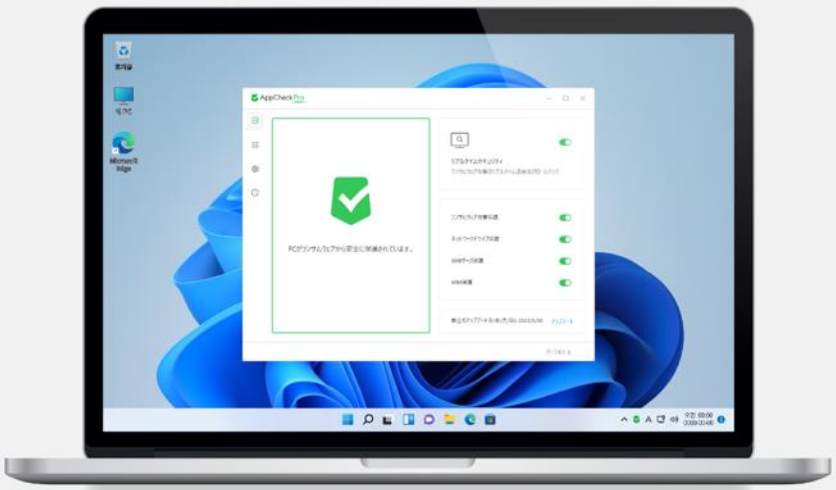
AppCheck
FOR WINDOWS SERVER

アンチランサムウェアマニュアル



NEVER MIND THE SECURITY

AppCheck can be used with other various vaccines without conflict thanks to its minimum usage capacity and use of system resources. It boasts greater safety by blocking even ransomware infections that come through networks.

JSECURITY

第八版	2023/6/15

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 V3.1.21.5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。

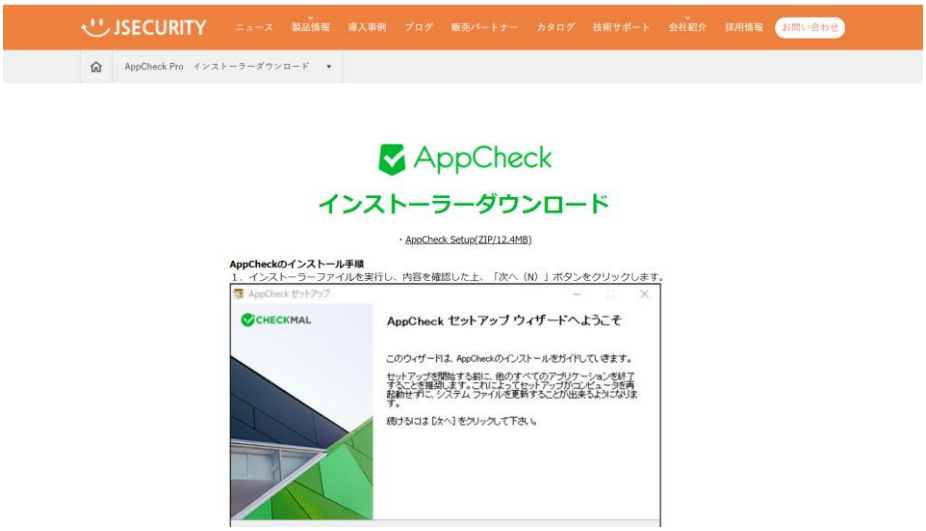
目 次

1. インストール

[1-1] インストール＆製品登録（CMSなし）

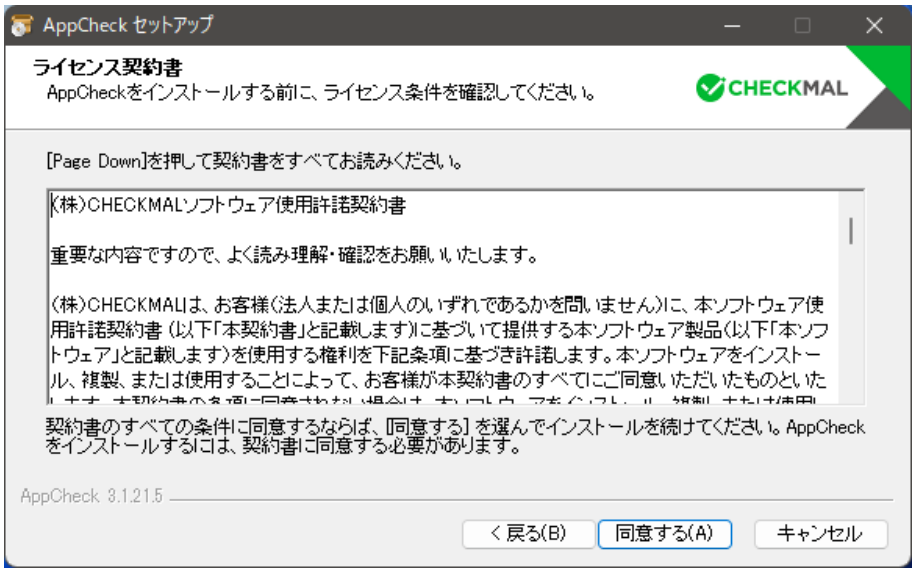
AppCheck Pro for Windows Server(以下AppCheck)は、Windows Server 2008 R2以上の日本語/英語/韓国語OSでインストールでき、OSの言語によって自動的にインストール言語が変更されます。

(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。

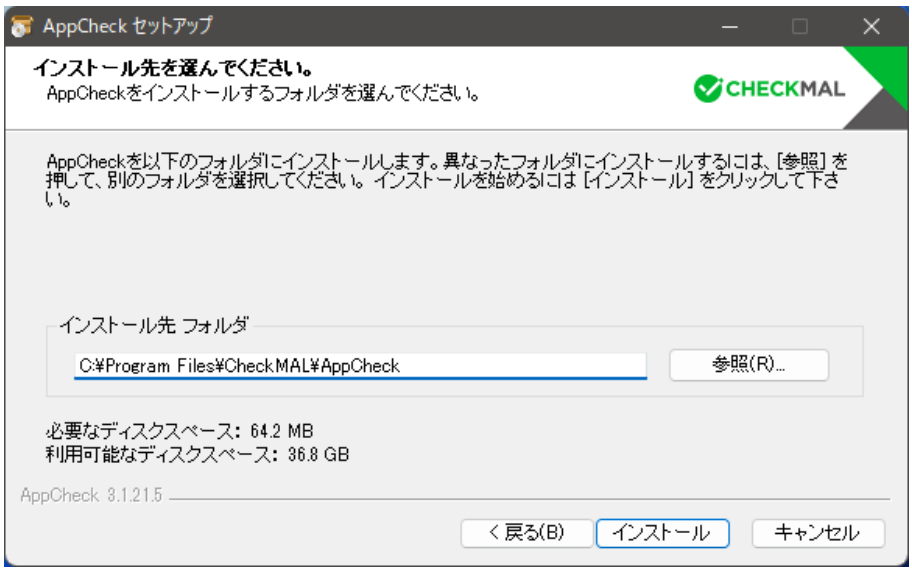


(2) AppCheckをインストールする前に実行中のすべてのプログラムを終了し、その後インストールを行ってください。

(3) (株)checkmalソフトウェア使用権契約書の内容に確認した後、「同意する」をクリックしてください。



(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。その後、「インストール」ボタンをクリックするとインストールが開始されます。



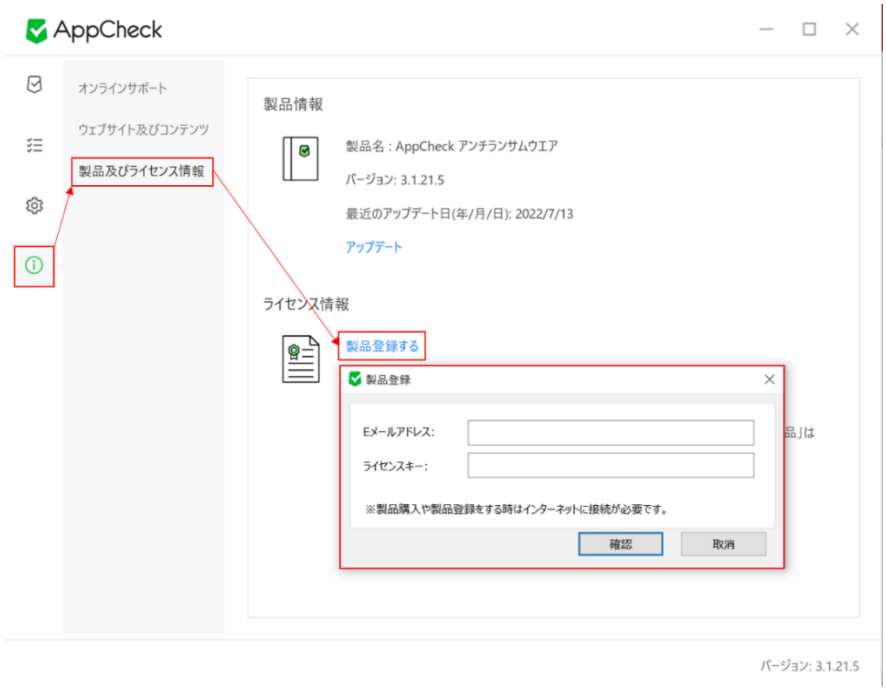
(5) インストールが完了した後「完了」ボタンをクリックするとAppCheckが自動的に起動します。

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

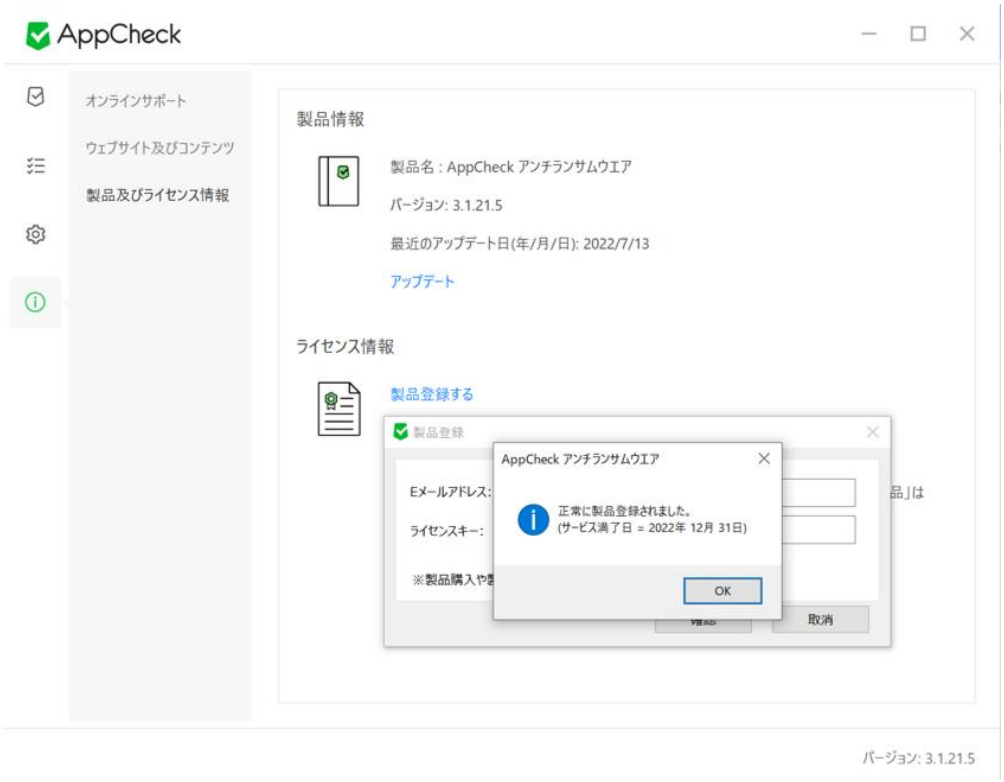
自動更新とは、お客様のPCにインストールしたAppCheckより新しいバージョンが存在した場合、自動的にダウンロードを行い、セットアップを開始することを言います。

(6) **「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。



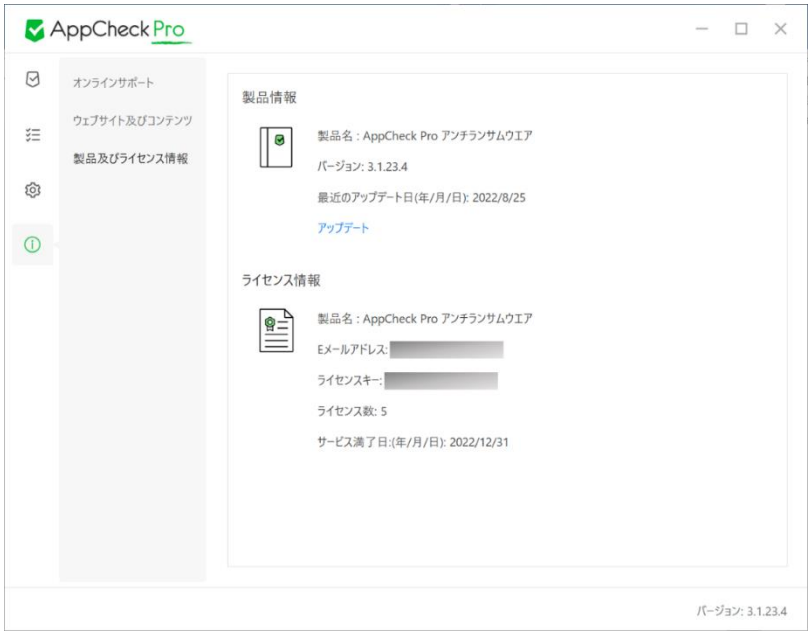
(7) サービス満了日は製品登録日から起算し、1年後となります。（1年ライセンス場合）



(8) 製品登録が完了すると、画面上部の表記が「AppCheck」→「AppCheck Pro」と変更されます。

AppCheck　AppCheckロゴ（無料版）

AppCheck Pro　AppCheckPro ロゴ（有料版）



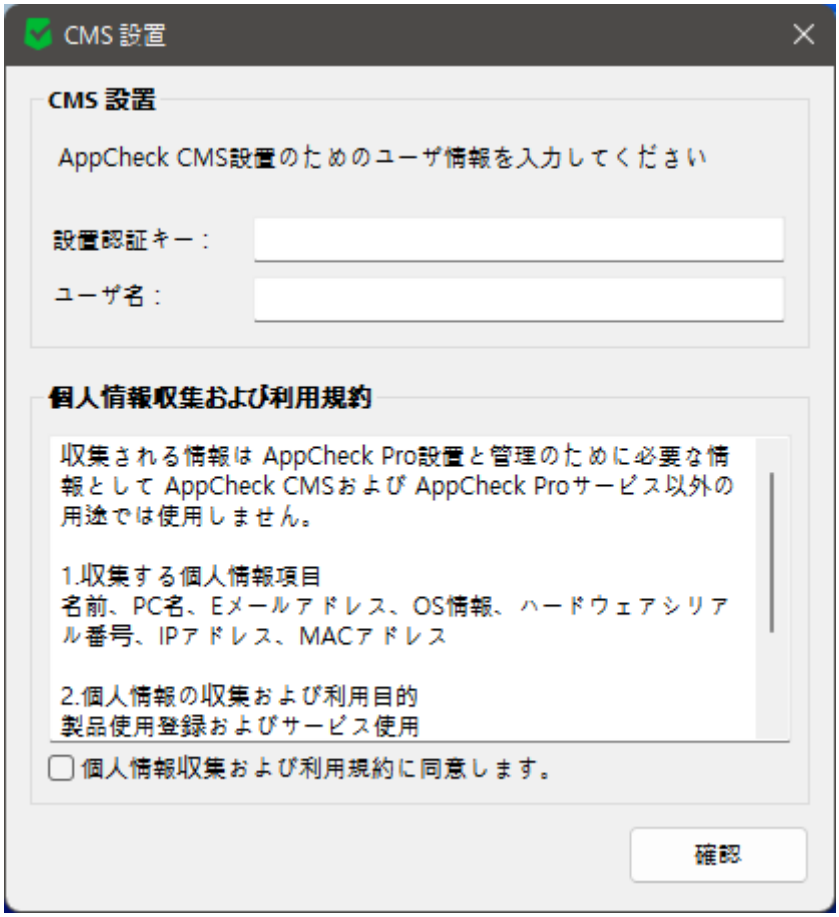
登録頂いた「E メールアドレス」「ライセンスキー」「満了日」「数量」をご確認頂き、AppCheck Pro をご利用下さい。

[1-2] インストール＆製品登録（CMSあり）

(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てください。

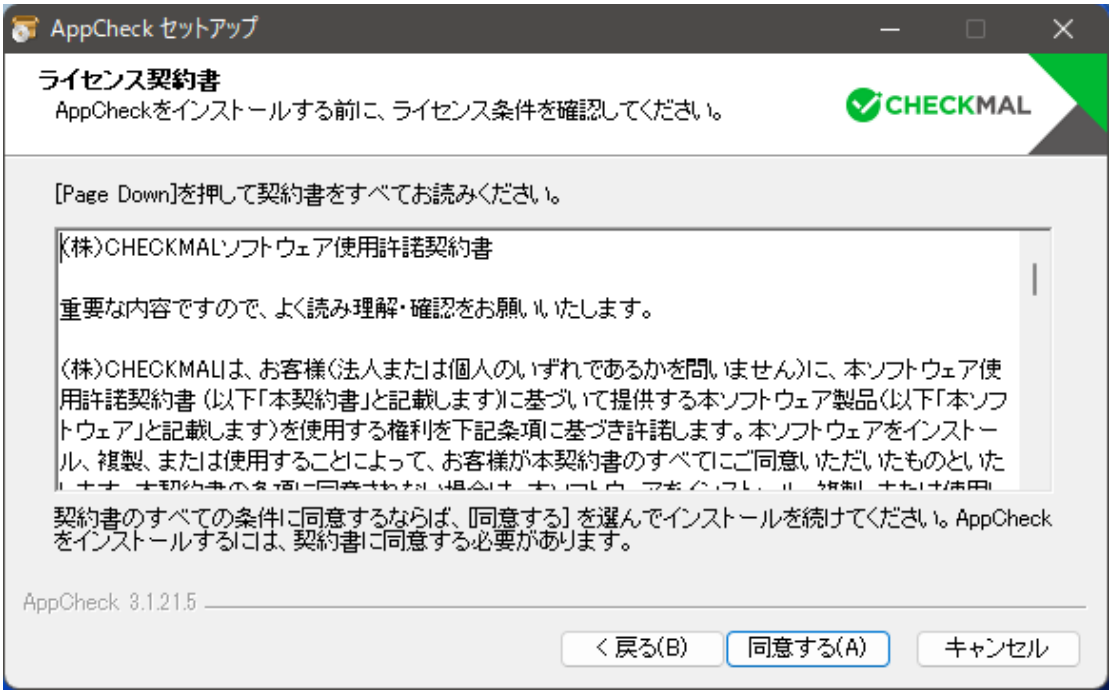
もし、CMSの配布管理で提供するAppCheckインストールファイルを利用する場合は、必ずCMSサーバーと通信可能状態である必要があります。「CMSインストール」ウィンドウに設置認証キー、ユーザー名を入力し、同意にチェックを入れてください。



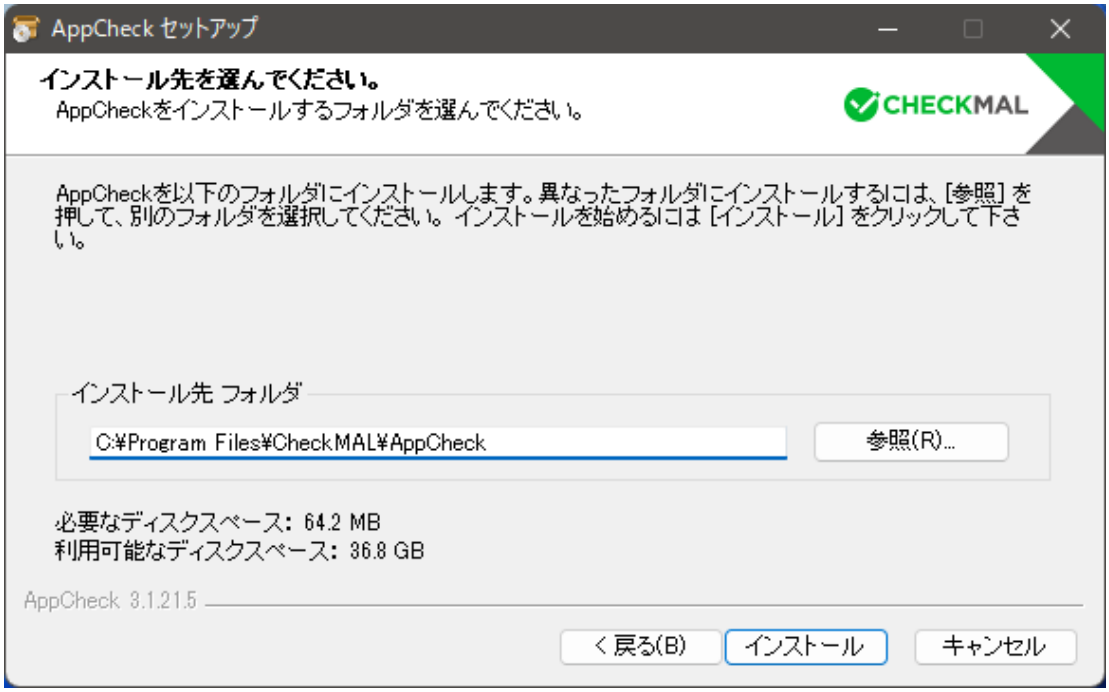
- **設置認証キー ：** 基本的に自動入力されており、CMS「配布管理」で提供する設置認証キーと同一
- **ユーザ名 :**ユーザーアカウント名のデフォルト値であり、会社のポリシーによって識別可能なユーザー名に修正可能

表示されたCMSインストールウィンドウに情報を入力した後、「個人情報収集及び利用約款に同意します」にチェックを入れ、確認ボタンをクリックしてください。 ただし、AppCheckインストールファイル名を任意に変更する場合は、自動登録された「インストール認証キー」が表示されないので、直接入力する必要がございます。

(3) (株)checkmalソフトウェア使用権契約書の内容に確認した後、「同意する」をクリックしてください。



(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。その後、「インストール」ボタンをクリックするとインストールが開始されます。

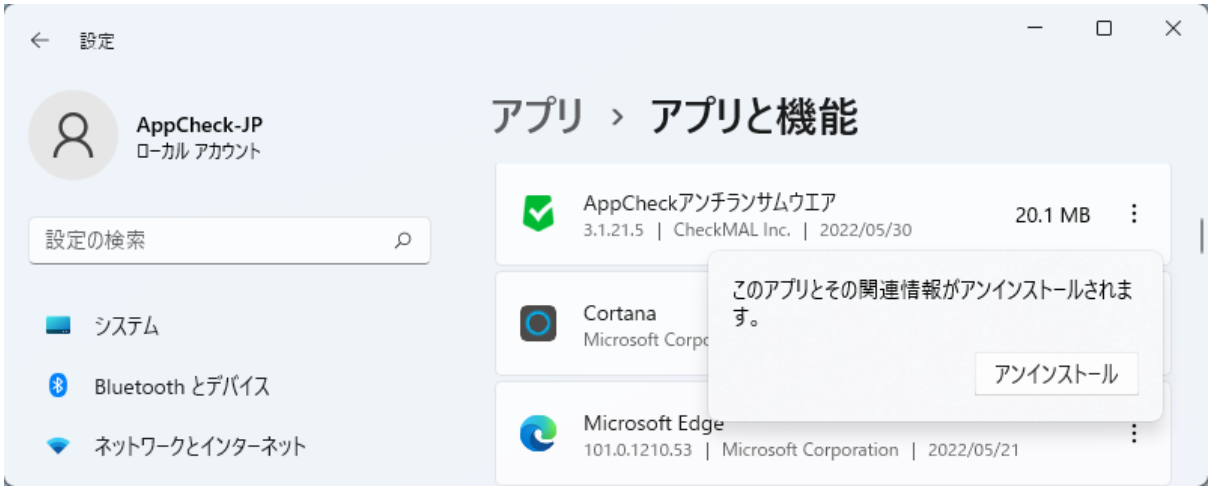


(5) AppCheckのインストールが完了した後、「完了」ボタンをクリックすると、AppCheckが自動に実行されます。

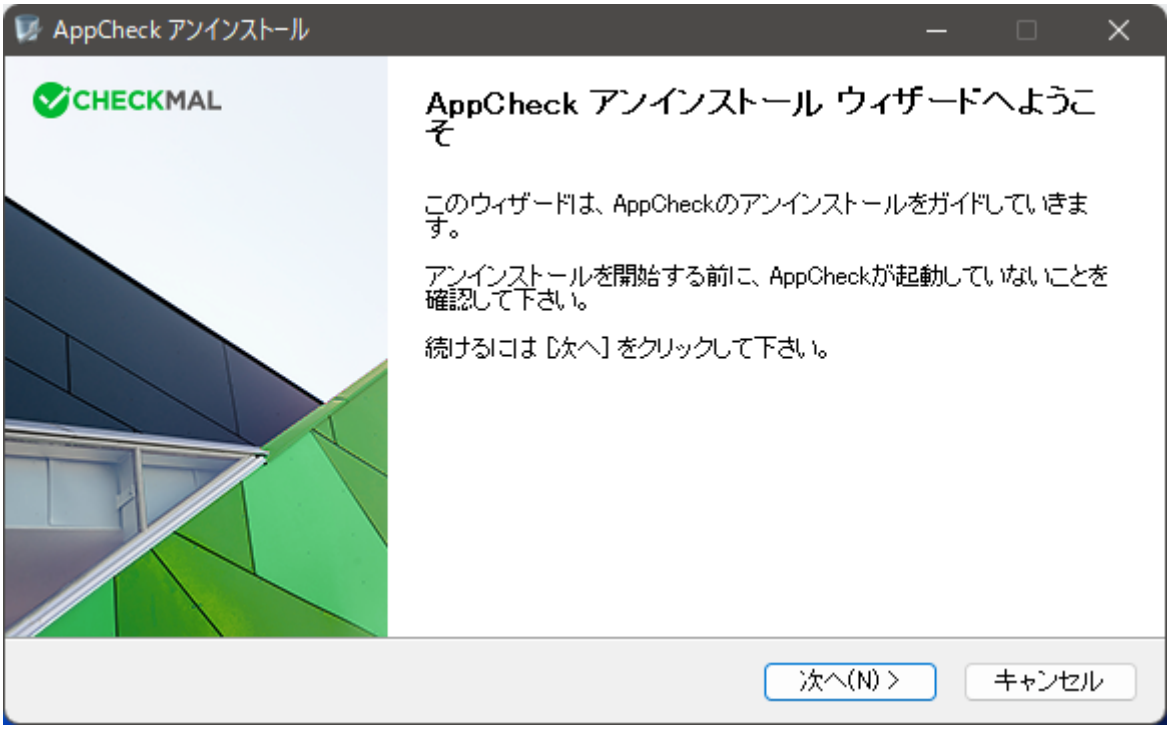

AppCheck セットアップ
CHECKMAL
AppCheck セットアップ ウィザードは完了しました。
AppCheckは、このコンピュータにインストールされました。
ウィザードを閉じるには [完了] を押してください。
AppCheckアンチランサムウエアを実行する
< 戻る(B)
完了(F)
キャンセル

2. アンインストール

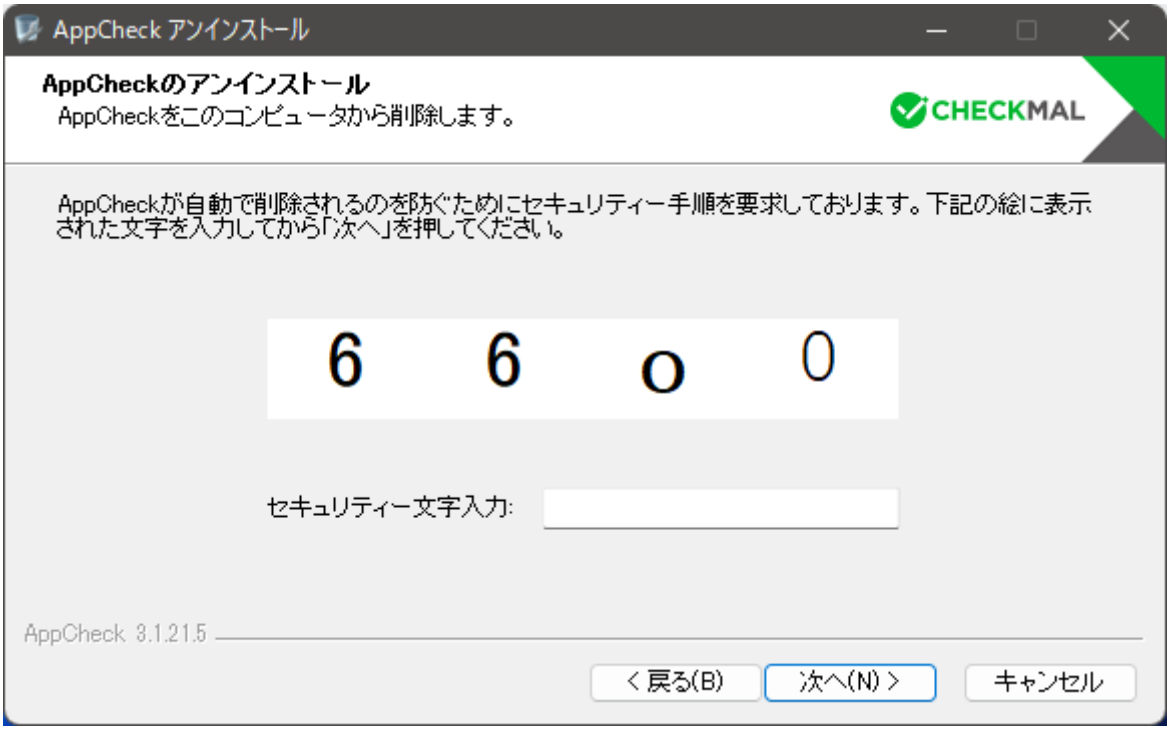
(1) AppCheckのアンインストールは、「設定」→「アプリと機能」のプログラムリストに登録されている"AppCheckアンチランサムウェア"を選択し アンインストールを実行します。



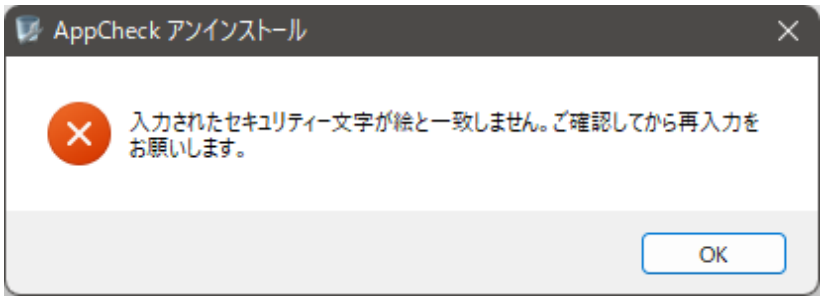
(2) 「次へ」をクリックします。



(3)「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。



※ もし、間違ったセキュリティ文字を入力した場合は、「入力されたセキュリティ文字が絵と一致しません。 ご確認してから再入力をお願いします。」というメッセージが表示されますので、セキュリティ文字を再度確認してください。

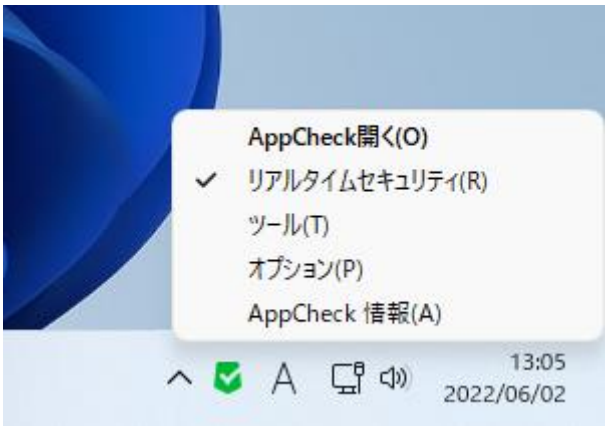


(4) システムからAppCheckを削除するためには、「アンインストール」ボタンをクリックし、アンインストール対象は「C:¥ProgramFiles¥CheckMAL¥AppCheck」フォルダ及びその他の関連ファイルでございます。

(5) 「完了」ボタンをクリックすると、AppCheckのアンインストールが終了し、システム環境によっては再起動を要求することもございます。

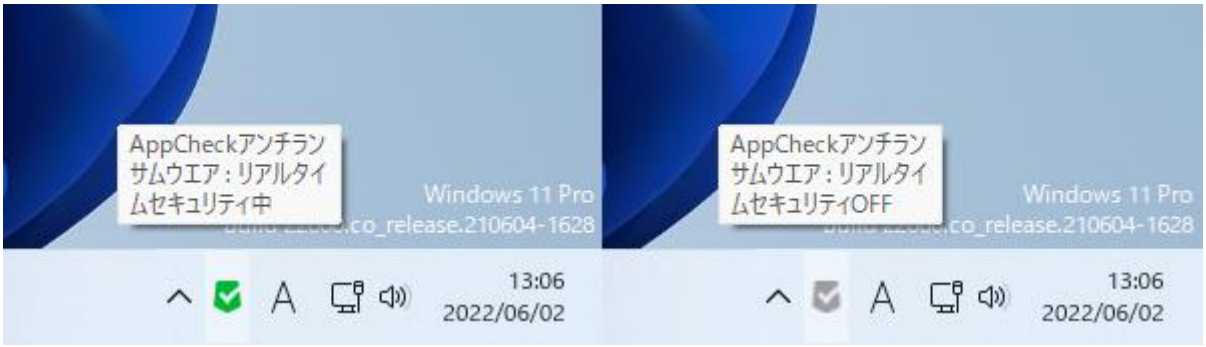
3. AppCheckのアイコンメニュ

タスクバー通知領域に表示される AppCheck アイコンメニューは、ロック機能または CMS 中央管理ポリシーによるロックモード適用時には、「リアルタイムセキュリティ」と「オプションメニュー」が非活性化されます。



⊙ **AppCheck 開く ：**AppCheck のダッシュボード画面表示

⊙ **リアルタイムセキュリティ ：** ランサムウェア行為リアルタイム遮断及び行為ロールバック機能の活性化・非活性化

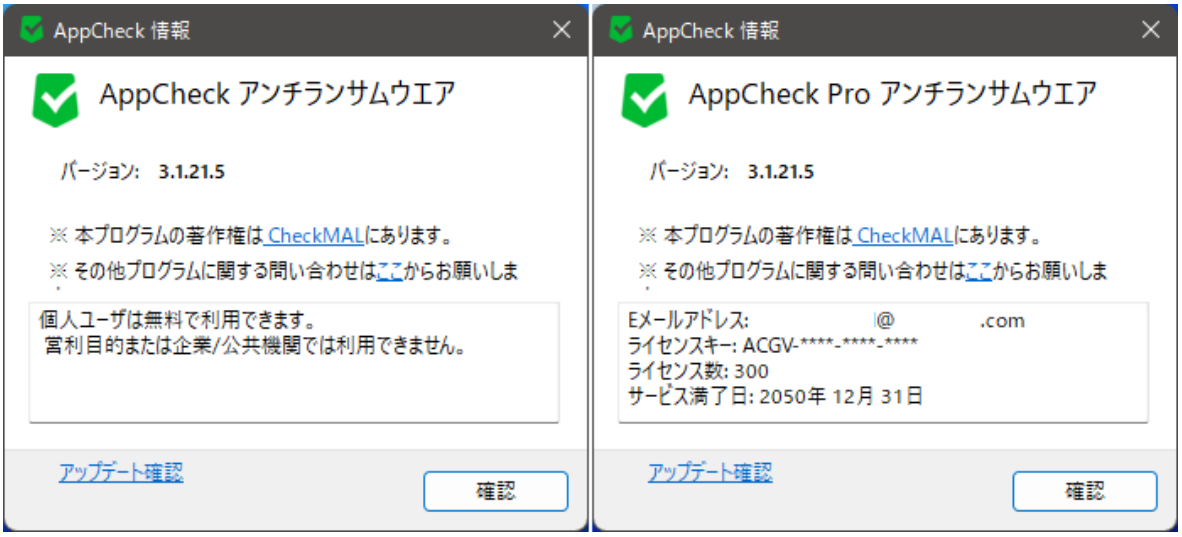


- **緑色のアイコン ：** リアルタイムセキュリティ機能が「ON」の状態
- **グレー色のアイコン ：** リアルタイムセキュリティ機能が「OFF」の状態

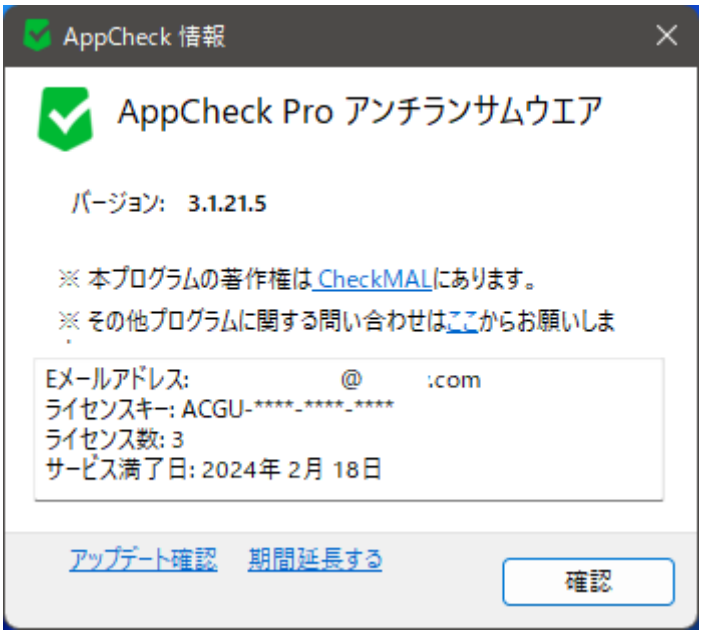
⊙ **ツール ：** 一般ログ、脅威ログ、検疫の画面表示

⊙ **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、自動バックアップ、例外設定、SMB 許容/遮断リスト設定

⊙ **AppCheck 情報 ：** AppCheck バージョン、著作権及びライセンス案内、正規品登録情報、手動アップデート確認表示

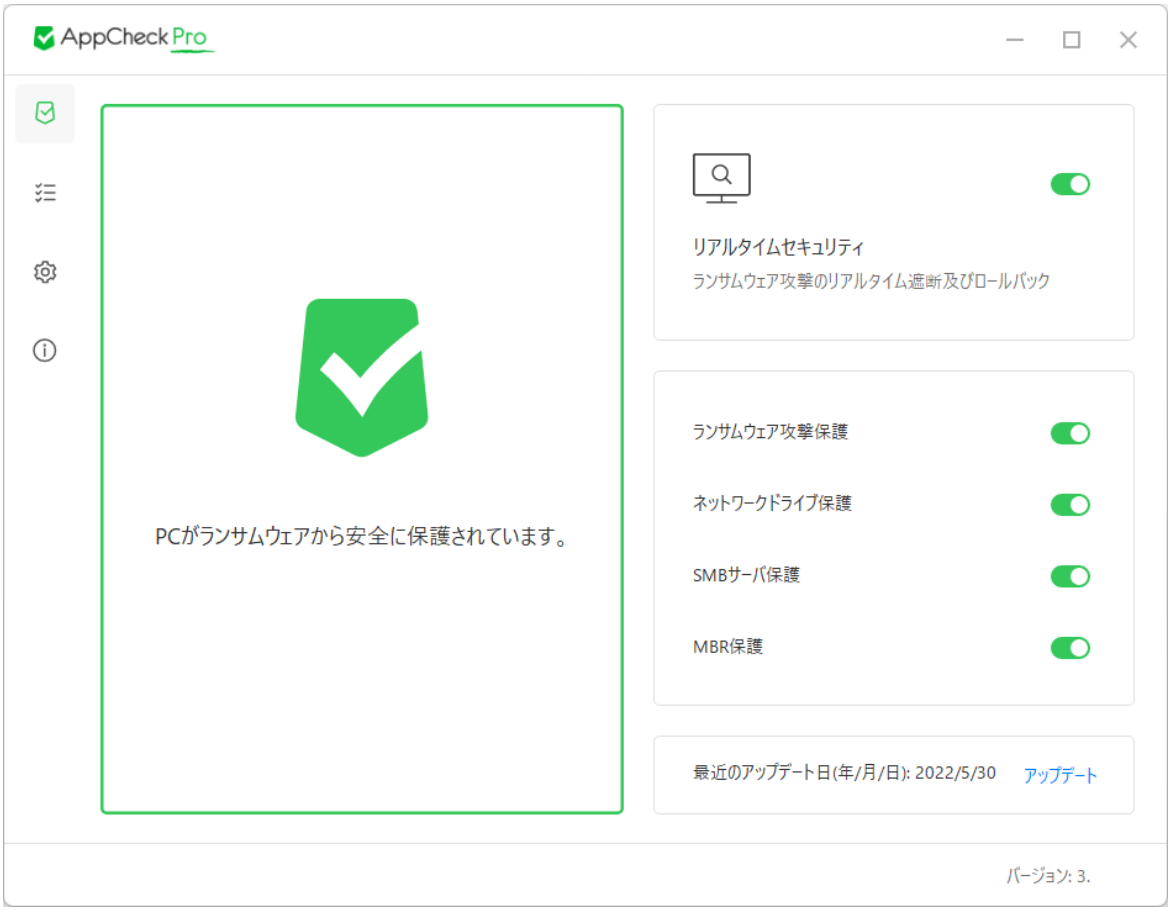


もし AppCheckPro ライセンスが 31 日以内に満了する場合、AppCheck 情報欄に「期間延長」メニューが自動に表示され、クリックすると checkmal のライセンス更新ページに自動接続され、ライセンス更新後には、既存のライセンス情報をそのまま利用できます。



ただし、「期間延長」メニューは更新型ライセンスの場合にのみ表示され、CMS 中央管理によって配布された AppCheck は表示されません。

4. ダッシュボード

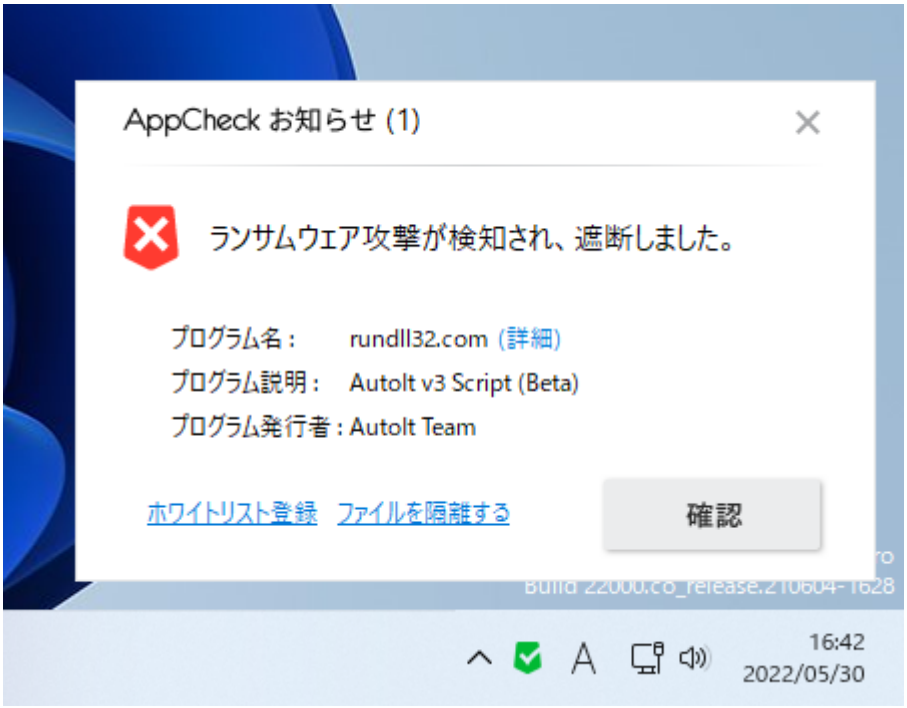


⊙ **リアルタイムセキュリティ ：** ランサムウェア攻撃保護、ネットワークドライブ保護、SMBサーバー保護、MBR保護、脆弱性ガード、退避フォルダ使用、自動バックアップ<AutoBackup(AppCheck)>フォルダ保護機能の活性化・非発生化ができます。

- **リアルタイムセキュリティ「ON」：** 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「OFF」：** ランサムウェアの脅威にさらされています。

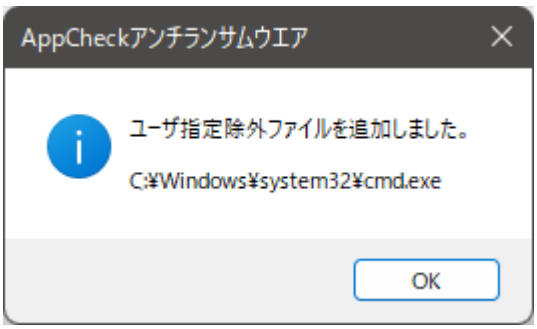
⊙ **ランサムウェア攻撃保護：**保護する拡張子のファイルが検知条件により変更される場合は、「ランサムウェア動作検知」による遮断/除去及び自動復元の活性化・非発生化ができます。

ランサムウェア攻撃保護を活性化すると、ネットワークドライブ保護とSMBサーバー保護も同時に活性化されます。



- **プログラム名 ：** ファイル毀損行為により遮断されたファイル名
- **プログラム名（詳細）：**「ツール」－「脅威ログ」画面に移動
- **プログラム説明 ：**「ランサムウェア動作探知」されたファイルのプロパティ内容
- **プログラム発行者 ：**「ランサムウェア動作探知」されたファイルのデジタル署名
- **ホワイトリスト登録 ：**「ランサムウェア動作探知」されたファイルの中、正常なプログラム行為を誤検知した場合、「ユーザ指定除外ファイル登録」を行うことができます。 除外ファイルとして登録されたファイルは、「オプション」-「例外設定」-「ユーザ指定除外ファイルリスト」に自動追加されます。 ただし、ロック設定利用またはCMS中央管理ポリシーの「ロックモード」利用環境では、該当ボタンが表示されません。

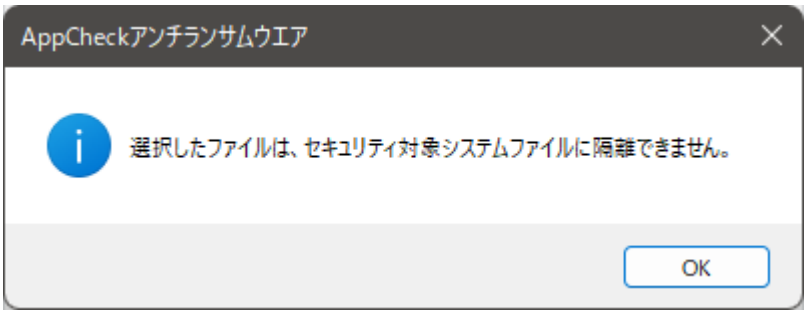
※CMS連動バージョンの場合、上記機能で登録を行ったホワイトリスト設定がCMSのポリシー自動適用により解除されますので、CMSポリシー変更により設定を反映するようお願いします。



-

ユーザーが「ランサムウェア動作検知」ウィンドウで「ホワイトリスト登録」機能として登録を行った場合、「ユーザ指定除外ファイルとして追加しました」という 通知メッセージが表示されます。

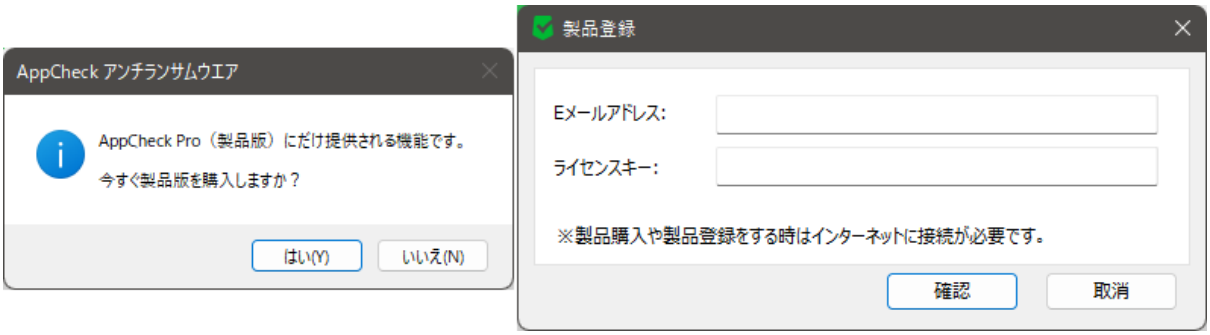
- **ファイルを隔離する ：** ランサムウェアとして検知されましたが、権限などの理由によってい自動削除できなかった場合は、検疫所フォルダに格納することができます。



ランサムウェアとして検知されたファイルの中、システムファイルであるため自動削除されなかったファイルを以下画面の「ファイルを隔離する」ボタンで削除を行うと、「選択したファイルは保護対象システムファイルのため、隔離できません」という通知メッセージが表示されます。

⊙ **ネットワークドライブ保護 ：** ネットワークドライブを通じて接続された共有フォルダ内のファイルが毀損された場合、「ランサムウェア動作検知」による遮断/除去および自動復元の活性化ができます。

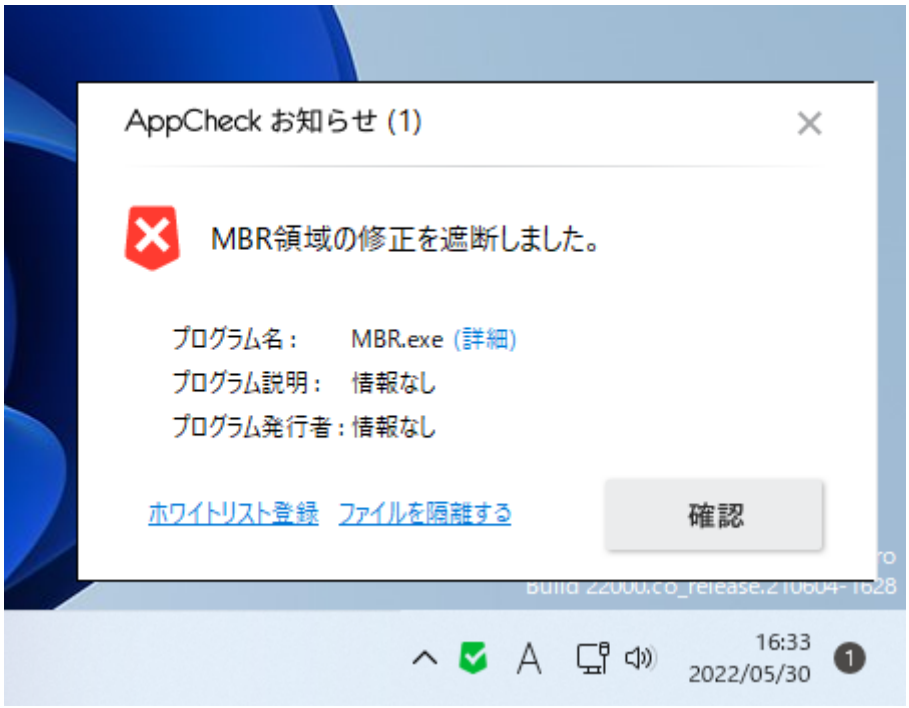
AppCheck無料バージョンで保護機能を活性化すると、「AppCheckProバージョンで提供される機能です。 今すぐ製品版を購入しますか?」という通知メッセージが表示されます。



「はい(Y)」をクリックすると、購入済みのAppCheckライセンス情報（Eメールアドレス、ライセンスキー)を入力するとAppCheckPro（有料版）に変更されます。この際にはインターネット接続が必要となります。

⊙ **SMBサーバー保護 ：** 遠隔地PCで実行されたランサムウェアがネットワークドライブとして繋がっている共有フォルダ内のファイルを毀損した場合、遠隔地IPからの接続遮断及び既存されたファイルの自動復元を行います。

⊙ **MBR保護 ：** MasterBootRecord(MBR)領域内のファイルを変更しようとするファイルに対し、遮断を行います。

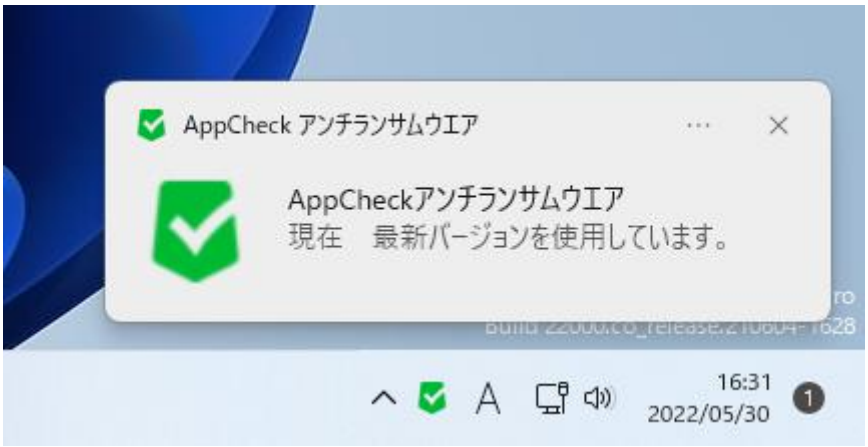


- **プログラム名 ：** MBR領域の毀損で検知、遮断されたファイル名
- **プログラム名（詳細）：**「ツール」－「脅威ログ」画面に移動
- **プログラム説明 ：** MBR領域の毀損で検知、遮断されたファイルのプロパティ内容

- **プログラム発行者 ：** MBR領域の毀損で検知、遮断されたファイルのデジタル署名
- **ホワイトリスト登録 ：** MBR保護機能で遮断されたファイルの中、正常なプログラムを誤検知した場合、「ホワイトリスト」として登録できます。ただし、ロック設定利用またはCMS中央管理ポリシーの「ロックモード」利用環境では、該当ボタンが表示されません。

  ※CMS連動バージョンの場合、上記機能で登録を行ったホワイトリスト設定がCMSのポリシー自動適用により解除されますので、CMSポリシー変更により設定を反映するようお願いします。
- **ファイルを隔離する ：** MBR保護機能で遮断されたファイルが悪性ファイルの場合、「ファイル隔離」機能により検疫所フォルダに格納することができます。

⊙ **最新アップデート日 ：** AppCheck自動(手動)アップデート機能により、最後バージョンアップデートが行われた日付



アップデートメニューをクリックすると、「現在、最新バージョンを使用しています」という 通知メッセージが表示されます。

5. ツール

[5-1] 一般ログ

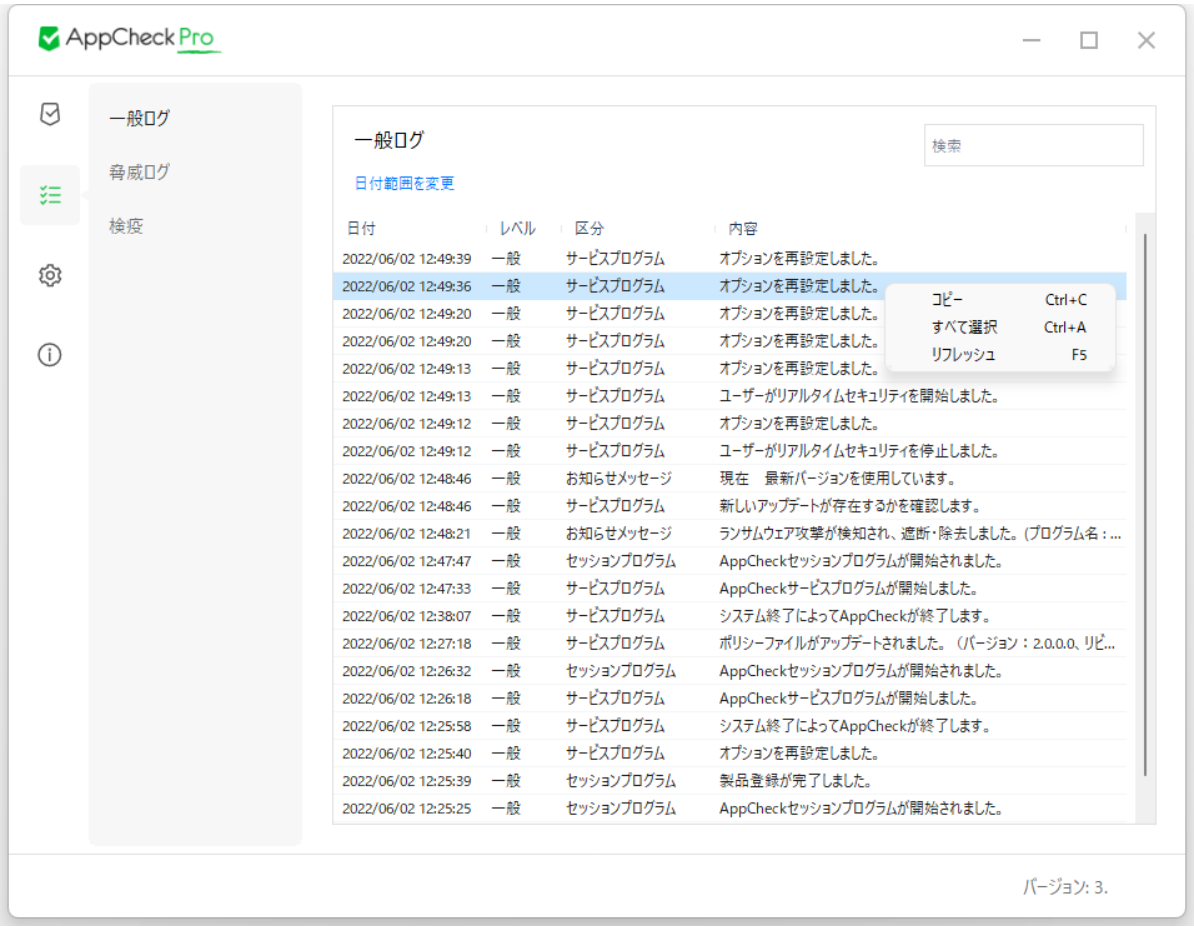
一般ログには過去30日間、AppCheckの動作中に発生するセッションプログラム、サービスプログラム、自動バックアップ、通知メッセージなど多様な情報が表示されます。

一般ログのカラム(Columns)は日付、レベル、区分、内容に分けられ、各項目ごとに降順/上げ順に整列することもできます。

一般ログの「日付範囲を変更」メニューにより、特定期間内に記録された一般ログをフィルタリングして確認することができます。

- **指定なし ：** すべての期間における一般ログの確認
- **今日 ：** 今日の日付基準で記録された一般ログの確認
- **過去7日間 ：** 直近7日基準で記録された一般ログの確認
- **過去30日間 ：** 直近30日基準で記録された一般ログ確認
- **ユーザー設定の範囲 ：** 特定期間（年-月-日指定）の間に記録された一般ログの確認

一般ログに記録された特定項目を選択し、右クリックメニューでコピー、すべて選択、更新することができます。



⊙ **コピー（Ctrl+C）：** 選択した項目の一般ログ詳細情報をコピーします。

⊙ **全て選択（Ctrl+A）：** 一般ログに記録されたすべての項目を一括選択します。

⊙ **リフレッシュ（F5）：** 一般ログに記録された情報を更新します。

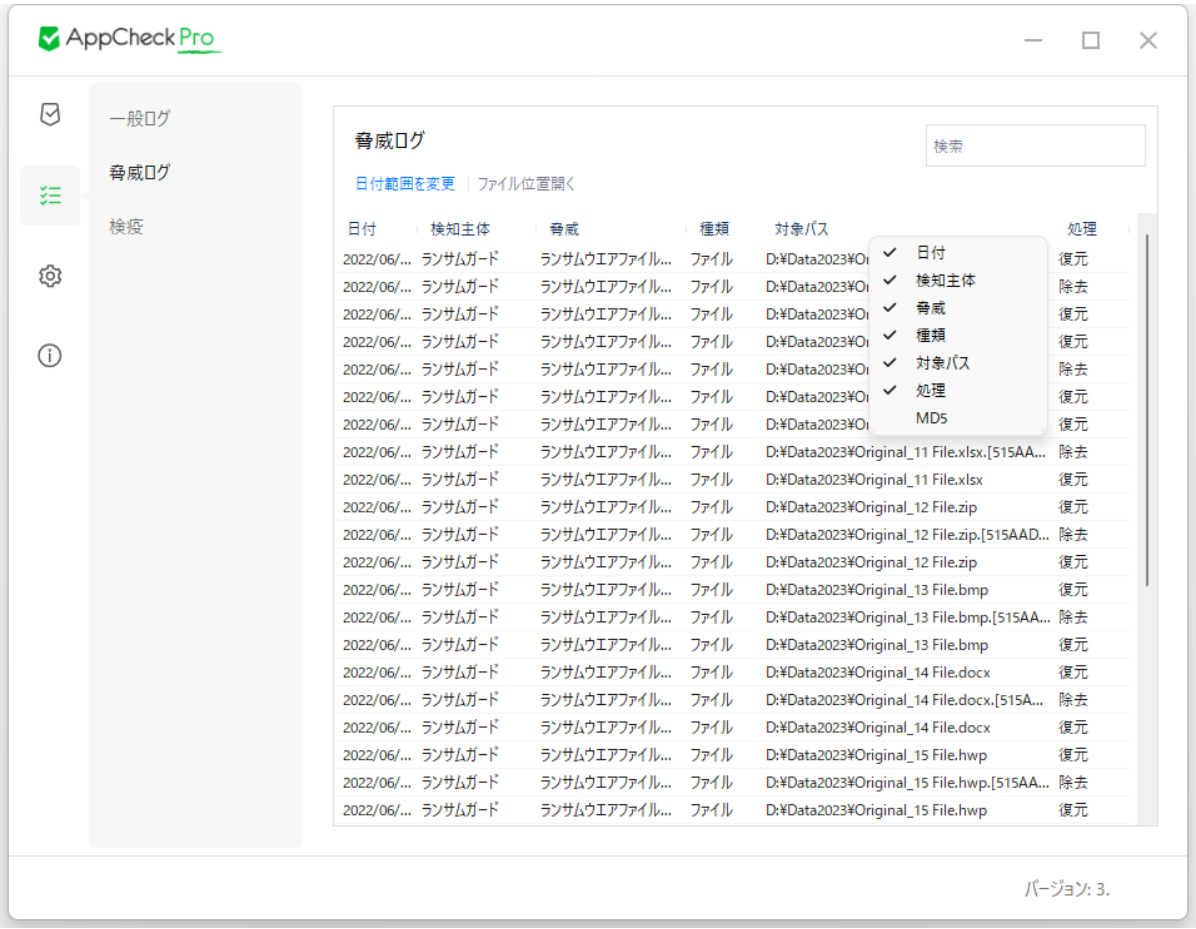
[5-2] 脅威ログ

脅威ログには過去30日間、ランサムガード、脆弱性ガード、MBR保護機能により処理された内容(遮断、除去、復元、除去失敗)情報を表示されます。

脅威ログの「日付範囲を変更」メニューにより、特定期間内に記録された脅威ログをフィルタリングして確認することができます。

- **指定なし ：** すべての期間における脅威ログの確認
- **今日 ：** 今日の日付基準で記録された脅威ログの確認
- **過去7日間 ：** 直近7日基準で記録された脅威ログの確認
- **過去30日間 ：** 直近30日基準で記録された脅威ログの確認
- **ユーザー設定の範囲 ：** 特定期間（年-月-日指定）の間に記録された脅威ログの確認

脅威ログのカラム(Columns)は、日付、検知主体、脅威、種類、対象経路、処理、MD5(デフォルト:無効化)に区分され、各項目ごとの降順/昇順に整列できます。

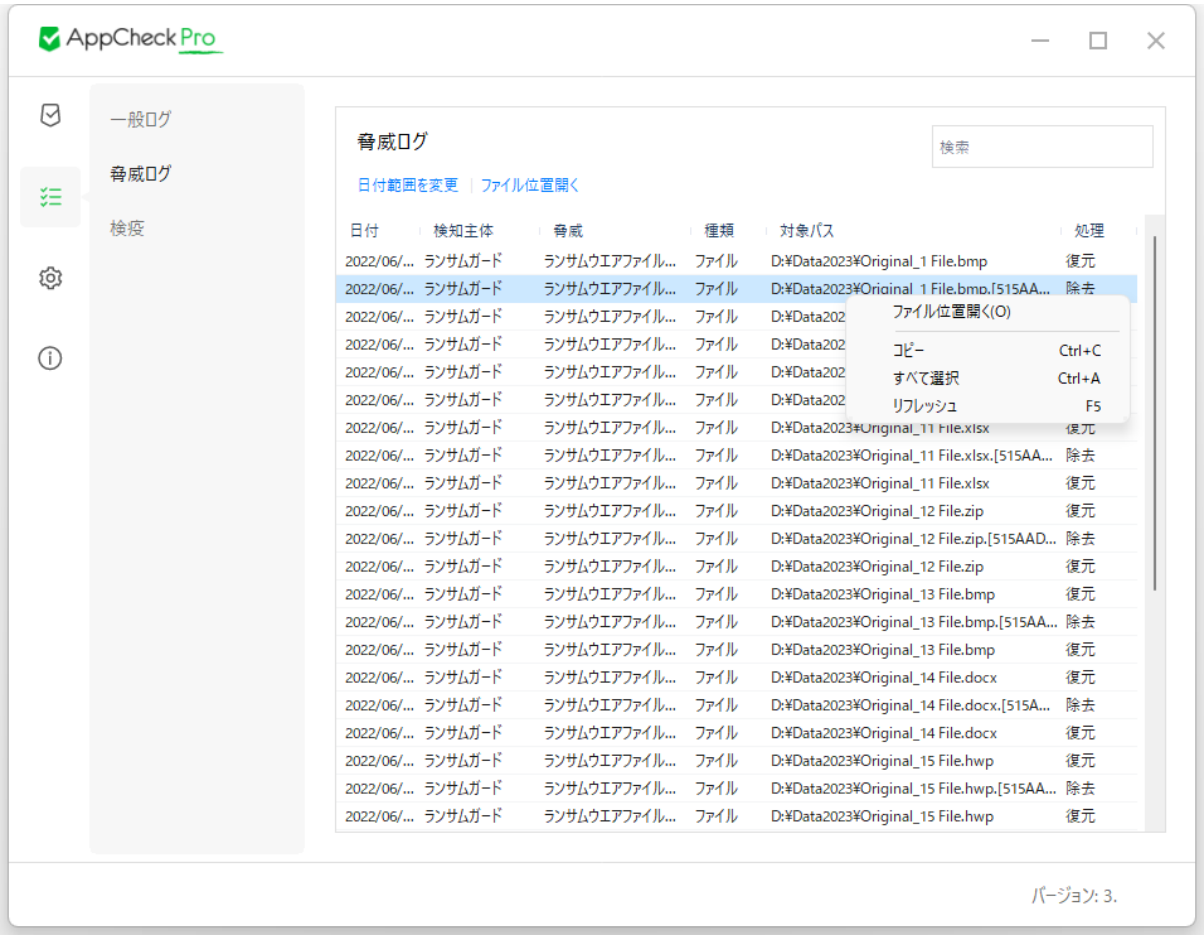


⊙ **遮断 ：** ランサムウェア動作検知、MBR保護で検知されたプロセス(ファイル)とIPアドレス、脆弱点ガードで検知された応用プログラムを遮断します。

⊙ **消去 ：** ランサムウェア動作検知で除去されたファイル、ランサムウェアによって暗号化されたファイルと生成されたファイルを自動削除します。

⊙ **復元 ：** 退避フォルダに臨時バックアップされたファイルを利用し、元の位置に復元します。

⊙ **削除失敗 ：** ランサムウェア動作検知が発生した時点を基準に、除去すべきファイルがすでに削除されてるか、ある問題でファイルを除去できなかった場合に記録される。脅威ログに記録された特定項目を選択し、右クリックメニューでファイルの位置を開く、コピー、すべて選択、更新することができます。



⊙ **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（Ctrl+C）：** 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（Ctrl+A）：** 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（F5）：** 脅威ログ情報を更新します。

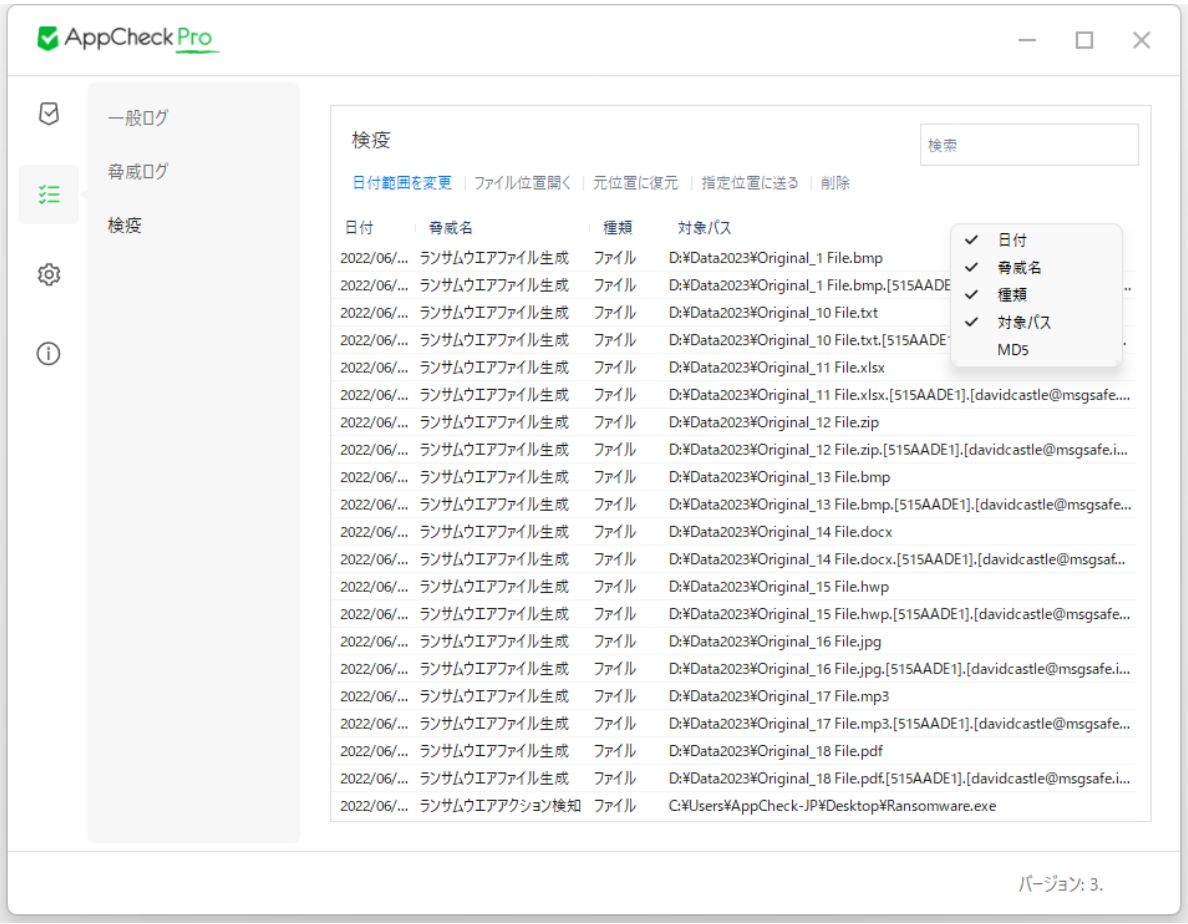
[5-3] 検疫

検疫所は過去30日間、ランサムウェア動作検知により除去され、検疫所フォルダ(C:¥ProgramData¥CheckMAL¥AppCheck¥Quarantine)にバックアップされたファイル情報を提供し、必要に応じてユーザーが検疫所にバックアップされた項目を復元することができます。

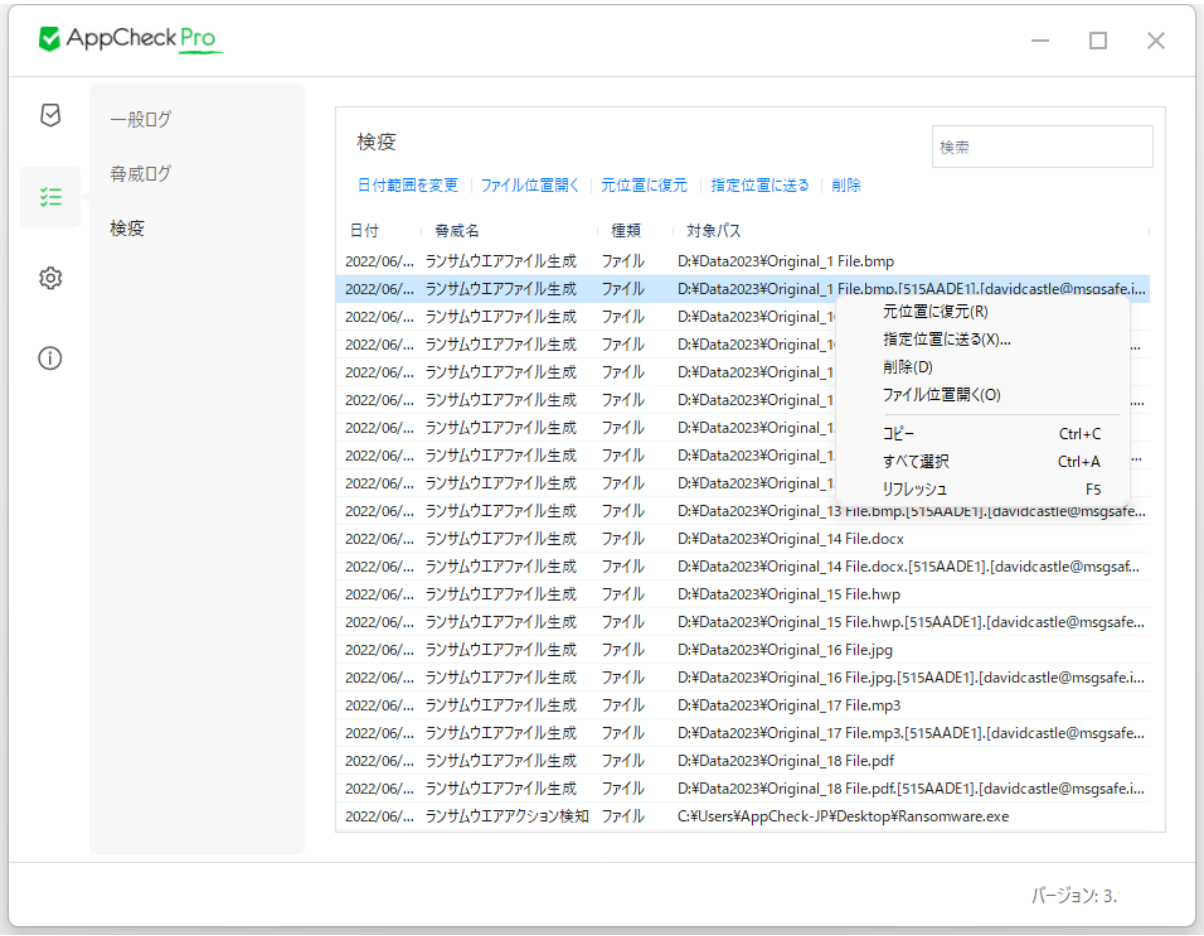
検疫所の「日付範囲を変更」メニューにより、特定期間内に記録された検疫ログをフィルタリングして確認することができます。

- **指定なし ：** あらゆる期間の検疫ログの確認
- **今日 ：** 今日の日付基準で記録された検疫ログの確認
- **過去7日間 ：** 直近7日基準で記録された検疫ログの確認
- **過去30日間 ：** 直近30日基準で記録された検疫ログの確認
- **ユーザー設定の範囲 ：** 特定期間（年-月-日指定）の間に記録された検疫ログの確認

検疫所のカラム(Columns)は日付、脅威名、種類、対象経路、MD5(デフォルト:無効化)に区分され、各項目別の降順/上げ順に整列できます。



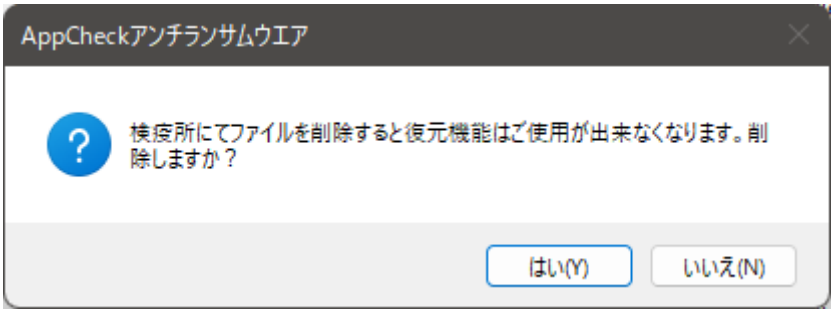
検疫所に記録された特定項目を選択し、右クリックメニューを通じてファイル位置を開く、コピー、すべて選択、更新することができます。



⊙ **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 ：** 検疫所フォルダにバックアップされているファイルを削除します。



検疫所のファイルを削除する際、「検疫所でファイルを削除すると復元機能はご使用出来なくなす。削除しますか?」というメッセージが表示されます。また、削除されたファイルはゴミ箱に移動せずに完全削除されます。

⊙ **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。

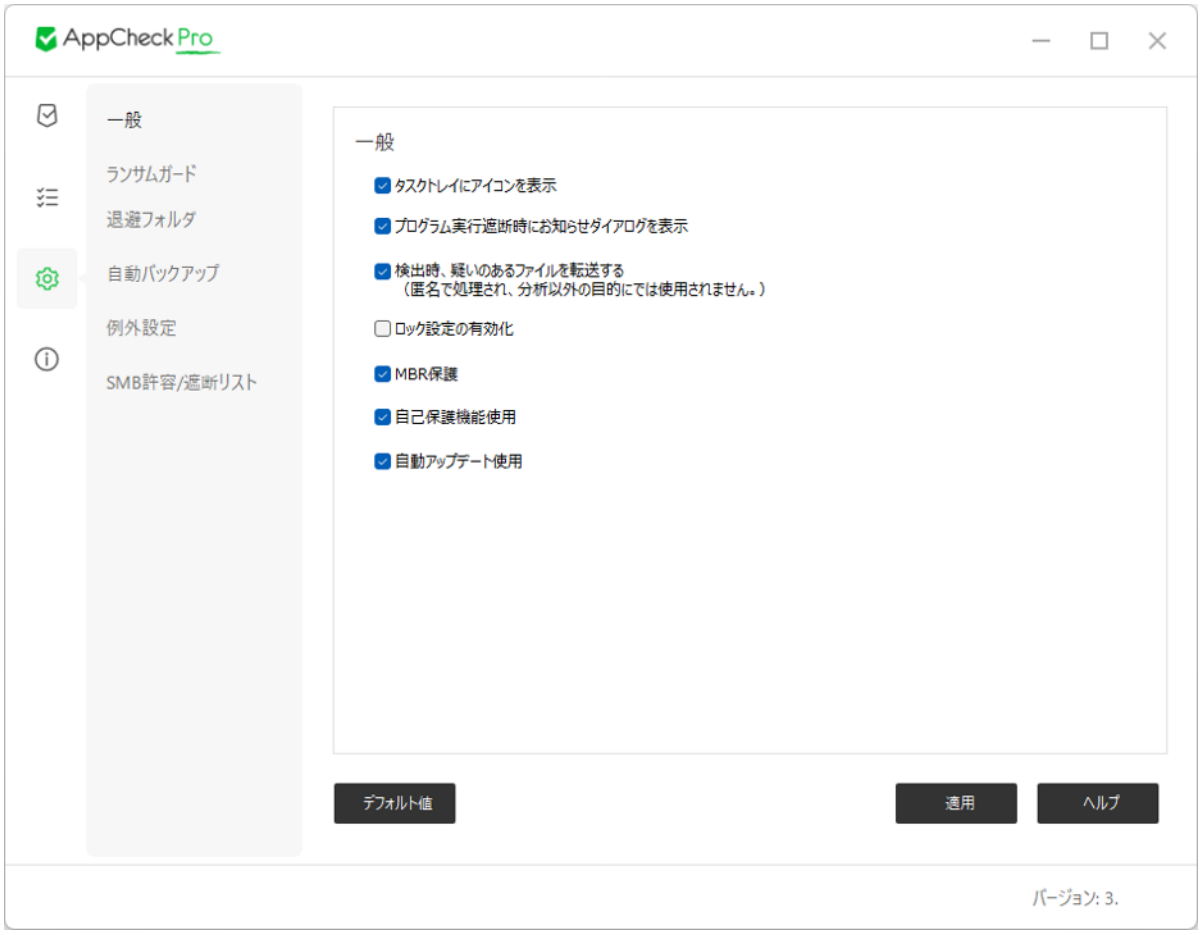
⊙ **コピー（Ctrl+C）：** 選択した項目の検疫ログの詳細情報をコピーします。

⊙ **全て選択（Ctrl+A）：** 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（F5）：** 検疫情報を更新します。

6. オプション

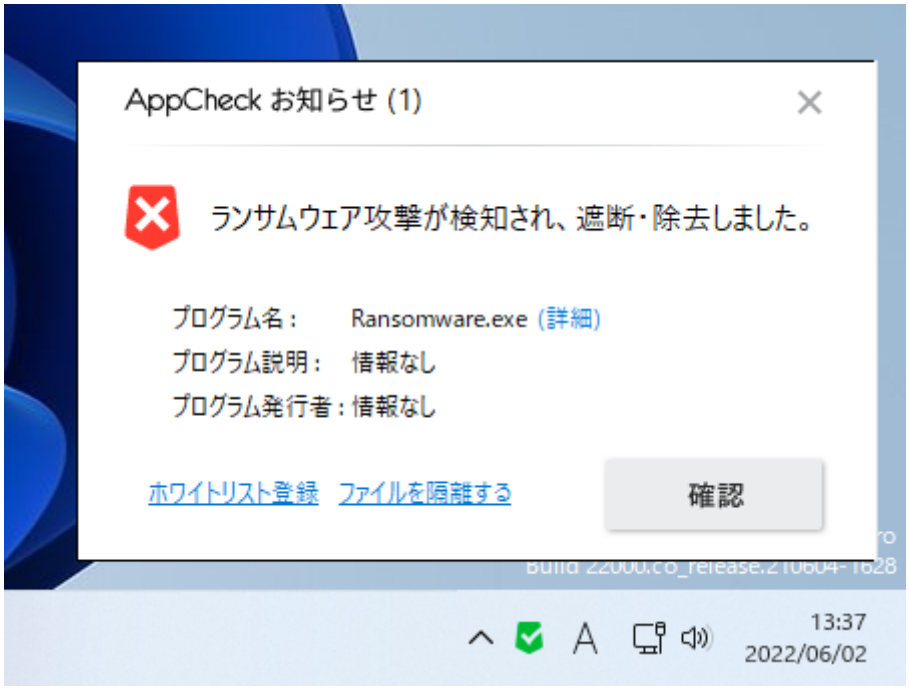
[6-1] 一般



⊙ **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。

「タスクトレイにアイコンを表示」にチェックが入っている場合は、AppCheckのアイコン（AppCheck.exe)が終了されたら最大2分以内に自動で再実行されます。

⊙ **プログラム実行遮断時にお知らせダイアログを表示 ：** ランサムウェア行為探知、MBR保護、脆弱性ガード保護機能による探知時の通知ウィンドウ表示



⊙ **検知時、疑いのあるファイルを送信する(匿名で処理され、分析以外の目的にでは使用されません) :** AppCheckの利用中、ランサムガード、脆弱性ガード、MBR保護機能で検知されたファイルを匿名でcheckmalサーバーに送信

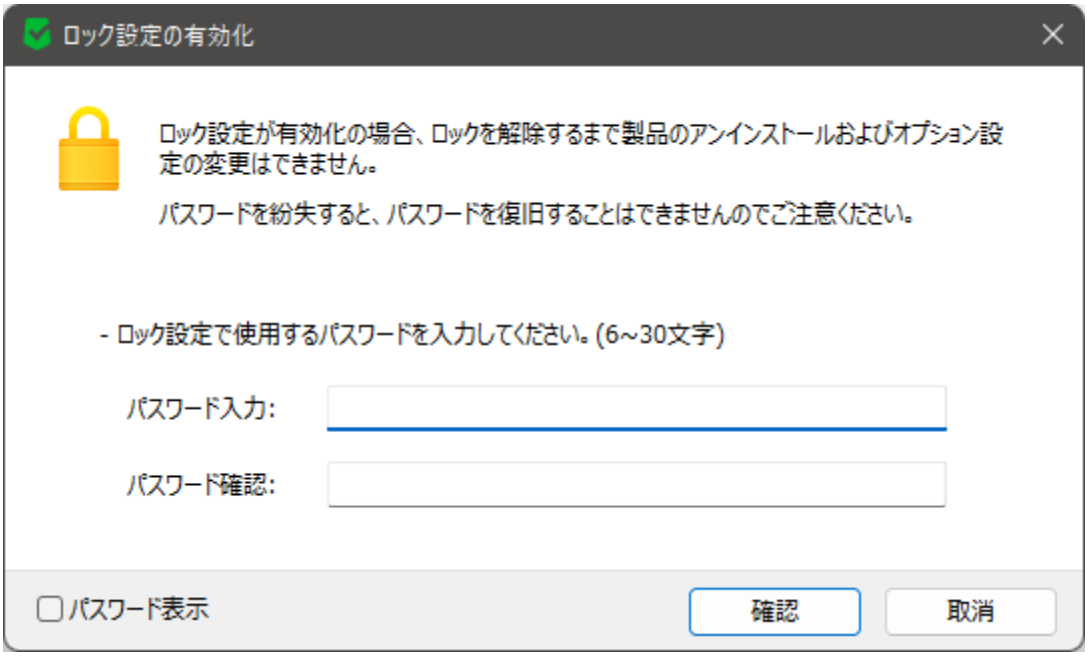
⊙ **MBR保護 :** MasterBootRecord(MBR)領域内のファイルを毀損しようとするファイルの実行遮断(検知されたファイルは遮断のみ行い、再度実行されたら削除する

⊙ **自己保護機能使用 :** AppCheck関連フォルダ(自動バックアップフォルダ<AutoBackup(AppCheck)>含む)及びファイル、レジストリ、一部セキュリティ製品の無力化ツールからAppCheckを保護

⊙ **ロック設定の有効化 :** ユーザーが入力したパスワードを通じてAppCheckのオプション、リアルタイムセキュリティ、AppCheckアンインストール機能変更遮断（AppCheckPro専用機能)

ただし、CMS中央管理で配布されたAppCheckProバージョンはロックモード機能として提供しているため、オプション内に「ロック設定の有効化」メニューは表示されません。

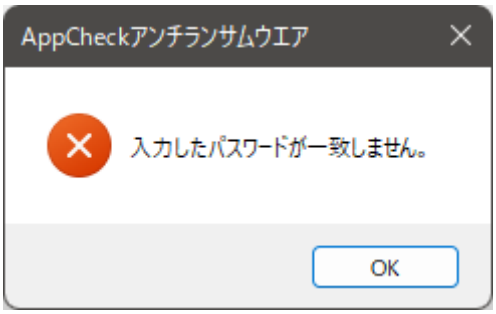
ロック設定の際には「6~30桁の暗証番号」の設定が必要であり、パスワードを紛失した場合は復旧できません。



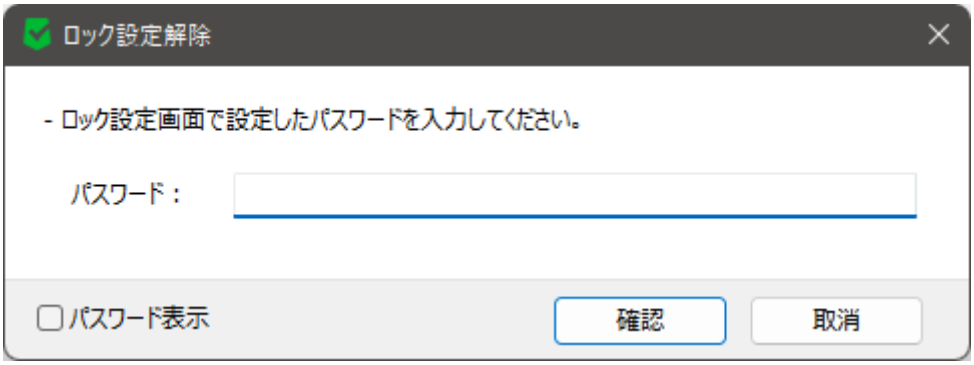
入力したパスワードを確認するためには、「パスワード表示」ボックスにチェックし、「確認」を押してください。

ロック設定に使用するパスワードを入力時、6~30文字の長さで指定しない場合、「パスワードの長さが正しくありません。（6~30文字以内で入力してください）」という通知メッセージが表示されます。

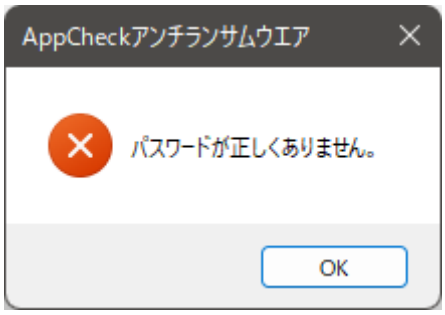
ロック設定に使用するパスワードを入力した後、パスワード確認欄に再入力したパスワードが異なる場合、「入力したパスワードが一致しません。」という通知メッセージが生成される。



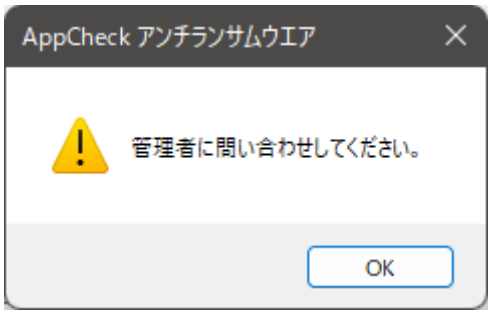
ロック設定が適用された環境でAppCheckオプションメニュー接続時にロック設定解除のためのパスワード入力ウィンドウが生成される。



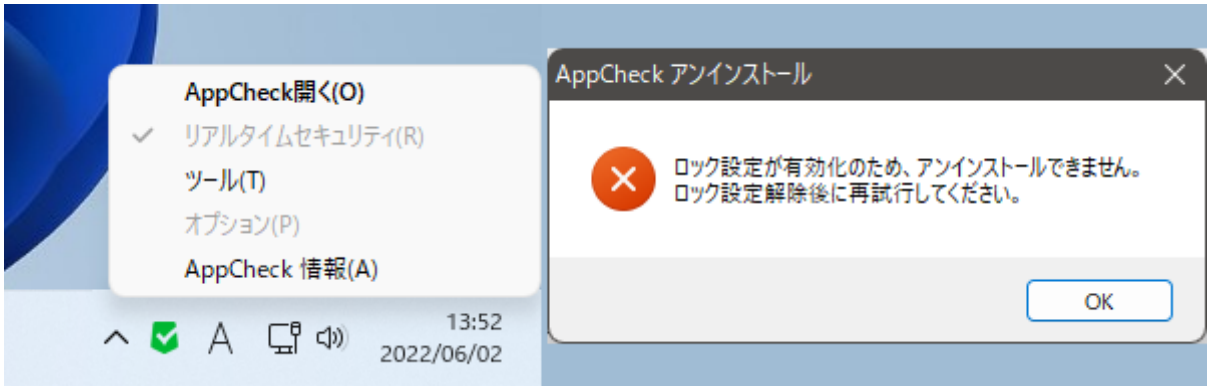
入力したパスワードが間違っていた場合、「パスワードが正しくありません。」という 通知メッセージが生成される。



CMS中央管理ポリシーによるロックモードが適用されている場合は、AppCheckオプションに接続する際、「管理者にお問い合わせください。」という通知メッセージが表示されます。



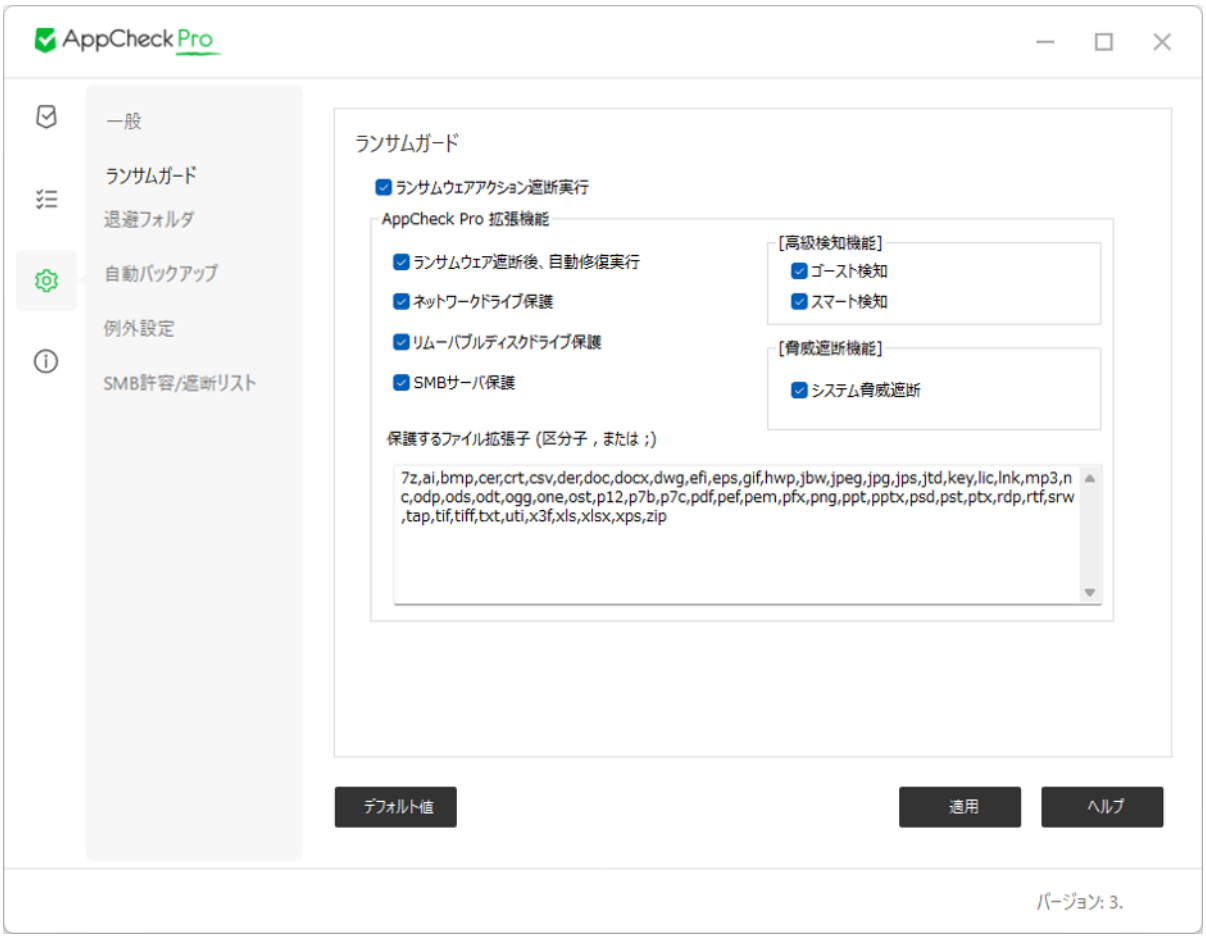
ロック設定の使用またはCMS中央管理ポリシーによるロックモードが適用されたAppCheckは、リアルタイムセキュリティのOFFと、AppCheckProのアンインストールができません。（※CMS中央管理ポリシーで、「アプリケーション削除許可」設定により、AppCheck削除許可設定可能）



- **アンインストール不可メッセージ ：** ロック設定が有効化のため、アンインストールできません。 ロック設定解除後再試行してください。

⊙ **自動アップデート使用 ：** 3時間周期でAppCheckのアップデート有無を確認し、自動アップデートを行います。

[6-2] ランサムガード



⊙ **ランサムウェアアクション遮断実行**： 保護するファイル拡張名に含まれるファイルが検知条件によって変更された場合、"ランサムウェア行為検知"による遮断

⊙ **AppCheck Pro拡張機能 ： ランサムウェア遮断後、自動復元実行**

ランサムウェア行為検知を通じて遮断された悪性ファイル自動治療(削除)する。 ただし、遮断されたファイルのうち有効なデジタル署名を持つファイルまたはシステムフォルダに位置するファイルは削除しない。

⊙ **AppCheck Pro拡張機能 ： ネットワークドライブ保護**

AppCheckが設置されたPCで実行されたランサムウェアがネットワークドライブで連結された他の装置に位置した共有フォルダ内のファイル毀損時に"ランサムウェア行為検知"で遮断および自動復元する。

⊙ **AppCheck Pro拡張機能 ： リムーバブルディスクドライブ保護**

AppCheckが設置されたPCで実行されたランサムウェアがUSBポートに連結されたリムーバブルディスク内ファイルを毀損した場合、"ランサムウェア行為検知"で遮断および自動復元する。

⊙ **AppCheck Pro拡張機能 ： SMBサーバー保護**

AppCheckが設置されていない遠隔地PCで実行されたランサムウェアがネットワークドライブで連結された共有フォルダ(AppCheck設置PC)内のファイルを毀損した場合、遠隔地IP遮断(1時間)および自動復元する。

⊙ **AppCheck Pro 拡張機能 ： 高級検知機能 - ゴースト検知**

該当PC内のメモリ内にゴーストファイルをおき、ランサムウェアが実際のデータファイルを毀損する前にゴーストファイルに触れさせることにより、いち早くランサムウェアを検知できるようにする機能。

⊙ **AppCheck Pro 拡張機能 ： 高級探知機能 - スマート探知**

ランサムウェアプロセスが実行され、少数のファイルだけを暗号化した後に終了し、再実行された同一プロセスがファイル暗号化をする反復ファイル毀損行為に対する検知方式。

⊙ **AppCheck Pro 拡張機能 ： 脅威遮断機能 - システム脅威遮断**

Windosに付属されるロールバック（復元機能）を無力化する動きから守る機能。

⊙ **AppCheck Pro 拡張機能 ： 保護するファイル拡張名(区分字、または;)**

ファイル毀損行為から保護される基本ファイル拡張名は、総65種となる。

(7z,ai,bmp,cer,cfg,chm,crt,csv,dcm,der,doc,docx,dotm,dotx,dwg,efi,eps,gif,hwp,hwpx,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,rar,rdp,rtf,srw,tap,tif,tiff,txt,uti,x3f,xls,xlsb,xlsm,xlsx,xps,zip)

エージェントの「保護する拡張子（区分子、または ; ）」で変更をした場合は、今後のアップデートで保護する拡張子が追加されたとしても追加されず、既存の設定内容が維持されます。

なお、「保護する拡張子（区分子、または ; ）」設定画面内の「デフォルト値」を押下すると、当該押下時点での最新拡張子が適用されます。

この場合、ユーザーが設定した変更内容(直接追加した拡張子など)に当該押下時点での最新拡張子が上書きされます。

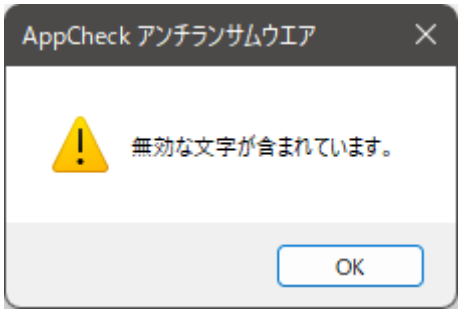
※注意事項

ADサーバーに導入される場合は、以下5種の拡張子を追加登録するようお願いします。

・ edb, htm, html, log, xml

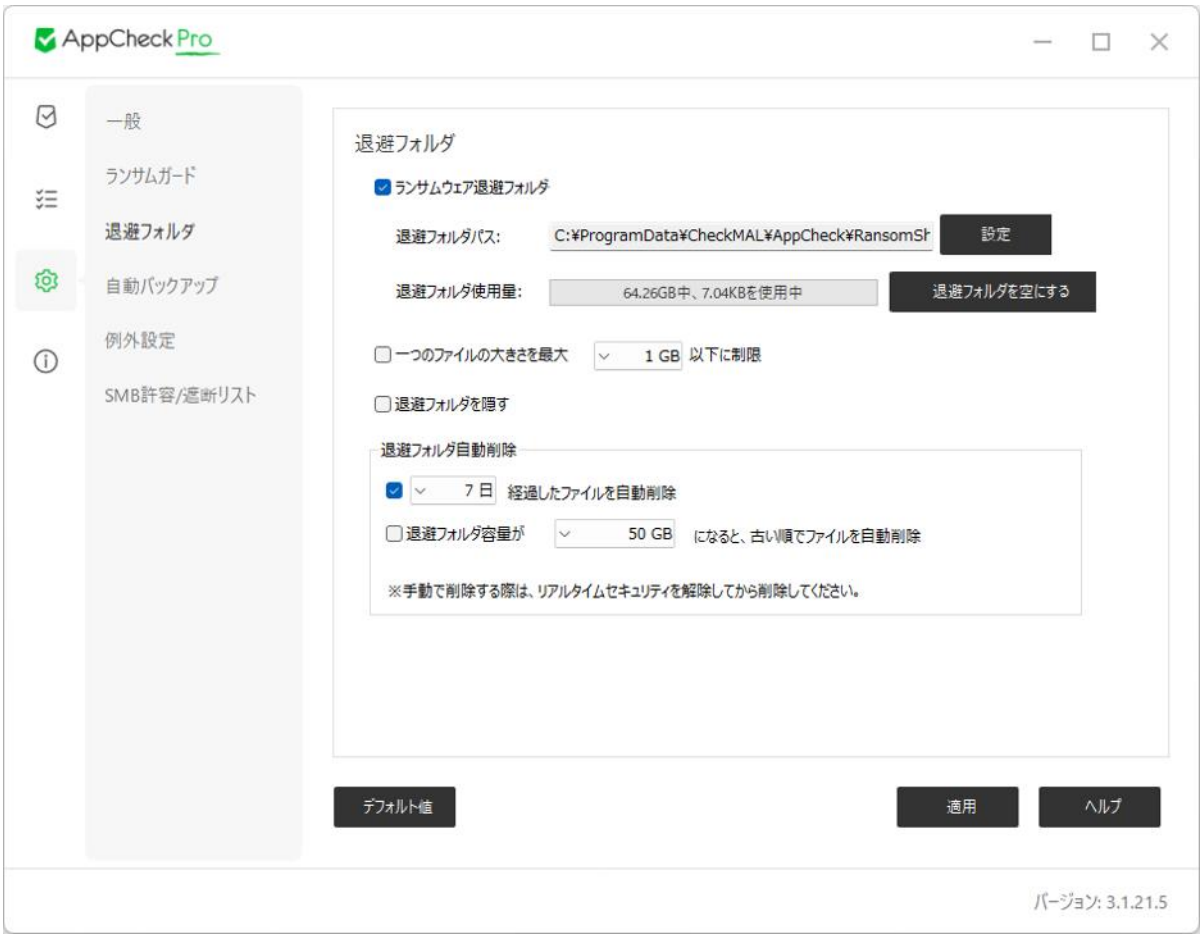
ただし、お客様の環境情報を考慮し、上記以外にも保護する必要があるファイルに関しては、該当ファイルの拡張子を追加するようお願いします。また、本運用で発生する誤検知などを事前把握するため、一定期間（約1～2週間など）はログモードでのテスト運用として誤検知の有無をご確認いただき、必要であれば信頼プロセス（ホワイトリスト登録）の設定後、通常モードに切り替えてください。

保護するファイル拡張名に追加した文字の中に許可されていない文字が含まれている場合、「使用できない文字が含まれています。」という通知メッセージを生成し、適用されません。



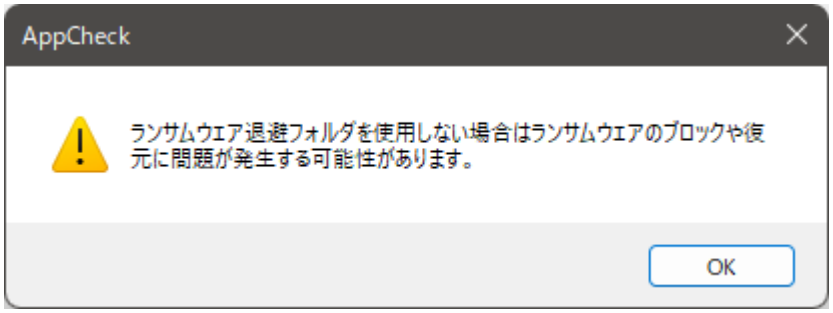
⊙ **デフォルト値 ：** ランサムガードオプション設定を初期化する。

[6-3] 退避フォルダ



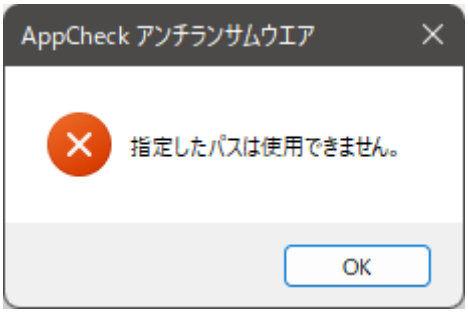
⊙ **ランサムウェア退避フォルダ ：** 保護するファイル拡張名に含まれたファイルが特定条件によって変更、削除などのファイル毀損が発生した場合、リアルタイムでランサムウェア待避所フォルダに臨時バックアップされ、ランサムウェア行為検知時に臨時バックアップされたファイルを利用して元の位置に自動復元する機能。

ランサムウェア待避所機能を使用しない場合、「ランサムウェア待避所を使用しない場合、ランサムウェア遮断およびファイル復元に問題が発生します。」という案内メッセージウィンドウが生成される。

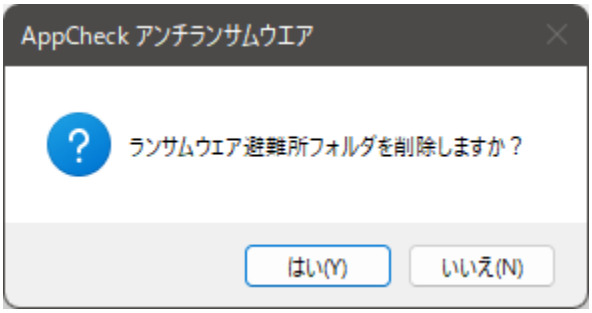


- **退避フォルダパス ：** 退避フォルダの基本位置は、「C:¥ProgramData¥CheckMAL¥AppCheck¥RansomShelter」フォルダであり、設定ボタンをクリックして他のフォルダに変更可能。 ただし、特定の位置に退避フォ

ルダを指定する場合、「指定されたパスは使用できません。」という案内メッセージが生成されるので、他のフォルダに指定する必要がある。



- **退避フォルダ使用量 ：** 退避フォルダパスとして指定されたドライブの全容量のうち、退避フォルダ内に保存されたファイル容量の表示
- **退避フォルダを空にする ：** 退避フォルダおよび内部ファイルを一括削除し、削除されたフォルダおよび内部ファイルはゴミ箱に移動せず、完全に削除する。 ユーザーが「待避所を空にする」をクリックすると、「ランサムウェア待避所を空にしますか？」という案内メッセージウィンドウが生成される。



もし、ランサムウェア退避フォルダ内のファイルを手動で削除する際には、「AppCheckオプション - 一般 - 独自保護使用」チェックを解除した後、削除する。

- **1つのフォイルの大きさを最大「」以下に制限:** 退避フォルダに一時的にバックアップされるファイル容量(100MB, 200MB, 500MB, 1GB, 2GB, 5GB) 制限
- **退避フォルダを隠す ：** 退避フォルダをデフオイル非表示とする
- **「○日」経過したファイルを自動削除:** 退避フォルダに一時的にバックアップされたファイルが「10分、20分、30分、1時間、3時間、6時間、12時間、1日、2日、3日、4日、5日、6日、7日」経過した際に自動削除(デフォルト：7日)
- 退避フォルダの自動削除時間を短く設定し、検知後に手動復元が必要な場合、一時バックアップされたファイルが削除され復元することができませんので、期間設定にご注意ください。

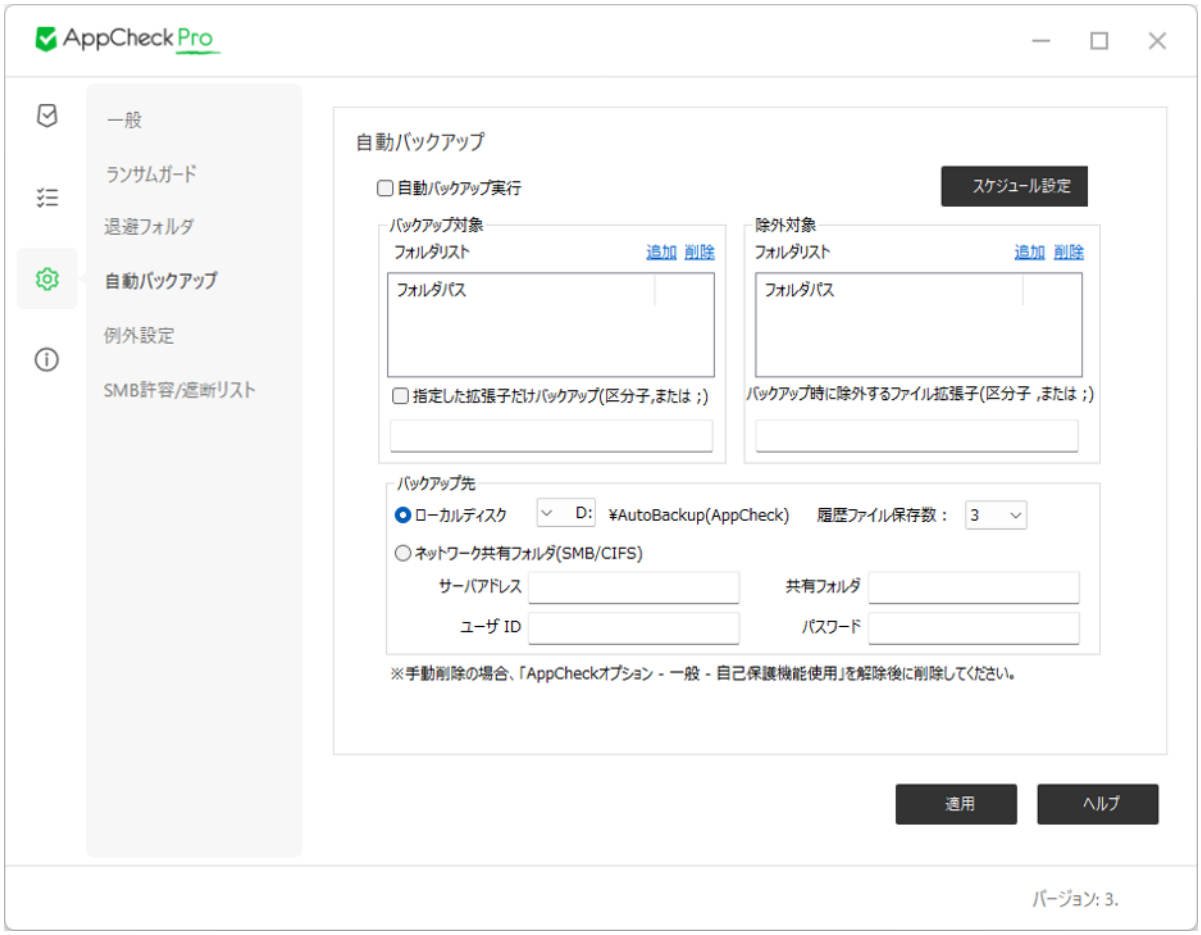
- **退避フォルダの容量が「○○」になると、古い順でファイルを自動削除 ：** 退避フォルダに一時バックアップされたファイル容量が「5GB、10GB、20GB、50GB、100GB、ディスクの10%、ディスクの20%、ディスクの30%、ディスクの40%、ディスクの50%」に到達すると古いファイル順に自動削除(デフォルト：50GB)

⊙ **デフォルト値 ：** 退避フォルダの設定を初期化する

[6-4] 自動バックアップ

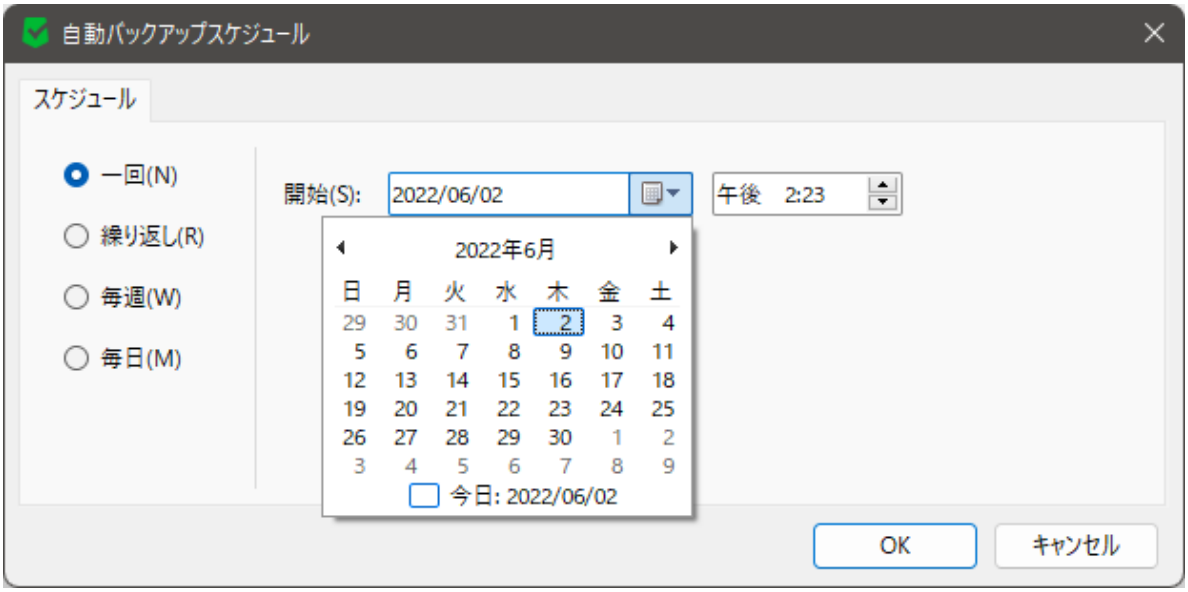
自動バックアップはバックアップ対象フォルダを指定してフォルダ内のすべてのファイルを自動バックアップフォルダ<AutoBackup(AppCheck)>にファイルヒストリーベースでスケジュール設定に従ってバックアップし、ランサムウェアによって自動バックアップされたフォルダ内のファイルは任意に変更できないよう保護する。

安全なバックアップのためには、バックアップ対象フォルダに指定されたフォルダがあるドライブ以外の保存装置に自動バックアップが行われるように設定することをお勧めします。

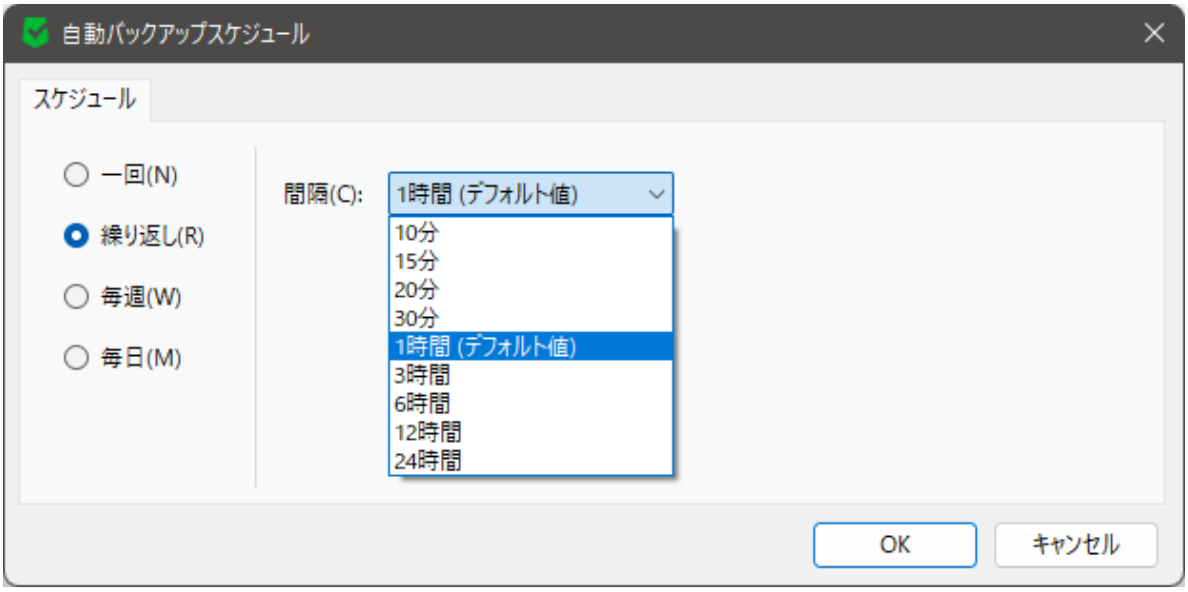


⊙ **スケジュール設定 ：** 一回、繰り返し、毎週、毎の月単位で自動バックアップ

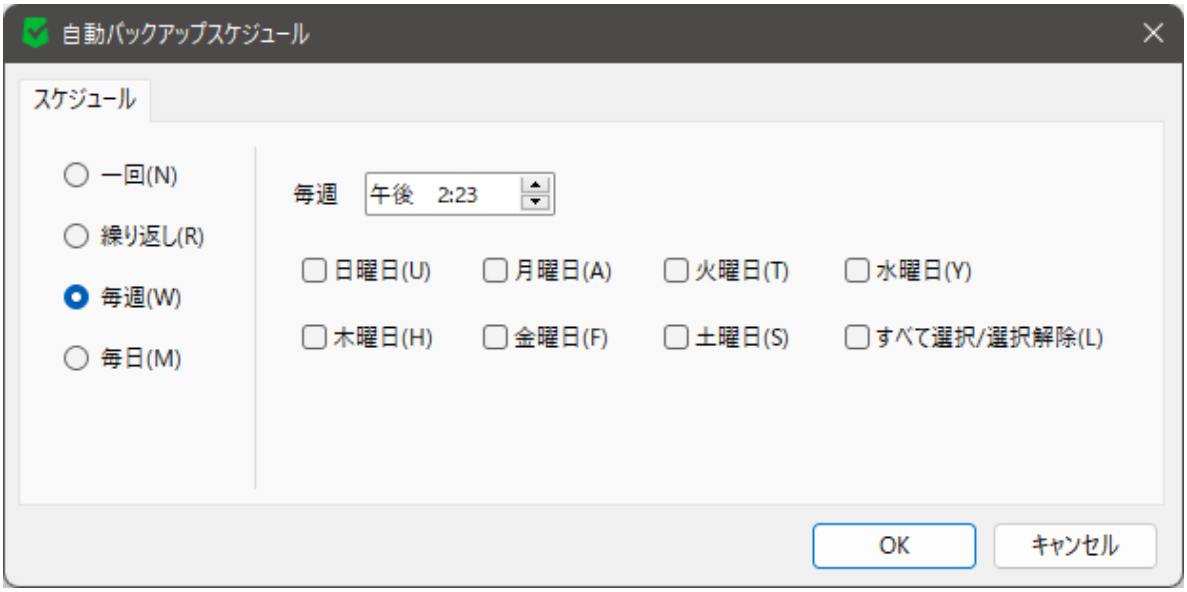
- **一回 ：** 指定した特定日の特定の時間に一回自動バックアップするように設定する。



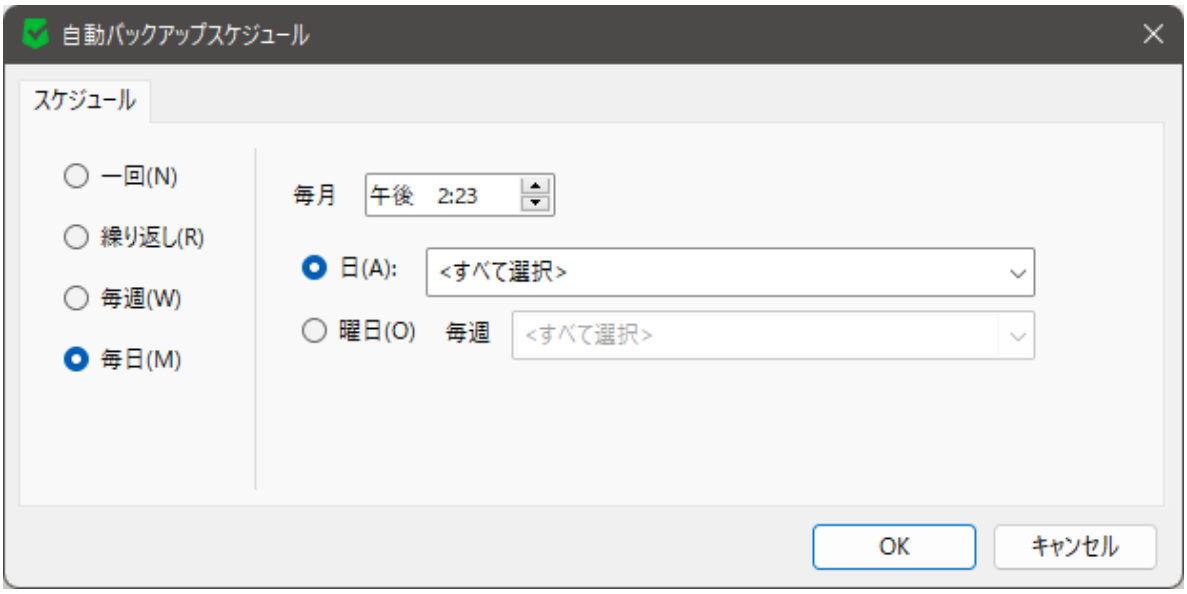
- **繰り返し ：** 10分、15分、20分、30分、1時間（デフォルト）、3時間、6時間、12時間、24時間単位で自動バックアップするよう設定する。



- **毎週 ：** 指定した特定の曜日の特定の時間に自動バックアップするように設定する。



- **毎日 ：** 毎月指定した特定日または特定の曜日の特定の時間に自動バックアップするように設定する。



⊙ **バックアップ対象 ：** バックアップをしたいフォルダの追加・削除

⊙ **指定した拡張名だけバックアップ(区分字、または;) ：** バックアップ対象フォルダ内に存在するファイルのうち、ユーザーが指定したファイル拡張名のみバックアップ

⊙ **除外対象 ：** バックアップする対象フォルダリストに含まれている下位フォルダのうち、ユーザー選択によって自動バックアップ時に除外処理を追加・削除

⊙ **バックアップ時に除外するファイル拡張名(区分字、または;) ：** バックアップ対象フォルダ内に存在するファイルの

うち、ユーザーが指定したファイル拡張名はバックアップ時に除外処理

⊙ **バックアップ先 ：** ローカルディスクまたはネットワーク共有フォルダ(SMB/CIFS)から選択

⊙ **ローカルディスク ：** PCと物理的に連結されたハードディスクの中で使用可能なディスク容量が最も多いドライブが基本的に自動選択され、ユーザー選択によって自動バックアップフォルダ<AutoBackup(AppCheck)>が保存されるドライブ指定できる。

⊙ **履歴ファイル保存数 ：** 自動バックアップ対象の原本ファイルが修正される場合、既存のバックアップファイルは履歴ファイル(.history)に変更され、履歴ファイル数は0~10個ユーザーが指定できる。 （デフォルト：3個）

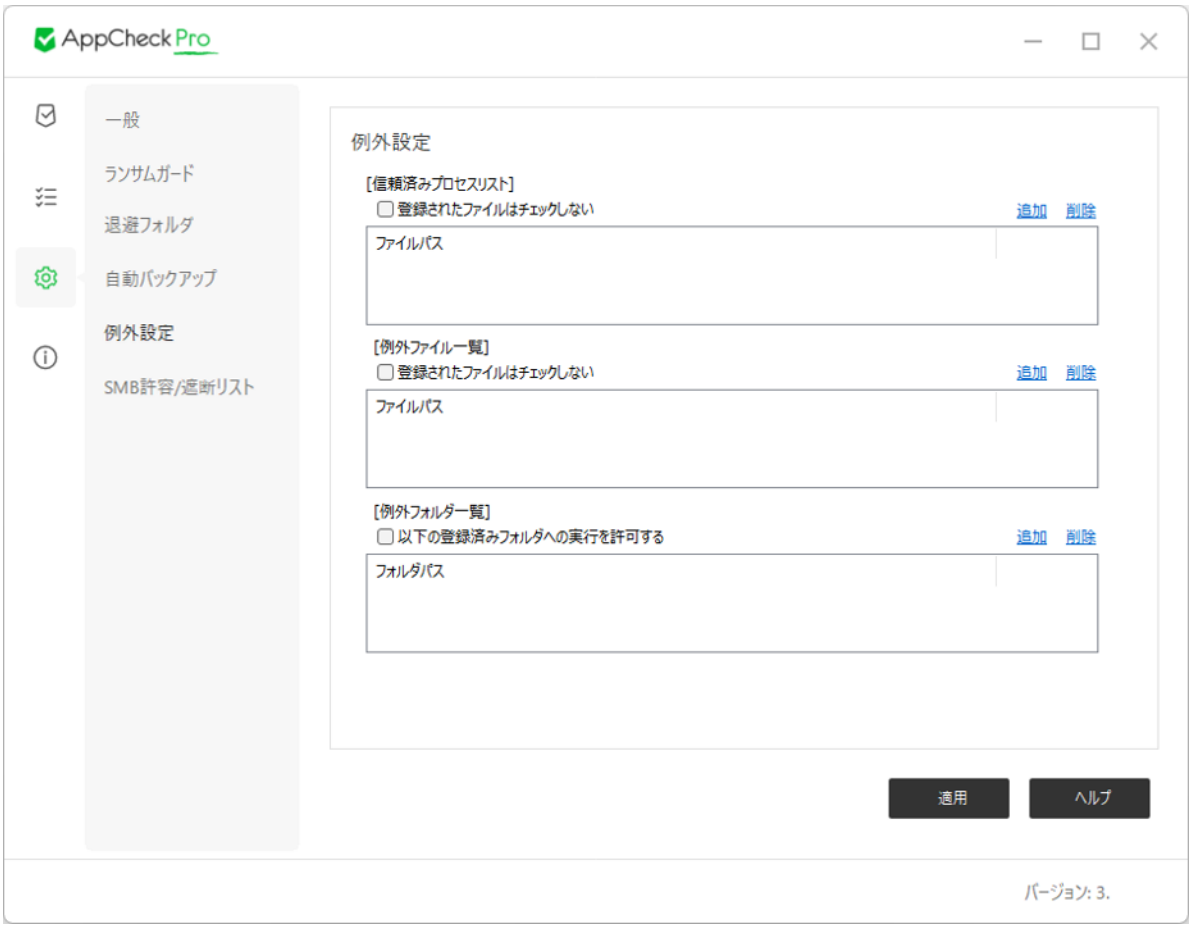
ご参考として、履歴ファイルの維持個数を超える場合、最も古い履歴ファイルから自動削除する。

⊙ **ネットワーク共有フォルダ(SMB/CIFS) ：** サーバーアドレス(IPアドレスまたは遠隔地装置名)、共有フォルダ(共有設定が行われた遠隔地ドライブ/フォルダ名)、ユーザーID、パスワード入力必須

安全にネットワーク共有フォルダを使用するためには、Windows アップデート機能を通じて提供される SMB 脆弱性に関する最新のセキュリティパッチを行い、共有フォルダへのアクセスのためのユーザーアカウントおよびパスワード管理とフォルダへのアクセス権限設定をお勧めします。

また、自動バックアップフォルダ<AutoBackup(AppCheck)>および内部ファイルを削除するためには、"オプション – 一般 – 自己保護機能使用"設定をチェック解除後、削除する。

[6-5] 例外設定



⊙ **信頼済みプロセスリスト**

- **登録されたファイルはチェックしない ：** ホワイトリストに追加されたファイルは、ランサムウェア行為検知、ランサムウェア行為高級検知知、MBR遮断が発生しないように許可する。 ただし、特定検知条件によってはホワイトリストに追加されたファイルを通じたファイル毀損時に遮断されることがある。

基本的にホワイトリストに追加されたファイルによって変更されるファイルは、ランサムウェア避難所フォルダにバックアップ処理が行われない。

注意すべき点は、ランサムウェアによって悪用可能なWindowsシステムファイル(Explorer.exe、svchost.exeなど)を登録する場合、検知されない可能性があるため、追加をしない、または一部のユーザーのみ追加すること。

⊙ **例外ファイル一覧**

AppCheckの保護するファイル拡張名に含まれたファイルの中で保護を望まない場合は例外ファイルリストに追加する。

- **登録されたファイルはチェックしない ：** 例外ファイルリストに追加されたファイルは、AppCheck保護対象から除外処理する。

  例外ファイルリストに追加されたファイルは、ランサムウェアによってファイル毀損時に避難所バックアップおよび遮断が行われない。

⊙ **例外フォルダー一覧**

例外フォルダリストに登録されたフォルダ内のファイルのうち、AppCheckの保護するファイル拡張名に含まれたファイルが存在するが、保護を望まない場合は例外フォルダリストに追加する。 ただし、例外フォルダリストに追加されたフォルダ内の下位フォルダとネットワークドライブ内のフォルダについては例外処理しない。

- **以下の登録済みフォルダへの実行を許可する ：** 例外フォルダリストに追加されたフォルダ内のすべてのファイルは、AppCheck保護対象から除外処理する。

例外フォルダリストに追加されたフォルダは、ランサムウェアによって内部ファイルが毀損された場合、避難所バックアップおよび遮断が行われない。

ご参考として、例外ファイルリストまたは例外フォルダリストに追加されたファイルは、AppCheck 自動バックアップ機能を通じて別途バックアップしておけば、ランサムウェアまたはデータ毀損などの事故から安全に保護することができる。

[6-6] SMBリスト

SMBリストはランサムガードの「SMBサーバー保護」機能のためのオプションであり、ネットワークドライブを通じて接続された特定IPアドレス(IPv4、IPv6)の遮断および許可可否を設定することができる。

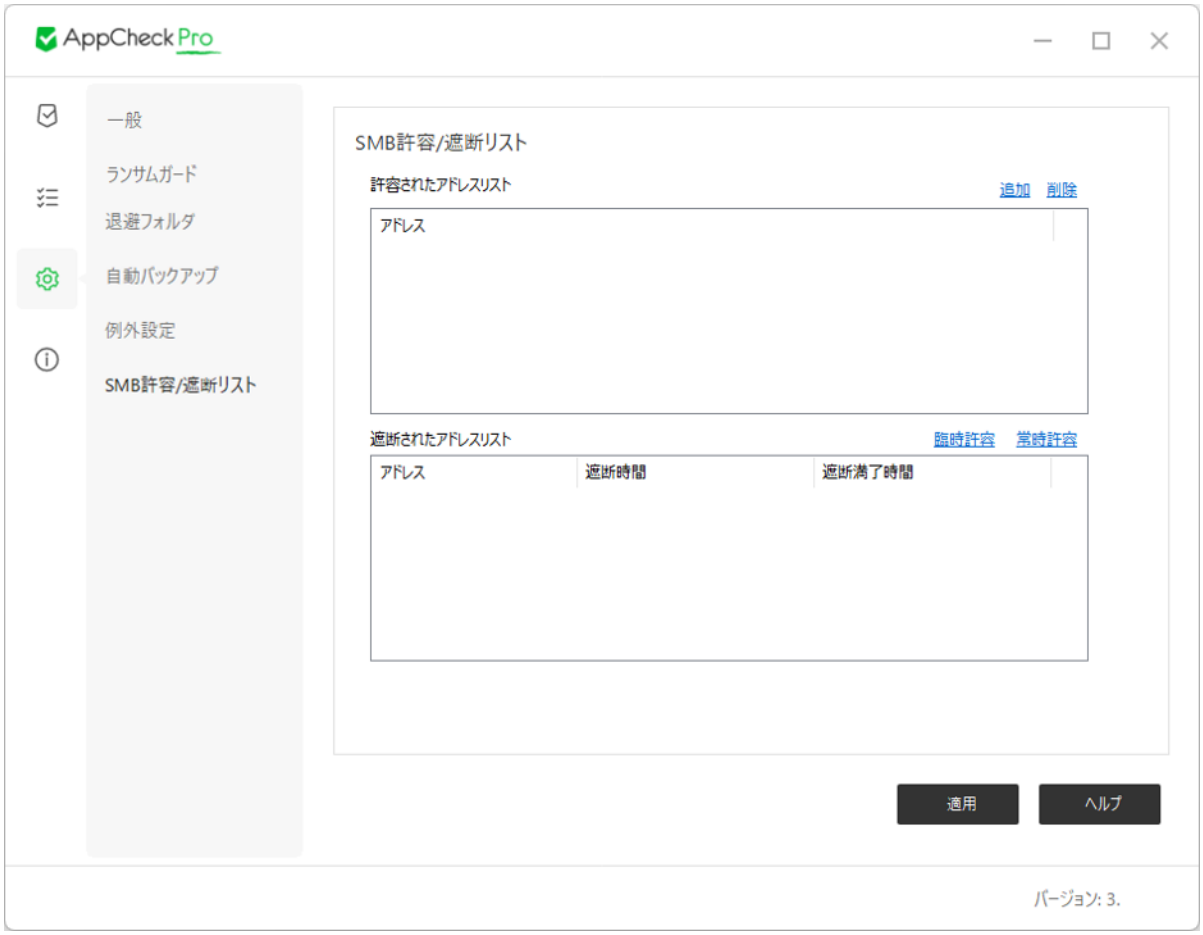
遠隔地PCで実行されたランサムウェアがネットワークドライブを通じて接続された共有フォルダ内のファイルを毀損した場合、「リポート先PCが共有中のファイルを多数破損したため、遮断しました。」という通知メッセージウィンドウを通じて遠隔地IPアドレスを遮断および毀損されたファイルを自動復元することができる。

- **IPアドレス(詳細) :** "ツール - 脅威ログ"メニューに移動
- **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 :** 遮断断された遠隔地IPアドレスを「臨時許容」する(再び検知されるまで許容)

※ロック設定使用またはCMS中央管理ポリシーによるロックモード適用環境では"常時許容"、"臨時許容"メニューが表示されない。

⊙ **許容されたアドレスリスト**

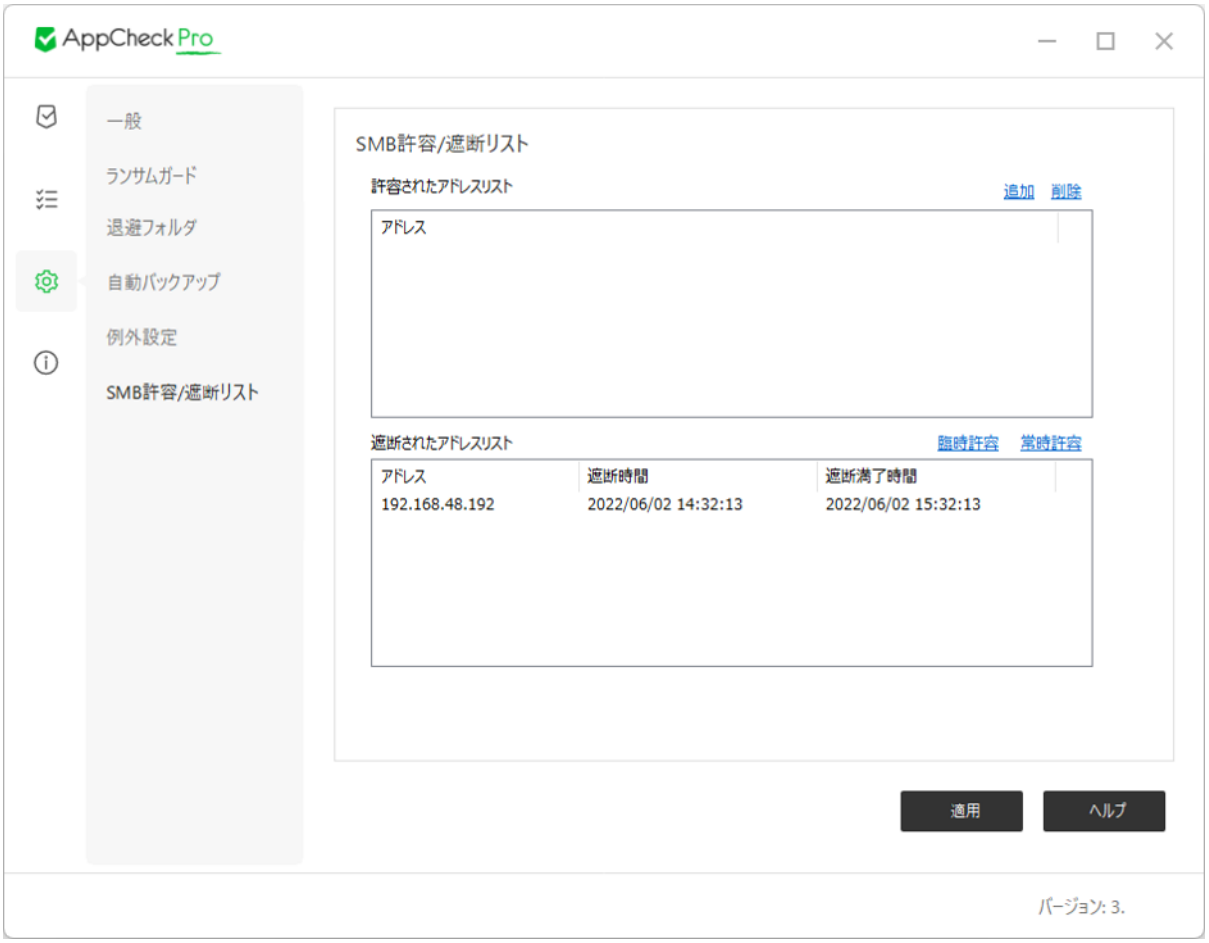
許可されたアドレスリストにユーザーが直接IPアドレスを追加するためには、追加ボタンをクリックしてIPv4またはIPv6アドレスを個別、順次、全体規則に従って特定IPを追加することができる。



許可されたアドレスリストに追加された遠隔地IPを通じて共有フォルダ内のファイル毀損時にAppCheckの遮断は行われないが、ランサムエア避難所バックアップは行われる場合がある。

⊙ 遮断されたアドレス一覧

遮断されたアドレスリストに登録された遠隔地IPアドレスは1時間だけ一時遮断され、遮断満了時間が経過すると自動的に遮断されたアドレスリストに登録されたIPアドレスは削除処理され、遠隔地PCでは共有フォルダ内ファイルへのアクセスが可能。

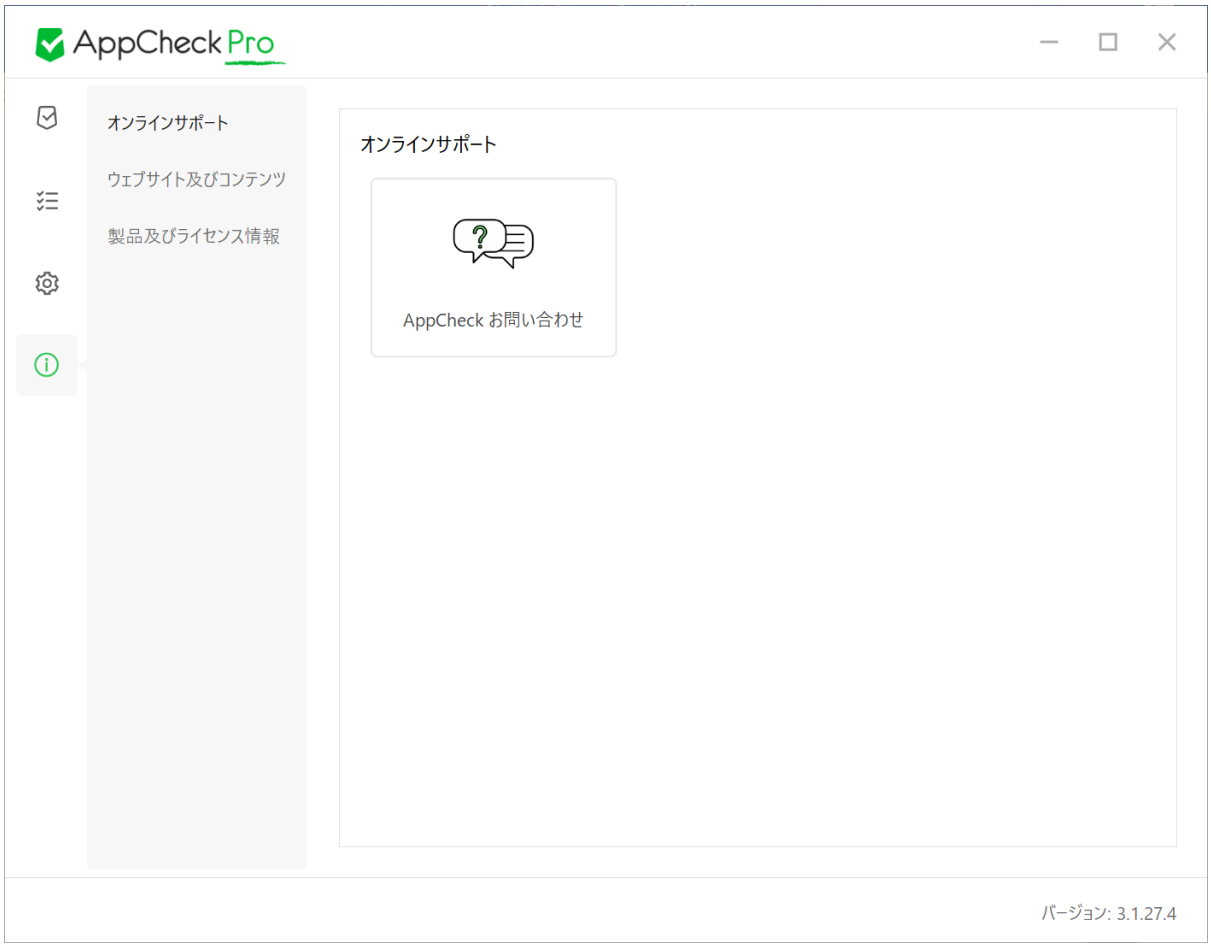


- **追加 ：** 登録された遮断IPアドレスを"許可されたアドレスリスト"に追加し、該当IPに対する遮断をしない。
- **削除 ：** 登録された遮断IPアドレスを削除する。

ご参考として、SMB サーバー保護(IP 遮断)機能を通じて遮断されたアドレスリストに IP が追加された際、AppCheck リアルタイム保護を無効化(OFF)する場合、遮断された IP アドレスを一時許可し、以後リアルタイム保護が活性化(ON)される場合、遮断満了時間まで IP アドレスが遮断される。 ただし、Windows 再起動が行われる場合、遮断満了時間と関係なく遮断された IP アドレスは自動削除される。

7. カスタマーセンター

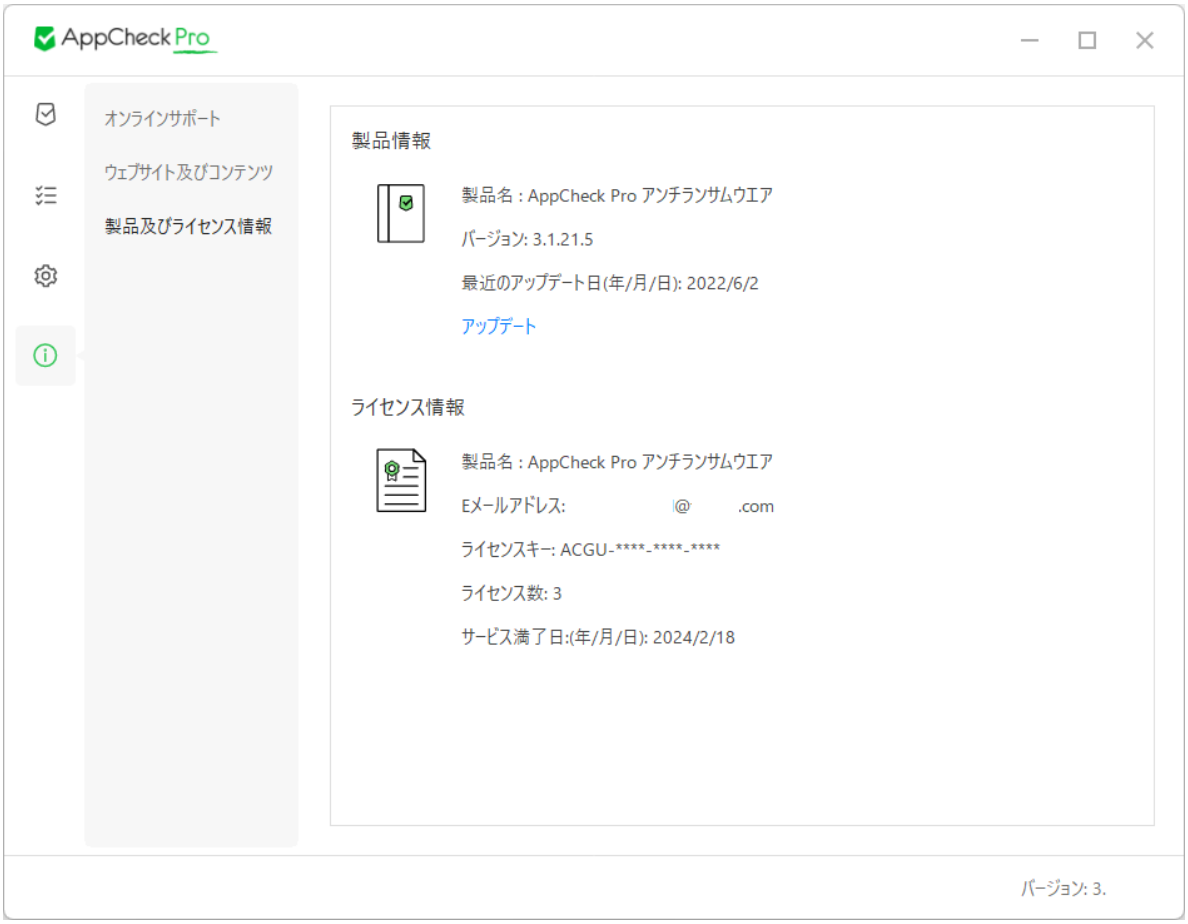
[7-1] オンラインサポート



⊙ **AppCheck お問い合わせ :** AppCheckお問い合わせページに移動

[7-2] 製品及びライセンス情報

⊙ 製品情報



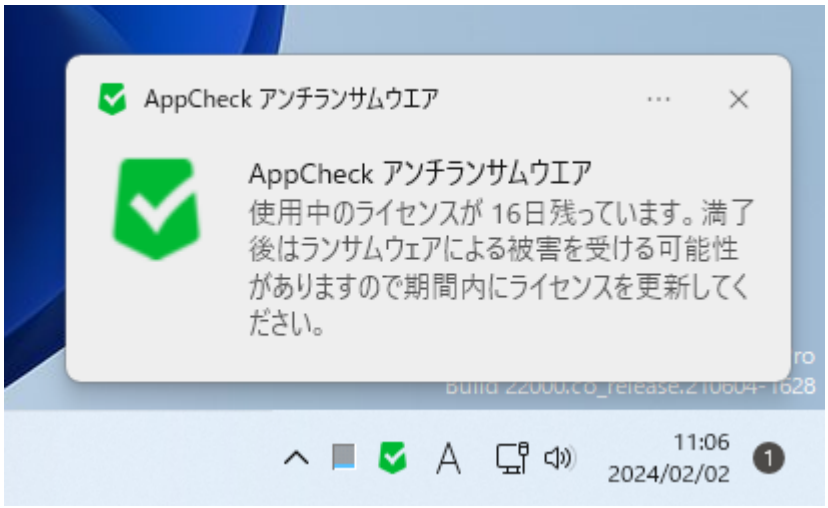
- **製品名 :** ライセンス登録可否により、AppCheckまたはAppCheckProで表示
- **バージョン :** 現在インストールされているAppCheckのバージョン
- **最新のアップデート日 :** 現在インストールされているAppCheckの最新アップデート日
- **アップデート :** AppCheck最新アップデートの手動確認

⊙ ライセンス情報

- **製品名 :** AppCheck Pro アンチランサムウェア
- **Eメールアドレス :** ライセンス登録時に入力したメールアドレス
- **ライセンスキー :** ライセンス登録時に入力したシリアル番号
- **ライセンス数 :** 登録したライセンスで利用できるデバイス数

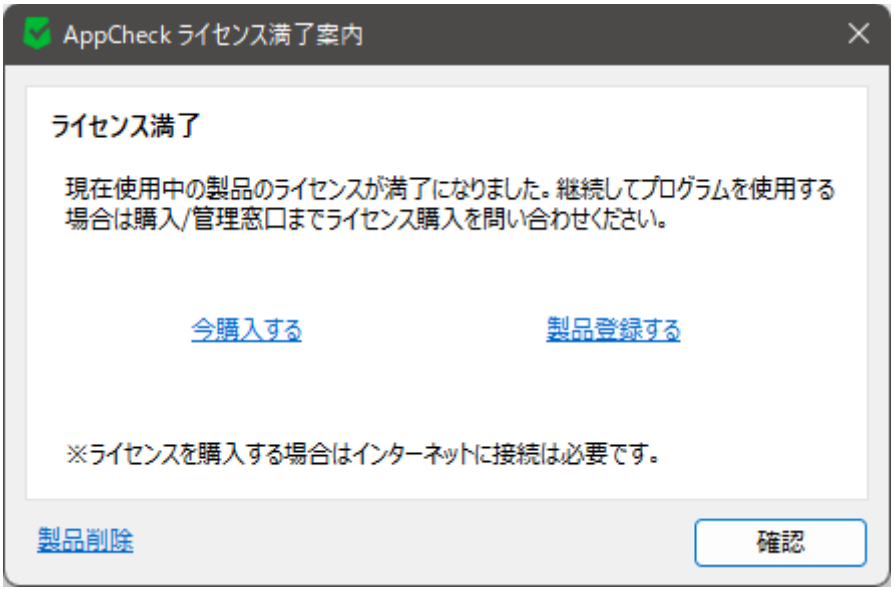
- **サービス満了日 ：** 登録したライセンスの満了日

ライセンスの満了31日前から、「使用中のライセンスが○○日残っています。 満了後はランサムウェアによる被害を受ける可能性がありますので期間内にライセンスを更新してください。」という案内メッセージが表示されます。



ライセンスが満了すると、すべての機能が停止し、AppCheck を実行したら「AppCheck ライセンス満了案内」というメッセージが表示され、「現在使用中の製品ライセンスが満了しました。 引き続きプログラムを使用するためには、購入/管理先にライセンス購入についてお問い合わせください。」 という案内メッセージが表示されます。

※ CMS 中央管理で配布した AppCheck バージョンである場合、上記のライセンス満了通知が表示されません。



- **今購入する ：** checkmal のライセンス購入ページに移動
- **製品登録する ：** 購入したライセンスのメールアドレス・シリアル番号を登録
- **製品削除 ：** AppCheck をアンインストールする