

TREND MICRO™ Deep Discovery Inspector 260 クイックスタートガイド



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。

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。

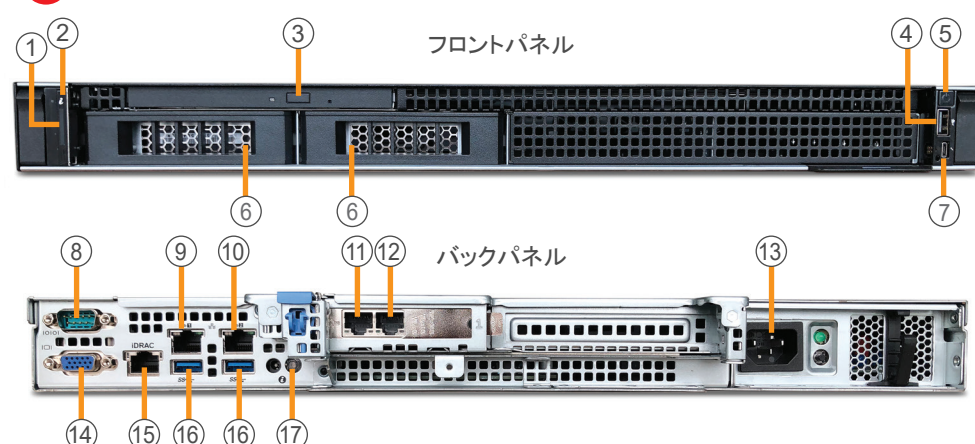
ネットワーク配置環境を計画する場合は、「インストールガイド」の「導入計画」を参照してください。

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。



2 Deep Discovery Inspectorアプライアンスを調べる



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

3 推奨するネットワーク環境

Deep Discovery Inspectorは、スイッチのミラーポートに接続するように配置されず。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ません。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。

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
モニターおよび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	<ul style="list-style-type: none"> 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1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1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1本 (オプション) アプライアンスのiDRACポートをネットワークに接続するケーブルを1本
管理コンソール	次のWebブラウザが1つ以上インストールされているコンピュータ <ul style="list-style-type: none"> Google Chrome Microsoft Edge Mozilla FireFox
IPアドレス	<ul style="list-style-type: none"> 管理ネットワーク内の静的IPアドレスを1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1つ (オプション) iDRAC用の追加IPアドレスを1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の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に5cm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。
- モニターをアプライアンスの後ろにある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ある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。
- (オプション) iDRAC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。
- (オプション) iDRACを設定します。
 - 起動メニューからiDRACコンソールに入り、iDRACの設定を行います。
 - iDRACの設定を保存して、アプライアンスを再起動します。

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「事前設定」の章を参照してください。

- 事前設定コンソールのログオン画面で、次の初期設定のログオン認証情報を入力します。
 - ユーザ名: admin
 - パスワード: admin
- 事前設定コンソールで、「2」と入力して [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を [dynamic] に切り替えます。

静的IPアドレスを設定するには:

A. [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。

B. 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 3.8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 [中] 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。

- ログオン画面で、次の初期設定の認証情報を入力します。
 - ユーザ名: admin
 - パスワード: admin
- [ログオン] 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1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

© 2021 Trend Micro Incorporated. All rights reserved. TRENDMICROは、トレンドマイクロ株式会社の登録商標です。その他の社名または製品名は、各社の商標または登録商標です。本書に含まれる内容は予告なしに変更される場合があります。

P/N:DDZZZH-AQ0203