Trend Micro Safe Lock™ Intelligent Manager 2.0 Service Pack 1 Patch 4

管理者ガイド

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: SLEM28557/181213_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：Safe Lock エージェントの管理

第 3 章：Safe Lock の監視

第 4 章：各種の管理設定

第 11 章：トラブルシューティングとよくある質問 (FAQ)

第 12 章：テクニカルサポート

第 13 章：付録: 参照

索引

はじめに

この管理者ガイドでは、Trend Micro Safe Lock Intelligent Manager について紹介するとともに、製品管理のあらゆる側面について説明します。

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 Intelligent Manager 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 Intelligent Manager のドキュメントは、Safe Lock Intelligent Manager 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

用語

次の表は、Trend Micro Safe Lock Intelligent 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。

表 3. Safe Lock Intelligent Manager の用語

用語	説明
サーバプログラム	Safe Lock Intelligent Manager のサーバプログラムです。
サーバコンピュータ	Safe Lock Intelligent Manager サーバがインストールされているホストです。

用語	説明
エージェント	Safe Lock クライアントプログラムを実行しているホストです。
NAT エージェント	ネットワークアドレス変換 (NAT) 機能が有効なルータの下に構成されたエージェントです。
管理対象エージェント 管理下のエージェント	Safe Lock Intelligent Manager サーバプログラムが認識している、Safe Lock クライアントプログラムを実行しているホストです。
対象エージェント	Safe Lock Intelligent Manager の管理対象エージェントをインストールするホストです。
管理者 (または Safe Lock Intelligent Manager 管理者)	Safe Lock Intelligent Manager サーバを管理している人物です。
管理サーバ画面	Safe Lock Intelligent Manager の設定や管理対象エージェントを設定して管理するユーザインタフェースです。
CLI	コマンドライン
ライセンスのアクティベーション	Safe Lock Intelligent Manager サーバのインストールの種類と、アプリケーションの使用許諾期間が含まれます。
エージェントのインストールフォルダ	Safe Lock エージェントのファイルが含まれるホスト上のフォルダです。インストール時に初期設定を使用すると、インストールフォルダは次の場所になります。 `"c:¥Program Files¥Trend Micro¥Safe Lock"`
サーバのインストールフォルダ	Safe Lock Intelligent Manager サーバファイルが含まれるホスト上のフォルダです。インストール時に初期設定を使用すると、インストールフォルダは次の場所になります。 `"c:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager"`

第 1 章

本製品の概要

Trend Micro Safe Lock Intelligent Manager 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 Intelligent Manager について

Trend Micro Safe Lock Intelligent Manager は、Safe Lock エージェントのインストール、ステータスおよびイベントの集中管理を実現します。たとえば、エージェントのインストールや、最初の許可リストの作成、アプリケーション制御の変更を、管理者はリモートで実行できます。さらに、Safe Lock Intelligent Manager で不正プログラム検索を実行したり、Safe Lock エージェントによって実行をブロックされたファイルの原因の情報を表示したりすることで、イベントの確認に必要な手間と時間を減らし、管理者が即座に対応できるようにします。

新機能

Trend Micro Safe Lock Intelligent Manager 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 Intelligent Manager 2.0 Service Pack 1 Patch 4 の新機能

機能	説明
Trend Micro Control Manager (以下、Contorol Manager) との統合	Safe Lock Intelligent Manager を Control Manager 7.0 と統合し、Control Manager から次の操作を実行できます。 • Control Manager の資格情報を使用して Safe Lock Intelligent Manager の管理サーバ画面にシングルサインオン • Safe Lock Intelligent Manager のダッシュボードウィジェットを表示
接続されていないエージェントの通知	Safe Lock Intelligent Manager はエージェントの接続ステータスを監視します。この設定を有効にすると、接続されていないエージェントが見つかった場合に Safe Lock Intelligent Manager から通知を送信できます。

サーバの機能と特徴

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

表 1-2. 機能と特徴

機能	特徴
ダッシュボード	管理サーバ画面のダッシュボードには、監視下の Safe Lock エージェントについての概要情報が表示されます。インストール済みの Safe Lock エージェントのステータスを簡単に確認でき、指定された期間内の Safe Lock エージェントのアクティビティについてセキュリティレポートを生成できます。
代理ウイルス検索	Trend Micro Intelligent Manager は、Safe Lock エージェントでブロックされたアプリケーションのウイルス検索を実行します。そして、検索したファイルに対しリモートでの削除、隔離、許可リストへの追加が実行できます。
エージェントの集中管理	Trend Micro Intelligent Manager では、管理者は次のタスクを実行できます。 • Safe Lock エージェントステータスの監視 • 接続ステータスの確認 • 設定の表示 • 手動またはポリシーによるエージェントログの収集 • エージェントのアプリケーション制御のリモートでのオン/オフ • 許可リストの初期化 • エージェントへの Patch の配信 • 信頼するファイルの追加
イベントの集中管理	Safe Lock エージェントで保護されたコンピュータでは、管理者がイベントやステータスを監視し、ファイルの実行がブロックされた場合はそれに対処できます。Safe Lock Intelligent Manager にはイベント管理機能があり、管理者はこれを使用して、ブロックされたファイルイベントを把握して管理できます。たとえば、追跡のために未処理や処理済みのマークをイベントに付けたり、問題の解決に必要な情報を簡単に収集したりできます。

機能	特徴
原因情報の分析	ファイルのブロックが重大な問題に起因するものかどうかを判断できます。Safe Lock Intelligent Manager では不正プログラムの検索機能や原因情報/原因分析図が提供されるため、ブロックされたファイルを調査できます。たとえば、ブロックされたファイルがミッションクリティカルなプログラムの起動に必要かどうか、不正プログラムとして検出されたのかどうかを確認できます。また、ブロックされたファイルの実行元や、ファイルを起動したプロセスも確認できる場合があります。
監査	Safe Lock Intelligent Manager の管理サーバ画面にアクセスするためのアカウントで実行された操作を監査することが可能です。Safe Lock Intelligent Manager では各アカウントの操作をログに記録して、ログインしたユーザ、設定を変更したユーザ、イベントログを削除したユーザなどを追跡できます。

Safe Lock Intelligent Manager 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

サーバアカウントの概要

Trend Micro Safe Lock Intelligent Manager では、管理サーバ画面にアクセスするためのアカウントにいくつかの権限と制限を適用できます。これらのアカウントを使用して Safe Lock Intelligent Manager を設定し、Safe Lock エージェントを監視または管理できます。

次の表は、一般的な Safe Lock Intelligent Manager のタスクと、その実行に必要なアカウントの権限を示しています。

	タスク	必要な権限
1	Safe Lock Intelligent Manager アカウントの追加	• 管理者

	タスク	必要な権限
2	リモート配信ツール (SLrst.exe) を使用した、サーバからのエージェントの一元的な配信	• なし 注意 SLrst.exe ツールを使用する際は特定のアカウント権限は不要ですが、タスクの配信には Safe Lock エージェントのパスワードが必要です。
3	Safe Lock Intelligent Manager の管理サーバ画面とリモート配信ツール (SLtasks.exe) を使用した、Safe Lock エージェントの許可リストと書き込み制御リストの管理	• 管理者 • フルコントロール
4	サーバイベントログの監視	• 管理者 • フルコントロール • ストレージデバイスコントロールの管理のみ • アプリケーション制御の管理のみ
5	エージェントイベントログの監視	• 管理者 • フルコントロール • ストレージデバイスコントロールの管理のみ • アプリケーション制御の管理のみ • 読み取りのみ

	タスク	必要な権限
6	Safe Lock エージェントインストーラのダウンロード	• 管理者 • フルコントロール • ストレージデバイスコントロールの管理のみ • アプリケーション制御の管理のみ • 読み取りのみ
7	管理者パスワードのリモートでの変更	• 管理者
8	Safe Lock Intelligent Manager のライセンス情報の更新	• 管理者 • フルコントロール
9	エージェントへの Patch の配信	• 管理者 • フルコントロール
10	信頼するファイルの追加	• 管理者 • フルコントロール
11	アプリケーション制御の管理	• 管理者 • フルコントロール • アプリケーション制御の管理のみ
12	ストレージデバイスコントロールの管理	• 管理者 • フルコントロール • ストレージデバイスコントロールの管理のみ

	タスク	必要な権限
13	接続の確認	• 管理者 • フルコントロール • ストレージデバイスコントロールの管理のみ • アプリケーション制御の管理のみ • 読み取りのみ

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 1-3. 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。

機能	説明
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。

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 1-4. 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

Safe Lock エージェントのアップデートでサポートされる方法

Safe Lock エージェントは、現在のバージョンに応じてさまざまな方法でアップデートできます。

表 1-5. Safe Lock エージェントのアップデートでサポートされる方法

現在のバージョン	対象バージョン	SAFE LOCK エージェントのアップデートでサポートされる方法			
		ローカルインストール		リモートインストール	
		インストーラを使用	PATCH モジュールを使用	リモートセットアップツール	リモートタスクツール
1.1	最新バージョン	✓			
2.0			✓	✓	
2.0 Patch 1			✓	✓	
2.0 SP 1			✓	✓	✓
2.0 SP1 Patch 1			✓	✓	✓
2.0 SP1 Patch 2			✓	✓	✓
2.0 SP1 Patch 3			✓	✓	✓

注意

Windows Server 2003 以前のバージョンで Safe Lock Intelligent Manager を実行している場合は、TLSv10 を有効にする HotFix (`tmsl_20_win_jp_hfb_enforce_TLSv10.exe`) を適用して、Intelligent Manager とエージェントの間に存在する可能性のある接続の問題を解決することをお勧めします。詳細については、法人カスタマーサイトを参照してください。

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。

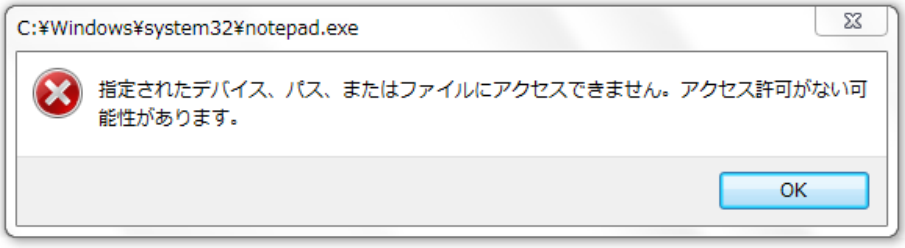


図 1-1. Trend Micro Safe Lock ブロックメッセージ

第 2 章

Safe Lock エージェントの管理

この章では、エージェント管理を行う管理サーバ画面の概要について説明します。

この章の内容は次のとおりです。

[エージェント管理] 画面について

[エージェント管理] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。この画面では、Safe Lock Intelligent Manager によって管理されているエージェントのリストが表示され、設定タスクを実行できます。

詳細については、次の各項を参照してください。

- 30 ページの「エージェントツリーを管理する」
- 36 ページの「エージェントを設定する」

エージェントツリーを管理する

Safe Lock Intelligent Manager では、エージェントツリーを編成して Safe Lock エージェントの情報を管理できます。

表 2-1. エージェントツリーの管理タスク

タスク	詳細
エージェントの検索	詳細については、31 ページの「エージェントを検索する」を参照してください。
エージェントグループの作成	詳細については、32 ページの「エージェントをグループ化する」を参照してください。
エージェントグループの削除	詳細については、33 ページの「エージェントとグループを削除する」を参照してください。
個別のエージェント情報の表示	詳細については、33 ページの「エージェントのステータスと設定を確認する」を参照してください。
エージェントまたはグループの移動	1 つ以上のエージェントまたはグループを選択して、[移動] をクリックします。
タグの編集	エージェントの識別と検索に役立つタグを編集します。 詳細については、35 ページの「タグを編集する」を参照してください。

タスク	詳細
エージェントの設定と概要のエクスポート (CSV 形式)	1 つ以上のエージェントを選択して、[エクスポート] をクリックします。

エージェントを検索する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [エージェント管理] 画面が表示されます。

2. ドロップダウンリストから条件を選択し、必要に応じて検索条件を追加して、特定のエージェントを検索します。

   ヒント

   Safe Lock Intelligent Manager では文字列の部分一致がサポートされます。

オプション	説明
エージェント	特定のエージェントを指定するには、エージェントの完全なホスト名を入力します。
タグ	タグ名を入力します。
IP アドレス	IPv4 アドレスを入力します。
IP アドレスの範囲	IPv4 アドレスを入力します。
OS	OS を選択します。
アプリケーション制御の状態	アプリケーション制御の状態を、[アプリケーション制御が有効です] または [アプリケーション制御が無効です] から選択します。
前回の接続	初期設定の期間を選択するか、[カスタム] を選択して時間範囲を独自に指定します。

3. 必要に応じて [検索] をクリックします。

   Safe Lock Intelligent Manager に検索条件と一致するホストがすべて表示されます。

エージェントをグループ化する

複数エージェントの管理を容易にするため、場所、種類、または目的に応じてエージェントをグループ化します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [エージェント管理] 画面が表示されます。

2. 左側のツリーで、サブグループを追加するグループフォルダをクリックし、[グループの追加] をクリックします。

   注意

   - グループ名は 64 文字以内で設定してください。
   - グループツリーには最大 9 階層のサブフォルダを、各グループ階層には最大 1000 フォルダを作成できます。

3. ツリーで [すべてのエージェント] をクリックし、表からエージェントを選択して [移動] をクリックします。

   ヒント

   または、エージェントやグループをツリー内の別のグループにドラッグアンドドロップします。

エージェントとグループを削除する

Safe Lock Intelligent Manager サーバでグループの削除、エージェントのグループ設定解除、またはエージェントの削除を行います。

エージェントはアンインストール時に Safe Lock Intelligent Manager から削除されます。ただし、Safe Lock Intelligent Manager からエージェントを削除する前にエージェントをアンインストールできなかった場合、エージェントは引き続き [エージェント管理] 画面に表示されます。今後 Safe Lock Intelligent Manager で管理しないエージェントを監視対象エージェントのリストから削除するには、[削除] 機能を使用します。

注意

監視対象エージェントのリストからエージェントを削除しても、既存のエージェントイベントログは削除されません。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [エージェント管理] 画面が表示されます。

2. 削除するグループ、グループ設定解除するエージェント、またはサーバから削除するエージェントをリストから選択します。

3. [削除] をクリックします。

4. 選択した操作に対する確認メッセージが表示されます。

   リストからエージェントが削除されます。

エージェントのステータスと設定を確認する

[エージェント管理] 画面では管理下のエージェントの次の情報を検索できます。

- エージェント情報: IP アドレス、OS およびタグが含まれます。

- エージェントの概要: 許可リストの最終アップデート日時、NAT の頻度、NAT の最終接続時間、ライセンス状況、ライセンス有効期限、エージェントのバージョン、エージェントの最終アップグレード日時などの概要情報が含まれます。
- エージェントの設定: 現在のエージェントの設定と最終変更日時が含まれます。
- 保留コマンド: Intelligent Manager との次回接続時に NAT エージェントに配信されるコマンドのリストです。接続間隔の設定の詳細については、232 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。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [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クリックします。

   [エージェントステータス] 画面が表示されます。

注意

[エクスポート] 機能を使用すると、エージェント情報をカンマ区切りのテキスト (.csv) ファイルにエクスポートしてダウンロードできます。

タグを編集する

エージェントの識別と検索に役立つタグを編集できます。

タグを編集するには、次の手順に従います。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [エージェント管理] 画面が表示されます。

2. 1 つ以上のエージェントを選択します。
3. [タグの編集] をクリックします。
4. エージェントタグを入力または編集します。

   ヒント

   Safe Lock Intelligent Manager ではタグに区切り文字を使用しません。

5. [OK] をクリックします。

エージェントを設定する

[エージェント管理] 画面の [コマンドの送信] メニューを使用すると、エージェントの設定を制御できます。

表 2-2. Safe Lock エージェントのコマンド

タスク	詳細
アプリケーション制御の設定	詳細については、37 ページの「アプリケーション制御のステータスをリモートで変更する」を参照してください。
デバイスコントロールの設定	管理下のエージェントへのストレージデバイス (CD/DVD ドライブ、フロッピーディスクドライブおよびネットワークドライブ) によるアクセスの許可またはブロック 1 つ以上のエージェントを選択して、[コマンドの送信] > [デバイスコントロールの設定] をクリックします。
信頼するファイルの追加	リストに追加されたすべてのファイルとインストーラの、ハッシュ値に基づく実行を許可するようにエージェントを設定 詳細については、38 ページの「信頼するアプリケーションとファイルをリモートで登録する」を参照してください。
許可リストのアップデート	選択したエージェントの許可リストの再作成による許可リストのアップデート 詳細については、40 ページの「Safe Lock エージェントの許可リストをアップデートする」を参照してください。

タスク	詳細
イベントログの収集	詳細については、41 ページの「イベントログを収集する」を参照してください。
接続の確認	選択した Safe Lock エージェントの接続ステータスの確認 詳細については、41 ページの「エージェントの接続を確認する」を参照してください。
設定のエクスポート	許可リストまたは選択したエージェントの設定のエクスポート 詳細については、42 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。
設定のインポート	許可リストまたは選択したエージェントの設定のインポート 詳細については、43 ページの「エージェントの設定をリモートでインポートする」を参照してください。
エージェントへの Patch の配信	Patch ファイルのアップロードによる選択したエージェントのアップグレード 詳細については、45 ページの「Safe Lock エージェントにリモートで Patch を配信する」を参照してください。

アプリケーション制御のステータスをリモートで変更する

注意

Safe Lock エージェントの管理者は、Safe Lock エージェントのメイン画面からアプリケーション制御のステータスを変更することもできます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。
2. 単一エージェントの場合は、エージェント名をクリックしてステータスの詳細を表示し、ボタンをクリックしてアプリケーション制御のステータスを変更します。

- アプリケーション制御を有効にする
- アプリケーション制御を無効にする

3. 複数エージェントおよびグループの場合は、該当する項目を [エージェント管理] の表で選択し、[コマンドの送信]→[アプリケーション制御の設定] の順に選択し、ボタンをクリックしてアプリケーション制御のステータスを変更します。
   - 有効
   - 無効

信頼するアプリケーションとファイルをリモートで登録する

ハッシュ値を使用して、管理対象エージェントのアプリケーションやファイルの実行をリモートで許可できます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [エージェント管理] 画面が表示されます。

2. 1 つまたは複数のエージェントやグループを選択します。
3. [コマンドの送信] をクリックして、[信頼するファイルの追加] を選択します。

   [信頼するファイルの追加] 画面が表示されます。

4. [ファイルハッシュ生成ツールのダウンロード] をクリックして、ハッシュ値を計算するためのツールをダウンロードします。

   手順の詳細については、39 ページの「ハッシュ値を計算する」を参照してください。

5. [追加] をクリックして単一のハッシュ値を追加するか、[インポート] をクリックしてハッシュ値をまとめて追加します。

6. 信頼するインストールパッケージによって作成または変更されたファイルが自動的に許可リストに追加されるようにするには、[インストーラ] 列で [アプリケーションインストーラ] を選択します。

注意

Safe Lock Intelligent Manager は、インストーラフラグがマークされた信頼するハッシュ値のリストを含む `.txt` ファイルの一括インポート/エクスポートをサポートします。

ただし、インポート/エクスポート処理により、[備考] フィールドに含まれる**タブ**文字が (信頼するハッシュの配信画面で表示されるように) **空白**に自動的に変換されます。

ハッシュ値を計算する

ファイルハッシュ生成ツールを使用してハッシュ値を計算できます。このツールをダウンロードするには、38 ページの「信頼するアプリケーションとファイルをリモートで登録する」を参照してください。

手順

1. ダウンロードしたフォルダから WKFileHashGen.exe を実行します。

   Trend Micro ファイルハッシュ生成ツールの画面が表示されます。

2. 次のいずれかの方法を使用してファイルを選択し、ハッシュ値を計算します。

注意

- すべての必要なファイルでハッシュ値を計算するには、対象アプリケーションのルートフォルダをファイルハッシュ生成ツールに追加することをお勧めします。
- [フォルダの追加] ボタンでは、インストーラファイル、スクリプトファイル、および PE (ポータブル実行可能) 形式のファイルのみが計算対象になります。

- フォルダまたはファイルを [ファイルハッシュ生成ツール] 画面にドラッグアンドドロップします。
- ドロップダウンボタンをクリックし、[ファイルの追加] をクリックしてファイルを選択します。
- ドロップダウンボタンをクリックし、[フォルダの追加] をクリックして、選択したフォルダのすべてのファイルを追加します。

[ハッシュ値 (SHA-1)] 列にハッシュ値が表示されます。

3. ファイルが 1 つの場合は、項目を右クリックして [ハッシュ値のコピー] を選択します。ファイルが複数の場合は、[すべてエクスポート] をクリックしてハッシュ値のリストを生成します。

Safe Lock エージェントの許可リストをアップデートする

アプリケーション制御が有効な場合は、実行したいアプリケーションを新規インストールした後、Safe Lock エージェントの許可リストを定期的にアップデートしてください。許可リストのアップデートを実行すると、選択したエージェントの許可リストが再作成され、新たに検出されたアプリケーションがグローバルな許可リストに追加されます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [エージェント管理] 画面が表示されます。

2. 1 つまたは複数のエージェントやグループを選択します。
3. [コマンドの送信] をクリックして、[許可リストのアップデート] を選択します。

   [許可リストのアップデート] ダイアログが表示されます。

4. [アップデート] をクリックして、選択したエージェントの許可リストの再作成を開始します。

注意

アップデート中はエージェントを再起動したりシャットダウンしたりしないでください。アップデートプロセスの完了には 30 分以上かかることがあります。

許可リストのアップデートステータスは、[詳細] 画面で確認できます。現在の進行状況が [許可リスト] 列にアイコンで表示されます。

イベントログを収集する

ログにはエージェントのアクティビティに関する情報が含まれています。イベントログを収集すると、Safe Lock Intelligent Manager のデータベースが更新され、選択したエージェント情報を最新の状態にすることができます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

   [エージェント管理] 画面が表示されます。

2. 1 つ以上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、[イベントログの収集] を選択します。

   ログとステータスが Safe Lock エージェントから Safe Lock Intelligent Manager に正常に送信されると、[前回の接続] 列に表示される日付と時刻が更新されます。

エージェントの接続を確認する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [エージェント] を選択します。

[エージェント管理] 画面が表示されます。

2. 1 つまたは複数のエージェントやグループを選択します。
3. [コマンドの送信] をクリックして、[接続の確認] を選択します。

   選択した Safe Lock エージェントへの接続が自動的に試行されます。

   重要

   Intelligent Manager は NAT エージェントへの接続を確認できません。
   Intelligent Manager と NAT エージェント間の直接接続がありません。

   接続の確認が完了すると、接続できなかったすべての Safe Lock エージェントのリストが表示されます。

4. [接続されていないエージェントを [エージェント管理] に表示する] をオンにして [閉じる] をクリックし、接続されていないエージェントのリストをエージェントツリーの検索結果に表示します。

   Safe Lock Intelligent Manager サーバに接続できないエージェントを特定したら、接続されていないエージェントのネットワーク接続を確認することをお勧めします。

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、42 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。

Safe Lock エージェントにリモートで Patch を配信する

Intelligent Manager を使用して、アップロードした Patch ファイルを選択した Safe Lock エージェントに配信することで、管理サーバ画面から直接エージェントをアップグレードできます。

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. 1 つまたは複数のエージェントやグループを選択します。
3. [コマンドの送信] > [エージェントに Patch を配信] をクリックします。
4. 配信する Patch ファイルを選択します。
5. [配信] をクリックします。

   アップロードプロセスの完了を待ちます。Intelligent Manager でファイルの有効性が検証されると、選択したエージェントに Patch ファイルが配信されます。

第 3 章

Safe Lock の監視

この章では、Trend Micro Safe Lock Intelligent Manager の監視方法の概要について説明します。

この章の内容は次のとおりです。

ダッシュボードについて

Safe Lock Intelligent Manager のダッシュボードでは、タブやウィジェットを使用して、情報を見やすく表示します。ダッシュボードには、管理サーバ画面にアクセスするためのアカウントごとに、次のコンポーネントがカスタマイズして表示されます。

- タブ: ユーザは、名前やレイアウトの変更、ウィジェットの追加や削除などができます。
- ウィジェット: タブにさまざまなデータの概要を表示します。

[レポートの作成] 画面を使用すると、Safe Lock Intelligent Manager のレポートを Adobe PDF 形式 (.PDF) でダウンロードできます。ユーザ指定の予約レポートの詳細については、68 ページの「予約レポート」を参照してください。

管理サーバ画面にアクセスするためのアカウントとダッシュボードについて

管理サーバ画面にアクセスするためのアカウントごとに、そのニーズに合わせてダッシュボードのタブとウィジェットをカスタマイズできます。あるアカウントのタブやウィジェットをカスタマイズしても、他のアカウントのタブやウィジェットには影響しません。

注意

アカウントで Safe Lock Intelligent Manager にはじめてログインすると、初期設定のタブとウィジェットがダッシュボードに表示されます。

49 ページの「初期設定のタブについて」を参照してください。

ダッシュボードのタブについて

Safe Lock Intelligent Manager のダッシュボードでは、タブを使用して管理者が柔軟にデータを監視できます。タブはウィジェットのコンテナとして提供され、管理サーバ画面にアクセスするためのアカウントを使用してダッシュボードを独自にカスタマイズできます。ダッシュボードでは、アカウントごとに最大 30 のタブがサポートされます。

タブを閉じると、そのタブはアカウントのダッシュボードから削除されます。閉じたタブを復元することはできませんが、同様のタブを後から再度作成することはできます。タブを閉じても、他のユーザアカウントのダッシュボードに影響はありません。

スライドショー機能を利用すると、次のコントロールを使用して異なるタブ上のウィジェットを監視できます。

- [タブスライドショーの再生] をクリックすると、指定した間隔でタブが自動的に入れ替わって表示されます。

  ヒント

  入れ替えの間隔は、[タブ設定] で指定します。

  51 ページの「タブを設定する」を参照してください。

- [タブスライドショーの一時停止] をクリックすると、現在のタブでのタブスライドショーが停止します。

  ヒント

  別のタブに移動することでも、スライドショーが停止します。

初期設定のタブについて

ダッシュボードには、次のタブが初期設定で用意されています。

- イベントの概要: 管理対象の Safe Lock エージェントのイベントに関する情報を表示するウィジェットが含まれます。

ウィジェット	説明
未処理の警告イベント	最新の未処理の警告イベントを表示します。
ブロックされた件数が上位のファイル	ブロックされた件数が上位のファイルを表示します。

ウィジェット	説明
ブロックされたイベントの履歴	指定した期間内にブロックされたイベントを表示します。
ブロック件数が上位のエージェント	ブロック件数が上位のエージェントを表示します。
ブロックされたファイルの検索結果	ブロックされたファイルに対する不正プログラムの検索結果を表示します。

- エージェント:管理対象の Safe Lock エージェントに関する情報を表示するウィジェットが含まれます。

ウィジェット	説明
アプリケーション制御の状態	エージェントのアプリケーション制御の状態を表示します。
バージョン	エージェントにインストールされている Safe Lock エージェントの数を、バージョンごとに表示します。
最新のコンポーネントアップデート	最新のコンポーネントを表示します。

注意

タブの初期設定の名前は、[タブ設定] 画面で変更します。

51 ページの「タブを設定する」

タブを追加する

ダッシュボードにタブを追加して、Safe Lock Intelligent Manager アカウントの情報の概要をカスタマイズして表示できます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ダッシュボード] を選択します。

2. [+] タブをクリックします。

   [新規タブ] 画面が表示されます。

3. [タイトル] に、タブのわかりやすいタイトルを入力します。

4. タブのレイアウトを選択します。

   注意

   タブに追加できるウィジェットの数は、タブのレイアウトに応じて異なります。タブに含まれるウィジェットが最大数に達した場合は、ウィジェットをタブから削除するか、追加するウィジェットに対して新しいタブを作成する必要があります。

5. スライドショーと自動調整の有無を設定します。

6. [保存] をクリックします。

   空白のタブがダッシュボードに表示されます。

7. [ウィジェットの追加] をクリックして、タブにウィジェットを配置します。

タブを設定する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ダッシュボード] を選択します。

2. [タブ設定] をクリックします。

   [タブ設定] 画面が表示されます。

3. [タイトル] に、タブのわかりやすいタイトルを入力します。

4. タブのレイアウトを選択します。

5. スライドショーと自動調整の有無を設定します。

タブの表示間隔を指定できます。5～3600 の整数を指定する必要があります。

ウィジェットについて

ウィジェットは、ダッシュボードの主要コンポーネントです。タブでレイアウトを指定し、ウィジェットを使用して、ダッシュボードに表示する実際のデータの概要を指定します。

多くのウィジェットのデータ範囲は個別に設定できます。たとえば、一部のウィジェットでは次の項目を指定できます。

- 期間
- 円グラフや折れ線グラフ
- 凡例

タブのウィジェットは、ドラッグアンドドロップしてタブ上のさまざまな場所に移動できます。ウィジェットを移動できる場所は、タブのレイアウトによって指定されます。

Safe Lock によるアプリケーション制御の状態

このウィジェットには、ネットワーク内のアプリケーション制御のステータスの概要が表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [エージェント] タブに表示されます。

このウィジェットには、次のデータが円グラフで表示されます。

ステータス	説明
アプリケーション制御が有効です	ネットワーク内のアプリケーション制御が有効なエージェントの数と割合

ステータス	説明
アプリケーション制御が無効です	ネットワーク内のアプリケーション制御が無効なエージェントの数と割合

円グラフのセクションをクリックすると、各ステータスの詳細が表示されます。

Safe Lock のバージョン

このウィジェットには、Safe Lock Intelligent Manager によって管理されている Safe Lock エージェントのバージョンの概要が表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [エージェント] タブに表示されます。

列	説明
エージェントバージョン	Safe Lock エージェントにより報告されたバージョン番号
エージェント	特定のバージョンがインストールされたエージェントの合計数

[エージェント] 列の値をクリックすると、特定のバージョンがインストールされたエージェントがすべて表示されます。

Safe Lock の未処理の警告イベント

このウィジェットには、Safe Lock エージェントにより報告された最新の未処理の警告イベントが表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。

列	説明
イベント時間	未処理の警告イベントが発生した日時

列	説明
エージェント名	影響を受けたエージェントの名前
イベント	未処理の警告イベントのメッセージ
ファイル / フォルダ	未処理の警告イベントが発生したファイルまたはフォルダ

[イベント] 列の値をクリックすると、そのイベントの詳細が表示されます。すべてのイベントを表示するには、[未処理の警告イベントをすべて表示] をクリックします。

表示するイベント数を指定するには、[ウィジェット設定] ダイアログを開き、[最新のイベント] の値を選択します。

Safe Lock によるブロック件数が上位のエージェント

このウィジェットには、ブロック件数が上位のエージェントが表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。

列	説明
エージェント名	エージェントの名前
タグ	エージェントに割り当てられたタグ
IP アドレス	エージェントの IP アドレス
ブロックされたイベント	エージェントでブロックされたイベントの合計数

[ブロックされたイベント] 列の値をクリックすると、そのイベントの詳細が表示されます。

指定した期間内のイベントデータのみを表示するには、[期間] のドロップダウンを使用します。

表示するイベント数を指定するには、[ウィジェット設定] ダイアログを開き、[表示するイベント] の値を選択します。

Safe Lock でブロックされたイベントの履歴

このウィジェットには、指定した期間内にブロックされたイベントの概要が表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。

表示アイコンをクリックすると、データが円グラフまたは折れ線グラフで表示されます。

- 指定した期間内のイベントデータのみを表示するには、[期間] のドロップダウンを使用します。
- グラフ下に並ぶカテゴリをクリックすると、そのイベントのデータが表示または非表示になります。
- グラフの値をクリックすると、ブロックされたイベントの詳細が表示されます。

Safe Lock でブロックされた件数が上位のファイル

このウィジェットには、ブロック件数が上位のファイルのリストが表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。

列	説明
ファイル名	ブロックされたファイルの名前
検索結果	ファイルが不正かどうかを示します
ファイルハッシュ	ブロックされたファイルの SHA-1 ハッシュ値
エージェント	当該ファイルのブロックイベントを報告したエージェントの数

列	説明
ブロックされたイベント	当該ファイルについて報告されたブロックイベントの合計数

[ブロックされたイベント] 列の値をクリックすると、そのイベントの詳細が表示されます。

表示するイベント数を指定するには、[ウィジェット設定] ダイアログを開き、[表示するイベント] の値を選択します。

Safe Lock でブロックされたファイルの検索結果

このウィジェットには、ブロックされたファイルに対する不正プログラムの検索結果が表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [イベントの概要] タブに表示されます。

データは円グラフで表示されます。

- 指定した期間内のイベントデータのみを表示するには、[期間] のドロップダウンを使用します。
- グラフ下に並ぶカテゴリをクリックすると、その検索結果のデータが表示または非表示になります。
- グラフの値をクリックすると、ブロックされたイベントの詳細が表示されます。

Safe Lock の最新のコンポーネントアップデート

このウィジェットには、最新のコンポーネントが表示されます。

初期設定で、このウィジェットは [ダッシュボード] の [エージェント] タブに表示されます。

列	説明
パターン検索エンジン	コンポーネントの名前
バージョン	Safe Lock エージェントにより報告されたバージョン番号
日時	コンポーネントの前回のアップデート日時

ウィジェットを追加する

タブに追加できるウィジェットの数は、タブのレイアウトに応じて異なります。タブに含まれるウィジェットが最大数に達した場合は、ウィジェットをタブから削除するか、追加するウィジェットに対して新しいタブを作成する必要があります。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ダッシュボード] を選択します。
2. ダッシュボードで、ウィジェットを追加するタブを選択します。
3. [ウィジェットの追加] をクリックします。

   [ウィジェットの追加] 画面が表示されます。
4. オプションで、次のいずれかをクリックすると、表示されるウィジェットをフィルタできます。

カテゴリ	説明
最新のウィジェット	最近タブに追加されたウィジェットをクエリします。
すべてのウィジェット	使用可能なすべてのウィジェットをクエリします。
エージェントの状況	管理対象の Safe Lock エージェントに関するデータを表示するウィジェットのみをクエリします。

カテゴリ	説明
イベント	管理対象の Safe Lock エージェントイベントに関するデータを表示するウィジェットのみをクエリします。
サーバの状況	Safe Lock Intelligent Manager に関するデータを表示するウィジェットのみをクエリします。

5. 現在のタブに追加するウィジェットを 1 つ以上選択します。
6. [追加] をクリックします。

ウィジェットを使用する

各ウィジェットで次のタスクを実行します。

タスク	手順
ウィジェットの移動	タブのウィジェットは、ウィジェット上部のタイトルバーをクリックしたまま、タブ上のさまざまな場所にドラッグして移動できます。 ヒント ウィジェットを移動できる場所は、タブのレイアウトによって指定されます。ドラッグする際、ウィジェットを移動できる領域に入ると、赤い点線の枠が表示されます。
ウィジェットのサイズ変更	列が複数あるタブでウィジェットのサイズを水平方向に変更するには、次の手順を実行します。 1. マウスポインタをウィジェットの右枠の上に重ねます。 灰色の縦線が表示されます。 2. マウスポインタを左または右にドラッグします。 列が複数あるタブでウィジェットのサイズを縦方向に変更するには、[タブ設定] で [自動調整] を有効にします。この機能は、1 列に含まれるウィジェットが 1 つだけのときに動作します。この機能を使用して、単一のウィジェットの高さを一番高い列に合わせます。

タスク	手順
ウィジェットデータの表示更新	ウィジェットの上部にある [表示更新] アイコンをクリックします。
自動更新設定の指定	1. ウィジェットの上部にある [その他のオプション] アイコンをクリックします。 2. [更新設定] を選択します。 [更新設定] 画面が表示されます。 3. このウィジェットの自動更新を有効にするには、次の手順を実行します。 a. [ウィジェットを自動的に更新する] を選択します。 b. 頻度を指定します。
ウィジェット名の変更	1. ウィジェットの上部にある [その他のオプション] アイコンをクリックします。 2. [ウィジェット設定] を選択します。 [ウィジェット設定] 画面が表示されます。 3. ウィジェットのわかりやすいタイトルを入力します。
ウィジェットを閉じる	1. ウィジェットの上部にある [その他のオプション] アイコンをクリックします。 2. [ウィジェットを閉じる] を選択します。

[エージェントイベント] 画面について

[エージェントイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [エージェントイベント] の順に選択します。

この画面には、Safe Lock Intelligent Manager の管理下のエージェントの許可リストにないアプリケーションに関するイベントのリストが表示されます。

ロックダウンが無効な場合、エージェントの許可リストにないファイルが動作しようとしたり、エージェントに変更を加えようとしたりすると、Safe Lock ではイベントをログに記録しますが、ファイルの実行は許可します。

ロックダウンが有効な場合、エージェントの許可リストにないファイルが動作しようとしたり、エージェントに変更を加えようとしたりすると、Safe Lock ではファイルを停止させ、適切な処理を求めるプロンプトを表示します。イベントログには、許可リストにないファイルと実行された処理に関する、管理下のエージェントからの情報が含まれます。

ロックダウンが有効な場合、許可リストにないファイルには次の処理を実行できます。

- 許可リストに追加: 今回のファイルの実行は防ぎますが、ファイルをエージェントの許可リストに追加します。
- 無視: ファイルの実行は防ぎますが、ファイルの移動や変更は行いません。
- 隔離: ファイルの実行を防ぎ、後で分析するためにファイルを隔離します。
- 削除: ファイルの実行を防ぎ、ファイルを削除します。

エージェントイベントログをクエリする

クエリを実行すると、表示されるエージェントイベントログのリストが更新されます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [エージェントイベント] の順に選択します。

   [エージェントイベント] 画面が表示されます。

2. 期間でフィルタするには、期間のドロップダウンを選択して条件を指定します。

   次のいずれかを実行します。

   - リストされる期間をクリックします。
   - [カスタム] をクリックし、期間を指定して [検索] をクリックします。

3. エージェントでフィルタするには、エージェントのドロップダウンを選択して条件を指定します。

   次のオプションを使用できます。

   - エージェント名: エージェントのホスト名の最初の文字またはすべてを入力し、[検索] をクリックします。
   - グループ名: グループ名を入力し、[検索] をクリックします。
   - IP アドレス: IPv4 アドレスを入力し、[検索] をクリックします。
   - IP アドレスの範囲: IPv4 アドレスの範囲を入力し、[検索] をクリックします。
   - タグ: タグの全部または一部を入力し、[検索] をクリックします。

4. イベントでフィルタするには、イベントのドロップダウンを選択して条件を指定します。

   次のオプションを使用できます。

   - イベントのタイプ: 特定のイベントを選択し、[適用] をクリックします。
   - ソース: イベントソースとして [Safe Lock] または [Portable Security] を選択します。
   - 重大度: イベントレベルとして [情報] または [警告] を選択します。
   - 処理の状態: [未処理] または [処理済] を選択します。
   - 変更監視: [ファイルまたはフォルダ] または [レジストリキーまたはレジストリ値] を選択し、[検索] をクリックします。[ファイルまたはフォルダ] 検索では、文字列の部分一致がサポートされます。
   - ブロックされたファイル: [ファイル名] または [ファイルハッシュ (SHA-1)] を選択し、[検索] をクリックします。[ファイル名] 検索では、文字列の部分一致がサポートされます。

5. 選択したフィルタに一致するエントリのみが表に表示されます。

エージェントイベントをエクスポートする

選択したエージェントのイベントログエントリに関するデータを CSV ファイル形式で保存します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [エージェントイベント] の順に選択します。

   [エージェントイベント] 画面が表示されます。

2. 情報をエクスポートするエージェントログエントリをリストから選択します。

   a. すべてのエントリをエクスポートするには、[エクスポート] > [すべてのログ] の順にクリックします。

   b. 選択したエントリのみをエクスポートするには、次のいずれかを実行します。

      - 単一のエントリを選択するには、エクスポートするエントリをクリックします。
      - 複数のエントリを選択するには、<Shift> キーを押しながら、エクスポートする最初と最後のエントリをクリックします。
      - 複数の連続しないエントリを選択するには、<Ctrl> キーを押しながら、エクスポートする各エントリをクリックします。

   c. [エクスポート] > [選択したログ] の順にクリックします。

3. ファイルを保存します。

エージェントイベントをインポートする

Safe Lock Intelligent Manager では、次のアプリケーションからのエージェントイベントのインポートをサポートしています。

- Trend Micro Safe Lock Intelligent Manager: Safe Lock Intelligent Manager 2.0 でエクスポートした CSV 形式のログ

- Trend Micro Portable Security: Trend Micro Portable Security バージョン 2.0 で検索を実行した Safe Lock エージェントから収集した DB 形式のログ

注意

Portable Security では初期設定で、Safe Lock のログを `tmsllog.db` ファイルにエクスポートします。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [エージェントイベント] の順に選択します。

   [エージェントイベント] 画面が表示されます。

2. [インポート] をクリックします。

   [インポート] 画面が表示されます。

3. インポートする CSV ファイルを選択します。

4. [開く] をクリックします。

5. [OK] をクリックします。

   イベントログが Safe Lock Intelligent Manager にインポートされます。

注意

インポートを中断またはキャンセルした場合、データは Safe Lock Intelligent Manager データベースに追加されません。

警告イベントをマークする

警告イベントの追跡に役立てるため、リストの [処理の状態] でイベントに対して表示されるステータスを変更します。

注意

Safe Lock Intelligent Manager では、情報イベントに [処理の状態] ステータスは表示されません。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [エージェントイベント] の順に選択します。

   [エージェントイベント] 画面が表示されます。

2. ステータスを変更する警告イベントを 1 つ以上選択します。

3. 次のいずれかを実行して、ステータスを変更します。

   - [未処理にする] をクリックします。
   - [処理済にする] をクリックします。

[サーバイベント] 画面について

[サーバイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [サーバイベント] の順に選択します。

この画面には、監査対象の Safe Lock Intelligent Manager の管理サーバ画面にアクセスするためのアカウントのアクティビティのログが表示されます。

注意

サーバイベントログには、Safe Lock Intelligent Manager のユーザアカウントとポリシーにより実行された処理について収集された情報が含まれます。

サーバイベントログをクエリする

クエリを実行すると、表示されるサーバイベントログのリストが更新されます。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [サーバイベント] の順に選択します。

   [サーバイベント] 画面が表示されます。

2. [サーバイベント] のドロップダウンリストをクリックします。

   検索条件のリストが表示されます。

3. 検索条件の種類を選択します。

   選択した条件に応じた検索フィールドが表示されます。

4. 選択した条件に応じた手順を実行します。

オプション	説明
期間	次のいずれかを実行します。 • リストから期間を選択します。 • 期間をカスタマイズして指定します。 a. リストの [カスタム] を選択します。 b. カスタマイズする期間を指定します。 c. [検索] をクリックします。
すべてのユーザ	すべてのユーザによりログに記録されたすべてのイベントを表示します。
ユーザ名	特定のユーザによりログに記録されたすべてのイベントを表示します。
エージェント名	エージェントのホスト名 (最初の数文字またはすべて) を入力し、[検索] をクリックします。
グループ名	特定のグループによりログに記録されたすべてのイベントを表示します。
すべてのイベント	エージェントによりログに記録されたすべてのイベントを表示します。

オプション	説明
イベントのタイプ	特定のイベントを選択します。

サーバイベントログのリストに検索結果が表示されます。

サーバイベントログをエクスポートする

選択したサーバのイベントログエントリに関するデータを CSV ファイル形式で保存します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [サーバイベント] の順に選択します。

   [サーバイベント] 画面が表示されます。

2. 情報をエクスポートするサーバログエントリをリストから選択します。

   a. すべてのエントリをエクスポートするには、[エクスポート] > [すべてのログ] の順にクリックします。

   b. 選択したエントリのみをエクスポートするには、次のいずれかを実行します。

      - 単一のエントリを選択するには、エクスポートするエントリをクリックします。
      - 複数のエントリを選択するには、<Shift> キーを押しながら、エクスポートする最初と最後のエントリをクリックします。
      - 複数の連続しないエントリを選択するには、<Ctrl> キーを押しながら、エクスポートする各エントリをクリックします。

   c. [エクスポート] > [選択したログ] の順にクリックします。

3. ファイルを保存します。

ログを管理する

古いログを削除して、Safe Lock Intelligent Manager で使用しているデータベースのサイズを削減します。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [ログの設定] の順に選択します。

   [ログの設定] 画面が表示されます。

2. [管理] タブをクリックします。

3. [次の期間を経過したエージェントのイベントログエントリを削除する] で、エージェントのイベントログエントリを保持する最長期間を指定します。

4. [最大 xxx 件のエントリを保持する] で、保持するエージェントイベントエントリの最大件数を指定します。

   注意

   - Safe Lock Intelligent Manager では、[処理済] としてマークされたエージェントイベントのみが削除されます。
   - エントリ数が [最大 xxx 件のエントリを保持する] で設定した件数の上限を超える場合は、[次の期間を経過したエージェントのイベントログエントリを削除する] に指定した期間に満たないエージェントのイベントログも削除されます。

5. [次の期間を経過したサーバ監査ログエントリを削除する] で、サーバのイベントログエントリを保持する最長期間を指定します。

6. バックアップせずに自動的に削除されないようにするには、次の手順を実行します。

   a. [自動的に削除する前にログをバックアップする] を選択します。

   b. [バックアップのパス] をクリックします。

c. バックアップのフルパスを指定します。

d. Safe Lock Intelligent Manager で、指定したパスにフォルダを新規作成する場合は、[存在しない場合は、フォルダを作成する] を選択します。

7. ログエントリを保持期間に基づいて手動で削除するには、次の手順を実行します。

a. [手動削除] で、エントリを保持する最短期間を選択します。

b. [今すぐ削除] をクリックします。

警告!

Safe Lock Intelligent Manager では、手動で削除したログエントリは自動的にバックアップされません。

既存のログエントリをバックアップするには、適切な手順を実行してエントリを手動でエクスポートします。

62 ページの「エージェントイベントをエクスポートする」を参照してください。

66 ページの「サーバイベントログをエクスポートする」を参照してください。

予約レポート

[予約レポート] 画面には、ユーザ指定のスケジュールで自動的に生成されるすべてのレポートのリストが表示されます。この画面を使用して、これまでに設定した予約レポート、レポートの内容、および受信者に関する基本情報を表示したり、予約レポートを有効および無効にしたりすることができます。

次の表は、[予約レポート] 画面で実行できるタスクを示しています。

タスク	説明
予約レポートの送信の有効化	[予約レポートの送信] チェックボックスをオンにして、予約レポートを有効にします。

タスク	説明
予約レポートの内容の編集	レポートに含める内容の種類を選択します。 詳細については、49 ページの「初期設定のタブについて」を参照してください。
予約レポートの送信	予約レポートの頻度と時間を日、週、または月単位で設定します。 **注意** 指定した日付けが存在しない月は予約タスクがスキップされます。タスクを定期的に実行するには、29 日、30 日、または 31 日を指定しないことをお勧めします。
予約レポートの受信者の指定	レポートの受信者を指定するには有効なメールアドレスが必要です。

重要

予約レポートを送信するには、SMTP サーバが正しく設定されていることを確認してください。

詳細については、82 ページの「SMTP サーバを設定する」を参照してください。

イベントを外部 Syslog サーバに転送する

サーバとエージェントのイベントログを外部 syslog サーバに転送することで、他のデバイスでの管理および監視が可能になります。Intelligent Manager は、Common Event Format (CEF) でログを転送します。syslog サーバが Common Event Format (CEF) をサポートしていることを確認してください。

手順

1. [ログとレポート] > [ログの設定] の順に選択します。
2. [Syslog サーバ] タブをクリックします。
3. [ログを Syslog サーバに転送 (CEF のみ)] を選択します。

4. syslog サーバのプロトコル、IP アドレスおよびポートを指定します。

Trend Micro Control Manager との統合

Safe Lock Intelligent Manager では、Trend Micro Control Manager (以下、Control Manager) との統合がサポートされます。統合後は、Control Manager から Safe Lock エージェントのステータスを監視できます。

手順

1. Control Manager サーバに登録します。
   a. Control Manager サーバの管理コンソールで、[運用管理] > [管理下のサーバ] > [サーバの登録] の順に選択します。
   b. [サーバの種類] で [Trend Micro Safe Lock] を選択します。
   c. [追加] をクリックし、[サーバの追加] 画面を表示します。
   d. 統合する Safe Lock Intelligent Manager サーバの情報を入力します。
   e. [保存] をクリックします。
2. Safe Lock のウィジェットを Control Manager のダッシュボードに追加します。
   a. Control Manager サーバの管理コンソールで、[ダッシュボード] に移動します。
   b. ウィジェットを含めるタブを決定します。
      - 新しいタブを追加するには、プラス記号のアイコン (+) をクリックし、タブ名を指定します。
      - 既存のタブを選択するには、タブ名をクリックします。
   c. 歯車のアイコンをクリックし、[ウィジェットの追加] をクリックします。
   d. [ウィジェットの追加] 画面で、追加する Safe Lock のウィジェットを探して選択します。

- 製品別にウィジェットをフィルタするには、ドロップダウンリストを使用します。
- 名前別にウィジェットをフィルタするには、検索ボックスを使用します。

ウィジェットの詳細については、52 ページの「ウィジェットについて」を参照してください。

e. [追加] をクリックします。

[ダッシュボード] に戻り、選択したウィジェットが表示されていることを確認します。

第 4 章

各種の管理設定

この章では、Trend Micro Safe Lock Intelligent Manager の管理設定の概要について説明します。

この章の内容は次のとおりです。

[コンポーネントアップデート] 画面について

[コンポーネントアップデート] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [管理] > [コンポーネント] > [アップデート] の順に選択します。

この画面には、Safe Lock Intelligent Manager で使用されるコンポーネントのリストが表示されます。

この画面では次のタスクを実行します。

機能	説明
アップデート	選択したコンポーネントを手動でアップデートします。
予約アップデート	アップデートスケジュールを設定します。 各コンポーネントの予約アップデートを有効または無効にします。
エージェントインストーラパッケージのダウンロード	最新のエージェントインストーラパッケージをダウンロードします。

コンポーネントを手動でアップデートする

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理] > [コンポーネント] > [アップデート] の順に選択します。

   [コンポーネントアップデート] 画面が表示されます。

2. [アップデート] をクリックします。
3. アップデートするコンポーネントを選択します。
4. [アップデート] をクリックします。

[アップデート進行状況]画面が表示されます。コンポーネントがアップデートされると、[現在のバージョン] および [最新のアップデート] の情報が更新されます。

コンポーネントアップデートを予約する

手順

1. 管理サーバ画面の上部にあるナビゲーションで[管理] > [コンポーネント] > [アップデート] の順に選択します。

   [コンポーネントアップデート] 画面が表示されます。

2. [予約アップデート] をクリックします。
3. 予約アップデートするコンポーネントを有効にします。
4. [アップデートスケジュール] で、使用するスケジュールを選択します。

重要

[月次, 日] を選択した場合、該当する月の日数より大きな数を選択すると、選択したコンポーネントがその月の最終日に置き換わります。

タスクを適切に予約するには、各月の 29 日、30 日、31 日は選択しないことをお勧めします。

最新のエージェントインストーラパッケージをダウンロードする

手順

1. 管理サーバ画面の上部にあるナビゲーションで[管理] > [コンポーネント] > [アップデート] の順に選択します。

   [コンポーネントアップデート] 画面が表示されます。

2. [エージェントインストーラパッケージのダウンロード] をクリックします。

3. インストールパッケージの言語を選択します。

   最新のエージェントインストーラパッケージがブラウザによりダウンロードされます。

   注意

   エージェントインストーラパッケージは、[コンポーネントアップデート] 画面に表示されるコンポーネントのバージョンに基づいて、Safe Lock Intelligent Manager によって最新と判断されます。キャッシュされたエージェントインストーラパッケージが最新でない場合、Safe Lock Intelligent Manager では、ダウンロードを開始する前に最新のパッケージを準備してキャッシュします。

   最新のエージェントインストーラパッケージを準備する際は、システムに高い負荷がかかります。Safe Lock Intelligent Manager を実行するハードウェアによっては、最新のエージェントインストーラパッケージの準備に時間がかかる場合があります。

4. コマンドラインで `SLrst` プログラムを使用してリモートインストールを行うために、ダウンロードしたエージェントインストーラパッケージを使用するときは、ダウンロードしたエージェントインストーラパッケージを `SLrst` で使用するパスにコピーします。

   たとえば、Safe Lock Intelligent Manager を C ドライブの初期設定のパスにインストールした場合は、ダウンロードしたエージェントインストーラパッケージを `c:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager¥CmdToolsRemoteAgentSetupTool¥package` にコピーします。

重要

ダウンロードしたファイルはパッケージファイル（.zip）に手動で圧縮する必要があります。

パッケージのファイル名は、TMSL2.0_<language_abbreviation>.zip の形式にする必要があります。

例:

有効	無効
TMSL2.0_EN.zip	TMSL2.0_EN (1).zip
TMSL2.0_JA.zip	TMSL2.0_EN_1.zip

エージェントインストーラパッケージの変更について

Safe Lock Intelligent Manager では、エージェントインストーラパッケージの個別変更がサポートされています。エージェントインストーラパッケージを変更する場合は、次の要件を確認して慎重に実行してください。

- Setup.ini ファイルと trend.cer ファイルのみを変更してください。
- エージェントインストーラパッケージの内部ディレクトリ構造は保持してください。
- エージェントインストーラパッケージの変更は自己責任で行ってください。

コンポーネントのアップデート元を設定する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理] > [コンポーネント] > [アップデート元]の順に選択します。

   サーバアップデート元の画面が表示されます。

2. 環境内で適切なアップデート元を選択します。

オプション	説明
トレンドマイクロのアップデートサーバ	トレンドマイクロが管理する、インターネット上のアップデートサーバです。
インターネットまたはローカル管理サーバ	認証が不要なアップデートサーバを指定します。
認証を要求するローカル管理サーバ	認証が必要なローカルのプライベートアップデートサーバを指定します。

通知を設定する

Safe Lock Intelligent Manager では、設定に応じて次の種類の通知が送信されます。

- 一般: エージェントでファイルがブロックされるとエージェントから Safe Lock Intelligent Manager に送信される、情報と警告メッセージの通知です。

- 大規模感染: 指定された期間内に、未処理の警告メッセージ数が指定されたしきい値を超えると送信される通知です。

81 ページの「通知メッセージの例」を参照してください。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理] > [通知設定] の順に選択します。

   [通知設定] 画面で [一般] タブが表示されます。

2. メールを使用して一般通知を送信するには、次の手順を実行します。

   a. [メールで通知を送信する] を選択します。

   b. 受信者のメールアドレスを指定します。

c. SMTP サーバの設定を行います。詳細については、82 ページの「SMTP サーバを設定する」を参照してください。

d. SMTP サーバで認証が必要な場合は、[SMTP 認証] を選択して資格情報を指定します。

e. この設定を使用してテストメッセージを送信するには、[テスト送信] をクリックします。

詳細については、82 ページの「SMTP サーバを設定する」を参照してください。

3. SNMP を使用して一般通知を送信するには、次の手順を実行します。

a. [SNMP で通知を送信する] を選択します。

b. SNMP サーバの IPv4 アドレスか、完全修飾ドメイン名 (FQDN) を指定します。

c. SNMP コミュニティ名を指定します。

4. サードパーティ製アプリケーションを使用して一般通知を送信するには、次の手順を実行します。

a. [サードパーティ製アプリケーションの起動] を選択します。

b. サードパーティ製アプリケーションのフルパスを指定します。

c. 必要に応じて、アプリケーションのランタイムパラメータを指定します。

5. アウトブレーク通知を送信するには、次の手順を実行します。

a. [大規模感染] タブを選択します。

b. [アウトブレーク通知を送信する] を選択します。

c. 指定期間内の未処理の警告件数のしきい値を指定します。

d. これらの警告の期間のしきい値を指定します。

e. 大規模感染時に Safe Lock Intelligent Manager の物理サーバコンピュータの画面に Windows 通知を表示するには、[Trend Micro Safe Lock Intelligent Manager にアウトブレーク通知のポップアップを表示する] を選択します。

通知メッセージの例

Safe Lock Intelligent Manager で SMTP または SNMP 通知の送信を設定すると、Safe Lock Intelligent Manager ではすべての種類のイベントについて通知が送信されます。

表 4-1. 通知の例

イベントのタイプ	原因	通知メッセージの例
大規模感染	大規模感染	Trend Micro Safe Lock: アウトブレーク通知
処理が必要	ブロックされたファイル	Trend Micro Safe Lock: [処理が必要です] <computer_name> でファイルのアクセスがブロックされました (<file_name>)
検索結果	不正プログラムの検出	Trend Micro Safe Lock: [検索結果] <computer_name> で不正プログラムが検出されました (<file_name>)
警告	不正変更	Trend Micro Safe Lock: [警告] <computer_name> でファイル/フォルダの変更許可されました
警告	アプリケーション制御のステータスの変更	Trend Micro Safe Lock: [警告] <computer_name> でアプリケーション制御が無効になりました
警告	デバイスのアクセスのブロック	Trend Micro Safe Lock: [警告] <computer_name> でデバイスのアクセスがブロックされました

SMTP サーバを設定する

この画面では、通知や予約レポートを送信する SMTP サーバの設定を指定できます。

手順

1. [管理] > [SMTP サーバの設定] の順に選択します。

   [SMTP サーバの設定] 画面が表示されます。

2. [SMTP サーバ] に SMTP サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。

3. ポート番号を入力します。

4. [送信者] に送信者のメールアドレスを入力します。

   Safe Lock Intelligent Manager では、このアドレスが送信者アドレスとして使用されます (一部の SMTP サーバの要件)。

5. SMTP サーバで認証が必要な場合は、[SMTP 認証] を選択します。

6. ユーザ名とパスワードを入力します。

7. [保存] をクリックします。

   Safe Lock Intelligent Manager からテストメールを送信するには、[テストメールの送信] ボタンをクリックします。

   注意

   テストメールを送信できるのは、一度に 1 つのメールアドレスまたは受信者に対してのみです。

[アカウント管理] 画面について

[アカウント管理] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [管理] > [アカウント管理] を選択します。

この画面は、Safe Lock Intelligent Manager の管理サーバ画面にアクセスするためのアカウントの管理に使用します。

Trend Micro Safe Lock Intelligent Manager のアカウントには、次の権限があります。

アカウントの種類	権限
管理者	• Safe Lock Intelligent Manager の管理サーバ画面にアクセスするためのアカウントを、[アカウント管理] 画面で追加、編集、有効化、無効化、または削除します。 • 自身のアカウントの説明、メールアドレス、およびパスワードを変更します。 • エージェントでブロックされたファイルに対する処理を指定します。 • Safe Lock Intelligent Manager の管理サーバ画面は、[ログとレポート] > [サーバイベント] 画面の順に選択して表示します。 • 管理下のエージェントへのストレージデバイスによるアクセスを許可またはブロックできます。
フルコントロール	• 自身のアカウントの説明、メールアドレス、およびパスワードを変更します。 • エージェントでブロックされたファイルに対する処理を指定します。 • Safe Lock Intelligent Manager の管理サーバ画面は、[ログとレポート] > [サーバイベント] 画面の順に選択して表示します。 • 管理下のエージェントへのストレージデバイスによるアクセスを許可またはブロックできます。
ストレージデバイスコントロールの管理のみ	• 自身のアカウントの説明、メールアドレス、およびパスワードを変更します。 • 管理下のエージェントへのストレージデバイスによるアクセスを許可またはブロックできます。

アカウントの種類	権限
アプリケーション制御の管理のみ	• 自身のアカウントの説明、メールアドレス、およびパスワードを変更します。 • 管理下のエージェントでアプリケーション制御を設定します。
読み取りのみ	• 自身のアカウントの説明、メールアドレス、およびパスワードを変更します。

注意

インストール時に作成される初期設定のアカウントの名前は「admin」で、管理者権限を持つ唯一のアカウントです。

アカウントを追加する

手順

1. 「admin」アカウントを使用して管理サーバ画面にログオンします。
2. 管理サーバ画面の上部にあるナビゲーションで [管理] > [アカウント管理] の順に選択します。

   [アカウント管理] 画面が表示されます。
3. [追加] をクリックします。

   [ユーザの追加] 画面が表示されます。
4. アカウントの権限を指定します。

   82 ページの「[アカウント管理] 画面について」を参照してください。
5. アカウント名を指定します。

注意

英小文字の a～z、0～9、- (ハイフン)、および _ (アンダースコア) のみがサポートされます。

6. アカウントを [有効] にするか [無効] にするかを作成時に指定します。
7. 必要に応じて、アカウントの説明を入力します。

注意

次の記号は使用できません。

> < & " '

8. 必要に応じて、このアカウントのメールアドレスを指定します。
9. パスワードを指定します。

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。次の記号および空白は使用できません。

| > " : < \

アカウントを編集する

管理者権限を持つアカウントのみが、アカウントの追加、有効化/無効化、または削除を実行できます。その他のアカウントでは、自身のアカウントの説明、メールアドレス、およびパスワードの編集のみが可能です。

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理] > [アカウント管理] の順に選択します。

   [アカウント管理] 画面が表示されます。
2. アカウントのユーザ名をクリックします。

   [ユーザの編集] 画面が表示されます。
3. 設定を変更します。

プロキシを設定する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理] > [プロキシの設定] の順に選択します。

   [プロキシの設定] 画面が表示されます。

2. アップデートのためのプロキシ設定を行うには、次の手順を実行します。

   a. [パターンファイルおよび検索エンジンのアップデートにプロキシサーバを使用する] を選択します。

   b. プロキシサーバの IPv4 アドレスか、FQDN を指定します。

   c. ポートを指定します。

   d. プロキシサーバで認証が必要な場合は、[プロキシサーバ認証] を選択して資格情報を指定します。

3. Safe Lock エージェントにリクエストを送信するために Safe Lock Intelligent Manager で使用するプロキシ設定を行うには、次の手順を実行します。

   a. [管理サーバと Safe Lock エージェント間の接続にプロキシサーバを使用する] を選択します。

   b. プロキシサーバの IPv4 アドレスか、FQDN を指定します。

   c. ポートを指定します。

   d. プロキシサーバで認証が必要な場合は、[プロキシサーバ認証] を選択して資格情報を指定します。

ヒント

Safe Lock Intelligent Manager にリクエストを送信するために Safe Lock エージェントで使用するプロキシ設定を行うには

- リモートインストール前: エージェントインストーラパッケージで使用する設定ファイルにプロキシ情報を追加します。
- リモートインストール後: Safe Lock エージェントがインストールされている環境で、コマンドラインツールの `SLCmd.exe` を使用します。

[ライセンス管理] 画面について

[ライセンス管理] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [管理] > [ライセンス管理] の順に選択します。

この画面には、次の詳細事項が表示されます。

項目	説明
ステータス	「有効」または「有効期限終了」が表示されます
タイプ	「製品版」または「体験版」が表示されます
有効期限	Safe Lock Intelligent Manager と Safe Lock エージェントのサポートサービスを受けられる期限の日付が表示されます
アクティベーションコード	アクティベーションコードが表示されます 詳細については、88 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。
最終更新日	アクティベーションコードの前回の更新日が表示されます

アクティベーションコードを変更する

手順

1. 管理サーバ画面の上部にあるナビゲーションで [管理] > [ライセンス管理] の順に選択します。

   [ライセンス管理] 画面が表示されます。

2. [アクティベーションコードの入力] をクリックします。

3. Trend Micro Safe Lock Intelligent Manager の新しいアクティベーションコードを入力します。

   エージェントのライセンスをリモートで更新するには、207 ページの「エージェントのライセンスを更新する」を参照してください。

   注意

   [表示更新] をクリックして、製品ライセンスを更新します。トレンドマイクロの製品ライセンスサーバへの接続が必要になります。

第 5 章

エージェントのメイン画面の使用

この章では、エージェントのメイン画面を使用して Trend Micro Safe Lock を設定する方法について説明します。

この章の内容は次のとおりです。

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。

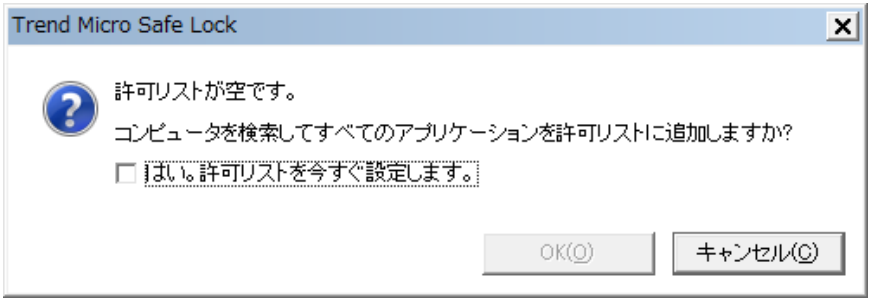
手順

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。

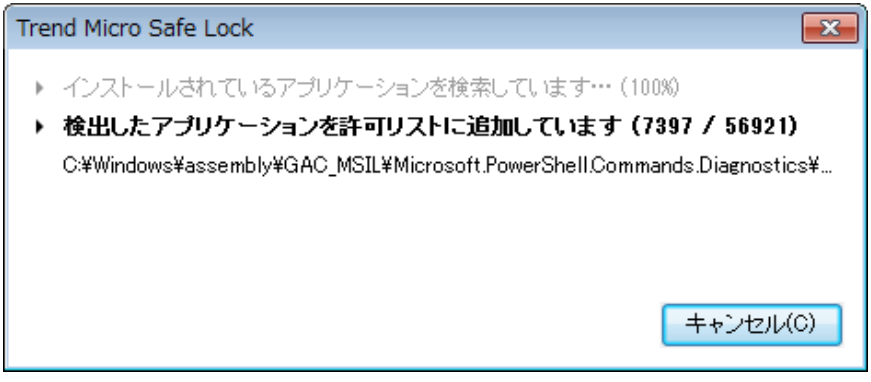
2. パスワードを入力して [ログイン] をクリックします。

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。

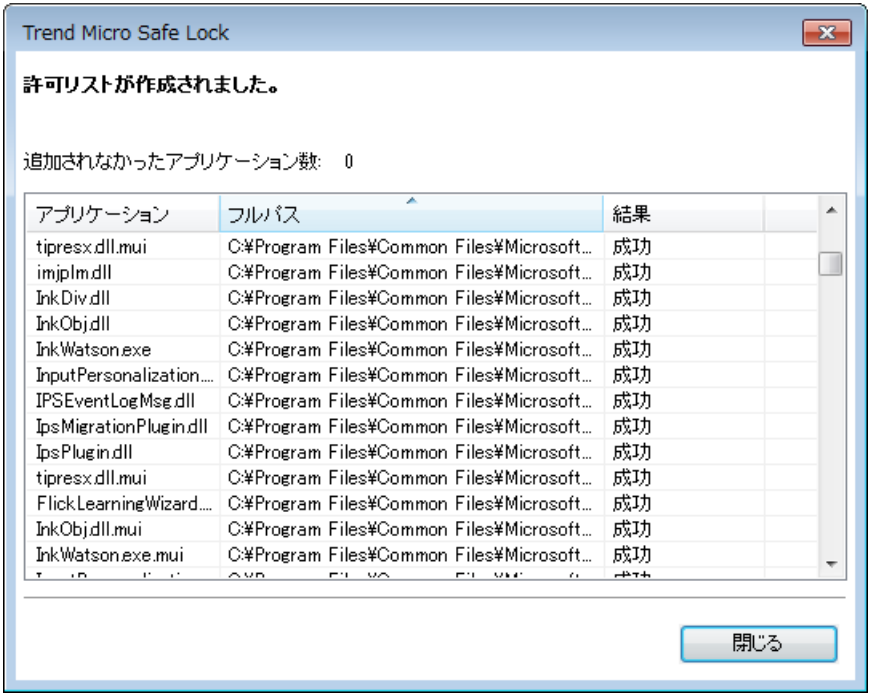


3. 通知ウィンドウで、[はい。許可リストを今すぐ設定します。] を選択して [OK] をクリックします。

   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。

ブロックされたファイルのポップアップ通知を設定する

許可されていないファイルの実行やエージェントへの変更を Safe Lock がブロックしたときに管理下のエージェントに表示する通知を設定できます。こ

の通知はあらゆるブロックイベントの管理者に送信され、ブロックされたファイルの詳細情報を提供します。

注意

- この機能は初期設定で無効になっています。
- Safe Lock では、エージェントの Setup.ini ファイルを使用した機能のカスタマイズのみがサポートされます。また、カスタマイズを適用にするには再配信が必要になります。

表 5-1. ブロックされたファイルのポップアップ通知を設定する

設定	初期設定	設定場所	
		エージェント配信前	エージェント配信後
通知を有効にする	無効	エージェントの Setup.ini ファイルの `[BlockNotification]` セクションをカスタマイズします。	エージェントのコマンドラインインタフェースに `blockedfilenotification` コマンドを入力します。
通知を閉じるときに管理者パスワードを要求する	有効 (通知機能が有効な場合)		サポートされていません
イベントの詳細を表示する (ファイル名、ファイルパス、イベント時間)			サポートされていません
通知のタイトルとメッセージをカスタマイズする	• タイトル: アプリケーションがブロックされました • メッセージ: プログラムがブロックされました。ヘルプデスクまたは管理者に問い合わせてください。		サポートされていません

エージェントのメイン画面について

エージェントのメイン画面を使用すると、Trend Micro Safe Lock でよく使用する機能に簡単にアクセスできます。

図 5-1. Safe Lock のメイン画面

次の表は、メイン画面で使用できる機能を示しています。

表 5-2. メイン画面の機能の説明

#	項目	説明
1	概要	Trend Micro Safe Lock のステータスを表示します
	許可リスト	実行が許可されているアプリケーションを表示し、ユーザがリストを管理できるようにします
	パスワード	Safe Lock 管理者と制限付きユーザのパスワードを変更します (管理者のみ可能)
	設定	脆弱性攻撃対策の設定の有効化または無効化とシステム設定のエクスポートまたはインポートを行います
	バージョン情報	製品およびコンポーネントのバージョンを表示します
2	ステータス情報	Trend Micro Safe Lock の現在のステータスを表示します
3	アプリケーション制御を有効にする	システムをロックダウンし、許可リストにないアプリケーションの実行をブロックします
	アプリケーション制御を無効にする	システムのロックダウンを解除し、許可リストにないアプリケーションの実行を許可します **注意** アプリケーション制御を無効にすると Safe Lock Intelligent Manager が「監視」モードに切り替わります。Safe Lock Intelligent Manager ではアプリケーションの実行がブロックされなくなりますが、許可リストにないアプリケーションが実行されるとログに記録されます。これらのログを使用して、エージェントで必要なアプリケーションがすべて許可リストに含まれているかどうかを判断できます。

#	項目	説明
4	アプリケーション制御が有効になった日時	アプリケーション制御が前回有効になった日付と時刻を表示します
	アプリケーション制御が無効になった日時	アプリケーション制御が前回無効になった日付と時刻を表示します
5	脆弱性攻撃対策	有効: すべての脆弱性攻撃対策機能が有効化されます ステータスをクリックすると、設定画面が開きます。
		有効 (一部): 脆弱性攻撃対策機能の一部が有効化されます ステータスをクリックすると、設定画面が開きます。
		無効: 脆弱性攻撃対策機能が有効化されません ステータスをクリックすると、設定画面が開きます。
6	許可リストステータス	許可リストの項目数または許可リストの更新日時をクリックすると、許可リストが表示されます。 前回のアプリケーションブロック日時をクリックすると、ブロックされたアプリケーションのログが表示されます。
7	ライセンス有効期限	Trend Micro Safe Lock の有効期限を表示します 日付をクリックすると、新しいアクティベーションコードを入力できます。

Safe Lock のステータスを表示する

Safe Lock のステータスは、システムトレイアイコンで以下のように表示されます。

注意

インストール時にシステムトレイアイコンを無効にしている場合は表示されません。

表 5-3. ステータスアイコンの説明

管理サーバ画面アイコン	システムトレイアイコン	ステータス	説明
		ロック	システムがロックダウンされています。許可リストに登録されていないアプリケーションは実行できません。
		ロック解除	システムのロックダウンが解除されています。許可リストに登録されていないアプリケーションも実行可能です。
該当なし		有効期限終了	Trend Micro Safe Lock のサポート契約の有効期限が終了していると、システムをロックできません。メイン画面から有効期限をクリックしてアクティベーションコードを入力します。
該当なし		ブロック	Safe Lock はブロックされており、許可されていないアプリケーションを実行したり、管理下のエージェントに変更を加えたりすることはできません。

許可リストについて

Trend Micro Safe Lock で実行を許可するファイルを追加/表示するには、許可リストを使用します。

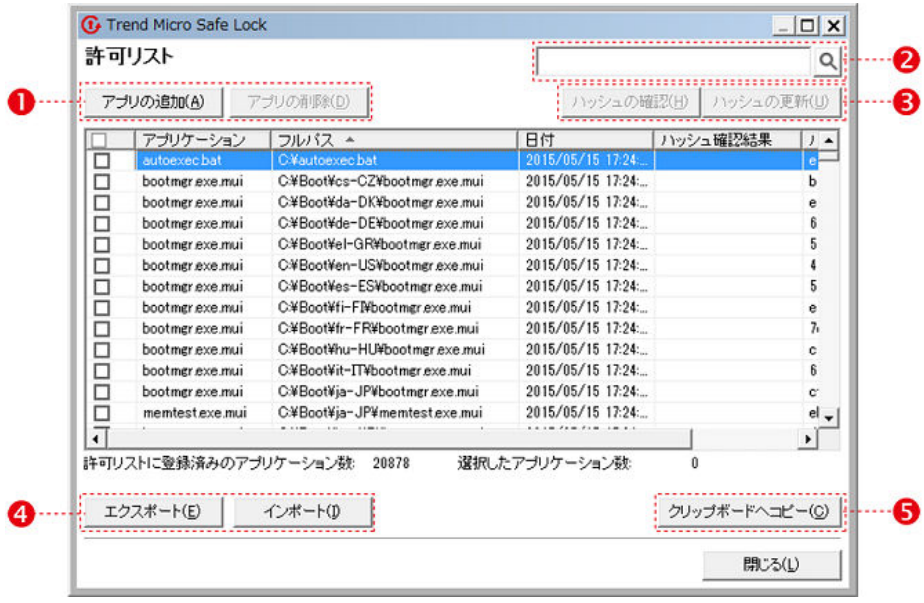


図 5-2. Trend Micro Safe Lock の許可リスト

次の表は、許可リストの画面で使用できる機能を示しています。

表 5-4. 許可リストの項目の説明

#	項目	説明
1	アプリの追加/アプリの削除	選択した項目を許可リストに追加または許可リストから削除します。
2	検索バー	[アプリケーション] 列および [ファイルパス] 列を検索します。
3	ハッシュの確認/ハッシュの更新	許可リストのアプリケーションに対するハッシュ値を確認または更新します。
4	エクスポート/インポート	許可リストをエクスポートまたはインポートします。

#	項目	説明
5	クリップボードへコピー	CSV 形式 (カンマ区切りのテキスト) で許可リストをクリップボードにコピーします。リストを確認したりレポートを作成するのが容易になります。

ハッシュについて

Trend Micro Safe Lock では、許可リスト内の各ファイルについて一意のハッシュ値が計算されます。ハッシュ値はファイル変更が行われるたびに変わるため、この値を使用してファイルに加えられた変更を検出できます。現在のハッシュ値を以前の値と比較することで、ファイルに対して変更が行われたかどうかを確認できます。

次の表は、ハッシュを確認するためのステータスアイコンを示しています。

表 5-5. ハッシュを確認するためのステータスアイコン

アイコン	説明
	計算されたハッシュ値は、保存されている値と一致しています。
	計算されたハッシュ値は、保存されている値と一致していません。
	ハッシュ値の計算でエラーが発生しました。

許可リスト自動更新を使用せずにファイルを移動または上書きすると、ハッシュ値が一致しなくなることがありますが、この不一致は、他のアプリケーション (不正プログラムを含む) によって既存ファイルが変更または上書きされた結果である可能性があります。ハッシュ値の不一致が発生した理由が不明な場合は、Trend Micro Portable Security を使用してエージェントを検索し、脅威が存在しないかどうか確認してください。

ハッシュを確認または更新する

許可リスト内のファイルのハッシュ値を確認すると、実行を許可されているファイルの整合性を確認できます。

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. [許可リスト] メニュー項目をクリックしてリストを開きます。

   ファイルのハッシュ値を確認するには

   a. 確認するファイルを選択します。すべてのファイルを確認するには、許可リストの上部にあるチェックボックスをオンにします。

   b. [ハッシュの確認] をクリックします。

   ファイルのハッシュ値を更新するには

   a. 更新するファイルを選択します。

   b. [ハッシュを更新] をクリックします。

重要

ハッシュ値の不一致が発生した原因が不明な場合は、エージェントのウイルス検索などを行って脅威が存在しないかどうか確認してください。

許可リストの設定

許可リストの設定後、ユーザは [アプリの追加] をクリックして新しいプログラムを追加できます。クリックすると、次の表に示すオプションが表示されます。

表 5-6. 許可リストにアプリケーションを追加する方法

オプション	使用する場面
手動で参照しファイルを選択する	対象ソフトウェアがすでにエージェント上に存在し、それが最新の状態である場合は、このオプションを選択します。ファイルを追加すると、そのファイルの起動が可能になりますが、そのファイルやシステムは変更されません。 たとえば、初期設定の後に Windows Media Player (`wmplayer.exe`) が許可リストに含まれていない場合、ユーザは画面から許可リストにそれを追加できます。
選択したアプリケーションインストーラによって作成または修正されたファイルを自動的に追加する (許可リスト自動更新)	Trend Micro Safe Lock をロック解除せずに管理下のエージェントに対して新規アプリケーションの追加やアップデートを実行する必要がある場合は、このオプションを選択します。Trend Micro Safe Lock によって新規または修正されたファイルが許可リストに追加されます。 たとえば、Mozilla Firefox をインストールまたはアップデートする必要がある場合は、このオプションを選択してインストールまたはアップデートを許可し、処理中に作成または修正されたファイルを許可リストに追加します。

ファイルを追加または削除する

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. [許可リスト] メニュー項目をクリックしてリストを開きます。

   項目を追加するには

   a. [アプリの追加] をクリックし、[手動で参照しファイルを選択する] を選択して、[次へ] をクリックします。

   b. 表示されるウィンドウで、[特定のアプリケーション]、[選択したフォルダ内のすべてのアプリケーション]、または [指定したパス以下のすべてのアプリケーション] をドロップダウンリストから選択します。

選択画面が開きます。

c. 追加するアプリケーションまたはフォルダを選択して、[開く] または [OK] をクリックします。

d. [OK] をクリックします。追加する項目を確認して、[許可(A)] をクリックします。

e. 必要な項目を許可リストに追加したら、[閉じる] をクリックします。

項目を削除するには

a. 許可リストで、削除するアプリケーションを検索します。

b. 削除するファイル名の横にあるチェックボックスをオンにして、[アプリの削除] をクリックします。

c. 項目を削除するかどうか確認する画面で、[OK] をクリックします。

d. もう一度 [OK] をクリックして、確認ウィンドウを閉じます。

許可リスト自動更新を使用して、アップデートまたはインストールする

Trend Micro Safe Lock では、許可リスト自動更新によってアプリケーションが追加または変更されると、そのアプリケーションが許可リストに自動的に追加されます。

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、管理サーバ画面を開きます。
2. パスワードを指定して [ログイン] をクリックします。
3. [許可リスト] メニュー項目をクリックしてリストを開きます。
4. アプリケーションをインストールまたはアップデートするには、許可リスト自動更新によって一時的に実行を許可するインストーラを選択します。

a. [アプリの追加] をクリックし、[選択したアプリケーションインストーラによって作成または修正されたファイルを自動的に追加する] を選択して、[次へ] をクリックします。

b. 表示されるウィンドウで、[特定のインストーラ]、[フォルダ/サブフォルダ内のすべてのインストーラ]、または [フォルダ内のすべてのインストーラ] をドロップダウンリストから選択します。

c. 追加するインストールパッケージまたはフォルダを選択して、[開く] をクリックします。

注意

許可リスト自動更新に追加できるのは、既存の EXE、MSI、BAT、および CMD ファイルのみです。

d. 期待する項目がリストに表示されていることを確認して、[開始] をクリックします。

進捗を表すアニメーションが表示されます。

図 5-3. 進捗を表すアニメーション

5. プログラムを通常どおりインストールまたはアップデートします。完了したら、進捗を表すアニメーションで [停止] をクリックします。
6. 期待する項目が許可リストに表示されていることを確認し、[許可] をクリックしてから、[閉じる] をクリックします。

許可リストをエクスポートまたはインポートする

許可リストをエクスポートまたはインポートして、大規模な展開を行う場合に再利用できます。[クリップボードへコピー] を使用すると、Windows のクリップボードに CSV バージョンのリストが作成されます。

注意

Trend Micro Safe Lock は OS の実行ファイルも制御対象として制御します。許可リストをインポートする際には、エクスポートしたシステムと OS ファイルレベルで同じことを確認してからインポートしてください。

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. [許可リスト] メニュー項目をクリックしてリストを開きます。

   許可リスト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。

   許可リストをインポートするには

   a. [インポート] をクリックして、許可リストを探します。
   b. ファイルを選択して、[開く] をクリックします。

アカウントの種類

Trend Micro Safe Lock の権限設定により、管理者はメイン画面の特定機能へのアクセス権をユーザに付与できます。設定ファイルを使用して、制限付きユーザアカウントで使用可能な機能を指定できます。

表 5-7. Trend Micro Safe Lock のアカウント

アカウント	詳細
管理者	• 初期設定のアカウント • Trend Micro Safe Lock の機能へのフルアクセス • メイン画面とコマンドラインの両方を使用可能
制限付きユーザ	• メンテナンス用セカンダリアカウント • Trend Micro Safe Lock の機能への制限付きアクセス • メイン画面のみ使用可能

制限付きユーザアカウントを有効にするには、106 ページの「パスワードの設定」を参照してください。特定のアカウントでログインするには、そのアカウントのパスワードを指定します。

パスワードの設定

Safe Lock 管理者と制限付きユーザのパスワードはメイン画面を使用して変更できますが、パスワードを変更できるのは管理者のみです。管理者アカウントでメイン画面にログインするには、メイン画面の起動時に管理者パスワードを入力します。

重要

Safe Lock 管理者と制限付きユーザのパスワードは同一にできません。

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. Safe Lock 管理者パスワードを指定して、[ログイン] をクリックします。
3. [パスワード] メニュー項目をクリックして管理者パスワードページを表示します。

   Safe Lock 管理者パスワードを変更するには

   a. 現在のパスワードを入力し、新しいパスワードを指定して確認し、[保存] をクリックします。

   警告!

   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。

   制限付きユーザのパスワードを作成するには

   a. メイン画面上部の [制限付きユーザ] をクリックします。
   b. [制限付きユーザを有効にする] チェックボックスをオンにします。
   c. パスワードを指定して確認し、[保存] をクリックします。

   既存の制限付きユーザのパスワードを変更するには

   a. 新しいパスワードを指定して確認し、[保存] をクリックします。

機能の設定について

Trend Micro Safe Lock では、以下の保護機能を提供します。

図 5-4. Trend Micro Safe Lock の設定画面

表 5-8. 不正侵入対策

設定	説明
USB 不正プログラム対策	USB 不正プログラム対策を使用すると、USB デバイスからエージェントへのウイルスの感染を防ぐことができます。ドライブの内容を表示するだけでも、ウイルスが感染する場合があります。 この機能を有効にすると、USB デバイス上のファイルからエージェントにウイルスが自動感染することを防止できます。

設定	説明
ネットワークウイルス対策	ネットワークトラフィックの送受信を検索して、ネットワーク上のコンピュータまたはその他のデバイスに脅威が感染しないようブロックします。 この機能を有効にすると、ネットワーク上の脅威がエージェントに感染することを防止できます。

表 5-9. 実行防止対策

設定	説明
メモリのランダム化 (再起動が必要)	Address Space Layout Randomization (アドレス空間配置のランダム化) は、重要な機能に対するメモリの場所をランダムに割り当てることで、攻撃者が特定のプロセスのメモリの場所を強引に推測して行うシェルコードインジェクションを防止します。 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 などの以前のオペレーティングシステムに対して、この機能を有効にしてください。 注意 メモリのランダム化を有効または無効にするには、エージェントを再起動する必要があります。
DLL インジェクション対策	DLL インジェクション対策は、不正なソフトウェアなどで使用される API コールの動作を検出してブロックします。これらの脅威をブロックすることで、不正なプロセスの実行を防止できます。 システムをさまざまな種類の重大な脅威から保護するために、トラブルシューティングを目的とする場合を除き、この機能は無効にしないでください。
API フッキング対策	API フッキング対策は、オペレーティングシステム内の重要なプロセスで使用されるメッセージの遮断や改変を実行しようとする不正なソフトウェアを検出してブロックします。 システムをさまざまな種類の重大な脅威から保護するために、トラブルシューティングを目的とする場合を除き、この機能は無効にしないでください。

表 5-10. アプリケーション制御

設定	説明	
DLL/ドライバ制御	DLL/ドライバファイルの制御を行います。DLL/ドライバファイル制御が有効な場合は、許可リストに含まれる DLL、ドライバファイルのみがロードされます。	**重要** DLL/ドライバ制御、スクリプト制御、書き込み制御、またはファイルレス攻撃対策を有効にするには、管理下のエージェントでアプリケーション制御が有効であることを確認してください。
スクリプト制御	スクリプトファイルの制御を行います。スクリプト制御が有効な場合は、許可リストに含まれるスクリプトファイルのみがインタープリタアプリケーションに読み込まれます。	
書き込み制御	書き込み制御リストに登録されたオブジェクト (ファイル、フォルダ、レジストリエントリ) への書き込みアクセスを防止し、オプションで、許可リストに登録されたファイルへの書き込みアクセスを防止します。	
ファイルレス攻撃対策	ファイルレス攻撃イベントにつながる可能性のある、許可されていないプロセスチェーンおよび引数の組み合わせを検出してブロックします。	

表 5-11. デバイスコントロール

設定	説明
ストレージデバイスのブロック	管理下のエージェントへの USB ドライブ、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。

表 5-12. その他

設定	説明
変更監視	変更監視では、管理下のエージェントのファイル、フォルダおよびレジストリの変更に関連するイベントを記録します。 **注意** 管理下のエージェントの変更監視ログを表示するには、[スタート] > [コントロール パネル] > [管理ツール] の順に選択し、[イベント ビューアー] にアクセスします。

機能の設定を有効または無効にする

注意

Trend Micro Safe Lock では、初期設定で脆弱性攻撃対策の [DLL/ドライバ制御] および [スクリプト制御] 機能が有効になっています。ネットワークウイルス対策は、初期インストール時にインストールしなかった場合は選択できません。そのためネットワークウイルス対策を利用したい場合は、Trend Micro Safe Lock の再インストールが必要です。

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、脆弱性攻撃対策の設定を行います。
4. 該当する機能を有効または無効にします。
5. [保存] をクリックします。

第 6 章

エージェントのコマンドラインの使用

この章では、コマンドラインを使用した Trend Micro Safe Lock の設定と使用方法について説明します。

この章の内容は次のとおりです。

コマンドラインで SLCmd を使用する

管理者は、SLCmd.exe プログラムを使用して、コマンドラインから直接 Trend Micro Safe Lock を操作できます。

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。
2. cd コマンドを使用して、Trend Micro Safe Lock のインストールフォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   ```
   cd /d "c:\Program Files\Trend Micro\Trend Micro Safe Lock\"
   ```

3. 「SLCmd.exe」と入力します。

SLCmd プログラムとメイン画面の機能の比較

次の表は、SLCmd プログラムと Safe Lock のメイン画面プログラムで使用できる Trend Micro Safe Lock の機能を一覧表示しています。

表 6-1. コマンドラインでの SLCmd プログラムとメイン画面の機能の比較

機能	コマンドラインでの SLCMD プログラム	メイン画面
アカウントの管理	あり	あり
許可リストの管理	あり	あり
設定ファイルの暗号化/復号	あり	なし
ブロックされたアプリケーションのログの表示	あり	あり
許可リストのエクスポート/インポート	あり	あり
設定のエクスポート/インポート	あり	あり

機能	コマンドラインでの SLCMD プログラム	メイン画面
インストール	あり	あり
Windows Update サポート	あり	なし
ロック/ロック解除	あり	あり
ライセンスの管理	あり	あり
設定	制限あり	制限あり
許可リスト自動更新の起動/停止	あり	あり
サービスの開始/停止	あり	なし
書き込み制御	あり	あり
管理者パスワード	あり	あり
アプリケーション制御の有効化/無効化	あり	あり
ブロックされたファイルのポップアップ通知の有効化/無効化	あり	なし
変更監視	あり	あり
信頼するハッシュリスト	あり	なし
除外設定	あり	なし
アンインストール	なし	なし
ストレージデバイスコントロール	あり	あり
ファイルレス攻撃対策	あり	あり

コマンドライン またはメイン画面ですべての設定を行えるわけではありません。システム設定の変更の詳細については、262 ページの「エージェント設定ファイルの操作」を参照してください。

SLCmd プログラムのコマンド

次の表は、コマンドラインで SLCmd プログラムとともに使用できる主なコマンドを一覧表示しています。SLCmd プログラムを使用するには、SLCmd および目的のコマンドを入力します。「SLCmd」と入力して <Enter> キーを押し、使用可能なコマンドのリストを表示します。

注意

SLCmd をコマンドラインで使用できるのは、Windows の管理者権限を持つ Safe Lock の管理者のみです。SLCmd では、コマンドを実行する前に管理者のパスワードを求めるプロンプトが表示されます。

SLCmd プログラムとともに使用できるコマンドの詳細なリストは次のとおりです。

汎用コマンド

コマンドラインインタフェースを使用して一般的な処理を実行します。

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-2. 省略表記と用法

パラメータ	省略表記	用法
adminpassword	ap	Trend Micro Safe Lock の管理者パスワードを管理します
lock	lo	アプリケーション制御のステータスを管理します
blockedlog	bl	Trend Micro Safe Lock でブロックされたアプリケーションを管理します
license	lc	Trend Micro Safe Lock のライセンスを管理します
settings	set	Trend Micro Safe Lock の設定を管理します
service	srv	Safe Lock サービスを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-3. 汎用コマンド

コマンド	パラメータ	説明
`help`		このヘルプファイルを表示します たとえば、次のように入力します。 `SLCmd.exe help`
`activate`	<activation_code>	本製品をアクティベートします たとえば、次のように入力します。 `SLCmd.exe activate XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`
`set adminpassword`		管理者のパスワードを設定します 確認のためのパスワードの再入力が必要です たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set adminpassword`
	<new_password>	管理者のパスワードを設定します 確認のためのパスワードの再入力は不要です たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set adminpassword P@ssW0Rd`
`set lock`		現在のアプリケーション制御のステータスを表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set lock` 注意 初期ステータスは `disable` です。

コマンド	パラメータ	説明
	enable	アプリケーション制御を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set lock enable
	disable	アプリケーション制御を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set lock disable
set blockedfilenotification		現在の通知設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set blockedfilenotification 注意 初期設定は disable です。
	enable	Safe Lock が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 たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set blockedfilenotification enable
	disable	Safe Lock がファイルをブロックしても通知を表示しません たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set blockedfilenotification disable
show blockedlog		ブロックされたアプリケーションログを表示します たとえば、次のように入力します。

コマンド	パラメータ	説明
		SLCmd.exe -p <admin_password> show blockedlog
show license		ライセンス情報を表示します たとえば、次のように入力します。 SLCmd.exe show license
show settings		現在の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show settings
start service		Safe Lock サービスを起動します たとえば、次のように入力します。 SLCmd.exe start service
status		現在の Safe Lock のステータスを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> status
stop service		Safe Lock サービスを停止します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> stop service
version		バージョン情報を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> version

集中管理コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、集中管理機能を設定します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-4. 省略表記と用法

パラメータ	省略表記	用法
managedmodeconfiguration	mmc	設定ファイルを管理します
servercertification	sc	サーバ証明書ファイルを管理します
managedmode	mm	エージェントの「集中管理モード」を管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-5. 集中管理コマンド

コマンド	パラメータ	説明
decrypt managedmodeconfiguration	<path_of_encrypted_file> <path_of_decrypted_output_file>	集中管理モードの設定ファイルを復号します
encrypt managedmodeconfiguration	<path_of_file> <path_of_encrypted_output_file>	集中管理モードの設定ファイルを暗号化します
export managedmodeconfiguration	<path_of_encrypted_output>	指定したファイルに集中管理モードの設定をエクスポートします
export servercertification	<path_of_certification_file>	指定したファイルに管理サーバの証明書ファイルをエクスポートします
import managedmodeconfiguration	<path_of_encrypted_input>	指定した集中管理モードの設定ファイルをインポートします
import servercertification	<path_of_certification_file>	管理サーバの証明書ファイルをインポートします

コマンド	パラメータ	説明
set managedmode	enable [-cfg <path_of_encrypted_file>] [-sc <path_of_certification_file]	集中管理モードを有効にします 注意 初期設定は disable です。 次のオプションのパラメータを使用できます。 • -cfg <path_of_encrypted_file> -cfg: 設定ファイルのパスを指定できます • -sc <path_of_certification_file -sc: 証明書ファイルのパスを指定できます
set managedmode		現在の集中管理モードを表示します
show managedmodeconfiguration		集中管理モードの設定を表示します
test managedmode		管理サーバにテスト接続します

オプション機能コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、オプションのセキュリティ機能を設定します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-6. 省略表記と用法

パラメータ	省略表記	用法
apihookingprevention	api	API フッキング対策を管理します
customaction	ca	Trend Micro Safe Lock で特定の種類のイベントがブロックされたときの処理を管理します
dlldriverlockdown	dd	DLL/ドライバ制御を管理します
dllinjectionprevention	dll	DLL インジェクション対策を管理します
exceptionpath	ep	アプリケーション制御の除外対象を管理します
integritymonitoring	in	変更監視を管理します
memoryrandomization	mr	メモリのランダム化を管理します
networkvirusprotection	net	ネットワークウイルス対策を管理します
script	scr	スクリプト制御を管理します
storagedeviceblocking	sto	管理下のエージェントへのストレージデバイス (CD/DVD ドライブ、フロッピーディスクドライブ、およびネットワークドライブ) によるアクセスを許可またはブロックします。
usbmalwareprotection	usb	USB 不正プログラム対策を管理します
writeprotection	wp	書き込み制御を管理します
writeprotection-includes-approvedlist	wpal	許可リストを含む書き込み制御を管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-7. オプション機能コマンド

コマンド	パラメータ	説明
`set apihookingprevention`	`enable`	API フッキング対策を有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set apihookingprevention enable` **注意** 初期ステータスは `Disabled` です。
	`disable`	API フッキング対策を無効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set apihookingprevention disable`
		API フッキング対策の設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set apihookingprevention`
`set customaction`		カスタムイベント処理の設定を表示します **注意** 初期設定は `Ask` です。
	`ignore`	カスタムイベント処理を「無視」にします アプリケーションがブロックされた後にアプリケーションに対して追加の処理を行いません

コマンド	パラメータ	説明
		たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set customaction ignore`
	`quarantine`	カスタムイベント処理を「隔離」にします アプリケーションがブロックされた後にアプリケーションに対して隔離処理を行います Windows 2000 や Windows XP などの環境では設定できません たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set customaction qurantine` **注意** Safe Lock は、Windows XP または Windows 2003 に対して「隔離」のカスタム処理をサポートしていません。
	`ask`	カスタムイベント処理を「確認」にします アプリケーションがブロックされた後にアプリケーションに対する処理を管理者がサーバで確認できるようにします 集中管理モードでのみ有効です たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set customaction ask`
`set dlldriverlockdown`		DLL/ドライバ制御の設定を表示します たとえば、次のように入力します。

コマンド	パラメータ	説明
		`SLCmd.exe -p <admin_password> set dlldriverlockdown` **注意** 初期ステータスは `Enabled` です。
	`enable`	DLL/ドライバ制御を有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dlldriverlockdown enable`
	`disable`	DLL/ドライバ制御を無効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dlldriverlockdown disable`
`set dllinjectionpreventi on`		DLL インジェクション対策の設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dllinjectionprevention` **注意** 初期ステータスは `Disabled` です。
	`enable`	DLL インジェクション対策を有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dllinjectionprevention enable`
	`disable`	DLL インジェクション対策を無効にします

コマンド	パラメータ	説明
		たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set dllinjectionprevention disable`
`set exceptionpath`		アプリケーション制御の除外パス設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set exceptionpath` **注意** 初期設定は `Disabled` です。
	`enable`	アプリケーション制御の除外パス設定を有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set exceptionpath enable`
	`disable`	アプリケーション制御の除外パス設定を無効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set exceptionpath disable`
`set integritymonitoring`		変更監視機能の設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set integritymonitoring` **注意** 初期ステータスは `Disabled` です。

コマンド	パラメータ	説明
	enable	変更監視機能を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set integritymonitoring enable
	disable	変更監視機能を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set integritymonitoring disable
set memoryrandomization		メモリのランダム化の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set memoryrandomization 注意 初期ステータスは Disabled です。
	enable	メモリのランダム化を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set memoryrandomization enable
	disable	メモリのランダム化を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set memoryrandomization disable
set networkvirusprotection		ネットワークウイルス対策の設定を表示します たとえば、次のように入力します。

コマンド	パラメータ	説明
		`SLCmd.exe -p <admin_password> set networkvirusprotection` **注意** 初期ステータスは `Enabled` です。
	`enable`	ネットワークウイルス対策を有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set networkvirusprotection enable`
	`disable`	ネットワークウイルス対策を無効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set networkvirusprotection disable`
`set script`		スクリプト制御の設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set script` **注意** 初期ステータスは `Enabled` です。
	`enable`	スクリプト制御を有効にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set script enable`

コマンド	パラメータ	説明
	disable	スクリプト制御を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set script disable
set storagedeviceblocking		ストレージデバイスのブロックの設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set storagedeviceblocking  注意 初期ステータスは Disabled です。
	enable	ストレージデバイスのブロックを有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set storagedeviceblocking enable
	disable	ストレージデバイスのブロックを無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set storagedeviceblocking disable
set usbmalwareprotection		USB 不正プログラム対策の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set usbmalwareprotection

コマンド	パラメータ	説明
		注意 初期ステータスは Disabled です。
	enable	USB 不正プログラム対策を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set usbmalwareprotection enable
	disable	USB 不正プログラム対策を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set usbmalwareprotection disable
set writeprotection		書き込み制御機能の設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set writeprotection 注意 初期ステータスは Disabled です。
	enable	書き込み制御機能を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set writeprotection enable
	disable	書き込み制御機能を無効にします たとえば、次のように入力します。

コマンド	パラメータ	説明
		`SLCmd.exe -p <admin_password> set writeprotection disable`
`set writeprotection-includes-approvedlist`		書き込み制御のオプション設定を表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist` **注意** 初期ステータスは `Disabled` です。ただし、書き込み制御が有効になると、ステータスは `Enabled` に変更されます。
	`enable`	書き込み制御有効時に許可リストを書き込み制御の保護対象にします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist enable`
	`disable`	許可リストを書き込み制御の保護対象から外します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> set writeprotection-includes-approvedlist disable`

制限付きユーザアカウントのコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、制限付きユーザアカウントを設定します。

`SLCmd.exe -p <admin_password> <command> <parameter> <value>`

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-8. 省略表記と用法

パラメータ	省略表記	用法
user	us	制限付きユーザアカウントを管理します
userpassword	up	制限付きユーザのパスワードを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-9. 制限付きユーザアカウントのコマンド

コマンド	パラメータ	説明
set user		制限付きユーザのアカウントの設定を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set user 注意 初期ステータスは Disabled です。
	enable	制限付きユーザのアカウントを有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set user enable
	disable	制限付きユーザのアカウントを無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set user disable

コマンド	パラメータ	説明
set userpassword		制限付きユーザのアカウントパスワードを設定します 確認のためのパスワードの再入力が必要です たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set userpassword
	<new_password>	制限付きユーザのアカウントパスワードを設定します 確認のためのパスワードの再入力は不要です たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set userpassword P@ssW0Rd

スクリプトコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、スクリプトを配信します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-10. 省略表記と用法

パラメータ	省略表記	用法
script	scr	スクリプトコマンドを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-11. スクリプトコマンド

コマンド	パラメータ	説明
`add script`	<extension><interpreter1> [interpreter2] ...	指定したファイル拡張子とスクリプトインタープリタをスクリプト制御のルールとして追加します たとえば、スクリプトの拡張子 `JSP` とインタープリタファイル `jscript.js` を追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> add script jsp C:\Scripts\jscript.js`
`remove script`	<extension> [interpreter1] [interpreter2] ...	指定したファイル拡張子とスクリプトインタープリタをスクリプト制御のルールから削除します たとえば、スクリプトの拡張子 `JSP` とインタープリタファイル `jscript.js` を削除するには、次のように入力します。 `SLCmd.exe -p <admin_password> remove script jsp C:\Scripts\jscript.js` **注意** インタープリタを指定しない場合は、スクリプトの拡張子に関連するすべてのインタープリタが削除されます。インタープリタを指定すると、指定したインタープリタのみがスクリプト拡張子ルールから削除されます。
`show script`		スクリプト制御のルールを表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show script`

注意

Safe Lock では次の初期設定のスクリプト制御のルールを使用します。

- bat <cmd.exe>
- cmd <cmd.exe>
- com <ntvdm.exe>
- dll <ntvdm.exe>
- drv <ntvdm.exe>
- exe <ntvdm.exe>
- js <cscript.exe>,<wscript.exe>
- msi <msiexec.exe>
- pif <ntvdm.exe>
- ps1 <powershell.exe>
- sys <ntvdm.exe>
- vbe <cscript.exe>,<wscript.exe>
- vbs <cscript.exe>,<wscript.exe>

許可リストコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、許可リストを設定します。

`SLCmd.exe -p <admin_password> <command> <parameter> <value>`

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-12. 省略表記と用法

パラメータ	省略表記	用法
`approvedlist`	`al`	許可リストのファイルを管理します

パラメータ	省略表記	用法
list	li	許可リストのインポート/エクスポート機能を管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-13. 許可リストコマンド

コマンド	パラメータ	説明
add approvedlist	[-r] <file_or_folder_path>	ファイルを許可リストに追加します たとえば、すべての Microsoft Office ファイルを許可リストに追加するには、次のように入力します。 SLCmd.exe -p <admin_password> add approvedlist -r "C:\Program Files\Microsoft Office" 注意 -r パラメータを使用すると、指定したフォルダのすべてのサブフォルダとファイルが含まれます。
remove approvedlist	<file_path>	指定したファイルを許可リストから削除します たとえば、notepad.exe を許可リストから削除するには、次のように入力します。 SLCmd.exe -p <admin_password> remove approvedlist C:\Windows\notepad.exe
show approvedlist		許可リストのファイルを一覧表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show approvedlist
check approvedlist	-f	許可リストのファイルをチェックしてハッシュの不一致を修復します たとえば、次のように入力します。

コマンド	パラメータ	説明
		SLCmd.exe -p <admin_password> check approvedlist -f
	-q	許可リストのファイルをチェックして確認結果を一覧表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> check approvedlist -q
	-v	許可リストのファイルをチェックして詳細な確認結果を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> check approvedlist -v
export list	<output_file>	指定したファイルに許可リストをエクスポートします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> export list c:\approvedlist\ap.db **注意** 出力ファイルのタイプは DB 形式である必要があります。
import list	[-o] <input_file>	指定したファイルから許可リストをインポートして既存のリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> import list c:\approvedlist\ap.db

コマンド	パラメータ	説明
		注意 入力ファイルのタイプは DB 形式である必要があります。 必要に応じて-o 値を使用して、既存のリストを上書きします。

アプリケーション制御関連のコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、アプリケーション制御に関連する処理を実行します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-14. 省略表記と用法

パラメータ	省略表記	用法
quarantinedfile	qf	隔離ファイルを管理します
exceptionpath	ep	アプリケーション制御の除外対象を管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-15. アプリケーション制御関連のコマンド

コマンド	パラメータ	説明
show quarantinedfile		隔離ファイルの一覧を表示します
restore quarantinedfile	<id> [-al] [-f]	指定した隔離ファイルを復元します -al: オプションで復元したファイルを許可リストに追加します

コマンド	パラメータ	説明
		-f: オプションで強制的にファイルを復元します
remove quarantinedfile	<id>	指定した隔離ファイルを削除します
show exceptionpath		アプリケーション制御の除外パスを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show exceptionpath
add exceptionpath	-e <file_path>-t file	指定したファイルをアプリケーション制御の除外パスリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add exceptionpath -e c:¥sample.bat -t file
	-e <folder_path>-t folder	指定したフォルダをアプリケーション制御の除外パスリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add exceptionpath -e c:¥folder -t folder
	-e <folder_path>-t folderandsub	指定したフォルダおよびサブフォルダをアプリケーション制御の除外パスリストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add exceptionpath -e c:¥folder -t folderandsub
	-e <regular_expression>-t regexp	正規表現を使用して除外を追加します たとえば、次のように入力します。 • SLCmd.exe -p <admin_password> add exceptionpath -e c:¥¥folder¥¥.*-t regexp

コマンド	パラメータ	説明
		• SLCmd.exe -p <admin_password> add exceptionpath -e ¥¥¥¥computer¥¥folder¥¥.*¥¥file¥.exe -t regexp
remove exceptionpath	-e <file_path>-t file	指定したファイルをアプリケーション制御の除外パスリストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove exceptionpath -e c:¥sample.bat -t file 注意 対応する add コマンドで最初に指定した、正確な<file_path>を指定してください。
	-e <folder_path>-t folder	指定したフォルダをアプリケーション制御の除外パスリストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove exceptionpath -e c:¥folder -t folder 注意 対応する add コマンドで最初に指定した、正確な <folder_path> を指定してください。
	-e <folder_path>-t folderandsub	指定したフォルダおよびサブフォルダをアプリケーション制御の除外パスリストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove exceptionpath -e c:¥folder -t folderandsub

コマンド	パラメータ	説明
		注意 対応する add コマンドで最初に指定した、正確な <folder_path> を指定してください。
	-e <regular_expression>-t regexp	正規表現を使用して除外を削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove exceptionpath -e c:¥¥test¥¥.* -t regexp 注意 対応する add コマンドで最初に指定した、正確な <regular_expression> を指定してください。
test exceptionpath	<regular_expression> <string> -t regexp	正規表現が文字列に一致するかどうか確認してください たとえば、次のように入力します。 SLCmd.exe -p <admin_password> test exceptionpath C:¥¥test¥¥.*C:¥test¥sample.exe -t regexp

書き込み制御コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、書き込み制御リストと書き込み制御の除外リストを設定します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-16. 省略表記と用法

パラメータ	省略表記	用法
writeprotection	wp	書き込み制御機能を管理します
writeprotection-file	wpfi	書き込み制御リストのファイルを管理します
writeprotection-folder	wpfo	書き込み制御リストのフォルダを管理します
writeprotection-regvalue	wprv	書き込み制御リストのレジストリ値と、関連するレジストリキーを管理します
writeprotection-regkey	wprk	書き込み制御リストのレジストリキーを管理します
writeprotection-file-exception	wpfie	書き込み制御の除外リストのファイルを管理します
writeprotection-folder-exception	wpfoe	書き込み制御の除外リストのフォルダを管理します
writeprotection-regvalue-exception	wprve	書き込み制御の除外リストのレジストリ値と、関連するレジストリキーを管理します
writeprotection-regkey-exception	wprke	書き込み制御の除外リストのレジストリキーを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-17. 書き込み制御リストの「File」コマンド

コマンド	パラメータ	値	説明
show	writeprotection		書き込み制御リストを表示します
	writeprotection-file		ファイルに関連する書き込み制御リストを表示します たとえば、次のように入力します。

コマンド	パラメータ	値	説明
			SLCmd.exe -p <admin_password> show writeprotection-file
	writeprotection-file-exception		ファイルに関連する書き込み制御除外リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show writeprotection-file-exception
	writeprotection-folder		フォルダに関連する書き込み制御リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show writeprotection-folder
	writeprotection-folder-exception		フォルダに関連する書き込み制御除外リストを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show writeprotection-folder-exception
add	writeprotection-file	<file_path>	指定したファイルを書き込み制御リストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add

コマンド	パラメータ	値	説明
			`writeprotection-file archive.txt` **注意** パスの最後から前方に向かって <file_path> 値のパターンマッチングが行われます。たとえば、`userfile.txt` を指定すると、`c:¥Windows¥userfile.txt` および `c:¥Temp¥userfile.txt` に一致します。
	`writeprotection-file-exception`	`-t` <file_path> `-p` <process_path>	指定したファイルに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt -p notepad.exe`

コマンド	パラメータ	値	説明
			 注意 パスの最後から前方に向かって`-p -t` 値のパターンマッチングが行われます。たとえば、`userfile.txt` を指定すると、`c:¥Windows¥userfile.txt` および `c:¥Temp¥userfile.txt` に一致します。
		`-t` <file_path>	指定したファイルに対する書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> add writeprotection-file-exception -t userfile.txt`  注意 パスの最後から前方に向かって`-t` 値のパターンマッチングが行われます。たとえば、`userfile.txt` を指定すると、`c:¥Windows¥userfile.txt` および `c:¥Temp¥userfile.txt` に一致します。

コマンド	パラメータ	値	説明
		-p <process_path>	指定したプロセスからのファイルへの書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-file-exception -p notepad.exe **注意** プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。たとえば、notepad.exe を指定すると、c:¥Windows¥notepad.exe および c:¥Temp¥notepad.exe に一致します。
	writeprotection-folder	[-r] <folder_path>	指定したフォルダを書き込み制御リストに追加します -r オプションでサブフォルダも追加できます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-folder -r c:\Windows\

コマンド	パラメータ	値	説明
			 注意 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 パスの最後から前方に向かって <folder_path> 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:¥Windows¥userfolder および c:¥Temp¥userfolder に一致します。
	writeprotection-folder-exception	[-r] -t <folder_path> -p <process_path>	指定したフォルダに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します -r: オプションでサブフォルダを含みます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -t c:\Windows\System32\Temp\ -p c:\Windows\notepad.exe

コマンド	パラメータ	値	説明
			注意 必要に応じて`-r` 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 パスの最後から前方に向かって`-p -t` 値のパターンマッチングが行われます。たとえば、`userfile.txt` を指定すると、`c:¥Windows¥userfile.txt` および `c:¥Temp¥userfile.txt` に一致します。
		[`-r`] `-t` <folder_path>	指定したフォルダに対する書き込みを許可するルールを書き込み制御除外リストに追加します `-r`: オプションでサブフォルダを含みます たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -t c:\Users\`

コマンド	パラメータ	値	説明
			注意 必要に応じて`-r` 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 フォルダパスの最後の部分から前方に向かって`-t` 値のパターンマッチングが行われます。たとえば、`userfolder` を指定すると、`c:¥Windows¥userfolder` および `c:¥Temp¥userfolder` に一致します。
		`-p <process_path>`	指定したプロセスからのフォルダへの書き込みを許可するルールを書き込み制御除外リストに追加します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> add writeprotection-folder-exception -r -p c:\Windows\System32\`

コマンド	パラメータ	値	説明
			注意 プロセスパスの最後からパスの前方に向かって`-p` 値のパターンマッチングが行われます。たとえば、`notepad.exe` と指定すると、`c:¥Windows¥notepad.exe` と `c:¥Temp¥notepad.exe` に一致します。
`remove`	`writeprotection-file`	<file_path>	指定したファイルを書き込み制御リストから削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove writeprotection-file archive.txt` 注意 対応する add コマンドで最初に指定した、正確な <file_path> を指定してください。
	`writeprotection-file-exception`	`-t` <file_path> `-p` <process_path>	指定したファイルに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。

コマンド	パラメータ	値	説明
			SLCmd.exe -p <admin_password> remove writeprotection-file-exception -t userfile.txt -p notepad.exe **注意** 対応する add コマンドで最初に指定した、正確な <file_path> および <process_path> を指定してください。
		-t <file_path>	指定したファイルに対する書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove writeprotection-file-exception -t userfile.txt

コマンド	パラメータ	値	説明
			 注意 パスの最後から前方に向かって`-t` 値のパターンマッチングが行われます。たとえば、`userfile.txt` を指定すると、`c:¥Windows¥userfile.txt` および `c:¥Temp¥userfile.txt` に一致します。
		`-p <process_path>`	指定したプロセスからのファイルへの書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove writeprotection-file-exception -p notepad.exe`  注意 プロセスパスの最後からパスの前方に向かって`-p` 値のパターンマッチングが行われます。たとえば、`notepad.exe` と指定すると、`c:¥Windows¥notepad.exe` と `c:¥Temp¥notepad.exe` に一致します。

コマンド	パラメータ	値	説明
	writeprotection-folder	[-r] <folder_path>	指定したフォルダを書き込み制御リストから削除します -r: オプションでサブフォルダを含みます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove writeprotection-folder -r c:\Windows\ **注意** 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 対応する add コマンドで最初に指定した、正確な <folder_path> および-r 値を指定してください。
	writeprotection-folder-exception	[-r] -t <folder_path> -p <process_path>	指定したフォルダに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します -r: オプションでサブフォルダを含みます たとえば、次のように入力します。 SLCmd.exe -p <admin_password> add

コマンド	パラメータ	値	説明
			`writeprotection-folder-exception -r -t c:\Windows\System32\Temp\ -p c:\Windows\notepad.exe` **注意** 必要に応じて`-r`値を使用して、指定したフォルダと関連するサブフォルダを含めます。 対応する add コマンドで最初に指定した、正確な <folder_path>、<process_path>、および`-r`値を指定してください。
		[`-r`] `-t` <folder_path>	指定したフォルダに対する書き込みを許可するルールを書き込み制御除外リストから削除します -r: オプションでサブフォルダを含みます たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -r -t c:\Users\`

コマンド	パラメータ	値	説明
			注意 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 フォルダパスの最後の部分から前方に向かって-t 値のパターンマッチングが行われます。たとえば、userfolder を指定すると、c:¥Windows¥userfolder および c:¥Temp¥userfolder に一致します。
		-p <process_path>	指定したプロセスからのフォルダへの書き込みを許可するルールを書き込み制御除外リストから削除します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> remove writeprotection-folder-exception -p c:\Windows\System32\

コマンド	パラメータ	値	説明
			注意 プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。たとえば、notepad.exe を指定すると、c:¥Windows¥notepad.exe および c:¥Temp¥notepad.exe に一致します。

表 6-18. 書き込み制御リストの「Registry」コマンド

コマンド	パラメータ	値	説明
show	writeprotection		書き込み制御リストを表示します
	writeprotection-regvalue		レジストリ値に関連する書き込み制御リストを表示します
	writeprotection-regvalue-exception		レジストリ値に関連する書き込み制御除外リストを表示します
	writeprotection-regkey		レジストリキーに関連する書き込み制御リストを表示します
	writeprotection-regkey-exception		レジストリキーに関連する書き込み制御除外リストを表示します
add	writeprotection-regvalue	<path_of_registry_key> <registry_value>	指定したレジストリ値を書き込み制御リストに追加します レジストリキーの指定が必要です たとえば、「HKEY\test\」レジストリキーのレジストリ値「testvalue」を書き込み制御リス

コマンド	パラメータ	値	説明
			トに追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> add writeprotection-regvalue HKEY\test testvalue`
	`writeprotection-regvalue-exception`	`-t` <path_of_registry_key> <registry_value> `-p` <process_path>	指定したレジストリ値に対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します レジストリキーの指定が必要です **注意** このコマンドにより、指定したプロセスによる指定したレジストリ値への書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって`-p`値のパターンマッチングが行われます。
		`-t` <path_of_registry_key> <registry_value>	指定したレジストリ値に対する書き込みを許可するルールを書き込み制御除外リストに追加します レジストリキーの指定が必要です

コマンド	パラメータ	値	説明
			注意 このコマンドにより、任意のプロセスによる指定したレジストリ値への書き込みアクセスが可能になります。
		-p <process_path>	指定したプロセスからのレジストリ値への書き込みを許可するルールを書き込み制御除外リストに追加します **注意** このコマンドにより、指定したプロセスによる任意のレジストリ値への書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。
	writeprotection-regkey	[-r] <path_of_registry_key>	指定したレジストリキーを書き込み制御リストに追加します -r: オプションでサブキーを含みます **注意** 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。
	writeprotection-regkey-exception	[-r] -t <path_of_registry_key> -p	指定したレジストリキーに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストに追加します

コマンド	パラメータ	値	説明
		<process_path>	-r: オプションでサブキーを含みます  注意 このコマンドにより、指定したプロセスによる指定したレジストリキーへの書き込みアクセスが可能になります。 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。
		[-r] -t <path_of_registry_key>	指定したレジストリキーに対する書き込みを許可するルールを書き込み制御除外リストに追加します -r: オプションでサブキーを含みます  注意 このコマンドにより、任意のプロセスによる指定したレジストリキーへの書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。

コマンド	パラメータ	値	説明
		-p <process_path>	指定したプロセスからのレジストリキーへの書き込みを許可するルールを書き込み制御除外リストに追加します **注意** このコマンドにより、指定したプロセスによる任意のレジストリキーへの書き込みアクセスが可能になります。 プロセスパスの最後から前方に向かって-p 値のパターンマッチングが行われます。
remove	writeprotection-regvalue	<path_of_registry_key> <registry_value>	指定したレジストリ値を書き込み制御リストから削除します レジストリキーの指定が必要です **注意** 対応する add コマンドで最初に指定した、正確な <path_of_registry_key> および <registry_value> を指定してください。
	writeprotection-regvalue-exception	-t <path_of_registry_key> <registry_value> -p <process_path>	指定したレジストリ値に対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します レジストリキーの指定が必要です

コマンド	パラメータ	値	説明
			注意 対応する add コマンドで最初に指定した、正確な <path_of_registry_key>、<registry_value>、および <process_path> を指定してください。 パスの最後から前方に向かって `-p` 値のパターンマッチングが行われます。
		`-t` <path_of_registry_key> <registry_value>	指定したレジストリ値に対する書き込みを許可するルールを書き込み制御除外リストから削除します レジストリキーの指定が必要です
		`-p` <process_path>	指定したプロセスからのレジストリ値への書き込みを許可するルールを書き込み制御除外リストから削除します **注意** パスの最後から前方に向かって `-p` 値のパターンマッチングが行われます。
	`writeprotection-regkey`	[`-r`] <path_of_registry_key>	指定したレジストリキーに対する指定したプロセスからの書き込みを許可するルールを書き込み制御除外リストから削除します `-r`: オプションでサブキーを含みます

コマンド	パラメータ	値	説明
			注意 対応する add コマンドで最初に指定した、正確な <path_of_registry_key> および-r 値を指定してください。 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。
	writeprotection-regkey-exception	[-r] -t <path_of_registry_key> -p <process_path>	指定したレジストリキーに対する書き込みを許可するルールを書き込み制御除外リストから削除します -r: オプションでサブキーを含みます **注意** 対応する add コマンドで最初に指定した、正確な <path_of_registry_key>、<process_path>、および-r 値を指定してください。 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。 パスの最後から前方に向かって-p 値のパターンマッチングが行われます。
		[-r] -t <path_of_registry_key>	指定したレジストリキーに対する書き込みを許可するルールを書き込み制御除外リストから削除します

コマンド	パラメータ	値	説明
			-r: オプションでサブキーを含みます 注意 必要に応じて-r 値を使用して、指定したフォルダと関連するサブフォルダを含めます。
		-p <process_path>	指定したプロセスからのレジストリキーへの書き込みを許可するルールを書き込み制御除外リストから削除します 注意 パスの最後から前方に向かって-p 値のパターンマッチングが行われます。

信頼するデジタル証明書コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、信頼するデジタル証明書を設定します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-19. 省略表記と用法

パラメータ	省略表記	用法
trustedcertification	tc	信頼するデジタル証明書の管理

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-20. 信頼するデジタル証明書コマンド

コマンド	パラメータ	説明
`set trustedcertification`		信頼するデジタル証明書の設定を表示します **注意** 初期設定は `Enabled` です。
	`enable`	信頼するデジタル証明書の設定を有効にします
	`disable`	信頼するデジタル証明書の設定を無効にします
`show trustedcertification`	[`-v`]	信頼するデジタル証明書のリストを表示します `-v`: オプションで詳細情報を表示します
`add trustedcertification`	`-c` <file_path> [`-l` <label>] [`-u`]	指定したファイルを信頼するデジタル証明書リストに追加します `-l`: オプションで一意のラベルを指定できます. `-u`: オプションで指定したデジタル証明書ファイルで署名されたファイルを許可リストの自動更新監視対象にします
`remove trustedcertification`	`-l` <label>	信頼するデジタル証明書リストから指定されたラベルのルールを削除します

信頼するハッシュリストのコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、信頼するハッシュ値を設定します。

`SLCmd.exe -p` <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-21. 省略表記と用法

パラメータ	省略表記	用法
trustedhash	th	Safe Lock 管理者が追加した信頼するハッシュ値 (ファイル) を管理します。

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-22. 信頼するハッシュリストのコマンド

コマンド	パラメータ	説明
set trustedhash		信頼するハッシュリストの設定を表示します 注意 初期設定は Disabled です。
	enable	信頼するハッシュリストの使用を有効にします
	disable	信頼するハッシュリストの使用を無効にします
show trustedhash		信頼するハッシュリストのハッシュ値を表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> show trustedhash
add trustedhash	-v <hash> [-l <label>] [-u][-al] [-t<file_path>][-n<note>]	指定したハッシュ値を信頼するハッシュリストに追加します ハッシュ値 xxx を含む信頼するファイルを信頼するハッシュリストに追加するには、次のように入力します。 SLCmd.exe -p <admin_password> add trustedhash -v xxx -l: オプションでこのハッシュに対する一意のラベルを指定できます

コマンド	パラメータ	説明
		-u: オプションでこのハッシュに一致するファイルを許可リストの自動更新の監視対象にできます **注意** -u オプションを使用する場合は、事前指定による許可リスト自動更新が有効である必要があります。 -al: オプションでファイルへの最初のアクセス時、このハッシュ値に一致するファイルを 許可リストに追加できます -t: オプションでハッシュの確認対象となるファイルのパスを指定できます **注意** パスの最後から前方に向かって-t 値のパターンマッチングが行われます。たとえば、userfile.txt を指定すると、c:¥Windows¥userfile.txt および c:¥Temp¥userfile.txt に一致します。 -n: オプションでメモを指定できます
remove trustedhash	-l <label>	指定したラベルのファイルを信頼するハッシュリストから削除します
remove trustedhash	-a	信頼するハッシュリストのハッシュ値をすべて削除します

許可リスト自動更新コマンド

エージェントの許可リストに指定されていないインストーラやファイルを実行するには、次の形式でコマンドを入力して許可リスト自動更新を設定します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-23. 省略表記と用法

パラメータ	省略表記	用法
trustedupdater	tu	事前指定による許可リスト自動更新のツールプロセスを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-24. 許可リスト自動更新コマンド

コマンド	パラメータ	説明
start trustedupdater	[-r] <path_of_installer>	許可リスト自動更新を開始して、指定するフォルダ内のインストールパッケージ (EXE および MSI ファイル形式) を許可リストに追加します。 **注意** -r: オプションでサブフォルダを含みます たとえば、C:¥Installers フォルダとそのサブフォルダのすべてのインストールパッケージを含めるには、次のように入力します。 SLCmd.exe -p <admin_password> start trustedupdater -r C:\Installers
stop trustedupdater	[-f]	許可リスト自動更新を無効にして、許可リストへの新規または更新済みファイルの追加を停止します。 **注意** -f: オプションで新規/更新ファイルを自動で許可リストに追加します たとえば、許可リスト自動更新を停止し、プロンプトが表示された後、指定したすべてのインストーラ (停止コマンドを受信する前に指定したも

コマンド	パラメータ	説明
		の) を許可リストに追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> stop trustedupdater -f`

事前指定による許可リスト自動更新コマンド

重要

事前指定による許可リスト自動更新にファイルを追加するための `add` コマンドは、事前指定による許可リスト自動更新のコマンド一覧に指定された汎用コマンドとは別の形式に準拠します。事前指定による許可リスト自動更新へのファイルの追加の詳細については、172 ページの「事前指定による許可リスト自動更新の「追加」コマンド」を参照してください。

コマンドラインインタフェースに次の形式でコマンドを入力して、事前指定による許可リスト自動更新を設定します。

`SLCmd.exe -p <admin_password> <command> <parameter> <value>`

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-25. 省略表記と用法

パラメータ	省略表記	用法
`predefinedtrustedupdater`	`ptu`	事前指定による許可リスト自動更新のファイルを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-26. 事前指定による許可リスト自動更新コマンド

コマンド	パラメータ	説明
`add predefinedtrustedupdater`	`-e <folder_or_file_exception>`	指定したファイル/フォルダを事前指定による許可リスト自動更新の除外リストに追加します

コマンド	パラメータ	説明
		このオプションは -u、-t オプションと同時に指定することはできません 重要 事前指定による許可リスト自動更新にファイルを追加するための add コマンドは、このリストに指定されたその他のコマンドとは別の形式に準拠します。事前指定による許可リスト自動更新の除外リストではなく、事前指定による許可リスト自動更新へのファイルの追加の詳細については、172 ページの「事前指定による許可リスト自動更新の「追加」コマンド」を参照してください。 たとえば、notepad.exe を事前指定による許可リスト自動更新の除外リストに追加するには、次のように入力します。 SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows\notepad.exe
decrypt predefinedtrustedupdater	<path_of_encrypted_file> <path_of_decrypted_output_file>	指定した事前指定による許可リスト自動更新の設定ファイルを指定した場所に復号します たとえば、C:¥Notepad.xen を C:¥Editors¥notepad.xml に復号するには、次のように入力します。 SLCmd.exe -p <admin_password> decrypt predefinedtrustedupdater C:

コマンド	パラメータ	説明
		\Notepad.xen C:\Editors \notepad.xml
encrypt predefinedtrustedupdater	<path_of_file> <path_of_encrypted_output_file>	指定した事前指定による許可リスト自動更新の設定ファイルを指定した場所に暗号化します たとえば、C:¥notepad.xml を C:¥Editors¥Notepad.xen に暗号化するには、次のように入力します。 SLCmd.exe -p <admin_password> encrypt predefinedtrustedupdater C:\Editors\notepad.xml C:\Notepad.xen
export predefinedtrustedupdater	<path_of_encrypted_output>	指定した場所に事前指定による許可リスト自動更新の設定ファイルをエクスポートします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> export predefinedtrustedupdater C:\Lists\ptu_list.xen
import predefinedtrustedupdater	<path_of_encrypted_input>	指定した場所の事前指定による許可リスト自動更新の設定ファイルをインポートします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> import predefinedtrustedupdater C:\Lists\ptu_list.xen
remove predefinedtrustedupdater	-l <label_name>	事前指定による許可リスト自動更新設定から指定されたラベルのルールを削除します たとえば、「Notepad」ルールを削除するには、次のように入力します。

コマンド	パラメータ	説明
		`SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -l Notepad`
	`-e <folder_or_file_exception>`	指定したファイル/フォルダを事前指定による許可リスト自動更新の除外リストから削除します たとえば、`notepad.exe` の除外を削除するには、次のように入力します。 `SLCmd.exe -p <admin_password> remove predefinedtrustedupdater -e C:\Windows\notepad.exe`
`set predefinedtrustedupdater`		事前指定による許可リスト自動更新のステータスを表示します **注意** 初期ステータスは `Disabled` です。
	`Enable`	事前指定による許可リスト自動更新を有効にします
	`disable`	事前指定による許可リスト自動更新を無効にします
`show predefinedtrustedupdater`		事前指定による許可リスト自動更新のルールを表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show predefinedtrustedupdater`
	`-e`	事前指定による許可リスト自動更新の除外リストを表示します たとえば、次のように入力します。

コマンド	パラメータ	説明
		SLCmd.exe -p <admin_password> show predefinedtrustedupdater -e

事前指定による許可リスト自動更新の「追加」コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、事前指定による許可リスト自動更新にプロセス、ファイル、またはフォルダを追加します。

SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u <folder_or_file> -t <type_of_object> [<optional_values>]

次の表は、コマンド、パラメータ、および基本の値の一覧を示しています。

表 6-27. 事前指定による許可リスト自動更新の「Add」コマンド

コマンド	パラメータ	値	説明
add	predefinedtrustedupdater	<folder_or_file>	指定したファイルまたはフォルダを事前指定による許可リスト自動更新に追加します たとえば、notepad.exe を事前指定による許可リスト自動更新の除外リストに追加するには、次のように入力します。 SLCmd.exe -p <admin_password> add predefinedtrustedupdater -e C:\Windows\notepad.exe

コマンドの末尾に次の値を追加します。

表 6-28. 事前指定による許可リスト自動更新の「Add」コマンドの追加値

値	必須/任意	説明		使用例
-u <folder_or_file>	必須	事前指定による許可リスト自動更新リストに追加するファイル/フォルダを指定します 指定したファイル/フォルダの種類を -t オプションで指定する必要があります		該当なし 注意 このパラメータには、-t <type_of_object> の値を使用する必要があります。
-t <type_of_object>	必須	-u オプションで指定したファイルの種類を指定します 以下のオブジェクト名が指定できます:		SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process
		process	EXE などの実行形式ファイル	
		file	MSI や BAT ファイルなどのファイル	
		folder	EXE、MSI や BAT ファイルを含むフォルダ	
		folderandsub	EXE、MSI や BAT ファイルを含むフォルダとサブフォルダ	
-p <parent_process>	任意	親プロセスのファイルパスを指定できます		SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -p C:

値	必須/任意	説明	使用例
			\batch files \note.bat
-l <label_name>	任意	許可リストの自動更新ルールに一意のラベルを指定できます 注意 指定しない場合、任意のラベルが設定されます	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -l EDITOR
-al Enable	任意	-u オプションで指定したファイルが実行されるときまたは指定したフォルダに含まれるファイルが実行されるときに、許可リストのハッシュ値と実行されるファイルの比較を行います 注意 何も指定しない場合はこのオプションが有効になりハッシュのチェックが行われます	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al enable
-al Disable	任意	-u オプションで指定したファイルが実行されるときまたは指定したフォルダに含まれるファイルが実行されるときに、許可リストのハッシュ値と実行されるファイルの比較を行わずに処理を継続させます	SLCmd.exe -p <admin_password> add predefinedtrustedupdater -u C:\Windows\notepad.exe -t process -al disable

Windows Update サポート

コマンドラインインタフェースに次の形式でコマンドを入力して、Windows Update サポートを設定します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-29. 省略表記と用法

パラメータ	省略表記	用法
windowsupdatesupport	wus	アプリケーション制御が有効なエージェントでの Windows Update の実行を許可します。

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-30. Windows Update サポートのコマンド

コマンド	パラメータ	説明
set windowsupdatesupport		Windows Update サポートの現在の設定を表示します 注意 初期設定は Disabled です。
	enable	Windows Update サポートを有効にします
	disable	Windows Update サポートを無効にします

ファイルのブロック通知コマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、ファイルのブロック通知を有効または無効にします。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-31. 省略表記と用法

パラメータ	省略表記	用法
blockedfilenotification	bfn	Safe Lock Intelligent Manager がアプリケーションの実行やエージェントへの変更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。

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-32. ファイルのブロック通知コマンド

コマンド	パラメータ	説明
set blockedfilenotification		現在の通知設定を表示します。 注意 初期設定は Disabled です。
	enable	ポップアップ通知を有効にします。
	disable	ポップアップ通知を無効にします。

設定ファイルコマンド

コマンドラインインタフェースに次のコマンドを入力して、設定ファイルに対して処理を実行します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-33. 省略表記と用法

パラメータ	省略表記	用法
configuration	con	設定ファイルを管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-34. 設定ファイルコマンド

コマンド	パラメータ	説明
`decrypt configuration`	<path_of_encrypted_file> <path_of_decrypted_output_file>	設定ファイルを復号します たとえば、`C:¥config.xen` を `C:¥config.xml` に復号する場合は、次のように入力します。 `SLCmd.exe -p <admin_password> decrypt configuration C:\config.xen C:\config.xml`
`encrypt configuration`	<path_of_file> <path_of_encrypted_output_file>	設定ファイルを暗号化します たとえば、`C:¥config.xml` を `C:¥config.xen` に暗号化する場合は、次のように入力します。 `SLCmd.exe -p <admin_password> encrypt configuration C:\config.xml C:\config.xen`
`export configuration`	<path_of_encrypted_output>	指定したファイルに設定をエクスポートします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> export configuration C:\config.xen`
`import configuration`	<path_of_encrypted_input>	指定したファイルから設定をインポートします たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> import configuration C:\config.xen`

ファイルレス攻撃対策のコマンド

コマンドラインインタフェースに次の形式でコマンドを入力して、ファイルレス攻撃対策機能を設定します。

SLCmd.exe -p <admin_password> <command> <parameter> <value>

次の表は、使用可能なパラメータの省略表記一覧を示しています。

表 6-35. 省略表記と用法

パラメータ	省略表記	用法
filelessattackprevention	flp	ファイルレス攻撃対策を管理します
filelessattackprevention-process	flpp	ファイルレス攻撃対策のプロセスを管理します
filelessattackprevention-exception	flpe	ファイルレス攻撃対策の除外を管理します

次の表は、使用可能なコマンド、パラメータ、および値の一覧を示しています。

表 6-36. ファイルレス攻撃対策のコマンド

コマンド	パラメータ	説明
set filelessattackprevention		ファイルレス攻撃対策の現在のステータスを表示します たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set filelessattackprevention
	enable	ファイルレス攻撃対策を有効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set filelessattackprevention enable
	disable	ファイルレス攻撃対策を無効にします たとえば、次のように入力します。 SLCmd.exe -p <admin_password> set filelessattackprevention disable

コマンド	パラメータ	説明
`show filelessattackprevention-process`		監視対象プロセスのリストを表示します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> show filelessattackprevention-process`
`add filelessattackprevention-exception`	`<monitored_process> <Parentprocess1> <Parentprocess2> <Parentprocess3> <Parentprocess4> -a <arguments> -regex -l <label>`	ファイルレス攻撃対策の除外を追加します 次の除外の場合: • 監視対象プロセス: `cscript.exe` • 親プロセス 1: `a.exe` • 親プロセス 2: • 親プロセス 3: `c.exe` • 親プロセス 4: • 引数: `-abc -def` • 引数のユーザ正規表現: `No` 除外を追加するには、次のように入力します。 `SLCmd.exe -p <admin_password> add flpe cscript.exe a.exe "" c.exe "" -a "-abc -def"`
`remove filelessattackprevention-exception`	`-l <label>`	ファイルレス攻撃対策の除外を削除します たとえば、次のように入力します。 `SLCmd.exe -p <admin_password> remove filelessattackprevention-exception -l <label>`

注意

- 監視対象プロセスが SafeLock の起動前に開始された場合、SafeLock はそのプロセスを検出およびブロックできません。
- Windows Vista x86 システム (Service Pack のインストールなし) では、ファイルレス攻撃対策機能でプロセスチェーンのチェックを実行できますが、コマンドライン引数のチェックを実行することはできません。プロセスチェーンのチェックをパスすると、コマンドライン引数のチェックはスキップされます。

第 7 章

エージェントのリモートでの管理

この章では、Trend Micro Safe Lock エージェントのリモートでの管理について説明します。

この章の内容は次のとおりです。

リモートセットアップツール (SLrst)

リモートセットアップツールを使用して、コマンドラインから Safe Lock エージェントプログラムのサイレントインストール、Patch の適用、およびアンインストールを実行できます。

SLrst.exe は対象コンピュータに対する操作をリモートで実行しますが、対象コンピュータは Safe Lock Intelligent Manager サーバに直接アクセスします。

Safe Lock Intelligent Manager では、初期設定で次の場所に SLrst.exe ファイルが保存されます。

```
C:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager
¥CmdTools¥RemoteAgentSetupTool¥
```

リモートセットアップツールでは、すべてのコマンドラインの機能で次の構文を使用します。

```
SLrst <targets CSV file> <parameter>
```

コマンドプロンプトで「SLrst」と入力して <Enter> キーを押すと、リモートセットアップツールの構文例が表示されます。

重要

SLrst をコマンドラインで使用できるのは、Windows の管理者権限を持つ Safe Lock Intelligent Manager の管理者のみです。

ヒント

必要に応じて、SLrst.exe を含む RemoteAgentSetupTool フォルダ全体を Program Files フォルダから別の場所にコピーしてプログラムを実行します。SLrst.exe が Safe Lock の許可リストに追加されているかアプリケーション制御が無効であり、さらに Safe Lock Intelligent Manager サーバにアクセス可能であれば、SLrst.exe は、.NET Framework 2.0 または 3.5 がインストールされたネットワーク内の任意のコンピュータ上の RemoteAgentSetupTool フォルダ内から実行できるように設計されています。

次の表は、SLrst プログラムで使用できる機能のリストを示しています。

表 7-1. SLrst リモートエージェントセットアップパラメータ

パラメータ	機能
`--install`	Safe Lock エージェントをコンピュータに配信してインストールします。 183 ページの「リモートインストールの考慮事項」を参照してください。
`--patch`	Safe Lock エージェントに Patch を適用します。
`--reboot`	エージェントを再起動します (Safe Lock エージェントを再インストールする場合に必要です)。 詳細については、203 ページの「エージェントをリモートで再起動する」を参照してください。 **注意** `reboot` 機能は、Windows 2000 プラットフォームを実行するシステムでは互換性がありません。Windows 2000 プラットフォームを実行するエージェントで Safe Lock エージェントを再インストールする場合は、エージェントを手動で再起動します。
`--uninstall`	Safe Lock エージェントをエージェントからアンインストールします。 詳細については、202 ページの「エージェントをリモートでアンインストールする」を参照してください。

リモートインストールの考慮事項

Safe Lock エージェントをリモートでインストールする前に、次のことを確認します。

- Safe Lock Intelligent Manager がサーバコンピュータにインストールされている。
- バージョン 1.0 の Safe Lock エージェントが対象コンピュータにインストールされていない。

  24 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。

- ネットワーク、対象コンピュータ、およびサーバコンピュータのファイアウォール設定で次のことが許可されている。
  - Safe Lock Intelligent Manager のポート (初期設定は 8000、8001、および 14336)
  - ファイル共有サービス
  - Windows Management Instrumentation (WMI) サービス
  - Windows プロセス間通信 (IPC) サービス
- 対象コンピュータが次のように設定されている。
  - 簡易ファイル共有サービスが無効化されている。(Windows XP)
  - ファイル共有サービスが有効化されている。
  - ローカルアカウントが初期設定の共有された `admin$`へのアクセス権を持っている。
  - Windows Management Instrumentation (WMI) サービスが有効化されている。
  - Windows プロセス間通信 (IPC) サービスが有効化されている。
- 対象コンピュータで Windows インストーラーのセッションが実行されていない。特に、Windows Update でコンピュータがバックグラウンドでアップデートされていないことを確認する。

リモートインストール用に Windows Server 2003 を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows Server 2003
- Windows Server 2003 R2

手順

1. Windows ファイアウォールを無効にします。

2. [Microsoft ネットワーク用ファイルとプリンタ共有] を有効にします。
   a. [スタート] > [コントロール パネル] > [ネットワーク接続] の順に選択します。
   b. [ローカル エリア接続] を右クリックし、[プロパティ] を選択します。
   c. [Microsoft ネットワーク用ファイルとプリンタ共有] を選択します。

リモートインストール用に Windows Server 2008 を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows Server 2008
- Windows Server 2008 R2

手順

1. Windows ファイアウォールを無効にします。
2. レジストリを編集して、ユーザー アカウント制御を無効にします。
   a. [**レジストリ エディター**] (`regedit.exe`) を開きます。

      たとえば、[スタート] > [実行...] の順に選択し、「`regedit`」と入力して <Enter> キーを押します。
   b. 次のレジストリサブキーを探してクリックします。
      `HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows ¥CurrentVersion¥Policies¥System`
   c. 右側で、次のエントリを探します。
      `LocalAccountTokenFilterPolicy`

      エントリが存在しない場合は、次を実行して作成します。
      i. [編集] > [新規] の順に選択します。
      ii. [DWORD 値] を選択します。

iii. 「LocalAccountTokenFilterPolicy」と入力して <Enter> キーを押します。

d. LocalAccountTokenFilterPolicy を右クリックして、[修正] を選択します。

e. [値のデータ] に「1」と入力します。

f. [OK] をクリックします。

g. [**レジストリ エディター**] を閉じます。

3. エージェントにログオンする各ユーザアカウントのネットワーク探索を有効にします。

a. [スタート] > [コントロール パネル] > [ネットワークと共有センター] の順に選択します。

b. [ローカル エリア接続] を右クリックし、[プロパティ] を選択します。

c. [Microsoft ネットワーク用ファイルとプリンタ共有] を選択します。

リモートインストール用に Windows Server 2012 を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows Server 2012
- Windows Server 2012 R2

手順

1. Windows ファイアウォールを無効にします。
2. レジストリを編集して、ユーザー アカウント制御を無効にします。

a. [**レジストリ エディター**] (regedit.exe) を開きます。

たとえば、[スタート] > [実行...] の順に選択し、「regedit」と入力して <Enter> キーを押します。

b. 次のレジストリサブキーを探してクリックします。
`HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows ¥CurrentVersion¥Policies¥System`

c. 右側で、次のエントリを探します。
`LocalAccountTokenFilterPolicy`

エントリが存在しない場合は、次を実行して作成します。

i. [編集] > [新規] の順に選択します。

ii. [DWORD 値] を選択します。

iii. 「`LocalAccountTokenFilterPolicy`」と入力して <Enter> キーを押します。

d. `LocalAccountTokenFilterPolicy` を右クリックして、[修正] を選択します。

e. [値のデータ] に「`1`」と入力します。

f. [OK] をクリックします。

g. ［**レジストリ エディター**］を閉じます。

3. エージェントにログオンする各ユーザアカウントのネットワーク探索を有効にします。

a. [スタート] > [コントロール パネル] > [すべてのコントロール パネル項目] > [ネットワークと共有センター] の順に選択します。

b. 左のパネルで、[共有の詳細設定の変更] をクリックし、[ドメイン (現在のプロファイル)] ドロップダウンリストをクリックします。

c. [ネットワーク探索を有効にする] を選択します。

リモートインストール用に Windows Server 2016 を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows Server 2016 Standard (64 ビット)

- Windows Storage Server 2016

手順

1. Windows ファイアウォールを無効にします。
2. レジストリを編集して、ユーザー アカウント制御を無効にします。
   a. [**レジストリ エディター**] (`regedit.exe`) を開きます。

      たとえば、[スタート] > [実行...] の順に選択し、「`regedit`」と入力して <Enter> キーを押します。

   b. 次のレジストリサブキーを探してクリックします。
      `HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows ¥CurrentVersion¥Policies¥System`

   c. 右側で、次のエントリを探します。
      `LocalAccountTokenFilterPolicy`

      エントリが存在しない場合は、次を実行して作成します。

      i. [編集] > [新規] の順に選択します。

      ii. [DWORD 値] を選択します。

      iii. 「`LocalAccountTokenFilterPolicy`」と入力して <Enter> キーを押します。

   d. `LocalAccountTokenFilterPolicy` を右クリックして、[修正] を選択します。

   e. [値のデータ] に「`1`」と入力します。

   f. [OK] をクリックします。

   g. [**レジストリ エディター**] を閉じます。
3. エージェントにログオンする各ユーザアカウントのネットワーク探索を有効にします。
   a. [スタート] > [コントロール パネル] > [すべてのコントロール パネル項目] > [ネットワークと共有センター] > [共有の詳細設定] の順に選択します。

b. [ネットワーク探索を有効にする] と [ネットワークに接続されているデバイスの自動セットアップを有効にする] をオンにします。

リモートインストール用に Windows XP を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows XP

手順

1. Windows ファイアウォールを無効にします。
2. [Microsoft ネットワーク用ファイルとプリンタ共有] を有効にします。
   a. [スタート] > [コントロール パネル] > [ネットワーク接続] の順に選択します。
   b. [ローカル エリア接続] を右クリックし、[プロパティ] を選択します。
   c. [Microsoft ネットワーク用ファイルとプリンタ共有] を選択します。
3. 簡易ファイルの共有を無効にします。

リモートインストール用に Windows 7 を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows 7

手順

1. Windows ファイアウォールを無効にします。
2. レジストリを編集して、ユーザー アカウント制御を無効にします。

a. [**レジストリ エディター**] (regedit.exe) を開きます。

たとえば、[スタート] > [実行...] の順に選択し、「regedit」と入力して <Enter> キーを押します。

b. 次のレジストリサブキーを探してクリックします。
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows ¥CurrentVersion¥Policies¥System

c. 右側で、次のエントリを探します。
LocalAccountTokenFilterPolicy

エントリが存在しない場合は、次を実行して作成します。

i. [編集] > [新規] の順に選択します。

ii. [DWORD 値] を選択します。

iii. 「LocalAccountTokenFilterPolicy」と入力して <Enter> キーを押します。

d. LocalAccountTokenFilterPolicy を右クリックして、[修正] を選択します。

e. [値のデータ] に「1」と入力します。

f. [OK] をクリックします。

g. [**レジストリ エディター**] を閉じます。

3. エージェントにログオンする各ユーザアカウントのネットワーク探索を有効にします。

リモートインストール用に Windows 8 を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows 8
- Windows 8.1

手順

1. Windows ファイアウォールを無効にします。
2. レジストリを編集して、ユーザー アカウント制御を無効にします。
   a. [**レジストリ エディター**] (regedit.exe) を開きます。

      たとえば、[スタート] > [実行...] の順に選択し、「regedit」と入力して <Enter> キーを押します。

   b. 次のレジストリサブキーを探してクリックします。
      HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows ¥CurrentVersion¥Policies¥System

   c. 右側で、次のエントリを探します。
      LocalAccountTokenFilterPolicy

      エントリが存在しない場合は、次を実行して作成します。

      i. [編集] > [新規] の順に選択します。

      ii. [DWORD 値] を選択します。

      iii. 「LocalAccountTokenFilterPolicy」と入力して <Enter> キーを押します。

   d. LocalAccountTokenFilterPolicy を右クリックして、[修正] を選択します。

   e. [値のデータ] に「1」と入力します。

   f. [OK] をクリックします。

   g. [**レジストリ エディター**] を閉じます。
3. エージェントにログオンする各ユーザアカウントのネットワーク探索を有効にします。
   a. [スタート] > [コントロール パネル] > [ネットワークと共有センター] の順に選択します。

   b. [ローカル エリア接続] を右クリックし、[プロパティ] を選択します。

c. [Microsoft ネットワーク用ファイルとプリンタ共有] を選択します。

リモートインストール用に Windows 10 を準備する

Safe Lock Intelligent Manager のセットアップを実行する前に、この手順を実行して、次の Windows バージョンのコンポーネントを準備します。

- Windows 10 Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Professional
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 October 2018 Update (Redstone 5)

手順

1. Windows ファイアウォールを無効にします。
2. レジストリを編集して、ユーザー アカウント制御を無効にします。

   a. [**レジストリ エディター**] (`regedit.exe`) を開きます。

      たとえば、[スタート] > [実行...] の順に選択し、「`regedit`」と入力して <Enter> キーを押します。

   b. 次のレジストリサブキーを探してクリックします。
      `HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows ¥CurrentVersion¥Policies¥System`

   c. 右側で、次のエントリを探します。
      `LocalAccountTokenFilterPolicy`

      エントリが存在しない場合は、次を実行して作成します。

i. [編集] > [新規] の順に選択します。

ii. [DWORD 値] を選択します。

iii. 「LocalAccountTokenFilterPolicy」と入力して <Enter> キーを押します。

d. LocalAccountTokenFilterPolicy を右クリックして、[修正] を選択します。

e. [値のデータ] に「1」と入力します。

f. [OK] をクリックします。

g. [**レジストリ エディター**] を閉じます。

3. エージェントにログオンする各ユーザアカウントのネットワーク探索を有効にします。

a. [スタート] > [コントロール パネル] > [すべてのコントロール パネル項目] > [ネットワークと共有センター] > [共有の詳細設定] の順に選択します。

b. [ネットワーク探索を有効にする] と [ネットワークに接続されているデバイスの自動セットアップを有効にする] をオンにします。

対象とするコンピュータの定義ファイルの準備

リモートセットアップツールでは、コマンドを処理する際、次の 2 つのファイルを使用します。

- endpoint_info.csv: 対象とするコンピュータの接続情報を保存します。
- targets.csv: 展開する特定のコンピュータを対象として指定します。

重要

「Program Files」フォルダの endpoint_info.csv ファイルまたは targets.csv ファイルを編集するには、ファイルの書き込み権限を持つパスにファイルをコピーして編集し、次の推奨パスにコピーします。

手順

1. エージェント情報ファイルを用意して、endpoint_info.csv のファイル名で次のパスに保存します。初期設定では次のパスになります。

   ```
   C:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager
   ¥CmdTools¥RemoteAgentSetupTool¥
   ```

   195 ページの「エージェント情報ファイルの仕様」を参照してください。

2. 対象ファイル (targets.csv)またはファイルのバッチを作成し、次のパスに保存します。

   ```
   C:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager
   ¥CmdTools¥RemoteAgentSetupTool¥
   ```

   194 ページの「対象ファイルの仕様」を参照してください。

対象ファイルの仕様

リモートエージェントインストールの際に使用される対象ファイル (targets.csv)には、対象コンピュータの IP アドレスが含まれています。対象ファイルは CSV 形式で、初期設定のファイル名は targets.csv です。

ヒント

SLrst コマンドラインプログラムを使用したリモートエージェントセットアップは、複数の対象ファイルと同じエージェント情報ファイルを使用することで一括で実行できます。エージェント情報ファイルには、対象ファイルに記載された対象コンピュータの範囲外のコンピュータの情報を含めることができます。

対象ファイル (targets.csv)をカスタマイズして作成するには、各対象コンピュータの IP アドレスを指定します。1 行に 1 つのレコードを記述します。スペース、引用符、その他の区切り文字はサポートされていません。

例:

有効
Targeted IP 10.1.199.199 10.1.199.201 192.168.1.20

無効
10.1.199.199,10.1.199.201
"10.1.199.199" "10.1.199.201" "192.168.1.20"

ヒント

対象ファイルは再使用できます。同じ対象ファイルを使用して、対象エージェントに一括で配信、Patch 適用、およびアンインストールを実行できます。SLrst プログラムを実行するたびに、ログ情報を確認し、重要な情報をバックアップしてください。SLrst は、実行のたびにファイル内のログ情報を自動で上書きします。

エージェント情報ファイルの仕様

リモートエージェントインストールで使用されるエージェント情報ファイル(endpoint_info.csv)には、IP アドレス、ユーザ名、および初期設定の共有 admin $にアクセス可能な各対象コンピュータのローカルアカウントのパスワードが含まれます。

ヒント

トレンドマイクロでは、各対象コンピュータのローカル管理者アカウントを使用することをお勧めします。

エージェント情報ファイルは CSV 形式を使用します。ファイル名は endpoint_info.csv です。

注意

エージェント情報ファイルを CSV 形式で作成するには、レコードを IP アドレス、ユーザ名、およびパスワードのフィールドに分割します。1 行に 1 つのレコードを記述します。各フィールドはカンマで分割します。スペース、引用符、その他の区切り文字はサポートされていません。

例:

有効

```
IP,Username,Password
10.1.199.199,Administrator,password1
10.1.199.200,Administrator,password2
10.1.199.201,Administrator,password3
192.168.1.20,Daniel,his_pwd
192.168.1.21,Sophia,her_pwd
```

無効

```
10.1.199.201,Administrator,password3,192.168.1.20,Daniel,his_pwd
```

```
"10.1.199.199","Administrator","password1"
"10.1.199.200""Administrator","password2"
"10.1.199.201","Administrator","password3"
"192.168.1.20","Daniel","his_pwd"
"192.168.1.21","Sophia","her_pwd"
```

Microsoft Excel では、有効な形式を使用して CSV を表で保存します。

最新のエージェントインストーラパッケージをダウンロードする

手順

1. 管理サーバ画面の上部にあるナビゲーションで[管理] > [コンポーネント] > [アップデート] の順に選択します。

   [コンポーネントアップデート] 画面が表示されます。

2. [エージェントインストーラパッケージのダウンロード] をクリックします。

3. インストールパッケージの言語を選択します。

   最新のエージェントインストーラパッケージがブラウザによりダウンロードされます。

   注意

   エージェントインストーラパッケージは、[コンポーネントアップデート] 画面に表示されるコンポーネントのバージョンに基づいて、Safe Lock Intelligent Manager によって最新と判断されます。キャッシュされたエージェントインストーラパッケージが最新でない場合、Safe Lock Intelligent Manager では、ダウンロードを開始する前に最新のパッケージを準備してキャッシュします。

   最新のエージェントインストーラパッケージを準備する際は、システムに高い負荷がかかります。Safe Lock Intelligent Manager を実行するハードウェアによっては、最新のエージェントインストーラパッケージの準備に時間がかかる場合があります。

4. コマンドラインで `SLrst` プログラムを使用してリモートインストールを行うために、ダウンロードしたエージェントインストーラパッケージを使用するときは、ダウンロードしたエージェントインストーラパッケージを `SLrst` で使用するパスにコピーします。

   たとえば、Safe Lock Intelligent Manager を C ドライブの初期設定のパスにインストールした場合は、ダウンロードしたエージェントインストーラパッケージを `c:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager¥CmdToolsRemoteAgentSetupTool¥package` にコピーします。

重要

ダウンロードしたファイルはパッケージファイル (.zip) に手動で圧縮する必要があります。

パッケージのファイル名は、TMSL2.0_<language_abbreviation>.zip の形式にする必要があります。

例:

有効	無効
TMSL2.0_EN.zip	TMSL2.0_EN (1).zip
TMSL2.0_JA.zip	TMSL2.0_EN_1.zip

エージェントをリモートでインストールする

重要

- リモートセットアップツールを使用して Safe Lock エージェントをリモートで管理する前に、エージェント情報ファイル (endpoint_info.csv) と対象ファイル (targets.csv)を用意します。

  193 ページの「対象とするコンピュータの定義ファイルの準備」を参照してください。

- Safe Lock エージェントをリモートでインストールする前に、最新のエージェントインストーラパッケージをダウンロードします。

  75 ページの「最新のエージェントインストーラパッケージをダウンロードする」を参照してください。

コマンドラインで SLrst.exe プログラムを使用して、ネットワークに接続された 1 つ以上の Safe Lock エージェントをインストールできます。

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。

2. cd コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「RemoteAgentSetupTool」フォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   ```
   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
   \RemoteAgentSetupTool\"
   ```

3. 初期設定の対象ファイル targets.csv を使用してエージェントをリモートでインストールするには、コマンドプロンプトで次のように入力します。

   ```
   SLrst.exe targets.csv --install
   ```

   リモートセットアップツールでは、targets.csv ファイル内でインストール先を検索します。大規模な本稼働環境では、エージェントをバッチ処理でインストールすることをお勧めします。リモートセットアップツールは、CSV ファイルに記述されているそれぞれの対象コンピュータに対して個別に処理します。

4. Safe Lock エージェントプログラムへのアクセスに使用するパスワードを入力し、パスワードを確認のため再度入力します。

5. インストール先の言語を選択します。

6. Safe Lock エージェントをインストールする前に、対象コンピュータで不正プログラムの事前検索を実行するかどうかを選択します。

7. 対象コンピュータで原因分析機能を有効化するかどうかを選択します。

8. リモートインストールプロセスの進捗状況を確認します。Safe Lock では、コマンドライン引数で指定された CSV ファイル (初期設定では targets.csv) にログ情報を直接書き込みます。

Setup.ini ファイルを使用してエージェントのリモートインストールをカスタマイズする

手順

1. Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「package」フォルダに移動します。

たとえば、次のように入力すると初期設定の場所に移動します。

"C:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentSetupTool\package"

2. `TMSL2.0_JA` ファイルを解凍します。

3. `Setup.ini` ファイルを開き、必要に応じてインストールパラメータを変更します。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、233 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。

4. `TMSL2.0_JA` として ZIP ファイルに圧縮して、手順 1 のインストールパスに保存します。

5. エージェントをリモートでインストールします。詳細については、198 ページの「エージェントをリモートでインストールする」を参照してください。

エージェントにリモートで Patch と HotFix を適用する

重要

- リモートセットアップツールを使用して Safe Lock エージェントをリモートで管理する前に、エージェント情報ファイル (endpoint_info.csv) と対象ファイル (targets.csv)を用意します。

  193 ページの「対象とするコンピュータの定義ファイルの準備」を参照してください。

- Safe Lock エージェントをリモートでアップデートする前に、テクニカルサポートダウンロードセンターの Web サイトからエージェントの最新の Patch または HotFix をダウンロードします。 http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

コマンドラインで `SLrst.exe` プログラムを使用して、ネットワークに接続された 1 つ以上の Safe Lock エージェントをインストールできます。

手順

1. ダウンロードしたエージェントの Patch または HotFix を SLrst で使用するパスにコピーします。

   たとえば、Safe Lock Intelligent Manager を C ドライブの初期設定のパスにインストールした場合は、ダウンロードしたエージェントインストーラ Patch または HotFix を c:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager¥CmdTools¥RemoteAgentSetupTool¥package¥にコピーします。

   重要

   Patch または HotFix のファイル名の形式は TMSL2.0_Hotfix_<language_abbreviation>.zip である必要があります。

   例:

有効	無効
TMSL2.0_Hotfix_EN.zip	TMSL2.0_Hotfix_EN (1).zip
TMSL2.0_Hotfix_JA.zip	TMSL2.0_Hotfix_EN_1.zip

2. cd コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「Safe Lock Remote Setup Tool」フォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   ```
   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
   \RemoteAgentSetupTool\"
   ```

3. 初期設定の対象ファイル targets.csv を使用してエージェントにリモートで Patch または HotFix を適用するには、コマンドプロンプトで次のように入力します。

   ```
   SLrst.exe targets.csv --patch
   ```

   リモートセットアップツールでは、targets.csv ファイル内でインストール先を検索します。大規模な本稼働環境では、エージェントにバッチ処理で Patch または HotFix を適用することをお勧めします。リモート

セットアップツールは、CSV ファイルに記述されているそれぞれの対象コンピュータに対して個別に処理します。

4. プロンプトで、Safe Lock エージェントプログラムへのアクセスに使用するパスワードを入力します。

5. リモートでの Patch または HotFix 適用の進捗状況を確認します。Safe Lock では、コマンドライン引数で指定された CSV ファイル (初期設定では `targets.csv`) にログ情報を直接書き込みます。

エージェントをリモートでアンインストールする

重要

リモートセットアップツールを使用して Safe Lock エージェントをリモートで管理する前に、エージェント情報ファイル (endpoint_info.csv) と対象ファイル (targets.csv)を用意します。

193 ページの「対象とするコンピュータの定義ファイルの準備」を参照してください。

コマンドラインで `SLrst.exe` プログラムを使用して、ネットワークに接続された 1 つ以上の Safe Lock エージェントをアンインストールできます。

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。

2. `cd` コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「RemoteAgentSetupTool」フォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   ```
   cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
   \RemoteAgentSetupTool\"
   ```

3. 初期設定の対象ファイル `targets.csv` を使用してエージェントをリモートでインストールするには、コマンドプロンプトで次のように入力します。

```
SLrst.exe targets.csv --uninstall
```

リモートセットアップツールでは、targets.csv ファイル内でインストール先を検索します。大規模な本稼働環境では、エージェントをバッチ処理でアンインストールすることをお勧めします。リモートセットアップツールは、CSV ファイルに記述されているそれぞれの対象コンピュータに対して個別に処理します。

4. Safe Lock エージェントプログラムへのアクセスに使用するパスワードを入力します。
5. リモートアンインストールプロセスの進捗状況を確認します。Safe Lock では、コマンドライン引数で指定された CSV ファイル (初期設定では targets.csv) にログ情報を直接書き込みます。
6. エージェントを再起動して、アンインストールプロセスを完了します。

エージェントをリモートで再起動する

重要

リモートセットアップツールを使用して Safe Lock エージェントをリモートで管理する前に、エージェント情報ファイル (endpoint_info.csv) と対象ファイル (targets.csv)を用意します。

193 ページの「対象とするコンピュータの定義ファイルの準備」を参照してください。

コマンドラインで SLrst.exe プログラムを使用して、ネットワークに接続された 1 つ以上の Safe Lock エージェントを再起動できます。

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。
2. cd コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「RemoteAgentSetupTool」フォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

```
cd /d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
\RemoteAgentSetupTool\"
```

3. 初期設定の対象ファイル `targets.csv` を使用してエージェントをリモートでインストールするには、コマンドプロンプトで次のように入力します。

   ```
   SLrst.exe targets.csv --reboot
   ```

   リモートセットアップツールでは、`targets.csv` ファイル内でインストール先を検索します。大規模な本稼働環境では、エージェントをバッチ処理で再起動することをお勧めします。リモートセットアップツールは、CSV ファイルに記述されているそれぞれの対象コンピュータに対して個別に処理します。

4. リモート再起動プロセスの進捗状況を確認します。Safe Lock では、コマンドライン引数で指定された CSV ファイル (初期設定では `targets.csv`) にログ情報を直接書き込みます。

   コマンドの受信後、エージェントが自動的に再起動します。

リモートタスクツール (SLtasks)

リモートタスクツールを使用すると、エージェントの許可リストの初期化、エージェントのロックダウン、ライセンスの照合、エージェントのファイアウォール設定を有効にしたままの Patch または HotFix の配信、コマンドラインを使用したエージェントステータスのクエリ、および管理者パスワードのリモートからの変更を実行できます。

Safe Lock Intelligent Manager では、初期設定で次の場所に `SLtasks.exe` ファイルが保存されます。

```
C:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager
¥CmdTools¥RemoteAgentTasksTool¥
```

重要

SLtasks をコマンドラインで使用できるのは、Windows の管理者権限を持つ Safe Lock Intelligent Manager の管理者のみです。

エージェントの許可リストからファイルを削除する

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。
2. cd コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「Safe Lock Remote Tasks Tool」フォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   ```
   cd/d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools
   \RemoteAgentTasksTool\"
   ```
3. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバにログインします。

   ```
   SLtasks.exe--logon
   ```
4. Safe Lock Intelligent Manager の資格情報を入力します。

   サーバに正常にログインしたことが、コマンドラインに表示されます。

   重要

   - タスクをエージェントに送信するには、ログインしたアカウントに「管理者」または「フルコントロール」権限が必要です。
   - ネットワークやエージェントへの影響を低減するため、Safe Lock Intelligent Manager は、対象エージェントの設定をクエリしてから必要と判断されるタスクのみを送信します。
5. 対象エージェントのリストを生成します。クエリの対象を特定バージョンより前または後のエージェントに制限するには、コマンドに--

minversion および--maxversion を追加して、エージェントのバージョンを入力します。

- SLtasks.exe--query--minversion<agent_version>
- SLtasks.exe--query--maxversion<agent_version>

重要

<agent_version> は x.x.xxxx の形式にする必要があります。たとえば「2.0.5000」のように指定します。

クエリの結果は query_results.csv に保存されます。

ヒント

エージェントステータスのクエリは、タスクを配信する前に実行することをお勧めします。タスクを配信する際、クエリ結果が古くなっていると警告メッセージが表示されます。

6. 次のいずれかの形式で、対象ファイルを UTF-8 形式の CSV ファイルにリストします。
   - ファイル名
   - ファイル名を含めたファイルパス
   - SHA-1 ハッシュを含めたファイルパス
   - ファイル名と SHA-1 ハッシュ
   - SHA-1 ハッシュ

   たとえば、次のすべての形式が有効です。
   - cal.exe,
   - C:\Windows\system32\calc.exe,
   - C:\Windows\system32\9018A7D6CDBE859A430E794E73381F77C840BE0,

- cal.exe, 9018A7D6CDBE859A430E794E73381F77C840BE0
- ,9018A7D6CDBE859A430E794E73381F77C840BE0,

7. 次の構文を入力して、すべてのエージェントの許可リストから項目を削除します。

   ```
   SLtasks.exe--removeitems<target_list_file_name>
   ```

   ヒント

   - 許可された項目のみを特定のエージェントから削除するには、コマンドに`--targetPC` を追加してエージェント名を入力します。

     例:

     `SLtasks.exe <task_parameter> --targetPC <endpoint_name>`

8. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバからログオフします。

   ```
   SLtasks.exe--logoff
   ```

   サーバから正常にログオフしたことが、コマンドラインに表示されます。

エージェントのライセンスを更新する

手順

1. Intelligent Manager のライセンス情報を更新します。
2. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。
3. `cd` コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「Safe Lock Remote Tasks Tool」フォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

cd/d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentTasksTool\"

4. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバにログインします。

   ```
   SLtasks.exe--logon
   ```

5. Safe Lock Intelligent Manager の資格情報を入力します。

   サーバに正常にログインしたことが、コマンドラインに表示されます。

重要

- タスクをエージェントに送信するには、ログインしたアカウントに「管理者」または「フルコントロール」権限が必要です。
- ネットワークやエージェントへの影響を低減するため、Safe Lock Intelligent Manager は、対象エージェントの設定をクエリしてから必要と判断されるタスクのみを送信します。

6. 対象エージェントのリストを生成します。クエリの対象を特定バージョンより前または後のエージェントに制限するには、コマンドに`--minversion` および`--maxversion` を追加して、エージェントのバージョンを入力します。

   - `SLtasks.exe--query--minversion<agent_version>`
   - `SLtasks.exe--query--maxversion<agent_version>`

重要

`<agent_version>` は `x.x.xxxx` の形式にする必要があります。たとえば「`2.0.5000`」のように指定します。

クエリの結果は `query_results.csv` に保存されます。

ヒント

エージェントステータスのクエリは、タスクを配信する前に実行することをお勧めします。タスクを配信する際、クエリ結果が古くなっていると警告メッセージが表示されます。

7. 次のコマンドを入力します。

   ```
   SLtasks.exe--match
   ```

   Safe Lock Intelligent Manager のライセンスに一致するように、対象エージェントのライセンスがただちにアップデートされます。

8. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバからログオフします。

   ```
   SLtasks.exe--logoff
   ```

   サーバから正常にログオフしたことが、コマンドラインに表示されます。

メッセージタイムグループを適用する

メッセージタイムグループは、メッセージ送信サイクルを使用して、Safe Lock エージェントから Safe Lock Intelligent Manager へ送信される自動送信メッセージに帯域幅コントロールを追加します。

メッセージ送信サイクルでは、アクティブグループのエージェントが Safe Lock Intelligent Manager に自動送信メッセージを送信します。このメッセージには、ログ、ステータス、および検索対象の隔離ファイルが含まれます。メッセージ送信サイクルが終了すると、次のエージェントグループがアクティブになり、自動送信メッセージを送信します。

アクティブグループ以外のエージェントは自動送信メッセージを送信しません。ただし、すべてのグループのエージェントは、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。たとえば、ログとステータスの送信という管理サーバ画面からの要求には、ネットワーク接続が許可され次第、対象エージェントが応答します。

注意

自動送信メッセージには次の条件が適用されます。

初期設定では、Safe Lock Intelligent Manager によりすべてのエージェントが 1 つの「always on」グループに入れられます。

メッセージ送信サイクルでは、メッセージは次の順序で送信されます。

- 優先度が高いものが先
- 最も古いもの (最も新しくないもの) が先

リモートタスクツールを使用してメッセージタイムグループを適用する

`SLtasks.exe` を使用してメッセージタイムグループをエージェントに適用します。

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。
2. `cd` コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「Safe Lock Remote Tasks Tool」フォルダに移動します。

   たとえば、次のコマンドを入力すると初期設定の場所に移動します。

   `cd/d "c:\Program Files\Trend Micro\Safe Lock Intelligent Manager\CmdTools\RemoteAgentTasksTool\"`
3. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバにログインします。

   `SLtasks.exe--logon`
4. Safe Lock Intelligent Manager の資格情報を入力します。

   サーバに正常にログインしたことが、コマンドラインに表示されます。

5. 次のコマンドを入力してメッセージタイムグループのクエリを実行します。

   ```
   SLtasks.exe--querygroup
   ```

   クエリの結果は group_info.csv に保存されます。

   重要

   メッセージタイムグループを適用するには、メッセージタイムグループのクエリを実行し、結果を必要に応じて編集して、設定したメッセージタイムグループをエージェントに適用する必要があります。メッセージタイムグループをエージェントに適用する際、クエリ結果が古くなっていると警告メッセージが表示されます。

6. group_info.csv を編集して、次のメッセージタイムグループのコントロールを設定します。

列名	説明
Total Group Num	エージェントを任意の数のグループに分割します。 **ヒント** 1 を設定すると機能は無効になります。
Own Group Index	Safe Lock エージェントのメッセージグループ ID 番号を設定します。
Time Period	メッセージ送信サイクルがアクティブになった場合に対象グループから Safe Lock Intelligent Manager へのメッセージ送信を許可する時間を設定します。

7. 次のコマンドを入力し、設定した group_info.csv ファイルを使用してメッセージタイムグループをエージェントに適用します。

   ```
   SLtasks.exe--applygroups
   ```

重要

- メッセージタイムグループをエージェントに適用するには、ログインしたアカウントに「管理者」または「フルコントロール」権限が必要です。
- `group_info.csv` にリストされたエージェントのみがコマンドを受け取ります。

8. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバからログオフします。

   ```
   SLtasks.exe--logoff
   ```

   サーバから正常にログオフしたことが、コマンドラインに表示されます。

設定ファイルを使用してメッセージタイムグループを適用する

手順

1. Trend Micro Safe Lock のメイン画面から [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。
   a. 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。
   b. パスワードを指定して [ログイン] をクリックします。
   c. [設定] メニュー項目をクリックします。
2. 設定ファイルをデータベースファイル (`.xen`) としてエクスポートします。
   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。
3. SLcmd を利用し、設定ファイルを復号します。

4. Windows のメモ帳などテキストエディタを使用して、<ManagedMode> セクションの MessageRandomization パラメータを次のように編集します。

列名	説明
TOTAL_GROUP_NUM	エージェントを任意の数のグループに分割します。
OWN_GROUP_INDEX	Safe Lock エージェントのメッセージグループ ID 番号を設定します。
TIME_PERIOD	メッセージ送信サイクルがアクティブになった場合に対象グループから Safe Lock Intelligent Manager へのメッセージ送信を許可する時間を設定します。

5. Trend Micro Safe Lock のメイン画面の [設定のエクスポート/インポート] セクションから、設定ファイルをデータベースファイル (.xen) としてインポートします。

   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、データベースファイルの新しい設定で上書きされます。

Setup.ini ファイルを使用してメッセージタイムグループを適用する

手順

1. Setup.ini ファイルで MESSAGERANDOMIZATION の引数を編集します。

   a. Trend Micro Safe Lock Intelligent Manager フォルダで Setup.ini をダブルクリックします。

   b. <MESSAGERANDOMIZATION> セクションで次の引数を編集します。

列名	説明
TOTAL_GROUP_NUM	エージェントを任意の数のグループに分割します。
OWN_GROUP_INDEX	Safe Lock エージェントのメッセージグループ ID 番号を設定します。
TIME_PERIOD	メッセージ送信サイクルがアクティブになった場合に対象グループから Safe Lock Intelligent Manager へのメッセージ送信を許可する時間を設定します。

2. Windows インストーラまたはコマンドラインのインストーラを使用して Safe Lock Intelligent Manager をインストールします。詳細については、Trend Micro Intelligent Manager インストールガイドの「Windows インストーラを使用したインストール」および「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。

エージェントのパスワードをリモートで更新する

Safe Lock Intelligent Manager を使用して Safe Lock エージェントのパスワードをリモートで更新します。

注意

- この機能を使用できるのは、管理者権限のあるユーザのみです。フルコントロール/読み取りのみ/ストレージデバイスコントロールの権限では、管理者パスワードをリモートで変更することはできません。
- ライセンスの有効期限が終了した Safe Lock エージェントを実行しており、バージョンが 2.0 Service Pack 1 Patch 2 より古い場合、パスワードのリモートでの更新は機能しません。

手順

1. Windows の管理者権限を使用して、コマンドプロンプトウィンドウを開きます。

2. cd コマンドを使用して、Trend Micro Safe Lock Intelligent Manager のインストールフォルダにある「Safe Lock Remote Tasks Tool」フォルダに移動します。

3. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバにログインします。

   ```
   SLtasks.exe--logon
   ```

4. Safe Lock Intelligent Manager の資格情報を入力します。

   サーバに正常にログインしたことが、コマンドラインに表示されます。

5. 対象エージェントのリストを生成します。クエリの対象を特定バージョンより前または後のエージェントに制限するには、コマンドに`--minversion` および`--maxversion` を追加して、エージェントのバージョンを入力します。

   - `SLtasks.exe--query--minversion<agent_version>`
   - `SLtasks.exe--query--maxversion<agent_version>`

   クエリの結果は `query_results.csv` に保存されます。

6. 次のコマンドを入力して、`query_results.csv` で指定されている対象エージェントに新しい管理者パスワードを設定します。

   ```
   --changepassword
   ```

   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。次の記号および空白は使用できません。| > < \ "
   - Safe Lock Intelligent Manager では、新しいエージェントパスワードを作成する際に古いパスワードは必要ありません。
   - 新しいパスワードと確認用のパスワードが一致することを確認してください。一致しない場合、コマンドは中止されます。

7. 次のコマンドを入力して、Safe Lock Intelligent Manager サーバからログオフします。

   ```
   SLtasks.exe--logoff
   ```

サーバから正常にログオフしたことが、コマンドラインに表示されます。

第 8 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、23 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、24 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 8-1. 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、220 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、229 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、232 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、90 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。

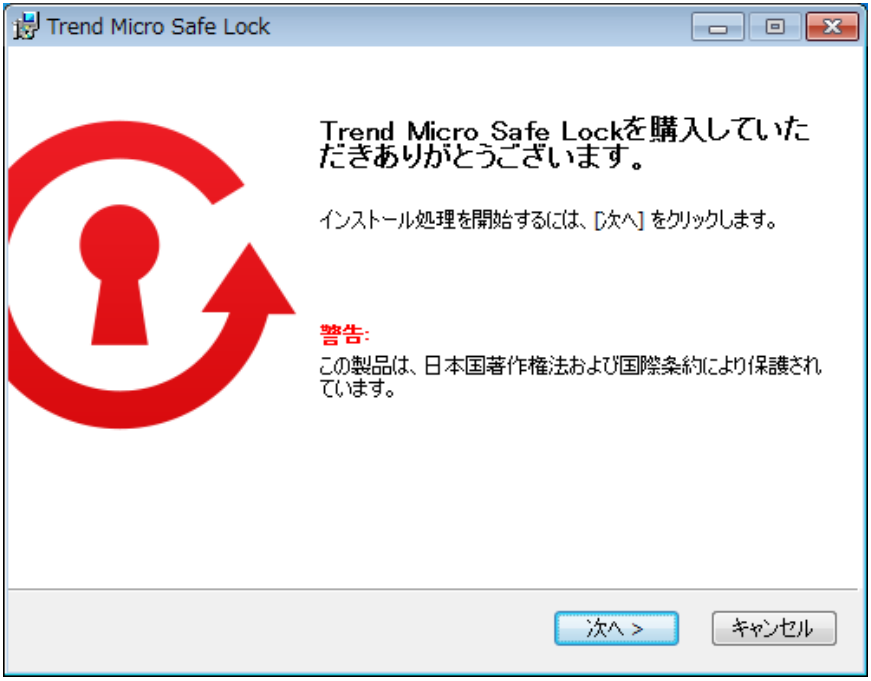
Windows インストーラを使用したインストール

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。

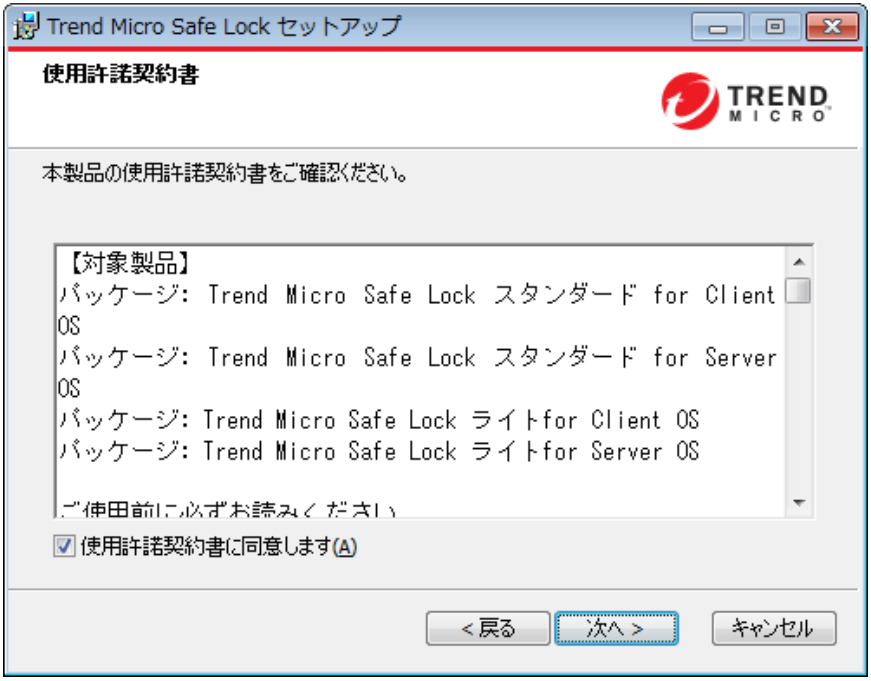


2. インストールウィザードが表示されたら、[次へ] をクリックします。

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。

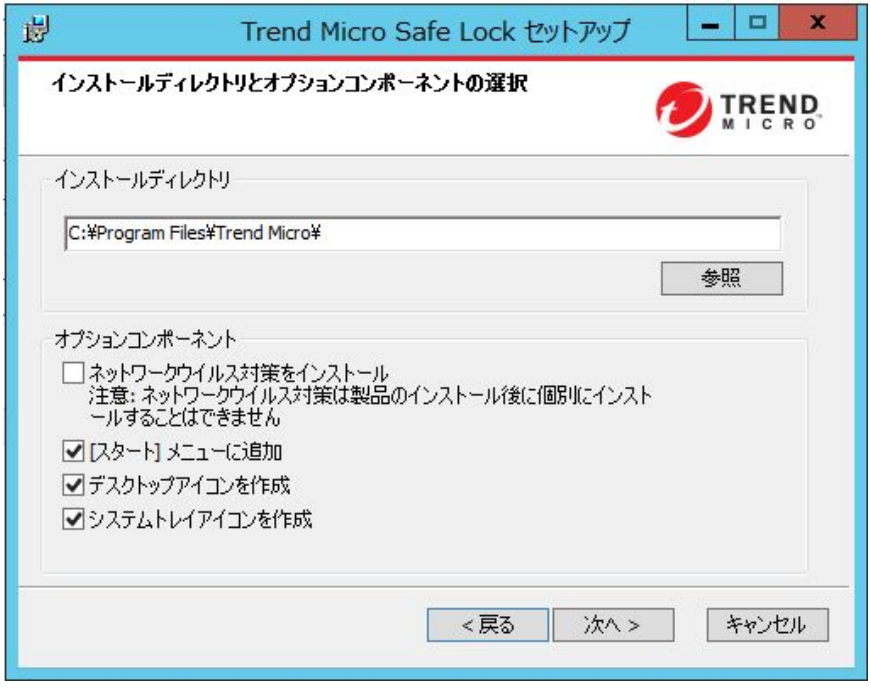
3. 使用許諾契約書を読み、[使用許諾契約書に同意します] を選択して [次へ] をクリックします。



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

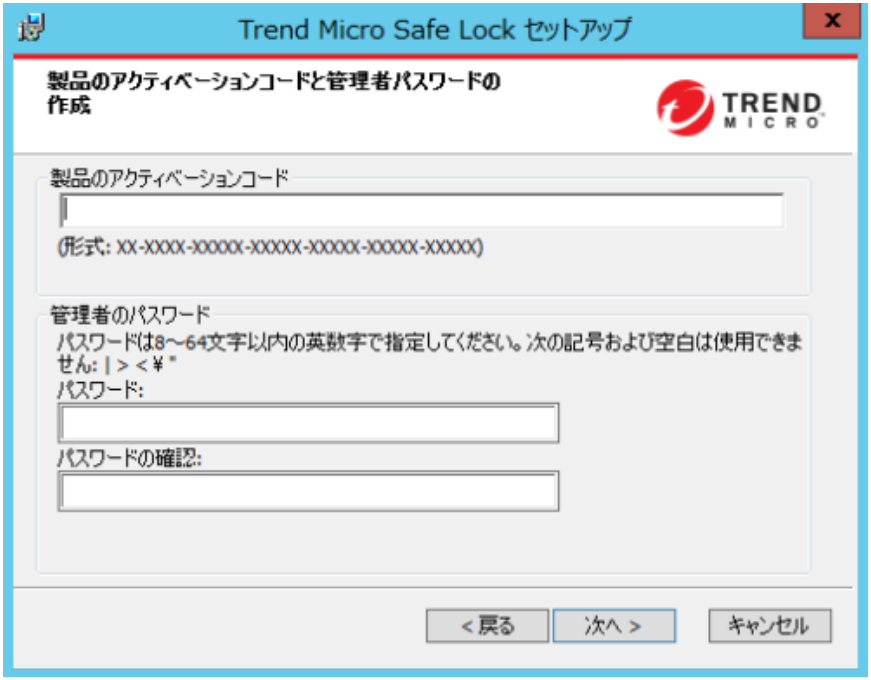
ネットワークウイルス対策をインストールできるのは初回のプログラムインストール時のみですが、必要に応じて後から無効にすることもできます。詳細については、管理者ガイドの「脆弱性攻撃対策の設定」を参照してください。



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

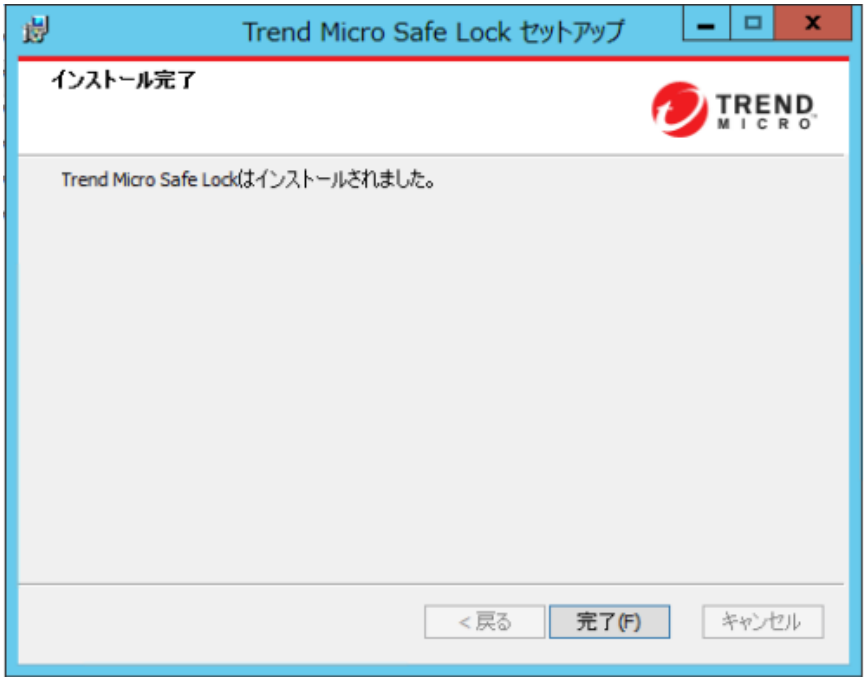
ジョンに脅威が含まれていないことを確認します。検出結果が誤検出であることが明らかな場合のみ、検出された脅威を無視します。

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、23 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。

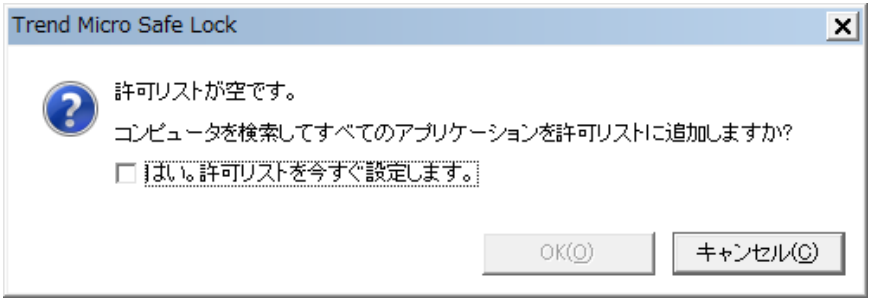
手順

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。

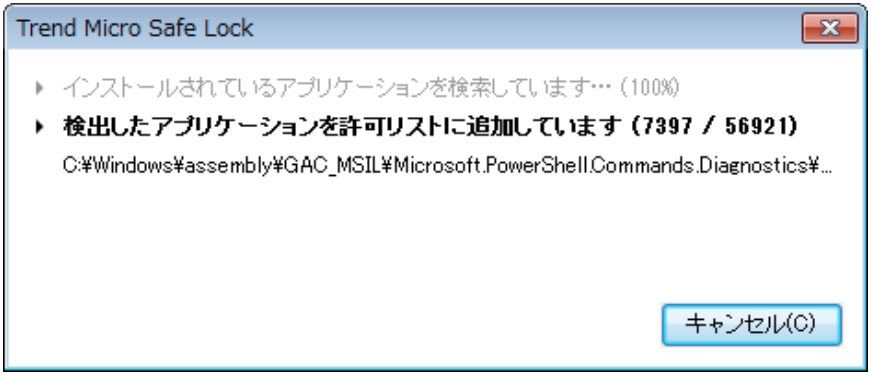
2. パスワードを入力して [ログイン] をクリックします。

   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。

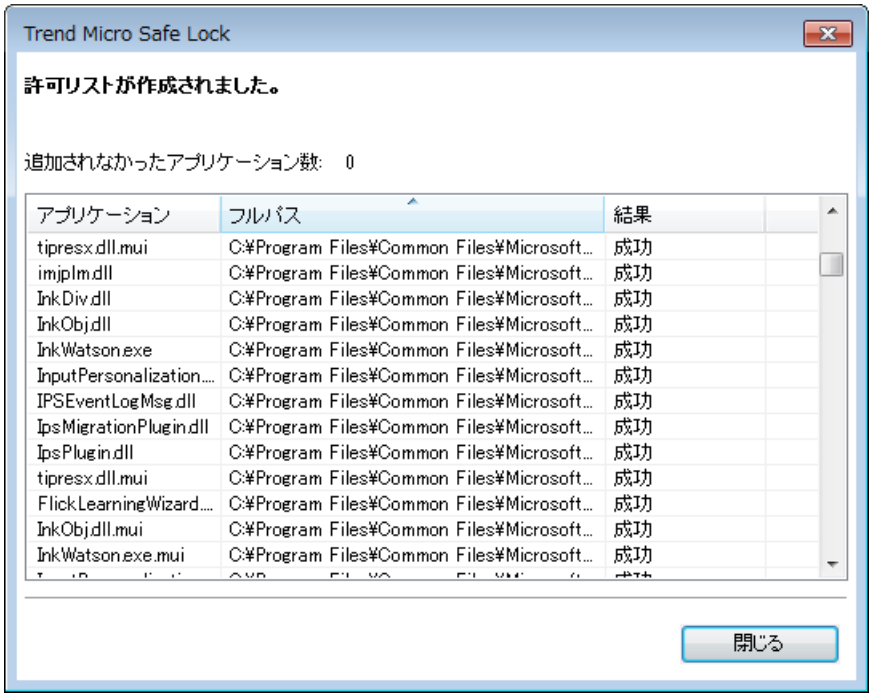


3. 通知ウィンドウで、[はい。許可リストを今すぐ設定します。] を選択して [OK] をクリックします。

   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 8-2. Safe Lock Intelligent Manager 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、233 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 8-3. 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 8-4. 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 8-5. 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 8-6. 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 Intelligent Manager 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 8-7. 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 Intelligent Manager 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 8-8. 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 8-9. 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 8-10. 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、233 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 8-11. 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 Intelligent Manager 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 9 章

エージェント設定ファイルの操作

この章では、設定ファイルを使用して Trend Micro Safe Lock を設定する方法について説明します。

この章の内容は次のとおりです。

エージェント設定ファイルの操作

設定ファイル管理者は設定ファイルを使用して、複数のコンピュータに同じ設定を適用できます。

詳細については、263 ページの「設定ファイルをエクスポートまたはインポートする」を参照してください。

詳細設定を変更する

一部の設定の変更は、コマンドラインを利用して設定ファイルを介してのみ可能です。詳細については、114 ページの「コマンドラインで SLCmd を使用する」を参照してください。

手順

1. 設定ファイルをエクスポートします。
2. SLcmd を利用し、設定ファイルを復号します。
3. Windows のメモ帳またはその他のテキストエディタで設定ファイルを編集します。

   重要

   設定ファイルでは UTF-8 エンコードのみがサポートされます。

   ヒント

   変更した設定のみをインポートして、複数エージェントの共有設定をアップデートできます。

4. SLcmd を利用し、編集した設定ファイルを暗号化します。
5. 編集した設定ファイルをインポートします。

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。

設定ファイルの構文

設定ファイルでは、XML 形式を使用して、Trend Micro Safe Lock で使用するパラメータを指定します。

重要

設定ファイルでは UTF-8 エンコードのみがサポートされます。

設定ファイルの例を次に示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<Configurations version="1.00.000"
    xmlns:xsi="http://www.w3.org/2001/
    XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="WKConfig.xsd">
    <Configuration>
        <AccountGroup>
            <Account
                Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}"
                Enable="no">
                <Password/>
            </Account>
        </AccountGroup>
        <UI>
            <SystemTaskTrayIcon Enable="yes">
                <BlockNotification Enable="no"
                    AlwaysOnTop="yes" ShowDetails="yes"
                    Authenticate="yes">
                    <Title/>
                    <Message/>
                </BlockNotification>
            </SystemTaskTrayIcon>
        </UI>
        <Feature>
            <ApplicationLockDown LockDownMode="2">
                <WhiteList RecentHistoryUnapprovedFilesLimit="50">
                            <ExclusionList>
                                  <Folder>C:\EXCLUDED_FOLDER\DLL\</Folder>
                                  <Folder>C:\EXCLUDED_FOLDER\EXE\</Folder>
                                  <Folder>C:\EXCLUDED_FOLDER\SCRIPT\</Folder>
                                  <Extension>png</Extension>
                                  <Extension>bmp</Extension>
                               </ExclusionList>
                            </WhiteList>
                <ScriptLockdown Enable="yes">
                    <Extension Id="bat">
```

```
                    <Interpreter>cmd.exe</Interpreter>
                </Extension>
                <Extension Id="cmd">
                    <Interpreter>cmd.exe</Interpreter>
                </Extension>
                <Extension Id="com">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="dll">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="drv">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="exe">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="js">
                    <Interpreter>cscript.exe</Interpreter>
                    <Interpreter>wscript.exe</Interpreter>
                </Extension>
                <Extension Id="msi">
                    <Interpreter>msiexec.exe</Interpreter>
                </Extension>
                <Extension Id="pif">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="ps1">
                    <Interpreter>powershell.exe
                    </Interpreter>
                </Extension>
                <Extension Id="sys">
                    <Interpreter>ntvdm.exe</Interpreter>
                </Extension>
                <Extension Id="vbe">
                    <Interpreter>cscript.exe</Interpreter>
                    <Interpreter>wscript.exe</Interpreter>
                </Extension>
                <Extension Id="vbs">
                    <Interpreter>cscript.exe</Interpreter>
                    <Interpreter>wscript.exe</Interpreter>
                </Extension>
```

```
                </ScriptLockdown>
                <TrustedUpdater>
                    <PredefinedTrustedUpdater Enable="no">
                        <RuleSet/>
                    </PredefinedTrustedUpdater>
                    <WindowsUpdateSupport Enable="no"/>
                </TrustedUpdater>
                <DllDriverLockDown Enable="yes"/>
                <ExceptionPath Enable="no">
                    <ExceptionPathList/>
                </ExceptionPath>
                <TrustedCertification Enable="yes"/>
                <TrustedHash Enable="no"/>
                <WriteProtection Enable="no" ActionMode="1"
                ProtectApprovedList="yes"/>
                <CustomAction ActionMode="0"/>
                <FilelessAttackPrevention Enable="no">
                    <ExceptionList/>
                </FilelessAttackPrevention>
            </ApplicationLockDown>
            <UsbMalwareProtection Enable="no" ActionMode="1"/>
            <NetworkVirusProtection Enable="yes"
            ActionMode="1"/>
            <IntegrityMonitoring Enable="no"/>
            <StorageDeviceBlocking Enable="no" ActionMode="1"/>
            <Log>
                <EventLog Enable="yes">
                    <Level>
                        <WarningLog Enable="yes"/>
                        <InformationLog Enable="no"/>
                    </Level>
                    <BlockedAccessLog Enable="yes"/>
                    <ApprovedAccessLog Enable="yes">
                        <TrustedUpdaterLog Enable="yes"/>
                        <DllDriverLog Enable="no"/>
                        <ExceptionPathLog Enable="yes"/>
                        <TrustedCertLog Enable="yes"/>
                        <TrustedHashLog Enable="yes"/>
                        <WriteProtectionLog Enable="yes"/>
                    </ApprovedAccessLog>
                    <SystemEventLog Enable="yes">
                        <ExceptionPathLog Enable="yes"/>
```

```
                    <WriteProtectionLog Enable="yes"/>
                </SystemEventLog>
                <ListLog Enable="yes"/>
                <UsbMalwareProtectionLog Enable="yes"/>
                <ExecutionPreventionLog Enable="yes"/>
                <NetworkVirusProtectionLog Enable="yes"/>
                <IntegrityMonitoringLog>
                    <FileCreatedLog Enable="yes"/>
                    <FileModifiedLog Enable="yes"/>
                    <FileDeletedLog Enable="yes"/>
                    <FileRenamedLog Enable="yes"/>
                    <RegValueModifiedLog Enable="yes"/>
                    <RegValueDeletedLog Enable="yes"/>
                    <RegKeyCreatedLog Enable="yes"/>
                    <RegKeyDeletedLog Enable="yes"/>
                    <RegKeyRenamedLog Enable="yes"/>
                </IntegrityMonitoringLog>
                <DeviceControlLog Enable="yes"/>
            </EventLog>
            <DebugLog Enable="no"/>
        </Log>
    </Feature>
    <ManagedMode Enable="no">
        <Agent>
            <Port/>
            <SslAllowBeast>1</SslAllowBeast>
            <PollServer>0</PollServer>
            <PollServerInterval>10</PollServerInterval>
        </Agent>
        <Server>
            <HostName/>
            <FastPort/>
            <SlowPort/>
            <ApiKey/>
        </Server>
        <Message InitialRetryInterval="120"
        MaxRetryInterval="7680">
            <Register Trigger="1"/>
            <Unregister Trigger="1"/>
            <UpdateStatus Trigger="1"/>
            <UploadBlockedEvent Trigger="1"/>
            <CheckFileHash Trigger="1"/>
```

```
                <QuickScanFile Trigger="1"/>
            </Message>
            <MessageRandomization TotalGroupNum="1"
            OwnGroupIndex="0" TimePeriod="0"/>
            <Proxy Mode="0">
                <HostName/>
                <Port/>
                <UserName/>
                <Password/>
            </Proxy>
        </ManagedMode>
    </Configuration>
    <Permission>
        <AccountRef
        Id="{24335D7C-1204-43d1-9CBB-332D688C85B6}">
            <UIControl Id="DetailSetting" State="no"/>
            <UIControl Id="LockUnlock" State="yes"/>
            <UIControl Id="LaunchUpdater" State="yes"/>
            <UIControl Id="RecentHistoryUnapprovedFiles"
                 State="yes"/>
            <UIControl Id="ImportExportList" State="yes"/>
            <UIControl Id="ListManagement" State="yes"/>
            <UIControl Id="SupportToolUninstall" State="no"/>
        </AccountRef>
    </Permission>
</Configurations>
```

設定ファイルのパラメータ

設定ファイルには、Safe Lock で使用するパラメータを指定するセクションが含まれています。

表 9-1. 設定ファイルのセクションと説明

セクション	説明	追加情報
`Configuration`	<Configuration> セクションのコンテナ	

セクション		説明	追加情報
AccountGroup		制限付きユーザアカウントを設定するパラメータ	270 ページの「<AccountGroup> セクション」を参照してください。 106 ページの「アカウントの種類」を参照してください。
UI		システムトレイアイコンの表示を設定するパラメータ	271 ページの「<UI> セクション」を参照してください。
Feature		<Feature> セクションのコンテナ	
	ApplicationLockDown	Trend Micro Safe Lock の機能を設定するパラメータ	272 ページの「<Feature> セクション」を参照してください。
	UsbMalwareProtection		
	DllInjectionPrevention		
	ApiHookingPrevention		
	MemoryRandomization		
	NetworkVirusProtection		
	IntegrityMonitoring		
	StorageDeviceBlocking	ストレージデバイスによる管理下のエージェントへのアクセスを制御するパラメータ	

セクション	説明	追加情報
Log	各種のログを設定するパラメータ	287 ページの「<Log> セクション」を参照してください。 318 ページの「エージェントのイベントログの説明」を参照してください。
ManagedMode	集中管理機能を設定するパラメータ	291 ページの「<ManagedMode> セクション」を参照してください。
Permission	<Permission> セクションのコンテナ	
AccountRef	制限付きユーザアカウントで使用できる Trend Micro Safe Lock のメイン画面のコントロールを設定するパラメータ	296 ページの「<AccountRef> セクション」を参照してください。 106 ページの「アカウントの種類」を参照してください。

<AccountGroup> セクション

制限付きユーザアカウントを設定するパラメータ

106 ページの「アカウントの種類」を参照してください。

表 9-2. <AccountGroup> セクションのパラメータ

パラメータ	設定	値	説明
Configuration			<Configuration> セクションのコンテナ
AccountGroup			<AccountGroup> セクションのコンテナ

パラメータ			設定	値	説明
		Account	ID	<GUID>	制限付きユーザアカウントの GUID
			Enable	yes	制限付きユーザアカウントを有効にします
				no	制限付きユーザアカウントを無効にします
			Password	<Safe_Lock_password>	メイン画面にアクセスするための、制限付きユーザアカウントのパスワード 注意 Safe Lock 管理者と制限付きユーザのパスワードは同一にできません。

<UI> セクション

システムトレイアイコンの表示を設定するパラメータ

表 9-3. <UI> セクションのパラメータ

パラメータ				設定	値	説明
Configuration						<Configuration> セクションのコンテナ
	UI					<UI> セクションのコンテナ
		SystemTrayIcon		Enable	yes	システムトレイアイコンと Windows 通知を表示します
					no	システムトレイアイコンと Windows 通知を非表示にします
			BlockNotification	Enable	yes	エージェントの許可リストに指定されていないファイルをブロックしたときに管理下の

パラメータ				設定	値	説明
						エージェントに通知を表示します。
					no	エージェントの許可リストに指定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せん。
				Authenticate	yes	通知を閉じるときに管理者パスワードの入力を求めるプロンプトを表示します。
					no	通知を閉じるときにパスワードは求められません。
				ShowDetails	yes	ブロックされたファイルのファイルパスとイベント時間を表示します。
					no	イベントの詳細情報を表示しません。
				AlwaysOnTop	yes	通知の最前面表示を維持します。
					no	他の画面を通知の前面に表示できます。
				Title	<Title>	通知のタイトルを指定します。
				Message	<Message>	通知のメッセージを指定します。

<Feature> セクション

Trend Micro Safe Lock の機能を設定するパラメータ

107 ページの「機能の設定について」を参照してください。

表 9-4. <Feature> セクションのパラメータ

パラメータ	設定	値	説明
Configuration			<Configuration> セクションのコンテナ
Feature			<Feature> セクションのコンテナ
ApplicationLockDown	LockDownMode	1	アプリケーション制御を有効にします
		2	アプリケーション制御を無効にします
WhiteList	RecentHistoryUnapprovedFilesLimit	0 - 65535	ブロックされたファイルのログエントリの最大数
ExclusionList			許可リスト初期化時の除外セクションのコンテナ
	Folder	<folder_path>	除外するフォルダパス
	Extension	<file_extension>	除外するファイル拡張子
ScriptLockDown	Enable	yes	スクリプト制御を有効にします
		no	スクリプト制御を無効にします
Extension	ID	<file_extension>	スクリプト制御でブロックするファイル拡張子 たとえば、MSI の値を指定すると .msi ファイルがブロックされます。
Interpreter		<file_name>	指定したファイル拡張子のインタープリタ

パラメータ	設定	値	説明
			たとえば、msiexec.exe を .msi ファイルのインタープリタとして指定します。
TrustedUpdater			<TrustedUpdater> セクションのコンテナ
PredefinedTrustedUpdater	Enable	yes	許可リスト自動更新を有効にします
		no	許可リスト自動更新を無効にします
RuleSet			<RuleSet> 条件のコンテナ
Condition	ID	<unique_ruleset_name>	ルールセットの一意の名前
ApprovedListCheck	Enable	yes	許可リスト自動更新を使用して実行されたプログラムのハッシュの確認を有効にします
		no	許可リスト自動更新を使用して実行されたプログラムのハッシュの確認を無効にします
ParentProcess	Path	<process_path>	許可リスト自動更新のリストに追加する親プロセスのパス
Exception	Path	<process_path>	許可リスト自動更新のリストから除外するパス
Rule	Label	<unique_rule_name>	このルールの一意の名前

パラメータ	設定	値	説明
Updater	Type	process	指定された EXE ファイルを使用します
		file	指定された MSI または BAT ファイルを使用します
		folder	指定されたフォルダの EXE、MSI、または BAT ファイルを使用します
		folderandsub	指定されたフォルダとそのサブフォルダの EXE、MSI、または BAT ファイルを使用します
	Path	<updater_path>	アップデートプログラムのパス
	ConditionRef	<condition_ID>	許可リスト自動更新の詳細なルールを提供するための条件 ID
WindowsUpdateSupport	Enable	yes	ロックダウンされている管理下のエージェントでの Windows Update の実行を許可します。
		no	ロックダウンされている管理下のエージェントでの Windows Update をブロックします。
DLLDriverLockdown	Enable	yes	DLL/ドライバ制御を有効にします
		no	DLL/ドライバ制御を無効にします

パラメータ	設定	値	説明
ExceptionPath	Enable	yes	除外パスを有効にします
		no	除外パスを無効にします
ExceptionPathList			除外リストのコンテナ
ExceptionPath	Path	<exception_path>	除外パス
	Type	file	指定されたファイルのみを使用します
		folder	指定されたフォルダのファイルを使用します
		folderandsub	指定されたフォルダとそのサブフォルダのファイルを使用します
		regexp	正規表現を使用して除外を使用します
TrustedCertification	Enable	yes	信頼するデジタル証明書の使用を有効にします
		no	信頼するデジタル証明書の使用を無効にします
PredefinedTrustedCertification	Type	updater	この証明書で署名されたファイルはアップデートプログラムとみなされます
		lockdown	この証明書で署名されたファイルはアップデートプログラムとみなされません

パラメータ	設定	値	説明
	Hash	<SHA-1_hash_value>	このデジタル証明書の SHA1 ハッシュ値です
	Label	<label>	このデジタル証明書の説明です
	Subject	<subject>	このデジタル証明書の発行先です
	Issuer	<issuer>	このデジタル証明書の発行者です
TrustedHash	Enable	yes	信頼するハッシュリストの使用を有効にします
		no	信頼するハッシュリストの使用を無効にします
PredefinedTrustedHash	Type	updater	このハッシュ値に一致したファイルはアップデートプログラムとみなされます
		lockdown	このハッシュ値に一致したファイルはアップデートプログラムとみなされません
	Hash	<SHA-1_hash_value>	このファイルの SHA-1 ハッシュ値です
	Label	<label>	このファイルの説明です
	AddToApprovedList	yes	初回アクセス時にこのハッシュ値に一致したファイルを許可リストに追加します

パラメータ	設定	値	説明
		no	このハッシュ値に一致したファイルを許可リストに追加しません
	Path	<file_path>	ファイルパス
	Note	<note>	このハッシュ値に一致したファイルのメモを追加します
WriteProtection	Enable	yes	書き込み制御を有効にします
		no	書き込み制御を無効にします
	ActionMode	0	編集、名前の変更、削除などの処理を許可します
		1	編集、名前の変更、削除などの処理をブロックします
	ProtectApprovedList	yes	書き込み制御が有効な場合に、書き込み制御リストとともに許可リストの保護を有効にします
		no	書き込み制御が有効な場合に、書き込み制御リストとともに許可リストの保護を無効にします
リスト			書き込み制御リストのコンテナ
File	Path	<file_path>	ファイルパス

パラメータ						設定	値	説明
					Folder	Path	<folder_path>	フォルダパス
						IncludeSubfolder	yes	指定されたフォルダとそのサブフォルダのファイルを使用します
							no	指定されたフォルダのファイルを使用します
					RegistryKey	Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用することも、省略せずに記述することもできます。 • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
						IncludeSubkey	yes	サブキーをすべて含めます
							no	サブキーを含めません

パラメータ		設定	値	説明
RegistryValue		Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用することも、省略せずに記述することもできます。 • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
		Name	<reg_value_name>	レジストリ値の名前
ExceptionList				書き込み制御の除外リストのコンテナ
	Process	Path	<process_path>	プロセスのパス
	File	Path	<file_path>	ファイルパス
	Folder	Path	<folder_path>	フォルダパス

パラメータ						設定	値	説明
						IncludeSubfolder	yes	指定されたフォルダとそのサブフォルダのファイルを使用します
							no	指定されたフォルダのファイルを使用します
					RegistryKey	Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用することも、省略せずに記述することもできます。 • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
						IncludeSubkey	yes	サブキーをすべて含めます
							no	サブキーを含めません
					RegistryValue	Key	<reg_key>	レジストリキー <reg_key> は、次に示すように省略形を使用す

パラメータ						設定	値	説明
								ることも、省略せずに記述することもできます。 • HKEY_LOCAL_MACHINE\test HKLM\test • HKEY_CURRENT_CONFIG\test HKCC\test • HKEY_CLASSES_ROOT\test HKCR\test • HKEY_CURRENT_USER\test HKCU\test • HKEY_USERS\test HKU\test
						Name	<reg_value_name>	レジストリ値の名前
			CustomAction			ActionMode	0	アプリケーション制御で次のいずれかのイベントがブロックされた場合に、ブロックされたファイルまたはプロセスを無視します • プロセスの起動 • DLL の読み込み • スクリプトファイルのアクセス
							1	アプリケーション制御で次のいずれかのイベ

パラメータ	設定	値	説明
			ントがブロックされた場合に、ブロックされたファイルまたはプロセスを隔離します • プロセスの起動 • DLL の読み込み • スクリプトファイルのアクセス
		2	アプリケーション制御で次のいずれかのイベントがブロックされた場合に、ブロックされたファイルまたはプロセスに対する処理を確認します • プロセスの起動 • DLL の読み込み • スクリプトファイルのアクセス
UsbMalwareProtection	Enable	yes	USB 不正プログラム対策を有効にします
		no	USB 不正プログラム対策を無効にします
	ActionMode	0	検出された不正プログラムによって処理を許可します
		1	検出された不正プログラムによって処理をブロックします
DllInjectionPrevention	Enable	yes	DLL インジェクション対策を有効にします

パラメータ	設定	値	説明
		no	DLL インジェクション対策を無効にします
	ActionMode	0	DLL インジェクションを許可します
		1	DLL インジェクションをブロックします
ApiHookingPrevention	Enable	yes	API フッキング対策を有効にします
		no	API フッキング対策を無効にします
	ActionMode	0	API フッキングを許可します
		1	API フッキングをブロックします
MemoryRandomization	Enable	yes	メモリのランダム化を有効にします
		no	メモリのランダム化を無効にします
NetworkVirusProtection	Enable	yes	ネットワークウイルス対策を有効にします
		no	ネットワークウイルス対策を無効にします
	ActionMode	0	検出されたネットワークウイルスによって処理を許可します
		1	検出されたネットワークウイルスによって処理をブロックします
IntegrityMonitoring	Enable	yes	変更監視を有効にします

パラメータ	設定	値	説明
		no	変更監視を無効にします
StorageDeviceBlocking	Enable	yes	管理下のエージェントへのストレージデバイス (CD/DVD ドライブ、フロッピーディスクドライブおよびネットワークドライブ) によるアクセスをブロックします
	Disable	no	管理下のエージェントへのストレージデバイス (CD/DVD ドライブ、フロッピーディスクドライブおよびネットワークドライブ) によるアクセスを許可します
	ActionMode	0	編集、名前の変更、削除などの処理を許可します
		1	編集、名前の変更、削除などの処理をブロックします
	Log		ログ設定のコンテナ 287 ページの「<Log> セクション」を参照してください。
FilelessAttackPrevention	Enable	yes	ファイルレス攻撃対策を有効にします
		no	ファイルレス攻撃対策を無効にします
ExceptionList			ファイルレス攻撃対策の除外リストのコンテナ

パラメータ			設定	値	説明
Exception			Target	<monitored process>	powershell.exe、wscript.exe、CScript.exe、または mshta.exe を指定します
			Label	<label>	この除外の一意の名前
	Arguments			<arguments>	許可される引数
			Regex	yes	引数に正規表現が含まれる場合は yes を指定します
				no	引数に正規表現が含まれない場合は no を指定します
	Parent1			<parent process>	監視対象プロセスの親プロセス
	Parent2			<grandparent process>	監視対象プロセスの祖父母プロセス
	Parent3			<greatgrandparent process>	監視対象プロセスの曾祖父母プロセス
	Parent4			<greatgreatgrandparent process>	監視対象プロセスの高祖父母プロセス

<Log> セクション

各種のログを設定するパラメータ

318 ページの「エージェントのイベントログの説明」を参照してください。

表 9-5. ログ設定のパラメータ

パラメータ	設定	値	説明
Configuration			<Configuration> セクションのコンテナ
Feature			<Feature> セクションのコンテナ
Log			ログ設定のコンテナ
EventLog	Enable	yes	次の要素に指定された Safe Lock イベントをログに記録します
		no	次の要素に指定された Safe Lock イベントをログに記録しません
Level			ログレベル設定のコンテナ
WarningLog	Enable	yes	警告レベルのイベントをログに記録します
		no	警告レベルのイベントをログに記録しません
InformationLog	Enable	yes	情報レベルのイベントをログに記録します
		no	情報レベルのイベントをログに記録しません
BlockedAccessLog	Enable	yes	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

パラメータ			設定	値	説明
				no	Trend Micro Safe Lock でブロックされたファイルをログに記録しません
		ApprovedAccessLog	Enable	yes	Trend Micro Safe Lock で許可されたファイルをログに記録します
				no	Trend Micro Safe Lock で許可されたファイルをログに記録しません
		TrustedUpdaterLog	Enable	yes	許可リスト自動更新で許可されたアクセスのログを有効にします
				no	許可リスト自動更新で許可されたアクセスのログを無効にします
		DLLDriverLog	Enable	yes	DLL/ドライバの許可されたアクセスのログを有効にします
				no	DLL/ドライバの許可されたアクセスのログを無効にします
		ExceptionPathLog	Enable	yes	アプリケーション制御除外パスの許可されたアクセスのログを有効にします
				no	アプリケーション制御除外パスの許可されたアクセスのログを無効にします
		TrustedCertLog	Enable	yes	信頼するデジタル証明書の許可されたアクセスのログを有効にします
				no	信頼するデジタル証明書の許可されたアクセスのログを無効にします
		WriteProtectionLog	Enable	yes	書き込み制御の許可されたアクセスのログを有効にします

パラメータ	設定	値	説明
		no	書き込み制御の許可されたアクセスのログを無効にします
SystemEventLog	Enable	yes	システムに関連するイベントをログに記録します
		no	システムに関連するイベントをログに記録しません
ExceptionPathLog	Enable	yes	アプリケーション制御からの除外を有効にします
		no	アプリケーション制御からの除外を無効にします
WriteProtectionLog	Enable	yes	書き込み制御のシステムログを有効にします
		no	書き込み制御のシステムログを無効にします
ListLog	Enable	yes	許可リストに関連するイベントをログに記録します
		no	許可リストに関連するイベントをログに記録しません
USBMalwareProtectionLog	Enable	yes	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
		no	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せん
ExecutionPreventionLog	Enable	yes	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
		no	実行防止対策を作動させるイベントをログに記録しません
NetworkVirusProtectionLog	Enable	yes	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

パラメータ		設定	値	説明
			no	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せん
IntegrityMonitoringLog				変更監視ログの設定のコンテナ
	FileCreatedLog	Enable	yes	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
			no	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せん
	FileModifiedLog	Enable	yes	ファイル変更イベントをログに記録します
			no	ファイル変更イベントをログに記録しません
	FileDeletedLog	Enable	yes	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
			no	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せん
	FileRenamedLog	Enable	yes	ファイルおよびフォルダ名変更イベントをログに記録します
			no	ファイルおよびフォルダ名変更イベントをログに記録しません
	RegValueModifiedLog	Enable	yes	レジストリ値変更イベントをログに記録します
			no	レジストリ値変更イベントをログに記録しません
	RegValueDeletedLog	Enable	yes	レジストリ値削除イベントをログに記録します

パラメータ	設定	値	説明
		no	レジストリ値削除イベントをログに記録しません
RegKeyCreatedLog	Enable	yes	レジストリキー作成イベントをログに記録します
		no	レジストリキー作成イベントをログに記録しません
RegKeyDeletedLog	Enable	yes	レジストリキー削除イベントをログに記録します
		no	レジストリキー削除イベントをログに記録しません
RegKeyRenamedLog	Enable	yes	レジストリキー名変更イベントをログに記録します
		no	レジストリキー名変更イベントをログに記録しません
DeviceControlLog	Enable	yes	ストレージデバイスコントロールイベントをログに記録します
		no	ストレージデバイスコントロールイベントをログに記録しません
EventLog	Enable	yes	デバッグ情報をログに記録します
		no	デバッグ情報をログに記録しません

<ManagedMode> セクション

集中管理機能を設定するパラメータ

表 9-6. <ManagedMode> セクションのパラメータ

パラメータ	設定	値	説明
Configuration			<Configuration> セクションのコンテナ
ManagedMode	Enable	yes	集中管理モードを有効にします
		no	集中管理モードを無効にします
Agent			Safe Lock エージェントの設定のコンテナ
Port		<server_messages_port>	サーバ通信用のセキュアポート番号を指定します (従来の呼称はエージェントの待機ポート)
SslAllowBeast		0	Windows Server 2008 プラットフォームで大きなファイル (10MB 超) のアップロードを可能にします
		1	Windows Server 2008 プラットフォーム (初期設定値) での大きなファイル (10MB 超) のアップロードの失敗を防止します
PollServer		0	エージェントを非 NAT エージェントとして識別します
		1	エージェントを NAT エージェントとして識別します
PollServerInterval		<interval_period>	NAT 接続の頻度を 1～64800 分の範囲で指定します (1～64800 分ごと

パラメータ	設定	値	説明
			に Safe Lock サーバに接続します)
Server			Safe Lock Intelligent Manager の設定のコンテナ
HostName		<hostname>	Intelligent Manager サーバのホスト名を指定します
FastPort		<logs_port>	ログとステータスを収集するためのセキュアポート番号を指定します (従来の呼称は高速接続)
SlowPort		<files_port>	検索対象ファイルを収集するためのセキュアポート番号を指定します (従来の呼称は低速接続)
ApiKey		<API_key>	API キーを指定します
Message			Safe Lock Intelligent Manager 宛自動送信メッセージの設定のコンテナ
Register	Trigger	1	イベントの発生後、可能なかぎり速やかに送信します
		2	Intelligent Manager に要求されるまで送信しません
Unregister	Trigger	1	イベントの発生後、可能なかぎり速やかに送信します
		2	Intelligent Manager に要求されるまで送信しません

<table>
<tr><th colspan="3">パラメータ</th><th>設定</th><th>値</th><th>説明</th></tr>
<tr><td colspan="2"></td><td>UpdateStatus</td><td>Trigger</td><td>1</td><td>イベントの発生後、可能なかぎり速やかに送信します</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td>2</td><td>Intelligent Manager に要求されるまで送信しません</td></tr>
<tr><td colspan="2"></td><td>UploadBlockedEvent</td><td>Trigger</td><td>1</td><td>イベントの発生後、可能なかぎり速やかに送信します</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td>2</td><td>Intelligent Manager に要求されるまで送信しません</td></tr>
<tr><td colspan="2"></td><td>CheckFileHash</td><td>Trigger</td><td>1</td><td>イベントの発生後、可能なかぎり速やかに送信します</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td>2</td><td>Intelligent Manager に要求されるまで送信しません</td></tr>
<tr><td colspan="2"></td><td>QuickScanFile</td><td>Trigger</td><td>1</td><td>イベントの発生後、可能なかぎり速やかに送信します</td></tr>
<tr><td colspan="2"></td><td></td><td></td><td>2</td><td>Intelligent Manager に要求されるまで送信しません</td></tr>
<tr><td colspan="2"></td><td colspan="4">MessageRandomization

  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 Intelligent Manager 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。</td></tr>
<tr><td colspan="2"></td><td></td><td>TotalGroupNum</td><td>正の整数 (>= 1)</td><td>メッセージタイムグループの合計数を指定します</td></tr>
</table>

パラメータ				設定	値	説明
				OwnGroupIndex	ゼロまたは正の整数、 < TotalGroupNum	この Safe Lock エージェントのメッセージタイムグループ ID 番号を指定します
				TimePeriod	ゼロまたは正の整数	このメッセージタイムグループのメッセージ送信サイクルがアクティブな場合に、このグループの ID 番号で Intelligent Manager に自動送信メッセージを送信する時間を秒単位で指定します **注意** メッセージタイムグループは、この時間がゼロ (0) に設定されている場合はアクティブになりません。
		Proxy		Mode	0	プロキシを使用しません (直接アクセス)
					1	プロキシを使用します (手動設定)
					2	プロキシ設定を Internet Explorer と同期します
			HostName		<proxy_hostname>	プロキシホスト名を指定します
			Port		<proxy_port>	プロキシポート番号を指定します
			UserName		<proxy_user_name>	プロキシユーザ名を指定します
			Password		<proxy_password>	プロキシパスワードを指定します

<AccountRef> セクション

制限付きユーザアカウントで使用できる Trend Micro Safe Lock のメイン画面のコントロールを設定するパラメータ

106 ページの「アカウントの種類」を参照してください。

表 9-7. <AccountRef> セクションのパラメータ

パラメータ	設定	値	説明
Configuration			<Configuration> セクションのコンテナ
Permission			<Permission> セクションのコンテナ
AccountRef			<AccountRef> セクションのコンテナ
UIControl	ID	DetailSetting	Trend Micro Safe Lock のメイン画面の [設定] ページの機能にアクセスします。 注意 制限付きユーザのアカウントでは [パスワード(P)] ページは使用できません。
		LockUnlock	[概要] 画面のアプリケーション制御の設定にアクセスします
		LaunchUpdater	制限付きユーザが [許可リスト] 画面の [アプリの追加] をクリックした場合の、[選択したアプリケーションインストーラによって作成または修正されたファイルを自動的に追加する] オプションにアクセスします。
		RecentHistoryUnapprovedFIles	制限付きユーザが [概要] 画面の [前回のアプリケーションブロック日時] をクリックした場合の、ブロックログにアクセスします。

パラメータ	設定	値	説明
		ImportExportList	[リストのインポート] ボタンと [リストのエクスポート] ボタンにアクセスします
		ListManagement	[許可リスト] 画面の次の項目にアクセスします • [アプリの削除] ボタン • [ハッシュを更新] ボタン • [アプリの追加] > [既存ファイルとフォルダの追加] メニュー
	State	yes	ID で指定された権限を有効にします
		no	ID で指定された権限を無効にします

第 10 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 11 章

トラブルシューティングとよくある質問 (FAQ)

この章では、Trend Micro Safe Lock Intelligent Manager の問題のトラブルシューティングに役立つリソースのリストを示します。

この章の内容は次のとおりです。

リモートエージェントインストールのトラブルシューティング

`SLrst` コマンドラインプログラムを使用して実行したリモートインストールでは、次のようなメッセージが表示されることがあります。

Unable to Run: ネットワークまたはファイアウォールが正しく設定されていないか、Safe Lock 1.1 より前のバージョンがインストールされています。設定を確認し、古いバージョンの Safe Lock を対象コンピュータから削除して、セットアップを再度実行します。

Went Offline: セットアップの実行中にコンピュータがオフラインになりました。ツールでは、インストールが正常に完了したかどうかを判別できません。Safe Lock Intelligent Manager の管理サーバ画面にコンピュータが表示される場合は、インストールが正常に完了しています。コンピュータが表示されない場合は、そのコンピュータをローカルで確認する必要があります。

よくある質問

インストール後またはアンインストール後は再起動が必要ですか?

次の場合を除き、インストール後に Safe Lock エージェントを再起動する必要はありません。

再起動が必要な場合	例
設定の変更	[メモリのランダム化] の設定を変更した場合は、管理下のエージェントを再起動して変更を適用する必要があります。
インストール	Safe Lock のインストール時にサードパーティのプログラムが検出されアンインストールされた場合は、インストールを続行する前に再起動する必要があります。

再起動が必要な場合	例
インストール	Safe Lock のインストール時にファイアウォールモジュールによって再起動が要求された場合は、インストールを続行する前に再起動する必要があります。
アンインストール	サポートツールを使用して Safe Lock エージェントをアンインストールした場合は、Safe Lock エージェントを再インストールする前に再起動する必要があります。

Safe Lock エージェントを別の Intelligent Manager に移行する方法について教えてください。

手順

1. 既存のエージェントからエクスポートおよびインポートすることによってエージェントの設定ファイルを収集します。

   手順の詳細については、263 ページの「設定ファイルをエクスポートまたはインポートする」を参照してください。

2. エクスポートした設定ファイルで、`<ManagedMode>` セクションの `Server` パラメータに移行先の Intelligent Manager を指定します。

3. 次のコマンドを入力して、設定ファイルを暗号化します。

   ```
   <TMSL>\SLCmd.exe encrypt managedmodeconfiguration test.xml
   test.xen
   ```

4. 次のコマンドを入力して、暗号化した設定ファイルと証明書を Intelligent Manager にインポートします。

   ```
   <TMSL>\SLCmd.exe set managedmode enable -cfg test.xen -sc
   trend.cer
   ```

エージェントがウイルスに感染した場合の対処方法

Trend Micro Portable Security を使用して、エージェントで許可リストをアップデートしたりアプリケーション制御を無効にすることなく、検出または削除することができます。

サポートが終了した SHA-1 証明書をエージェントで使用している場合はどうしたらいいですか?

Windows Vista 以前の OS を実行しているエージェントは、サポート終了日を過ぎた有効期限切れの SHA-1 証明書を使用して設定されている可能性があります。これにより、Trend Micro Safe Lock がインストールされているエージェントで Trend Micro Portable Security または Trend Micro USB Security を実行すると、問題が発生する場合があります。Trend Micro Portable Security または Trend Micro USB Security を問題なく実行するには、次の手順を実行します。

手順

1. エージェントで、Trend Micro Safe Lock の設定画面を表示します。

   詳細については、111 ページの「機能の設定を有効または無効にする」を参照してください。

2. [不正侵入対策] で [USB 不正プログラム対策] をオフにします。

3. [許可リスト] メニュー項目をクリックします。

4. 各製品に必要なすべてのモジュールを許可リストに追加します。

   - Trend Micro Portable Security のモジュールを許可リストに追加します。
   - Trend Micro USB Security のモジュールを許可リストに追加します。

   詳細については、102 ページの「ファイルを追加または削除する」を参照してください。

注意

必要なモジュールの判断については、テクニカルサポートにお問い合わせください。

5. Trend Micro Portable Security または Trend Micro USB Security を起動します。

   Trend Micro Portable Security または Trend Micro USB Security が問題なく実行されます。

第 12 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。

第 13 章

付録: 参照

この管理者ガイドでは、Trend Micro Safe Lock Intelligent Manager 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。

ローカル管理者アカウントを有効にする

Windows NT 6.x (Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows Server 2008、Windows Server 2012) および Windows NT 10.x (Windows 10、Windows Server 2016) では、ローカル Windows 管理者アカウントを使用できるようにするための特別な手順が必要です。

手順

1. [コンピューターの管理] を開きます。
   a. [スタート] メニューを開きます。
   b. [コンピューター] を右クリックします。
   c. [管理] を選択します。

      [コンピューターの管理] 画面が表示されます。
2. 左側のリストで、[コンピューターの管理] > [システム ツール] > [ローカル ユーザーとグループ] > [ユーザー] の順に選択します。

   ローカル Windows ユーザアカウントのリストが表示されます。
3. ユーザアカウントのリストで [Administrator] を右クリックし、[プロパティ] を選択します。

   [Administrator のプロパティ] 画面が表示されます。
4. [全般] タブで、[アカウントを無効にする] をオフにします。
5. [OK] をクリックします。

   [コンピューターの管理] 画面が再び表示され、ローカル Windows ユーザアカウントのリストが表示されます。
6. [Administrator] を右クリックして、[パスワードの設定...] を選択します。

   パスワード設定の手順を示すメッセージが表示されます。
7. パスワードを設定します。

8. [コンピューターの管理] を終了します。

ローカルアカウントの初期設定の共有を有効にする

Windows NT Version 6.x、Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows Server 2008、および Windows Server 2012 では、ローカル Windows 管理者アカウントを使用して初期設定の共有 (初期設定の共有された `admin$`など) にアクセスできるようにするための特別な手順が必要です。

ヒント

手順は Windows のバージョンによって異なります。お使いの Windows のバージョンに合わせた手順およびヘルプが必要な場合は、https://msdn.microsoft.com/ja-jp/default.aspx でマイクロソフトのサポート技術情報を参照してください。

手順

1. [レジストリ エディター] (`regedit.exe`) を開きます。
   a. [スタート] > [ファイル名を指定して実行] の順に選択します。
   b. 「`regedit`」と入力して <Enter> キーを押します。
2. 次のレジストリサブキーを探してクリックします。

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
   \Policies\System
   ```

3. レジストリエントリ `LocalAccountTokenFilterPolicy` を探します。

   このレジストリエントリがない場合は、次の手順を実行します。

   a. [編集] > [新規] の順に選択します。
   b. `[DWORD 値]` を選択します。
   c. 「`LocalAccountTokenFilterPolicy`」と入力して <Enter> キーを押します。

4. `LocalAccountTokenFilterPolicy` を右クリックして、[修正] を選択します。
5. [値のデータ] に「`1`」と入力します。
6. [OK] をクリックします。
7. [レジストリ エディター] を終了します。

エージェントのイベントログの説明

Trend Micro Safe Lock Intelligent Manager では、Safe Lock Intelligent Manager イベントログを表示するために Windows イベントビューアを使用します。イベントビューアにアクセスするには、[スタート] > [コントロール パネル] > [管理ツール] > [イベントビューア] の順にクリックします。

ヒント

イベントログへの出力内容は、setup.ini もしくは設定ファイルにて変更することができます。

詳しくは 262 ページの「エージェント設定ファイルの操作」を参照してください

表 13-1. Windows イベントログの説明

イベント ID	タスクカテゴリ	レベル	ログの説明
1000	システム	情報	サービスが開始されました。
1001	システム	警告	サービスが停止されました。
1002	システム	情報	アプリケーション制御が有効になりました。
1003	システム	警告	アプリケーション制御が無効になりました。
1004	システム	情報	無効化されました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1005	システム	情報	管理者パスワードが変更されました。
1006	システム	情報	制限付きユーザのパスワードが変更されました。
1007	システム	情報	制限付きユーザのアカウントが有効になりました。
1008	システム	情報	制限付きユーザのアカウントが無効になりました。
1009	システム	情報	製品が有効になりました。
1010	システム	情報	製品が無効になりました。
1011	システム	警告	ライセンスの有効期限が終了しています。猶予期間が有効になりました。
1012	システム	警告	ライセンスの有効期限が終了しています。猶予期間が終了しました。
1013	システム	情報	製品の設定のインポートを開始しました: %path%
1014	システム	情報	製品の設定のインポートが完了しました: %path%
1015	システム	情報	製品の設定のエクスポート先: %path%
1016	システム	情報	USB 不正プログラム対策が [許可] に設定されました。
1017	システム	情報	USB 不正プログラム対策が [ブロック] に設定されました。
1018	システム	情報	USB 不正プログラム対策が有効になりました。
1019	システム	警告	USB 不正プログラム対策が無効になりました。
1020	システム	情報	ネットワークウイルス対策が [許可] に設定されました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1021	システム	情報	ネットワークウイルス対策が [ブロック] に設定されました。
1022	システム	情報	ネットワークウイルス対策が有効になりました。
1023	システム	警告	ネットワークウイルス対策が無効になりました。
1025	システム	情報	メモリのランダム化が有効になりました。
1026	システム	警告	メモリのランダム化が無効になりました。
1027	システム	情報	API フッキング対策が [許可] に設定されました。
1028	システム	情報	API フッキング対策が [ブロック] に設定されました。
1029	システム	情報	API フッキング対策が有効になりました。
1030	システム	警告	API フッキング対策が無効になりました。
1031	システム	情報	DLL インジェクション対策が [許可] に設定されました。
1032	システム	情報	DLL インジェクション対策が [ブロック] に設定されました。
1033	システム	情報	DLL インジェクション対策が有効になりました。
1034	システム	警告	DLL インジェクション対策が無効になりました。
1035	システム	情報	事前指定による許可リスト自動更新が有効になりました。
1036	システム	情報	事前指定による許可リスト自動更新が無効になりました。
1037	システム	情報	DLL/ドライバ制御が有効になりました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1038	システム	警告	DLL/ドライバ制御が無効になりました。
1039	システム	情報	スクリプト制御が有効になりました。
1040	システム	警告	スクリプト制御が無効になりました。
1041	システム	情報	スクリプトが追加されました。 [詳細] ファイル拡張子: %extension% インタープリタ: %interpreter%
1042	システム	情報	スクリプトが削除されました。 [詳細] ファイル拡張子: %extension% インタープリタ: %interpreter%
1044	システム	情報	除外パスが有効になりました。
1045	システム	情報	除外パスが無効になりました。
1047	システム	情報	信頼するデジタル証明書が有効になりました。
1048	システム	情報	信頼するデジタル証明書が無効になりました。
1049	システム	情報	書き込み制御が有効になりました。
1050	システム	警告	書き込み制御が無効になりました。
1051	システム	情報	書き込み制御が [許可] に設定されました。
1052	システム	情報	書き込み制御が [ブロック] に設定されました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1055	システム	情報	書き込み制御リストに追加されたファイル。 パス: %path%
1056	システム	情報	書き込み制御リストから削除されたファイル。 パス: %path%
1057	システム	情報	書き込み制御の除外リストに追加されたファイル。 パス: %path% プロセス: %process%
1058	システム	情報	書き込み制御の除外リストから削除されたファイル。 パス: %path% プロセス: %process%
1059	システム	情報	書き込み制御リストに追加されたフォルダ。 パス: %path% 範囲: %scope%
1060	システム	情報	書き込み制御リストから削除されたフォルダ。 パス: %path% 範囲: %scope%
1061	システム	情報	書き込み制御の除外リストに追加されたフォルダ。 パス: %path% 範囲: %scope% プロセス: %process%

イベント ID	タスクカテゴリ	レベル	ログの説明
1062	システム	情報	書き込み制御の除外リストから削除されたフォルダ。 パス: %path% 範囲: %scope% プロセス: %process%
1063	システム	情報	書き込み制御リストに追加されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue%
1064	システム	情報	書き込み制御リストから削除されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue%
1065	システム	情報	書き込み制御の除外リストに追加されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% プロセス: %process%
1066	システム	情報	書き込み制御の除外リストから削除されたレジストリ値。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% プロセス: %process%
1067	システム	情報	書き込み制御リストに追加されたレジストリキー。 パス: %regkey% 範囲: %scope%

イベント ID	タスクカテゴリ	レベル	ログの説明
1068	システム	情報	書き込み制御リストから削除されたレジストリキー。 パス: %regkey% 範囲: %scope%
1069	システム	情報	書き込み制御の除外リストに追加されたレジストリキー。 パス: %regkey% 範囲: %scope% プロセス: %process%
1070	システム	情報	書き込み制御の除外リストから削除されたレジストリキー。 パス: %regkey% 範囲: %scope% プロセス: %process%
1071	システム	情報	カスタム処理が [無視] に設定されました。
1072	システム	情報	カスタム処理が [隔離] に設定されました。
1073	システム	情報	カスタム処理が [Intelligent Manager で確認する] に設定されました
1074	システム	情報	隔離ファイルが復元されました。 [詳細] 元の場所: %path% ソース: %source%

イベント ID	タスクカテゴリ	レベル	ログの説明
1075	システム	情報	隔離ファイルは削除されました。 [詳細] 元の場所: %path% ソース: %source%
1076	システム	情報	変更監視が有効になりました。
1077	システム	情報	変更監視が無効になりました。
1078	システム	情報	原因分析レポートに失敗しました。 [詳細] パス: %path%
1079	システム	情報	管理サーバの証明書のインポート先: %path%
1080	システム	情報	管理サーバの証明書のエクスポート先: %path%
1081	システム	情報	集中管理モードの設定のインポート先: %path%
1082	システム	情報	集中管理モードの設定のエクスポート先: %path%
1083	システム	情報	集中管理モードが有効になりました。
1084	システム	情報	集中管理モードが無効になりました。
1085	システム	情報	書き込み制御が有効の場合、書き込み制御リストと許可リストが対象に含まれます。
1086	システム	警告	書き込み制御が有効の場合、書き込み制御リストのみが対象になります。
1088	システム	情報	Windows Update サポートが有効になりました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1089	システム	情報	Windows Update サポートが無効になりました。
1094	システム	情報	Trend Micro Safe Lock がアップデートされました。 適用されたファイル: %file_name%
1096	システム	情報	信頼するハッシュリストが有効になりました。
1097	システム	情報	信頼するハッシュリストが無効になりました。
1099	システム	情報	ストレージデバイスのアクセスが [許可] に設定されました
1100	システム	情報	ストレージデバイスのアクセスが [ブロック] に設定されました
1101	システム	情報	ストレージデバイスのブロックが有効になりました
1102	システム	警告	ストレージデバイスのブロックが無効になりました

イベント ID	タスクカテゴリ	レベル	ログの説明
1103	システム	情報	イベントログの設定が変更されました。 [詳細] Windows イベントログ: %ON|off% レベル: 警告ログ: %ON|off% 情報ログ: %ON|off% システムログ: %ON|off% 除外パスログ: %ON|off% 書き込み制御ログ: %ON|off% リストログ: %ON|off% 許可されたアクセスのログ: Dll ドライバログ: %ON|off% アップデートプログラムのログ: %ON|off% 除外パスログ: %ON|off% 信頼するデジタル証明書のログ: %ON|off% 信頼するハッシュのログ: %ON|off% 書き込み制御ログ: %ON|off% ブロックされたアクセスのログ: %ON|off% USB 不正プログラム対策ログ: %ON|off% 実行防止対策のログ: %ON|off% ネットワークウイルス対策のログ: %ON|off%

イベント ID	タスクカテゴリ	レベル	ログの説明
			変更監視ログ ファイル作成ログ: %ON|off% ファイル変更ログ: %ON|off% ファイル削除ログ: %ON|off% ファイル名変更ログ: %ON|off% RegValue 変更ログ: %ON|off% RegValue 削除ログ: %ON|off% RegKey 作成ログ: %ON|off% RegKey 削除ログ: %ON|off% RegKey 名前変更ログ: %ON|off% デバイスコントロールのログ: %ON|off% デバッグログ: %ON|off%
1104	システム	警告	このバージョンの Windows ではメモリのランダム化は使用できません。
1105	システム	情報	ファイルのブロック通知が有効になりました。
1106	システム	情報	ファイルのブロック通知が無効になりました。
1107	システム	情報	管理者パスワードがリモートで変更されました。
1111	システム	情報	ファイルレス攻撃対策が有効になりました。
1112	システム	警告	ファイルレス攻撃対策が無効になりました。
1500	リスト	情報	許可リスト自動更新が開始されました。
1501	リスト	情報	許可リスト自動更新が停止されました。

イベント ID	タスクカテゴリ	レベル	ログの説明
1502	リスト	情報	許可リストのインポートを開始しました: %path%
1503	リスト	情報	許可リストのインポートが完了しました: %path%
1504	リスト	情報	許可リストのエクスポート先: %path%
1505	リスト	情報	許可リストに追加されました: %path%
1506	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストに追加されました: %path%
1507	リスト	情報	許可リストから削除されました: %path%
1508	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストから削除されました: %path%
1509	リスト	情報	許可リストがアップデートされました: %path%
1510	リスト	情報	許可済みインストーラまたはアップデートプログラムのリストがアップデートされました: %path%
1511	リスト	警告	許可リストに対して追加またはアップデートを実行できません: %path%
1512	リスト	警告	許可済みインストーラまたはアップデートプログラムのリストに対して追加またはアップデートを実行できません: %path%
1513	システム	情報	除外パスリストに追加されました。 [詳細] 種類: %exceptionpathtype% パス: %exceptionpath%

イベント ID	タスクカテゴリ	レベル	ログの説明
1514	システム	情報	除外パスリストから削除されました。 [詳細] 種類: %exceptionpathtype% パス: %exceptionpath%
1515	システム	情報	信頼するデジタル証明書リストに追加されました。 [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 件名: %subject% 発行者: %issuer%
1516	システム	情報	信頼するデジタル証明書リストから削除されました。 [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 件名: %subject% 発行者: %issuer%

イベント ID	タスクカテゴリ	レベル	ログの説明
1517	システム	情報	信頼するハッシュリストに追加されました。%n [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 許可リストに追加: %yes|no% パス: %path% メモ: %note%
1518	システム	情報	信頼するハッシュリストから削除されました。%n [詳細] ラベル: %label% ハッシュ: %hashvalue% 種類: %type% 許可リストに追加: %yes|no% パス: %path% メモ: %note%
1519	リスト	情報	許可リストからリモートで削除されました: %path%
1520	リスト	警告	%1 でファイルの列挙中に予期しないエラーが発生したため、許可リストを作成できません。%n エラーコード: %2 %n

イベント ID	タスクカテゴリ	レベル	ログの説明
1521	システム	情報	ファイルレス攻撃対策の除外を追加しました。 [詳細] ラベル: %label% 対象プロセス: %process_name% 引数: %arguments% %regex_flag% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path%
1522	システム	情報	ファイルレス攻撃対策の除外を削除しました。 [詳細] ラベル: %label% 対象プロセス: %process_name% 引数: %arguments% %regex_flag% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path%

イベント ID	タスクカテゴリ	レベル	ログの説明
2000	許可されたアクセス	情報	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% リスト: %list%
2001	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% ファイルハッシュが許可されました: %hash%
2002	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 許可リストの確認中にファイルパスを取得できません。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2003	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 許可リストの確認中にハッシュを計算できません。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2004	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% プロセスを監視するための通知を取得できません。
2005	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% プロセスを例外リスト以外に追加できません。
2006	許可されたアクセス	情報	ファイルのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2007	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 除外パスリストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2008	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 信頼するデジタル証明書リストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2011	許可されたアクセス	情報	レジストリのアクセスが許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2012	許可されたアクセス	情報	レジストリのアクセスが許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2013	許可されたアクセス	情報	除外リストによってファイル/フォルダの変更が許可されました。%path% [詳細] パス: アクセスユーザ: %username% モード: %mode%
2015	許可されたアクセス	情報	除外リストによってレジストリ値の変更が許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2016	許可されたアクセス	情報	除外リストによってレジストリキーの変更が許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2017	許可されたアクセス	警告	ファイル/フォルダの変更が許可されました。%path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2019	許可されたアクセス	警告	レジストリ値の変更が許可されました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%

イベント ID	タスクカテゴリ	レベル	ログの説明
2020	許可されたアクセス	警告	レジストリキーの変更が許可されました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2021	許可されたアクセス	警告	ファイルのアクセスが許可されました: %path% 信頼するハッシュリストの確認中にエラーが発生しました。 [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2022	許可されたアクセス	警告	ファイルレス攻撃対策によりプロセスが許可されました: %path% %argument% [詳細] アクセスユーザ: %username% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path% モード: アプリケーション制御が無効の状態 理由: %reason%

イベント ID	タスクカテゴリ	レベル	ログの説明
2503	ブロックされたアクセス	警告	ファイル/フォルダの変更がブロックされました。%path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2505	ブロックされたアクセス	警告	レジストリ値の変更がブロックされました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2506	ブロックされたアクセス	警告	レジストリキーの変更がブロックされました。 レジストリキー: %regkey% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2507	ブロックされたアクセス	情報	指定した処理が実行されました: %path% [詳細] 操作: %action% ソース: %source%

イベント ID	タスクカテゴリ	レベル	ログの説明
2508	ブロックされたアクセス	警告	指定された処理の実行に失敗しました: %path% [詳細] 操作: %action% ソース: %source%
2509	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% 理由: 許可リスト内に存在しません。 ファイルハッシュがブロックされました: %hash%
2510	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode% 理由: 計算されたハッシュ値が、保存されている値と一致しません。 ファイルハッシュがブロックされました: %hash%

イベント ID	タスクカテゴリ	レベル	ログの説明
2511	ブロックされたアクセス	情報	ファイル/フォルダの変更がブロックされました。%path% [詳細] パス: %path% アクセスユーザ: %username% モード: %mode%
2512	ブロックされたアクセス	警告	レジストリ値の変更がブロックされました。 レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスユーザ: %username% **注意** イベント ID 2512 は、サービス作成対策機能を有効にすることに起因します。

イベント ID	タスクカテゴリ	レベル	ログの説明
2513	ブロックされたアクセス	警告	ファイルレス攻撃対策によりプロセスがブロックされました: %path% %argument% [詳細] アクセスユーザ: %username% 親プロセス 1 のパス: %path% 親プロセス 2 のパス: %path% 親プロセス 3 のパス: %path% 親プロセス 4 のパス: %path% モード: アプリケーション制御が有効の状態 理由: %reason%
2514	ブロックされたアクセス	警告	ファイルのアクセスがブロックされました: %BLOCKED_FILE_PATH% [詳細] パス: %PARENT_PROCESS_PATH% アクセスユーザ: %USER_NAME% 理由: ブロックされたファイルは、大文字と小文字を区別する属性が有効になっているフォルダ内にあります。
3000	USB 不正プログラム対策	警告	デバイスのアクセスが許可されました: %path% [詳細] パス: %path% アクセスユーザ: %username% デバイスタイプ: %type%

イベント ID	タスクカテゴリ	レベル	ログの説明
3001	USB 不正プログラム対策	警告	デバイスのアクセスがブロックされました: %path% [詳細] パス: %path% アクセスユーザ: %username% デバイスタイプ: %type%
3500	ネットワークウイルス対策	警告	ネットワークウイルスが許可されました: %name% [詳細] プロトコル: TCP 送信元 IP アドレス: %ip_address% 送信元ポート: %port% 送信先 IP アドレス: %ip_address% 送信先ポート: 80
3501	ネットワークウイルス対策	警告	ネットワークウイルスがブロックされました: %name% [詳細] プロトコル: TCP 送信元 IP アドレス: %ip_address% 送信元ポート: %port% 送信先 IP アドレス: %ip_address% 送信先ポート: 80

イベント ID	タスクカテゴリ	レベル	ログの説明
4000	プロセス保護イベント	警告	API フッキング/DLL インジェクションが許可されました: %path% [詳細] パス: %path% ユーザ: %username%
4001	プロセス保護イベント	警告	API フッキング/DLL インジェクションがブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4002	プロセス保護イベント	警告	API フッキング対策が許可されました: %path% [詳細] パス: %path% ユーザ: %username%
4003	プロセス保護イベント	警告	API フッキング対策がブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4004	プロセス保護イベント	警告	DLL インジェクションが許可されました: %path% [詳細] パス: %path% ユーザ: %username%

イベント ID	タスクカテゴリ	レベル	ログの説明
4005	プロセス保護イベント	警告	DLL インジェクションがブロックされました: %path% [詳細] パス: %path% ユーザ: %username%
4500	システム内の変更	情報	作成されたファイル/フォルダ: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4501	システム内の変更	情報	変更されたファイル: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4502	システム内の変更	情報	削除されたファイル/フォルダ: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%

イベント ID	タスクカテゴリ	レベル	ログの説明
4503	システム内の変更	情報	名前が変更されたファイル/フォルダ: %path% 新しいパス: %path% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4504	システム内の変更	情報	変更されたレジストリ値: レジストリキー: %regkey% レジストリ値の名前: %regvalue% レジストリ値の種類: %regvaluetype% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4505	システム内の変更	情報	削除されたレジストリ値: レジストリキー: %regkey% レジストリ値の名前: %regvalue% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%

イベント ID	タスクカテゴリ	レベル	ログの説明
4506	システム内の変更	情報	作成されたレジストリキー: レジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4507	システム内の変更	情報	削除されたレジストリキー: レジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%
4508	システム内の変更	情報	名前が変更されたレジストリキー: レジストリキー: %regkey% 新しいレジストリキー: %regkey% [詳細] パス: %path% アクセスプロセス ID: %pid% アクセスユーザ: %username%

エージェントのエラーコードの説明

このリストでは、Trend Micro Safe Lock で使用されるさまざまなエラーコードについて説明します。

表 13-2. Trend Micro Safe Lock のエラーコードの説明

コード	説明
0x00040200	操作に成功しました。
0x80040201	操作に失敗しました。
0x80040202	操作に失敗しました。
0x00040202	一部のみ操作に成功しました。
0x00040203	要求された機能はインストールされていません。
0x80040203	要求された機能はサポートされていません。
0x80040204	無効な引数です。
0x80040205	無効なステータスです。
0x80040206	メモリが不足しています。
0x80040207	ビジー状態です。要求は無視されました。
0x00040208	やりなおしてください。(通常はタスクの実行時間が長すぎる場合に出力されます)
0x80040208	システムにより予約済み。(未使用)
0x80040209	ファイルパスが長すぎます。
0x0004020a	システムにより予約済み。(未使用)
0x8004020b	システムにより予約済み。(未使用)
0x0004020c	システムにより予約済み。(未使用)
0x0004020d	システムにより予約済み。(未使用)
0x8004020d	システムにより予約済み。(未使用)
0x0004020e	再起動が必要です。
0x8004020e	予期しないエラーのため再起動が必要です。
0x0004020f	タスクの実行が許可されました。
0x8004020f	許可が拒否されました。

コード	説明
0x00040210	システムにより予約済み。(未使用)
0x80040210	無効または予期しないサービスモードです。
0x00040211	システムにより予約済み。(未使用)
0x80040211	要求されたタスクは現在のステータスでは許可されていません。ライセンスを確認してください。
0x00040212	システムにより予約済み。(未使用)
0x00040213	システムにより予約済み。(未使用)
0x80040213	パスワードが一致しません。
0x00040214	システムにより予約済み。(未使用)
0x80040214	システムにより予約済み。(未使用)
0x00040215	見つかりません。
0x80040215	「必要ですが見つかりません。」
0x80040216	認証がロックされています。
0x80040217	パスワードの長さが無効です。
0x80040218	パスワードに無効な文字が含まれています。
0x00040219	パスワードが重複しています。管理者と制限付きユーザのパスワードは同一にできません。
0x80040220	システムにより予約済み。(未使用)
0x80040221	システムにより予約済み。(未使用)
0x80040222	システムにより予約済み。(未使用)
0x80040223	ファイルが見つかりません (予想どおりでエラーではありません)。
0x80040224	システムにより予約済み。(未使用)
0x80040225	システムにより予約済み。(未使用)
0x80040240	ライブラリが見つかりません。

コード	説明
0x80040241	ライブラリ関数で無効なライブラリステータスまたは予期しないエラーが発生しました。
0x80040260	システムにより予約済み。(未使用)
0x80040261	システムにより予約済み。(未使用)
0x80040262	システムにより予約済み。(未使用)
0x80040263	システムにより予約済み。(未使用)
0x80040264	システムにより予約済み。(未使用)
0x00040265	システムにより予約済み。(未使用)
0x80040265	システムにより予約済み。(未使用)
0x80040270	システムにより予約済み。(未使用)
0x80040271	システムにより予約済み。(未使用)
0x80040272	システムにより予約済み。(未使用)
0x80040273	システムにより予約済み。(未使用)
0x80040274	システムにより予約済み。(未使用)
0x80040275	システムにより予約済み。(未使用)
0x80040280	アクティベーションコードが無効です。
0x80040281	アクティベーションコードの形式が正しくありません。

サーバのイベントログの説明

[サーバイベント] 画面を表示するには、管理サーバ画面の上部にあるナビゲーションで [ログとレポート] > [サーバイベント] の順に選択します。

表 13-3. サーバのイベントログの説明

イベント ID	サーバイベント	説明
1001	コンソールにログオン	管理サーバ画面にログオンしました
1002	コンソールからログオフ	管理サーバ画面からログオフしました
1003	セッションタイムアウト	管理サーバ画面のセッションがタイムアウトしました。アカウント「%user_name%」は自動的にログオフしました。
1011	レポートを送信できません	予約レポートを%email_address%に送信できません。
1012	通知を送信できません	通知を%email_address%に送信できません。
2001	アカウントの作成	Intelligent Manager アカウント「%user_name%」が作成されました
2002	アカウントの削除	Intelligent Manager アカウント「%user_name%」を削除しました
2003	アカウントの変更	Intelligent Manager アカウント「%user_name%」%field_name%を変更しました
3001	エージェントイベントログの削除 - 自動	エージェントイベントログの自動削除。
3002	エージェントイベントログの削除 - 手動	エージェントイベントログの手動削除。
3003	エージェントイベントログのバックアップ	エージェントイベントログの自動バックアップ。パス: %filepath%。
3004	サーバイベントログの削除 -自動	サーバイベントログの自動削除。
3005	サーバイベントログの削除 -手動	サーバイベントログの手動削除。

イベント ID	サーバイベント	説明
3006	サーバイベントログのバックアップ	サーバイベントログの自動バックアップ。パス: %filepath%。
4001	許可されていないブロックされたファイルの処理	エージェントに要求を送信しました (ブロックされたファイルを許可リストに追加する)。ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (ブロックされたファイルを削除する)。ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (ブロックされたファイルを無視する)。ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (ファイルを隔離する)。ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1) エージェントに要求を送信しました (隔離されたファイルを復元する)。ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)
4002	処理済みとしてマーク	%num%件のイベントが処理済みとしてマークされました。
4003	未処理としてマーク	%num%件のイベントが未処理としてマークされました。
4004	隔離された不正ファイルの解除	エージェントに要求を送信しました (隔離されたファイルを復元する)。ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)
4005	隔離された不正ファイルの削除	エージェントに要求を送信しました (隔離されたファイルを削除する)。ファイル名: %file_name% ファイルハッシュ: %file_hash% (SHA-1)

イベント ID	サーバイベント	説明
4006	許可されていないファイルレス攻撃の処理	エージェントに要求を送信しました (ブロックされたプロセスチェーンとコマンド引数の組み合わせを追加する)。プロセスチェーン: %process_name% コマンド引数: %parameter% エージェントに要求を送信しました (ブロックされたプロセスチェーンとコマンド引数の組み合わせを無視する)。プロセスチェーン: %process_name% コマンド引数: %parameter%
5001	アプリケーション制御の有効化	エージェントのアプリケーション制御を有効化しました。
5002	アプリケーション制御の無効化	エージェントのアプリケーション制御を無効化しました。
5011	信頼するファイルのハッシュを追加しました	エージェントに信頼するファイルのハッシュを 1 個追加しました。 エージェントに信頼するファイルのハッシュを%num%個追加しました。
5013	許可されたファイルの削除	指定された項目をエージェントの許可リストから SLtasks.exe を使用して削除しました。
5021	ストレージデバイスのアクセスをブロックしました	エージェントでストレージデバイスのアクセスをブロックしました。
5023	ストレージデバイスのアクセスを許可しました	エージェントでストレージデバイスのアクセスを許可しました。
5601	エージェントの設定のエクスポート	ファイル (%file_desc%) をエージェント%endpoint_name%からエクスポートしました。
5602	エージェントの設定のインポート	ファイル (%file_desc%) をエージェントにインポートしました。
5800	エージェントの管理者パスワードの変更	エージェントのパスワードを変更しました。

イベント ID	サーバイベント	説明
5900	エージェントの許可リストの更新	エージェントの許可リストを更新しました。
6001	エージェントに Patch を配信	エージェントに Patch を配信します。Patch 名: %patch_name%

索引

か