WhiteDefender ユーザーガイド

WhiteDefender Agent

Version 1.0.0

Date 2026.03

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

お知らせ

Copyright ⓒ RSUPPORT Co., Ltd。 All Rights Reserved

本マニュアルは、製品の検証を行った内容に基づいて作成していますが、製品のアップデートなどを行った場合、実際の動作と異なる場合があります。

なお、マニュアルの内容は性能向上および機能改善などのために予告なしに変更される場合があります。

本マニュアルに対する著作権と知的所有権はRSUPPORT CO., Ltd。が所有し、国内の著作権法と国際著作権条約によって保護されています。

RSUPPORT CO., Ltd。の事前書面同意なしに本マニュアルの一部、あるいは全体の内容を無断にコピー、複製、転載なさらぬようお願い申し上げます。

本マニュアルに記載された他社所有の登録商標及び著作権保護を受けている用語は引用のために使用しています。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

目次

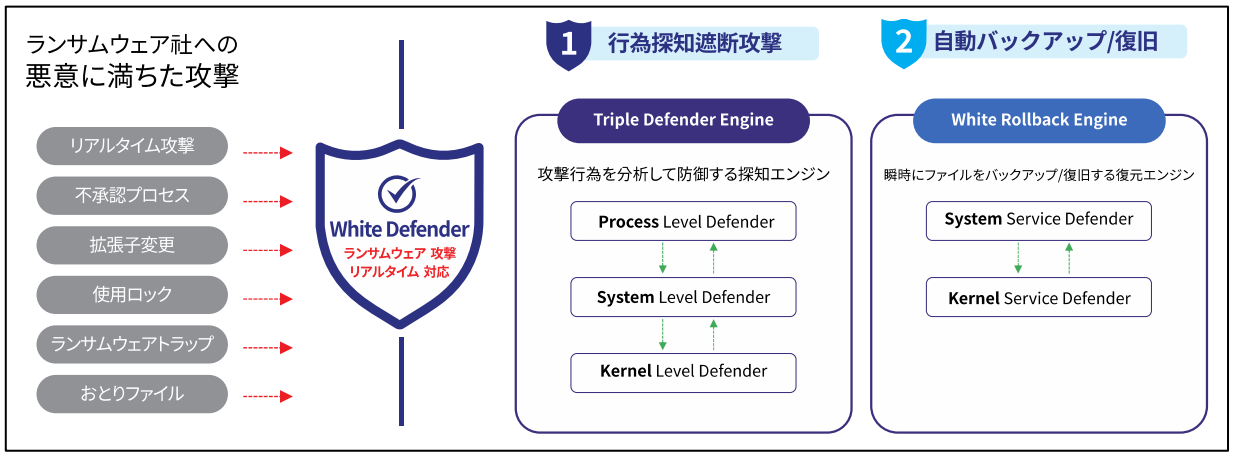
Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

1. 概要

1.1. WhiteDefenderについて

WhiteDefender（ホワイトディフェンダー）は、進化し続けるランサムウェアの脅威から企業の情報資産をリアルタイムで保護する、エンドポイント専用のセキュリティソリューションです。

従来のパターンマッチング方式では検知が困難な「未知のランサムウェア」や「変種」に対しても、独自の挙動検知エンジンと自動復旧機能を組み合わせることで、強固な防御環境を提供いたします。



Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

1.1.1. 主な特徴と機能

WhiteDefenderは、リアルタイム保護、行為検知、罠検知などの機能を通じてランサムウェアを事前に検知してブロックし、ランサムウェアが暗号化を進行する場合、瞬時に元のファイルをバックアップし、ランサムウェア行為をブロック後に復元してデータを安全に保護します。

- **多層防御によるランサムウェア遮断**
  シグネチャベースの検知に加え、ファイルへの不正な暗号化の動きを即座に察知し、攻撃を未然にブロックします。
- **自動バックアップおよび復旧（ロールバック）機能**
  万が一、ランサムウェアによってファイルが損壊・暗号化された場合でも、検知の瞬間に保護されたバックアップデータから、ファイルを正常な状態へ自動的に復元します。
- **ホワイトリストによる安全な実行環境**
  信頼されたプロセスのみを許可するホワイトリスト形式の運用により、未知の実行ファイルによる被害を最小限に抑えます。
- **低負荷なパフォーマンス設計**
  高度なセキュリティ機能を備えながらも、PCやサーバーのシステムリソースへの負荷を最小限に抑え、日常の業務を妨げることなく安全な環境を維持します。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

1.2. White Security Platform Agentについて

White Security Platform Agent（ホワイトセキュリティプラットフォームエージェント、以下WSP Agent）は、エンドポイント（PC、サーバー）にインストールされ、セキュリティポリシーの適用、プログラム配布の実行、検知およびイベントログの収集などの機能を担う主要な構成要素です。 エージェントは、管理者サーバー（WSP）との定期的な接続を通じて管理者のコマンドを迅速に受信・処理し、実行結果および各種情報をサーバーに送信することで、一元的な中央管理モニタリングと制御を可能にします。

1.2.1. 主な特徴と役割

WSP Agentは、エンドポイント上で以下の主要な機能を実行します。

[特徴]

- ポリシーの適用
  管理者が設定したセキュリティポリシーをエンドポイントPCおよびサーバーに自動的に適用します。
- プログラムの配布
  セキュリティ製品「ホワイトディフェンダー」の配布およびインストールを実行します。
- イベントおよびログの収集
  セキュリティイベント、検知ログ、およびユーザ活動ログの収集とサーバーへの送信を行います。
- 状態の報告
  システム状態、ポリシーの適用有無、配布の成功有無など、端末の状況を定期的に報告します。
- 自動更新
  製品バージョンのアップデートおよびポリシーの変更内容を自動的に反映します。

[役割]

- 統制手段
  セキュリティポリシーおよびコマンドを対象端末に送信し、自動で適用させます。
- 情報収集
  各エンドポイントの状態、ログ、セキュリティイベントを漏れなく収集し、管理サーバーに送信します。
- 迅速な対応
  ランサムウェアなどの脅威が発生した際に、即座にブロックを実行し管理サーバーへ報告を行います。
- 運用効率性の確保
  管理者が現場の端末に直接介入することなく、遠隔でのセキュリティ状況の把握や資産管理を実現します。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

1.2.2. 使用環境

OS推奨仕様	**Windows** ▪ Windows 7 / 8.1 / 10 / 11 (32/64ビット) ▪ Windows Server 2008 R2 ～ 2022 (32/64ビット) **Linux** ▪ RHEL 7.0以上 / CentOS 7.0～8.5 ▪ AlmaLinux / Rocky Linux 8.3以上 ▪ Ubuntu 18.04以上 / Oracle Linux 7.0（※対応予定）
ハードウェア **最小仕様**	▪ Intel Pentium Core 2 Duo 1.8GHz以上 ▪ 最小メモリ1 G B以上 ▪ 100MB以上のハードドライブの取り付け空き容量 ▪ 5GB以上のハードドライブ操作の空き容量を推奨 ▪ IPv4 、IPv6ネットワーク環境を推奨
ハードウェア **推奨仕様**	▪ Intel Pentium Core i3 2.6GHz以上 ▪ 推奨メモリ2 G B以上 ▪ 100MB以上のハードドライブの取り付け空き容量 ▪ 5GB以上のハードドライブ操作の空き容量を推奨 ▪ IPv4 、IPv6ネットワーク環境を推奨

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

2.インストール方法

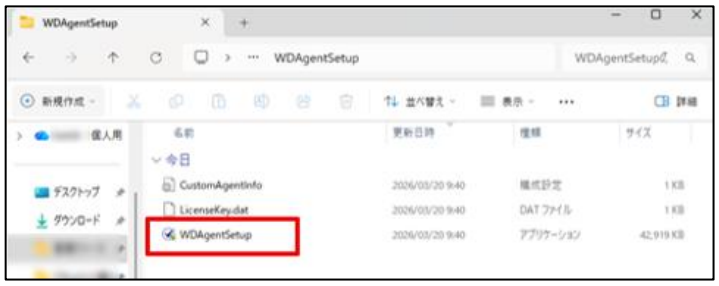
[事前準備]

管理者からインストールファイルを受け取ってください。

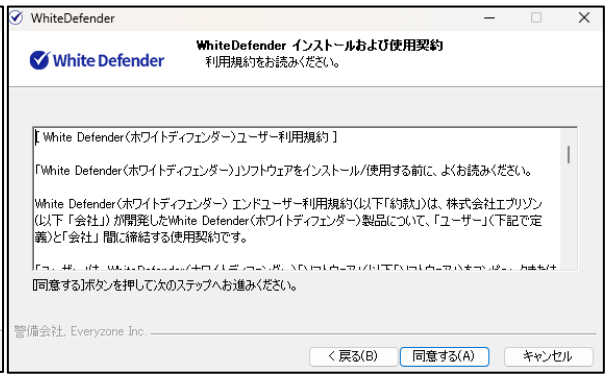
※　ファイルの配布方法は「管理者マニュアル」をご参照ください。

①　管理者から配布されたzipファイルを展開します。

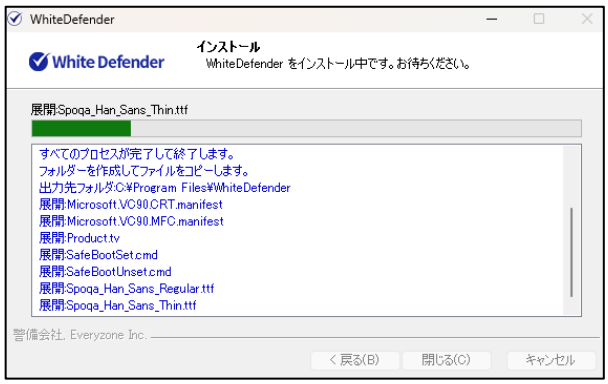
②　「WDAgentSetup」をクリックしインストールプログラムを実行します。



③　実行後の案内に沿って「次へ」をクリックし、利用規約に同意します。

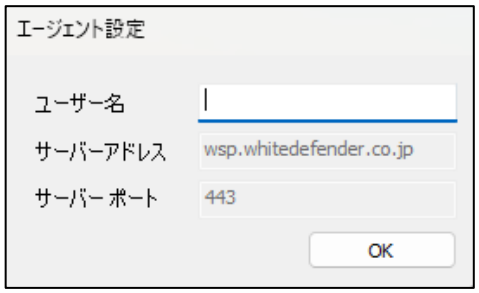


④　インストールが開始されます。

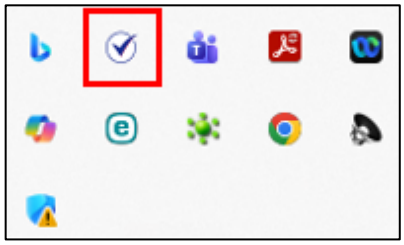


Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

⑤　インストール成功の案内が表示されたら、エージェント設定画面で「ユーザー名」を入力します。



⑥　タスクトレイにWSP Agentアイコンが表示されればインストール完了です。

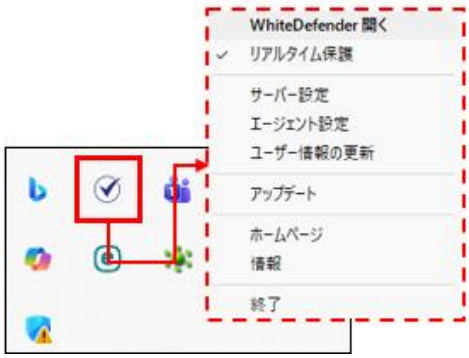


Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

3. Agent画面について

3.1. メイン画面

タスクバー＞WSP Agent アイコン右クリック＞「WhiteDefender を開く」でメイン画面が開きます。



[画面構成]

A：製品関連登録情報、および環境設定機能をサポートします。

	ヘルプ	WhiteDefenderヘルプページが開きます。
	アカウント	マイアカウント情報と製品ステータスを確認できます。
	ログを表示	一般、検知、検疫所、常時ログを表示します。 ログの詳細については「3.3 ログを表示」をご確認ください。
	環境設定	各種環境設定を行うことができます。 環境設定詳細については「3.2 環境設定」をご確認ください。
	閉じる	メイン画面を閉じます。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

B：WhiteDefender の現在の防御機能の動作状態とバージョン情報を表示します。

		
<安全防御状態>		**<脅威暴露状態>**
振る舞い検知/トラップ検知 どちらも有効状態	振る舞い検知/トラップ検知 どちらか1つが有効状態	振る舞い検知/トラップ検知 どちらも**無効**状態

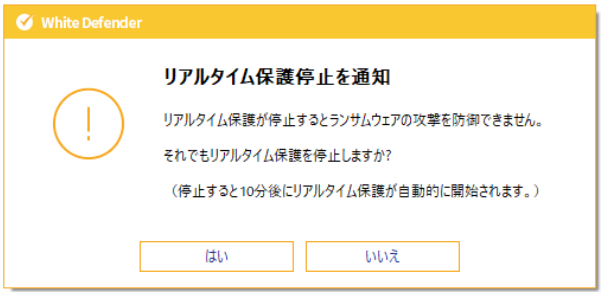
C：主要防御機能状態を有効化(ON)/無効化(OFF)することができます。

すべての保護機能を有効にしている状態です。

トラップ探知ブロック機能のみを無効にした場合、
振る舞い探知ブロック機能のみ動作します。

振る舞い検知ブロック機能のみを無効にすると、
トラップ検検知ブロック機能のみが動作します。

リアルタイム保護が無効になり、
システム保護が正常に動作しません。



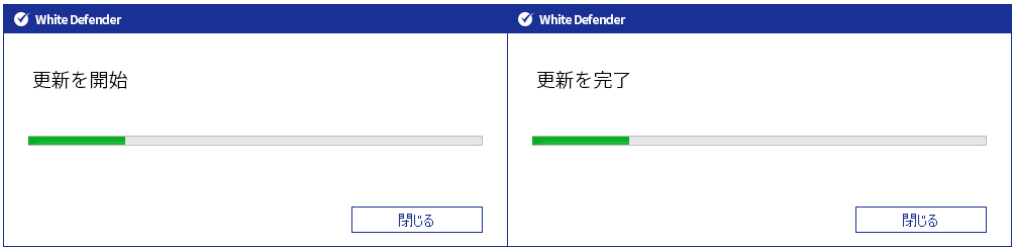
保護を停止すると、ランサムウェア攻撃を防ぐことができず、脅威にさらされます。
(該当オプションは停止から10分後、リアルタイム保護が自動的に開始します。)

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

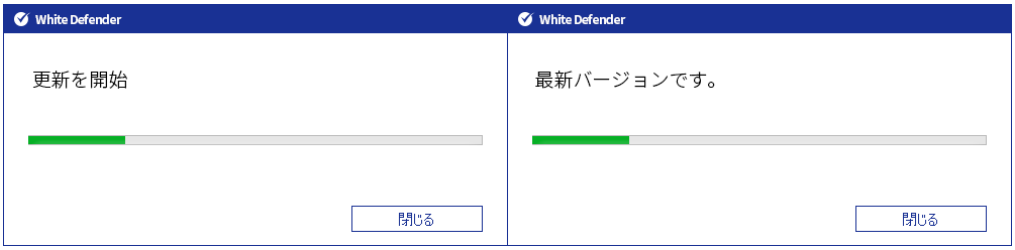
D：WSP Agent のアップデートチェックを行います。

update	Agentを最新の状態に更新するために、 ターゲットファイルを検索してダウンロードします。

Agentを更新する必要がある場合は、最新バージョンの適用を行います。



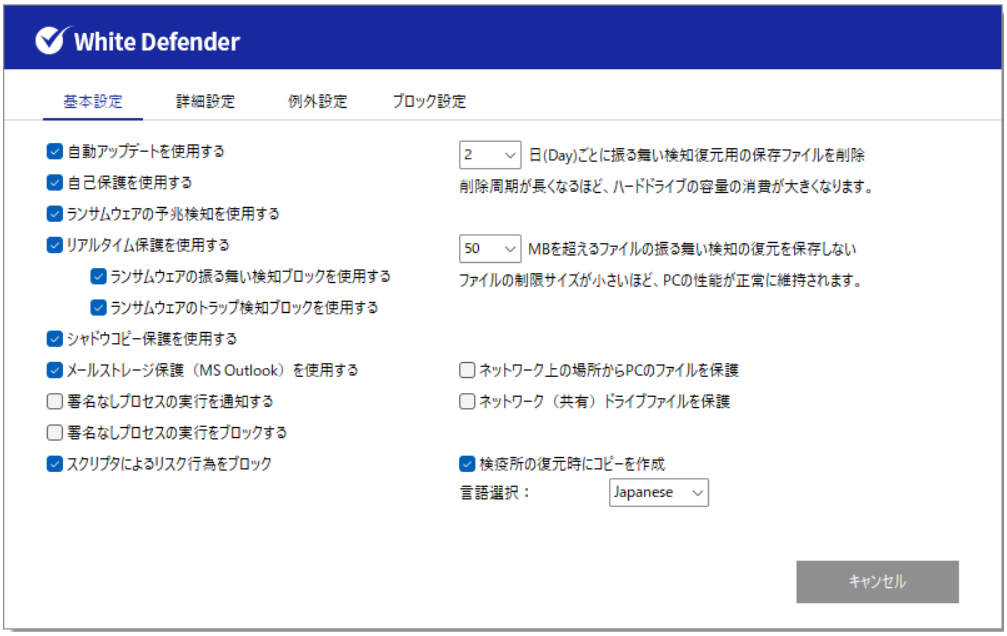
最新の場合は、最新バージョンであることをお知らせします。



Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

3.2. 環境設定

3.2.1. 基本設定



1	自動アップデート を使用する	・PC再起動時に自動更新機能を実行します。 ・起動中1時間単位でサーバーと通信し、アップデートチェックを行います。
2	自己保護を使用する	プログラムのインストールフォルダや構成ファイル、レジストリ、およびプログラムの正常動作に関連する主要プロセスの強制終了、未認可の改ざん、削除活動による損傷から保護する機能です。
3	ランサムウェアの 予兆検知を使用する	ランサムウェアの検知データベース（DB）に基づき、暗号化攻撃を行うランサムウェアが事前に登録されている場合、暗号化の不審な挙動が開始される前に検知および遮断をサポートします。
4	リアルタイム保護 を使用する	プログラムの主要なアンチランサムウェア機能を制御します。 詳細項目の有効/無効を切り替えることで、部分的な運用も可能ですが、効果的なランサムウェア防御を実現するため、すべての項目においてリアルタイムでの動作（有効化）を推奨します。 ※　当該項目を無効（OFF）に設定した場合、ランサムウェアの振る舞い検知、およびトラップ検知のいずれも動作しません。
5	シャドウコピー保護 を使用する	Windows OS標準でサポートされている「シャドウコピー」は、システムの復元を目的として、特定のファイルやフォルダ、または特定のボリュームのコピーやスナップショットを保存しておく機能です。 ランサムウェアによるシャドウコピーの破壊や損傷を防ぐため、当該領域への不審なアクセスや攻撃の兆候を検知した場合、これを遮断・防御する機能を提供します。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

6	メールストレージ保護 (MS Outlook)を使用する	Outlookプログラムで使用されるメールデータ保存ファイル（PST/OST等）に対する、不正な改ざんの試みを検知・遮断する機能を提供します。
7	署名なしプロセスの実行 を通知する	デジタル署名によるアプリケーションの信頼性や、開発元の実体性の検証が不十分なプロセスが実行される際、ユーザーに通知を行う機能です。
8	署名なしプロセスの実行 をブロックする	デジタル署名によるアプリケーションの信頼性、および開発元の実体性の検証が不十分なプロセスについて、実行自体が行われないよう遮断する機能です。
9	スクリプタによるリスク行為 をブロック	スクリプト（VBS、JS、PSなど）を悪用して生成される、システムセキュリティへの脅威となる攻撃行為を遮断します。
10	[ ]日ごとに振る舞い検知用の 保存ファイルを削除	デフォルト（既定値）は1日に設定されており、最長7日まで変更可能です。 ※　周期が長いほど、ハードドライブの空き容量の消費が大きくなります。 ※　バックアップフォルダの既定パス： C:¥Program Files¥WhiteDefender¥BACKUP
11	[ ]MBを超えるファイルの 振る舞い検知の復元を保存しない	デフォルト（既定値）は50MBに設定されており、10MBから100MBまで設定可能です。 ※ ファイルサイズの上限設定が小さいほど、PCのパフォーマンスを正常に維持しやすくなります。 ※ 100MBを超えるファイルの場合、リアルタイムバックアップの対象外となるためご注意ください。
12	ネットワーク上の場所からの PCのファイルを保護	ネットワーク経由で外部エンティティが、自身のコンピュータ内の特定の場所へファイルを書き込もうとする動作を遮断する機能です。 PC内の共有フォルダに対し、外部から接続した他のPCがファイル内容を閲覧したり外部へコピーしたりすることは可能ですが、外部接続されたPCからファイルを新規作成したり、既存のファイルを修正したりすることはできないよう遮断します。 例：ネットワークで接続された他のPCがランサムウェアに感染し、そのランサムウェアがネットワーク上の共有データに対して二次的な暗号化攻撃を仕掛けてきた場合、WSP Agentがインストールされた PCの共有データを保護します。
13	ネットワーク(共有) ドライブファイルを保護	WSP Agentがインストールされた PCから、外部の共有フォルダ等へアクセスし、ファイルの新規作成や既存のファイルを修正することを遮断します。
14	検疫所の復元時に コピーを作成	ファイルの復元中に発生しうるデータの消失や再感染に備え、元データを復旧した後も検疫内にバックアップを維持する安全機能です。
15	言語選択	WSP Agentでの言語選択ができます。

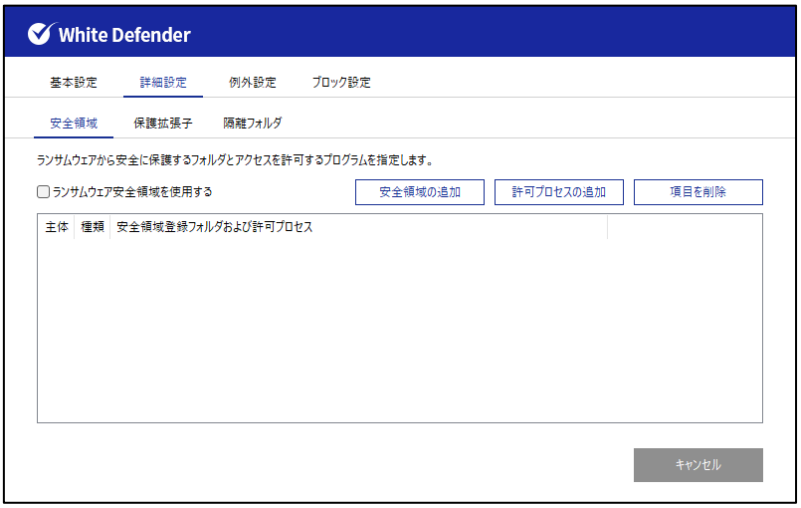
※　各設定はリアルタイム保護機能が無効の場合には動作しません。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

3.2.2.　詳細設定

デフォルトの設定に加えて、カスタマイズプログラム、フォルダ、拡張機能を追加します。

[安全領域]　ランサムウェア安全地帯（保護フォルダ）機能



・安全領域の追加

ランサムウェアによる不正な暗号化プロセスからフォルダやファイルを強力に保護するための機能です。
ユーザーのPC内にある特定のフォルダに対し、アクセスを許可するプログラムを指定することで、それ以外のプログラムによるアクセスを完全に遮断します。
※ Windowsの特殊パス（システムパス）についてはOSの動作要件上、登録が制限されます。
「安全領域の追加」ボタンをクリックし設定するフォルダのパスを直接入力するか、ドラック&ドロップで追加します。
登録した情報追加後［すべてを追加］ボタンを押してから、「適用&確認」ボタンをクリックしてを情報を適用します。

・許可プロセスの追加

「ランサムウェア安全地帯」として設定したフォルダに対し、アクセスを許可するプログラム（プロセス）を指定する機能です。
「許可プロセスの追加」ボタンをクリックし設定するフォルダのパスを直接入力するか、ドラック&ドロップで追加します。
登録した情報追加後［すべてを追加］ボタンを押してから、「適用&確認」ボタンをクリックしてを情報を適用します。

・項目を削除

既に登録されてい項目を選択し、リストから削除します。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

3.2.3. 例外設定

・自動生成例外情報

WSP Agentがインストールされ たPCの「コントロールパネル ＞ プログラムと機能」の一覧に登録されている正規プログラムに対し、例外設定を自動的に処理する機能です。

削除：削除したいプログラムの右側にチェックを入れて「選択項目を削除」をクリックします。

リストエクスポート：「エクスポート(TEXT)」をクリックするとテキストでエクスポートされます。

・例外項目の追加

WSP Agentのリアルタイム保護機能によって誤検知が発生した場合、該当プログラムの動作を許可するために、ユーザーが直接例外項目を登録する機能です。

「例外項目の追加」ボタンをクリックした後、対象のプロセスを選択し、[すべてを例外に追加] ボタンを押して登録を完了します。

・例外項目の削除

既に登録されている例外項目を選択し、リストから削除します。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

3.2.4. ブロック設定

運用中に発生した検知・遮断の履歴を確認できます。

・例外リストへ移動

WSP Agentにてブロックされたプロセスが「誤検知」であると判断・確認された場合、手動で例外設定リストへ移動させる機能です。

・ブロック項目の追加

ブロック対象のプロセスを手動で追加する機能です。操作方法は「例外プロセスの追加」と同様です。

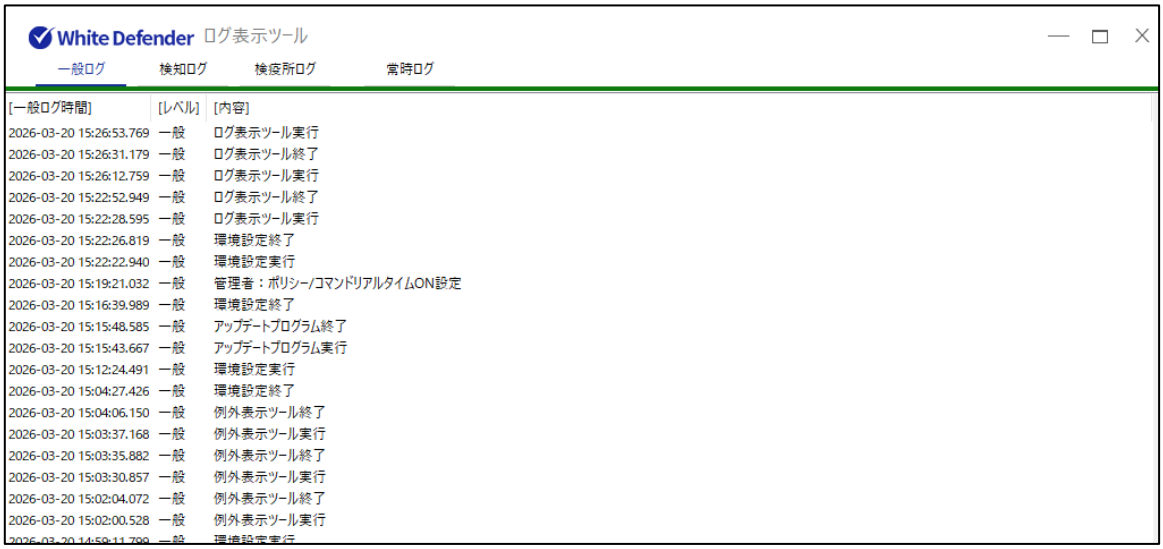
・ブロック項目の削除

既に登録されているブロック項目を選択し、リストから削除する機能です。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

3.3. ログを表示

サービス、アップデート、メインプログラム、および個別の一般機能の実行や終了に関するログを確認できる機能です。



3.3.1. 検知ログ

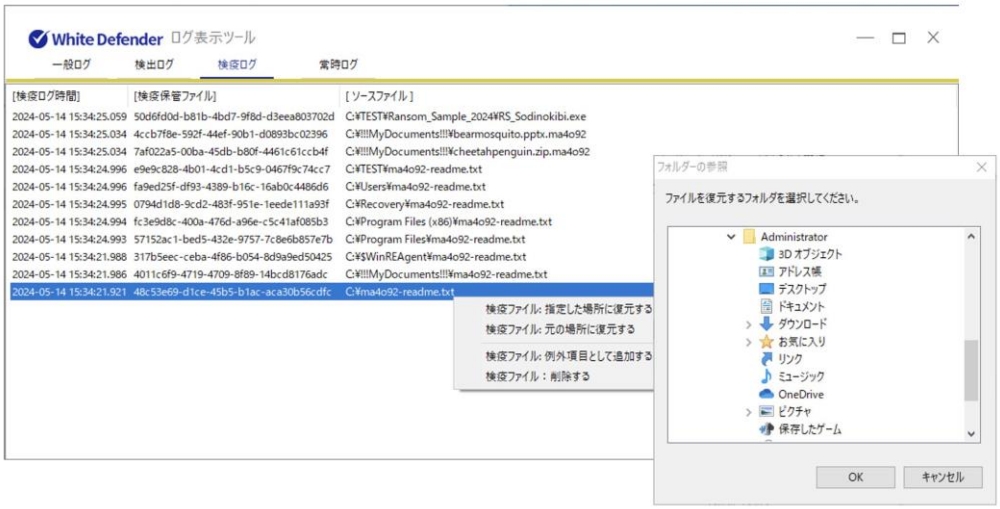
ランサムウェアの「振る舞い検知」および「トラップ検知」に関する詳細（検知時間、脅威、種類、項目、結果など）を確認できる機能です。

「結果ログ：検疫所に保管」と表示される項目については、「検疫所ログ」タブにて詳細の確認および処理が可能です。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

3.3.2. 検疫所ログ

検疫所に移動したファイルを確認し、マウスの右クリックで追加の処理を行うことができます。



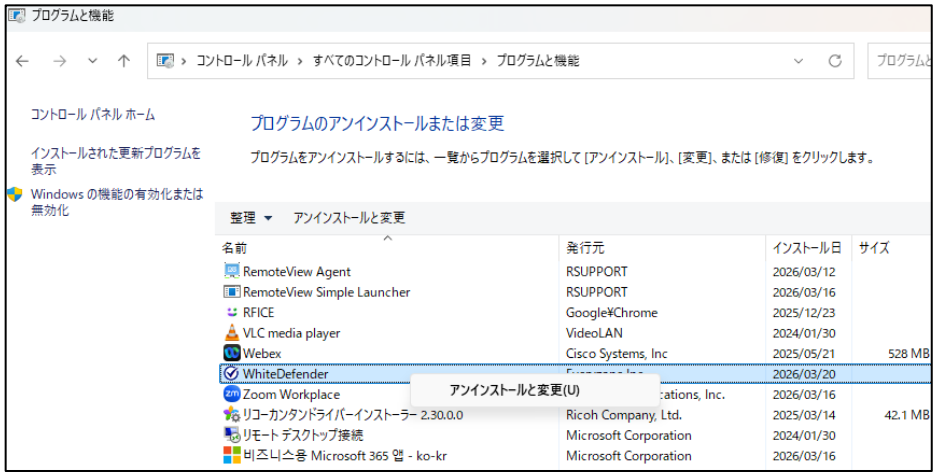
Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

4.アンインストール方法

WSP Agentのアンインストールは下記の3つの方法から実行できます。

① コントロールパネルからアンインストールする

コントロールパネル> プログラムと機能> 「WhiteDefender」を選択し「アンインストールと変更」を選択し、削除を進めます。



② スタートメニューからアンインストールする

スタートメニュー> アプリ> すべてのアプリ> 「インストールされているアプリ」から「WhiteDefender」を検索しアンインストールします。

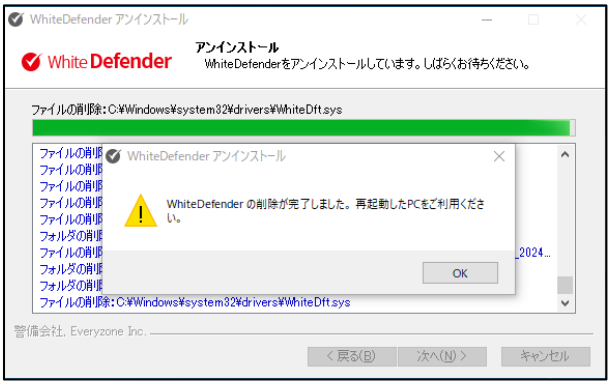
③ フォルダパスから直接削除する

「C:¥Program Files¥WhiteDefender¥WhiteDRemove.exe」からアンインストールを実行します。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED

①～③でアンインストールを実行すると、WhiteDefenderアンインストールウィザードが開きます。

案内に沿って「次へ」をクリックするとアンインストールが開始されます。



アンインストール完了の画面が表示されたら、削除完了となります。

※　アンインストール後はPCの再起動を行ってください。

Copyright © RSUPPORT Co。, Ltd。 ALL RIGHTS RESERVED