# Deep Discovery™ Inspector 6.7

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。

商標について

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

P/N: APEM69874/231211_JP (2024/03)

### 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


## パート I：はじめに

### 第 1 章：はじめに

Deep Discovery Inspector について ..... 4
新機能 ..... 4
機能と利点 ..... 5
脅威の管理機能 ..... 5
APT 攻撃シーケンス ..... 6
ホストの重大度 ..... 7
高度な脅威検索エンジン ..... 10
仮想アナライザ ..... 10

## パート II：ハードウェアアプライアンスのインストールと導入

### 第 2 章：システムについて

パッケージの内容 ..... 16
Deep Discovery Inspector アプライアンス ..... 17
前面パネル ..... 18
前面パネル — 1300 アプライアンス ..... 18
前面パネル — 4300/9300 アプライアンス ..... 19
背面パネル ..... 19
背面パネル — 1300 アプライアンス ..... 20
背面パネル — 4300/9300 アプライアンス ..... 21
ネットワークカード ..... 23
ポートの順番 ..... 23
ポートの順番 - 1300 アプライアンス ..... 23
ポートの順番 - 4300/9300 アプライアンス ..... 23
NIC インジケータ ..... 25
NIC インジケータ — 1300 ..... 25

NIC インジケータ — 4300/9300 ..... 27
データポートのインジケータ — 4300/9300 1Gbps ..... 28
データ NIC のインジケータ — 4300/9300 10/25Gbps ..... 30
電源装置のインジケータ ..... 31
ハードウェアの設定 ..... 32

## 第 3 章：ハードウェアアプライアンスの導入

導入の概要 ..... 36
ハードウェアアプライアンスの 導入計画 ..... 36
導入シナリオ ..... 37
アウトオブバンド ..... 38
中継リンクのミラーリング ..... 38
複数ポートの監視 ..... 39
ネットワーク TAP の監視 ..... 40
プロキシの監視 ..... 41
冗長化されたネットワーク ..... 43
リモートポートまたは VLAN ミラーリング ..... 43
単一ポートの監視 ..... 44
VLAN ベースポートの監視 ..... 46
VMware ポートミラーリング ..... 46
インライン ..... 46
透過型ブリッジ ..... 46
ハードウェアアプライアンスのインストール 要件 ..... 48
ハードウェアアプライアンスのシステム 要件 ..... 49
ハードウェアアプライアンスの 要件 ..... 49
事前設定コンソールの要件 ..... 50
管理コンソールの要件 ..... 50
仮想アナライザイメージの OS の要件 ..... 51

## 第 4 章：ハードウェアアプライアンスへのインストール

オプションの設定 ..... 54
Chrome の JavaScript オプションの設定 ..... 54
Firefox の JavaScript オプションの設定 ..... 54

Deep Discovery Inspector ハードウェアアプライアンスのインストール ..... 55
光学ディスクドライブのあるハードウェアアプライアンスへの Deep Discovery Inspector のインストール ..... 55
光学ディスクドライブのないハードウェアアプライアンスへの Deep Discovery Inspector のインストール ..... 61
製品出荷時のモードへの復元 ..... 66

第 5 章：VMware 仮想分散スイッチでのポートミラーリング

VMware vSphere Distributed Switch (VDS) の作成 ..... 68
Deep Discovery Inspector ハードウェアアプライアンスと VDS ..... 70
ハードウェアアプライアンス - カプセル化されたリモートミラーリングによりミラーリングされたトラフィックの VDS からの監視の設定 ..... 71
ハードウェアアプライアンス - リモートミラーリングによりミラーリングされたトラフィックの VDS からの監視の設定 ..... 76

パート III：仮想アプライアンスのインストールと導入

第 6 章：仮想アプライアンスの導入

導入の概要 ..... 84
仮想アプライアンスの導入計画 ..... 84
導入シナリオ ..... 85
VMware ポートミラーリング ..... 86
仮想アプライアンスのインストール要件 ..... 86
仮想アプライアンスのシステム要件 ..... 87
仮想ホストアプライアンスの要件 ..... 87
管理コンソールの要件 ..... 88

## 第 7 章：仮想アプライアンスの新規作成

VMWare ESXi 仮想アプライアンスの 作成 ..... 92
VMware ESXi での仮想マシンの要件 ..... 92
VMware ESXi サーバネットワークの設定 ..... 92
VMware ESXi での仮想マシンの作成 ..... 97
VMware ESXi のハードウェア仮想化支援機能を有効にする ..... 103
Microsoft Hyper-V 仮想アプライアンスの作成 ..... 104
Microsoft Hyper-V で仮想マシンを作成する ..... 104
Microsoft Hyper-V でのトラフィックのミラーリングの設定 ..... 127
Microsoft Hyper-V で外部トラフィックのミラーリングを設定する ..... 127
Microsoft Hyper-V で内部仮想マシントラフィックのミラーリングを設定する ..... 129

## 第 8 章：仮想アプライアンスへのインストール

オプションの設定 ..... 132
Chrome の JavaScript オプションの設定 ..... 132
Firefox の JavaScript オプションの設定 ..... 132
ESXi での仮想アプライアンスのオプションの 設定 ..... 133
Deep Discovery Inspector 仮想アプライアンスのインストール ..... 134

## 第 9 章：VMware 仮想分散スイッチでのポートミラーリング

VMware vSphere Distributed Switch (VDS) の作成 ..... 140
Deep Discovery Inspector 仮想アプライアンスと VDS ..... 142
VDS を使用する仮想アプライアンスの要件 ..... 143
仮想アプライアンス - ミラーリングされた外部ネットワークトラフィックの VDS を使用した監視 ..... 145
仮想アプライアンス - カプセル化されたリモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視の設定 ..... 146

仮想アプライアンス - リモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視の設定 ..... 149
仮想アプライアンス - ミラーリングされた仮想マシントラフィックの VDS からの監視 ..... 153
仮想アプライアンス - ミラーリングされたトラフィックの異なる ESXi ホストからの監視 ..... 153
仮想アプライアンス - カプセル化されたリモートミラーリングによりミラーリングされた仮想マシントラフィックの監視の設定 ..... 154
仮想アプライアンス - リモートミラーリングによりミラーリングされた仮想マシントラフィックの監視の設定 ..... 159
仮想アプライアンス - ミラーリングされたトラフィックの同じ ESXi ホストからの監視 ..... 165
仮想アプライアンス - VDS での分散ポートミラーリングの設定 ..... 166

パート IV：インストール後

第 10 章：事前設定

事前設定コンソール ..... 174
事前設定コンソールへのアクセス ..... 174
VGA ポートを使用した事前設定コンソールへのアクセス ..... 175
シリアルポートを使用した事前設定コンソールへのアクセス ..... 175
事前設定コンソールのメインメニュー ..... 176
アプライアンス情報とステータスの表示 ..... 177
デバイス設定の変更 ..... 178
インタフェース設定の変更 ..... 180

第 11 章：システムタスク

システムタスクの概要 ..... 184
診断テストの実行 ..... 184

Ping テストの実行 ..... 185
Deep Discovery Inspector の再起動 ..... 186
管理者パスワードの変更 ..... 187
ログオフ ..... 187
手動のトラフィックバイパスの 設定 ..... 188

## 第 12 章：トラブルシューティング

よくある質問 (FAQ) ..... 190
FAQ - アプライアンスの復元 ..... 190
FAQ - 設定 ..... 191
FAQ - 検出 ..... 191
FAQ - 設置 ..... 191
FAQ - アップグレード ..... 192
FAQ - 仮想アナライザイメージ ..... 192
トラブルシューティング ..... 193
管理コンソールの応答が遅くなります ..... 193
検出 ..... 194
[すべての検出] 画面に検出が表示されません ..... 194
[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 ..... 195
不明な IP アドレスが画面に表示されます ..... 195
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 ..... 196
[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 ..... 196
仮想アナライザ ..... 196
OVA をアップロードできません ..... 196
仮想アナライザがファイルの送信に応答しません .... 197
仮想アナライザのイメージ ..... 198
インストール CD/DVD が起動しません ..... 198
[Found New Hardware] ウィザード ..... 198
イメージによるブルースクリーンの 表示 ..... 199
ネットワークサービスに接続できない ..... 199
診断 ..... 200
インライン導入と TLS インスペクション ..... 201
ネットワーク接続の問題 ..... 201
TLS 接続の問題 ..... 203

# パート V：テクニカルサポート


## 第 13 章：トラブルシューティングのリソース

サポートポータルの利用 ..... 208

脅威データベース ..... 208

## 第 14 章：製品サポート情報

サポートサービスについて ..... 210

## 第 15 章：トレンドマイクロへのウイルス解析依頼

メールレピュテーションについて ..... 212

ファイルレピュテーションについて ..... 212

Web レピュテーションについて ..... 212

## 第 16 章：その他のリソース

最新版ダウンロード ..... 214

脅威解析・サポートセンター TrendLabs (トレンドラボ) ..... 214

## 付録 A：アプライアンスで使用されるポート

## 索引

索引 ..... 225

# 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。<br><br>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。<br><br>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 |

# パート I

## はじめに

# 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。


- 4 ページの「Deep Discovery Inspector について」
- 5 ページの「機能と利点」
- 5 ページの「脅威の管理機能」
- 6 ページの「APT 攻撃シーケンス」
- 7 ページの「ホストの重大度」
- 10 ページの「高度な脅威検索エンジン」
- 10 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 Inspector6.7 の新機能を示しています。

| 機能 | 詳細 |
|---|---|
| Trend Vision One からの一元管理 | Trend Vision One の Network Inventory アプリを使用して、Deep Discovery Inspector の次の設定を管理できるようになります。<br>• 検出の除外設定<br>• パケットキャプチャ<br>• SSH アクセス<br>• ハイパーセンシティブモード |
| Service Gateway を使用した Trend Vision One への接続 | Service Gateway をプロキシとして使用し、Deep Discovery Inspector から Trend Vision One に接続できるようになります。 |
| 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。<br>• スループット情報: Deep Discovery Inspector から Trend Vision One の [監視対象のネットワークスループット] ウィジェットに、ネットワークスループットログを送信できるようになります。<br>• ネットワークセキュリティ設定: Deep Discovery Inspector から Trend Vision One に、ユーザ設定やその他の使用統計を送信できるようになります。Deep Discovery Inspector アプライアンスの全体のステータスを、[Executive Dashboard] から確認できます。 |

| 機能 | 詳細 |
| --- | --- |
| 新しいハードウェアアプライアンス | 新しい 4300/9300 Deep Discovery Inspector アプライアンスモデルを使用できるようになります。 |
| ハイパーバイザのサポートの強化 | Deep Discovery Inspector 仮想アプライアンスを次のハイパーバイザに導入できるようになります。<br>• Red Hat Enterprise Linux (RHEL) 9 上の KVM<br>• VMware ESXi 8 |

# 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。


- 5 ページの「脅威の管理機能」
- 6 ページの「APT 攻撃シーケンス」
- 7 ページの「ホストの重大度」
- 10 ページの「高度な脅威検索エンジン」
- 10 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。 |
| 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。<br><br>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。 |

| 段階 | 説明 |
| --- | --- |
| 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。<br>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。<br>C&C 通信により、攻撃者は感染したコンピュータを攻撃してネットワーク内を動き回り、データを抜き出すことができます。 |
| 内部活動 (Lateral Movement) | さらにコンピュータを感染させる攻撃です。<br>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。<br>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)<br>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。<br>• 情報送出<br>• 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。<br>• 既知の APT に関連付けられた IP アドレスへの接続<br>• 既知の APT に関連付けられた URL へのアクセス<br>• 既知の APT に関連付けられたダウンロードファイル<br>• 内部活動の証拠 |

| カテゴリ | レベル | 説明 |
|---|---|---|
| | 8 | ホストは次を示している可能性があります。<br>• 重大度が高のネットワークイベント<br>• 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<br>• 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)<br>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。<br>• 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。<br>• 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。<br>• Web レピュテーションサービスにより検出された危険なサイトへの接続 |
| | 5 | ホストは次を示している可能性があります。<br>• 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。<br>• 重大度が中のネットワークイベント<br>• 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)<br>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。<br>• 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<br>• 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<br>• 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 |

| カテゴリ | レベル | 説明 |
|---|---|---|
| | 2 | ホストは次を示している可能性があります。<br>• 重大度が低のネットワークイベント<br>• 危険な URL を含むメールメッセージを受信した証拠<br>• 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)<br>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。<br>• 重大度が情報のネットワークイベント<br>• 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<br>• 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。

# パート II

# ハードウェアアプライアンスのインストールと導入

# 第 2 章

## システムについて

Deep Discovery Inspector アプライアンスについては、次の項目を参照してください。


- 16 ページの「パッケージの内容」
- 17 ページの「Deep Discovery Inspector アプライアンス」
- 32 ページの「ハードウェアの設定」

# パッケージの内容

ネットワークでアプライアンスを正しく設定するため、Deep Discovery Inspector アプライアンスパッケージの内容物とハードウェアを確認します。

次の図は、Deep Discovery Inspector アプライアンスパッケージに含まれるアイテムを示しています (本ドキュメント記載のアプライアンスより前のモデルをご使用の場合は、購入時同梱のクイックスタートガイドを参照してください)。


図 2-1. パッケージの内容

表 2-1. Deep Discovery Inspector パッケージの内容

| # | 名前 | 説明 |
|---|---|---|
| 1 | スライドおよびレールセット * 1 | アプライアンスは固定するか (固定取り付け)、4 柱ラックにスライド可能な状態で取り付けます (スライド取り付け)。<br><br>**注意**<br>パッケージの出荷時、レールはスライドに組み付けられています。アプライアンスを取り付ける際は、スライドからレールを外してください。 |

| # | 名前 | 説明 |
|---|---|---|
| 2 | Deep Discovery Inspector 用トレンドマイクロインストール DVD * 1<br><br>Deep Discovery Inspector クイックスタートガイド * 1 | インストール DVD には、インストールイメージと、次の PDF ドキュメントが含まれています。<br>• Deep Discovery Inspector 管理者ガイド<br>• Deep Discovery Inspector インストールガイド<br>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。 |
| 3 | 電源コード * 2 | アプライアンスに電源を供給します (長さは 79 インチ/200cm) |
| 4 | Deep Discovery Inspector * 1 | アプライアンス本体 |

# Deep Discovery Inspector アプライアンス

Deep Discovery Inspector 6.7 では、次のハードウェアアプライアンスモデルがサポートされます。モデル番号は、物理アプライアンスの 前面ステッカーで確認できます。

- 260 (詳細はクイックスタートガイドを 参照してください)
- 270 (詳細はクイックスタートガイドを 参照してください)
- 1100
- 1200
- 1300
- 4100
- 4200
- 4300
- 9200
- 9300

# 前面パネル

## 前面パネル – 1300 アプライアンス

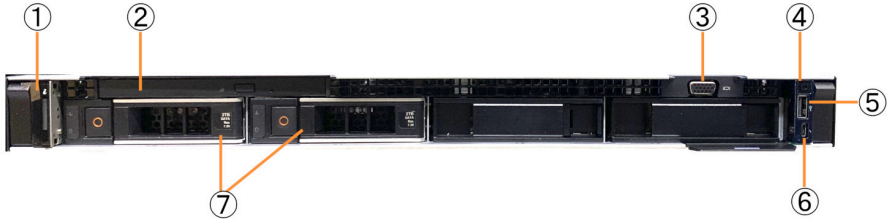



図 2-2. Deep Discovery Inspector 1300 の前面パネル

次の表は、1300 アプライアンスの前面パネルの機能を示しています。

| 番号 | 機能 | 説明 |
|---|---|---|
| 1 | ステータス LED インジケータ | システム ID、ステータス情報、システムエラーメッセージを表示します。 |
| 2 | 光学ディスクドライブ | DVD ドライブ |
| 3 | ビデオコネクタ | VGA ディスプレイをアプライアンスに接続します。 |
| 4 | 電源インジケータ<br>電源ボタン | • システムの電源がオンのときに点灯します。<br>• アプライアンスへの電源の出力を制御します。 |
| 5 | USB コネクタ | キーボードやマウスなどの USB デバイスをアプライアンスに接続します。 |
| 6 | iDRAC ダイレクトポート (Micro-AB USB) | iDRAC ダイレクト (Micro-AB) の機能にアクセスできるようになります。 |
| 7 | ハードドライブ * 2 | 3.5 インチ、ホットスワップ対応ハードドライブ |

## 前面パネル – 4300/9300 アプライアンス


図 2-3. Deep Discovery Inspector 4300/9300 の前面パネル

次の表は、4300/9300 アプライアンスの前面パネルの機能を示しています。

| 番号 | 機能 | 説明 |
|---|---|---|
| 1 | ステータス LED インジケータ | システム ID、ステータス情報、システムエラーメッセージを表示します。 |
| 2 | 前面の識別ボタン/インジケータ | Deep Discovery Inspector ではサポートされていません。 |
| 3 | 電源ボタン/インジケータ | • システムの電源がオンのときに点灯します。<br>• アプライアンスへの電源の出力を制御します。 |
| 4 | USB コネクタ | USB デバイスをアプライアンスに接続できます。 |
| 5 | ビデオコネクタ | VGA ディスプレイをアプライアンスに接続できます。 |
| 6 | iDRAC ダイレクトポート (Micro-AB USB) | iDRAC ダイレクト (Micro-AB) の機能にアクセスできるようになります。 |
| 7 | ハードドライブ * 4 | 3.5 インチ、ホットスワップ対応ハードドライブ |

## 背面パネル

## 背面パネル — 1300 アプライアンス

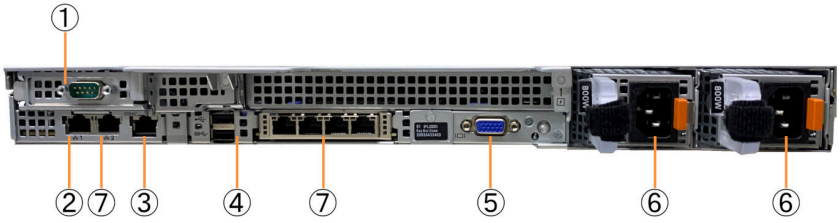



図 2-4. Deep Discovery Inspector 1300 の背面パネル

次の表は、1300 アプライアンスの背面パネルの機能を示しています。

| 番号 | 機能 | 説明 |
|---|---|---|
| 1 | RS-232 シリアルコネクタ | RS-232 タイプの接続でコンピュータのシリアルポートに接続して事前設定を行います。 |
| 2 | 管理ポート | 他の製品やサービスと通信してデータをやり取りするための管理ネットワークに接続します。 |
| 3 | iDRAC ポート | iDRAC カードの専用管理ポートに接続します。 |
| 4 | USB コネクタ * 2 | キーボードやマウスなどの USB デバイスをアプライアンスに接続します。 |
| 5 | ビデオコネクタ | VGA ディスプレイをアプライアンスに接続します。 |

| 番号 | 機能 | 説明 |
|---|---|---|
| 6 | 電源コネクタ * 2 | 800W ホットプラグ電源装置 2 つ:<br>• メイン電源<br>• バックアップ電源<br><br>注意<br>「ホットプラグ」とは、アプライアンスの実行中に電源を交換できる機能のことです。Deep Discovery Inspector では、操作の中断やリスクを発生させることなく、電源交換を自動的かつ安全に認識します。<br><br>パッケージに含まれる電源コードを使用してください (詳細は、16 ページの「パッケージの内容」を参照)。 |
| 7 | データポート * 5 | 統合された 1Gbps NIC コネクタ 5 つ |

## 背面パネル – 4300/9300 アプライアンス

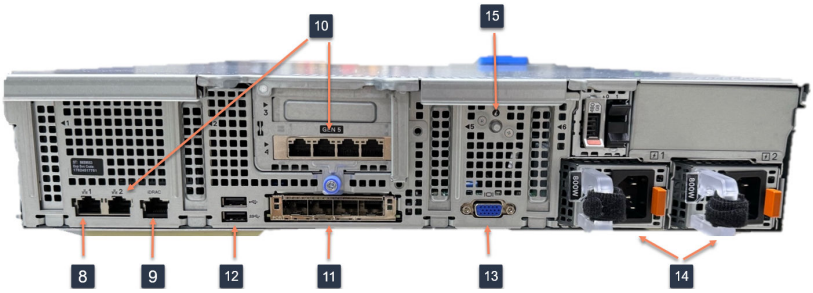



図 2-5. Deep Discovery Inspector 4300/9300 の背面パネル

次の表は、4330/9300 アプライアンスの 背面パネルの機能を示しています。

| 番号 | 機能 | 説明 |
|---|---|---|
| 8 | 管理ポート | 他の製品やサービスと通信してデータをやり取りするための管理ネットワークに接続します。 |
| 9 | iDRAC ポート | iDRAC カードの専用管理ポートに接続します。 |
| 10 | 1Gbps データポート * 5 | 統合された 10/100/1000Mbps Base-T NIC コネクタ 5 つ |
| 11 | 10/25Gbps データポート * 4 | 10/25Gbps NIC コネクタ 4 つ |
| 12 | USB コネクタ * 2 | キーボードやマウスなどの USB デバイスをアプライアンスに接続します。 |
| 13 | ビデオコネクタ | VGA ディスプレイをアプライアンスに 接続します。 |
| 14 | 電源コネクタ * 2 | 800W (4300) または 1100W (9300) ホットプラグ電源装置 2 つ (ワット数についてはデバイスのラベルを参照):<br>• メイン電源<br>• バックアップ電源<br>注意<br>「ホットプラグ」とは、アプライアンスの実行中に電源を交換できる機能のことです。Deep Discovery Inspector では、操作の中断やリスクを発生させることなく、電源交換を自動的かつ安全に認識します。<br>パッケージに含まれる電源コードを使用してください (詳細は、16 ページの「パッケージの内容」を参照)。 |
| 15 | アプライアンスの識別ボタン/アプライアンスのステータスインジケータ | Deep Discovery Inspector ではサポートされていません。 |

# ネットワークカード

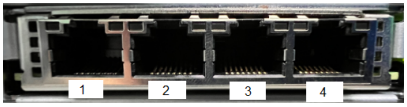
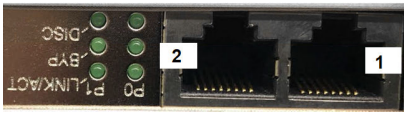
## ポートの順番

### ポートの順番 - 1300 アプライアンス


**ヒント**

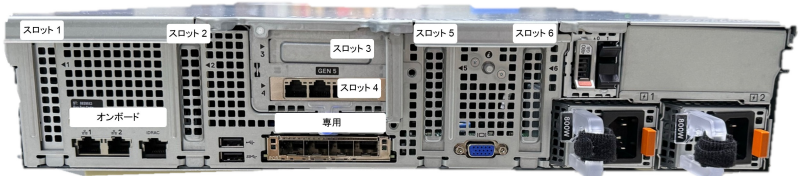
カードスロットの詳細については、Deep Discovery Inspector 管理コンソールの [管理] > [システム設定] > [ネットワークインタフェース] で確認できます。

次の表は、1300 アプライアンスのネットワークカードのポートの順番を示しています。

| NIC | スロット | ポートの順番 |
|---|---|---|
| Dedicated_Quad_Port_1GbE_Copper | 専用 |  |
| Dual_Port_1GbE_Copper_Bypass_Card | スロット 1 |  |
| Dual_Port_10GbE_Fiber-SR_Bypass_Card | スロット 1 |  |

### ポートの順番 - 4300/9300 アプライアンス

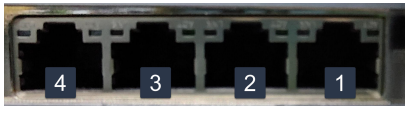
カードスロットの詳細については、Deep Discovery Inspector 管理コンソールの [管理] > [システム設定] > [ネットワークインタフェース] で確認できます。

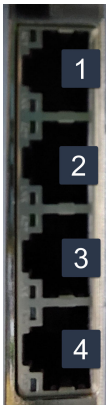
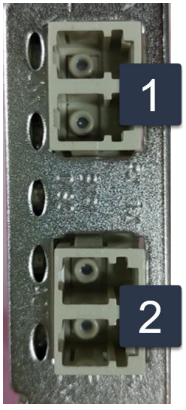



**重要**

- スロット 1 は RAID コントローラです。
- スロット 5 およびスロット 6 は、4300 アプライアンスでは使用できません。

次の表は、4300/9300 アプライアンスのネットワークカードのポートの順番を示しています。

| NIC | スロット | ポートの順番 |
|---|---|---|
| Dedicated_Quad_Port_10/25GbE_SFP28 | • 専用 |  |
| Quad_Port_1GbE_Copper | • スロット 3<br>• スロット 4 |  |

| NIC | スロット | ポートの順番 |
|---|---|---|
| | • スロット 2<br>• スロット 5 (9300 のみ)<br>• スロット 6 (9300 のみ) |  |
| Dual_Port_10GbE_Fiber-SR_Bypass_Card | スロット 2 |  |

## NIC インジケータ

### NIC インジケータ — 1300

アウトオブバンド導入向けに、Deep Discovery Inspector 1300 にはユーザ設定可能な銅線ベースの Ethernet NIC ポートが 5 つあります。いずれも、統合された 10/100/1000Mbps コネクタを使用できます。

各ポートには現在の状態を示すインジケータがあります。

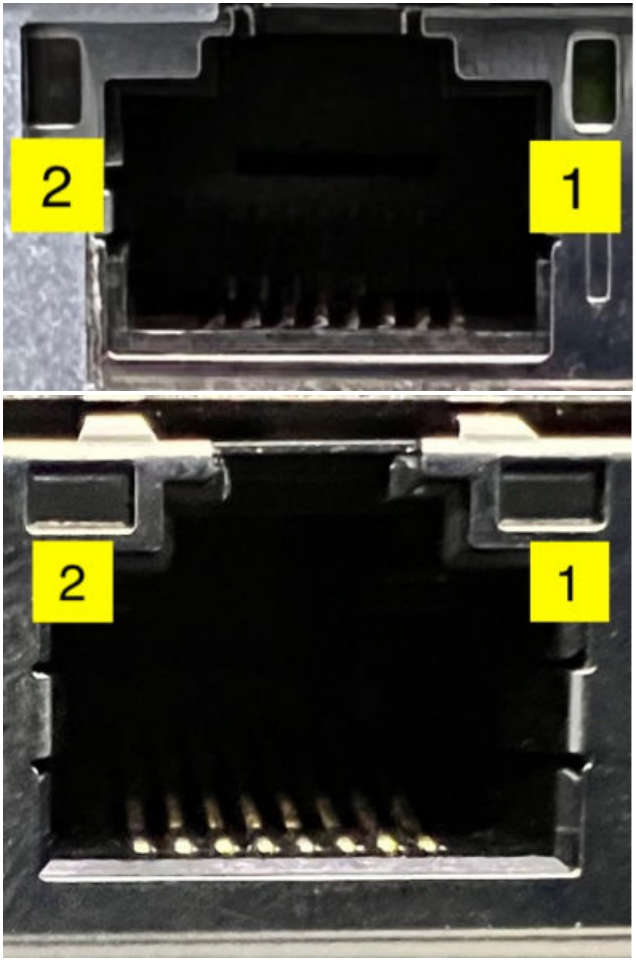



図 2-6. Deep Discovery Inspector 1300 アプライアンスの 2 種類のポート

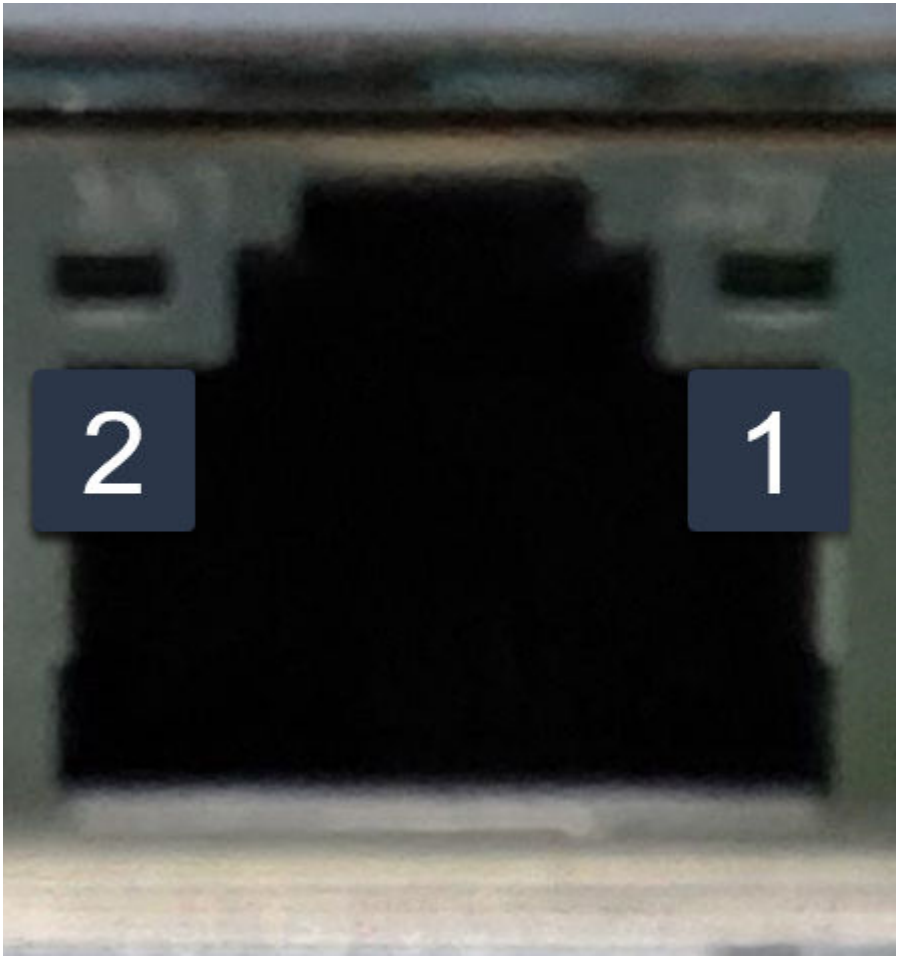
次の表は、1300 アプライアンスの NIC インジケータについて説明しています。

| インジケータ | 説明 | インジケータのパターン |
|---|---|---|
| 1 | 接続ステータスとデータアクティビティステータスを示します。 | • 消灯: ネットワークに接続されていません。<br>• 緑色の点滅: ネットワークデータを送受信しています。 |
| 2 | データ転送速度を示します。 | • 黄色: 10Mbps または 100Mbps<br>• 緑色: 1000Mbps |

### NIC インジケータ — 4300/9300

### データポートのインジケータ — 4300/9300 1Gbps

各ポートには現在の状態を示すインジケータがあります。




次の表は、4300/9300 アプライアンスの 1Gbps ポートのインジケータについて説明しています。

| インジケータ | 説明 | インジケータのパターン |
| --- | --- | --- |
| 1 | 接続ステータスとデータアクティビティステータスを示します。 | • 消灯: ネットワークに接続されていません。<br>• 緑色の点滅: データを送受信しています。 |
| 2 | データ転送速度を示します。 | • 黄色: 10Mbps または 100Mbps<br>• 緑色: 1000Mbps |

### データ NIC のインジケータ — 4300/9300 10/25Gbps

各ポートには現在の状態を示すインジケータがあります。

次の表は、4300/9300 アプライアンスの 10/25Gbps NIC のインジケータについて説明しています。

| インジケータ | 説明 | インジケータのパターン |
|---|---|---|
| 1 | 接続ステータスとデータアクティビティステータスを示します。 | • 消灯: ネットワークに接続されていません。<br>• 緑色の点滅: ネットワークデータを送受信しています。 |
| 2 | データ転送速度を示します。 | • 黄色: 10Gbps<br>• 緑色: 25Gbps |

## 電源装置のインジケータ

次の表は、電源装置のステータスインジケータを示しています。

| インジケータのパターン | 説明 |
|---|---|
| 消灯 | 電源が接続されていません。 |
| 緑色 | 有効な電源が電源装置に接続されており、電源装置が動作しています。 |
| 緑色で点滅 | 電源装置をホットアドする場合に、その電源装置が他の電源装置と (効率性、機能セット、状態ステータス、およびサポートされる電圧において) 一致していないことを示します。<br>インジケータが点滅している電源装置を、その他のインストール済みの電源装置の容量と一致する電源装置に交換します。 |

| インジケータのパターン | 説明 |
| --- | --- |
| 黄色で点滅 | 電源装置に問題があることを示します。<br><br>**重要**<br>電源装置の不一致を修正する際は、インジケータが点滅している電源装置のみを交換してください。反対の電源装置を交換すると、エラー状態や予期しないシステムのシャットダウンが発生する可能性があります。<br><br>高出力設定から低出力設定、またはその逆に変更する場合は、最初にシステムの電源を切ります。<br><br>AC 電源装置では、220V および 110V の両方の入力電圧がサポートされます。2 つの同じ電源装置に異なる入力電圧がかかる場合は、それらが異なるワット数を出力し、不一致が発生することがあります。<br><br>2 つの電源装置を使用する場合は、それらが同じ種類であり、同じ最大電力を出力する必要があります。 |

# ハードウェアの設定

**手順**

1. アプライアンスは、標準の 19 インチの 4 柱ラック、または丈夫な机などの独立したオブジェクトに設置します。

   **注意**
   アプライアンスを設置する際は、適切な換気と冷却を確保するために周囲に 5cm 以上の空間を設けてください。

2. アプライアンスを電源に接続します。

   Deep Discovery Inspector には 2 つの電源装置があります。1 つはメイン電源として、もう 1 つはバックアップ電源として機能します。

3. モニタを背面パネルの VGA ポートに接続します。

   19 ページの「背面パネル」の図を参照してください。

4. キーボードとマウスを背面パネルの USB ポートに接続します。

5. 管理ポートをネットワークに接続します。

6. アプライアンスの電源をオンにします。

   電源ボタンは、アプライアンスの前面パネルのベゼルの奥にあります。
   18 ページの「前面パネル」の図を参照してください。

次のような画面が表示されます。

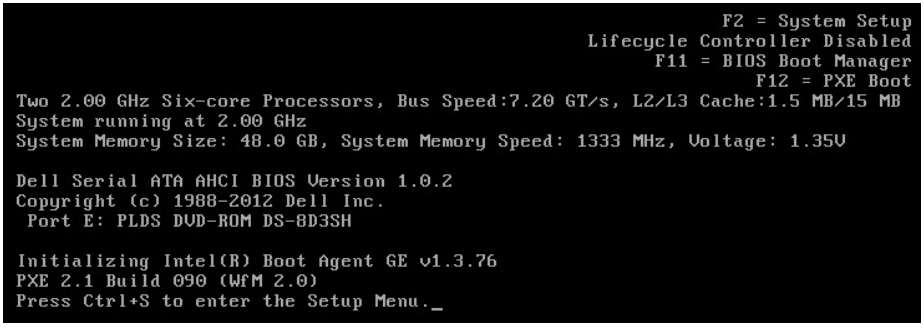



図 2-7. パワーオンセルフテスト (POST)

### 次に進む前に

可能な場合は、事前設定コンソールを使用して最初の事前設定を行います。
詳細については、173 ページの事前設定を参照してください。

# 第 3 章

# ハードウェアアプライアンスの導入

Deep Discovery Inspector ハードウェアアプライアンスをインストールする際のヒント、推奨事項、および要件について、次の項目を参照してください。

# 導入の概要

**手順**

1. 導入を計画します。

   36 ページの「ハードウェアアプライアンスの 導入計画」を参照してください。

2. インストール要件を確認します。

   48 ページの「ハードウェアアプライアンスのインストール 要件」を参照してください。

3. システム要件を確認します。

   49 ページの「ハードウェアアプライアンスのシステム 要件」を参照してください。

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

   53 ページのハードウェアアプライアンスへのインストール を参照してください。

5. Deep Discovery Inspector を事前設定します。

   173 ページの事前設定を参照してください。

# ハードウェアアプライアンスの導入計画

Deep Discovery Inspector の最善の導入方法を計画するには、次を実行します。

- 保護を必要とするネットワークセグメントを特定します。
- メール、Web、およびアプリケーションサーバなどの 運用に欠かせないアプライアンスの 場所を考慮して、ネットワークトラフィックについて計画します。
- セキュリティニーズを 満たすために必要なアプライアンスの 数と、それらのネットワーク上の場所を特定します。
- ネットワークのテストセグメント上でパイロット導入を実施します。

- パイロット導入の結果に基づいて、導入戦略を再定義します。
- 次の例を使用して、カスタマイズされた Deep Discovery Inspector の導入を計画します。

## 導入シナリオ

Deep Discovery 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導入できます。

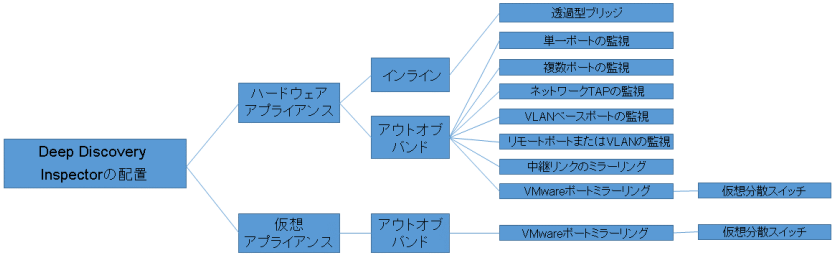
- ハードウェアアプライアンス: Deep Discovery Inspector をインラインアプライアンスまたはアウトオブバンドアプライアンスとして 導入できます。
  - インライン: Deep Discovery Inspector は透過型ブリッジとして機能し、復号された TLS トラフィックを検査します。インラインアプライアンスとして導入した場合、インラインポートを流れるトラフィックのみが検査されます。

    **注意**

    インライン導入では、インライン (LAN Bypass) ネットワークインタフェースカードを追加でインストールする必要があります。インストール手順および互換性のある Deep Discovery Inspector アプライアンスモデルについては、「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。

  - アウトオブバンド: Deep Discovery Inspector は、スイッチのミラーポートに接続することで、ネットワークの切断を発生させることなく、または最小限に留めながらネットワークトラフィックを監視します。アウトオブバンドアプライアンスとして 導入した場合、データポートにミラーリングされたトラフィックのみが検査されます。
- 仮想アプライアンス: Deep Discovery Inspector はアウトオブバンドアプライアンスとしてのみ導入できます。Deep Discovery Inspector は、スイッチのミラーポートに接続することで、ネットワークの切断を発生させることなく、または最小限に留めながらネットワークトラフィックを監視します。

次の図は、サポートされる導入の概要を示しています。



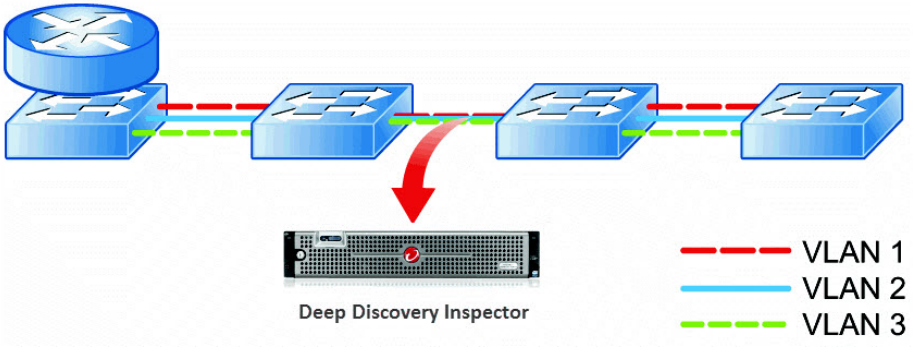

## アウトオブバンド

アウトオブバンド導入では、Deep Discovery Inspector はスイッチのミラーポートに接続することで、ネットワークの切断を発生させることなく、または最小限に留めながらネットワークトラフィックを監視します。

### 中継リンクのミラーリング

複数の VLAN が同一の物理リンクをカプセル化する場合は、中継リンクからの送信元ポートをミラーリングします。Deep Discovery Inspector での双方

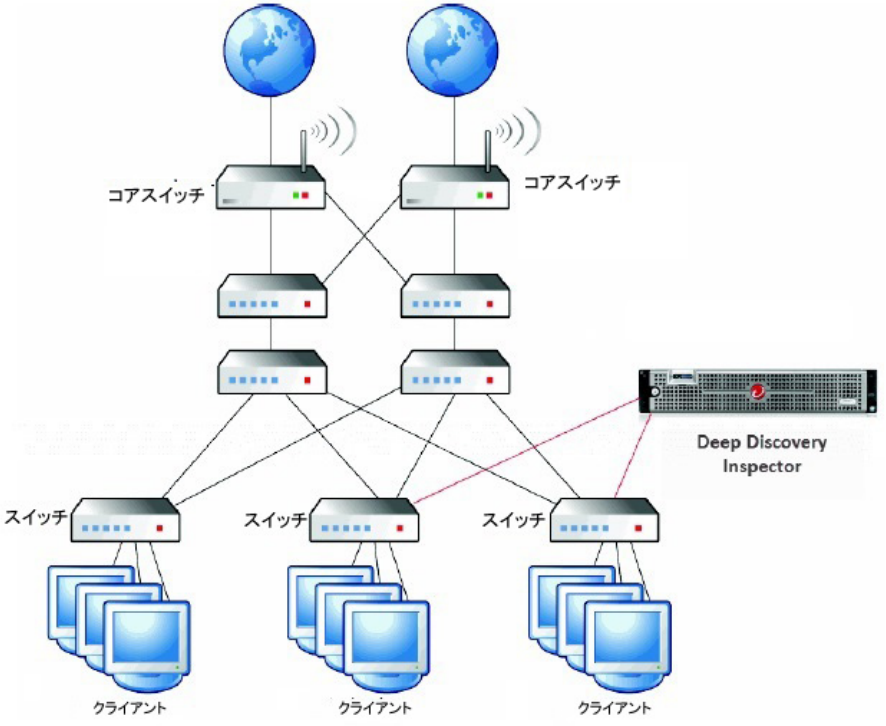
向の通信の VLAN タグがスイッチによって正しくミラーリングされることを確認してください。




## 複数ポートの監視

Deep Discovery Inspector では、複数のデータポートを使用して異なるネットワークセグメントを監視できます。Deep Discovery Inspector のデータポー

トをアクセススイッチまたはディストリビューションスイッチのミラーポートに接続します。

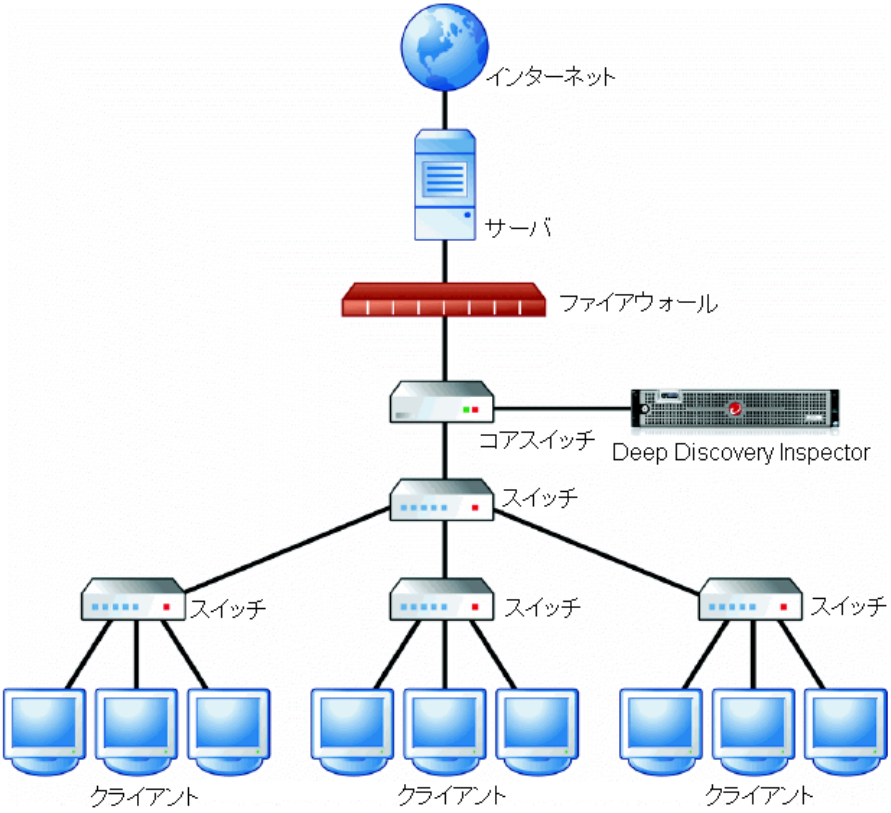



## ネットワーク TAP の監視

ネットワーク TAP は、内部で接続されたスイッチ、ルータ、およびクライアントから、ネットワークを通過するデータを監視します。1 台のネットワーク TAP に複数の Deep Discovery Inspector アプライアンスを接続できます。

**注意**

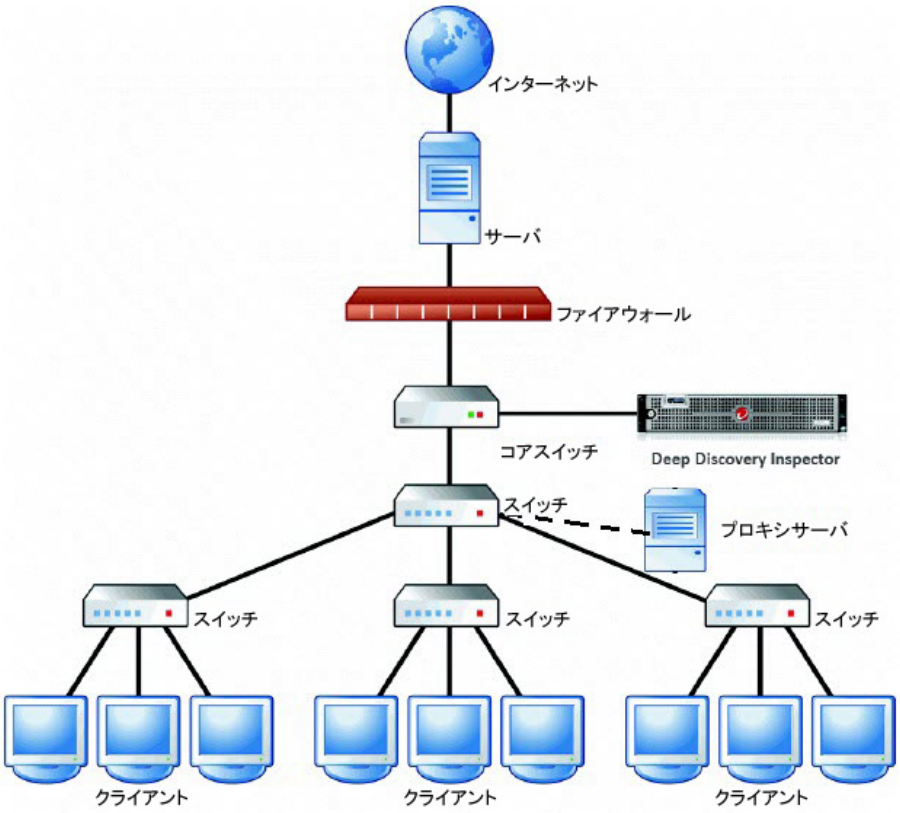
ネットワーク TAP を使用する場合は、DHCP トラフィックをフィルタ処理するのではなく、Deep Discovery Inspector への DHCP トラフィックをコピーするようにします。




## プロキシの監視

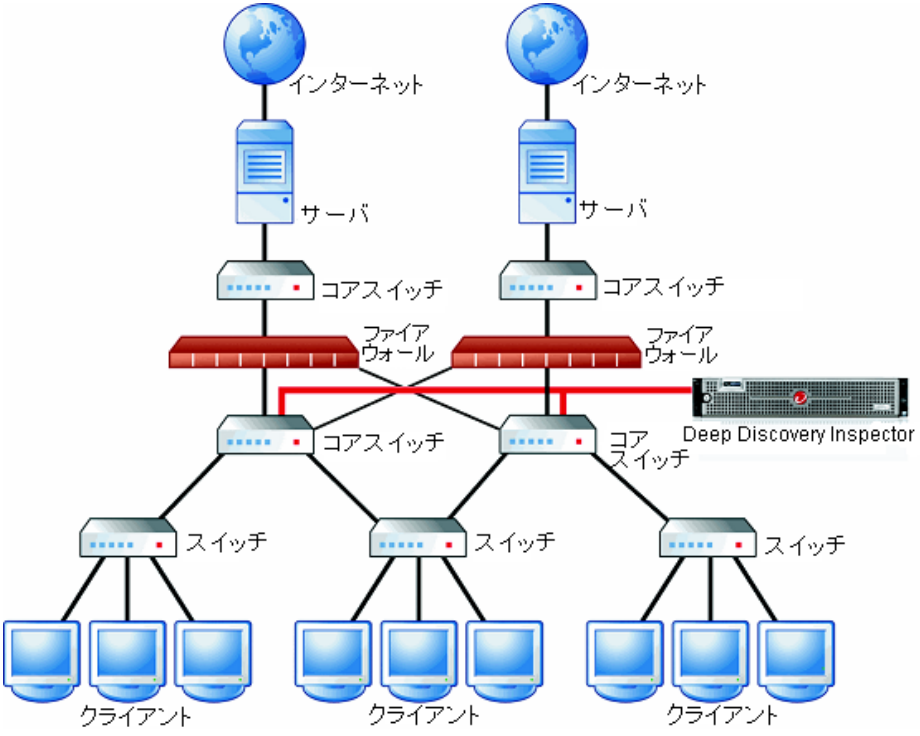
Deep Discovery Inspector がプロキシサーバの外部にあるプロキシ環境に配置されている場合、そのプロキシサーバで XFF (X-Forwarded-For) を有効にします。

Deep Discovery Inspector がプロキシサーバの内部または外部にあるプロキシ環境に配置されている場合、誤通知を回避するために、Deep Discovery Inspector で HTTP プロキシを登録済みサービスとして追加します。



## 冗長化されたネットワーク

多くの企業環境では、高い可用性を提供するために冗長化されたネットワークを使用しています。使用可能な場合は、非対称ルートを使用して冗長化スイッチに Deep Discovery Inspector を接続します。



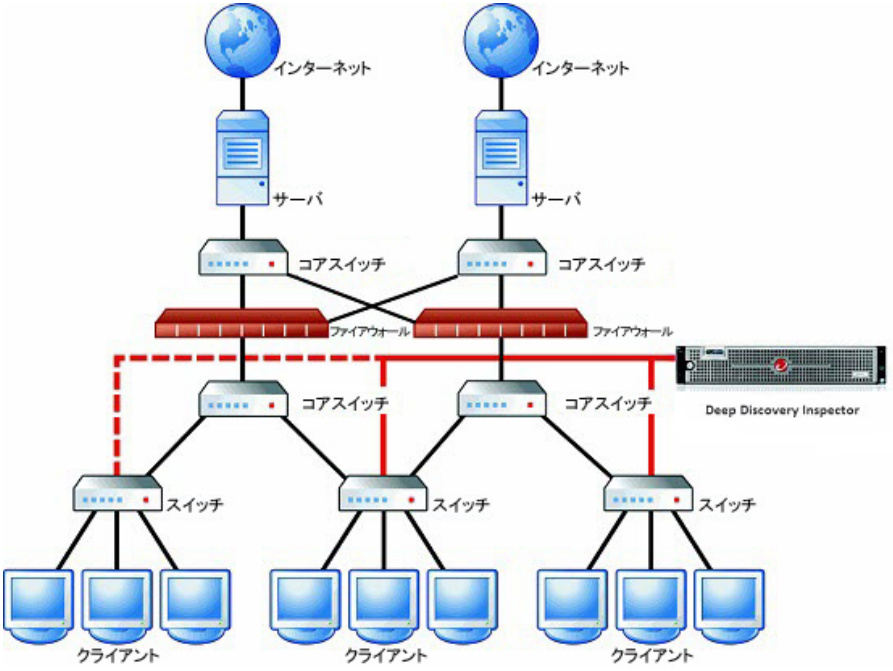

## リモートポートまたは VLAN ミラーリング

次の状況ではリモートミラーリングを使用してください。

- スイッチの監視
- ローカルスイッチに十分な数の物理ポートがない
- ローカルスイッチのポート速度が一致していない (GB/MB)

注意

この図では、破線はリモートミラーを表し、実線は直接ミラーを表します。



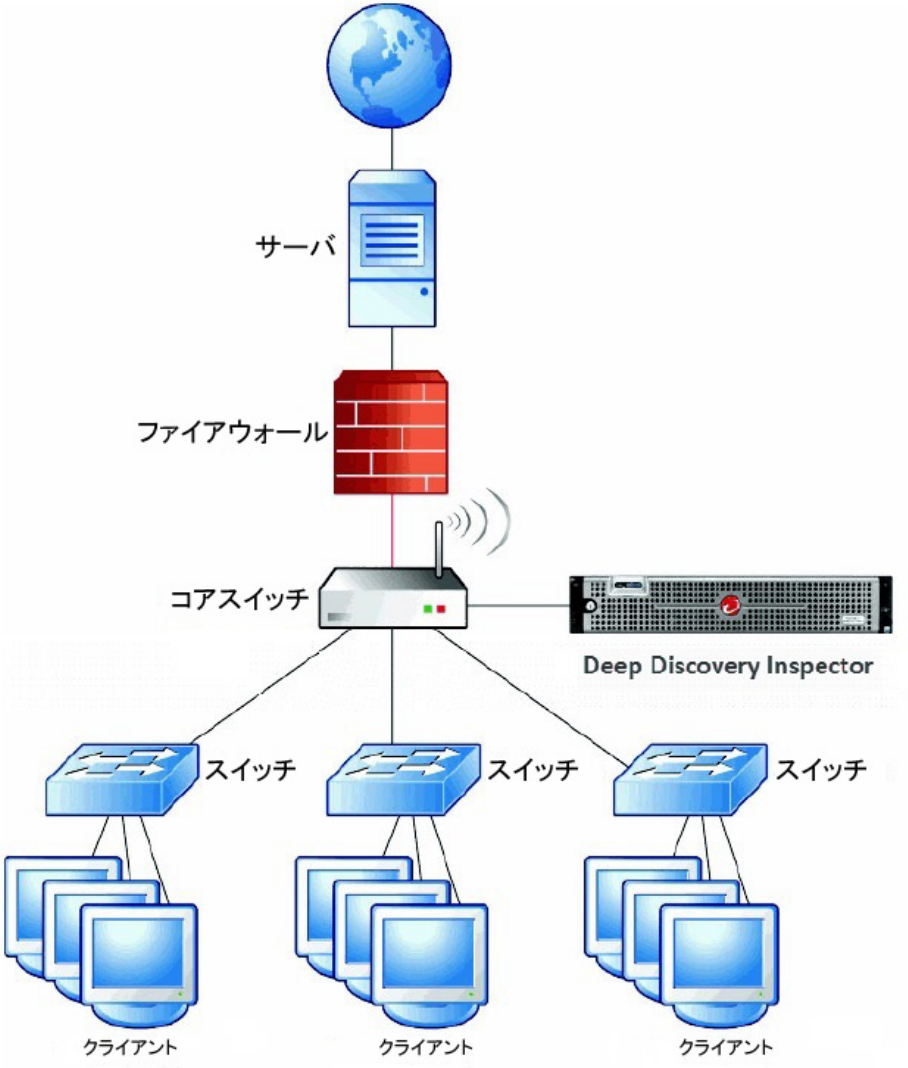

## 単一ポートの監視

Deep Discovery Inspector のデータポートをコアスイッチのミラーポートに接続して、ポートを介してファイアウォールへのトラフィックをミラーリングします。

(オプション) 単一または複数の送信元ポートからの送受信トラフィックをミラーリングするよう、ミラーポートを設定します。

注意

ネットワークインタフェースカードの 容量を超えてトラフィックをミラーリングすることはできません。


サーバ
ファイアウォール
コアスイッチ
Deep Discovery Inspector
スイッチ
スイッチ
スイッチ
クライアント
クライアント
クライアント

### VLAN ベースポートの監視

VLAN ベースのポートのミラーリングでは、特定の VLAN に属するすべてのポート上のトラフィックを監視するよう選択できます。Deep Discovery Inspector をスイッチに接続します。ミラー設定が VLAN ベースになります。

### VMware ポートミラーリング

トラフィックが仮想分散スイッチを通過する場合は、VMware ポートミラーリングを使用します。

詳細については、67 ページの「VMware 仮想分散スイッチでのポートミラーリング」を参照してください。

## インライン

インライン導入では、Deep Discovery Inspector は透過型ブリッジとして機能し、復号された TLS トラフィックを検査します。

**注意**

インライン導入では、インライン (LAN Bypass) ネットワークインタフェースカードを追加でインストールする必要があります。インストール手順および互換性のある Deep Discovery Inspector アプライアンスモデルについては、「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。

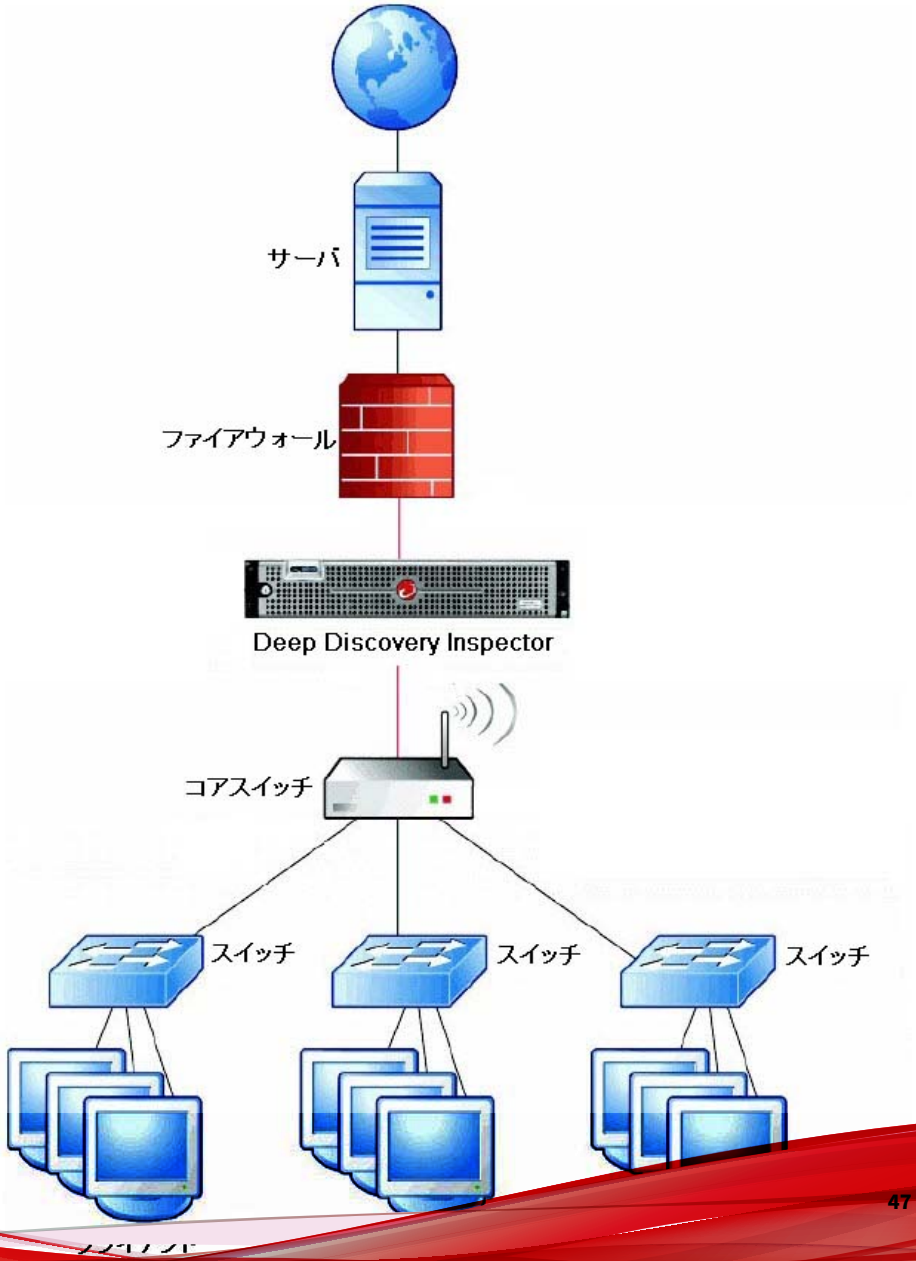
Deep Discovery Inspector によってトラフィックをブロックすることはできません。Deep Discovery Inspector をインラインアプライアンスとして導入した場合は、トラフィックを検査するかしないかだけを指定できます。

### 透過型ブリッジ

透過型ブリッジ導入は、Deep Discovery Inspector をインラインデバイスとして使用する場合に適しています。透過型ブリッジ導入は、TLS トラフィックインスペクションに必要になります。

透過型ブリッジとして導入した場合、Deep Discovery Inspector はネットワークデバイス間のレイヤ 2 ブリッジとして機能し、ネットワーク上では透過的

になります。監視したいネットワークパスにアプライアンスを 配置するだけで、ネットワークを再設定する必要はありません。



# ハードウェアアプライアンスのインストール要件

Deep Discovery Inspector をインストールする際は、次の点に留意してください。

| 要件 | 説明 |
|---|---|
| ポート速度を一致させる | ポートミラーリングを実現するために、送信先ポートの速度を送信元ポートの速度と同じにする必要があります。送信元ポートの速度が速いために送信先ポートで処理できない場合、送信先ポートで一部のデータが欠落する可能性があります。<br><br>Deep Discovery Inspector 1300 では、一致しない場合、インラインポートの速度が低下します。<br><br>Deep Discovery Inspector 4200/9200 では、一致しない場合、インラインポートが無効になります。 |
| 仮想アナライザデータポートを設定する | 内部仮想アナライザが有効な場合、次のネットワークオプションのいずれかを選択して、データポートを設定します。<br><br>• ネットワークなし<br><br>インターネットに接続しません。<br><br>• カスタムネットワーク<br><br>指定した追加のデータポートを使用して、インターネットに接続します。<br><br>• 管理ネットワーク<br><br>管理ポートを使用してインターネットに接続します。<br><br>詳細については、「Deep Discovery Inspector 管理者ガイド」の「内部仮想アナライザ」を参照してください。 |

| 要件 | 説明 |
| --- | --- |
| すべてのデータを監視する | Deep Discovery Inspector は送受信されるすべてのネットワークトラフィックを監視します。<br><br>**注意**<br>Deep Discovery Inspector をインストールする際のパフォーマンスを向上させるため、データポートにはオンボードの NIC ではなく、ネットワークカードで追加された NIC を使用することをお勧めします。<br><br>**注意**<br>Deep Discovery Inspector で双方向からのトラフィックが取得されるよう、ミラーポートを設定して、双方向のトラフィックがポートにミラーリングされるようにしてください。 |

## ハードウェアアプライアンスのシステム要件

Deep Discovery Inspector システム要件については、次の項目を参照してください。

- 49 ページの「ハードウェアアプライアンスの 要件」
- 50 ページの「事前設定コンソールの要件」
- 50 ページの「管理コンソールの要件」
- 51 ページの「仮想アナライザイメージの OS の要件」

### ハードウェアアプライアンスの要件

Trend Micro がサポートするハードウェアは、Deep Discovery 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。

インライン導入では、インライン (LAN Bypass) ネットワークインタフェースカードを追加でインストールする必要があります。インストール手順および互換性のある Deep Discovery Inspector アプライアンスモデルについては、

「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。

## 事前設定コンソールの要件

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、174 ページの「事前設定コンソール」を参照してください。

事前設定コンソールへのアクセスには、次の要件があります。

- VGA 接続:
  - VGA ポートを備えたモニタ
  - USB キーボード
  - VGA ケーブル
- シリアル接続:
  - シリアルポートを備えたコンピュータ
  - RS-232 シリアルケーブル
  - シリアル通信アプリケーション (HyperTerminal)

## 管理コンソールの要件

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。

詳細については、「Deep Discovery Inspector 管理者ガイド」の「管理コンソール」を参照してください。

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

推奨される解像度: 1280 x 800

## 仮想アナライザイメージの OS の要件

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**

Trend Micro では、Deep Discovery Inspector 内で作成する仮想アナライザのイメージまたはサンドボックスインスタンスへのインストールに 必要な Microsoft Windows OS または Microsoft Office 製品は提供しません。OS および Microsoft Office 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。

# 第 4 章

# ハードウェアアプライアンスへのインストール

Deep Discovery Inspector をハードウェアアプライアンスとしてインストールするための手順について、次の項目を参照してください。

# オプションの設定

Deep Discovery Inspector の管理コンソールナビゲーションを有効にするには、次のオプションを設定します。

- 54 ページの「Chrome の JavaScript オプションの設定」
- 54 ページの「Firefox の JavaScript オプションの設定」

## Chrome の JavaScript オプションの設定

**手順**

1. ブラウザで、[設定] に移動します。
2. [詳細設定を表示...] をクリックします。
3. [プライバシー] の [コンテンツの設定...] をクリックします。
4. [JavaScript] の下の [すべてのサイトで Javascript の実行を許可する (推奨)] をクリックします。
5. [完了] をクリックします。

## Firefox の JavaScript オプションの設定

**手順**

1. バージョン 23 より前の Firefox では、次の操作を実行します。
   a. ブラウザで、[オプション] > [コンテンツ] タブの順に選択します。
   b. [JavaScript を有効にする] が選択されていることを確認します。
   c. [OK] をクリックします。
2. バージョン 23 以上の Firefox では、次の操作を実行します。
   a. アドレスバーで「`about:config`」と入力し、<Enter> キーを押します。
   b. [細心の注意を払って使用する] をクリックします。

c. [設定名] の [javascript.enabled] の [値] が [true] に設定されていることを確認します。

# Deep Discovery Inspector ハードウェアアプライアンスのインストール

- Deep Discovery Inspector がプレインストールされたベアメタルサーバがトレンドマイクロにより提供されます。
- トレンドマイクロでは、Deep Discovery Inspector をインストール DVD にパッケージされた ISO ファイルとして提供します。

48 ページの「ハードウェアアプライアンスのインストール 要件」に示す要件を満たすベアメタルサーバに、Deep Discovery Inspector ソフトウェアをインストールします。

## 光学ディスクドライブのあるハードウェアアプライアンスへの Deep Discovery Inspector のインストール

**手順**

1. Deep Discovery Inspector をインストールする前に、インストール先のハードドライブ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ドライブ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。

   ヒント

   Deep Discovery Inspector を再インストールする場合は、Deep Discovery Inspector 管理コンソールで [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択することで、現在の設定をバックアップできます。

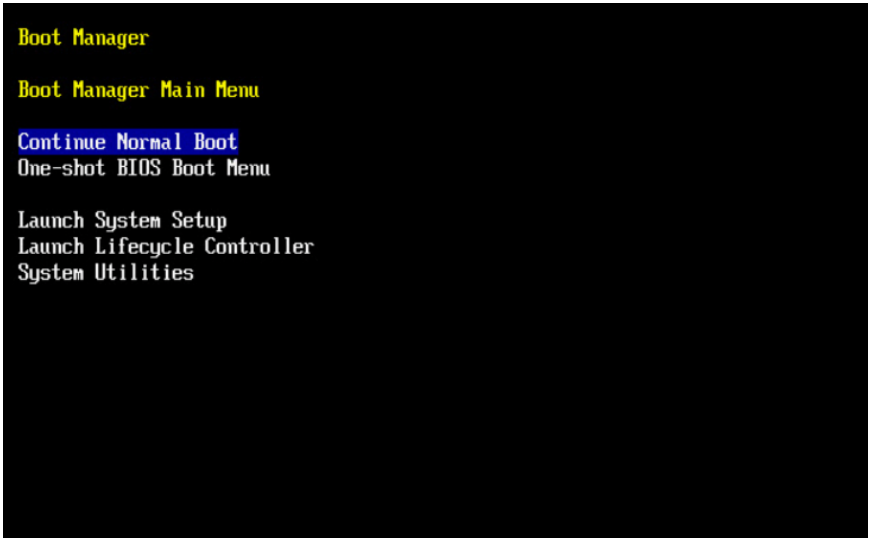
2. VGA 画面をアプライアンスのビデオコネクタに 接続します。
3. Deep Discovery Inspector のインストール DVD を CD/DVD ドライブに挿入します。

4. アプライアンスの電源をオンにします。

   [BIOS] 画面が表示されます。


5. F11 キーを押します。

   [Boot Manager] が表示されます。

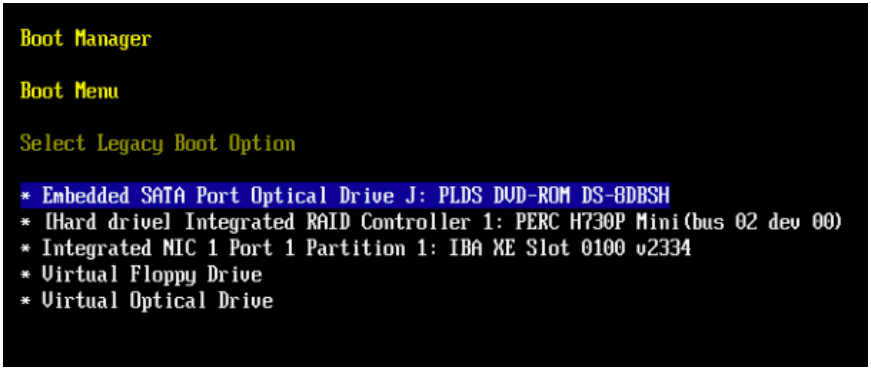


6. [BIOS Boot Menu] を選択し、Enter キーを押します。

**重要**

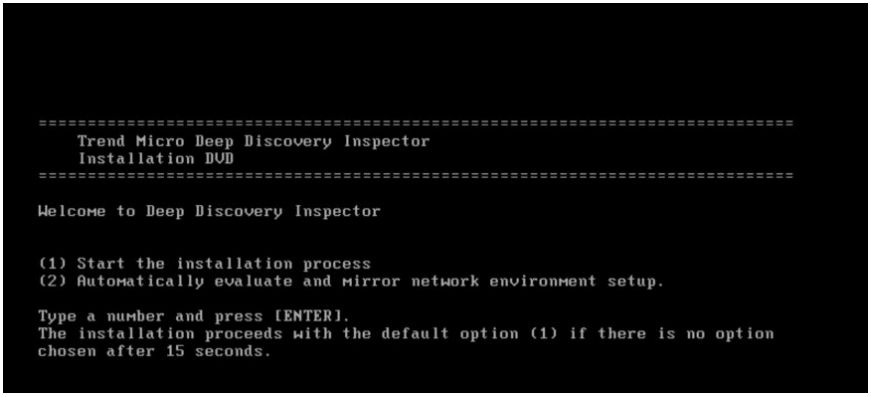
Deep Discovery Inspector をシリアル接続でインストールする場合は、Esc キーを押してから Shift キー+1 を押し、BIOS Boot Manager を起動します。

[BIOS Boot Manager] が表示されます。




7. [TSSTcorp DVD-ROM SN-108BB] を選択し、Enter キーを押します。

インストール DVD 画面が表示されます。

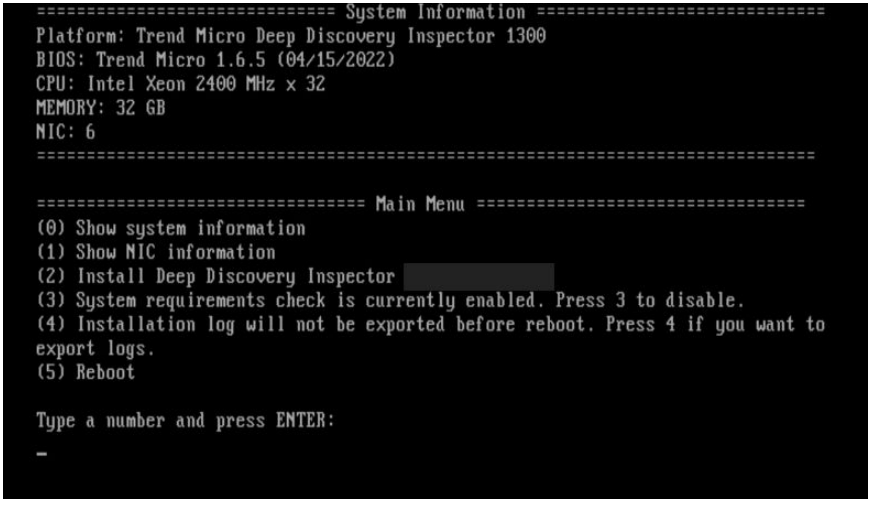


8. Enter キーを押します。

**重要**

シリアル接続で Deep Discovery Inspector をインストールしている場合は、「`serial`」と入力して Enter キーを押します

[System Information] 画面が表示されます。




9. 体験版の導入の場合は、「`3`」と入力して Enter キーを押し、システム要件のチェックを省略します。

**注意**

初期設定では、Deep Discovery Inspector をインストールする前にシステム要件のチェックが行われ、製品の実行に必要なリソースがアプライアンスにあるかどうかが確認されます。

10. トラブルシューティング用にインストールログを取得する必要がある場合は、「`4`」と入力して Enter キーを押します。
11. 「`2`」と入力して Enter キーを押し、インストールを開始します。

[Management Port Selection] 画面が表示されます。

管理ポートとして使用できるアクティブなネットワークインタフェースが自動的に検出され、「Link UP」と表示されます。

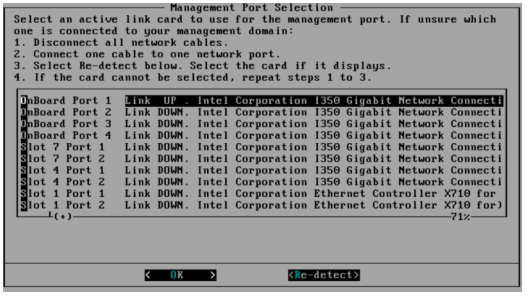
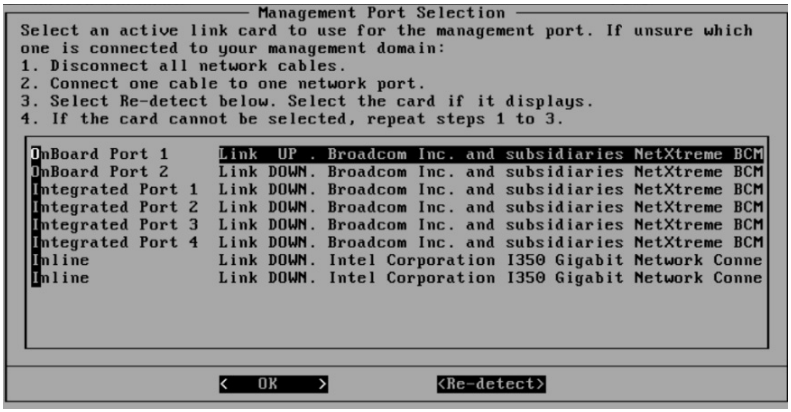



図 4-1. [Management Port Selection]

---

**重要**

インライン NIC のポートを管理ポートに選択することはできません。




---

12. ネットワークポートのステータスと、実際のポートのステータスが一致することを確認します。

    ステータスに矛盾がある場合は、[Re-detect] を選択し、Enter キーを押します。

13. [Management Port Selection] 画面に表示される手順を実行して、管理ドメインに接続するアクティブなネットワークインタフェースを 確認します。
14. アクティブなネットワークインタフェースを 選択して、Enter キーを押します。

    インストールが続行され、完了します。
15. [System Information] 画面でインストールログのエクスポートを有効にした場合は、インストールログを保存します。

    a. ストレージデバイスを選択して、Enter キーを押します。

       目的のストレージデバイスがリストにない場合は、[Re-detect] に移動し、Enter キーを押してリストを更新します。

    b. インストールログのファイル名が表示されたら、Enter キーを押します。

       後で参照できるようにファイル名をメモに記録します。ファイル名には次の形式が使用されます。

       ```
       install.log.YYYY-MM-DD-hh-mm-ss
       ```

       ヒント

       エクスポートされたインストールログは [sda11] に保存することをお勧めします。

    システムが自動的に再起動し、事前設定コンソールが表示されます。使用している場合は、インストール DVD が CD/DVD ドライブから排出されます。
16. (オプション) 再度インストールが実行されないように DVD を取り出します。
17. Deep Discovery Inspector のネットワークを設定します。

    - 事前設定コンソールにアクセスしてデバイス設定を変更します。

      詳細については、173 ページの事前設定を参照してください。
    - 管理コンソールを開き、アプライアンスの IP 設定を変更します。

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

### 次に進む前に

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

ヒント

トレンドマイクロでは、リモートによるシステム管理とトラブルシューティングを可能にするため、アプライアンスで iDRAC (Integrated Dell Remote Access Controller) を設定することをお勧めします。

## 光学ディスクドライブのないハードウェアアプライアンスへの Deep Discovery Inspector のインストール

### 手順

1. Deep Discovery Inspector をインストールする前に、インストール先のハードドライブ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ドライブ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。

   ヒント

   Deep Discovery Inspector を再インストールする場合は、Deep Discovery Inspector 管理コンソールで [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択することで、現在の設定をバックアップできます。

2. Deep Discovery Inspector のインストール ISO を、https://appweb.trendmicro.com/ecs/default.aspx にある法人カスタマーサービス & サポートからダウンロードします。

3. Deep Discovery Inspector アプライアンスの BIOS の [Integrated Devices] 画面で、iDRAC ダイレクト USB ポートを有効にします。

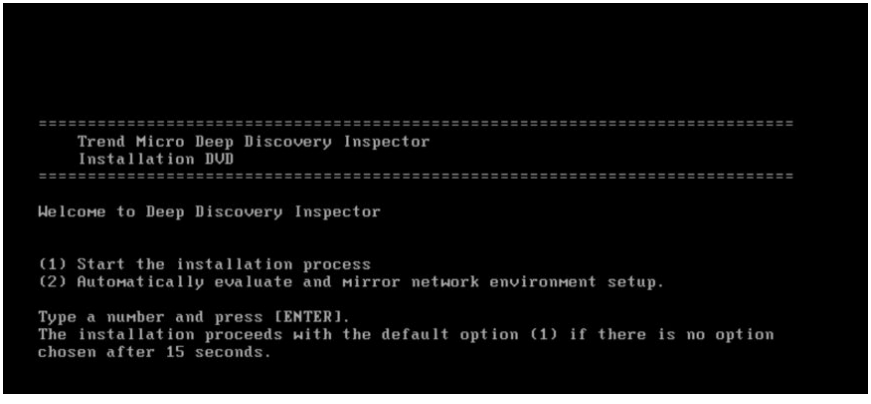
4. USB - microUSB ケーブルを使用して、お使いのコンピュータを Deep Discovery Inspector アプライアンスに接続し、USB ポートを介して iDRAC インタフェースにアクセスします。

   詳細については、https://www.dell.com/support/kbdoc/ja-jp/000130077/poweredge-idrac-%E3%83%80%E3%82%A4%E3%83%AC%E3%82%AF%E3%83%88-%E6%A9%9F%E8%83%BD-%E3%81%AE-%E4%BD%BF%E7%94%A8-%E6%96%B9%E6%B3%95 にある Dell のドキュメントを参照してください。

5. iDRAC9 の仮想メディア機能を使用して、Deep Discovery Inspector インストーラを起動します。

   詳細については、https://www.dell.com/support/kbdoc/ja-jp/000124001/using-the-virtual-media-function-on-idrac-6-7-8-and-9 にある Dell のドキュメントを参照してください。

   インストール DVD 画面が表示されます。




6. Enter キーを押します。

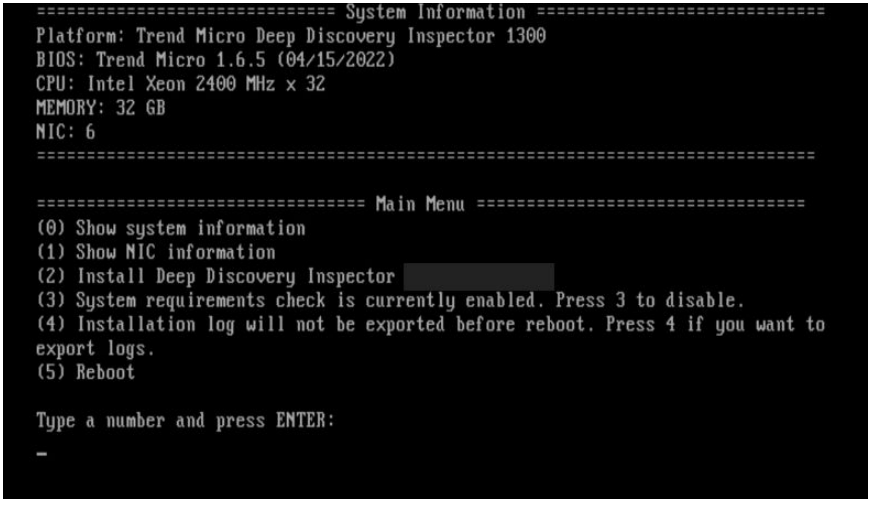
---

**重要**

シリアル接続で Deep Discovery Inspector をインストールしている場合は、「`serial`」と入力して Enter キーを押します

---

[System Information] 画面が表示されます。




7. 体験版の導入の場合は、「3」と入力して Enter キーを押し、システム要件のチェックを省略します。

   **注意**

   初期設定では、Deep Discovery Inspector をインストールする前にシステム要件のチェックが行われ、製品の実行に必要なリソースがアプライアンスにあるかどうかが確認されます。

8. トラブルシューティング用にインストールログを取得する必要がある場合は、「4」と入力して Enter キーを押します。
9. 「2」と入力して Enter キーを押し、インストールを開始します。

   [Management Port Selection] 画面が表示されます。

管理ポートとして使用できるアクティブなネットワークインタフェースが自動的に検出され、「Link UP」と表示されます。

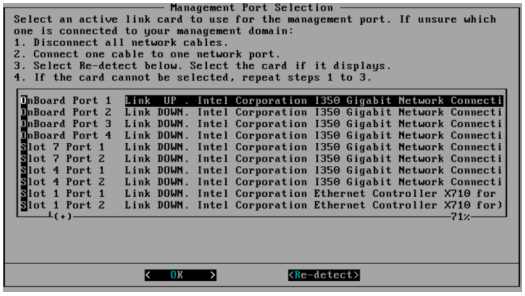
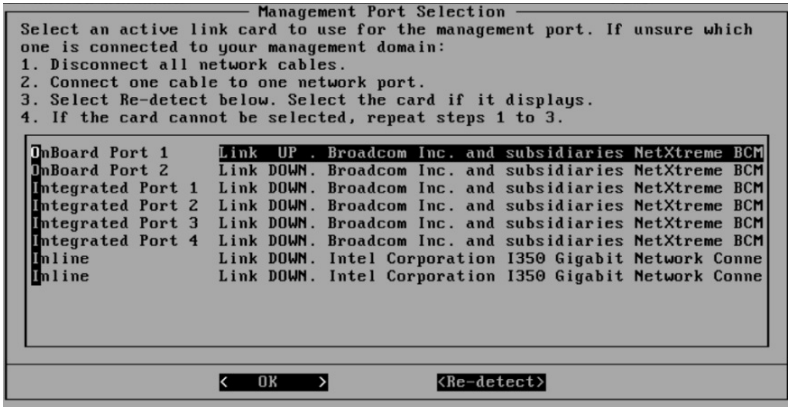



図 4-2. [Management Port Selection]

**重要**

インライン NIC のポートを管理ポートに選択することはできません。




10. ネットワークポートのステータスと、実際のポートのステータスが一致することを確認します。

    ステータスに矛盾がある場合は、[Re-detect] を選択し、Enter キーを押します。

11. [Management Port Selection] 画面に表示される手順を実行して、管理ドメインに接続するアクティブなネットワークインタフェースを 確認します。
12. アクティブなネットワークインタフェースを 選択して、Enter キーを押します。

    インストールが続行され、完了します。
13. [System Information] 画面でインストールログのエクスポートを有効にした場合は、インストールログを保存します。

    a. ストレージデバイスを選択して、Enter キーを押します。

       目的のストレージデバイスがリストにない場合は、[Re-detect] に移動し、Enter キーを押してリストを更新します。

    b. インストールログのファイル名が表示されたら、Enter キーを押します。

       後で参照できるようにファイル名をメモに記録します。ファイル名には次の形式が使用されます。

       ```
       install.log.YYYY-MM-DD-hh-mm-ss
       ```

       **ヒント**

       エクスポートされたインストールログは [sda11] に保存することをお勧めします。

    システムが自動的に再起動し、事前設定コンソールが表示されます。使用している場合は、インストール DVD が CD/DVD ドライブから排出されます。
14. (オプション) 再度インストールが実行されないように DVD を取り出します。
15. Deep Discovery Inspector のネットワークを設定します。

    - 事前設定コンソールにアクセスしてデバイス設定を変更します。

      詳細については、173 ページの事前設定を参照してください。
    - 管理コンソールを開き、アプライアンスの IP 設定を変更します。

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

### 次に進む前に

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

ヒント

トレンドマイクロでは、リモートによるシステム管理とトラブルシューティングを可能にするため、アプライアンスで iDRAC (Integrated Dell Remote Access Controller) を設定することをお勧めします。

## 製品出荷時のモードへの復元

製品出荷時の初期設定を復元することで Deep Discovery Inspector をリセットします。

### 手順

1. VGA ケーブルを使用して、モニタの VGA ポートを Deep Discovery Inspector アプライアンスの VGA ポートに接続し、アプライアンスに電源を投入します。

   Deep Discovery Inspector の起動中、事前設定コンソールが開く前に、「Press ESC key to enter the menu」というプロンプトが表示されます。操作を行わなければ、システムは 10 秒以内に自動的に起動します。

2. <Esc> キーを押して、起動システムのオプションメニューを 表示します。
3. 矢印キーを使用して、[Restore to factory mode] を選択し、<Enter> キーを押します。

   Deep Discovery Inspector が再起動し、事前設定コンソールが開きます。

# 第 5 章

# VMware 仮想分散スイッチでのポートミラーリング

Deep Discovery Inspector では、ミラーリングされたトラフィックを仮想分散スイッチを使用して監視できます。仮想分散スイッチの作成方法、およびミラーリングされたトラフィックを Deep Discovery Inspector のハードウェアアプライアンスで監視するための設定方法については、次の項目を参照してください。


- 68 ページの「VMware vSphere Distributed Switch (VDS) の作成」
- 70 ページの「Deep Discovery Inspector ハードウェアアプライアンスと VDS」

# VMware vSphere Distributed Switch (VDS) の作成

**手順**

1. 新しい仮想分散スイッチを作成します。
   a. vSphere Web Client にログインします。
   b. [Networking] をクリックします。
   c. 左側のパネルでデータセンターを選択します。
   d. 右側のパネルで [Create a new distributed switch] アイコンをクリックします。

      [New Distributed Switch] 画面が表示されます。
   e. スイッチの名前を入力し、[Next] をクリックします。
   f. 分散スイッチのバージョンを選択し、[Next] をクリックします。
   g. [Number of uplinks] で、SPAN トラフィックが専用 NIC を通過する場合は 2 以上を設定します。それ以外の場合は 1 を設定します。

      注意
      トレンドマイクロでは、専用 NIC を使用することをお勧めします。
   h. [Network I/O Control] で、次のいずれかのオプションを選択します。
      - Disabled: SPAN トラフィックが専用 NIC を通過する場合

        注意
        トレンドマイクロでは、専用 NIC を使用することをお勧めします。
      - Enabled: SPAN トラフィックが監視対象トラフィックと同じ NIC を通過する場合
   i. [Create a default port group] をオフにします。
   j. [Next] をクリックします。

k. 概要情報が正しいことを確認して、[Finish] をクリックします。

2. 仮想スイッチを設定します。

   a. 前の手順で作成した仮想分散スイッチを右クリックし、[Settings] > [Edit Settings] の順に選択します。

      [Edit Settings] 画面が表示されます。

   b. [Advanced] をクリックします。

      詳細設定が表示されます。

   c. [MTU (Bytes)] に「`1600`」と指定します。

3. ポートグループを仮想分散スイッチに追加します。

   a. [Networking] をクリックします。

   b. 前の手順で作成した仮想分散スイッチを右クリックし、[Distributed Port Group] > [New Distributed Port Group] の順に選択します。

      [New Distributed Port Group] 画面が表示されます。

   c. ポートグループの名前を入力し、[Next] をクリックします。

   d. [Port binding] で [Static binding] を選択します。

   e. [Port allocation] で [Fixed] を選択します。

   f. [Number of ports] に、接続するポートの数を入力します。

   g. [Next] をクリックします。

   h. 概要画面で設定が正しいことを確認して、[Finish] をクリックします。

      新しいポートグループが [Manage] タブに表示されます。

4. (オプション) 手順 3 を繰り返して、ポートグループをさらに追加します。

5. ESXi ホストを仮想分散スイッチに追加します。

   a. 前の手順で作成した仮想スイッチを右クリックし、[Add and Manage Hosts] を選択します。

      [Add and Manage Hosts] 画面が表示されます。

b. [Select task] で [Add host and manage host networking (advanced)] を選択します。

c. [Next] をクリックします。

d. [Select hosts] で [+ New hosts] をクリックし、管理下の ESXi ホストを追加します。

e. [Next] をクリックします。

f. [Selet network adapter tasks] で、[Manage physical adapters] と [Migrate virtual machine networking] のチェックマークをオンにします。

g. [Next] をクリックします。

h. [Manage physical network adapters] で、ネットワーク環境に応じて物理ネットワークアダプタを管理します。

i. [次へ] をクリックします。

j. [Analyze impact] で [No impact] を指定します。

k. [Next] をクリックします。

l. [Migrate VM networking] で、ネットワーク環境に応じて仮想マシンネットワークを移行します。

m. [Next] をクリックします。

n. [終了準備の完了] で [Finish] をクリックします。

[Add and Manage Hosts] 画面が閉じます。

o. 前の手順で作成した仮想スイッチをクリックし、[Configure] タブ、[Topology] の順にクリックして、設定した仮想スイッチのトポロジを確認します。

## Deep Discovery Inspector ハードウェアアプライアンスと VDS

Deep Discovery Inspector ハードウェアアプライアンスでは、カプセル化されたリモートミラーリングまたはリモートミラーリングを使用して、ミラーリングされたトラフィックを仮想分散スイッチから監視できます。Deep

Discovery Inspector と仮想分散スイッチの設定方法については、次の項目を参照してください。

- 71 ページの「ハードウェアアプライアンス - カプセル化されたリモートミラーリングによりミラーリングされたトラフィックの VDS からの監視の設定」
- 76 ページの「ハードウェアアプライアンス - リモートミラーリングによりミラーリングされたトラフィックの VDS からの監視の設定」

## ハードウェアアプライアンス - カプセル化されたリモートミラーリングによりミラーリングされたトラフィックの VDS からの監視の設定

カプセル化されたリモートミラーリングにより複数のネットワークインタフェースまたは VLAN のトラフィックを監視して、対象トラフィックを 1 つ以上のミラーリング先に送信できます。

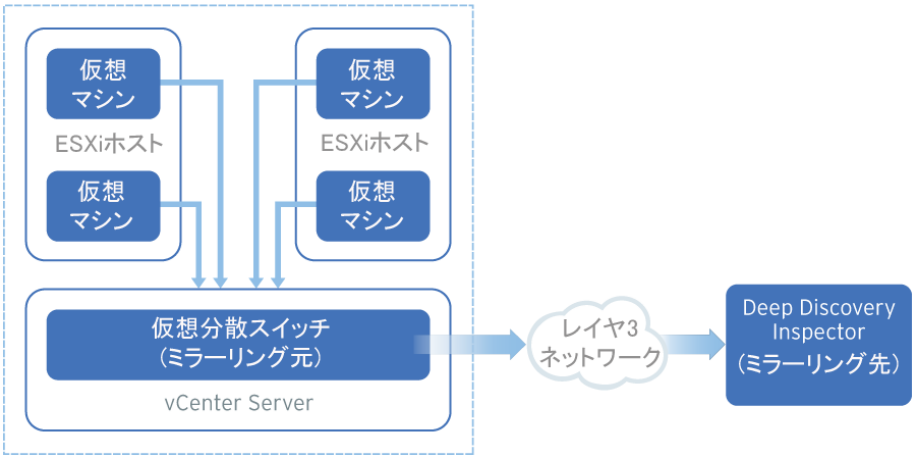



図 5-1. カプセル化されたリモートミラーリングによりミラーリングされたトラフィックの VDS からの監視

仮想スイッチのカプセル化されたリモートミラーリングでは、初期設定で、ESXi ホストの管理 VMkernel ポートがカプセル化の送信元 IP アドレスとして使用されます。

以下の手順におけるミラーリング元とミラーリング先は次のようになります。

- ミラーリング元: ミラーリングされたトラフィックを転送する仮想分散スイッチ
- ミラーリング先: Deep Discovery Inspector

**手順**

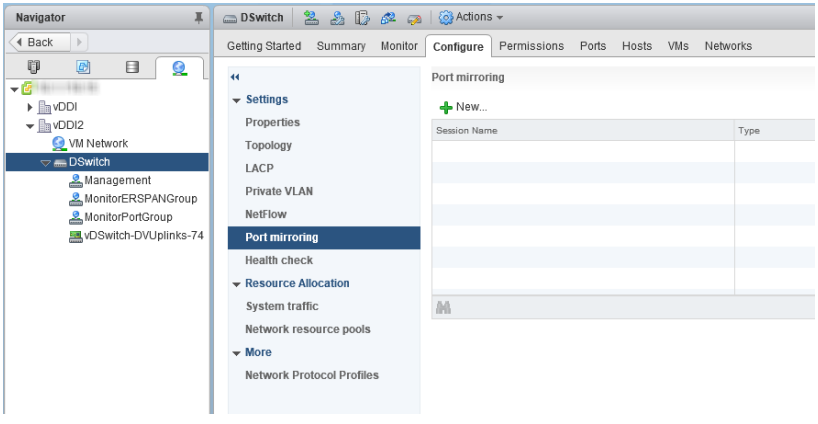
1. カプセル化され、リモートミラーリングされたトラフィックを転送するようにミラーリング元を設定します。

   a. vSphere Web Client にログインします。

   b. 左側のペインで仮想分散スイッチを選択し、[Configure] をクリックします。

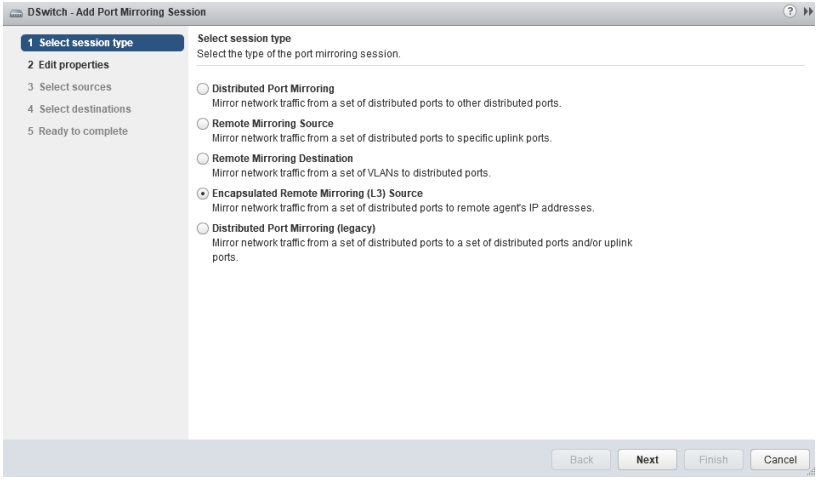
   c. [Port Mirroring] をクリックします。

      [Port mirroring] 画面が表示されます。




   d. [New...] をクリックします。

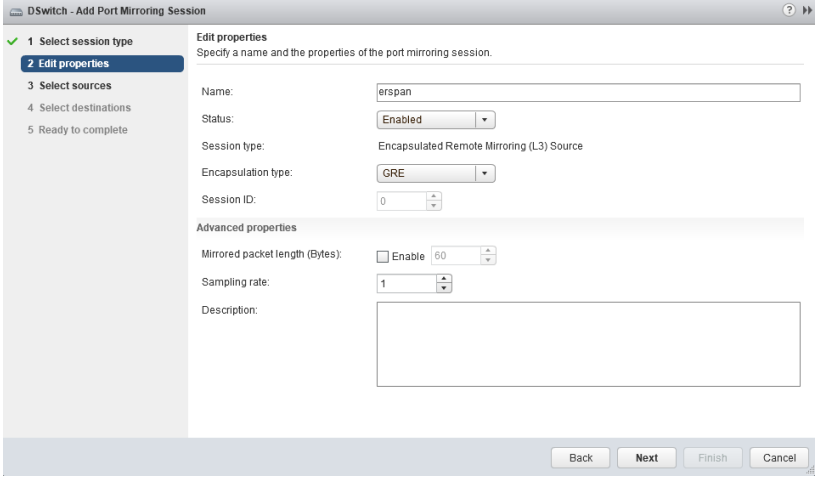
      [Add Port Mirroring Sessions] 画面が表示されます。




e. [Encapsulated Remote Mirroring (L3) Source] を選択します。

f. [Next] をクリックします。

[Edit properties] 画面が表示されます。




g. [Name] にセッション名を入力します。

h. [Status] で [Enabled] を選択します。

i. [Encapsulation type] でカプセル化の種類を選択します。

---

注意

[ERSPAN THREE] を使用すると問題が発生する場合があります。トレンドマイクロでは、[GRE] または [ERSPAN TWO] を使用することをお勧めします

---

j. [Next] をクリックします。

[Select sources] 画面が表示されます。

k. プラス記号のアイコン
(

) をクリックして、監視するミラーリング元の仮想マシンを追加します。

l. [Next] をクリックします。

[Select destinations] 画面が表示されます。

m. プラス記号のアイコンをクリックして、ミラーリング先の IP アドレスを追加します。

---

注意

ミラーリング先の IP アドレスは、次の手順の Deep Discovery Inspector で設定するアドレスです。

---

n. [Next] をクリックします。

[Ready to complete] 画面が表示されます。

o. 設定が正しいことを確認して、[Finish] をクリックします。

2. カプセル化され、リモートミラーリングされたトラフィックを受信するようにミラーリング先を設定します。

a. Deep Discovery Inspector 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。

[ネットワークインタフェース ] 画面が表示されます。

b. データポートを見つけ、行の先頭にある右向き矢印
(

) をクリックします。

c. [カプセル化されたリモートミラーリング] を選択します。

d. カプセル化されたリモートミラーリングのミラーリング先アドレスを指定します。

**重要**

カプセル化されたリモートミラーリングのミラーリング先アドレスは、ESXi ホストの管理 VMkernel ポートからルーティング可能である必要があります。

e. [保存] をクリックします。

# ハードウェアアプライアンス - リモートミラーリングによりミラーリングされたトラフィックの VDS からの監視の設定

リモートミラーリングにより、あるスイッチ上のトラフィックを別のスイッチのデバイスから監視して、対象トラフィックを 1 つ以上のミラーリング先に送信できます。

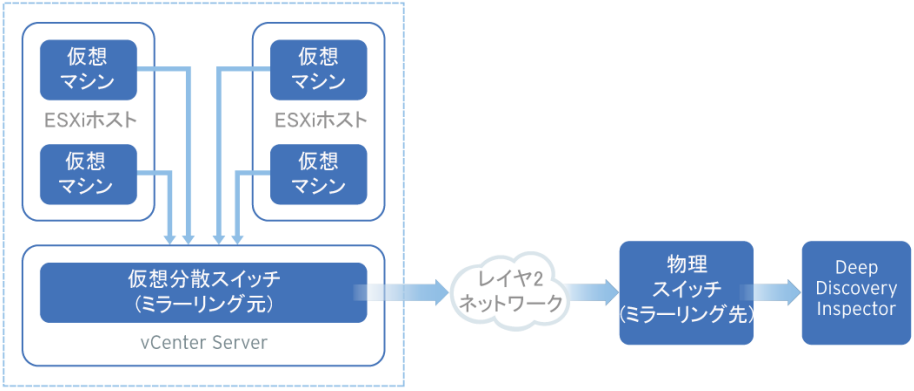



図 5-2. リモートミラーリングによりミラーリングされたトラフィックの VDS からの監視

リモートミラーリングでは、リモートミラーリング VLAN を物理スイッチ上に設定する必要があります。リモートミラーリング VLAN を設定できない場合は、代わりにカプセル化されたリモートミラーリングを使用することを検討してください。

以下の手順におけるミラーリング元とミラーリング先は次のようになります。

- ミラーリング元: ミラーリングされたトラフィックを転送する仮想分散スイッチ
- ミラーリング先: ミラーリングされたトラフィックを受信して Deep Discovery Inspector にルーティングできる物理スイッチ

開始する前に、トラフィックを受信する ESXi ホストのアップリンクポートが物理スイッチのトランクポートにリンクしていることを確認します。

**手順**

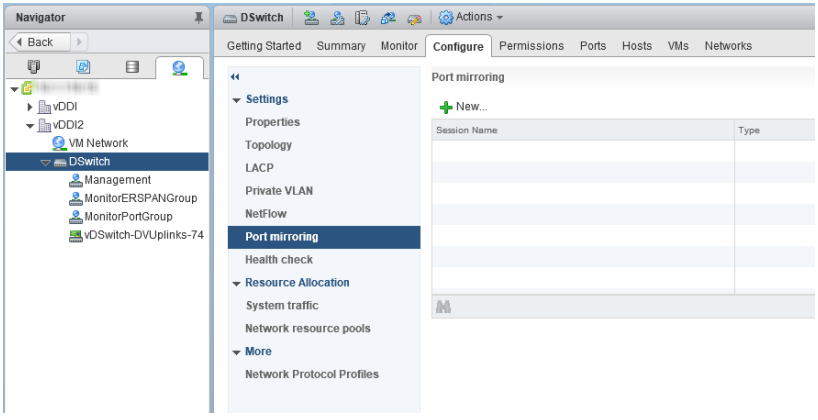
1. リモートミラーリングされたトラフィックをミラーリング先に転送するようにミラーリング元を設定します。

   a. vSphere Web Client にログインします。

   b. 左側のペインで仮想分散スイッチを選択し、[Configure] をクリックします。

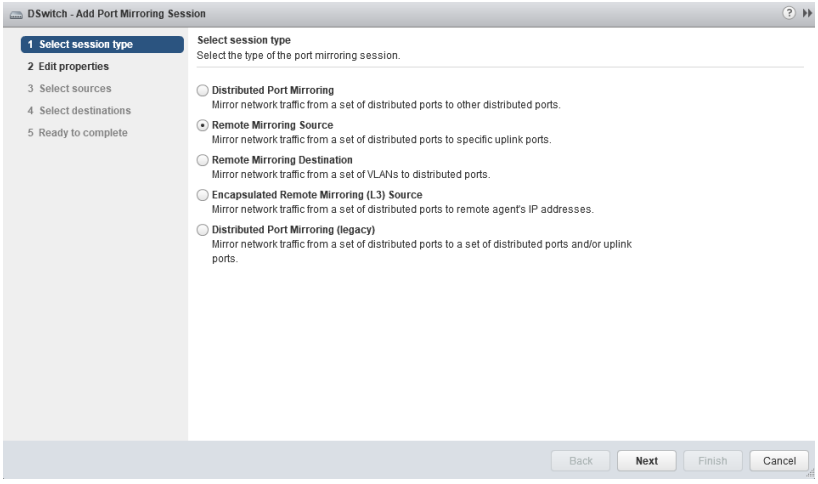
   c. [Port Mirroring] をクリックします。

      [Port mirroring] 画面が表示されます。




   d. [New...] をクリックします。

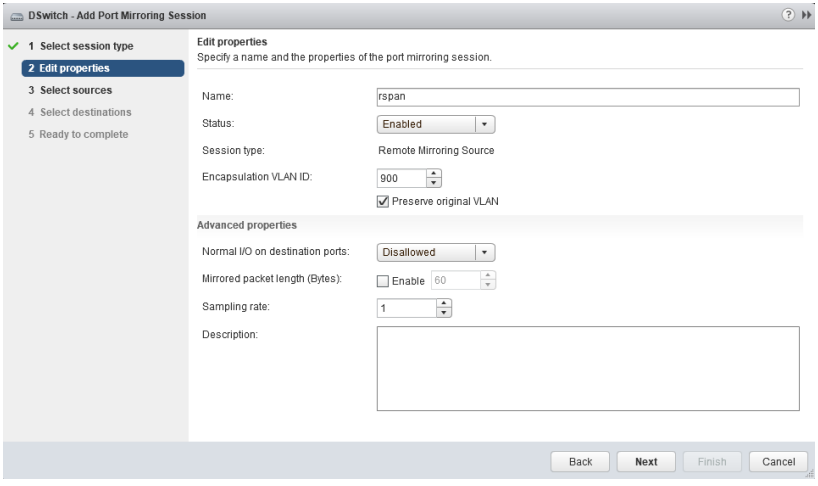
      [Add Port Mirroring Sessions] 画面が表示されます。




e. [Remote Mirroring Source] を選択します。

f. [Next] をクリックします。

[Edit properties] 画面が表示されます。




g. [Name] にセッション名を入力します。

h. [Status] で [Enabled] を選択します。

i. [Encapsulation VLAN ID] で VLAN ID を指定します。

> **注意**
> これは VDS で設定したリモートミラーリング VLAN ID です。

j. [Next] をクリックします。

[Select sources] 画面が表示されます。

k. プラス記号のアイコン
(

) をクリックして、監視するミラーリング元の仮想マシンを追加します。

l. [Next] をクリックします。

[Select destinations] 画面が表示されます。

m. [Available uplinks] のアップリンクを [Selected uplinks] に追加します。

n. [Next] をクリックします。

[Ready to complete] 画面が表示されます。

o. 設定が正しいことを確認して、[Finish] をクリックします。

2. カプセル化され、リモートミラーリングされたトラフィックを Deep Discovery Inspector に転送するようにミラーリング先を設定します。

# パート III

# 仮想アプライアンスのインストールと導入

# 第 6 章

# 仮想アプライアンスの導入

Deep Discovery Inspector 仮想アプライアンスをインストールする 際のヒント、推奨事項、および要件について、次の項目を参照してください。

# 導入の概要

**手順**

1. 導入を計画します。

   84 ページの「仮想アプライアンスの導入計画」を参照してください。

2. インストール要件を確認します。

   86 ページの「仮想アプライアンスのインストール 要件」を参照してください。

3. システム要件を確認します。

   87 ページの「仮想アプライアンスのシステム 要件」を参照してください。

4. 仮想アプライアンスを作成します。

   91 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。

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

   134 ページの「Deep Discovery Inspector 仮想アプライアンスのインストール」を参照してください。

6. Deep Discovery Inspector を事前設定します。

   173 ページの「事前設定」を参照してください。

# 仮想アプライアンスの導入計画

Deep Discovery Inspector の最善の導入方法を計画するには、次を実行します。

- 保護を必要とするネットワークセグメントを特定します。
- メール、Web、およびアプリケーションサーバなどの 運用に欠かせないアプライアンスの場所を考慮して、ネットワークトラフィックについて計画します。
- セキュリティニーズを満たすために必要なアプライアンスの数と、それらのネットワーク上の場所を特定します。

- ネットワークのテストセグメント上でパイロット導入を実施します。
- パイロット導入の結果に基づいて、導入戦略を再定義します。
- 次の例を使用して、カスタマイズされた Deep Discovery Inspector の導入を計画します。

## 導入シナリオ

Deep Discovery 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導入できます。

- ハードウェアアプライアンス: Deep Discovery Inspector をインラインアプライアンスまたはアウトオブバンドアプライアンスとして 導入できます。
  - インライン: Deep Discovery Inspector は透過型ブリッジとして機能し、復号された TLS トラフィックを検査します。インラインアプライアンスとして導入した場合、インラインポートを流れるトラフィックのみが検査されます。

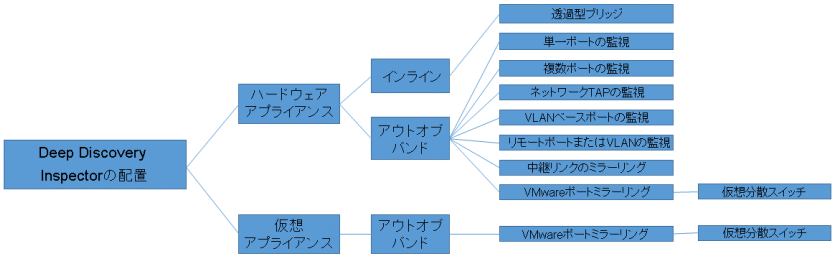
    

    **注意**

    インライン導入では、インライン (LAN Bypass) ネットワークインタフェースカードを追加でインストールする必要があります。インストール手順および互換性のある Deep Discovery Inspector アプライアンスモデルについては、「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。

  - アウトオブバンド: Deep Discovery Inspector は、スイッチのミラーポートに接続することで、ネットワークの切断を発生させることなく、または最小限に留めながらネットワークトラフィックを監視します。アウトオブバンドアプライアンスとして 導入した場合、データポートにミラーリングされたトラフィックのみが検査されます。
- 仮想アプライアンス: Deep Discovery Inspector はアウトオブバンドアプライアンスとしてのみ導入できます。Deep Discovery Inspector は、スイッチのミラーポートに接続することで、ネットワークの切断を発生させることなく、または最小限に留めながらネットワークトラフィックを監視します。

次の図は、サポートされる導入の概要を示しています。




## VMware ポートミラーリング

トラフィックが仮想分散スイッチを通過する場合は、VMware ポートミラーリングを使用します。

詳細については、139 ページの「VMware 仮想分散スイッチでのポートミラーリング」を参照してください。

# 仮想アプライアンスのインストール要件

Deep Discovery Inspector をインストールする際は、次の点に留意してください。

| 要件 | 説明 |
|---|---|
| ポート速度を一致させる | ポートミラーリングを実現するために、送信先ポートの速度を送信元ポートの速度と同じにする必要があります。送信元ポートの速度が速いために送信先ポートで処理できない場合、送信先ポートで一部のデータが欠落する可能性があります。 |

| 要件 | 説明 |
| --- | --- |
| すべてのデータを監視する | Deep Discovery Inspector は送受信されるすべてのネットワークトラフィックを監視します。<br><br>注意<br>Deep Discovery Inspector で双方向からのトラフィックが取得されるよう、ミラーポートを設定して、双方向のトラフィックがポートにミラーリングされるようにしてください。 |

## 仮想アプライアンスのシステム要件

システム要件については、次の項目を参照してください。

- 87 ページの「仮想ホストアプライアンスの 要件」

### 仮想ホストアプライアンスの要件

Deep Discovery Inspector は、次のハイパーバイザにインストールできます。

- VMware ESXi 7.0 または 8.0
- Windows Server 2019 または 2022 上の Microsoft Hyper-V
- RHEL 9.2 KVM

Deep Discovery 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。Deep Discovery Inspector 仮想アプライアンスを仮想アナライザと併用する場合は、外部仮想アナライザと Sandbox as a Service のみがサポートされます。

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 6-1. 仮想アプライアンスの仕様

| スループット (Mbps) | 仮想 CPU 数* | 仮想メモリ (GB) | 仮想ディスク (GB) | 仮想 NIC 数** | Sandbox as a Service のサポート |
|---|---|---|---|---|---|
| 250 | 6 | 32 | 500 | 2 | あり |
| 500 (日本語版では提供しておりません) | 6 | 32 | 500 | 2 | あり |
| 1000 | 12 | 32 | 1000 | 3 | あり |

注意

- * 仮想 CPU には 2.5GHz 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。
- ** トレンドマイクロでは、ESXi には VMXNET 3 ネットワークアダプタを、RHEL KVM には VirtIO または E1000 ネットワークアダプタを使用することをお勧めします。

## 管理コンソールの要件

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。

詳細については、「Deep Discovery Inspector 管理者ガイド」の「管理コンソール」を参照してください。

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

推奨される解像度: 1280 x 800

# 第 7 章

# 仮想アプライアンスの新規作成

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。

- 92 ページの「VMWare ESXi 仮想アプライアンスの作成」
- 104 ページの「Microsoft Hyper-V 仮想アプライアンスの作成」

仮想ホストアプライアンスの最小システム要件とサポートされるハイパーバイザの詳細については、49 ページの「ハードウェアアプライアンスのシステム要件」を参照してください。

# VMWare ESXi 仮想アプライアンスの作成

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。

- 92 ページの「VMware ESXi での仮想マシンの要件」
- 92 ページの「VMware ESXi サーバネットワークの設定」
- 97 ページの「VMware ESXi での仮想マシンの作成」
- 103 ページの「VMware ESXi のハードウェア仮想化支援機能を有効にする」

## VMware ESXi での仮想マシンの要件

重要

VMware ESXi は個別にライセンスを取得する必要があり、その製品の VMware の使用許諾契約の条件に従う必要があります。

Deep Discovery Inspector を VMware ESXi サーバにインストールするには、次のものが必要です。

- バージョン 7.0 または 8.0 の VMware ESXi サーバ
- VMware ESXi サーバ上の 2 つ以上の NIC: 1 つの管理ネットワークと、少なくとも 1 つのデータネットワーク

  詳細については、92 ページの「VMware ESXi サーバネットワークの設定」を参照してください。
- VMware ホストと VMware vSphere 設定の両方で有効になっている仮想化技術 (VT)

  VMware vSphere 設定の詳細については、103 ページの「VMware ESXi のハードウェア仮想化支援機能を有効にする」を参照してください。

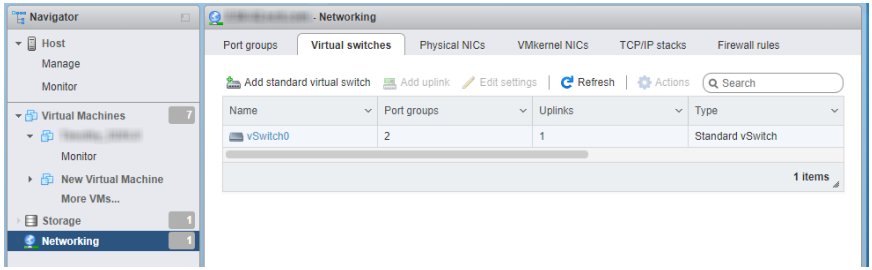
### VMware ESXi サーバネットワークの設定

ブラウザを使用して ESXi サーバに接続します。

**手順**

1. VMware ESXi サーバにサインインします。


2. [Networking] > [Virtual switches] に移動します。初期の状態を確認します。




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

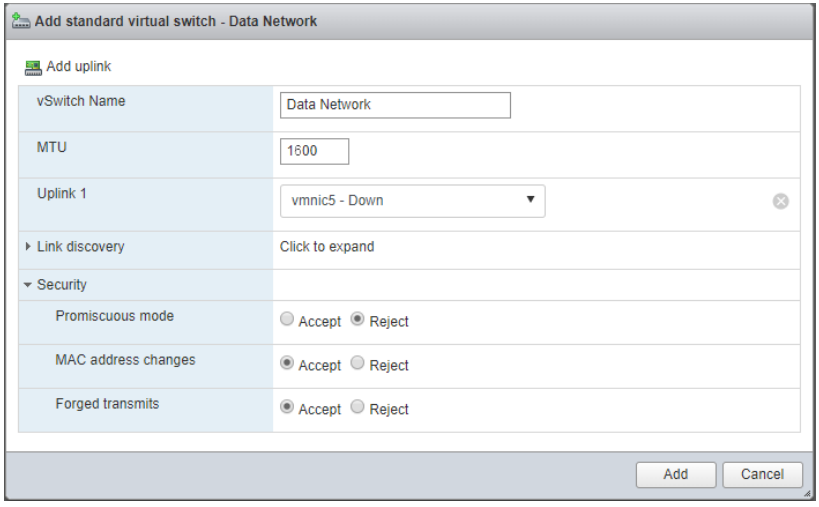
a. [vSwitch Name] に `Data Network` と入力します。

b. [MTU] に `1600` と入力します。

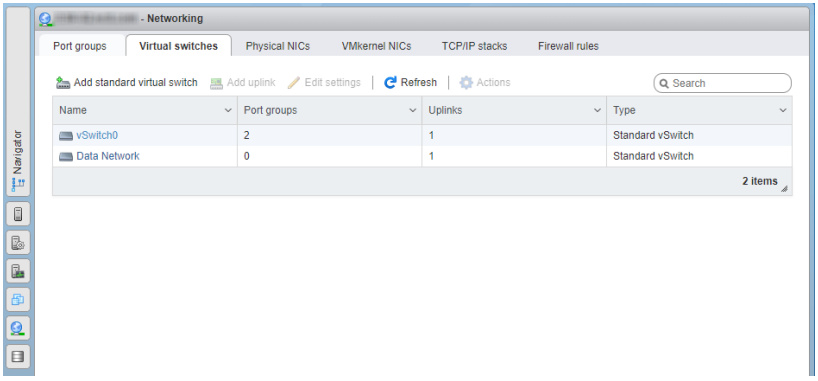
c. [Uplink 1] で Data Network 用の NIC カードを選択します。

d. [Security] を展開して、設定を行います。

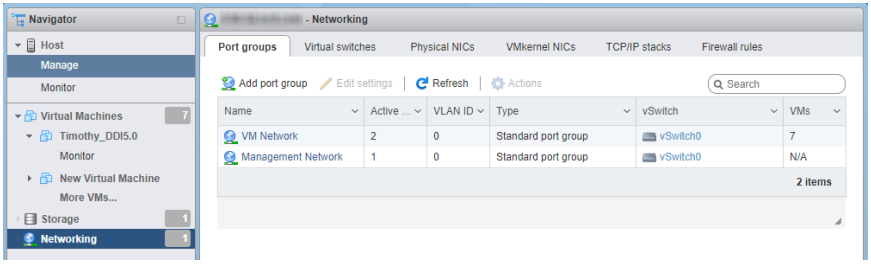
   1. [Promiscuous mode] で [Reject] を選択します。
   2. [MAC address changes] で [Accept] を選択します。
   3. [Forged transmits] で [Accept] を選択します。



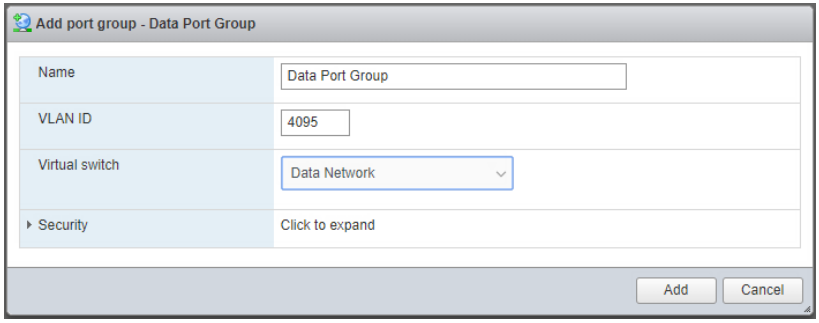

e. [Add] をクリックします。




4. [Port groups] タブをクリックして、最初の状態を確認します。
5. [Add port group] をクリックして、設定を行います。

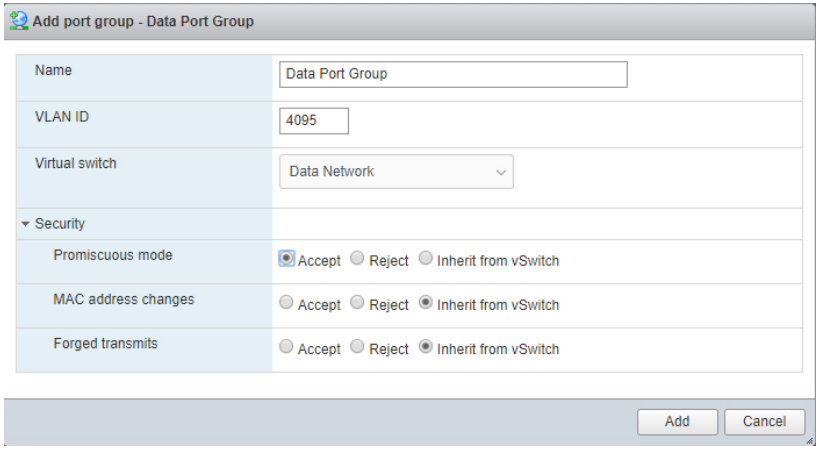



a. [Name] に `Data Port Group` と入力します。
b. [VLAN ID] に `4095` と入力します。
c. [Virtual switch] で [Data Network] を選択します。

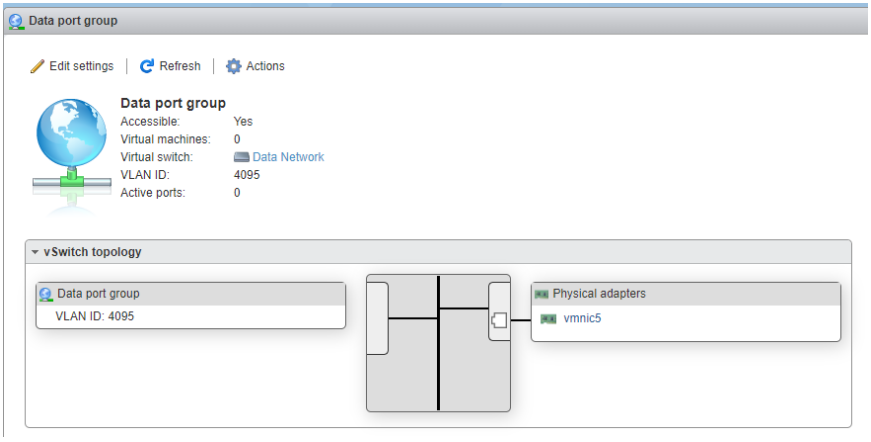



d. [Security] を展開して、設定を行います。

1. [Promiscuous mode] で [Accept] を選択します。
2. [Mac Address changes] と [Forged transmits] の両方で、[Inherit from vSwitch] を選択します。



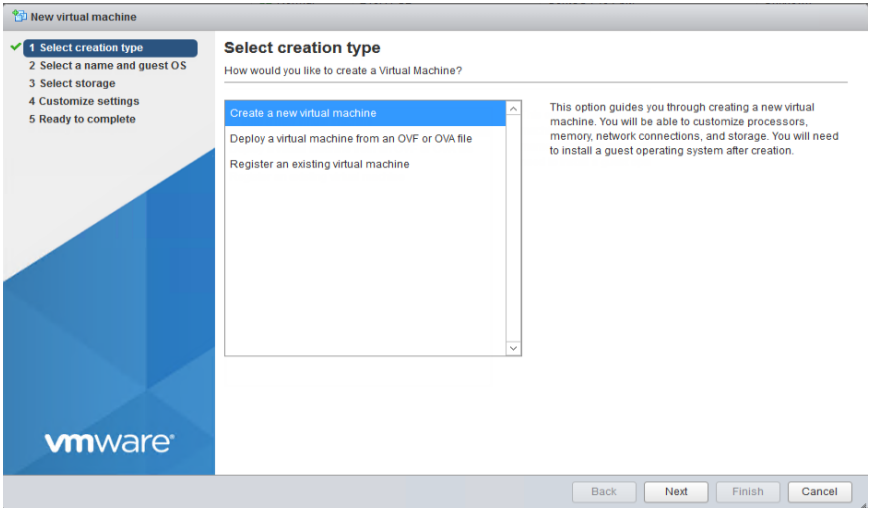

6. [Add] をクリックします。
7. [Port groups] タブで、[Data port group] をクリックし、[Data Network] に接続されていることを確認します。



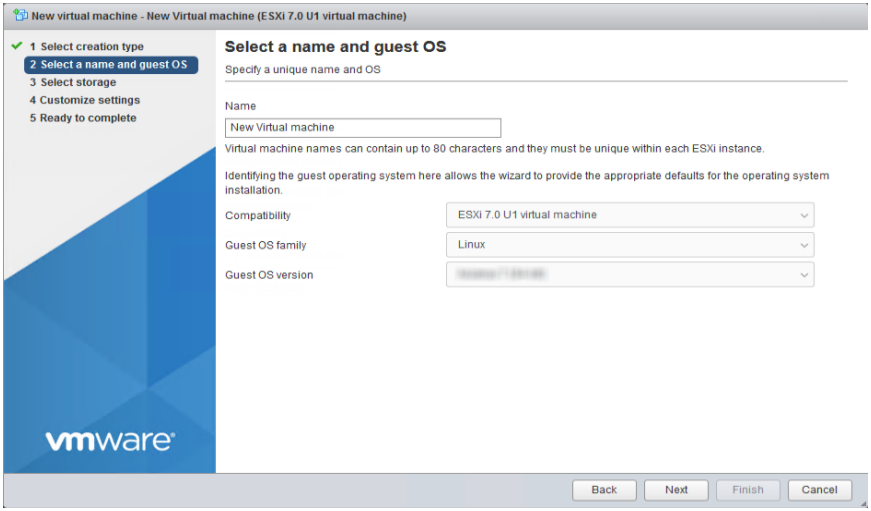

## VMware ESXi での仮想マシンの作成

**手順**

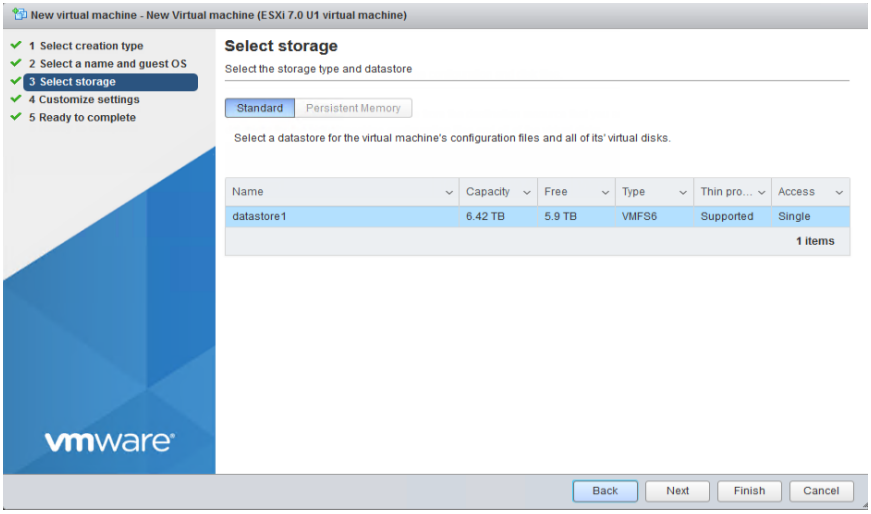
1. [Virtual Machines] を右クリックして、[Create/Register VM] をクリックします。
2. [Select creation type] 画面で、[Create a new virtual machine] をクリックして、[Next] をクリックします。




3. [Select a name and guest OS] 画面の設定を行います。
   a. [Name] に `New Virtual Machine` と入力します。
   b. [Compatibility] で [ESXi 7.0] を選択します。
   c. [Guest OS family] で [Linux] を選択します。
   d. [Guest OS version] で [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、仮想マシンを配置する送信先ストレージを選択して、[Next] をクリックします。




6. [Customize settings] 画面の設定を行います。

a. [CPU]でご利用になる Deep Discovery Inspector の仮想環境に応じた値を選択します。

   - スループットが 250 または 500Mbps の場合は、[6] CPU 以上を選択します。
   - スループットが 1000Mbps の場合は、 [12] CPU 以上を選択します。

b. [Memory] で、仮想マシンに対して少なくとも [32 GB] のメモリを選択します。

c. [Hard disk] で、ご利用になる Deep Discovery Inspector の仮想環境に応じたハードディスク容量を選択します。

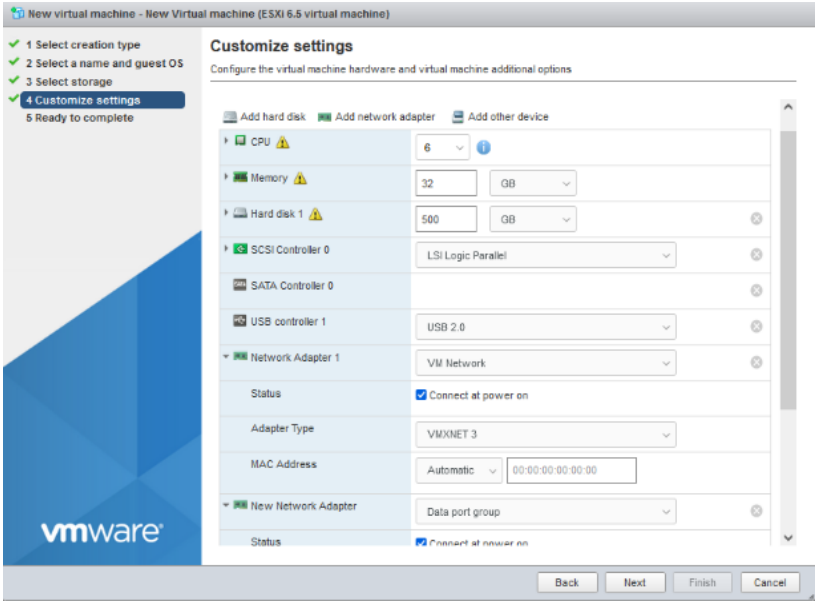
   - スループットが 250 または 500Mbps の場合は、[500 GB] 以上の値を選択します。
   - スループットが 1000Mbps の場合は、[1000 GB] 以上の値を選択します。

d. [SCSI Controller 0] で [LSI Logic Parallel] を選択します。

e. [Network] で、ご利用になる Deep Discovery Inspector の仮想環境に応じた数の NIC を設定します。

   - スループットが 250 または 500Mbps の場合は、2 つ以上の NIC を設定します。
   - スループットが 1000Mbps の場合は、3 つ以上の NIC を設定します。

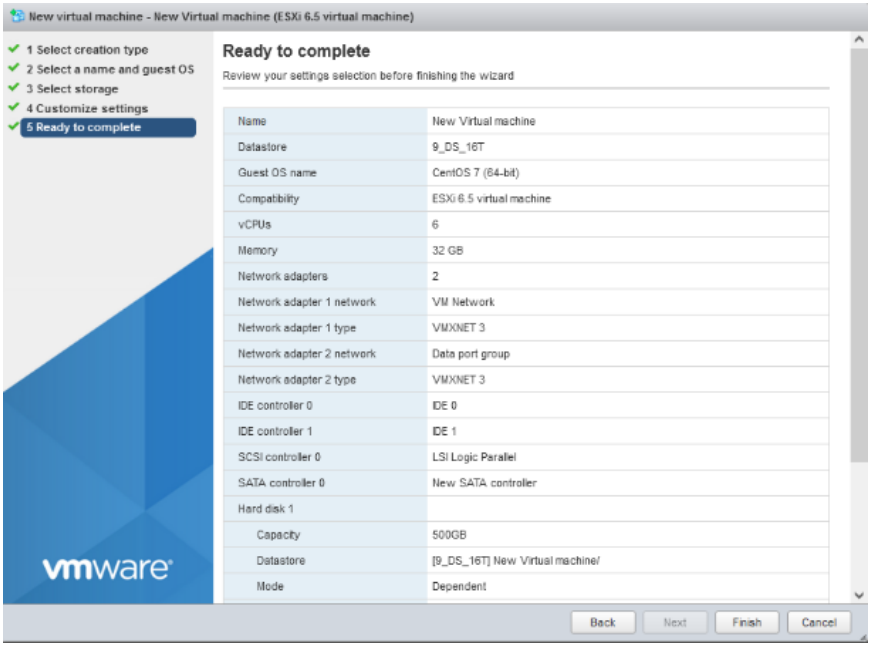
   1. Deep Discovery Inspector の管理ネットワーク (NIC 1) として、VMware ESXi サーバの [VM Network] を設定します。
   2. Deep Discovery Inspector のデータネットワーク (NIC 2) として、[Data port group] を設定します。




**注意**

トレンドマイクロでは、ESXi 7.0 または 8.0 で VMXNET 3 ネットワークアダプタを使用することをお勧めします。

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



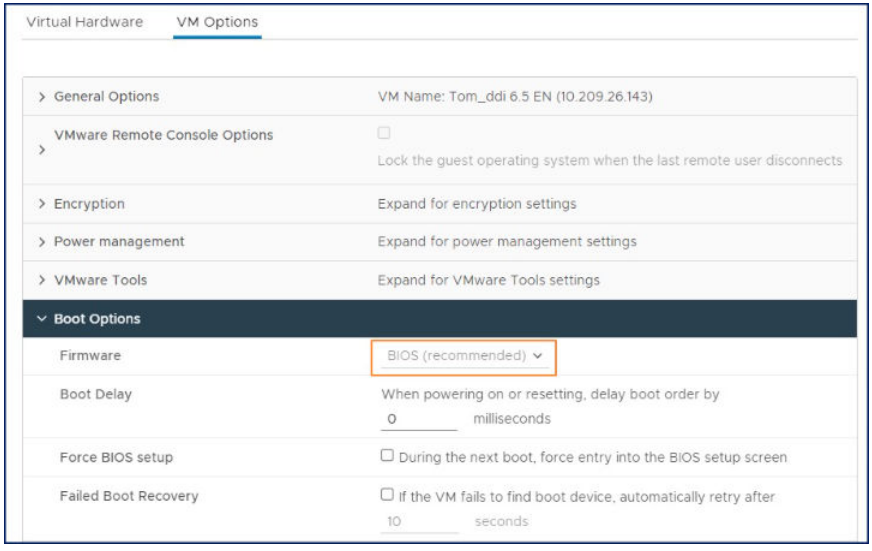

9. Vmware vSphere Web Client のハードウェアによる仮想化支援を有効にします。

   詳細については、103 ページの「VMware ESXi のハードウェア仮想化支援機能を有効にする」を参照してください。

10. VMware vSphere Web Client で、仮想マシンを右クリックして [Edit Settings] をクリックします。

11. [VM Options] > [Boot Options] の順に選択します。

12. [Firmware] が `[BIOS]` に設定されていることを確認します。




## VMware ESXi のハードウェア仮想化支援機能を有効にする

### 手順

1. 仮想化技術 (VT) が VMware ホストで有効になっていることを確認します。

   ヒント

   仮想化技術の設定は一般に BIOS 設定内で有効にしますが、その場所はシステムベンダによって異なります。この機能はベンダによって、AMD-V、VT、VT-x、Vanderpool Technology、仮想化技術 (Virtualization Technology)、VMX、または仮想マシン拡張機能 (Virtual Machine Extension) と呼ばれています。

2. VMware vSphere Web Client で、仮想マシンを右クリックして [Edit Settings] をクリックします。
3. [Virtual Hardware] タブで [CPU] を展開します。

4. [Expose hardware-assisted virtualization to guest OS] を有効にします。
5. [OK] をクリックします。

# Microsoft Hyper-V 仮想アプライアンスの作成

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。

- 104 ページの「Microsoft Hyper-V で仮想マシンを作成する」
- 127 ページの「Microsoft Hyper-V でのトラフィックのミラーリングの設定」

## Microsoft Hyper-V で仮想マシンを作成する

**重要**

Microsoft Hyper-V の仮想マシンにインストールされた Deep Discovery Inspector 仮想アプライアンスでは、第 2 世代 (UEFI) はサポートされません。

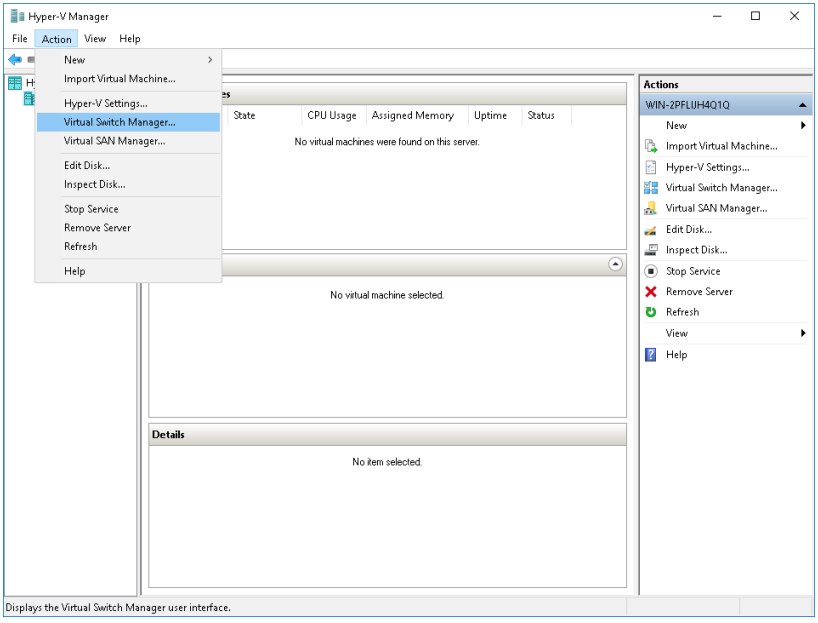
**重要**

Deep Discovery Inspector のインストールは、Windows Server 2019 または 2022 で稼働する Hyper-V 仮想マシンでのみサポートされます。

**手順**

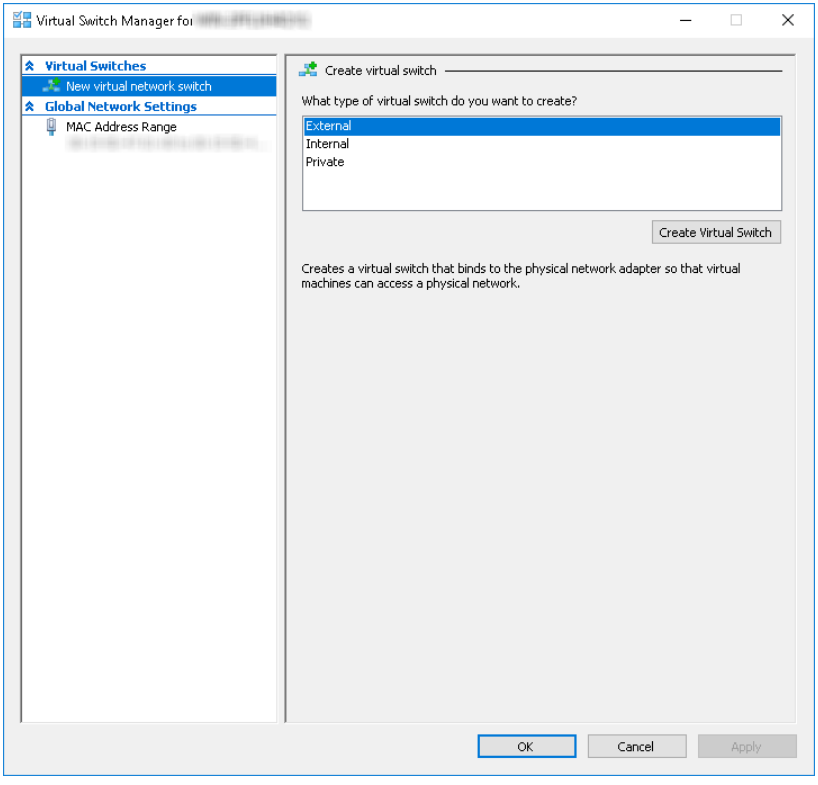
1. 管理用、データ用の仮想スイッチを作成します。
   a. Hyper-V マネージャーで、[Action] > [Virtual Switch Manager] の順に選択します。

      [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。

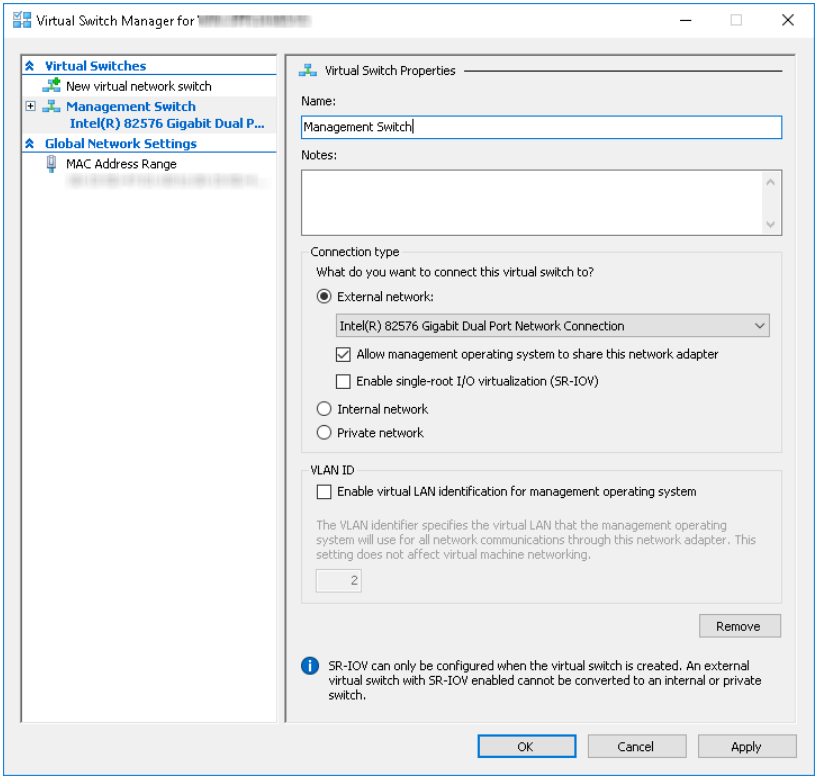



d. [Create Virtual Switch] をクリックします。

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

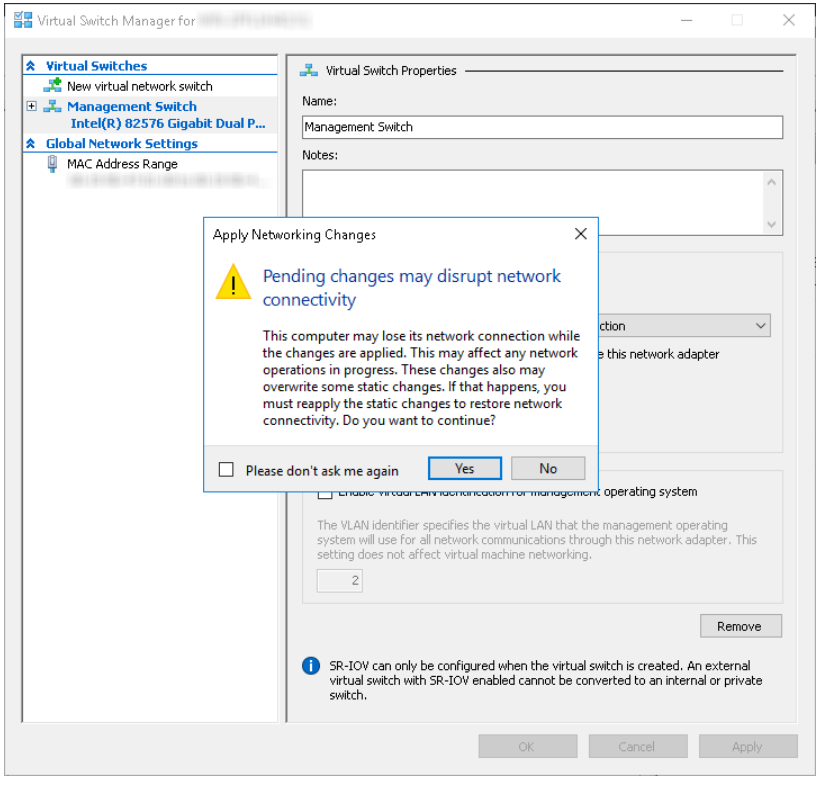
e. [Name] に「`Management Switch`」と入力します。

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。

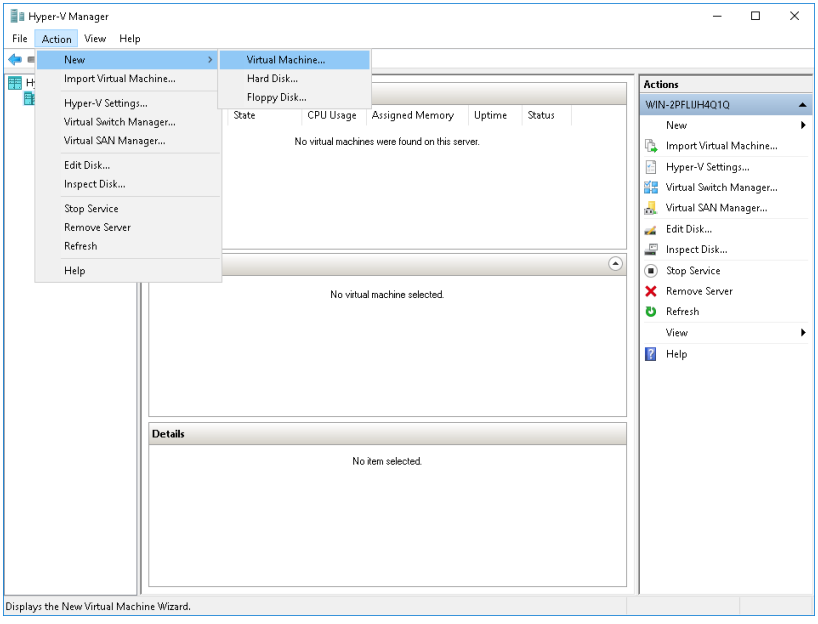
o. 警告を読んで、[Yes] をクリックします。

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。

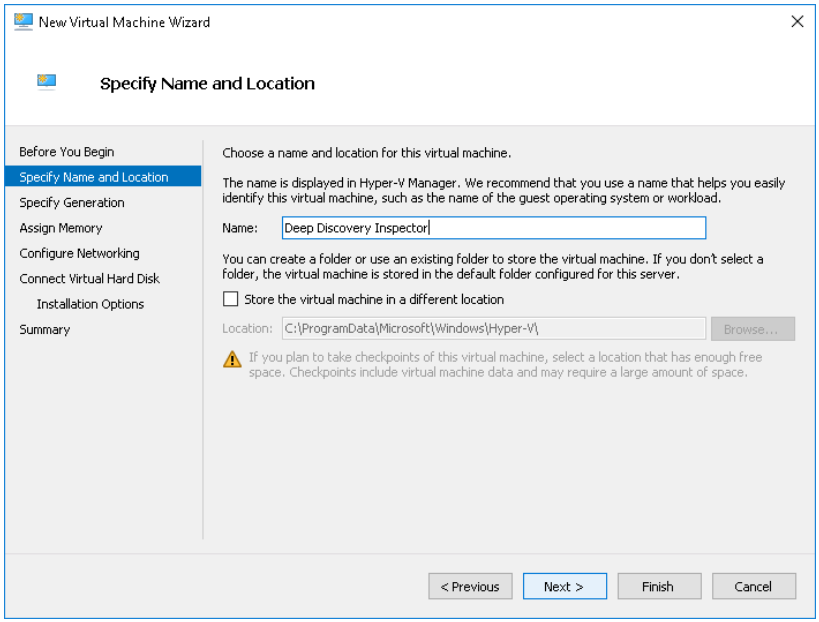



[New Virtual Machine Wizard] 画面が、[Before You Begin] 画面とともに開きます。

b. [Next] をクリックします。

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

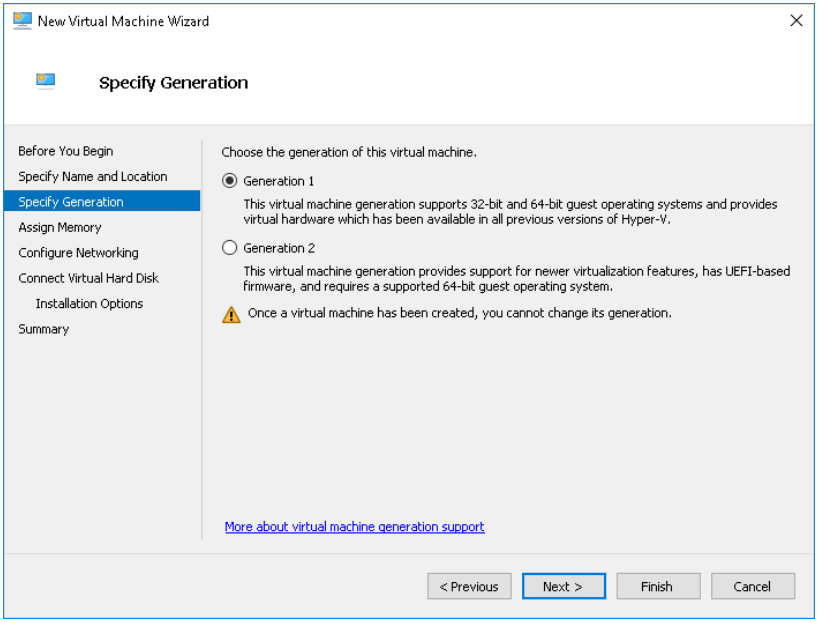
c. [Name] に「`Deep Discovery Inspector`」と入力します。




d. [Next] をクリックします。

[Specify Generation] 画面が表示されます。

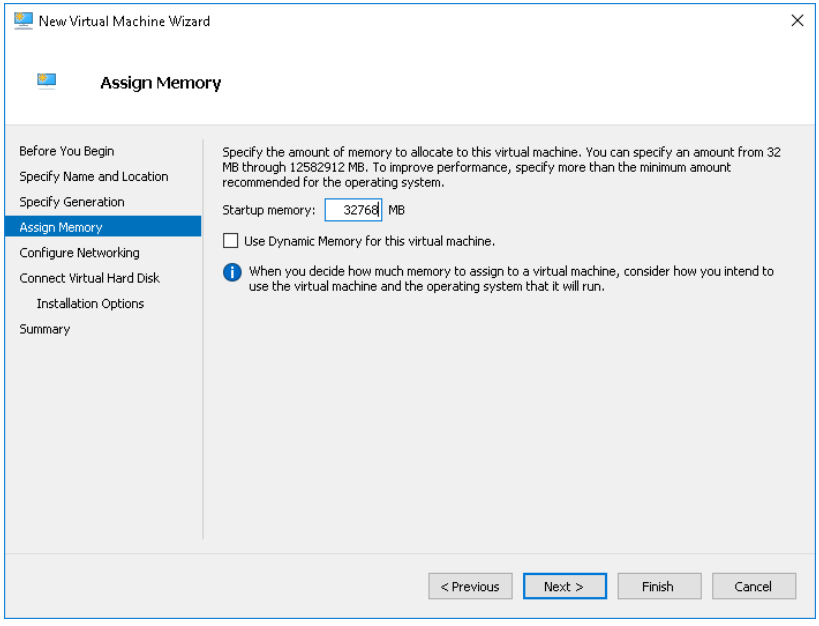
e. [Generation 1] を選択します。




f. [Next] をクリックします。

[Assign Memory] 画面が表示されます。

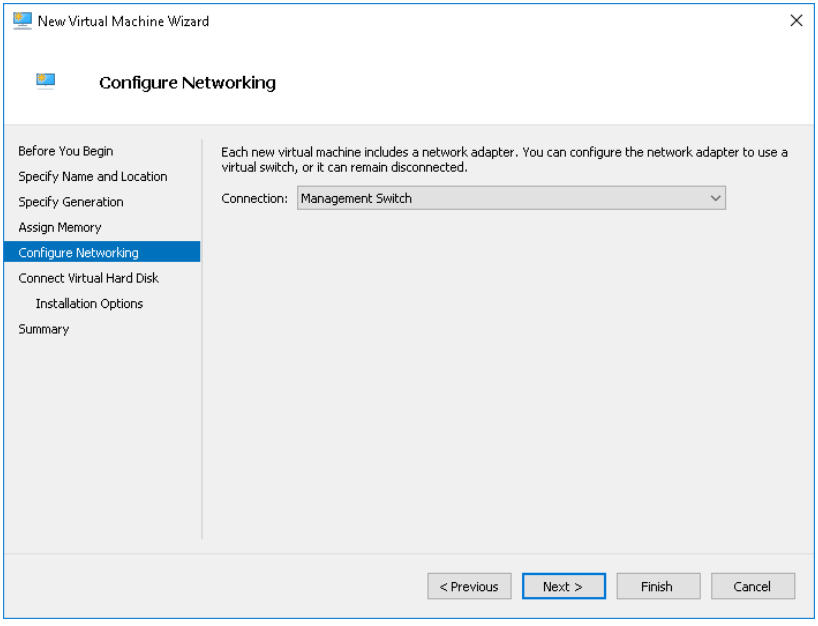
g. [Startup memory] に少なくとも 32768MB (32GB) を割り当てます。




h. [Next] をクリックします。

[Configure Networking] 画面が表示されます。

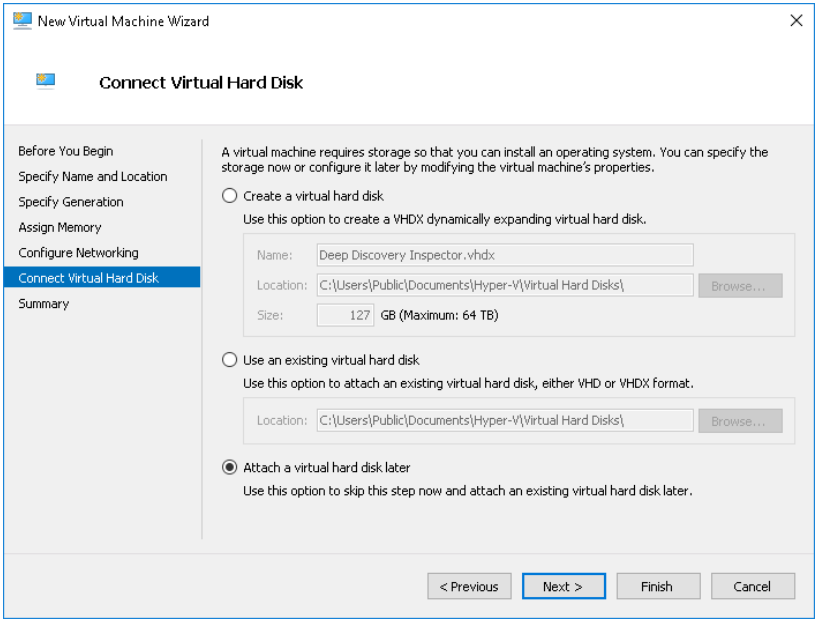
i. [Connection] で [Management Switch] を選択します。




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。



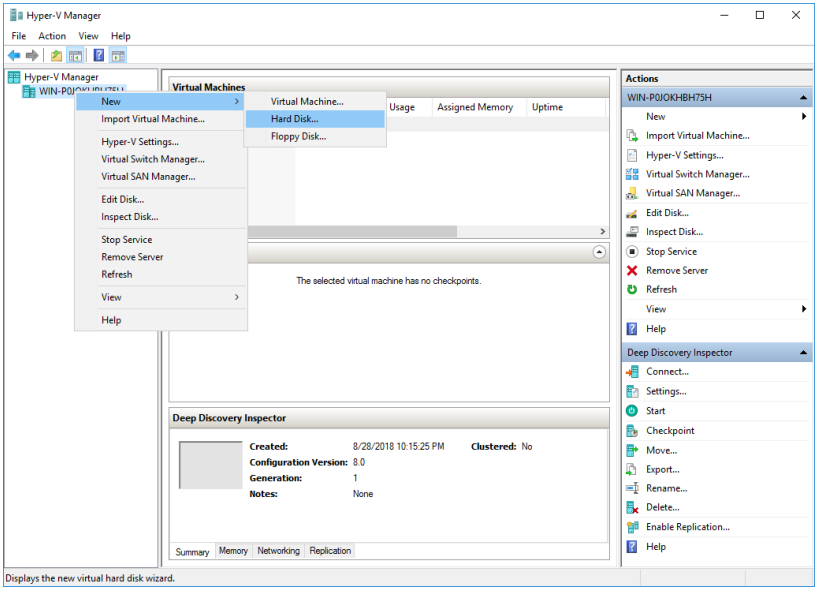

l. [Next] をクリックします。

[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 Inspector 仮想マシンを選択し、[Action] > [New] > [Hard Disk] の順に選択します。

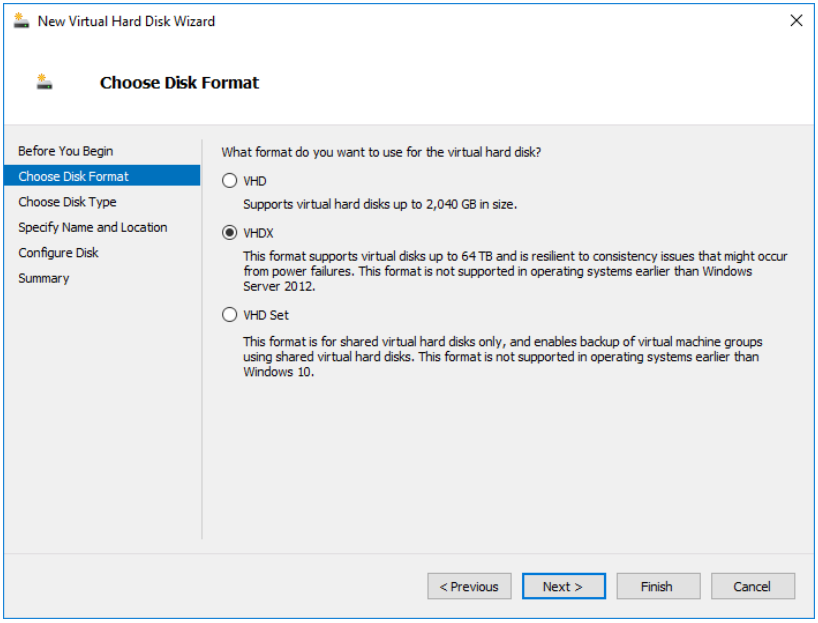



[New Virtual Hard Disk Wizard] 画面が、[Before You Begin] 画面とともに開きます。

b. [Next] をクリックします。

[Choose Disk Format] 画面が表示されます。

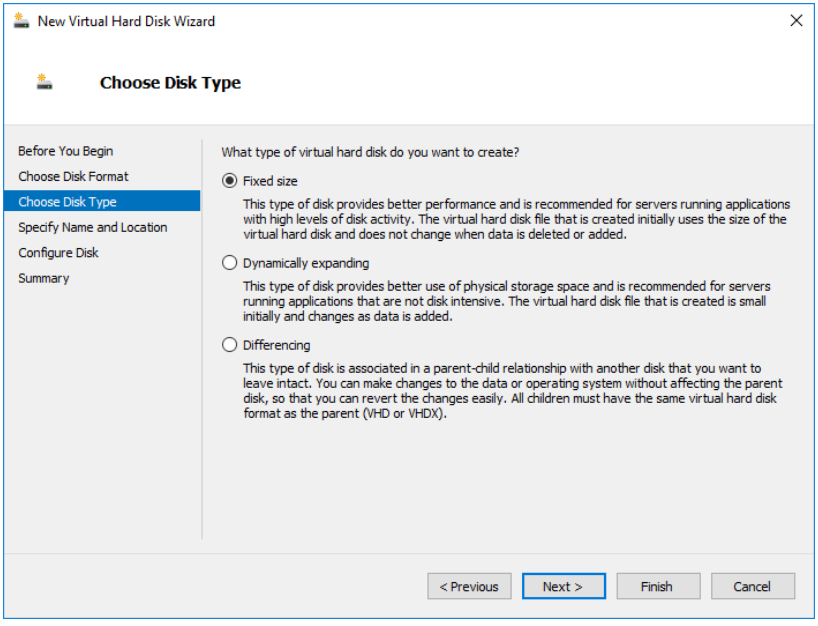
c. [VHDX] を選択します。




d. [Next] をクリックします。

[Choose Disk Type] 画面が表示されます。

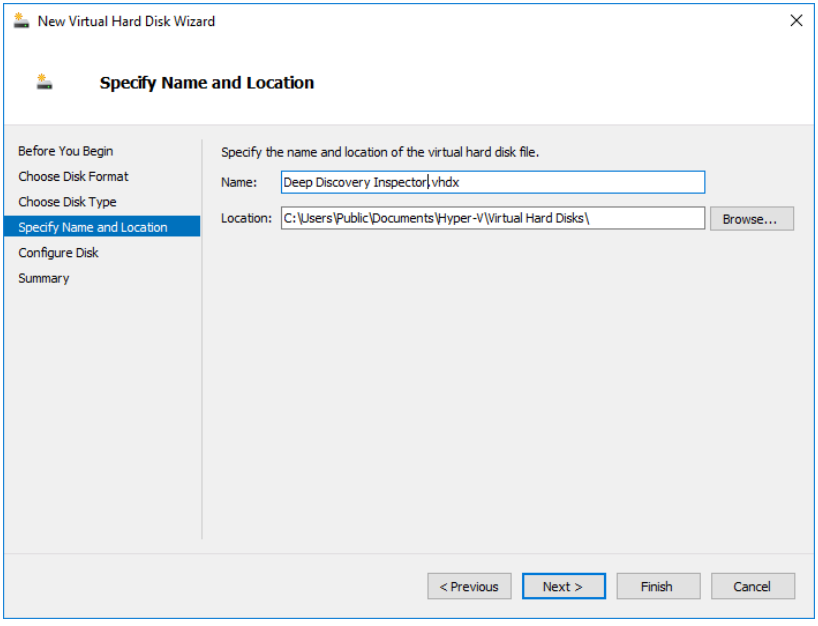
e. [Fixed size] を選択します。




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 Inspector.vhdx`」と入力します。



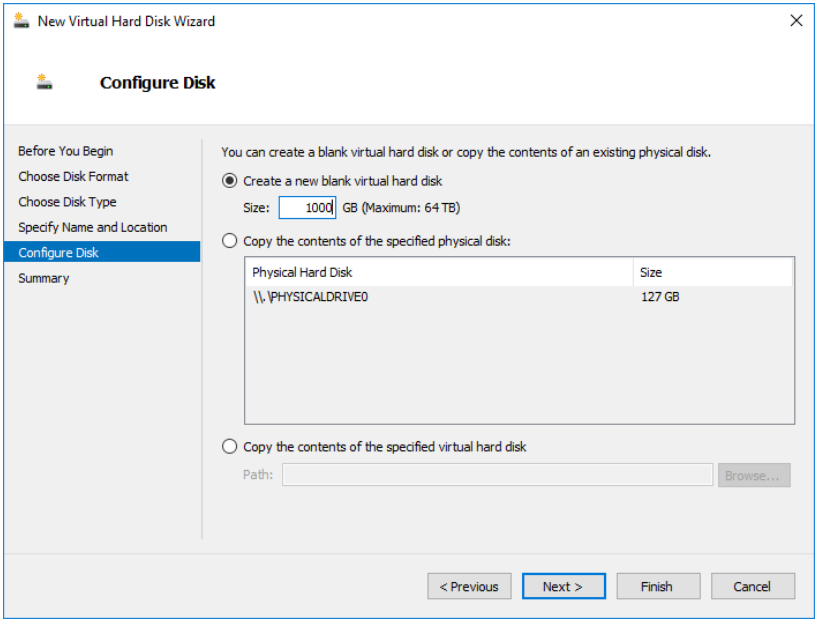

h. [Next] をクリックします。

[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] で、使用する Deep Discovery Inspector のモデルに応じて次のように指定します。

- 250 または 500Mbps スループットモデルでは、500GB 以上を指定します。
- 1000Mbps スループットモデルでは、1000GB 以上を指定します。




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。

---

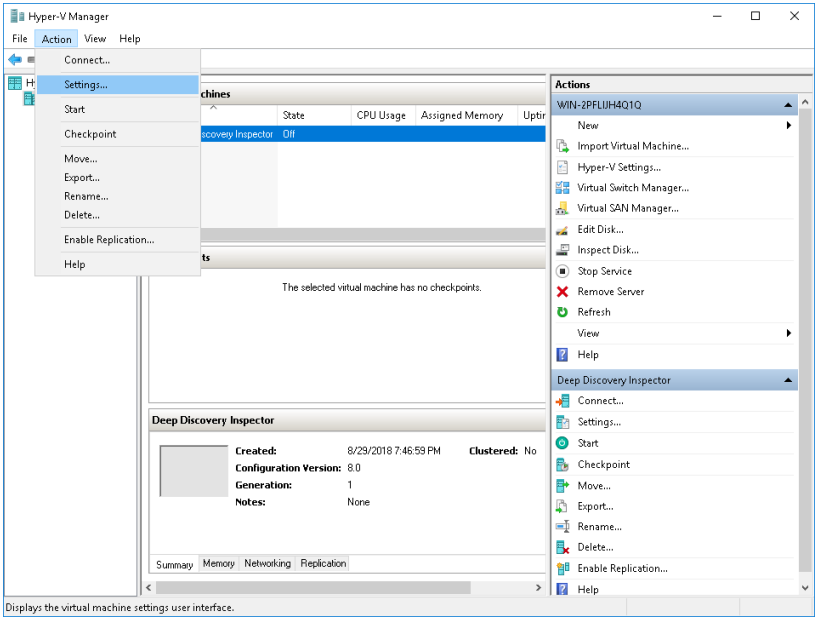
**注意**

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 Inspector 仮想マシンを選択し、[Action] > [Settings] の順に選択します。



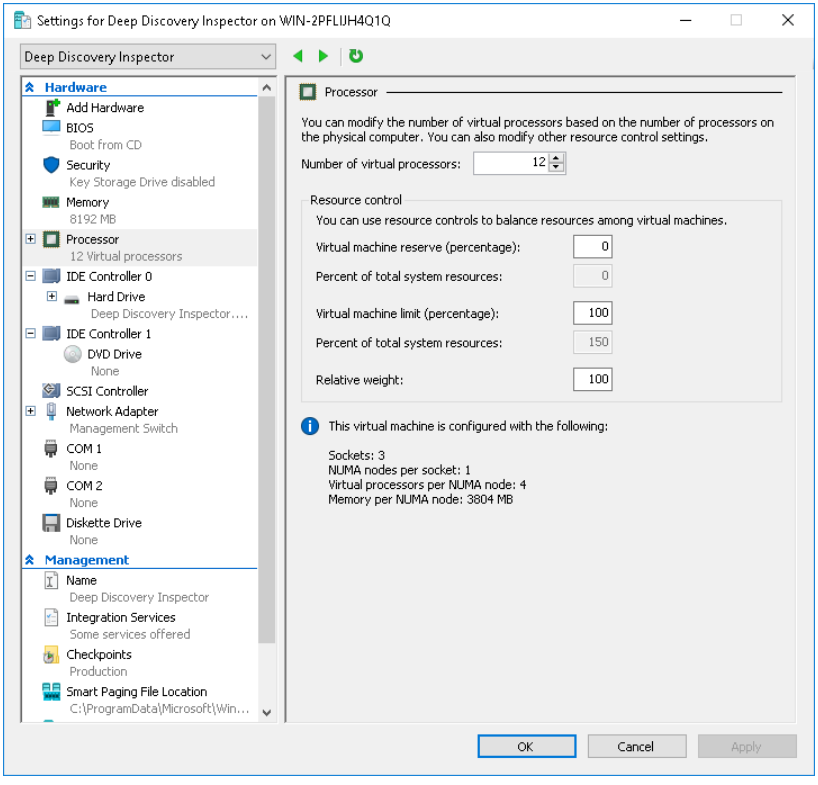

設定画面が表示されます。

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. [For Number of virtual processors] で、使用する Deep Discovery Inspector のモデルに応じて次のように指定します。

- 250 または 500Mbps スループットモデルでは、少なくとも 6 個の仮想プロセッサを指定します。
- 1000Mbps スループットモデルでは、少なくとも 12 個の仮想プロセッサを指定します。

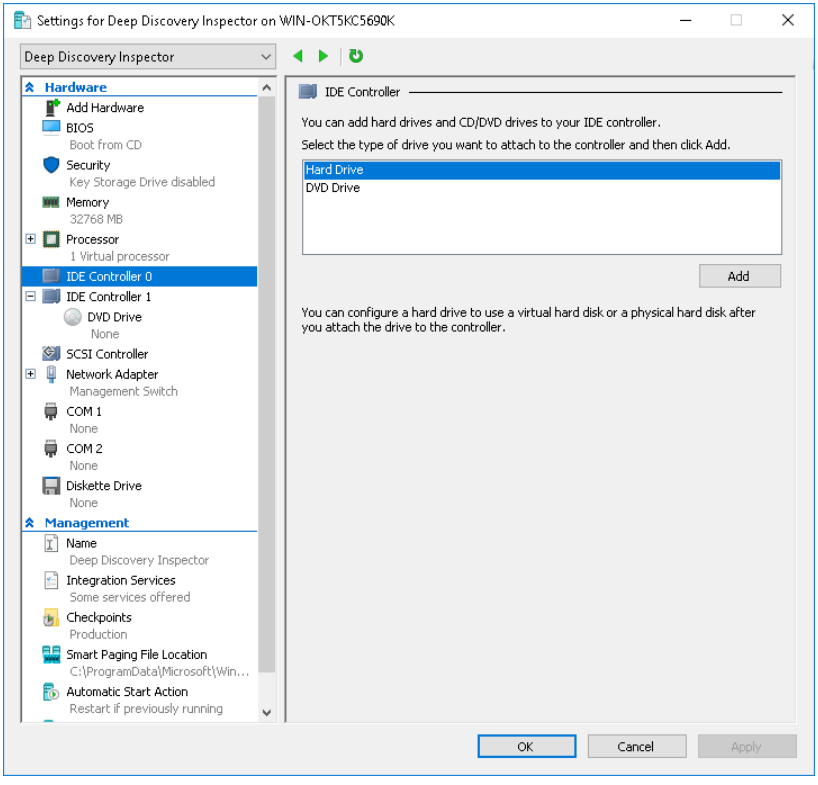



d. [Apply] をクリックします。

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。

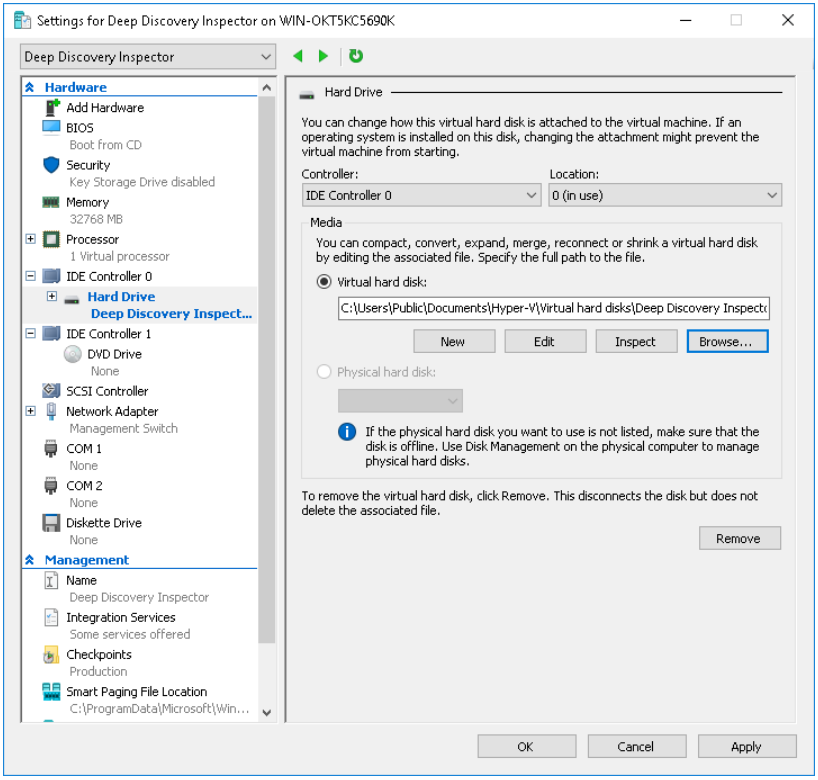
f. コントローラに接続するドライブの種類に、[Hard Drive] を選択します。




g. [Add] をクリックします。

[Hard Drive] の設定が表示されます。

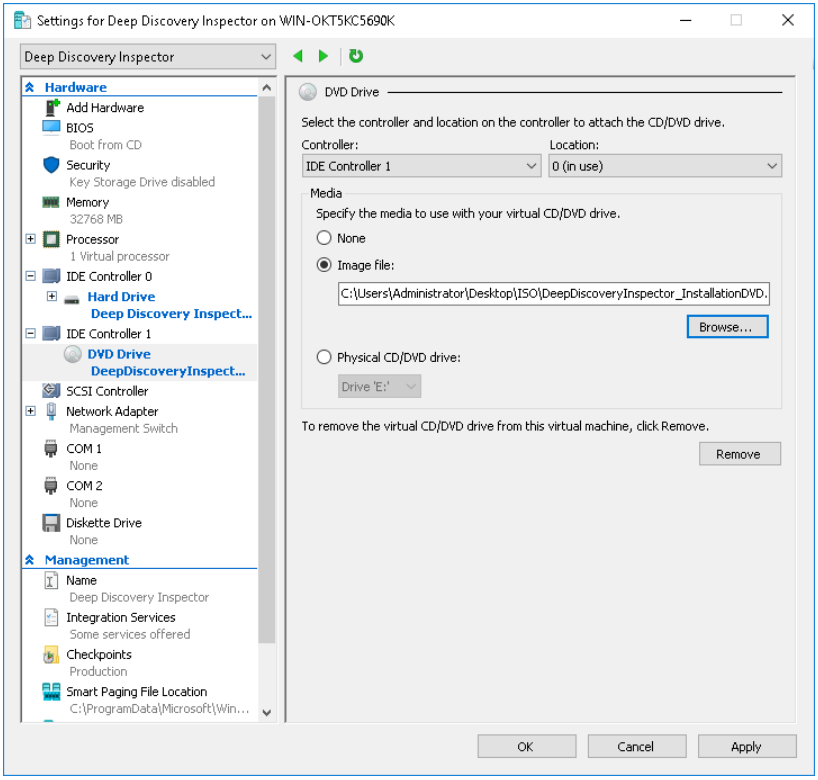
h. [Virtual hard disk] に `Deep Discovery Inspector.vhdx` の場所を指定します。




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。

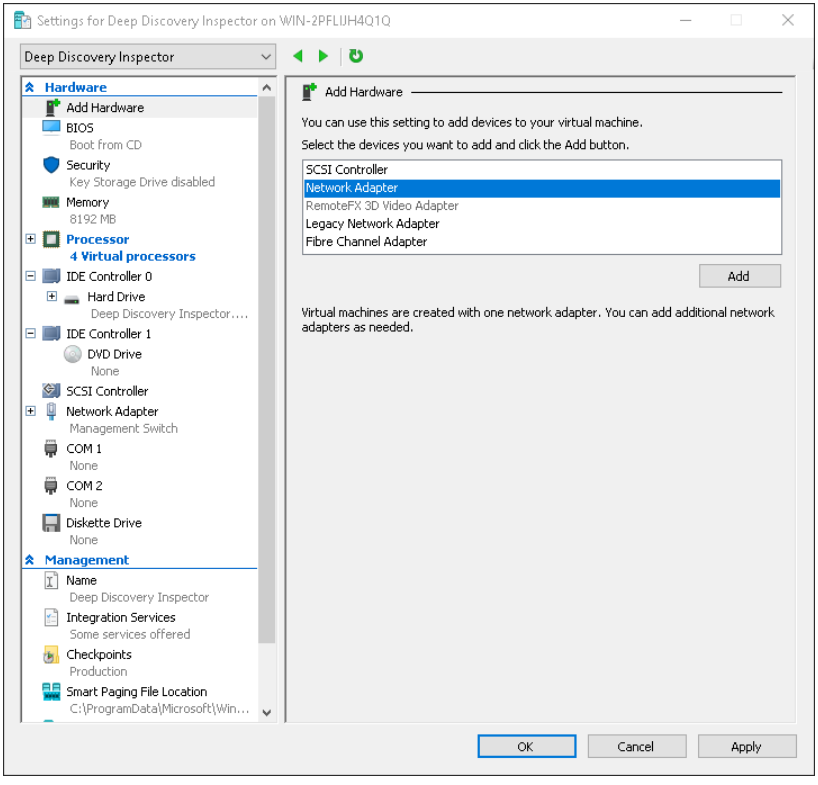
j. [Media] に [Image file] を選択し、Deep Discovery Inspector の ISO ファイルの場所を指定します。




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。

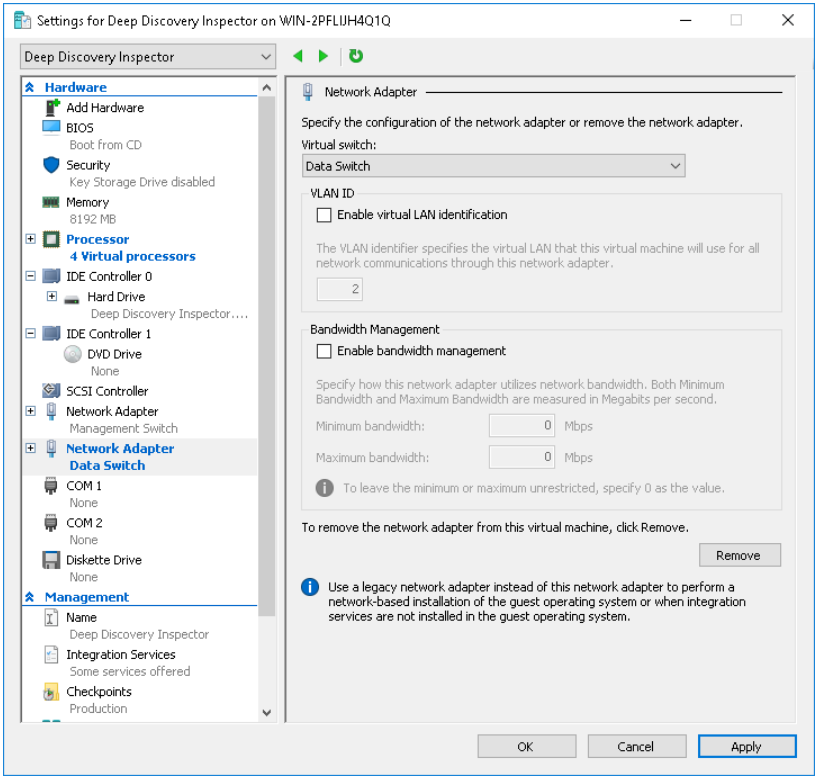
l. 追加するデバイスに [Network Adapter] を選択します。




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。

5. ミラーリング用に Hyper-V ネットワークを設定します。

詳細については、129 ページの「Microsoft Hyper-V で内部仮想マシントラフィックのミラーリングを設定する」および 127 ページの「Microsoft Hyper-V で外部トラフィックのミラーリングを設定する」を参照してください。

## Microsoft Hyper-V でのトラフィックのミラーリングの設定

外部および内部の仮想マシントラフィックの取得を有効にする方法については、次の項目を参照してください。

- 127 ページの「Microsoft Hyper-V で外部トラフィックのミラーリングを設定する」
- 129 ページの「Microsoft Hyper-V で内部仮想マシントラフィックのミラーリングを設定する」

### Microsoft Hyper-V で外部トラフィックのミラーリングを設定する

ミラーリングされた外部トラフィックの取得を有効にするには、Deep Discovery Inspector のホストで次の手順を実行します。

**手順**

1. Hyper-V ホストの Powershell で次のコマンドを実行し、Data Switch の監視モードを設定します。

```
$DataSwitch = "Data Switch"
$extFeature = Get-VMSystemSwitchExtensionPortFeature `
    -FeatureName "Ethernet Switch Port Security Settings"
$extFeature.SettingData.MonitorMode = 2
Add-VMSwitchExtensionPortFeature `
    -ExternalPort -SwitchName $DataSwitch `
    -VMSwitchExtensionFeature $extFeature
```

2. Powershell で次のコマンドを実行し、設定が正しく行われたことを確認します。

```
$extFeature = Get-VMSwitchExtensionPortFeature `
    -ExternalPort -SwitchName $DataSwitch `
    -FeatureName "Ethernet Switch Port Security Settings"
$extFeature.SettingData.MonitorMode
```

正しく設定されている場合、結果の出力は「2」となり、ポートミラーリングモードが「source」であることが示されます。

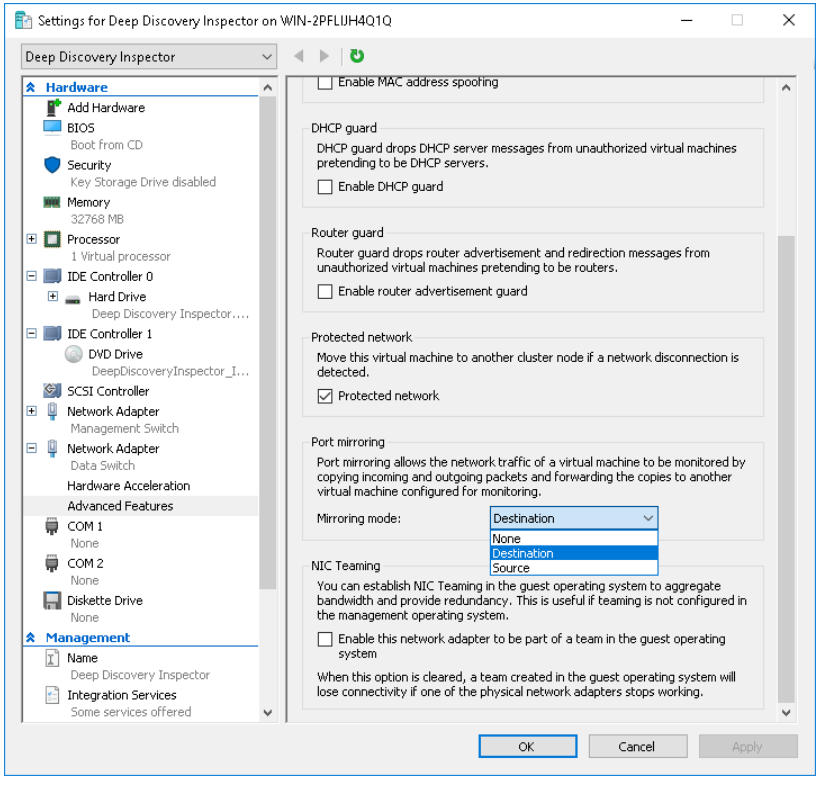
3. 仮想マシンネットワークアダプタの 監視モードを設定します。

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

      設定画面が表示されます。

   b. [Data Switch] を展開し、[Advanced Features] をクリックします。

   c. [Mirroring mode] で [Destination] を選択します。




   d. [OK] をクリックします。

4. Powershell で次のコマンドを実行し、Data Switch の VLAN モードを設定します。

```
$VMName = "Deep Discovery Inspector"
$DataSwitch = "Data Switch"
Get-VMNetworkAdapter -VMName $VMName |
    ? SwitchName -eq "$DataSwitch" |
    % { Set-VMNetworkAdapterVlan -VMNetworkAdapter $_ `
    -Trunk -AllowedVlanIdList 1-4094 -NativeVlanId 0 }
```

5. (オプション) Powershell で次のコマンドを実行し、物理アダプタにジャンボ MTU を設定して、ネットワークパケットの破棄を防止します。

**注意**

`$NetAdapter` の値には、Hyper-V ホストの物理ネットワークアダプタの名前を使用します。

```
$NetAdapter = "Ethernet0"
Get-NetAdapterAdvancedProperty -Name $NetAdapter `
-RegistryKeyword "*jumbopacket" |
Set-NetAdapterAdvancedProperty -RegistryValue 4088
```

6. 仮想マシンを起動し、トラフィックがミラーリングされ、検出されることを確認します。

## Microsoft Hyper-V で内部仮想マシントラフィックのミラーリングを設定する

同じホスト上の仮想マシンからミラーリングされたトラフィックの取得を有効にするには、Deep Discovery Inspector のホストで次の手順を実行します。

### 手順

1. Hyper-V マネージャーで、Deep Discovery Inspector 仮想マシンをクリックし、[Action] > [Settings] の順に選択します。

   設定画面が表示されます。

2. 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。

3. 追加するデバイスに [Network Adapter] を選択します。
4. [Add] をクリックします。

   [Network Adapter] の設定が表示されます。
5. [Virtual switch] で [Management Switch] を選択します。
6. 左側のペインで [Management Switch] を展開し、[Advanced Features] をクリックします。
7. [Mirroring mode] で [Destination] を選択します。
8. [OK] をクリックします。
9. Hyper-V マネージャーで、Deep Discovery Inspector と同じホスト上にある仮想マシンをクリックし、[Action] > [Settings] の順に選択します。

   設定画面が表示されます。
10. 左側のペインで [Management Switch] を展開し、[高度な機能] をクリックします。
11. [Mirroring mode] で [Source] を選択します。
12. [OK] をクリックします。
13. Deep Discovery Inspector 仮想マシンを起動し、トラフィックがミラーリングされ、検出されることを確認します。

# 第 8 章

# 仮想アプライアンスへのインストール

Deep Discovery Inspector を仮想アプライアンスとしてインストールするための手順について、次の項目を参照してください。

# オプションの設定

Deep Discovery Inspector の管理コンソールナビゲーションを有効にするには、次のオプションを設定します。


- 132 ページの「Chrome の JavaScript オプションの設定」
- 132 ページの「Firefox の JavaScript オプションの設定」
- 133 ページの「ESXi での仮想アプライアンスのオプションの 設定」


## Chrome の JavaScript オプションの設定

**手順**

1. ブラウザで、[設定] に移動します。
2. [詳細設定を表示...] をクリックします。
3. [プライバシー] の [コンテンツの設定...] をクリックします。
4. [JavaScript] の下の [すべてのサイトで Javascript の実行を許可する (推奨)] をクリックします。
5. [完了] をクリックします。

## Firefox の JavaScript オプションの設定

**手順**

1. バージョン 23 より前の Firefox では、次の操作を実行します。
   a. ブラウザで、[オプション] > [コンテンツ] タブの順に選択します。
   b. [JavaScript を有効にする] が選択されていることを確認します。
   c. [OK] をクリックします。
2. バージョン 23 以上の Firefox では、次の操作を実行します。
   a. アドレスバーで「`about:config`」と入力し、<Enter> キーを押します。

b. [細心の注意を払って使用する] をクリックします。

c. [設定名] の [javascript.enabled] の [値] が [true] に設定されていることを確認します。

## ESXi での仮想アプライアンスのオプションの設定

以下の手順は、サポート対象バージョンの ESXi に適用されます。詳細については、92 ページの「VMware ESXi での仮想マシンの要件」を参照してください。

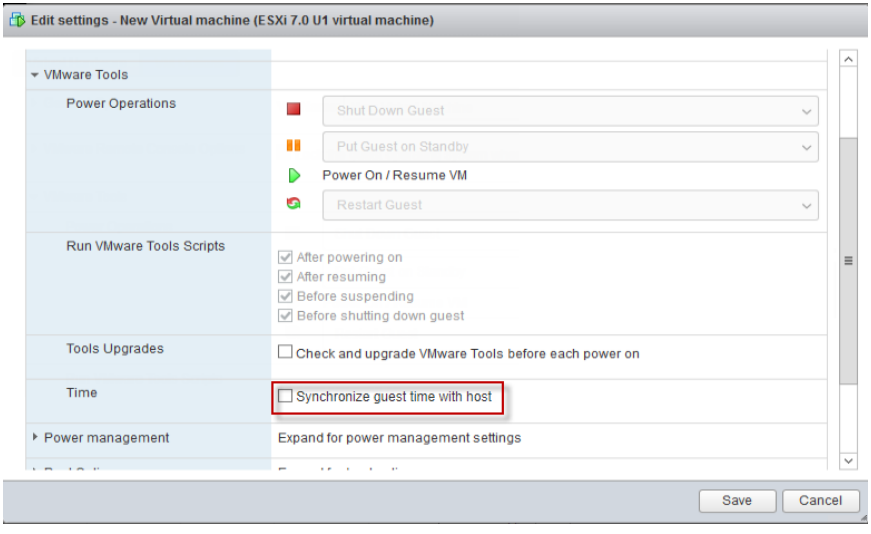
### 手順

1. [VMware ESXi] > [Virtual Machines] の順に選択し、アプライアンス名を右クリックして、[Edit Settings...] を選択します。

   設定画面が表示されます。

2. 設定画面で [VM Options] タブをクリックして、[VMware Tools] を選択します。

3. [Synchronize guest time with host] オプションを無効にします。



# Deep Discovery Inspector 仮想アプライアンスのインストール

Deep Discovery Inspector は、次のハイパーバイザにインストールできます。

- VMware ESXi 7.0 または 8.0

  VMware ESXi のライセンスは別途取得する必要があり、その使用は、製品に固有の VMware 使用許諾契約に記載されている条項に従うものとします。

- Windows Server 2019 または 2022 上の Microsoft Hyper-V
- RHEL 9.2 KVM

**手順**

1. Deep Discovery Inspector をインストールする前に、インストール先のハードドライブ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ドライブ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。

   ヒント

   Deep Discovery Inspector を再インストールする場合は、Deep Discovery Inspector 管理コンソールで [管理] > [システムのメンテナンス] > [バックアップ/復元] の順に選択することで、現在の設定をバックアップできます。

2. 仮想アプライアンスを作成します。

   詳細については、91 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。

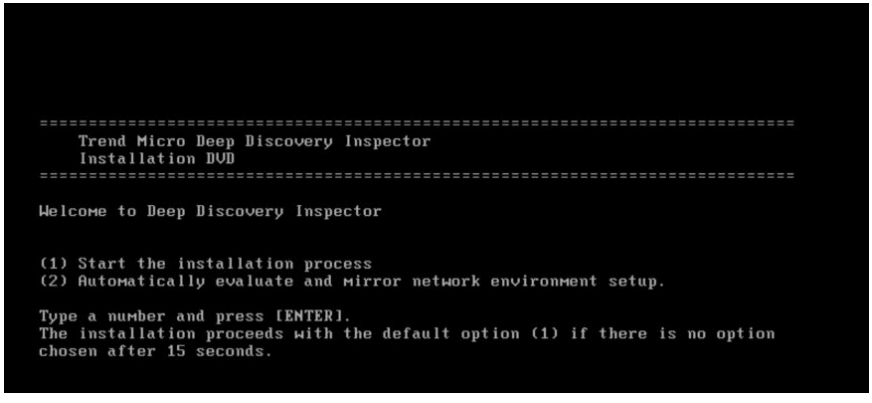
   VMware ESXi サーバに Deep Discovery Inspector をインストールする場合は、ハードディスク容量を確保できるよう、仮想アプライアンスのスナップショット機能を無効にします。

3. 仮想マシンを起動します。
4. Deep Discovery Inspector のインストール DVD をハイパーバイザサーバの物理 CD/DVD ドライブに挿入します。

5. 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。
6. 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。
7. 仮想アプライアンスを再起動します。
   - VMware vSphere Client では、[Inventory] > [Virtual Machine] > [Guest] > [Send] の順に選択し、Ctrl+Alt+Delete キーを押します。
   - RHEL KVM サーバでは、管理ツールを使用します。

     詳細については、https://www.linux-kvm.org/page/Management_Tools を参照してください。
   - Hyper-V マネージャでは、サーバを選択し、シャットダウンしてから起動します。

   インストール DVD 画面が表示されます。

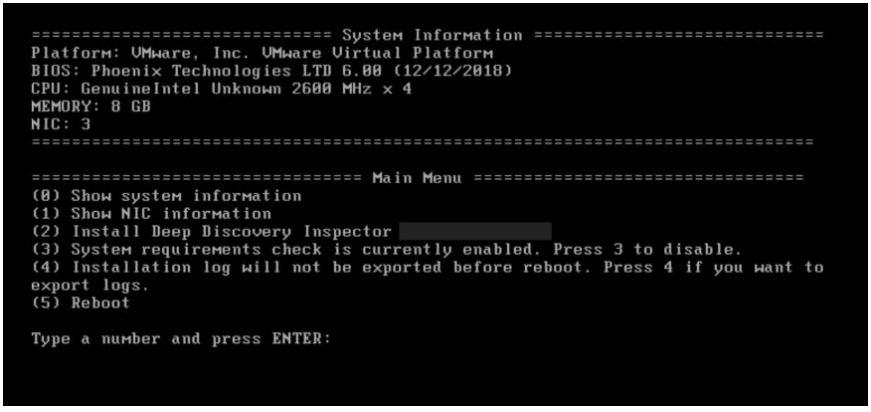



8. Enter キーを押します。

**重要**

シリアル接続で Deep Discovery Inspector をインストールしている場合は、「`serial`」と入力して Enter キーを押します

[System Information] 画面が表示されます。




9. 体験版の導入の場合は、「3」と入力して Enter キーを押し、システム要件のチェックを省略します。

---

**注意**

初期設定では、Deep Discovery Inspector をインストールする前にシステム要件のチェックが行われ、製品の実行に必要なリソースがアプライアンスにあるかどうかが確認されます。

---

10. トラブルシューティング用にインストールログを取得する必要がある場合は、「4」と入力して Enter キーを押します。
11. 「2」と入力して Enter キーを押し、インストールを開始します。

    [Management Port Selection] 画面が表示されます。

管理ポートとして使用できるアクティブなネットワークインタフェースが自動的に検出され、「Link UP」と表示されます。

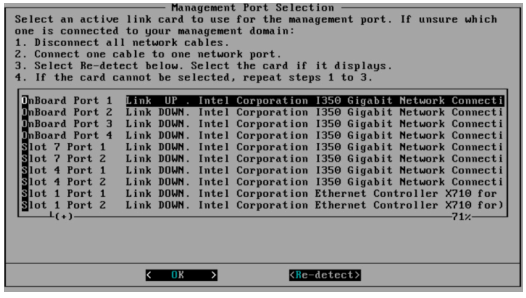



図 8-1. [Management Port Selection]

12. ネットワークポートのステータスと、実際のポートのステータスが一致することを確認します。

    ステータスに矛盾がある場合は、[Re-detect] を選択し、Enter キーを押します。

13. [Management Port Selection] 画面に表示される手順を実行して、管理ドメインに接続するアクティブなネットワークインタフェースを 確認します。

14. アクティブなネットワークインタフェースを 選択して、Enter キーを押します。

    インストールが続行され、完了します。

15. [System Information] 画面でインストールログのエクスポートを有効にした場合は、インストールログを保存します。

    a. ストレージデバイスを選択して、Enter キーを押します。

       目的のストレージデバイスがリストにない場合は、[Re-detect] に移動し、Enter キーを押してリストを更新します。

    b. インストールログのファイル名が表示されたら、Enter キーを押します。

       後で参照できるようにファイル名をメモに記録します。ファイル名には次の形式が使用されます。

```
install.log.YYYY-MM-DD-hh-mm-ss
```

ヒント

エクスポートされたインストールログは [sda11] に保存することをお勧めします。

システムが自動的に再起動し、事前設定コンソールが表示されます。使用している場合は、インストール DVD が CD/DVD ドライブから排出されます。

16. (オプション) 再度インストールが実行されないように DVD を取り出します。

17. Deep Discovery Inspector のネットワークを設定します。

    - 事前設定コンソールにアクセスしてデバイス設定を変更します。

      詳細については、173 ページの事前設定を参照してください。

    - 管理コンソールを開き、アプライアンスの IP 設定を変更します。

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

### 次に進む前に

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

# 第 9 章

# VMware 仮想分散スイッチでのポートミラーリング

Deep Discovery Inspector では、ミラーリングされたトラフィックを仮想分散スイッチを使用して監視できます。仮想分散スイッチの作成方法、およびミラーリングされたトラフィックを Deep Discovery Inspector の仮想アプライアンスで監視するための設定方法については、次の項目を参照してください。


- 140 ページの「VMware vSphere Distributed Switch (VDS) の作成」
- 142 ページの「Deep Discovery Inspector 仮想アプライアンスと VDS」

# VMware vSphere Distributed Switch (VDS) の作成

**手順**

1. 新しい仮想分散スイッチを作成します。
   a. vSphere Web Client にログインします。
   b. [Networking] をクリックします。
   c. 左側のパネルでデータセンターを選択します。
   d. 右側のパネルで [Create a new distributed switch] アイコンをクリックします。

      [New Distributed Switch] 画面が表示されます。
   e. スイッチの名前を入力し、[Next] をクリックします。
   f. 分散スイッチのバージョンを選択し、[Next] をクリックします。
   g. [Number of uplinks] で、SPAN トラフィックが専用 NIC を通過する場合は 2 以上を設定します。それ以外の場合は 1 を設定します。

      
      注意
      トレンドマイクロでは、専用 NIC を使用することをお勧めします。
   h. [Network I/O Control] で、次のいずれかのオプションを選択します。
      - Disabled: SPAN トラフィックが専用 NIC を通過する場合

        
        注意
        トレンドマイクロでは、専用 NIC を使用することをお勧めします。
      - Enabled: SPAN トラフィックが監視対象トラフィックと同じ NIC を通過する場合
   i. [Create a default port group] をオフにします。
   j. [Next] をクリックします。

k. 概要情報が正しいことを確認して、[Finish] をクリックします。

2. 仮想スイッチを設定します。

   a. 前の手順で作成した仮想分散スイッチを右クリックし、[Settings] > [Edit Settings] の順に選択します。

      [Edit Settings] 画面が表示されます。

   b. [Advanced] をクリックします。

      詳細設定が表示されます。

   c. [MTU (Bytes)] に「`1600`」と指定します。

3. ポートグループを仮想分散スイッチに追加します。

   a. [Networking] をクリックします。

   b. 前の手順で作成した仮想分散スイッチを右クリックし、[Distributed Port Group] > [New Distributed Port Group] の順に選択します。

      [New Distributed Port Group] 画面が表示されます。

   c. ポートグループの名前を入力し、[Next] をクリックします。

   d. [Port binding] で [Static binding] を選択します。

   e. [Port allocation] で [Fixed] を選択します。

   f. [Number of ports] に、接続するポートの数を入力します。

   g. [Next] をクリックします。

   h. 概要画面で設定が正しいことを確認して、[Finish] をクリックします。

      新しいポートグループが [Manage] タブに表示されます。

4. (オプション) 手順 3 を繰り返して、ポートグループをさらに追加します。

5. ESXi ホストを仮想分散スイッチに追加します。

   a. 前の手順で作成した仮想スイッチを右クリックし、[Add and Manage Hosts] を選択します。

      [Add and Manage Hosts] 画面が表示されます。

b. [Select task] で [Add host and manage host networking (advanced)] を選択します。

c. [Next] をクリックします。

d. [Select hosts] で [+ New hosts] をクリックし、管理下の ESXi ホストを追加します。

e. [Next] をクリックします。

f. [Selet network adapter tasks] で、[Manage physical adapters] と [Migrate virtual machine networking] のチェックマークをオンにします。

g. [Next] をクリックします。

h. [Manage physical network adapters] で、ネットワーク環境に応じて物理ネットワークアダプタを管理します。

i. [次へ] をクリックします。

j. [Analyze impact] で [No impact] を指定します。

k. [Next] をクリックします。

l. [Migrate VM networking] で、ネットワーク環境に応じて仮想マシンネットワークを移行します。

m. [Next] をクリックします。

n. [終了準備の完了] で [Finish] をクリックします。

[Add and Manage Hosts] 画面が閉じます。

o. 前の手順で作成した仮想スイッチをクリックし、[Configure] タブ、[Topology] の順にクリックして、設定した仮想スイッチのトポロジを確認します。

## Deep Discovery Inspector 仮想アプライアンスと VDS

Deep Discovery Inspector 仮想アプライアンスでは、仮想環境内部および外部のミラーリングされた仮想分散スイッチトラフィックを監視できます。要件

および Deep Discovery Inspector と仮想分散スイッチの設定方法については、次の項目を参照してください。

- 143 ページの「VDS を使用する仮想アプライアンスの 要件」
- 145 ページの「仮想アプライアンス - ミラーリングされた外部ネットワークトラフィックの VDS を使用した監視」
- 153 ページの「仮想アプライアンス - ミラーリングされた仮想マシントラフィックの VDS からの監視」

## VDS を使用する仮想アプライアンスの要件

次の表は、Deep Discovery Inspector 仮想アプライアンスの物理 NIC の最小要件を示しています。

表 9-1. 仮想アプライアンスの物理 NIC の要件

| トラフィック元 | リモートミラーリング | カプセル化されたリモートミラーリング | 分散ポートミラーリング |
|---|---|---|---|
| 外部ネットワークトラフィック | ミラーリング先の ESXi ホストには、アップリンクとして 1Gbps Ethernet ネットワークポートが必要です。 | ミラーリング先の ESXi ホストには、アップリンクとして 1Gbps Ethernet ネットワークポートが必要です。<br><br>注意<br>このポートはカプセル化されたリモートミラーリングのミラーリング元からルーティング可能である必要があります。 | サポートされていません。 |

| トラフィック元 | リモートミラーリング | カプセル化されたリモートミラーリング | 分散ポートミラーリング |
|---|---|---|---|
| 仮想マシンネットワークトラフィック | 各 ESXi ホストには、アップリンクとして 1Gbps Ethernet ネットワークポートが必要です。 | ミラーリング先の ESXi ホストには、アップリンクとして 1Gbps Ethernet ネットワークポートが必要です。<br><br>注意<br>このポートは他の ESXi ホストの管理 VMkernel ポートからルーティング可能である必要があります。 | 物理ポートの要件はありません。 |

## 仮想アプライアンス - ミラーリングされた外部ネットワークトラフィックの VDS を使用した監視

Deep Discovery Inspector 仮想アプライアンスでは、カプセル化されたリモートミラーリングまたはリモートミラーリングにより、ミラーリングされたトラフィックを仮想分散スイッチを使用して監視できます。Deep Discovery Inspector とネットワークデバイスの設定方法については、次の項目を参照してください。

- 146 ページの「仮想アプライアンス - カプセル化されたリモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視の設定」
- 149 ページの「仮想アプライアンス - リモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視の設定」

## 仮想アプライアンス - カプセル化されたリモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視の設定

カプセル化されたリモートミラーリングにより複数のネットワークインタフェースまたは VLAN のトラフィックを監視して、対象トラフィックを 1 つ以上のミラーリング先に送信できます。

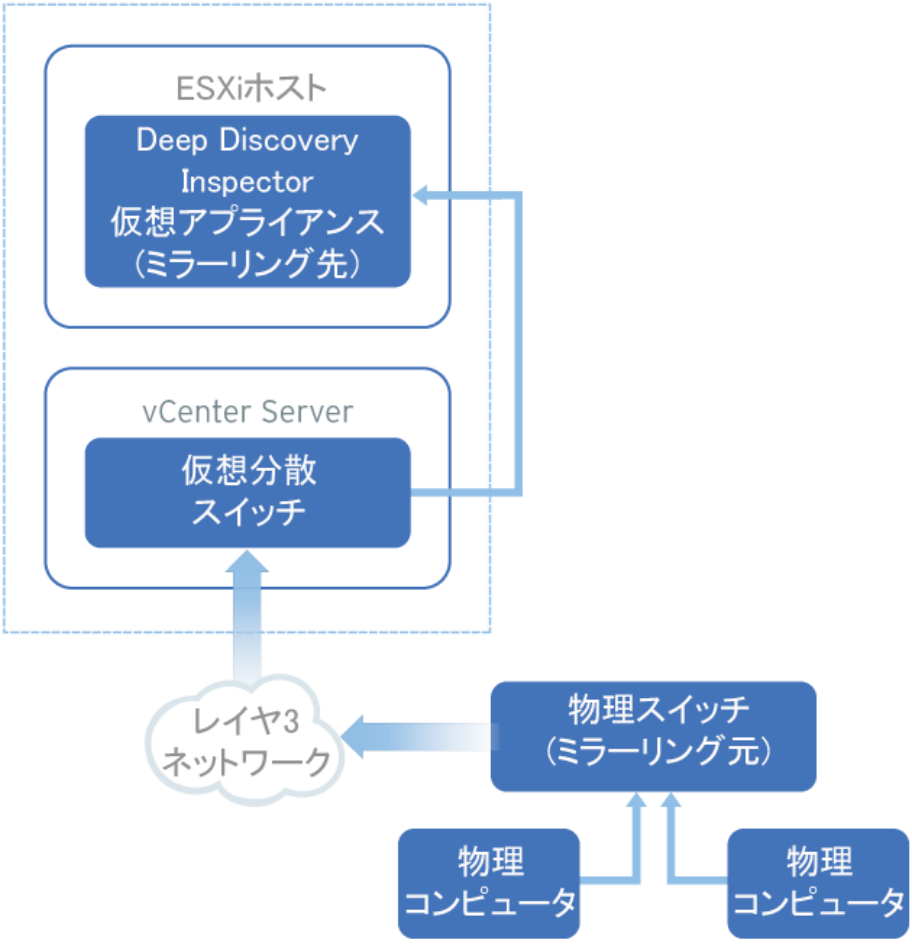



図 9-1. カプセル化されたリモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視

仮想スイッチのカプセル化されたリモートミラーリングでは、初期設定で、ESXi ホストの管理 VMkernel ポートがカプセル化の送信元 IP アドレスとして使用されます。

以下の手順におけるミラーリング元とミラーリング先は次のようになります。

- ミラーリング元: ミラーリングされたトラフィックを転送する物理スイッチ
- ミラーリング先: Deep Discovery Inspector

---

**手順**

1. カプセル化され、リモートミラーリングされたトラフィックを転送するようにミラーリング元を設定します。

   ---

   **重要**

   次の手順の Deep Discovery Inspector で設定する、カプセル化されたリモートミラーリングのミラーリング先 IP アドレスに、スイッチからトラフィックをルーティングできることを確認します。

   ---

2. カプセル化され、リモートミラーリングされたトラフィックを受信するようにミラーリング先を設定します。

   a. Deep Discovery Inspector 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。

      [ネットワークインタフェース] 画面が表示されます。

   b. データポートを見つけ、行の先頭にある右向き矢印
      (
      
      ) をクリックします。

   c. [カプセル化されたリモートミラーリング] を選択します。

   d. カプセル化されたリモートミラーリングのミラーリング先アドレスを指定します。

e. [保存] をクリックします。

## 仮想アプライアンス - リモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視の設定

リモートミラーリングにより、あるスイッチ上のトラフィックを別のスイッチのデバイスから監視して、対象トラフィックを 1 つ以上のミラーリング先に送信できます。

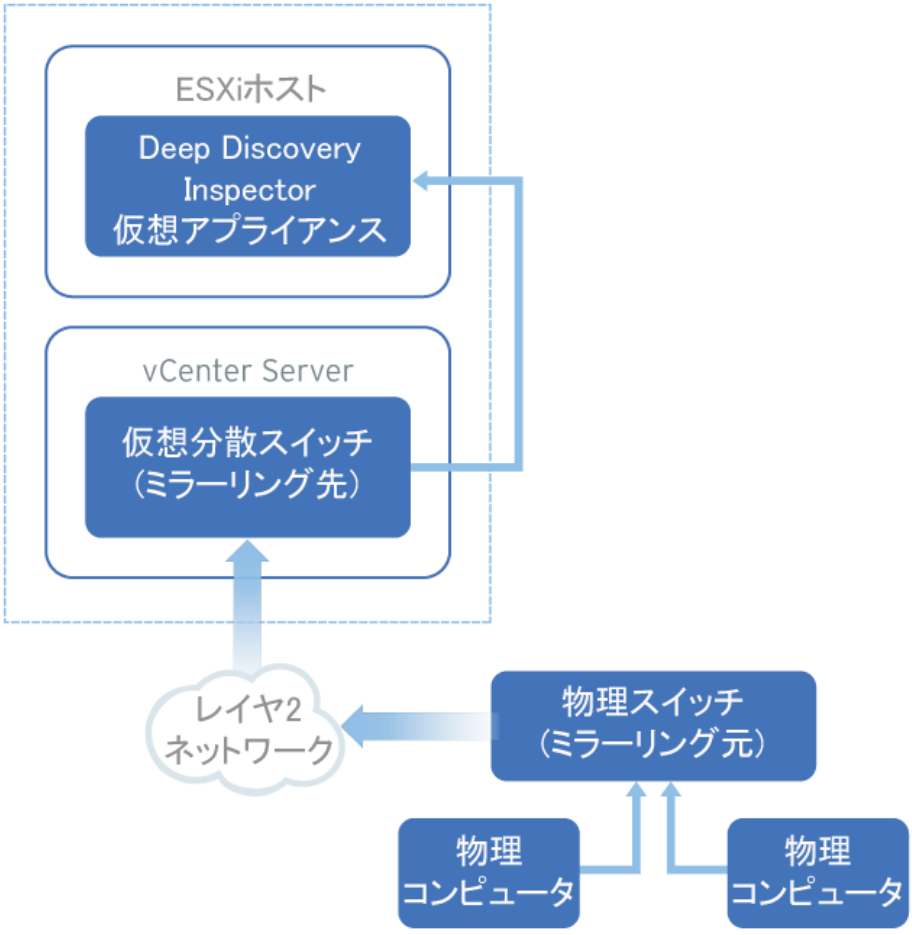



図 9-2. リモートミラーリングによりミラーリングされた外部ネットワークトラフィックの監視

リモートミラーリングでは、リモートミラーリング VLAN を物理スイッチ上に設定する必要があります。リモートミラーリング VLAN を設定できない場合は、代わりにカプセル化されたリモートミラーリングを使用することを検討してください。

以下の手順におけるミラーリング元とミラーリング先は次のようになります。

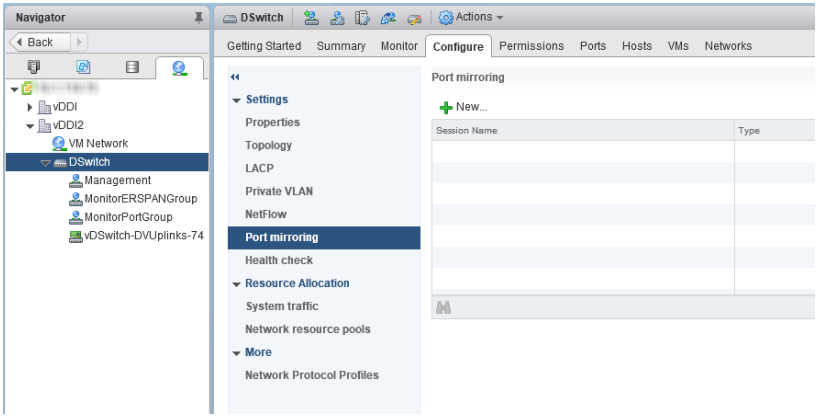
- ミラーリング元: ミラーリングされたトラフィックを仮想分散スイッチに転送する物理スイッチ
- ミラーリング先: ミラーリングされたトラフィックを受信する仮想分散スイッチ

開始する前に、トラフィックを受信する ESXi ホストのアップリンクポートが物理スイッチのトランクポートにリンクしていることを確認します。

**手順**

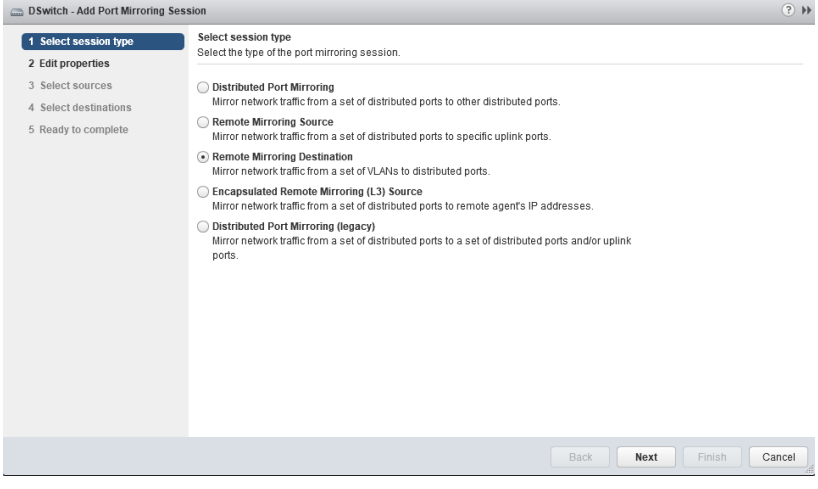
1. ミラーリングされたトラフィックをミラーリング先に転送するようにミラーリング元を設定します。
2. ミラーリングされたトラフィックを受信するようにミラーリング先を設定します。
   a. vSphere Web Client にログインします。
   b. 左側のペインで仮想分散スイッチを選択し、[Configure] をクリックします。
   c. [Port Mirroring] をクリックします。

      [Port mirroring] 画面が表示されます。




d. [New...] をクリックします。

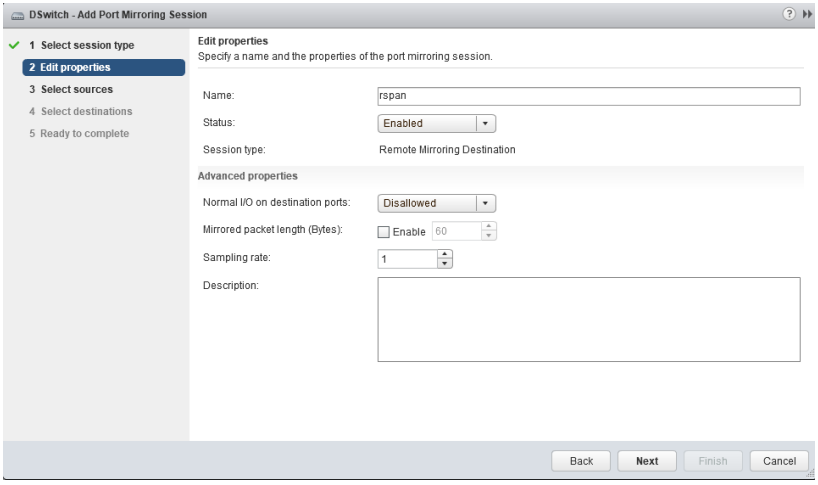
[Add Port Mirroring Sessions] 画面が表示されます。




e. [リモート ミラーリング ターゲット] を選択します。

f. [Next] をクリックします。

[Edit properties] 画面が表示されます。




g. [Name] にセッション名を入力します。

h. [Status] で [Enabled] を選択します。

i. [Next] をクリックします。

[Select sources] 画面が表示されます。

j. プラス記号のアイコンをクリックして、監視する VLAN ID を追加します。

---

**注意**

これは VDS で設定したリモートミラーリング VLAN ID です。

---

k. [Next] をクリックします。

[Select destinations] 画面が表示されます。

l. プラス記号のアイコン
(

) をクリックして、Deep Discovery Inspector データポートのポート ID を追加します。

m. [Next] をクリックします。

[Ready to complete] 画面が表示されます。

n. 設定が正しいことを確認して、[Finish] をクリックします。

## 仮想アプライアンス - ミラーリングされた仮想マシントラフィックの VDS からの監視

Deep Discovery Inspector 仮想アプライアンスでは、Deep Discovery Inspector を含む同じ ESXi ホストまたは異なる ESXi ホストから、ミラーリングされたトラフィックを監視できます。Deep Discovery Inspector と仮想分散スイッチの設定方法については、次の項目を参照してください。

- 153 ページの「仮想アプライアンス - ミラーリングされたトラフィックの異なる ESXi ホストからの監視」
- 165 ページの「仮想アプライアンス - ミラーリングされたトラフィックの同じ ESXi ホストからの監視」

### 仮想アプライアンス - ミラーリングされたトラフィックの異なる ESXi ホストからの監視

Deep Discovery Inspector 仮想アプライアンスでは、カプセル化されたリモートミラーリングまたはリモートミラーリングを使用して、ミラーリングされた仮想マシントラフィックを異なる ESXi ホストから監視できます。Deep Discovery Inspector と仮想分散スイッチの設定方法については、次の項目を参照してください。

- 154 ページの「仮想アプライアンス - カプセル化されたリモートミラーリングによりミラーリングされた仮想マシントラフィックの監視の設定」
- 159 ページの「仮想アプライアンス - リモートミラーリングによりミラーリングされた仮想マシントラフィックの監視の設定」

### 仮想アプライアンス - カプセル化されたリモートミラーリングによりミラーリングされた仮想マシントラフィックの監視の設定

カプセル化されたリモートミラーリングにより複数のネットワークインタフェースまたは VLAN のトラフィックを監視して、対象トラフィックを 1 つ以上のミラーリング先に送信できます。

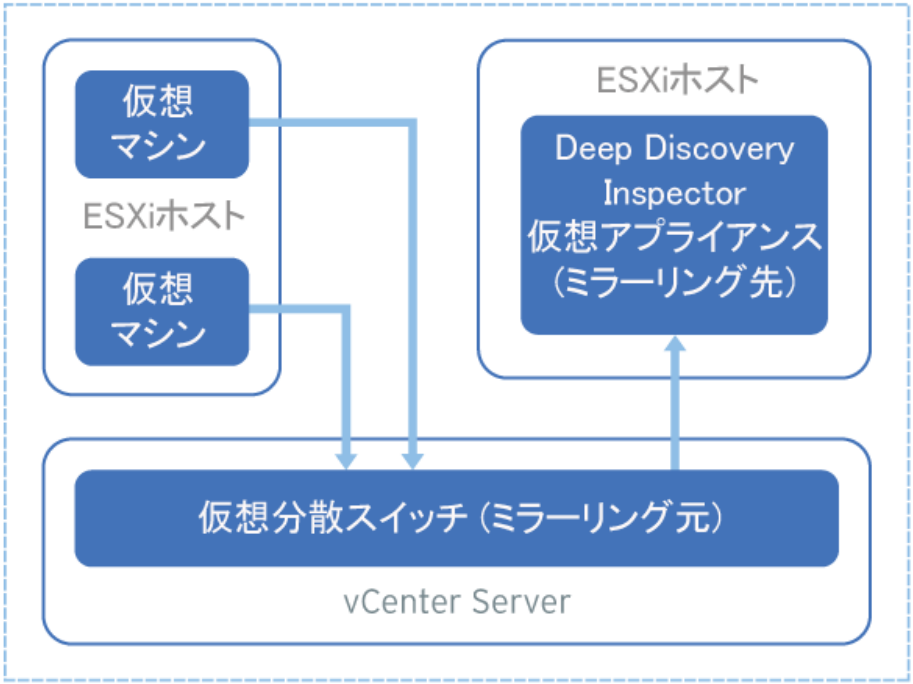



図 9-3. カプセル化されたリモートミラーリングによりミラーリングされた仮想マシントラフィックの監視

仮想スイッチのカプセル化されたリモートミラーリングでは、初期設定で、ESXi ホストの管理 VMkernel ポートがカプセル化の送信元 IP アドレスとして使用されます。

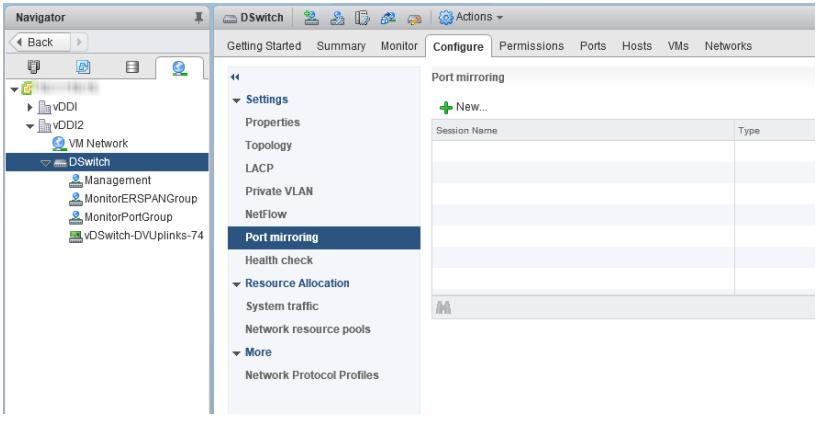
以下の手順におけるミラーリング元とミラーリング先は次のようになります。

- ミラーリング元: ミラーリングされたトラフィックを転送する仮想分散スイッチ
- ミラーリング先: Deep Discovery Inspector

**手順**

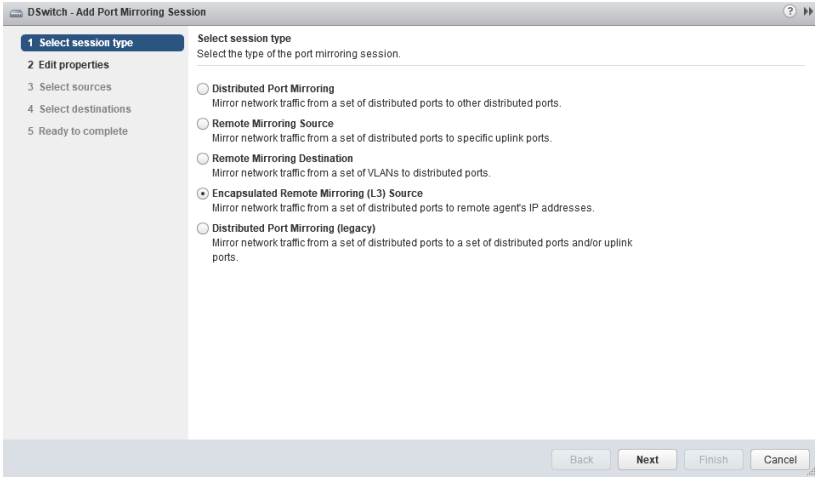
1. カプセル化され、リモートミラーリングされたトラフィックを転送するようにミラーリング元を設定します。
   a. vSphere Web Client にログインします。
   b. 左側のペインで仮想分散スイッチを選択し、[Configure] をクリックします。
   c. [Port Mirroring] をクリックします。

      [Port mirroring] 画面が表示されます。




   d. [New...] をクリックします。

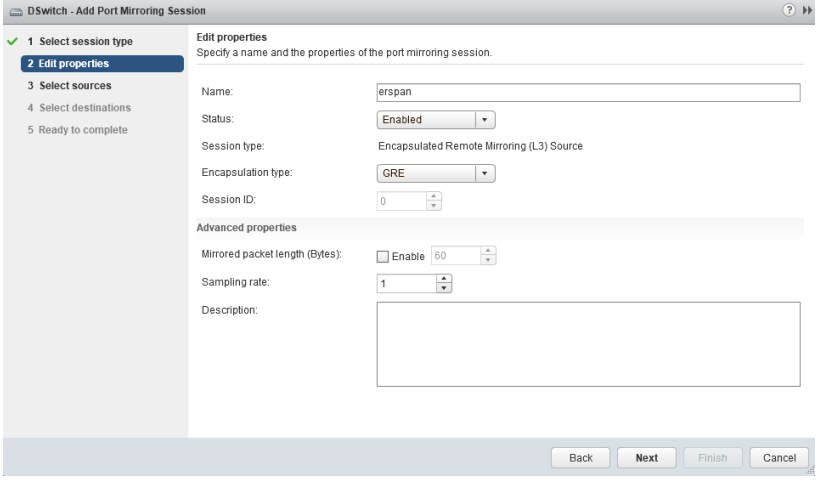
      [Add Port Mirroring Sessions] 画面が表示されます。




e. [Encapsulated Remote Mirroring (L3) Source] を選択します。

f. [Next] をクリックします。

[Edit properties] 画面が表示されます。




g. [Name] にセッション名を入力します。

h. [Status] で [Enabled] を選択します。

i. [Encapsulation type] でカプセル化の種類を選択します。

---

**注意**

[ERSPAN THREE] を使用すると問題が発生する場合があります。トレンドマイクロでは、[GRE] または [ERSPAN TWO] を使用することをお勧めします

---

j. [Next] をクリックします。

[Select sources] 画面が表示されます。

k. プラス記号のアイコン
(

) をクリックして、監視するミラーリング元の仮想マシンを追加します。

l. [Next] をクリックします。

[Select destinations] 画面が表示されます。

m. プラス記号のアイコンをクリックして、ミラーリング先の IP アドレスを追加します。

---

**注意**

ミラーリング先の IP アドレスは、次の手順の Deep Discovery Inspector で設定するアドレスです。

---

n. [Next] をクリックします。

[Ready to complete] 画面が表示されます。

o. 設定が正しいことを確認して、[Finish] をクリックします。

2. カプセル化され、リモートミラーリングされたトラフィックを受信するようにミラーリング先を設定します。

a. Deep Discovery Inspector 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。

[ネットワークインタフェース ] 画面が表示されます。

b. データポートを見つけ、行の先頭にある右向き矢印
(

) をクリックします。

c. [カプセル化されたリモートミラーリング] を選択します。

d. カプセル化されたリモートミラーリングのミラーリング先アドレスを指定します。

**重要**

カプセル化されたリモートミラーリングのミラーリング先アドレスは、ESXi ホストの管理 VMkernel ポートからルーティング可能である必要があります。

e. [保存] をクリックします。

### 仮想アプライアンス - リモートミラーリングによりミラーリングされた仮想マシントラフィックの監視の設定

リモートミラーリングにより、あるスイッチ上のトラフィックを別のスイッチのデバイスから監視して、対象トラフィックを 1 つ以上のミラーリング先に送信できます。

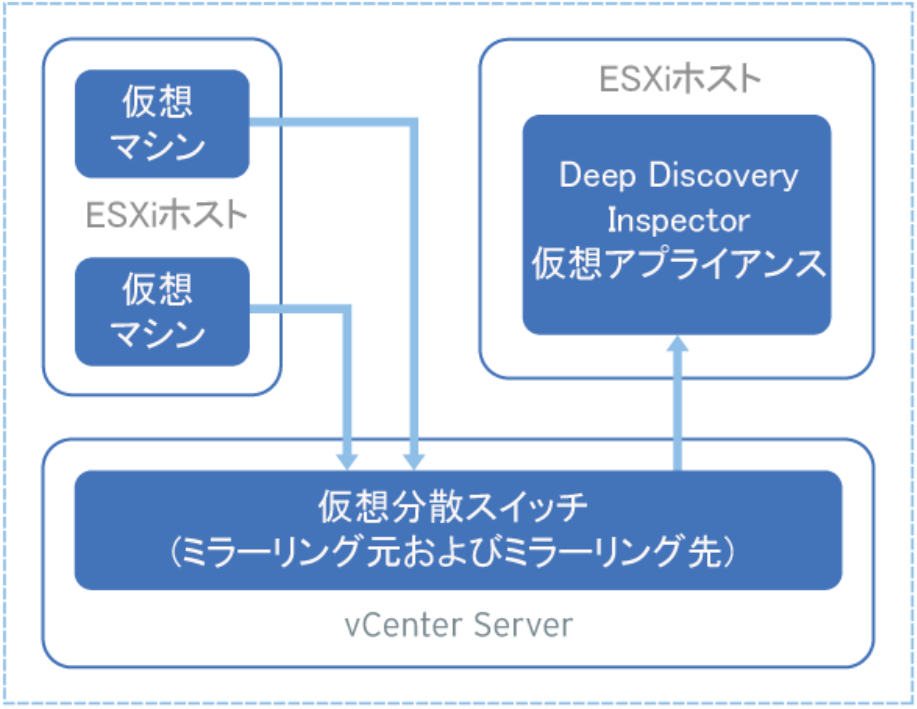



図 9-4. リモートミラーリングによりミラーリングされた仮想マシントラフィックの監視

リモートミラーリングでは、リモートミラーリング VLAN を物理スイッチ上に設定する必要があります。リモートミラーリング VLAN を設定できない場合は、代わりにカプセル化されたリモートミラーリングを使用することを検討してください。

以下の手順におけるミラーリング元とミラーリング先は次のようになります。

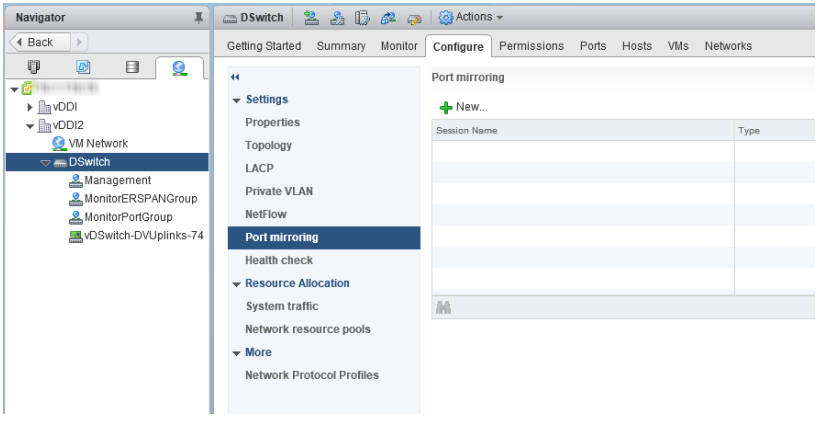
- ミラーリング元: ミラーリングされたトラフィックを転送する仮想分散スイッチ
- ミラーリング先: ミラーリングされたトラフィックを受信して Deep Discovery Inspector にルーティングできる仮想分散スイッチ

開始する前に、トラフィックを受信する ESXi ホストのアップリンクポートが物理スイッチのトランクポートにリンクしていることを確認します。

**手順**

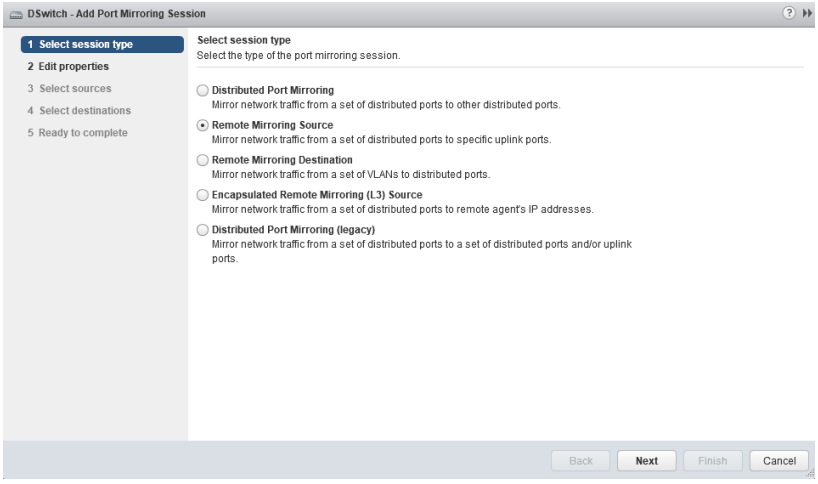
1. リモートミラーリングされたトラフィックをミラーリング先に転送するようにミラーリング元を設定します。
   a. vSphere Web Client にログインします。
   b. 左側のペインで仮想分散スイッチを選択し、[Configure] をクリックします。
   c. [Port Mirroring] をクリックします。

      [Port mirroring] 画面が表示されます。




   d. [New...] をクリックします。

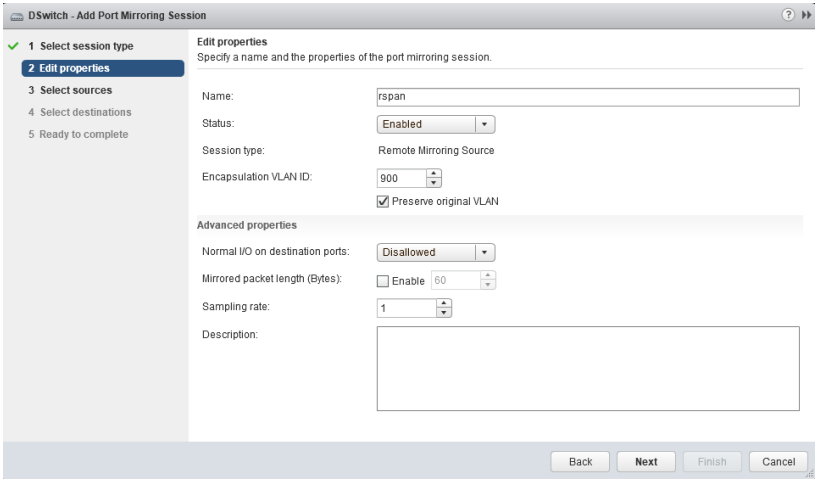
      [Add Port Mirroring Sessions] 画面が表示されます。




e. [Remote Mirroring Source] を選択します。

f. [Next] をクリックします。

[Edit properties] 画面が表示されます。




g. [Name] にセッション名を入力します。

h. [Status] で [Enabled] を選択します。

i. [Encapsulation VLAN ID] で VLAN ID を指定します。

> **注意**
> これは VDS で設定したリモートミラーリング VLAN ID です。

j. [Next] をクリックします。

[Select sources] 画面が表示されます。

k. プラス記号のアイコン
(

) をクリックして、監視するミラーリング元の仮想マシンを追加します。

l. [Next] をクリックします。

[Select destinations] 画面が表示されます。

m. [Available uplinks] のアップリンクを [Selected uplinks] に追加します。

n. [Next] をクリックします。

[Ready to complete] 画面が表示されます。

o. 設定が正しいことを確認して、[Finish] をクリックします。

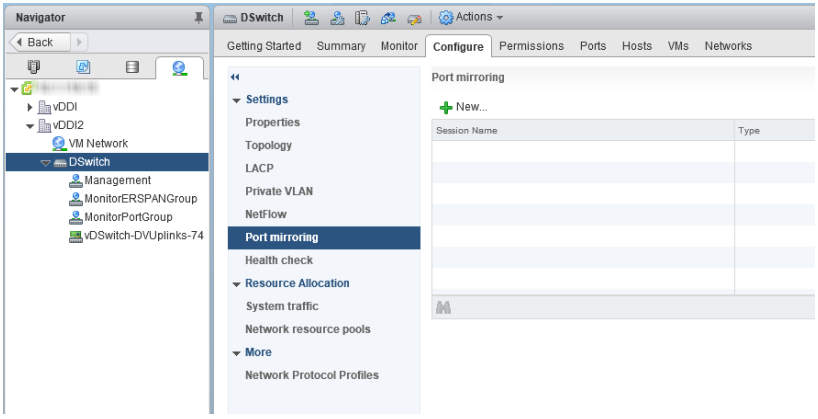
2. ミラーリングされたトラフィックを受信するようにミラーリング先を設定します。

a. vSphere Web Client にログインします。

b. 左側のペインで仮想分散スイッチを選択し、[Configure] をクリックします。

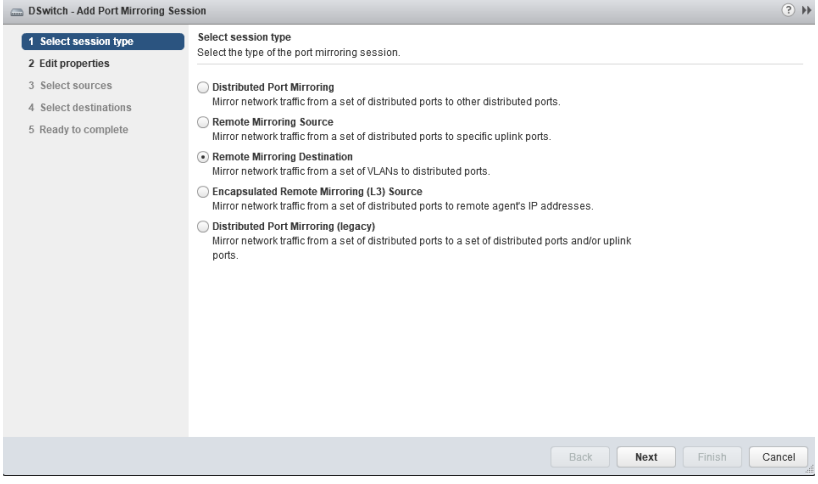
c. [Port Mirroring] をクリックします。

[Port mirroring] 画面が表示されます。




d. [New...] をクリックします。

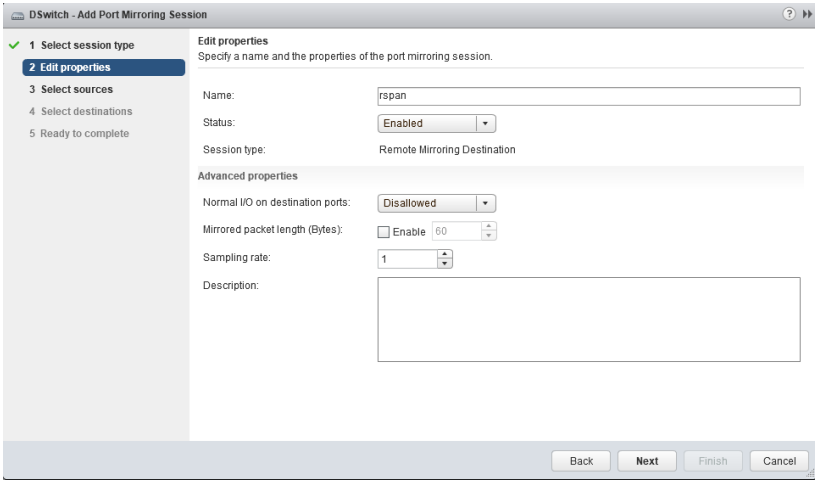
[Add Port Mirroring Sessions] 画面が表示されます。




e. [リモート ミラーリング ターゲット] を選択します。

f. [Next] をクリックします。

[Edit properties] 画面が表示されます。




g. [Name] にセッション名を入力します。

h. [Status] で [Enabled] を選択します。

i. [Next] をクリックします。

[Select sources] 画面が表示されます。

j. プラス記号のアイコンをクリックして、監視する VLAN ID を追加します。

---

**注意**

これは VDS で設定したリモートミラーリング VLAN ID です。

---

k. [Next] をクリックします。

[Select destinations] 画面が表示されます。

l. プラス記号のアイコン
(

) をクリックして、Deep Discovery Inspector データポートのポート ID を追加します。

m. [Next] をクリックします。

[Ready to complete] 画面が表示されます。

n. 設定が正しいことを確認して、[Finish] をクリックします。

## 仮想アプライアンス - ミラーリングされたトラフィックの同じ ESXi ホストからの監視

Deep Discovery Inspector 仮想アプライアンスでは、ミラーリングされた仮想マシントラフィックを同じ ESXi ホストから監視できます。仮想分散スイッチの設定方法については、次の項目を参照してください。

- 166 ページの「仮想アプライアンス - VDS での分散ポートミラーリングの設定」

### 仮想アプライアンス - VDS での分散ポートミラーリングの設定

仮想分散スイッチの分散ポートミラーリングにより、分散ポートのセットから別の分散ポートに送信されるトラフィックを監視できます。

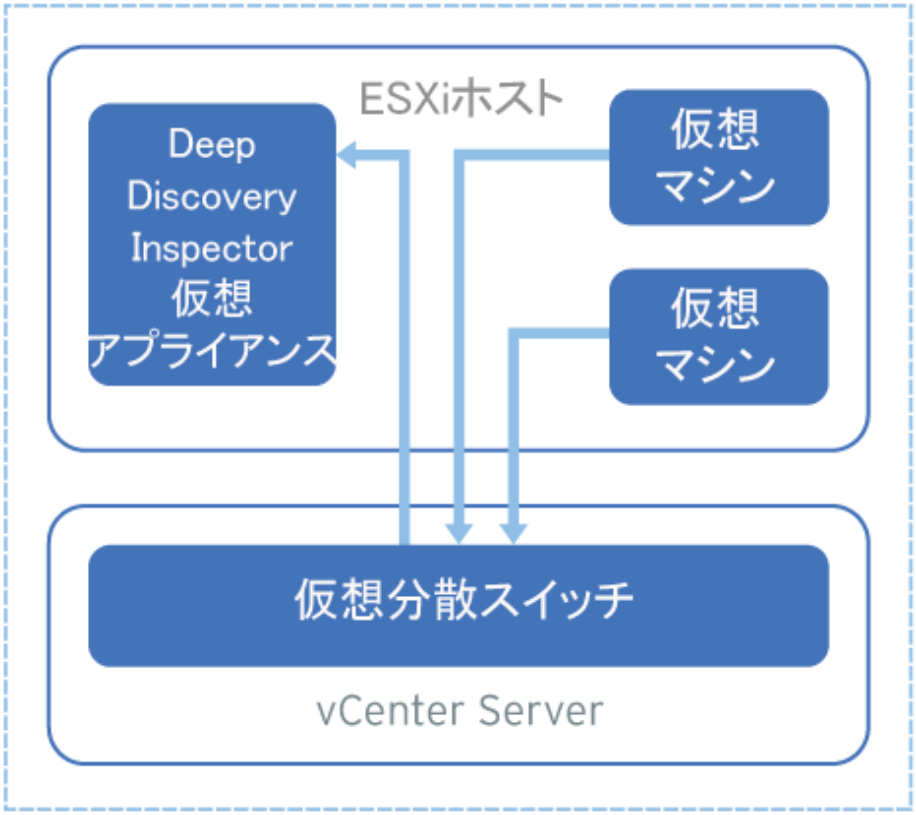


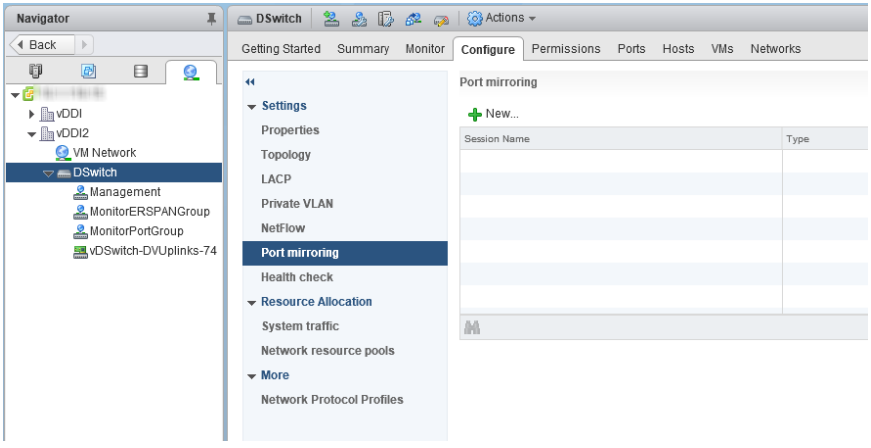

図 9-5. VDS での分散ポートミラーリング

ミラーリング元の仮想マシンとミラーリング先の Deep Discovery Inspector は、同じ ESXi ホスト上にある必要があります。異なる ESXi ホスト上にある場合は、代わりにリモートミラーリングまたはカプセル化されたリモートミラーリングを使用することを検討してください。

**手順**

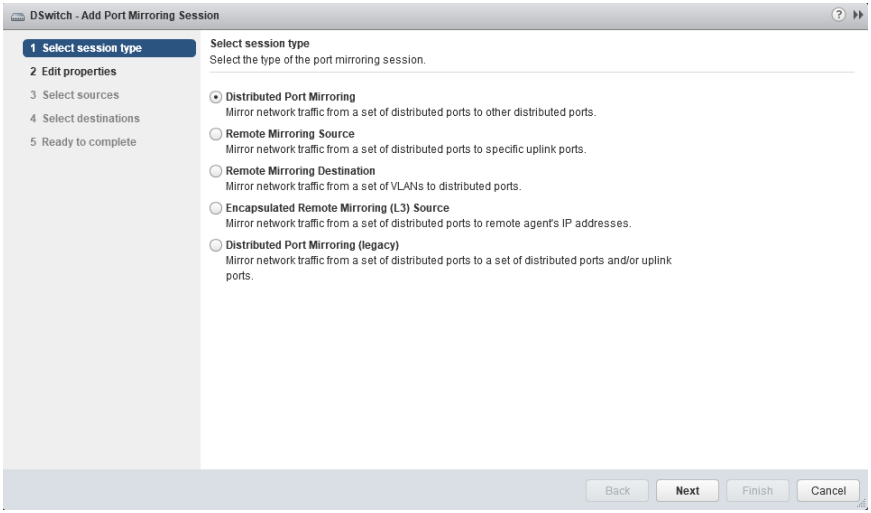
1. vSphere Web Client にログインします。
2. 左側のペインで仮想分散スイッチを選択し、[Configure] をクリックします。
3. [Port Mirroring] をクリックします。

   [Port mirroring] 画面が表示されます。



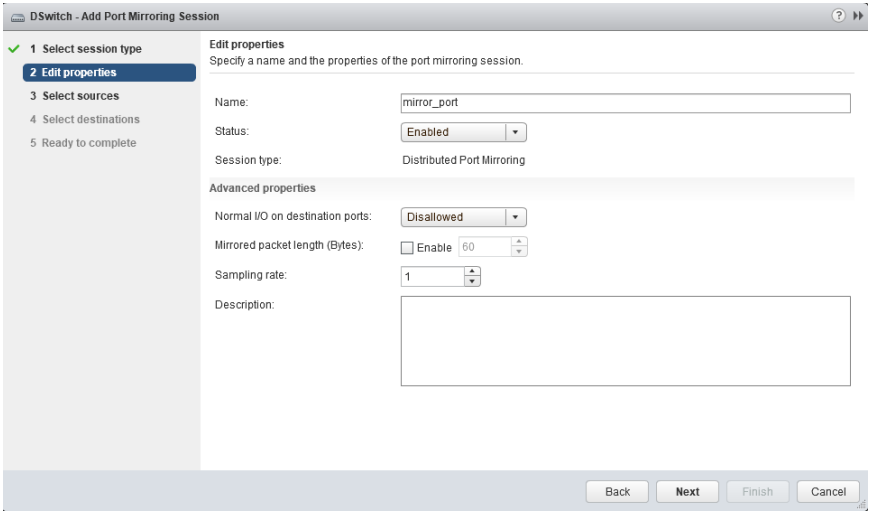

4. [New...] をクリックします。

   [Add Port Mirroring Sessions] 画面が表示されます。




5. [Distributed Port Mirroring] を選択します。
6. [Next] をクリックします。

   [Edit properties] 画面が表示されます。



7. [Name] にセッション名を入力します。
8. [Status] で [Enabled] を選択します。
9. [Next] をクリックします。

   [Select sources] 画面が表示されます。
10. プラス記号のアイコン
    (
    
    ) をクリックして、監視するミラーリング元の仮想マシンを追加します。
11. [Next] をクリックします。

    [Select destinations] 画面が表示されます。
12. プラス記号のアイコン
    (
    
    ) をクリックして、Deep Discovery Inspector データポートのポート ID を追加します。
13. [Next] をクリックします。

    [Ready to complete] 画面が表示されます。
14. 設定が正しいことを確認して、[Finish] をクリックします。

# パート IV

## インストール後

# 第 10 章

# 事前設定

事前設定コンソールを使用して Deep Discovery Inspector の初期設定を実行する方法については、次の項目を参照してください。


- 174 ページの「事前設定コンソールへのアクセス」
- 176 ページの「事前設定コンソールのメインメニュー」

# 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。

事前設定コンソールでは、管理コンソールが使用できない場合の回復操作もサポートされます。

事前設定コンソールを使用すると、次の操作を実行できます。

- 製品の IP アドレスやホスト名の初期設定
- 診断テストの実行
- 設定確認のためのネットワークの Ping
- アプライアンスの再起動
- デバイスの情報とステータスの表示
- 管理者パスワードの変更
- 手動のトラフィックバイパスの設定

**注意**

トラフィックバイパスは、サポートされているハードウェアモデルでのみ設定できます。

**注意**

HyperTerminal を使用してデータを入力するには、キーボードのスクロールロック機能を無効にします。

## 事前設定コンソールへのアクセス

Deep Discovery Inspector の事前設定コンソールには、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からアクセスできます。

事前設定コンソールにアクセスするには、次の手順を実行します。

- 175 ページの「VGA ポートを使用した事前設定コンソールへのアクセス」

ヒント

事前設定コンソールには、VGA ポートを備えたモニタを使用してアクセスすることをお勧めします。

- 175 ページの「シリアルポートを使用した事前設定コンソールへのアクセス」

## VGA ポートを使用した事前設定コンソールへのアクセス

**手順**

1. VGA ケーブルを使用して、モニタの VGA ポートをアプライアンスの VGA ポートに接続します。
2. 事前設定コンソールの画面が表示されたら、初期設定のパスワード (`admin`) を入力して、<Enter> キーを 2 回押します。

注意

HyperTerminal を使用してデータを入力するには、キーボードのスクロールロック機能を無効にします。

## シリアルポートを使用した事前設定コンソールへのアクセス

**手順**

1. RS232 シリアルケーブルを使用して、Deep Discovery Inspector アプライアンスのシリアルポートをコンピュータのシリアルポートに接続します。
2. コンピュータで、HyperTerminal などのシリアル通信アプリケーションを開きます。
3. はじめて事前設定コンソールにアクセスする場合は、次の値を入力します。
   - ビット/秒: `115200`

- データビット: 8
- パリティ: なし
- ストップビット: 1
- フロー制御: なし

注意

HyperTerminal を使用してデータを入力するには、キーボードのスクロールロック機能を無効にします。

4. 事前設定コンソールの画面が表示されたら、初期設定のパスワード (admin) を入力して、<Enter> キーを 2 回押します。

# 事前設定コンソールのメインメニュー

事前設定コンソールのメインメニューには、次のメニュー項目が表示されます。

表 10-1. メインメニューの項目

| 項目 | 説明 |
|---|---|
| 1) Device Information and Status | Deep Discovery Inspector に関する情報を表示し、メモリ使用率を監視します。 |
| 2) Device Settings | Deep Discovery Inspector の IP アドレス、サブネットマスク、ネットワークの初期設定のゲートウェイアドレス、および DNS サーバを変更します。 |
| 3) Interface Settings | Deep Discovery Inspector により自動的に検出された、管理ポートのネットワーク速度と二重化モードを表示します。 |

| 項目 | 説明 |
|---|---|
| 4) System Tasks | 次の設定を行います。<br>• 診断テストの実行<br>• 同じサブネット内のサーバに対する Ping の実行<br>• SSH 接続の設定<br>• システムの再起動<br>• 手動のトラフィックバイパスの設定<br><br>注意<br>トラフィックバイパスは、サポートされているハードウェアモデルでのみ設定できます。 |
| 5) Change Password | 管理者パスワードを変更します。 |
| 6) Log Off with Saving | 変更を保存した後、事前設定コンソールからログオフします。 |
| 7) Log Off without Saving | 変更を保存せずに、事前設定コンソールからログオフします。 |

メニュー項目にアクセスするには、メニュー項目の番号を入力して、<Enter> キーを押します。

## アプライアンス情報とステータスの表示

製品名、バージョン、およびメモリ使用率を表示するには、[Device Information & Status] 画面を使用します。

注意

Deep Discovery Inspector の管理コンソールで、メモリの使用率を表示します。[ダッシュボード] > [システムステータス] の順に選択します。

詳細については、「Deep Discovery Inspector 管理者ガイド」の「システムステータス」を参照してください。

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. 「1」と入力して [Device Information & Status] を選択し、<Enter> キーを押します。

   注意

   HyperTerminal を使用してデータを入力するには、キーボードのスクロールロック機能を無効にします。

   [Device Information and Status] 画面が表示されます。

3. <Enter> キーを押して、[Main Menu] に戻ります。

## デバイス設定の変更

[Device Settings] 画面を使用して、管理 IP アドレスを設定します。

注意

これらのタスクは管理コンソールでも実行できます。

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. [Device Settings] を選択するには、「2」と入力して <Enter> キーを押します。

   注意

   HyperTerminal などのシリアル通信アプリケーションを使用してデータを入力するには、キーボードのスクロールロック機能を無効にします。

[Device Settings] 画面が表示されます。

3. スペースキーを使用して、[Type] で次のいずれかのプロパティを選択します。
   - dynamic
   - static
4. 次の IPv4 アドレス設定を行います。
   a. [IP address] フィールドに IPv4 アドレスを入力します。

      [Subnet mask] にサブネットマスクを入力します。

   b. [Gateway] にゲートウェイ IP アドレスを入力します。

   c. [Primary] および [Secondary DNS server] にそれぞれ IP アドレスを入力します。
5. (オプション) 次の IPv6 アドレス設定を行います。
   a. [Enable] フィールドで [yes] を選択します。

   b. [IP address] フィールドに IPv6 アドレスを入力します。

      [Subnet prefix] にサブネットのプレフィックスを 入力します。

   c. [Gateway] にゲートウェイ IP アドレスを入力します。

   d. [DNS server] に DNS サーバの IP アドレスを入力します。
6. (オプション) VLAN ID を入力します。

**注意**

VLAN ID は、Deep Discovery Inspector の管理ポートとスイッチの間でトランク接続が必要な場合に使用されます。VLAN ID は、802.1Q Ethernet フレームで VLAN タグとして使用されます。

7. [Return to main menu] に移動して、<Enter> キーを押します。
8. 設定を保存するには、「6」と入力して <Enter> キーを押します。

# インタフェース設定の変更

初期設定では、Deep Discovery Inspector は管理ポートのネットワーク速度と二重化モードを自動的に検出します。これらは手動で設定することもできます。

ヒント

スループットを最大化するには、全二重モードをお勧めします。半二重も許容されますが、ネットワークスループットが伝送の遅延により制限されます。

注意

ネットワークインタフェースの 設定は管理コンソールで確認できます。[管理] > [システム設定] > [ネットワークインタフェース ] の順に選択します。詳細については、「Deep Discovery Inspector 管理者ガイド」の「ネットワークインタフェース」を参照してください。

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. 「3」と入力して [Interface Settings] を選択し、<Enter> キーを押します。

   注意

   HyperTerminal を使用してデータを入力するには、キーボードのスクロールロック機能を無効にします。

   [Interface Settings] 画面が表示されます。

3. インタフェース 設定を変更するには、次のタスクを実行します。

   a. 「1」と入力して、<Enter> キーを押します。

   b. [Speed] および [Duplex] で、スペースキーを使用してネットワーク速度と二重化モードを変更します。

c. [Return to upper menu] に移動して、<Enter> キーを押します。

4. 「2」と入力して <Enter> キーを押し、メインメニューに戻ります。
5. 「6」と入力して <Enter> キーを押し、設定を保存します。

# 第 11 章

# システムタスク

事前設定コンソールでステムタスクを実行する方法については、次の項目を参照してください。


- 184 ページの「診断テストの実行」
- 185 ページの「Ping テストの実行」
- 186 ページの「Deep Discovery Inspector の再起動」
- 187 ページの「管理者パスワードの変更」
- 188 ページの「手動のトラフィックバイパスの 設定」
- 187 ページの「ログオフ」

# システムタスクの概要

[System Tasks] 画面を使用して、次のシステムタスクを実行できます。

- 診断テスト
- システムの再起動
- Ping テスト
- SSH 接続
- トラフィックバイパス

注意

トラフィックバイパスは、サポートされているハードウェアモデルでのみ表示されます。

## 診断テストの実行

Deep Discovery Inspector で診断テストを実行し、ハードウェアおよびソフトウェアのステータスとイベントのログを取得して表示します。

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. 「4」と入力して、<Enter> キーを押します。

   [System Tasks] 画面が表示されます。

3. 「1」と入力して、<Enter> キーを押します。

   [Diagnostic Test] 画面が表示されます。

4. ハイパーターミナルコンソールで、[Transfer] > [Capture Text] の順に選択します。

注意

この手順では、例としてハイパーターミナルを使用します。その他のシリアル通信アプリケーションも使用できますが、手順は異なる場合があります。

5. フォルダを参照し、ログのファイル名を指定します。

注意

この手順では、例としてハイパーターミナルを使用します。その他のシリアル通信アプリケーションも使用できますが、手順は異なる場合があります。

6. [Start] をクリックします。

注意

この手順では、例としてハイパーターミナルを使用します。その他のシリアル通信アプリケーションも使用できますが、手順は異なる場合があります。

7. `[Run diagnostic test now?]` の下で、[OK] に移動し、<Enter> キーを押します。

   診断テストの実行中、コンソールにログエントリが表示されます。

   診断テストが終了したら、ログ概要レポートが生成され、Deep Discovery Inspector が自動的に再起動します。

8. Deep Discovery Inspector が再起動したら、ログ概要レポートを開いて結果を表示します。

## Ping テストの実行

Ping テストを実行して、ネットワークの設定を確認します。

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. 「4」と入力して、<Enter> キーを押します。

   [System Tasks] 画面が表示されます。

3. 「3」と入力して、<Enter> キーを押します。

   [Ping Test] 画面が表示されます。

4. サーバ IP アドレスを入力して、[Ping] を押します。

   Ping テストの結果が画面に表示されます。

5. <Esc> キーを押して、[Main Menu] に戻ります。

## Deep Discovery Inspector の再起動

Deep Discovery Inspector を再起動するには、ハイパーターミナルなどのシリアル接続アプリケーションを使用して事前設定コンソールにアクセスします。Deep Discovery Inspector を使用して事前設定コンソールにアクセスすると、アプライアンスをリモートで 再起動できます。

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。

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. 「4」と入力して、<Enter> キーを押します。

   [System Tasks] 画面が表示されます。

3. 「2」と入力して、<Enter> キーを押します。

[Restart System] 画面が表示されます。

4. [Restart System] 画面で [OK] に移動して、<Enter> キーを押します。

## 管理者パスワードの変更

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. 「5」と入力して、<Enter> キーを押します。

   [Change Password] 画面が表示されます。

3. 現在のパスワードと新しいパスワードを入力します。
4. 新しいパスワードを確認入力します。
5. [Return to main menu] に移動し、<Enter> キーを押してメインメニューに戻り、設定を保存します。

## ログオフ

変更を保存して、または保存せずに、事前設定コンソールからログオフします。

**手順**

1. 設定を変更したら、メインメニューに戻ります。
2. 次のいずれかのログオフオプションを選択します。
   - 変更を保存するには、「6」と入力して <Enter> キーを押します。
   - 変更を保存せずに終了するには、「7」と入力して <Enter> キーを押します。
3. [OK] に移動して <Enter> キーを押します。

# 手動のトラフィックバイパスの設定

**手順**

1. 事前設定コンソールにログオンします。

   [Main Menu] が表示されます。

2. 「4」と入力して、<Enter> キーを押します。

   [System Tasks] 画面が表示されます。

3. 「5」と入力して、<Enter> キーを押します。

   [Manual Traffic Bypass] 画面が表示されます。

4. [Disabled] または [Enabled] を選択します。

5. <Esc> キーを押して、[Main Menu] に戻ります。

# 第 12 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。


- 190 ページの「よくある質問 (FAQ)」
- 193 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。


- 190 ページの「FAQ - アプライアンスの復元」
- 191 ページの「FAQ - 設定」
- 191 ページの「FAQ - 検出」
- 191 ページの「FAQ - 設置」
- 192 ページの「FAQ - アップグレード」
- 192 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 6.7 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。


- 193 ページの「管理コンソールの応答が遅くなります」
- 194 ページの「検出」
- 196 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」
- 196 ページの「仮想アナライザ」
- 198 ページの「仮想アナライザのイメージ」
- 199 ページの「ネットワークサービスに接続できない」
- 200 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 12-1. 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。<br>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


- 194 ページの「[すべての検出] 画面に検出が表示されません」
- 195 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」
- 195 ページの「不明な IP アドレスが画面に表示されます」
- 196 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


- 196 ページの「OVA をアップロードできません」
- 197 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


- 198 ページの「インストール CD/DVD が起動しません」
- 198 ページの「[Found New Hardware] ウィザード」
- 199 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 CD/DVD 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


- 201 ページの「ネットワーク接続の問題」
- 203 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。

# パート V

# 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。


- 207 ページのトラブルシューティングのリソース
- 209 ページの製品サポート情報
- 211 ページのトレンドマイクロへのウイルス解析依頼
- 213 ページのその他のリソース

# 第 13 章

# 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

# 第 14 章

# 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。

# 第 15 章

# 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

# 第 16 章

# 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 A

# アプライアンスで使用されるポート

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

表 A-1. ポート 22

| | |
|---|---|
| ポート | 22 |
| プロトコル | TCP |
| 機能 | インバウンド |
| 目的 | 次のことを実行します。<br>• 事前設定コンソールに接続します。<br>• SSH 経由で Deep Discovery Inspector が登録されると、Threat Management Services Portal にログとデータが送信されます。 |

表 A-2. ポート 25

| | |
|---|---|
| ポート | 25 |
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | SMTP にて通知と予約レポートを送信します。 |

表 A-3. ポート 53

| | |
|---|---|
| ポート | 53 |

| | |
|---|---|
| プロトコル | TCP/UDP |
| 機能 | アウトバウンド |
| 目的 | このポートは DNS による名前解決用に使用されます。 |

表 A-4. ポート 67

| | |
|---|---|
| ポート | 67 |
| プロトコル | UDP |
| 機能 | アウトバウンド |
| 目的 | IP アドレスが動的に割り当てられている場合、DHCP サーバに要求を送信します。 |

表 A-5. ポート 68

| | |
|---|---|
| ポート | 68 |
| プロトコル | UDP |
| 機能 | インバウンド |
| 目的 | DHCP サーバから応答を受信します。 |

表 A-6. ポート 80

| | |
|---|---|
| ポート | 80 |
| プロトコル | TCP |
| 機能 | インバウンド |
| 目的 | 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。<br>• 脅威インテリジェンス情報を他の製品と共有します。 |
| 機能 | アウトバウンド |

| | |
|---|---|
| 目的 | 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。<br>• Deep Discovery 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。<br>• 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。 |

表 A-7. ポート 123

| | |
|---|---|
| ポート | 123 |
| プロトコル | UDP |
| 機能 | アウトバウンド |
| 目的 | このポートを使用して NTP サーバに接続し、時間を同期します。 |

表 A-8. ポート 137

| | |
|---|---|
| ポート | 137 |
| プロトコル | UDP |
| 機能 | アウトバウンド |
| 目的 | NetBIOS を使用して IP アドレスをホスト名に解決します。 |

表 A-9. ポート 161

| | |
|---|---|
| ポート | 161 |
| プロトコル | UDP |
| 機能 | インバウンド |
| 目的 | このポートを SNMP エージェントの待機およびプロトコル変換に使用します。 |

表 A-10. ポート 162

| | |
|---|---|
| ポート | 162 |
| プロトコル | UDP |
| 機能 | アウトバウンド |

| | |
|---|---|
| 目的 | このポートを使用して SNMP トラップ通知を送信します。 |

表 A-11. ポート 389

| | |
|---|---|
| ポート | 389 |
| プロトコル | TPC/UDP |
| 機能 | アウトバウンド |
| 目的 | このポートを使用して LDAP サーバからユーザ情報を取得します。<br><br>注意<br>これは初期設定のポートです。管理コンソールで設定します。 |

表 A-12. ポート 443

| | |
|---|---|
| ポート | 443 |
| プロトコル | TCP |
| 機能 | インバウンド |
| 目的 | 次のことを実行します。<br>• 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。 |
| 機能 | アウトバウンド |

| | |
|---|---|
| 目的 | 次のことを実行します。<br>• オンプレミスバージョンの Deep Discovery Director と通信します。<br>  <br>注意<br>これは初期設定のポートです。管理コンソールで設定します。<br>• Trend Micro Apex Central と通信します。<br>  <br>注意<br>これは初期設定のポートです。管理コンソールで設定します。<br>• Trend Micro Service Gateway と通信します。<br>• Trend Vision One と通信します。<br>• MITRE ATT&CK™の Tactics と Techniques に関する Web サイトに接続します。<br>• Trend Micro Threat Connect に接続します。<br>• Smart Protection Server を使用して Mobile App Reputation Service に対してクエリを実行します。<br>• 機械学習型検索エンジンに対してクエリを実行します。<br>• Web レピュテーションサービスによるブロックの理由をクエリします。<br>• Mitigation Server に登録します。<br>• APK ファイルを検索し、検出情報を Mobile App Reputation Service に送信します。<br>• サンドボックス分析対象ファイルを Deep Discovery Analyzer に送信します。<br>  <br>注意<br>これは初期設定のポートです。管理コンソールで設定します。<br>• SSL 暗号化を使用する場合、Threat Management Services Portal にログとデータを送信します。<br>• Trend Micro Smart Protection Network と匿名の脅威情報を共有します。 |

| | |
|---|---|
| | • Trend Micro TXOne OT Defense Console と脅威インテリジェンス情報を共有します。<br>• CSSS (Certified Safe Software Service) を使用してファイルの安全性を確認します。 |

表 A-13. ポート 465

| | |
|---|---|
| ポート | 465 |
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | SMTP で SSL/TLS 暗号を使用して通知と予約レポートを送信します。(SMTP over SSL) |

表 A-14. ポート 514

| | |
|---|---|
| ポート | 514 |
| プロトコル | UDP |
| 機能 | アウトバウンド |
| 目的 | UDP 経由で Syslog サーバにログを送信します。<br><br>注意<br>ポートは Syslog サーバと一致している必要があります。<br><br>注意<br>これは初期設定のポートです。管理コンソールで設定します。 |

表 A-15. ポート 587

| | |
|---|---|
| ポート | 587 |
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | SMTP で STARTTLS 暗号を使用して通知と予約レポートを送信します。(STARTTLS) |

表 A-16. ポート 601

| | |
|---|---|
| ポート | 601 |
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | このポートを使用してログを Syslog サーバに送信します。<br>  注意<br>ポートは Syslog サーバと一致している必要があります。<br>  注意<br>これは初期設定のポートです。管理コンソールで設定します。 |

表 A-17. ポート 636

| | |
|---|---|
| ポート | 636 |
| プロトコル | UDP |
| 機能 | アウトバウンド |
| 目的 | このポートを使用して LDAP サーバからユーザ情報を取得します。<br>  注意<br>これは初期設定のポートです。管理コンソールで設定します。 |

表 A-18. ポート 3268

| | |
|---|---|
| ポート | 3268 |
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | このポートを使用して LDAP サーバからユーザ情報を取得します。 |

表 A-19. ポート 3269

| | |
|---|---|
| ポート | 3269 |

| | |
|---|---|
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | このポートを使用して LDAP サーバからユーザ情報を取得します。 |

表 A-20. ポート 4343

| | |
|---|---|
| ポート | 4343 |
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | Smart Protection Server と通信します。 |

表 A-21. ポート 5275

| | |
|---|---|
| ポート | 5275 |
| プロトコル | TCP |
| 機能 | アウトバウンド |
| 目的 | • HTTPS を使用して Smart Protection Server 経由で 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。<br>• HTTPS を使用して Service Gateway の Smart Protection Server 経由で 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。 |

表 A-22. ポート 6514

| | |
|---|---|
| ポート | 6514 |
| プロトコル | TCP |
| 機能 | アウトバウンド |

| | |
|---|---|
| 目的 | TCP 経由で SSL 暗号を使用して Syslog サーバにログを送信します。<br><br>注意<br>ポートは Syslog サーバと一致している必要があります。<br><br>注意<br>これは初期設定のポートです。管理コンソールで設定します。 |

表 A-23. ポート 8514

| | |
|---|---|
| ポート | 8514 |
| プロトコル | UDP |
| 機能 | アウトバウンド |
| 目的 | Deep Discovery Inspector Deep Discovery Advisor と統合される場合、Syslog 情報を Deep Discovery Advisor に送信します。<br><br>注意<br>これは初期設定のポートです。管理コンソールで設定でき、Deep Discovery Advisor の Syslog 設定と一致している必要があります。 |

表 A-24. ポート 8080

| | |
|---|---|
| ポート | 8080 |
| プロトコル | TCP |
| 機能 | インバウンド |
| 目的 | このポートを使用して脅威インテリジェンスを他の製品と共有します。<br><br>注意<br>これは初期設定のポートです。管理コンソールで設定します。 |

# 索引