



AppCheck Pro

誤検知対応マニュアル

株式会社 JSecurity

第3版 2025/1/10



目 次

1.	【CMS有】誤検知対応方法	 3
2.	【CMS無】誤検知対応方法	 9



1. 【CMS有】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。

AppCheck Pro			- □	\times
○ 一般ログ	脅威ログ	検索		
并 (mu) 検疫	日付範囲を変更 ファイル位置開く 日付 検知主体 日付 検知主体		処理	1
®	1			
0				
			バージョン: 3.1	1.32.1



(3)「ツール」>「検疫」から、誤検知により削除されたプロセスファイルとデータファイルを選択し、「元位置に復元」で復元してください。

AppChack Pro		×
		- 1 ^
 一般□グ 育成□グ ジェ 検疫 ② ① 	検疫 検索 日付範囲を変更 ファイル位置開く 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	1
		16-21-21-21-21
		バージョン: 3.1.32.1

(4) 以下のURLにアクセスし、CMSにログインします。

https://jp.cms.checkn	nal.com
CMS CLOUD	
使用するにはログインしてください	
日本語 🗸	
EX-V	
パスワード 🔒	
✓ IDを記憶する	
パスワードを忘れた場合 管理者初期登録	



※CMS Cloudから例外設定に関しては、「誤検知が発生したエージェントのみ適用」と「ポリシー単位の設定による一括適用」の二つの方法がございます。もし、誤検知が発生している特定エージェントのみ例外設定を適用する場合は(5)~(9)の手順を実施頂き、AppCheckによる誤検知が行われる同様な動作を複数エージェントで行われており、ポリシー単位の設定による一括適用にて誤検知発生を完全に防ぎたい場合は(10)~(12)の手順を行ってください。

(5) 【該当エージェントのみ例外設定を行う場合】「該当エージェント」>「ツール」>「ログビュー」ボタ ンをクリックします。

CMS Cloud	=									4	s 🖓 shi
INTEL MEVI GATION											> エージェン
A ダッシュボード <	■エージェントリス	<u>۲</u> ۲								全体	v
■ ポリシー管理 く	Export Basic	▼ □ 部業別−所式リシー语	▲ 個別ポリシー	油用 田 協範一括定軍	# K=27=77=6	ダを立にする メエージェン	ノト新修				
₽ エージェント									検索	0 11 - 2	• •
▲ 記布管理 《	レス 🕴 ホストそ	S ⊕ 0S情報 ⊕ ユーザ名	◎ 部署名 ○ イ	シ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	0現状態 0	リアルタイムセキュリティ (最終オンライン時間 ()	ツール
ログ管理 く				8.1.32.1	基本ボリシー		58	オンライン	アクション	2028-07-05 11:17:38	•=•
■ レポート <				8.1.32.1	基本ポリシー	-	58	オンライン	アクション	2023-07-05 11:10:56	= 4
□ 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	= 4
▲ ユーザ管理 <											
▶ 設定 〈	Showing I to 3 of	f 3 rovs									

(6)「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。

脅威ログ 検知	支所 一般ログ			
			税需	H
検知主体	骨底	· 82:59	対象バス	処理
ランサムガード	ランサムウエアファイル生成	ファイル	C:WJsers¥shin∀Documents¥Wondershare¥Wondershare Filmora¥Download¥Temp¥title¥1_Credit_1_A5¥TempData¥thumbnail.png	削除
ランサムガード	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_Credit_1_A5Wthumbnail-png	復元
ランサムガード	ランサムウエアファイル生成	ファイル	C:\Users\shin\Documents\Uondershare\Uondershare Filmora\Download\Temp\tite\I_Opener_1\TempData\thumbnail.png	削除
ランサムガード	ランサムウエアファイル生成	ファイル	C:WUsersWshinWDocumentsWWondershareWWondershare FilmoraWDownloadWTempWtitleW1_Opener_1Wthumbnail.png	復元
ランサムガード	ランサムウエアファイル生成	ファイル	C:WUsers¥shinWDocumentsWWondershareWWondershare FilmoraWDownloadWTemp¥titleW1_Default_LowerthirdWTempDataWthumbnall.png	削除
ランサムガード	ランサムウエアファイル生成	ファイル	C:WUsersWshinWDocumentsWWondershareWWondershare FilmoraWDownloadWTempWtitleW1_Default_LowerthirdWthumbnail.png	復元
ランサムガード	ランサムウエアアクション検知	ファイル	C:¥Users¥shin¥AppData¥Local¥Wondershare¥Wondershare Filmora¥11.8.7.752¥Wondershare Filmora 11.exe	遮断

閉じる

(7)「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		and and a shire a shir
MRIN BAVE GATION	例外設定	國 Home > 例外数3
🚳 ダッジュボード 🔍 🗧		
■ ポリシー管理 🔹	¥ 1明月設定1 初期化	Search 🛛 🕮 - 💙
■ 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 ◎ 05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 🌵 ツール
▲ \$18 £9.2		8+1+32+1 オンライン 2028+07+05 11+23+38 → III
査 返 ² フォルダ 設定		3.1.32.1 オンライン 2023-07-05 11:22:56
■ 例外設定		8.1.32.1 オンライン 2023-07-05 11:22:58 🔳
₽ エージェント ・	Sharing 1 to 3 of 3 rows	
▲ 配布管理 <		
■ ログ管理 <		
■ L-# F <		
D 部署管理 <		
▲ ユーザ管理 <		
⊁ 2£ <		



(8)「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	×
【雪酸深みプロセス-覧】 □ 以下に登録されたプロセスファイルによるファイル変更は検知しない [温加] 修正 削除	
	^
「例外ファイルー覧」 □ 以下に登録されたファイル変更は被知しない 追加 修正 削除	
	A
	-
「例外フォルダー報」 □ 以下に登録されたフォルダ内のファイル変更は検知しない 追加 修正 削除	
	*
	Ŧ
<u>6</u> (7)	する取消

(9)「以下に登録されたプロセスファイルによるファイル変更は検知しない」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。





(10) 【ポリシー単位の設定として、例外設定を一括適用する場合】「ポリシー管理」>「ポ リシー管理」>ご利用されているポリシー(基本ポリシーなど)を選択してください。

CMS Cloud	=												e 1	Shin .
MAIN NAVIGATION	ポ!													
🙆 ダッシュボード 🗸		ポリシー管理												
■ ポリシー管理 く		1000 BA												
□□ ポリシー管理		Export Basic	~	C 部署別一括1	(リシー週用) + 追加	+ Linuciatio	一別除			shin@jiran.com	0	8 ⊞ •	≛ -	*
SVB 1975	0	□ ポリシー名	🗄 Туре 🔅	初期作成時間	⇒最終変更時間	最終適用時間	◊ バージョン ◊	対象エージェント数	適用された	エージェント数 🔅	オンライン	エージェン	ト数	說明
★ 追避フォルタ 設定 面 例外設定														
▲ 自動バックアップ設定		基本ポリシー	Windows	2019-10-28	2024-12-23	-	88	-		-		-		
□ エージェント 〈				16:39:33	16:21:14									
▲ 配布管理 〈														
雪 ログ管理 く		0												
■ レポート <														
Ch 就要链理 (
• - +63678														
▲ ユーザ管理 <		<		_										•
▶ 設定 く	S	howing 1 to 6 of	6 rows 10) - rows per pa	ge									

(11) 「例外設定」>「信頼済みプロセス一覧」>「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。

基本ポリシー	
一般 ランサムガード エクスプロイトガード 道道フォルダ 自動パックアップ 的外級定	
【保護系持プロセス→版】 □ 以下に創設されたプロセスファイルによるファイル接受に目知しない (min) ★E 制限	
	^
	~
【9所ラフィル→版】 □ 以下に登録されたファイル安美には約31.43× 株正 約98	
	^
	Ţ
(例)パラオルダー覧] □ 以下に登録されたフォルダ学校のファイル変更は検知しない 総約 相正 問題	
	^
	Ŧ



(12) 「以下に登録されたプロセスファイルによるファイル変更は検知しない」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。





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。

S AppCheck Pro		_	- 🗆 ×
○ 一般ログ	脅威ログ	検索	
詳書 詳書 詳書 詳書 詳書 # 1 # 2	日付範囲を変更 ファイル位置開く 日付 検知主体 脅威 種類 対象パス		処理
®	7		
0			
			° ≥ ¹ −24 2 4 22 4
		7	ーンヨン: 3.1.32.1



(3)「ツール」>「検疫」から、誤検知により削除されたプロセスファイルとデータファイルを選択し、「元位置に復元」で復元してください。

S AppCheck Pro	- 🗆 X
一般ログ 検疫 予成ログ 日付範囲を変更 ファイル位置開く 元位置に復元 指定位置に送る 前日 検疫 日付 脅威名 種類 対象/(ス)	 除
	バージョン: 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。

JSecurity

AppCheck Pro – \Box ×			
Θ	般	例从設定	
šΞ	ランサムガード	レフノ・ムマスー覧] [信頼プロセス一覧] □ 密録されたファイルはチェックしない	→ 追加 削除
Ø	エクスプロイトガード	<u>קר</u>	
	自動バックアップ	[例分77711-覧]	
U	例外設定	 □ 登録されたファイルはチェックしない ファイルルズス 	<u>追加 削除</u>
	SMB許容/遮断リスト		
		[例外フォルダー類] □ 以下の登録済みフォルダへの実行を許可する	追加 削除
		フォルダバス	
		٢	>
		適用	ヘルプ
			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。

