

## Deep Discovery™ Inspector powered by Express5800

ディープ ディスカバリ インスペクター

# 標的型攻撃対策アプライアンス



標的型攻撃で利用される新型ウイルスなどを検知し、ネットワーク内の感染状況を可視化することで、機密情報漏えいなどの被害を防ぐ。

### 導入効果

#### ■ 新型ウイルスを検知（入口対策）

パターンマッチングでは検知できない新型ウイルスを、静的解析（ルールに基づいた挙動分析など）と動的解析（サンドボックスと呼ばれる仮想環境での検体解析）の多段階解析で検知します。

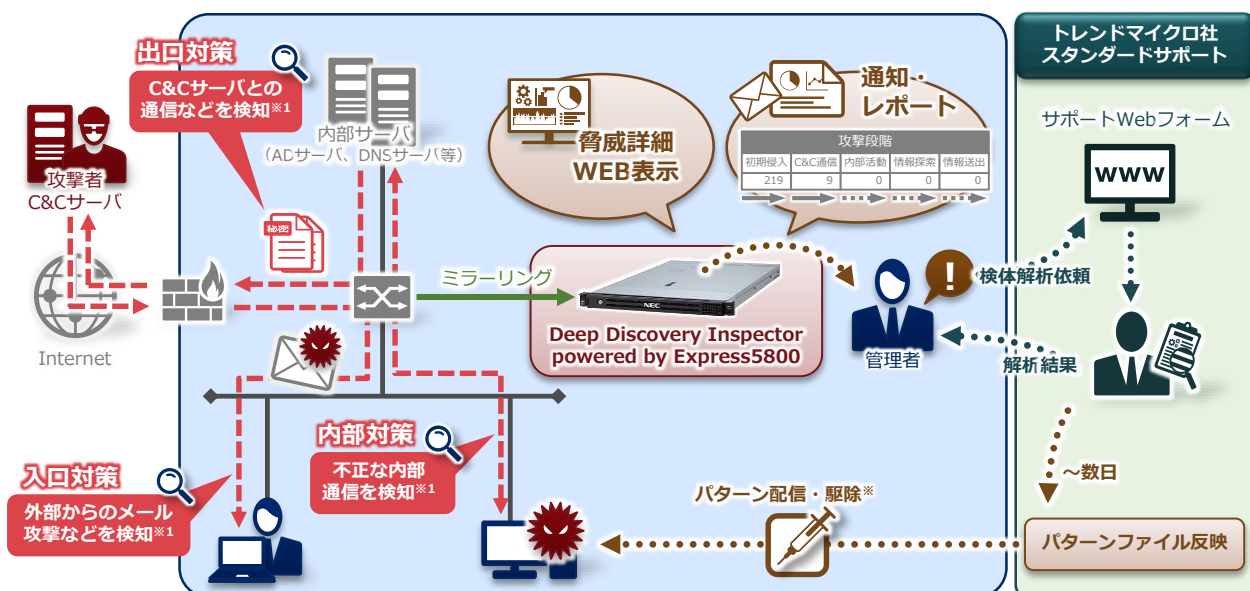
#### ■ ウイルス感染端末からの不正通信を検知・可視化（内部通信・出口対策）

ウイルスの特徴のある通信や挙動、接続先を分析することで、ウイルスに感染したクライアント端末からの外部サーバとの不正通信や内部サーバへの感染拡大などを可視化します。

#### ■ 脅威の可視化・分析レポート

検知した脅威をリアルタイムにログとして可視化し、分析結果をレポートとして自動作成します。また、エンジニアによる脅威分析などを提供します（オプション）。

### システムイメージ



※1 スイッチ機器からミラーリングされる通信内容により可視化する内容が変わります。

※2 ウイルスバスター コーポレートエディション利用時

機能一覧

■ 多段解析（静的解析・動的解析）

PDFやWordなど文書ファイルの脆弱性攻撃の検出や挙動分析、URL判定等による脅威分析（静的解析）と、不審なファイルを仮想環境上で動作を再現する動的解析（Sandbox機能）の、多段解析により脅威を検知します。

■ ネットワーク監視型アプライアンス

ミラーポートを利用したネットワーク監視により、既存システムに影響無く、未知や既知のウイルスに感染した端末を検知します。クライアントに対してエージェントの展開作業も不要です。

■ 脅威を可視化

脅威として解析された通信をフルローカライズされたWebコンソールにより、リアルタイムに可視化が可能です。また、脅威として解析された通信を相関分析し、レポートを自動的に作成することで、ウイルスに感染した端末や攻撃段階を脅威として可視化できます。

■ 復旧支援（オプション）と解析対象のチューニング

感染端末の復旧支援や、脅威の詳細分析による感染端末の洗い出しを実施する「法人向け有償サポートサービス」をオプションにてご用意しています。また、お客様にて詳細分析を実施する際にも、解析対象を絞るといったチューニングの実施が可能です。

仕様\*1

	250モデル	500モデル	1000モデル
スループット	最大250Mbps	最大500Mbps	最大1Gbps
CPU	インテル® Xeon® プロセッサー E3ファミリー x1	インテル®Xeon®プロセッサー Silver x1	インテル®Xeon®プロセッサー Silver x2
メモリ	32GB	32GB	
内蔵HDD	500GB（RAIDなし）	1TB（RAID1）	
標準ネットワークI/F	1000BASE-T LANコネクタ x 6 （含 管理ポートx 1）	1000BASE-T LANコネクタ x 8 （含 管理ポートx 1）	
外形寸法(W×D×H)	444.0mm x 615.2mm x 43.6mm（1U）	434.6mm x 749.8mm x 42.9mm（1U）	
重量（最小／最大）	10.0kg／17.5kg（レール含む）	14kg／29kg（レール含む）	
電源	400W（冗長構成なし）	800W（冗長構成）	
温度条件	動作時：5～40℃、保管時：-10～55℃	動作時：10～35℃、保管時：-30～60℃	
出荷時バージョン	Deep Discovery Inspector 5.0		

\*1 2018年6月現在の仕様となります。最新の仕様はWebをご覧ください。

製品一覧

製品名	概要
Deep Discovery Inspector 1000 powered by Express5800 V5 新規	入口・出口対策を行うためのネットワーク監視アプライアンスです。1年間のソフトウェア利用許諾ライセンスを含みます。
Deep Discovery Inspector 500 powered by Express5800 V5 新規	1000版と同機能でハードウェアスペックを抑えた <b>NEC専用モデル</b> です。1年間のソフトウェア利用許諾ライセンスを含みます。
Deep Discovery Inspector 250 powered by Express5800 V5 新規	1000版と同機能でハードウェアスペックを抑えたローエンドモデルです。1年間のソフトウェア利用許諾ライセンスを含みます。
Deep Discovery Inspector 1000 powered by Express5800 V5 更新	Deep Discovery Inspector 1000 powered by Express5800の2年目以降における1年間のソフトウェア利用許諾ライセンスです。
Deep Discovery Inspector 500 powered by Express5800 V5 更新	Deep Discovery Inspector 500 powered by Express5800の2年目以降における1年間のソフトウェア利用許諾ライセンスです。
Deep Discovery Inspector 250 powered by Express5800 V5 更新	Deep Discovery Inspector 250 powered by Express5800の2年目以降における1年間のソフトウェア利用許諾ライセンスです。

※ ソフトウェア保守（PP・サポートサービス）やハードウェア保守は別途手配となります。また、サンドボックス構築用のWindows OS、Microsoft Officeライセンスの手配も同様に別途手配となります。その他、価格やその他オプション製品などはお問い合わせください。

**NEC プラットフォームソリューション事業部 ソフトウェアお問い合わせ**

〒108-8424 東京都港区芝五丁目33番地8号 第一田町ビル

TEL: 03 (3798) 7177

【受付時間】 9:00～12:00 13:00～17:00 月曜日～金曜日（祝日・NEC所定の休日を除く）

URL: <https://jpn.nec.com/soft/trendmicro/dd/>

- 本紙に掲載された社名、商品名は各社の商標または登録商標です。
- 本製品の輸出（非居住者への役務提供等を含む）に際しては、外国為替及び外国貿易法等、関連する輸出管理法令等をご確認の上、必要な手続きをお取りください。  
ご不明な場合、または輸出許可等申請手続きにあたり資料等が必要な場合には、お買い上げの販売店またはお近くの弊社営業拠点にご相談ください。
- 本紙に掲載された製品の色は、印刷の都合上、実際のものと多少異なることがあります。また、改良のため予告なく形状、仕様を変更することがあります。