



AppCheck Pro

マニュアル

株式会社 JSecurity

第十三版

2021/12/17

はじめに

このたびは、ランサムウェア対策ソフト AppCheck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 V2.5.51.5を参考に作成しています。

動作環境について

[表1] AppCheck Pro 動作環境

システム動作環境	
ハードウェア	・CPU : Intel 1.6GHz 以上 ・メモリ : 1GB以上 ・ハードディスク : 2GB以上の空き容量が必要であり
OS	・Windows7 以降 (32bit/64bit)
サーバーOS	・Windows Server 2008 R2 以降

※上記は推奨仕様です。

目 次

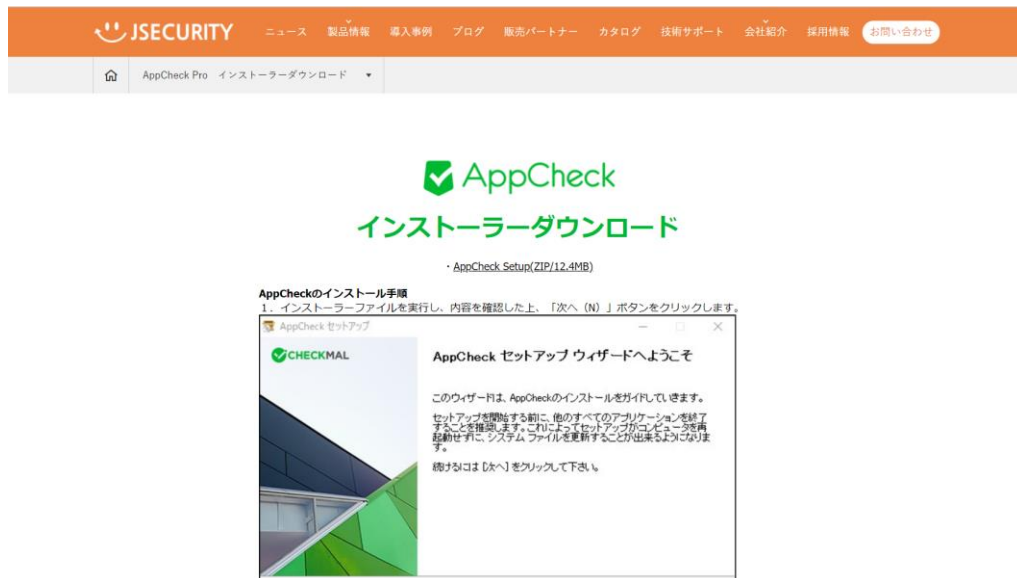
1. 製品のセットアップおよびアンインストール	1
1.1.【CMSなし】製品のセットアップ	1
1.2.【CMSあり】製品のセットアップ	4
1.3.AppCheck Pro 製品登録	7
1.4.AppCheckアンインストール	9
2. AppCheck :メニュー構成	12
2.1.メイン画面メニュー構成	12
2.2.クリーナー	13
2.3.リアルタイムセキュリティ	14
2.4.エクスプロイトガード	15
2.5.MBR保護	15
2.6.ネットワークドライブ保護	15
3. AppCheck メニュー詳細	16
3.1 ツール	16
3.1.1 ツール：脅威ログ	16
3.1.2 ツール：一般ログ	17
3.1.3 ツール：検疫	18
3.2 オプション	20
3.2.1 オプション：一般	20
3.2.2 オプション：ランサムガード	26
3.2.3 オプション：自動バックアップ	29
3.2.4 オプション：ユーザ指定除外ファイル	30
3.2.5 オプション：SMB許容/遮断リスト	31
3.2.6 オプション：エクスプロイトガード	33
3.2.7 オプション：クリーナー	35
3.2.8 オプション：退避フォルダ	36
4. 遮断/検知されたプログラム処理方法	37

1. 製品のセットアップおよびアンインストール

AppCheckはインターネットにアクセスできるWindows 7 (32/64bit)以降のOSでインストールが可能です。

1.1. 【CMSなし】製品のセットアップ

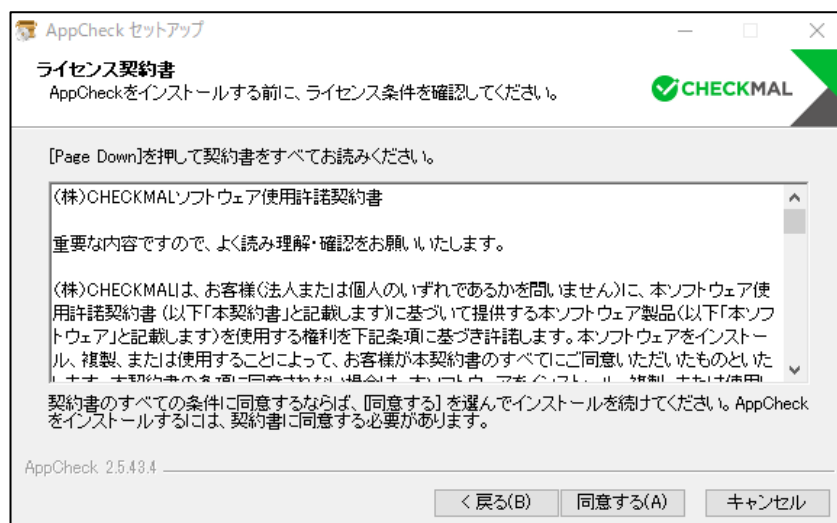
- (1) インストーラダウンロード専用ページ（ <https://jsecurity.co.jp/appcheck-instldl> ）でファイルをダウンロードします。



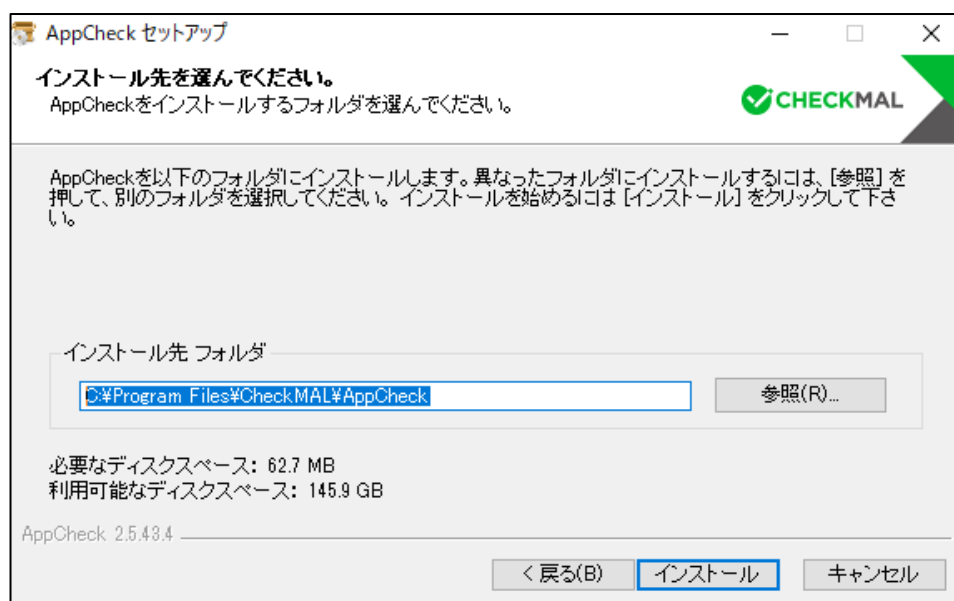
- (2) AppCheckをインストールする前に実行中のすべてのプログラムを終了し、その後インストールを行ってください。



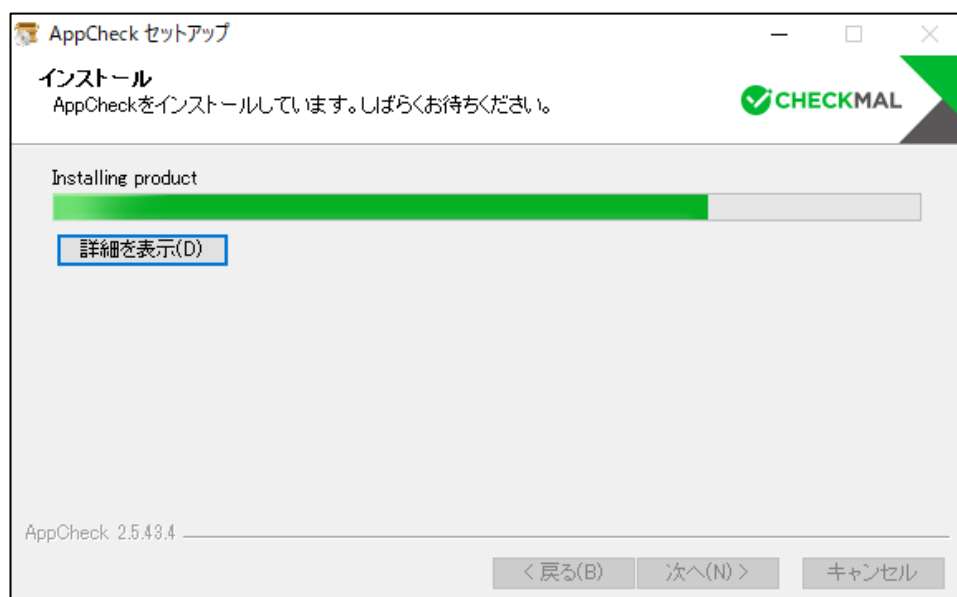
- (3) ライセンス契約書（ソフトウェア使用許諾契約書）をお読みにになり、同意する場合は「同意する」ボタンをクリックしてください。セットアップを開始します。



- (4) AppCheckは"C:\Program Files\CheckMAL\AppCheck"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。



(5) 「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。



(6) 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。

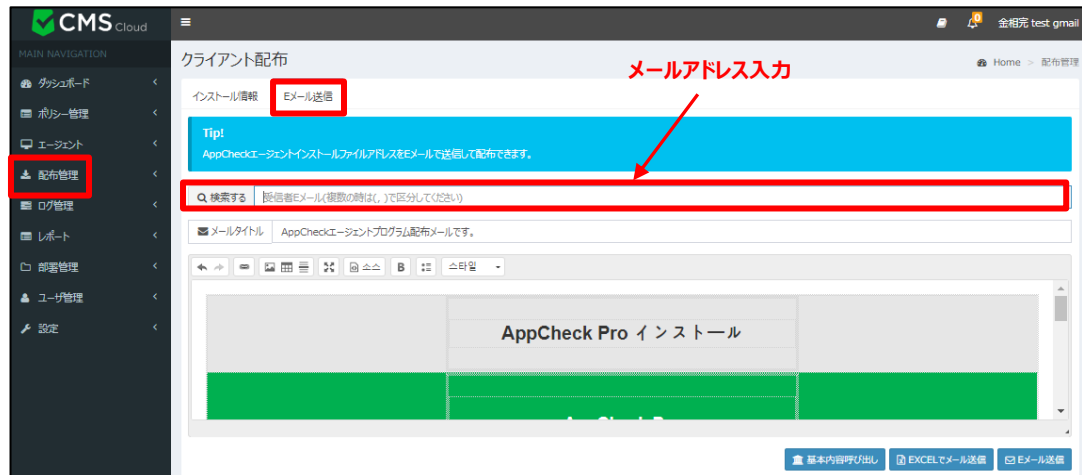


(注) AppCheckの起動時に、「AUTO UPDATE（自動更新）」を行う場合があります。

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. 【CMSあり】製品のセットアップ

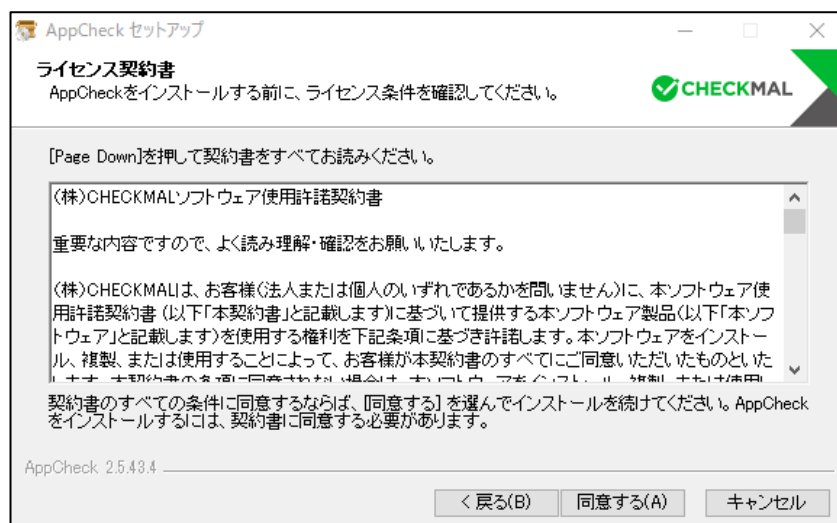
- (1) CMSにログインし、下記画面赤枠のメールアドレス入力スペースに受信者のメールアドレスを入力します。
その後「Eメール送信」ボタンをクリックすると、AppCheckエージェントプログラム配布メールが送信されます。
受信したメールより、ライセンス登録済みのインストールプログラムをダウンロードすることが可能です。



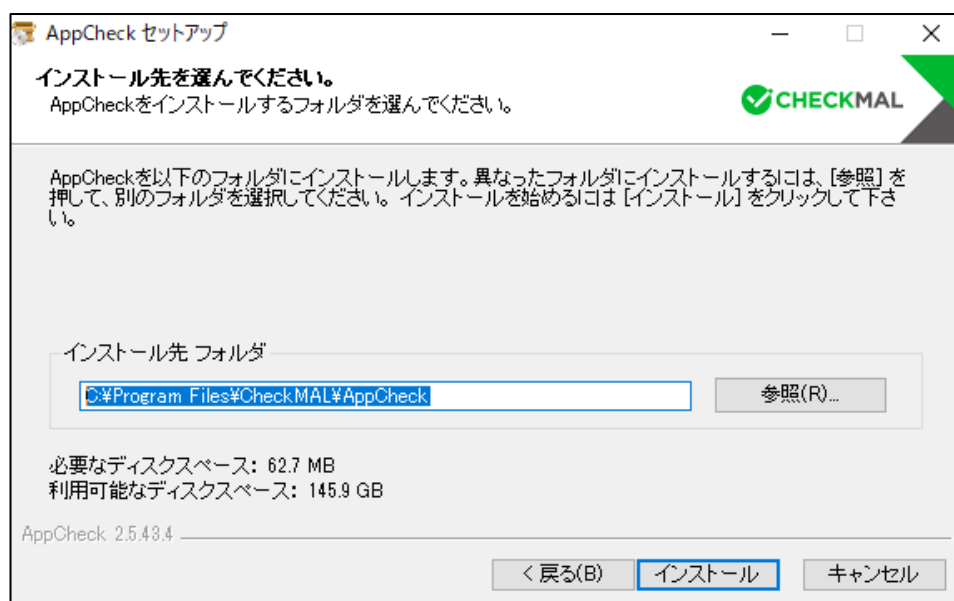
- (2) AppCheckをインストールする前に実行中のすべてのプログラムを終了し、その後インストールを行ってください。



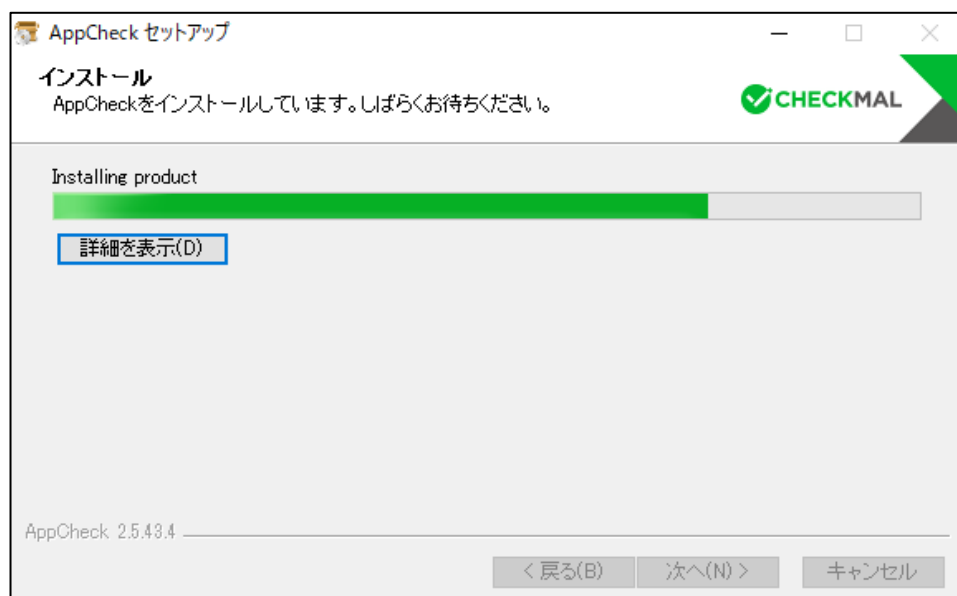
- (3) ライセンス契約書（ソフトウェア使用許諾契約書）をお読みにになり、同意する場合は「同意する」ボタンをクリックしてください。セットアップを開始します。



- (4) AppCheckは"C:\Program Files\CheckMAL\AppCheck"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。



(5) 「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。



(6) 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。



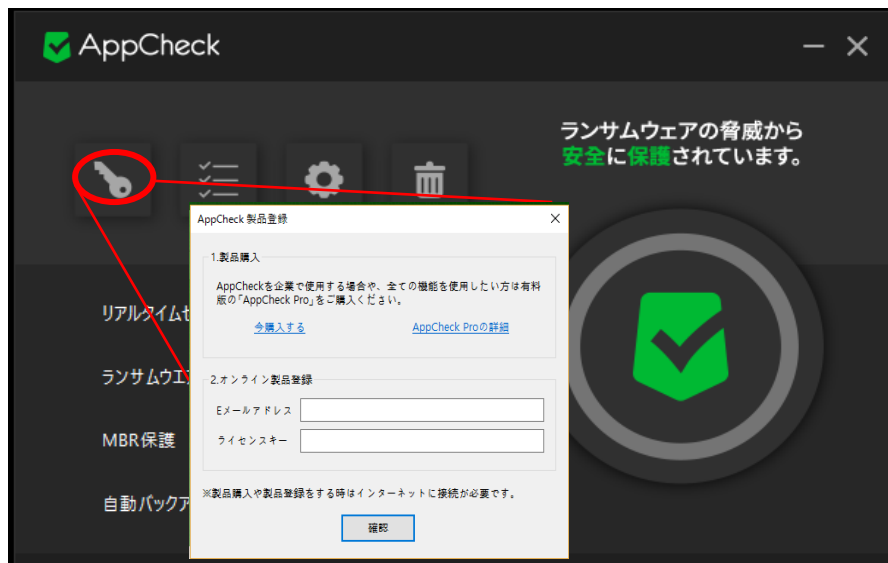
(注) AppCheckの起動時に、「AUTO UPDATE（自動更新）」を行う場合があります。

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。

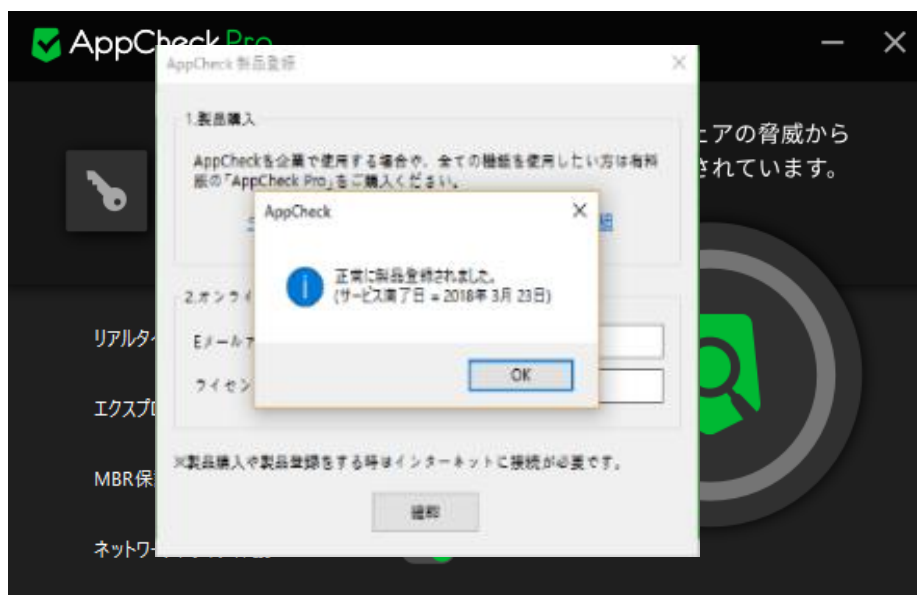
1.3. AppCheck Pro 製品登録

(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**製品バージョン**に更新されます。

※ **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。**



(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。



AppCheck ロゴ（無償版）



AppCheckPro ロゴ（有料版）

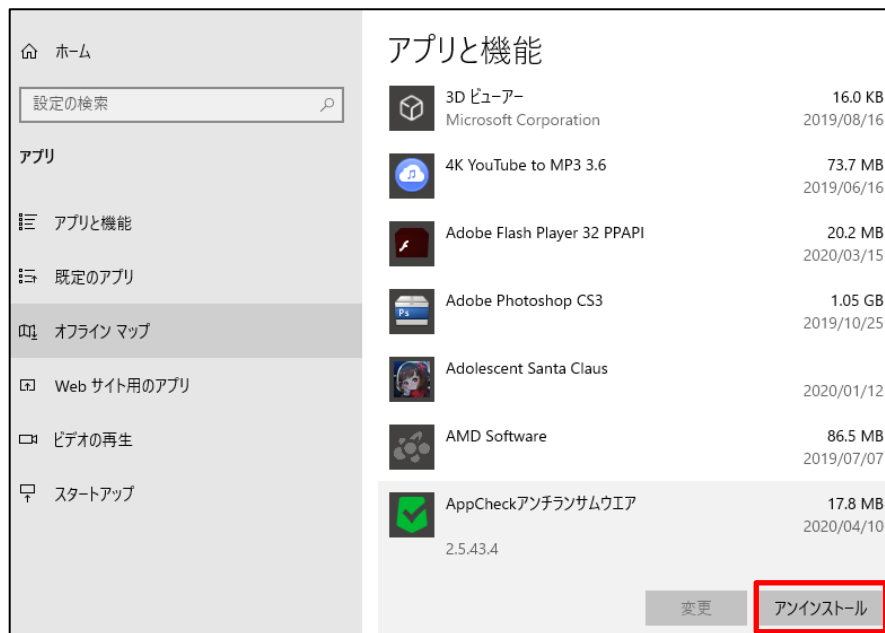


登録頂いた「E メールアドレス」「ライセンスキー」「満了日」「数量」をご確認頂き、AppCheck Pro をご利用下さい。

1.4. AppCheck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。

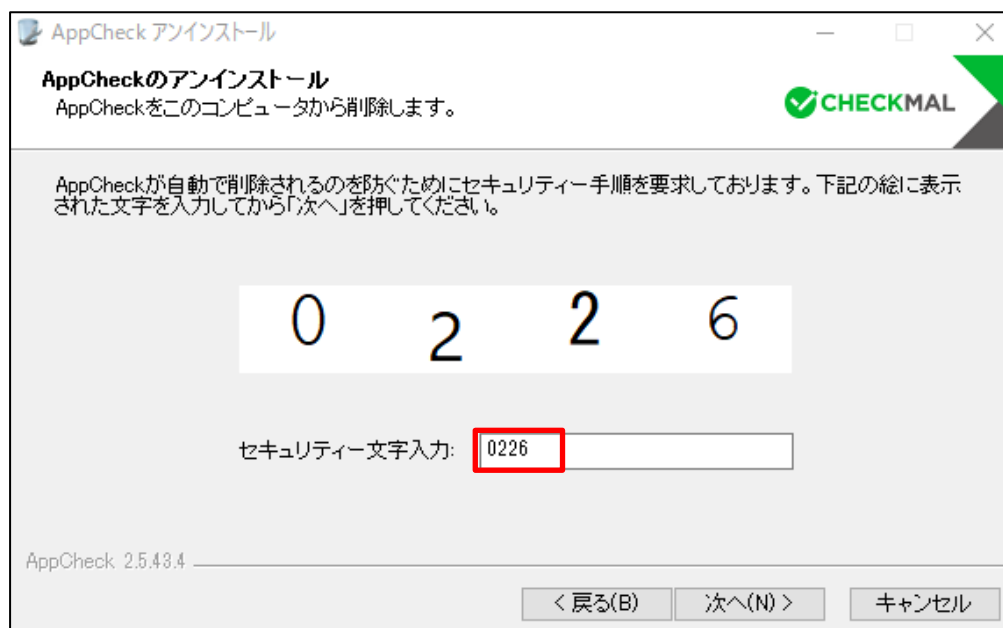
- (1) コンピュータ上で起動しているすべてのアプリケーションを終了します。
- (2) 「設定」→「アプリと機能」のプログラムリストに登録されている"AppCheckアンチランサムウェア"を選択しアンインストールを実行します。



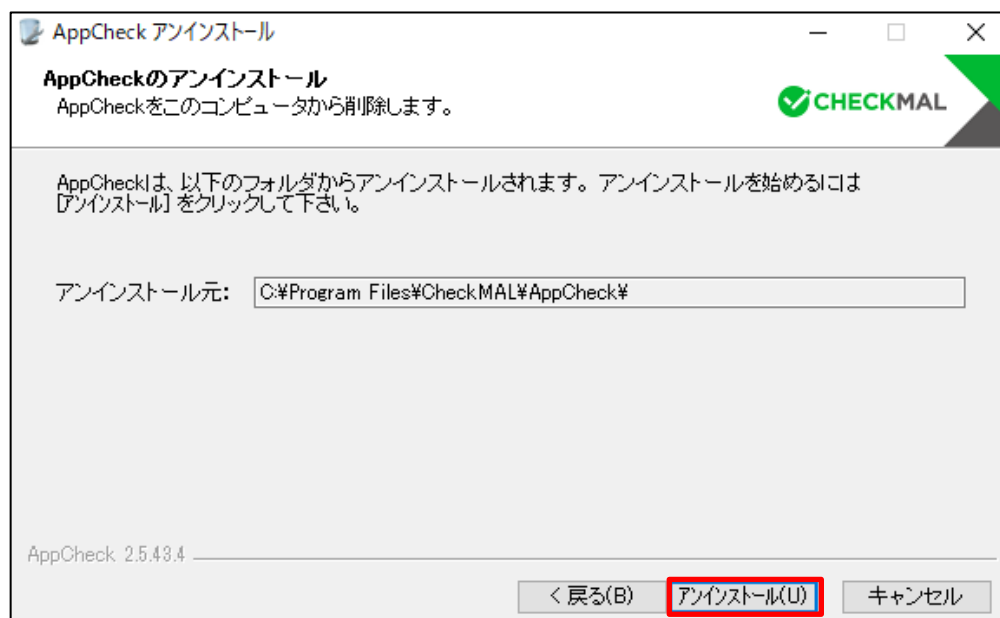
- (3) 「次へ」をクリックします。



(4) 「セキュリティ文字入力」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。



(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。



(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

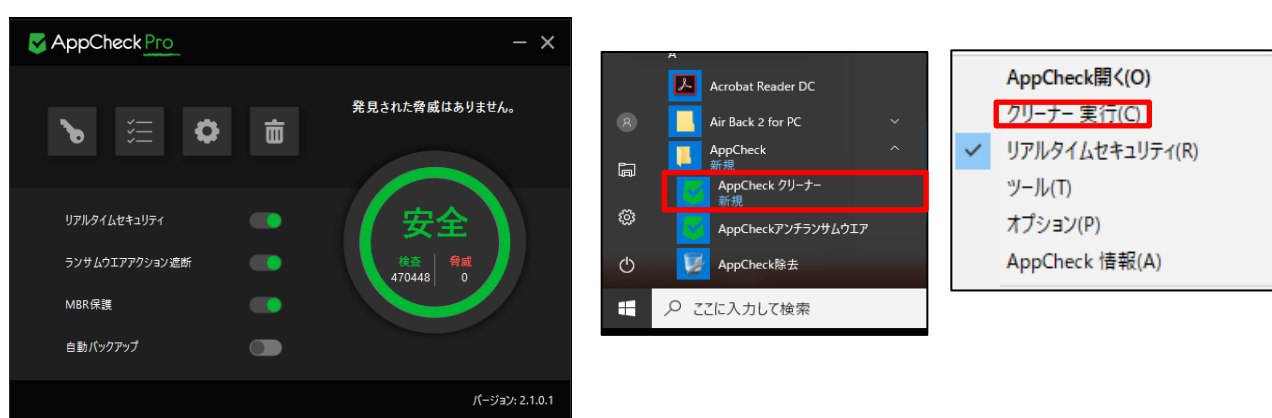


製品登録	AppCheck製品案内およびオンライン製品登録
ツール	検疫、脅威ログ、一般ログ情報の閲覧機能
オプション	一般、ランサムガード、エクスプロイトガード、退避フォルダ、クリーナー、自動バックアップ、ユーザ指定除外ファイル、SMB許容/遮断リスト機能を設定
クリーナー	変造されたシステム検査、ネットワーク環境検査、悪性プログラム除去、広告プログラム除去、ブラウザ拡張プログラム除去、ショートカットファイル内悪性URL除去、ランサムウェアノート除去、臨時ファイル/フォルダ除去機能によりシステムにインストールされた悪性コードおよび広告プログラム除去と臨時ファイル/フォルダ削除機能を提供
ファイル削除	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、エクスプロイトガード、クリーナー機能などのon/offを設定
エクスプロイトガード	Webブラウザやマイクロソフトオフィスの他、各種プラグインなどのアプリケーションの脆弱性を突く、悪意のある攻撃からPCを保護
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. クリーナー

クリーナー機能は、変造されたシステム検査、ネットワーク環境検査、悪性プログラム除去、広告プログラム除去、ブラウザ拡張プログラム除去、ショートカットファイル内悪性URL除去、ランサムウェア支払ファイル除去、臨時ファイル/フォルダ除去機能によりシステムにインストールされた悪性コードおよび広告プログラム除去と臨時ファイル/フォルダ削除機能を提供します。変造されたシステム検査システム検査（手動）はランサムウェアによる悪性の支払案内ファイル・脅迫メッセージを検査し、"安全"または"危険"で検査結果を表示します。

クリーナー機能の実行はAppCheckメイン画面のクリーナーボタン、プログラムリストの「AppCheckクリーナー」またはタスクトレイのAppCheckメニューから提供される「クリーナー実行」メニューより可能です。



AppCheckメイン画面のクリーナーボタンでは検査完了時に「発見された脅威はありません」または「脅威が全て除去されました。確認する場合は、クリックしてください。」のいずれかのメッセージが表示されます。



クリーナー検査中にAppCheckメイン画面のクリーナーボタンを再度クリックすると、クリーナー検査ダイアログが追加で生成され各検査項目および詳細検知履歴と処理結果を確認することができます。（検査中止をする場合にも詳細画面より操作をすることができます）

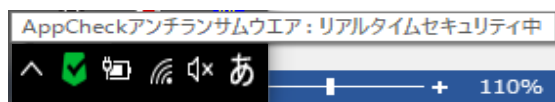
クリーナー検査により検知および除去された詳細情報はAppCheck ツールの脅威ログで確認でき、除去された項目を復元するには、検疫所にバックアップされた項目を選定し、復元することができます。

2.3. 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。



リアルタイム監視機能のオン/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更します。



緑：リアルタイム保護オン



グレイ：リアルタイム保護オフ

2.4. エクスプロイトガード

Webブラウザやマイクロソフトオフィスその他、各種プラグインなどのアプリケーションの脆弱性を突く、悪意のある攻撃からPCを保護します。

パッチ適用がリアルタイムで行えない端末や不十分な端末などを脆弱性悪用攻撃から防御することができます。

2.5. 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。

2.6. ネットワークドライブ保護

ネットワークドライブ内のファイルが、AppCheck がインストールされた PC のローカルディスクからランサムウェアによって毀損されないよう、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感染し、共有フォルダ経由で被害を拡大することを防ぎます。

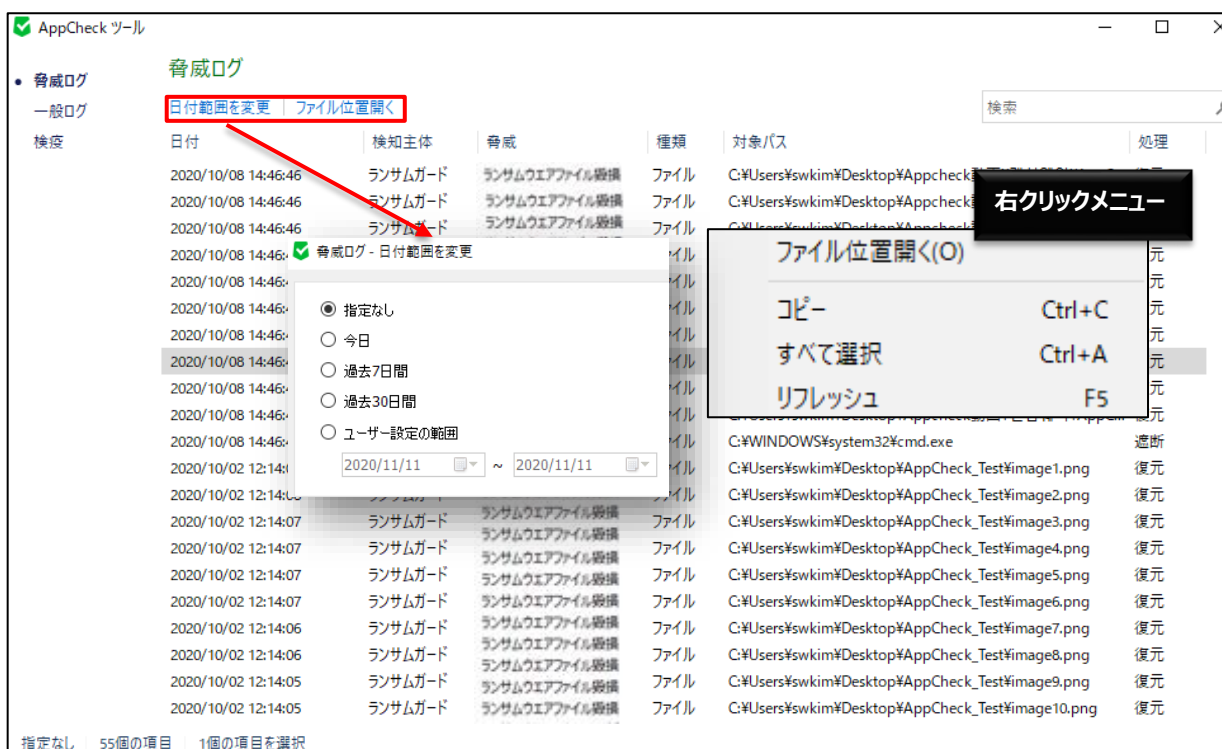
3. AppCheck メニュー詳細

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、クリーナーにより診断（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。



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。
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	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

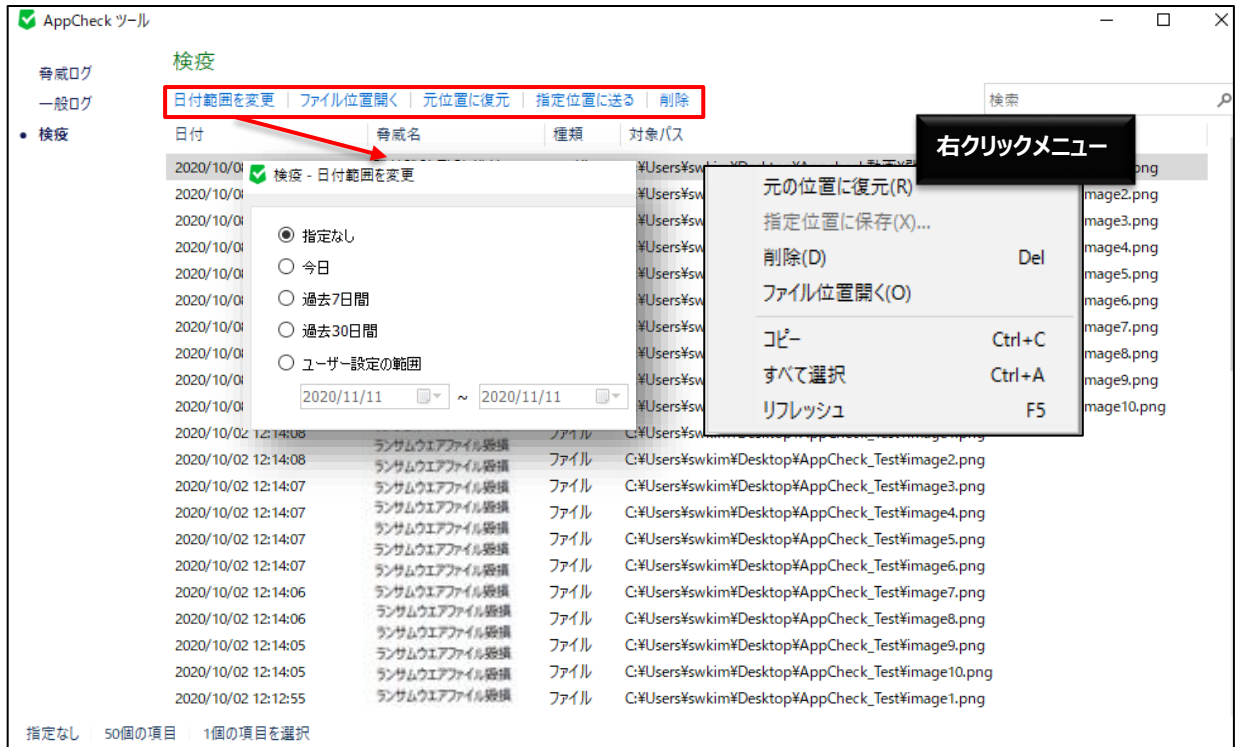
一般ログはAppCheck使用時に発生するプログラム開始/終了、サービス開始/終了、リアルタイム監視開始/終了、ランサムガード開始/終了、アップデート、オプション設定、ランサムウェアおよびランサムガードお知らせメッセージ等の情報を表示します。検疫タグの上段のメニューと、リストから右クリックして、選択するメニューがあります。



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、クリーナーにより自動治療（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。



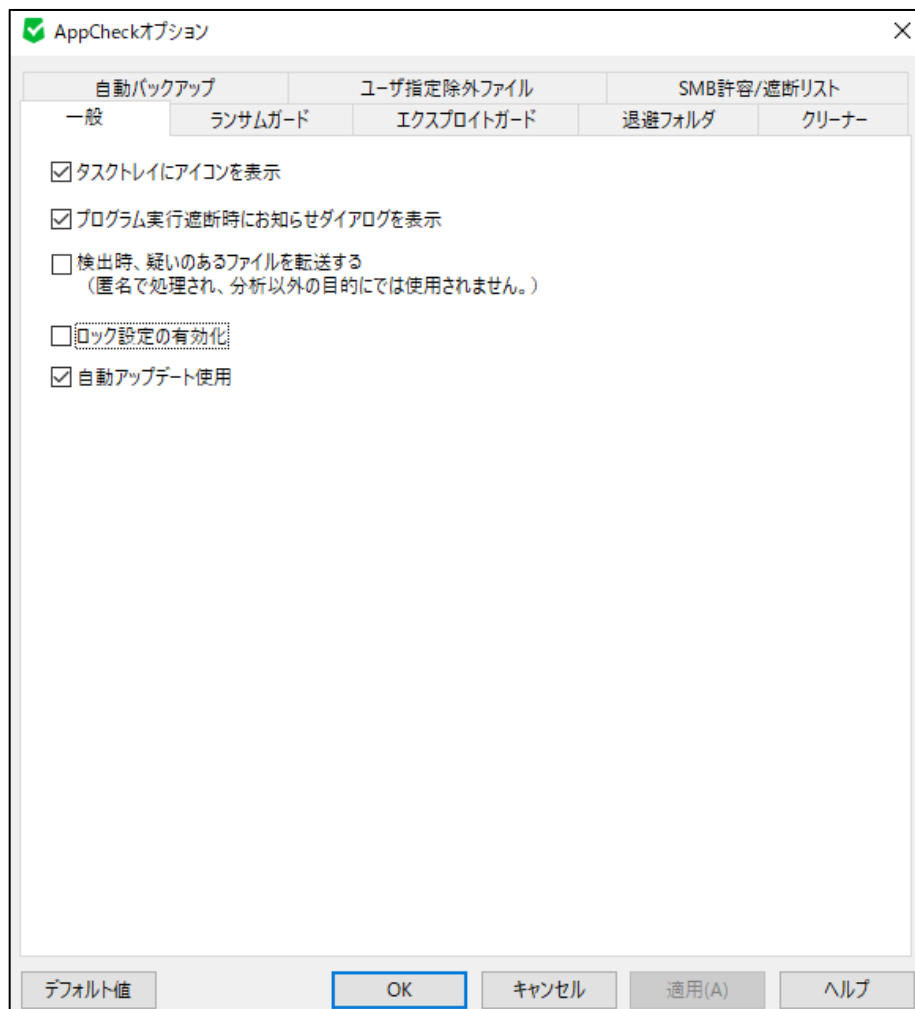
日付範囲を変更	検疫情報を日付で検索します。
元の位置に復元	選択したファイルを元の位置（フォルダ）に復元します。
指定位置に保存	選択したファイルをユーザが指定した位置（フォルダ）に保存します。
削除	検疫して保存された待避ファイルを削除します。
ファイル位置開く	選択したファイルが存在するフォルダを開きます。
コピー	選択したファイルの詳細ファイル情報をコピーします。
すべて選択	検疫で表示されているすべての項目を選択します。
リフレッシュ	検疫情報を更新します。

※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	ランサムウェア行為・ファイル毀損・ファイル名変更脅威等を検知した機能。「リアルタイムスキャン」「システム検査」「ランサムガード」など。
	脅威	ランサムウェアによる脅威と思われる行為内容を表示します。「ランサムウェアファイル名変更」「ランサムウェアアクション検知」「ランサムウェアファイル毀損」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	「自動バックアップ」「セッションプログラム」「サービスプログラム」「アップデート」「お知らせメッセージ」のうちいずれかを表示します。
	内容	区分の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	ランサムウェアによる脅威と思われる行為内容を表示します。(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



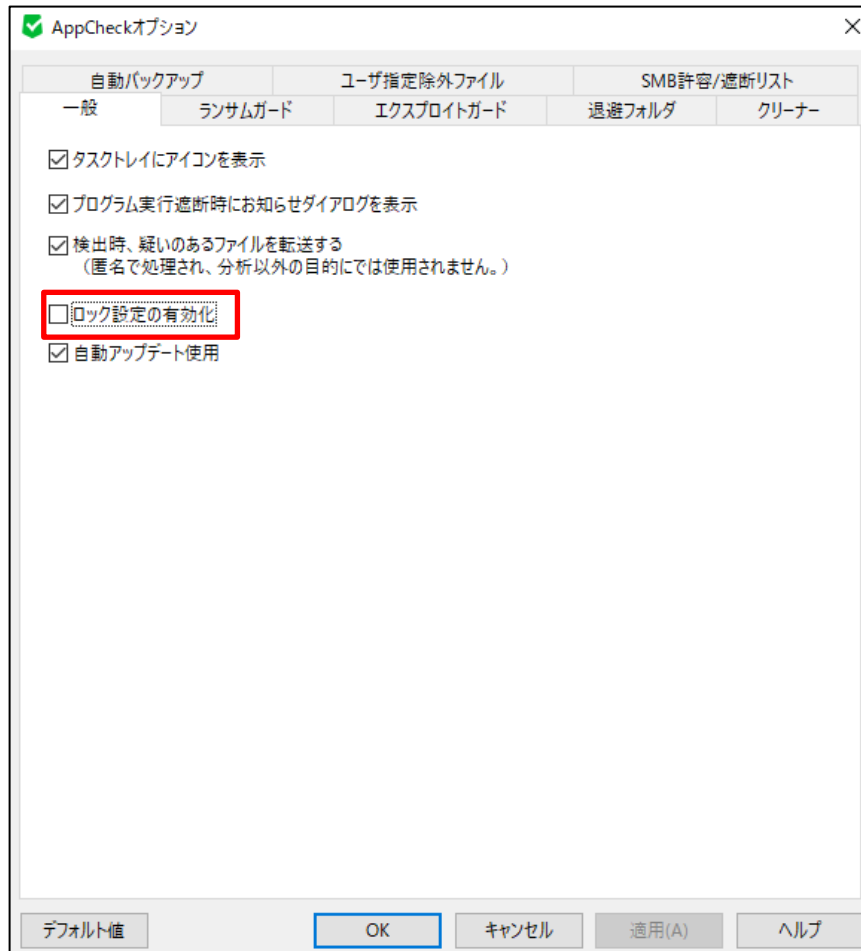
タスクトレイにアイコンを表示	タスクバーお知らせ領域にAppCheckアイコンを表示します。
プログラム実行遮断時にお知らせダイアログを表示	ランサムウェアの実行アクションを遮断した時にタスクバーお知らせ領域にランサムウェアが検知されたことを表示します。
検出時、疑いのあるファイルを転送する	ランサムガードで検出された疑わしいファイルを転送します。 ※CMS版のデフォルト値は「OFF」です
ロック設定の有効化	AppCheckのアンインストールおよびオプション設定の変更の可否を設定します。※CMS版では、表示されません。
自動アップデート使用	3時間ごとにAppCheck CARBエンジンのア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

※「デフォルト値」ボタンをクリックすることにより、設定値がデフォルト値に戻ります。

- 「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に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。



(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プ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、パスワードを復旧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: [パスワード入力欄]

パスワード確認: [パスワード確認欄]

☐ パスワード表示

確認(O) 取消(C)

！ 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。

AppCheckオプション

自動バックアップ ユーザ指定除外ファイル SMB許可/遮断リスト

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 クリーナー

☒ 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

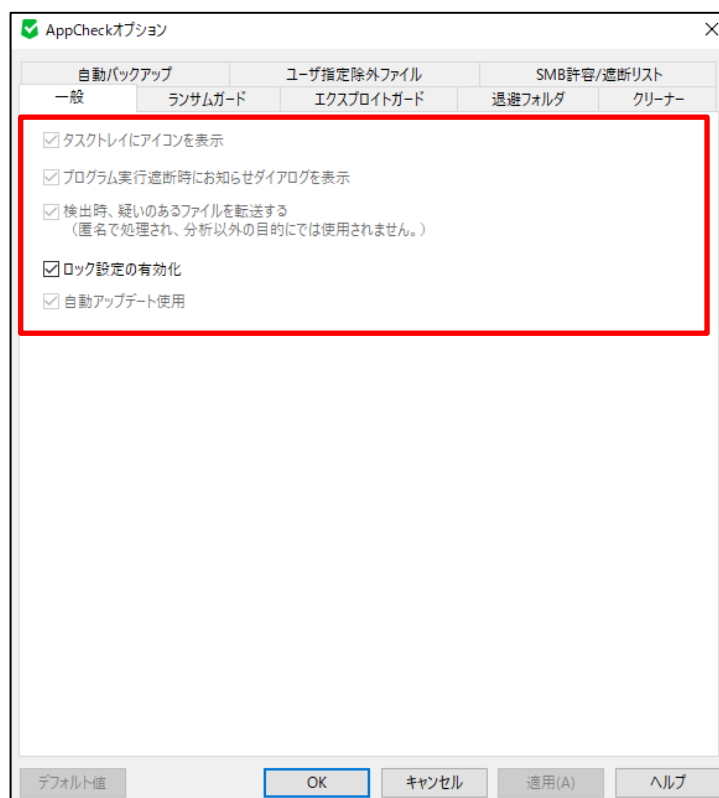
☒ 検出時、疑いのあるファイルを転送する
(匿名で処理され、分析以外の目的には使用されません。)

☒ ロック設定の有効化

☒ 自動アップデート使用

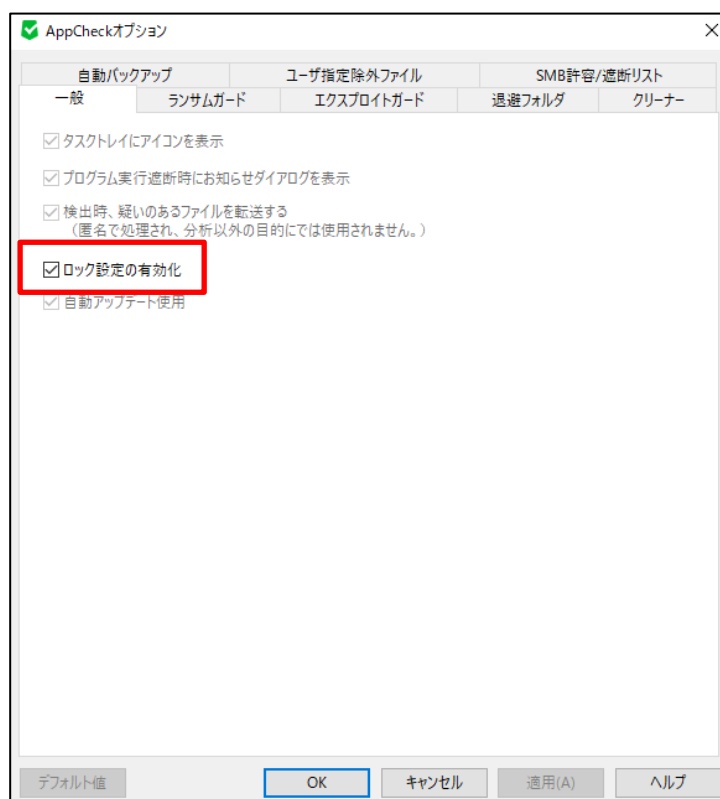
デフォルト値 **OK** キャンセル 適用(A) ヘルプ

(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。

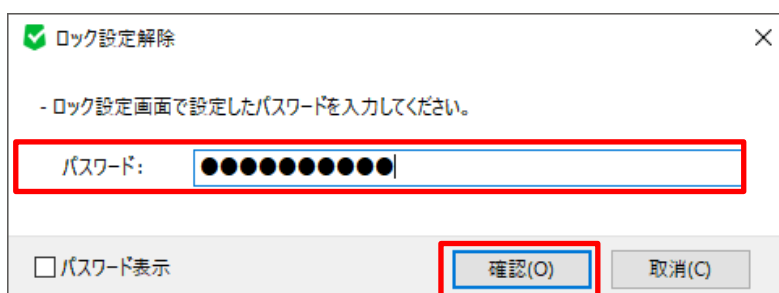


<解除方法>

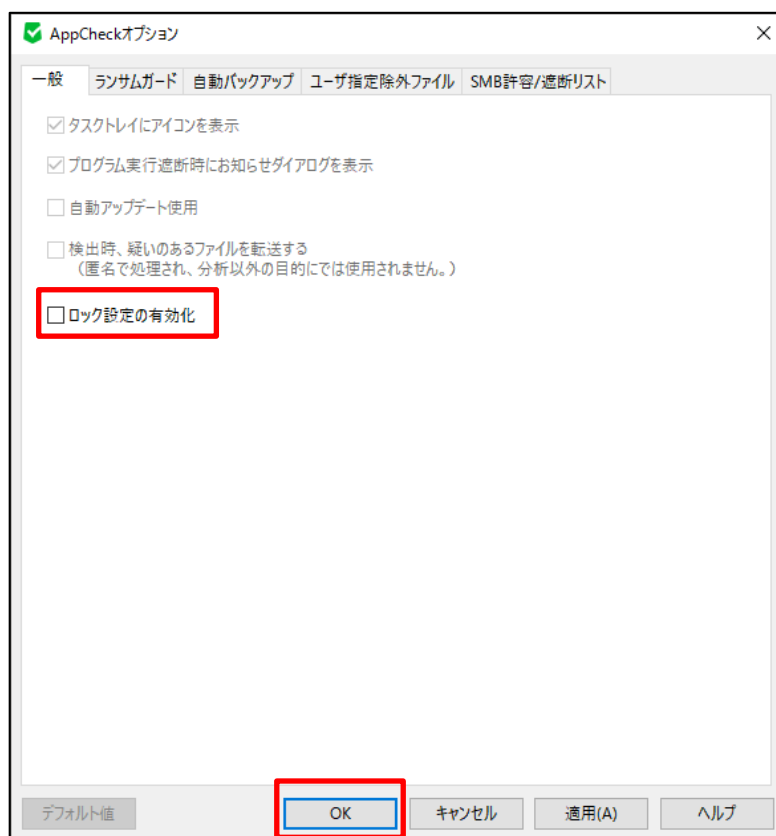
- (1) 「ロック設定の有効化」のチェックをはずします。



- (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。



(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。



3.2.2 オプション : ランサムガード

AppCheckオプション

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

一般 ランサムガード エクスプロイトガード 隠蔽フォルダ クリーナー

☒ ランサムウェアアクション遮断実行

☒ 毀損動作検知実行

☒ 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,cs,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,tiff,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

☒ SMBサーバ保護

デフォルト値 OK キャンセル 適用(A) ヘルプ

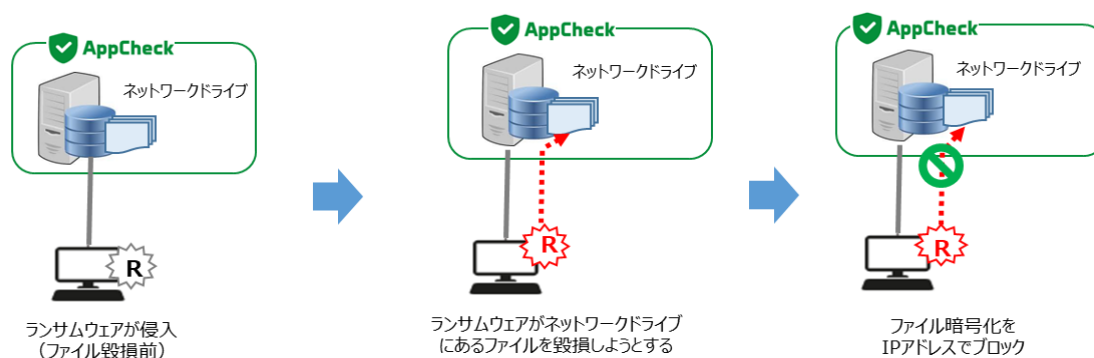
ランサムウェアアクション遮断実行	ランサムウェア感染でファイル毀損の動作が発見された時に、"ランサムウェア動作検知"お知らせを表示しプロセスを遮断します。
毀損動作検知実行	ランサムウェアにより元のファイルを復旧不可能状態に削除する動作を検知して遮断します。
MBR保護	Master Boot Record (MBR) 領域を改竄しようとするファイルの実行アクションを遮断することによる保護機能を実行します。
AppCheck Pro 拡張機能	
ランサムウェア遮断後、自動修復実行	ランサムウェアプロセスを遮断後、検知したランサムウェアプロセスのファイルまで自動で削除します。

保護するファイル拡張子 (区分子、または ;)	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となります。 7z、ai、bmp、cer、crt、csv、der、doc、docx、dwg、eps、gif、hwp、jbgw、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。

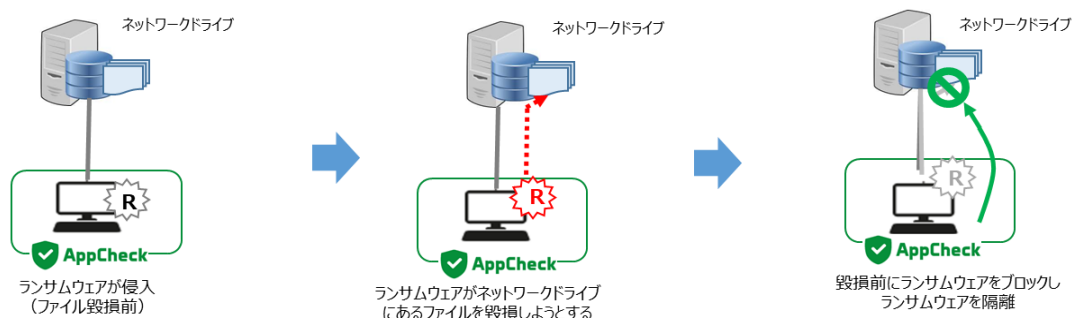
※「デフォルト値」ボタンをクリックすることにより、設定値がデフォルト値に戻ります。

※CMS版の場合、デフォルトで登録されている拡張子が異なる場合があります。

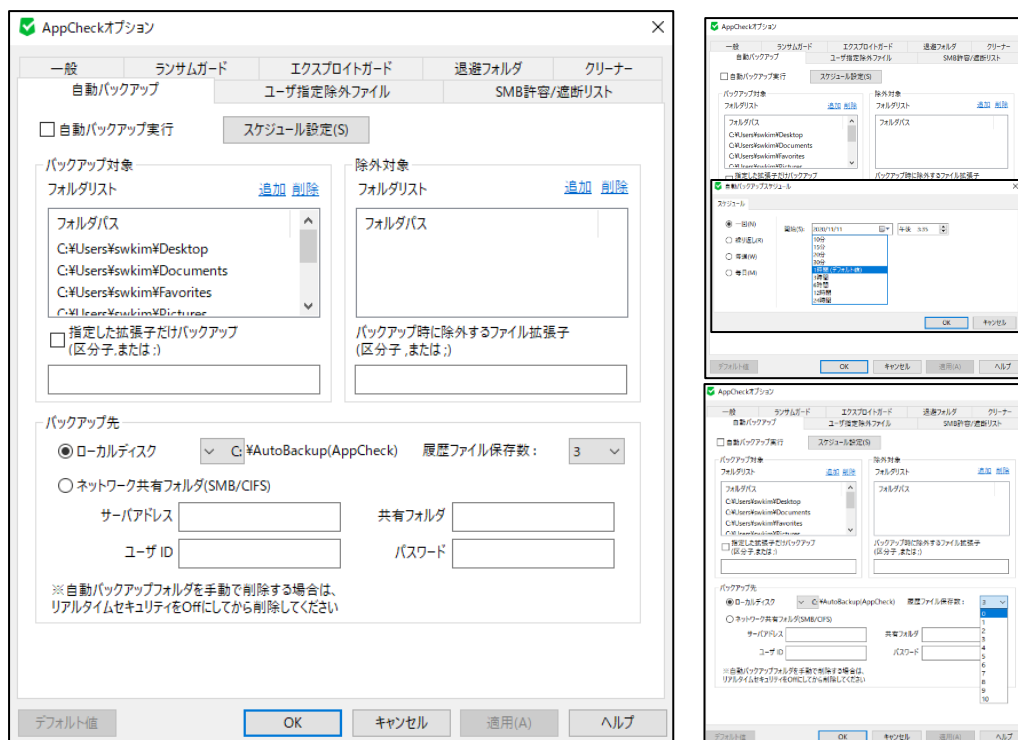
・SMB サーバ保護



・ネットワークドライブ保護



3.2.3 オプション：自動バックアップ



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 (区分子,または ;)	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 拡張子(区分子,または ;)	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。
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 (SMB/CIFS)	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。

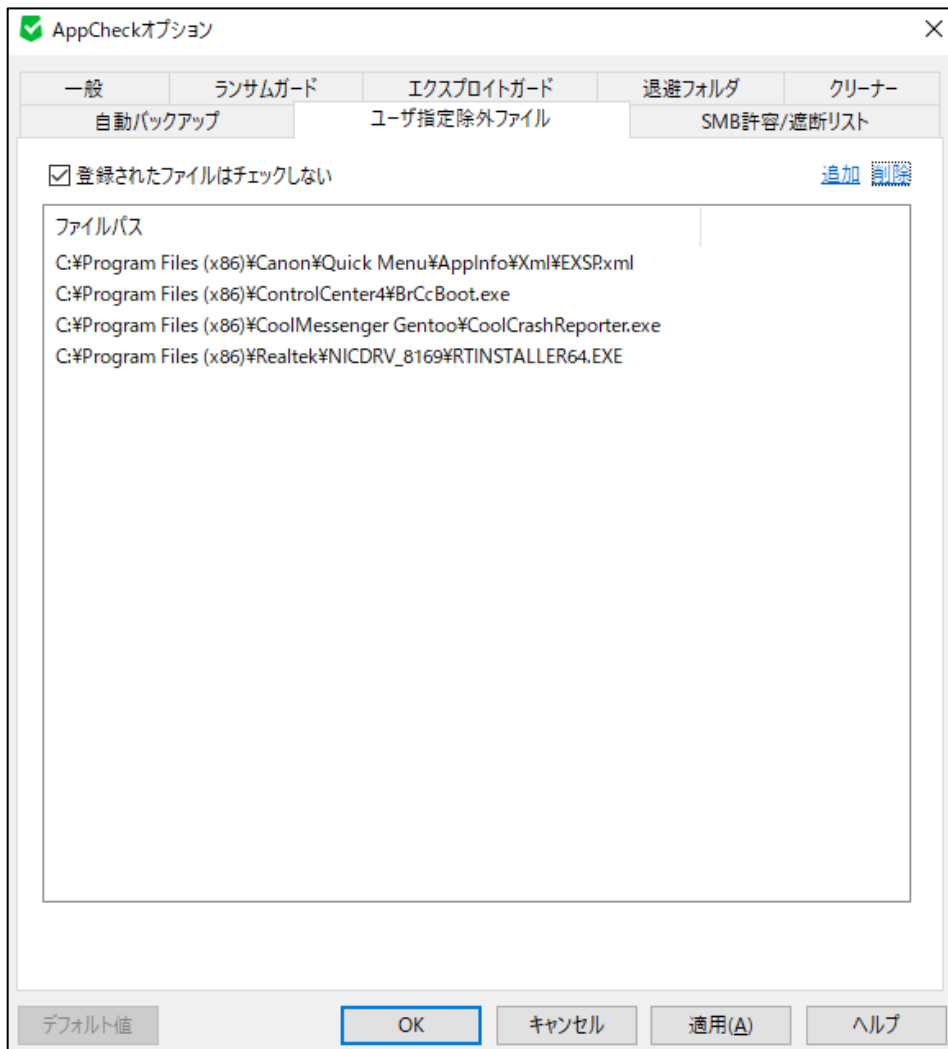
<注意> 自動バックアップを行う際には、バックアップ先の空き容量を十分確保して下さい。

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。

3.2.4 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いません。



<注意>

基本的にAppCheck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。

3.2.5 オプション : SMB許可/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。



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許可/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。

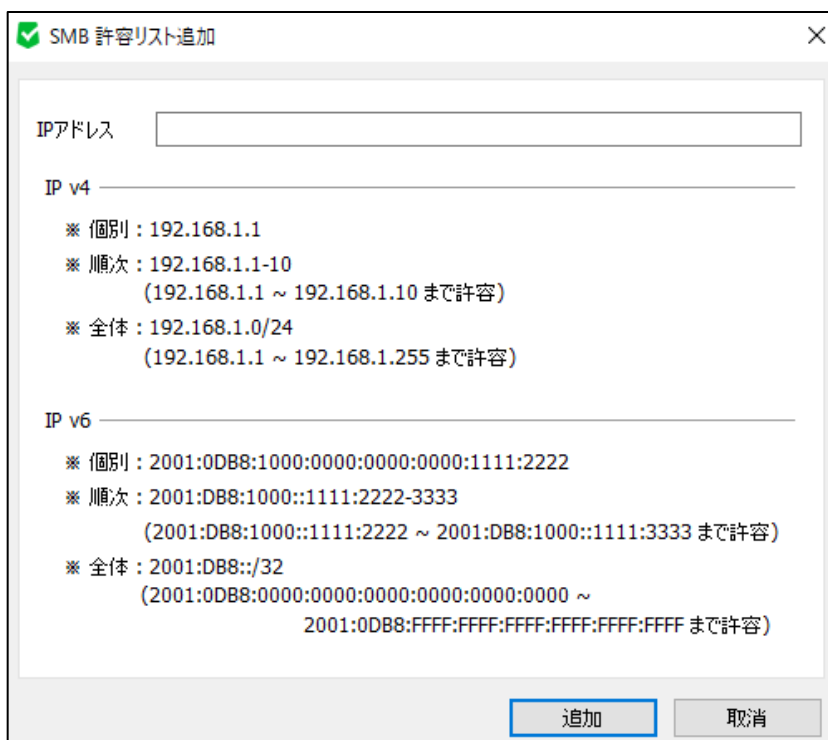
なお、ユーザーが臨時許可または常時許可を使用することによって、遮断されたIPアドレスを許可するかどうかを決定することができます。ブロックされたIPアドレスは、遮断満了時間（1時間）が経過すると、自動的に「遮断されたアドレスリスト」から削除処理され、当該遠隔PCでの再接続が可能になります。

臨時許可：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。

常時許可：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。

※「許可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 : 192.168.1.1
- ※ 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 : 2001:0DB8:1000:0000:0000:0000:1111:2222
- ※ 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)

「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。

3.2.6 オプション : エクスプロイトガード



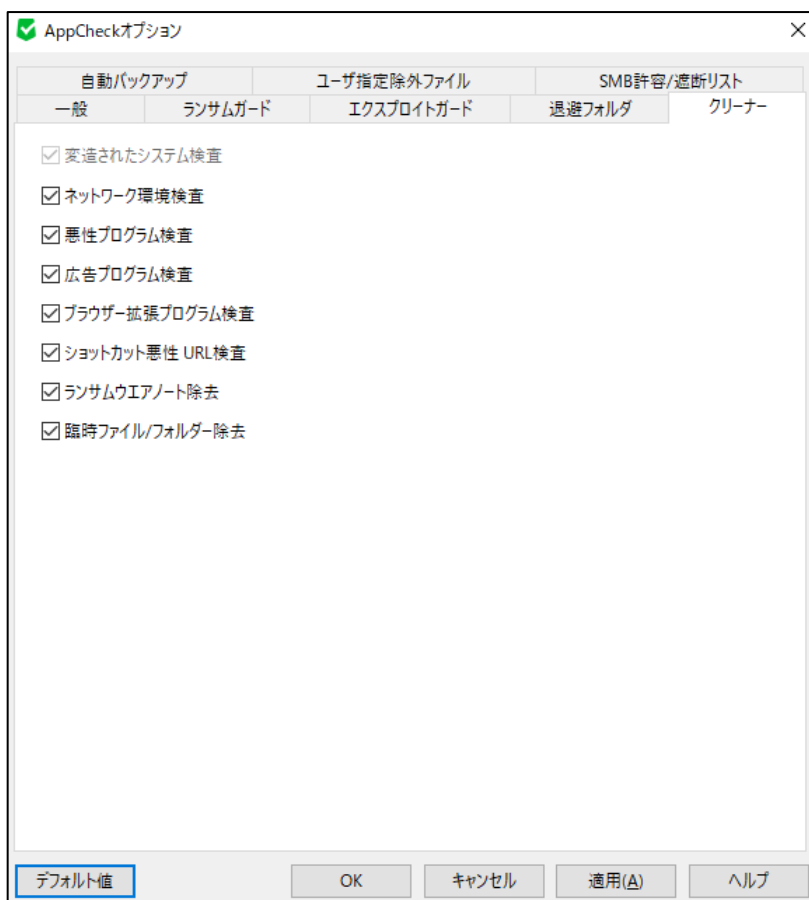
エクスプロイトガードは、「保護するアプリケーション」に対して脆弱点コードが実行される場合、悪性コードの自動感染を遮断します。「エクスプロイトガードを使用」チェックボックスを解除する場合、全体の機能が停止します。ただし、保護するアプリケーション別にチェックをすることで、選択されているアプリケーションに対して保護することが可能です。

- Webブラウザ: (IE、MS Edge、Chrome、Firefox、Opera)
- プラグイン: (Java、Flash)
- メディアプレーヤー (WMP、WMC、GOM Player、PotPlayer)
- オフィス: Microsoft Office、ハンコムオフィス、Adobe Acrobat

※CMS版のデフォルト値は「OFF」です。

※「デフォルト値」ボタンをクリックすることにより、設定値がデフォルト値に戻ります。

3.2.7 オプション：クリーナー



- 変造されたシステムスキャン: Windowsシステム関連項目中、変造されたファイルまたはレジストリが存在する場合は修正し、必要によってはWindows再起動を要求する場合があります。必須検査項目です。
- ネットワーク環境検査: システムのネットワーク構成情報を確認し、悪意のある設定がされている場合、修正します。
- 悪性プログラム検査: システムに不正なプログラムがインストールされている場合、削除します。
- 広告プログラム削除: システムに悪質な広告プログラムがインストールされている場合、削除します。
- ブラウザー拡張プログラム削除: ウェブブラウザで動作する悪性ブラウザ拡張プログラム(BHO)がインストールされている場合に削除します。
- ショットカット悪性URL検査: デスクトップ画面または、お気に入りにショートカットを作成し、クリックすると悪性サイトへアクセスされる場合、削除します。
- ランサムウェアノート除去: ランサムウェア(Ransomware)感染により、生成される決済案内ファイルが存在する場合、削除します。
- 臨時ファイル/フォルダー除去: 臨時フォルダ（%Temp%）内に存在する不要なファイル、フォルダを削除します。
- デフォルト値: クリーナーオプションの設定を初期化

3.2.8 オプション：退避フォルダ

AppCheckオプション

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

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** クリーナー

☒ ランサムウェア退避フォルダ

退避フォルダパス:

退避フォルダ使用量:

☐ 一つのファイルの大きさを最大 以下に制限

☐ 退避フォルダを隠す

退避フォルダ自動削除

☒ 経過したファイルを自動削除

☐ 退避フォルダ容量が 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。

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 〇〇以下に制限	退避するファイルの大きさを設定可能です。 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 〇〇経過したファイルを自動削除	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。 10分～7日まで、設定可能です。
退避フォルダ容量が〇〇になると、 古い順でファイルを自動削除	退避フォルダの容量を設定することが可能です。 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

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。