

誤検知対応マニュアル

株式会社 JSecurity

第4版 2025/2/20

1

目次

1.	検疫された	とファイル/プロセスの復元手順	3
2.	例外設定	:(プロセス)手順	5
	2.1.【CMS有】	- ポリシー適用手順	5
	2.2.【CMS有】	エージェント別	7
	2.3.【CMS無】	エージェント別	10
3.	SMB例夕	▶設定(IPアドレス)手順1	1
3.	SMB例 夕 3.1.【CMS有】	▶設定(IPアドレス)手順1 _{全体適用}	L 1 11
3.	SMB例夕 3.1.【CMS有】 3.2.【CMS有】	ト設定(IPアドレス)手順1 全体適用 エージェント別	L 1 11 13
3.	SMB例夕 3.1.【CMS有】 3.2.【CMS有】 3.3.【CMS無】	ト設定(IPアドレス)手順1 全体適用 エージェント別 エージェント別	L 1 11 13 16

1. 検疫されたファイル/プロセスの復元手順

(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。

※Windowsシステムが提供するプロセス、及びデジタル署名を取得しているプロセスは遮断で留まり、AppCheckにより検疫/隔離されません。(例:Windows標準プロセスcmd.exe等)

S	AppCheck Pro						_	
Ø	一般ログ							
		脅威ログ					検索	
š≡	脅威ログ	日付範囲を変更	ファイル位置開く					
	検疫	日付	検知主体	脅威	種類	対象パス		処理
~		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
<u>9</u>		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
î)		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	OneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 18:25:11	ランサムガード	ランサムウエアアク	ファイル	C:¥Windows¥syst	em32¥cmd.exe	遮断
		2025/02/18 17:59:46	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 17:59:46	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 17:59:46	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 17:59:46	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 17:59:46	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	OneDrive¥デスクト	復元
		2025/02/18 17:59:46	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	OneDrive¥デスクト	復元
		2025/02/18 17:59:46	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 17:59:45	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 17:59:45	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元
		2025/02/18 17:59:45	ランサムガード	ランサムウエアファ	ファイル	C:¥Users¥kurok¥C	DneDrive¥デスクト	復元

バージョン: 3.1.39.3

(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。

v /	AppCheck Pro	_				— 🗆
3	一般ログ	検疫			档	
Ξ	脅威ログ	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	置に送る 削除	
	検疫	日付	育威名	種類 対象パス		
<u> </u>		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
\$		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
\ \		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
/		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 18:25:11	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 17:59:46	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 17:59:46	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	ブ¥調査ツール¥appcheck_t
		2025/02/18 17:59:46	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	ブ¥調査ツール¥appcheck_t
		2025/02/18 17:59:46	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 17:59:46	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	ブ¥調査ツール¥appcheck_t
		2025/02/18 17:59:46	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 17:59:45	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 17:59:45	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 17:59:45	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t
		2025/02/18 17:59:45	ランサムウエアファイル生成	ファイル C:¥Users¥	kurok¥OneDrive¥デスクトッ	プ¥調査ツール¥appcheck_t

バージョン: 3.1.39.3

2. 例外設定(プロセス)手順

・誤検知により「遮断」されたプロセスを、AppCheckの例外設定(ホワイトリスト)機能を利用し検知対象外 に設定することで、再度誤検知してしまう動作を防ぐことができます。

※CMS Cloud ・・・【ポリシー別設定】、【エージェント別】の2パターンで設定可能AppCheck (CMS無) ・・・【エージェント別】のみの1パターンで設定可能

2.1. 【CMS有】ポリシー適用手順

(1) 下のURLにアクセスし、CMSにログインします。

https://jp.cms.checkmal.com

CMS CLOUD
使用するにはログインしてください
日本語 🗸
E×−ル ▼
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

(2)「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		🖧 shi
	エージェント Wite Jaconty a New York	エージェン
 あ ダッシュボード く ■ ポリシー管理 く 	皇エージェントリスト	~
□ I-9I>	Export Basic v C 営業所一般ポリシー連用 金融第ポリシー連用 田田福一級文庫 ダイックアップフェルタを全立にする X エージェント総数 総合 〇 田・ 乙・	~
▲ 記布管理 〈	レス 🔋 木スト名 🔋 00倍線 🕴 ユーザ名 🔋 部署名 🗧 インストールバージョン 🕆 米リシー名 🦂 ポリシーリビジョン 🔋 最新ポリシーリビジョン 🔋 現状地 🖉 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 基本ホリシー - 58 オソシーン 7クション 2023-07-55 TT-11-32 M	= A
	3.1.32.1 養木ポリシー - 59 オンライン アクション 2023-07-05 11:116:56	= 4
□ 部署管理 <	8.1.12.1 基本ポリシー - 58 オンライン アクション 2023-07-45 11:16:53	= 4
		•
▶ 銀定 《	Showing I to 3 of 3 revs	

(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。

骨威ログ 検知	支所 一般ログ				
			税需		
検知主体	春威	0 8230 O	対象バス	0 死	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:WUsersWshinWDocumentsWWondershareVWondershare FilmoraWDownloadWTempWtitleW1_Credit_1_A5WTempDataWthumbnail.png	BUR	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:WUsersVshinVDocumentsVWondershareVWondershare FilmoraVDownloadVTempVtitleV1_Credit_1_ASVthumbnail.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:WUsersWshinWDocumentsWWondershareWWondershare FilmoraWDownloadWTempWtitleW1_Opener_1WTempDataWthumbnail.png	aus	
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¥shinWDocumentsWWondershare¥Wondershare FilmoraWDownload¥Temp¥title¥1_Default_Lowerthird¥TempData¥thumbnail.png	MI	18
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:WUsers¥shin¥AppData¥Local¥Wondershare¥Wondershare Filmora¥11.6.7.752¥Wondershare Filmora 11.exe	遊	新

閉じる

(4) 「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	= 2	shin
MAIN NAVIGATION	ポリシー管理 <u>& Home > パリ</u> シー	管理
■ ポリシー管理 く		
□□ ポリシー管理	Export Basic V Children - Anto 9-344 + 410 + Linestan - Mile shin@jran.com C III - Z - Y	
🛎 SMB 1302	□ ポリシー名 → Type → 初期作成時間 → 最終変更時間 → 最終適用時間 → パージョン → 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 → 脚	ų
資 過避フォルタ 設定 同 例外設定		
▲ 自動バックアップ設定		
□ I−ジェント <	6 30 10 10 10 10 10 10 10 10 10 10 10 10 10	
▲ 配布管理 <	la <mark>o</mark>	
■ ログ管理 <		
■ レポート く		
ロ 部署管理 く	o	
▲ ユーザ管理 <		
▶設定 <	Showing 1 to 6 of 6 rows 10 - rows per page	

(5)「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(フ アイルのパスまで含めた形)を入力し、「OK」を押してください。

. 基本ボリシー 🖌	
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 自動バックアップ 一部所設定	
(1985年)プロセスー第] □ 以下に登録されたプロセスファイルによるファイルを実は特別しない (100) 本王 (100)	
	^
	-
18967フィルー型1 □ 以下に登録とれたファイル支援を見ない 追加 単正 勝勝	
	•
	-
(例外フォルジー覧) □ 以下に認識えてはこクォルジサのファイル変更は特別しない 追加 利正 削除	
	^
	Ŧ

(6)「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。



2.2. 【CMS有】 エージェント別

(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	https:/	//jp.cms.	checkma	l.com
-----------------------------	---------	-----------	---------	-------

CMS CLOUD
使用するにはログインしてください
日本語 🗸
EX-JV
パスワード
✓ IDを記憶する ログイン
パスワードを忘れた場合 管理者初期登録

(2)「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	= e d	shī
MAIN MEVISATION	エージェント Wife Jaconty a New Street	ジェント
ダッシュボード ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・		
■ ポリシー管理 く	12 − 1 − 1 − 1 − 1 − 1 − 1 − 1 − 1 − 1 −	•
□ エージェント	Export Basic C 回着具一板灯りシーム目 品 者形式パリシーム目 田田田一田安里 # パックアップフロ69ち空ロビアら X エージェント組織 社会 〇 田・ ▲ ▲	•
▲ 記布管理 <	レス 🔹 木スト名 🔹 (6情報 🗧 ユーザ名 👘 部署名 🕴 インストールパージョン 🔹 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 🔹 最新ポリシーリビジョン 🔹 載新ポリシーリビジョン 🔹 載新ポリシーリビジョン	r
11日 ログ管理 く	3-1.次.1 基本ポリシー - 50 オンライン アクション 2015-07-60 T111-33 争目	
■ L-#= F <	3.1-132.1 製木作りシー - 50 オンライン アクション 2023-07-63 11:116:36 🖬	
□ 部署常理 <	8.1.32.1 基本ポリシー - 58 オンライン アクション 2023-07-05 1116-33 🖬	
▲ ユーザ管理 <		
▶ 銀定 <	Dhowing 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。

脅威ログ 検	支所 一般ログ			
			検索	III
検知主体	春飯	· 19:19 ·	対象バス	0 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:WUsersWshinWDocumentsWWondershareWWondershare FilmoraWDownloadWTempWtitleW1_Credit_1_A5WTempDataWthumbnail.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:WUsersVshinWDocumentsVWondershareVWondershare FilmoraVDownloadWTempVtitleV1_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:WUsersWshinWDocumentsWWondershareWWondershare FilmoraWDownloadWTempWtitleW1_Opener_1WTempDataWthumbnail.png	削除
ランサムガー F	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:WUsersWshinWDocumentsWWondershareWWondershare FilmoraWDownloadWTempWtitleW1_Default_LowerthirdWTempDataWthumbnail.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: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:VUsers¥shin¥AppData¥Local¥Wondershare¥Wondershare Filmora¥11.6.7.752¥Wondershare Filmora 11.exe	遮断

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	-	l 🖧 shir		
HEIN BAVE GATE ON	例外設定 🔹	ione > 915122		
🚳 ダッシュボード 🔍	2 < KINADZI JUNE			
■ ポリシー管理 く	Earch D	1. Y		
■ ポリシー管理	□ エージェント10 ◎ 1Pアドレス ◎ MACアドレス ◎ ホスト名 ◎ 05価程 ◎ ユーザ名 夢音名 ◎ インストールパージョン ◎ 現状態 ◎ 発発オンライン時間 ◎	ツール		
■ 380 設定 ● 初期フォレガ 設定		▶		
■ 例外設定	3.1.32.1 725-72 2023-07-06 11:22:96	-		
▲ 自動バックアップ設定	3/1/32/1 X/25/2 2022/9//96/11/22/35			
₽ エージェント く	Bhoring 1 to 3 of 3 rees			
▲ 記布管理 <				
■ ログ管理 <				
E µ#∽F K				
□ 部署管理 <				
▲ ユージ管理 <				
וא ביי אינע אינע אינע אינע אינע אינע אינע אי				

(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(ファイルのパスまで含めた形)を入力し、「OK」を押してください。

例外設定	×
【依頼済みブロセス−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 [追加]#i正 勝節	
	*
	÷
【朝外ファイル─覧】 □ 以下に登録されたファイル変更は検知しない 追加 修正 開除	
	•
	÷
- 「男外フォルダー類」 □ 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	
	*
	.
	27-7 Z 101W

(6)「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。



2.3. 【CMS無】 エージェント別

(1)「オプション」>「例外設定」>「信頼プロセス一覧」>「追加」により、誤検知プロセスファイルを入 カし、追加してください。

V	AppCheck Pro		- 0	\times
) S	一般 ランサムガード	例外設定 [信頼プロセス一覧] □ 登録されたファイルはチェックしない	道加 建	<u>判除</u>
\$	エクスフロイトカート 退避フォルダ 自動バックアップ	ファイルパス [例外ファイルー覧]		
	例外設定 SMB許容/遮断リスト	□ 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>1186</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		<u>判除</u>
		< 適用	ヘル <i>プ</i>	>
			バージョン: 3.	.1.32.1

(2)「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。

S 4	AppCheck <u>Pro</u>		- 0	×
\boxdot	—般	例外設定		
* ==	ランサムガード エクスプロイトガード	[信類プロセス一覧] [ジ]登録されたファイルはチェックしない]	<u>追加</u>	<u>削除</u>
0	退避フォルダ	ファイルバス C:¥Users¥shin¥AppData¥Local¥Wondershare¥Wondershare Filmora¥Wondershare Filmo	ra	
ĺ	自動バックアップ 例外設定	[例外ファイル−覧] □ 登録されたファイノレはチェックしない	<u>追加</u>	<u>削除</u>
	SMB許容/遮断リスト	77416/13		
		[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	追加	削除
		7711/31(2		
		<		>
		適用	へル ;	Ĵ
			バージョン:	3.1.32.1

3. SMB例外設定(IPアドレス)手順

・誤検知により「遮断」されたIPアドレスを、AppCheckのSMB例外設定(ホワイトリスト)機能を利用し検知 対象外に設定することで、再度誤検知してしまう動作を防ぐことができます。

※CMS Cloud ・・・【全体設定】、【エージェント別】の2パターンで設定可能AppCheck (CMS無) ・・・【エージェント別】のみの1パターンで設定可能

3.1.【CMS有】全体適用

(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

CMS CLOUD	
使用するにはログインしてください	
日本語	~
Е X — Л/]
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	

(2)「SMB設定」>「共通」>「許容されたアドレス一覧」の「追加」をクリックしてください。

CMS Cloud	=	e 4 ⁰ #
MAIN NAVIGATION	SMB設定	øa Home ≥ SMB ≣
& ダッシュボード < <	井通 エージェント	
■ ポリシー管理 く	許容されたアドレス一長追加削除	
■ ポリシー管理		
▲ SMB 設定		-
■ 例外設定		
💁 自動バックアップ設定		
□ エージェント		-
▲ 配布管理 <		
こ ログ管理 く		
■ レポート く		
い 部署管理 くり くうしん おおお しんかん しんかん しんかん しんかん しんかん しんかん しんか		
▲ ユーザ管理 <		
▶ 設定 〈		

(3) 追加するIPアドレスを入力し、「保存する」をクリックしてください。

許容されたアドレス一覧	×
IP v4 - 個別 : 192.168.1.1 - 順次 : 192.168.1.1-10 (192.168.1.10 ~ 192.168.1.10 まで許容) - 全体 : 192.168.1.0/24 (192.168.1.1 ~ 192.168.1.255 まで許容)	
IP v6 - 個別 : 2001:0DB8:1000:0000:0000:0000:1111:2222 - 順次 : 2001:DB8:1000::1111:2222-3333 (2001:DB8:1000::1111:2222 ~ 2001:DB8:1000::1111:3333 まで許容) - 全体 : 2001:DB8::/32 (2001:0DB8:0000:0000:0000:0000:0000 ~ 2001:0DB8:FFFF:FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	
123. 123. 123. 123	

保存する

閉じる

(4)「許容されたアドレス一覧」に入力したIPアドレス記載されていることを確認してください。



3.2. 【CMS有】 エージェント別

(1) 以下のURLにアクセスし、CMSにログインします。

https://jp.cms.checkr	mal.com
CMS CLOUD	
使用するにはログインしてください	
日本語 🗸	
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	

(2)「ポリシー設定」>「SMB設定」をクリックしてください。

CMS Cloud	≡
MAIN NAVIGATION	SMB設定
🖚 ダッシュボード	
■ ポリシー管理	共通 エージェント
■ ポリシー管理	計合されにアドレス一見 温加 削除
📥 SMB 設定	
 	
🖵 エージェント	c
▲ 配布管理	c
ヨログ管理	¢
■ レポート	¢
口 部署管理	c la
▲ ユーザ管理	¢
▶ 設定	

(3)「エージェント」>「ツール」をクリックし、「SMB許容/遮断リスト」を表示してください。

CMS Cloud	= 🖉 🖉 dhin
MAIN NAVIGATION	SMB設定 @ How > 398 設定
ダッシュボード <	共通 エージェント
■ ポリシー管理 く	x and/2007/00/1
 ■ ボリシー管理 ▲ SMB 設定 	Search 2 III - V
賽 退避フォルダ 設定	□ Agent 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 ◎ インストールパージョン ◎ 現状態 ● 最終オンライン時間 ◎ ツール
₽ エージェント く	
▲ 配布管理 <	atoming Lo For Froms
目 ログ管理 く	
■ レポート <	
□ 部署管理 〈	
▲ ユーザ管理 く	
▶ 該定 く	

(4) 「遮断されたアドレス一覧」にあるIPアドレスを選択し、「常時許容」をクリックしてください。

	SMB許容/遮断リスト	
	許容されたアドレス一覧 追加 削除	
	遮断されたアドレス一覧 臨時許容 常時許容	
-	常時許容:遮断された遠隔地IPアドレスを「常時許容」する(ホワイトリ	ストとして常に許容)
-	臨時許容:遮断された遠隔地IPアドレスを「臨時許容」する(再度検知]が発生するまで許容)
(5)	「許容されたアドレス一覧」に追加されていることを確認してください。	

SMB許容/遮断リスト

許容されたアドレス一覧 追加 削除

132. 132. 132. 132

遮断されたアドレス一覧 臨時許容 常時許容

15

3.3. 【CMS無】 エージェント別

(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)「オプション」>「SMB許容/遮断リスト」を表示し、「遮断されたアドレス一覧」に記載されているア アドレスを選択し「常時許容」をクリックしてください。

⊘ ≆≣ ©	一般 ランサムガード エクスプロイトガード 退避フォルダ 自動パックアップ 例外設定	SMB許容/遮断リスト 許容されたアドレス一覧 アドレス			追加 削除	
¥≣ ©	ランサムガード エクスプロイトガード 退避フォルダ 自動バックアップ 例外設定	許容されたアドレス一覧 アドレス			<u>追加 削除</u>	
\$	エクスプロイトガード 退避フォルダ 自動バックアップ 例外設定	7۴レス				
بو ن آ	退避フォルダ 自動バックアップ 例外設定					
î	自動バックアップ 例外設定					
ſ	DUZNEZ JE					
	SMB許容/遮断リスト	遮断されたアドレス一覧		臨時許容	常時許容	
U		アドレス	遮断時間	遮断満了時間		
				適用	7,11,7	f

(3)「許容されたアドレス一覧」に追加されていることを確認してください。

AppCheck Pro – \Box ×							
Ø	一般	SMD 許容 / 使新日子					
\$ <u> </u>	ランサムガード	SIVIDAT台/巡回り入下 許容されたアドレス一覧			<u> 自加</u> 削除		
	エクスプロイトガード	78L7 192.168.48.192					
Ø	退避フォルダ						
(j)	自動バックアップ						
	例外設定						
	SMB許容/遮断リスト	遮断されたアドレス一覧		<u>臨時許容</u> 渡艇業了時間	<u>常時許容</u>		
				適用	へルブ		
パージョン: 3.1.39.3							

4. 補足

(1) プロセスの例外設定(誤検知が行われるプロセスの登録)時のメリット・デメリットについて

・メリット:正規プロセスから行われた正常なファイル処理がAppCheckにて誤検知されることを防ぐことができます。

・デメリット:該当プロセスから行われるファイル処理を全て許可することになるため、もし設定した該当プロセスからファイル毀損が行われても検知されなくなります。

- ※汎用的なプログラム等は、場合によってはランサムウェア攻撃に悪用されるプロセスがある為、安易に 例外設定を行うことはお奨めできません。どうしても、誤検知が頻発してしまう場合は、エージェント別 の例外設定されることをお奨めいたします。
- (2) SMB例外設定(誤検知が行われるIPアドレスの登録)時のメリット・デメリットについて

・メリット: 遠隔地PCから行われた正常なファイル処理がAppCheckにて誤検知されることを防ぐことができます。

・デメリット:遠隔地PCのIPアドレスから行われるファイル処理を全て許可することになるため、もし設定したIPアドレスからファイル毀損が行われても検知されなくなります。

※上記のデメリットがあるため、誤検知対策として、SMB例外設定は行わず、運用方法(例:ファイル 一括削除の数を少なくする等)の変更で対応して頂くことが望ましいです。 (3) SMBサーバ保護機能の各設定パターンによる挙動について

	学動	遠隔地からのアクセス遮断
SMB サーバー保護機能が 「ON」状態	変更を受けるサーバー側のファイルが「保護するフ ァイル拡張子」に該当すれば、ランサムウェアの攻 撃として判断し、検知・遮断・リアルタイムバックア ップ(サーバー側)による <mark>自動復元を行います。</mark> ※「脅威ログ」と「検疫」にて詳細確認可能	遮断される
SMB サーバー保護機能が 「ON」状態で、遠隔地の IP アドレスが「例外設定」に登 録済み	変更を受けるサーバー側のファイルが「保護するフ ァイル拡張子」に該当すれば、遠隔地からのアク セスは遮断しないが、検知・リアルタイムバックアッ プ(サーバー側の退避フォルダ内)は行うため、 手 動作業による復元が可能です。 ※ログは残らない	遮断されない
SMB サーバー保護機能が 「OFF」状態	変更を受けるサーバー側のファイルが「保護するフ ァイル拡張子」に該当すれば、遠隔地からのアク セスは遮断しないが、検知・リアルタイムバックアッ プ(サーバー側の退避フォルダ内)は行うため、 手 動作業による復元が可能です。 ※ログは残らない	遮断されない
補足説明	手動復元の方法としては、エクスプローラー 上で「退避フォルダ」から、元場所への上書き コピーとなります。	※1時間の間、該当 IP ア ドレスからサーバーへのアクセ スが遮断されます。遮断後 「臨時許容」や「常時許容」 機能によりアクセス許可がで きます。