



AppCheck Pro 3.0

誤検知対応マニュアル

株式会社 JSecurity

第二版

2024/4/22

目次

1. 【CMS有】誤検知対応方法	1
2. 【CMS無】誤検知対応方法	4

1. 【CMS有】誤検知対応方法

(1) 以下のURLにアクセスし、CMSにログインします。

<https://jp.cms.checkmal.com>



(2) 「エージェント」>「ツール」>「ログビュー」ボタンをクリックします。



レス	ホスト名	OS情報	ユーザ名	部署名	インストールバージョン	ポリシー名	ポリシーバージョン	最新ポリシーバージョン	機状態	リアルタイムセキュリティ	最終オンライン時間	ツール
					3.1.32-1	基本ポリシー	-	50	オンライン	アクション	2023-07-05 11:16:58	ログビュー
					3.1.32-1	基本ポリシー	-	50	オンライン	アクション	2023-07-05 11:16:58	
					3.1.32-1	基本ポリシー	-	50	オンライン	アクション	2023-07-05 11:16:58	

(3) 「脅威ログ」から「ランサムウェアアクション検知」として誤検知、遮断されているプロセスを確認してください。

ログビュー

脅威ログ 検疫所 一般ログ

検索

検知主体	脅威	種類	対象パス	処理
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Filmora\Download\Temp\Title\1_Credit_1_45W\thumbnaill.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Download\Temp\Title\1_45W\thumbnaill.png	復元
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Download\Temp\Title\1_Opener_1\thumbnaill.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Download\Temp\Title\1_Opener_1\thumbnaill.png	復元
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Download\Temp\Title\1_Default_Lowert\thumbnaill.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Download\Temp\Title\1_Default_Lowert\thumbnaill.png	復元
ランサムガード	ランサムウェアアクション検知	ファイル	C:\Users\kshin\AppData\Local\Wondershare\Filmora\11-6-7-752\Wondershare\Filmora 11.exe	遮断

Showing 1191 to 1197 of 1197 rows 10 rows per page

閉じる

(4) 「ポリシー管理」>「例外設定」から、誤検知が発生したエージェントの「ツール」ボタンをクリックしてください。

CMS Cloud

例外設定

ポリシー管理

エージェントID	IPアドレス	MACアドレス	ホスト名	OS情報	ユーザ名	部署名	インストールバージョン	現状態	最終オンライン時間	ツール
							3.1.32.1	オンライン	2023-07-06 11:22:53	🔧
							3.1.32.1	オンライン	2023-07-06 11:22:56	🔧
							3.1.32.1	オンライン	2023-07-06 11:22:53	🔧

Showing 1 to 3 of 3 rows

(5) 「信頼済みプロセスリスト」>「追加」をクリックし、(3)で確認した誤検知プロセスをファイルのパスまで含めた形として入力し、「OK」を押してください。

例外設定

【信頼済みプロセスリスト】

以下に登録されたファイルは常に許可 追加 修正 削除

追加するファイルのパスを入力してください

#Wondershare\Wondershare\Filmora\Wondershare\Filmora Launcher.exe

OK キャンセル

【例外ファイル一覧】

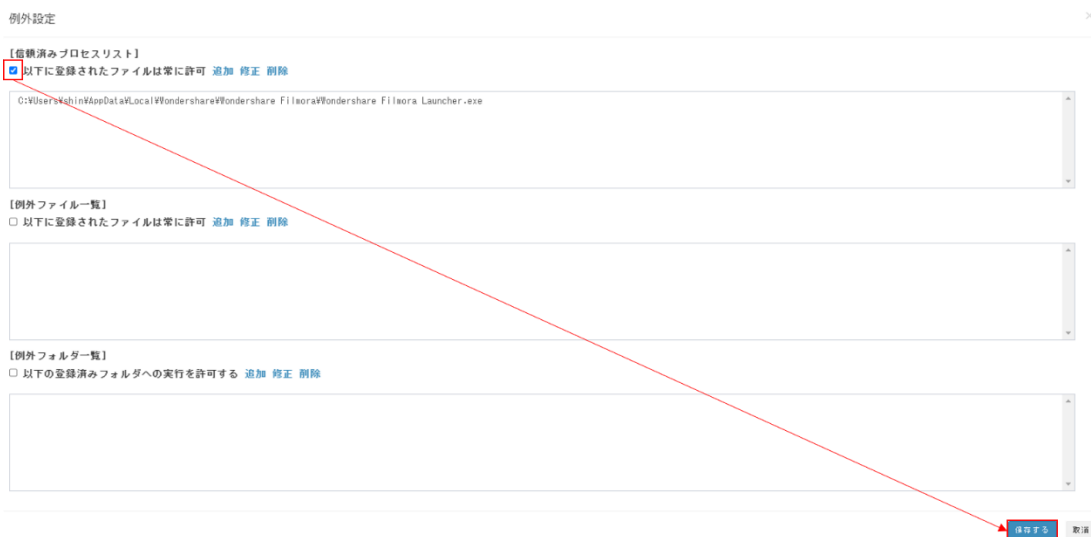
以下に登録されたファイルは常に許可 追加 修正 削除

【例外フォルダ一覧】

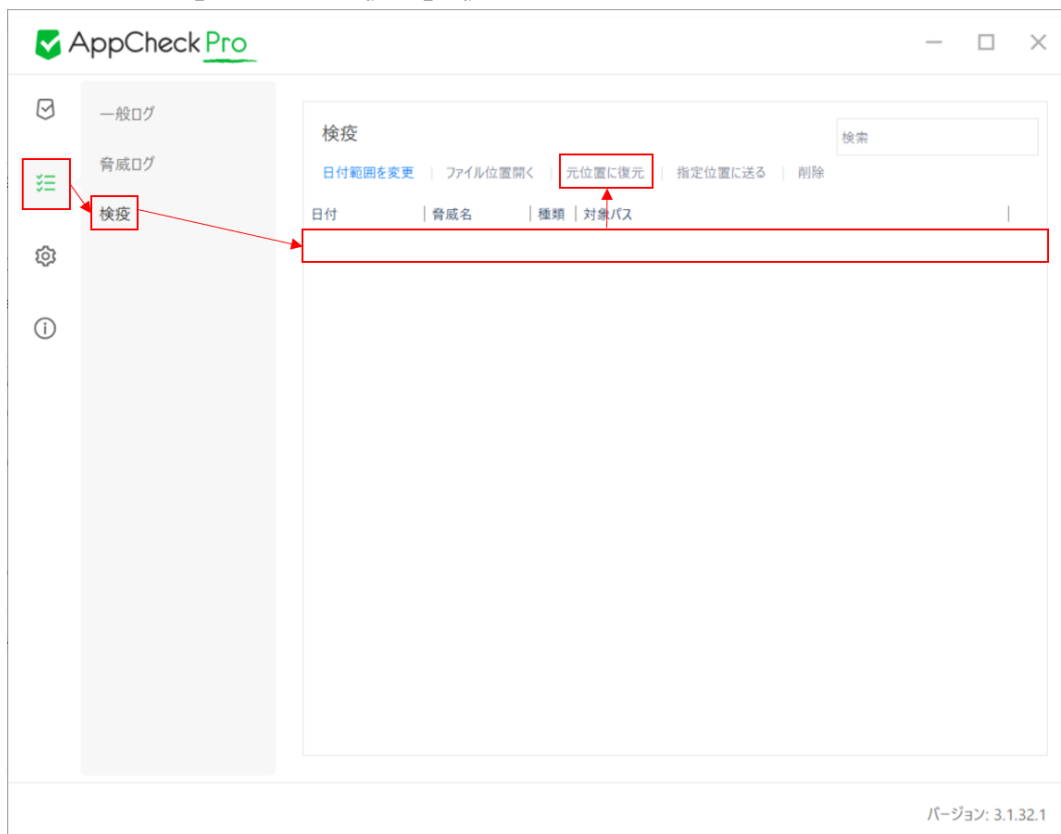
以下に登録済みフォルダへの実行を許可する 追加 修正 削除

追加する

(6) 「以下に登録されたファイルは常に許可」にチェックを入れ、「保存する」ボタンをクリックしてください。



(7) 該当エージェントのAppCheckPro画面から「ツール」>「検疫」>「誤検知により削除されたプロセスファイルを選択」>「元位置に復元」で復元を行ってください。

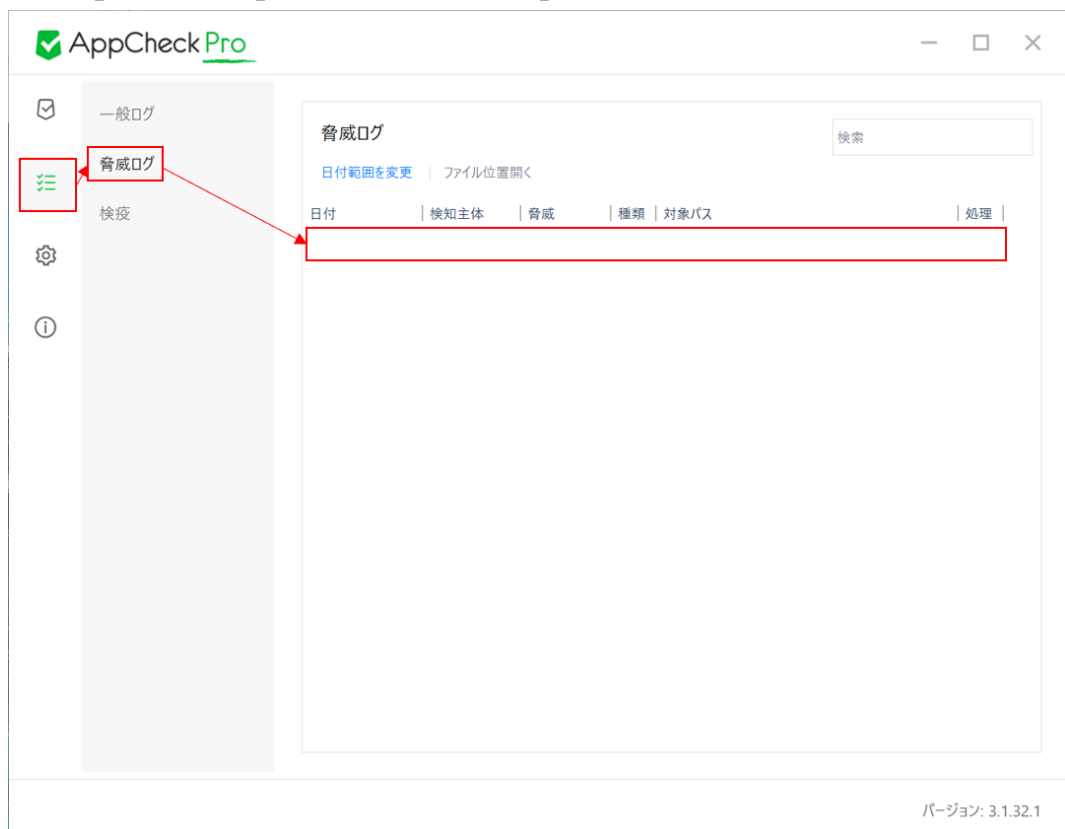


2. 【CMS無】誤検知対応方法

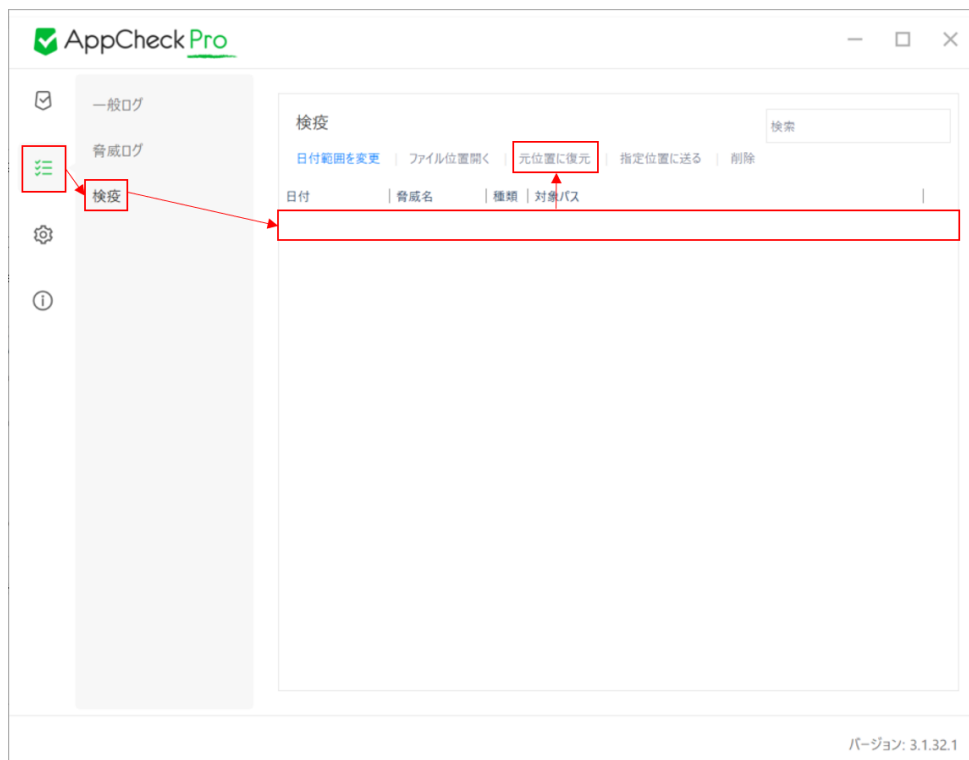
(1) Windows右下のAppCheckのアイコンをダブルクリックし、AppCheckProを開いてください。



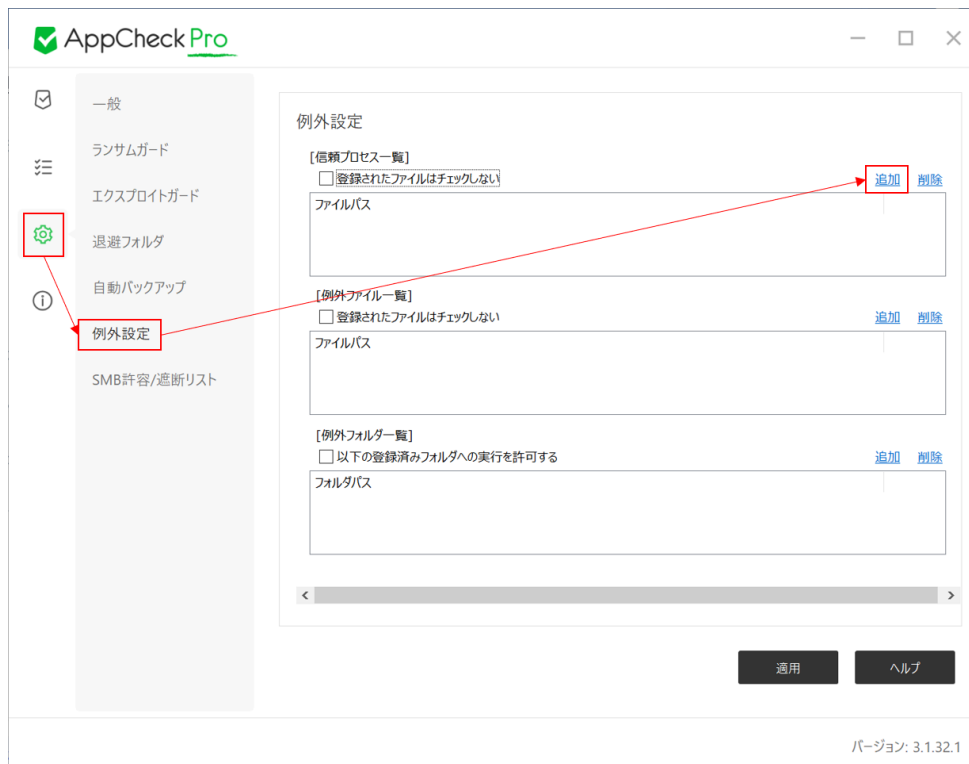
(2) 「ツール」>「脅威ログ」から誤検知により「遮断」されたプロセスファイルをご確認ください。



- (3) 「ツール」>「検疫」>「誤検知により削除されたプロセスファイルを選択」>「元位置に復元」で復元を行ってください。



- (4) 「オプション」>「例外設定」>「信頼プロセス一覧」>「追加」により、(3)で復元した誤検知プロセスファイルを選択し、追加してください。



(5) 「登録されたファイルはチェックしない」にチェックを入れ、「適用」を押してください。

