

Deep Discovery Inspectorは、APTや標的型攻撃の可視性、洞察、および制御を強化する第3世代の脅威管理ソリューションで、Deep Discovery Inspectorは、重要なセキュリティ情報、警告、およびレポート管理者に提供します。

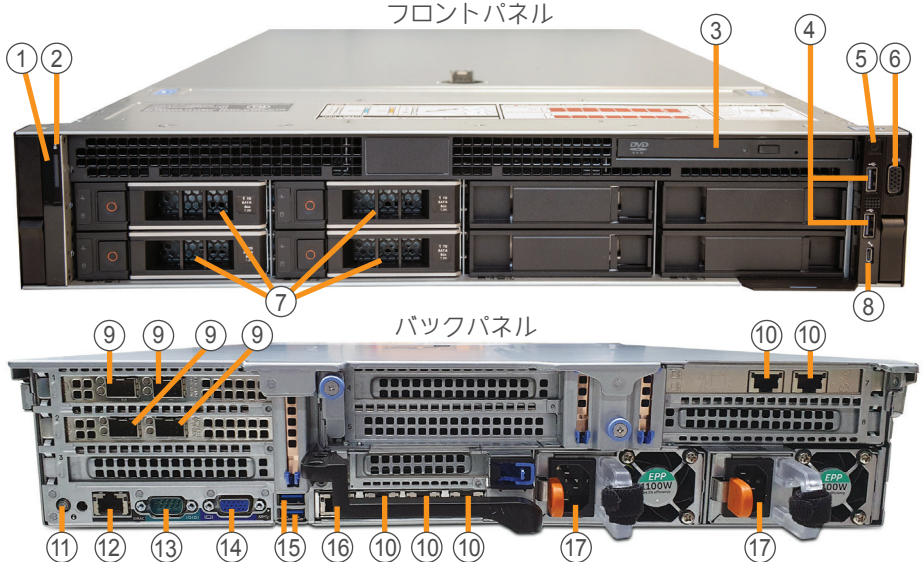
1 箱を開いて内容物を確認する

Deep Discovery Inspectorの箱に次のものが同梱されていることを確認します。



Deep Discovery Inspectorアプライアンス

2 Deep Discovery Inspectorアプライアンスを調べる



注意: データポートのレイアウトは、提供されるアプライアンスによって異なる場合があります。詳細については、次のサイトにある「インストールガイド」を参照してください。
https://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=5554®s=jp&lang_loc=13

- | | | |
|--------------------|----------------------------------|---------------------|
| (1) ステータスLEDインジケータ | (7) ハードドライブ4 | (12) iDRACポート |
| (2) 前面識別ボタンインジケータ | (8) iDRACダイレクトポート (Micro-AB USB) | (13) RS-232シリアルコネクタ |
| (3) 光学ドライブ | (9) 10Gbpsデータポート 4 | (14) 背面ビデオコネクタ |
| (4) USBコネクタ | (10) 1Gbpsデータポート 5 | (15) 背面USBコネクタ |
| (5) 電源ボタンインジケータ | (11) 背面識別ボタンインジケータ | (16) 管理ポート |
| (6) 前面ビデオコネクタ | | (17) 電源コネクタ |

注意: AC電源スロットは、いずれかが故障しても稼働できるように用意されています。

3 推奨するネットワーク環境

Deep Discovery Inspectorは帯域外に配置されます。そのためDeep Discovery Inspectorはネットワークトラフィックをブロックし、Deep Discovery Inspectorは、スイッチからミラーリングされたトラフィックを受信して、既知の脅威と潜在的な脅威を監視します。

スイッチのミラーポートを、管理ポートを除くいずれかのポートに接続します。

サンプル分析にはカスタムネットワークを使用することをお勧めします。カスタムネットワークは独自のネットワーク設定でインターネットに接続されている必要があります。アプライアンスにはカスタムネットワークにプロキシを設定するオプションがあり、プロキシ認証もサポートされます。

カスタムネットワーク内の不正なサンプルが管理ネットワーク内のホストに影響を及ぼさないよう、ネットワークは互いに独立している必要があります。

ネットワーク配置環境を計画する場合は、「インストールガイド」の「導入計画」を参照してください。

4 配置チェックリスト

要件	詳細
アクティベーションコード	トレンドマイクロより取得
モニタおよびVGAケーブル	アプライアンスのVGAポートに接続
USBキーボード	アプライアンスのUSBポートに接続
USBマウス	アプライアンスのUSBポートに接続
Ethernetケーブル	- アプライアンスの管理ポートを管理ネットワークに接続するケーブルを本 - トラフィックの監視用に、管理ポートを除くアプライアンスのいずれかのポートとスイッチのミラーポートを接続するケーブルを本以上 (オプション) 管理ポートを除くアプライアンスのいずれかのポートを、内部仮想アナライザ専用のカスタムネットワークに接続するケーブルを本
管理コンソール	- 次のWebブラウザが7つ以上インストールされているコンピュータ - Google Chrome - Microsoft Edge - Mozilla FireFox
IPアドレス	- 管理ネットワーク内の静的IPアドレスを7つ (オプション) インターネット接続のあるカスタムネットワークに接続されている場合、内部仮想アナライザ用の追加IPアドレスを7つ

5 ハードウェアを設定する

- Deep Discovery Inspectorアプライアンスを標準19インチサーバラックに設置するか、丈夫な机などの独立した器具に取り付けます。

注意: アプライアンスを設置する際は、適切な通気と冷却を確保するために、周囲10cm以上の空間を設けてください。

- アプライアンスを電源に接続します。
- モニタをアプライアンスの後ろにVGAポートに接続します。
- キーボードとマウスをアプライアンスの後ろにUSBポートに接続します。
- 管理ポートをネットワークに接続します。
- アプライアンスの電源をオンにします。

6 初期設定を実行する 事前設定コンソール

次のいずれかを使用して、事前設定コンソールから初期設定を実行します。

- VGAポート
- シリアルポート

事前設定コンソールへのアクセス方法の詳細については、「インストールガイド」の章を参照してください。

- 事前設定コンソールのログイン画面で、次の初期設定のログイン認証情報を入力します。
 - ユーザー名: admin
 - パスワード: admin

- 事前設定コンソールで「2」を入力し「[Device Settings]」を選択し「<Enter>」キーを押します。
- [Device Settings] 画面で「IPアドレス」を設定します。
動的IPアドレスを設定するにはスペースバーを使用してIPアドレスオプション[dynamic] に切り替えます。
静的IPアドレスを設定するには

- [Type] フィールドで、スペースバーを使用してIPアドレスオプションを[dynamic] から[static] に切り替えます。
- ネットワーク設定を次のように入力します。
 - IPアドレス(IPv4): 初期設定は192.168.252.1
 - サブネットマスク: 初期設定は255.255.255.0
 - (オプション) ゲートウェイ: 初期設定は192.168.252.254
 - (オプション) DNSサーバ1
 - (オプション) DNSサーバ2

注意: Deep Discovery Inspector 5.0以上はIPv6環境に導入可能です。

- (オプション) VLAN IDを入力します。
- [Return to main menu] に移動して「<Enter>」キーを押します。
初期設定が完了し、管理コンソールにアクセスできるようになります。

7 初期設定を実行する 管理コンソール

- サポートされているWebブラウザを使用して、次の場所にある管理コンソールを開きます。
<https://<Deep Discovery InspectorのIPアドレス>>

注意:

- インターネットのセキュリティレベルを4に設定します。
ActiveXのバイナリビヘイビアとスクリプトビヘイビアを有効にします。
- 初期設定で指定したIPアドレスを使用します。

- ログイン画面で、次の初期設定の認証情報を入力します。
 - ユーザー名: admin
 - パスワード: admin
- [ログイン] をクリックします。
- 新しいパスワードを入力し、確認のため、もう一度同じパスワードを入力します。
- [管理]→[システム設定]→[時間] の順に選択して、システム時刻を設定します。
- [管理]→[ライセンス] で「Deep Discovery Inspector」をアクティベートします。
セットアップガイド画面が表示されます。
- 配置後の設定を行うには、セットアップガイドの手順に従ってください。
脅威対策の設定方法の詳細は、「管理者ガイド」の「はじめに」の章を参照してください。
- スイッチのミラーポートから、管理ポートを除くアプライアンスのいずれかのポートにケーブルを本以上接続します。

8 連絡先情報

- Webサイト: <https://www.trendmicro.com/>
- 電話: 03-5334-3601(営業代表)
- 住所: 〒151-0053 東京都渋谷区代々木 2-1-1 新宿メインズタワー