Trend Micro Safe Lock™ 2.0 Service Pack 1 Patch 4

インストールガイド

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。

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

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、および Trend Micro Policy-based Security Orchestration は、トレンドマイクロ株式会社の登録商標です。

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

P/N: SLEM28556/181213_JP (2019/01)

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条例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 Safe Lock 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。

http://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 Safe Lock 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

はじめに

第 1 章：本製品の概要

第 2 章：ローカルエージェントのインストール

第 3 章：エージェント設定ファイルの配信

第 4 章：ローカルエージェントのアンインストール

第 5 章：テクニカルサポート

索引

はじめに

このインストールガイドでは、Trend Micro Safe Lock の概要を説明し、さらに管理者がインストールおよび管理するための手順を説明します。

この章の内容は次のとおりです。

ドキュメントについて

本製品には、次のドキュメントが付属しています。

表 1. Trend Micro Safe Lock のドキュメント

ドキュメント	説明
インストールガイド	製品の概要、インストール計画、インストール、設定の説明
管理者ガイド	製品の概要、設定、および製品環境を管理するために必要な詳細情報の説明
Readme ファイル	既知の制限事項に関する説明

マニュアルは、弊社の「最新版ダウンロード」サイトから入手することも可能です。

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

対象読者

Trend Micro Safe Lock のドキュメントは、Safe Lock の管理やエージェントをインストールする担当者を対象としています。これらのユーザがネットワークとサーバ管理に関する高度な知識を備えていることを前提としています。

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 2. 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
 重要	避けるべき操作や設定についての注意
 警告!	使用上の重要事項

第 1 章

本製品の概要

Trend Micro Safe Lock は、システムを特定用途化 (ロックダウン) することにより、不正プログラムの侵入や実行を防止します。また、使いやすいユーザインタフェースや製品連携機能を有しているため、迅速な導入と高い運用性を実現します。

この章の内容は次のとおりです。

Trend Micro Safe Lock について

Trend Micro Safe Lock は、産業用制御システム (ICS)、POS (Point of Sale) 端末、キオスク端末、ATM 機器のような特定用途のコンピュータを不正なソフトウェアや不正使用から保護します。本製品は使用するリソースの量が少なく、パフォーマンスへの影響やダウンタイムを最小限に抑えながら、特定用途のコンピュータを保護します。

新機能

Trend Micro Safe Lock 2.0 Service Pack 1 Patch 4 には、次の新機能および機能強化が含まれています。

表 1-1. Trend Micro Safe Lock 2.0 Service Pack 1 Patch 4 の新機能

機能	説明
Windows 10 October 2018 Update のサポート	Windows 10 October 2018 Update のサポートが追加されます。
ハッシュ確認のパフォーマンスの向上	DLL/ドライバ制御機能が強化され、許可リストに対して実行されるハッシュ確認のパフォーマンスが向上します。
許可リストのイベント処理機能の強化	許可リストが初期化されていない場合のイベント処理機能が強化されます。
許可リストの初期化時の除外設定	許可リストの初期化時にファイルの自動列挙からフォルダパスまたはファイル拡張子を除外するオプションが追加されます。

エージェントの機能と特徴

Trend Micro Safe Lock には、次の機能と特徴があります。

アプリケーション (プログラム、DLL ファイル、ドライバ、およびスクリプト) のロックダウン

Trend Micro Safe Lock で、アプリケーションのロックダウン時にアプリケーションの許可リスト (アプリケーションのホワイトリスト) に登録されていな

いプログラム、DLL ファイル、ドライバ、およびスクリプトの実行を許可しません。これにより、不正なソフトウェアの実行をブロックし、プログラムの予期しない使用を防ぐことで、生産性とシステムの整合性が向上します。制御対象とするスクリプトファイルはユーザが個別に指定することができます。

また、書き込み制御によりファイル/フォルダ/レジストリの変更や削除を防止します。

脆弱性攻撃対策

新しい脅威や未知の脅威だけでなく、Downad や Stuxnet などの既知の標的型攻撃の脅威は ICS やキオスクのコンピュータにおける重大なリスクです。最新の OS アップデートが行われていないシステムは、標的型攻撃に対して特に脆弱です。

Trend Micro Safe Lock は、不正侵入対策によってエージェントへの脅威の蔓延を防止し、実行防止対策によってエージェントでの脅威を防止します。

簡易オペレーション

ソフトウェアのインストールまたはアップデートが必要な場合は、許可リスト自動更新、および事前指定による許可リストの自動更新を使用することで、エージェントに加えた変更を許可リストに自動的に追加できます。これらの機能では Trend Micro Safe Lock をロック解除する必要はありません。

スモールフットプリント

大容量のパターンファイルを絶えずアップデートしなければならない他のエンドポイントセキュリティソリューションと比較すると、アプリケーションのロックダウンで使用するメモリやディスク容量は少なく、パターンファイルなどをダウンロードする必要もありません。

権限設定

管理者アカウントと制限付きユーザアカウントの 2 種類が用意されており、制限付きユーザアカウントが利用できる機能を制限することが可能です。

インタフェース

CLI (コマンドラインインタフェース) だけでなく、操作性や視認性の良い GUI (グラフィカルインタフェース) を提供します。

Trend Micro Portable Security 2 との互換性

初期状態で Trend Micro Portable Security 2 と互換性があるため、エージェントに侵入してくる脅威を簡単に削除できます。Trend Micro Portable Security のプログラムを許可リストに登録したり、エージェントをロック解除したりする必要はありません。

セルフプロテクション

セルフプロテクション機能を使用すると、Trend Micro Safe Lock が正常に機能するために必要なプロセスおよびその他のリソースを保護できます。この機能は、アプリケーションや実際のユーザが Trend Micro Safe Lock を無効化しようとする試みをブロックします。

セルフプロテクション機能は、以下のサービスを停止しようとするすべての試みをブロックします。

- Trend Micro Safe Lock サービス (`WkSrv.exe`)
- Trend Micro 不正変更防止サービス (`TMBMSRV.exe`)
- Trend Micro パーソナルファイアウォール (`TmPfw.exe`)

Safe Lock エージェントの要件

システム要件については、次の Web サイトを参照してください。

http://www.trendmicro.co.jp/jp/business/products/tmsl/index.html#requirement

エージェントがサポートする OS

システム要件については、次の Web サイトを参照してください。

http://www.trendmicro.co.jp/jp/business/products/tmsl/index.html#requirement

エージェントのアップグレード準備

警告!

アップグレード前に、選択したインストール方法およびインストール済みの Safe Lock エージェントのバージョンについて次に該当する処理を実行します。

最新のモジュールは以下の URL を参照してください。

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

表 1-2. インストール方法およびインストール済みのエージェントのバージョン別に要求されるアップグレード処理

インストール方法	インストール済みのエージェントバージョン	要求される処理	保持される設定
Windows インストーラを使用したローカルインストール	1.0	準備は不要です	保持される設定はありません
	1.1	準備は不要です	互換設定が保持されます
	2.0 以降	準備は不要です	保持される設定はありません
コマンドラインインタフェースインストーラを使用したローカルインストール	1.0	手動アンインストール	保持される設定はありません
	1.1	準備は不要です	互換設定が保持されます
	2.0 以降	手動アンインストール	保持される設定はありません

インストール方法	インストール済みのエージェントバージョン	要求される処理	保持される設定
リモートインストール 注意 Safe Lock では Safe Lock Intelligent Manager を使用したリモートインストールがサポートされます。	1.0	手動アンインストール	保持される設定はありません
	1.1	手動アンインストール	保持される設定はありません
	2.0 以降	手動アンインストール	保持される設定はありません

エージェント利用時の概要

Trend Micro Safe Lock はホワイトリストを使用したソリューションです。コンピュータをロックダウンして、許可リストに登録されていないプログラムが実行されないようにします。Safe Lock は、グラフィカルユーザインタフェース (GUI) を使用したエージェントのメイン画面か、コマンドラインを使用して設定および管理できます。システムのアップデートは、事前指定による許可リスト自動更新や許可リスト自動更新を使用して、エージェントでアプリケーション制御を解除せずに適用できます。

一般的な使用例は次のとおりです。

1. 許可リストを設定し、エージェントでアプリケーション制御を有効にして、未登録のアプリケーションの起動をブロックします。
2. 許可リスト自動更新を使用して、事前指定による許可リスト自動更新にインストーラが登録されていないソフトウェアをアップデートまたはインストールします。
3. 後でメンテナンスするために、制限付きユーザアカウントを設定して有効にします。

許可リストに登録されていないプログラムをユーザが実行しようとした場合、Trend Micro Safe Lock はそのプログラムの実行をブロックしますが、画面上にメッセージを表示することはありません。ただし、プログラムを実行し

た元のプログラムによって以下のようなメッセージが表示される場合があります。

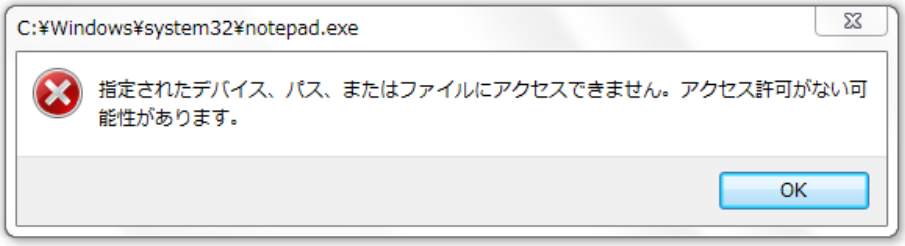


図 1-1. Trend Micro Safe Lock ブロックメッセージ

第 2 章

ローカルエージェントのインストール

この章では、ローカルの Trend Micro Safe Lock エージェントのインストールとセットアップの手順について説明します。

この章の内容は次のとおりです。

ローカルインストールの概要

手順

1. コンピュータが Trend Micro Safe Lock のシステム要件を満たしていることと、アップグレードの制限事項について確認します。

   詳細については、12 ページの「Safe Lock エージェントの要件」を参照してください。

   警告!

   Safe Lock のバージョンによっては、選択したインストール方法に応じて、アップグレード前に準備が必要になる場合があります。

   詳細については、13 ページの「エージェントのアップグレード準備」を参照してください。

2. 任意のインストール方法で、Trend Micro Safe Lock をインストールします。

   Trend Micro Safe Lock は、Windows インストーラ、またはコマンドラインからインストーラを実行してインストールできます。

   表 2-1. Trend Micro Safe Lock のローカルインストールの方法

インストール方法	メリット
Windows インストーラ	Windows インストーラは、初回または単一のインストール向けに簡易化されたインストールウィザードを提供します。 詳細については、20 ページの「Windows インストーラを使用したインストール」を参照してください。
コマンドライン	コマンドラインからインストールを実行する方法は、サイレントインストールや、大規模に展開するためのバッチファイル作成に適しています。 詳細については、29 ページの「コマンドラインを使用したインストール」を参照してください。

注意

Windows インストーラ、コマンドラインインタフェースのどちらでも、`setup.ini` ファイルを変更することで Trend Micro Safe Lock エージェントの設定をカスタマイズできます。

詳細については、32 ページの「インストールパラメータをカスタマイズする」を参照してください。

3. インストールしたエージェントを設定します。

   a. Trend Micro Safe Lock のメイン画面を開き、許可リストを設定します。

      Trend Micro Safe Lock によるエージェントの保護を開始するには、最初に、システムの正常な実行に必要な既存のアプリケーションおよびファイルを、エージェントの許可リストに追加する必要があります。

      詳細については、27 ページの「許可リストの設定」を参照してください。

   b. Trend Micro Safe Lock の設定を変更します。

      注意

      [アプリケーション制御] は許可リストの設定後に有効にする必要があります。

      詳細については、Trend Micro Safe Lock エージェントの管理者ガイドを参照してください。

   c. (オプション) アップデートされた設定を複数のエージェントに配信します。

      複数の Trend Micro Safe Lock エージェントに設定を配信するには、エージェント設定ファイルを使用します。

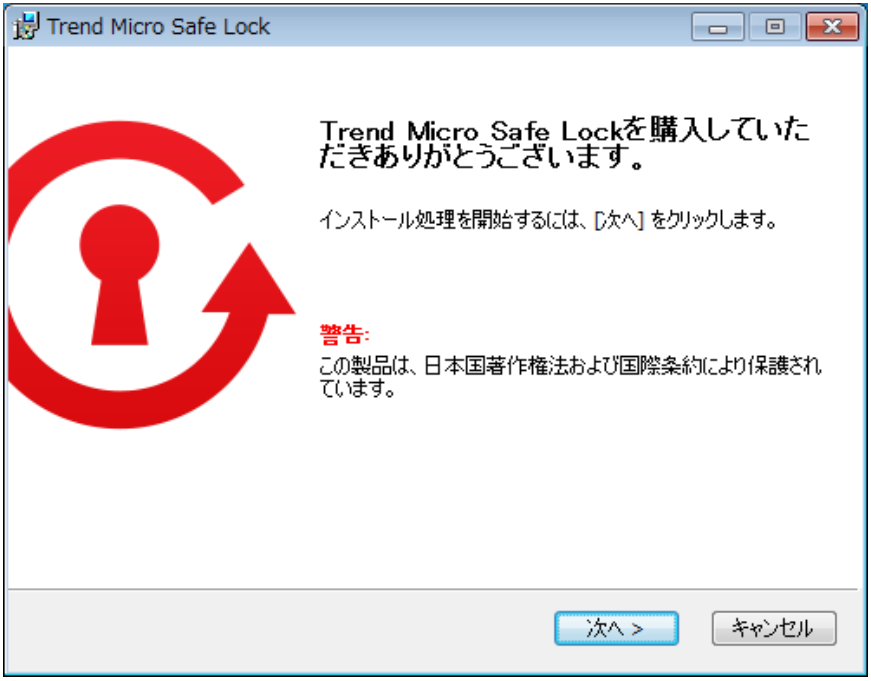
Windows インストーラを使用したインストール

Trend Micro Safe Lock をインストールするには、管理者権限のあるアカウントでログインする必要があります。

手順

1. `SL_Install.exe` をダブルクリックします。

   Windows の [ユーザー アカウント制御] の警告が表示される場合は、[はい] をクリックします。

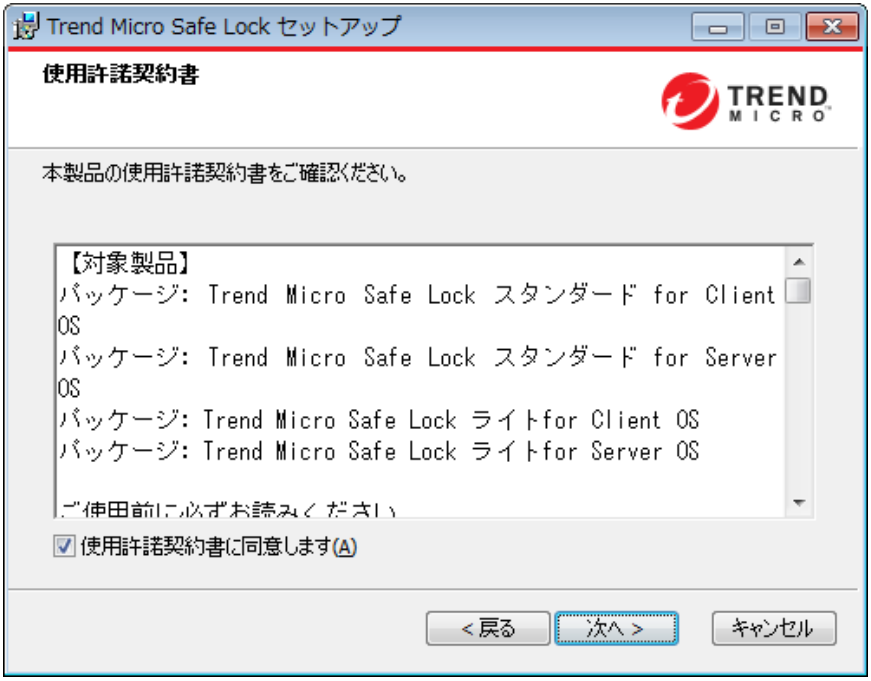


2. インストールウィザードが表示されたら、[次へ] をクリックします。

注意

コンピュータ上に別のバージョンの Trend Micro Safe Lock が存在する場合、インストーラはそれを削除してから最新バージョンをインストールします。

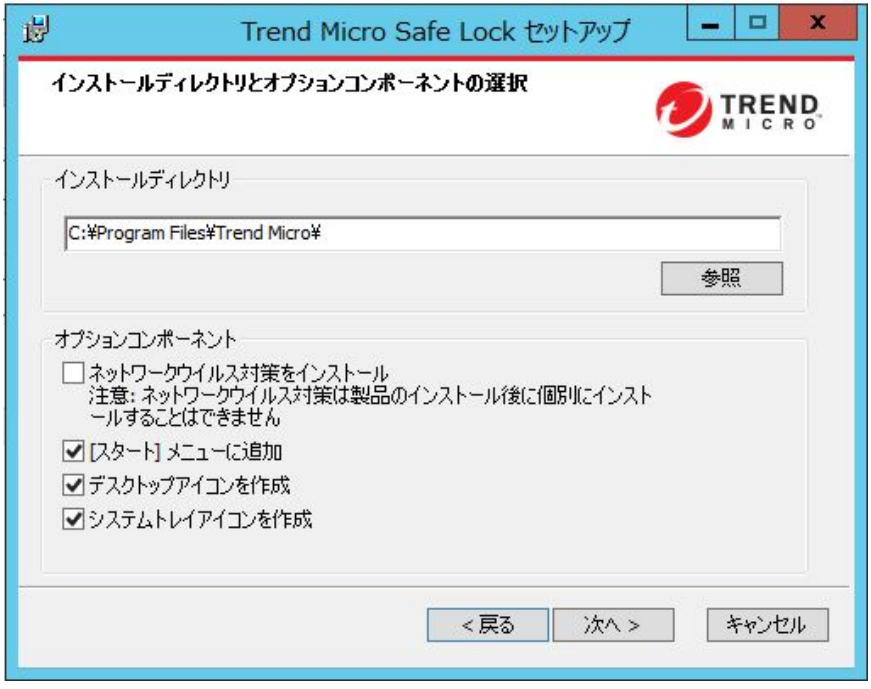
3. 使用許諾契約書を読み、[使用許諾契約書に同意します] を選択して [次へ] をクリックします。



4. インストールオプションを必要に応じて変更して、[次へ] をクリックします。

重要

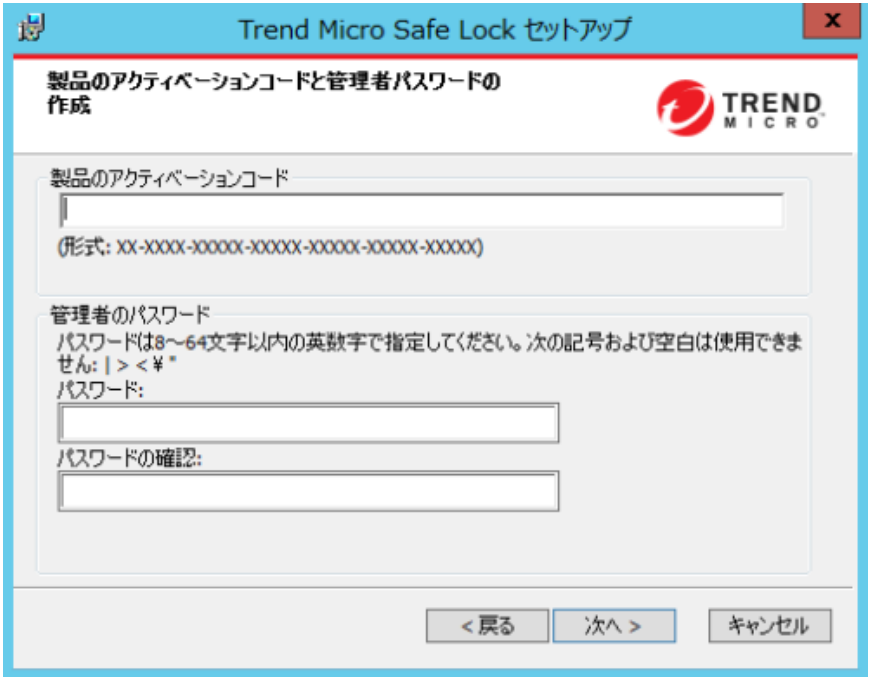
ネットワークウイルス対策をインストールできるのは初回のプログラムインストール時のみですが、必要に応じて後から無効にすることもできます。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。



5. Trend Micro Safe Lock のアクティベーションコードと管理者のパスワードを入力します。

注意

パスワードは 8～64 文字の英数字で指定してください。| > < \ "の記号および空白は使用できません。Trend Micro Safe Lock 管理者のパスワードは、Windows 管理者のパスワードとは別に設定されます。



警告!

Safe Lock 管理者のパスワードは忘れないようにしてください。Safe Lock 管理者のパスワードを忘れた場合は、OS を再インストールする必要があります。

6. [次へ] をクリックします。

インストールを続行する前に、コンピュータで事前に脅威を検索するかどうかを確認するメッセージが表示されます。

7. 必要に応じて、インストールを続行する前にコンピュータで脅威の事前検索を実行します。この検索は実行することをお勧めします。

   - コンピュータで脅威を検索するには、[検索する] をクリックします。

     a. [コンピュータの事前検索] 画面が表示されます。

     b. 検索設定をカスタマイズするには、[検索設定の編集] をクリックします。

     c. [検索開始] をクリックします。

        コンピュータの事前検索でセキュリティリスクが検出された場合は、インストールをキャンセルすることをお勧めします。コンピュータの脅威を削除してから、再度実行してください。重要なプログラムが脅威として検出された場合は、コンピュータが安全であることと、インストール済みのプログラムのバー

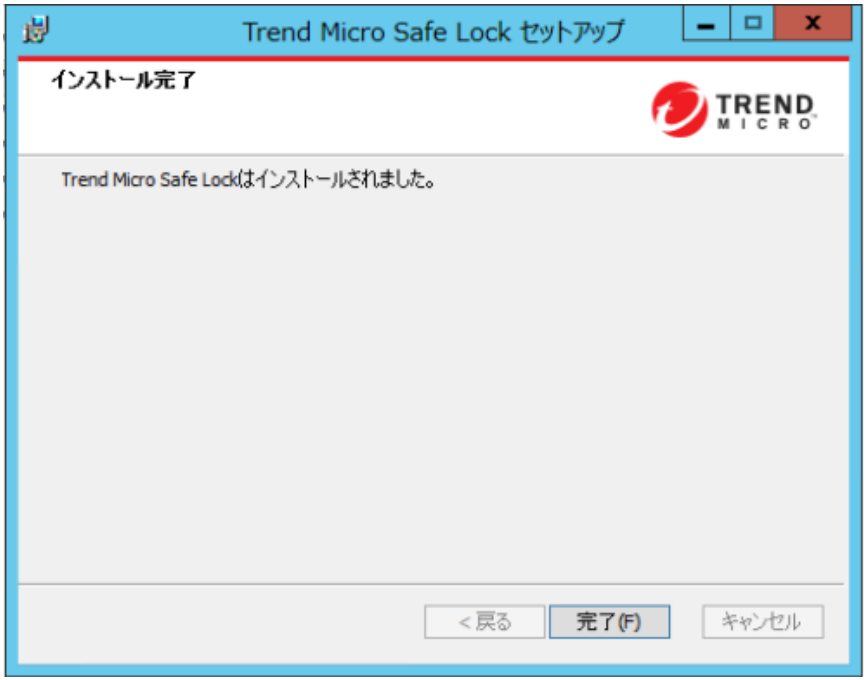
ジョンに脅威が含まれていないことを確認します。検出結果が誤検出であることが明らかな場合のみ、検出された脅威を無視します。

ヒント

トレンドマイクロは、脅威を検出して削除するためのソリューションを提供しています。ネットワークアクセスが制限または禁止されているコンピュータでは、Trend Micro Portable Security 2 を使用することをお勧めします。詳細については、12 ページの「Trend Micro Portable Security 2 との互換性」を参照してください。トレンドマイクロが提供するソリューションの詳細については、http://www.trendmicro.co.jp/jp/business/products/tmps2/index.html を参照してください。

- 検索を省略するには、[検索しない] をクリックします。

8. [インストール完了] 画面が表示されたら、[完了] をクリックします。



注意

Address Space Layout Randomization (ASLR) がサポートされていない、またはサポートが制限されている Windows XP や Windows Server 2003 などの以前の OS 対して、オプションでメモリのランダム化を有効にします。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。

許可リストの設定

Trend Micro Safe Lock でエージェントの保護を開始するには、最初に、エージェントをチェックしてシステムの正常な実行に必要なアプリケーションとファイルを確認する必要があります。

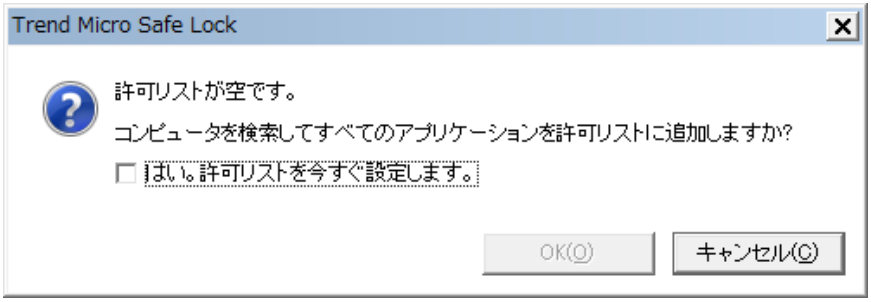
手順

1. Safe Lock のメイン画面を開きます。

   Safe Lock のログイン画面が表示されます。

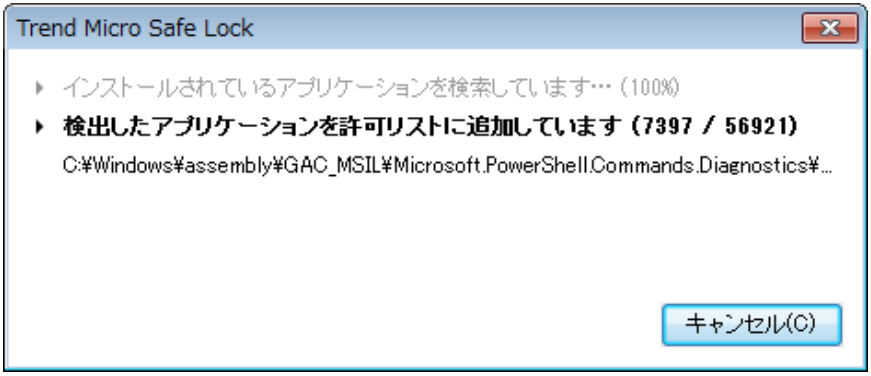
2. パスワードを入力して [ログイン] をクリックします。

   許可リストを今すぐ設定するかどうかを確認するメッセージが表示されます。

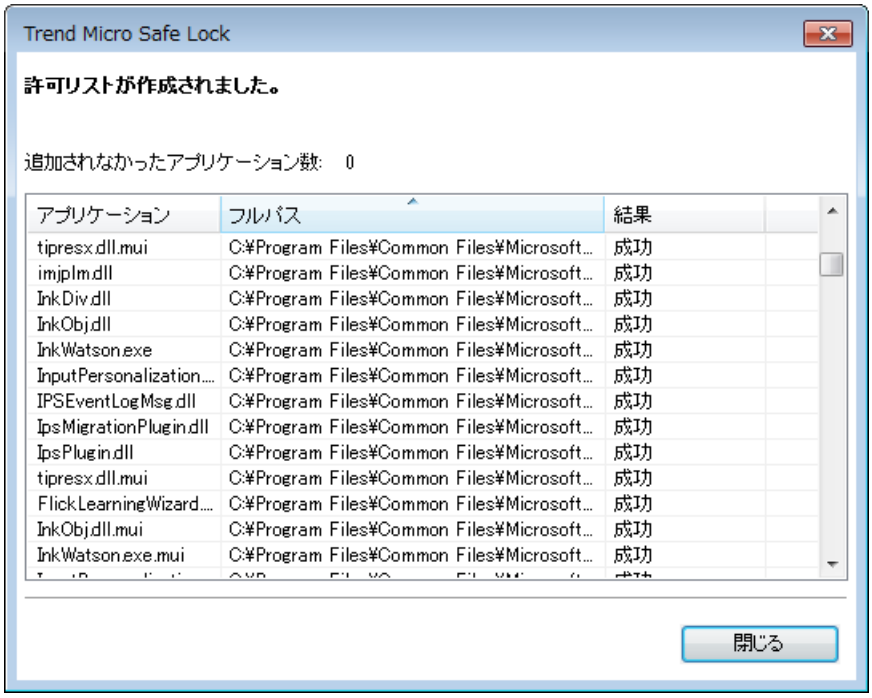


3. 通知ウィンドウで、[はい。許可リストを今すぐ設定します。] を選択して [OK] をクリックします。

   エージェントが検索され、すべてのアプリケーションが許可リストに追加されます。



許可リストの設定結果が表示されます。



注意

Trend Micro Safe Lock のアプリケーション制御が有効な場合は、許可リストに含まれるアプリケーションのみを実行できます。

4. [閉じる] をクリックします。

コマンドラインを使用したインストール

管理者は、サイレントインストールおよび大規模な展開を考慮して、コマンドラインから、またはバッチファイルを使用して Trend Micro Safe Lock をイン

ストールできます。大規模な展開の場合、カスタマイズされたインストールでは設定ファイルと許可リストが必要となることがあるため、最初に試験的にエージェントに Trend Micro Safe Lock をインストールすることを推奨します。許可リストと設定ファイルの詳細については、「Trend Micro Safe Lock 管理者ガイド」を参照してください。

警告!

- Safe Lock 管理者のパスワードは忘れないようにしてください。Safe Lock 管理者のパスワードを忘れた場合は、OS を再インストールする必要があります。
- Address Space Layout Randomization (ASLR) がサポートされていない、またはサポートが制限されている Windows XP や Windows Server 2003 などの以前の OS に対して、必ずメモリのランダム化を有効にしてください。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。

重要

ネットワークウイルス対策をインストールできるのは初回のプログラムインストール時のみですが、必要に応じて後から無効にすることもできます。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。

注意

パスワードは 8～64 文字の英数字で指定してください。| > < \ "の記号および空白は使用できません。Trend Micro Safe Lock 管理者のパスワードは、Windows 管理者のパスワードとは別に設定されます。

インストーラのコマンドラインインタフェースのパラメータ

次の表は、`SL_Install.exe` で使用可能なコマンド一覧を示しています。

表 2-2. Safe Lock インストーラのコマンドラインオプション

パラメータ	値	説明
`-q`		サイレントモードでインストールします

パラメータ	値	説明
-p	<administrator_password>	管理者パスワードを指定します
-d	<path>	インストールパスを指定します
-ac	<activation_code>	アクティベーションコードを指定します
-nd		デスクトップショートカットを作成しません
-fw		ネットワークウイルス対策を有効にします
-ns		[スタート] メニューにショートカットを追加しません
-ni		タスクトレイアイコンを非表示にします
-cp	<path>	Safe Lock 設定ファイルを指定します 注意 設定ファイルは Safe Lock のインストール後にエクスポートできます。
-lp	<path>	許可リストを指定します 注意 許可リストは、Safe Lock をインストールして許可リストを作成した後にエクスポートできます。
-qp	<path>	カスタム処理が「隔離」モードに設定されている場合に隔離ファイルのフォルダパスを指定します
-nrca		原因分析 (RCA) レポートを無効にします
-nps		事前検索を実行しないようにします。
-ips		事前検索によって脅威が検出されてもインストールを中止しません

コマンドラインインストールの例は、次のようになります。

```
SL_Install.exe -q -ac XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -p
P@ssW0Rd -nd
```

重要

インストールを続行するには、管理者のパスワードとアクティベーションコードを入力する必要があります。

インストールパラメータをカスタマイズする

Setup.ini ファイルを使用して初期設定のインストールパラメータを変更するには、次の手順に従います。

手順

1. インストールフォルダで Setup.ini ファイルを見つけます。
2. 必要に応じてインストールパラメータをカスタマイズします。

   インストールパラメータと設定可能な値の詳細については、33 ページの「インストールのカスタマイズ」を参照してください。
3. 重要な設定への無許可でのアクセスを防ぐため、必要に応じて、Setup.ini ファイルを暗号化します。

   a. インストールフォルダから、Setup.ini ファイルと WKSupportTool.exe ファイルをデスクトップにコピーします。

   b. コマンドプロンプトウィンドウを管理者として実行します。

   c. デスクトップに移動し、「`WKSupportTool.exe encryptsetupini Setup.ini Setup.bin`」と入力して Setup.ini ファイルを暗号化し、暗号化したファイルに「Setup.bin」という名前を付けます。

   d. Setup.bin ファイルをインストールフォルダに保存し、Setup.ini ファイルを削除します。

インストールのカスタマイズ

初期設定のインストールパラメータを変更するには、SL_Install.exe と同じフォルダに setup.ini という名前のテキストファイルを編集します。次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

注意

コマンドラインで指定した引数はセットアップファイルより優先されます。セットアップファイルは初期設定値より優先されます。たとえば、SL_Install.exe にスイッチ-nd が追加され、setup.ini に NO_DESKTOP=0 が含まれる場合は、スイッチが優先され、Safe Lock Intelligent Manager のデスクトップショートカットは作成されません。

Property セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-3. Setup.ini ファイルの [Property] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
ACTIVATION_CODE	アクティベーションコード	<activation_code>	<空白>	なし
NO_DESKTOP	デスクトップにショートカットを作成します	• 0: ショートカットを作成します • 1: ショートカットを作成しません	0	なし
NO_STARTMENU	[スタート] メニューにショートカットを作成します	• 0: ショートカットを作成します • 1: ショートカットを作成しません	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
NO_SYSTRAY	システムトレイアイコンと Windows 通知を表示します	• 0: システムトレイにアイコンを作成します • 1: システムトレイにアイコンを作成しません	0	なし
NO_NSC	ファイアウォールをインストールします	• 0: ファイアウォールを作成します • 1: ファイアウォールを作成しません	0	なし
CONFIG_PATH	設定ファイルのパス	<path>	<空白>	なし
LIST_PATH	インポートする許可リストのパスです	<path>	<空白>	なし
APPLICATION FOLDER	エージェントプログラムのインストールパスです	<path>	<空白>	なし
MANAGED_MODE	Trend Micro Safe Lock を Safe Lock Intelligent Manager サーバで管理するかどうかを指定します	• 0: スタンドアロンモード • 1: 集中管理モード	0	なし
PASSWORD	SLCmd.exe と Trend Micro Safe Lock のメイン画面で使用するパスワード	<password>	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
CUSTOM_ACTION	ブロックしたイベントに対するカスタム処理です	• 0: 無視 • 1: 隔離 • 2: サーバに確認	0	なし
QUARANTINE_FOLDER_PATH	エージェントプログラムの隔離パスです	<path>	<空白>	なし
ROOT_CAUSE_ANALYSIS	原因分析レポートを有効にします	• 0: 無効 • その他の値: 有効	1	なし
INTEGRITY_MONITOR	変更監視を有効にします	• 0: 無効 • 1: 有効	0	なし
PREDEFINED_TRUSTED_UPDATER	事前指定による許可リスト自動更新を有効にします	• 0: 無効 • 1: 有効	0	なし
WINDOWS_UPDATE_SUPPORT	Windows Update サポートを有効にします	• 0: 無効 • 1: 有効	0	なし
PRESCAN	Trend Micro Safe Lock をインストールする前に対象コンピュータを事前検索します	• 0: コンピュータを事前検索しません • 1: コンピュータを事前検索します	1	なし
MAX_EVENT_DB_SIZE	データベースファイルの最大サイズ (MB)	正の整数	1024	なし
WEL_SIZE	Windows イベントログのサイズ (KB)	正の整数	10240	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		注意 インストールしたエージェントの初期設定値です。Safe Lock をアップグレードしても、以前のインストールで設定されたユーザ指定の WEL_SIZE 値は変更されません。		
WEL_RETENTION	イベントログのサイズが [Windows イベントログ] の最大値に達したときの [Windows イベントログ] のオプションです	Windows XP 以前のプラットフォームの場合: • 0: 必要に応じてイベントを上書きします • 1〜365: 指定した日数 (1〜365 日) よりも古いイベントを上書きします • -1: イベントを上書きしません (ログは手動で消去します) Windows Vista 以降のプラットフォームの場合: • 0: 必要に応じてイベントを上書きします (最も古いイベントから)	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		• 1: ログがいっぱいになったらアーカイブし、イベントを上書きしません • -1: イベントを上書きしません (ログは手動で消去します)		
WEL_IN_SIZE	変更監視イベントの Windows イベントログのサイズ (KB)	正の整数	10240	なし
WEL_IN_RETENTION	変更監視イベントのイベントログのサイズが [Windows イベントログ] の最大値に達したときの [Windows イベントログ] のオプションです	Windows XP 以前のプラットフォームの場合: • 0: 必要に応じてイベントを上書きします • 1〜365: 指定した日数 (1〜365 日) よりも古いイベントを上書きします • -1: イベントを上書きしません (ログは手動で消去します) Windows Vista 以降のプラットフォームの場合: • 0: 必要に応じてイベントを上書きします (最も古いイベントから)	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		• 1: ログがいっぱいになったらアーカイブし、イベントを上書きしません • -1: イベントを上書きしません (ログは手動で消去します)		
USR_DEBUGLOG_ENABLE	ユーザセッションのデバッグログを有効にします	• 0: ログに記録しません • 1: ログに記録します	0	なし
USR_DEBUGLOGLEVEL	ユーザセッションに許可されたデバッグログエントリの数です	• 273	273	なし
SRV_DEBUGLOG_ENABLE	サービスセッションのデバッグログを有効にします	• 0: ログに記録しません • 1: ログに記録します	0	なし
SRV_DEBUGLOGLEVEL	サービスセッションに許可されたデバッグログエントリの数です	• 273	273	なし
SILENT_INSTALL	サイレントモードでインストールを実行します	• 0: サイレントモードを使用しません • 1: サイレントモードを使用します	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化

	 重要
	サイレントモードを使用するには、ACTIVATION_CODE および PASSWORD のキーと値も指定する必要があります。例:
	`[PROPERTY]`
	`ACTIVATION_CODE=XX-XXXXX-XXXXX-XXXXX-XXXXX`
	`PASSWORD=P@ssW0Rd`
	`SILENT_INSTALL=1`			

STORAGE_DEVICE_BLOCKING	管理下のエージェントへの CD/DVD ドライブ、フロッピーディスクドライブやネットワークドライブなどのストレージデバイスによるアクセスをブロックします	• 0: ストレージデバイスのアクセスを許可します • 1: ストレージデバイスのアクセスをブロックします	0	なし
INIT_LIST	インストール時に許可リストを初期化します	• 0:インストール時に許可リストを初期化しません • 1:インストール時に許可リストを初期化します	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	注意 LIST_PATH は INIT_LIST より優先されます。 例: [PROPERTY] LIST_PATH=liststore.db INIT_LIST=1 この場合、liststore.db はインポートされますが、INIT_LIST は無視されます。			
INIT_LIST_PATH	許可リストの初期化で横断するフォルダパスで、空白の場合は各ローカルディスクのルートディレクトリを横断します	<フォルダパス>	<空白>	なし
INIT_LIST_PATH_OPTIONAL	許可リストの初期化で横断するフォルダパスで、空白の場合は各ローカルディスクのルートディレクトリを横断します	<フォルダパス>	<空白>	なし
INIT_LIST_EXCLUDED_FOLDER	許可リストの初期化時にファイルの自動列挙から除外するフォルダの絶対パスです この設定は許可リストの最初の初期化と、それ	<フォルダパス>	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	以降のすべての許可リストのアップデートに適用されます 複数のフォルダを指定する場合は、INIT_LIST_EXCLUDED_FOLDER から始まる名前で新しいエントリを作成します。各エントリの名前は一意にします。次に例を示します INIT_LIST_EXCLUDED_FOLDER=c:\folder1 INIT_LIST_EXCLUDED_FOLDER2=c:\folder2 INIT_LIST_EXCLUDED_FOLDER3=c:\folder3	注意 • 最大 260 文字まで指定できます。 • 存在しないフォルダパスを指定することもできます。 • 除外はサブフォルダには適用されません。		
INIT_LIST_EXCLUDED_EXTENSION	許可リストの初期化時にファイルの自動列挙から除外するファイルの拡張子です この設定は許可リストの最初の初期化と、それ以降のすべての許可リストのアップデートに適用されます	<ファイル拡張子> 注意 実行可能ファイルのファイル拡張子 (例: exe、dll、sys) を指定すると、アプリケーション制御で問題が発生する場合があります。	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	複数の拡張子を指定する場合は、INIT_LIST_EXCLUDED_EXTENSION から始まる名前で新しいエントリを作成します。各エントリの名前は一意にします。次に例を示します INIT_LIST_EXCLUDED_EXTENSION=bmp INIT_LIST_EXCLUDED_EXTENSION2=png			
LOCKDOWN	インストール後にアプリケーション制御を有効にします	• 0:アプリケーション制御を無効にします • 1:アプリケーション制御を有効にします	0	なし
FILELESS_ATTACK_PREVENTION	ファイルレス攻撃対策機能を有効にします	• 0: 機能を無効にします • 1: 機能を有効にします	0	なし
SERVICE_CREATION_PREVENTION	サービス作成対策機能を有効にします	• 0: 機能を無効にします • 1: 機能を有効にします	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	注意 Safe Lock は、次の場合にサービス作成対策機能を一時的に無効にします。 • 許可リスト自動更新によって許可されたインストーラを使用して、新しいアプリケーションをアップデートまたはインストールする場合。許可リスト自動更新のプロセス完了後、自動的に本機能が再度有効になります。 • Windows Update サポートを有効にしている場合。Windows Update サポートを無効にすると、自動的に本機能が再度有効になります。			
VERIFY_PATCH_SIGNATURE	続行する前に、Safe Lock Intelligent Manager から受信した Patch の署名を検証します。	• 0: Patch の署名を検証しません • 1: Patch の署名を検証します • 2 またはその他: Windows 7 以降では Patch の署名を検証しますが、Windows Vista 以前では検証をスキップします	2	なし
USR_DEBUGLOG_ENABLE	ユーザセッションのデバッグログを有効にします	• 0: デバッグログを無効にします • 1: デバッグログを有効にします	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
USR_DEBUGLOGLEVEL	ユーザセッションのデバッグレベル	273	273	なし
SRV_DEBUGLOG_ENABLE	サービスセッションのデバッグログを有効にします	• 0: デバッグログを無効にします • 1: デバッグログを有効にします	0	なし
SRV_DEBUGLOGLEVEL	サービスセッションのデバッグレベル	• 273	273	なし
FW_USR_DEBUGLOG	ファイアウォールのユーザセッションのデバッグログを有効にします	• 0: デバッグログを無効にします • 1: デバッグログを有効にします	0	なし
FW_USR_DEBUGLOG_LEVEL	ファイアウォールのユーザセッションのデバッグレベル	数値	273	なし
FW_SRV_DEBUGLOG_ENABLE	ファイアウォールのサービスセッションのデバッグログを有効にします	• 0: デバッグログを無効にします • 1: デバッグログを有効にします	0	なし
FW_SRV_DEBUGLOG_LEVEL	ファイアウォールのサービスセッションのデバッグレベル	数値	273	なし
BM_SRV_DEBUGLOG_ENABLE	挙動監視コアサービスのデバッグログを有効にします	• 0: デバッグログを無効にします • 1: デバッグログを有効にします	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
BM_SRV_DEBUGLOG_LEVEL	挙動監視コアサービスのデバッグレベル	• 51	51	なし

EventLog セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-4. Setup.ini ファイルの [Eventlog] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
ENABLE	Trend Micro Safe Lock のイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
LEVEL_WARNINGLOG	Trend Micro Safe Lock の警告レベルのイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
LEVEL_INFORMATIONLOG	Trend Micro Safe Lock の情報レベルのイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	0	なし
BLOCKEDACCESSLOG	Trend Micro Safe Lock でブロックされたファイルをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
APPROVEDACCESSLOG	Trend Micro Safe Lock で許可されたファイ	• 1: ログに記録します	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	ルをログに記録します	• 0: ログに記録しません		
APPROVEDACCESSLOG_TRUSTEDUPDATER	許可リスト自動更新で許可されたアクセスをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
APPROVEDACCESSLOG_TRUSTEDHASH	信頼するハッシュで許可されたアクセスをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
APPROVEDACCESSLOG_DLLDRIVER	DLL/ドライバ制御で許可されたアクセスをログに記録します	• 1: ログに記録します • 0: ログに記録しません	0	なし
APPROVEDACCESSLOG_EXCEPTIONPATH	アプリケーション制御除外パスで許可されたアクセスをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
APPROVEDACCESSLOG_TRUSTEDCERT	信頼するデジタル証明書で許可されたアクセスをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
APPROVEDACCESSLOG_WRITEPROTECTION	書き込み制御で許可されたアクセスをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
SYSTEMEVENTLOG	Trend Micro Safe Lock のシステムに関連するイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
SYSTEMEVENTLOG_EXCEPTIONPATH	アプリケーション制御の機能に関連するイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
SYSTEMEVENTLOG_WRITEPROTECTION	書き込み制御の機能に関連するイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
LISTLOG	許可リストに関連するイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
USBMALWAREPROTECTIONLOG	USB 不正プログラム対策を作動させるイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
EXECUTIONPREVENTIONLOG	実行防止対策を作動させるイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
NETWORKVIRUSPROTECTIONLOG	ネットワークウイルス対策を作動させるイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_FILECREATED	変更監視のファイルおよびフォルダ作成イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG	変更監視のファイル変更イベン	• 1: ログに記録します	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
_FILEMODIFIED	トをログに記録します	• 0: ログに記録しません		
INTEGRITYMONITORINGLOG_FILEDELETED	変更監視のファイルおよびフォルダ削除イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_FILERENAMED	変更監視のファイル名およびフォルダ名変更イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGVALUEMODIFIED	変更監視のレジストリ値変更イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGVALUEDELETED	変更監視のレジストリ値削除イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGKEYCREATED	変更監視のレジストリキー作成イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGKEYDELETED	変更監視のレジストリキー削除イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし
INTEGRITYMONITORINGLOG_REGKEYRENAMED	変更監視のレジストリキー名変更イベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし

KEY	説明	使用可能な値	初期設定値	暗号化
DEVICECONTROLLOG	デバイスアクセスコントロールに関連するイベントをログに記録します	• 1: ログに記録します • 0: ログに記録しません	1	なし

Server セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-5. Setup.ini ファイルの [Server] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
HOSTNAME	サーバのホスト名	<host_name>	<空白>	なし
PORT_FAST	高速接続用のサーバの待機ポート	1 - 65535	<空白>	なし
PORT_SLOW	低速接続用のサーバの待機ポート	1 - 65535	<空白>	なし
CERT	証明書ファイル名	<certificate_file_name>	<空白>	なし
API_KEY	API キー	<API_key>	<空白>	なし

Agent セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-6. Setup.ini ファイルの [Agent] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
PORT	エージェントの待機ポート	1 - 65535	<空白>	なし
SSL_ALLOW_BEAST	SSL3 プロトコルと TLS 1.0 プロトコルの BEAST 攻撃に対するセキュリティ脆弱性に対応します	• 0: BEAST 攻撃から保護されます • 1: BEAST 脆弱性に対するセキュリティ対策を実装しません	1	なし
POLL_SERVER	エージェントを NAT エージェントとして識別します	• 0: 非 NAT エージェント • 1: NAT エージェント	0	なし
POLL_SERVER_INTERVAL	NAT 接続の頻度を設定します	• 1 - 64800: Safe Lock サーバに (1 - 64800) 分ごとに接続します	10	なし

注意

POLL_SERVER のステータスは、次のいずれかを実行して NAT エージェントから非 NAT エージェントに切り替えることもできます。

- SLCmd.exe コマンドを実行する
- 別のエージェントの設定をインポートする

Message セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-7. Setup.ini ファイルの [Message] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
REGISTER_TRIGGER	メッセージトリガを登録します	• 1: ただちに開始 • 2: 手動	1	なし
UNREGISTER_TRIGGER	メッセージトリガの登録を解除します	• 1: ただちに開始 • 2: 手動	1	なし
UPDATESTATUS_TRIGGER	ステータスメッセージのトリガをアップデートします	• 1: ただちに開始 • 2: 手動	1	なし
UPLOADBLOCKEDEVENT_TRIGGER	ブロックされたイベントメッセージのトリガをアップロードします	• 1: ただちに開始 • 2: 手動	1	なし
CHECKFILEHASH_TRIGGER	ファイルハッシュメッセージのトリガを確認します	• 1: ただちに開始 • 2: 手動	1	なし
QUICKSCANFILE_TRIGGER	ファイルメッセージのトリガをクイック検索します	• 1: ただちに開始 • 2: 手動	1	なし
INITIAL_RETRY_INTERVAL	Intelligent Manager にイベントの再送信を試行する間隔 (秒) の初期設定値です。この間隔は、MAX_RETRY_INTERVAL 値に達するまで、試行が失敗するた	• 0 ～ 2147483647	120	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	びに倍増します。			
MAX_RETRY_INTERVAL	Intelligent Manager にイベントの再送信を試行する間隔 (秒) の最大値です。	• 0 ～ 2147483647	7680	なし

MessageRandomization セクション

注意

Safe Lock エージェントは、可能なかぎり速やかに Safe Lock Intelligent Manager からの要求に応答します。詳細については、Trend Micro Safe Lock 管理者ガイドの「メッセージタイムグループを適用する」を参照してください。

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-8. Setup.ini ファイルの [MessageRandomization] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
TOTAL_GROUP_NUM	サーバコントロールで制御されるグループ数	0 - 2147483646	0	なし
OWN_GROUP_INDEX	このエージェントが所属するグループのインデックス	0 - 2147483646	0	なし
TIME_PERIOD	エージェントがデータをアップロード	0 - 2147483647	0	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	する最長時間 (秒単位)			

Proxy セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-9. Setup.ini ファイルの [PROXY] セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
MODE	プロキシのモード	• 0: プロキシを使用しません • 1: 手動設定でプロキシを使用します • 2: Internet Explorer から自動的に取得された設定でプロキシを使用します	0	なし
HOSTNAME	プロキシホスト名	<host_name>	<空白>	なし
PORT	プロキシポート番号	1 - 65535	<空白>	なし
USERNAME	プロキシユーザ名	<user_name>	<空白>	なし
PASSWORD	プロキシのパスワード	<password>	<空白>	なし

Prescan セクション

次の表は、setup.ini (セットアップファイル) で使用可能なコマンド一覧を示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

表 2-10. Setup.ini ファイルの[PRESCAN]セクションの引数

KEY	説明	使用可能な値	初期設定値	暗号化
IGNORE_THREAT	事前検索中に不正プログラムを検出したらインストールを取り消します 注意 サイレントインストールのみで有効です。	• 0: キャンセル • 1: 事前検索中に不正プログラムを検出してもインストールを続行します	0	なし
REPORT_FOLDER	事前検索の結果レポートを保存するフォルダの絶対パスです	• <folder_path> • <空白>: 初期設定は%windir%¥temp¥prescan¥log です	<空白>	なし
SCAN_TYPE	サイレントインストール中に実行する検索の種類です	• Full: コンピュータのすべてのフォルダを検索します • Quick: 次のフォルダを検索します • 固定ルートドライブ 例:	Full	なし

KEY	説明	使用可能な値	初期設定値	暗号化
	注意 選択した値は UI インストールの初期設定値として使用されます。	C:¥ d:¥ • システムのルートフォルダ 例: c:¥Windows • システムフォルダ 例: c:¥Windows¥System • System32 フォルダ 例: c:¥Windows¥System32 • ドライバフォルダ 例: c:¥Windows¥System32¥Drivers • 一時フォルダ 例: c:¥Users¥Trend¥AppData¥Local¥Temp • デスクトップフォルダ (サブフォルダとファ		

KEY	説明	使用可能な値	初期設定値	暗号化
		イルを含む) 例: c:¥Users¥Trend¥Desktop • Specific: SPECIFIC_FOLDER エントリで指定したフォルダを検索します		
COMPRESS_LAYER	圧縮ファイルを検索する際の圧縮階層数です	• 0: 圧縮ファイルは検索しません • 1 - 20: 指定された階層数まで圧縮ファイルを検索します	2	なし
MAX_FILE_SIZE	検索可能な最大ファイルサイズです	• 0: すべてのサイズのファイルを検索します • 1 - 9999: 指定したサイズ (MB) 以下のファイルのみを検索します	0	なし
SCAN_REMOVABLE_DRIVE	リムーバブルドライブを検索する	• 0: リムーバブルドライブを検索しない • 1: リムーバブルドライブを検索する	0	なし
SPECIFIC_FOLDER	検索の種類が [Specific] の場合に検索するフォルダの絶対パスです	<folder_path> SPECIFIC_FOLDER で始まる名前の新しいエントリを作成することにより複数の	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		フォルダを指定できます。各エントリ名は一意である必要があります。 例: SPECIFIC_FOLDER=c:\folder1 SPECIFIC_FOLDER2=c:\folder2 SPECIFIC_FOLDER3=c:\folder3		
EXCLUDED_FILE	検索から除外するファイルの絶対パスです	<file_path> EXCLUDED_FILE で始まる名前の新しいエントリを作成することにより複数のファイルを指定できます。各エントリ名は一意である必要があります。 例: EXCLUDED_FILE=c:\file1.exe EXCLUDED_FILE2=c:\file2.exe EXCLUDED_FILE3=c:\file3.exe	<空白>	なし
EXCLUDED_FOLDER	検索から除外するフォルダの絶対パスです	<folder_path> EXCLUDED_FOLDER で始まる名前の新しいエントリを作成することにより複数のフォルダを指定できます。各エントリ名	<空白>	なし

KEY	説明	使用可能な値	初期設定値	暗号化
		は一意である必要があります。 例: EXCLUDED_FOLDER=c:\file1.exe EXCLUDED_FOLDER2=c:\file2.exe EXCLUDED_FOLDER3=c:\file3.exe		
EXCLUDED_EXTENSION	検索から除外するファイル拡張子です	<file_extension> EXCLUDED_EXTENSION で始まる名前の新しいエントリを作成することにより複数の拡張子を指定できます。各エントリ名は一意である必要があります。 例: EXCLUDED_EXTENSION=bmp EXCLUDED_EXTENSION2=png	<空白>	なし

BlockNotification セクション

次の表は、setup.ini (セットアップファイル) で使用可能な通知コマンドを示しています。セットアップファイルで値を指定しない場合は、初期設定値が使用されます。

詳細については、33 ページの「Property セクション」を参照してください。

重要

この機能を有効にする場合は、必ず、システムトレイアイコンと通知の表示も有効にしてください。詳細については、この表の「NO_SYSTRAY」を参照してください。

表 2-11. Setup.ini ファイルの[BlockNotification]セクションの引数

キー	説明	使用可能な値	初期設定値	暗号化
ENABLE	Safe Lock が許可されていないファイルをブロックしたときに管理下のエージェントに通知を表示します。	• 0: 無効 • 1: 有効	0	なし
ALWAYS_ON_TOP	開かれている画面の上部にポップアップ通知を表示します。	• 0: 無効 • 1: 有効	1	なし
SHOW_DETAILS	通知にファイル名、ファイルパス、およびイベント時間を表示します。	• 0: 無効 • 1: 有効	1	なし
AUTHENTICATE	通知を閉じるときに管理者パスワードを要求して、ユーザを認証します。	• 0: 無効 • 1: 有効	1	なし
TITLE	通知のタイトル	<notification_title>	<空白>	なし
MESSAGE	通知内容	<notification_content>	<空白>	なし

第 3 章

エージェント設定ファイルの配信

この章では、エージェント設定ファイルを使用して複数の Trend Micro Safe Lock エージェントに設定を配信する方法について説明します。

スタンドアロンエージェントへの配信

スタンドアロンモードでインストールされたエージェントは Trend Micro Safe Lock Intelligent Manager サーバによって管理されません。単一の設定を複数の**スタンドアロン**エージェントに手動で配信するには、エージェント設定ファイルを使用します。

設定ファイルをエクスポートまたはインポートする

注意

Trend Micro Safe Lock では、エクスポート前に設定ファイルを暗号化します。ユーザは、設定ファイルを復号してから内容を変更する必要があります。

詳細については、Safe Lock エージェントの管理者ガイドを参照してください。

手順

1. Trend Micro Safe Lock のデスクトップアイコン、または [スタート] メニューから [すべてのプログラム] > [Trend Micro Safe Lock] をクリックして、メイン画面を開きます。
2. パスワードを指定して [ログイン] をクリックします。
3. [設定] メニュー項目をクリックして [設定のエクスポート/インポート] セクションにアクセスします。

   設定ファイルをエクスポートするには

   a. [エクスポート] をクリックして、ファイルの保存場所を選択します。

   b. ファイル名を指定して、[保存] をクリックします。

   設定ファイルをインポートするには

   a. [インポート] をクリックして、設定ファイルを指定します。

   b. ファイルを選択して、[開く] をクリックします。

Trend Micro Safe Lock の既存の設定が、設定ファイルの内容で上書きされます。

Intelligent Manager を使用した配信

集中管理モードでインストールされたエージェントは Trend Micro Safe Lock Intelligent Manager サーバによって管理されており、サーバからすべての管理対象エージェントにリモートでコマンドを発行できます。複数の管理対象エージェントにエージェントの設定を配信するには、Trend Micro Safe Lock Intelligent Manager の管理サーバ画面を起動して、[エージェント管理] 画面にある [コマンドの送信] メニューを使用します。

エージェントの設定をリモートでエクスポートする

Intelligent Manager からエージェントの設定と許可リストをエクスポートしダウンロードすることで、それらをリモートで取得できます。

手順

1. Intelligent Manager の管理サーバ画面で [エージェント] をクリックします。

   [エージェント管理] 画面が表示されます。

2. 対象のエージェントを選択します。

3. [コマンドの送信] をクリックして、[設定のエクスポート] を選択し、次のいずれかを選択します。

   - 許可リスト
   - エージェントの設定

   Intelligent Manager がコマンドの発行を開始します。[詳細] ポップアップウィンドウで進行状況を確認できます。

4. 複数の設定をエクスポートするには、上記手順を繰り返します。

エクスポートが完了すると、画面上部に次のメッセージが表示されます。

5. [詳細を表示] をクリックして、エクスポートされた設定をダウンロードします。

注意

Intelligent Manager は、最大 20 セットのエクスポートされた設定を保持できます。ダウンロードされたファイルはリストから消去されます。

エージェントの設定をリモートでインポートする

Trend Micro Safe Lock Intelligent Manager の管理サーバ画面からエージェントまたはエージェントグループに新しい設定をリモートで適用できます。この機能により次のことが可能になります。

- エージェントの設定をリモートで上書きする
- 許可リストをリモートで上書きする
- 許可する項目を許可リストにリモートで追加する

手順

1. カスタマイズするエージェントの設定ファイルまたは許可リストを準備します。

   a. エージェントの設定ファイルまたは許可リストをエクスポートしてダウンロードします。手順の詳細については、63 ページの「エージェントの設定をリモートでエクスポートする」を参照してください。

   b. ダウンロードしたファイルをカスタマイズします。

注意

正常にインポートするため、インポートするファイルが次の要件を満たしていることを確認します。

- CSV 形式で UTF-8 エンコーディングを使用している
- 許可リストの場合、サポートされるファイルの最大サイズは 20MB
- エージェントの設定ファイルの場合、サポートされるファイルの最大サイズは 1MB

2. Trend Micro Safe Lock Intelligent Manager の管理サーバ画面で [エージェント] をクリックします。

   [エージェント管理] 画面が表示されます。

3. カスタマイズしたファイルを 1 つ以上のグループ未設定エージェントまたは異なるグループ内のエージェントにインポートするには、次の手順を実行します。

   a. エージェント列でエージェントを 1 つ以上選択します。

   b. [コマンドの送信] をクリックします。

   c. [設定のインポート] を選択します。

   d. [許可リスト] または [エージェントの設定] を選択します。

      インポートダイアログが表示されます。

4. カスタマイズしたファイルをエージェントグループにインポートするには、次の手順を実行します。

   a. 左のパネルでエージェントグループを右クリックし、[コマンドの送信] > [設定のインポート] の順に選択します。

   b. [許可リスト] または [エージェントの設定] を選択します。

      インポートダイアログが表示されます。

5. 初期設定で、Trend Micro Safe Lock Intelligent Manager では以下が実行されます。

   - 許可リスト: カスタマイズした許可リストから対象の許可リストに項目が累積されます。対象の許可リストをカスタマイズした許可リ

ストで置き換えるには、[既存の許可リストを上書き] をオンにします。

- エージェントの設定: カスタマイズした許可リストで対象の許可リストが上書きされます。

6. [参照] をクリックして、カスタマイズしたファイルを選択します。
7. [インポートして適用] をクリックします。

第 4 章

ローカルエージェントのアンインストール

この章では、Trend Micro Safe Lock エージェントのアンインストール手順について説明します。

この章の内容は次のとおりです。

エージェントを Windows からアンインストールする

注意

エージェントから Trend Micro Safe Lock をアンインストールするには、管理者パスワードが必要です。

手順

1. Safe Lock エージェントがインストールされたエージェントで、Trend Micro Safe Lock のセットアップを起動します。

   お使いの OS に応じて、次のいずれかを実行します。

オプション	説明
次のいずれかの OS を使用している場合: • Windows 10 Enterprise • Windows 10 IoT Enterprise • Windows 10 Professional • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 October 2018 Update (Redstone 5)	a. [スタート] > [設定] の順に選択します。 b. Windows 10 のバージョンに応じて、次のいずれかのカテゴリから [アプリと機能] セクションを見つけます。 • システム • アプリ c. 左側のペインで [アプリと機能] をクリックします。 d. 表示されるリストで [Trend Micro Safe Lock] を選択します。 e. [アンインストール] をクリックします。
次のいずれかの OS を使用している場合: • Windows Server 2016 • Windows Server 2012 • Windows Server 2008 • Windows Storage Server 2016	a. [スタート] > [コントロール パネル] > [プログラムと機能] の順に選択します。 b. 表示されるリストで [Trend Micro Safe Lock] をダブルクリックします。

オプション	説明
• Windows 8 • Windows 7 • Windows Vista	
次のいずれかの OS を使用している場合: • Windows Server 2003 • Windows XP • Windows 2000	a. [スタート] > [コントロール パネル] > [プログラムの追加と削除] の順に選択します。 b. 表示されるリストで [Trend Micro Safe Lock] を選択します。 c. [削除] をクリックします。

Trend Micro Safe Lock のセットアップがアンインストーラモードで開きます。

2. Safe Lock のセットアップが開いたら、[次へ] をクリックします。
3. Safe Lock 管理者パスワードを指定して、[次へ] をクリックします。
4. Trend Micro Safe Lock のアンインストールが完了したら、[完了] をクリックします。

第 5 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。

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

トレンドマイクロでは、最新のセキュリティニュースをインターネットで公開しています。トレンドマイクロのセキュリティニュースでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティニュースは、次の URL からアクセスできます。

https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html

- ウイルス名やキーワードから検索できる脅威データベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティニュースに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

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専門のスタッフが解析し、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。

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。

索引