Trend Micro Control Manager™ 7.0

Connected Threat Defense 入門

※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。

http://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx

P/N: CMEM78079/171019_JP(2018/03)

目次

はじめに

第 1 章：Connected Threat Defense

はじめに

はじめに

Trend Micro™ Control Manager™ *Connected Threat Defense Primer* へようこそ。このドキュメントでは、Control Manager と、統合されるトレンドマイクロ製品を使用して標的型攻撃や高度な脅威を検出して分析し、被害が拡大する前に対処する方法を説明しています。

このセクションの内容:

ドキュメント

Control Manager のドキュメントには、次の情報が含まれます。

ドキュメント	説明
Readme ファイル	既知の問題の一覧が含まれます。また、オンラインヘルプや印刷ドキュメントにまだ収録されていない最新の製品情報が含まれる場合があります。
インストールおよびアップグレードガイド	Control Manager をインストールするための要件や手順を説明する PDF ドキュメント **注意** マイナーリリースバージョン、Service Pack、またはパッチでは、インストールおよびアップグレードガイドを利用できない場合があります。
システム要件	Control Manager をインストールするための要件や手順を説明する PDF ドキュメント
管理者ガイド	Control Manager と管理下の製品の設定および管理方法に加えて、Control Manager の概要と機能の説明が記載された PDF ドキュメント
オンラインヘルプ	操作手順、使用のアドバイス、および目的別の作業手順を提供する、WebHelp 形式でコンパイルされた HTML ファイル。このヘルプは、Control Manager コンソールからもアクセスできます。
Connected Threat Defense 入門	Control Manager とトレンドマイクロのさまざまな製品やソリューションを統合することで、標的型攻撃や高度な脅威を検出して分析し、被害が拡大する前に対処するための方法を説明した PDF ドキュメント
ウィジェットおよびポリシー管理ガイド	Control Manager でのダッシュボードウィジェットおよびポリシー管理の設定方法を説明した PDF ドキュメント
情報漏えい対策リスト	情報漏えい対策用の事前定義済みデータ識別子およびテンプレートを記載した PDF ドキュメント

ドキュメント	説明
製品 Q&A	問題解決およびトラブルシューティング情報のオンラインデータベース。既知の製品の問題についての最新情報を提供します。製品 Q&A にアクセスするには、https://success.trendmicro.com/jp/technical-support を参照してください。

PDF ドキュメントおよび Readme の最新バージョンをダウンロードするには、次の Web サイトにアクセスしてください。

http://downloadcenter.trendmicro.com/index.php?regs=jp

対象読者

このドキュメントは、次のユーザを対象としています。

- Control Manager の管理者: Control Manager のインストール、設定、および管理を担当し、高度なネットワークおよびサーバ管理の知識を持っていることが求められます。
- 管理下の製品の管理者: Control Manager と統合されているトレンドマイクロ製品の管理を担当し、高度なネットワークおよびサーバ管理の知識を持っていることが求められます。

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 1. ドキュメントの表記規則

表記	説明
 注意	設定上の注意
 ヒント	推奨事項

表記	説明
 重要	必須の設定や初期設定、および製品の制限事項に関する情報
 警告!	避けるべき操作や設定についての注意

用語

次の表は、Control Manager 付属のドキュメントで使用されている用語を示しています。

用語	説明
管理者 (または Control Manager 管理者)	Control Manager サーバを管理しているユーザ
エージェント	エンドポイントにインストールされている管理下の製品プログラム
コンポーネント	セキュリティリスクの検索、検出、および処理を実行するもの
Control Manager コンソールまたは管理コンソール	Control Manager のアクセス、設定、および管理を実行するための Web ベースのユーザインタフェース  注意 統合された管理下の製品のコンソールは、管理下の製品名で示されます。たとえば、ウイルスバスター Corp.管理コンソールなどです。
管理下のエンドポイント	管理下の製品エージェントがインストールされているエンドポイント
管理下の製品	Control Manager と統合されるトレンドマイクロ製品
管理下のサーバ	管理下の製品がインストールされているエンドポイント

用語	説明
サーバ	Control Manager サーバがインストールされているエンドポイント
セキュリティリスク	ウイルス、不正プログラム、スパイウェア、グレーウェア、および Web からの脅威の総称
製品サービス	Microsoft 管理コンソール (MMC) を使用してホストされる Control Manager サービス
デュアルスタック	IPv4 アドレスと IPv6 アドレスの両方のアドレスを持つエンティティ
IPv4 シングルスタック	IPv4 アドレスのみを持つエンティティ
IPv6 シングルスタック	IPv6 アドレスのみを持つエンティティ

第 1 章

Connected Threat Defense

このセクションでは、標的型攻撃や高度な脅威を、検出して分析し、被害が拡大する前に対処する方法について説明します。

次のトピックがあります。

Connected Threat Defense について

Control Manager では、トレンドマイクロのさまざまな製品やソリューションを統合することで、標的型攻撃や高度な脅威を検出して分析し、被害が拡大する前に対処することができます。

詳細については、「Connected Threat Defense 製品の統合」を参照してください。

機能要件

次の表は、Connected Threat Defense アーキテクチャで使用可能な機能、および各機能と統合する必須の製品とオプションの製品をまとめたものです。

機能	必須の製品	オプションの製品
脅威の監視	• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降) **注意** ログデータを評価するには、少なくとも 1 つのオプションの製品が必要です。	• ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 10.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降) • InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (またはそれ以降) • InterScan for Microsoft Exchange 12.5 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降)

機能	必須の製品	オプションの製品
不審オブジェクトリストの同期 詳細については、19 ページの「不審オブジェクトリスト」および41 ページの「Connected Threat Defense 製品の統合」を参照してください。	• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降) 注意 同期には少なくとも 1 つのオプションの製品が必要です。	• Smart Protection Server 3.0 Patch 1 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 10.0 (またはそれ以降) • InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降)
不審オブジェクトのサンプルの送信	• Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降)	• Deep Security 10.0 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降) • InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (またはそれ以降) • InterScan for Microsoft Exchange 12.5 (またはそれ以降) • Deep Discovery Email Inspector 3.0 (またはそれ以降)

機能	必須の製品	オプションの製品
不審オブジェクト管理	• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降) または Deep Discovery Analyzer 5.1 (またはそれ以降)	• ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 10.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降) • InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降)
不審オブジェクト検出時の処理 詳細については、22 ページの「不審オブジェクト検出時の処理」を参照してください。	• Control Manager 7.0 (またはそれ以降)	• Smart Protection Server 3.0 Patch 1 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) • Deep Security 10.0 (またはそれ以降) • InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降) • InterScan Web Security Virtual Appliance 6.5 SP2 Patch 2 (またはそれ以降) • Cloud App Security 5.0 (またはそれ以降)
影響診断	• Control Manager 7.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降)	• なし

機能	必須の製品	オプションの製品
エンドポイントの隔離 詳細については、38 ページの「エンドポイントを隔離する」を参照してください。	• Control Manager 7.0 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降)	• Endpoint Sensor 1.5 (またはそれ以降)
IOC の管理	• Control Manager 7.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降)	• なし

不審オブジェクトリスト管理

Control Manager では、不審オブジェクトリストを管理下の製品の間で同期したり、ユーザ指定リストや例外リストを作成して不審オブジェクトの拡散を細かく制御したりできます。環境内で不審オブジェクトを検出したときにサポート対象の管理下の製品で実行する具体的な処理を設定することもできます。

Control Manager は、仮想アナライザで検出された不審オブジェクトリストとユーザ指定の不審オブジェクトリスト (除外リストのオブジェクトを除く) を合わせ、そのリストを統合された管理下の製品と同期します。

不審オブジェクトリストを Control Manager と同期できる製品の詳細については、16 ページの「機能要件」の「不審オブジェクトリストの同期」を参照してください。

不審オブジェクトリスト

Control Manager は、多数の管理下の製品の間で、仮想アナライザで検出された不審オブジェクトリストを合わせ、すべての不審オブジェクトリストを同期します。それぞれの管理下の製品でリストを実装する方法は、その製品にお

ける本機能の実装方法によって異なります。管理下の製品で不審オブジェクトリストを使用および同期する方法の詳細については、その製品の管理者ガイドを参照してください。

注意

管理者は、Control Manager コンソールを使用して不審オブジェクトに対して具体的な検索処理を設定できます。その後、不審オブジェクトリスト設定に基づいて処理を実行するように特定の管理下の製品を設定できます。

詳細については、22 ページの「不審オブジェクト検出時の処理」を参照してください。

リストの種類	説明
仮想アナライザで検出された不審オブジェクト	仮想アナライザを使用する管理下の製品は、分析のために不審なファイルまたは URL を仮想アナライザに送信します。仮想アナライザは、オブジェクトに脅威の可能性があると判断した場合、そのオブジェクトを不審オブジェクトリストに追加します。仮想アナライザは、統合と同期の目的でリストを登録済みの Control Manager サーバに送信します。 Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] > [オブジェクト] タブに移動して、仮想アナライザで検出された不審オブジェクトのリストを表示します。
仮想アナライザで検出された不審オブジェクトの除外設定	Control Manager 管理者は、仮想アナライザの不審オブジェクトリストから安全と考えられるオブジェクトを選択し、除外リストに追加できます。 Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] > [除外] タブに移動して、仮想アナライザで検出された不審オブジェクトの除外設定を確認します。 Control Manager は、除外リストを利用する仮想アナライザにそのリストを送信します。仮想アナライザでは、除外リストに含まれている不審オブジェクトを検出すると、そのオブジェクトは「安全」と認識され、再度分析されません。」 詳細については、21 ページの「仮想アナライザで検出された不審オブジェクトリストに除外を追加する」を参照してください。

リストの種類	説明
ユーザ指定の不審オブジェクト	Control Manager の管理者は、[運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] で、仮想アナライザの不審オブジェクトリストに含まれていないオブジェクトを不審オブジェクトとして追加できます。 詳細については、33 ページの「脅威の兆候に対する予防的対策」を参照してください。

仮想アナライザで検出された不審オブジェクトリストに除外を追加する

Control Manager では、ファイル SHA-1、ドメイン、IP アドレス、または URL に基づいて、仮想アナライザで検出された不審オブジェクトリストからオブジェクトを除外できます。

重要

ユーザ指定の不審オブジェクトリストは、仮想アナライザの不審オブジェクトリストよりも優先されます。

手順

1. [運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。

   [仮想アナライザで検出された不審オブジェクト] 画面が表示されます。

2. [除外] タブをクリックします。
3. [追加] をクリックします。
4. オブジェクトの [種類] を指定します。
   - ファイル SHA-1: ファイルの SHA-1 ハッシュ値を指定します。
   - IP アドレス: IP アドレスを指定します。
   - URL: URL を指定します。

- ドメイン: ドメインを指定します。

  Control Manager では、ワイルドカード文字 (*) を使用して、仮想アナライザで検出された不審オブジェクトリストから特定のサブドメインまたはサブディレクトリを除外できます。

EXAMPLE	説明
https://*.domain.com/	ドメイン「domain.com」のすべてのサブドメインを、仮想アナライザで検出された不審オブジェクトリストから除外します。
*.abc.domain.com	サブドメイン「abc」のすべてのサブドメインを、仮想アナライザで検出された不審オブジェクトリストから除外します。
https:// *.domain.com/abc/*	ドメイン「domain.com」のすべてのサブドメインと、サブディレクトリ「abc」のサブディレクトリを、仮想アナライザで検出された不審オブジェクトリストから除外します。

5. (オプション) 不審オブジェクトの識別に役立つ [メモ] を指定します。
6. [追加] をクリックします。

   オブジェクトが仮想アナライザの除外リストに表示されます。管理下の製品が不審オブジェクトリストを利用する場合、その管理下の製品は、次回の同期処理中に新しいオブジェクト情報を受信します。

不審オブジェクト検出時の処理

管理者は Control Manager コンソールを使用して、特定の管理下の製品が仮想アナライザで検出された不審オブジェクトリストまたはユーザ指定の不審オブジェクトリスト内の特定の不審オブジェクトを検出したときに実行する検出時の処理を設定できます。

表 1-1. 検出時の処理の製品サポート

製品	仮想アナライザリスト	ユーザ指定リスト
ウイルスバスター Corp. XG SP1 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック
Deep Security 10.2 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック
• Deep Discovery Inspector 5.0 (またはそれ以降) • Deep Discovery Email Inspector 3.0 (またはそれ以降)	以下の不審オブジェクトの種類に対して同期処理を実行します。 • ファイル: 検索処理は行われません。 • IP アドレス: 検索処理は行われません。 • URL: 検索処理は行われません。 • ドメイン: 検索処理は行われません。	以下の不審オブジェクトの種類に対して同期処理を実行します。 • ファイル: 検索処理は行われません。 • IP アドレス: 検索処理は行われません。 • URL: 検索処理は行われません。 • ドメイン: 検索処理は行われません。

製品	仮想アナライザリスト	ユーザ指定リスト
InterScan Messaging Security Virtual Appliance 9.1 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • ファイル SHA-1: ログ、ブロック、または隔離
InterScan Web Security Virtual Appliance 6.5 Patch 2 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • ファイル SHA-1: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • ファイル SHA-1: ログ、ブロック、または隔離 • IP アドレス: ログ、ブロック • URL: ログ、ブロック • ドメイン: ログ、ブロック
Cloud App Security 5.0 (またはそれ以降)	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • URL: ログ、ブロック	以下の不審オブジェクトの種類に対して処理を実行します。 • ファイル: ログ、ブロック、または隔離 • URL: ログ、ブロック

<table>
<tr><th>製品</th><th>仮想アナライザリスト</th><th>ユーザ指定リスト</th></tr>
<tr><td rowspan="2">Smart Protection Server 3.0 Patch 1 (またはそれ以降)
ウイルスバスター Corp. 11.0 SP1 (以降) と統合された Smart Protection Server
サポートされている Smart Protection Server に Web レピュテーションクエリを送信するトレンドマイクロ製品</td><td>管理下の製品は、Web レピュテーションクエリ時に以下の不審オブジェクトの種類に対して処理を実行します。
URL: ログ、ブロック</td><td>管理下の製品は、Web レピュテーションクエリ時に以下の不審オブジェクトの種類に対して処理を実行します。
URL: ログ、ブロック
重要
Smart Protection Server はユーザ指定の不審オブジェクトリスト内のすべての URL を「高」リスクとして分類します。</td></tr>
<tr><td colspan="2">注意
不審 URL オブジェクトに対して Control Manager で設定した処理を直接実行できるのは特定の管理下の製品のみです。その他の管理下の製品は、その製品に設定された Web レピュテーション設定に基づいて不審 URL オブジェクトに対して処理を実行します。

管理下の製品に表示されるログには、不審オブジェクトの検出に関連する情報が含まれない場合があります。Control Manager は、管理下の製品から送信されたログを解釈して、Control Manager コンソールに不審オブジェクトの検出を表示します。</td></tr>
</table>

配信を設定する

配信を設定すると、Control Manager は仮想アナライザで検出された不審オブジェクトとユーザ指定の不審オブジェクト (除外リストのオブジェクトを除く) を統合し、特定の管理下の製品に送信できます。管理下の製品は、受け取ったオブジェクトのすべてまたは一部を同期して使用します。

Control Manager では、不審 IP アドレスとドメインを TippingPoint に送信することもできます。

手順

1. [運用管理] > [不審オブジェクト] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。

2. 不審オブジェクトを管理下の製品に送信するには、以下の手順を実行します。

   a. [管理下の製品] タブをクリックします。

   b. [不審オブジェクトを管理下の製品に送信します] チェックボックスをオンにします。

   c. 以下の情報を記録し、管理下の製品で Control Manager を仮想アナライザとして設定する際に使用します。

      - サービス URL: Control Manager のサービス URL
      - API キー: 管理下の製品で Control Manager を識別するコード

   d. [保存] をクリックします。

   e. [今すぐ同期] をクリックします。

3. 不審オブジェクトを TippingPoint に送信するには、以下の手順を実行します。

   a. [不審オブジェクト (IP アドレスとドメイン名のみ) を TippingPoint に送信します] チェックボックスをオンにします。

      注意

      Control Manager は、Deep Discovery Inspector および Deep Discovery Analyzer によって分析された不審 IP アドレスとドメイン名を送信します。TippingPoint は、レピュテーションフィルタを使用して、レピュテーショングループ全体にブロック、許可、または通知の処理を適用します。レピュテーションフィルタの詳細については、TippingPoint のドキュメントを参照してください。

   b. 次の項目を指定します。

      - サーバ名: TippingPoint 配信用のサーバ URL とポート番号を入力します。

- ユーザ名: TippingPoint コンソールへのアクセス権限があるアカウントのユーザ名を入力します。
- パスワード: アカウントのパスワードを入力します。

c. (オプション) [接続テスト] をクリックして接続を確認します。

d. TippingPoint にドメイン名または IP アドレス情報を送信する重大度レベルを選択します。

- 高のみ: 重大度の高い IP アドレスとドメイン名
- 中/高: 重大度が高および中程度の IP アドレスとドメイン名
- すべて: 重大度が高、中、低の IP アドレスとドメイン名

4. [保存] をクリックします。

5. [今すぐ同期] をクリックします。

不審オブジェクトの検出

環境内の不審オブジェクトの検出は、Control Manager コンソールを使用してさまざまな方法で確認できます。不審オブジェクトの検出を確認する別の方法については、以下を参照してください。

- 27 ページの「危険性の高いエンドポイントや受信者を確認する」
- 29 ページの「Endpoint Sensor を使用して影響を分析する」

注意

Control Manager では、環境内の不審オブジェクトにさらされているユーザやエンドポイントを識別することだけができます。Control Manager コンソールでは不審オブジェクトに対して直接の処理を実行できません。

危険性の高いエンドポイントや受信者を確認する

Control Manager は、すべての管理下の製品から受け取った Web レピュテーション、URL フィルタ、ネットワークコンテンツ検査、およびルールベース検出のログを確認し、それらのログを不審オブジェクトリストと照合します。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • 少なくとも 1 つのオプション製品	• Control Manager によって管理されるトレンドマイクロ製品 • Endpoint Sensor 1.5 (またはそれ以降) 重要 • Endpoint Sensor 1.5 は、ファイルおよび IP アドレスの不審オブジェクトの種類に関する情報のみを提供します。 • Endpoint Sensor 1.6 (またはそれ以降) は、ファイル、IP アドレスおよびドメインの不審オブジェクトの種類に関する情報のみを提供します。

手順

1. Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。
2. 確認するオブジェクトの左側にある矢印を展開します。
   - [危険性の高いエンドポイント] リストには、引き続き不審オブジェクトの影響を受けているすべてのエンドポイントとユーザが表示されます。
     - 「ファイル」の検出では、[最新の処理結果] 列に管理下の製品によって報告された最新の処理結果が表示されます。
     - その他のすべての検出の種類では、[最新の処理結果] 列に「N/A」と表示されます。
   - [危険性の高い受信者] リストには、引き続き不審オブジェクトの影響を受けているすべての受信者が表示されます。

Endpoint Sensor を使用して影響を分析する

Endpoint Sensor は、エージェントと通信し、クライアントログの履歴検索を実行して、不審オブジェクトが検出されずに一定期間にわたって環境に影響を与えているかどうか判断します。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • Endpoint Sensor 1.5 (またはそれ以降) **重要** • Endpoint Sensor 1.5 は、ファイルおよび IP アドレスの不審オブジェクトの種類に関する情報のみを提供します。 • Endpoint Sensor 1.6 (またはそれ以降) は、ファイル、IP アドレスおよびドメインの不審オブジェクトの種類に関する情報のみを提供します。	• なし

手順

1. Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。
2. 診断するオブジェクトの横のチェックボックスをオンにします。
3. [影響の診断] をクリックします。

   Endpoint Sensor はエージェントと通信し、検出された不審オブジェクトのクライアントログを評価します。

Endpoint Sensor の Retro Scan

Retro Scan は、指定された検索条件に基づいて、過去のイベントとそのアクティビティチェーンを調査します。調査結果は、疑わしいアクティビティの

実行フローを示すマインドマップの形式で表示されます。これにより、組織全体を巻き込んだ、標的型攻撃のイベントチェーンを分析できます。

Retro Scan の調査では、次の種類のオブジェクトが使用されます。

- DNS レコード
- IP アドレス
- ファイル名
- ファイルパス
- SHA-1 ハッシュ値
- MD5 ハッシュ値
- ユーザアカウント

Retro Scan は、エンドポイントのイベント履歴が格納された、標準化されたデータベースに対してクエリを実行します。この方法は、従来のログファイルに比べて使用するディスク容量が少なく、リソースを消費しません。

処理プロセスを表示する

[処理プロセス] 画面には、環境内の不審オブジェクトのライフサイクルとその不審オブジェクトがユーザやエンドポイントに与えている現在の影響について概要が表示されます。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (または以降) または Deep Discovery Analyzer 5.1 (または以降) • [影響診断] および [軽減] のデータを表示するには、少なくとも 1 つのオプションの製品が必要です。	• Control Manager によって管理されるトレンドマイクロ製品 • Endpoint Sensor 1.5 (またはそれ以降) 重要 • Endpoint Sensor 1.5 は、ファイルおよび IP アドレスの不審オブジェクトの種類に関する情報のみを提供します。 • Endpoint Sensor 1.6 (またはそれ以降) は、ファイル、IP アドレスおよびドメインの不審オブジェクトの種類に関する情報のみを提供します。

手順

1. Control Manager コンソールで、[運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。
2. 特定の不審オブジェクトについて、表の [処理プロセス] 列にある [表示] リンクをクリックします。

   [処理プロセス] 画面が表示されます。
3. 次のいずれかのタブをクリックして、不審オブジェクトに関する詳細情報を表示します。

タブ	説明
サンプル送信	不審オブジェクトの最初の分析と最新の分析に関連する情報が表示されます。 Control Manager では、次の製品と統合して、仮想アナライザを使用してその他の管理下の製品から送信された不審オブジェクトを分析します。 • Deep Discovery Analyzer 5.1 (またはそれ以降) • Deep Discovery Endpoint Inspector 3.0 (またはそれ以降) • Deep Discovery Inspector 3.8 (またはそれ以降)
分析	送信されたオブジェクトの仮想アナライザによる分析が表示されます。 システムを危険にさらしたり、情報漏えいを引き起こす可能性があるオブジェクトが見つかると、不審オブジェクトのリスクレベルが判定されます。サポートされるオブジェクトには、ファイル (SHA-1 ハッシュ値)、IP アドレス、ドメイン、URL などがあります。
配信	不審オブジェクトリストを同期したすべての製品と、最後の同期時刻が表示されます。 Control Manager は、仮想アナライザで検出された不審オブジェクトリストとユーザ指定の不審オブジェクトリスト (除外リストのオブジェクトを除く) を合わせ、そのリストを統合された管理下の製品と同期します。
影響の診断と軽減	不審オブジェクトの影響を受けているすべてのエンドポイントとユーザが表示されます。 • 「ファイル」の検出では、[最新の処理結果] 列に管理下の製品によって報告された最新の処理結果が表示されます。 • その他のすべての検出の種類では、[最新の処理結果] 列に「N/A」と表示されます。 [不審アクティビティ] リンクをクリックすると、オブジェクトがユーザやエンドポイントに与えた影響を調査できます。

脅威の兆候に対する予防的対策

Control Manager では、ネットワーク内でまだ確認されていない不審オブジェクトからネットワークを保護するさまざまな方法を用意しています。ユーザ指定の不審オブジェクトリストを利用、または侵入の痕跡 (IOC) をインポートして、外部ソースによって識別された脅威の兆候に対して処理方法を設定します。

機能	説明
ユーザ指定の不審オブジェクトリスト	ユーザ指定の不審オブジェクトリストを使用すると、登録した仮想アナライザがネットワークで検出していない不審なファイル、IP アドレス、URL、およびドメインオブジェクトを定義できます。 サポートされている管理下の製品が不審オブジェクトリストを利用する場合、その管理下の製品は、未知の脅威が拡散することを防ぐためにこのリストで見つかったオブジェクトに対して処理を実施できます。 34 ページの「ユーザ指定の不審オブジェクトリストにオブジェクトを追加する」 22 ページの「不審オブジェクト検出時の処理」
侵入の痕跡	IOC ファイルをインポートしてネットワークのエンドポイントで詳細な履歴分析を実施し、脅威の兆候が環境に影響を及ぼしているかどうかを判断します。 IOC での影響診断には、エンドポイントの動作の推移に関する詳細なログ情報が必要です。Endpoint Sensor 1.5 (またはそれ以降) がインストールされているエンドポイントのみが、この種類の詳細分析に必要なログ情報を収集します。 ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) のクライアントと統合することで、感染したエンドポイントを隔離し、エンドポイントで識別された脅威が拡散することを防ぎます。 36 ページの「影響を診断して IOC に対応する」

ユーザ指定の不審オブジェクトリストにオブジェクトを追加する

不審オブジェクトをユーザ指定の不審オブジェクトリストに追加することにより、ネットワークでまだ確認されていないオブジェクトからネットワークを保護できます。Control Manager には、ファイル、ファイル SHA-1、ドメイン、IP アドレス、および URL に基づいてオブジェクトを追加するオプションがあります。また、不審オブジェクト (ドメインオブジェクトを除く) の検出後にサポート対象のトレンドマイクロの製品で実行する検索処理を指定することもできます。

手順

1. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [追加] をクリックします。

3. オブジェクトの [種類] を指定します。

   - ファイル: [参照] をクリックして不審なオブジェクトファイルをアップロードします。
   - ファイル SHA-1: ファイルの SHA-1 ハッシュ値を指定します。
   - IP アドレス: IP アドレスを指定します。
   - URL: URL を指定します。
   - ドメイン: ドメインを指定します。

4. サポート対象の製品でオブジェクトの検出後に実行する [検出時の処理] を指定します。

   - ログ
   - ブロック
   - 隔離

注意

このオプションはファイルオブジェクトまたはファイル SHA-1 オブジェクトに対してのみ使用できます。

5. (オプション) 不審オブジェクトの識別に役立つ [メモ] を指定します。
6. [追加] をクリックします。

   ユーザ指定の不審オブジェクトリストにオブジェクトが表示されます。管理下の製品が不審オブジェクトリストを利用する場合、その管理下の製品は、次回の同期処理中に新しいオブジェクト情報を受信します。

ユーザ指定の不審オブジェクトリストをインポートする

適切な形式の CSV ファイルを使用して、複数の不審オブジェクトをユーザ指定の不審オブジェクトリストに追加します。

手順

1. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。
2. [インポート] をクリックします。
3. 不審オブジェクトのリストを含む CSV ファイルを選択します。

ヒント

[サンプル CSV のダウンロード] リンクをクリックして、適切な形式のサンプル CSV ファイルと、ユーザ指定の不審オブジェクトリストの作成に関する詳しい説明を取得します。

4. [インポート] をクリックします。

   ユーザ指定の不審オブジェクトリストに CSV ファイル内のオブジェクトが表示されます。管理下の製品が不審オブジェクトリストを利用する場

合、その管理下の製品は、次回の同期処理中に新しいオブジェクト情報を受信します。

影響を診断して IOC に対応する

適切な形式の IOC ファイルを信頼された外部ソース (セキュリティフォーラムや他の Deep Discovery 仮想アナライザ製品) から取得した後、そのファイルを Control Manager にインポートしてネットワーク内に脅威が存在するかどうかを判別し、脅威が他のエンドポイントに拡散するのを防ぐために軽減処理を実行します。

重要

- 外部 IOC データの影響を診断するには、Endpoint Sensor 1.5 (またはそれ以降) が Control Manager に登録され、対象エンドポイントにインストールされている必要があります。
- エンドポイントを隔離するには、ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) のクライアントをインストールし、対象エンドポイントでウイルスバスター Corp.のファイアウォールを有効にする必要があります。

手順

1. [運用管理] > [侵入の痕跡] に移動します。

   [侵入の痕跡 (IOC)] 画面が表示されます。

2. [追加] をクリックします。
3. 調査のソースとして使用する IOC ファイルを選択します。
4. [アップロード] をクリックします。

   ファイルに含まれるサポート対象の痕跡を示した画面が表示されます。

5. 調査を開始するには、リストから IOC ファイルを選択して、[影響の診断] をクリックします。

   [調査を開始する] 画面が表示されます。

6. [対象エンドポイント] ドロップダウンから、[すべて] または [指定] を選択して、調査するエンドポイント名または IP アドレスを入力します。

   複数のエンドポイント名または IP アドレスを追加するには、新しい行を使用します。

7. [調査を開始する] をクリックします。

   注意

   調査が完了するまでには多少の時間がかかります。[進行状況] 列で調査の進行状況を確認してください。

8. 診断が完了したら、[危険] 列の数字をクリックして詳細を確認するか、または感染したエンドポイントで処理を実行します。

   注意

   [保留/問題あり] 列には、まだ診断が終了していないエンドポイントの数が表示されます。たとえば、エンドポイントがネットワークに再接続するまで、そのエンドポイントでは診断を開始できません。

   [侵入の痕跡]→[危険性の高いエンドポイント] 画面が表示されます。

9. 不審なオブジェクトがネットワーク全体に拡散しないようにするには、[処理] 列で [隔離] をクリックして、感染したエンドポイントでネットワークトラフィックを停止します。

   重要

   エンドポイントを隔離するには、ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) のクライアントをインストールし、対象エンドポイントでウイルスバスター Corp.のファイアウォールを有効にする必要があります。

10. [許可するトラフィックの変更] ボタンをクリックして、隔離されたすべてのエンドポイントに許可する送受信トラフィックを必要に応じて設定します。

    a. [隔離されたエンドポイント上のトラフィック制御] を選択します。

    b. [受信トラフィック] または [送信トラフィック] セクションを展開します。

c. [プロトコル]、[IP アドレス]、および [送信先ポート] を指定して、許可するトラフィックを指定します。

コンマを使用して複数の送信先ポートを区切ります。

d. [送信先ポート] 情報の右側の - コントロールをクリックして、複数の送受信エントリを追加します。

注意

許可するトラフィックの設定を変更した後、以前に隔離されたエンドポイントと後で隔離されるエンドポイントはすべて、送受信トラフィックの設定が適用されます。

エンドポイントを隔離する

危険性の高いエンドポイントを隔離して調査を実行し、セキュリティの問題を解決します。すべての問題を解決したら、すぐに接続を復元します。

必須の製品	オプションの製品
• Control Manager 7.0 (またはそれ以降) • ウイルスバスター Corp. 11.0 SP1 (またはそれ以降) **重要** エンドポイントを隔離するには、ウイルスバスター Corp.クライアントをインストールし、対象エンドポイントでウイルスバスター Corp.のファイアウォールを有効にする必要があります。	• Endpoint Sensor 1.5 (またはそれ以降)

手順

1. [ディレクトリ] > [ユーザ/エンドポイント] に移動します。

2. エンドポイントの表示を選択します。
3. リスト内のエンドポイントの名前をクリックします。
4. 表示される [エンドポイント - <名前>] 画面で [タスク] > [隔離] をクリックします。

   Control Manager では、次の理由により、エンドポイント上で [隔離] オプションが無効になります。

   - エンドポイントのクライアントでサポート対象外のバージョンが実行されています。
   - Control Manager へのログオンに使用されているユーザアカウントに必要な権限がありません。

5. [エンドポイント - <名前>] 画面の上部にメッセージが表示され、その画面で隔離ステータスを監視できます。隔離が終了すると、メッセージが閉じられ、対象エンドポイントにユーザへの通知が表示されます。

   隔離プロセス中に問題が発生した場合、[エンドポイント - <名前>] 画面の上部に問題を通知するメッセージが表示されます。

6. Control Manager ネットワーク上の隔離されたエンドポイントをすべて表示するには、[ユーザ/エンドポイントディレクトリ] ツリーで [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み] ノードをクリックします。
7. [許可するトラフィックの変更] ボタンをクリックして、隔離されたすべてのエンドポイントに許可する送受信トラフィックを必要に応じて設定します。

   a. [隔離されたエンドポイント上のトラフィック制御] を選択します。
   b. [受信トラフィック] または [送信トラフィック] セクションを展開します。
   c. [プロトコル]、[IP アドレス]、および [送信先ポート] を指定して、許可するトラフィックを指定します。

      コンマを使用して複数の送信先ポートを区切ります。

   d. [送信先ポート] 情報の右側の - コントロールをクリックして、複数の送受信エントリを追加します。

注意

許可するトラフィックの設定を変更した後、以前に隔離されたエンドポイントと後で隔離されるエンドポイントはすべて、送受信トラフィックの設定が適用されます。

8. 隔離されたエンドポイントでセキュリティの脅威が解決したら、次の場所からネットワーク接続を復元します。

   - エンドポイント - <名前>: [タスク] > [復元] をクリックします。
   - [エンドポイント] > [フィルタ] > [ネットワーク接続] > [隔離済み]: 表の中のエンドポイントの行を選択して、[ネットワーク接続の復元] をクリックします。

9. 画面の上部にメッセージが表示され、その画面で復元ステータスを監視できます。復元が終了すると、メッセージが閉じられ、対象エンドポイントにユーザへの通知が表示されます。

   復元プロセス中に問題が発生した場合、画面の上部に問題を通知するメッセージが表示されます。

Connected Threat Defense 製品の統合

Connected Threat Defense 戦略では、多くのトレンドマイクロ製品を統合します。次の図は主な製品との関係を示しています。

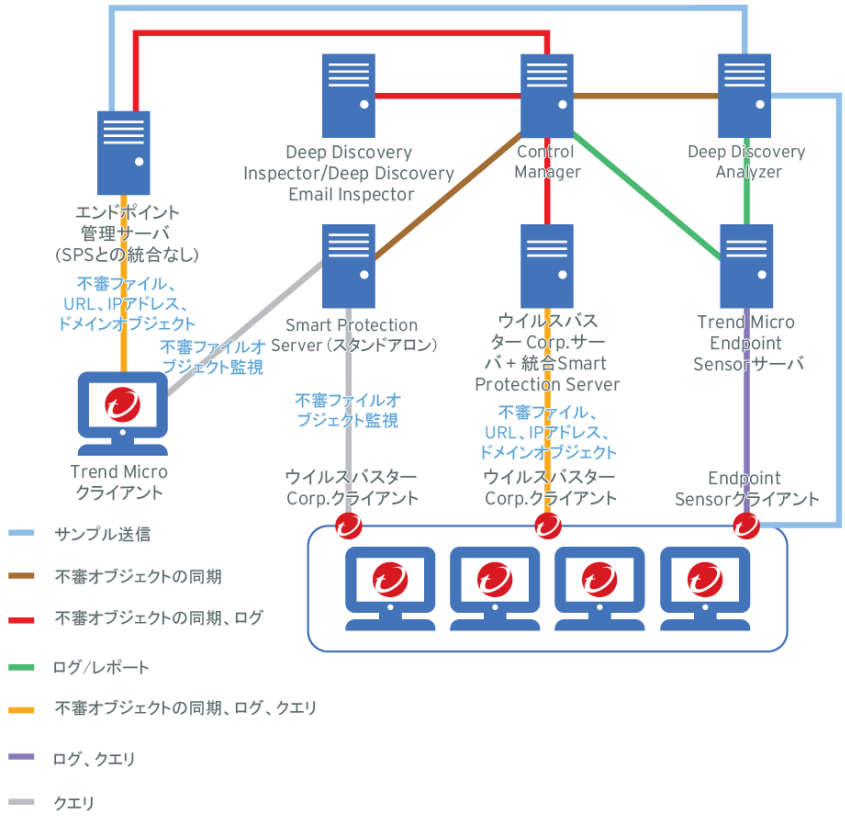


図 1-1. エンドポイントの保護

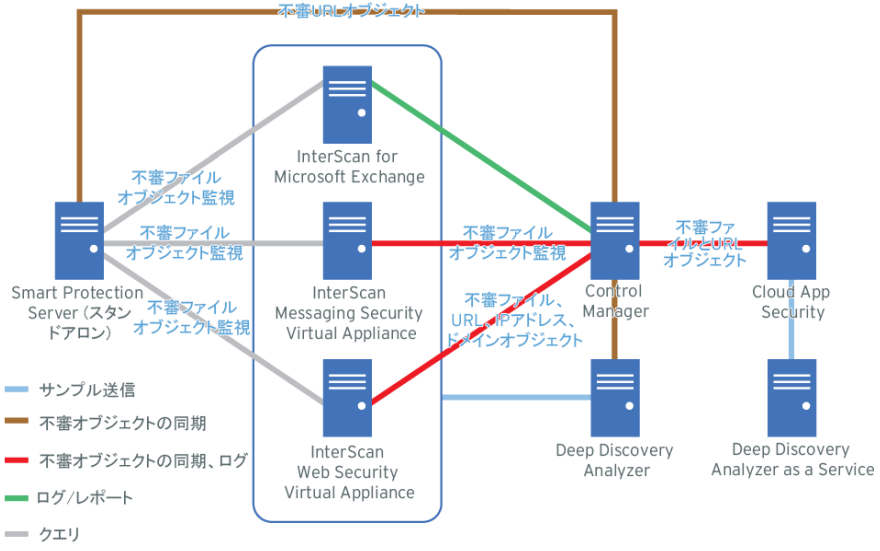


図 1-2. メッセージングとネットワークセキュリティ

Control Manager は、ログ分析の実行や検出ファイルと同期した不審オブジェクトリストを比較することにより、登録された他のトレンドマイクロ製品の監視を強化します。

各主要製品の Control Manager の登録および不審オブジェクトリストの同期については、以下を参照してください。

- 43 ページの「Control Manager」
- 44 ページの「Deep Discovery Analyzer」
- 45 ページの「Trend Micro Endpoint Sensor」
- 45 ページの「Deep Discovery Inspector」
- 46 ページの「Deep Security」
- 47 ページの「ウイルスバスター Corp.」

- 48 ページの「Smart Protection Server」
- 49 ページの「InterScan Messaging Security Virtual Appliance」
- 50 ページの「InterScan Web Security Virtual Appliance」
- 51 ページの「InterScan for Microsoft Exchange」
- 51 ページの「Trend Micro Endpoint Application Control 」
- 51 ページの「Deep Discovery Email Inspector」
- 52 ページの「Cloud App Security」

Control Manager

要件	説明
製品バージョン	7.0 (またはそれ以降)
Control Manager 登録情報	Control Manager コンソールを使用して Control Manager に登録されていない製品の場合、次の Control Manager 登録情報が必要です。 • サーバの FQDN または IP アドレス • ポート: 初期設定では、Control Manager は HTTP ポート 80 または HTTPS ポート 443 を使用します。 Control Manager 管理コンソールを使用して登録されている製品の場合、[運用管理] > [管理下のサーバ] > [サーバの登録] に進み、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	不審オブジェクトリストを Control Manager と自動的に同期しない製品の場合、次の API 情報が必要です。 • API キー: API キーを入手するには、Control Manager 管理コンソールを開いて、[運用管理] > [不審オブジェクト] > [配信設定] に移動します。

要件	説明
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • 影響診断 • エンドポイントの隔離 • IOC の管理

Deep Discovery Analyzer

要件	説明
製品バージョン	5.1 (またはそれ以降)
Control Manager の登録	Control Manager の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	Control Manager への登録後に自動的に実行します。 初期設定では、不審オブジェクトリストは Control Manager サーバと 10 分ごとに同期します。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理

Trend Micro Endpoint Sensor

注意

- 以前の名前は Deep Discovery Endpoint Sensor です (バージョン 1.5 以前)。
- Endpoint Sensor では不審オブジェクトリストの同期はサポートされません。

要件	説明
製品バージョン	1.5 (またはそれ以降)
Control Manager の登録	Control Manager の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 影響診断 • エンドポイントの隔離 • IOC の管理

Deep Discovery Inspector

要件	説明
製品バージョン	3.8 (またはそれ以降)

要件	説明
Control Manager の登録	Deep Discovery Inspector の管理コンソールの [運用管理] > [統合製品/サービス] > [Control Manager] 必須の Control Manager 情報: • サーバの FQDN または IP アドレス • ポート: 初期設定では、Control Manager は HTTP ポート 80 または HTTPS ポート 443 を使用します。 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。
不審オブジェクトリストの同期	Deep Discovery Inspector の管理コンソールの [運用管理] > [統合製品/サービス] > [Control Manager] 必須の Control Manager 情報: • API キー: API キーを入手するには、Control Manager 管理コンソールを開いて、[運用管理] > [不審オブジェクト] > [配信設定] に移動します。 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。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理

Deep Security

要件	説明
製品バージョン	10.0 以降
Control Manager の登録	Control Manager の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。

要件	説明
不審オブジェクトリストの同期	Control Manager への登録後に自動的に実行します。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

ウイルスバスター Corp.

要件	説明
製品バージョン	11.0 SP1 (またはそれ以降)
Control Manager の登録	ウイルスバスター Corp.管理コンソールの [運用管理] > [設定] > [Control Manager] 必須の Control Manager 情報: • サーバの FQDN または IP アドレス • ポート: 初期設定では、Control Manager は HTTP ポート 80 または HTTPS ポート 443 を使用します。
不審オブジェクトリストの同期	ウイルスバスター Corp.管理コンソールの [運用管理] > [設定] > [不審オブジェクトリスト] 必須の Control Manager 情報: • なし 注意 ウイルスバスター Corp.は、Control Manager の登録中に、必要な API キー情報を Control Manager サーバから自動的に取得します。

要件	説明
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • エンドポイントの隔離

Smart Protection Server

要件	説明
製品バージョン	3.0 Patch 1 (またはそれ以降)
Control Manager の登録	Control Manager の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。

要件	説明
不審オブジェクトリストの同期	Smart Protection Server の管理コンソールから: • Smart Protection Server 3.0 Patch 1 の場合は、[Smart Protection] > [C&C コンタクトアラート] に移動します。 • Smart Protection Server 3.0 Patch 2 以降の場合は、[Smart Protection] > [不審オブジェクト] に移動します。 不審オブジェクトリストのソースに必要な情報: • サービスの URL • ポート番号 リストのソースが Control Manager である場合、初期設定のポートは HTTP ポート 80 または HTTPS ポート 443 です。 • API キー: サーバ管理者から提供されます。 リストのソースが Control Manager である場合、Control Manager 管理コンソールを開き、[運用管理] > [不審オブジェクト] > [配信設定] に移動します。 **注意** Smart Protection Server 3.3 以降の場合は、Control Manager への登録中に、必要な API キー情報が Smart Protection Server に送信されます。 詳細については、Smart Protection Server 管理ガイドを参照してください。
統合された Connected Threat Defense 機能	• 不審オブジェクトリストの同期 • 不審オブジェクト検出時の処理

InterScan Messaging Security Virtual Appliance

要件	説明
製品バージョン	9.1 (またはそれ以降)

要件	説明
Control Manager の登録	詳細については、InterScan Messaging Security Virtual Appliance 管理者ガイドを参照してください。
不審オブジェクトリストの同期	Control Manager への登録後に自動的に実行します。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

InterScan Web Security Virtual Appliance

要件	説明
製品バージョン	6.5 SP2 Patch 2 (またはそれ以降)
Control Manager の登録	詳細については、InterScan Web Security Virtual Appliance 管理者ガイドを参照してください。
不審オブジェクトリストの同期	詳細については、InterScan Web Security Virtual Appliance 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

InterScan for Microsoft Exchange

要件	説明
製品バージョン	12.5 (またはそれ以降)
Control Manager の登録	詳細については、InterScan for Microsoft Exchange 管理者ガイドを参照してください。
不審オブジェクトリストの同期	詳細については、InterScan for Microsoft Exchange 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトのサンプルの送信

Trend Micro Endpoint Application Control

要件	説明
製品バージョン	2.0 SP1 Patch 1 (またはそれ以降)
Control Manager の登録	Control Manager の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	Control Manager への登録後に自動的に実行します。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理

Deep Discovery Email Inspector

要件	説明
製品バージョン	3.0 (またはそれ以降)

要件	説明
Control Manager の登録	詳細については、Deep Discovery Email Inspector 管理者ガイドを参照してください。
不審オブジェクトリストの同期	詳細については、Deep Discovery Email Inspector 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• 不審オブジェクトリストの同期 • 不審オブジェクトのサンプルの送信

Cloud App Security

要件	説明
製品バージョン	5.0 (またはそれ以降)
Control Manager の登録	Control Manager の管理コンソールで登録します。[運用管理] > [管理下のサーバ] > [サーバの登録] に移動し、[サーバの種類] リストから製品を選択して、[追加] をクリックします。
不審オブジェクトリストの同期	詳細については、Cloud App Security 管理者ガイドを参照してください。
統合された Connected Threat Defense 機能	• セキュリティの脅威の監視 • 不審オブジェクトリストの同期 • 不審オブジェクト管理 • 不審オブジェクト検出時の処理

第 2 章

不審オブジェクトリストエクスポート/インポートツールユーザガイド

このセクションでは、Control Manager の不審オブジェクトリストエクスポートツール (`SuspiciousObjectExporter.exe`) およびインポートツール (`ImportSOFromCSV.exe`) を使用する方法について説明します。

次のトピックがあります。

- 69 ページの「Control Manager を使用してユーザ指定リストをインポートする」

不審オブジェクトリストエクスポート/インポートツールユーザガイド

Trend Micro Control Manager™の不審オブジェクトリストエクスポート/インポートツールでは、Control Manager の不審オブジェクトリストをエクスポートおよびインポートできます。Control Manager 管理コンソールにサインインする必要はありません。

- 不審オブジェクトリストエクスポートツール: 不審オブジェクトリストを Control Manager サーバから複数のファイル形式でエクスポートします。
- 不審オブジェクトリストインポートツール: 適切な形式のコンマ区切り値 (CSV) の不審オブジェクトデータを Control Manager にインポートします。

エクスポート/インポートツールを使用して、不審オブジェクトデータを複数の Control Manager サーバや他社製アプリケーションで活用することにより、未知の脅威や発生しつつある脅威に対する保護を強化します。

不審オブジェクトリストエクスポートツールを使用する (SuspiciousObjectExporter.exe)

Control Manager 不審オブジェクトリストを複数のファイル形式でエクスポートするには、不審オブジェクトリストエクスポートツール (`SuspiciousObjectExporter.exe`) を使用します。初期設定では、不審オブジェクトリストエクスポートツールは不審オブジェクトデータを XML 形式でエクスポートします。

出力ファイル形式を変更する方法の詳細については、60 ページの「設定ファイルを変更する」を参照してください。

重要

不審オブジェクトエクスポートツールは、Control Manager7.0 以降で使用できます。

最新のインストールパッケージをダウンロードするには、http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp を参照してください。

手順

1. Control Manager サーバでコマンドプロンプトを開きます。
2. 次のコマンドを使用して、SuspiciousObjectExporter.exe ファイルが含まれるディレクトリを見つけます。

   ```
   cd <Control Manager インストールディレクトリ>\SOTools
   ```

3. 次のコマンドを使用して、SuspiciousObjectExporter.exe を実行します。

   ```
   SuspiciousObjectExporter.exe [/s <開始 ID> /e <終了 ID>] [/f
   <y | n>] [/d]
   ```

   注意

   パラメータなしで SuspiciousObjectExporter.exe を実行すると、詳細な使用方法が表示され、<開始 ID>と<終了 ID>の値を指定するように要求されます。

パラメータ	説明	例
/s <開始 ID>	エクスポートする最初のオブジェクトの ID を指定します。 **注意** • /e <終了 ID> 値を指定する必要があります。 • 値に 0 を指定するとリストの先頭を示します。	• `SuspiciousObjectExporter.exe /s 0 /e 0` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 3 /e 8` ID 3 から ID 8 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 0 /e 4` リストの先頭から ID 4 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。

パラメータ	説明	例
/e <終了 ID>	エクスポートする最後のオブジェクトの ID を指定します。 注意 • /s <開始 ID> 値を指定する必要があります。 • 値に 0 を指定するとリストの末尾を示します。	• `SuspiciousObjectExporter.exe /s 0 /e 0` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 3 /e 8` ID 3 から ID 8 までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 4 /e 0` ID 4 からリストの末尾までの不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。

パラメータ	説明	例
/f <y | n>	エクスポート処理中にコマンドラインインタフェースをロックするかどうかを指定します。 **注意** オプションのパラメータです。指定しない場合の初期設定は「yes」です。 **重要** `SuspiciousObjectExporter.exe` ツール、PowerShell スクリプト、または Windows タスクスケジューラのバッチスクリプトを使用して自動エクスポートを予約する場合は、[引数の追加 (オプション)] フィールドで次のパラメータを指定する必要があります。 `/f n`	• `SuspiciousObjectExporter.exe /f y` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /s 0 /e 0 /f y` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロックします。 • `SuspiciousObjectExporter.exe /f n` すべての不審オブジェクトをエクスポートし、エクスポート処理中はコマンドラインインタフェースをロック解除します。
/d	デバッグモードを有効にします。 **注意** サポートセンターから指示があった場合にのみ使用してください。	`SuspiciousObjectExporter.exe /d` すべての不審オブジェクトをエクスポートし、デバッグログを出力します。

4. エクスポートされた不審オブジェクトリストを確認するには、**<現在のディレクトリ>**`¥SOTools¥`ディレクトリに移動し、`SuspiciousObjectList.xml` ファイルを開きます。

注意

この手順は、<**現在のディレクトリ**>が<Control Manager **インストールディレクトリ**>であることを前提としています。

5. すべてのエクスポートログを確認するには、<**現在のディレクトリ**>¥SOTools¥ディレクトリに移動し、ExportRecord.txt ファイルを開きます。

注意

この手順は、<**現在のディレクトリ**>が<Control Manager **インストールディレクトリ**>であることを前提としています。

設定ファイルを変更する

不審オブジェクトリストインポートツールの初期設定の設定ファイルを変更するには、<Control Manager **インストールディレクトリ**>¥SOTools ディレクトリにある SuspiciousObjectExporter.exe.config ファイルを変更します。

ヒント

設定ファイルを変更する前にバックアップファイルを作成することをお勧めします。

キー	説明	例
outputRootFolderPath 場所: <appSettings>	SuspiciousObjectExporter.exe ツールの作業ディレクトリを指定します。	• <add key="outputRootFolderPath" value="."/> SuspiciousObjectExporter.exe プログラムが存在するディレクトリを使用してリストを処理します。 • <add key="outputRootFolderPath" value="C:\Program Files (x86)\Trend Micro\Control Manager"/> 指定したディレクトリ (C:¥Program Files (x86)¥Trend Micro¥Control Manager) を使用してリストを処理します。
outputFolderName 場所: <appSettings>	エクスポートする不審オブジェクトリストの出力ディレクトリを指定します。	• <add key="outputFolderName" value="SOTools"/> ファイルを<outputRootFolderPath>¥SOTools ディレクトリにエクスポートします。 • <add key="outputFolderName" value="SOList"/> ファイルを<outputRootFolderPath>¥SOList ディレクトリにエクスポートします。

キー	説明	例
styleSheetFile 場所: <appSettings>	エクスポートするリストに適用するスタイルシートを指定します。	• <add key="styleSheetFile" value=""/> outputFile キーで指定した*.txt または *.xml ファイルに、すべてのリストを XML 形式でエクスポートします。 • <add key="styleSheetFile" value="ExportCSV.xslt"/> 仮想アナライザで検出された不審オブジェクトリスト、ユーザ指定の不審オブジェクトリスト、または除外リストについて、列のサブセットを CSV 形式でエクスポートします。 重要 ExportCSV.xslt スタイルシートを選択すると、このツールでエクスポートする列を設定できなくなります。スタイルシートで指定した列のみがエクスポートされます。 • <add key="styleSheetFile" value="ExportSTIX.xslt"/> すべての不審オブジェクトリストを STIX 形式でエクスポートします。 • <add key="styleSheetFile" value="ExportCPL.xslt"/> すべての不審オブジェクトリストを CPL 形式でエクスポートします。 重要 スタイルシートを指定する場合は、defaultSampleTemplates キーに同じ値を設定する必要があります。

キー	説明	例
outputFile 場所: <appSettings>	エクスポートする不審オブジェクトリストのファイル名と拡張子を指定します。 出力ファイル形式を変更するには、新しいファイル拡張子を指定します。	• <add key="outputFile" value="SuspiciousObjectList.xml"/> 不審オブジェクトリストを SuspiciousObjectList.xml という名前の *.xml ファイルとしてエクスポートします。 • <add key="outputFile" value="SuspiciousObjectList.txt"/> 不審オブジェクトリストを SuspiciousObjectList.txt という名前の *.txt ファイルとしてエクスポートします。
defaultSampleTemplates 場所: <appSettings>	エクスポートするリストに適用するスタイルシートのソースファイルを指定します。	• <add key="defaultSampleTemplates" value="ExportCSV.xslt"/> 指定したスタイルシートファイルの場所を特定します。 **重要** 指定する値は、styleSheetFile キーまたは defaultSampleTemplates キー用に指定した値と一致する必要があります。 **注意** 初期設定値は"ExportCPL.xslt|ExportSTIX.xslt|ExportCSV.xslt"です。

キー	説明	例
<suspiciousObjectColumns> 場所: <soDataColumnSettings>	選択したリストのデータ列を指定します。 isEnable="true"に設定すると、指定したデータ列をエクスポートします。	• <add id="1" name="SeqID" isEnable="true"></add> 選択したリストから「SeqID」データ列をエクスポートします。 • <add id="1" name="MD5Key" isEnable="false"></add> 選択したリストから「MD5Key」データ列を明示的に除外します。 重要 「ExportCSV.xslt」スタイルシートを指定した場合、スタイルシートで指定した列のみがエクスポートされます。
<suspiciousObjectTypeList> 場所: <soTypeSettings>	選択したリストからエクスポートするオブジェクトの種類を指定します。 isEnable="true"に設定すると、指定したオブジェクトの種類をエクスポートします。	• <add value="0" description="IP" isEnable="true"></add> 選択したリストからすべての IP アドレスのオブジェクトをエクスポートします。 • <add value="1" description="Domain" isEnable="false"></add> エクスポートするリストからすべての「Domain」オブジェクトを明示的に除外します。

キー	説明	例
<suspiciousObjectSourceType> 場所: <soTypeSettings>	不審オブジェクトのソースの種類を指定します。 isEnable="true"に設定すると、指定したオブジェクトの種類をエクスポートします。	• <add value="0" description="SourceType" isEnable="true"/> 仮想アナライザの不審オブジェクトリストを選択します。 • <add value="1" description="SourceType" isEnable="true"/> ユーザ指定の不審オブジェクトリストを選択します。 • <add value="2" description="SourceType" isEnable="true"/> 仮想アナライザの除外リストを選択します。 重要 • ExportCSV.xslt スタイルシートを指定し、仮想アナライザで検出された不審オブジェクトリストまたはユーザ指定の不審オブジェクトリストを選択した場合、エクスポートされる列は [オブジェクト]、[種類]、[Scan Prefilter]、[メモ]、および [検出時の処理] です。 • ExportCSV.xslt スタイルシートを指定し、仮想アナライザの除外リストを選択した場合、エクスポートされる列は [オブジェクト]、[種類]、[Scan Prefilter]、および [メモ] です。

Control Manager を使用して仮想アナライザ不審オブジェクトの除外リストをエクスポートする

重要

Control Manager では、CSV 形式でのみ仮想アナライザで検出された不審オブジェクト除外リストをエクスポートできます。

手順

1. [運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。

   [仮想アナライザで検出された不審オブジェクト] 画面が表示されます。

2. [除外] タブをクリックします。

3. [すべてエクスポート] をクリックします。

   進行状況の画面が表示されます。

4. エクスポートが完了したら、[ダウンロード] をクリックします。

   確認ボックスが表示されます。

5. [保存] をクリックします。

   [名前を付けて保存] 画面が表示されます。

6. (オプション) 新しい場所またはファイル名を指定します。

7. [保存] をクリックします。

Control Manager を使用してユーザ指定リストをエクスポートする

重要

Control Manager では、CSV 形式でのみユーザ指定の不審オブジェクトリストをエクスポートできます。

手順

1. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [すべてエクスポート] をクリックします。

   進行状況の画面が表示されます。

3. エクスポートが完了したら、[ダウンロード] をクリックします。

   確認ボックスが表示されます。

4. [保存] をクリックします。

   [名前を付けて保存] 画面が表示されます。

5. (オプション) 新しい場所またはファイル名を指定します。

6. [保存] をクリックします。

不審オブジェクトリストインポートツールを使用する (ImportSOFromCSV.exe)

適切な形式の不審オブジェクトデータファイル (`*.csv`) を Control Manager にインポートするには、不審オブジェクトリストインポートツール (`ImportSOFromCSV.exe`) を使用します。

重要

不審オブジェクトインポートツールは、Control Manager7.0 以降で使用できます。

最新の Control Manager インストールパッケージをダウンロードするには、http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp を参照してください。

手順

1. Control Manager サーバでコマンドプロンプトを開きます。

2. 次のコマンドを使用して、`ImportSOFromCSV.exe` ファイルが含まれるディレクトリを見つけます。

   `cd <Control Manager インストールディレクトリ>`

3. 次のコマンドを使用して、ImportSOFromCSV.exe を実行します。

   ```
   ImportSOFromCSV.exe "<フルパス>" {UserDefinedSO |
   ExceptionSO}
   ```

   ここでは次を意味します。

   - <**フルパス**>: 適切な形式の CSV ファイルのディレクトリとファイル名を指定します。
   - {UserDefinedSO}: ユーザ指定の不審オブジェクトリストデータが含まれるファイルを指定します。
   - {ExceptionSO}: 仮想アナライザ不審オブジェクトの除外リストデータが含まれるファイルを指定します。

   例:

   - ```
     SuspiciousObjectImporter.exe "c:\Program Files
     (x86)\Trend Micro\Control Manager
     \importExceptionSample.csv" ExceptionSO
     ```

     importExceptionSample.csv ファイルを c:¥Program Files (x86)¥Trend Micro¥Control Manager ディレクトリから Control Manager の仮想アナライザ不審オブジェクトの除外リストにインポートします。

Control Manager を使用して仮想アナライザ不審オブジェクトの除外リストをインポートする

重要

Control Manager でインポートできる仮想アナライザ不審オブジェクトの除外リストデータは、適切な形式の*.csv ファイルのみです。

手順

1. [運用管理] > [不審オブジェクト] > [仮想アナライザオブジェクト] に移動します。
     ```

[仮想アナライザで検出された不審オブジェクト] 画面が表示されます。

2. [除外] タブをクリックします。
3. [インポート] をクリックします。

   [除外設定のインポート] 画面が表示されます。
4. [参照] をクリックし、除外リストデータが含まれる*.csv ファイルを選択します。

   ヒント

   サンプル CSV のダウンロードリンクをクリックすると、詳細な手順が記載された*.csv ファイルをダウンロードできます。
5. [開く] をクリックします。
6. [インポート] をクリックします。

   [除外設定のインポート] 画面が閉じられ、インポートした除外設定が仮想アナライザで検出された不審オブジェクト除外リストに表示されます。

Control Manager を使用してユーザ指定リストをインポートする

重要

Control Manager でインポートできるユーザ指定の不審オブジェクトデータは、適切な形式の*.csv ファイルのみです。

手順

1. [運用管理] > [不審オブジェクト] > [ユーザ定義オブジェクト] に移動します。

   [ユーザ指定の不審オブジェクト] 画面が表示されます。

2. [インポート] をクリックします。

   [ユーザ指定リストのインポート] 画面が表示されます。

3. [参照] をクリックし、ユーザ指定の不審オブジェクトデータが含まれる *.csv ファイルを選択します。

   ヒント

   サンプル CSV のダウンロードリンクをクリックすると、詳細な手順が記載された*.csv ファイルをダウンロードできます。

4. [開く] をクリックします。

5. [インポート] をクリックします。

   [ユーザ指定リストのインポート] 画面が閉じられ、インポートしたオブジェクトがユーザ指定の不審オブジェクトリストに表示されます。

第 3 章

不審オブジェクトハブおよびノードの Control Manager アーキテクチャ

本章では、管理者が、不審オブジェクトリストを複数の Control Manager サーバ間で同期するために必要な情報について説明します。

次のトピックがあります。

不審オブジェクトハブおよびノードの Control Manager アーキテクチャ

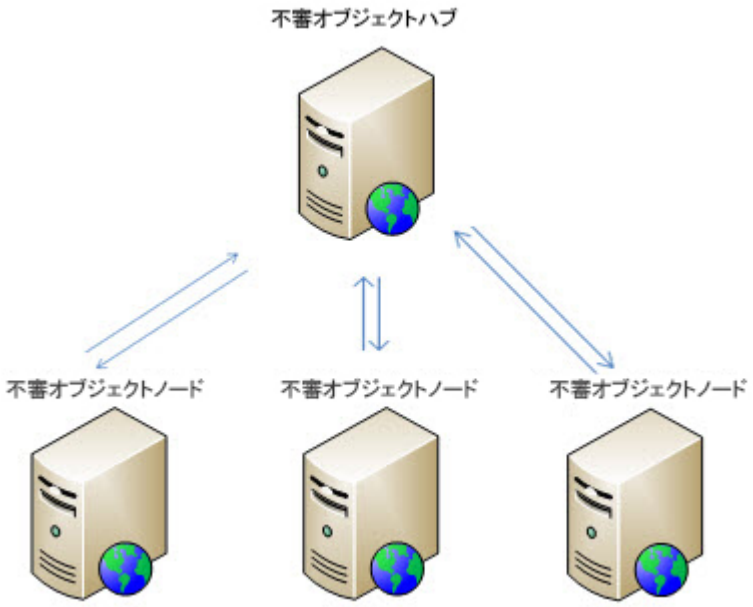
Trend Micro Control Manager™の不審オブジェクトハブおよびノードのアーキテクチャにより、不審オブジェクトリストを複数の Control Manager サーバ間で同期できます。ハブ Control Manager サーバの不審オブジェクトリストは、すべてのノード Control Manager サーバとそれらのサーバに登録されているその他の管理下の製品からの不審オブジェクトリストを統合して、そのリストをノード Control Manager サーバに配信します。

管理者は、不審オブジェクトハブ Control Manager サーバを設定しておく必要があります。また、環境によっては、他の Control Manager サーバを不審オブジェクトノードサーバとして動作するように割り当てる必要もあります。Trend Micro Deep Discovery 製品は、不審オブジェクトハブまたはノード Control Manager サーバに登録できます。このアーキテクチャでは、不審オブジェクトに対するすべての処理を不審オブジェクトハブ Control Manager サーバコンソールから設定する必要があります。

重要

すべてのノード Control Manager サーバが適切に同期され続けるように、不審オブジェクトリストに対するすべての操作は、不審オブジェクトハブ Control Manager から実行する必要があります。

不審オブジェクトノード Control Manager から不審オブジェクトに対して実行した検索処理は、接続されたすべてのサーバに同期されるとは限りません。



不審オブジェクトハブとノードを設定する

手順

1. 不審オブジェクトハブ用の Control Manager のサーバコンソールにログオンします。
2. [運用管理] > [不審オブジェクト] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。
3. [管理下の製品] タブをクリックして、次の設定をメモします。
   - サービス URL
   - API キー

4. 不審オブジェクトノードの Control Manager サーバコンソールにログオンします。
5. [運用管理] > [不審オブジェクト] > [配信設定] に移動します。

   [配信設定] 画面が表示されます。
6. [不審オブジェクトハブ Control Manager] タブで、不審オブジェクトハブ用の Control Manager でメモした内容を入力します。
   - サービス URL
   - API キー
7. [登録] をクリックします。

   確認ダイアログが表示され、サーバが不審オブジェクトハブ Control Manager に正常に登録されたことを示すメッセージが示されます。
8. 各不審オブジェクトノードの Control Manager サーバに対してこの処理を繰り返します。
9. 初期設定の同期間隔を設定するには、次の手順を実行します。
   a. [同期頻度] ドロップダウンから期間を選択します。
   b. [保存] をクリックします。

不審オブジェクトハブ Control Manager から不審オブジェクトノードを登録解除する

注意

ノードの Control Manager サーバを登録解除した後も、以前に同期されたすべてのオブジェクトがノードの Control Manager サーバの不審オブジェクトリストに残ります。

手順

1. 不審オブジェクトノードの Control Manager サーバコンソールにログオンします。
2. [運用管理] > [不審オブジェクト] > [配信設定] に移動します。
3. [不審オブジェクトハブ Control Manager の設定] セクションで、[登録解除] をクリックします。

   確認ダイアログが表示され、サーバが不審オブジェクトハブ Control Manager から正常に登録解除されたことを示すメッセージが示されます。
4. 複数のノード Control Manager サーバが存在する場合は、各サーバで同様の手順を繰り返してください。

設定に関する補足

不審オブジェクトハブの設定と不審オブジェクトノードの Control Manager サーバの登録が正常に終了したら、次の設定情報に注意してください。

注意

ノードの Control Manager サーバを登録解除した後も、以前に同期されたすべてのオブジェクトがノードの Control Manager サーバの不審オブジェクトリストに残ります。

設定	不審オブジェクトハブ CONTROL MANAGER	ノードの CONTROL MANAGER
同期間隔	該当なし	5 分 (初期設定)

<table>
<tr><th>設定</th><th>不審オブジェクトハブ
Control Manager</th><th>ノードの Control Manager</th></tr>
<tr><td rowspan="2">不審オブジェクトリストの同期</td><td>不審オブジェクトハブ Control Manager からノード:
• 仮想アナライザリスト
• ユーザ指定リスト</td><td>ノードの Control Manager からハブ:
• 仮想アナライザリスト</td></tr>
<tr><td colspan="2">注意
• ハブの Control Manager サーバは、ユーザ指定リストまたは除外リストの [メモ] 列のデータをノードの Control Manager サーバにデータを送信しません。
• リストを同期する際に、ユーザ指定リストは仮想アナライザリストよりも優先されます。
• 次回の同期の前にオブジェクトが不審オブジェクトハブ Control Manager のユーザ指定リストと仮想アナライザリストの両方に追加される場合、不審オブジェクトハブ Control Manager サーバは両方のリストをノードの Control Manager サーバに配信します。
• ノードの Control Manager の仮想アナライザリストに含まれるオブジェクトが不審オブジェクトハブ Control Manager のユーザ指定リストにも存在する場合、ノードの Control Manager の仮想アナライザリストでの不審オブジェクトのリスクレベルは次回の同期中に [高] に変わります。
• 移行済みの Control Manager 6.0 のインストールから除外リストの自動同期を実行するには、移行前に Control Manager 6.0 サーバで不審オブジェクトハブおよびノードの Control Manager アーキテクチャを有効にしておく必要があります。
• Control Manager 7.0 では、Control Manager 6.0 から移行された不審オブジェクトハブおよびノードのアーキテクチャが保持されます。
• Control Manager 6.0 サーバの移行前に不審オブジェクトハブおよびノードの Control Manager アーキテクチャを有効にするには、<code>SystemConfiguration.xml</code> ファイルで <code>m_iTmcmSoDist_ForceSyncWhitelist</code> タグを検索し、値を「1」に変更します。</td></tr>
</table>

設定	不審オブジェクトハブ Control Manager	ノードの Control Manager
不審オブジェクトの設定	不審オブジェクトハブ Control Manager から不審オブジェクトを設定すると、登録済みのノードの Control Manager サーバ全体で一貫性が確保されます。	**重要** ノードの Control Manager サーバですべての不審オブジェクトリストを同期の取れた状態にしておくには、ノードの Control Manager サーバコンソールから不審オブジェクトリストに対して何の処理も実行しないでください (たとえば、オブジェクトの [追加] や [期限切れにする] など)。

索引