



Trend Micro Safe Lock™ Intelligent Manager 1.1 インストールガイド

TXOne Edition



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/end-of-support/default.aspx>

著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

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 NAS Security、Trend Micro Data Loss Prevention、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、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、および Smart Check 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。

Copyright © 2020 Trend Micro Incorporated. All rights reserved.

P/N: SLEM08836/191007_JP (2020/04)

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、お客様の製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客様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。

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



重要

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

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客様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

はじめに	xi
ドキュメントについて	xi
対象読者	xii
ドキュメントの表記規則	xii
用語	xii

第 1 章 : 本製品の概要

Trend Micro Safe Lock Intelligent Manager について	16
新機能	16
サーバの機能と特徴	17
Safe Lock Intelligent Manager の要件	19
サーバアカウントの概要	19
Trend Micro Safe Lock について	22
新機能	22
エージェントの機能と特徴	23
Safe Lock エージェントの要件	25
エージェント利用時の概要	27

第 2 章 : Intelligent Manager のインストール準備

Trend Micro Safe Lock 構築フロー	30
インストール前の確認事項	33
データベースの要件	33
サーバホストの選択	34
サーバで要求されるパフォーマンス	35
サーバの OS とコンポーネント	35
Windows Server 2012 および 2016 のコンポーネントを準備する	36
Windows Server 2008 のコンポーネントを準備する	37

Windows 8 および Windows 10 のコンポーネントを準備する	40
Windows 7 のコンポーネントを準備する	42
サーバで使用されるポート	43
既存のデータベースを移行する	44
既存のデータベースをエクスポートする	45
データベースをインポートする	47
既存のデータベースに接続する	49
Intelligent Manager プログラムを新しいサーバコンピュータに移行する	50
サーバインストールのチェックリスト	51

第 3 章 : Intelligent Manager のインストール

セットアップの流れ	54
Safe Lock Intelligent Manager サーバのインストール	58
[データベースの設定] 画面	60
[サーバの識別方法の選択] 画面	65
[ネットワークの設定] 画面	66
インストール先フォルダの指定と [サーバ通信用ポート] 画面	68
管理サーバ画面の管理者アカウントのパスワードについて	69
フェイルオーバークラスタを設定する	69

第 4 章 : Intelligent Manager のアンインストール

Intelligent Manager の削除を準備する	76
Intelligent Manager をアンインストールする	77

第 5 章 : テクニカルサポート

トラブルシューティングのリソース	80
サポートポータルの利用	80
脅威データベース	80
製品サポート情報	81
サポートサービスについて	81

トレンドマイクロへのウイルス解析依頼	81
メールレピュテーションについて	82
ファイルレピュテーションについて	82
Web レピュテーションについて	83
その他のリソース	83
最新版ダウンロード	83
脅威解析・サポートセンター TrendLabs (トレンドラボ)	83

索引

索引	85
----------	----

はじめに

このインストールガイドでは、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。

- [xi ページの「ドキュメントについて」](#)
- [xii ページの「対象読者」](#)
- [xii ページの「ドキュメントの表記規則」](#)
- [xii ページの「用語」](#)

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®s=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。
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 TXOne Edition 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。

- 16 ページの「Trend Micro Safe Lock Intelligent Manager について」
- 22 ページの「Trend Micro Safe Lock について」

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 TXOne Edition 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 TXOne Edition の新機能

機能	説明
許可リストのエクスポートの強化	許可リストのエクスポート機能で、ファイルが追加または変更された時間がリストに含まれるようになります。
検索フィルタの強化	エージェントの検索フィルタに次の機能が含まれるようになります。 <ul style="list-style-type: none">エージェント名の部分検索システム時間がサーバのシステム時間よりも遅い登録済みエージェントの表示
新しいシステムイベントログ	このリリースの Safe Lock Intelligent Manager では、Intelligent Manager コンポーネントのアップデート用に新しいイベントログが作成されます。

機能	説明
不正プログラム検索	<p>Intelligent Manager の管理サーバ画面からエージェントの手動検索と予約検索を実行できます。</p> <hr/> <p> 注意</p> <p>この機能を使用するには、別途ライセンスが必要になります。正しいアクティベーションコードがあることを確認してから使用してください。アクティベーションコードの取得方法の詳細については、販売代理店にお問い合わせください。</p>

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。

機能	特徴
エージェントの集中管理	<p>Trend Micro Intelligent Manager では、管理者は次のタスクを実行できます。</p> <ul style="list-style-type: none">• 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有効化または無効化• エージェントのデバイスコントロールの有効化または無効化• エージェントのメンテナンスモードの設定• エージェントコンポーネントのアップデート• 許可リストの初期化• エージェントへの Patch の配信• 信頼するファイルおよび USB デバイスの追加
イベントの集中管理	<p>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。</p>
原因情報の分析	<p>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なかどうか、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。</p>

機能	特徴
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。
不正プログラム検索	セキュリティリスクとは、ウイルス/不正プログラムおよびスパイウェア/グレーウェアの総称です。Safe Lock Intelligent Manager はファイルを検索し、検出された各セキュリティリスクに特定の処理を実行することで、エージェントをセキュリティリスクから保護します。通知とログは、ユーザがセキュリティリスクを追跡し、ただちに処理が必要かどうか確認する際に役立ちます。

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> なし <hr/>  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	<ul style="list-style-type: none"> 管理者 フルコントロール
4	サーバイベントログの監視	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 管理者
8	Safe Lock Intelligent Manager のライセンス情報の更新	<ul style="list-style-type: none">• 管理者• フルコントロール
9	エージェントへの Patch の配信	<ul style="list-style-type: none">• 管理者• フルコントロール
10	信頼するファイルの追加	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 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
14	信頼する USB デバイスの追加	<ul style="list-style-type: none"> • 管理者 • フルコントロール
15	メンテナンスモードの設定	<ul style="list-style-type: none"> • 管理者 • フルコントロール
16	エージェントコンポーネントのアップデート	<ul style="list-style-type: none"> • 管理者 • フルコントロール
17	エージェントの移動	<ul style="list-style-type: none"> • 管理者 • フルコントロール

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 TXOne Edition 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 TXOne Edition の新機能

機能	説明
エージェント/サーバ間通信の強化	Safe Lock のエージェント/サーバ間通信で、固定 IP アドレスの Safe Lock エージェントがサポートされるようになります。
新しい OS のサポート	Safe Lock エージェントのインストールで、次の OS がサポートされます。 <ul style="list-style-type: none"> • Microsoft Windows 10 May 2019 Update (19H1) • Microsoft Windows 10 November 2019 Update (19H2) • Microsoft Windows 10 20H1
不正プログラム検索	Safe Lock エージェントで不正プログラム検索を手動で実行できる検索機能が提供されます。
イベント処理の強化	Safe Lock のデータフローとシステム機能の処理が強化され、システム操作の効率性が向上します。

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。

許可リストの管理

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、次のいずれかの方法を使用することで、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、ロック解除の操作を実施する必要はありません。

- メンテナンスモード
- 許可リスト自動更新
- 事前指定による許可リスト自動更新リスト
- コマンドラインインタフェース (CLI):
 - 信頼するハッシュ
 - 信頼する証明書

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。

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



注意

このバージョンの Safe Lock では、次のバージョンからのアップグレードがサポートされます。

- Safe Lock TXOne Edition



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®s=jp

表 1-4. Safe Lock エージェントの新規インストール



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	TXOne Edition 1.1	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	TXOne Edition 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
リモートインストール	TXOne Edition 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
 注意 Safe Lock では、Safe Lock Intelligent Manager Intelligent Manager のリモートセットアップツール (SLrst) を使用したリモートインストールがサポートされます。			

表 1-5. インストール後のエージェントのアップグレード

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
Patch パッケージ たとえば、 tmsl_txone_11_win_en.exe を実行します	<ul style="list-style-type: none"> TXOne Edition 1.0 TXOne Edition 1.1 	準備は不要です	互換性設定が保持されます

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	<ul style="list-style-type: none"> TXOne Edition 1.0 TXOne Edition 1.1 	準備は不要です	互換性設定が保持されます
 注意 Safe Lock では、Safe Lock Intelligent Manager Intelligent Manager からのリモート Patch 配信がサポートされます。			

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、ローカルまたはリモートの方法でアップデートできます。



注意

TXOne Edition のインストールパッケージでは、以前のバージョンの Safe Lock エージェントから TXOne Edition へのアップグレードがサポートされません。TXOne Edition の Safe Lock エージェントは、コンピュータに新規インストールする必要があります。

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。

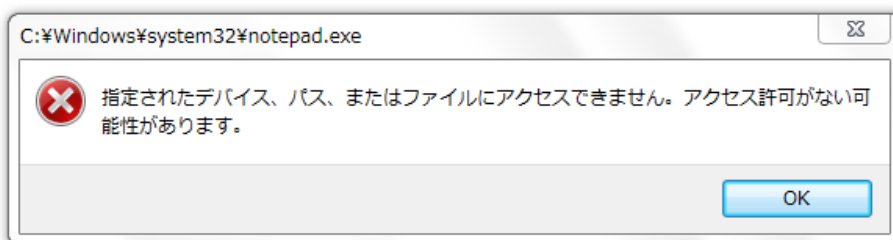


図 1-1. Trend Micro Safe Lock ブロックメッセージ

第 2 章

Intelligent Manager のインストール準備

この章では、Trend Micro Safe Lock Intelligent Manager の概要、インストールの推奨事項、およびシステム要件について説明します。

この章の内容は次のとおりです。

- 30 ページの「Trend Micro Safe Lock 構築フロー」
- 33 ページの「インストール前の確認事項」
- 35 ページの「サーバの OS とコンポーネント」
- 43 ページの「サーバで使用されるポート」
- 44 ページの「既存のデータベースを移行する」
- 50 ページの「Intelligent Manager プログラムを新しいサーバコンピュータに移行する」
- 51 ページの「サーバインストールのチェックリスト」

Trend Micro Safe Lock 構築フロー

始める前に

Trend Micro Safe Lock は最初に管理コンソールの環境を構築します。その後、エージェントのインストーラパッケージ (管理コンソールとの接続設定情報を含む) を管理コンソール上で作成し、エージェントのインストールを行います。

各作業の詳細は、以下を参照してください。

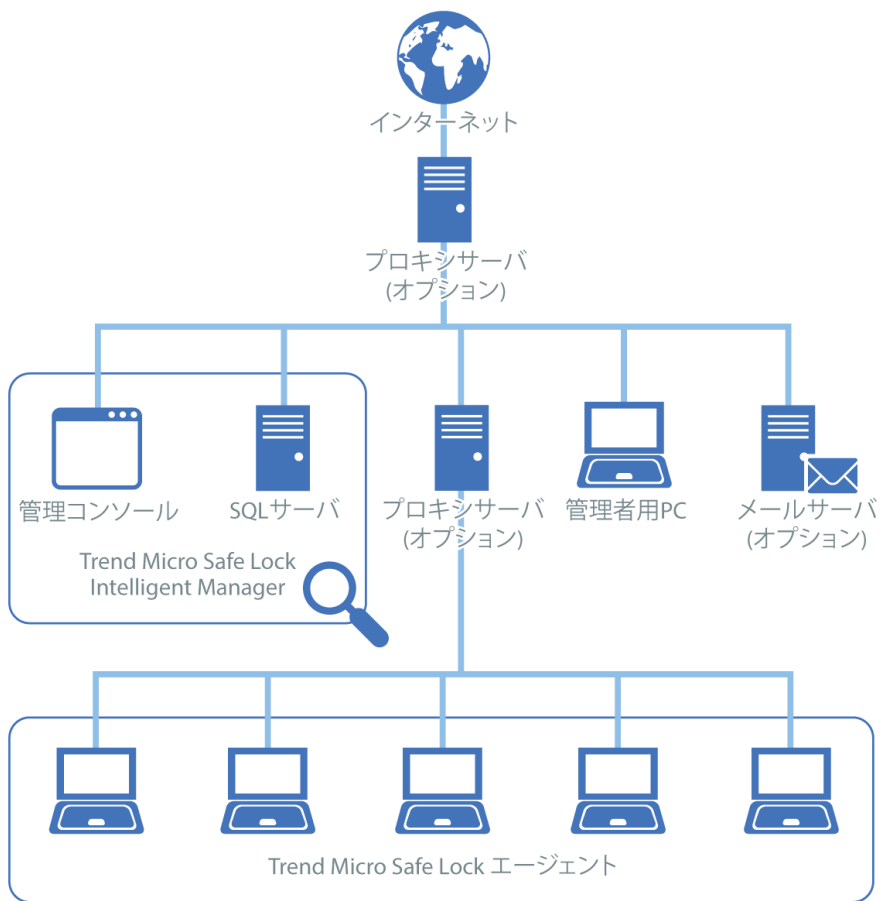


図 2-1. Trend Micro Safe Lock の基本構成

手順

1. Trend Micro Safe Lock Manager の構築

- インストール準備 (29 ページの [Intelligent Manager のインストール準備](#)を参照)
 - インストール (53 ページの [Intelligent Manager のインストール](#)を参照)
2. Safe Lock エージェントインストーラのカスタマイズ
- インストーラ準備 (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「エージェントインストーラパッケージの変更について」を参照)
3. エージェントのインストール
- エージェントのリモートインストール
- a. エージェントインストールの準備 (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「リモートインストールの考慮事項」を参照)
 - b. リモートインストール (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「リモートセットアップツール」を参照)
 - c. 初期許可リスト作成 (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「リモートタスクツール」を参照)
 - d. ロックダウン (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「リモートタスクツール」を参照)
- エージェントのローカルインストール
- a. モジュールダウンロード (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「最新のエージェントインストーラーパッケージをダウンロードする」を参照)
 - b. ローカルインストール (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「ローカルインストールの概要」を参照)
 - c. 初期許可リスト作成 (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「許可リストの設定」を参照)
 - d. ロックダウン (Trend Micro Safe Lock Intelligent Manager 管理者ガイド「エージェントのメイン画面について」を参照)
-

インストール前の確認事項

ここでは、Safe Lock Intelligent Manager サーバをインストールする前に確認する必要がある詳細事項を示します。

データベースの要件

Safe Lock Intelligent Manager では、データを Microsoft SQL データベースに保存します。このデータベースには収集されたログ、レポート、および管理下のすべてのエージェント情報が含まれます。

Safe Lock Intelligent Manager では、SQL データベースを管理するために次のいずれかが必要です。

- Microsoft SQL Server Standard Edition または Enterprise Edition



注意

- セキュリティ上の理由により、マイクロソフトでは SQL Server をドメインコントローラにインストールしないよう推奨しています。
http://msdn.microsoft.com/ja-JP/library/ms143506.aspx#DC_support
- Safe Lock Intelligent Manager では、SQL Server の混合モード認証がサポートされます。ただし、Windows 認証モードはサポートされません。

-
- Microsoft SQL 2008 Express

Safe Lock Intelligent Manager を、お使いの環境内で Microsoft SQL Server にアクセスできないサーバにインストールする場合、セットアップでは Microsoft SQL 2008 Express をインストールするオプションが提示されます。

**重要**

SQL Express 2008 は評価用の試験的な環境に適していますが、より大規模な本稼働環境には適していません。トレンドマイクロでは、Safe Lock Intelligent Manager で監視する大規模ネットワークには、Microsoft SQL Server Standard または Enterprise Edition を使用することをお勧めします。

Windows Server 2008 SP1 (32 ビットおよび 64 ビット) では、Safe Lock Intelligent Manager はサポートされますが、Microsoft SQL Express 2008 の必須コンポーネントである Microsoft .NET Framework 3.5 Service Pack 1 はサポートされません。

パフォーマンスの詳細については、[35 ページの「サーバで要求されるパフォーマンス」](#)を参照してください。

サーバホストの選択

インストール対象を選択する際は、次のことを確認してください。

- サーバ CPU で十分な処理能力があること
- サーバ上で実行するその他の機能

Safe Lock Intelligent Manager をインストールするコンピュータに別の役割がある場合は、次のいずれかを実行します。

- ミッションクリティカルなアプリケーション、またはリソースを大量消費するアプリケーションを実行していないことを確認します。
- ミッションクリティカルなアプリケーション、またはリソースを大量消費するアプリケーションを実行しない、別のホストを選択します。
- Safe Lock Intelligent Manager と Safe Lock エージェントを同じコンピュータにインストールする際には、Safe Lock Intelligent Manager を先にインストールする必要があります。Safe Lock エージェントは、Safe Lock Intelligent Manager のインストールが完了した後にインストールしてください。

**重要**

Safe Lock 1.x のエージェントでは、Safe Lock Intelligent Manager はブロックされインストールできません。

サーバで要求されるパフォーマンス

Safe Lock Intelligent Manager は接続されるエージェントの数によっては、多くの処理能力やネットワーク帯域を必要とすることがあります。

**ヒント**

トレンドマイクロ では、Safe Lock Intelligent Manager サーバには少なくとも 2GHz 以上のデュアルコアプロセッサと 4GB 以上の RAM を推奨しています。

単一の Safe Lock Intelligent Manager サーバで最大 100,000 台のエージェントをサポートできます。

ただし、単一の Safe Lock Intelligent Manager サーバのパフォーマンスは、使用可能なサーバリソースやネットワークトポロジなど、複数の要素に応じて決まります。お使いの Safe Lock Intelligent Manager サーバの環境で管理可能な最適なエージェント数を判断するには、トレンドマイクロのテクニカルサポートに問い合わせてください。

サーバの OS とコンポーネント

Safe Lock Intelligent Manager は、Microsoft Windows の多くのバージョンをサポートしています。そのため、Safe Lock Intelligent Manager では、お使いの Windows プラットフォームによってはさまざまなコンポーネントが必要となります。Safe Lock Intelligent Manager のセットアップを実行する前に、必要なコンポーネントを手動で有効化またはインストールして環境を準備してください。

**重要**

Microsoft SQL Express 2008 を使用する場合は、お使いのシステムが SQL Express 2008 の要件を満たすことを確認してください。詳細については、以下の Web サイトをご覧ください。

<http://www.microsoft.com/ja-JP/download/details.aspx?id=1695>

Safe Lock Intelligent Manager のセットアップを実行する前に必要なコンポーネントを準備するには、お使いの Windows バージョンに適した手順を確認します。

Windows Server 2012 および 2016 のコンポーネントを準備する

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 (SP なし) (64 ビット)
- Windows Server 2012 Foundation/Essentials/Standard/Datacenter (SP なし) (64 ビット)
- Windows Server 2012 Foundation/Essentials/Standard/Datacenter R2 (SP なし) (64 ビット)
- Windows Server 2012 R2 (SP なし) (64 ビット)
- Windows Server 2012 R2 for Embedded Systems (SP なし) (64 ビット)
- Windows Server 2016 Standard (64 ビット)
- Windows Storage Server 2016

手順

1. [サーバー マネージャ] > [ダッシュボード] > [役割と機能の追加] の順に選択します。
2. [インストールの種類の選択] 画面で、[役割ベースまたは機能ベースのインストール] を選択します。

3. 左側のメニューで [サーバーの役割] を選択します。
 4. 表示されるリストで [Web サーバー (IIS)] を選択します。
 5. 左側のメニューで [機能] を選択します。
 6. 表示されるリストで [メッセージキュー] を選択します。
 7. 左側のメニューで [サーバーの役割] を選択します。
 8. リスト内の次の機能を有効にします。
 - [Web サーバー (IIS)] を選択します。
 - [Web サーバー (IIS)] > [HTTP 共通機能] の順に選択し、[静的なコンテンツ] を選択します。
 - [Web サーバー(IIS)] > [アプリケーション開発] の順に選択し、次の項目を選択します。
 - Application Initialization
 - CGI
 - ASP.NET 3.5
 9. [インストール] をクリックし、プロセスが完了したら [閉じる] をクリックします。
-

Windows Server 2008 のコンポーネントを準備する

Windows Server 2008 R2 (SP なし/SP1) (64 ビット)

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 R2 (SP なし/SP1) (64 ビット)

手順

1. 次のいずれかのバージョンの Microsoft .NET Framework をダウンロードしてインストールします。

- 2.0 Service Pack 2

<https://www.microsoft.com/ja-jp/download/details.aspx?id=1639>

- 3.5 Service Pack 1

<http://www.microsoft.com/ja-JP/download/details.aspx?id=22>



注意

Safe Lock Intelligent Manager のインストール時に Microsoft SQL Server 2008 Express をインストールするには、まず、Microsoft .NET Framework 3.5 Service Pack 1 をダウンロードしてインストールします。

2. Application Initialization 1.0 for IIS 7.5 をダウンロードしてインストールします。
 - 32 ビット: <http://go.microsoft.com/fwlink/?LinkID=247816>
 - 64 ビット: <http://go.microsoft.com/fwlink/?LinkID=247817>
3. 次の Windows コンポーネントを有効にします。
 - a. [サーバー マネージャ] > [役割] > [役割の追加] の順に選択します。
 - b. 左側のメニューで [サーバーの役割] を選択します。
 - c. 表示されるリストで [Web サーバー (IIS)] を選択します。
 - d. 左側のメニューで [Web サーバー (IIS)] > [役割サービス] を選択します。
 - e. リスト内の次の機能を有効にします。
 - [Web サーバー] > [HTTP 共通機能] の順に選択し、[静的なコンテンツ] を選択します。
 - [Web サーバー] > [アプリケーション開発] の順に選択し、次の項目を選択します。

- CGI

- ASP.NET

- f. [インストール] をクリックし、プロセスが完了したら [閉じる] をクリックします。
- g. [サーバー マネージャ] に戻り、[機能] > [機能の追加] の順に選択します。
- h. 表示されるリストで [メッセージ キュー] を選択します。
- i. [インストール] をクリックし、プロセスが完了したら [閉じる] をクリックします。

Windows Server 2008 (SP1/SP2) (32 ビットおよび 64 ビット)

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 (SP1/SP2) (32 ビット/64 ビット)

手順

1. 次のいずれかのバージョンの Microsoft .NET Framework をダウンロードしてインストールします。
 - 2.0 Service Pack 2
<https://www.microsoft.com/ja-jp/download/details.aspx?id=1639>
 - 3.5 Service Pack 1
<https://www.microsoft.com/ja-jp/download/details.aspx?id=22>



重要

Windows Server 2008 SP1 (32 ビットおよび 64 ビット) では、Safe Lock Intelligent Manager はサポートされますが、Microsoft SQL Express 2008 の必須コンポーネントである Microsoft .NET Framework 3.5 Service Pack 1 はサポートされません。

2. 次の Windows コンポーネントを有効にします。
 - a. [サーバー マネージャ] > [役割] > [役割の追加] の順に選択します。
 - b. 左側のメニューで [サーバーの役割] を選択します。
 - c. 表示されるリストで [Web サーバー] を選択します。
 - d. 左側のメニューで [Web サーバー (IIS)] > [役割サービス] を選択します。
 - e. リスト内の次の機能を有効にします。
 - [Web サーバー (IIS)] > [HTTP 共通機能] の順に選択し、[静的なコンテンツ] を選択します。
 - [Web サーバー] > [アプリケーション開発] の順に選択し、次の項目を選択します。
 - CGI
 - ASPNET 3.5
 - f. [インストール] をクリックし、プロセスが完了したら [閉じる] をクリックします。
 - g. [サーバー マネージャ] に戻り、[機能] > [機能の追加] の順に選択します。
 - h. 表示されるリストで [メッセージキュー] を選択します。
 - i. [インストール] をクリックし、プロセスが完了したら [閉じる] をクリックします。
-

Windows 8 および Windows 10 のコンポーネントを準備する

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 8.1 Pro/Enterprise (SP なし) (32 ビット/64 ビット)

- Windows 8 Pro/Enterprise (SP なし) (32 ビット/64 ビット)
- Windows 10 Enterprise (32 ビット/64 ビット)
- Windows 10 IoT Enterprise (32 ビット/64 ビット)

手順

1. <Windows> キーを押しながら <R> キーを押して [ファイル名を指定して実行] ダイアログボックスを開き、次のコマンドを入力します。

Control Panel

コントロール パネルがクラシック表示で開きます。



注意

コントロール パネルを開くその他の方法の詳細については、次の URL を参照してください。

<https://support.microsoft.com/ja-jp/help/13764/windows-where-is-control-panel>

2. 現在の [表示方法] に応じて、次のいずれかをクリックします。
 - [カテゴリ] 表示の場合、[プログラム] をクリックします。
 - [大きいアイコン] または [小さいアイコン] 表示の場合、[プログラムと機能] をクリックします。
3. [Windows の機能の有効化または無効化] を選択します。
4. 新しい画面でリスト内の次の機能を有効にします。
 - [Microsoft メッセージ キュー (MSMQ) サーバー] を選択します。
 - [インターネット インフォメーション サービス] を選択し、[World Wide Web サービス] を選択します。
 - [インターネット インフォメーション サービス] > [World Wide Web サービス] > [HTTP 共通機能] の順に選択し、[静的なコンテンツ] を選択します。

- [インターネット インフォメーション サービス] > [World Wide Web サービス] > [アプリケーション開発機能] の順に選択し、次の項目を選択します。
 - Application Initialization
 - CGI
 - ASP.NET

5. [OK] をクリックしてプロセスが完了するまで待ちます。

Windows 7 のコンポーネントを準備する

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 Professional/Enterprise/Ultimate (SP なし/SP1) (32 ビット/64 ビット)

手順

1. Application Initialization 1.0 for IIS 7.5 をダウンロードしてインストールします。
 - 32 ビット: <http://go.microsoft.com/fwlink/?LinkID=247816>
 - 64 ビット: <http://go.microsoft.com/fwlink/?LinkID=247817>
2. <Windows> キーを押しながら <R> キーを押して [ファイル名を指定して実行] ダイアログボックスを開き、次のコマンドを入力します。

Control Panel

コントロール パネルがクラシック表示で開きます。

**注意**

コントロール パネルを開くその他の方法の詳細については、次の URL を参照してください。

<https://support.microsoft.com/ja-jp/help/13764/windows-where-is-control-panel>

3. 現在の [表示方法] に応じて、次のいずれかをクリックします。
 - [カテゴリ] 表示の場合、[プログラム] をクリックします。
 - [大きいアイコン] または [小さいアイコン] 表示の場合、[プログラムと機能] をクリックします。
4. [Windows の機能の有効化または無効化] を選択します。
5. 新しい画面でリスト内の次の機能を有効にします。
 - [Microsoft メッセージ キュー (MSMQ) サーバー] を選択します。
 - [インターネット インフォメーション サービス] を選択し、[World Wide Web サービス] を選択します。
 - [インターネット インフォメーション サービス] > [World Wide Web サービス] > [HTTP 共通機能] の順に選択し、[静的なコンテンツ] を選択します。
 - [インターネット インフォメーション サービス] > [World Wide Web サービス] > [アプリケーション開発機能] の順に選択し、次の項目を選択します。
 - CGI
 - ASP.NET
6. [OK] をクリックしてプロセスが完了するまで待ちます。

サーバで使用されるポート

次の表は、Safe Lock Intelligent Manager サーバで使用されるポートを示しています。

表 2-1. サーバで使用されるポート

ポート番号	目的
25	通知やレポートを送信するための SMTP サーバ接続
443 (初期設定)	管理サーバ画面への HTTPS 経由のアクセス
514	ログ転送用の Syslog サーバ接続
3128	コンポーネントアップデートとサーバ/エージェント間通信用のプロキシサーバ接続
8000 (初期設定)	エージェントステータスのアップデートとログの収集
8001 (初期設定)	検索用のエージェントファイルの収集
14336 (初期設定)	リモートエージェントのインストール

既存のデータベースを移行する

始める前に

このデータベース移行手順にはスタンドアロンの Microsoft SQL Server が必要です。



警告!

この手順では、既存のデータベースを 2 つの SQL サーバ間で移行します。たとえば、以前に Safe Lock Intelligent Manager のセットアップでインストールした Microsoft SQL Express の場所からスタンドアロンの Microsoft SQL Server に移行します。以前に Microsoft SQL Server をインストールしており、同じ Microsoft SQL Server を今回のインストールでも使用する場合は、この手順を省略します。

Safe Lock Intelligent Manager を再インストールする場合は、前にインストールしたときのデータを移行する必要がある場合があります。Safe Lock Intelligent Manager では、データを Microsoft SQL データベースに保存します。このデータベースには収集されたログ、レポート、および管理下のすべてのエージェント情報が含まれます。

これまで Microsoft SQL Express を使用して Safe Lock Intelligent Manager データベースを管理していた場合は、次の手順を使用してデータベースを Microsoft SQL Server に移行することをお勧めします。

手順

1. Microsoft SQL Server 2008 Management Studio Express をダウンロードしてインストールします。
 - a. マイクロソフトの Web サイト (<http://www.microsoft.com/ja-jp/download/details.aspx?id=7593>) からインストーラをダウンロードします。
 - b. Microsoft SQL Server 2008 Management Studio Express を、ソースデータベースを備えたコンピュータにインストールします。
2. 手順に従って、エクスポート元の Safe Lock Intelligent Manager データベースを備えたコンピュータからスクリプトをエクスポートします。

45 ページの「既存のデータベースをエクスポートする」を参照してください。



注意

Safe Lock Intelligent Manager データベースの初期設定の名前は SafeLock です。

-
3. 手順に従って、インポート先の SQL サーバコンピュータにデータベーススクリプトをインポートし、Safe Lock Intelligent Manager に接続します。

47 ページの「データベースをインポートする」を参照してください。

既存のデータベースをエクスポートする

手順

1. ソースデータベースを備えたコンピュータで、Microsoft SQL Server 2008 Management Studio を起動します。

[Microsoft SQL Server Management Studio] ソリューション画面が表示されます。

2. ソースデータベーススクリプトをエクスポートします。
 - a. [ファイル]>[データベース スクリプトのエクスポート] の順に選択します。

ソリューション画面に [オブジェクト エクスプローラー] 画面が表示されます。
 - b. [オブジェクト エクスプローラー] 画面にソースデータベースの位置が含まれていることを確認します。
 - c. エクスポート元の SQL サーバを選択して展開し、SafeLock データベースを表示します。
 - d. SafeLock データベースを右クリックして、[タスク]>[スクリプトの生成] の順に選択します。

[スクリプトの生成とパブリッシュ] 画面が表示されます。
 - e. 左側のメニューで [オブジェクトの選択] を選択します。
 - f. [データベース全体とすべてのデータベース オブジェクトのスクリプトを作成] を選択します。
 - g. [次へ>] をクリックします。
 - h. 次の項目を選択します。
 - スクリプトを指定した場所に保存
 - ファイルに保存
 - 単一ファイル
 - 既存のファイルの上書き
 - Unicode テキスト
 - i. ファイルを保存するパスを設定して書き留めておきます。
 - j. [詳細設定] をクリックします。

[スクリプト作成の詳細オプション] 画面が表示されます。

k. [全般] で次のように設定します。

- [ANSI Padding] を [False] に設定します。
- [サーバーのバージョン互換のスクリプト] を、インポート先の SQL サーバで使用する Microsoft SQL のバージョンに設定します。たとえば、[SQL Server 2012] を指定します。
- [スクリプトを作成するデータの種類] を [スキーマとデータ] に設定します。

l. [OK] をクリックします。

[スクリプトの保存方法またはパブリッシュ方法を指定してください。] 画面が再び表示されます。

m. [次へ] をクリックします。

n. 設定を確認し、[次へ] をクリックしてエクスポートプロセスを開始します。

[スクリプトの保存またはパブリッシュ] 画面が表示されます。ソース SQL データベースのデータがコンパイルされ、前述の手順で指定したパスのファイルに保存されます。

o. プロセスが正常に完了したら、[完了] をクリックします。

3. エクスポートされたファイルをインポートプロセスに使用します。

データベースをインポートする

手順

1. ソースデータベースを備えたコンピュータで、Microsoft SQL Server 2008 Management Studio を起動します。

[Microsoft SQL Server Management Studio] ソリューション画面が表示されます。

2. データベーススクリプトを、インポート先のコンピュータの Microsoft SQL Server にインポートします。
 - a. インポート先の SQL サーバを選択して展開し、[データベース] フォルダを表示します。
 - b. [データベース] フォルダをクリックして選択します。
 - c. [ファイル]>[開く]の順に選択します。
 - d. インポート先の既存の Safe Lock Intelligent Manager データベース用にエクスポートしたスクリプトファイルを開きます。

エディタ画面が開きます。

- e. 新しく作成するデータベースのコピーに応じて、対象データベースのフルパスをカスタマイズします。

次のスクリプト例で、データベースのパスを e:¥SQL_STORE
¥SafeLock.mdf に変更する場合を考えます。

```
NAME = N'SafeLock', FILENAME = N'd:\SafeLock.mdf'
```

ここでは、FILENAME パラメータを N'e:\SQL_STORE
¥SafeLock.mdf' に変更します。

- f. 新しく作成するデータベースのコピーに応じて、対象データベースのログのフルパスをカスタマイズします。

次のスクリプト例で、ログのパスを e:¥SQL_STORE
¥SafeLock_log.LDF に変更する場合を考えます。

```
NAME = N'SafeLock_log', FILENAME =  
N'd:\SafeLock_log.LDF'
```

ここでは、FILENAME パラメータを N'e:\SQL_STORE
¥SafeLock_log.LDF' に変更します。

- g. [実行] をクリックしてスクリプトを実行し、データベースをインポート先の SQL サーバにインポートします。

3. Safe Lock Intelligent Manager をすでにインストールしているかどうかに応じて、次の操作を実行します。

- まだセットアップを完了していない場合は、新しい SQL サーバのパスを書き留めておきます。インストールする前に、サーバインストールのチェックリストを完了させます。インストール時、[データベースの設定] セットアップ画面で [既存の Microsoft SQL Server を使用] を選択して、新しい SQL サーバのパスを指定します。

詳細については、次を参照してください。

- [51 ページの「サーバインストールのチェックリスト」](#)
- [60 ページの「\[データベースの設定\] 画面」](#)
- セットアップをすでに完了している場合は、新しくインポートしたデータベースに Safe Lock Intelligent Manager を接続します。

[49 ページの「既存のデータベースに接続する」](#) を参照してください。

既存のデータベースに接続する

Safe Lock Intelligent Manager は既存の Safe Lock Intelligent Manager データベースに接続できます。この機能を使用して、たとえばサーバコンピュータハードウェアの入れ替えの際などに、新しくインストールした Safe Lock Intelligent Manager を古いデータベースに接続します。



警告!

このプロセスでは、古い Safe Lock Intelligent Manager データベースの移行中に、現在インストールされている Safe Lock Intelligent Manager で新しいデータが蓄積されていた場合、そのデータが失われるリスクがあります。

セットアップを完了して Safe Lock Intelligent Manager の使用をすでに開始している場合は、新しく収集したログ、レポート、および管理下のすべてのエージェントのエージェント情報をエクスポートしてデータをバックアップします。古いデータベースの移行後、このデータをインポートします。データのエクスポートおよびインポートの詳細については、Safe Lock Intelligent Manager 管理者ガイドを参照してください。

Safe Lock Intelligent Manager のセットアップを完了したら、次の操作を実行します。

手順

1. Safe Lock Intelligent Manager のサーバコンピュータから、Windows の管理者権限を使用して次のコマンドを実行し、画面に表示される指示に従います。

```
<Safe_Lock_Intelligent_Manager_installation_path>CmdTools  
\Installer\Commands\ConfigSQLSetting.bat
```

Intelligent Manager プログラムを新しいサーバコンピュータに移行する

始める前に

Safe Lock Intelligent Manager プログラムを新しいサーバコンピュータに移行するために、Safe Lock エージェントで特別な準備をする必要はありません。



注意

Safe Lock Intelligent Manager が使用可能になってログやレポートを収集するまで、Safe Lock エージェントがログとレポートをローカルにキャッシュします。Safe Lock エージェントに十分なディスク空き容量がある場合、Safe Lock Intelligent Manager から数時間分離されたままになっても未収集のログやレポートは保持されます。

Safe Lock Intelligent Manager プログラムを新しいサーバコンピュータに移行するには、次の手順を実行します。

手順

1. Safe Lock Intelligent Manager を現在のサーバコンピュータからアンインストールします。

[77 ページの「Intelligent Manager をアンインストールする」](#)を参照してください。

2. アンインストールしたサーバで使用していたサーバ ID 設定 (「サーバの識別方法の選択」画面で入力した設定) を使用して、新しいサーバコンピュータに Safe Lock Intelligent Manager をインストールします。

65 ページの「[\[サーバの識別方法の選択\] 画面](#)」を参照してください。

サーバインストールのチェックリスト

Safe Lock Intelligent Manager のセットアップを実行する前に、次の手順を完了します。

- トrendマイクロから次のものを取得します。
 - Safe Lock Intelligent Manager のインストーラパッケージ
 - 製品版または体験版のアクティベーションコード使用可能な Safe Lock Intelligent Manager のバージョンの詳細については、付属するドキュメントを参照してください。
- 次の手順で環境を準備します。
 - 必要なソフトウェアコンポーネントがすべてインストールされていることを確認します。
35 ページの「[サーバの OS とコンポーネント](#)」を参照してください。
 - 必要なハードウェアおよびソフトウェアの仕様を確認します。
19 ページの「[Safe Lock Intelligent Manager の要件](#)」を参照してください。
 - 対象サーバに IP アドレスと DNS 設定が割り当てられていることを確認します。
- 次の情報を確認します。
 - Safe Lock Intelligent Manager のファイルのインストールパス
 - Safe Lock Intelligent Manager で、Safe Lock エージェントから収集したログ、レポート、およびエージェント情報の記録に使用するデータベースサーバ設定

60 ページの「[データベースの設定] 画面」を参照してください。

- Safe Lock エージェントが Safe Lock Intelligent Manager サーバを識別するための完全修飾ドメイン名 (FQDN)、ホスト名、または IP アドレス

65 ページの「[サーバの識別方法の選択] 画面」を参照してください。

- Safe Lock Intelligent Manager の管理サーバ画面の Web サーバ設定
Safe Lock Intelligent Manager サーバがエージェントとの通信に使用するポート番号

66 ページの「[ネットワークの設定] 画面」を参照してください。

- 初期設定の Safe Lock Intelligent Manager 管理者アカウントのパスワード

69 ページの「管理サーバ画面の管理者アカウントのパスワードについて」を参照してください。

これは、Safe Lock Intelligent Manager の管理サーバ画面へのログインに使用するアカウントです。

- Safe Lock Intelligent Manager がリモートエージェントインストールのインストールパッケージの配信に使用するポート番号

68 ページの「インストール先フォルダの指定と [サーバ通信用ポート] 画面」を参照してください。

準備が完了したら、サーバコンピュータで Safe Lock Intelligent Manager のセットアップを実行します。

第 3 章

Intelligent Manager のインストール

この章では、Trend Micro Safe Lock Intelligent Manager の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。

- 54 ページの「セットアップの流れ」
- 58 ページの「Safe Lock Intelligent Manager サーバのインストール」
- 69 ページの「フェイルオーバークラスタを設定する」

セットアップの流れ

Safe Lock Intelligent Manager サーバをインストールする際、セットアップでは次の情報の入力を求められます。







重要

Safe Lock Intelligent Manager のセットアップを実行する前に、51 ページの「サーバインストールのチェックリスト」のチェックリストを完了させます。


表 3-1. セットアップの流れと必要な情報

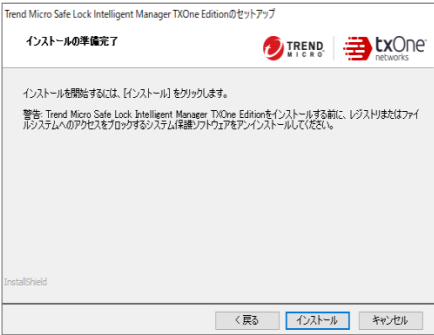
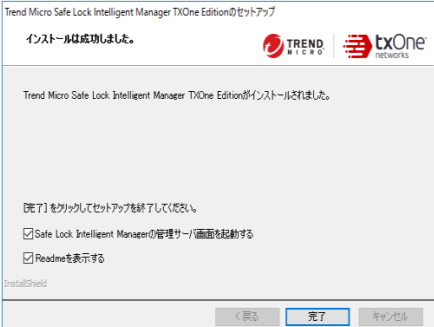
インストーラ画面	必要な情報
	なし
	なし

インストーラ画面	必要な情報
<p>Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ</p> <p>データベースの設定</p>  <p>Safe Lock Intelligent ManagerデータベースのSQLサーバのタイプを選択します。</p> <p><input checked="" type="radio"/> 既存のMicrosoft SQL Serverを使用 これは、Microsoft SQL Server (推奨) またはこのコンピュータでSafe Lock Intelligent Managerデータベースを管理している既存のSQL Expressが含まれます。</p> <p><input type="radio"/> Microsoft SQL Expressをインストール このコンピュータにSQL Expressをインストールして新しいデータベースを作成します。既存のSQL Expressデータベースは無視されます。SQL Expressはテスト環境に適していますが、より大規模な本番環境には適していません。</p> <p><small>[InstallShield]</small></p> <p><input type="button" value="戻る"/> <input checked="" type="button" value="次へ"/> <input type="button" value="キャンセル"/></p>	<p>Safe Lock Intelligent Manager で、収集したログ、レポート、およびエージェント情報の記録に使用するデータベースサーバの種類</p> <p>60 ページの「[データベースの設定] 画面」を参照してください。</p>
<p>Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ</p> <p>SQLのデータベース認証</p>  <p>既存のSQLサーバの場所</p> <p><input type="text"/></p> <p>10.128.5.1, server.trend.com\sqlsrv1, または [local]\MSQLSRV</p> <p>データベース認証</p> <p>ユーザ名 <input type="text"/></p> <p>パスワード <input type="password"/></p> <p><small>[InstallShield]</small></p> <p><input type="button" value="戻る"/> <input checked="" type="button" value="次へ"/> <input type="button" value="キャンセル"/></p>	<p>Safe Lock Intelligent Manager データベースのパスワード</p> <p>既存の SQL サーバを使用するには、サーバの場所を指定します。</p>
<p>Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ</p> <p>SQL Expressのデータベース認証</p>  <p>Microsoft SQL Expressを使用してTrend Micro Safe Lock Intelligent Manager TXOne Editionで作成されるデータベースの管理者の資格情報を入力します。</p> <p>データベース認証</p> <p>ユーザ名 <input type="text" value="sa"/></p> <p>パスワード <input type="password"/></p> <p>パスワードの確認入力 <input type="password"/></p> <p><small>SQL Expressはテスト環境に適していますが、より大規模な本番環境には適していません。SQL Expressには制限があるため、より大規模なネットワークはMicrosoft SQL Serverを使用することをお勧めします。</small></p> <p><small>[InstallShield]</small></p> <p><input type="button" value="戻る"/> <input checked="" type="button" value="次へ"/> <input type="button" value="キャンセル"/></p>	



56

インストーラ画面	必要な情報
<p>Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ</p> <p>サーバの識別方法の選択</p> <p>Safe LockエージェントによるIntelligent Managerの識別方法を選択してください。</p> <p><input checked="" type="radio"/> ホスト名 TEST-22</p> <p><input type="radio"/> 完全修飾ドメイン名 (FQDN):</p> <p><input type="text"/></p> <p><input type="radio"/> IPアドレス</p> <p><input type="text"/></p> <p>InstallShield</p> <p>< 戻る 次へ > キャンセル</p>	<p>エージェントが Safe Lock Intelligent Manager サーバを識別するための完全修飾ドメイン名 (FQDN)、ホスト名、または IP アドレス</p> <p>65 ページの「[サーバの識別方法の選択] 画面」を参照してください。</p> <hr/> <p> ヒント</p> <p>後で簡単に移行できるように、このサーバのホスト名を選択するか、完全修飾ドメイン名 (FQDN) を指定することをお勧めします。</p>
<p>Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ</p> <p>ネットワークの設定</p> <p>Safe Lock Intelligent Managerの管理サーバ画面にアクセスするためのポート番号を指定してください。</p> <p>HTTPSポート番号: <input type="text" value="443"/></p> <p>Safe Lock Intelligent ManagerがSafe Lockエージェントとともに使用する一意のポート番号を指定してください。</p> <p>セキュアポート番号 (ログステータスの収集用): <input type="text" value="8000"/></p> <p>セキュアポート番号 (検索ファイルの収集用): <input type="text" value="8001"/></p> <p>InstallShield</p> <p>< 戻る 次へ > キャンセル</p>	<p>Safe Lock Intelligent Manager の管理サーバ画面の Web サーバ設定</p> <p>Safe Lock Intelligent Manager サーバがエージェントとの通信に使用するポート番号</p> <p>66 ページの「[ネットワークの設定] 画面」を参照してください。</p>
<p>Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ</p> <p>サーバ通信ポート</p> <p>初期設定のセキュアポート番号 (管理サーバとの通信用):</p> <p><input type="text" value="14396"/></p> <p>Safe Lockエージェントがリモートインストールに使用するインストールディレクトリ (PROGRAMFILES\Trend Micro\Safe Lock)</p> <p>InstallShield</p> <p>< 戻る 次へ > キャンセル</p>	<p>Safe Lock Intelligent Manager がリモートエージェントインストールのインストールパッケージの配信に使用するポート番号</p> <p>68 ページの「インストール先フォルダの指定と [サーバ通信用ポート] 画面」を参照してください。</p>

インストーラ画面	必要な情報
	なし
	なし

Safe Lock Intelligent Manager サーバのインストール

始める前に

前提条件については、[51 ページの「サーバインストールのチェックリスト」](#)を参照してください。

手順

1. 対象サーバで、Safe Lock Intelligent Manager のセットアッププログラム (SLIM_Install.exe) を起動します。

2. [次へ>] をクリックします。

[使用許諾契約] 画面が表示されます。

3. サーバ設定を行います。

必要なコンポーネントがインストールされ、正しく設定されていることを確認するメッセージが表示されます。Windows プラットフォームの設定に問題がある場合は、続行する前に、解決の必要な問題をリストしたメッセージが表示されます。[トラブルシューティング情報] をクリックすると、検出された問題の解決に役立ちます。

4. 60 ページの「[データベースの設定] 画面」を完了します。

5. 管理サーバ画面の管理者の設定を完了します。

69 ページの「管理サーバ画面の管理者アカウントのパスワードについて」を参照してください。

6. Safe Lock Intelligent Manager プログラムをインストールするパスを指定します。

初期設定のインストールパスは次のとおりです。

"c:¥Program Files¥Trend Micro¥Safe Lock Intelligent Manager"

新しいインストールパスを指定するか、初期設定のパスを使用します。パスが存在しない場合は自動的に作成されます。

7. Safe Lock Intelligent Manager の製品版または体験版のアクティベーションコードを入力します。

使用可能な Safe Lock Intelligent Manager のバージョンの詳細については、付属するドキュメントを参照してください。

8. 65 ページの「[サーバの識別方法の選択] 画面」を完了します。

9. 66 ページの「[ネットワークの設定] 画面」を完了します。

10. 68 ページの「インストール先フォルダの指定と [サーバ通信用ポート] 画面」を完了します。

11. [インストール] をクリックします。

12. [完了] をクリックします。

初期設定の Web ブラウザが起動し、Safe Lock Intelligent Manager の管理サーバ画面にアクセスできます。この管理サーバ画面のショートカットがデスクトップに作成されます。



図 3-1. 管理サーバ画面のショートカット

Safe Lock Intelligent Manager の Readme ファイルも表示されます。

次に進む前に

IIS の設定から、Safe Lock Intelligent Manager の各チャネルでポートが正しく設定されているかどうかを確認することができます。確認後、Safe Lock Intelligent Manager 管理者ガイドのインストール手順に従ってエージェントをインストールします。

[データベースの設定] 画面

始める前に

データベースの要件を確認し、必要な手順を実行して環境を準備します。

**注意**

これまで Microsoft SQL Express を使用して Safe Lock Intelligent Manager データベースを管理していた場合は、データベースを Microsoft SQL Server に移行することをお勧めします。

[44 ページの「既存のデータベースを移行する」](#)を参照してください。

このデータベースインスタンスとインストールしていた SQL Express を引き続き使用する場合は、以下の該当するヒントに従ってください。

この画面では、収集したログ、レポート、およびエージェント情報のデータを Safe Lock Intelligent Manager で保存する方法を指定します。Safe Lock Intelligent Manager サーバのインストール時には、この接続のほかに、Safe Lock Intelligent Manager でデータベースへのアクセスに使用するユーザ名とパスワードも指定します。

Safe Lock Intelligent Manager の環境で使用するデータベースの種類を選択します。

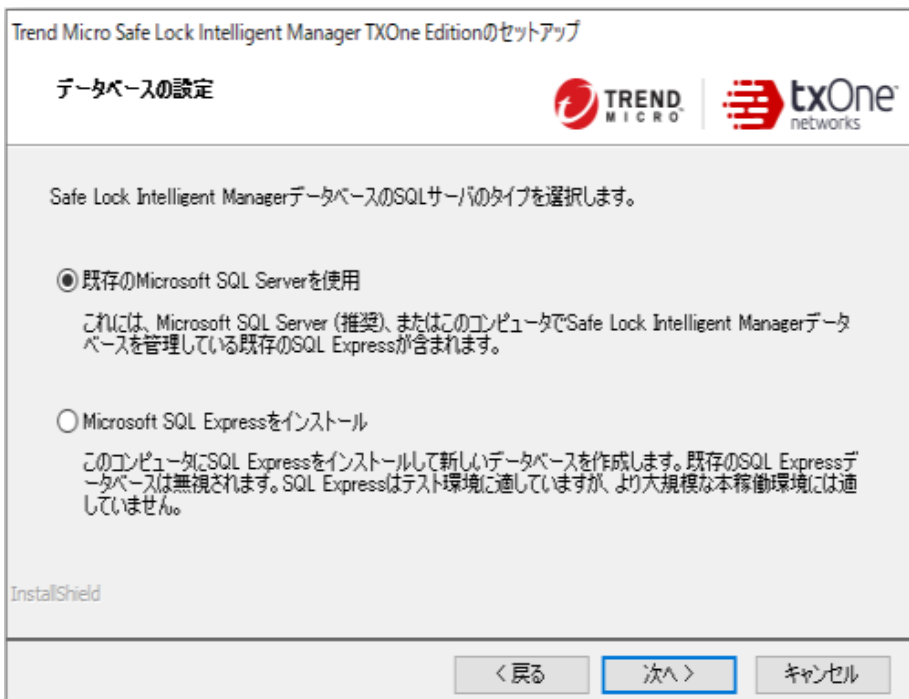


図 3-2. データベースサーバの設定

手順

- 既存の Microsoft SQL Server を使用: 使用する SQL Server (\Instance) を入力します。別の SQL サーバを使用するには、完全修飾ドメイン名 (FQDN)、IPv4 アドレス、または NetBIOS 名を使用してサーバを指定します。



ヒント

これまで Microsoft SQL Express を使用して Safe Lock Intelligent Manager データベースをホストしており、このデータベースインスタンスとインストールしていた SQL Express を引き続き使用する場合は、このオプションを選択します。次の画面の [既存の SQL サーバの場所] に、以前インストールした SQL サーバを実行しているコンピュータの IP アドレス、完全修飾ドメイン名、またはホスト名を入力し、¥SQLEXPRESS を追加します。



重要

データベースのホストを継続するには、元々インストールしていた SQL Express の新しいインストール場所からも、以前インストールしていたコンピュータに引き続きアクセス可能である必要があります。可能であれば、以前のインストールと同じコンピュータとユーザアカウントを使用することが理想です。

- Microsoft SQL Express をインストール: お使いの環境で Microsoft SQL Server を設定していない場合は、Safe Lock Intelligent Manager のセットアッププログラムを使用して、Microsoft SQL Server 2008 R2 SP2 - Express Edition をインストールできます。

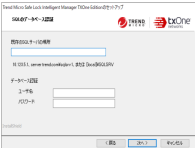
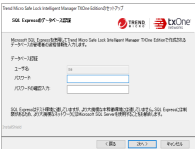



重要

SQL Express 2008 は評価用の試験的な環境に適していますが、より大規模な本稼働環境には適していません。トレンドマイクロでは、Safe Lock Intelligent Manager で監視する大規模ネットワークには、Microsoft SQL Server Standard または Enterprise Edition を使用することをお勧めします。

Windows Server 2008 SP1 (32 ビットおよび 64 ビット) では、Safe Lock Intelligent Manager はサポートされますが、Microsoft SQL Express 2008 の必須コンポーネントである Microsoft .NET Framework 3.5 Service Pack 1 はサポートされません。

- 選択内容に応じて、次のいずれかの画面が表示されます。

選択内容	表示画面	指定する情報
既存の Microsoft SQL Server を使用	 <p>図 3-3. データベースサーバの設定</p>	<p>既存の SQL サーバの場所: Safe Lock Intelligent Manager データベースをホストする SQL サーバのパスを指定します。</p> <p>[ユーザ名] と [パスワード]: Safe Lock Intelligent Manager でデータベースへのアクセスに使用するパスワードを設定します。</p>
Microsoft SQL Express をインストール	 <p>図 3-4. データベースサーバの設定</p>	<p>[ユーザ名] と [パスワード]: 初期設定のユーザ名は sa です。Safe Lock Intelligent Manager でデータベースへのアクセスに使用するパスワードを設定します。</p> <hr/> <p> ヒント</p> <p>次のガイドラインに従って、安全なパスワードを選択してください。</p> <ul style="list-style-type: none"> 長いパスワードを使用します。トレンドマイクロでは、少なくとも 10 文字のパスワードを使用することをお勧めしますが、より長いほうが安全性が高くなります。 大文字/小文字、数字、その他の記号を組み合わせで使用します。 名前や辞書に記載されている言葉は避けます。 「101010」や「abcde」などの単純なパターンは避けます。

[サーバの識別方法の選択] 画面

この画面では、エージェントと Safe Lock Intelligent Manager サーバとの通信方法を指定します。

Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ

サーバの識別方法の選択

Safe LockエージェントによるIntelligent Managerの識別方法を選択してください。

☒ ホスト名 TEST-22

☐ 完全修飾ドメイン名 (FQDN):

☐ IPアドレス

InstallShield

< 戻る 次へ > キャンセル

図 3-5. サーバの識別方法の指定

エージェントとサーバとの通信方法を選択します。

**重要**

この画面の設定を元に戻すことはできません。サーバの識別方法を後から変更する必要がある場合は、Safe Lock Intelligent Manager サーバとすべての登録済みエージェントを再インストールする必要があります。

Safe Lock Intelligent Manager を再インストールする場合は、[サーバの識別方法の選択] と同じ設定を使用します。この設定を使用しない場合、既存の管理下の Safe Lock エージェントが新しい Safe Lock Intelligent Manager と通信できなくなります。

手順

- 完全修飾ドメイン名 (FQDN): Safe Lock Intelligent Manager サーバの完全修飾ドメイン名です。
- ホスト名: Safe Lock Intelligent Manager サーバのホスト名です。
- IP アドレス: 使用可能な IPv4 アドレスのリストです。

[ネットワークの設定] 画面

始める前に

必要な IIS サーバと役割サービスをインストールします。

[51 ページの「サーバインストールのチェックリスト」](#)を参照してください。

この画面では、次のことを行います。

- ネットワークでの Safe Lock Intelligent Manager サーバの接続の識別方法を指定します。
- Safe Lock Intelligent Manager サーバがエージェントからの通信をリッスン (待ち受け) するポートを指定します。

初期設定値を使用するか、新しい値を指定します。

Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ

ネットワークの設定

Safe Lock Intelligent Managerの管理サーバ画面にアクセスするためのポート番号を指定してください。

HTTPSポート番号:

Safe Lock Intelligent ManagerがSafe Lockエージェントとともに使用する一意のポート番号を指定してください。

セキュアポート番号 (ログとステータスの収集用):

セキュアポート番号 (検索ファイルの収集用):

InstallShield

< 戻る 次へ > キャンセル

図 3-6. 管理サーバ画面の設定

手順

- HTTPS ポート番号: 初期設定値 (443) を使用するか、新しくポート番号を指定します。変更する場合は、そのポートを使用して管理サーバ画面にアクセスします。
- セキュアポート番号 (ログとステータスの収集用): 初期設定値 (8000) を使用するか、新しくポート番号を指定します。
- セキュアポート番号 (検索ファイルの収集用): 初期設定値 (8001) を使用するか、新しくポート番号を指定します。

インストール先フォルダの指定と [サーバ通信用ポート] 画面

この画面では、Safe Lock エージェントが Safe Lock Intelligent Manager から受信する通信をリッスン (待ち受け) するポートを指定します。また、エージェントの初期設定のインストールパスも表示されます。

Trend Micro Safe Lock Intelligent Manager TXOne Editionのセットアップ

サーバ通信用ポート

TREND MICRO | txOne networks

初期設定のセキュアポート番号 (管理サーバとの通信用):

14336

Safe Lockエージェントのリモートインストールに使用されるインストールディレクトリ:
<PROGRAMFILES>#Trend Micro#Safe Lock

InstallShield

< 戻る 次へ > キャンセル

図 3-7. サーバ通信用ポートを設定する

手順

- 初期設定のセキュアポート番号 (管理サーバとの通信用): 初期設定値 (14336) を使用するか、新しくポート番号を指定します。

管理サーバ画面の管理者アカウントのパスワードについて

Safe Lock Intelligent Manager では、次のパスワードがサポートされます。

- 長さが 8～64 文字
 - 英数字や次の記号の組み合わせ: !@#\$%^&* () _+=-
 - 次のサポート対象外の記号を含まない: |><\"またはスペース
- ユーザ名とパスワードは忘れないようにしてください。



ヒント

次のガイドラインに従って、安全なパスワードを選択してください。

- 長いパスワードを使用します。トレンドマイクロでは、少なくとも 10 文字のパスワードを使用することをお勧めしますが、より長いほうが安全性が高くなります。
- 名前や辞書に記載されている言葉は避けます。
- 大文字/小文字、数字、その他の記号を組み合わせで使用します。
- 「101010」や「abcde」などの単純なパターンは避けます。

フェイルオーバークラスタを設定する

Safe Lock Intelligent Manager をフェイルオーバークラスタにインストールします。

手順

1. Active Directory のドメインネットワークを準備します。

目的: Active Directory サーバを設定して、クラスタに 2 つのノードを用意します。

参照: <http://support.microsoft.com/kb/324753>

期待される結果:

- Active Directory サーバ: `ad.mycompany.local`
- ノード 1: `n1.mycompany.local`
- ノード 2: `n2.mycompany.local`

2. (オプション) SQL Server のフェイルオーバークラスタを用意します。

目的: SQL Server のフェイルオーバークラスタを設定して、全体的な SQL Server の不具合のリスクを削減します。

参照: <http://msdn.microsoft.com/ja-jp/library/hh231721.aspx>

期待される結果:

- SQL Server: `sqlcluster.mycompany.local`

3. Windows のフェイルオーバークラスタ機能を設定します。

目的: Windows のフェイルオーバークラスタ機能を有効にして、Safe Lock Intelligent Manager のクラスタを作成します。

参照: <http://technet.microsoft.com/ja-JP/library/dn505754.aspx>

期待される結果:

- ノード 1 とノード 2 が、新しく作成された、クラスタ共有ボリュームの設定されたフェイルオーバークラスタに接続します (ドライブ文字は x: と仮定します)。
- クラスタ名: `tmslcluster.mycompany.local`

4. 分散トランザクション コーディネーター (DTC) の役割を作成します。

目的: Safe Lock Intelligent Manager と IIS のフェイルオーバー用に DTC を設定します。

- a. フェイルオーバークラスタマネージャを開きます。
- b. クラスタ `tmslcluster.mycompany.local` に接続します。
- c. クラスタの構成パネルで [役割の構成...] をクリックします。
- d. [開始する前に] 画面で [次へ] をクリックします。

- e. [役割の選択] 画面で [分散トランザクション コーディネーター (DTC)] を選択し、[次へ] をクリックします。
- f. アクセスポイント名に「`tmslconsole.mycompany.local`」と入力します。
- g. IP アドレスを割り当てます。
- h. [クライアント アクセス ポイント] 画面で [次へ] をクリックします。
- i. この DTC のボリュームを選択してウィザードを完了します。

期待される結果:

- DTC アクセスポイントが設定されます。

5. Safe Lock Intelligent Manager を設定します。

- a. DTC を選択し、[移動...] をクリックして、すべてのリソースをノード 1 に移動します。
- b. ノード 1 で Safe Lock Intelligent Manager インストーラを実行します。
- c. インストール先を指定するよう求められたら、パスを `x:\SafeLock` に変更します (x:を DTC のストレージのドライブ文字と仮定します)。
- d. データベース設定を求められたら、SQL Server のアドレスを入力します。
- e. サーバの完全修飾ドメイン名 (FQDN) を求められたら、「`tmslconsole.mycompany.local`」と入力します。
- f. インストールの完了後、フェイルオーバークラスタマネージャで DTC を選択し、リソースをノード 2 に移動します。
- g. ノード 2 で Safe Lock Intelligent Manager インストーラを実行します。
- h. ノード 2 でインストール先を指定するよう求められたら、パスをノード 1 のインストールに使用されるものと同じパスに変更します。

たとえば、ノード 1 とノード 2 の両方のインストール時に `x:\SafeLock` を使用します。

- i. データベース設定を求められたら、SQL Server のアドレスを入力します。
インストーラはデータベースがすでに存在することを検出します。
 - j. 既存のデータベースを選択して、確認用パスワードを入力します。
6. Safe Lock Intelligent Manager を設定してフェイルオーバーの準備をします。
- a. DTC を選択して、[リソースの追加] をクリックします。
 - b. [汎用サービス] を追加します。
 - c. リストで [TmslSrvSvc] を選択し、ウィザードを完了します。
 - d. [TmslSrvSvc] を右クリックして [プロパティ] を選択します。
 - e. [レジストリのレプリケーション] タブを選択し、ノード間で同期できるように、SOFTWARE¥TrendMicro¥SafeLock¥Console を追加します。
7. IIS のフェイルオーバーを設定します。

参照: <http://support.microsoft.com/kb/970759>

- a. 次の例外事項を除いて、マイクロソフトのサポート技術情報に記載されている指示に従います。

「フェイルオーバークラスマネージャで汎用スクリプトを作成することによって Web サイトの高可用性を構成する」の手順 5 では、説明どおりではなく、DTC を選択して [リソースの追加...] をクリックします。



注意

スクリプトをコピーする際は、スクリプトが正しい IIS サイトを監視するように、SITE_NAME を ConsoleChannel に、APP_POOL_NAME を ConsoleChannel に変更してください。

8. テストを行います。

前述の手順を実行すると、Safe Lock Intelligent Manager でのフェイルオーバーの準備が完了します。

**注意**

コンソールアドレスは `tmslconsole.mycompany.local` です。

いずれかのノードをオフラインにして、クラスタ機能をテストすることもできます。

第 4 章

Intelligent Manager のアンインストール

この章では、Trend Micro Safe Lock Intelligent Manager 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。

- 76 ページの「Intelligent Manager の削除を準備する」
- 77 ページの「Intelligent Manager をアンインストールする」

Intelligent Manager の削除を準備する

始める前に

Safe Lock Intelligent Manager をお使いの環境から削除するには、次のことを任意の順序で実行します。

手順

- 必要に応じて、管理下の Safe Lock エージェントをアンインストールした後に、スタンドアロンの Safe Lock エージェントとして再インストールします。



注意

Safe Lock Intelligent Manager が使用可能になってログやレポートを収集するまで、Safe Lock エージェントがログとレポートをローカルにキャッシュします。Safe Lock エージェントに十分なディスク空き容量がある場合、Safe Lock Intelligent Manager から数時間分離されたままになっても未収集のログやレポートは保持されます。

管理下のエージェントの設定をアンインストール前にバックアップするには、管理下の Safe Lock エージェントのそれぞれに対して次の操作を実行します。

- a. Safe Lock の管理サーバ画面を開きます。
- b. [許可リスト] を選択します。
- c. すべてのアプリケーションを選択します。
- d. [エクスポート] をクリックして、保存場所を選択します。
許可リストがエクスポートされます。
- e. [設定] を選択します。
- f. [エクスポート] をクリックして、保存場所を選択します。
設定がエクスポートされます。

- Safe Lock Intelligent Manager をアンインストールします。

77 ページの「[Intelligent Manager をアンインストールする](#)」を参照してください。

Intelligent Manager をアンインストールする

手順

1. [スタート] > [すべてのプログラム] > [Trend Micro Safe Lock Intelligent Manager] > [Safe Lock Intelligent Manager のアンインストール] の順に選択します。

Safe Lock Intelligent Manager のセットアップがアンインストールモードで開きます。

2. [次へ>] をクリックします。
3. 既存のデータベースを使用しない場合は、必要に応じて [Safe Lock Intelligent Manager データベース] を選択します。



ヒント

データベースの削除後、Safe Lock Intelligent Manager ではいずれのデータも復元できません。トレンドマイクロでは、データベースを削除する前に、管理サーバ画面を使用して重要なデータをエクスポートすることをお勧めします。データのエクスポートの詳細については、Safe Lock Intelligent Manager 管理者ガイドを参照してください。

別の Safe Lock Intelligent Manager サーバコンピュータへ移行する場合は、データをすでに移行している場合のみ [Safe Lock Intelligent Manager データベース] を選択します。

44 ページの「[既存のデータベースを移行する](#)」を参照してください。

-
4. [次へ>] をクリックします。

アンインストールが開始され、[アンインストール進行状況] 画面が表示されます。

**重要**

アンインストール中はパフォーマンスが低下する場合があります。アンインストールが完了するまで、アンインストールを中止したり、エージェントをシャットダウンしたりしないでください。

アンインストールが完了すると、[アンインストールに成功しました] 画面が表示されます。

5. [完了] をクリックします。

Safe Lock Intelligent Manager のセットアップが終了します。

6. 必要に応じて、PHP をアンインストールします。

Safe Lock Intelligent Manager のセットアップでは、コンピュータに PHP 5.3.29 よりも新しいバージョンがインストールされていなければ PHP 5.3.29 がインストールされます。ただし、Safe Lock Intelligent Manager をアンインストールしても、セットアップで PHP は削除されません。インストール済みの PHP がセットアップでインストールされたものであれば、アンインストールしても構いません。

**注意**

Safe Lock Intelligent Manager を同じコンピュータに再インストールする前に、トレンドマイクロでは PHP の既存のインストールを削除することをお勧めします。

第 5 章

テクニカルサポート

ここでは、次の項目について説明します。

- 80 ページの「トラブルシューティングのリソース」
- 81 ページの「製品サポート情報」
- 81 ページの「トレンドマイクロへのウイルス解析依頼」
- 83 ページの「その他のリソース」

トラブルシューティングのリソース

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

サポートポータルの利用

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

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

脅威データベース

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

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

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

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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



注意

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

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

メールレピュテーションについて

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

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

ファイルレピュテーションについて

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

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

Web レピュテーションについて

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

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

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

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

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



注意

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

脅威解析・サポートセンター TrendLabs (トレンドラボ)

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

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

索引

アルファベット

OS. 参照 エージェント, OS
Safe Lock, 16, 22
Safe Lock Intelligent Manager, 16

あ

アップグレード, 26
アプリケーション制御, 23
アンインストール, 77
インストーラ
 エージェント, 26
エージェント, 22
 OS, 25
 アカウント, 25
 機能と特徴, 23
 利用時の概要, 27
エージェントインストーラ
 アップグレード準備, 26

か

機能, 16
 概要, 17
機能と特徴, 17

さ

サーバ, 16, 69
 OS, 35
 アカウント, 19, 69
 アンインストール, 76, 77
 移行, 50
 機能と特徴, 17
 システムの要件, 34, 35
 パスワード, 69
サーバインストーラ
 サーバクラスタ, 69

サーバの識別方法, 65
チェックリスト, 51
手順, 58
データベースの設定, 60
ネットワークの設定, 66
パスワードの要件, 69
フロー, 54
ポート, 68

サーバデータベース, 49

サーバの準備, 35

Windows 7, 42

Windows 8, 41

Windows 8.1, 41

Windows Server 2008, 39

Windows Server 2008 R2, 38

Windows Server 2012, 36

Windows Server 2012 R2, 36

新機能, 16

脆弱性攻撃対策, 24

た

データベース

移行, 44

インポート, 47

エクスポート, 45

既存のものを使用, 49

要件, 33

ドキュメント, xi

や

用語, xii

