Trend Micro Portable Security™ 3.0

ユーザガイド

Endpoint Security

※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。
  https://success.trendmicro.com/jp/solution/000207383

P/N: TPEM39285_210610_JP (2021/06)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Trend Micro Portable Security により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Trend Micro Portable Security における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

第 4 章：検索ツール画面を使用する

第 5 章：Linux コンピュータを検索する

第 6 章：追加のツール

第 7 章：テクニカルサポート

第 1 章

はじめに

この章では、Trend Micro Portable Security およびその機能について説明します。

Trend Micro Portable Security

Trend Micro Portable Security は、高性能でコスト効率の高いセキュリティサービスを提供し、インターネットに接続していない、またはウイルス対策ソフトをインストールできないコンピュータからウイルスを検索して駆除することにより、企業をセキュリティ上の脅威から保護します。

USB メモリ型の検索ツールを使用することで、ウイルス対策ソフトをインストールすることなく、コンピュータから簡単にウイルスを検出して駆除できます。また、すべてのアップデート、検索設定、および検索ツールにより生成されたログは管理プログラムで集中的に管理することが可能です。

多くのウイルス対策プログラムは、コンピュータごとにインストールされ、最新コンポーネントをダウンロードするためにインターネットに接続する必要があります。Trend Micro Portable Security では、ウイルス対策ソフトが搭載された USB メモリ型の検索ツールを接続するだけで、コンピュータから簡単にウイルスを検索して駆除できます。

Trend Micro Portable Security は、次の 2 つの主要なコンポーネントで構成されています。

- 管理プログラム: 検索ツールを管理します。
- 検索ツール: 管理プログラムに登録して使用することも、スタントアロンモードで使用することもできます。検索ツールを使用すれば、ウイルス対策ソフトをインストールする必要はありません。

管理プログラム

管理プログラムでは、検索設定を行ったり、複数の検索ツールからログデータをインポートしたりするなどの処理を実行できます。

管理プログラムでは次の操作を実行できます。

- パターンファイルや検索エンジンなどのコンポーネントのアップデートと登録済み検索ツールへの配信
- ウイルス検索の設定や登録済み検索ツールとの同期
- 指定されたファイル、フォルダ、および拡張子の検索除外

- 検索時に生成されるログデータのインポートや管理
- 管理者のアカウントとパスワードを設定して管理者権限のないアカウントでの検索を可能にする

検索ツール (USB メモリ型)

接続したコンピュータのウイルス検索を行い、ウイルスが検出された場合は駆除、隔離などの処理を行います。検索結果は検索ツールにログデータとして保存されます。

注意

- 検索ツールが開始されない場合は、Windows エクスプローラで [TMPS3 SYS] ドライブ内にある Launcher.exe をダブルクリックします。
- 検索ツール画面は Windows コンピュータでのみ使用できます。

検索ツールは独自の画面を起動します。ただし、画面に表示される機能は選択するモードによって異なります。集中管理モードとスタンドアロンモードのいずれかを選択できます。

11 ページの「集中管理モード」を参照してください。

注意

アクティベーション後にモードを変更するには、USB デバイスのリセットをする必要があるため、適切なモードを選択するよう確認してください。

詳細については、80 ページの「デバイスのリセット」を参照してください。

表 1-1. 検索ツールのモード

	集中管理モード	スタンドアロンモード
アップデート方法	トレンドマイクロのアップデートサーバや指定したアップデート元から特定のコンポーネントをダウンロードするだけでなく、管理プログラムからコンポーネントをアップデートすることもできます。	トレンドマイクロのアップデートサーバ、インターネットに接続している任意のコンピュータ、または指定したアップデート元から最新のコンポーネントをダウンロードします。
検索設定	管理プログラムの検索設定を使用するか、検索ツールから設定します。	検索ツール画面から検索設定を直接変更します。
ログ	• 管理プログラムからのエクスポートが可能です。 • 検索ツールからのインポートが可能です。	コンピュータでインポートまたはエクスポートします。

注意

管理用コンピュータのセキュリティ対策には、「ウイルスバスター コーポレートエディション」などのセキュリティソフトを使用してください。

セキュリティの脅威の検索中、コンピュータに一時ファイルが作成される場合があります。これらのファイルは、検索ツールが実行中のプロセスを停止すると削除されます。一時ファイルを保存せずにコンピュータを検索することも可能です。

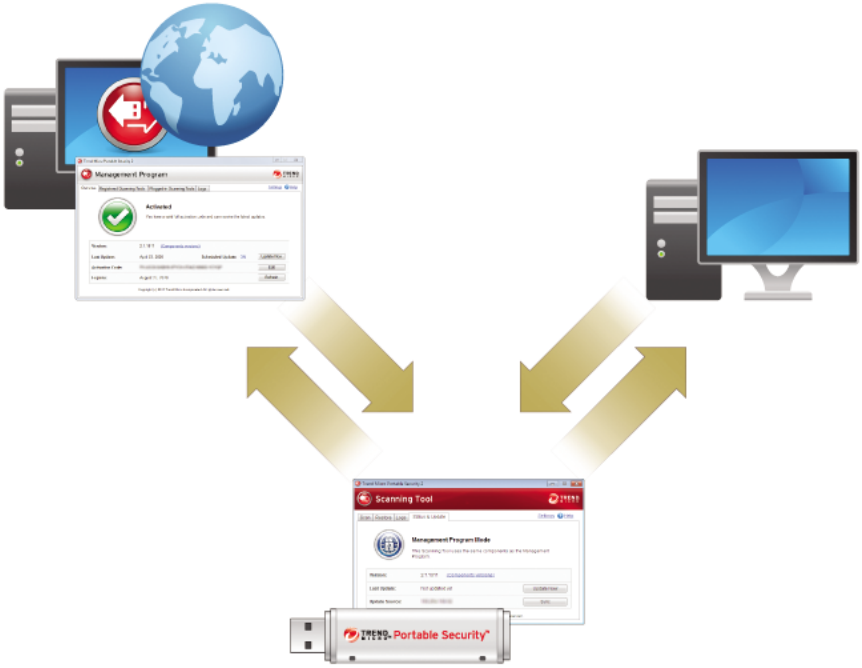
集中管理モード

管理プログラムを使用して複数の検索ツールを管理する場合は、このモードを選択します。管理プログラムでダウンロードした最新コンポーネントや検索設定を検索ツールへ同期したり、ログを管理したりすることができます。

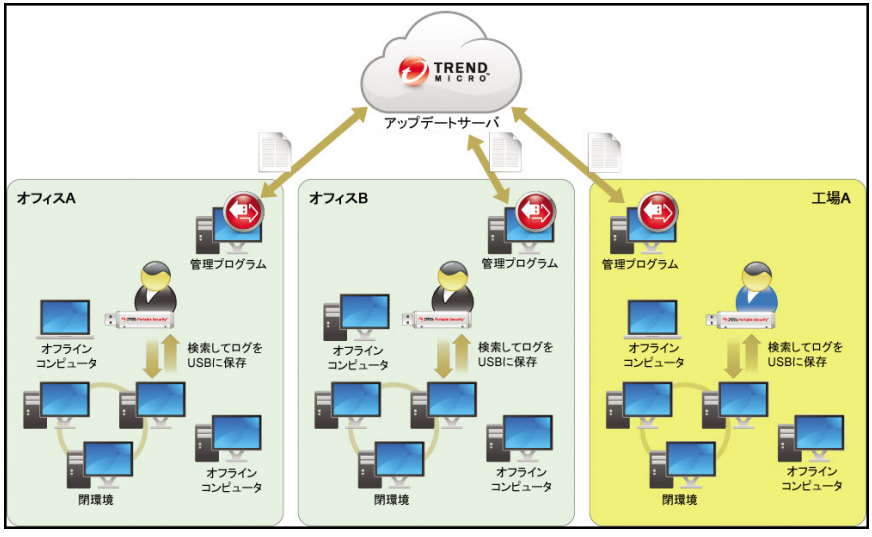
検索ツールを管理プログラムに接続する方法は 2 つあります。1 つは管理用コンピュータに直接接続する方法、もう 1 つはネットワークに接続されたコンピュータを介して管理用コンピュータにリモートで接続する方法です。

- 直接接続

検索ツールを管理用コンピュータに直接接続して、アップデートや設定を取得したりログを転送したりできます。



この方法は、すべてのコンピュータが 1 つの環境にまとまって配置されており、管理用コンピュータに直接接続できる場合に適しています。次に例を示します。

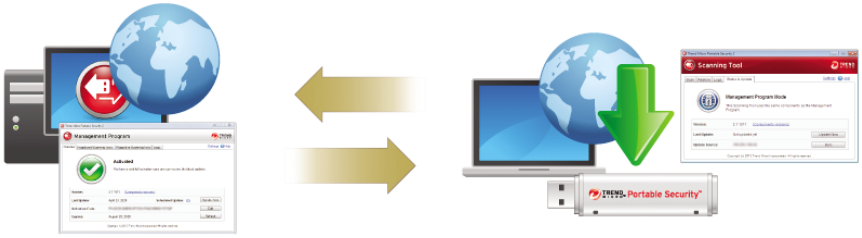


- リモート接続

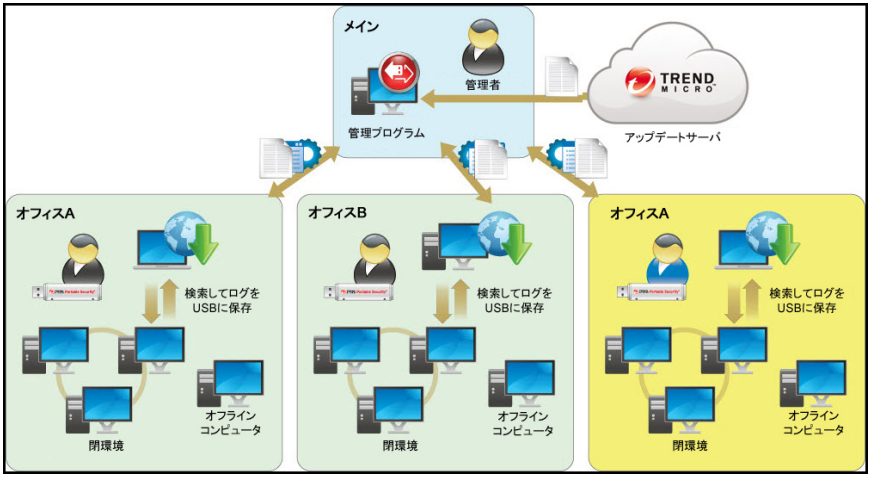
  インターネットに接続された任意のコンピュータを介して管理用コンピュータにリモートで接続し、アップデートや設定を取得したりログを転送したりできます。

注意

管理用コンピュータでファイアウォール製品をご利用の場合は、通信エラーが発生する可能性があります。通信エラーが発生する場合は、ファイアウォール製品の設定から `C:¥Program Files¥Trend Micro¥Portable Security 3¥SfSrvCom.exe` サービスに対する通信の許可設定を行ってください。



この方法は、検索対象となる環境が複数の場所に存在する場合に適しています。それぞれの場所でインターネットまたはネットワークに接続されたコンピュータを 1 台用意し、そのコンピュータを介して定期的に管理プログラムに接続します。次に例を示します。



スタンドアロンモード

管理プログラムを使用せずに検索ツール単体で使用する場合は、このモードを選択します。コンポーネントのアップデート、検索設定の変更、ログの確認を行うには、検索ツールが接続されたコンピュータがインターネットへ接続できる必要があります。

スタンドアロンモードは、最新コンポーネントのダウンロードや検索設定の変更を、管理プログラムを介さずに検索ツール単体で行いたい場合に適して

います。このモードでは、検索ツール画面から、検索ツールに対して任意の変更を実行できます。

注意

最新の脅威に対応できるように、コンピュータを検索する前にコンポーネントを定期的にアップデートすることをお勧めします。

新機能

Trend Micro Portable Security の新機能および機能拡張は次のとおりです。

機能	説明
Linux のサポート	次の OS を実行する Linux コンピュータの検索がサポートされます。 • Red Hat Enterprise Linux 6.0 以降 • CentOS 6.0 以降
資産情報の収集	システム統計やアプリケーションリストなど、検索ツールを接続するコンピュータに関する基本情報を収集できます。 **注意** • 資産情報のログをエクスポートするには、管理プログラムをインストールする必要があります。 • 資産情報を収集できるのは、アクティベーションを実行した検索ツールのみです。アクティベーションの実行後、検索ツールを取り外してから再度コンピュータに接続すると資産情報の収集が開始されます。 • 検索ツールでは、管理用コンピュータの資産情報を収集することはできません。
USB の機能拡張	検索ツールのストレージ容量が 16GB に拡張されます。

古いバージョンの Trend Micro Portable Security

Trend Micro Portable Security 3 の管理プログラムでは Trend Micro Portable Security 2 検索ツールは使用できません。Trend Micro Portable Security 2 検索ツールの使用を継続する場合は、Trend Micro Portable Security 2 管理プログラムを使用してください。

第 2 章

設定

検索ツールの使用を開始する前に、次の点に留意してください。

重要

初めてお使いになる場合は、検索ツールのアクティベーションを実行する必要があります。詳細については、24 ページの「集中管理モードで設定されている検索ツールのアクティベーションを実行する」を参照してください。

- お使いのユーザアカウントに管理者権限があれば、Trend Micro Portable Security を使用して対象端末を検索できます。
- ユーザアカウントに管理者権限がない場合は、[管理者として検索] オプションを有効にしてから、Windows エクスプローラを開き、[TMPS3 SYS] ドライブ内にある Launcher.exe をダブルクリックします。または、Launcher.exe を右クリックして、[管理者として実行] を選択してください。
- Portable Security は終了時に検索結果ログを検索ツール内に保存します。

管理プログラムをインストールする

管理プログラムは、すべての検索ツールのコンポーネント、設定、およびログを一元管理します。集中管理モードで設定されている検索ツールは、それぞれ離れた場所にあるコンピュータで使用できます。さらにローカルまたはリモートで管理プログラムにファイルをアップロードしたり、管理プログラムと設定を同期したりできます。

ヒント

古いバージョンの管理プログラムがインストールされているコンピュータに管理プログラムをインストールすることはお勧めしません。古い検索ツールが引き続きログを同期できるよう、管理プログラムは別のコンピュータにインストールしてください。

表 2-1. システム要件

項目	要件
ディスク容量	管理用コンピュータには 2GB 以上のディスク容量を確保することをお勧めします • 管理プログラム用に 700MB • ログファイル用に 1.3GB
権限	コンピュータに対する管理者権限が必要です

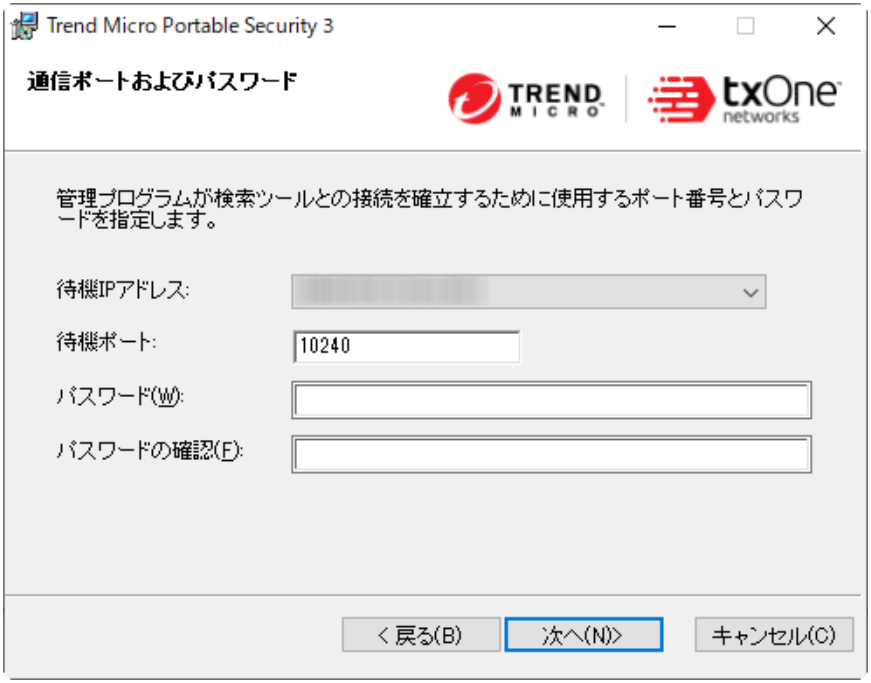
手順

1. 検索ツールを検索対象コンピュータに接続します。
2. Windows エクスプローラで `TMPS3 SYS¥MP` ディレクトリにある `MP_Install.exe` をダブルクリックします。
3. [使用許諾契約書] 画面が表示されたら、契約書を読み、[同意する] をクリックします。

4. [インストール先] 画面が表示されたら、パスを直接入力するか、フォルダを参照して、[次へ] をクリックします。

5. [アクティベーションコード] 画面が表示されたら、アクティベーションコードを指定し、[次へ] をクリックします。

6. [通信ポートおよびパスワード] 画面が表示されたら、管理用コンピュータの IP アドレスとポート番号を指定し、パスワードを作成します。



注意

管理用コンピュータでファイアウォール製品をご利用の場合は、ファイアウォール製品の設定から `C:¥Program Files¥Trend Micro¥Portable Security 3¥SfSrvCom.exe` サービスに対する通信の許可設定を行ってください。

7. [次へ] をクリックします。
8. [インストールが完了しました] 画面が表示されたら、[閉じる] をクリックします。

アクティベーション

検索ツールを接続した後、コンピュータの検索を開始する前に、動作モードを選択して検索ツールのアクティベーションを実行する必要があります。後から動作モードを (たとえばスタンドアロンモードから集中管理モードに) 変更する場合は、検索ツールを初期出荷状態にリセットする必要があります。

詳細については、82 ページの「USB デバイスを初期出荷状態にする」を参照してください。

重要

この機能は Windows コンピュータでのみ使用できます。

検索ツールの現在のアクティベーションステータスを確認するには、コンソールを開いて [ステータスとアップデート] タブに移動します。

管理プログラムの現在のアクティベーションステータスを確認するには、コンソールを開いて [概要] タブに移動します。

表 2-2. アクティベーションコードに関するアイコンとメッセージ

アイコン	メッセージ
	すでに有効化されているため、アクティベーションを実行する必要はありません。
	• 有効期限が近づいているため、サポート契約を更新する必要があります。
	• 有効化されていません。製品を使用するにはアクティベーションを実行する必要があります。 • 有効期限が切れています。製品を継続して使用される場合は、新しいアクティベーションコードを入手するか、サポート契約を更新してください。

ヒント

検索ツールを常に最新の状態でお使いいただくためにも、有効期限が切れる前にライセンスを更新されることをお勧めします。

集中管理モードで設定されている検索ツールのアクティベーションを実行する

集中管理モードで設定されている検索ツールは、管理プログラムに登録されています。各検索ツールは検索設定を同期し、管理プログラムから最新のコンポーネントをダウンロードできます。また、各検索ツールから管理プログラムに最新のコンポーネントをアップロードすることもできます。

手順

- オプション 1: 管理プログラム経由で行うアクティベーション

1. 管理プログラムをインストールします。
2. 新規の検索ツールまたはまだアクティベーションが実行されていない任意の検索ツールを同じコンピュータに接続します。検索ツールは自動的に有効化され、管理プログラムに登録されます。

- オプション 2: 検索ツールから直接行うアクティベーション

1. 新規の検索ツールまたはまだアクティベーションが実行されていない任意の検索ツールを、管理用コンピュータに接続します。

注意

管理用コンピュータでファイアウォール製品をご利用の場合は、ファイアウォール製品の設定から `C:¥Program Files¥Trend Micro ¥Portable Security 3¥SfSrvCom.exe` サービスに対する通信の許可設定を行ってください。

[検索ツールの初期設定] 画面が開きます。

注意

画面が開かない場合は、セキュリティソフトウェアまたはコンピュータが autorun プロセスをブロックしている可能性があります。Windows エクスプローラでドライブ内の `[TMPS3 SYS]` を開き `Launcher.exe` をダブルクリックします。

2. [集中管理モード] を選択して、[次へ] をクリックします。

   [管理プログラムとプロキシの設定] 画面が開きます。

3. 以下を指定します。
   - 検索ツール名
   - 管理プログラムのアドレス、ポート、およびパスワード
   - (オプション)プロキシサーバ
4. [有効にする] をクリックします。

5. (オプション) [ステータスとアップデート] タブに移動し、[アップデート] をクリックして最新のコンポーネントを取得します。

スタンドアロンモードで設定されている検索ツールのアクティベーションを実行する

スタンドアロンモードで設定されている検索ツールは、管理プログラムから独立しているため、検索エンジンやパターンファイルをインターネットから直接アップデートできます。

重要

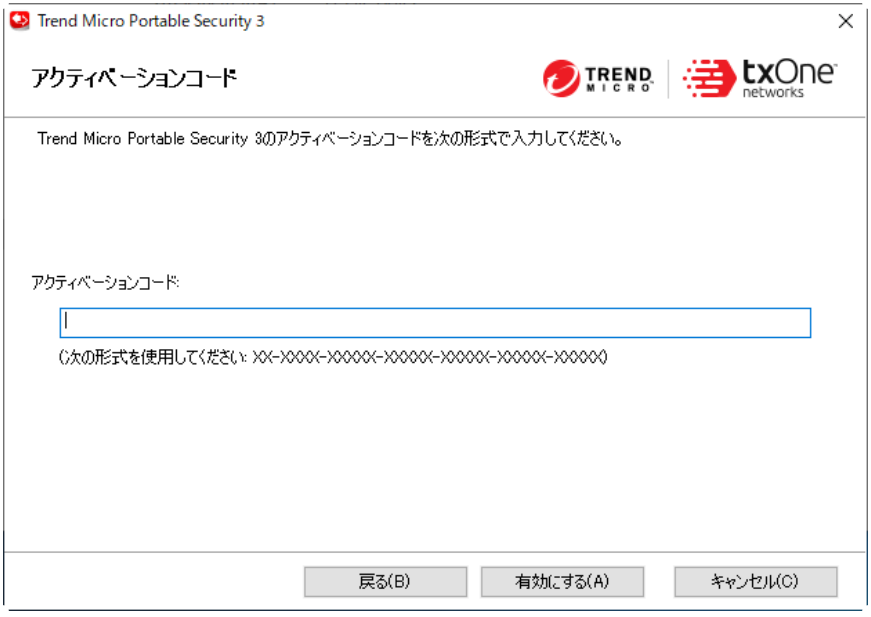
この機能は Windows コンピュータでのみ使用できます。

手順

1. 新規の検索ツールまたはまだアクティベーションが実行されていない任意の検索ツールをコンピュータに接続します。
2. Windows エクスプローラで [TMPS3 SYS] ドライブ内にある Launcher.exe をダブルクリックします。

3. [スタンドアロンモード] を選択して、[次へ] をクリックします。

4. [使用許諾契約書] 画面が表示されたら、契約書を読み、[同意する] をクリックします。



5. アクティベーションコードを入力して、[有効にする] をクリックします。

   検索ツール画面が開きます。

> **注意**
>
> ライセンスを有効化するかプログラムをアップグレードしたら、ただちにすべてのコンポーネントをアップデートすることをお勧めします。[ステータスとアップデート] タブに移動し、[アップデート] をクリックします。

アクティベーションコードを変更する

[有効期限] にアクティベーションコードの有効期限が日付で表示されます。サポート契約を更新した場合は、[更新] をクリックして有効期限を更新するか、[編集] をクリックしてアクティベーションコードを変更します。

詳細については、23 ページの「アクティベーション」を参照してください。

手順

1. 検索ツールのモードに応じた正しい画面を開きます。

   a. 集中管理モードで設定されている検索ツールの場合は、管理プログラムを開きます。

   b. スタンドアロンモードで設定されている検索ツールの場合は、検索ツール画面を開いて [ステータスとアップデート] タブをクリックします。

2. [編集] をクリックします。
3. 新しいアクティベーションコードを入力します。
4. [OK] をクリックします。

アップグレード

トレンドマイクロでは、Trend Micro Portable Security の機能を拡充し、パフォーマンスを向上させるためのアップデートを定期的にリリースしています。

注意

Portable Security では、古いバージョンからのアップグレードはサポートされません。

詳細については、16 ページの「古いバージョンの Trend Micro Portable Security」を参照してください。

ライセンスを有効化するかプログラムをアップグレードしたら、ただちにすべてのコンポーネントをアップデートすることをお勧めします。[ステータスとアップデート] タブに移動し、[アップデート] をクリックします。

管理プログラムをアップグレードする

トレンドマイクロでは、Trend Micro Portable Security の機能を拡充し、パフォーマンスを向上させるためのアップデートを定期的にリリースしています。

注意

- Portable Security では、古いバージョンの Trend Micro Portable Security からのアップグレードはサポートされません。

  詳細については、16 ページの「古いバージョンの Trend Micro Portable Security」を参照してください。

- アップグレード時に一時的に使用するため、管理用コンピュータに 2.3GB 以上の空き容量があることを確認します。

手順

1. セットアップパッケージをダウンロードしてダブルクリックします。[使用許諾契約書] 画面が表示されます。
2. 契約書を読み、[同意する] を選択します。
3. アップグレードが完了したら、[閉じる] をクリックします。

検索ツールをアップグレードする

トレンドマイクロでは、Trend Micro Portable Security の機能を拡充し、パフォーマンスを向上させるためのアップデートを定期的にリリースしています。

ライセンスを有効化するかプログラムをアップグレードしたら、ただちにすべてのコンポーネントをアップデートすることをお勧めします。[ステータスとアップデート] タブに移動し、[アップデート] をクリックします。

注意

Portable Security では、古いバージョンからのアップグレードはサポートされません。

手順

- 管理プログラムとの同期によるアップグレード
  a. 管理プログラムをアップグレードします。
  b. 検索ツールを管理用コンピュータに直接接続するか、インターネットを介してリモートで接続します。
  c. [検索ツール] から検索ツールを選択し、[コンポーネントと検索設定の同期] をクリックします。
- サポートツールを使用したアップグレード
  a. 開いている場合は検索ツール画面を閉じます。
  b. 管理者権限のあるアカウントを使用してコンピュータにログオンし、検索ツールを接続します。
  c. Trend Micro Portable Security の Service Pack をダウンロードします。
  d. 検索ツールを接続したコンピュータ上のローカルフォルダに Service Pack の内容を抽出します。
  e. [TMPS3 SYS] ドライブで、SupportTool フォルダを USB デバイスからローカルディスクにコピーします。
  f. 該当する Win32 または x64 フォルダで、TMPSSuprt.exe ファイル () をダブルクリックします。
  g. [他の機能] タブに移動します。
  h. [アップデートの適用] をクリックします。
  i. [修正モジュールを適用] を選択して、[次へ] をクリックします。[新しいコンポーネントの適用] 画面が開きます。

j. [参照] をクリックし、トレンドマイクロにより提供された Service Pack から.bin ファイルを選択します。

k. [適用] をクリックします。確認画面が表示されます。

第 3 章

管理プログラムを使用する

この章では、管理プログラムの使用方法と設定について説明します。

管理プログラム画面について

管理プログラム画面は、タブ付きの画面と、検索ツールの設定、ログの収集と表示、画面の管理へのリンクで構成されています。

表 3-1. 画面の使用方法

表示項目	説明
概要	必要に応じて、コンポーネントのステータスを確認したりアップデートを実行したりできます 詳細については、36 ページの「[概要] タブ」を参照してください。
登録済み検索ツール	この管理プログラムで管理している、すべての登録済み検索ツールの検索設定を行います 詳細については、41 ページの「[登録済み検索ツール] タブ」を参照してください。
現在接続中の検索ツール	管理用コンピュータに現在接続されている検索ツールのステータスを確認できます 詳細については、47 ページの「[現在接続中の検索ツール] タブ」を参照してください。
ログとレポート	検索ツールで以前に実行した検索の結果を確認できます 詳細については、48 ページの「[ログとレポート] タブ」を参照してください。
設定	管理プログラムの設定を確認または変更します 詳細については、49 ページの「管理プログラムの設定」を参照してください。
ヘルプ	ユーザガイドへのリンクを表示します

[概要] タブ

管理プログラムのステータスが表示されます。この画面からプログラムの設定を変更できます。

項目	説明
バージョン	Trend Micro Portable Security 管理プログラムのビルド番号 コンポーネントの詳細と最新のアップデート日時を確認するには、[コンポーネントバージョン] リンクをクリックしてください。 詳細については、38 ページの「最新のコンポーネントを確認する」を参照してください。
前回のアップデート	前回のコンポーネントアップデートの日付 • 予約アップデート: 設定したスケジュールで管理プログラムのコンポーネントを自動的にアップデートできます 詳細については、40 ページの「予約アップデート」を参照してください。 • アップデート: 管理プログラムのコンポーネントを手動でアップデートする場合にクリックします
アクティベーションコード	管理プログラムと検索ツールによって現在使用されているアクティベーションコード • 編集: アクティベーションコードを変更またはアップデートする場合にクリックします • 更新: アクティベーションコードを変更した後、有効期限切れのままステータスが更新されない場合にクリックします
有効期限	現在のアクティベーションコードでサポートまたはコンポーネントのアップデートを受信できる最後の日付

最新のコンポーネントを確認する

コンポーネントのバージョンと最新のアップデート日時を確認するには、[概要] タブの [コンポーネントバージョン] リンクをクリックします。

Trend Micro Portable Security では次のコンポーネントが使用されています。

ダウンロードするコンポーネントを選択するには、46 ページの「検索設定 (その他)」を参照してください。

表 3-2. Trend Micro Portable Security のコンポーネント

コンポーネント	説明
ウイルス検索エンジン (32 ビット/64 ビット)	すべてのトレンドマイクロ製品は検索エンジンを中心に構成されています。当初、検索エンジンは、初歩的なファイルベースのコンピュータウイルスに対応するために開発されました。今日の検索エンジンは飛躍的に高度化され、さまざまな種類のウイルスや不正プログラムを検出する能力があります。また、調査用に開発され使用されている管理ウイルスも検出します。 各ファイルのすべてのバイトを検索するのではなく、次の項目を識別するためにエンジンとパターンファイルが連携します。 • ウイルスコードを示唆する特性 • ファイル内でウイルスが存在する正確な場所
挙動監視コアドライバ (32 ビット/64 ビット)	共通システム API を使用するツールからドライバ、プロセス、およびレジストリエントリを隠すルートキットの影響を受けないように Trend Micro Portable Security 2 を保護します。
検索サービス (32 ビット/64 ビット)	このエンジンはタスクを検索、駆除、および復元します。
ダメージクリーンナップエンジン (32 ビット/64 ビット)	トロイの木馬とそのプロセスを検索して削除します。
ウイルスパターンファイル	セキュリティエージェントが最新のウイルス/不正プログラムおよび複合型脅威の攻撃を特定するために利用する情報が含まれています。 トレンドマイクロは、1 週間に数回、および有害なウイルス/不正プログラムが検出されたときは随時、新しいバージョンのウイルスパターンファイルを作成および公開しています。
ダメージクリーンナップテンプレート	ウイルスクリーンナップエンジンで、トロイの木馬とそのプロセスを識別して除去するために使用されます。
スパイウェア/グレーウェアパターンファイル	ファイルやプログラム、メモリのモジュール、Windows レジストリ、および URL ショートカットに含まれるスパイウェア/グレーウェアを識別します。

コンポーネント	説明
デジタル署名パターンファイル	安全であると見なされ検索から除外されるプログラムのリストです。
プログラム検査パターンファイル	このパターンファイルにはプログラム検査用のルールセットが含まれています。ルールの種類には、CLSID、ファイルパス、製品名、企業名、ショートカット、および関連するレジストリがあります。また、偽セキュリティソフト (FakeAV) の検出ルールも含まれています。現在ではほとんどの場合、偽セキュリティソフトの検出に使用されているため、FakeAV パターンファイルとも呼ばれます。

予約アップデート

予約アップデートを有効にすると、指定した時刻に最新のコンポーネントが自動的にダウンロードされます。

手順

1. [概要] タブで、[予約アップデート] の横にあるリンクをクリックします。

   注意

   アップデート設定の現在のステータスに応じて、リンクには [オン] または [オフ] が表示されます。[オン] が表示されている場合は予約アップデートが有効です。[オフ] が表示されている場合は予約アップデートが無効で、[アップデート] をクリックしないと最新のコンポーネントは取得できません。

2. [予約アップデートを使用する] オプションを有効にします。
3. アップデートの頻度と開始時刻を選択します。
4. [保存] をクリックします。

   設定を変更したら、予約アップデートが有効か無効かに応じて、[概要] タブのリンクが変わります。

[登録済み検索ツール] タブ

[登録済み検索ツール] タブには、この管理プログラムで管理しているすべての登録済み検索ツールが表示され、検索設定を変更することができます。

セクション	説明
検索ツールの標準設定	「標準」の検索ツールに現在適用されている、限定された設定を表示します 開く: 管理プログラムに登録されている、「標準」の検索ツールの検索設定を表示または変更する場合にクリックします
検索ツールリスト	管理プログラムに登録されている、すべての検索ツールに関する情報を表示します • 検索ツール: 検索ツール名をクリックすると、検索ツールで実行された検索、同期、およびアップデートに関するログが表示されます • 検索ツール ID: 検索ツールの一意の ID • 前回の同期日時: 検索ツールでデータと設定が管理プログラムと前回同期された日時 • 前回のアップデート: 検索ツールでコンポーネントが前回アップデートされた日時 • デバイス設定: [標準] (検索ツールが検索ツールの標準設定を使用している場合) と [カスタム] (既存の設定を変更する場合) を切り替える場合にクリックします • ロック: ユーザが検索ツール画面から直接設定を変更できる機能をロックまたはロック解除する場合にクリックします

検索設定 (基本)

検索ツールの検索の種類、検索オプション、および検出時の処理を変更します。次の設定を変更できます。

- 検索の種類: 検索するフォルダの場所を指定し、不正プログラムに対して脆弱なファイルタイプのみを検索するか、[Safe Lock アプリケーション制御検索] 違反のみを検索するかを指定します

- すべてのローカルフォルダ: すべてのフォルダを検索します
- 初期設定のフォルダ (クイック検索): ウイルスに感染しやすいフォルダ (Windows のシステムフォルダなど) のみを検索します
- Safe Lock アプリケーション制御検索: Trend Micro Safe Lock の [Safe Lock アプリケーション制御] を有効にした後に隔離またはブロックされたファイルと、実行されたファイル (ただし、許可リストには含まれないもの) のみを検索します。
- 特定のフォルダ: 選択したドライブやフォルダを検索します

- 検索オプション
  - リムーバブルドライブを検索する: コンピュータに接続されているリムーバブルドライブを検索する場合に選択します
  - 検索プロセス優先度を下げる: 選択すると、コンピュータでのパフォーマンスへの影響は軽減されますが、検索時間は長くなります
  - 検索の中断を有効にする: 検索中に [中断] ボタンを表示する場合に選択します
- 検出時の処理: 脅威の検出後に検索ツールで実行する処理を指定します。
  - 手動で処理を選択: 実行する処理を確認するようメッセージが表示されます
  - ログに記録のみ: 検出した脅威をログに記録しますが、それ以上の処理は実行しません
  - トレンドマイクロの推奨処理を使用: 脅威の種類に従い、自動的にトレンドマイクロの推奨処理を行います

注意

検索ツールプログラムを再起動して、変更内容を有効にしてください。検索ツールを再起動するには、検索ツールの画面を一度閉じて、再度開いてください。

検索の種類

ウイルス検索するドライブやフォルダを設定します。

ヒント

管理プログラムの検索設定を変更した場合は、その設定を検索ツールに同期してください。

- すべてのローカルフォルダ: すべてのフォルダを検索します
- 初期設定のフォルダ (クイック検索): ウイルスに感染しやすいフォルダ (Windows のシステムフォルダなど) のみを検索します
- Safe Lock アプリケーション制御検索: Trend Micro Safe Lock の [Safe Lock アプリケーション制御] を有効にした後に隔離またはブロックされたファイルと、実行されたファイル (ただし、許可リストには含まれないもの) のみを検索します。
- 特定のフォルダ: 選択したドライブやフォルダを検索します
  - ドライブやフォルダをリストに追加するには [追加] をクリックします。
  - 選択した項目を削除するには [削除] をクリックします。
  - 選択した項目を変更するには [編集] をクリックします。

検索オプション

リムーバブルドライブの検索や検索プロセスの優先度に関するオプションを選択できます。

- リムーバブルドライブを検索する: コンピュータに接続されているリムーバブルストレージが検索されます
- 検索プロセス優先度を下げる: システムリソースの使用率を下げるために、検索プロセスに最も低い優先度が設定されます

注意

これにより検索時間が長くなります。

- 検索の中断を有効にする: 検索中に [中断] ボタンが表示され、コンピュータの検索を中断して後で再開することができます

注意

これにより検索時間が長くなり、コンピュータに一時ファイルが保存されます。

検出時の処理

検索処理方法を設定します。

- 手動で処理を選択: ウイルス検索を行い、ウイルスが検出された場合はその都度、実行する処理を確認します。
- ログに記録のみ: ウイルス検索のみ行います。ウイルスが検出された場合にも処理は実行しません。
- トレンドマイクロの推奨処理を使用: ウイルス検索を行い、ウイルスが検出された場合はトレンドマイクロ推奨の処理を行います。

ヒント

「トレンドマイクロの推奨処理」では、検出されたウイルスの種類に応じて、駆除、隔離、または放置などの処理を行います。推奨の処理方法は定期的に見直され、パターンファイルや検索エンジンなどをアップデートする際に変更されます。

検索設定 (詳細)

検索ツールの詳細な検索設定にアクセスするには、[詳細] タブに移動します。

- 検索除外リスト: 検索しないファイル、フォルダ、または拡張子を追加します

  45 ページの「検索除外リストの設定を変更する」を参照してください。

- 一時ファイルを保存せずに検索: 検索対象コンピュータにファイルを保存せずに検索します

重要

この機能は管理用コンピュータの検索には適していません。

- 管理者として検索: 管理者権限のないユーザでも管理者のユーザ名とパスワードを使用して検索できます

注意

ドメインアカウントを利用する場合は、円記号「\」またはアットマーク「@」を使用してユーザ名とドメインを区切ります。

- 検索する圧縮階層: 圧縮階層の数を選択して、その数を超える階層の検索を省略します

検索除外リストの設定を変更する

検索から除外するファイル、フォルダ、または拡張子を選択します。

注意

100 個までのファイルやフォルダを除外できます。複数の拡張子を設定するにはカンマ「,」で区切ります。拡張子にはドット「.」を含めないでください。

さらに、次の操作を実行できます。

- ドライブやフォルダをリストに追加する
- 選択した項目をリストから削除する
- リストの項目を編集する

ヒント

画面右下の [保存] をクリックして変更した設定を保存したら、その設定を検索ツールに反映してください。

検索設定 (Rescue Disk)

Rescue Disk での検出時の処理を変更します。次の設定を変更できます。

- 検索して隔離する: 検出されたファイルをローカルディスクに隔離する場合は、このオプションを選択します。ファイルを隔離する前に確認メッセージを表示するには、[隔離する前に確認する] を選択します。

- 検索のみ: 検出された脅威を隔離せずに検索のみ実行する場合は、このオプションを選択します。

詳細については、84 ページの「Trend Micro Rescue Disk」を参照してください。

検索設定 (その他)

検索ツールのその他の設定を変更します。次の設定を変更できます。

- 検索ツール名: 検索ツールの名前を変更します。

  注意

  検索ツールの [カスタム] 設定を変更する場合にのみ使用できます。

- ネットワーク接続にプロキシサーバを使用する: プロキシサーバ経由で管理プログラムに接続する必要がある場合は、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - Internet Explorer 設定からプロキシサーバ情報を自動でインポートする: 管理用コンピュータにインストールされている Internet Explorer と同じ設定にする場合に選択します。
  - プロキシサーバ情報を指定する: プロキシサーバの設定を個別に行う場合に選択します。
- プログラムコンポーネント: [設定] をクリックして、ダウンロードするコンポーネントを指定します。

  詳細については、38 ページの「最新のコンポーネントを確認する」を参照してください。
- 検索ツールにエンドポイント情報の収集を許可する: 検索ツールを接続後、コンピュータの現在の状態に関するデータの収集を自動的に開始する場合に選択します
- Trend Micro Safe Lock からログを収集する: Trend Micro Safe Lock がインストールされたコンピュータからログを収集する場合は、このチェックボックスをオンにします。

[現在接続中の検索ツール] タブ

[現在接続中の検索ツール] タブでは、管理用コンピュータに現在接続されている検索ツールを表示および管理できます。

項目	説明
名前の変更	検索ツールの名前を変更します
ログの転送	検索ツールから管理プログラムにログを転送します [転送後、検索ツールからログファイルを削除します] 確認ダイアログオプションを選択して、検索ツールのディスク空き容量を確保することをお勧めします。
コンポーネントと検索設定の同期	管理プログラムから検索ツールにコンポーネントと設定をダウンロードします
検索ツールリスト	同期とコンポーネントアップデートの情報を表示する検索ツールを選択します

検索ツールからコンポーネントをアップデートする

最新コンポーネントを含む検索ツールからコンポーネントをインポートして管理プログラムをアップデートできます。この方法は次の場合に適しています。

- ローカルネットワーク内で管理プログラムが設定されており、トレンドマイクロのアップデートサーバに接続できない。
- 検索ツールに最新コンポーネントが含まれている。

手順

1. 検索ツールを管理用コンピュータに接続します。管理プログラム画面が開きます。
2. [現在接続中の検索ツール] タブをクリックします。
3. 検索ツールを選択します。選択したツールに最新コンポーネントが含まれる場合は、コンポーネントが [(最新)] と表示され、[インポート] ボタンが有効になります。

4. [インポート] をクリックして、コンポーネントのアップデートを開始します。

[ログとレポート] タブ

[ログとレポート] タブでは、ログデータをインポート、エクスポート、および管理できます。

項目	説明
ログのインポート	別の管理プログラムからエクスポートしたデータベース形式のログをインポートします
ログのエクスポート	すべての検索ログをデータベースまたは CSV 形式にエクスポートします 重要 検索ログを別の管理プログラムにインポートする場合は、[すべての検索ログとデータを DB 形式でエクスポート] を選択する必要があります。
ログの削除	指定された検索ログを削除します 注意 削除処理を実行する前に、ログをエクスポートしておくことをお勧めします。
資産情報のエクスポート	検索ツールで収集した資産情報を CSV 形式でエクスポートします • システムおよびハードウェア情報 • アップデート情報 (Microsoft アプリケーションのみ) • インストール済みアプリケーションのリスト

項目	説明
結果のフィルタリングと表示	• コンピュータ: コンピュータ名に基づいて検索ログを表示します • 検索ツール: 検索ツール名に基づいて検索ログを表示します • カレンダー: 指定された期間に基づいて、検索ログのエントリをフィルタリングします
コンピュータ名ごとの検索ログの表示	• [コンピュータ] 名をクリックし、そのコンピュータで実行されたすべての検索ログのリストを表示します • [前回の検索日時] をクリックし、コンピュータで使用可能な前回の検索データの検索結果を表示します

検索ツール名ごとの検索ログの表示	• [検索ツール] 名をクリックし、その検索ツールに関する概要画面を表示します
	  • 概要: 検索ツールで実行された検索、同期、およびアップデート処理に関する一般情報を表示します
	  • 検索: 検索ツールで実行されたすべての検索ログを表示します
	  • 同期: 検索ツールのログ転送およびコンポーネントアップデートに関する情報を表示します
	  • アップデート: 検索ツールでアップデートされたコンポーネントに関する情報を表示します
	  • デバイス情報: 検索ツールの現在のコンポーネントバージョンを表示します
	• [前回の検索日時] をクリックし、検索ツールによって転送された使用可能な前回の検索データの検索結果を表示します

管理プログラムの設定

- [設定] > [管理プログラムの設定] の順にクリックして、管理コンソールからインターネットや検索ツール、およびコンポーネントのアップデート元に接続する方法を変更します。

- [設定] > [設定のインポート]/[設定のエクスポート] の順にクリックして、管理プログラムの設定をバックアップまたは復元します。

一般設定

[一般] タブでは、プロキシ、外部通信の認証、画面の言語など、管理プログラムの設定を制御できます。

重要

別の画面またはタブに移動する前に、変更内容をすべて [保存] する必要があります。

- ネットワーク接続にプロキシサーバを使用する: プロキシサーバ経由で管理プログラムに接続する必要がある場合は、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - Internet Explorer 設定からプロキシサーバ情報を自動でインポートする: 管理用コンピュータにインストールされている Internet Explorer と同じ設定にする場合に選択します。
  - プロキシサーバ情報を指定する: プロキシサーバの設定を個別に行う場合に選択します。
- 待機設定: リモートで接続する検索ツールとの通信に管理プログラムが使用する、パスワードとポートを指定します。
- 言語: 管理プログラムの表示言語を変更します。

アップデート設定

[アップデート] タブでは、管理プログラムがコンポーネントのアップデートを受信するアップデート元を変更できます。

重要

別の画面またはタブに移動する前に、変更内容をすべて [保存] する必要があります。

- トレンドマイクロのアップデートサーバ: トレンドマイクロのアップデートサーバからアップデートを取得します。インターネットに接続する必要があります。
- その他のアップデート元: ローカルネットワーク内に設置可能な特定のアップデート元からアップデートを取得します。

管理プログラムの設定をバックアップおよび復元する

管理プログラム環境の移行または復元に備えて、管理プログラムの設定をバックアップしておくことをお勧めします。

エクスポートされる設定は次のとおりです。

- 基本設定
- 登録済み検索ツールのリスト
- 検索ツールの設定

注意

次の設定はエクスポートされません。

- アクティベーションコード
- セキュリティパターンファイルと検索コンポーネント
- サポートツールの設定
- 管理プログラムのパスワードと接続ポート

管理プログラムの設定をエクスポートおよびインポートする

設定にアクセスするには、管理プログラム画面で [設定] をクリックし、[設定のエクスポート] または [設定のインポート] をクリックします。

第 4 章

検索ツール画面を使用する

この章では、検索ツール画面のさまざまなタブで使用できる機能について概説します。

重要

この機能は Windows コンピュータでのみ使用できます。

Windows コンピュータを検索する

[検索] タブからコンピュータの検索を手動で開始し、検索の進捗状況を監視するか、検索設定を変更します。

手順

1. 検索ツール画面を開きます。
2. [検索] タブをクリックします。
3. [検索開始] をクリックし、現在の検索設定でコンピュータの検索を開始します。

   検索を開始する前に検索設定を変更するには、[編集] リンクをクリックします。

   詳細については、56 ページの「検索設定」を参照してください。

検索ツールの LED ライトによって検索のステータスを確認することができます。

表 4-1. 検索ツールのインジケータライト

インジケータライト	説明
青色 (点滅)	検索ツールに情報を書き込んでいるか、検索ツールから情報を取得しています。
青色	検索が完了し、脅威は検出されませんでした。
黄色	検索が完了し、検出された脅威はすべて駆除されました。
赤色	検索が完了し、さらなる対処が必要な脅威が検出されました。
青色、黄色、赤色 (連続して点灯)	検索を実行しています。

4. [検索と問題の解決] 画面で、検索の進捗状況を監視します。

   - コンピュータの検索を停止したい場合は、[停止] をクリックします。
   - 現在の検索を中断したい場合は、[中断] をクリックします。[再開] ボタンを使用すると、中断した検索を検索ツールの再起動後に再開できます。

     [中断] は、検索管理者が設定している場合にのみ使用できます。

     詳細については、57 ページの「検索設定 (基本)」を参照してください。
   - 適用 (脅威の検出): 検出された脅威に処理を適用する場合にクリックします。

     詳細については、61 ページの「脅威の検出」を参照してください。
   - コメント: 検索のログエントリに追加するコメントを入力します。

警告!

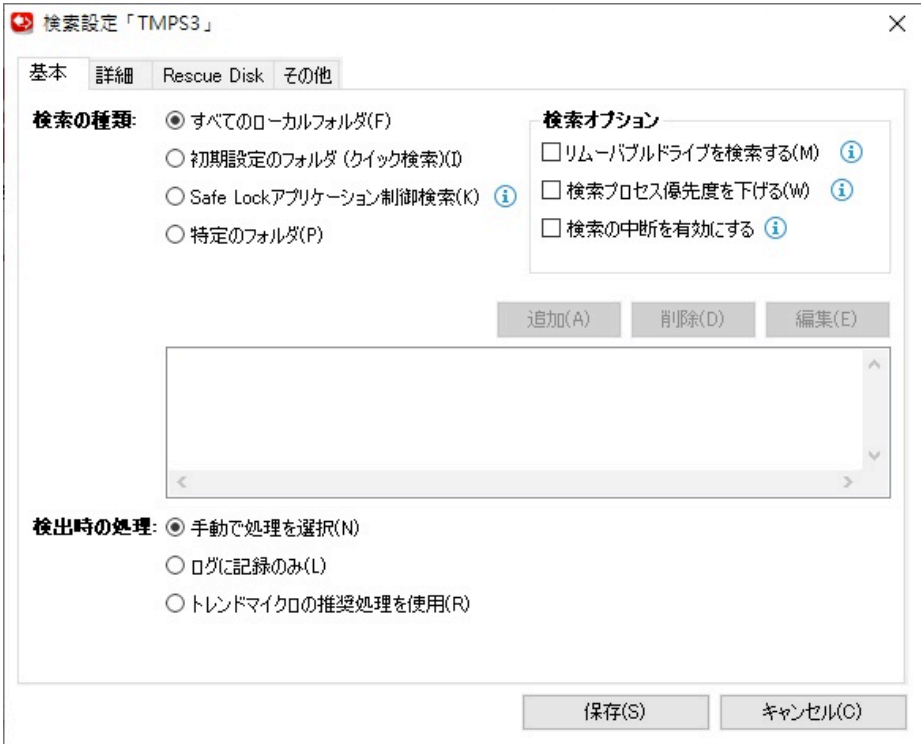
LED が点灯している場合や検索ツール画面を終了していない場合は検索ツールを取り外さないでください。

5. 検索の完了後、[結果の表示] 画面に次のオプションが表示されます。
   - 再度検索する: [開始] 画面に戻ってコンピュータの新しい検索を開始する場合にクリックします。
   - コメント: 検索のログエントリに追加するコメントを入力します。
   - 閉じる: 検索ツール画面を閉じます。

検索設定

検索設定を変更するには、検索ツール画面で [検索] タブをクリックして、[編集] をクリックします。

検索設定 (基本)



検索ツールの検索の種類、検索オプション、および検出時の処理を変更します。次の設定を変更できます。

- 検索の種類: 検索するフォルダの場所を指定し、不正プログラムに対して脆弱なファイルタイプのみを検索するか、[Safe Lock アプリケーション制御検索] 違反のみを検索するかを指定します
  - すべてのローカルフォルダ: すべてのフォルダを検索します
  - 初期設定のフォルダ (クイック検索): ウイルスに感染しやすいフォルダ (Windows のシステムフォルダなど) のみを検索します

- Safe Lock アプリケーション制御検索: Trend Micro Safe Lock の [Safe Lock アプリケーション制御] を有効にした後に隔離またはブロックされたファイルと、実行されたファイル (ただし、許可リストには含まれないもの) のみを検索します。
- 特定のフォルダ: 選択したドライブやフォルダを検索します

- 検索オプション
  - リムーバブルドライブを検索する: コンピュータに接続されているリムーバブルドライブを検索する場合に選択します
  - 検索プロセス優先度を下げる: 選択すると、コンピュータでのパフォーマンスへの影響は軽減されますが、検索時間は長くなります
  - 検索の中断を有効にする: 検索中に [中断] ボタンを表示する場合に選択します
- 検出時の処理: 脅威の検出後に検索ツールで実行する処理を指定します。
  - 手動で処理を選択: 実行する処理を確認するようメッセージが表示されます
  - ログに記録のみ: 検出した脅威をログに記録しますが、それ以上の処理は実行しません
  - トレンドマイクロの推奨処理を使用: 脅威の種類に従い、自動的にトレンドマイクロの推奨処理を行います

検索設定 (詳細)

検索ツールの詳細な検索設定にアクセスするには、[詳細] タブに移動します。

- 検索除外リスト: 検索しないファイル、フォルダ、または拡張子を追加します

  45 ページの「検索除外リストの設定を変更する」を参照してください。
- 一時ファイルを保存せずに検索: 検索対象コンピュータにファイルを保存せずに検索します

重要

このオプションを使用すると、一部の不正プログラムに対する検索機能が低下する場合があります。また、検索対象に一時ファイルを保存しない場合は、検索時間が長くなることがあります。

- 管理者として検索: 管理者権限のないユーザでも管理者のユーザ名とパスワードを使用して検索できます

注意

ドメインアカウントを利用する場合は、円記号「\」またはアットマーク「@」を使用してユーザ名とドメインを区切ります。

- 検索する圧縮階層: 圧縮階層の数を選択して、その数を超える階層の検索を省略します

検索除外リストの設定を変更する

検索から除外するファイル、フォルダ、または拡張子を選択します。

注意

100 個までのファイルやフォルダを除外できます。複数の拡張子を設定するにはカンマ「,」で区切ります。拡張子にはドット「.」を含めないでください。

さらに、次の操作を実行できます。

- ドライブやフォルダをリストに追加する
- 選択した項目をリストから削除する
- リストの項目を編集する

ヒント

画面右下の [保存] をクリックして変更した設定を保存したら、その設定を検索ツールに反映してください。

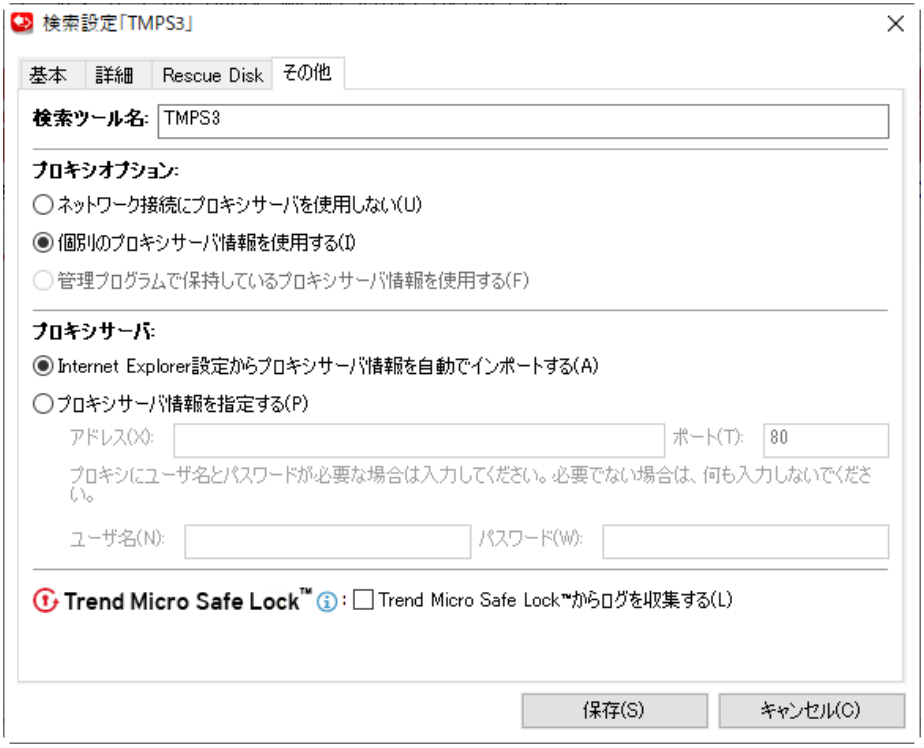
検索設定 (Rescue Disk)

Rescue Disk での検出時の処理を変更します。次の設定を変更できます。

- 検索して隔離する: 検出されたファイルをローカルディスクに隔離する場合は、このオプションを選択します。ファイルを隔離する前に確認メッセージを表示するには、[隔離する前に確認する] を選択します。
- 検索のみ: 検出された脅威を隔離せずに検索のみ実行する場合は、このオプションを選択します。

Rescue Disk の詳細については、84 ページの「Trend Micro Rescue Disk」を参照してください。

検索設定 (その他)



検索ツールのその他の設定を変更します。次の設定を変更できます。

- 検索ツール名: 検索ツールの名前を変更します。
- プロキシサーバ: プロキシサーバ経由でインターネットに接続する必要がある場合は、このチェックボックスをオンにして、次のいずれかのオプションを選択します。
  - Internet Explorer 設定からプロキシサーバ情報を自動でインポートする: Internet Explorer と同じ設定にする場合に選択します。
  - プロキシサーバ情報を指定する: プロキシサーバの設定を個別に行う場合に選択します。
- Trend Micro Safe Lock からログを収集する: Trend Micro Safe Lock がインストールされたコンピュータからログを収集する場合は、このチェックボックスをオンにします。

脅威の検出

ウイルスが検出された場合は、ウイルスに関する情報を確認してから処理を選択してください。

脅威を解決する

手順

1. ファイル名や危険度などを確認し、[処理] から処理方法を選択します。
   - 無視: 何も処理しません。
   - 解決: トレンドマイクロの推奨処理を行います。

ヒント

検出されたウイルスの種類に応じて、駆除、隔離、または放置などの処理を行います。推奨の処理方法は定期的に見直され、パターンファイルや検索エンジンなどをアップデートする際に変更される場合があります。

2. [適用] をクリックします。

注意

[再度検索する] をクリックし、もう一度ウイルス検索を行うこともできます。

3. ウイルスが再検出されていないことを確認し、[コメント] に簡単な説明などを入力して [閉じる] をクリックします。

ヒント

[コメント] に入力できる文字数は 63 文字までです。[コメント] の内容は、ログデータとともに検索結果に表示されます。[コメント] の初期設定値はコンピュータ名です。

隔離ファイルを復元する

Portable Security でファイルが解決され隔離された場合、そのファイルを復元して使用できます。

警告!

選択したファイルを復元すると危険な場合があります。感染ファイルを復元した場合、検索ツールの安全性を保証できないため、ファイルを復元する前にそのファイルが既知のウイルスではないことを十分確認してください。

手順

1. 検索ツール画面を開きます。
2. [復元] タブに移動します。
3. [前回の検索結果] のドロップダウンリストから検索日時を選択すると、その検索時に隔離されたファイルが表示されます。
4. ファイルを選択し、[復元] をクリックします。

注意

復元は隔離を実施したコンピュータでのみ行うことができます。検索を行っていないコンピュータに復元することはできません。

5. [OK] をクリックして確認します。

警告!

そのファイルが絶対に必要であり、感染していないことがわかっている場合にのみ実行してください。

6. [閉じる] をクリックします。

[復元] タブ

注意

検索ツールでは、通常の USB デバイスのようにファイルを保存することはできません。ただし、隔離ファイルは検索対象コンピュータではなく検索ツールに保存されます。

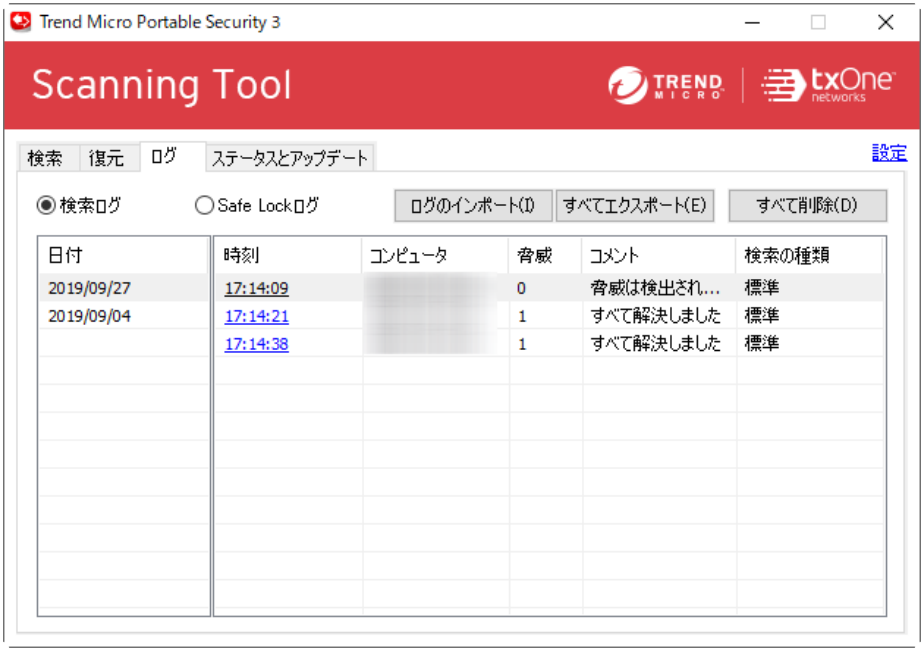
- 前回の検索結果: 検索が実行された日時を選択します。
- 検索: この機能は「無視しました」または「解決できません」がタグ付けされたファイルに対して有効になります。

  [検索] を選択すると、選択したファイルに適用する検出時の処理を選択する確認画面が表示されます。
- 復元: ファイルを 1 つ以上選択してクリックすると、そのファイルが元の場所に戻されます。62 ページの「隔離ファイルを復元する」を参照してください。

警告!

感染していないことがわかっているファイルのみ復元してください。

[ログ] タブ



検索結果を表示するには、[検索ログ] を選択して、[時刻] 列の項目をクリックします。Trend Micro Safe Lock のログを表示するには、[Safe Lock ログ] を選択します。

Safe Lock ログの収集の詳細については、60 ページの「検索設定 (その他)」を参照してください。

- ログのインポート: データベース形式のログをインポートする場合にクリックします。
- すべてエクスポート: すべてのログをデータベース形式または CSV 形式でエクスポートする場合にクリックします。
- すべて削除: すべてのログエントリを削除する場合にクリックします。

[ステータスとアップデート] タブ

[ステータスとアップデート] タブには、検索ツールのコンポーネントのステータスが表示されます。

アクティベーションのステータスの詳細については、23 ページの「アクティベーション」を参照してください。

- デバイス名: 検索ツールの名前です。
- 検索ツール ID: すべての検索ツールに割り当てられる一意の識別番号です。
- バージョン: Portable Security 検索ツールのビルド番号は、[バージョン] の横に表示されます。コンポーネントの詳細と最新のアップデート日時を確認するには、[コンポーネントバージョン] リンクをクリックしてください。

- 前回のアップデート: アップデートのステータスが表示されます。[アップデート] をクリックすると、検索ツールのコンポーネントと HotFix が最新の状態に更新されます。
- アクティベーションコード: アクティベーションコードを変更または更新するには、[編集] をクリックします。

  詳細については、29 ページの「アクティベーションコードを変更する」を参照してください。
- 有効期限: アクティベーションコードの有効期限が表示されます。アクティベーションコードを変更した後、有効期限切れのままステータスが更新されない場合は、[更新] をクリックします。

コンポーネントのアップデート

トレンドマイクロから最新のパターンファイルや検索エンジンをダウンロードして、検索ツールをアップデートします。コンポーネントのバージョンと

最新のアップデート日時を確認するには、[コンポーネントバージョン] リンクをクリックしてください。

コンポーネントを手動でアップデートする

必要に応じて検索ツールをアップデートします。

手順

1. アップデート元に接続可能なコンピュータに検索ツールを接続します。

> **注意**
>
> アップデート元の設定の詳細については、68 ページの「検索ツールの設定を変更する」を参照してください。

2. 検索ツール画面で [ステータスとアップデート] タブをクリックします。

図 4-1. スタンドアロンモードで設定されている検索ツール

3. [アップデート] をクリックします。

検索ツールの設定を変更する

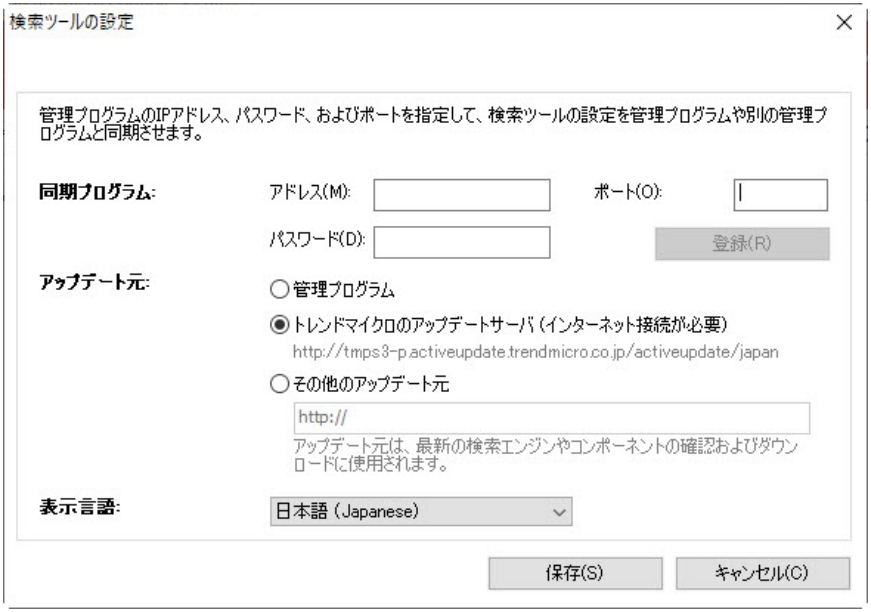
検索ツールのアップデート元と表示言語を設定します。

手順

1. 検索ツール画面を開きます。

図 4-2. スタンドアロンモードで設定されている検索ツール画面

2. 画面右上にある [設定] をクリックします。



注意

管理プログラムの設定は、スタンドアロンモードで設定されている検索ツールでは自動的に無効になります。

3. アップデート元を指定します。
   - トレンドマイクロのアップデートサーバ: トレンドマイクロのアップデートサーバからアップデートを取得します。インターネットに接続する必要があります。
   - その他のアップデート元: ローカルネットワーク内に設置可能な特定のアップデート元からアップデートを取得します。
4. (オプション) ドロップダウンリストから検索ツールの表示言語を選択します。
5. [保存] をクリックします。

第 5 章

Linux コンピュータを検索する

この章では、検索ツールを使用して Linux コンピュータを検索する方法について概説します。

重要

Linux コンピュータで検索ツールを使用するには、スタンドアロンモードと集中管理モードのいずれかを選択して、Windows コンピュータで検索ツールのアクティベーションを実行しておく必要があります。

詳細については、23 ページの「アクティベーション」を参照してください。

Linux のシステム要件

項目	要件
OS	• Red Hat Enterprise Linux 6.0 以降 • CentOS 6.0 以降
権限	ログオンアカウントには次のいずれかの権限が必要です。 • 「root」ユーザ • 「sudo」権限

Linux のコマンドラインリファレンス

検索ツールのフォルダをマウントした後は、すべての処理を Linux のコマンドラインから実行する必要があります。

用法:

- `sudo sh ./LauncherLinux.sh -c scan [<scan options>] <scan targets>`
- `sudo sh ./LauncherLinux.sh -c restore`

コマンド構造	説明
コマンド	• `-c	--command <scan	restore>` • `-h	--help` ヘルプ画面を表示します
<scan options>	• `-a	--action <action>` 初期設定を上書きする、適用する検出時の処理: `log	confirm	recommended`
<scan targets>	フォルダの場所またはファイルのフルパスを指定します。検索対象を複数指定する場合は空白文字で区切ってください。

Linux コンピュータのセキュリティリスクを検索する

この作業は、お使いの Linux 環境で USB ドライブの自動マウントがサポートされていることを前提としています。自動マウントがサポートされていない場合は、Linux のドキュメントで USB デバイスを手動でマウントする方法について参照してください。

重要

Linux コンピュータで検索ツールを使用するには、スタンドアロンモードと集中管理モードのいずれかを選択して、Windows コンピュータで検索ツールのアクティベーションを実行しておく必要があります。

詳細については、23 ページの「アクティベーション」を参照してください。

手順

1. 「root」または「sudo」の権限を持つアカウントを使って検索対象の Linux コンピュータに検索ツールを接続します。

   コンピュータで検索ツールが自動マウントされ、[TMPS3 DAT] および [TMPS3 SYS] ドライブが画面に表示されます。

2. [TMPS3 SYS] ドライブを開きます。

3. フォルダ内 (ファイルまたはフォルダアイコン以外) を右クリックして、[端末で開く] をクリックします。

   TMPS3 SYS ディレクトリをポイントして端末が開きます。

4. 次のコマンド構造を使用して、コンピュータを検索します。

   ```
   sudo sh ./LauncherLinux.sh -c scan [<scan options>] <scan targets>
   ```

   管理プログラムの設定を使用してコンピュータ全体を検索するには、次のように入力します。

   ```
   sudo sh ./LauncherLinux.sh -c scan /
   ```

/tmp フォルダ内のすべてのファイルを検索して、「推奨」処理を実行するには、次のように入力します。

```
sudo sh ./LauncherLinux.sh -c scan -a recommended /tmp
```

使用可能なオプションの詳細については、72 ページの「Linux のコマンドラインリファレンス」を参照してください。

コンピュータの検索が開始されます。

5. 検索が完了するまで待つか、<Ctrl>+<C> キーを押して進行中の検索をキャンセルします。
6. 設定している検出時の処理が [手動で処理を選択] の場合、脅威が検出されると、処理を求めるメッセージが表示されます。
   - f: Portable Security attempts to clean or quarantine the detected threat
   - i: Portable Security takes no action on the detected threat
   - F: Portable Security attempts to clean or quarantine all detected threats
   - I: Portable Security takes no action on any detected threat
7. 検索結果と処理の結果が表示され、検索ログが検索ツールに保存されます。

Linux コンピュータでファイルを復元する

この作業は、お使いの Linux 環境で USB ドライブの自動マウントがサポートされていることを前提としています。自動マウントがサポートされていない場合は、Linux のドキュメントで USB デバイスを手動でマウントする方法について参照してください。

手順

1. 「root」または「sudo」の権限を持つアカウントを使って検索対象の Linux コンピュータに検索ツールを接続します。

コンピュータで検索ツールが自動マウントされ、[TMPS3 DAT] および [TMPS3 SYS] ドライブが画面に表示されます。

2. [TMPS3 SYS] ドライブを開きます。
3. フォルダ内 (ファイルまたはフォルダアイコン以外) を右クリックして、[端末で開く] をクリックします。

   TMPS3 SYS ディレクトリをポイントして端末が開きます。
4. 次のコマンド構造を使用して、コンピュータでファイルを復元します。

   ```
   sudo sh ./LauncherLinux.sh -c restore
   ```

   当該コンピュータの以前の検索ログのリストが表示されます。
5. ファイルを復元する検索ログの索引を入力します。

   隔離ファイルのリストが表示されます。
6. 復元する隔離ファイルの索引を入力します。

   隔離ファイルがコンピュータに復元されます。
7. 処理の結果が表示され、ログが検索ツールに保存されます。

Linux システムでデバッグログを生成する

Linux コンピュータの検索中にエラーが発生した場合は、トラブルシューティングするためのデバッグログを生成してサポート担当者に送信できます。

手順

1. 「root」または「sudo」の権限を持つアカウントを使って検索対象の Linux コンピュータに検索ツールを接続します。

   コンピュータで検索ツールが自動マウントされ、[TMPS3 DAT] および [TMPS3 SYS] ドライブが画面に表示されます。
2. [TMPS3 SYS] ドライブを開きます。

3. フォルダ内 (ファイルまたはフォルダアイコン以外) を右クリックして、[端末で開く] をクリックします。

   TMPS3 SYS ディレクトリをポイントして端末が開きます。

4. 次のコマンドを使用して、コンピュータを検索します。

   ```
   [root@localhost]# sudo sh ./LaucherLinux.sh --debug -c scan
   [target folder] > /tmp/tmps.log 2>&1
   ```

   コンピュータの検索が開始され、すべてのログデータが/tmp/tmps.log ファイルに記録されて、画面にステータスメッセージが表示されます。

5. 検索終了後、次のコマンドを実行して追加のログ情報を収集します。

   ```
   [root@localhost]# sudo dmesg > /tmp/dmesg.log
   ```

6. 次のログファイルをコピーしてサポート担当者に送信します。

   - /tmp/tmps.log
   - /tmp/dmesg.log
   - /var/log/syslog

Linux の検索ログを表示する

Linux コンピュータを使用して、検索ログ全体を直接表示することはできません。検索ログ全体を表示するには、検索ツールを Windows コンピュータまたは管理用コンピュータに接続します。

第 6 章

追加のツール

この章では、Trend Micro Portable Security に付属する追加のツールの使用法について説明します。

Trend Micro Portable Security サポートツール

Trend Micro Portable Security サポートツールを使用すると、問題を診断してトラブルシューティングすることができます。サポートツールは自動的にインストールに含められ、Windows の [スタート] メニューからアクセスできます。

デバッグ

[デバッグ] タブを使用して、製品の問題をトラブルシューティングするためのデバッグログを生成します。

インストールの問題についてデバッグログを生成する

検索ツールエージェントのインストールの問題についてデバッグログを生成するには、次の手順を実行します。

手順

1. Trend Micro Portable Security コンピュータの [スタート] メニューから、[Trend Micro Portable Security 3] > [サポートツール] の順にクリックします。

   a. 検索ツールをコンピュータに接続します。

   b. SupportTool フォルダを USB デバイスからローカルディスクにコピーします。

   c. `TMPSSuprt.exe` ファイル () をダブルクリックします。

2. [[A] デバッグ] タブで [インストールに関するデバッグ情報を収集する] を選択して、[開始] をクリックします。

3. [データの収集] をクリックします。

4. [完了] をクリックします。

5. [フォルダを開く] をクリックします。

検索ツールのデバッグログを生成する

手順

1. 検索ツールをコンピュータに接続します。
2. [TMPS3 SYS] ドライブで、`SmallDebugTool` フォルダに移動します。
3. `SmallDebugTool.exe` を起動して、ログを収集します。
   a. `SmallDebugTool.exe` ファイル () をダブルクリックします。
   b. [検索ツールの開始] をクリックして、デバッグモードを開始します。
   c. Trend Micro Portable Security で発生した問題を再現します。
   d. 問題を再現したら、[デバッグ情報の収集が完了しました] を有効にします。
   e. [デバッグモードの停止] をクリックします。
   f. [データの転送] をクリックします。

      検索ツールへのログの転送が開始されます。このプロセスの完了には時間がかかることがあります。
   g. [閉じる] をクリックします。
4. コンピュータから検索ツールを取り外して、Trend Micro Portable Security がインストールされているコンピュータに接続します。
5. Trend Micro Portable Security 3 サポートツールを起動します。

   Trend Micro Portable Security コンピュータの [スタート] メニューから、[Trend Micro Portable Security 3] > [サポートツール] の順にクリックします。

   異なるコンピュータを使用している場合は、次の手順を実行します。

a. 検索ツールをコンピュータに接続します。

b. `SupportTool` フォルダを USB デバイスからローカルディスクにコピーします。

c. `TMPSSuprt.exe` ファイル () をダブルクリックします。

6. Trend Micro Portable Security 3 サポートツールを使用して、ログをエクスポートします。

a. [デバッグ] タブで [検索ツールからログを読み込む] を選択して、[開始] をクリックします。

b. 検索ツールをコンピュータに接続して、[次へ] をクリックします。

ログの保存先のパスが表示されます。

c. [フォルダを開く] をクリックして、パスに移動します。

zip ファイルを見つけて開き、デバイスログが正常に生成されていることを確認します。

デバイスのリセット

Trend Micro Portable Security サポートツールを使用して、検索ツールの設定または USB デバイスの状態をリセットできます。

現在の検索ツールのモードを変更する場合にも、デバイスをリセットする必要があります。たとえば、検索ツールが現在スタンドアロンモードである場合、モードを変更して管理プログラムに登録するには、デバイスをリセットする必要があります。

リセットには 2 つのモードがあります。

- 検索ツールの設定を初期状態にする: 一部のコンポーネントが破損した可能性があるために検索ツールが動作していない場合は、このオプションを選択してください。このモードではアクティベーションコードとステータスが保持されます。
- USB デバイスを初期出荷状態にする: 初期出荷状態にリセットするには、このオプションを選択してください。

注意

- 一度に 1 つのデバイスのみをリセットできます。
- Trend Micro Portable Security サポートツールでは、以前のバージョンの Trend Micro Portable Security 検索ツールのリセットはサポートされません。

検索ツールの設定を初期状態にする

手順

1. Trend Micro Portable Security 3 検索ツールをコンピュータに接続します。
2. SupportTool フォルダを USB デバイスからローカルディスクにコピーします。
3. `TMPSSuprt.exe` ファイル () をダブルクリックします。
4. [他の機能] タブに移動します。
5. [デバイスのリセット] をクリックします。
6. [検索ツールの設定を初期状態にする] を選択して、[次へ] をクリックします。
7. [はい] をクリックします。

   注意

   リセット処理が完了するまでの間 (メッセージが出るまで)、USB デバイスを取り外さないでください。

8. デバイスを取り外してから再度接続し、検索ツールがリセットされたことを確認します。

USB デバイスを初期出荷状態にする

手順

1. Trend Micro Portable Security 3 検索ツールをコンピュータに接続します。
2. [TMPS3 SYS] ドライブで、SupportTool フォルダを USB デバイスからローカルディスクにコピーします。
3. 該当する Win32 または x64 フォルダで、TMPSSuprt.exe ファイル () をダブルクリックします。
4. [他の機能] タブに移動します。
5. [デバイスのリセット] をクリックします。
6. [USB デバイスを初期出荷状態にする] を選択して、[次へ]をクリックします。
7. アクティベーションコードをコピーし、[アクティベーションコードを保存しました] チェックボックスをオンにします。
8. [はい] をクリックします。

   注意

   リセット処理が完了するまでの間 (メッセージが出るまで)、USB デバイスを取り外さないでください。

9. デバイスを取り外してから再度挿入し、Launcher.exe を実行して、検索ツールがリセットされたことを確認します。

   検索ツールのリセットが完了すると、[検索ツールの初期設定] 画面が表示されます。

修正プログラムなどの適用

Trend Micro Portable Security サポートツールを使用して、必要に応じて検索ツールに修正モジュールまたはバンデージパターンを適用します。

注意

これらのアップデートは、一度に 1 つのデバイスにのみ適用できます。

警告!

バンデージパターンは有償サポートでの提供となります。詳細は、担当のテクニカルアカウントマネージャに問い合わせてください。

修正モジュールを適用する

修正モジュールには、お客さまから報告された問題に対する回避策や解決方法が含まれています。トレンドマイクロでは、個々のお客さまに修正モジュールを提供します。修正モジュールは、`xxx.bin` の形式を使用します。

警告!

修正モジュールは、特定の問題を修正するために提供されるプログラムで、トレンドマイクロから個別に提供いたします。

手順

1. `SupportTool` フォルダを USB デバイスからローカルディスクにコピーします。
2. Trend Micro Portable Security 3 サポートツールを開きます。
3. [他の機能] タブに移動します。

   [他の機能] タブが表示されます。
4. [アップデートの適用] をクリックします。

   [アップデートの適用] 画面が開きます。
5. [修正モジュールを適用] を選択して、[次へ] をクリックします。

   [新しいコンポーネントの適用] 画面が開きます。
6. トレンドマイクロにより提供された修正モジュールを選択します。

7. [適用] をクリックします。

   確認画面が表示されます。

8. 別の検索ツールをアップデートするには、[はい] をクリックします。

   アップデートを終了するには [いいえ] を選択し、検索ツールを取り外してから再度接続してアップデートを有効にします。

Trend Micro Rescue Disk

Trend Micro Rescue Disk を使用すると、OS を起動せずにコンピュータを検索できます。OS の深層部に潜み駆除することが困難なセキュリティ上の脅威を見つけて削除できます。

OS の処理を妨げることなく、コンピュータのハードディスクの隠しファイル、システムドライバ、およびマスターブートレコード (MBR) を検索できます。Rescue Disk では、感染の疑いのあるシステムファイルを削除する前に、それらをメモリにロードしません。

注意

Trend Micro Rescue Disk は初期設定で、検出した脅威をローカルディスクに隔離します。ローカルディスクに情報を書き込まずに検索を実行したい場合は、検出時の処理を [検索のみ] に変更します。

詳細については、45 ページの「検索設定 (Rescue Disk)」を参照してください。

Rescue Disk でサポートされるファイルシステムは次のとおりです。

OS	ファイルシステム
Windows	NTFS および FAT

OS	ファイルシステム
Linux	EXT、EXT2、EXT3、EXT4 および XFS **注意** Rescue Disk は、サポート対象のファイルシステムにインストールされた任意の Linux ディストリビューションで実行できます。

手順 1: 準備

手順

1. USB デバイスをコンピュータに挿入します。
2. コンピュータを再起動します。
3. コンピュータが起動したら、BIOS または UEFI セットアップユーティリティを開きます。
4. メニューで [Boot]、[Boot Order]、または [Boot Options] を探して、[First Boot Device] を USB デバイスに変更します。
5. メニューを終了します。

   再起動後、Trend Micro Rescue Disk が自動的に開きます。

手順 2: Rescue Disk を使用する

手順

1. 再起動後、Trend Micro Rescue Disk が自動的に開きます。
2. <Enter> キーを押すか、しばらく待ちます。[Confirm Disk Log] 画面 (検索ログをローカルハードディスク上に残すことへの承認) が表示されます。

3. [Yes] を選択します。

   [Choose Action] 画面が表示されます。

4. [[1] Scan for Security Threats] を選択して、検索の種類を選択します。

   - [1] Quick Scan: ウイルスに感染しやすいフォルダ (Windows のシステムフォルダなど) のみを検索します
   - [2] Full Scan: すべてのフォルダを検索します

   自動的に検索が開始されるので、検索が終了するまで待ちます。

5. 脅威が検出された場合、「Are you sure you want to resolve these objects?」というメッセージが表示されます。

   [Yes] を選択して脅威を駆除します。

   注意

   確認メッセージは、次を行うように Rescue Disk を設定している場合にのみ表示されます。

   - 検索して隔離する
   - 隔離する前にユーザに通知する

6. 検索ログが検索ツールに保存されたら、コンピュータからの検索ツールの取り外しを確認します。

7. <Enter> キーを押して、コンピュータを再起動します。

検索ツールエージェント

検索ツールエージェントは、接続された検索ツールの処理を開始できるようにするためのサービスです。この処理には、コンピュータの検索、コンポーネントのアップデート、設定、および管理プログラムとの設定の同期が含まれます。処理は、検索ツールが接続されたときに開始することも、接続された検索ツールから定期的に開始するように予約することもできます。予約された処理は、検索ツールエージェントの設定に従って実施されます。検索ツールエージェントがインストールされたコンピュータに複数の検索ツール

が接続されている場合、その処理は 1 つずつ実行されます。つまり、複数の検索ツールが同時にアクティブになることはありません。

検索ツールエージェントが実行する処理には次のものがあります。

- 集中管理モードで設定されている検索ツールのアクティベーションの自動実行
- コンポーネントの自動アップデート
- 自動検索
- ログと設定の自動同期
- 定期的な検索
- 定期的なコンポーネントのアップデート

検索ツールエージェントは、最低限の処理が必要な環境、および通常使用時に画面が表示されないコンピュータで使用することをお勧めします。

ツール (STAgentConfigGen.exe) を使用して設定をカスタマイズし、インストールを実行する前のインストーラに保存できます。アクティベーションの自動実行が必要な場合は、このツールを使用できます。

重要

この機能は Windows コンピュータでのみ使用できます。

検索ツールエージェントをインストールする

検索ツールの `TMPS3 SYS` にある `TMPSAgent` フォルダがインストールパッケージです。インストールする前に検索ツールエージェントの設定をカスタマイズするには、後続の「インストールする前に設定をカスタマイズする」の項を参照してください。

検索ツールエージェントは、GUI またはコマンドプロンプトのいずれかを使用してインストールできます。

注意

既存の検索ツールエージェントをアップグレードしても、その設定は変更されません。

GUI を使用してインストールする場合:

手順

1. 検索ツールエージェントをインストールするコンピュータに検索ツールを接続します。
2. [TMPS3 SYS] ドライブで [TMPSAgent] フォルダを開き、Setup.exe ファイルをダブルクリックします。
3. セットアッププログラムにより Microsoft Visual C++ 2008 再頒布可能パッケージがシステムで確認され、必要であればパッケージをインストールするようメッセージが表示されます。
4. [使用許諾契約書] 画面が表示されたら、契約書を読み、[同意する] をクリックします。

   注意

   次に進む前に、検索ツール画面を閉じる必要があります。

5. [インストール先の指定] 画面が表示されたら、パスを直接入力するか、フォルダを参照して、[インストール] をクリックします。
6. [インストール完了] 画面が表示されたら、[終了] をクリックします。

   終了後、検索ツールエージェントの設定画面が初期設定で表示されます。この機能を無効にするには、[検索ツールエージェントのコンソールを開く] オプションをオフにします。

コマンドラインを使用してインストールする場合:

手順

1. 管理者権限で Windows のコマンドプロンプトを起動します。
2. TMPSAgent フォルダに移動して、実行したい操作のコマンドを入力します。

検索ツールエージェントをアンインストールする

検索ツールエージェントのアンインストールも、GUI またはコマンドプロンプトのいずれかを使用して実行できます。

注意

- 続行する前に、検索ツールがコンピュータに接続されていないことを確認してください。

  検索ツールエージェントをアンインストールする前に、Trend Micro Safe Lock のロックを解除します。

GUI を使用してアンインストールする場合:

手順

- Windows のコントロールパネルを使用して、検索ツールエージェントをアンインストールします。

コマンドラインを使用してアンインストールする場合:

手順

1. 管理者権限で Windows のコマンドプロンプトを起動します。
2. 検索ツールエージェントのインストールフォルダに移動して、次のコマンドを入力します。

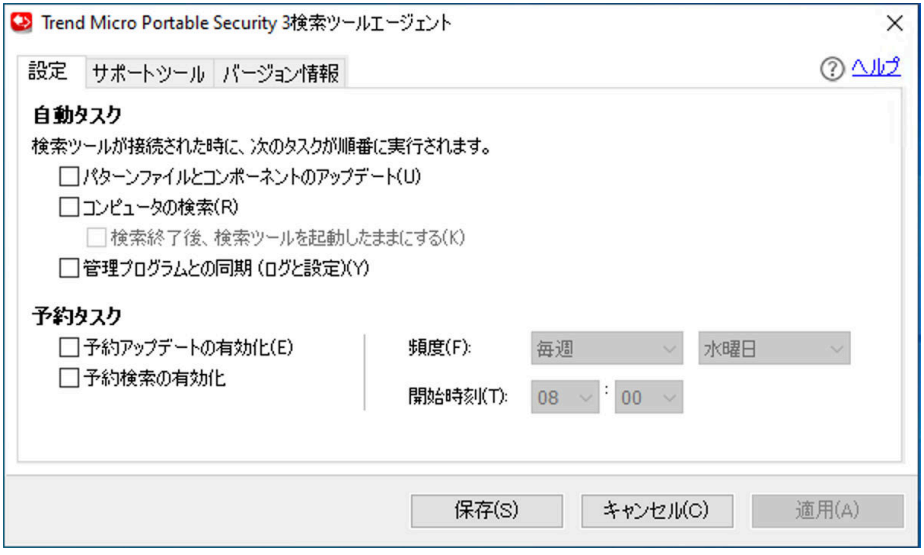
```
Uninstall.exe -silent
```

検索ツールエージェントのコンソール

重要

この機能は Windows コンピュータでのみ使用できます。

検索ツールエージェントのコンソールでは、コンピュータで検出された接続中の検索ツールについて、いくつかの基本的な自動タスクを実行できます。検索ツールエージェントを使用して、診断タスクを実行することもできます。



[設定] タブ

次の表で、[設定] タブで使用できるオプションについて概説します。

セクション	オプション
自動タスク	• セキュリティパターンファイルと検索コンポーネントのアップデート: 検索ツールのセキュリティパターンファイルと検索コンポーネントを自動的にアップデートする場合に選択します。 • コンピュータの検索: 検索を自動的に開始する場合に選択します。検索終了後ただちに検索結果を表示するには、[検索終了後、検索プログラムを常に起動したままにする] を選択します。 • 検索終了後、検索プログラムを常に起動したままにする: 検索終了後、ただちに検索ログを表示する場合に選択します。 **重要** • このオプションを選択すると、検索ツールエージェントによる同期や予約アップデートなどのすべての自動タスクが中断されます。 • 管理プログラムとの同期 (ログと設定): 検索ツールのログや設定を管理プログラムと同期する場合は、このオプションを選択します。 **注意** 検索ツールエージェントと管理プログラムがネットワークで接続されていることを確認してください。 **重要** この機能は、集中管理モードで動作する検索ツールでのみ使用できます。
予約タスク	• 予約アップデートの有効化: 頻度と開始時刻を指定して検索ツールをアップデートする場合に選択します。 • 予約検索の有効化: 頻度と開始時刻を指定してコンピュータを検索する場合に選択します。 **注意** 予約アップデートと予約検索の両方が有効な場合は、アップデートが最初に実行されます。両方のタスクが完了すると、検索ツール画面が自動的に閉じます。

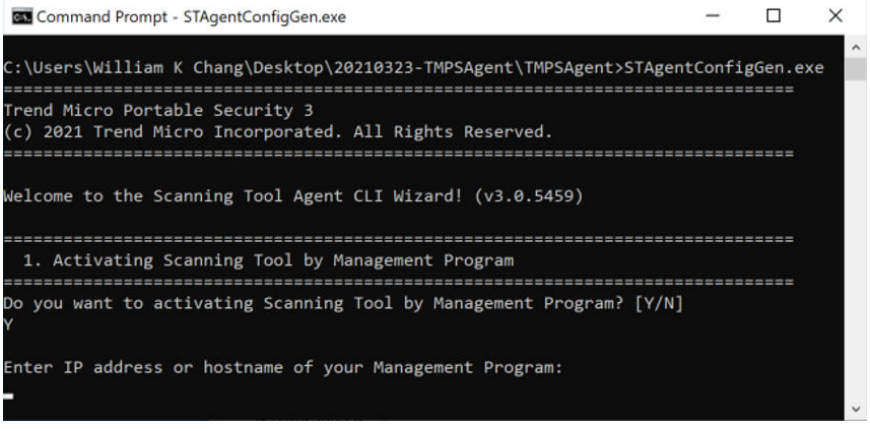
インストールする前に設定をカスタマイズする

検索ツールエージェントのインストールパッケージ (TMPSAgent フォルダ) には 2 つの実行可能ファイルがあります。`Setup.exe` はインストーラ、`STAgentConfigGen.exe` は設定をカスタマイズするためのウィザードモードツールです。

すべての設定は初期設定で無効になっています。自身のインストールパッケージ内で設定をカスタマイズするには、次の手順を実行します。設定をカスタマイズしたパッケージごとコンピュータにコピーして、検索ツールエージェントをインストールできます。

手順

1. 検索ツールを Windows コンピュータに接続して、`TMPSAgent` フォルダを USB デバイスからローカルディスクにコピーします。
2. Windows のメニューからコマンドプロンプトを起動し、コピーした `TMPSAgent` フォルダに移動して、`STAgentConfigGen.exe` を実行します。



注意

このウィザードでは最初に「アクティベーションの自動実行」を設定します。詳細については、後続の「検索ツールエージェント経由で検索ツールのアクティベーションを実行する」を参照してください。

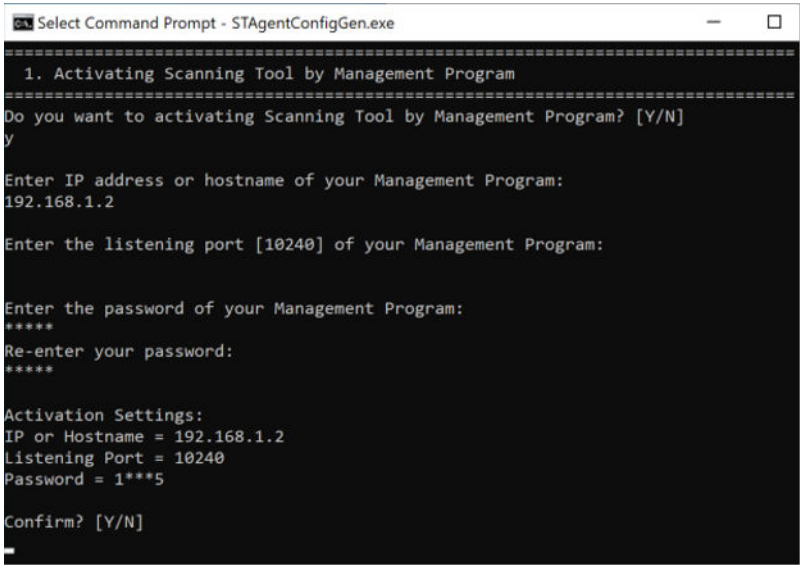
3. CLI ウィザードの指示に従って検索ツールエージェントを設定します。カスタマイズが完了した設定ファイル (tmps_agent_config.xml) は、ローカルのインストールパッケージに保存されます。
4. これで Setup.exe を実行できるようになります。

検索ツールエージェント経由で検索ツールのアクティベーションを実行する

アクティベーションが実行されていない 1 つまたは複数の検索ツールを、検索ツールエージェントがインストールされた Windows コンピュータに接続した場合、検索ツールエージェントの設定に従って管理プログラムのアクティベーションプロセスを自動的に実行することができます。

手順

- この機能は初期設定で無効になっており、インストール後は変更できません。この機能を使用するには、設定をカスタマイズする必要があります。



- 検索ツールエージェント経由で管理プログラムを使用して検索ツールのアクティベーションを実行するには、管理プログラムの IP アドレス/ホスト名、待機ポート、およびパスワードが必要です。

重要

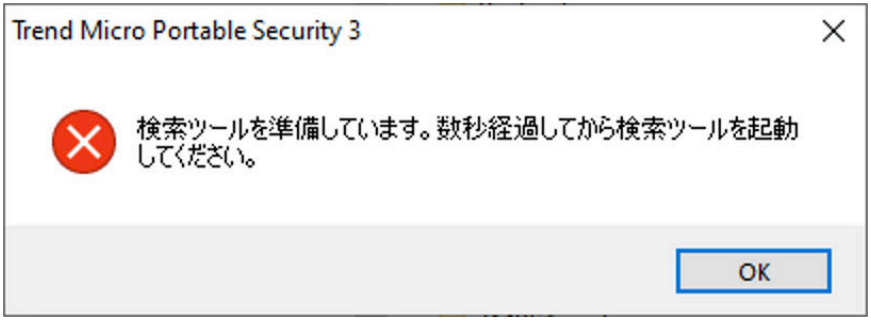
検索ツールエージェント経由で管理プログラムを使用して検索ツールのアクティベーションを実行するには、管理プログラムの IP アドレス/ホスト名、待機ポート、およびパスワードが必要です。

- アクティベーションの実行中、検索ツールの LED が数秒間青く点滅しますが、この時間は接続している Windows コンピュータによって異なることがあります。
- アクティベーションプロセスの実行中は検索ツールを取り外さないでください。
- アクティベーションが完了したかどうかを確認するには、TMPS3 SYS フォルダにある Launcher.exe を起動します。確認の終了後は、すべてのコンソールを適切に閉じてください。

  アクティベーションが実行された検索ツールでは、次のような画面が表示されます。

アクティベーションが実行されていない検索ツールでは、次のような画面が表示されます。設定が正しいことと、管理プログラムが使用可能なネットワークがあることを確認してください。

検索ツールエージェントが操作を実行中に Launcher.exe を実行すると、次のような警告メッセージが表示されます。



[サポートツール] タブ

トラブルシューティング情報を収集します。このツールはテクニカルサポートから指示があった場合のみ使用してください。

手順

1. 検索ツールエージェント画面で、[サポートツール] タブをクリックします。
2. [サポートツールの開始] をクリックします。
3. [デバッグの開始] をクリックして、情報の収集を開始します。
4. 調査している問題をコンピュータで再現します。
5. [デバッグの停止] をクリックして、システム情報の記録を停止します。

   サポートツールで最終的なシステムチェックが実行され、収集したログデータが ZIP パッケージに保存されます。
6. [フォルダを開く] をクリックして、ZIP パッケージを含むフォルダを開きます。
7. さらに分析するため、収集した情報をテクニカルサポートに送信します。

第 7 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。