



株式会社 JSecurity

第十一版 2021/03/08

はじめに

このたびは、ランサムウェア対策ソフト AppCheck Pro for Windows Server をお買い上げいただき誠にありがとうご ざいます。本製品の機能を十分に活用していただくために、ご使用になる前に本書をよくお読みください。また本書をお読 みになった後は必ず保管してください。使用方法がわからない、機能についてもっと詳しく知りたいときに参考にして下さい。

製品名について

AppCheckはランサムウェア対策ソフトの製品ブランドの総称です。弊社では評価版と製品版を区別するために 評価版を「AppCheck」、製品版を「AppCheck Pro」と呼んでいます。

ご注意

本製品の誤作動・不具合などの外的要因、または第三者による妨害行為などの要因によって生じた損害などの純粋 経済損失につきましては、当社は一切その責任を負いかねます。

通信内容や保持情報の漏洩、改竄、破壊などによる経済的・精神的損害につきましては、当社は一切その責任を負いかねます。

ソフトウェア、外観に関しては、将来予告なく変更されることがあります。 最新リリース情報は AppCheck のホームページ (https://www.appcheck.jp/support/) でご確認ください。

著作権について

本書は AppCheck Pro for Windows Server をお買い上げいただいたお客様、および評価版をご利用のお客様 に提供されます。

取扱説明書(イメージ、写真、音楽、テキストを含めますが、それだけに限りません)の文書、および複製物についての 権限および著作権は、株式会社JSecurityが有するもので、ソフトウェア製品は著作権法および国際条約の規定に よって保護されています。お客様は、取扱説明書の文書を複製・配布することはできません。

株式会社JSecurityが事前に承諾している場合を除き、形態および手段を問わず、本書の記載内容の一部、または 全部を転載または複製することを禁じます。

本書の作成にあたっては細心の注意を払っておりますが、本書の記述に誤りや欠落があった場合も株式会社 JSecurityはいかなる責任も負わないものとします。

本書の記述に関する、不明な点や誤りなどお気づきの点がございましたら、弊社までご連絡ください。 本書および記載内容は、予告なく変更されることがあります。

バージョンについて

本マニュアルはAppCheck Pro for Windows Server 2.5.51.5を参考に作成しています。

目 次

1. 製品のセットアップおよびアンインストール	1
1.1.製品のセットアップ	1
1.2.AppCheck Pro for Windows Server 製品登録確認	4
1.3.AppCheck Pro for Windows Server アンインストール	6
2. AppCheck メニュー構成	9
2.1.メイン画面メニュー構成	9
2.2 リアルタイムセキュリティ	10
2.3 MBR保護 エラー! ブックマークが定 す	遠されていません。
2.4 ネットワークドライブ保護	11
3. AppCheck メニュー詳細	12
3.1 ツール	
3.1 ツール 3.1.1 ツール:脅威ログ	
3.1 ツール 3.1.1 ツール:脅威ログ 3.1.2 ツール:一般ログ	
 3.1 ツール 3.1.1 ツール:脅威ログ 3.1.2 ツール:一般ログ 3.1.3 ツール:検疫 	
 3.1 ツール 3.1.1 ツール:脅威ログ 3.1.2 ツール:一般ログ 3.1.3 ツール:検疫 3.2 オプション 	
 3.1 ツール 3.1.1 ツール:脅威ログ 3.1.2 ツール:一般ログ 3.1.3 ツール:検疫 3.2 オプション 3.2.1 オプション:一般 	
 3.1 ツール 3.1.1 ツール:脅威ログ 3.1.2 ツール:一般ログ 3.1.3 ツール:検疫 3.2 オプション 3.2.1 オプション:一般 3.2.2 オプション:ランサムガード 	12 12 13 14 16 16 22
 3.1 ツール 3.1.1 ツール:脅威ログ 3.1.2 ツール:一般ログ 3.1.3 ツール:検疫 3.2 オプション 3.2.1 オプション:一般 3.2.2 オプション:ランサムガード 3.2.3 オプション:退避フォルダ 	12 12 13 14 14 16 16 22 24
 3.1 ツール 3.1.1 ツール:脅威ログ	12 12 13 14 14 16 16 22 24 24 25
 3.1 ツール 3.1.1 ツール:脅威ログ	
 3.1 ツール	12 12 13 14 14 16 16 22 24 24 25 26 27

1. 製品のセットアップおよびアンインストール

1.1. 製品のセットアップ

AppCheck Pro for Windows Server は、Windows Server 2008 R2以降のOSで インストールが可能です。

(1) AppCheck Pro for Windows Serverをインストールする前に実行中のすべてのプログラムを 終了し、その後インストールを行ってください。「次へ」をクリックします。

큟 AppCheck セットアップ	- 🗆 X
CHECKMAL	AppCheck セットアップ ウィザードへようこそ
	このウィザードは、AppCheckのインストールをガイドしていきます。 セットアップを開始する前に、他のすべてのアプリケーションを終了 することを推奨します。これによってセットアップがコンピュータを再 起動せずに、システム ファイルを更新することが出来るようになりま す。 続けるには [広へ] をクリックして下さい。
	次へ(N) > キャンセル

(2) ライセンス契約書(ソフトウェア使用許諾契約書)をお読みになり、同意する場合は「同意する」 ボタンをクリックしてください。セットアップを開始します。





(3) AppCheck Pro for Windows Serverは "C:¥Program Files¥CheckMAL¥App Check"を標準のインストールフォルダとしています。変更するときには「参照」ボタンによりインストール先を指定してください。「インストール」ボタンをクリックすることによりインストールを開始します。

😨 AppCheck セットアップ	_		×
インストール先を選んでください。 AppCheckをインストールするフォルダを選んでください。	СНЕ	CKMAL	
AppCheckを以下のフォルダにインストールします。異なったフォルダにインストー 押して、別のフォルダを選択してください。 インストールを始めるには [インストー) い。	ルするには い をクリック	、[参照] を たして下さ	
インストール先 フォルダ ^{C¥Program Files¥CheckMAL¥AppCheck}	参照(F	V	
必要なディスクスペース: 62.7 MB 利用可能なディスクスペース: 145.9 GB AppCheck 2.5.43.4			
< 戻る(B) インスト・	ール	キャンセル	V

(4)「インストール」ボタンをクリックすることによりインストールを開始します。

蒙 AppCheck セットアップ		_		\times
インストール AppCheckをインストールしています。しばらくお待ちくだ	さい。	Sici	HECKMAL	
Installing product				
AppCheck 2.5.43.4				
	< 戻る(B))次へ(N) >	キャンセル	Ψ.

(5) インストールが完了した後「完了」ボタンをクリックするとAppCheckが自動的に起動します。



(注) AppCheckの起動時に、「AUTO UPDATE(自動更新)」を行う場合があります。

自動更新とは、お客様のPCにインストールしたAppCheckより新しいバージョンが存在した場合、 自動的にダウンロードを行い、セットアップを開始することを言います。

1.2. AppCheck Pro for Windows Server 製品登録確認

(1)「Eメールアドレス」と「ライセンスキー」を入力し、確認ボタンを押すと評価バージョンから<u>製品バージ</u> <u>ョンに更新されます。</u>

※ CMS 版 (CMS よりインストールファイルをダウンロード)の場合、プログラムインストール後に、ライ センス情報が自動的に登録されるため、製品登録は必要ありません。

S AppCheck	- ×
`	ランサムウェアの脅威から 安全に保護されています。
AppCheck 製品登録 × 1.製品購入 AppCheck 3企業で使用する場合や、全ての機能を使用したい方は有料 版の「AppCheck Pro」をご購入ください。 今購入する AppCheck Proの詳細 2.オンライン製品登録 Eメールアドレス うイセンスキー	
※製品購入や製品登録をする時はインターネットに接続が必要です。 確却	

🗸 АррС	heckPro	_	×
6	AppCheck 教品登録 1.製品購入 AppCheck 8企業で使用する場合で、全ての機能を使用したい方は有料 成のTAppCheck Pro. 本ご購入ください。	× _ム ウェアの脅威から 呆護されています。	
リアルタ MBR係 ネットワ	AppCheck × 2.オンライ Eメール7 フィセン OK ※製品購入や製品量類をする時はインターネットに接続が必要です。 通知		
リアルタ MBRቒ ネットワ	2.オンライ 正常に製品登録されました。 (サービス凍了日 = 2018年3月23日) アイセン X製品購入や製品登録をする時はインターネットに接続が必要です。 通際		

(2)サービス満了日は製品登録日から起算し、1年後となります。(1年ライセンス場合)

(3) 製品登録が完了すると、画面上部の表記が「AppCheck」→「AppCheck Pro」となります。

Seperation AppCheck		- ×	AppCheck	「ロゴ(無償版)
AppCheck Pro		- ×	AppCheck	Pro ロゴ(有料版)
S AppCheck	Pro			- ×
	AppCheck ライセンス ※ AppCheck Pro製品	品をご購入いただきありが。	とうございます。	Pの脅威から 1ています。
`	製品登録情報 Eメールアドレス			
リアルタイムセキュ	ライセンスキー ライセンス数			
MBR保護	サービス満了			- //
ネットワークドライ			確認	

登録頂いた「Eメールアドレス」「ライセンスキー」「満了日」「数量」をご確認頂き、AppCheck Proをご利用下さい。

1.3. AppCheck Pro for Windows Server アンインストール

本製品をアンインストールする場合は、次の手順にて行ってください。

- (1) コンピュータ上で起動しているすべてのアプリケーションを終了します。
- (2)「設定」→「アプリと機能」のプログラムリストに登録されている"AppCheckアンチランサムウェア"を選択し アンインストールを実行します。

		プログラムと機能	L	_ □	x
0	🕒 💿 🔻 🕈 📷 « রুৎতে১১	ントロール パネル項目 → プログラムと機能 > 0	プログラムと機能の検索		Q,
	コントロール パネル ホーム インストールされた更新プログラムを 表示	プログラムのアンインストールまたは変更 カグラムをアンインストールするには、一覧からカログラムを選択して [アンインストール]、[変更]、ま	こは [修復]	
6	Windows の機能の有効化または 無効化	至7797049。 整理 ▼		•	۲
	ネットワークからプロクラムをインスト −ル	名前 AppCheckアンチランサムウエア Immorosoft Visual C++ 2008 Redistributable - x64 9.0.3 Microsoft Visual C++ 2008 Redistributable - x86 9.0.3 WWare Tools	発行元 CheckMAL Inc. Microsoft Corporation Microsoft Corporation VMware, Inc.		

(3)「次へ」をクリックします。



(4)「セキュリティー文字入力」欄に、白い枠内に表示されている数字を入力して「次へ」をクリックします。

🕑 AppCheck アンインスト	~-Jl				-	\times
AppCheckのアンイ ン AppCheckをこのコン	ノストール ビュータから削除	礼ます。		•	CHECKMAL	
AppCheckが自動で削 された文字を入力して	川除されるのを防 こから「次へ」を押	ぐためにセキョ 心てください。	リティー手順を	要求しております	。下記の絵に表示	
	0	2	2	6		
	セキュリティー文	字入力: 022	26			
AppCheck 2.5.43.4			< 戻る(B))次へ(N) >	キャンセル	

(5) AppCheckのインストールされているフォルダが表示されます。「アンインストール」をクリックすることにより 関連フォルダ・ファイルが削除されます。

	_		Х
AppCheckのアンインストール AppCheckをこのコンビュータから削除します。	СНЕ	CKMAL	
AppChecklま、以下のフォルダからアンインストールされます。 アンインストールを IPンインストール] をクリックして下さい。	始めるコま		
アンインストール元: C¥Program Files¥CheckMAL¥AppCheck¥			
AppCheck 2.5.43.4 く戻る(B) アンインストー	-ル(U)	キャンセル	Ψ

(6) AppCheckのアンインストール完了となります。



- 2. AppCheck メニュー構成
 - 2.1. メイン画面メニュー構成

Seperative AppCheck Pro		- ×
製品登録 ソール ・ ・ ・ ・	オプション マアイル 削除 ()	ランサムウェアの脅威から 安全に保護されています。
リアルタイムセキュリティ MBR保護 ネットワークドライブ保護		

製品登録	AppCheck製品案内およびオンライン製品登録	
ツール	検疫、脅威ログ、一般ログ情報の閲覧機能	
オプション	一般、ランサムガード、退避フォルダ、自動バックアップ、ユーザ指定除外ファイル、	
	SMB許容/遮断リスト機能を設定	
ファイル削除	ランサムウェア避難所フォルダ(退避フォルダ)を削除	
リアルタイムセキュリティ	ランサムガード機能のon/offを設定	
MBR保護	Master Boot Record (MBR) 領域を改竄しようとするランサムウェアの実行	
	アクションを遮断	
ネットワークドライブ保護	AppCheckがインストールされたPCで使用されているネットワークドライブをランサム	
	ウェアの攻撃から保護する機能	

2.2 リアルタイムセキュリティ

リアルタイムセキュリティでは、ランサムガード機能、ランサムウェア待避、バックアップファイルの自動削除機能を オン/オフできます。



リアルタイムセキュリティのオン/オフによりタスクバーのお知らせ領域に表示されるAppCheckのアイコンの色が変化します。

AppCheckアンチランサムウエア:リアルタイムセキュリティ中 ^ ✓ 10% + 110%	AppCheckアンチランサムウエア:リアルタイムセキュリティOFF へ ● (信 ①× あ) + 110%
▲ : リアルタイム保護オン	グレイ:リアルタイム保護オフ



2.3 MBR保護

ディスクレベルでデータを暗号化するランサムウェアによる変更に対して、マスターブートレコード(MBR)を保護 します。ランサムウェアによっては一定時間後に強制的にPCを再起動させ、その際にマスターブートレコード (MBR)を暗号化させ、通常Windowsの起動をさせないものもあります。

MBR保護には、MBRを暗号化させない保護機能を提供します。

このスイッチは、オプションーランサムガードーMBR保護 スイッチと連動します。どちらかで行った操作がもう一方に反映されます。

2.4 ネットワークドライブ保護

PC が使用しているネットワークドライブ内のファイルがランサムウェアによって毀損されないように、AppCheck をインストールすると、ランサムウェアの毀損行為を遮断します。

AppCheck がインストールされた端末がランサムウェアに感染し、ネットワークドライブ経由で被害が拡大する ことを防ぎます。

このスイッチは、オプションーランサムガードーネットワークドライブ保護 スイッチと連動します。 どちらかで行った操作がもう一方に反映されます。

3. AppCheck メニュー詳細

3.1 ツール

脅威ログ、一般ログ、検疫情報の詳細を表示します。

3.1.1 ツール:脅威ログ

脅威ログはランサムガード、リアルタイム監視、システム検査により診断(遮断)および削除(治療)された 項目に対する情報を表示します。脅威ログタグの上段のメニューと、リストから右クリックして、選択するメニュー があります。

S AppCheck ツール						_		×
● 毎成日グ	脅威□グ							
 ・ 一般ログ 	日付範囲を変更 フ	ァイル位置開く				検索		م
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	日付	検知主体	森威	種類	対象パス		机理	
12.02	2020/10/08 14:45:45	=>,#1,#_ ピ	DALATIDA (1958		CVI Ison Vaultin VDselten VA as should		~~~	_ '
	2020/10/08 14:46:46	575 <u>L</u> J-F	ランダムウエアファイル破壊	ファイル	C.¥Users¥swkim¥Desktop¥Appcheck	七カロックメー		
	2020/10/08 14:46:46	=>+++++	ランサムウェアファイル破壊	7717	C:#Users#swkim#Desktop#Appcheck	ロンリッンメ_	-1-	
	2020/10/08 14:46:46	フノリム 「ト みばログ 日付新国を亦再		11	ファイル位置間((0))		=	
	2020/10/08 14:46:	有成日/-日刊範四紀友史		11	アイル位置用((0)		л. =	
	2020/10/08 14:46:			11	712	Chillion Chillion		
	2020/10/08 14:46:4	 指定なし 		41	76-	Ctri+C	л. =	
	2020/10/08 14:46:4			211	すべて選択	Ctrl+A	-	- 1
	2020/10/08 14:46:4	○ 過去7日間		11			一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	
	2020/10/08 14:46:4	○ 過去30日間		11	リフレッシュ	F5	л. =	
	2020/10/08 14:46:4	○ ユーザー設定の範囲			CWAINDOW/SY-ustanz20Y-ustanz	seren meren	一般し	
	2020/10/08 14:46:4	2020/11/11			C#WINDOWS#system32#cmd.exe	T	過町	
	2020/10/02 12:14:1	2020/11/11	~ ~ 2020/11/11		Citusers+swkim+Desktop+AppCneck	_lest#image1.png	復元	
	2020/10/02 12:14:02	->+++++	ランサムウエアファイル要撮	7- 41	C#Users#swkim#Desktop#AppCneck	_iest#image2.png	復几	
	2020/10/02 12:14:07		ランサムウエアファイル扱振	ノアイル	C#Users#swkim#Desktop#AppCneck	Test#image3.png	復兀	
	2020/10/02 12:14:07	ランサムガート	ランサムウエアファイル擬損	77176	C:#Users#swkim#Desktop#AppCheck	lest¥image4.png	復兀	
	2020/10/02 12:14:07	ランサムルート	ランサムウェアファイル毀損	77170	C#Users#swkim#Desktop#AppCheck	lest#image5.png	復兀	
	2020/10/02 12:14:07	ランサムガート	ランサムウエアファイル破損	ノアイル	C:¥Users¥swkim¥Desktop¥AppCheck_	lest¥image6.png	復元	
	2020/10/02 12:14:06	ランサムカート	ランサムウェアファイル優損	ノアイル	Ci¥Users¥swkim¥Desktop¥AppCheck_	lest¥image7.png	復元	
	2020/10/02 12:14:06	ランサムカート	ランサムウェアファイル級損	ノアイル	C:#Users#swkim#Desktop#AppCheck_	lest¥image8.png	復元	
	2020/10/02 12:14:05	ランサムカード	ランサムウエアファイル毀損	ファイル	C:¥Users¥swkim¥Desktop¥AppCheck	lest¥image9.png	復元	
	2020/10/02 12:14:05	ランサムカード	ランサムウエアファイル极損	ファイル	C:¥Users¥swkim¥Desktop¥AppCheck_	Test¥image10.png	復兀	
指定なし 55個の項	[目 1個の項目を選択							

日付範囲を変更	脅威ログ情報を日付で検索します。
ファイル位置開く	選択したファイルが存在するフォルダ(ファイル)を開きます。
של–	選択したファイルの詳細ファイル情報をコピーします。
すべて選択	脅威ログに表示されたすべての項目を選択します。
リフレッシュ	脅威ログ情報を更新します。

特にランサムガードで検知した脅威ログにはランサムウェア情報、ファイル自動復元情報、脅迫メッセージ自動削除情報、変更されたファイル名自動復元情報が含まれています。

3.1.2 ツール:一般ログ

一般ログはAppCheck Pro for Windows Server使用時に発生するプログラム開始/終了、サービス 開始/終了、リアルタイム監視開始/終了、ランサムガード開始/終了、アップデート、オプション設定、ランサム ウェアおよびランサムガードお知らせメッセージ等の情報を表示します。一般ログタブをダブルクリックした場合、 再表示し最新の情報を表示することができます。

S AppCheck ツール									_		×
春威ログ	一般	ログ									
 一般ログ 	日付範	囲を変更						検索			, p
検疫	日付		レベル	区分	内容						1.1
	2020/1	1/11 17:29:58	注意	検疫	ファイルを復元	こできません。(コード: 3,位置:	C:¥Users¥swkim¥	Desktop¥App(Check_Test¥i	mag	. 1
	2020/1	1/11 17:00:50	*=	***	ファイルを復元	亡できません。(コード: 3,位置:	C:¥Users¥swkim¥	Desktop¥App(Check_Test¥i	mag	
	202(🌶 一般ログ - 日付範囲	を変更		ファイルを復元	こできません。 (コード: 3,1		p	Check_Test¥i	mag	
	202(クリーナー検査	こが中断されました。	コクリックメ:	<u> </u>			
	202(● 指定なし			クリーナースキー	ャンが開始されました。()					
	202(○ 今日			クリーナール	⊐Ľ-	Ctrl+C				
	202(1ーザーがリア)	-+					
	202(1ーザーがリアリ	すべく選択	Ctrl+A	1000	1010-00		
	202(○ 過去30日間			md.exe(22	ביצעיולו	Es	ステム検査を	実行していたさい	A.	
	202(〇 ユーザー設定の	範囲		1ーザーがリアルタ		- 13	VALUE: 42	SPCERMOL	00000	е -
	202(2020/11/11		2020/11/11	1-ザーガリアルタ	イムセキュリティを停止しました。					
	2026, .	1/00 1101101	114		プションを再設定	しました。					
	2020/1	1/09 14:07:04	一般	サービスプログラム	ユーザーがリアルタ	イムセキュリティを開始しました。					
	2020/1	1/09 14:06:58	一般	サービスプログラム	ユーザーがリアルタ	イムセキュリティを開始しました。					
	2020/1	1/09 14:06:58	一般	サービスプログラム	ユーザーがリアルタ	イムセキュリティを停止しました。					

日付範囲を変更	一般ログ情報を日付で検索します。
コピー	選択したファイルの詳細情報をコピーします。
すべて選択	一般ログに表示されたすべての項目を選択します。
リフレッシュ	一般ログ情報を更新します。

3.1.3 ツール:検疫

検疫はAppCheckでランサムガードにより自動治療(削除)されたランサムウェアが隔離されている情報を 表示します。検疫タグの上段のメニューと、リストから右クリックして、選択するメニューがあります。

S AppCheck ツール								- 🗆	×
春威ログ	検疫								
一般ログ	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 削除		検索		م ر
• 検疫	日付		脅威名	種類	対象パス	+	カリックメー		
	2020/10/04 2020/10/04 2020/10/04 2020/10/04 2020/10/04	検疫 - 日付範 ● 指定なし ○ 今日	田を変更		:¥Users¥sw :¥Users¥sw :¥Users¥sw :¥Users¥sw :¥Users¥sw	元の位置に復元(R) 指定位置に保存(X) 削除(D)	Del	mage2.png mage3.png mage4.png mage5.png	
	2020/10/0i 2020/10/0i	○ 過去7日間 ○ 過去30日	間		:¥Users¥sw :¥Users¥sw	ファイル位置開く(O) コピー	Ctrl+C	mage6.png mage7.png	
	2020/10/04 2020/10/04 2020/10/04	〇 ユーザー影 2020/11	定の範囲 /11 2020/1	1/11	:¥Users¥sw :¥Users¥sw :¥Users¥sw	ー すべて選択 リフレッシュ	Ctrl+A F5	mage8.png mage9.png mage10.png	
	2020/10/02 1	2:14:08	ランサムウェアファイル吸損	ノアイノレ	C:¥Users¥sw		e		
	2020/10/02 1	2:14:08	ランサムウエアファイル毀損	ノアイル	C:¥Users¥swkim	1¥Desktop¥AppCheck_lest¥image2	2.png		
	2020/10/02 1	2:14:07	ランサムウエアファイル設備	7711	C:#Users#swkim	1#Desktop#AppCneck_lest#image:	s.png		
	2020/10/02 1	2:14:07	ランサムウエアファイル毀損	ファイル	C:#Users#swkin	1#Desktop#AppCheck_test#image	spng Spng		
	2020/10/02 12	2:14:07	ランサムウェアファイル吸損	ファイル	C:¥Users¥swkin	HDesktop#AppCheck_Test#image	5.png		
	2020/10/02 12	2:14:06	ランサムウエアファイル毀損	ファイル	C:¥Users¥swkim	1¥Desktop¥AppCheck_Test¥image	.png		
	2020/10/02 12	2:14:06	ランサムウェアファイル破損	ファイル	C:¥Users¥swkim	1¥Desktop¥AppCheck_Test¥image8	3.png		
	2020/10/02 12	2:14:05	ランサムウエアファイル毀損	ファイル	C:¥Users¥swkim	¥Desktop¥AppCheck_Test¥image).png		
	2020/10/02 12	2:14:05	ランサムウエアファイル級損	ファイル	C:¥Users¥swkim	h¥Desktop¥AppCheck_Test¥image*	I0.png		
	2020/10/02 12	2:12:55	ランサムウェアファイル毀損	ファイル	C:¥Users¥swkim	h¥Desktop¥AppCheck_Test¥image*	l.png		
指定なし 50個の項	目 1個の項目	目を選択							

日付範囲を変更	検疫情報を日付で検索します。
元の位置に復元	選択したファイルを元の位置(フォルダ)に復元します。
指定位置に保存	選択したファイルをユーザが指定した位置(フォルダ)に保存します。
削除	検疫して保存された待避ファイルを削除します。
ファイル位置開く	選択したファイルが存在するフォルダを開きます。
コピー	選択したファイルの詳細ファイル情報をコピーします。
すべて選択	検疫で表示されているすべての項目を選択します。
リフレッシュ	検疫情報を更新します。

※ログの項目について

脅威ログ	日付	処理した日付を 年/月/日 時:分:秒で表示します。
		UTC 基準はローカルシステム時間です。
	検知主体	該当脅威が探知された主体を意味します。
	脅威	探知主体が探知した内容がどのような脅威であるか表示します。(ファイル名変更、
		ファイル毀損など)
	種類	対象パスに該当する項目がどんなタイプかを表示します。ファイル、レジストリ、ホストな
		ど。
		※探知主体がランサムウェアの場合、ファイルになります。
		但し、IP アドレスでランサム行為が探知された場合、「Host」で表示します。クリーナ
		ーで探知された場合、レジストリやファイルで表示されます。
	対象パス	該当脅威が発生したパスを表示します。 (SBM 探知の場合、IP アドレス (IPv4
		または IPv6)、ファイルの場合はファイルパス)
	処理	探知主体が脅威をどのように処理したか、表示されます。(削除、復元)
一般ログ	日付	ランサムガードのように、該当脅威が探知された主体を意味し
	レベル	危険度を表示します。(一般、注意)
	区分	処理プログラムの区分を表示します。(サービスプログラム、セッションプログラム)
	内容	処理内容を表示します。
検疫	日付	探知した日付を年-月-日 時:分:秒で表示します。 UTC 基準はローカルシステ
		ム時間です。
	脅威名	ランサムウェアの脅威を表示します。(ランサムウェアファイル生成など)
	種類	対象パスに該当する項目がどんなタイプかを表示します。ファイル、レジストリ、ホストな
		ど。
		※探知主体がランサムウェアの場合、ファイルになります。
		但し、IP アドレスでランサム行為が探知された場合、「Host」で表示します。クリーナ
		ーで探知された場合、レジストリやファイルで表示されます。
	対象パス	該当脅威が発生したパスを表示します。(SBM 探知の場合、IP アドレス(IPv4
		または IPv6)、ファイルの場合はファイルパス)

3.2 オプション

3.2.1 オプション: 一般

AppCheckオプション
一般 ランサムガード 退避フォルダ 自動バックアップ ユーザ指定除外ファイル SMB許容/遮断リスト
☑ タスクトレイにアイコンを表示
☑ プログラム実行遮断時にお知らせダイアログを表示
✓ 検出時、疑いのあるファイルを転送する (匿名で処理され、分析以外の目的にでは使用されません。)
□ロック設定の有効化
☑ 自動アップデート使用
デフォルト値 OK キャンセル 適用(A) ヘルプ

タスクトレイにアイコンを表示	タスクバーお知らせ領域にAppCheckアイコンを表示します。
プログラム実行遮断時にお知	ランサムウェアの実行アクションを遮断した時にタスクバーお知らせ領域にラ
うビライアロジを扱い	クリムフェアが換知されたことを表示しより。
検出時、疑いのあるファイルを	ランサムガードで検出された疑わしいファイルを転送します。
転送する	
ロック設定の有効化	AppCheckのアンインストールおよびオプション設定の変更の可否を設定
	します。※CMS版では、表示されません。
自動アップデート使用	3時間ごとにAppCheck CARBエンジンのアップデートを確認します。

■ 「ロック設定の有効化」の手順について 「ロック設定の有効化」に関する設定手順や解除方法ついてご説明します。

<設定方法>

(1) 「ロック設定の有効化」にチェックします。

5	AppCheckオプション		x
一般 ランサムガード 退避フォルダ 自動	カバックアップ│ユーザ指定除外ファ	イル SMB許容/遮断リスト	
☑ タスクトレイにアイコンを表示			
☑ プログラム実行遮断時にお知らせダイアロ	びを表示		
√検出時、疑いのあるファイルを転送する (唐名で処理され、分析以外の目的に)	では使用されません。)		
□ロック設定の有効化			
☑ 自動アップデート使用			
デフォルト値	OK キャンセル	適用(A) ヘルプ	

(2) パスワードを入力して、「確認」をクリックします。

ロック設定の有効化
ロック設定が有効化の場合、ロックを解除するまで製品のアンインストールおよびオブション設定の変更はできません。 パスワードを紛失すると、パスワードを復日することはできませんのでご注意ください。
- ロック設定で使用するパスワードを入力してください。(6~30文字)
パスワード入力: ••••••
パスワード確認: •••••••
パスワード表示 確認 取消

注意事項
 パスワードを忘れた場合、パス
 ワードの通知や再設定はでき
 ませんので、厳重な管理をお
 願いいたします。

(3) 「ロック設定の有効化」にチェックが入っていることを確認し、「OK」をクリックします。

V	i -			AppCheo	:kオプション		x
Γ	一般	ランサムガード	退避フォルダ	自動バックアップ	ユーザ指定除外ファイル	SMB許容/遮断リスト	
	✓ 97	マクトレイにアイコン	ンを表示				
	ע גר	コグラム実行遮断	f時にお知らせダ	イアログを表示			
	⊻ 検 (出時、疑いのある 唐名で処理され	5ファイルを転送 、分析以外の目	する 目的にでは使用され	1ません。)		
ľ		の設定の有効化	-				
	☑自	動アップデート使	用				
	デフォル	小値	[ОК	キャンセル	適用(A) へル	プ

(4) 「ロック設定の有効化」以外の設定について変更できなくなっていることを確認します。

	i			AppChec	:kオプション			x
Γ	一般	ランサムガード	退避フォルダ	自動バックアップ	ユーザ指定除外ファ	イル SMB許容	/遮断リスト	
ſ	√ 9	スクトレイにアイコン	ンを表示					
	√ ブ	ログラム実行遮断	「時にお知らせダ	イアログを表示				
	☑ 検	出時、疑いのある (匿名で処理され	るファイルを転送 、分析以外の目	する 目的にでは使用され	1ません。)			
	√ □	ック設定の有効化	Ł					
l	√ É	動アップデート使	用					
L								
	デフォル	いし値		ОК	キャンセル	適用(A)	NU	プ

<解除方法>

(1) 「ロック設定の有効化」のチェックをはずします。

				AppChec	kオプション		x
Γ	一般	ランサムガード	退避フォルダ	自動バックアップ	ユーザ指定除外ファイル	SMB許容/遮断リスト	
	✓ 9	スクトレイにアイコン	いを表示				
	マブ	ログラム実行遮断	行時にお知らせダ	イアログを表示			
	√ 椅	は出時、疑いのある (匿名で処理され	るファイルを転送 、分析以外の目	する 目的にでは使用され	1ません。)		
		ック設定の有効化	3				
	V É	目動アップデート使	用				
	デフォ	小値		ОК	キャンセル	適用(<u>A</u>) へル	プ

(2) 「ロック設定解除」画面が表示されるので、パスワードを入力し、「確認」をクリックします。

S	ロック設定	定解除	×
- ロック設定画面	で設定したパスワードを入力して	てください。	
パスワード:	パスワード:		
□ パスワード表示	ŧ	確認	取消

(3) 「ロック設定の有効化」のチェックがはずれていることを確認し、「OK」をクリックします。

				AppChec	kオプション		X
ſ	一般	ランサムガード	退避フォルダ	自動バックアップ	ユーザ指定除外ファイル	SMB許容/遮断リスト	•
	√ 97	くクトレイにアイコン	を表示				
	√ Ĵ	コグラム実行遮断	i時にお知らせら	ライアログを表示			
		出時、疑いのある 著名で処理され。	5ファイルを転送 、分析以外のE	する 目的にでは使用され	ません。)		
ľ		ゆ設定の有効化					
		動アップテート使	≕ 用				
	デフォル	卜値	ſ	ОК	キャンセル	適用(<u>A)</u> /	ヽルプ

3.2.2 オプション:ランサムガード

C AppCheckオプション X
一般 ランサムガード 退避フォルダ 自動バックアップ ユーザ指定除外ファイル SMB許容/遮断リスト
▼ ランサムウェアアクション遮断実行
☑ 毁損動作検知実行
☑ MBR保護
AppCheck Pro 拡張機能
▶ ランサムウェア遮断後、自動修復実行
保護するファイル拡張子 (区分子,または;)
7z,ai,bmp,cer,crt,csv,der,doc,docx,dwg,eps,gif,hwp,jpeg,jpg,key,lic,lnk,mp3,nc,ods, odt,ogg,one,p12,p7b,p7c,pdf,pef,pem,pfx,png,ppt,pptx,psd,ptx,rdp,rtf,srw,tap,tif,ti ff,txt,uti,x3f,xls,xlsx,xps,zip
✓ ネットワークドライブ保護
▼リムーバブルディスクドライブ保護
I SMBサーバ保護
デフォルト値 OK キャンセル 適用(A) ヘルプ

ランサムウェアクション遮断実行	ランサムウェア感染でファイル毀損の動作が発見された時に、"ランサムウェア動作検知 "お知らせを表示しプロセスを遮断します。
毀損動作検知実行	ランサムウェアにより元のファイルを復旧不可能状態に削除する動作を検知して遮断します。
MBR保護	Master Boot Record (MBR) 領域を改竄しようとするファイルの実行アクションを 遮断することによる保護機能を実行します。
AppCheck Pro 拡張機能	
ランサムウェア遮断後、自動修復	ランサムウェアプロセスを遮断後、検知したランサムウェアプロセスのファイルまで自動で
実行	削除します。

保護するファイル拡張子名(区	ここで設定されている拡張子を持ったファイルが、ランサムガードの動作対象ファイル
分子、または ;)	となります。
	7z, ai, bmp, cer, crt, csv, der, doc, docx, dwg, eps, gif, hwp, jbw,
	jpeg、jpg、jps、jtd、key、lic、lnk、mp3、nc、odp、ods、odt、ogg、one、
	ost、p12、p7b、p7c、pdf、pef、pem、pfx、png、ppt、pptx、psd、pst、
	ptx, rdp, rtf, srw, tap, tif, tiff, txt, uti, x3f, xls, xlsx, xps, zip
ネットワークドライブ保護	AppCheckがインストールされたPCで使用されているネットワークドライブをランサムウェ
	アの攻撃から保護する機能です。
リムーバブルディスクドライブ保護	USBメモリまたはCFメモリに保存されたファイルがランサムウェアによって暗号化された場
	合、遮断および自動復元される機能です。
	*USB接続HDDは「ランサムウェアクション遮断機能」により保護されます。
SMBサーバ保護	AppCheckがインストールされたPCやサーバ内のドライブにある共有フォルダがランサム
	ウェアに感染しないように、ランサムウェアに感染したPCからのネットワークアクセスを一
	時的に遮断します。

・ネットワークドライブ保護







3.2.3 オプション:退避フォルダ

AppCheckオプション ×				
一般 ランサムガード 退避フォルダ 自動バックアップ ユーザ指定除外ファイル SMB許容/遮断リスト				
▼ランサムウェア退避フォルダ				
退避フォルダバス: C:¥ProgramData¥CheckMAL¥AppCheck¥RansomShelter 設定(<u>S</u>)				
退避フォルダ使用量: 99.66GB中、0Byteを使用中 退避フォルダを空にする(E)				
□ 一つのファイルの大きさを最大 💙 1 GB 以下に制限				
□退避フォルレダを隠す				
退避フォルダ自動削除				
▼ 7日 経過したファイルを自動削除				
□ 退避フォルダ容量が マ 50 GB になると、古い順でファイルを自動削除				
※手動で削除する際は、リアルタイムセキュリティを解除してから削除してください。				
デフォルト値 OK キャンセル 適用(A) ヘルプ				

ランサムウェア退避フォルダ	退避フォルダのパスを指定します。
	退避フォルダ使用量を確認し、手動で削除することが可能です。
1つのファイルの大きさを最大	退避するファイルの大きさを設定可能です。
○○以下に制限	100MB~5GBまで、設定可能です。
退避フォルダを隠す	退避フォルダを見えないように設定することが可能です。
退避フォルダ自動削除	退避フォルダのファイルを定期的に削除することが可能です。
○○経過したファイルを自動削除	10分~7日まで、設定可能です。
退避フォルダ容量が○○になると、	退避フォルダの容量を設定することが可能です。
古い順でファイルを自動削除	5GBディスクの50%まで、設定可能です。
デフォルト値	エクスプロイトガードオプションの設定を初期化

3.2.4 オプション:自動バックアップ

1	AppCheo	:kオプション	
一般 ランサムガード 退避フォル	ダ 自動バックアップ	ユーザ指定除外ファイル SMB影	肝容/遮断リスト
□自動バックアップ実行	スケジュール設定(5)	
バックアップ対象		除外対象	
フォルダリスト	追加 削除	フォルダリスト	<u>追加 削除</u>
フォルダパス	^	フォルダパス	
C:¥Users¥Administrator.W	/IN-GR ≡		
C:¥Users¥Administrator.W	/IN-GR		
C:¥Users¥Administrator.W	/IN-GR 🗡		
□ 指定した拡張子だけバックアッ	ז	バックアップ時に除外するファイル	拡張子
- バックアップ先 ③ □ ーカルディスク ○ ネットワーク共有フォルダ(SM)	C:¥AutoBackup(B/CIFS)	AppCheck 履歴ファイル保存数	: 3 v
サーバアドレス		共有フォルダ	
ユーザ ID		パスワード	
※自動バックアップフォルダを手動 リアルタイムセキュリティをOfficして	で削除する場合は、 から削除してください		

自動バックアップ実行	一定時間に重要ファイルをバックアップする機能の使用有無を選択します。
	デフォルトは1時間毎の自動バックアップとなります。
バックアップ対象 フォルダリスト	バックアップする対象フォルダの追加および削除が可能です
指定した拡張子だけバックアップ	バックアップする対象フォルダに含まれたファイルのうち、指定したファイル拡張名を
	持つファイルだけバックアップするように設定可能です。
除外対象 フォルダリスト	「バックアップ対象」に含まれるサブフォルダを指定し、自動バックアップを除外する
	フォルダを指定できます。
バックアップ時に除外するファイル	バックアップする対象フォルダに含まれたファイルのうち、指定したファイル拡張名は
拡張子	バックアップから除外するように設定可能です。
バックアップ先	バックアップする対象フォルダを保存する自動バックアップフォルダ
	<autobackup(appcheck)>の指定を選択します。</autobackup(appcheck)>
履歴ファイルの保存数	自動バックアップフォルダ内のファイルを最大10までHistory fileとして保存しま
	す。
ネットワーク共有フォルダ	サーバアドレス(リモートIPアドレスまたはリモートPC名)、共有フォルダ(共有
(SMB/CIFS)	設定が行われたリモートドライブ、フォルダ名)、ネットワーク共有フォルダのユーザ
	ID、パスワードを正確に入力して下さい。

<注意> 自動バックアップを行う際には、バックアップ先の空き容量を十分確保して下さい。

十分な空き容量がない場合、バックアップができない可能性があります。

3.2.5 オプション:ユーザ指定除外ファイル

ユーザ指定除外ファイルではランサムガード、システム検知によりランサムウェアと検知(遮断)されたファイル の内、お客様の判断により常に検査実行を行わないように設定許可したいファイルを記述します。(ホワイト リスト)※デフォルトではファイルが登録されてない状態です。

一般 ランサムガード 退避フォルダ 自動バックアップ ユーザ指定除外ファイル SMB許容/遮断/ 登録されたファイルはチェックしない 道 ファイルパス ご C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-ntservi C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥mackerel-age C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-ntservi C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-procs.e C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-windo C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-windo C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio	
	スト
ファイルパス C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-ntservi C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-procs.e C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-tro.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-tcp.exe C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-windo C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-windo C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥mackerel-plu C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio	<u> </u>
C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-ntservi C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-procs.e C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-tcp.exe C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-tcp.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥wrapper.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-windo C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-windo C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Mackerel¥mackerel-agent¥check-log.exe C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protectio	

ユーザ指定除外ファイルではランサムガードによりランサムウェアと検知(遮断)されたファイルの内、お客様の 判断により常に検査実行を行わないように設定許可したいファイルを記述します。(ホワイトリスト)

<注意>

基本的にAppCheck Pro for Windows Serverでは特定プログラムに対するホワイトリストが含まれていますが、 正常的なexplorer.exeまたはsvchost.exeシステムファイルを利用しファイル暗号化行為を実行するランサムウェアが 存在するため、システムファイルをユーザ指定除外ファイルに勝手に追加しないでください。

3.2.6 オプション: SMB許容/遮断リスト

SMB保護機能が有効な場合、遠隔PCがランサムウェアに感染し、ネットワークを介して共有フォルダにアクセスし、ファイルの毀損を行った場合、SMBサーバ保護機能が働き、遠隔PCからのアクセスを遮断します。

			AppCheo	:kオプション	2			×
一般	ランサムガード	退避フォルダ	自動バックアップ	ユーザ指定	除外ファイル	, SMB許容/j	塵断リスト]
許容さ	れたアドレスリスト						<u>追加</u>	<u>削除</u>
ፖドレ	<i>ب</i> ر							
192.	.168.254.0/24							
) Fritz +	ชะจะ วมวง					陈庄子	~ ~~	
遮断さ	れたアドレスリスト		-+ 22			<u>臨時許</u>	容 <u>常時</u>	許容
遮断さ アドレ 192	れたアドレスリスト バス 168 254 53	遮断	時間 //11/12 20·51·4	.7	遮断満了B 2019/11/1	<u>臨時許</u> 寺間 2 21・51・47	容 常時	許容
遮断さ アドレ 192.	れたアドレスリスト ・ス 168.254.53	· 遮断 2019	時間 //11/12 20:51:4	.7	遮断満了B 2019/11/1	<u>臨時許</u> 寺間 2 21:51:47	容 <u>常時</u>	許容
遮断さ アドレ 192.	れたアドレスリスト ・ス 168.254.53	· 	時間 I//11/12 20:51:4	.7	遮断満了® 2019/11/1	<u>臨時許</u> 寺間 2 21:51:47	<u>容 常時</u>	許容
遮断さ アドレ 192.	れたアドレスリスト ス 168.254.53	· 	時間)/11/12 20:51:4	.7	遮断満了8 2019/11/1	<u>臨時許</u> 寺間 2 21:51:47	密 常時	許容
遮断さ アドレ 192.	れたアドレスリスト バス 168.254.53	· 2019	時間 1/11/12 20:51:4	7	遮断満了® 2019/11/1	<u>臨時許</u> 奇間 2 21:51:47	容 <u>常時</u>	許容
遮断さ アドレ 192.	れたアドレスリスト ・ス 168.254.53		時間 I/11/12 20:51:4	.7	遮断満了8 2019/11/1	<u>臨時許</u> 寺間 2 21:51:47	容:常時	許容
遮断さ アドレ 192.	れたアドレスリスト ス 168.254.53		時間 I/11/12 20:51:4	17	遮断満了8 2019/11/1	<u>臨時許</u> 寺間 2 21:51:47	容 <u>常時</u>	許容
遮断さ アドレ 192	れたアドレスリスト ベス 168.254.53		時間 1/11/12 20:51:4	.7	遮断満了8 2019/11/1	<u>臨時許</u> 奇間 2 21:51:47	容 常時	許容
遮断さ アドレ 192.	れたアドレスリスト ・ス 168.254.53		時間 I/11/12 20:51:4	.7	遮断満了B 2019/11/1	<u>臨時許</u> 寺間 2 21:51:47	容 常時	<u>許容</u>

遠隔PCで実行されたランサムウェアによって、共有フォルダ内のファイルが毀損される場合は、IP(IPv4、 IPv6)アドレスのブロックメッセージが表示されます。

AppCheckオプションの「SMB許容/遮断リスト」を確認してみると、「遮断されたアドレスリスト」にブロックされたIPアドレスの情報が表示されます。基本的にブロックされたIPアドレスは、1時間の間、共有フォルダへのアクセスが遮断されます。※デフォルトではアドレスが登録されていません。

なお、ユーザーが臨時許容または常時許容を使用することによって、遮断されたIPアドレスを許容するかどうか を決定することができます。ブロックされたIPアドレスは、遮断満了時間(1時間)が経過すると、自動的に 「遮断されたアドレスリスト」から削除処理され、当該遠隔PCでの再接続が可能になります。

臨時許容:ブロックされたIPアドレスから共有フォルダへのアクセスを可能にする。 再検出した場合は、ブロックされる。

常時許容:ブロックされたIPアドレスから共有フォルダへのアクセスを常に許可する。 ※「許容されたアドレスリスト」に登録(ホワイトリスト)

SMB 許容リスト追加 ×
IPアドレス
IP v4
※個別:19216811
※ 順次:192.168.1.1-10
(192.168.1.1 ~ 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:2001:0DB8:1000:0000:0000:1111:2222
※ 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:FFFF:FFFF:FFFF:FFFF:FFFF まで許容)
道加(A) 取消(C)

「許容されたアドレスリスト」に、IP(IPv4、IPv6)アドレスを追加したい場合は、「許容されたアドレスリスト」の[追加]ボタンを使用して登録することができます。

「SMB許容リスト追加」では、IPv4、IPv6プロトコルアドレスについて、マスク設定の考え方により個別、順次、全体という範囲を指定した登録が可能であり、各例を参考にして追加することができます。

特定のIPアドレスのSMB許容時には、遠隔PCにAppCheckがインストールされている場合や、信頼できる 機器にのみ追加することをおすすめします。

※遮断されたアドレスリストにIPアドレスが登録されている状態で、メインメニューのリアルタイム セキュリティスイッチをOFFにすると、登録されている遮断されたIPアドレスが削除され、そのIP アドレスからの通信が可能になります。 遮断されたアドレスリストから許容されたアドレスリストに設定を登録したい場合は、リアルタイム セキュリティスイッチをOFFする前に実施するようにしてください。

4. 遮断/検知されたプログラム処理方法

AppCheckは基本的に自動削除(治療)機能を提供していますが、ランサムウェアの中にデジタル署名が含まれていた場合には自動遮断機能だけを提供します。

AppCheckを使用している時にランサムウェア検知、または実行アクションで遮断された場合、次の方法にて 処理するようにお願いします。

(1) AppCheckツールの"脅威ログ"に表示されたランサムガードによる検知一覧を確認していただくことにより、より早くランサムウェア情報を確認することができます。

(2) 広告のような不要なプログラムは、コントロールパネルのプログラムリストで削除することが可能です。 AppCheckツール"脅威ログ"情報を参考にしてコントロールパネルから削除していただくようにお願いします。

※注意:一部悪性広告プログラムの場合、コントロールパネルからのプログラム削除を実行しても削除されない場合があります。この時には継続して実行アクションが行われる場合があります。