

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。

CMS Cloud	=										🖧 shi
MALM MEVISATION	エージェント Wite JSecurit	ty								Ноте >	エージェン
ダッシュボード ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	 エージェントリスト								Ŷ	12	~
■ ポリシー管理 く	Event Bacin y (* 1881	- 14月1日 - 14日 - 140 - 1		# X~07~77+6-	501125 ¥ 1-0+	2 h 2016					
₽ エージェント								検索	0 ⊞-	4 -	*
▲ 記布管理 《	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	ポリシーリビジョン	最新ポリシーリビジョン	現状態 (リアルタイムセキュリティ 🌼	最終オンライン時間	1 0 7	-1
■ ログ管理 く			8.1.32.1	基本ポリシー		58	オンライン	アクション	2028-07-05 11:17:	38	<u>-</u>
■ レポート <			3.1.32.1	基本ポリシー	-	58	オンライン	アクション	2023-07-05 11:16:	56	8 A -
白 部署管理 <			3.1.32.1	基本ポリシー		58	オンライン	アクション	2023-07-05 11:16:	53	6 A .
▲ ユーザ管理 <	4										Þ
▶韻定 <	Showing I to 3 of 3 rows										

(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。

申威ログ 検灯	夏所 一般ログ					
			税金		H	1.
换知主体	脊底	0 8239 0	対象バス	0	処理	
シサムガード	ランサムウエアファイル生成	ファイル	C:WUsers¥shinWDocuments¥Wondershare¥Wondershare Filmora¥Download¥Temp¥title¥1_Credit_1_AS¥TempData¥thumbnail.png	ŧ	耶除	
シサムガード	ランサムウエアファイル生成	ファイル	C:VUsersVshinVDocumentsVWondershareVWondershare FilmoraVDownloadVTempVtitleV1_Credit_1_A5Vthumbnail.png	1	夏元	
ンサムガード	ランサムウエアファイル生成	ファイル	C:\Users\shin\Documents\Wondershare\Wondershare Filmora\Download\Temp\title\1_Opener_1\TempData\thumbnail.png	ŧ	川除	
ンサムガード	ランサムウエアファイル生成	ファイル	C:WUsersWshinWDocumentsWWondershareVWondershare FilmoraWDownloadWTempWtitleV1_Opener_1Wthumbnail.png	f	夏元	
ンサムガード	ランサムウエアファイル生成	ファイル	C:WUsers¥shinWDocuments¥Wondershare¥Wondershare FilmoraWDownloadWTemp¥title¥1_Default_LowerthirdWTempOata¥thumbnail.png	1	NIP#	
ンサムガード	ランサムウエアファイル生成	ファイル	C:WUsersWshinWDocumentsWWondershareVWondershare FilmoraWDownloadWTempWtitleW1_Default_LowerthirdWthumbnail.png	1	夏元	
ンサムガード	ランサムウエアアクション検知	ファイル	C:VUsers¥shin¥AppData¥Local¥Wondershare¥Wondershare Filmora¥11.6.7.752¥Wondershare Filmora 11.exe	ł	忠断	

- 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	±				🖧 shir
MALE BAYLGETIN	例外設定			6 Hong	> N#R2
 ▲ ダッシュボード く ■ ボリシー管理 く 	* (MARI)URC		Search	σ ⊞.	*
■ ポリシー常理	□ エージェントID ◎ IPアドレス ◎ MACアドレス ◎ ホスト名 ◎ 06情報 ◎ ユーザ名 部署名 ◎	インストールパージョン 🕴 現状態	◎ 最終オンライン時間	0 9	- 1L
▲ 548 832 		8-1-82-1 オンライン	2078-07-05 11:28:88	•	
# ALE 7 T A 7 BOAL		3.1.32.1 オンライン	2023-07-05 11:22:56		
▲ 自動バックアップ設定		3.1.32.1 オンライン	2023-07-05 11:22:53		
₽ エージェント く	Showing 1 to S of 3 rows				
🔺 記布管理 🔷 🤟					
■ ログ管理 <					
■ Lat-F K					
C) 部署管理 <					
▲ ユーザ管理 く					
▶ @2 <					

(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。

	追加するファイルのバスを入力してください	~
例外設定	Wondershare Wondershare Filmora Wondershare Filmora Launcher.exe	
【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 姓正 削除	OK (4620)	
		Î
		*
【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		
		۵
[例外フォルダー覧]		¥
□ 以下の登録済みフォルタへの実行を許可する 追加 修正 削除		
		A
		保存する 取消

(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。

AppCheck Pro		_		\times
 ○ 一般ログ ● 一般ログ ● 育成ログ ジェ 検疫 ③ ① 	検疫 元位置に復元 指定位置に送る 削除 日付 脅威名 種類 対対/(ス	検索		
		バーシ	วี่อว: 3.1.	32.1

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。

 →般ログ 育威ログ 検疫 ① 	検索 加	理
	バージョン	: 3.1.32.1

(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。

AppCheck Pro			_		\times
 →般ログ 育成ログ 	検疫 元位置に復元 指定位置に送る 削除 日付 脅威名 種類 対象パス	快索			
			バージョ	ョン: 3.1.	32.1

(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。

V	AppCheck Pro		- [) ×
ÿ≡	一般 ランサムガード エクスプロイトガード	例外設定 [信頼プロセスー覧] □登録されたファイルはチェックしない ファイルル「ス	追加	<u>削除</u>
\$ ()	 退避フォルダ 自動バックアップ 例外設定 SMB許容/遮断リスト 	[例外ファイルー覧] □ 登録されたファイルはチェックしない ファイルパス	追加	<u>削除</u>
		[例外フォルダー覧] □ 以下の登録済みフォルダへの実行を許可する フォルダバス	追加	<u>削除</u>
		<	^ <i>I</i> I	> .7
			バージョン:	3.1.32.1

(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。



UJSECURITY