JSECURITY

AppCheck Pro for Windows Server

マニュアル

株式会社 JSecurity

第十二版	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 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JSecurityのホームページ（https://www.jsecurity.co.jp/contact）でご確認ください。

著作権について

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。

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

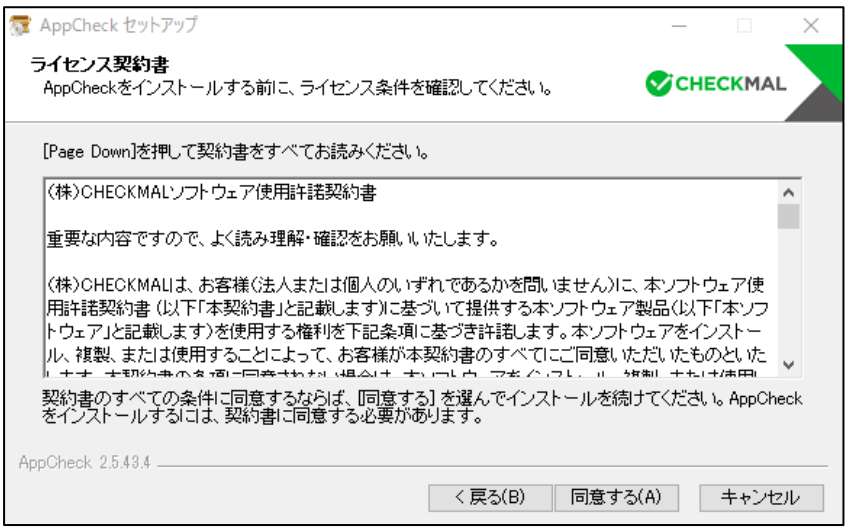
AppCheck Pro for Windows Serverは、Windows Server 2008 R2以降のOSでインストールが可能です。

1.1. 【CMSなし】製品のセットアップ

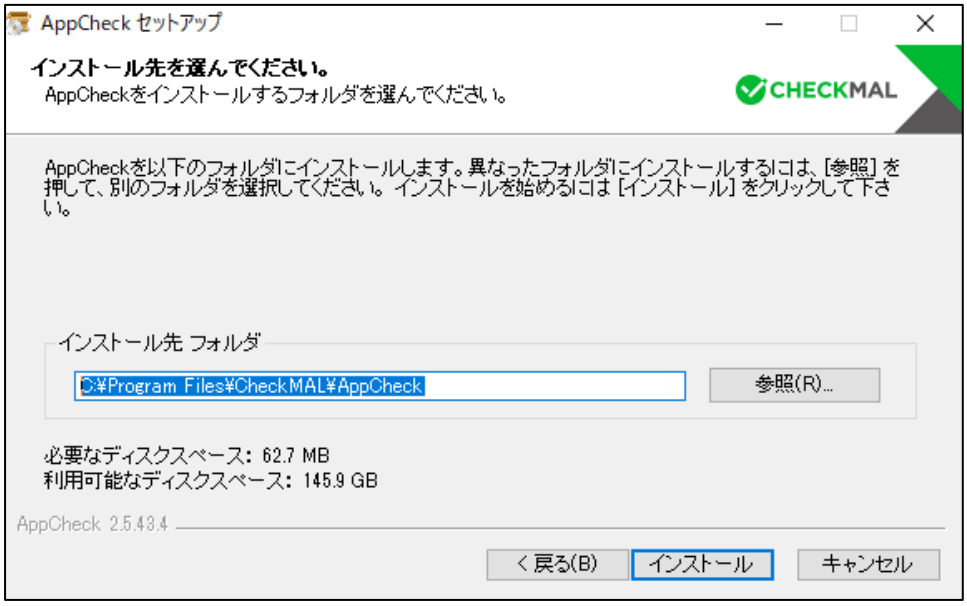
(1) インストーラーダウンロード専用ページ（ https://jsecurity.co.jp/appcheck-instdl ）でファイルをダウンロードします。

(2) 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。

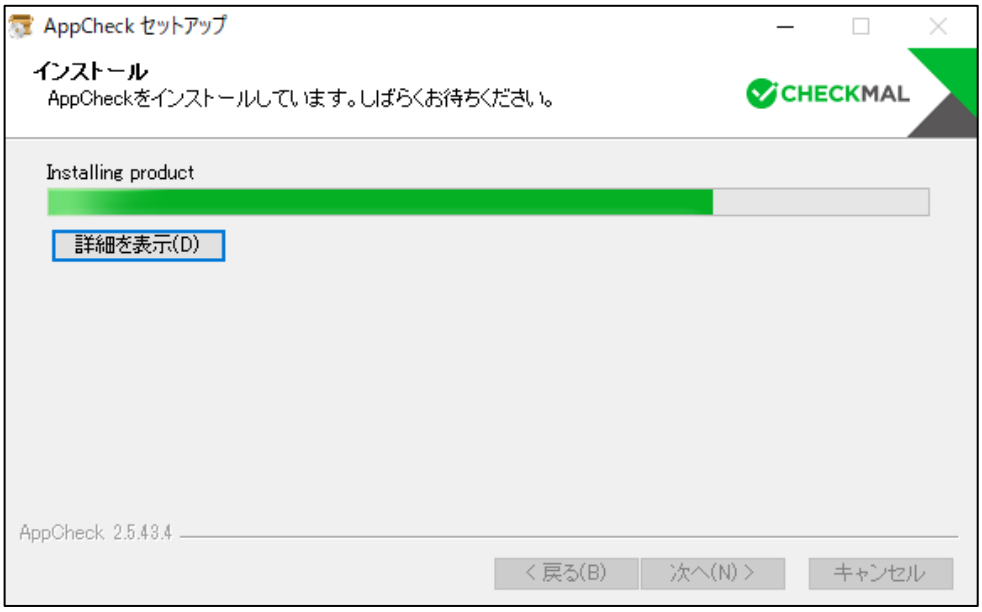
(3) ライセンス契約書（ソフトウェア使用許諾契約書）をお読みになり、同意する場合は「同意する」ボタンをクリックしてください。セットアップを開始します。



(4) AppCheck Pro for Windows Server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。「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。



(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。

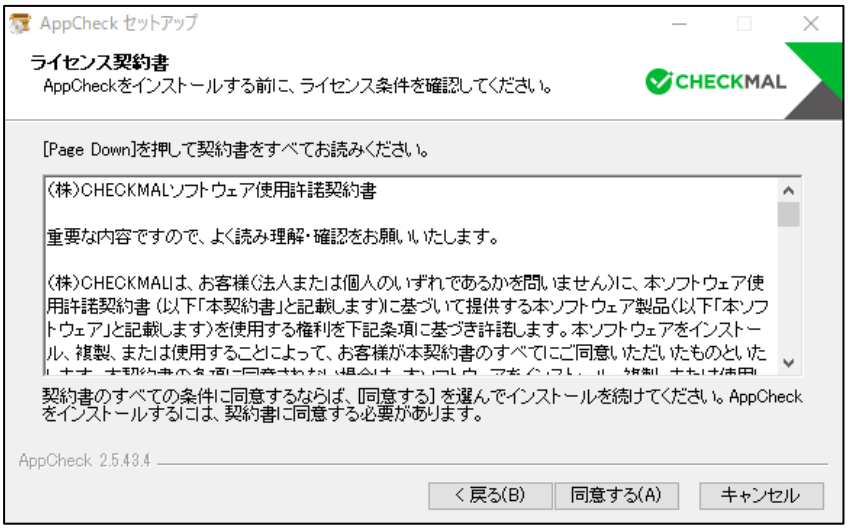
自動更新とは、お客様のPCにインストールしたAppCheckより新しいバージョンが存在した場合、自動的にダウンロードを行い、セットアップを開始することを言います。

1.2. 【CMSあり】製品のセットアップ

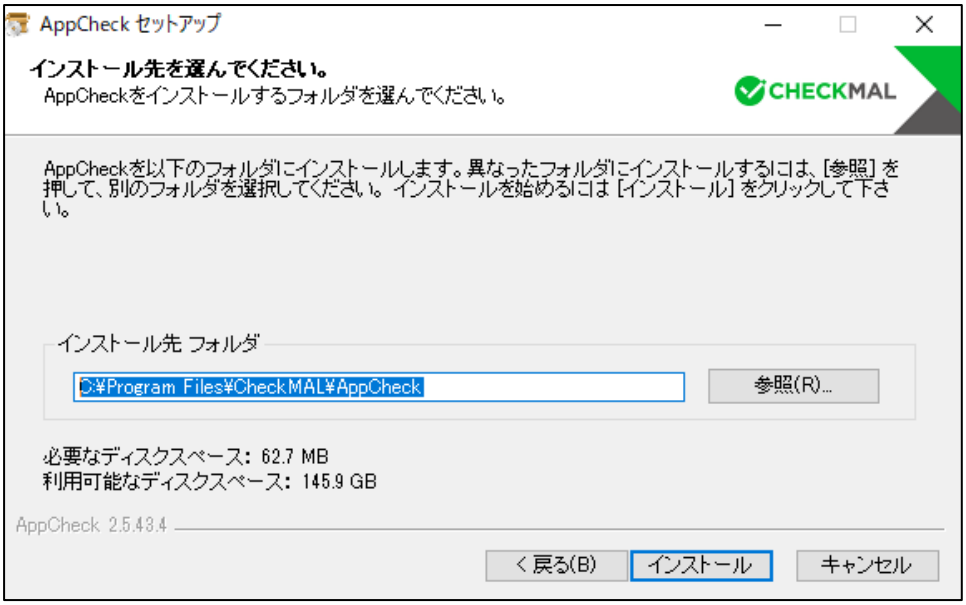
(1) CMSにログインし、下記画面赤枠のメールドレス入力スペースに受信者のメールアドレスを入力します。その後に「Eメール送信」ボタンをクリックすると、AppCheckエージェントプログラム配布メールが送信されます。受信したメールより、ライセンス登録済みのインストールプログラムをダウンロードすることが可能です。

(2) AppCheck 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。

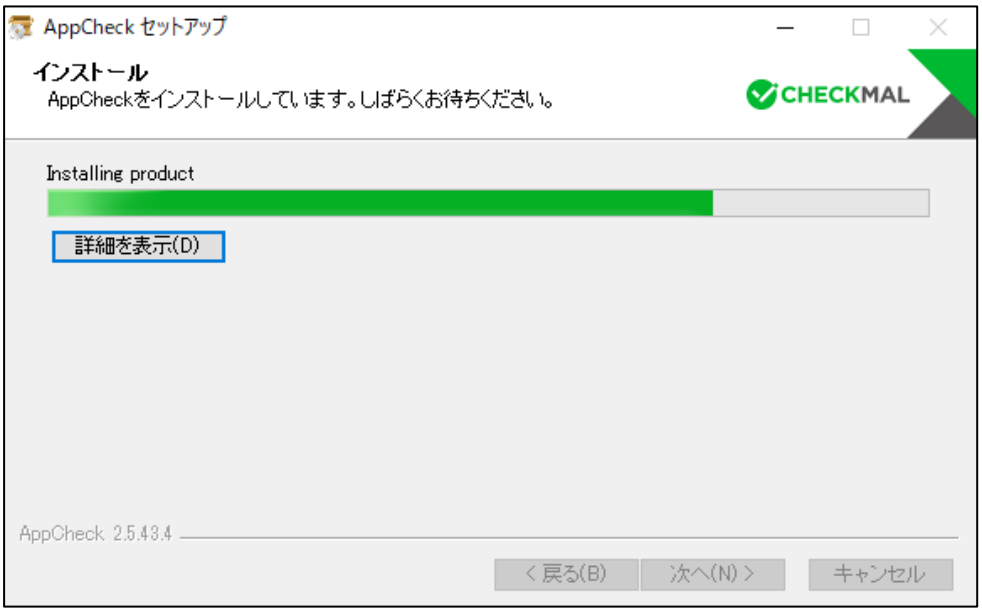
(3) ライセンス契約書（ソフトウェア使用許諾契約書）をお読みになり、同意する場合は「同意する」ボタンをクリックしてください。セットアップを開始します。



(4) AppCheck Pro for Windows Server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。「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。



(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。

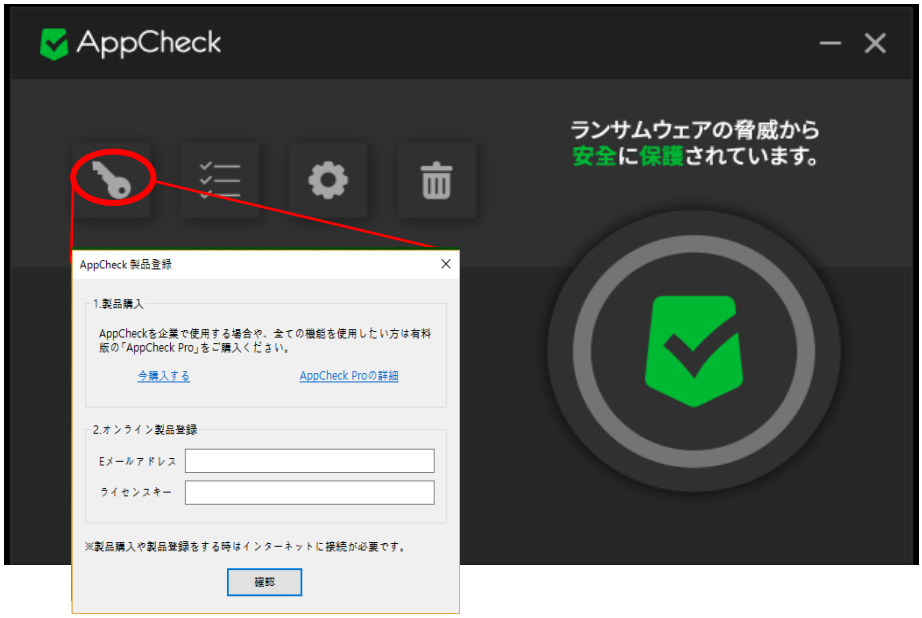
（注）AppCheckの起動時に、「AUTO UPDATE（自動更新）」を行う場合があります。

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 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。**

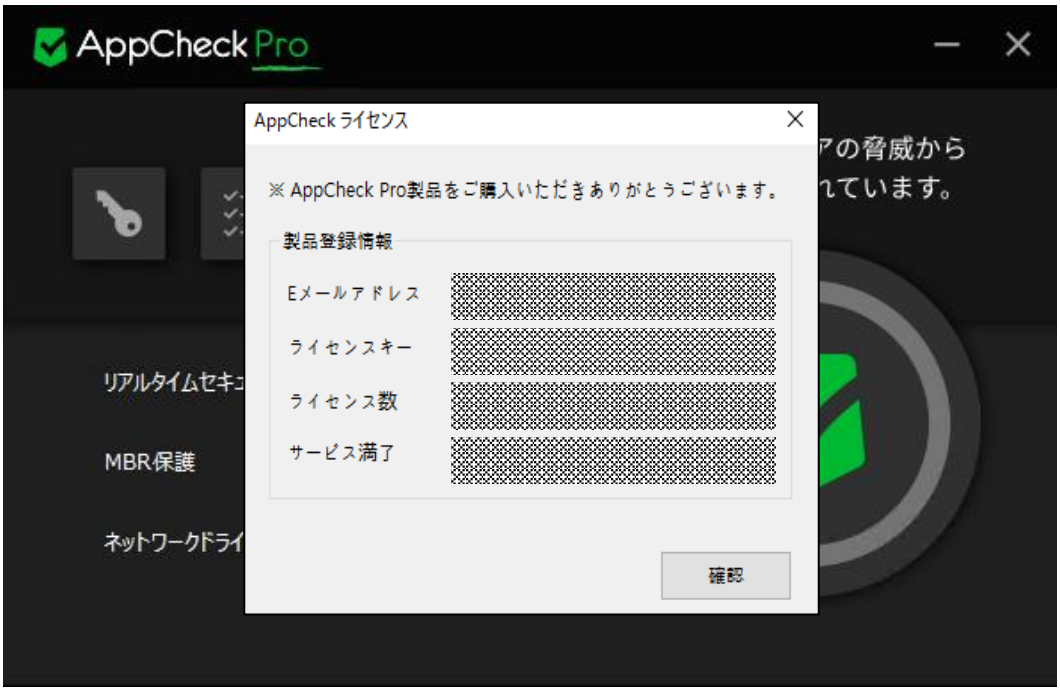


(2)サービス満了日は製品登録日から起算し、1年後となります。（1年ライセンス場合）

（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）

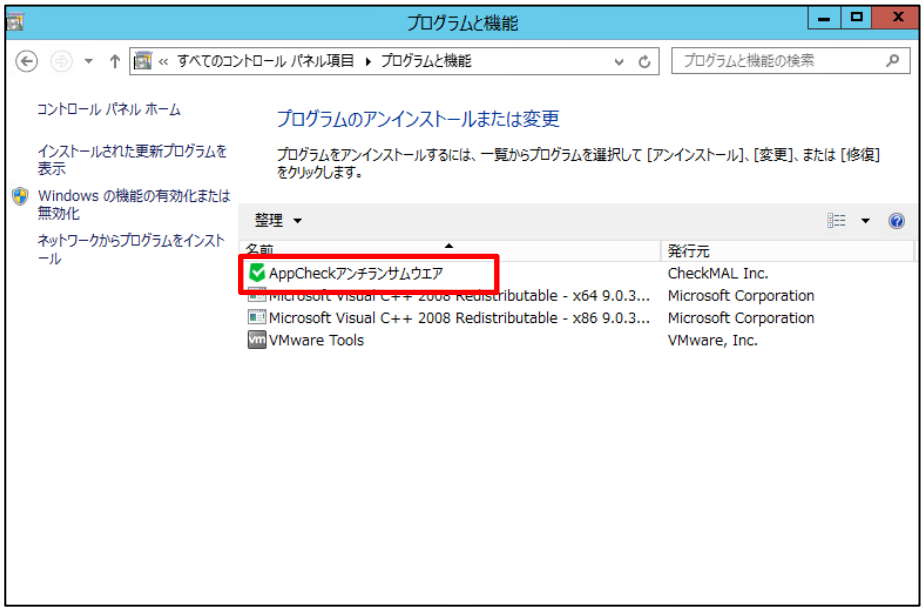


登録頂いた「E メールアドレス」「ライセンスキー」「満了日」「数量」をご確認頂き、AppCheck Pro をご利用下さい。

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

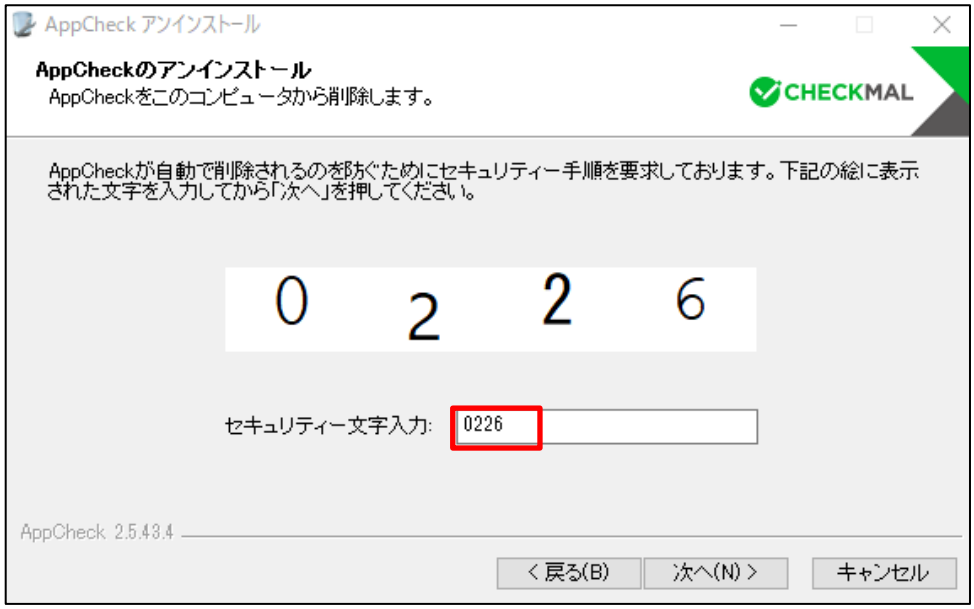
本製品をアンインストールする場合は、次の手順にて行ってください。

(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。

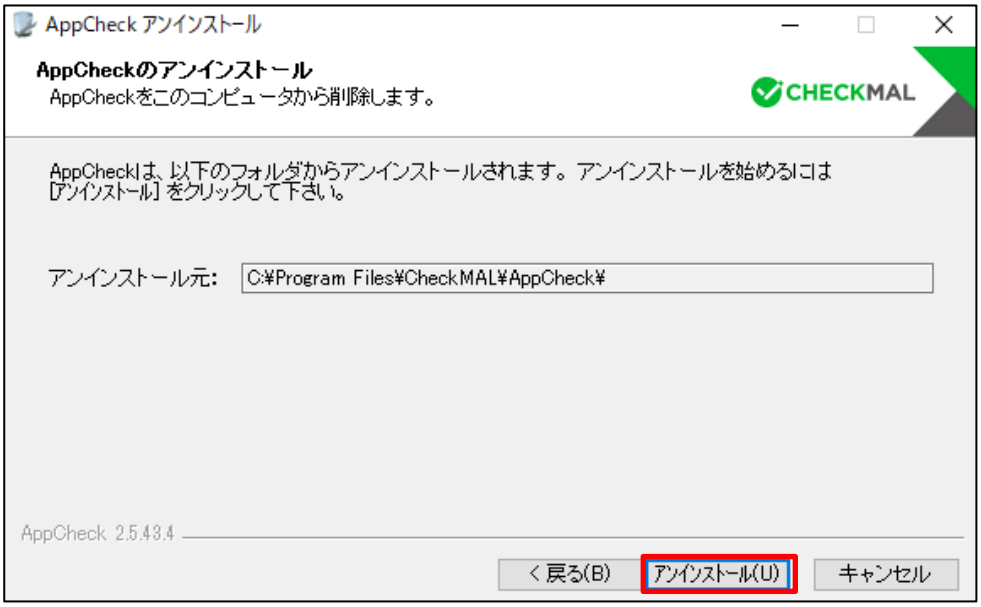


(3) 「次へ」をクリックします。

(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。



(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、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。

緑：リアルタイム保護オン

グレイ：リアルタイム保護オフ

2.3 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。

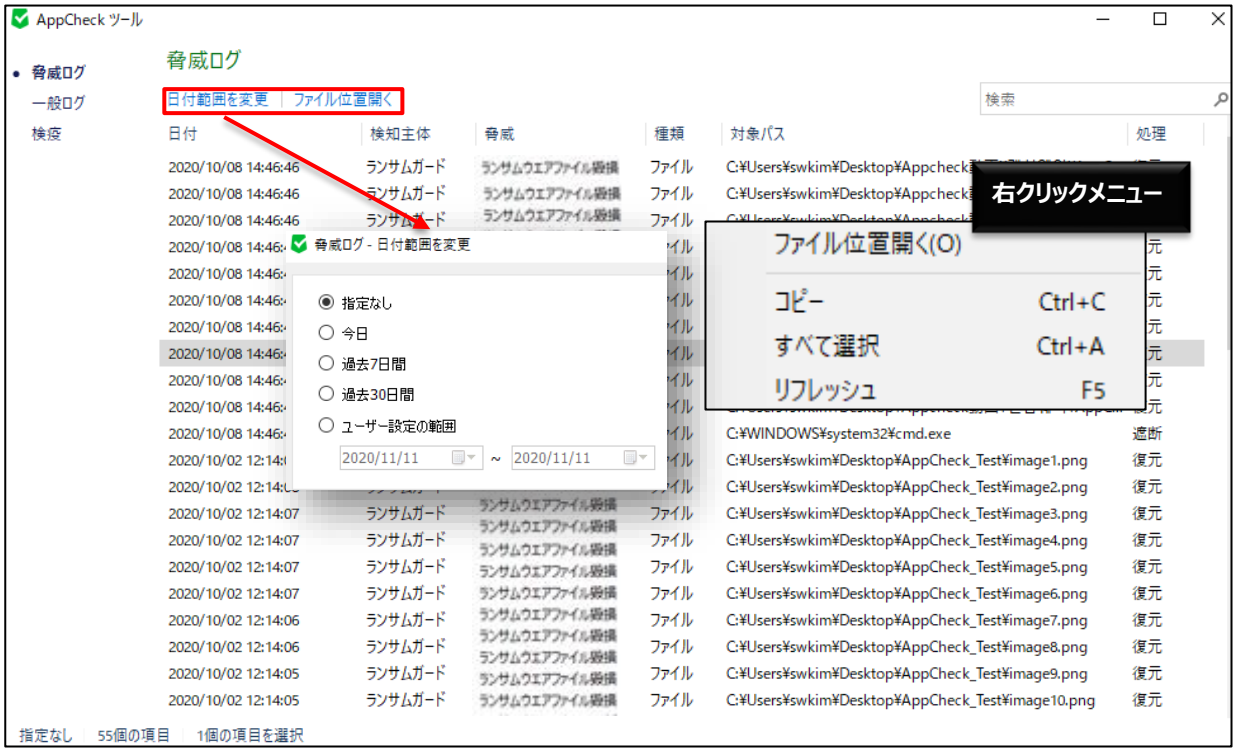
3. AppCheck メニュー詳細

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。



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。

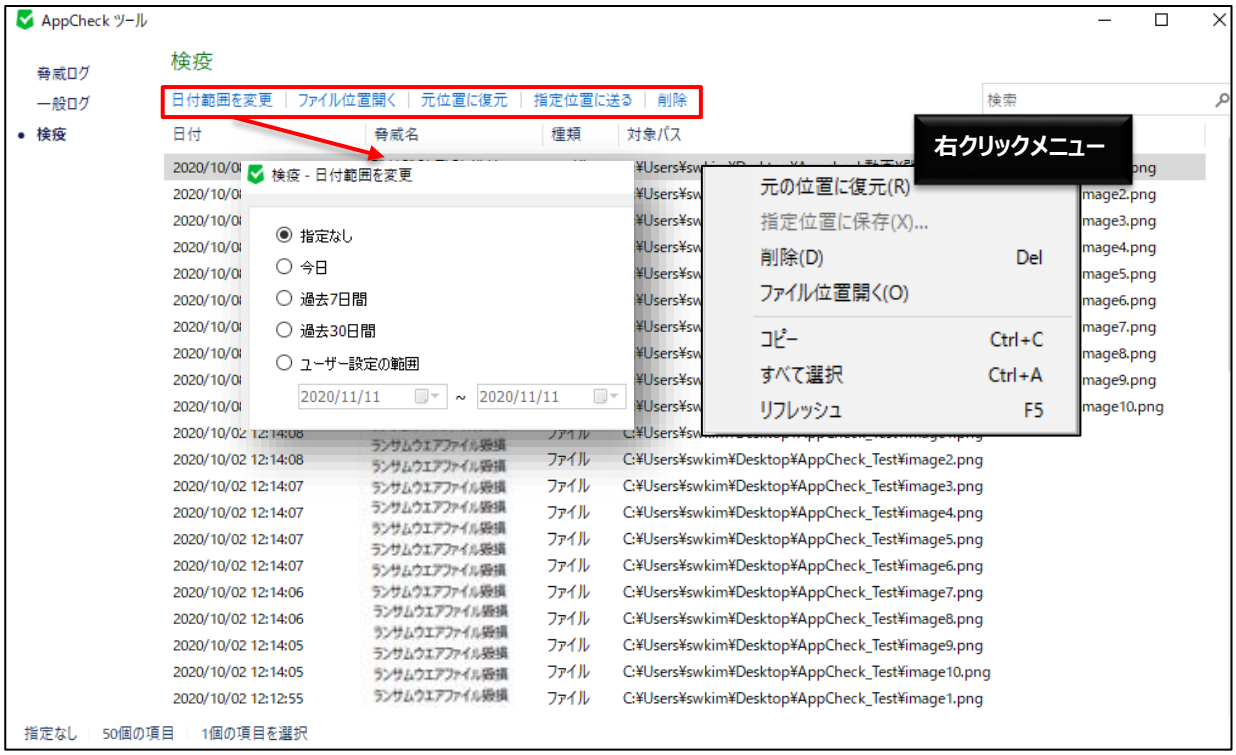
3.1.2　ツール：一般ログ

一般ログはAppCheck 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。

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。



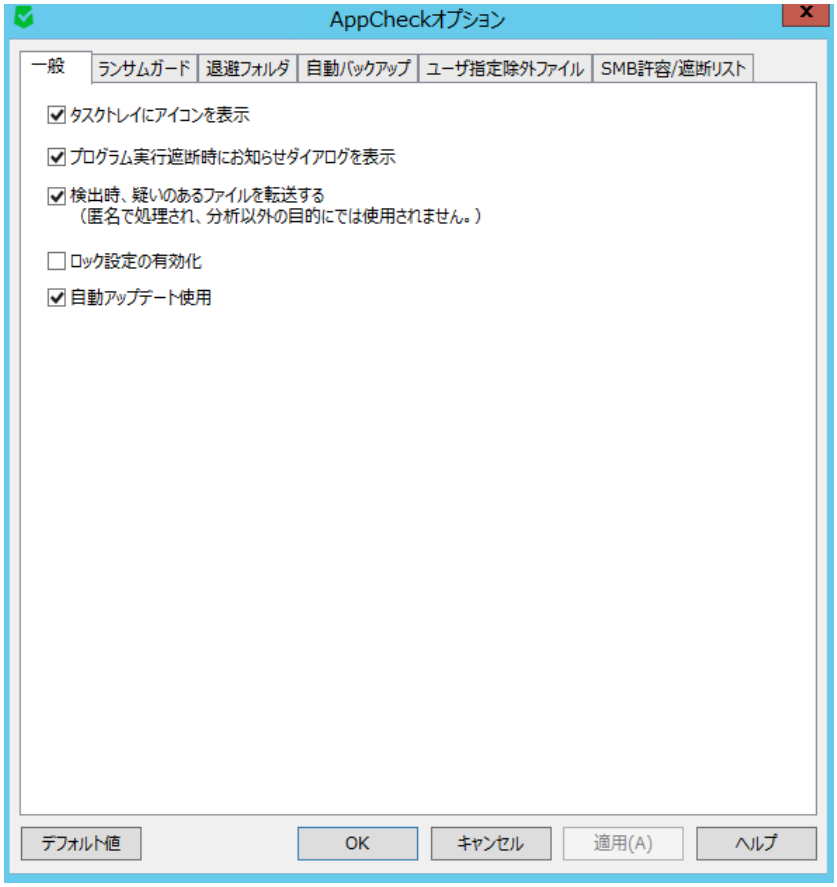
日付範囲を変更	検疫情報を日付で検索します。
元の位置に復元	選択したファイルを元の位置（フォルダ）に復元します。
指定位置に保存	選択したファイルをユーザが指定した位置（フォルダ）に保存します。
削除	検疫して保存された待避ファイルを削除します。
ファイル位置開く	選択したファイルが存在するフォルダを開きます。
コピー	選択したファイルの詳細ファイル情報をコピーします。
すべて選択	検疫で表示されているすべての項目を選択します。
リフレッシュ	検疫情報を更新します。

※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



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。
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。

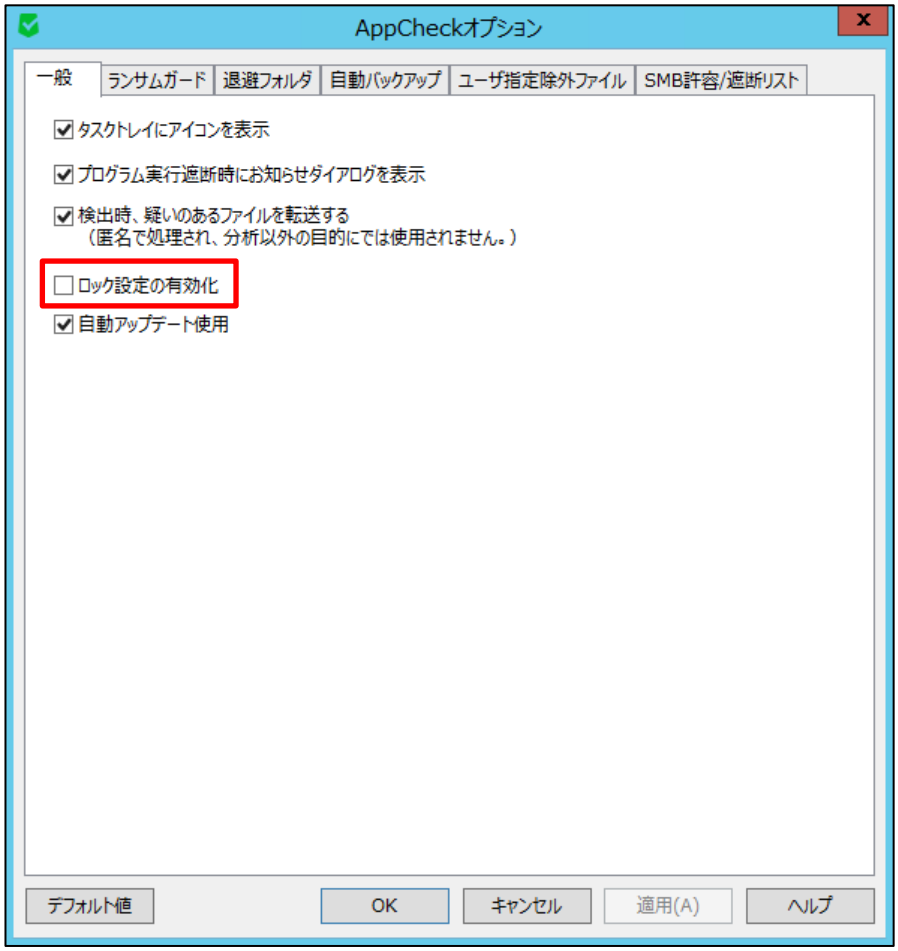
※「デフォルト値」ボタンをクリックすることにより、設定値がデフォルト値に戻ります。

■ 「ロック設定の有効化」の手順について

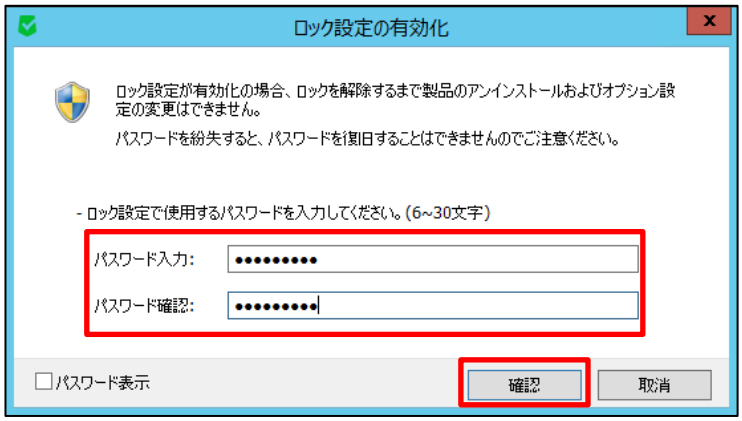
「ロック設定の有効化」に関する設定手順や解除方法ついてご説明します。

＜設定方法＞

(1)　　「ロック設定の有効化」にチェックします。



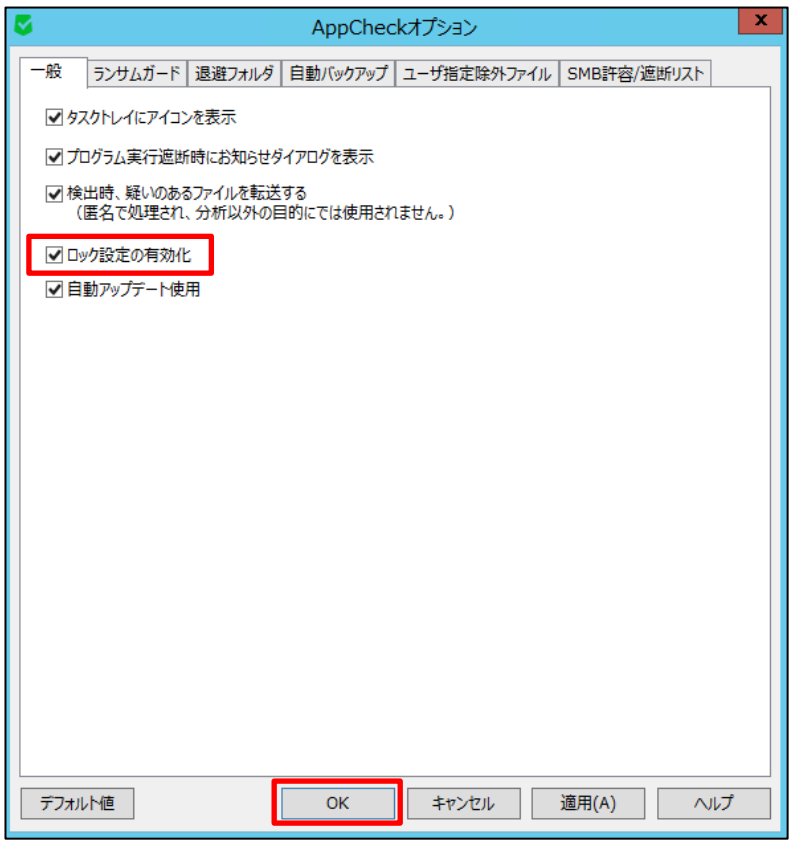
(2)　　パスワードを入力して、「確認」をクリックします。



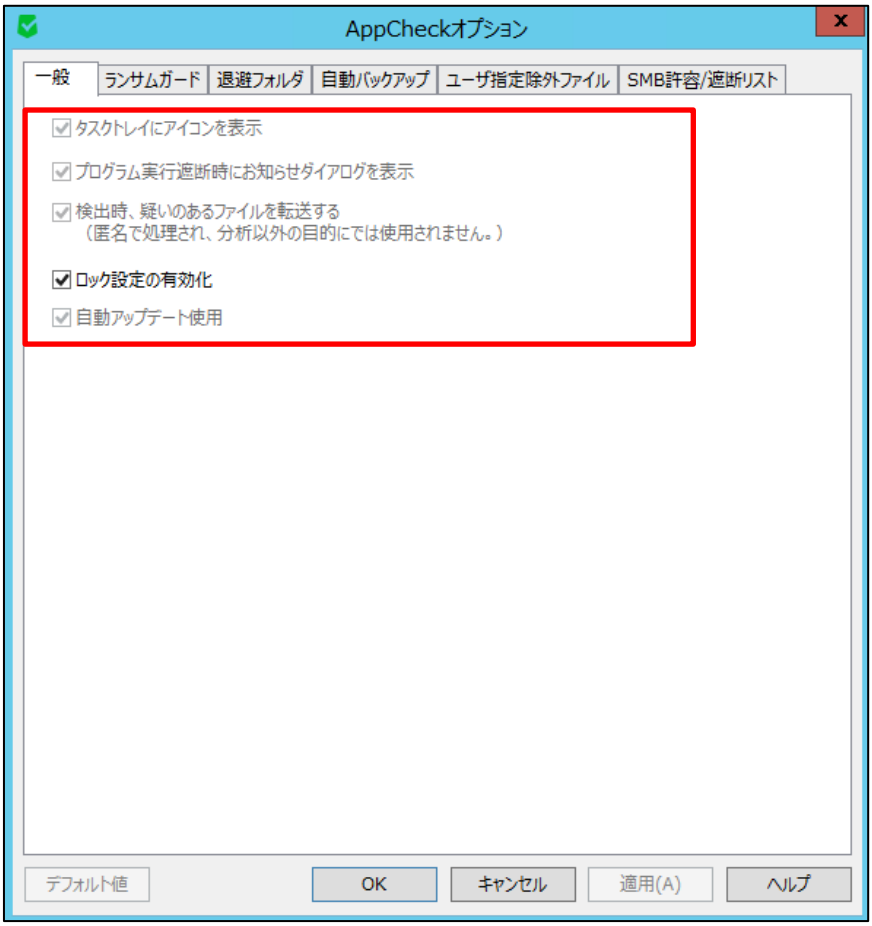
注意事項

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。

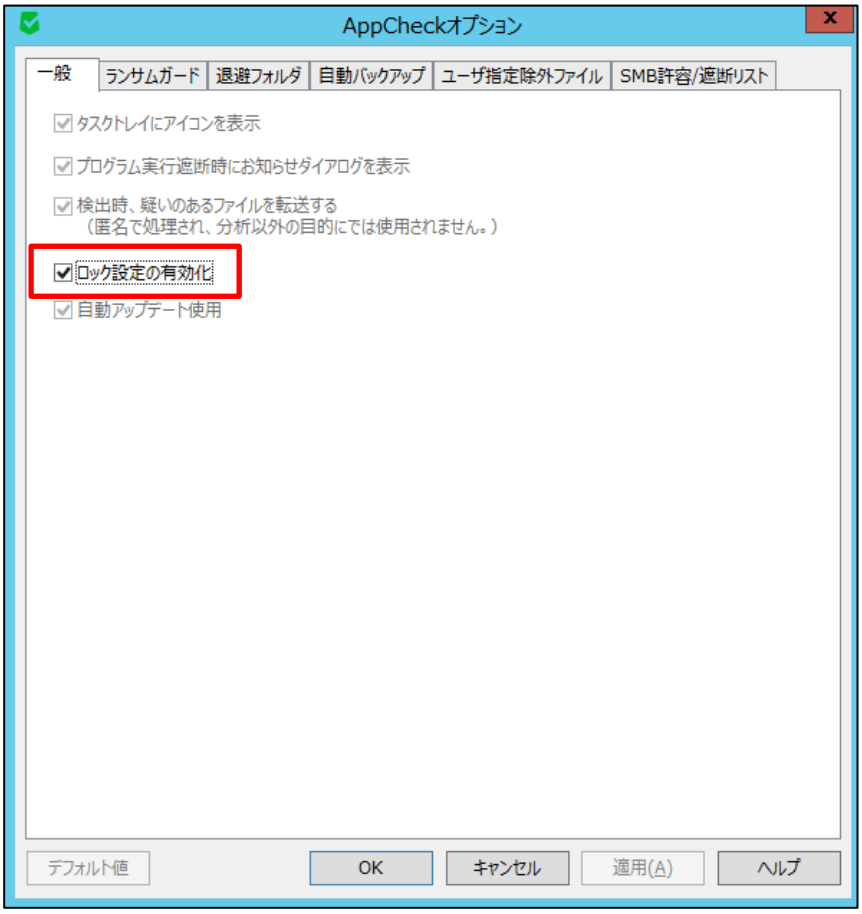


(4)　　「ロック設定の有効化」以外の設定について変更できなくなっていることを確認します。

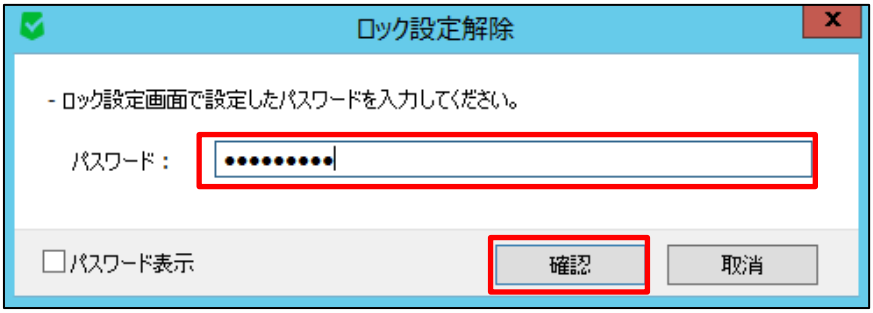


＜解除方法＞

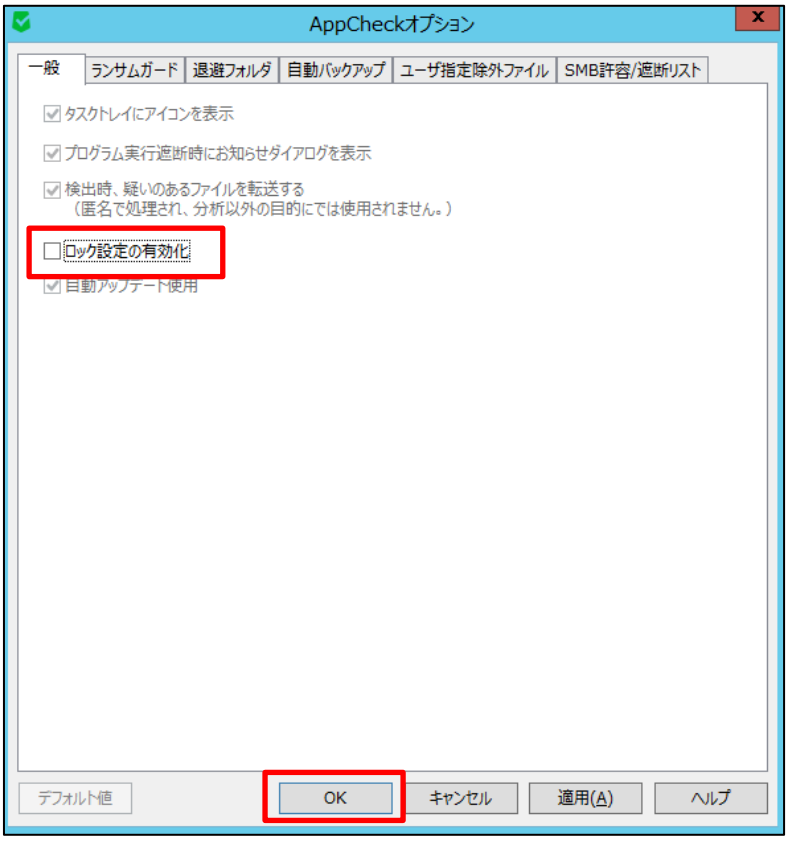
(1)　「ロック設定の有効化」のチェックをはずします。



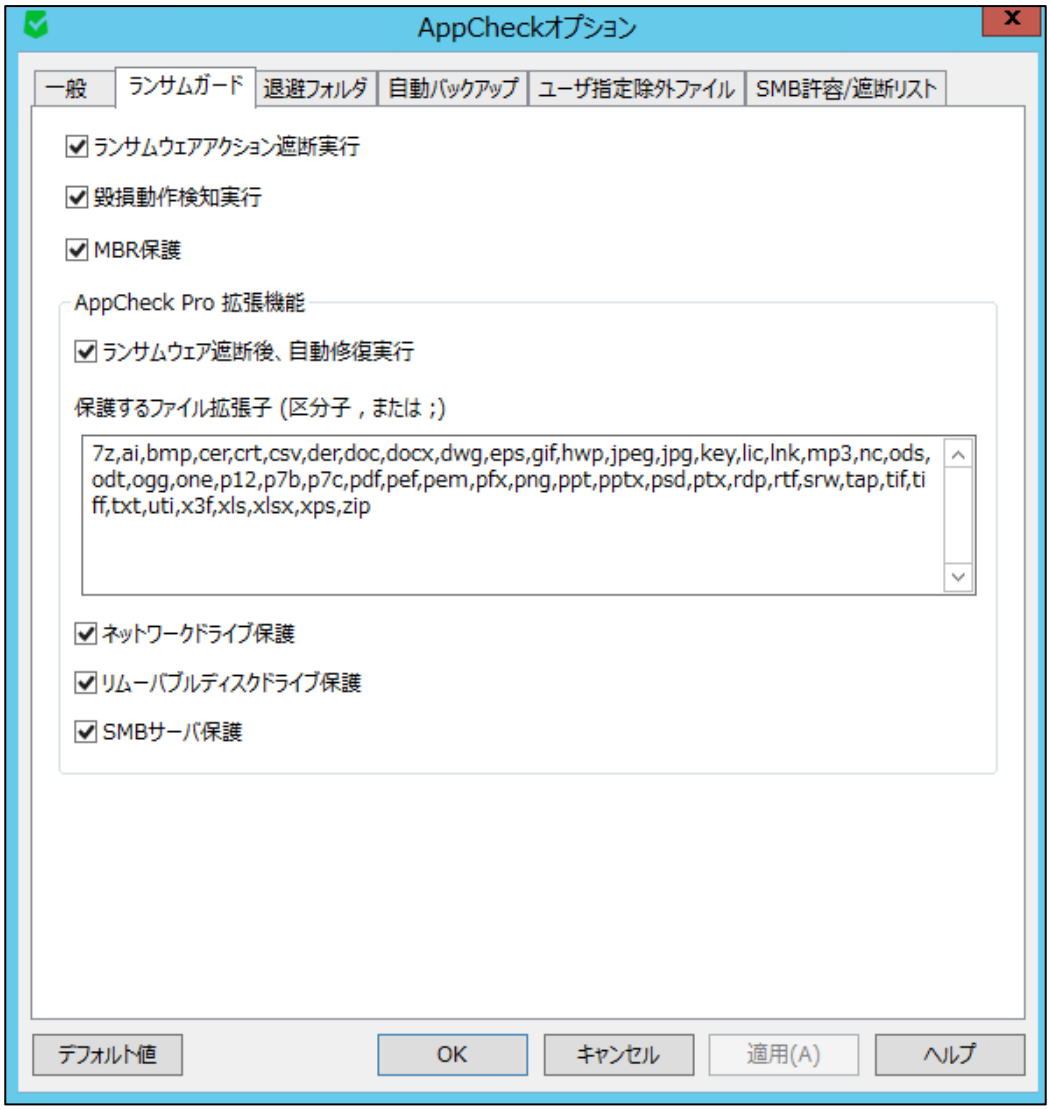
(2)　「ロック設定解除」画面が表示されるので、パスワードを入力し、「確認」をクリックします。



(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

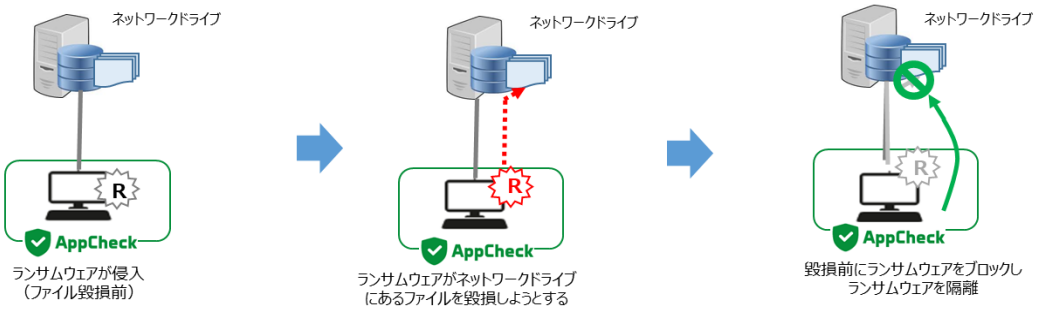


※「デフォルト値」ボタンをクリックすることにより、設定値がデフォルト値に戻ります。

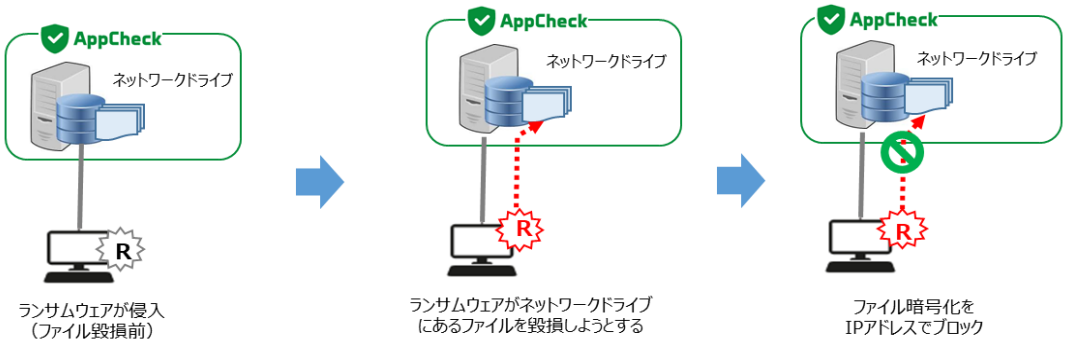
ランサムウェアクション遮断実行	ランサムウェア感染でファイル毀損の動作が発見された時に、"ランサムウェア動作検知"お知らせを表示しプロセスを遮断します。
毀損動作検知実行	ランサムウェアにより元のファイルを復旧不可能状態に削除する動作を検知して遮断します。
MBR保護	Master Boot Record（MBR）領域を改竄しようとするファイルの実行アクションを遮断することによる保護機能を実行します。
AppCheck Pro 拡張機能	
ランサムウェア遮断後、自動修復実行	ランサムウェアプロセスを遮断後、検知したランサムウェアプロセスのファイルまで自動で削除します。

保護するファイル拡張子名（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、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。

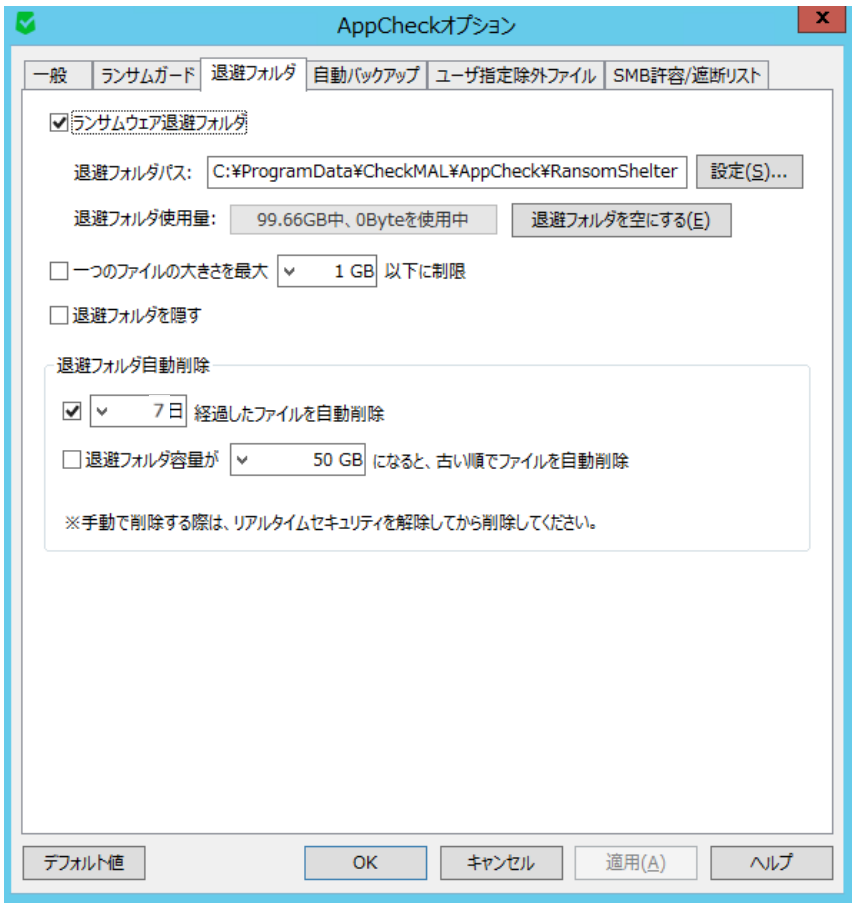
・ネットワークドライブ保護



・SMB サーバ保護

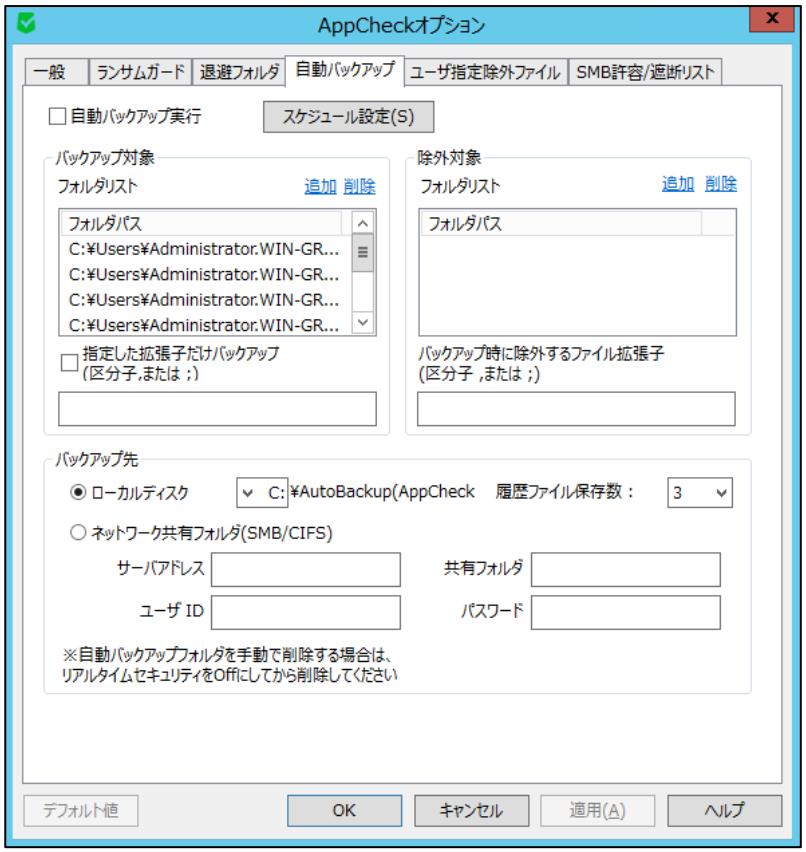


3.2.3 オプション：退避フォルダ



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 ○○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 ○○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○○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

3.2.4 オプション：自動バックアップ

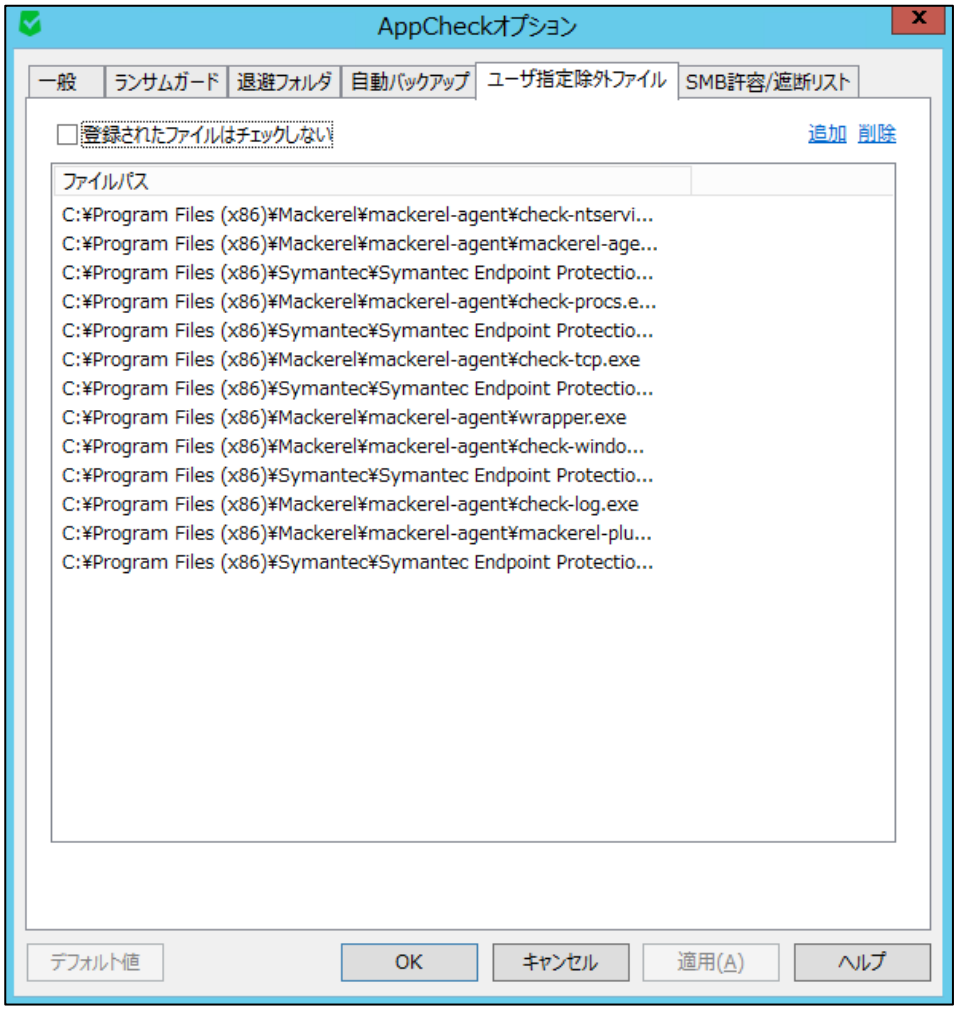


自動バックアップ実行	一定時間に重要ファイルをバックアップする機能の使用有無を選択します。 デフォルトは1時間毎の自動バックアップとなります。
バックアップ対象　フォルダリスト	バックアップする対象フォルダの追加および削除が可能です
指定した拡張子だけバックアップ	バックアップする対象フォルダに含まれたファイルのうち、指定したファイル拡張名を持つファイルだけバックアップするように設定可能です。
除外対象　フォルダリスト	「バックアップ対象」に含まれるサブフォルダを指定し、自動バックアップを除外するフォルダを指定できます。
バックアップ時に除外するファイル拡張子	バックアップする対象フォルダに含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。

3.2.5 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。

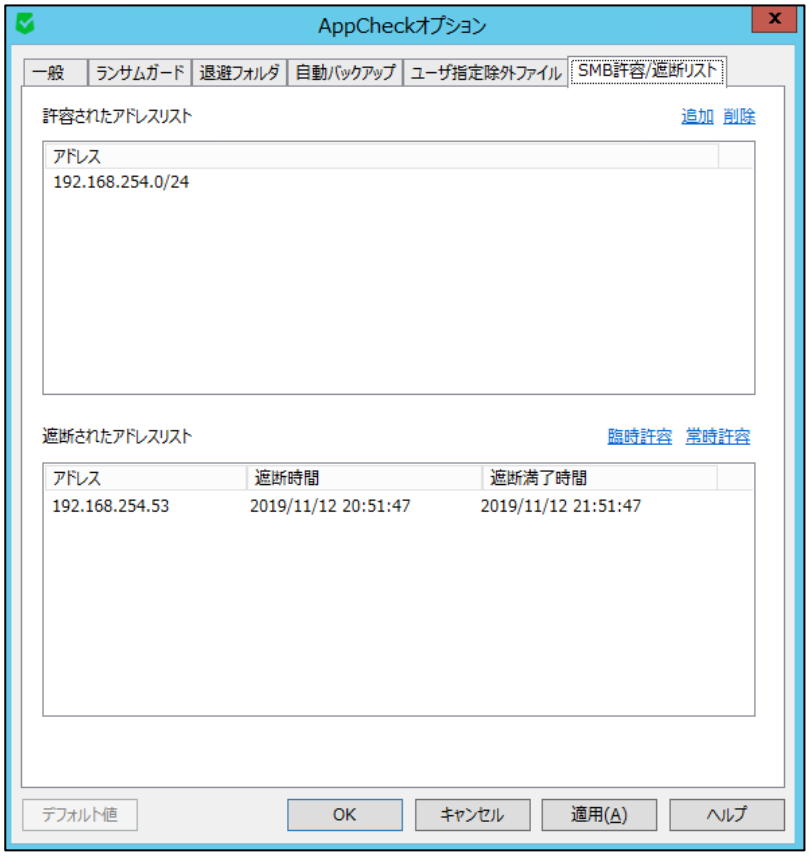


ユーザ指定除外ファイルではランサムガードによりランサムウェアと検知（遮断）されたファイルの内、お客様の判断により常に検査実行を行わないように設定許可したいファイルを記述します。（ホワイトリスト）

＜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

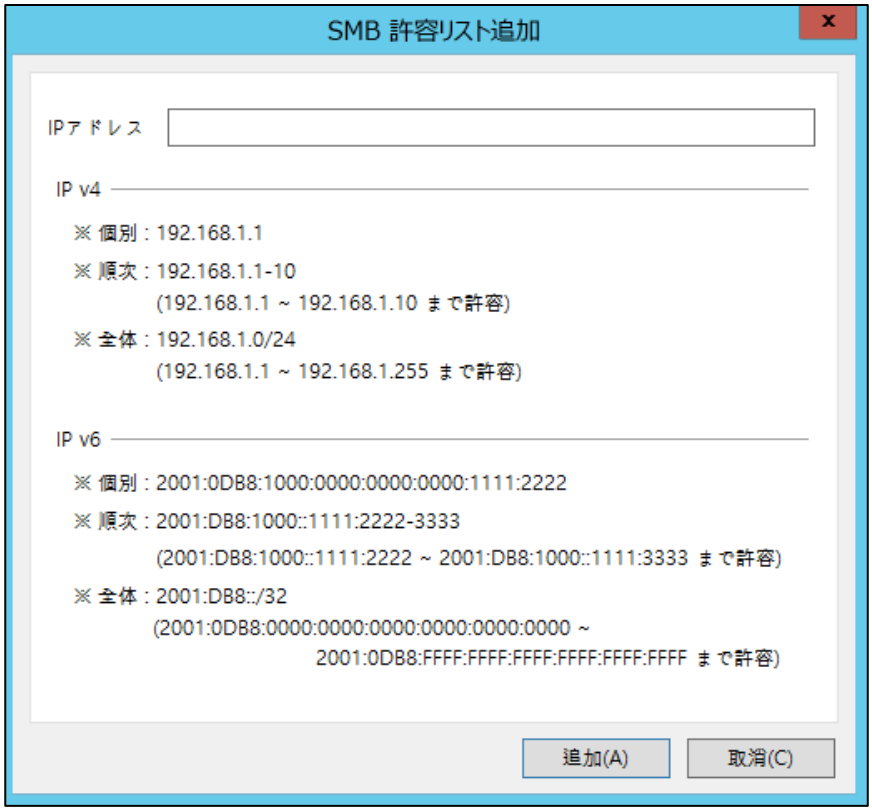
SMB保護機能が有効な場合、遠隔PCがランサムウェアに感染し、ネットワークを介して共有フォルダにアクセスし、ファイルの毀損を行った場合、SMBサーバ保護機能が働き、遠隔PCからのアクセスを遮断します。



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）



「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。