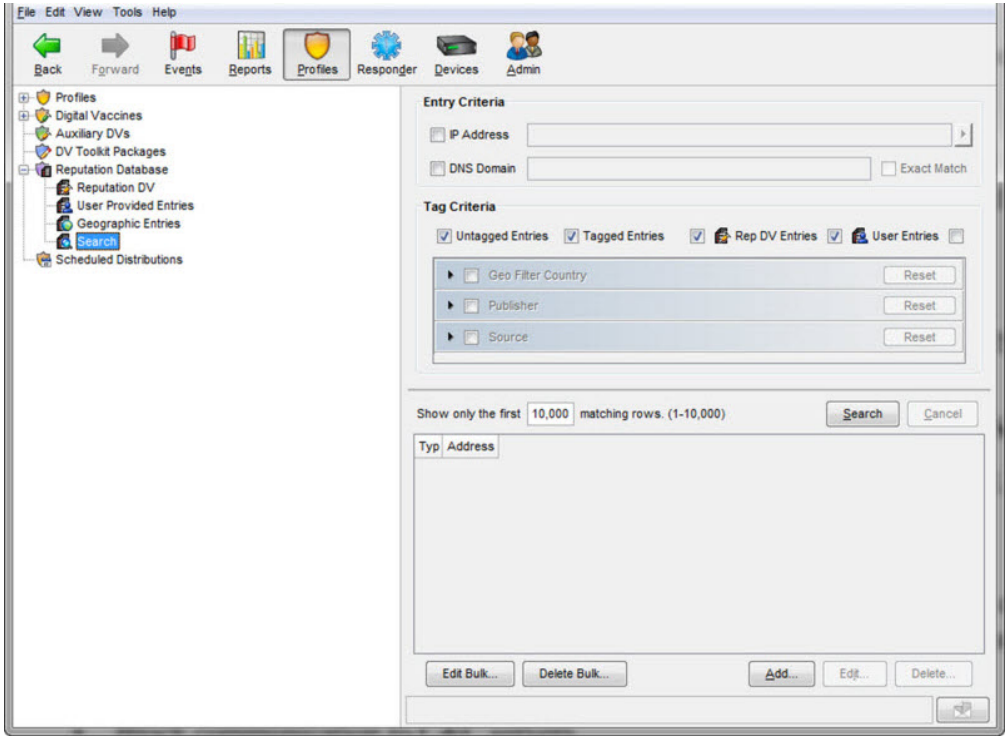
タグのカテゴリ	値
Trend Micro Publisher	Deep Discovery Inspector の製品名
Trend Micro Detection Category	脅威の検出の種類

10. (オプション) 配信された不審オブジェクトと C&C コールバックアドレスを TippingPoint SMS で表示します。

    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。

TippingPoint SMS コンソールに、Deep Discovery Inspector によって配信された不審オブジェクトと 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 Inspector は、SAM (Suspicious Activities Monitoring) API を介して OPSEC と統合されます。

SAM API を実装した SAM クライアント (Deep Discovery Inspector) は、Check Point ファイアウォールとの通信を行い、SAM サーバとして機能します。Deep Discovery Inspector は、SAM API を使用して、特定の接続に対して指定した処理を実行するようファイアウォールに要求します。

たとえば、Deep Discovery Inspector は、不正なコマンドを発行しているクライアントやログオンに繰り返し失敗しているクライアントとの接続をブロックするよう Check Point OPSEC に求める場合があります。

Check Point OPSEC (Open Platform for Security) の設定

手順

1. Check Point のアプライアンスを設定します。
   a. Check Point のアプライアンスで、SAM の通信モードポートを確認または設定します。

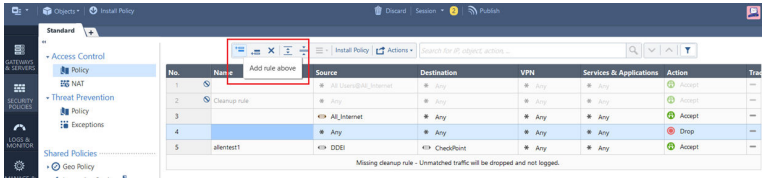
      詳細については、303 ページの「セキュリティゲートウェイの事前設定」を参照してください。

   b. Check Point のアプライアンスで、OPSEC アプリケーションを設定します。

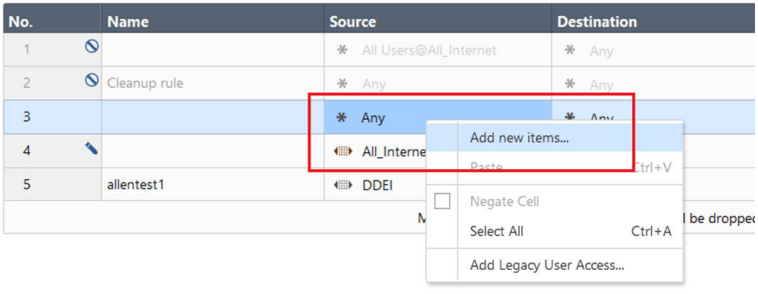
      詳細については、305 ページの「保護された接続を設定する」を参照してください。

   c. Check Point のアプライアンスで、SAM ファイルの削除を有効にします。
      1. Check Point SmartDashboard を開きます。
      2. [Other] を展開し、[SAM] に移動します。
      3. [Purge SAM file when it reaches:] を有効にします。
      4. ファイルサイズを指定します。
      5. [OK] をクリックします。
      6. 保存します。
   d. Check Point のアプライアンスで、セキュリティポリシーを設定します。

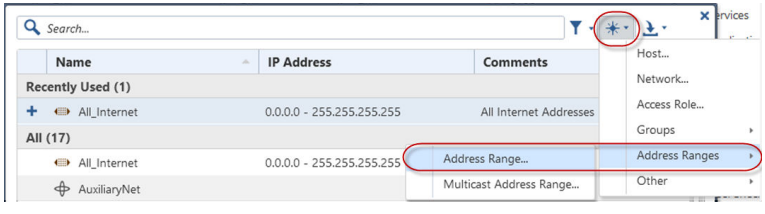
1. Check Point SmartConsole を開きます。
2. [SECURITY POLICIES] タブで、[Access Control] > [Policy] の順に選択します。



3. ルールを追加するには、[Add rule above] アイコン ( ) をクリックします。
4. 新しいポリシーを設定するには、Action を右クリックします。
5. 処理を [Accept] に変更します。
6. 送信元を右クリックします。

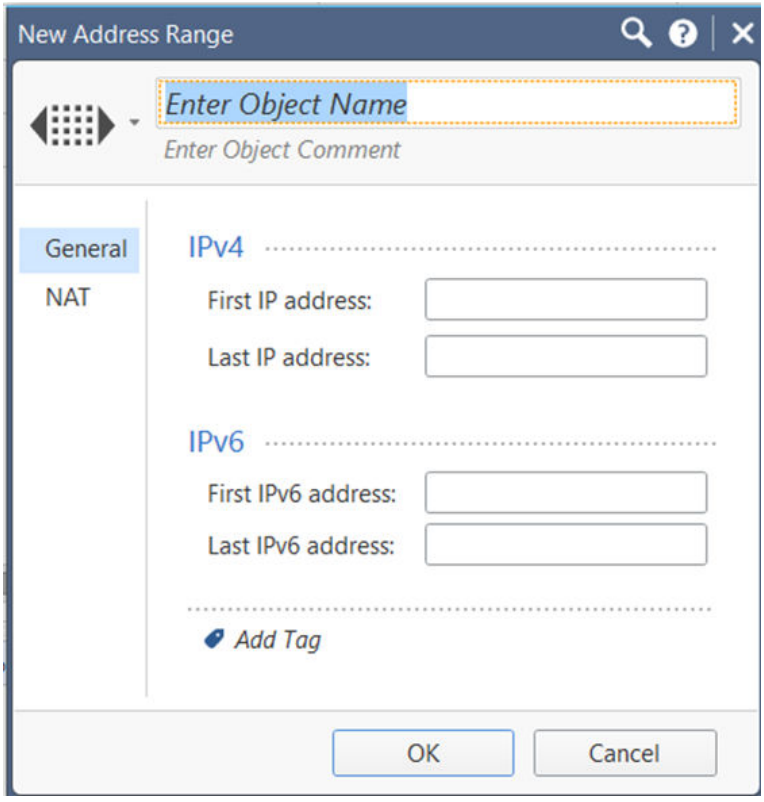


7. [Add new items...] を選択します。
8. 新規アイコン ( ) をクリックします。



9. [Address Ranges] > [Address Range...] の順に選択します。

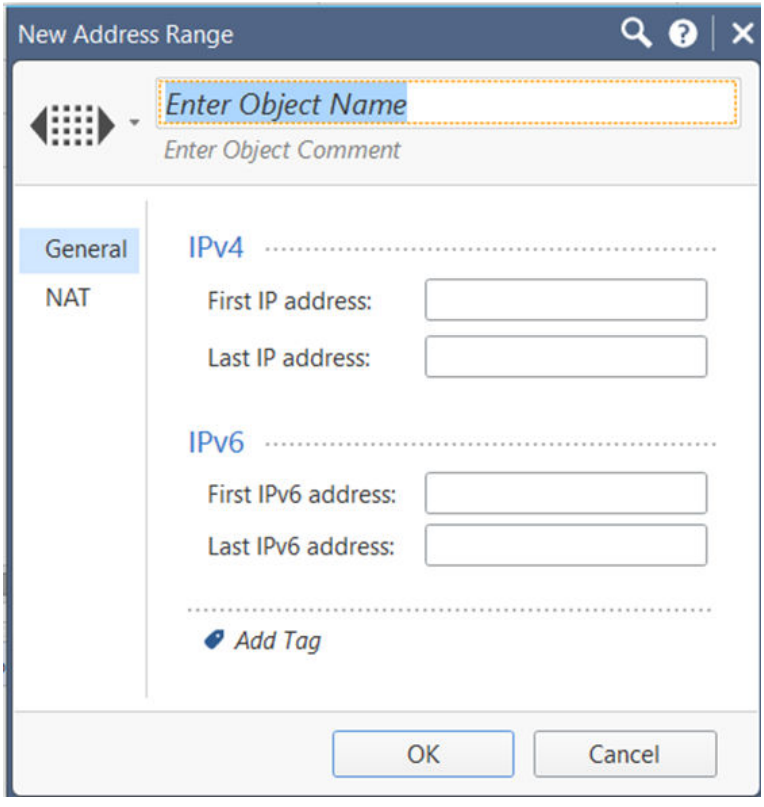
   [New Address Range] 画面が表示されます。



10. [Enter Object Name] フィールドに `DDI` と入力します。
11. [First IP address] には、Deep Discovery Inspector の IP アドレスを入力します。
12. [Last IP address] には、Deep Discovery Inspector の IP アドレスを入力します。
13. [OK] をクリックします。
14. Destination を右クリックします。

15. [Add new items...] を選択します。
16. 新規アイコン ( ) をクリックします。
17. [Address Ranges] > [Address Range...] の順に選択します。

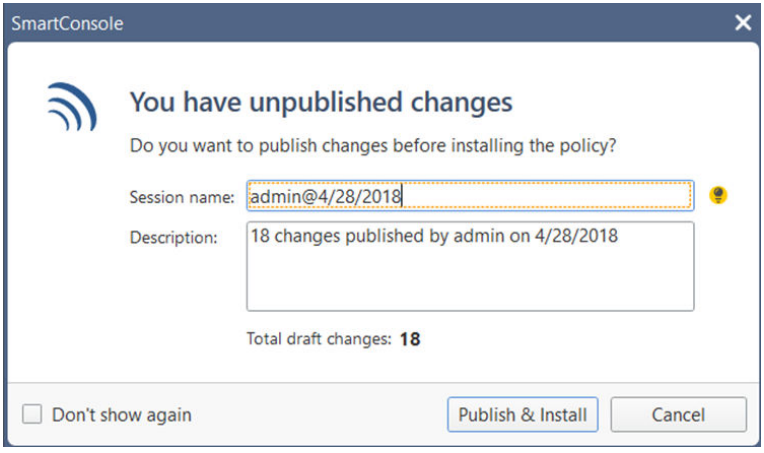
    [New Address Range] 画面が表示されます。



18. [Enter Object Name] フィールドに `CheckPoint` と入力します。
19. [First IP address] には、CheckPoint の IP アドレスを入力します。
20. [Last IP address] には、CheckPoint の IP アドレスを入力します。

21. [OK] をクリックします。
22. [Install Policy] をクリックします。

    次の画面が表示されます。



23. [Publish & Install] をクリックします。
24. [Install] をクリックします。

    Check Point のアプライアンスで、Deep Discovery Inspector 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。

2. Deep Discovery Inspector を設定します。
   a. Deep Discovery Inspector の管理コンソールで、[管理] > [統合製品/サービス] > [インライン製品/サービス] の順に選択します。
   b. [Check Point Open Platform for Security (OPSEC)] を選択します。
   c. 接続の種類を選択します。

注意

ネットワーク設定で、Deep Discovery Inspector から Check Point のアプライアンスへの接続が許可されていることを確認します。

Deep Discovery Inspector では接続先の Check Point で設定されている保護された接続ポートまたは通常の接続ポートを介して接続することがあります。また、Deep Discovery Inspector は、18210 番ポートを介して Check Point のアプライアンスから証明書を取得します。

[保護された接続] を選択した場合、[OPSEC アプリケーション名] 設定と [SIC ワンタイムパスワード] 設定が表示されます。

d. サーバのアドレスを入力します。

注意

サーバアドレスは、インライン製品の 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。

e. 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、303 ページの「セキュリティゲートウェイの事前設定」を参照してください。

f. [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、305 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には、以前とは異なるものを使用する必要があります。

g. (オプション) [接続テスト] をクリックします。

h. [オブジェクトの配信] で [有効] をクリックします。

[使用許諾契約/利用規約] が開きます。

i. [使用許諾契約/利用規約] を読み、同意できる場合は同意します。

注意

この製品/サービスとの連携を有効にするには、[使用許諾契約/利用規約] に同意する必要があります。

j. (オプション) 新しい [実行間隔] を選択します。

k. 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 Inspector から Check Point のアプライアンスに送信します。

- 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

l. [詳細設定] で、次の処理のいずれかを選択します。

- 拒否: パケットが拒否され、パケットが拒否された通信先に通知が送信されます。
- 破棄: パケットは破棄されますが、通信先には通知が送信されません。
- 通知: 定義されたアクティビティについて通知が送信されますが、そのアクティビティはブロックされません。

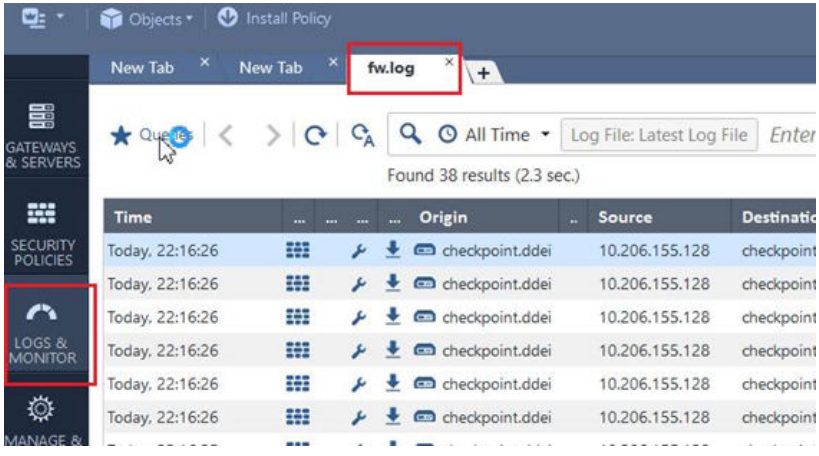
m. [保存] をクリックします。

n. (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。

3. Deep Discovery Inspector から配信された不審オブジェクトおよび C&C コールバックアドレスを Check Point の SmartView Monitor で表示するには、次の手順を実行します。

a. Check Point SmartConsole で、[Logs & Monitor] に移動します。

b. 新しいタブを追加します。



c. [Tunnels & User Monitoring] をクリックして、SmartView Monitor を開きます。

d. [Launch Menu] アイコンをクリックして、[Tools] > [Suspicious Activity Rules] の順にクリックします。

[Enforced Suspicious Activity Rules] 画面が開きます。

e. [Show On] で目的のアプライアンス名を選択します。

f. [Refresh] をクリックします。

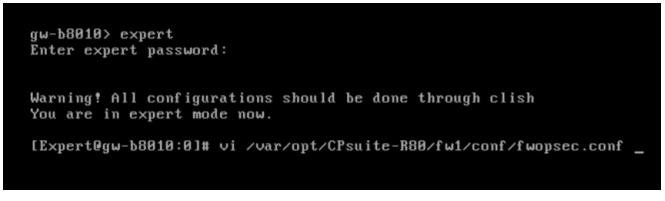
Deep Discovery Inspector から配信された不審オブジェクトおよび C&C コールバックアドレスが表示されます。

セキュリティゲートウェイの事前設定

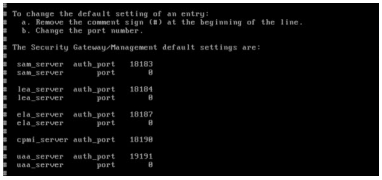
手順

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 Inspector の [管理] > [統合製品/サービス] > [インライン製品/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 Inspector の [管理] > [統合製品/サービス] > [インライン製品/サービス] の [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 Inspector の [管理] > [統合製品/サービス] > [インライン製品/サービス] の [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。

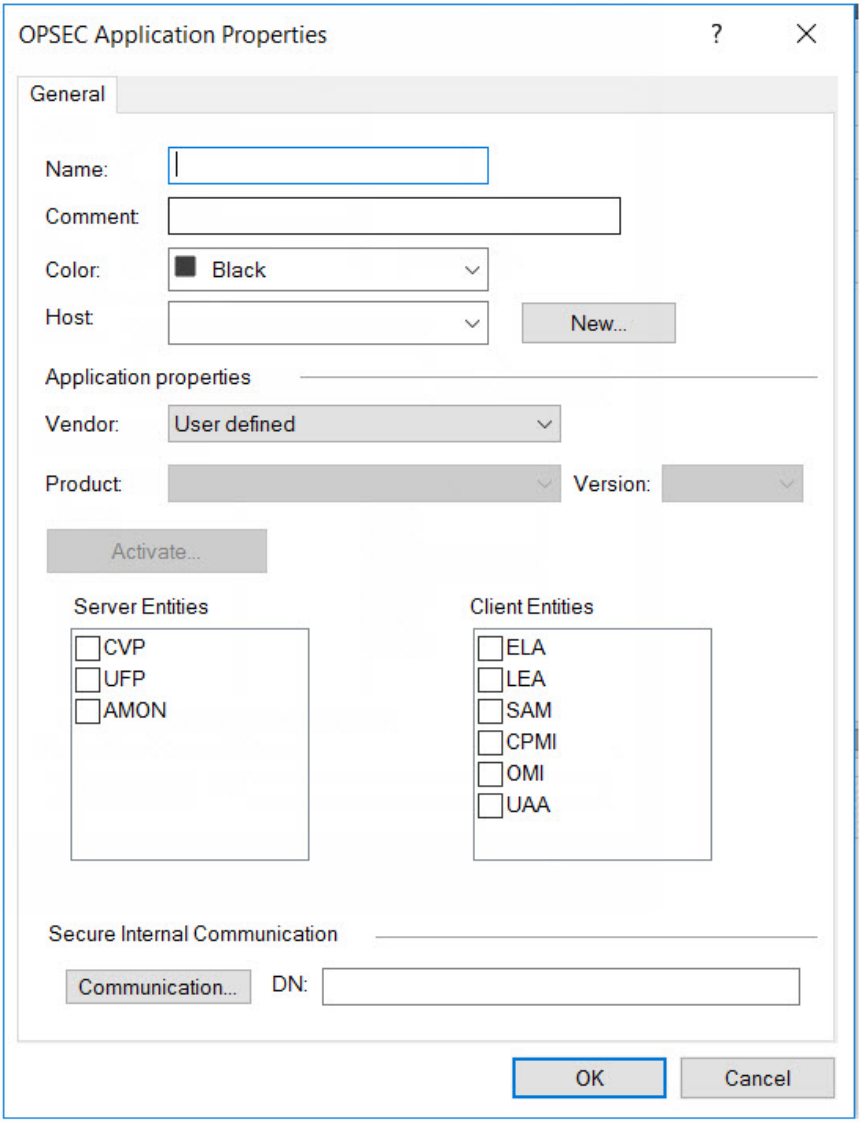
6. `fwopsec.conf` ファイルに変更を行った場合は、`fwopsec.conf` ファイルを保存して Check Point アプライアンスを再起動します。

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。



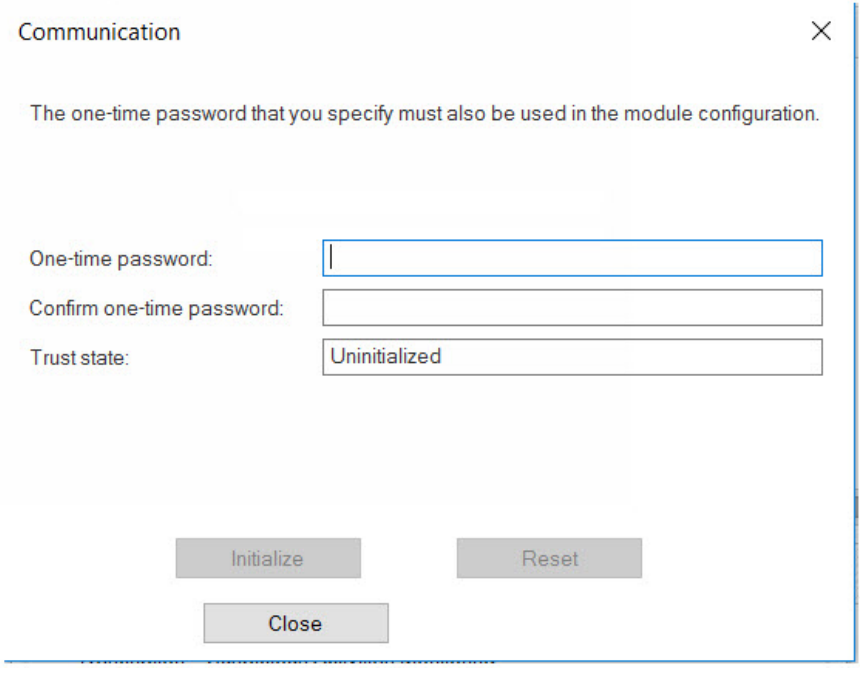
3. [Name] に名前を入力します。

注意

- Deep Discovery Inspector では、この名前を [OPSEC application name] に使用します。
- アプリケーション名は 100 文字以下で入力してください。英文字で始まり、英文字、ピリオド、アンダースコア、またはダッシュのみが使用されている必要があります。

4. [Host] でホストを選択します。
5. [Client Entities] で [SAM] を選択します。
6. [Communication...] をクリックします。

[Communication] 画面が表示されます。



7. [One-time password] にパスワードを入力し、同じパスワードを [Confirm one-time password] に入力します。

注意

Deep Discovery Inspector では、このパスワードを [SIC one-time password] に使用します。

注意

Check Point のアプライアンスでワンタイムパスワードがリセットされた場合、新しいワンタイムパスワードには、以前とは異なるものを使用する必要があります

8. [Initialize] をクリックします。

   [Trust state] が [Initialized but trust not established] になります。

9. ユーザ定義をインストールします。

   a. メイン画面の [Check Point SmartConsole] で、 をクリックし、[Install database...] を選択します。

      [Install database] 画面が表示されます。

   b. インストールするコンポーネントを選択し、[OK] をクリックします。

      ユーザ定義のインストールが開始されます。

IBM Security Network Protection

IBM Security Network Protection (XGS) の提供する Web サービス API を使用すると、Deep Discovery Inspector などのサードパーティ製アプリケーションから不審オブジェクトおよび C&C コールバックアドレスを直接送信できます。IBM XGS では次の機能を実行できます。

- 不正プログラムに感染したホストの隔離
- C&C サーバへの通信のブロック
- 不正プログラムの配信が検出された URL へのアクセスのブロック

Deep Discovery Inspector を IBM XGS と統合するには、次のことを実行するように汎用エージェントを設定します。

- 特定のスキーマに従ったアラートの許可
- 一般的な ATP 変換ポリシーに基づく隔離ルールの作成

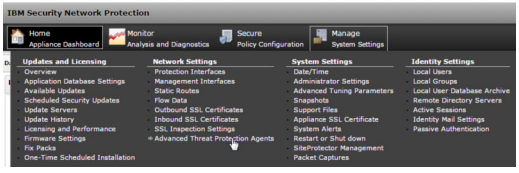
ATP 変換ポリシーにより、IBM XGS に対してメッセージの複数のカテゴリを使用してブロックやアラートなどの異なる処理を実行できます。

IBM Security Network Protection の設定

手順

1. IBM XGS のコンソールで次の手順を実行して、汎用エージェントを設定します。

   a. [Manage System Settings] > [Network Settings] > [Advanced Threat Protection Agents] の順に選択します。



   [Advanced Threat Protection Agents] 画面が開きます。

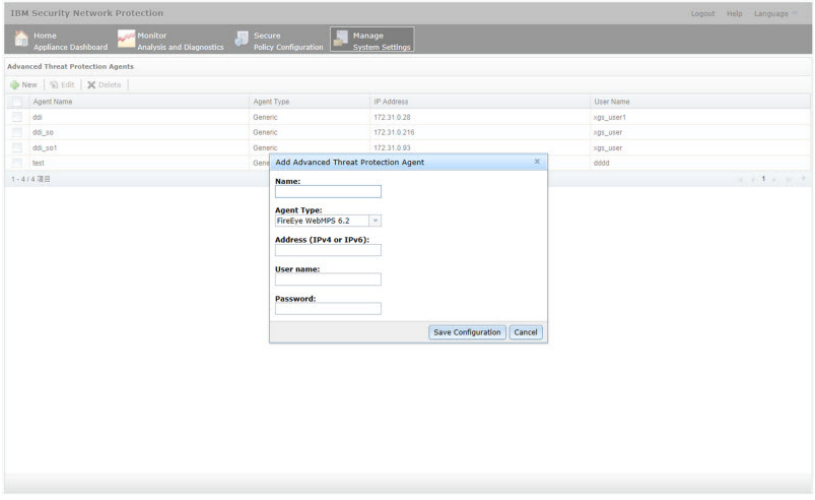
   b. [New] をクリックします。

   c. 次の情報を入力します。

      - Name: 名前を入力
      - Agent Type: [Generic] を選択
      - Address: Deep Discovery Inspector 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 6-16. 有効な文字セット

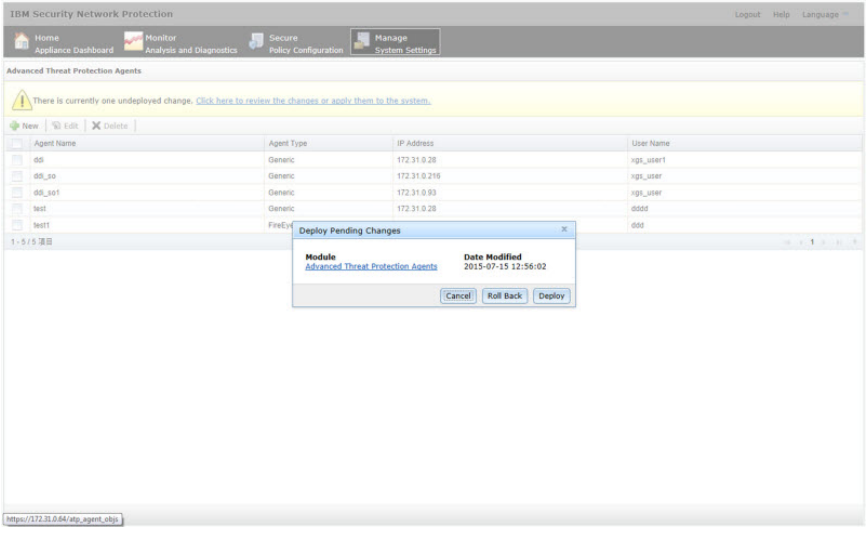
	ユーザ名	パスワード
最小文字数	1 文字	1 文字
最大文字数	15 文字	15 文字



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 Inspector の管理コンソールで、[管理] > [統合製品/サービス] > [インライン製品/サービス] の順に選択し、[IBM Security Network Protection (XGS)] を選択します。
5. 次の情報を入力します。
   - サーバアドレス

     注意
     サーバアドレスは、インライン製品の 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。
   - ユーザ名: 既存の認証情報
   - パスワード:既存の認証情報

   表 6-17. 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

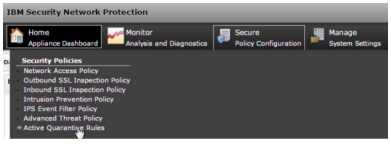
6. (オプション) [接続テスト] をクリックします。
7. [オブジェクトの配信] で [有効] をクリックします。

   [使用許諾契約/利用規約] が開きます。
8. [使用許諾契約/利用規約] を読み、同意できる場合は同意します。

   注意
   この製品/サービスとの連携を有効にするには、[使用許諾契約/利用規約] に同意する必要があります。
9. (オプション) 新しい [実行間隔] を選択します。
10. Deep Discovery Inspector からこのインライン製品/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

11. [保存] をクリックします。
12. (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 Inspector から IBM XGS に送信された不審オブジェクトおよび C&C コールバックアドレスを表示します。



注意

リスクレベルの低い不審オブジェクトは、IBM XGS の [Active Quarantine Rules] には表示されません。Deep Discovery Inspector から送信された不審オブジェクトをすべて表示するには、[Security Policy Configuration] > [Advanced Threat Policy] の順に選択し、次のように設定します。

- Agent Type: Generic
- Alert Type: Reputation
- Alert Severity: Low

Deep Discovery Inspector から配信された不審オブジェクトおよび C&C コールバックアドレスが表示されます。

Palo Alto Panorama または Firewall

Palo Alto Firewall は、ポート番号、プロトコル、暗号化方式 (SSL や SSH)、または秘匿技術に関係なくアプリケーションを識別して制御します。

Deep Discovery Inspector では、一致条件として Palo Alto Firewall または Palo Alto Panorama™の URL カテゴリに IPv4、ドメイン、および URL の不審オブジェクトを送信でき、これによって例外ベースの動作が可能になります。

ポリシーで URL カテゴリを使用するには、次のように設定します。

- Active Directory 内の複数のグループに属するユーザについて、一般的なセキュリティポリシーに対する例外を特定して許可します。

  例: すべてのユーザには不正プログラムやハッキングサイトへのアクセスを拒否しますが、セキュリティグループに属するユーザには許可します。

- ストリーミングメディアカテゴリへのアクセスを許可しますが、サービスの品質ポリシーを適用して帯域幅の使用量を制御します。
- リスクレベルの高い URL カテゴリでのファイルのダウンロードとアップロードを防止します。

例: 未知のサイトへのアクセスは許可しますが、未知のサイトからの実行可能ファイルのアップロードとダウンロードは防止して、不正プログラムの伝播を防ぎます。

- 金融およびショッピングカテゴリへの暗号化アクセスを許可し、その他すべての URL カテゴリへのトラフィックを復号して検査する、SSL 復号ポリシーを適用します。

Palo Alto Panorama または Firewall の設定

手順

1. Deep Discovery Inspector の管理コンソールで、[管理] > [統合製品/サービス] > [インライン製品/サービス] > [Palo Alto Panorama または Firewall] の順に選択します。
2. 次の情報を入力します。
   - サーバアドレス

     注意

     サーバアドレスは、インライン製品の 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。
   - サーバの種類
     - Panorama
     - Firewall

     注意

     Deep Discovery Inspector では、Palo Alto Panorama および Firewall が仮想システムでサポートされます。

     仮想システムの Panorama デバイスと Firewall では、不審オブジェクトと C&C コールバックアドレスを使用するようにポリシールールを設定する必要があります。
   - ユーザ名: 既存の認証情報

- パスワード: 既存の認証情報

表 6-18. 有効な文字セット

	ユーザ名	パスワード
最小文字数	1 文字	1 文字
最大文字数	15 文字	15 文字

3. (オプション) [接続テスト] をクリックします。
4. [オブジェクトの配信] で [有効] をクリックします。

   [使用許諾契約/利用規約] が開きます。
5. [使用許諾契約/利用規約] を読み、同意できる場合は同意します。

注意

この製品/サービスとの連携を有効にするには、[使用許諾契約/利用規約] に同意する必要があります。

---

6. (オプション) 新しい [実行間隔] を選択します。
7. Deep Discovery Inspector からこのインライン製品/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
     - 不審オブジェクト
       - IPv4 アドレス
       - ドメイン
       - URL

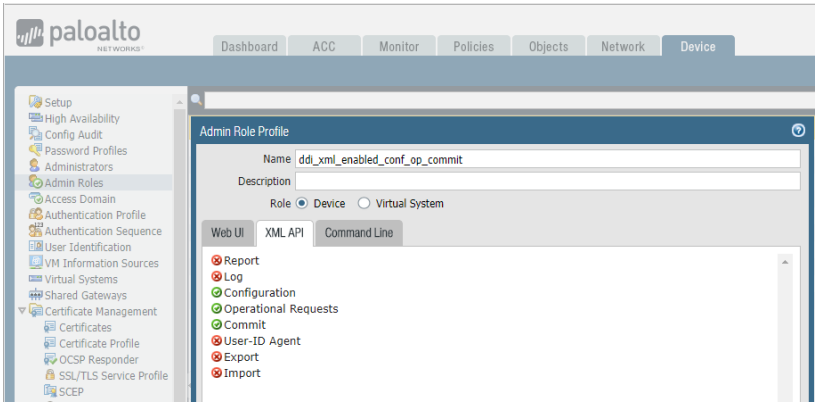
- リスクレベル:
  - 高のみ
  - 高および中
  - 高、中、および低

8. [詳細設定] で URL カテゴリ名をカスタマイズします。

   URL カテゴリ名は、次の文字を使用して 1〜31 文字で作成します。

   - 大文字 (A〜Z)
   - 小文字 (a〜z)
   - 数字 (0〜9)
   - 特殊文字: - _
   - スペース

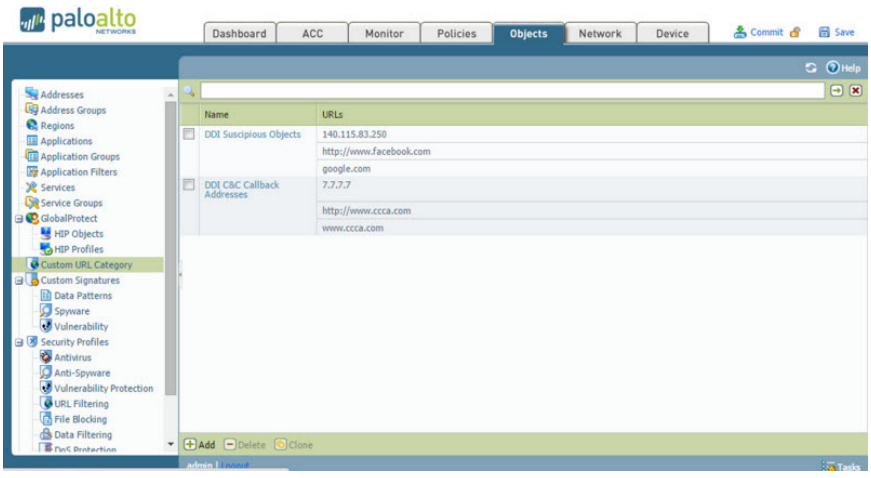
9. [保存] をクリックします。
10. PAN-OS 7.1 以降では、XML API アクセスを有効にします。
    a. Palo Alto 製品のコンソールで、[Device] > [Admin Roles] の順に選択し、管理者の役割を選択または作成します。
    b. [XML API] タブを選択します。
    c. リストから次の XML API の機能を有効にします。
       - Configuration
       - Operation Requests
       - Commit



d. [OK] をクリックします。

e. 管理者のアカウントに管理者の役割を割り当てます。

11. (オプション) Palo Alto 製品のコンソールで Deep Discovery Inspector から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するには、[Objects] > [Custom URL Category] の順に選択します。



Deep Discovery Inspector から配信された不審オブジェクトおよび C&C コールバックアドレスが表示されます。

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 Inspector で SAML の設定を行うと、組織のポータルにサインインしているユーザは、既存の Deep Discovery Inspector アカウントなしで Deep Discovery Inspector にシームレスにログオ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 Inspector) は、ID プロバイダのユーザ ID 情報を使用してユーザの認証と認可を行います。

Deep Discovery Inspector は、シングルサインオンに対応する次の ID プロバイダをサポートしています。

- Microsoft Active Directory フェデレーションサービス (AD FS) 4.0 または 5.0
- Microsoft Entra ID
- Okta

組織の環境に Deep Discovery Inspector のシングルサインオンの設定を行うには、次の手順を実行します。

1. Deep Discovery Inspector の管理コンソールにアクセスして、サービスプロバイダのメタデータファイルを取得します。

   Deep Discovery Inspector 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 Inspector 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 Inspector からサービスプロバイダメタデータを取得して、ID プロバイダに提供します。

[SAML 認証] 画面の [サービスプロバイダ] セクションに、次のサービスプロバイダ情報が表示されます。

- エンティティ ID: サービスプロバイダのアプリケーションを識別します。
- シングルサインオン URL: SAML アサーションの受信と解析を行うエンドポイント URL です (「Assertion Consumer Service」と呼ばれることもあります)。
- シングルサインアウト URL: SAML ログアウトプロセスを開始するエンドポイント URL です。
- 証明書: X.509 形式の暗号化証明書 (検証証明書) です。

[サービスプロバイダ] セクションでは、次の項目をクリックできます。

- メタデータのダウンロード: Deep Discovery Inspector のメタデータファイルをダウンロードします。メタデータファイルは、Active Directory フェデレーションサービス (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 Inspector 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 Inspector の証明書ファイルをダウンロードします。

- 更新: 新しい証明書を Deep Discovery Inspector 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 Inspector 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 Inspector 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 Inspector 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 の設定

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 Inspector へのユーザアクセス管理を可能にします。

ここでは Okta を SAML (2.0) ID プロバイダとして設定し、Deep Discovery Inspector で使用する方法について説明します。

Okta の設定を開始する前に、次のことを確認してください。

- サインインプロセスを処理して Deep Discovery Inspector 管理コンソールに認証資格情報を提供する、Okta の有効なライセンスを購入している。
- Deep Discovery Inspector の管理者として管理コンソールにログオンしている。

手順

1. 管理者権限のあるユーザとして Okta にログインします。
2. 画面右上にある [Admin] をクリックし、 [Applications] > [Applications] の順に選択します。
3. [Add Application] をクリックし、[Create New App] をクリックします。

[Create a New Application Integration] 画面が表示されます。

4. [Platform] に [Web] を、[Sign on method] に [SAML 2.0] を選択し、[Create] をクリックします。
5. [General Settings] 画面の [App name] に、「Deep Discovery Inspector」など Deep Discovery Inspector の名前を入力し、[Next] をクリックします。
6. [Configure SAML] 画面で、次を指定します。
   a. Deep Discovery Inspector の [Single sign on URL] を入力します。

      注意

      Deep Discovery Inspector のシングルサインオン URL を取得するには、Deep Discovery Inspector 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: `DDI_GROUP`
      - Filter: Matches `^(.*)*$`
   f. [次へ] 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 Inspector アプリケーションの [Sign On] タブが表示されます。
8. [Identity Provider Metadata] をクリックし、Okta からメタデータファイルをダウンロードします。

注意

このメタデータファイルを Deep Discovery Inspector にインポートします。

9. アプリケーションをグループに割り当て、人をグループに追加します。

   a. [Directory] > [Groups] の順に選択します。

   b. アプリケーションを割り当てるグループをクリックし、[Manage Apps] をクリックします。

      [Assign Applications] 画面が表示されます。

   c. 追加した Deep Discovery Inspector を探し、[Assign] をクリックします。

   d. [Manage People] をクリックします。

      [Add People to Groups] 画面が表示されます。

   e. Deep Discovery Inspector へのアクセスを許可するユーザを指定し、Deep Discovery Inspector グループに追加します。

   f. アプリケーションがユーザとグループに割り当てられていることを確認します。

      アプリケーションをグループに割り当てると、グループ内のすべてのユーザにアプリケーションが自動的に割り当てられます。

   g. 上記手順を繰り返し、必要に応じて他のグループにアプリケーションを割り当てます。

   これで、Okta を使用したシングルサインオンを設定し、必要な SAML グループを Deep Discovery Inspector 管理コンソールで作成できます。

Active Directory フェデレーションサービスを設定する

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 Inspector と連動させる方法について説明します。

注意

Deep Discovery Inspector では、AD FS 4.0 および 5.0 を使用したフェデレーションサーバへの接続がサポートされます。

Active Directory フェデレーションサービス (AD FS) は、Windows Server や Active Directory の技術に関連した要求対応の ID 管理ソリューションを提供します。AD FS では、WS-Trust、WS-Federation、および SAML (Security Assertion Markup Language) の各プロトコルがサポートされます。

AD FS の設定を開始する前に、次のことを確認してください。

- フェデレーションサーバとして機能する、AD FS 4.0 または AD FS 5.0 を搭載した Windows Server がある。
- Deep Discovery Inspector の管理者として管理コンソールにログオンしている。
- Deep Discovery Inspector からメタデータファイルを取得している。
- 各エンドポイントで Web ブラウザが Deep Discovery Inspector 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、327 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 Inspector から取得するメタデータファイルを選択します。次に [次へ] をクリックします。

c. [表示名の指定] タブで、「Deep Discovery Inspector」など Deep Discovery Inspector の表示名を指定し、[次へ] をクリックします。

d. [アクセス制御ポリシーの選択] タブで、[すべてのユーザーを許可] 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「`DDI_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 Inspector にインポートします。

AD FS を介したシングルサインオンについてエンドポイントを設定する

Active Directory フェデレーションサービス (AD FS) を介したシングルサインオンを使用して Deep Discovery Inspector にアクセスするには、Deep Discovery Inspector とフェデレーションサーバの両方を信頼するように各エンドポイントの Web ブラウザを設定します。

Web ブラウザの設定は、手動でもグループポリシーを介しても実行できます。

Windows 10 を実行するエンドポイントでの手順を以下に示します。この手順は、Windows のバージョンによって異なる可能性があります。

手順

1. エンドポイントで、[スタート] メニューから [コントロール パネル] を開きます。
2. [ネットワークとインターネット] > [インターネット オプション] の順にクリックします。

   [インターネットのプロパティ] 画面が表示されます。
3. [セキュリティ] タブをクリックします。
4. [ローカル イントラネット] を選択し、[サイト] をクリックします。
5. [Advanced] 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 Inspector の FQDN または IP アドレスを [Web サイト] リストに追加します。
8. [閉じる] をクリックします。
9. [OK] をクリックします。
10. [OK] をクリックします。

Microsoft Active Directory

[Microsoft Active Directory] 画面を使用して、Microsoft Active Directory サーバを Deep Discovery Inspector と統合します。その後、Deep Discovery Inspector 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。

Deep Discovery Inspector では、Microsoft Windows Server 2012 R2 以上がサポートされます。

Microsoft Active Directory との統合を設定する

注意

開始する前に、サーバ管理者から Active Directory との統合設定に必要な情報を取得します。

手順

1. [管理] > [統合製品/サービス] > [Microsoft Active Directory] の順に選択します。
2. [Microsoft Active Directory を使用] を選択します。
3. 次の設定を行います。

設定	説明
サーバの種類	接続先の Active Directory サーバの種類。 次のオプションを選択できます。 • Microsoft Active Directory • Microsoft Active Directory グローバルカタログ
サーバアドレス	Active Directory サーバの IP アドレスまたはパブリック FQDN。
暗号化	Deep Discovery Inspector と Active Directory サーバ間の通信においてデータを保護するために使用するプロトコル。 次のオプションを選択できます。 • SSL • STARTTLS

設定	説明

ポート	Active Directory サーバとの通信に使用するネットワークポート番号。
	
	注意
	次の初期設定のポートを使用することをお勧めします。
	• Microsoft Active Directory または OpenLDAP の場合:
	  • SSL: 636
	  • StartTLS: 389
	• Microsoft Active Directory グローバルカタログの場合:
	  • SSL: 3269
	  • STARTTLS: 3268

基本識別名	Deep Discovery Inspector がデータを同期する Active Directory 階層内の開始点。
ユーザ名	Active Directory サーバのユーザ名。
パスワード	ユーザアカウントに関連付けられているパスワード。

4. 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。
5. (オプション) [接続テスト] をクリックして、LDAP サーバへの接続を確認します。
6. [保存] をクリックします。

Syslog

Deep Discovery Inspector は、次のチャネルを介して Syslog サーバにログコンテンツを転送します。

- TCP (Transmission Control Protocol)

- SSL (Secure Sockets Layer) 暗号化を使用した TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Deep Discovery Inspector で、ログコンテンツを次の形式で送信するように設定します。

- CEF (Common Event Format)
- LEEF (Log Event Extended Format)
- TMEF (Trend Micro Event Format)

Syslog サーバの追加

最大 3 件の Syslog サーバを追加します。

手順

1. [管理] > [統合製品/サービス] > [Syslog] の順に選択します。
2. [追加] をクリックします。

   [Syslog サーバの追加] 画面が表示されます。
3. [Syslog サーバを有効にする] を選択します。
4. Syslog サーバのサーバ名または IP アドレスとポート番号を入力します。

   次の初期設定の Syslog ポートを使用することをお勧めします。

   - UDP: 514
   - TCP: 601
   - SSL: 6514
5. ファシリティを選択します。

   ファシリティは、メッセージの送信元を指定します。
6. Syslog の重大度 (Severity) を選択します。

   Syslog の重大度 (Severity) は、Syslog サーバに送信されるメッセージの種類を指定します。

表 6-19. Syslog の重大度 (Severity) レベル

レベル	重大度	説明
0	緊急	• 明らかなシステム障害 すぐに処理します。
1	重大	• 重大なシステム障害 すぐに処理します。
2	アラート	• 緊急性のある障害 すぐに処理します。
3	エラー	• 緊急性のない障害 できる限り速やかに問題を解決します。
4	警告	• 保留中のエラー エラー回避処理を行います。
5	通知	• 異常なイベント ただちに処理する必要はありません。
6	情報	• レポート、スループットの測定、およびその他の目的に役立つ通常動作に関するメッセージ 処理する必要はありません。
7	デバッグ	• アプリケーションのデバッグ時に役立つ情報 **注意** デバッグレベルを設定すると、負荷の高いネットワークでは大量の Syslog トラフィックが発生することがあります。注意して使用してください。

7. Syslog サーバにイベントログを送信する形式を選択します。

- CEF

  Common Event Format (CEF) は、Micro Focus ArcSight によって開発されたオープンなログ管理標準です。CEF は、標準のプレフィックス、およびキー/値のペアとして形式化された変数拡張から構成されます。

- LEEF

  Log Event Extended Format (LEEF) は、IBM QRadar Security Intelligence Platform のカスタマイズされたイベント形式です。LEEF は、LEEF ヘッダ、イベント属性、およびオプションの Syslog ヘッダから構成されます。

- Trend Micro Event Format (TMEF)

  Trend Micro Event Format (TMEF) は、トレンドマイクロ製品でイベント情報のレポートに使用される形式です。Deep Discovery Advisor は、TMEF を使用してさまざまなトレンドマイクロ製品のイベントを統合します。

8. Syslog サーバに送信するログを選択します。
9. [プロキシサーバを使用して接続する] を選択すると、[管理] > [システム設定] > [プロキシ] の設定を使用して Syslog サーバに接続します。

   インターネット接続にプロキシサーバを使用する場合は、このオプションを選択します。
10. [保存] をクリックします。

システム設定

Deep Discovery Inspector の基本設定を行うには、[管理] > [システム設定] の順に選択します。

ここで説明する内容には、次の基本設定が含まれます。

- 334 ページの「ネットワーク」
- 334 ページの「ネットワークインタフェース」
- 336 ページの「プロキシ」

- 337 ページの「SMTP」
- 338 ページの「SNMP」
- 341 ページの「HTTPS 証明書」
- 343 ページの「時間」
- 344 ページの「セッションタイムアウト」

ネットワーク

[ネットワーク] 画面では、TLS 1.2 以上の適用など、アプライアンスのネットワーク設定を管理できます。

[管理] > [システム設定] > [ネットワーク] の順に選択します。

ネットワーク設定の詳細については、19 ページの「アプライアンス IP の設定」を参照してください。

ネットワークインタフェース

[ネットワークインタフェース] 画面では、管理ポート、データポート、およびインラインポートを管理します。

詳細については、次の項目を参照してください。

- 335 ページの「データポートと管理ポート」
- 335 ページの「インラインポート」

注意

インラインポートはインライン (LAN Bypass) ネットワークインタフェースカードがインストールされた Deep Discovery Inspector でのみ使用できます (日本における本機能の提供は検討中です。最新の提供状況については、以下をご参照ください。http://www.go-tm.jp/ddi)。詳細については、「インライン (LAN Bypass) ネットワークインタフェースカード インストールガイド」を参照してください。

データポートと管理ポート

データおよび管理ネットワークインタフェースポートの管理の詳細については、24 ページの「ネットワークインタフェースのポートの管理」を参照してください。

[ネットワークインタフェース] 画面では、次の操作を実行できます。

- ポートのステータスの確認
- ポートのネットワークインタフェースの確認
- カプセル化されたリモートミラーリングの設定
- 復号された SSL トラフィック特定の設定

インラインポート

インラインポートはインライン (LAN Bypass) ネットワークインタフェースカードがインストールされた Deep Discovery Inspector でのみ使用できます。詳細については、「インストールガイド」および「インライン (LAN Bypass) ネットワークインタフェースカード インストールガイド」を参照してください。

Deep Discovery Inspector をインラインアプライアンスとして導入し、TLS トラフィックを復号するように設定している場合、システムクラッシュ、停電、その他の予期しない状況といったイベントによってネットワークアクセスが影響を受けることがあります。Deep Discovery Inspector では、トラフィックバイパスを使用して 2 つの物理ネットワークポートを相互接続します。トラフィックバイパスにより、Deep Discovery Inspector がネットワークの単一障害点とならないように防止できます。

トラフィックバイパスは、Deep Discovery Inspector で自動的に有効にすることも、管理者が手動で有効にすることもできます。

- 自動でのトラフィックバイパス

  Deep Discovery Inspector では自己ヘルスチェックが実行されます。問題が検出されると、Deep Discovery Inspector は自動的にトラフィックバイパスモードに入り、ネットワークに影響が及ばないように防止します。このような状況が発生した場合、管理コンソールにグローバル通知が表示されるとともに、設定している場合は Deep Discovery Inspector からメール通知または SNMP トラップを送信できます。

重要

停電、システムハング、カーネルパニックなどの問題が発生した場合、Deep Discovery Inspector からメール通知や SNMP トラップを送信できないことがあります。その際は、NMS やシステム監視などのツールを使用して問題を特定することをお勧めします。

- 手動でのトラフィックバイパス

  トラフィックバイパスモードを手動で有効にできます。トラフィックバイパスモードを有効にするには、[管理] > [システム設定] > [ネットワークインタフェース] の順に選択して、[手動のトラフィックバイパスを有効にする] を切り替えます。

  事前設定コンソールでトラフィックバイパスモードを有効にすることもできます。詳細については、「インストールガイド」を参照してください。

プロキシ

次の操作を実行するためにプロキシサーバを設定します。

- トレンドマイクロのアップデートサーバやその他のアップデート元からのアップデートのダウンロード
- 製品ライセンスのアップデート
- 他のトレンドマイクロ製品 (Deep Discovery Director、Apex Central、および Smart Protection Server) への接続

プロキシサーバの設定

プロキシサーバは、パターンファイル、エンジン、およびライセンスのアップデートに使用できます。他の製品およびサービスが同じプロキシサーバを使用することもできます。各製品またはサービスの設定ページでプロキシサーバ設定を有効にする必要があります。

手順

1. [管理] > [システム設定] > [プロキシ] の順に選択します。

2. [コンポーネントとライセンスのアップデートにプロキシサーバを使用する] を選択します。
3. [サーバアドレス] と [ポート] 番号を入力します。

注意

Deep Discovery Inspector では、HTTP プロキシサーバおよび HTTPS プロキシサーバがサポートされます。

4. プロキシサーバで認証が必要な場合は、[プロキシサーバの認証を使用] を選択して [ユーザ名] と [パスワード] を指定します。
5. [接続のテスト] をクリックして接続設定を確認します。
6. [保存] をクリックします。

SMTP

Simple Mail Transfer Protocol (SMTP) は、メール通知やレポートの送信に使用されます。

SMTP を設定する

手順

1. [通知およびレポートの送信に SMTP サーバを使用] を有効にします。
2. SMTP サーバの有効なアドレスとポート番号を入力します。
3. [接続のセキュリティ] を選択します。
4. [送信者のメールアドレス] を入力します。
5. SMTP サーバの接続に認証が必要な場合は、認証設定を指定します。

重要

Deep Discovery Inspector の IP アドレスを SMTP リレーリストに追加します。

注意

Deep Discovery Inspector では、LOGIN、PLAIN、および CRAM-MD5 の SMTP 認証がサポートされます。

a. [SMTP サーバの認証を使用] を有効にします。

b. ユーザ名とパスワードを入力します。

6. [保存] をクリックします。

7. (オプション) SMTP サーバを使用してテストメールを送信します。

a. [テストメール] をクリックします。

b. [送信先メールアドレス] を入力します。

c. [OK] をクリックします。

SMTP サーバが正しく設定されている場合、Deep Discovery Inspector は送信先アドレスにテストメールメッセージを送信します。

SNMP

SNMP(Simple Network Management Protocol) は IP ネットワーク上のデバイスの管理に使用されます。Deep Discovery Inspector では、SNMP のバージョン 1、2 および 3 がサポートされます。

SNMP を有効にして、システムの実行ステータス、ネットワークカードのリンクアップやリンクダウン、およびコンポーネントのアップデートステータスを確認します。

SNMP には次の 2 つのモードがあります。

- SNMP トラップ

  SNMP トラップでは、管理下の製品のステータスを SNMP マネージャにレポートできます。

- SNMP エージェント

  SNMP エージェントは、製品に関する情報を収集して事前定義された階層に編成し、SNMP プロトコルを使用してクエリに応答するプログラムです。

SNMP エージェントを使用すると、次を含む Deep Discovery Inspector のシステム情報を取得できます。

- 製品バージョン
- CPU、メモリ、およびディスクの情報
- ネットワークインタフェースのスループットと同時接続数

SNMP トラップのモードの設定

次の表に、トラップモードの製品固有の SNMP OID を示します。

OID の値	OID の説明
.1.3.6.1.4.1.6101.999.2.2	重要なコンポーネントのアップデート失敗
.1.3.6.1.4.1.6101.3003.3.1	NTP の同期の失敗
.1.3.6.1.4.1.6101.3003.3.2	予期しないトラフィックバイパスモードへの移行

手順

1. [管理] > [システム設定] > [SNMP] の順に選択します。
2. [SNMP トラップメッセージの送信] を選択します。
3. マネージャのサーバのアドレスを指定します。
4. SNMP トラップのモードを設定します。
   - [SNMP v1/v2c] の場合は、コミュニティ名を指定します。
   - [SNMP v3] の場合は、セキュリティモデルを指定します。
     - 認証およびプライバシーなし: ユーザ名を指定します
     - 認証あり: ユーザ名とパスワードを指定します
     - 認証およびプライバシーあり: ユーザ名、パスワード、およびプライバシーパスフレーズを指定します。

5. [保存] をクリックします。

SNMP エージェントのモードの設定

SNMP マネージャを使用して Deep Discovery Inspector を監視できます。

次の表に、エージェントモードの製品固有の SNMP OID を示します。

OID の値	OID の説明
.1.3.6.1.4.1.6101.3003.1	製品のバージョン
.1.3.6.1.4.1.6101.3003.2	ネットワークインタフェースのスループット
1.3.6.1.4.1.6101.3003.4	同時接続数
.1.3.6.1.4.1.6101.3003.5	インラインネットワークカードのステータス

手順

1. [管理] > [システム設定] > [SNMP] の順に選択します。
2. [SNMP マネージャからの要求を待機] を選択します。
3. 必要に応じて、[システムの場所] と [管理者管理者の連絡先] を入力します。
4. SNMP エージェントのモードを設定します。
   - [SNMP v1/v2c] の場合:
     a. 許可するコミュニティ名を入力します。
     b. 信頼するマネージャのサーバアドレスを入力します。
   - [SNMP v3] の場合は、セキュリティモデルを指定します。
     - 認証およびプライバシーなし: ユーザ名を指定します
     - 認証あり: ユーザ名とパスワードを指定します

- 認証およびプライバシーあり: ユーザ名、パスワード、およびプライバシーパスフレーズを指定します。

5. [保存] をクリックします。
6. 必要に応じて、 [MIB のダウンロード] をクリックします。

   MIB ファイルを SNMP マネージャにインポートできます。

HTTPS 証明書

HTTPS 証明書の詳細が正しいことを確認します。

表 6-20. HTTPS 証明書の詳細

項目	説明
バージョン	証明書のバージョン番号
シリアル番号	証明書の一意の識別番号
署名アルゴリズム	署名を作成するために使用するアルゴリズム
発行元	情報を確認して証明書を発行したエンティティ
発効日	証明書が最初に有効になった日付
失効日	証明書の有効期限
件名	識別される個人またはエンティティ
公開鍵	暗号化に使用される 2048 ビット以上の公開鍵

HTTPS 証明書の生成

Deep Discovery Inspector は、次の形式の HTTPS をサポートしています。

- X509 PEM

手順

1. Linux OS で、次のコマンドを使用して証明書を生成します。(実際のコマンド入力画面では、改行は不要です)

```
openssl req -newkey rsa:2048 -x509 -sha512 -days 365 -nodes
-out server.pem -keyout server.pem
```

2. 次の値を指定します。
   - 国名 (2 文字のコード)
   - 都道府県名 (フルネーム)
   - 地域名 (市区町村など)
   - 組織名 (会社名など)
   - 部署名 (部、課など)
   - 一般名 (ユーザ名やサーバのホスト名など)
   - メールアドレス
3. <Enter> キーを押します。

   `server.pem` というファイルが生成されます。
4. `server.pem` ファイルを保存して、Deep Discovery Inspector に HTTPS 証明書としてインポートします。

   詳細については、343 ページの「HTTPS 証明書のインポート」を参照してください。
5. (オプション) HTTPS 証明書が正常にインポートされたことを確認するには、次の手順を実行します。
   a. [管理] > [システムログ] の順に選択します。
   b. HTTPS 証明書をインポートした日付が含まれる期間を選択します。
   c. [ログの種類] で [システムイベント] を選択します。

      正常にインポートされていると、次のログがリストに表示されます。

      証明書のインポート: 新しい証明書のインポートが正常に完了しました。

HTTPS 証明書のインポート

ブラウザでセキュリティ問題が発生する可能性を排除するため、Deep Discovery Inspector の初期設定のセキュリティ証明書を、信頼できる証明機関からインポートしたセキュリティ証明書に置き換えます。

Deep Discovery Inspector は、次の形式の HTTPS をサポートしています。

- X509 PEM

手順

1. [管理] > [システム設定] > [HTTPS 証明書] の順に選択します。
2. [HTTPS 証明書] 画面の [証明書の置換] をクリックします。

   [証明書のインポート] 画面が表示されます。
3. [証明書のインポート] 画面で [参照] をクリックし、新しい証明書を選択します。
4. [インポート] をクリックします。

   新しい証明書がインポートされます。
5. 別のブラウザから Deep Discovery Inspector にログオンして、新しい証明書を確認します。

   注意

   Deep Discovery Inspector を再起動する必要はありません。

時間

システム時刻を NTP (Network Time Protocol) サーバと同期するか、手動で設定します。

時刻オプションの設定

手順

1. [管理] > [システム設定] > [時間] の順に選択します。
2. [システム時間の設定] で、次のいずれかの方法を選択します。
   - アプライアンスの時刻を NTP サーバと同期する:
     a. NTP サーバのアドレスを入力します。
     b. [今すぐ同期] をクリックします。

     注意
     Deep Discovery Inspector 仮想アプライアンスの場合、NTP サーバを使用してアプライアンスの時刻を同期することをお勧めします。
   - システム時間を手動で設定する:
     a. カレンダアイコンをクリックするか、yyyy/mm/dd の形式で年、月、日を入力します。
     b. 時、分、秒を選択します。
3. [タイムゾーン] ドロップダウンメニューを使用して、タイムゾーンを選択します。
4. [保存] をクリックします。

セッションタイムアウト

使用されていない管理コンソールユーザセッションをログアウトするまでの Deep Discovery Inspector の待機時間を設定します。

セッションタイムアウトの設定

手順

1. [管理] > [システム設定] > [セッションタイムアウト] の順に選択します。

2. [タイムアウト設定] で、使用されていないセッションをログアウトするまでの時間を選択します。
   - 2 分
   - 5 分
   - 10 分
   - 15 分 (推奨)
   - 30 分
   - 60 分
   - 1 日
   - 3 日
3. [保存] をクリックします。

注意

管理コンソールのタイムアウトの初期設定は 15 分です。

アカウント

ここで説明する内容には、次の項目が含まれます。

- 346 ページの「アカウントについて」
- 347 ページの「ユーザの役割とメニュー項目の権限」
- 350 ページの「ローカルアカウントの追加」
- 351 ページの「Active Directory アカウントの追加」
- 354 ページの「アカウントの編集」
- 356 ページの「アカウントパスワードのリセット」
- 357 ページの「アカウントの削除」
- 357 ページの「アカウントのロック解除」

アカウントについて

Deep Discovery Inspector では、管理コンソールの選択されたセクションに対してアクセス権を付与できます。

重要

「Trend Vision One 管理者」および「Trend Vision One 閲覧者」アカウントを無効化または変更することはできません。

Deep Discovery Inspector では、次の役割を含めた 128 件のローカルアカウント、512 件の Active Directory アカウント、および 512 件の SAML アカウントがサポートされます。

- システム管理者 (初期設定)
- 管理者 (ユーザが作成)
- 閲覧者 (ユーザが作成)

すべてのユーザ (システム管理者、その他の管理者、閲覧者) は 1 つのダッシュボードを共有します。管理コンソールの閲覧者アカウントのそれぞれで、部分的に独立したダッシュボードが提供されます。任意のアカウントのダッシュボードを変更すると、他のアカウントのダッシュボードに影響します。

Deep Discovery Inspector では、すべてのユーザの次のアクティビティをログに記録します。

- ログオン
- アカウントパスワードの変更
- ログオフ
- セッションタイムアウト

各ユーザの状態は次のように表示されます。

- オンライン: 緑色
- オフライン: 灰色

Deep Discovery Inspector では、Trend Micro Apex Central から Deep Discovery Inspector にログインするユーザが表示されます。

作成者	例
Deep Discovery Inspector	SYSTEM
Deep Discovery Inspector のユーザ名	admin
Trend Micro Apex Central のユーザ名	admin(admin)

ユーザの役割とメニュー項目の権限

ユーザにはそれぞれ特定の役割が割り当てられます。役割によって、ユーザがアクセスできる管理コンソールのメニュー項目が決まります。

表 6-21. ユーザの役割

役割	説明
システム管理者	管理コンソールのすべてのセクションにアクセスします。
管理者	管理コンソールのすべてのセクションにアクセスします。
閲覧者	検出とシステム情報を表示します。

権限によって、管理コンソール上の各メニュー項目にアクセスできるレベルが決まります。Deep Discovery Inspector の権限を次に示します。

- 設定: メニュー項目へのフルアクセスが可能

  ユーザはすべての設定、すべてのタスクの実行、およびデータの表示ができます。

- 表示: 設定、タスク、およびデータの表示のみ可能
- アクセス拒否: メニュー項目が表示されない

セクション	サブセクション	システム管理者	管理者	閲覧者
ダッシュボード	適用外	設定	設定	設定 除外: ネットワークグループ、登録済みドメイン、および登録済みサービスへの IP アドレスの追加
検出	影響を受けたホスト	設定	設定	設定 除外: 設定 ネットワークグループ、登録済みドメイン、および登録済みサービスへの IP アドレスの追加
	注意すべきイベント発生ホスト	設定	設定	設定 除外: ネットワークグループ、登録済みドメイン、および登録済みサービスへの IP アドレスの追加
	C&C コールバックアドレス	設定	設定	アクセス拒否
	不審オブジェクト	設定	設定	アクセス拒否
	Retro Scan	設定	設定	表示

セクション	サブセクション	システム管理者	管理者	閲覧者
	すべての検出	設定	設定	設定 除外: ネットワークグループ、登録済みドメイン、および登録済みサービスへの IP アドレスの追加
レポート	予約レポート	表示	表示	表示
	スケジュール	設定	設定	表示
	手動レポート	設定	設定	表示
	カスタマイズ	設定	設定	表示
管理	すべて	設定	設定	アクセス拒否
	アカウント	設定	設定 除外: • システム管理者のパスワードのリセット • システム管理者の編集	
	システムログ	表示	表示	
	システムのメンテナンス	設定	設定	
ヘルプ	すべて	表示	表示	表示
ユーザアカウント	パスワードの変更	設定	設定	設定

セクション	サブセクション	システム管理者	管理者	閲覧者
	ログオフ	表示	表示	表示

ローカルアカウントの追加

手順

1. [管理] > [アカウント] の順に選択します。
2. [ローカル] タブをクリックします。
3. [追加] をクリックします。

   [ローカルアカウントの追加] 画面が表示されます。
4. アカウントのステータスを設定します。
   - 有効 (初期設定)
   - 無効

   注意
   ユーザは自身のアカウントを無効にできません。
5. [種類] が [ローカルユーザ] であることを確認します。
6. ユーザ名を 4〜32 文字の英数字で入力します。

   注意
   ユーザ名には次の特殊文字を使用できます。
   - アンダースコア (_)
   - ピリオド (.)
   - ハイフン (-)
7. ユーザの役割を選択します。

- 閲覧者 (初期設定)
- 管理者

8. (オプション) 閲覧者アカウントで [検出を解決済みに設定することをユーザに許可する] を選択します。

   詳細については、109 ページの「すべての検出の表示」を参照してください。

   注意

   初期設定では、[検出を解決済みに設定することをユーザに許可する] は選択解除されています。

9. [保存] をクリックします。

   ローカルアカウントリストにアカウント情報が追加され、初期設定のアカウントパスワードが生成されます。

   ヒント

   パスワードの表示/非表示を切り替えるには、パスワードの表示アイコン (◎) をクリックします。

次に進む前に

生成された初期設定のパスワードを新規ユーザに提供します。ユーザは、はじ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。詳細については、16 ページの「管理コンソールのアカウントのパスワード」を参照してください。

Active Directory アカウントの追加

手順

1. [管理] > [アカウント] の順に選択します。
2. [Active Directory] タブをクリックします。

3. [追加] をクリックします。

   [Active Directory ユーザ/グループの追加] 画面が表示されます。

4. アカウントのステータスを設定します。

   - 有効 (初期設定)
   - 無効

   注意
   ユーザは自身のアカウントを無効にできません。

5. アカウントの [種類] に [Active Directory ユーザまたはグループ] を選択します。

6. 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、Active Directory の一致するユーザアカウントまたはグループを探します。

   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 Active Directory サーバで指定されていない
   - ユーザアカウントが Active Directory サーバで無効になっている

7. 追加する Active Directory のユーザアカウントまたはグループを選択します。

8. ユーザの役割を選択します。

   - 閲覧者 (初期設定)
   - 管理者

9. (オプション) 閲覧者アカウントで [検出を解決済みに設定することをユーザに許可する] を選択します。

   詳細については、109 ページの「すべての検出の表示」を参照してください。

注意

初期設定では、[検出を解決済みに設定することをユーザに許可する] は選択解除されています。

10. [保存] をクリックします。

    新しいアカウントが Active Directory アカウントリストに追加されます。

SAML アカウントの追加

注意

ユーザの検出フィルタと生成されたレポートを Active Directory アカウントから SAML アカウントに転送するには、SAML アカウントを作成してユーザを SAML アカウントにログインさせてから、ユーザの Active Directory アカウントを削除します。

手順

1. [管理] > [アカウント] の順に選択します。
2. [SAML] タブをクリックします。
3. [追加] をクリックします。

   [SAML アカウントの追加] 画面が表示されます。
4. アカウントのステータスを設定します。

注意

ユーザは自身のアカウントを無効にできません。

5. クレーム値を入力します。

注意

クレーム値は、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。

6. (オプション) アカウントの説明を入力します。
7. ユーザの役割を選択します。
   - 閲覧者 (初期設定)
   - 管理者
8. (オプション) 閲覧者アカウントで [検出を解決済みに設定することをユーザに許可する] を選択します。

   詳細については、109 ページの「すべての検出の表示」を参照してください。

   注意

   初期設定では、[検出を解決済みに設定することをユーザに許可する] は選択解除されています。
9. [保存] をクリックします。

   新しいアカウントが SAML アカウントリストに追加されます。

アカウントの編集

アカウントを編集できるのは管理者のみです。管理者は、アカウントの追加と、システム管理者のアカウントを除く管理者アカウントの編集や削除を実行できます。管理者は自身のアカウントのパスワードを変更できますが、そのアカウントを編集したり削除したりすることはできません。

手順

1. [管理] > [アカウント] の順に選択します。
2. アカウントの種類のタブをクリックします。
   - ローカル
   - Active Directory
   - SAML
3. アカウントのステータスを設定します。

- 有効 (初期設定)
- 無効

4. (オプション) ローカルアカウントのパスワードをリセットするには、次の操作を実行します。

重要

[リセット] をクリックする前に、対象アカウントを正しく選択していることを確認してください。

a. 対象アカウントの [パスワードのリセット] 列にある [リセット] をクリックします。

アカウントのパスワードがただちにリセットされ、新しい初期設定パスワードが生成されます。

b. 生成された初期設定のパスワードをユーザに提供します。ユーザは、はじ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。詳細については、16 ページの「管理コンソールのアカウントのパスワード」を参照してください。

5. ユーザ名をクリックします。

[アカウントの編集] 画面が表示されます。

6. ユーザの役割を選択します。

- 閲覧者 (初期設定)
- 管理者

7. (オプション) 閲覧者アカウントで [検出を解決済みに設定することをユーザに許可する] を選択します。

詳細については、109 ページの「すべての検出の表示」を参照してください。

注意

初期設定では、[検出を解決済みに設定することをユーザに許可する] は選択解除されています。

8. [保存] をクリックします。

   [アカウント] 画面の表内のアカウント情報が更新されます。

アカウントパスワードのリセット

システム管理者は各ローカルアカウントのパスワードをリセットできます。その他の管理者は、システム管理者のアカウントを除くローカルアカウントのパスワードをリセットできます。

重要

Microsoft Active Directory アカウント、SAML アカウント、および Trend Micro Apex Central シングルサインオン (SSO) アカウントのパスワードは管理コンソールからは変更できません。

手順

1. [管理] > [アカウント] の順に選択します。
2. [ローカル] タブをクリックします。

   重要

   [リセット] をクリックする前に、正しいアカウントを選択していることを確認してください。

3. 対象アカウントの [パスワードのリセット] 列にある [リセット] をクリックします。

   アカウントのパスワードがただちにリセットされ、新しい初期設定パスワードが生成されます。

   ヒント

   パスワードの表示/非表示を切り替えるには、パスワードの表示アイコン (◎) をクリックします。

次に進む前に

生成された初期設定のパスワードをユーザに提供します。ユーザは、はじ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。詳細については、16 ページの「管理コンソールのアカウントのパスワード」を参照してください。

アカウントの削除

管理者は、システム管理者アカウント、ログオンアカウント、ログオンアカウントを含む Active Directory および SAML グループアカウントを除く任意のアカウントを削除できます。

重要

アカウントが削除されると、そのアカウントで保存された検索条件フィルタや作成されたレポートのスケジュールも削除されます。ただし、生成されたレポートは削除されません。

手順

1. [管理] > [アカウント] の順に選択します。
2. アカウントの種類のタブをクリックします。
3. ユーザ名の横にあるチェックボックスをオンにします。
4. [削除] をクリックします。

重要

[削除] をクリックする前に、対象アカウントを正しく選択していることを確認してください。

アカウントのロック解除

ログインに 5 回失敗すると、ローカルアカウントが自動的にロックされます。ロックされたアカウントは 10 分後に自動的にロック解除されます。アカウントを手動でロック解除するには、次の手順を実行します。

手順

1. ロックされていない管理者アカウントを使用して、Deep Discovery Inspector 管理コンソールにログインします。
2. [管理] > [アカウント] の順に選択します。
3. [ローカル] タブをクリックします。
4. アカウントのロック状態が [ロックの有無] 列に表示されます。
5. いちばん左の列で、ロック解除する各アカウントを選択します。
6. [ロック解除] をクリックします。

   [アカウントのロック解除] 画面に、どのアカウントがロック解除されたか表示されます。
7. [アカウントのロック解除] 画面で [閉じる] をクリックします。

システムログ

Deep Discovery Inspector では、コンポーネントのアップデートやアプライアンスの再起動など、システムイベントをまとめたシステムログが保存されます。

これらのログは、Deep Discovery Inspector のデータベースまたは Syslog サーバに保存されます。

ログデータベースから情報を収集するには、ログのクエリを実行します。クエリで問い合わせたログは、.csv ファイルにエクスポートします。

詳細については、358 ページの「システムログのクエリ」を参照してください。

システムログのクエリ

Deep Discovery Inspector は、システムイベントやコンポーネントのアップデート結果をシステムログに保存します。

Deep Discovery Inspector 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。

手順

1. [管理] > [システムログ] の順に選択します。
2. ログの種類を選択します。
   - すべて
   - システムイベント
   - アップデートイベント

   イベントには次の情報が自動的に表示されます。

列	説明
タイムスタンプ	イベントの日時
ログの種類	次のいずれかのオプションが表示されます。 • すべて • システムイベント • アップデートイベント
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	次のいずれかのイベント結果が表示されます。 • 成功 • 失敗

列	説明
アカウント	アカウントによるアクティビティ 次のアカウントの種類についての情報が表示されます。 • Deep Discovery Inspector のユーザ名 例: `johnadmin` • Deep Discovery Inspector システム 例: `SYSTEM` • Trend Micro Apex Central のユーザ名 例: `admin(admin)` • Trend Micro Apex Central システム 例: `admin(SYSTEM)`
IP アドレス	イベントの IP アドレス
説明	イベントの詳細

3. 期間を指定するか、カレンダアイコンをクリックして特定の日時を選択します。

4. [エクスポート] をクリックして、システムログを.CSV ファイルにエクスポートします。

システムのメンテナンス

次の操作を実行するには、[システムのメンテナンス] を選択します。

- 360 ページの「ストレージ管理」
- 362 ページの「バックアップ/復元」
- 367 ページの「電源オフ/再起動」

ストレージ管理

[ストレージ管理] 画面を使用して、次の操作を実行します。

- ログおよびレポートのストレージの管理
- Deep Discovery Inspector データベースのステータスの表示
- 破損したデータベースファイルの修復

Deep Discovery Inspector では、ログとレポートをアプライアンスのハードディスクで管理しています。条件を設定してログを表示するには、53 ページの検出および 358 ページの「システムログのクエリ」を参照してください。

ハードディスクの空き容量を確保するには、ログとレポートを定期的に手動で削除します。削除のスケジュールは、ご使用の環境と、保持するログおよびレポートの量によって異なります。

ログとレポートのストレージがディスクの最大容量を超えると、Deep Discovery Inspector では、最新のログを保持できる容量になるまで、日付が古いものから順にログが自動的に削除されます。

注意

Deep Discovery Inspector の Syslog サーバまたは Apex Central にログを送信できます。詳細については、330 ページの「Syslog」および 278 ページの「Apex Central への登録」を参照し てください。

ストレージ管理の実行

手順

1. [管理] > [システムのメンテナンス] > [ストレージ管理] の順に選択します。
2. [ログ/レポートの削除] で、削除するログを選択します。
3. 削除処理を選択します。
   - 選択したログをすべて削除する
   - 選択したログで次の日数を経過したものを削除する

   注意

   ログは 121 日後に、PCAP ファイルは 16 日後に自動的に削除されます。

4. [削除] をクリックします。

製品データベースの管理の実行

手順

1. [管理] > [システムのメンテナンス] > [ストレージ管理] の順に選択します。
2. [ログデータベースのステータス] で [データベースのステータスの確認] をクリックします。
3. (オプション) データベースファイルが破損している場合は、[修復] をクリックします。

   Deep Discovery Inspector によって破損したファイルが修復され、修復処理の完了時、データベースのステータスが表示されます。

ファイルサイズの設定

Deep Discovery Inspector によって検出されたファイルで最大サイズを超えるものは破棄されます。

仮想アナライザへのファイルの送信を有効にすると、最大ストレージファイルサイズが自動的に 15MB に増大します。

手順

1. [管理] > [システムのメンテナンス] > [ストレージ管理] の順に選択します。
2. [ファイルサイズの設定] で、ファイルの最大サイズを指定します。
3. [保存] をクリックします。

バックアップ/復元

設定には、Deep Discovery Inspector とネットワークの両方の設定が含まれます。設定は暗号化ファイルにエクスポートすることでバックアップできます。このファイルを必要に応じてインポートして、設定を復元します。

Deep Discovery Inspector は、製品出荷時の初期設定を復元することでリセットできます。

次の設定はバックアップできません。

- アプライアンス IP の設定
- Apex Central の設定
- ダッシュボード (ウィジェット) の設定
- Deep Discovery Director の設定
- ライセンスとアクティベーションコード
- Mitigation デバイスの設定
- ネットワークインタフェースの設定
- Retro Scan の設定
- SAML 認証の設定
- Sandbox as a Service の設定
- [Web レピュテーション] 画面での Smart Protection の設定
- Threat Investigation Center の設定
- [インスペクション設定] 画面での TLS トラフィックインスペクション機能を有効にするための TLS トラフィックインスペクションの設定
- Trend Vision One の設定
- [証明書の管理] 画面での署名証明書の設定
- [ファイル送信] および [パスワード] 以外の仮想アナライザの設定

注意

設定の復元後、仮想アナライザは無効になります。

- HTTPS 証明書

ヒント

設定ファイルのインポート後は、上記のすべての設定を確認してください。

注意

- 暗号化ファイルは変更できません。
- 暗号化ファイルをインポートすると、そのファイルに含まれている設定はすべて上書きされますが、現在の設定のすべてが上書きされるということではありません。

  たとえば、バックアップ設定を Deep Discovery Inspector の以前のバージョンから復元する際、そのバージョンに含まれない機能は上書きされません。これは該当する設定が Deep Discovery Inspector の以前のバージョンにはなく、バックアップに含まれないためです。
- 別の Deep Discovery Inspector で設定を複製するために、暗号化ファイルを使用することもできます。

ファイルの設定のバックアップ

手順

1. [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択します。
2. [設定のバックアップ] で、[バックアップ] をクリックします。

   ファイルダウンロード画面が表示されます。
3. [保存] をクリックしてファイルの保存先を参照し、もう一度 [保存] をクリックします。

   暗号化されたバックアップファイルが保存されます。

ファイルの設定をインポートする

Deep Discovery Inspector 6.8 では、6.6、6.7、6.8 のバックアップファイルのみを復元できます。また Deep Discovery Inspector では、同じ言語バージョ

ンを使用する Deep Discovery Inspector アプライアンスのバックアップファイルのみを復元できます。

手順

1. ファイルをインポートする前に、現在の設定をバックアップします。詳細については、364 ページの「ファイルの設定のバックアップ」を参照してください。
2. [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択します。
3. [設定の復元] で、暗号化したバックアップファイルの場所を参照します。

   [アップロードするファイルの選択] 画面が表示されます。
4. インポートする暗号化ファイルを選択して、[設定の復元] をクリックします。

   確認メッセージが表示されます。
5. [OK] をクリックします。

   設定ファイルがインポートされ、整合性が確認された後、Deep Discovery Inspector が再起動されます。

   重要

   - 設定ファイルのインポート後、Deep Discovery Inspector では仮想アナライザが無効になります。
   - パスワード情報を含んでいる設定ファイルが壊れた場合、管理コンソールのパスワードがリセットされることがあります。

     指定したパスワードで管理コンソールにサインインできない場合は、代わりに初期設定のパスワード (`admin`) を使用してください。
6. 仮想アナライザを手動で有効にするには、[管理] > [仮想アナライザ] > [セットアップ] の順に選択します。

初期設定の復元

重要

初期設定を復元すると、アプライアンスのネットワーク設定や製品ライセンスを含めたすべての設定がリセットされます。

手順

1. 設定を復元する前に、現在の設定をバックアップします。詳細については、364 ページの「ファイルの設定のバックアップ」を参照してください。
2. [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択します。
3. [初期設定] で [初期設定にリセットする] をクリックします。

   確認メッセージが表示されます。
4. [OK] をクリックします。

   初期設定の復元後、Deep Discovery Inspector が再起動します。
5. 再起動したら 1 分間待ってから管理コンソールにログオンしてください。

ヒント

事前設定コンソールを使用してアプライアンスのネットワーク設定を変更するか、初期設定の IP アドレス (192.168.252.1/24) で管理コンソールにアクセスします。

注意

Deep Discovery Inspector の起動時には、設定ファイルの整合性が確認されます。パスワード情報を含んでいる設定ファイルが壊れた場合、管理コンソールのパスワードがリセットされることがあります。指定したパスワードで管理コンソールにログオンできない場合は、初期設定のパスワード (`admin`) を使用してログオンします。

電源オフ/再起動

[電源オフ/再起動] 画面には、Deep Discovery Inspector アプライアンスと関連サービスの電源オフや再起動を行うためのオプションがあります。

注意

Deep Discovery Inspector の起動時には、設定ファイルの整合性が確認されます。パスワード情報を含んでいる設定ファイルが壊れた場合、管理コンソールのパスワードがリセットされることがあります。指定したパスワードで管理コンソールにログオンできない場合は、初期設定のパスワード (`admin`) を使用してログオンします。

Deep Discovery Inspector の再起動

手順

1. [管理] > [システムのメンテナンス] > [電源オフ/再起動] の順に選択します。
2. [再起動] をクリックします。
   - サービスを再起動するには、[サービス] をクリックします。
   - Deep Discovery Inspector を再起動するには、[システム] をクリックします。
3. (オプション) [コメント] に、システムまたはサービスを再起動する理由を入力します。

4. [OK] をクリックします。

Deep Discovery Inspector の電源オフ

手順

1. [管理] > [システムのメンテナンス] > [電源オフ/再起動] の順に選択します。
2. [電源オフ] をクリックします。
3. (オプション) [コメント] に、Deep Discovery Inspector の電源をオフにする理由を入力します。
4. [OK] をクリックします。

ライセンス

[ライセンス] 画面にはライセンス情報が表示され、Deep Discovery Inspector と Sandbox as a Service の有効なアクティベーションコードを入力できます。

Deep Discovery Inspector の体験版のライセンスでは、次のウィジェット画面に表示される情報の一部が制限されます。

- 検索されたすべてのトラフィック
- 不正なネットワークアクティビティ
- 検索された不正トラフィック
- 過去 30 日間の監視対象のネットワークトラフィック
- リアルタイム検索されたトラフィック
- 仮想アナライザ

アクティベーションコード

有効なアクティベーションコードを使用して、Deep Discovery Inspector と Sandbox as a Service を有効にします。Deep Discovery Inspector と Sandbox as a Service は、アクティベーションが完了するまで操作できません。

アクティベーションコードはハイフンを含んだ 37 文字のコードで、次のように表示されます。

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

アクティベーションコードではなくレジストレーションキーを受け取った場合は、そのキーを使用して、次のサイトで Deep Discovery Inspector を登録します。

https://clp.trendmicro.com/

レジストレーションキーはハイフンを含んだ 22 文字のキーで、次のように表示されます。

xx-xxxx-xxxx-xxxx-xxxx

登録後、アクティベーションコードが記載されたメールメッセージが届きます。

製品バージョン

トレンドマイクロが提供するアクティベーションコードは、製品のバージョンに関連付けられています。

- 体験版: 製品のすべての機能が含まれます。

  製品版にいつでもアップグレードできます。

- 製品版: 製品のすべての機能とテクニカルサポートが含まれます。

  ライセンスの有効期限の終了後には更新猶予期間があります。更新猶予期間の長さはライセンスによって異なります。更新猶予期間の長さを確認するには、トレンドマイクロのテクニカルサポートにお問い合わせください。有効期限が終了する前に、メンテナンス更新を購入してライセンスを更新してください。

Deep Discovery Inspector のライセンスの有効期限

ライセンス情報は [ライセンス] 画面に表示されます。ライセンスの更新方法について確認するには、[ライセンスの更新方法を確認] をクリックします。

ライセンス情報には、ライセンスの有効期限が近づいていることや、有効期限が終了したことを知らせるメッセージも表示されます。

表 6-22. ライセンスの有効期限に関するメッセージ

バージョン	メッセージ
体験版	ライセンスの有効期限が表示されます。
製品版	• 有効期限が終了する 60 日前にメッセージが表示されます。 • 更新猶予期間が終了する 30 日前にメッセージが表示されます。 • 有効期限が終了し、更新猶予期間が過ぎたときにメッセージが表示されます。

製品版にアップグレードしない場合は、次のようになります。

表 6-23. ライセンスの有効期限が終了した場合

ライセンスの種類とステータス	結果
体験版 (有効期限終了)	Deep Discovery Inspector は、次の機能を無効にします。 • コンポーネントのアップデート • 検索 • TLS トラフィックインスペクション • 仮想アナライザのサンプル分析
製品版 (有効期限終了)	テクニカルサポートとコンポーネントのアップデートを利用できなくなります。 Deep Discovery Inspector は、古いコンポーネントを使用してネットワークを監視します。これらのコンポーネントでは最新の脅威からネットワークを十分に保護できない可能性があります。

ライセンスのアクティベートまたは更新

手順

1. [管理] > [ライセンス] の順に選択します。
2. Deep Discovery Inspector をアクティベートします。
   a. [Deep Discovery Inspector] で [新しいアクティベーションコード] をクリックします。

[新しいアクティベーションコード] 画面が表示されます。

b. 新しいアクティベーションコードを入力し、[保存] をクリックします。

[Trend Micro License Agreement] が表示されます。

c. 使用許諾契約を読んで、[同意する] をクリックします。

Deep Discovery Inspector をアクティベートすると、[セットアップガイド] が表示されます。

d. [セットアップガイド] の手順を実行します。

3. (オプション) Sandbox as a Service をアクティベートします。

注意

このオプションは、サポートされる Deep Discovery Inspector モデルでのみ表示されます。

---

a. [Sandbox as a Service] で、[新しいアクティベーションコード] をクリックします。

[新しいアクティベーションコード] 画面が表示されます。

b. 新しいアクティベーションコードを入力し、[保存] をクリックします。

4. (オプション) [ライセンス] 画面で、ライセンスの有効期限の横にある [更新] をクリックして、ライセンスの詳細を更新します。

5. (オプション) ライセンスの詳細情報は、サポート契約ポータルの Web サイトでも確認できます。表示するには、[詳細の表示] をクリックします。

6. (オプション) 製品について使用許諾契約を表示するには、`https://<Deep Discovery Inspector の IP アドレス>/html/eula.htm` に移動します。

注意

Deep Discovery Inspector には 1 つ以上のサードパーティ製コンポーネントが含まれるか同梱されていることがあります。一部のコンポーネントはオープンソースのソフトウェアであるか他の同様のライセンス契約が必要であり、トレンドマイクロのライセンス契約で定めた内容とは異なるライセンス契約条項、条件、制限、および権利の放棄の対象となる場合があります。詳細については、[ヘルプ] > [バージョン情報] の順に選択します。

7. (オプション) 内部仮想アナライザの macOS 向けサンドボックスを再度有効にします。

注意

内部仮想アナライザの macOS 向けサンドボックスは、Deep Discovery Inspector のアクティベーションコードが置き換えられると自動的に無効になります。

詳細については、251 ページの「macOS 向けサンドボックス」を参照してください。

第 7 章

トラブルシューティング

Deep Discovery Inspector 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と、よくある質問およびその回答については、次の項目を参照してください。

- 374 ページの「よくある質問 (FAQ)」
- 377 ページの「トラブルシューティング」

よくある質問 (FAQ)

よくある質問とその回答については、次の項目を参照してください。

- 374 ページの「FAQ - アプライアンスの復元」
- 375 ページの「FAQ - 設定」
- 375 ページの「FAQ - 検出」
- 375 ページの「FAQ - 設置」
- 376 ページの「FAQ - アップグレード」
- 376 ページの「FAQ - 仮想アナライザイメージ」

FAQ - アプライアンスの復元

Deep Discovery Inspector アプライアンスを復元するにはどうしたらよいでしょうか?

Deep Discovery Inspector アプライアンスを復元するには、次のいずれかを実行します。

- Deep Discovery Inspector を再インストールし、保存されている設定または初期設定に戻す

  重要

  再インストール時、すべてのログデータは削除されます。

- 管理コンソールで [管理] > [アップデート] > [製品のアップデート] > [Service Pack/バージョンアップグレード] の順に選択し、Service Pack またはバージョンアップグレードファイル (*.R.tar) を適用する

  重要

  Service Pack またはバージョンアップグレードファイルのバージョンは、インストールされているバージョンと同じである必要があります。

Deep Discovery Inspector アプライアンスを予期しないトラフィックバイパスから復元するにはどうしたらよいでしょうか?

Deep Discovery Inspector アプライアンスを予期しないトラフィックバイパスから復元するには、Deep Discovery Inspector アプライアンスを再起動します。詳細については、「Deep Discovery Inspector 管理者ガイド」の「電源オフ/再起動」を参照してください。

FAQ - 設定

複数の Apex Central サーバに Deep Discovery Inspector を登録できますか?

いいえ、複数の Apex Central サーバに Deep Discovery Inspector を登録することはできません。Apex Central サーバへの登録の詳細については、「Deep Discovery Inspector 管理者ガイド」の「Apex Central への登録」を参照してください。

FAQ - 検出

Deep Discovery Analyzer の再インストール後、ウィジェットまたは [ログクエリ] 画面に仮想アナライザによる検出が表示されなくなる理由は何ですか?

Deep Discovery Analyzer が再インストールされると、API キーが変更されます。Deep Discovery Inspector 管理コンソールの [管理] > [仮想アナライザ] > [セットアップ] から API キーを変更してください。

FAQ - 設置

Deep Discovery Inspector を設置することによって、ネットワークトラフィックが遮断されることはないですか?

アウトオブバンドアプライアンスとして導入すれば、Deep Discovery Inspector によってネットワークトラフィックが遮断されることはありません。アウトオブバンド導入の場合、Deep Discovery Inspector はスイッチのミラーポートに接続しネットワークには直接接続しないため、このアプライアンスを設置することによりネットワークトラフィックが遮断されることはありません。

インライン導入の場合、Deep Discovery Inspector によってネットワークトラフィックが遮断される可能性があります。

新規インストールした Deep Discovery Inspector で、動的 IP アドレスを取得できません。どうすればよいでしょうか?

アプライアンスを再起動し、そのアプライアンスで IP アドレスを取得できることを確認します。次に、正常に機能していることがわかっている Ethernet 接続に Ethernet ケーブルで管理ポートを接続し、アプライアンスを再起動します。

FAQ - アップグレード

Deep Discovery Inspector 6.8 にアップグレード後、以前のバージョンにロールバックできますか?

できません。ロールバック機能はサポートされていません。

ソフトウェアをアップデートして再起動した後も、Deep Discovery Inspector で古いコンポーネントが使用されているのはなぜですか?

コンポーネントをアップデートする場合、ソフトウェアが最初にアップデートされます。その後 Deep Discovery Inspector が再起動されて、ネットワークコンテンツ検査エンジンがアップデートされます。ネットワークコンテンツ検査エンジンのアップデートを終了した後、[アップデート] をクリックするか、次回の予約アップデートを待ちます。

移行に成功したことを確認するにはどうしたらよいでしょうか?

アップグレード後、[管理] > [システムログ] の順に選択し、[説明] 列で「データベースインスタンスのアップグレードが試行されました」や「Deep Discovery Inspector を<旧バージョン>から<新バージョン>にアップデートしています」のような内容の 2 つのイベントを探します。この 2 つのイベントの [結果] が [成功] であることを確認します。

データベースのアップグレードプロセスに失敗すると、Deep Discovery Inspector ではどのような操作が行われますか?

新しい空のデータベースが再構築されます。以前のデータベースのデータを回復することはできません。

FAQ - 仮想アナライザイメージ

FTP サーバからイメージをダウンロードできません。どうすればよいでしょうか?

次を確認してください。

- 指定したサーバパス、ユーザ名、およびパスワードが正しい
- FTP サーバでアクティブモードおよびパッシブモードの両方が有効になっている
- FTP サーバで UTF-8 がサポートされている (イメージ名やファイルパスにマルチバイト文字が含まれている場合)

VirtualBox でイメージがテストされると [新しいハードウェアの検出ウィザード] が開きます。これは仮想アナライザに影響しますか?

[新しいハードウェアの検出ウィザード] は、マシン間でイメージが転送されるたびに自動的に実行されます。VirtualBox でのイメージのテスト時に [新しいハードウェアの検出ウィザード] が表示されると、CD/DVD の自動実行が妨げられる可能性があります。

トラブルシューティング

ここでは、Deep Discovery Inspector 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。

- 377 ページの「管理コンソールの応答が遅くなります」
- 378 ページの「検出」
- 380 ページの「[データベースが破損しています。] アラートが表示されます」
- 380 ページの「仮想アナライザ」
- 382 ページの「仮想アナライザのイメージ」
- 383 ページの「ネットワークサービスに接続できない」
- 384 ページの「診断」

管理コンソールの応答が遅くなります

管理コンソールの応答が遅いか、タイムアウトします。

これはシステムリソースが不足している場合に発生します。

手順

1. CPU、メモリ、およびディスク使用量を確認するには、`https://<アプライアンスの IP アドレス>/html/troubleshooting.htm` に移動します。
2. [リアルタイムステータス] で [システムプロセス (ATOP)] を選択します。

   [システムプロセス] 画面が表示されます。
3. [中止] をクリックして、システムリソースをリアルタイムで確認します。

表 7-1. システムリソース

項目	行	列	説明
CPU	CPU	idle	この数値が低いほど、CPU はビジー状態にあります。 この数値が低い場合は、プロセス情報を表示して使用率が最も高い CPU を記録します。
MEM	MEM	free、cache	「free」フィールドは利用可能なメモリを示します。数値が低い場合は、特定の処理を実行するための十分なメモリがないことを意味します。
ディスク	DSK	busy	数値が高い場合は、ディスクがビジー状態にあることを示します。

検出

- 378 ページの「[すべての検出] 画面に検出が表示されません」
- 379 ページの「[すべての検出] クエリでの [登録されていないサービス] サーバの表示」
- 379 ページの「不明な IP アドレスが画面に表示されます」
- 380 ページの「既知の安全なオブジェクトに不正のフラグが付けられます」

[すべての検出] 画面に検出が表示されません

管理コンソールの [すべての検出] 画面に検出が表示されません。

手順

1. スイッチのミラーポートが、双方向のネットワークトラフィックをミラーポートにミラーリングするように設定されていることを確認します。

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

2. ネットワークパケットが取得可能であることを確認します。

   a. `https://<アプライアンスの IP アドレス>/html/troubleshooting.htm` のトラブルシューティング画面に移動して、[ネットワークトラフィックダンプ] をクリックします。

   b. ドロップダウンメニューで、使用しているデータポートを選択します。

   c. [パケットの取得] をクリックします。

   d. 10 秒間待機してから [停止] をクリックします。

   e. [表示] をクリックします。

      [パケットキャプチャ情報] 画面が表示されます。

      1. [Capfile の情報] セクションで、データレートがリアルタイムのトラフィックレートと一致していることを確認します。
      2. [TCP による通信] または [UDP による通信] をクリックし、TCP および UDP パケットが表示されていることを確認します。

[すべての検出] クエリでの [登録されていないサービス] サーバの表示

サーバが [すべての検出] 画面に [登録されていないサービス] として表示されます。

サーバが [登録済みサービス] リストに追加されていることを確認します。詳細については、「Deep Discovery Inspector 管理者ガイド」の「登録済みサービスの追加」を参照してください。

不明な IP アドレスが画面に表示されます

ネットワークに属していない IP アドレスが画面に表示されます。

ネットワーク内のすべての IP アドレスがネットワークグループに正しく追加されていることを確認してください。詳細については、「Deep Discovery Inspector 管理者ガイド」の「ネットワークグループの追加」を参照してください。

既知の安全なオブジェクトに不正のフラグが付けられます

仮想アナライザによって、既知の安全なファイル、IP アドレス、ドメイン、および URL に不正のフラグが付けられます。

- 安全なオブジェクトは許可リストに追加してください。詳細については、「Deep Discovery Inspector 管理者ガイド」の「カスタム許可リストの作成」を参照してください。
- 安全なオブジェクトは不審オブジェクトリストから許可リストに移動してください。詳細については、「Deep Discovery Inspector 管理者ガイド」の「不審オブジェクトの表示」を参照してください。

[データベースが破損しています。] アラートが表示されます

管理コンソールに [データベースが破損しています。] アラートが表示されます。

このメッセージはデータベースが破損しているときに表示されます。データはデータベースに書き込まれていないため、手動で修復する必要があることに注意してください。詳細については、「Deep Discovery Inspector 管理者ガイド」の「製品データベースの管理の実行」を参照してください。

警告!

データベースに手動修復を実行すると、データが永続的に失われます。

仮想アナライザ

- 380 ページの「OVA をアップロードできません」
- 381 ページの「仮想アナライザがファイルの送信に応答しません」

OVA をアップロードできません

OVA が大きすぎて Deep Discovery Inspector にアップロードできません。

OVA イメージのサイズは 1〜30GB にする必要があります。

仮想アナライザがファイルの送信に応答しません

ファイルサンプルを Deep Discovery Inspector に送信しましたが、仮想アナライザから応答がありません。

結果を受信するには、仮想アナライザへのファイルの送信を有効にします。

手順

1. 仮想アナライザが有効になっていることを確認してください。

   詳細については、「Deep Discovery Inspector 管理者ガイド」の「仮想アナライザの有効化」を参照してください。

2. [管理] > [仮想アナライザ] > [ファイル送信] > [追加] の順に選択し、ファイル送信ルールが次のように設定されていることを確認します。

   - [条件] で、適切なファイルの種類をクリックします。
   - [処理] で、[送信する] をクリックします。

     詳細については、「Deep Discovery Inspector 管理者ガイド」の「ファイル送信ルール」を参照してください。

3. [ダッシュボード] > [仮想アナライザのステータス] の順に選択して、[仮想アナライザ] ウィジェットの [仮想アナライザのステータス] フィールドを表示します。

   a. 仮想アナライザのステータスが [無効] の場合は、仮想アナライザを有効にしてください。[管理] > [仮想アナライザ] > [セットアップ] の順に選択して、仮想アナライザへのファイル送信を有効にします。

      詳細については、「Deep Discovery Inspector 管理者ガイド」の「仮想アナライザの有効化」を参照してください。

   b. 仮想アナライザのステータスが [有効] の場合は、Deep Discovery Inspector を再起動します。

4. 通知の設定を確認します。

   詳細については、「Deep Discovery Inspector 管理者ガイド」の「メール通知の設定」を参照してください。

5. 問題が解決しない場合は、サポートプロバイダにお問い合わせください。

仮想アナライザのイメージ

- 382 ページの「インストールメディアが起動しません」
- 382 ページの「[Found New Hardware] ウィザード」
- 383 ページの「イメージによるブルースクリーンの表示」

インストールメディアが起動しません

インストール CD/DVD が自動的に起動しません。

VirtualBox で仮想アナライザイメージをテストして、該当する項目を確認してください。

手順

1. Oracle VM VirtualBox Manager で、左側のパネルにあるインポート済みのカスタム仮想アナライザイメージをクリックします。
2. [Settings] ボタンをクリックして [Storage] を選択します。
3. [Controller: IDE] を選択して、指定したタイプが[PIIX4] であることを確認します。
4. 光ディスクアイコンを選択して、指定した CD/DVD ドライブが [IDE Secondary Master] であることを確認します。

[Found New Hardware] ウィザード

仮想アナライザのイメージ作成時、[Found New Hardware] ウィザードが表示されます。

[Found New Hardware] ウィザードは、マシン間でイメージが転送されるたびに自動的に実行されます。

イメージがインポートされると、[Found New Hardware] ウィザードは CD/DVD の自動実行を妨げる可能性があります。仮想アナライザイメージが作成され、正しい手順で準備されていることを確認してください。詳細につ

いては、https://appweb.trendmicro.com/ecs/default.aspx にある「Virtual Analyzer Image Preparation Tool ユーザガイド」を参照してください。

イメージによるブルースクリーンの表示

VirtualBox でイメージがテストされると、ブルースクリーンで「Cannot find Operating System」と表示されます。

VirtualBox で仮想アナライザイメージをテストして、該当する項目を確認してください。

手順

1. Oracle VM VirtualBox Manager で、左側のパネルにあるインポート済みのカスタム仮想アナライザイメージをクリックします。
2. [Settings] をクリックして [System] を選択します。
3. [Motherboard] タブで、次の項目が選択されていることを確認します。
   - Chipset:ICH9
   - [Enable IO API]
4. [Processor] タブで、PAE/NX が有効になっていることを確認します。
5. [Acceleration] タブで、VT-x/AMD-V が有効になっていることを確認します。

ネットワークサービスに接続できない

[ネットワークサービス診断] 画面を使用して、内部仮想アナライザや他のネットワークサービスに対するネットワーク接続をテストできます。

手順

1. `https://<アプライアンスの IP アドレス>/html/troubleshooting.htm` に移動して、[ネットワークサービス診断] をクリックします。
2. 有効なサービスを 1 つ以上選択して、[テスト] をクリックします。

接続テストが完了するまで待ちます。テストに要する時間はネットワーク環境や選択したサービスの数に応じて異なります。接続テストの結果は [結果] 列に表示されます。

診断

未対応の問題については、診断を実行し、テスト結果とデバッグログをトレンドマイクロサポートセンターに送信してください。

手順

1. 事前設定コンソールを開きます。
2. 「4) System Tasks」を選択して、<Enter> キーを押します。
3. 「Deep Discovery Inspector インストールガイド」の「診断テストの実行 (ハイパーターミナルでの例)」の指示に従ってください。
4. デバッグログを生成します。
   a. `https://<アプライアンスの IP アドレス>/html/troubleshooting.htm` に移動します。
   b. [ログ] > [デバッグログ] に移動します。
   c. [デバッグログ設定] で、デバッグするモジュールのデバッグレベルを [デバッグ] に設定します。

      パフォーマンスの低下を防ぐため、必要なモジュールのみデバッグレベルを [Debug] に設定します。レベルをデバッグに設定してデバッグレポートを取得する方法については、サポートプロバイダにお問い合わせください。
   d. [保存] をクリックします。
   e. 可能な場合は問題を再現します。
   f. エクスポートするデバッグログを 1 つ以上選択します。
      - デバッグログのエクスポート
      - 詳細デバッグログのエクスポート

- [詳細デバッグログのエクスポート] で古くなったデバッグログを 1 つ以上選択して、その日付の詳細デバッグログをエクスポートします。

g. [エクスポート] をクリックします。

ヒント

システムリソースの消費を抑えるため、エクスポートは一度に 1 回実行します。

h. [デバッグログ設定] で [ログを初期設定にリセットする] をクリックします。

i. [デバッグログのメンテナンス] で [デバッグログの削除] をクリックします。

インライン導入と TLS インスペクション

- 385 ページの「ネットワーク接続の問題」
- 387 ページの「TLS 接続の問題」

ネットワーク接続の問題

手順

1. インラインポートのリンクステータスが接続になっていることを確認します。

   a. 管理コンソールで [管理] > [システム設定] > [ネットワークインタフェース] の順に選択します。

   b. [インラインインタフェース] の [ステータス] 列で接続ステータスを確認します。

   行の先頭にある右向き矢印
   (

) をクリックすると、接続ステータスに関する追加情報が表示されます。

2. インラインポートのリンクステータスが接続になっていない場合、次の該当する項目が正しいことを確認します。
   - インタフェースの速度の設定
   - インタフェースの二重化の設定
   - インタフェースとトランシーバの互換性 (特にファイバ接続の場合)
3. ネットワークアクティビティがあることを確認します。
   a. 管理コンソールの右上隅にあるスループットにマウスを重ねて、ネットワークアクティビティの詳細を表示します。

4. ネットワークアクティビティがない場合、Deep Discovery Inspector で TLS トラフィックインスペクションが有効になっていることと、ケーブルが Deep Discovery Inspector とネットワークデバイスに安全に接続されていることを確認します。
5. (オプション) 予期せず発生するトラフィックバイパスを監視するには、Deep Discovery Inspector で SNMP をエージェントモードまたはトラップモードに設定します。

   詳細については、「管理者ガイド」の「ネットワークインタフェース」および「SNMP」を参照してください。

TLS 接続の問題

手順

1. TLS 接続の問題の原因を特定します。
   a. 管理コンソールで [管理] > [監視/検索] > [TLS トラフィックインスペクション] > [インスペクション設定] > [ドメイントンネリング] > [トンネリングされたドメインの設定] の順に選択します。
   b. 原因がわかり問題を解決できる場合は対処します。そうでない場合は、以下の手順に沿ってトラブルシューティングを続けます。
2. [ドメイントンネリング] で問題が見つからない場合は、[TLS 接続の監視] トラブルシューティング画面で異常な接続に関する情報を確認します。
   a. `https://<アプライアンスの IP アドレス>/html/troubleshooting.htm` に移動して、[TLS 接続の監視] をクリックします。

      [TLS 接続の監視] 画面が表示されます。
   b. クライアントの IP アドレスを入力して、[監視] をクリックします。
   c. 十分なデータを監視した後、監視を停止します。

      注意

      監視では最大 10 分間のデータのみ保存できます。
   d. 原因がわかり問題を解決できる場合は対処します。そうでない場合は、以下の手順に沿ってトラブルシューティングを続けます。
3. [TLS 接続の監視] で問題が見つからない場合は、より多くの情報を収集してテクニカルサポートに問い合わせます。
   a. `https://<アプライアンスの IP アドレス>/html/troubleshooting.htm` に移動して、[TLS ネットワークトラフィックダンプ] をクリックします。

      [TLS ネットワークトラフィックダンプ] 画面が表示されます。
   b. クライアントの IP アドレス、およびオプションでサーバの IP アドレスとポートを入力し、[パケットのキャプチャ] をクリックします。

c. 十分なデータをキャプチャした後、キャプチャを停止します。

d. 使用しているクライアントアプリケーションに TLS 接続情報を含むログファイルがある場合は、そのクライアントアプリケーションログのスクリーンショットを撮ります。

e. TLS トラフィックインスペクション設定のスクリーンショットを撮ります。

f. トラフィックダンプとスクリーンショットをテクニカルサポートに送信します。

第 8 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。

- 390 ページの「トラブルシューティングのリソース」
- 390 ページの「製品サポート情報」
- 391 ページの「トレンドマイクロへのウイルス解析依頼」
- 393 ページの「その他のリソース」

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

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

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

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

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録

付録

付録 A

仮想アナライザがサポートするファイルタイプ

表 A-1. ファイルタイプ

完全なファイルタイプ	ファイル拡張子の例
Adobe Portable Document Format (PDF)	`.pdf`
Adobe Shockwave Flash ファイル	`.swf`

AMD 64 ビット DLL ファイル
 	
注意
64 ビット DLL ファイルは 64 ビット OS を使用するイメージでのみ分析されます。
 	
Microsoft Windows 16 ビット DLL ファイル
Microsoft Windows 32 ビット DLL ファイル
	`.dll`
	`.ocx`
	`.drv`

完全なファイルタイプ	ファイル拡張子の例
AMD 64 ビット EXE ファイル ARJ 圧縮 EXE ファイル ASPACK 1.x 圧縮 32 ビット EXE ファイル ASPACK 2.x 圧縮 32 ビット EXE ファイル DIET DOS EXE ファイル GNU UPX 圧縮 EXE ファイル IBM OS/2 EXE ファイル LZEXE DOS EXE ファイル LZH 圧縮 EXE ファイル LZH 圧縮 EXE ファイル、ZipMail 対応 MEW 0.5 圧縮 32 ビット EXE ファイル MEW 1.0 圧縮 32 ビット EXE ファイル MEW 1.1 圧縮 32 ビット EXE ファイル Microsoft Windows 16 ビット EXE ファイル Microsoft Windows 32 ビット EXE ファイル MIPS EXE ファイル MSIL ポータブル実行可能ファイル PEPACK 圧縮実行可能ファイル PKWARE PKLITE 圧縮 DOS EXE ファイル PETITE 圧縮 32 ビット実行可能ファイル PKZIP 圧縮 EXE ファイル WWPACK 圧縮実行可能ファイル	.cpl .exe .sys .crt .scr
ALZip 圧縮ファイル	.alz
ALZip アーカイブファイル	.egg
Apple QuickTime メディア	.mov

完全なファイルタイプ	ファイル拡張子の例
コンパイル済み HTML (CHM) ヘルプファイル	.chm
カンマ区切り値 (CSV) ファイル	.csv
Hancom Hancell 表計算ファイル	.cell
Hancom Hangul Word Processor (2014 以降) (HWPX) ドキュメント	.hwpx
Hancom Hangul Word Processor (HWP) ドキュメント	.hwp
HTML アプリケーションファイル	.hta
Java アーカイブ 注意 仮想アナライザは Java ライブラリをサポートしていません。	.jar
Java アプレット	.class .cla
Hypertext Markup Language ファイル	.htm .html
JavaScript エンコードスクリプトファイル	.jse
JavaScript ファイル	.js
JungUm Global ドキュメント	.gul
JustSystems 一太郎ドキュメント	.jtd
OpenDocument	.odt .odp .ods
MHTML Web アーカイブファイル	.mht
Microsoft DOS COM ファイル	.com

完全なファイルタイプ	ファイル拡張子の例
Microsoft Excel スプレッドシート	.xls .xla .xlt .xlm
Microsoft Excel Web クエリファイル	.iqy
Microsoft Office 2003 XML ファイル Microsoft Word 2003 XML ドキュメント Microsoft Excel 2003 XML スプレッドシート Microsoft PowerPoint 2003 XML プレゼンテーション	.xml
Microsoft Office Excel スプレッドシート (Excel 2007 以降) マクロが有効な Microsoft Office Excel スプレッドシート (Excel 2007 以降)	.xlsx .xlsb .xltx .xlsm .xlam .xltm
Microsoft Office PowerPoint プレゼンテーション (PowerPoint 2007 以降) マクロが有効な Microsoft Office PowerPoint プレゼンテーション (PowerPoint 2007 以降)	.pptx .ppsx
Microsoft Office Publisher ファイル (Publisher 2016)	.pub
Microsoft Office Word ドキュメント (Word 2007 以降) マクロが有効な Microsoft Office Word ドキュメント (Word 2007 以降)	.docx .dotx .docm .dotm

完全なファイルタイプ	ファイル拡張子の例
Microsoft PowerPoint プレゼンテーション	.ppt .pps
Microsoft リッチテキストフォーマット (RTF) ドキュメント	.rtf
Microsoft Windows バッチファイル	.bat
Microsoft Windows コマンドスクリプトファイル	.cmd
Microsoft Windows PowerShell スクリプトファイル	.ps1
Microsoft Windows スクリプトファイル	.wsf
Microsoft Windows Shell Binary Link ショートカット Microsoft Windows 95/NT ショートカット	.lnk
Microsoft Word 1.0 ドキュメント Microsoft Word 2.0 ドキュメント	.doc .dot
スケーラブルベクターグラフィックスファイル	.svg
Visual Basic エンコードスクリプトファイル	.vbe
Visual Basic スクリプトファイル	.vbs
Extensible Hypertext Markup Language (XHTML) ファイル	.xht .xhtml

表 A-2. Mac ファイルタイプ

完全なファイルタイプ	ファイル拡張子の例
Apple ディスクイメージ	.dmg
Mac OS X インストーラパッケージ	.pkg
Mach-O x86/x64	ほとんどの実行可能ファイルに拡張子なし

注意

Deep Discovery Inspector では、Java アーカイブファイル (.jar) とクラスファイル (.class) の macOS 向けサンドボックスへのサブミッションもサポートしています。

表 A-3. Linux ファイルタイプ

完全なファイルタイプ	ファイル拡張子の例
Executable and Linkable Format (ELF) ファイル	`.elf`
シェルスクリプトファイル	`.sh`

付録 B

Deep Discovery Director および Trend Vision One で複製される設定

Deep Discovery Director および Trend Vision One では、次の画面の設定が複製されます。

メインメニューの場所	サブメニューの場所	設定
[管理] > [アカウント]		すべての設定
[管理] > [統合製品/サービス]	Microsoft Active Directory	すべての設定
	Syslog	すべての設定
	脅威インテリジェンスの共有	すべての設定
[管理] > [監視/検索]	ホスト/ポート	すべての設定
	脅威の検出	すべての設定

メインメニューの場所	サブメニューの場所	設定
	Web レピュテーション	すべての設定 重要 Smart Protection サービスを有効にして Deep Discovery Inspector が Service Gateway に接続されている場合は、[Web レピュテーションを有効にする] および [検出フィルタ] の設定のみが複製されます。
	アプリケーションフィルタ	すべての設定
	拒否リスト/許可リスト	すべての設定
	検出ルール	すべての設定
	検出の除外設定	すべての設定
	パケットキャプチャ	すべての設定
	[TLS トラフィックインスペクション]] > [証明書の管理]	信頼済み CA 証明書の設定のみ
	[TLS トラフィックインスペクション] > [復号ポリシー]	すべての設定
[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	すべての設定
	登録済みサービス	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

メインメニューの場所	サブメニューの場所	設定
	[通知設定] > [高リスクホストの検出]	すべての設定
	[通知設定] > [不審ホストの検出]	すべての設定
	[通知設定] > [高ネットワークトラフィック]	すべての設定
	[通知設定] > [分析されていないサンプルの検出]	すべての設定
	[通知設定] > [仮想アナライザによる検出]	すべての設定
	[通知設定] > [拒否リスト]	すべての設定
	[通知設定] > [Retro Scan 検出]	すべての設定
	[配信オプション] > [メールの設定]	すべての設定
[管理] > [システムメンテナンス]	ストレージ管理	[ファイルサイズの設定] のみ
[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	すべての設定
	SNMP	すべての設定
	時間	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] > [仮想アナライザ]	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]	すべての設定

メインメニューの場所	サブメニューの場所	設定
	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
[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
[検出] > [影響を受けたホスト]		[保存された検索条件] のみ
[検出] > [影響を受けたホスト] - [ホストの詳細]		[保存された検索条件] のみ
[検出] > [すべての検出]		[保存された検索条件] のみ
[レポート] > [スケジュール]		すべての設定
[レポート] > [カスタマイズ]		すべての設定

付録 C

統合製品/サービスでの TLS のサポート

セキュアプロトコルオプションが有効な場合、次の統合製品/サービスでは TLS 1.2 以降が使用されます。詳細については、19 ページの「アプライアンス IP の設定」を参照してください。

- Active Directory
- Check Point Open Platform for Security (OPSEC) R81 以降

注意

Check Point Open Platform for Security で TLS 1.2 以降を使用するには、HotFix が必要になる場合があります。詳細については、Check Point の公式サポート Web サイトを参照してください。

- IBM Security Network Protection (XGS) 5.5 以降
- 内部仮想アナライザサービス
- Trend Micro Apex Central 2019 以降

注意

Apex Central サーバの OS で TLS 1.2 以降を有効にする必要があります。サポートされる OS は Microsoft Windows Server 2008 R2 以降のみです。

Microsoft Windows での TLS 1.2 以降の有効化の詳細については、Microsoft Windows のドキュメントを参照してください。

- 管理コンソールアクセス
- Palo Alto Panorama および Firewall
  - PAN-OS 10.2 以降
  - Panorama 10.2 以降
- SMTP
- SSL による Syslog
- 脅威インテリジェンスの共有
- トレンドマイクロのアップデート
- トレンドマイクロのソフトウェア安全性評価サービス
- トレンドマイクロのコミュニティドメイン/IP レピュテーションサービス
- トレンドマイクロのコミュニティファイルレピュテーションサービス
- トレンドマイクロのサポート契約ポータル
- Trend Micro Deep Discovery Analyzer 5.5 以降
- Trend Micro Deep Discovery Director - オンプレミスバージョン
- Trend Micro Deep Discovery Director - クラウドバージョン
- Trend Micro Deep Discovery Director - Network Analytics
- Trend Micro Deep Discovery Director - Network Analytics as a Service
- トレンドマイクロのモバイルアプリレピュテーションサービス
- トレンドマイクロの機械学習型検索エンジン
- Trend Micro Retro Scan
- Trend Micro Sandbox as a Service
- Trend Micro Service Gateway
- トレンドマイクロスマートフィードバック
- Trend Micro Smart Protection Server 3.3 以降

- Trend Micro Threat Investigation Center
- Trend Micro TippingPoint Security Management System (SMS) 4.4 以降
- Trend Micro TXOne OT Defense Console
- トレンドマイクロの Web 検査サービス
- トレンドマイクロの Web レピュテーションサービス
- Trend Vision One
- Web サービス (SOAP)

付録 D

サービスのアドレスとポート

トレンドマイクロでは、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。

各サービスへの接続を確認するには、[ネットワークサービス診断] 画面を使用することをお勧めします。詳細については、383 ページの「ネットワークサービスに接続できない」を参照してください。

表 D-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。	ddi68-p.activeupdate.trendmicro.co.jp:443/activeupdate/japan	製品バージョンと地域に関連
CSSS (ソフトウェア安全性評価サービス)	ファイルの安全性を確認します。CSSS を使用すると誤検出が減少し、計算時間や計算リソースが節約されます。	grid-global.trendmicro.com:443	
コミュニティドメイン/IP レピュテーションサービス	検出されたドメインと IP アドレスの出現率を判断します。出現率とは、あるドメインまたは IP アドレスが一定期間内にトレンドマイクロのセンサで検出された回数を示す統計的概念です。	ddi680-jp-domaincensus.trendmicro.com:443	製品バージョンと地域に関連
コミュニティファイルレピュテーション	検出したファイルの出現率を判断します。出現率とは、あるファイルが一定期間内にトレンドマイクロのセンサで検出された回数を示す統計的概念です。	ddi680-jp-census.trendmicro.com:443	製品バージョンと地域に関連
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:443	
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。	*.nacloud.trendmicro.com:443	製品バージョンと地域に関連

サービス	説明	アドレスとポート	備考
動的な URL 検索	URL のリアルタイム分析を実行して、ゼロデイ攻撃を検出します。	ddi6-8-jp-t0.url.trendmicro.com:443	製品バージョンと地域に関連 Smart Protection Server を使用する場合は無効
Mobile App Reputation Service (MARS)	モバイルデバイスで検出された脅威に関するデータを収集します。このサービスは高度なサンドボックス環境であり、モバイルアプリの実行時の動作を分析して個人情報の漏えい、再パックされたモバイルアプリ、サードパーティの広告 SDK、脆弱性、およびアプリのカテゴリを検出します。	rest.mars.trendmicro.com:443	
機械学習型検索エンジン	不正プログラムモデリングの使用により、機械学習型検索では、サンプルを不正プログラムモデルと比較して可能性スコアを割り当て、ファイルに含まれる潜在的な不正プログラムの種類を判別します。	ddi68-jp-f.trx.trendmicro.com	製品バージョンと地域に関連
Retro Scan	クラウドベースのサービスで、ネットワーク内での C&C サーバへのコールバック回数や、関連するその他のアクティビティについての Web アクセス履歴ログを検索します。	intelliconnect.trendmicro.com:443 ddi68.retroscan.trendmicro.com:443	製品バージョンと地域に関連
Sandbox as a Service (macOS 向け)	macOS の潜在的な脅威を分析するホステッドサービスです。	ddaaas.trendmicro.com:443	

サービス	説明	アドレスとポート	備考
Sandbox as a Service	潜在的な脅威を分析するホステッドサービスです。	`*.ddcloud.trendmicro.com:443`	製品バージョンと地域に関連 このサービスに登録されている製品をアップグレードした場合は、サービスに再登録して新しいアドレスに接続することをお勧めします。
スマートフィードバック	脅威データベースを Trend Micro Smart Protection Network と共有し、トレンドマイクロが新しい脅威を迅速に特定し、対処できるようにします。 Trend Micro スマートフィードバックには、製品名、ID、バージョンなどの製品情報に加えて、ファイルタイプ、SHA-1 ハッシュ値、URL、IP アドレス、ドメインなどの検出情報も含まれる場合があります。	`gp.fbs.trendmicro.com:443`	製品バージョンと地域に関連
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。	`ddi68.threatconnect.trendmicro.com:443`	製品バージョンと地域に関連

サービス	説明	アドレスとポート	備考
Trend Vision One	検出と対応をエンドポイントを超えて拡張し、より広範な可視性と専門家によるセキュリティ分析を提供することで、より多くの脅威の検出と早期の迅速な対応を実現します。Trend Vision One により、効果的に脅威に対応し、侵害の重大度と範囲を最小限に抑えることができます。	*.xdr.trendmicro.com:443 / *.xdr.trendmicro.co.jp:443	製品バージョンと地域に関連
Trend Vision One - Network Inventory	Trend Vision One への接続を可能にします。	api-ni*.xdr.trendmicro.com:443 *.dddxdr.trendmicro.co.jp:443	製品バージョンと地域に関連
Web 検査サービス	Web レピュテーションサービスの補助サービスで、脅威結果の詳細なレベルと包括的な脅威名を提供します。 この脅威名と重大度は、積極的な処理とより集約的な検索を実行するためのフィルタ条件として使用できます。	ddi6-8-jp-wis.trendmicro.com:443	製品バージョンと地域に関連
Web レピュテーションサービス	Web ドメインの信頼性を追跡します。Web サイトの新しさ、場所の変更履歴、不正プログラム動作分析で検出された不審活動の兆候などの要素に基づいて、レピュテーションスコアを割り当てます。	ddi6-8-jp.url.trendmicro.com:443	製品バージョンと地域に関連

索引