TREND MICRO™

Securing Your Connected World

Deep Discovery Email Inspector

導入向け補足ドキュメント

Version 1.1

更新履歴

Version	日付	内容
1.0	2019/12/27	初版作成
1.1	2020/07/03	SPAN/TAP モード導入時の注意を追加

本ドキュメントについて

本ドキュメントは Deep Discovery Email Inspector (以下、DDEI)を、ご利用いただく上での留意事項の情報をまとめた補足資料となります。該当製品の導入を計画されているお客様は、本ドキュメントを必ず一読ください。

各種機能の詳細または設定方法については、付属のインストールガイドおよび管理者ガイドをご参照ください。

カテゴリ	サブカテゴリ	重要度	内容	リンク・補足事項
機能・仕様	仮想アナライザ	高	**仮想アナライザのサンドボックスの FAQ リンク集** 仮想アナライザのサンドボックスに関するよくある質問については、右記の FAQ にまとめております。	https://success.trendmicro.com/jp/solution/1119475
機能・仕様	仮想アナライザ	高	**仮想アナライザがインターネットに接続できない場合の影響について** DDEI 管理画面の[管理] > [検索/分析] > [仮想アナライザ] > [設定] > [ネットワークの種類]で"ネットワークアクセスなし"とすることで、仮想アナライザをインターネットにアクセスさせないようにすることが可能です。ただし、仮想アナライザ内での不審オブジェクト解析が不十分となるため、未知の潜在的な脅威を検出する精度は低下いたします。極力、仮想アナライザがインターネットにアクセスできるよう設定することをご検討ください。	https://success.trendmicro.com/jp/solution/1115540
機能・仕様	仮想アナライザ	低	**SFTP により送付される検出情報について** DDEI では、仮想アナライザでの分析結果の情報を SFTP で SFTP サーバへ送付可能です。こちらの送付情報の概要につきましては右記の FAQ にてご紹介しております。	https://success.trendmicro.com/jp/solution/1121525
機能・仕様	ポリシー	中	**ポリシーの作成方法について** DDEI 3.0 以降から、ポリシーは複数の種類のフィルタリングルールを組み合わせて構成されるようになりました。ポリシーの概要および作成例等につきましては、右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/000154692
機能・仕様	ポリシー	中	**不正プログラムの侵入で利用されるメール添付ファイルの検出** 不審な添付ファイルをチェックするポリシーを検討される場合は、右記の FAQ も併せてご参照ください。	https://success.trendmicro.com/jp/solution/000154703

カテゴリ	サブカテゴリ	重要度	内容	リンク・補足事項
機能・仕様	ポリシー	低	**ポリシーの除外設定(メッセージ)で使用可能なメールアドレスの表記方法について** ポリシーによる検索の除外設定をメールアドレスで行う場合の記述例(ワイルドカードの使い方含め)を説明しております。	https://success.trendmicro.com/jp/solution/1123587
機能・仕様	ポリシー	低	**分割メールに対する処理について** DDEI は、分割メール(Content-Type が message/partial であるメール)に対しては検索をスキップする挙動となります。	https://success.trendmicro.com/jp/solution/000155985
機能・仕様	通知	低	**アラート通知の設定方法** DDEI のアラート通知メールの設定については、右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/1115699
機能・仕様	その他	高	**トレンドマイクロ提供のサーバと通信できなかった際の影響** 管理者ガイドの「付録 D: 接続とポート」の「サービスのアドレスとポート」の章に記載の通り、DDEI はトレンドマイクロ提供の各種サーバと適宜通信いたします。当該サーバと通信できない場合の影響につきましては、右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/1121955
機能・仕様	その他	中	**Connected Threat Defense（CTD）設定について** DDEI は、TMCM または Apex Central と連携して不審オブジェクト情報を同期することで、Connected Threat Defense ソリューションを行うことが可能です。詳細は右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/1121430

カテゴリ	サブカテゴリ	重要度	内容	リンク・補足事項
機能・仕様	その他	中	**連携可能な Smart Protection Server について** DDEI と連携可能な Smart Protection Server については、右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/1117938
機能・仕様	その他	中	**アクティベーションコードやライセンスの概要について** 管理画面からアクティベーションコードを登録することで、当該アクティベーションコードに紐づいたライセンス情報で DDEI が稼働するようになります。アクティベーションコードやライセンスの更新、失効時の挙動等につきましては右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/000155819
機能・仕様	その他	低	**送信者ドメイン認証機能について** DDEI では送信者ドメイン認証の機能を用意しており、SPF/DKIM/DMARC に対応しております。本機能の詳細につきましては、右記 FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/000148943
機能・仕様	その他	低	**Time-of-Click プロテクションについて** DDEI では、バージョン 3.0 より Time-of-Click プロテクション機能が使用できます。メールに記載の不審 URL へのアクセスの防止に活用できます。詳細は右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/000148940
運用	その他	高	**SPAN/TAP モードにおける SMTP over TLS/SMTP STARTTLS 対応について** SPAN/TAP モードには「導入時に既存のメール配送経路そのものに影響を与えない」というメリットがございます。しかしながら、SMTP が TLS で通信経路暗号化されている場合、SPAN/TAP モードではメールを取得して解析を行うことができません。 SPAN/TAP モード導入の際は、監視対象となるメールサーバ間が通信経路暗号化されていないことを予めご確認ください。	https://success.trendmicro.com/jp/solution/000257066

カテゴリ	サブカテゴリ	重要度	内容	リンク・補足事項
運用	バックアップ	中	**仮想アナライザのサンドボックスのバックアップについて** DDEI のアップグレード(バージョンアップ)の際、ごく稀に仮想アナライザのイメージがアップグレード不可能と判断され、自動削除されることがあります。この場合、アップグレード後に仮想アナライザのサンドボックスの再インポートが必要になります。そのため、仮想アナライザのサンドボックス用 OVA ファイルを新規作成された際は、バックアップを保持しておくことをお勧めします。	https://success.trendmicro.com/jp/solution/1118468
運用	バックアップ	中	**DDEI の設定バックアップ/リストアの注意事項について** DDEI の設定をバックアップ/リストアする場合、同一 build でバックアップ、リストアを実施いただく必要がございます。また、異なるバージョン同士でのバックアップ/リストアはサポートされません。	https://success.trendmicro.com/jp/solution/1115257
運用	バックアップ	低	**DDEI の設定バックアップ/リストア対象について** 設定ファイルのバックアップ/リストア対象の設定項目について、バージョン毎に FAQ にまとめております。	https://success.trendmicro.com/jp/solution/1120705
運用	バックアップ	低	**OS およびサービスの停止/再起動機能について** DDEI の OS およびサービスの停止/再起動方法については、右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/000149697

カテゴリ	サブカテゴリ	重要度	内容	リンク・補足事項
運用	UI	低	**メッセージ追跡ログの Processing history / 処理履歴のステータスについて** DDEI へ配送されたメッセージの処理結果を、メッセージ追跡ログから確認することができます。メッセージ追跡ログの処理履歴の見方について右記 FAQ にまとめております。	https://success.trendmicro.com/jp/solution/1115810
運用	その他	中	**バージョンアップについて** DDEI をバージョンアップする場合は、右記の FAQ をご参照のうえ実施してください。	https://success.trendmicro.com/jp/solution/000148939
運用	その他	低	**ホスト名/IP アドレスの設定変更時の対応** DDEI では、管理画面からホスト名/IP アドレスの変更が可能です。	https://success.trendmicro.com/jp/solution/1123590
運用	その他	低	**TLS/SSL 通信用のサーバ証明書の導入手順** DDEI では、管理コンソールへのアクセスおよびメール送受信の際に TLS/SSL 通信が使用されます。これらの TLS/SSL 通信用のサーバ証明書を変更する場合は、右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/000153237
トラブルシュート	仮想アナライザ	低	**仮想アナライザのサンドボックスのインポートに失敗する** サンドボックス用 OVA ファイルの DDEI へのインポートが失敗する場合は、こちらの FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/1102416

カテゴリ	サブカテゴリ	重要度	内容	リンク・補足事項
トラブルシュート	誤判定	高	**今まで受信できていたメールがスパムメールとして検出されてしまう場合の対処** DDEI 3.0 より、スパムメール対策ルールが利用可能です。正常なメールが突然当該ルールによってスパムメールと判定されてしまった場合は、右記の FAQ に記載の対処方法をご検討ください。	https://success.trendmicro.com/jp/solution/000148758 https://success.trendmicro.com/jp/solution/1123585
トラブルシュート	ポリシー	中	**特定のメッセージが「不正な形式」として隔離される** DDEI は、メールデータの構造をチェックし、データの構造に関するしきい値を超えるメールを「不正な形式」という理由で隔離いたします。詳細は右記の FAQ をご参照ください。	https://success.trendmicro.com/jp/solution/000149699
トラブルシュート	その他	高	**問題発生時の調査に必要な情報一覧** DDEI にて問題が発生し、弊社サポートにて調査が必要な場合は、右記の FAQ に記載の情報を採取いただき、サポート窓口までお問合せをお願いいたします。	https://success.trendmicro.com/jp/solution/1105180
トラブルシュート	その他	低	**DDEI と Control Manager/Apex Central の問題発生時の情報取得一覧** DDEI と Control Manager/Apex Central 間の連携で問題が発生し、弊社サポートにて調査が必要な場合は、右記の FAQ に記載の情報を採取いただき、サポート窓口までお問合せをお願いいたします。	https://success.trendmicro.com/jp/solution/1121585