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) 以下のURLにアクセスし、CMSにログインします。

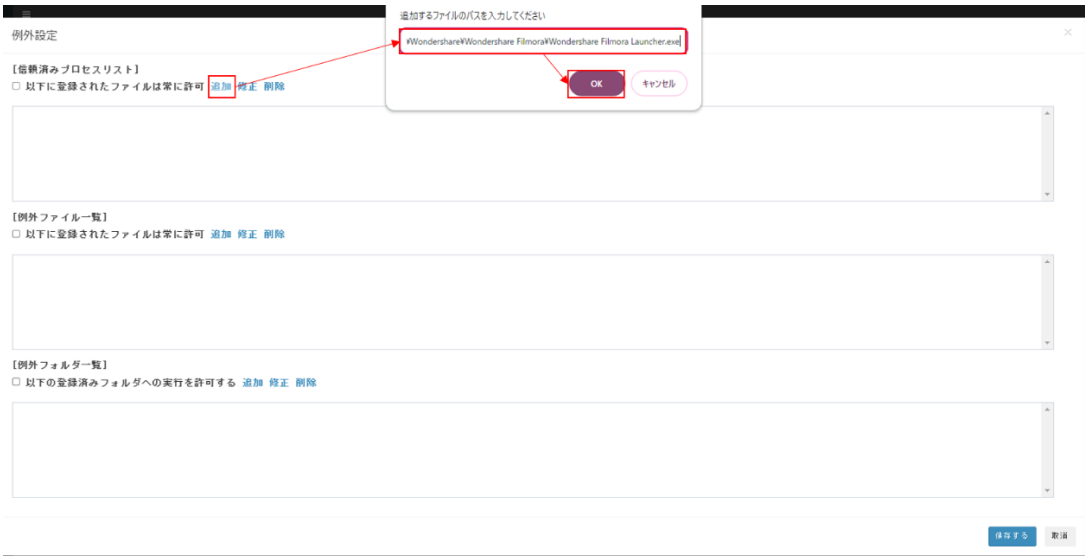
https://jp.cms.checkmal.com

(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。

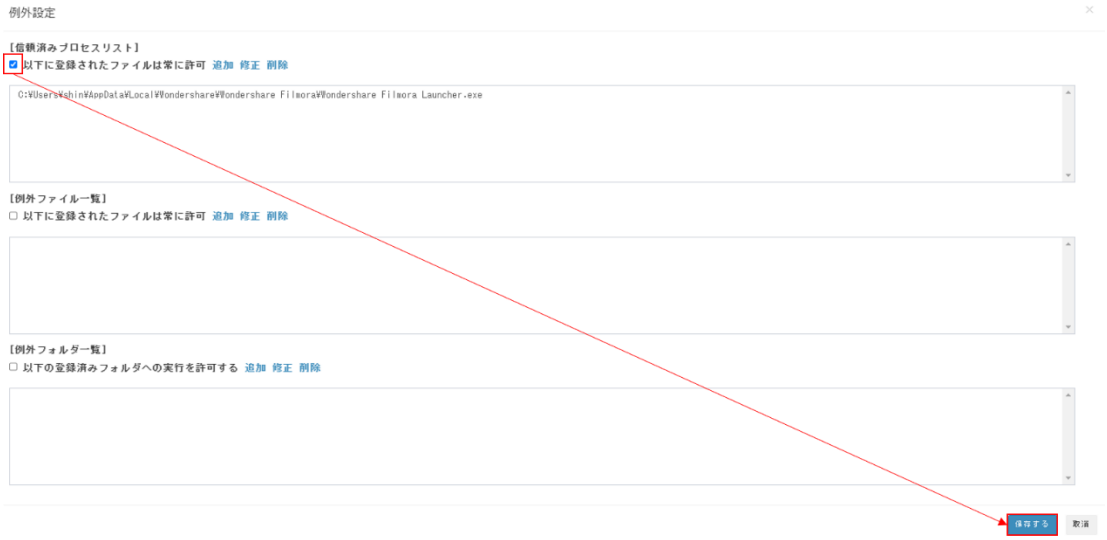
(3)「脅威ログ」から「ランサムウェアアクション検知」として誤検知、遮断されているプロセスを確認してください。

(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。

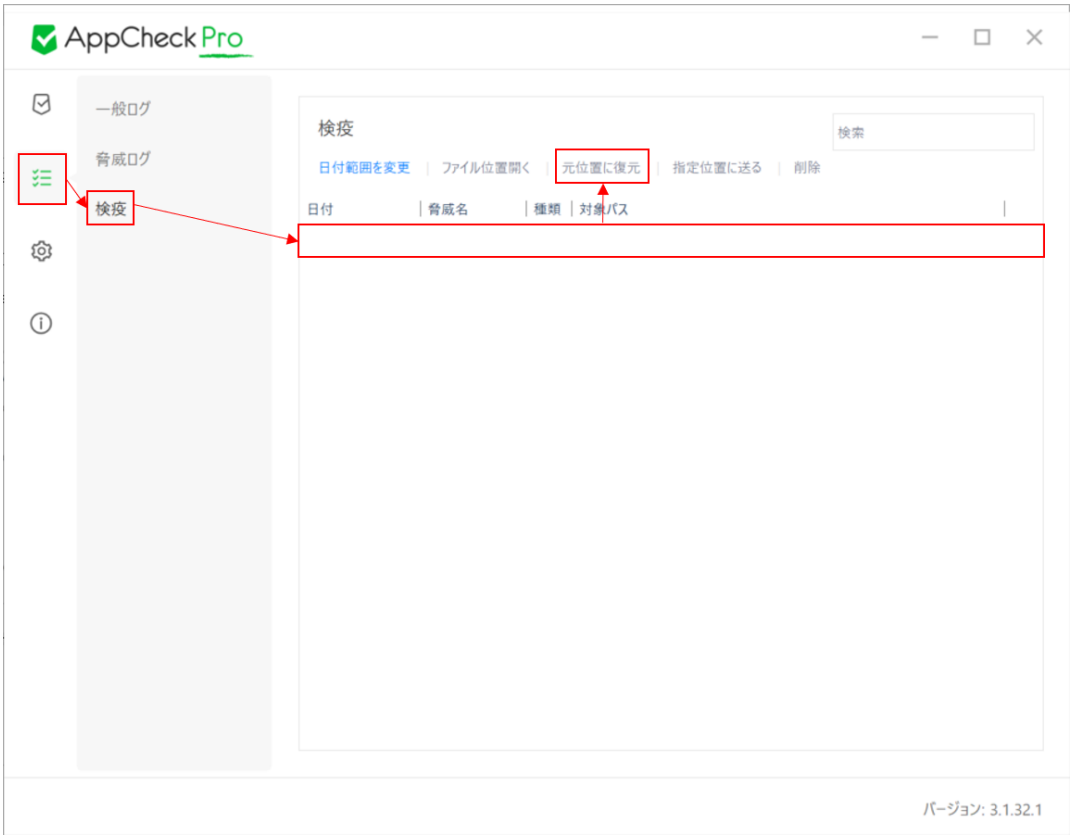
(5)「信頼済みプロセスリスト」>「追加」をクリックし、(3)で確認した誤検知プロセスを**ファイルのパスまで含めた形**として入力し、「OK」を押してください。



(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。



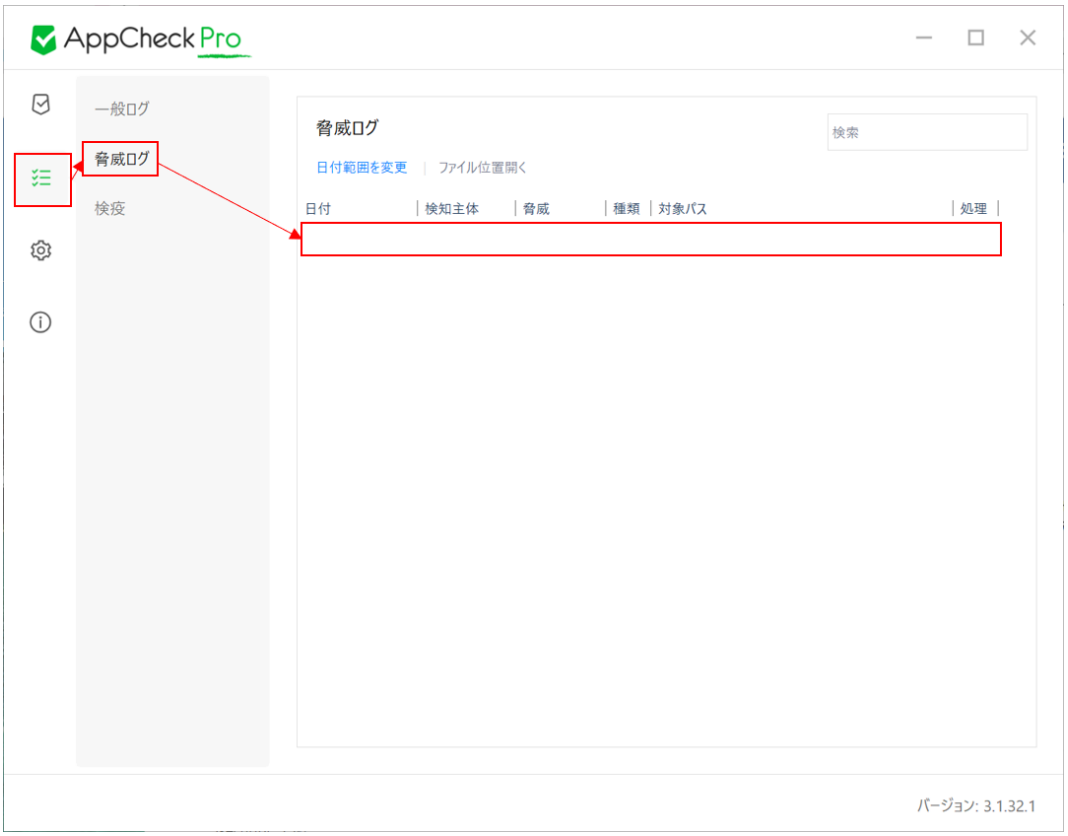
(7) 該当エージェントのAppCheckPro画面から「ツール」>「検疫」>「誤検知により削除されたプロセスファイルを選択」>「元位置に復元」で復元を行ってください。



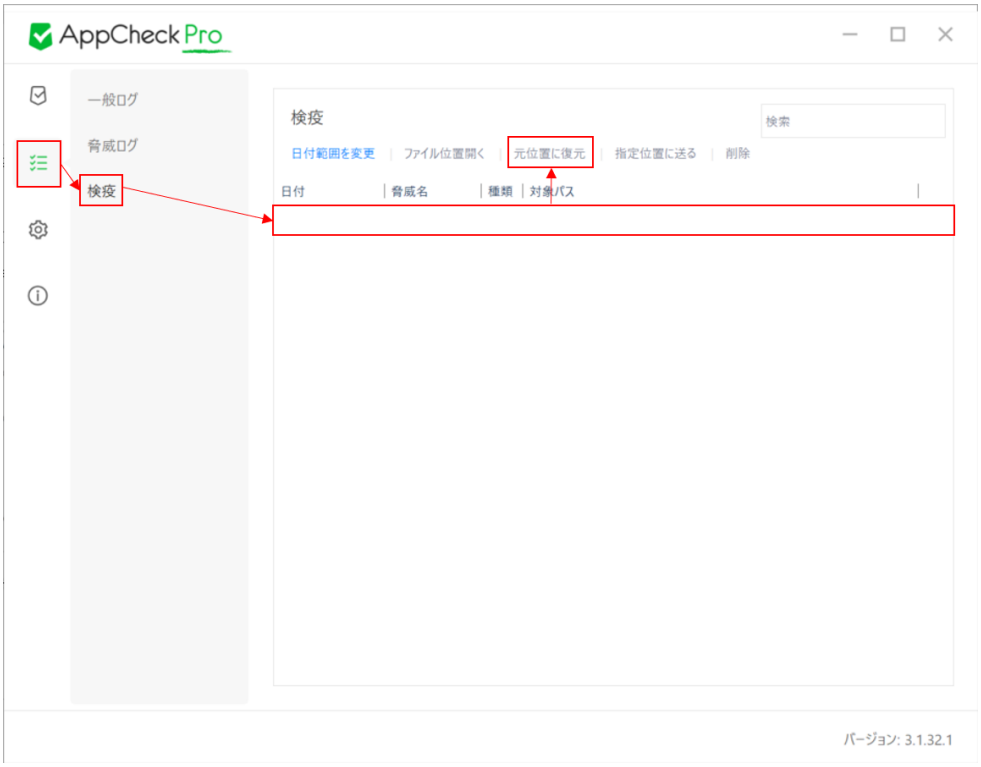
2. 【CMS無】誤検知対応方法

(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。

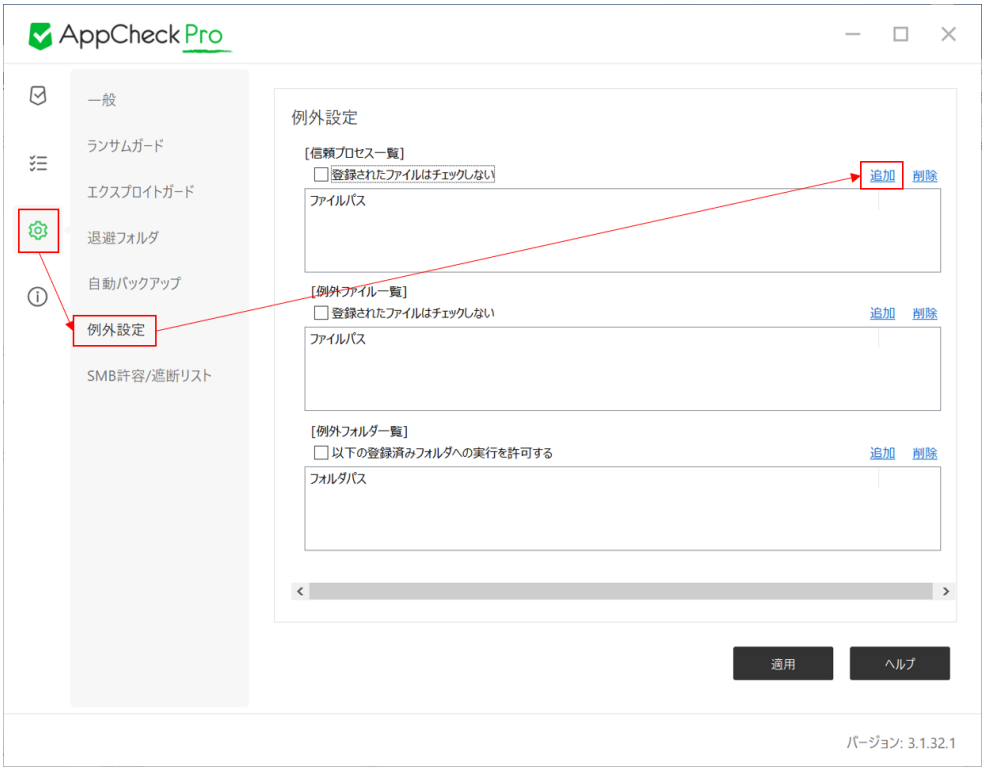
(2)「ツール」>「脅威ログ」から誤検知により「遮断」されたプロセスファイルをご確認ください。



(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。