Deep Discovery™ Email Inspector 5.1

インストールガイド

※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: APEM59195/210115_JP_R2 (2024/04)

プライバシーと個人データの収集に関する規定

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

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

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

重要

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

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

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

目次

第 4 章：コマンドラインインタフェースの使用

第 6 章：仮想アプライアンスの新規作成

第 7 章：テクニカルサポート

索引

はじめに

本書について

この章の内容は次のとおりです。

Deep Discovery Email Inspector のドキュメント

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

表 1. 製品ドキュメント

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

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

対象読者

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

- ネットワークトポロジ
- メールルーティング
- SMTP

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

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記規則	説明
 注意	設定上の注意
 ヒント	推奨事項

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

トレンドマイクロについて

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

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

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

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

第 1 章

はじめに

この章の内容は次のとおりです。

Deep Discovery Email Inspector について

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

新機能

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

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

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

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

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

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

第 2 章

Deep Discovery Email Inspector の配置

この章の内容は次のとおりです。

配置の概要

次の手順は、Deep Discovery Email Inspector の配置計画とインストールの概要を示しています。

注意

旧バージョンの Deep Discovery Email Inspector からアップグレードする場合は、現在配置されている Deep Discovery Email Inspector の「Deep Discovery Email Inspector 管理者ガイド」の「ファームウェアのアップグレード」を参照してください。

手順

1. 配置モードを決定します。

   9 ページの「ネットワークトポロジの注意事項」を参照してください。

2. システム要件を確認します。

   20 ページの「システム要件」を参照してください。

3. Deep Discovery Email Inspector をインストールします。

   次を参照してください。

   - 28 ページの「光学ドライブを持つハードウェアアプライアンスに Deep Discovery Email Inspector をインストールする」
   - 29 ページの「光学ドライブを持たないハードウェアアプライアンスに Deep Discovery Email Inspector をインストールする」
   - 32 ページの「仮想アプライアンスに Deep Discovery Email Inspector をインストールする」

4. Deep Discovery Email Inspector のネットワークを設定して管理コンソールにアクセスします。

   「Deep Discovery Email Inspector 管理者ガイド」の「基本設定」を参照してください。

ネットワークトポロジの注意事項

Deep Discovery Email Inspector は、ファイアウォールまたはエッジ MTA (Message Transfer Agent) とネットワークの内部メールサーバとの間に配置します。

アプライアンスの背面にある管理インタフェース eth0 は、コマンドラインインタフェース (SSH) の場合は TCP ポート 22、管理コンソール (HTTPS) の場合は TCP ポート 443 からアクセスできるようにしてください。

BCC モード

BCC モードでは、Deep Discovery Email Inspector はネットワークトラフィックを妨げないアウトオブバンドアプライアンスとして 動作します。Deep Discovery Email Inspector は、脅威のチェック後、複製されたすべてのメールメッセージを破棄します。複製されたメールメッセージは受信者には配信されません。

MTA として配置する前に Deep Discovery Email Inspector がどのようにメールメッセージを処理してリスクを特定するかを把握するには、BCC モードを使用します。メールトラフィックをミラーリングしてメッセージ配信を処理するには、アップストリーム MTA を設定します。Deep Discovery Email Inspector は、不審メールメッセージがネットワークを通過した場合にアラートの通知を送信しますが、メールメッセージは配信しません。

次の図は、BCC モードで配置された Deep Discovery Email Inspector で、メールメッセージがネットワークをどのように通過するかを示しています。メールメッセージはネットワークに入り、スパムメール対策ゲートウェイを通過します。スパムメール対策ゲートウェイは、ネットワークを通じてメールメッセージを受信者に送信し、さらにメールメッセージのコピーを Deep

Discovery Email Inspector に送信します。Deep Discovery Email Inspector はそのメールメッセージを調査した後、これを破棄します。

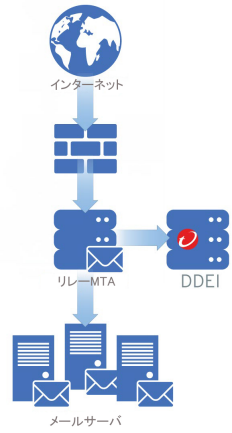


図 2-1. BCC モード

MTA モード

MTA モードの Deep Discovery Email Inspector は、メールトラフィックフロー内でメッセージ転送エージェント (MTA) として機能します。

Deep Discovery Email Inspector は、エッジ MTA または非エッジ MTA として配置できます。

Deep Discovery Email Inspector がネットワークに非エッジ MTA として配置されると、メールメッセージはネットワークに入り、リレー MTA を介して

Deep Discovery Email Inspector にルーティングされます。次の図に例を示します。

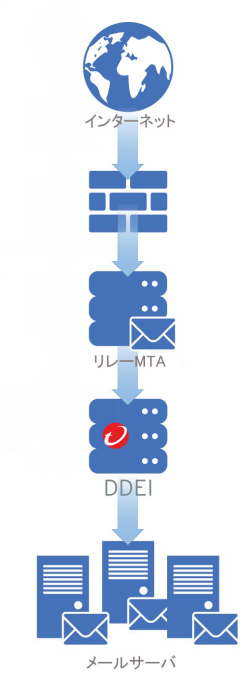


図 2-2. 非エッジ MTA

Deep Discovery Email Inspector がメールネットワークにエッジ MTA として配置されると、Deep Discovery Email Inspector はメールメッセージをルーテ

ィングゲートウェイから受信し、検出されたメッセージに対してユーザ指定の処理を実行します。

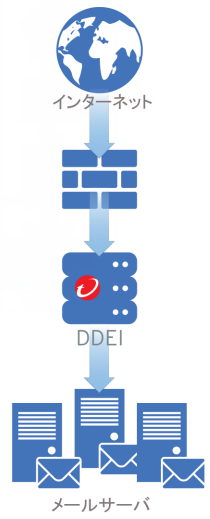


図 2-3. エッジ MTA

調査を通過したメールメッセージは、ダウンストリーム MTA にルーティングされます。スパムメールやグレーメールとして検出されたメールメッセージ、コンテンツ違反により検出されたメールメッセージ、不正な添付ファイル、埋め込まれたリンク (URL)、または不審な特徴を持つメールメッセージに対して、Deep Discovery Email Inspector ではポリシー設定に基づいたユーザ指定の処理を実行します。その後、受信者に通知が送信されます。

SPAN/TAP モード

SPAN/TAP モードでは、Deep Discovery Email Inspector はネットワークトラフィックを妨げないアウトオブバンドアプライアンスとして 動作します。Deep Discovery Email Inspector は、脅威のチェック後、複製されたすべてのメールメッセージを破棄します。複製されたメールメッセージは受信者には配信されません。

ミラーリングされたトラフィックを Deep Discovery Email Inspector に送信するように、スイッチまたはネットワークタップを設定します。Deep

Discovery Email Inspector は、不審メールメッセージがネットワークを通過した場合にアラートの通知を送信しますが、メールメッセージは配信しません。

次の図は、SPAN/TAP モードの Deep Discovery Email Inspector が配置されたネットワークを、メールメッセージがどのように通過するかを示しています。メールメッセージはネットワーク内部のスイッチまたはネットワークタップを通過します。スイッチまたはネットワークタップは、ネットワークを通じてメールメッセージを受信者に送信し、さらにメールメッセージのコピーを Deep Discovery Email Inspector に送信します。Deep Discovery Email Inspector はそのメールメッセージを調査した後、これを破棄します。

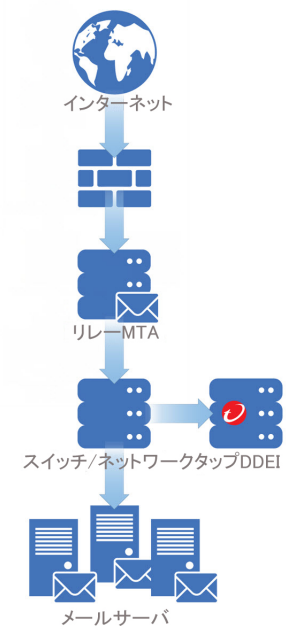


図 2-4. SPAN/TAP モード

注意

Microsoft Hyper-V にインストールされた Deep Discovery Email Inspector 仮想アプライアンスでは、SPAN/TAP モードはサポートされません。

Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。

Apex Central の配置

Apex Central は、複数の Deep Discovery Email Inspector アプライアンスを含むネットワークで、ログや不審オブジェクトデータを集約し、レポートを生成することや、製品コンポーネントのアップデートを行うことができます。また、任意の登録済み Deep Discovery Email Inspector アプライアンスの管理コンソールへの Apex Central を介したシングルサインオン (SSO) をすることもできます。

次の図は、Apex Central に登録されている複数の MTA モードの Deep Discovery Email Inspector アプライアンスを、メールメッセージがネットワーク上でどのように通過するかを示しています。Apex Central によって一元

管理される一方、各 Deep Discovery Email Inspector アプライアンスはメールメッセージを MTA として個別に処理します。

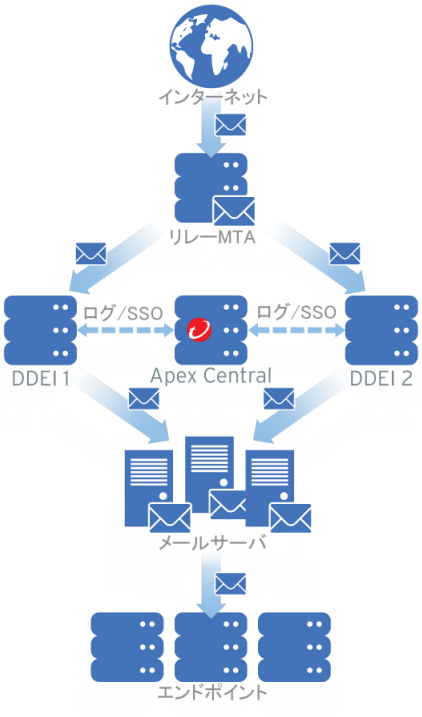


図 2-5. Apex Central の配置

Apex Central の設定の詳細については、「Deep Discovery Email Inspector 管理者ガイド」を参照してください。

推奨ネットワーク環境

Deep Discovery Email Inspector では管理ネットワークに接続する必要があります。配置した後、管理者は管理ネットワーク上の任意のコンピュータから設定作業を実行できます。

カスタムネットワークへの接続は、インターネット接続時の不正プログラムの動作をシミュレートするために推奨されます。最適な結果を得るため、プロキシ設定、プロキシ認証、および接続制限のないインターネット接続を使用することをお勧めします。

カスタムネットワーク内の不正なオブジェクトが管理ネットワーク内のエンティティに影響を及ぼさないよう、ネットワークは互いに独立している必要があります。

通常、管理ネットワークは組織のイントラネットであるのに対し、カスタムネットワークはインターネット接続されたテストネットワークなど、イントラネットから隔離された環境です。

準備する項目

要件	詳細
アクティベーションコード	トレンドマイクロから取得します
モニタと VGA ケーブル	アプライアンスの VGA ポートに接続します
USB キーボード	アプライアンスの USB ポートに接続します
USB マウス	アプライアンスの USB ポートに接続します
Ethernet ケーブル	管理ポートとデータポートに接続します • 必須: アプライアンスの管理ポート (eth0) を管理ネットワークに接続 • 推奨: データポート (eth1、eth2、または eth3) をカスタムネットワークに接続 • (オプション)メールのルーティングと監視のために未使用のデータポートをメールネットワークに接続

要件	詳細
インターネットに接続可能なコンピュータ	次のソフトウェアがインストールされたコンピュータから管理コンソールにアクセスします。 サポートされる Web ブラウザ: • Microsoft Internet Explorer 11 • Microsoft Edge • Google Chrome 66 以降 • Mozilla Firefox 59 以降
IP アドレス	• 必須: 管理ネットワークの IPv4 アドレス 1 つ • 推奨: カスタムネットワークの IPv4 アドレス 1 つ • (オプション)メールネットワークに 2 つの IPv4 アドレスと管理ネットワークに 1 つの IPv6 アドレス
サードパーティソフトウェアのライセンス	サンドボックスイメージにインストールされているすべてのサードパーティソフトウェアのライセンス

第 3 章

インストール

この章の内容は次のとおりです。

システム要件

ここで説明する内容には、Deep Discovery Email Inspector の次の要件情報が含まれています。

- 20 ページの「ハードウェアホストアプライアンスの 要件」
- 20 ページの「仮想ホストアプライアンスの 要件」
- 22 ページの「Deep Discovery Email Inspector にアクセスするための要件」

ハードウェアホストアプライアンスの要件

Deep Discovery Email Inspector は、ハードウェアアプライアンスまたは仮想アプライアンスとしてネットワークに配置できます。トレンドマイクロがサポートするハードウェアは、Deep Discovery Email Inspector アプライアンスです。それ以外のハードウェアはサポートしていません。

Deep Discovery Email Inspector は、自己完結型のインストールを実現し、製品専用に強化およびパフォーマンスチューニングされた Linux OS を実装します。別途 OS は必要ありません。

仮想ホストアプライアンスの要件

Deep Discovery Email Inspector は、VMware ESXi 6.7/7.0 および Windows Server 2016/2019 上の Microsoft Hyper-V にインストールできます。Deep Discovery Email Inspector 仮想アプライアンスでは、ネストされた仮想マシンはサポートされません。

注意

ファイルまたは URL のサンドボックス分析では、Deep Discovery Email Inspector 仮想アプライアンスを Deep Discovery Analyzer に接続してください。

Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。

ライセンスされたモデルのスループットに 基づいて、次の最小限の仕様を満たすことをお勧めします。

表 3-1. 仮想アプライアンスの仕様

1 日あたりのメッセージ数	仮想 CPU 数*	仮想メモリ (GB)	仮想ディスク	仮想 NIC 数**	Deep Discovery Analyzer 1100 アプライアンス***
30 万	3	10	500GB	次の表を参照	2 台の Deep Discovery Email Inspector 仮想アプライアンスにつき 1 台
70 万	6	16	1TB	次の表を参照	各 Deep Discovery Email Inspector 仮想アプライアンスにつき 1 台

次の表は、各動作モードでの仮想 NIC の最小要件を示しています。

表 3-2. 仮想 NIC の最小要件

動作モード	必要な仮想 NIC 数**	使用される仮想 NIC
BCC	1	• ETH0 (データ/管理ポート)
MTA	1	• ETH0 (データ/管理ポート)
SPAN/TAP	3	• ETH0 (管理ポート) • ETH1 (予約) • ETH2 (データポート)

注意

* 仮想 CPU には 2.3GHz の最小速度、ハイパースレッディングのサポート、仮想化テクノロジ (VT)、および 64 ビットアーキテクチャが必要です。

** 仮想 NIC には 1000Mb/秒の最小速度が必要です。トレンドマイクロは、ESXi 上で VMXNET 3 ネットワークアダプタのみサポートしています。仮想アプライアンスに 4 つ以上の仮想 NIC を設定する場合は、最後の 2 つのポートのみ SPAN/TAP モードに使用できます。

***1 日に最大 16,000 のサンプルを分析するには、Deep Discovery Analyzer 1100 アプライアンスに、60 のインスタンスを持つ 2 つの仮想アナライザイメージを設定することをお勧めします。

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

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

表 3-3. Deep Discovery Email Inspector へのアクセス要件

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

注意

- 1280 x 1024 以上の解像度をサポートするモニタを使用してコンソールを表示することをお勧めします。
- SSH サービスは初期設定で無効になり、有効な場合は開始されません。SSH サービスを有効にするには、50 ページの「configure service ssh enable」を参照してください。SSH サービスを開始するには、63 ページの「start service ssh」を参照してください。

トレンドマイクロの統合製品

シームレスな統合を実現するために、Deep Discovery Email Inspector と統合するトレンドマイクロ製品は、必須または推奨バージョンを使用してください。

表 3-4. Deep Discovery Email Inspector と統合できるトレンドマイクロ製品およびサービス

製品/サービス	バージョン
Trend Vision One	
Deep Discovery Director - オンプレミスバージョン	• 5.3
Deep Discovery Analyzer	• 7.0 • 6.9
Apex Central	• 2019
Smart Protection Server	• 3.3 • 3.2
TippingPoint Security Management System (SMS)	• 5.4 • 5.3

アプライアンスで使用されるポート

次の表は、Deep Discovery Email Inspector で使用されるポートとその目的を示しています。

表 3-5. Deep Discovery Email Inspector で使用されるポート

ポート	プロトコル	機能	目的
22	TCP	インバウンド	エンドポイントは SSH 経由で Deep Discovery Email Inspector に接続します。
25	TCP	インバウンド	MTA とメールサーバは、Deep Discovery Email Inspector に SMTP 経由で接続します。
53	TCP/UDP	アウトバウンド	次のことを実行します。 • DNS を解決します。 • 送信者の認証 (SPF、DKIM、DMARC) のクエリを実行します。
80	TCP	待機およびアウトバウンド	他のコンピュータやトレンドマイクロの統合製品およびホステッドサービスに接続します。 • サポート契約ポータルに接続して製品ライセンスを管理します。 • コミュニティファイルレピュテーションサービスのクエリを実行します。 • コミュニティドメイン/IP レピュテーションサービスのクエリを実行します。 • Trend Micro Smart Protection Network を使用して Web レピュテーションサービスに対してクエリを実行します。 • イメージアップロードツールを使用して Deep Discovery Email Inspector に仮想アナライザイメージをアップロードします。 • Deep Discovery Email Inspector が HTTP 経由で登録されている場合、Trend Micro Apex Central と通信します。

ポート	プロトコル	機能	目的
123	UDP	アウトバウンド	NTP サーバに接続して時間を同期します。
161	TCP	インバウンド	このポートは SNMP マネージャからの要求を待機するために使用されます。
162	TCP	アウトバウンド	SNMP マネージャに接続して SNMP トラップメッセージを送信します。

ポート	プロトコル	機能	目的
443	TCP	待機およびアウトバウンド	次のことを実行します。 • 機械学習型検索エンジンに対してクエリを実行します。 • Web 検査サービスのクエリを実行します。 • コンピュータを使用して HTTPS 経由で管理コンソールにアクセスします。 • Trend Micro Apex Central と通信します。 • Trend Micro Smart Protection Network に接続して Web レピュテーションサービスのクエリを実行します。 • トレンドマイクロ Threat Connect に接続します。 • スマートフィードバックに保護された脅威情報を送信します。 • アップデートサーバに接続してコンポーネントをアップデートします。 • フィードバックサーバに製品の使用に関する情報を送信します。 • CSSS (Certified Safe Software Service) を使用してファイルの安全性を確認します。 • オンプレミスバージョンの Deep Discovery Director と通信します。 • 脅威インテリジェンス情報と除外リストを他の製品と共有します。
4459	TCP	待機およびアウトバウンド	エンドポイントはこのポートを通じて Deep Discovery Email Inspector のエンドユーザメール隔離の管理コンソールに接続します。

ポート	プロトコル	機能	目的
5274	TCP	アウトバウンド	Deep Discovery Email Inspector では、このポートを初期設定のポートとして使用し、Smart Protection Server に接続して Web レピュテーションサービスを利用します。
ユーザ指定	適用外	アウトバウンド	次のことを実行します。 • Syslog サーバにログを送信します。 • 脅威インテリジェンスを統合製品/サービスと共有します。 • 検出ログを SFTP サーバにアップロードします。 • Check Point Open Platform for Security (OPSEC) と通信します。 • サードパーティ認証や LDAP クエリのために LDAP サーバに接続します。

Deep Discovery Email Inspector のインストール

Deep Discovery Email Inspector はハードウェアアプライアンスまたは 仮想アプライアンスとして利用できます。

注意

Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。

ハードウェアアプライアンス	トレンドマイクロは、Deep Discovery Email Inspector が事前インストールされた 2 つのサーバモデルを提供しています。Deep Discovery Email Inspector アプライアンスが届いたら、コマンドラインインタフェース (CLI) を使用してネットワーク設定を行い、管理コンソールにアクセスしてください。 詳細については、35 ページの「管理コンソールのアクセス設定」を参照してください。

仮想アプライアンス	Deep Discovery Email Inspector は、VMware ESXi 6.7/7.0 および Windows Server 2016 または 2019 上の Microsoft Hyper-V にインストールできます。 詳細については、20 ページの「仮想ホストアプライアンスの要件」を参照してください。

光学ドライブを持つハードウェアアプライアンスに Deep Discovery Email Inspector をインストールする

重要

Deep Discovery Email Inspector アプライアンスには、最初からアプライアンスソフトウェアがインストールされています。次の手順では、新規インストールについてのみ示します。

トレンドマイクロがサポートするハードウェアは、Deep Discovery Email Inspector アプライアンスです。それ以外のハードウェアはサポートしていません。ソフトウェア要件の詳細については、20 ページの「システム要件」を参照してください。

警告!

インストール時に、すべての既存のデータとパーティションが選択したディスクから削除されます。インストール前に既存データをバックアップしてください。

手順

1. サーバの電源を入れます。
2. Deep Discovery Email Inspector のインストール DVD を光学ディスクドライブに挿入します。
3. サーバを再起動します。
4. Deep Discovery Email Inspector のインストール DVD からサーバが起動し、インストールが開始されます。[Install Appliance] を選択します。

   セットアップが開始されると、[使用許諾契約] 画面が表示されます。

5. [同意する] をクリックします。
6. Deep Discovery Email Inspector をインストールするデバイスを選択します。
7. [続行] をクリックします。
8. 警告メッセージが表示されたら、[はい] をクリックして続行します。

   Deep Discovery Email Inspector のインストーラは、ハードウェアが最小限の仕様を満たしていることを確認します。
9. [次へ] をクリックします。

   [概要] 画面が表示されます。
10. [続行] をクリックして、インストールを開始します。
11. 警告メッセージが表示されたら、[続行] をクリックします。

    ディスクがフォーマットされると、OS がインストールされます。再起動後に、Deep Discovery Email Inspector アプライアンスがインストールされます。
12. 再インストールを防ぐため、光学ディスクドライブからインストール DVD を取り出します。
13. ネットワークを設定して管理コンソールにアクセスします。

    詳細については、35 ページの「管理コンソールのアクセス設定」を参照してください。
14. 管理コンソールを開きます。

    詳細については、37 ページの「管理コンソール」を参照してください。

    Deep Discovery Email Inspector の設定の詳細については、「Deep Discovery Email Inspector 管理者ガイド」を参照してください。

光学ドライブを持たないハードウェアアプライアンスに Deep Discovery Email Inspector をインストールする

光学ドライブを持たない Deep Discovery Email Inspector アプライアンスの場合、iDRAC (Integrated Dell Remote Access Controller) ポートを介して Deep Discovery Email Inspector をインストールできます。

手順

1. iDRAC の IP アドレスを設定します。次の操作を実行します。
   a. アプライアンスの電源がオンになっている場合はオフにします。
   b. Deep Discovery Email Inspector アプライアンスの iDRAC ポートを、DHCP 対応ネットワークに接続します。
   c. アプライアンスの VGA ポートにモニタを、USB ポートにキーボードを接続します。
   d. アプライアンスの電源をオンにするか、再起動します。

      注意
      電源ボタンは、アプライアンスの前面パネルのベゼルの後ろにあります。

   e. POST (Power-On Self-Test) 画面が表示されたら、`<F2>` キーを押して [System Setup] を起動します。
   f. [iDRAC Settings] > [Connectivity] > [Network] の順に選択します。
   g. [IPv4 Settings] セクションで [DHCP] を無効にし、アプライアンスで静的 IP アドレスを使用するために必要な設定を行います。
   h. [Apply] をクリックして変更を保存します。
2. iDRAC インタフェースにログインします。次の操作を実行します。
   a. Web ブラウザを開き、次のアドレスを入力します。

      https://<iDRAC の IP アドレス>

      iDRAC のログイン画面が表示されます。
   b. ログイン資格情報を入力して、[Log In] をクリックします。

      [Dashboard] が表示されます。
3. アプライアンスの電源をオフにします。[Dashboard] で、[Graceful Shutdown] ドロップダウンリストから [Power Off System] を選択します。

4. [Start Virtual Console] をクリックします。

   コンソール画面が表示されます。

5. [Boot] をクリックして [Virtual CD/DVD/ISO] を選択します。

6. [Virtual Media] をクリックして [Connect Virtual Media] を選択したら、[Connect Virtual Media] をクリックします。

7. [Map CD/DVD] の下で、[Choose File] をクリックして Deep Discovery Email Inspector のインストール ISO ファイルを選択し、[Map Device] をクリックします。

   デバイスが正常にマップされたことが示されます。

8. [Dashboard] で、[Power On System] をクリックします。

   [Deep Discovery Email Inspector Appliance Installation] 画面が表示されるまで待ちます。

9. [1. Install Appliance] を選択し、<Enter> キーを押します。

   - シリアルポートを介して Deep Discovery Email Inspector をインストールする場合は、[2. Install Appliance via Serial Port] を選択して <Enter> キーを押します。

   [License Agreement] 画面が表示されます。

10. [同意する] をクリックします。

11. Deep Discovery Email Inspector をインストールするデバイスを 選択します。

12. [続行] をクリックします。

13. 警告メッセージが表示されたら、[はい] をクリックして続行します。

    Deep Discovery Email Inspector のインストーラは、ハードウェアが最小限の仕様を満たしていることを確認します。

14. [次へ] をクリックします。

    [概要] 画面が表示されます。

15. [続行] をクリックして、インストールを開始します。

16. 警告メッセージが表示されたら、[続行] をクリックします。

    ディスクがフォーマットされると、OS がインストールされます。再起動後に、Deep Discovery Email Inspector アプライアンスがインストールされます。

17. ネットワークを設定して管理コンソールにアクセスします。

    詳細については、35 ページの「管理コンソールのアクセス設定」を参照してください。

18. 管理コンソールを開きます。

    詳細については、37 ページの「管理コンソール」を参照してください。

    Deep Discovery Email Inspector の設定の詳細については、「Deep Discovery Email Inspector 管理者ガイド」を参照してください。

仮想アプライアンスに Deep Discovery Email Inspector をインストールする

警告!

Deep Discovery Email Inspector をインストールする前に、インストール先のハードディスク上の既存データをバックアップしてください。インストール処理によりハードディスクのフォーマットと再パーティションが行われるため、すべての既存データが削除されます。

重要

- VMware ESXi のライセンスは別途購入する必要があり、そのような使用は当該製品の VMware の使用許諾契約の条項に従うものとします。
- Deep Discovery Email Inspector 仮想アプライアンス上で Eth ポートを削除すると、再インストールが必要となります。

  Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。

手順

1. 仮想アプライアンスを作成します。

   詳細については、83 ページの仮想アプライアンスの新規作成を参照してください。

   VMware ESXi サーバに Deep Discovery Email Inspector をインストールする場合は、ハードディスク容量を保持するために仮想アプライアンスのスナップショット機能を無効にしてください。

2. 仮想マシンを起動します。

3. 次のタスクを実行します。

   a. ハイパーバイザサーバの物理 CD/DVD ドライブに、Deep Discovery Email Inspector のインストール DVD を挿入します。

   b. 仮想アプライアンスの仮想 CD/DVD ドライブをハイパーバイザサーバの物理 CD/DVD ドライブに接続します。

   c. 仮想アプライアンスの仮想 CD/DVD ドライブを ISO ファイルに接続します。

4. 仮想アプライアンスを再起動します。

   a. VMware vSphere Client で、[仮想マシン] > [<仮想マシン名>] の順に選択します。

   b. [コンソール] をクリックし、[ブラウザ コンソールを開く] を選択します。

   c. 表示されるコンソール画面で、左上隅の [アクション] をクリックし、[ゲスト OS] > [キーの送信] > [Ctrl+Alt+Delete] の順にクリックします。

   インストール画面が表示されます。

5. [Install Appliance] を選択し、<Enter> キーを押します。次に、28 ページの「光学ドライブを持つハードウェアアプライアンスに Deep Discovery Email Inspector をインストールする」の手順に従ってインストール処理を完了します。

6. (オプション) DVD を取り出して、再インストールを防止します。

7. ネットワークを設定して管理コンソールにアクセスします。

   詳細については、35 ページの「管理コンソールのアクセス設定」を参照してください。

8. 管理コンソールを開きます。

   詳細については、37 ページの「管理コンソール」を参照してください。

   Deep Discovery Email Inspector の設定の詳細については、「Deep Discovery Email Inspector 管理者ガイド」を参照してください。

ESXi での仮想アプライアンスのオプションの設定

ESXi で設定を行い、Deep Discovery Email Inspector 管理コンソールのナビゲーションを有効にします。

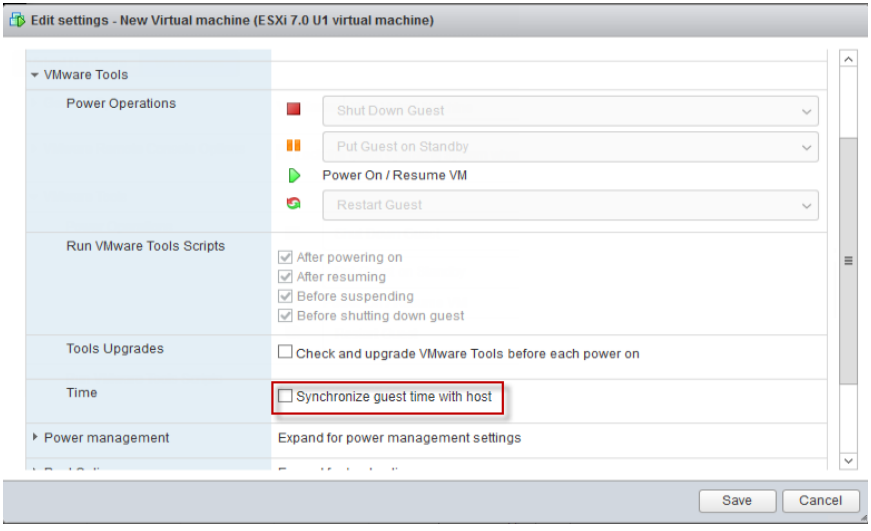
手順

1. [VMware ESXi] > [仮想マシン] の順に選択し、アプライアンス名を右クリックして、[設定の編集...] を選択します。

   設定画面が表示されます。

2. [設定] 画面で [仮想マシン オプション] タブをクリックし、[VMware Tools] を選択します。

3. [ホストとゲスト時間を同期] オプションを無効にします。



管理コンソールのアクセス設定

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

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

- 管理 IP アドレスとネットマスク
- ホスト名
- DNS
- ゲートウェイ

手順

1. 初期設定のアカウント情報で CLI にログオンします。
   - ユーザ名: `admin`

- パスワード: `ddei`

2. プロンプトで「`enable`」と入力して <Enter> キーを押し、特権モードに切り替えます。
3. 初期設定パスワードの「`trend#1`」を入力し、<Enter> キーを押します。

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

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

   注意

   IPv6 の設定は任意です。

   - ホスト名 (Host name)
   - IPv4 アドレス (IPv4 address)
   - サブネットマスク (Subnet mask)
   - IPv4 ゲートウェイ (IPv4 gateway)
   - 優先 IPv4 DNS (Preferred IPv4 DNS)
   - 代替 IPv4 DNS (Alternate IPv4 DNS)
   - IPv6 アドレス (IPv6 address)
   - プレフィックス長 (Prefix length)
   - IPv6 ゲートウェイ (IPv6 gateway)
   - 優先 IPv6 DNS (Preferred IPv6 DNS)
   - 代替 IPv6 DNS (Alternate IPv6 DNS)
6. 「`Y`」と入力して設定を確認し、再起動します。

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

これで、初期設定が完了し、管理コンソールにアクセスできるようになりました。

管理コンソール

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

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

管理コンソールにアクセスする前に必要なネットワーク設定の詳細については、35 ページの「管理コンソールのアクセス設定」を参照してください。

ログオンするには、ブラウザ画面を開き、次の URL を入力します。

`https://<アプライアンスの IP アドレス>`

注意

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

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

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

ローカルアカウントを使用してログオンする

手順

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

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

- ユーザ名: `admin`
- パスワード: `ddei`

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

注意

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

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

シングルサインオンでログオンする

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

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

手順

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

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

第 4 章

コマンドラインインタフェースの使用

この付録の内容は次のとおりです。

CLI を使用する

コマンドラインインタフェース (CLI) を使用して、次のタスクを実行します。

- デバイスの IP アドレスやホスト名の初期設定
- デバイスの再起動
- デバイスのステータスの表示
- デバイスのデバッグとトラブルシューティング

注意

HyperTerminal の使用時はキーボードのスクロールロックを有効にしないでください。スクロールロックが有効な場合、データを入力できません。

CLI を開始する

サーバに直接接続するか、SSH を使用して接続し、CLI にログオンします。

手順

- サーバに直接接続するには
  a. モニタまたはキーボードをサーバに接続します。
  b. CLI にログオンします。

注意

初期設定のアカウント情報は次のとおりです。

- ユーザ名:`admin`
- パスワード:`ddei`

- SSH サービスが有効な場合は、次の手順を実行し、SSH を使用して接続します。
  a. 使用しているコンピュータから Deep Discovery Email Inspector の IP アドレスに Ping を実行できることを確認します。

b. SSH クライアントを使用して、Deep Discovery Email Inspector の IP アドレスと TCP ポート 22 に接続します。

注意

初期設定の IP アドレス/サブネットマスクは `192.168.252.1/255.255.0.0` です。

コマンドラインインタフェースのコマンド

Deep Discovery Email Inspector の CLI コマンドは、標準コマンドと特権コマンドの 2 つのカテゴリに分類されます。標準コマンドは、システム情報を取得したり単純なタスクを実行したりするための基本コマンドです。特権コマンドは、設定のフルコントロールと、高度な監視およびデバッグ機能を提供します。特権コマンドは、`enable` コマンドとパスワードによって保護されています。

特権モードを開始する

警告!

シェル環境に入るのは、サポートプロバイダからデバッグ操作の指示があった場合のみです。

手順

1. CLI にログオンします。

   40 ページの「CLI を開始する」を参照してください。

2. プロンプトで「`enable`」と入力して <Enter> キーを押し、特権モードに切り替えます。

3. 初期設定パスワードの「`trend#1`」を入力し、<Enter> キーを押します。

   プロンプトが>から#に変更されます。

CLI コマンドリファレンス

次の表では、CLI コマンドについて説明します。

注意

CLI コマンドの実行には特権モードが必要です。詳細については、41 ページの「特権モードを開始する」を参照してください。

configure product management-port

表 4-1. configure product management-port

管理ポートの IP アドレスを設定します。	
構文: `configure product management-port [ipv4 | ipv6] <ip> <mask>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <ip>: インタフェースの IP アドレス <mask>: NIC のネットワークマスク
例:	
管理ポートの IPv4 アドレスを設定するには: `configure product management-port ipv4 192.168.10.21 255.255.255.0`	

configure product operation-mode

表 4-2. configure product operation-mode

Deep Discovery Email Inspector の動作モードを設定します。 **注意** Microsoft Hyper-V にインストールされた Deep Discovery Email Inspector 仮想アプライアンスでは、SPAN/TAP モードはサポートされません。 Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。
構文: `configure product operation-mode [BCC | MTA | TAP]`

表示	特権
パラメータ	BCC: BCC モードで配置します MTA: MTA モードで配置します TAP: SPAN/TAP モードで配置します
例:	
BCC モードで配置するには: `configure product operation-mode BCC`	

configure network basic

表 4-3. configure network basic

ホスト名、IP アドレス、サブネットマスク、ゲートウェイ、および DNS など、ネットワークの基本設定を行います。
構文: `configure network basic`

表示	特権
パラメータ	なし

例:
Network Configuration Specify value for each item and press ENTER.Settings apply to the management port (Eth0) and require a restart. Host name: mail.com IPv4 address: 10.64.70.151 Subnet mask: 255.255.254.0 IPv4 gateway: 10.64.70.1 Preferred IPv4 DNS: 10.64.1.55 Alternate IPv4 DNS: 10.64.1.54 IPv6 address: Prefix length: IPv6 gateway: Preferred IPv6 DNS: Alternate IPv6 DNS: Confirm changes and restart (Y/N):

configure network dns

表 4-4. configure network dns

Deep Discovery Email Inspector デバイスの DNS を設定します。	
構文: configure network dns [ipv4 | ipv6] <dns1> <dns2>	
表示	特権

パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <dns1>: プライマリ DNS サーバ <dns2>: セカンダリ DNS サーバ  注意 プライマリとセカンダリの DNS 値は、空白で区切ります。
例:	
プライマリ DNS に IP アドレス 192.168.10.21 を設定するには: `configure network dns ipv4 192.168.10.21`	
プライマリおよびセカンダリ DNS に次の値を設定するには: • プライマリ DNS: `192.168.10.21` • セカンダリ DNS: `192.168.10.22` `configure network dns ipv4 192.168.10.21 192.168.10.22`	

configure network hostname

表 4-5. configure network hostname

Deep Discovery Email Inspector デバイスのホスト名を設定します。	
構文: `configure network hostname <hostname>`	
表示	特権
パラメータ	<hostname>: Deep Discovery Email Inspector デバイスのホスト名または完全修飾ドメイン名
例:	
Deep Discovery Email Inspector デバイスのホスト名を test.host.com に変更するには: `configure network hostname test.example.com`	

configure network interface

表 4-6. configure network interface

ネットワークインタフェースカード (NIC) の IP アドレスを設定します。	
構文: `configure network interface [ipv4 | ipv6] <interface> <ip> <mask>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <interface>: NIC 名 <ip>: インタフェースの IP アドレス <mask>: NIC のネットワークマスク
例:	
NIC に次の値を設定するには: • インタフェース: `eth0` • IPv4 アドレス: `192.168.10.10` • IPv4 サブネットマスク: `255.255.255.0` `configure network interface ipv4 eth0 192.168.10.10 255.255.255.0`	

configure network teaming reinit

表 4-7. configure network teaming reinit

ネットワークインタフェースカード (NIC) チーミングを無効にして、ネットワークカードの設定を復元します。	
構文: `configure network teaming reinit`	
表示	特権
パラメータ	なし

例:
NIC チーミングを無効にするには: `configure network teaming reinit`

configure network route add

表 4-8. configure network route add

新しいルートエントリを追加します。	
構文: `configure network route add [ipv4 | ipv6] <ip_prefixlen> <via> <dev>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <ip_prefixlen>: IP_Address/Prefixlen 形式の送信先ネットワーク ID <via>: 次のホップの IP アドレス <dev>: デバイス名
例:	
新しいルートエントリを追加するには: `configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1`	

configure network route default

表 4-9. configure network route default

初期設定のルートを設定します。	
構文: `configure network route default [ipv4 | ipv6] <gateway>`	
表示	特権

パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <gateway>: 初期設定のゲートウェイの IP アドレス
例:	
Deep Discovery Email Inspector アプライアンスの初期設定のルートを設定するには: `configure network route default ipv4 192.168.10.1`	

configure network route del

表 4-10. configure network route del

ルートを削除します。	
構文: `configure network route del [ipv4 | ipv6] <ip_prefixlen> <via> <dev>`	
表示	特権
パラメータ	ipv4: IPv4 を設定します ipv6: IPv6 を設定します <ip_prefixlen>: IP_Address/Prefixlen 形式の送信先ネットワーク ID <via>: 次のホップの IPv4 アドレス <dev>: デバイス名
例:	
Deep Discovery Email Inspector アプライアンスのルートを削除するには: `configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1`	

configure network route del default/default ipv6

表 4-11. configure network route del default/default ipv6

初期設定の IPv6 ゲートウェイを削除します。

構文: `configure network route del default ipv6 <gateway> <device>`	
表示	特権
パラメータ	gateway: 初期設定のゲートウェイの IPv6 アドレス device: IPv6 初期設定ゲートウェイに対してリンクローカル
例: デバイス eth0 上の初期設定 IPv6 ゲートウェイ fe80::20c:29ff:fe75:b579 を削除するには:`configure network route del default ipv6 fe80::20c:29ff:fe75:b579 eth0`	

configure service nscd disable

表 4-12. configure service nscd disable

システムの起動時にネームサービスキャッシュデーモン (nscd) を無効にします。	
構文: `configure service nscd disable`	
表示	特権
パラメータ	なし
例: システムの起動時にネームサービスキャッシュデーモン (nscd) を無効にするには: `configure service nscd disable`	

configure service nscd enable

表 4-13. configure service nscd enable

システムの起動時にネームサービスキャッシュデーモン (nscd) を有効にします。	
構文: `configure service nscd enable`	
表示	特権

パラメータ	なし
例:	
システムの起動時にネームサービスキャッシュデーモン (nscd) を有効にするには: `configure service nscd enable`	

configure service ssh disable

表 4-14. configure service ssh disable

すべてのネットワークインタフェースカード (NIC) で SSH を無効にします。	
構文: `configure service ssh disable`	
表示	特権
パラメータ	なし
例:	
すべての NIC で SSH を無効にするには: `configure service ssh disable`	

configure service ssh enable

表 4-15. configure service ssh enable

特定の 1 つのネットワークインタフェースカード (NIC) で SSH を有効にします。	
構文: `configure service ssh enable`	
表示	特権
パラメータ	なし
例:	
SSH を有効にするには: `configure service ssh enable`	

configure service ssh port

表 4-16. configure service ssh port

SSH サービスポートを変更します。	
構文: `configure service ssh port <port>`	
表示	特権
パラメータ	<port>: SSH サービスポート番号
例: SSH サービスポートを 56743 に変更するには: `configure service ssh port 56743`	

configure service ntp

表 4-17. configure service ntp

Deep Discovery Email Inspector のシステム時刻を NTP サーバと同期します。	
構文: `configure service ntp [enable | disable | server-address <address>]`	
表示	特権
パラメータ	enable: NTP を有効にします disable: NTP を無効にします server-address: NTP サーバのアドレスを設定します <address>: NTP サーバの FQDN または IP アドレスを指定します
例:	
NTP サーバのアドレスを 192.168.10.21 に設定するには: `configure service ntp server-address 192.168.10.21`	
NTP サーバとの同期を有効にするには: `configure service ntp enable`	

configure system date

表 4-18. configure system date

日時を設定して、CMOS にそのデータを保存します。	
構文: `configure system date <date> <time>`	
表示	特権
パラメータ	<date>:yyyy-mm-dd の形式で時刻を設定します。 <time>:hh:mm:ss の形式で時刻を設定します。
例:	
日付を 2010 年 8 月 12 日、時刻を午後 3 時 40 分に設定するには: `configure system date 2010-08-12 15:40:00`	

configure system password enable

表 4-19. configure system password enable

特権モードを開始するためのパスワードを変更します。	
構文: `configure system password enable`	
表示	特権
パラメータ	なし
例:	
特権モードを開始するためのパスワードを変更するには: `configure system password enable`	

configure system timezone

表 4-20. configure system timezone

Deep Discovery Email Inspector で使用するタイムゾーンを設定します。

構文: `configure system timezone <region> <city>`	
表示	特権
パラメータ	<region>: 地域名 <city>: 都市名
例:	
次の場所のタイムゾーンを使用するように Deep Discovery Email Inspector アプライアンスを設定するには: 地域: America 都市: New York `configure system timezone America New_York`	

表 4-21. タイムゾーン設定の例

地域/国	都市
Africa	Cairo
	Harare
	Nairobi
America	Anchorage
	Bogota
	Buenos_Aires
	Caracas
	Chicago
	Chihuahua
	Denver
	Godthab
	Lima

地域/国	都市
	Los_Angeles
	Mexico_City
	New_York
	Noronha
	Phoenix
	Santiago
	St_Johns
	Tegucigalpa
Asia	Almaty
	Baghdad
	Baku
	Bangkok
	Calcutta
	Colombo
	Dhaka
	Hong_Kong
	Irkutsk
	Jerusalem
	Kabul
	Karachi
	Katmandu
	Krasnoyarsk
	Kuala_Lumpur

地域/国	都市
	Kuwait
	Magadan
	Manila
	Muscat
	Rangoon
	Seoul
	Shanghai
Asia (続き)	Singapore
	Taipei
	Tehran
	Tokyo
	Yakutsk
Atlantic	Azores
Australia	Adelaide
	Brisbane
	Darwin
	Hobart
	Melbourne
	Perth
Europe	Amsterdam
	Athens
	Belgrade
	Berlin

地域/国	都市
	Brussels
	Bucharest
	Dublin
	Moscow
	Paris
Pacific	Auckland
	Fiji
	Guam
	Honolulu
	Kwajalein
	Midway
US	Alaska
	Arizona
	Central
	East-Indiana
	Eastern
	Hawaii
	Mountain
	Pacific

enable

表 4-22. enable

特権モードを開始して、特権コマンドを入力できるようにします。

構文: `enable`	
表示	標準
パラメータ	なし
例:	
特権モードを開始するには: `enable`	

exit

表 4-23. exit

特権モードを終了します。 特権モードではないセッションを終了します。	
構文: `exit`	
表示	標準
パラメータ	なし
例:	
特権モードを終了する、または特権モードではないセッションを終了するには: `exit`	

help

表 4-24. help

CLI のヘルプ情報を表示します。	
構文: `help`	
表示	標準

パラメータ	なし
例:	
CLI のヘルプ情報を表示するには: `help`	

history

表 4-25. history

現在のセッションのコマンドライン履歴を表示します。	
構文: `history [limit]`	
表示	標準
パラメータ	[limit]: 現在のセッションの履歴リストのサイズを指定します。 「0」を指定すると、セッションのすべてのコマンドが維持されます。
例:	
履歴リストのサイズに 6 コマンドを指定するには: `history 6`	

logout

表 4-26. logout

現在の CLI セッションからログアウトします。	
構文: `logout`	
表示	標準
パラメータ	なし
例:	

現在のセッションからログアウトするには: `logout`

ping

表 4-27. ping

指定したホストに Ping を実行します。	
構文: `ping [-c num_echos] [-i interval] <dest>`	
表示	標準
パラメータ	[-c num_echos]: 送信するエコー要求の数を指定します。初期設定値は 5 です。 [-i interval]: パケットの送信間隔を秒単位で指定します。初期設定値は 1 です。 <dest>: 送信先のホスト名または IP アドレスを指定します。
例:	
IP アドレス 192.168.1.1 に Ping を実行するには: `ping 192.168.1.1`	
ホスト remote.host.com に Ping を実行するには: `ping remote.host.com`	

ping6

表 4-28. ping6

インタフェース eth0 を介して指定した IPv6 ホストに ping を実行します。	
構文: `ping6 [-c num_echos] [-i interval] <dest>`	
表示	標準

パラメータ	[-c num_echos]: 送信するエコー要求の数を指定します。初期設定値は 5 です。 [-i interval]: パケットの送信間隔を秒単位で指定します。初期設定値は 1 です。 <dest>: 送信先のホスト名または IP アドレスを指定します。
例:	
IPv6 アドレス fe80::21a:a5ff:fec1:1060 に ping を実行するには: `ping6 fe80::21a:a5ff:fec1:1060`	
ホスト remote.host.com に ping を実行するには: `ping6 remote.host.com`	

start task postfix drop

表 4-29. start task postfix drop

指定したメッセージまたはメールメッセージキュー内のすべてのメッセージを 削除します。	
構文: `start task postfix drop { <mail_id> | all }`	
表示	特権
パラメータ	<mail_id>: Postfix キューから削除するメッセージの ID を指定します。
例:	
メールメッセージキューからメールメッセージ D10D4478A5 を削除するには: `start task postfix drop D10D4478A5`	
メールメッセージキューからすべてのメールメッセージを 削除するには: `start task postfix drop all`	

start task postfix flush

表 4-30. start task postfix flush

キューにあるすべてのメールメッセージを 配信します。	
構文: `start task postfix flush`	
表示	特権
パラメータ	なし
例:	
キューにあるすべてのメールメッセージを 配信するには: `start task postfix flush`	

start task postfix queue

表 4-31. start task postfix queue

Postfix のキューにあるすべてのメールメッセージを 表示します。	
構文: `start task postfix queue`	
表示	特権
パラメータ	なし
例:	
Postfix のキューにあるすべてのメールメッセージを 表示するには: `start task postfix queue`	

start service nscd

表 4-32. start service nscd

ネームサービスキャッシュデーモン (nscd) を起動します。

構文: `start service nscd`	
表示	特権
パラメータ	なし
例:	
ネームサービスキャッシュデーモン (nscd) を起動するには: `start service nscd`	

start service postfix

表 4-33. start service postfix

Postfix メールシステムを開始します。	
構文: `start service postfix`	
表示	特権
パラメータ	なし
例:	
Postfix メールシステムを開始するには: `start service postfix`	

start service product

表 4-34. start service product

製品サービスシステムを開始します。	
構文: `start service product`	
表示	特権
パラメータ	なし

例:
製品サービスシステムを開始するには: `start service product`

start service ssh

表 4-35. start service ssh

ssh サービスシステムを開始します。	
構文: `start service ssh`	
表示	特権
パラメータ	なし
例:	
ssh サービスシステムを開始するには: `start ssh service`	

stop process core

表 4-36. stop process core

実行中のプロセスを停止してコアファイルを生成します。	
構文: `stop process core <pid>`	
表示	特権
パラメータ	<pid>: プロセス ID です
例:	
ID 33 のプロセスを中止するには: `stop process core 33`	

stop service nscd

表 4-37. stop service nscd

ネームサービスキャッシュデーモン (nscd) を停止します。	
構文: `stop service nscd`	
表示	特権
パラメータ	なし
例:	
ネームサービスキャッシュデーモンを停止するには: `stop service nscd`	

stop service postfix

表 4-38. stop service postfix

Postfix メールシステムを停止します。	
構文: `stop service postfix`	
表示	特権
パラメータ	なし
例:	
Postfix メールシステムを停止するには: `stop service postfix`	

stop service product

表 4-39. stop service product

製品サービスシステムを停止します。

構文: `stop service product`	
表示	特権
パラメータ	なし
例:	
製品サービスシステムを停止するには: `stop service product`	

stop service ssh

表 4-40. stop service ssh

ssh サービスシステムを停止します。	
構文: `stop service ssh`	
表示	特権
パラメータ	なし
例:	
ssh サービスシステムを停止するには: `stop ssh service`	

reboot

表 4-41. reboot

Deep Discovery Email Inspector アプライアンスを即時にまたは指定時間の経過後に再起動します。	
構文: `reboot [time]`	
表示	特権

パラメータ	[time]: Deep Discovery Email Inspector アプライアンスを再起動するまでの時間を分単位で指定します。
例:	
Deep Discovery Email Inspector アプライアンスを即時に再起動するには: `reboot`	
Deep Discovery Email Inspector アプライアンスを 5 分後に再起動するには: `reboot 5`	

resolve

表 4-42. resolve

ホスト名から IPv4 アドレスを解決したり、IPv4 アドレスからホスト名を解決したりします。	
構文: `resolve <dest>`	
表示	特権
パラメータ	<dest>: 解決する IPv4 アドレスまたはホスト名を指定します。
例:	
IP アドレス 192.168.10.1 からホスト名を解決するには: `resolve 192.168.10.1`	
ホスト名 parent.host.com から IP アドレスを解決するには: `resolve parent.host.com`	

show storage statistic

表 4-43. show storage statistic

ファイルシステムのディスク領域使用率を表示します。
構文: `show storage statistic [partition]`

表示	標準
パラメータ	[partition]: パーティションを指定します。このパラメータはオプションです。
例:	
Deep Discovery Email Inspector アプライアンスのファイルシステムのディスク領域使用率を表示するには: `show storage statistic`	

show network

表 4-44. show network

Deep Discovery Email Inspector のさまざまなネットワーク設定を表示します。	
構文: `show network [arp <address> | connections | dns | dns ipv6| hostname | interface | route | route ipv4 | route default ipv4 | route default ipv6]`	
表示	標準

パラメータ	arp: 指定したアドレスに対してアドレス解決プロトコル (ARP) で返された値を表示します。 <address>: アドレス解決プロトコル (ARP) で解決される FQDN または IP アドレスです。 connections: Deep Discovery Email Inspector アプライアンスの現在のネットワーク接続を表示します。 dns: Deep Discovery Email Inspector アプライアンスの DNS の IP アドレスを表示します。 dns ipv6: IPv6 のシステム DNS 設定を表示します。 hostname: Deep Discovery Email Inspector アプライアンスのホスト名を表示します。 interface: ネットワークインタフェースカード (NIC) のステータスと設定を表示します。 route: IP アドレスのルーティングテーブルを表示します。 route ipv4: システムの IPv4 ルーティングテーブルを表示します。 route default ipv4: 初期設定の IPv4 ルーティングテーブルを表示します。 route default ipv6: 初期設定の IPv6 ルーティングテーブルを表示します。
例:	
アドレス「10.2.23.41」に対する ARP の情報を表示するには: `show network arp 10.2.23.41`	
Deep Discovery Email Inspector アプライアンスの現在のネットワーク接続を表示するには: `show network connections`	
DNS 設定を表示するには: `show network dns`	
IPv6 のシステム DNS 設定を表示するには: `show network dns ipv6`	

Deep Discovery Email Inspector アプライアンスのホスト名を表示するには: `show network hostname`
NIC のステータスと設定を表示するには: `show network interface`
IP アドレスのルーティングテーブルを 表示するには: `show network route`
システムの IPv4 ルーティングテーブルを 表示するには: `show network route ipv4`
システムの初期設定の IPv4 ゲートウェイを表示するには: `show network route default ipv4`
システムの初期設定の IPv6 ゲートウェイを表示するには: `show network route default ipv6`

show kernel

表 4-45. show kernel

Deep Discovery Email Inspector アプライアンスの OS カーネル情報を表示します。	
構文: `show kernel {messages | modules | parameters | iostat}`	
表示	標準
パラメータ	messages: カーネルメッセージを表示します。 modules: カーネルモジュールを表示します。 parameters: カーネルパラメータを表示します。 iostat: デバイスとパーティションの CPU 統計および I/O 統計を表示します。
例:	

OS カーネルのメッセージを表示するには: `show kernel messages`
OS カーネルのモジュールを表示するには: `show kernel modules`
OS カーネルのパラメータを表示するには: `show kernel parameters`
CPU 統計および I/O 統計を表示するには: `show kernel iostat`

show service

表 4-46. show service

Deep Discovery Email Inspector サービスのステータスを表示します。	
構文: `show service [ntp <enabled | server-address> | ssh | nscd]`	
表示	標準
パラメータ	nscd: ネームサービスキャッシュデーモン (nscd) のステータスを表示します。 ntp enabled: システムの NTP サービスのステータスを表示します。 ntp server-address: システムの NTP サービスのサーバアドレスを表示します。 ssh: SSH のステータスを表示します。
例:	
ネームサービスキャッシュデーモン (nscd) のステータスを表示するには: `show service nscd`	
NTP サービスのステータスを表示するには: `show service ntp`	

SSH のステータスを表示するには: `show service ssh`

show memory

表 4-47. show memory

デバイスのシステムメモリ情報を表示します。	
構文: `show memory [vm | statistic]`	
表示	標準
パラメータ	vm:仮想メモリの統計を表示します。 statistic: システムメモリの統計を表示します。
例:	
仮想メモリの統計を表示するには: `show memory vm`	
システムメモリの統計を表示するには: `show memory statistic`	

show process

表 4-48. showprocess

現在実行中のプロセスのステータスを表示します。	
構文: `show process [top | stack | itrace | trace] [pid]`	
表示	標準

パラメータ	top: 現在実行中のプロセスとシステム関連プロセスのステータスを表示します。 stack: 実行プロセスのスタックトレースの印刷 itrace: ライブラリコールのトレース trace: システムコールとシグナルのトレース pid: プロセス ID 番号
例:	

現在実行中のプロセスのステータスを表示するには:
`show process`
プロセス 1233 のスタックトレースを表示するには:
`show process stack 1233`
プロセス 1233 のシステムコールを表示するには:
`show process trace 1233`
プロセス 1233 のライブラリコールを表示するには:
`show process itrace 1233`	

show product-info

表 4-49. show product-info

製品情報を表示します。	
構文: `show product-info [management-port | operation-mode | service-status | version`	
表示	標準

パラメータ	management-port: 管理ポートの IP アドレスとサブネットマスクを表示します。 operation-mode: Deep Discovery Email Inspector の操作モードを表示します。 service-status: サービスのステータスを表示します。 version: 製品バージョンを表示します。
例:	
管理ポートの IP アドレスとサブネットマスクを表示するには: `show product-info management-port` 操作モードを表示するには: `show product-info operation-mode` サービスのステータスを表示するには: `show-product-info service-status` Deep Discovery Email Inspector のビルドバージョンを表示するには: `show product-info version`	

show system

表 4-50. show system

さまざまなシステム設定を表示します。	
構文: `show system [date | timezone [continent | city | country]| uptime | version]`	
表示	標準

パラメータ	date: 現在の日付と時刻を表示します。 timezone: タイムゾーン設定を表示します。オプションで次のタイムゾーン情報を指定できます。 • continent: システムの大陸を表示 • city: システムの都市を表示 • country: システムの国/地域を表示 uptime: Deep Discovery Email Inspector アプライアンスの稼働時間を表示します。 version: Deep Discovery Email Inspector アプライアンスのバージョン番号を表示します。
例:	
Deep Discovery Email Inspector アプライアンスの現在の日時を表示するには: `show system date`	
タイムゾーン設定を表示するには: `show system timezone`	
Deep Discovery Email Inspector アプライアンスの大陸を表示するには: `show system timezone continent`	
Deep Discovery Email Inspector アプライアンスの都市を表示するには: `show system timezone city`	
Deep Discovery Email Inspector アプライアンスの国/地域を表示するには: `show system timezone country`	
Deep Discovery Email Inspector の稼働時間を表示するには: `show system uptime`	
Deep Discovery Email Inspector アプライアンスのバージョン番号を表示するには: `show system version`	

shutdown

表 4-51. shutdown

Deep Discovery Email Inspector アプライアンスを即時にまたは指定時間の経過後にシャットダウンします。	
構文: `shutdown [time]`	
表示	特権
パラメータ	[time]: Deep Discovery Email Inspector アプライアンスを指定した分数の経過後にシャットダウンします。
例:	
Deep Discovery Email Inspector アプライアンスを即時にシャットダウンするには: `shutdown`	
Deep Discovery Email Inspector アプライアンスを 5 分後にシャットダウンするには: `shutdown 5`	

traceroute

表 4-52. traceroute

指定した送信先への追跡ルートを表示します。	
構文: `traceroute [-h hops] <dest>`	
表示	標準
パラメータ	[-h hops]: 送信先までの最大ホップ数を指定します。最少数は 6 です。 <dest>: トレースするリモートシステムを指定します。
例:	
最大 6 ホップまでの IP アドレス 172.10.10.1 へのルートを表示するには: `traceroute 172.10.10.1`	

最大 30 ホップまでの IP アドレス 172.10.10.1 へのルートを表示するには:

```
traceroute -h 30 172.10.10.1
```

第 5 章

Deep Discovery Email Inspector のアップグレード

この章の内容は次のとおりです。

システムアップデート

トレンドマイクロからの製品リリース後に、各種問題への対応、製品パフォーマンスの向上、新機能の追加などの理由でシステムアップデートが配布されます。

表 5-1. システムアップデート

システムアップデート	説明
HotFix	HotFix は、特定の問題を修正するために提供されるプログラムです。サポートセンターにお問い合わせいただいた際に、このプログラムで障害が回避されると判断させていただいた場合、お問い合わせいただいたお客さまに個別に送付させていただくことがあります。 注意 トレンドマイクロが Patch を配布するまで、新しい HotFix には以前の HotFix が含まれる場合があります。
Critical Patch	至急対策の必要がある問題のみを修正する目的で一般公開されるプログラムです。特定の問題を修正するプログラムであるため、基本的に、他の修正は含まれませんが、同時期に発見された問題に対する複数の修正が含まれる場合があります。一般公開時期に応じて、後述の Patch に統合されます。問題発生条件に合致するすべてのお客さまに適用を推奨いたします。

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

http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

Patch を管理する

トレンドマイクロでは、報告された既知の問題に対する新しいファームウェアバージョン、または製品に適用するアップグレードを不定期にリリースし

ています。使用可能なファームウェアバージョンについては、https://appweb.trendmicro.com/ecs/Default.aspx を参照してください。

Patch ファイルは次のいずれかの方法でトレンドマイクロにインストールできます。

- Deep Discovery Email Inspector 管理コンソール
- Deep Discovery Director からの計画配信。詳細については、Deep Discovery Director のドキュメントを参照してください。

手順

1. [管理] > [製品のアップデート] > [HotFix/Patch]の順に選択します。
2. [履歴] で、ソフトウェアのバージョン番号を確認します。
3. 製品の Patch を管理します。
   - トレンドマイクロのサポートで提供される Patch ファイルを参照し、[HotFix/Patch のインストール] で [インストール] をクリックして、Patch をアップロードします。
   - Patch をロールバックするには、[履歴] で [ロールバック] をクリックします。ロールバック後、Deep Discovery Email Inspector ではそれ以前の最新の設定を使用します。たとえば、Patch 3 をロールバックすると、Deep Discovery Email Inspector は Patch 2 の状態に戻ります。

ファームウェアをアップグレードする

トレンドマイクロでは、報告された既知の問題に対する新しいファームウェアバージョン、または製品に適用するアップグレードを不定期にリリースしています。使用可能なファームウェアバージョンについては、https://appweb.trendmicro.com/ecs/Default.aspx を参照してください。

ファームウェアをアップグレードすることで、新しいセキュリティ機能が利用可能になったとき、または機能強化されたときに、Deep Discovery Email Inspector からそれらの機能に確実にアクセスできるようになります。

Deep Discovery Email Inspector でファームウェアをアップグレードするには、次のいずれかの方法を使用します。

- Deep Discovery Email Inspector 管理コンソール
- Deep Discovery Director からの計画配信。詳細については、Deep Discovery Director のドキュメントを参照してください。

注意

続行する前に、すべての管理コンソールタスクを完了していることを確認してください。アップグレードプロセスには時間がかかり、アップグレード内容によっては 1 時間以上かかることがあります。 ピーク時間外の時間帯にアップグレードを開始することをお勧めします。アップデートをインストールすると、Deep Discovery Email Inspector が再起動されます。

手順

1. 設定をバックアップします。

   81 ページの「設定のバックアップと復元」

2. ファームウェアイメージを 入手します。
3. このイメージをコンピュータの任意のフォルダに保存します。
4. [管理] > [製品のアップデート] > [ファームウェア] の順に選択します。
5. [ソフトウェアのバージョン] の横で、ファームウェアのバージョンを確認します。
6. アップグレード用のファームウェアパッケージを 参照します。
7. [インストール] をクリックします。

   ヒント

   コマンドラインインタフェースからインストール 処理の進捗が確認できます。

   インストールが完了すると、Deep Discovery Email Inspector が自動的に再起動され、コマンドラインインタフェースが 表示されます。

8. 次のインストール後の手順を実行します。

- ブラウザのキャッシュをクリアします。
- Web コンソールにログオンします。
- プロキシサーバ経由でインターネットに接続する内部仮想アナライザを Deep Discovery Email Inspector で使用している場合は、内部仮想アナライザのプロキシを再設定します。

設定のバックアップと復元

Deep Discovery Email Inspector の設定をバックアップするには、管理コンソールから設定をエクスポートします。システム障害が発生した場合は、以前バックアップした設定ファイルをインポートして、その設定を復元できます。

重要

Deep Discovery Email Inspector で復元できるのは、ライセンスのステータスに互換性があり、ファームウェアバージョン、ハードウェアモデル、およびロケールが同じ別の Deep Discovery Email Inspector サーバの設定のみです。たとえば、バージョン 3.2 以前のバージョンを実行しているサーバからバックアップした設定ファイルで、バージョン 5.1 を実行しているサーバを復元することはできません。

ライセンスの互換性の詳細については、82 ページの「ライセンスの互換性」を参照してください。

注意

設定のエクスポート/インポートを行う際はデータベースがロックされます。そのため、データベースアクセスに依存する Deep Discovery Email Inspector のすべての処理が機能しません。

推奨事項:

- 各インポート操作の前には、現在の設定をバックアップしてください。
- Deep Discovery Email Inspector がアイドル状態のときに操作を実行してください。インポートとエクスポートは Deep Discovery Email Inspector のパフォーマンスに影響します。

設定をバックアップして、Deep Discovery Email Inspector アプライアンスの設定のコピーを作成し、別の Deep Discovery Email Inspector アプライアンスで設定を復元したり、後からバックアップした設定に戻したりします。複数の Deep Discovery Email Inspector アプライアンス間で同じ設定ファイルを各アプライアンスに復元することにより、設定を複製します。

ライセンスの互換性

次の表は、製品ライセンスの互換性について説明しています。復元できるのは、ライセンスに互換性があり、ファームウェアバージョン、ハードウェアモデル、およびロケールが同じ別の Deep Discovery Email Inspector サーバからバックアップした設定ファイルのみです。

表 5-2. ライセンスの互換性

ライセンスのアクティベーション	高度な脅威対策 + ゲートウェイモジュール	ゲートウェイモジュールのみ	高度な脅威対策のみ
高度な脅威対策 + ゲートウェイモジュール	互換性あり	互換性あり	互換性あり
ゲートウェイモジュールのみ	互換性なし	互換性あり	互換性なし
高度な脅威対策のみ	互換性なし	互換性なし	互換性あり

第 6 章

仮想アプライアンスの新規作成

注意

Deep Discovery Email Inspector 日本語版では、仮想アプライアンスは提供しておりません。

VMware ESXi または Microsoft Hyper-V を使用して仮想アプライアンスを作成する方法については、次の項目を参照してください。

- 84 ページの「VMWare ESXi 仮想アプライアンスを作成する」
- 91 ページの「Microsoft Hyper-V で仮想マシンを作成する」

仮想ホストアプライアンスシステムの 最小要件とサポートされるハイパーバイザについては、20 ページの「仮想ホストアプライアンスの 要件」を参照してください。

VMWare ESXi 仮想アプライアンスを作成する

VMware ESXi を使用して仮想アプライアンスを作成する方法については、次の項目を参照してください。

- 84 ページの「VMware ESXi サーバのネットワークを設定する」
- 87 ページの「VMware ESXi で仮想マシンを作成する」

VMware ESXi サーバのネットワークを設定する

ブラウザを使用して ESXi サーバに接続します。

手順

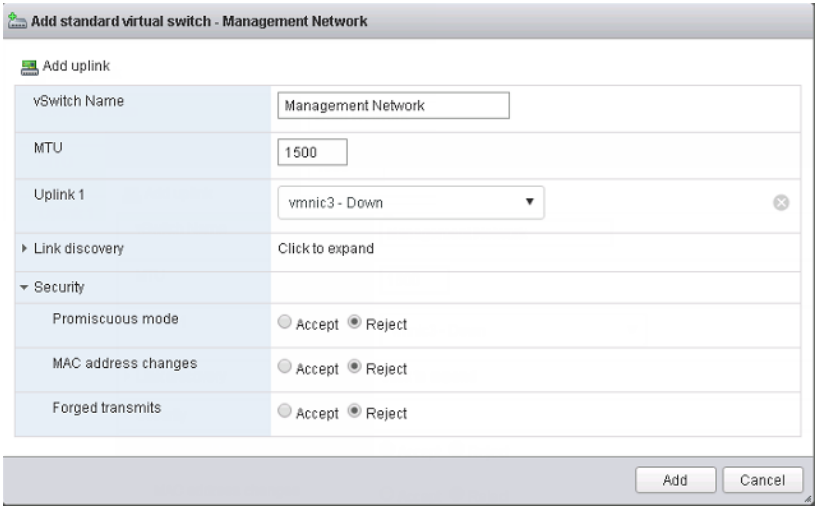
1. VMware ESXi サーバにログインするには、[User name] と [Password] を入力し、[Log in] をクリックします。

2. [Networking] をクリックし、[Virtual switches] タブをクリックします。初期の状態を確認します。

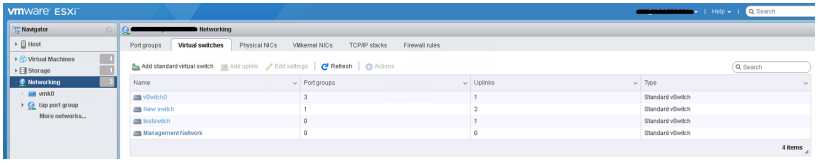
3. [Add standard virtual switches] をクリックし、次の設定を行います。

   a. [vSwitch Name] に名前を入力します (「Management Network」など)。

   b. [Uplink 1] で [Management Network] の NIC カードを選択します。



   c. [Add] をクリックします。



4. (オプション) データネットワークを追加します。[Virtual switches] タブで、[Add standard] をクリックして設定を行います。

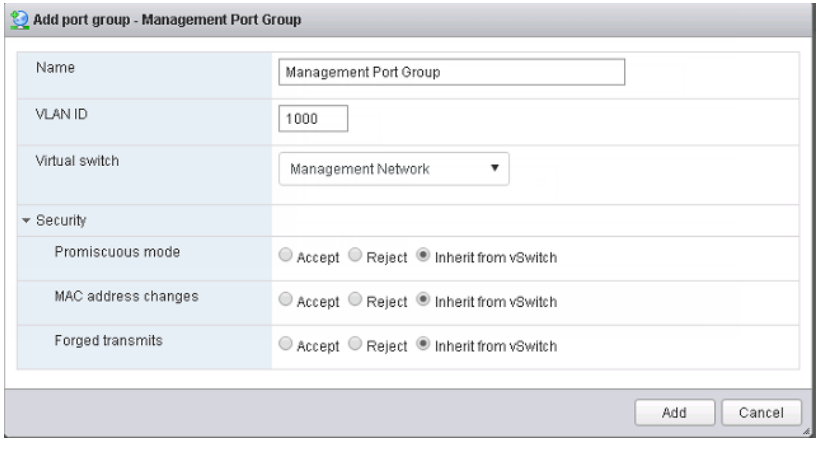
   注意

   Deep Discovery Email Inspector が SPAN/TAP モードで、標準仮想スイッチへのアップリンクポートを使用して設定されている場合は、仮想スイッチのプロミスキャスモードを有効にします。

   a. [vSwitch Name] に名前を入力します。
   b. [Uplink 1] でデータネットワークの NIC カードを選択します。
   c. [Security] を展開し、[Promiscuous mode] で [Accept] を選択します。

5. [Port groups] タブをクリックし、初期の状態を確認します。
6. [Add port group] をクリックし、次の設定を行います。

   a. [Name] に名前を入力します (「Management Port Group」など)。
   b. [VLAN ID] に数字を入力します (「1000」など)。
   c. [Virtual switch] で [Management Network] を選択します。

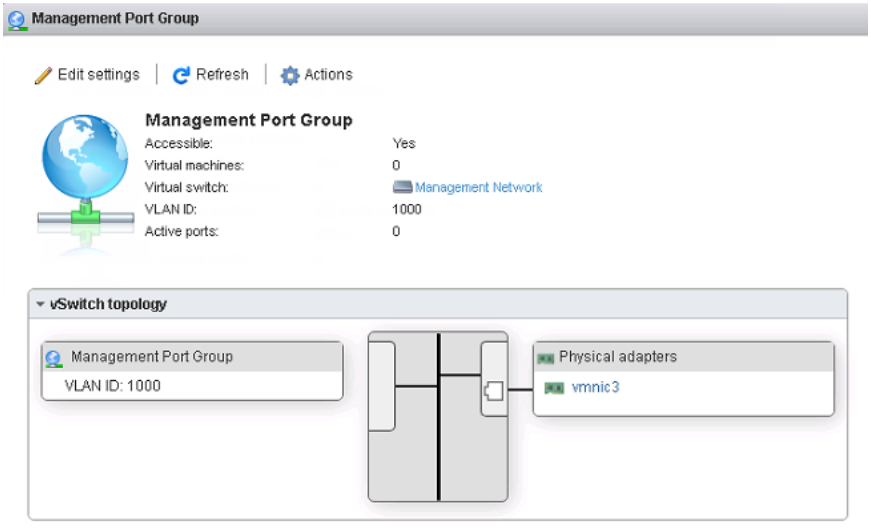


7. [Add] をクリックします。

8. (オプション) データポートグループを追加します。

> **注意**
> SPAN/TAP モードが有効な場合、追加のポートグループを 1 つ設定します。

9. [Port groups] タブで [Data port group] をクリックし、それが [Management Network] に接続されていることを確認します。

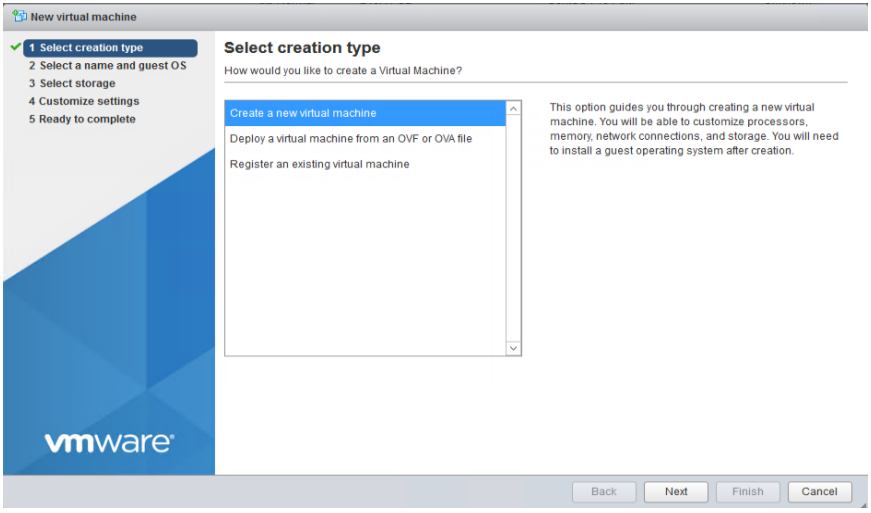


VMware ESXi で仮想マシンを作成する

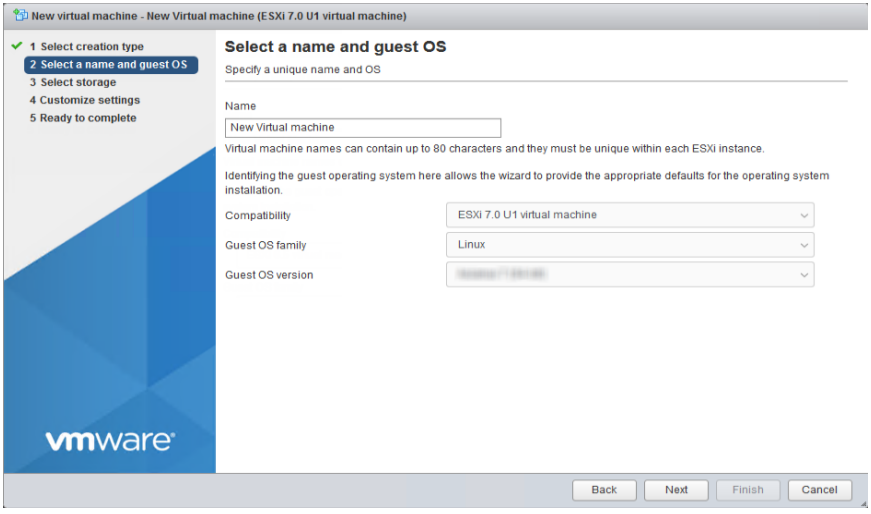
次の手順は VMware に適用されます。

手順

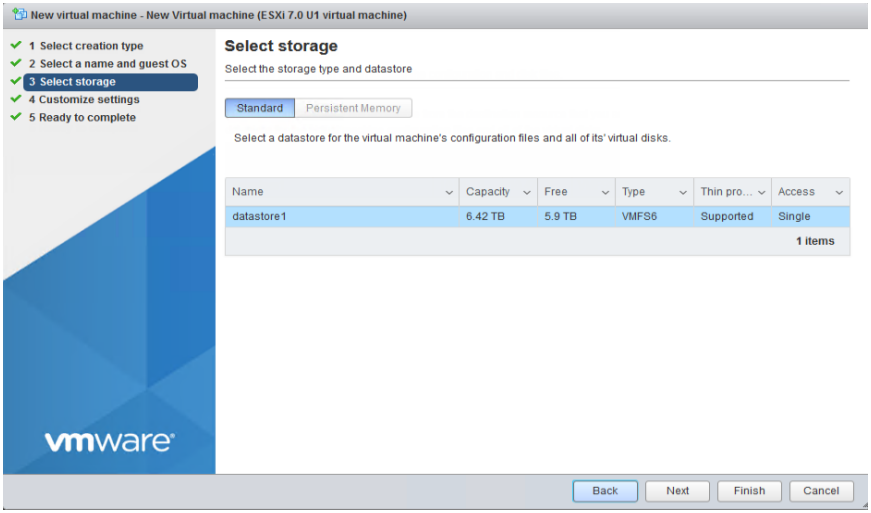
1. [Virtual machines] をクリックし、[Create / Register VM] をクリックします。
2. [Select creation type] 画面で [Create a new virtual machine] をクリックし、[Next] をクリックします。



3. [Select a name and guest OS] 画面で設定を行います。
   a. [Name] に「`New Virtual Machine`」と入力します。
   b. [Compatibility] に [ESXi 7.0 U1 virtual machine] を選択します。
   c. [Guest OS family] に [Linux] を選択します。
   d. [Guest OS version] に [CentOS 7 (64-bit)] を選択します。



4. [Next] をクリックします。
5. [Select storage] 画面で、仮想マシンが存在する保存先のストレージを選択して、[Next] をクリックします。



6. [Customize settings] 画面で設定を行います。

a. [CPU] で、仮想 Deep Discovery Email Inspector ライセンスのスループットに基づいた仮想 CPU の数を選択します。

   - 1 日のメッセージ数が 30 万の場合は、少なくとも 3 つの仮想 CPU を選択します。
   - 1 日のメッセージ数が 70 万の場合は、少なくとも 6 つの仮想 CPU を選択します。

b. [Memory] で、仮想 Deep Discovery Email Inspector ライセンスのスループットに基づいたメモリ容量を設定します。

   - 1 日のメッセージ数が 30 万の場合は、仮想マシンに少なくとも 10GB のメモリを設定します。
   - 1 日のメッセージ数が 70 万の場合は、仮想マシンに少なくとも 16GB のメモリを選択します。

c. [Hard disk] で、仮想 Deep Discovery Email Inspector ライセンスのスループットに基づいたディスク容量を設定します。

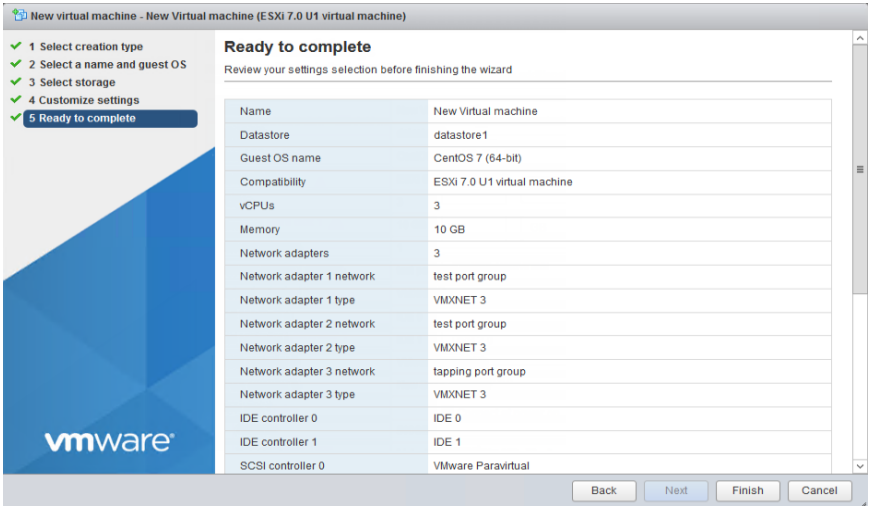
   - 1 日のメッセージ数が 30 万の場合は、仮想マシンに少なくとも 500GB のディスク容量を設定します。
   - 1 日のメッセージ数が 70 万の場合は、仮想マシンに少なくとも 1TB のディスク容量を選択します。

d. [Network] で、仮想 Deep Discovery Email Inspector ライセンスの機能に基づいた NIC 数を設定します。

   - Deep Discovery Email Inspector が MTA または BCC モードで設定されている場合は、NIC を少なくとも 1 つ設定します。
   - SPAN/TAP モードが有効な場合は、管理ネットワークとデータネットワークに 1 つずつ、少なくとも 3 つの NIC を設定します。

     1. VMware ESXi サーバの [VM Network] を Deep Discovery Email Inspector の管理ネットワーク (NIC 1) として設定します。
     2. [Data port group] を Deep Discovery Email Inspector のデータネットワーク (NIC 2) として設定します。
     3. [Adapter Type] で、[VMXNET 3] を選択します。

7. [Next] をクリックします。
8. [Ready to complete] 画面で設定を確認し、[Finish] をクリックします。

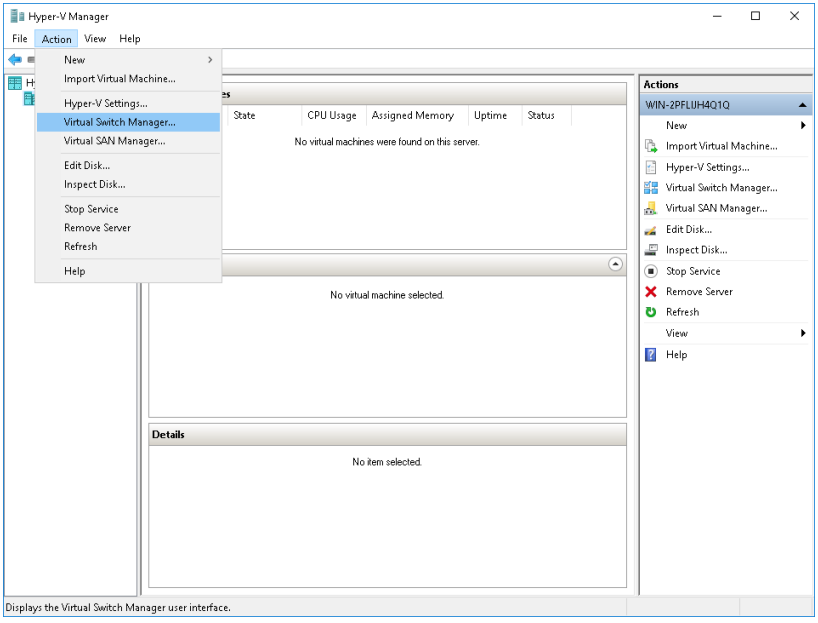


Microsoft Hyper-V で仮想マシンを作成する

手順

1. 仮想管理とデータのスイッチを作成します。
   a. Hyper-V マネージャーで、[Action] > [Virtual Switch Manager] の順に選択します。

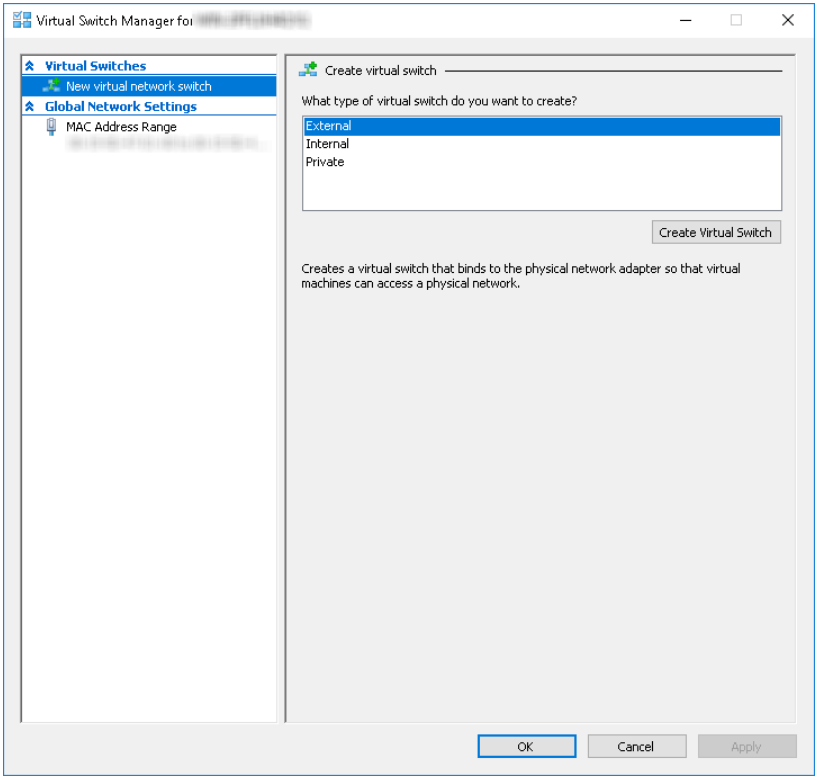
      [Virtual Switch Manager] 画面が表示されます。



b. 左側のペインで、[New Virtual network switch] をクリックします。

[Create virtual switch] 画面が表示されます。

c. 作成するスイッチの種類に、[External] を選択します。

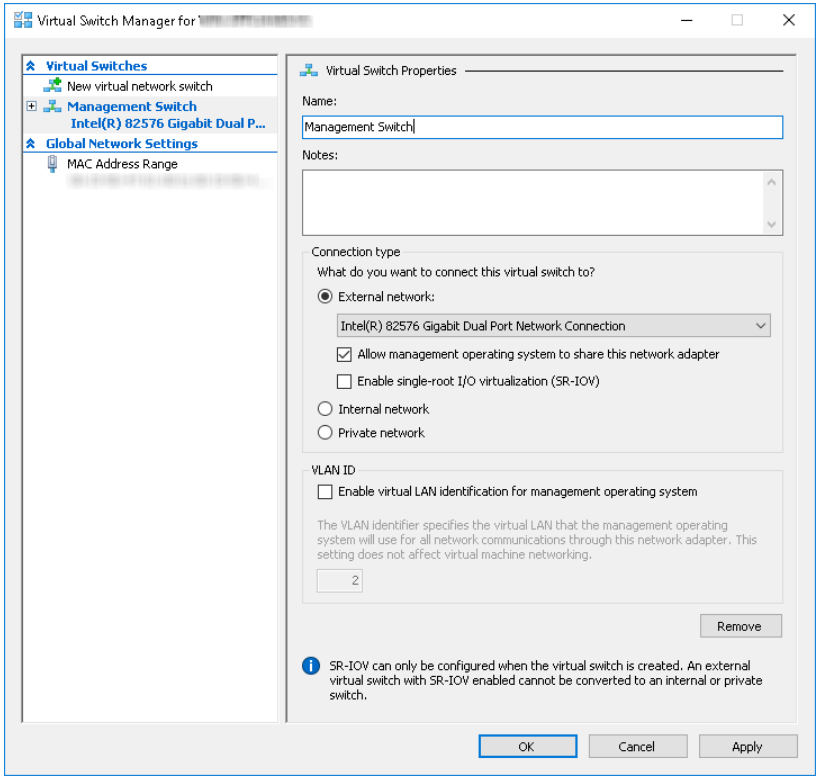


d. [Create Virtual Switch] をクリックします。

[Virtual Switch Properties] 画面が表示されます。

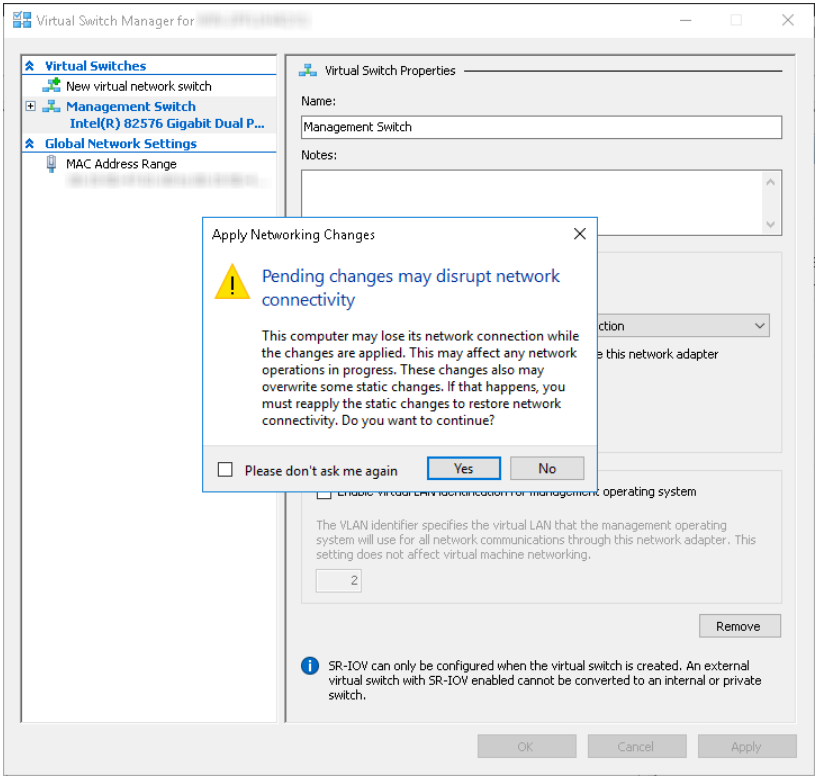
e. [Name] に「`Management Switch`」と入力します。

f. [Connection type] に [External Network] を選択し、管理ネットワークに使用する NIC カードを選択します。



g. [Apply] をクリックします。

[Apply Networking Changes] 確認画面が表示されます。



h. 警告を読んで、[Yes] をクリックします。

i. 左側のペインで、[New Virtual network switch] をクリックします。

[Create virtual switch] 画面が表示されます。

j. 作成するスイッチの種類に、[External] を選択します。

k. [Create Virtual Switch] をクリックします。

[Viritual Switch Properties] 画面が表示されます。

l. [Name] に「`Data Switch`」と入力します。

m. [Connection type] に [External Network] を選択し、データネットワークに使用する NIC カードを選択します。

n. [Apply] をクリックします。

[Apply Networking Changes] 確認画面が表示されます。

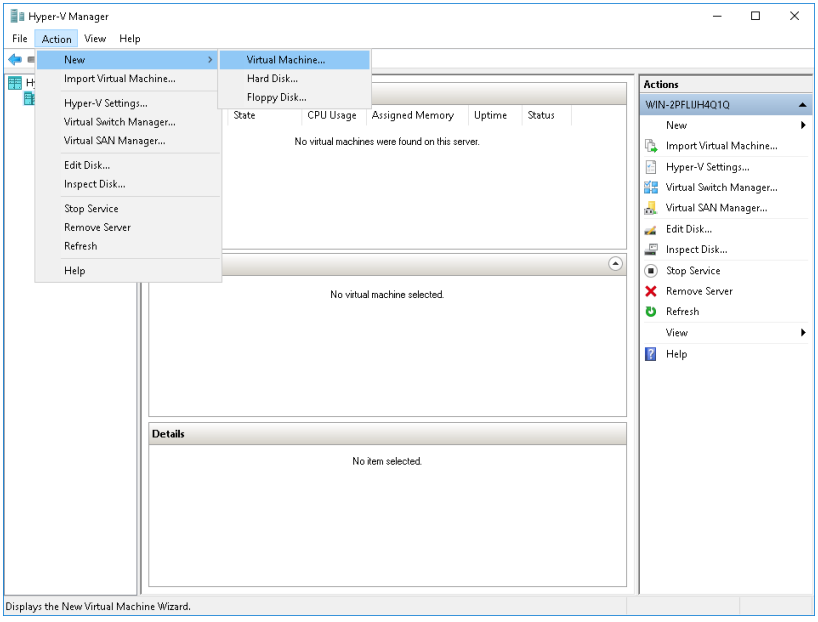
o. 警告を読んで、[Yes] をクリックします。

確認画面が閉じます。

p. [OK] をクリックします。

2. 仮想マシンを作成します。

a. Hyper-V マネージャーで、[Action] > [New] > [Virtual Machine] の順に選択します。

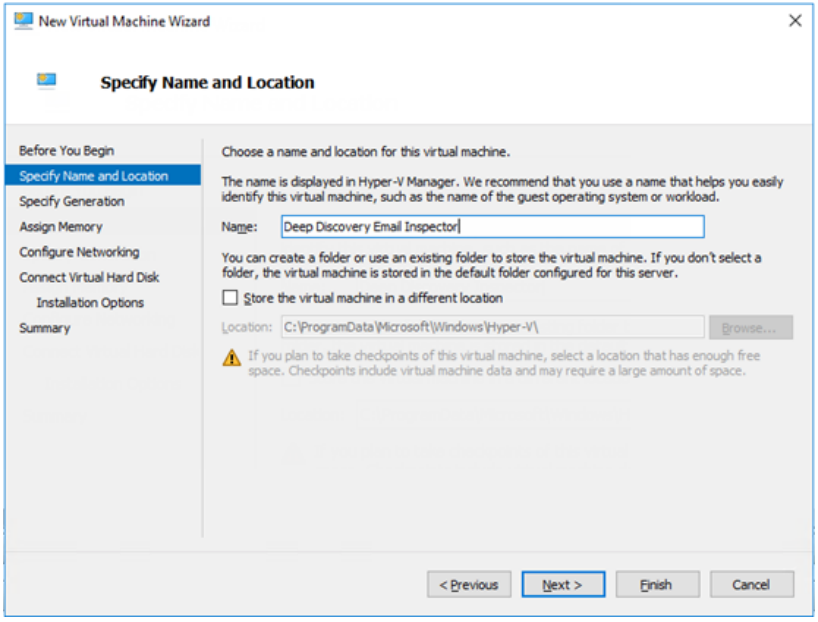


[New Virtual Machine Wizard] 画面が、[Before You Begin] 画面とともに開きます。

b. [Next] をクリックします。

[Specify Name and Location] 画面が表示されます。

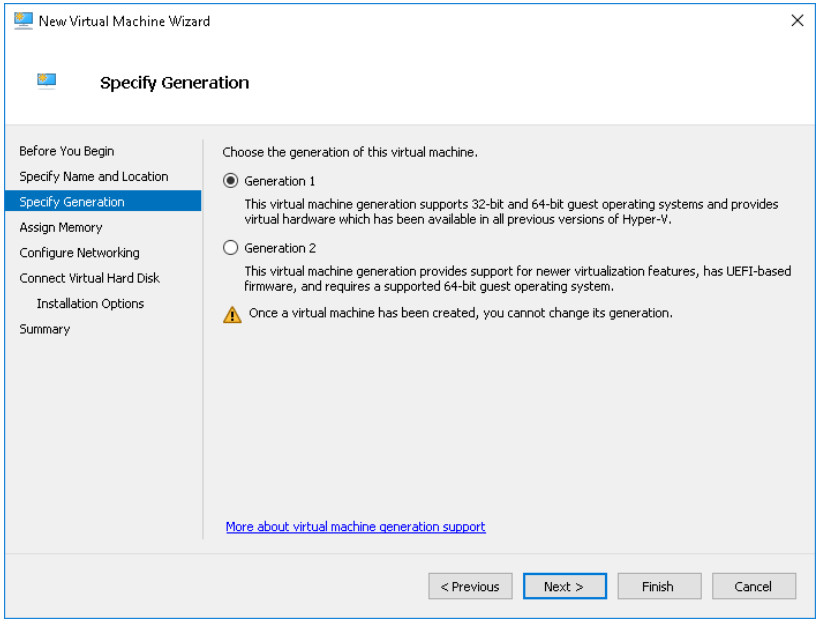
c. [Name] に「`Deep Discovery Email Inspector`」と入力します。



d. [Next] をクリックします。

[Specify Generation] 画面が表示されます。

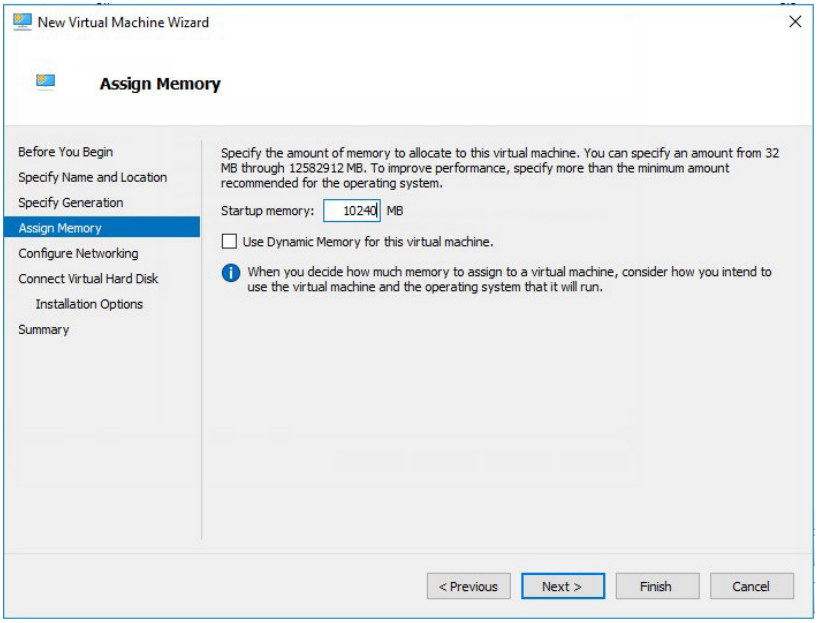
e. [Generation 1] を選択します。



f. [Next] をクリックします。

[Assign Memory] 画面が表示されます。

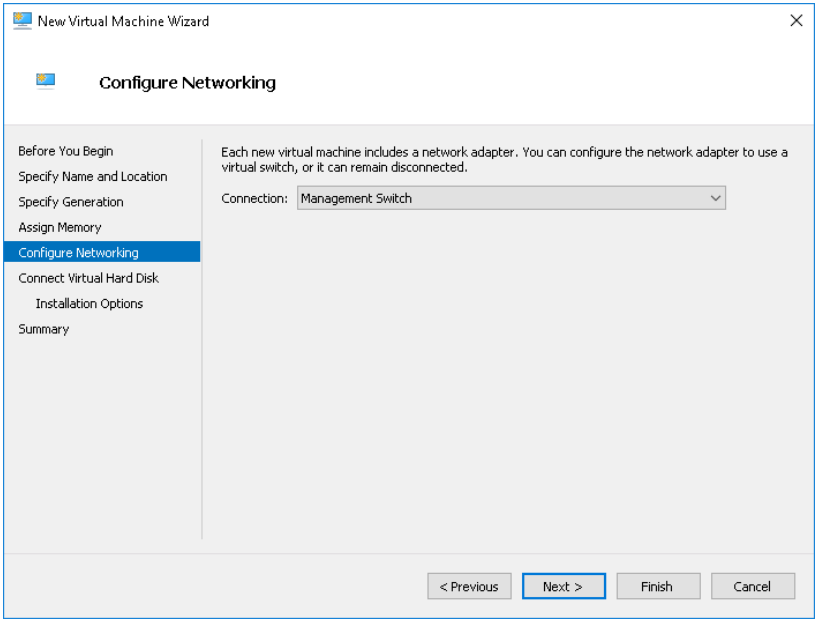
g. [Startup memory] に少なくとも `10240`MB (10GB) を割り当てます。



h. [Next] をクリックします。

[Configure Networking] 画面が表示されます。

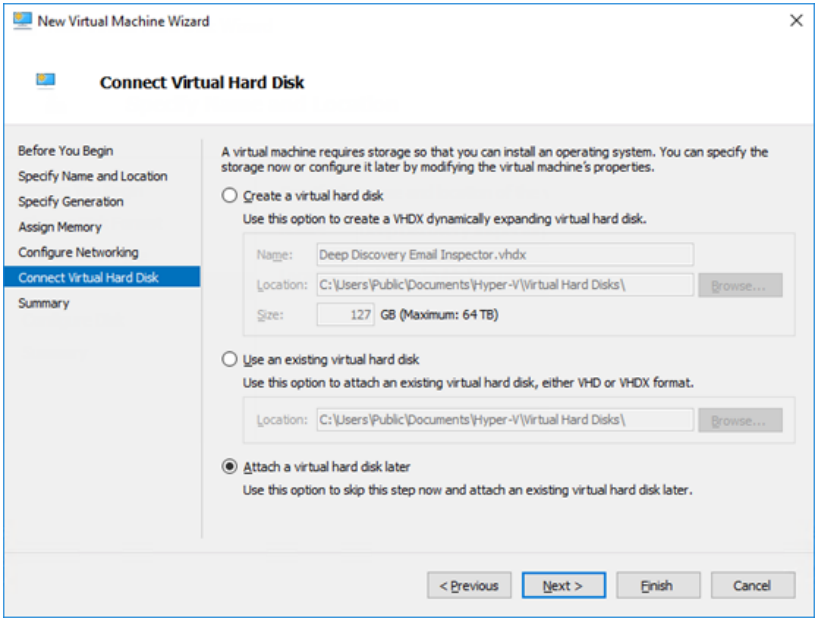
i. [Connection] で [Management Switch] を選択します。



j. [Next] をクリックします。

[Connect Virtual Hard Disk] 画面が表示されます。

k. [Attach a virtual hard disk later] を選択します。



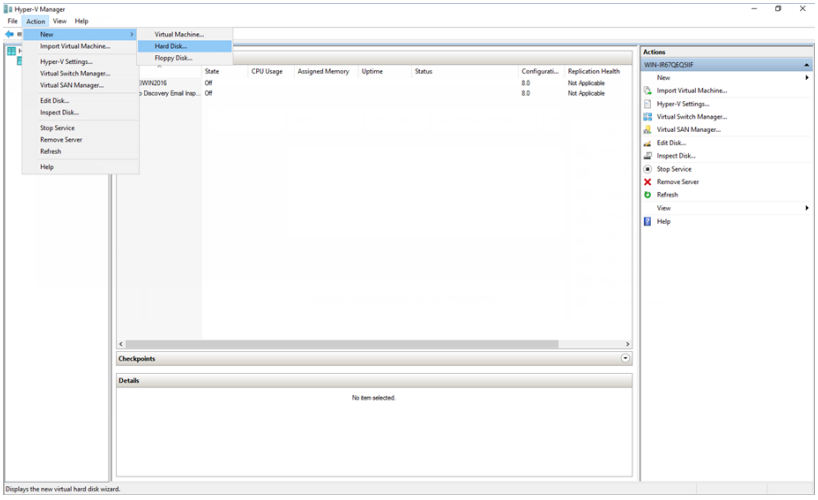
l. [Next] をクリックします。

[Completing the New Virtual Machine Wizard] 画面が表示されます。

m. 仮想マシンの設定が正しいことを確認し、[Finish] をクリックします。

3. 仮想ハードディスクを作成します。

a. Hyper-V マネージャーで、Deep Discovery Email Inspector 仮想マシンを選択し、[Action] > [New] > [Hard Disk] の順に選択します。

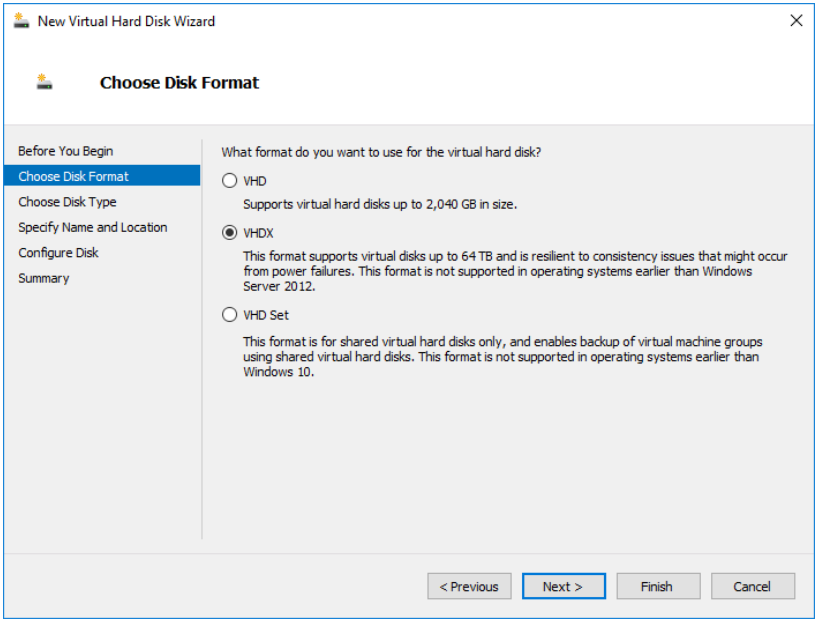


[New Virtual Hard Disk Wizard] 画面が、[Before You Begin] 画面とともに開きます。

b. [Next] をクリックします。

[Choose Disk Format] 画面が表示されます。

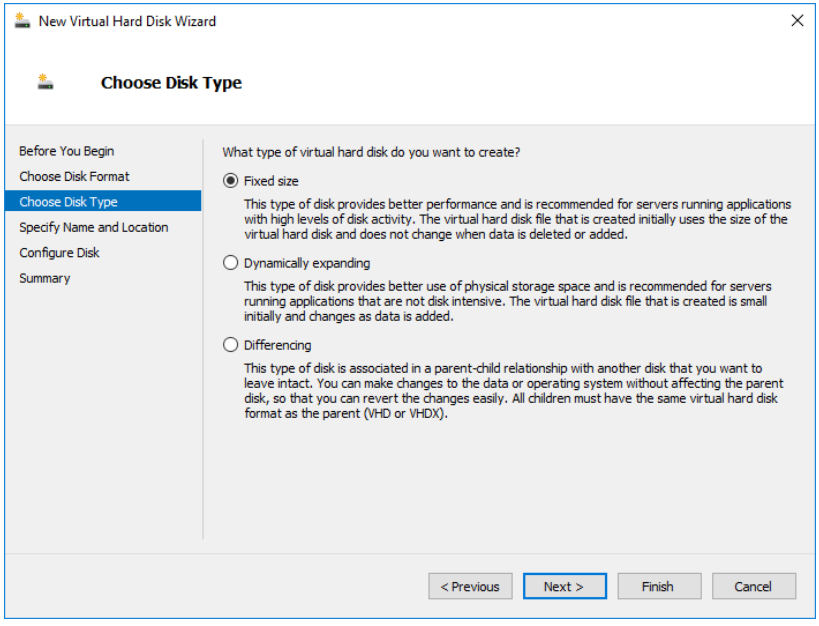
c. [VHDX] を選択します。



d. [Next] をクリックします。

[Choose Disk Type] 画面が表示されます。

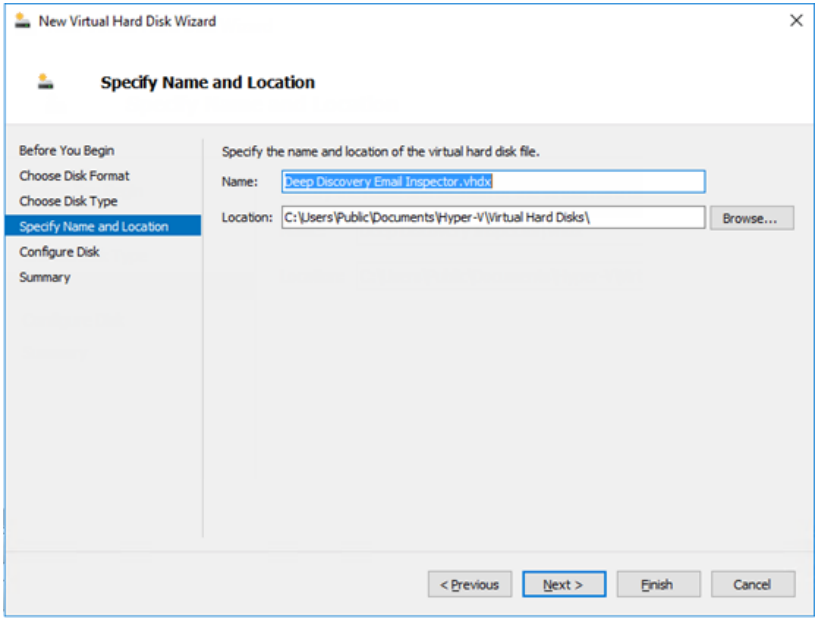
e. [Fixed size] を選択します。



f. [Next] をクリックします。

[Specify Name and Location] 画面が表示されます。

g. [Name] に「`Deep Discovery Email Inspector.vhdx`」と入力します。

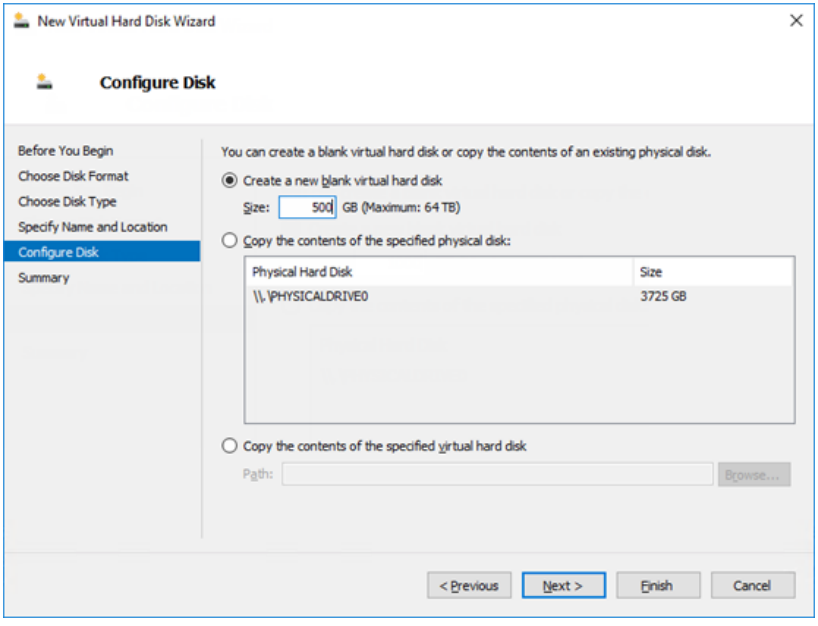


h. [Next] をクリックします。

[Configure Disk] 画面が表示されます。

i. [Create a New blank virtual hard disk] を選択します。

j. [Size] に少なくとも 500GB を指定します。



k. [Next] をクリックします。

[Completing the New Virtual Hard Disk Wizard] 画面が表示されます。

l. 仮想ハードディスクの設定が正しいことを確認し、[Finish] をクリックします。

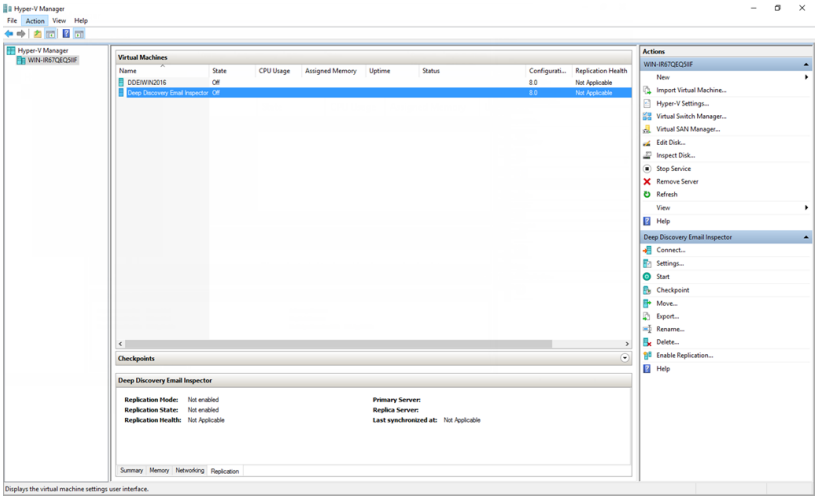
注意

完了には数分かかる場合があります。処理が完了するまで待ち、続行します。

---

4. 仮想マシンを設定します。

a. Hyper-V マネージャーで、Deep Discovery Email Inspector 仮想マシンを選択し、[Action] > [Settings] の順に選択します。

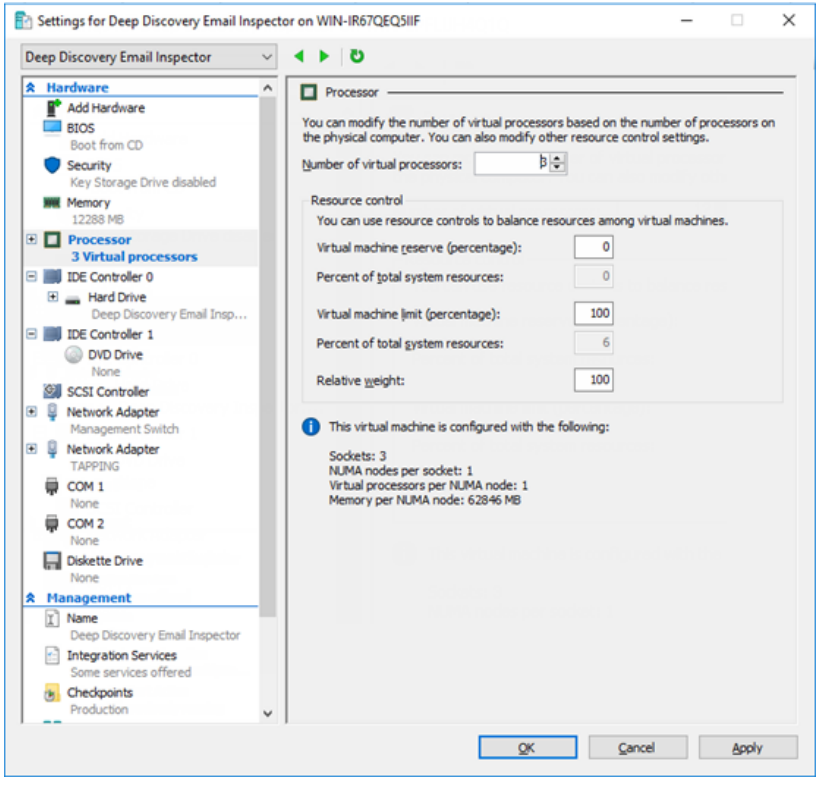


設定画面が表示されます。

b. 左側のペインで、[Processor] をクリックします。

[Processor] の設定が表示されます。

c. [Number of virtual processors] に、少なくとも 3 つの仮想プロセッサを指定します。

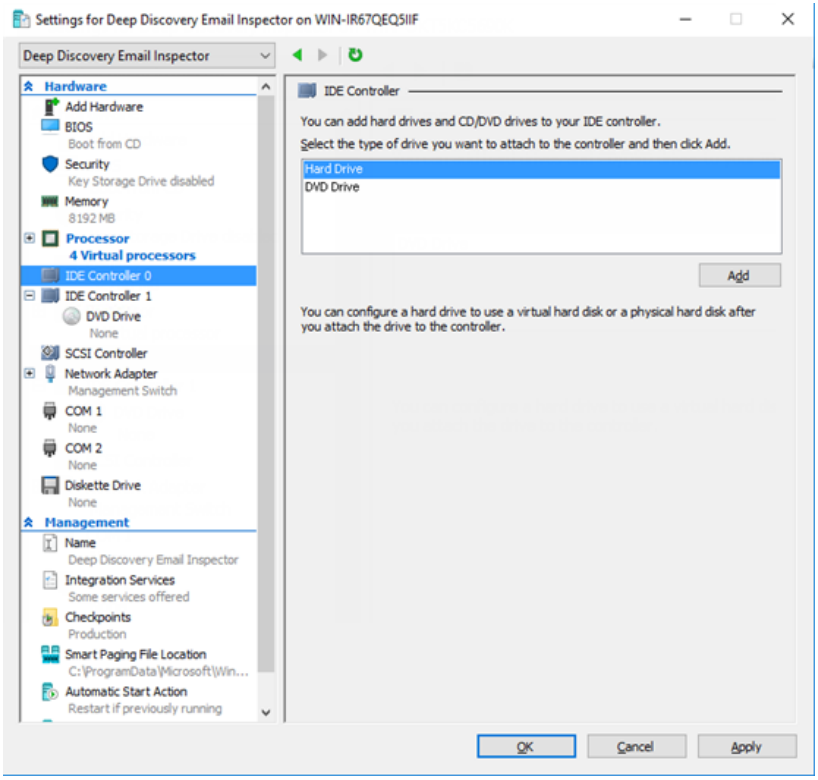


d. [Apply] をクリックします。

e. 左側のペインで、[IDE Controller 0] をクリックします。

   [IDE Controller] の設定が表示されます。

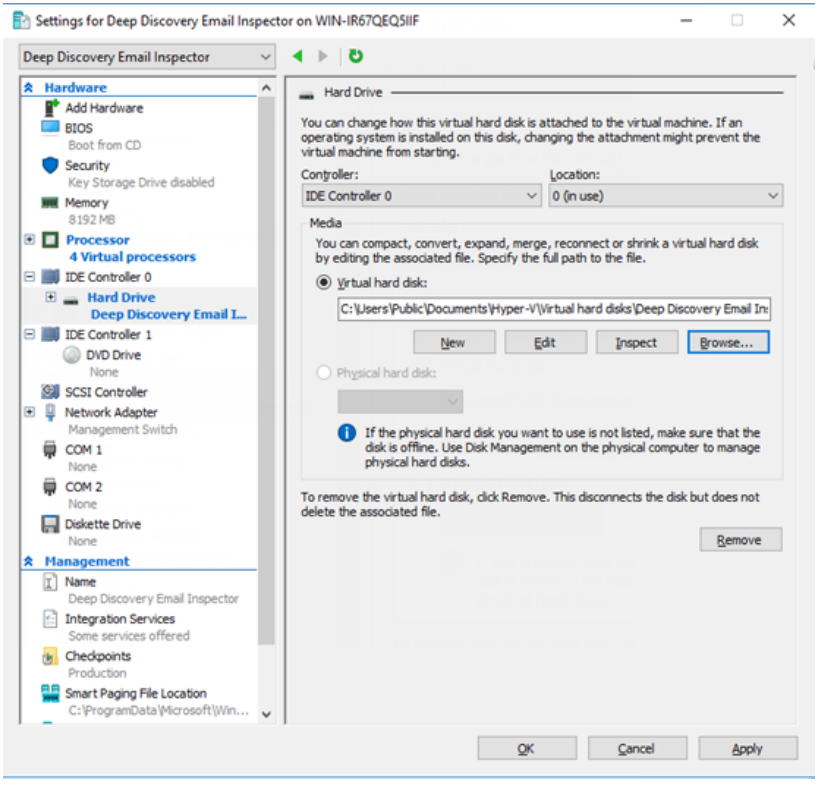
f. コントローラに接続するドライブの種類に、[Hard Drive] を選択します。



g. [Add] をクリックします。

[Hard Drive] の設定が表示されます。

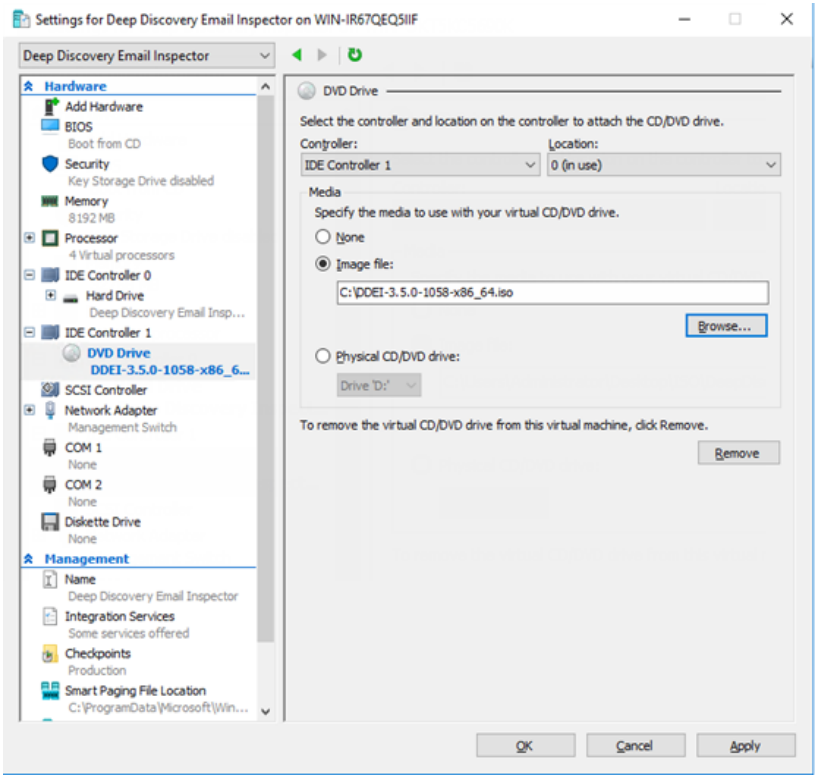
h. [Virtual hard disk] に `Deep Discovery Email Inspector.vhdx` の場所を指定します。



i. 左側のペインで [IDE Controller 1] をクリックし、[DVD Drive] をクリックします。

   [DVD Drive] の設定が表示されます。

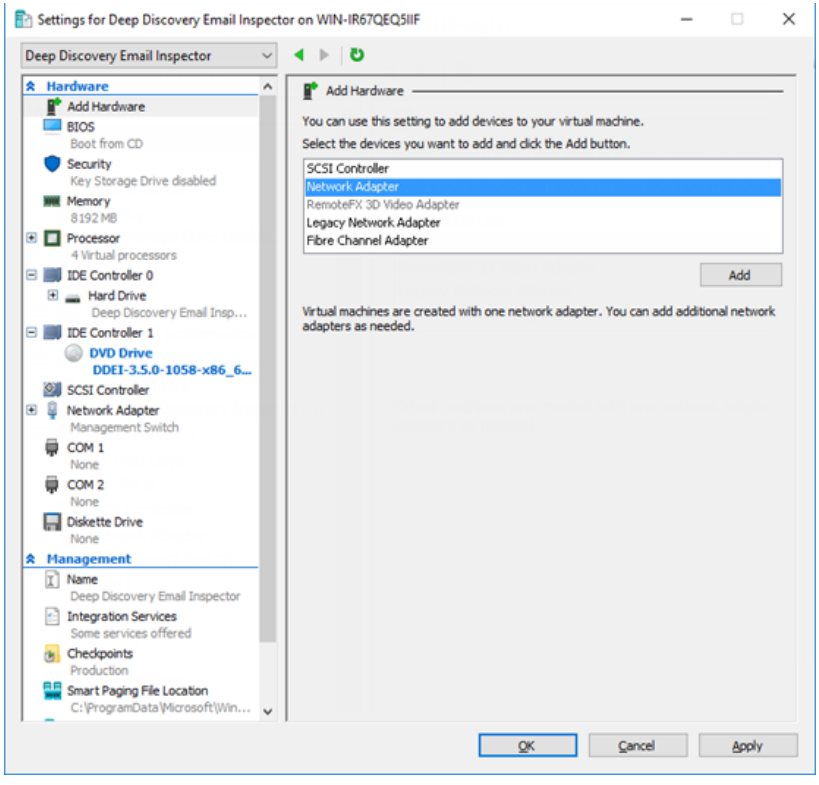
j. [Media] に [Image file] を選択し、Deep Discovery Email Inspector の ISO ファイルの場所を指定します。



k. 左側のペインで、[Add Hardware] をクリックします。

[Add Hardware] の設定が表示されます。

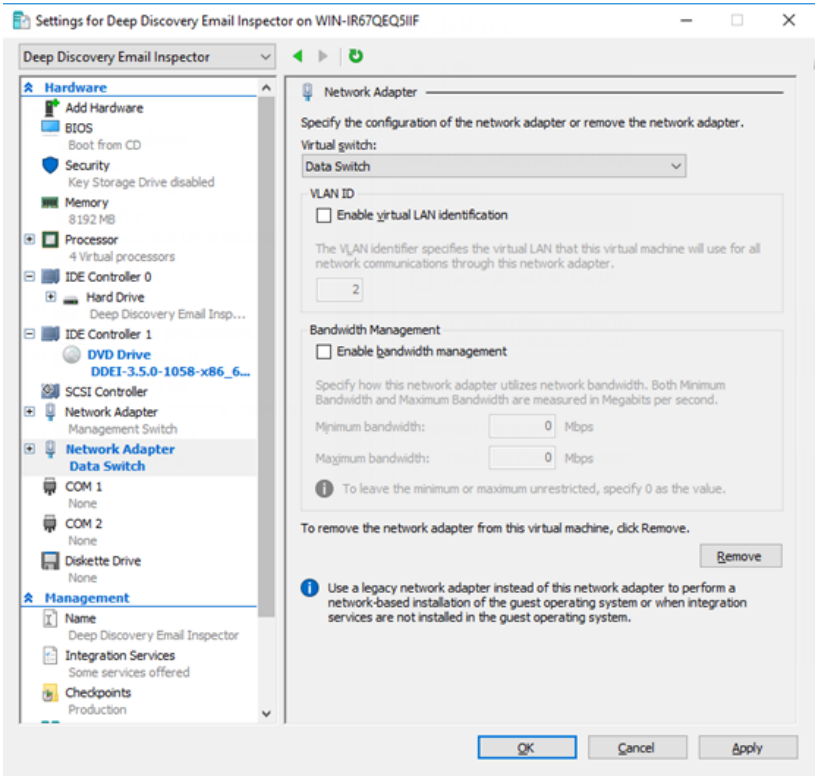
l. 追加するデバイスに [Network Adapter] を選択します。



m. [Add] をクリックします。

[Network Adapter] の設定が表示されます。

n. [Virtual switch] で [Data Switch] を選択します。



o. [Apply] をクリックします。

p. [OK] をクリックします。

第 7 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/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。

索引

や