JSecurity

AppCheck Pro

設定マニュアル

株式会社 JSecurity

v202605

はじめに

この度は、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、ご利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

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 V3.1.43.10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 4世代Core i3 以上 / AMD FXシリーズ 以上 ・メモリ：2GB以上 ・ハードディスク：10GB以上の空き容量が必要
OS	・Windows 7 (32/64ビット) SP1* *SHA-2認証書のMicrosoft最新パッチがインストールされていること ・Windows 8 (32/64ビット) ・Windows 8.1 (32/64ビット) ・Windows 10 (32/64ビット) ・Windows 10 IoT (32/64ビット) ・Windows 11 (64ビット) ・Windows 11 IoT (32/64ビット)

※ARMプロセッサーは未対応となります。

※上記ハードウェア表記は最小仕様です。

JSecurity

目次

1. インストール

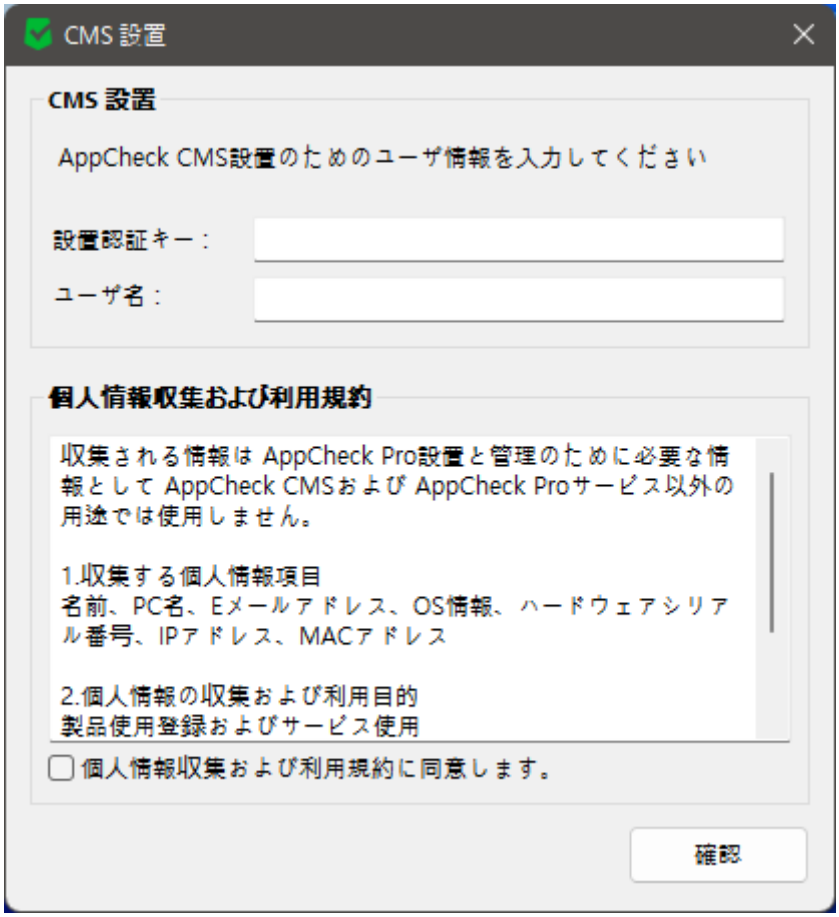
1.1 CMS有

(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。

※Windows設定にある「アプリを入手する場所の選択」の項目内容によっては、お客様環境によりインストールできない場合があります。そのため、アプリ入手制限の緩和設定をお願いいたします。

(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」ウィンドウにインストール認証キー、ユーザー名を入力し、同意にチェックを入れてください。

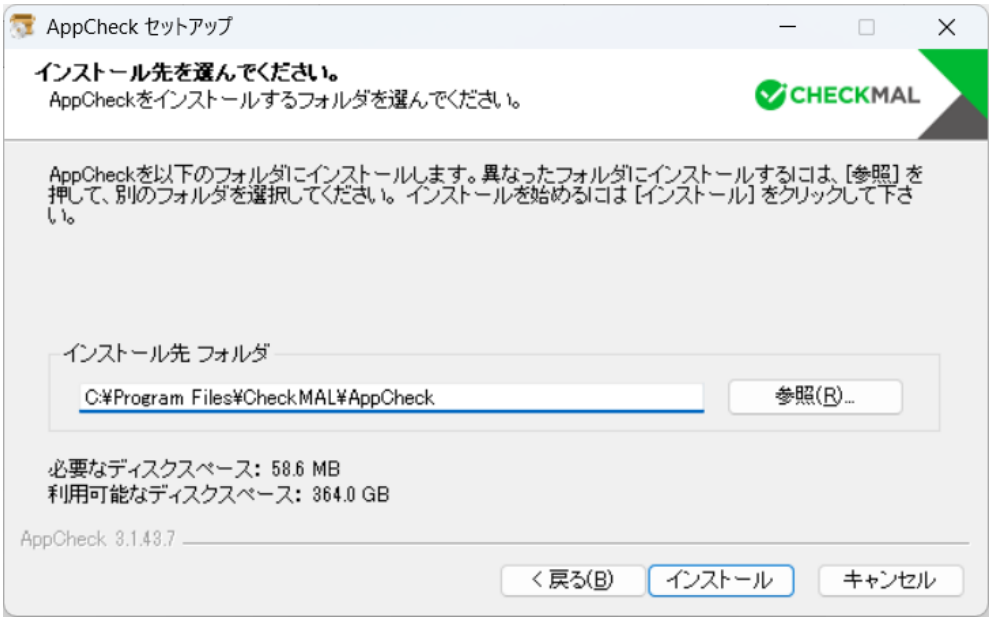


- **設置認証キー ：** 基本的に自動入力されており、CMS「配布管理」で提供するインストール認証キーと同一
- **ユーザー名 :**ユーザーカウント名のデフォルト値であり、会社のポリシーによって識別可能なユーザー名に修正可能

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、「個人情報収集および利用規約に同意します。」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「設置認証キー」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。

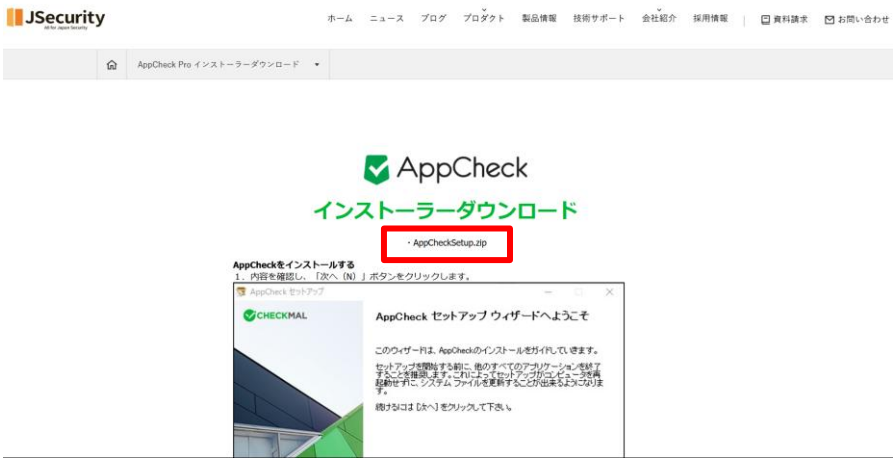


(5) AppCheckのインストールが完了した後、「完了」ボタンをクリックすると、AppCheckが自動に実行されます。

1.2 CMS無

AppCheckはインターネットにアクセスできるWindows 7 (32/64bit)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。

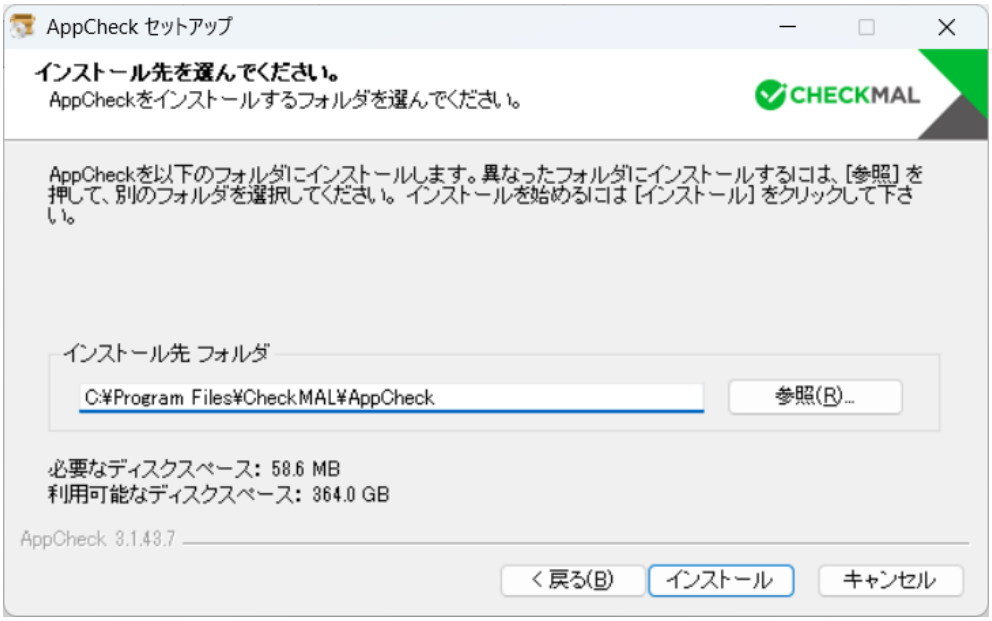


※Windows設定にある「アプリを入手する場所の選択」の項目内容によっては、お客様環境により インストールできない場合があります。そのため、アプリ入手制限の緩和設定をお願いいたします。

(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。

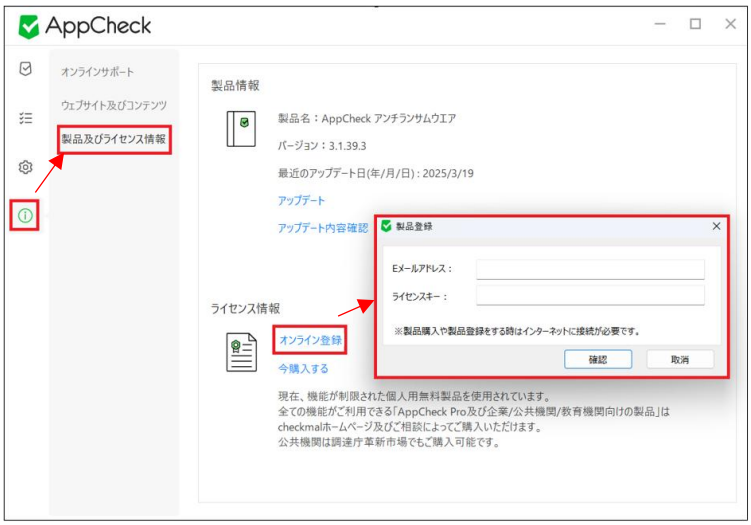


(5) インストールが完了した後「完了」ボタンをクリックするとAppCheckが自動的に起動します。

（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指します。

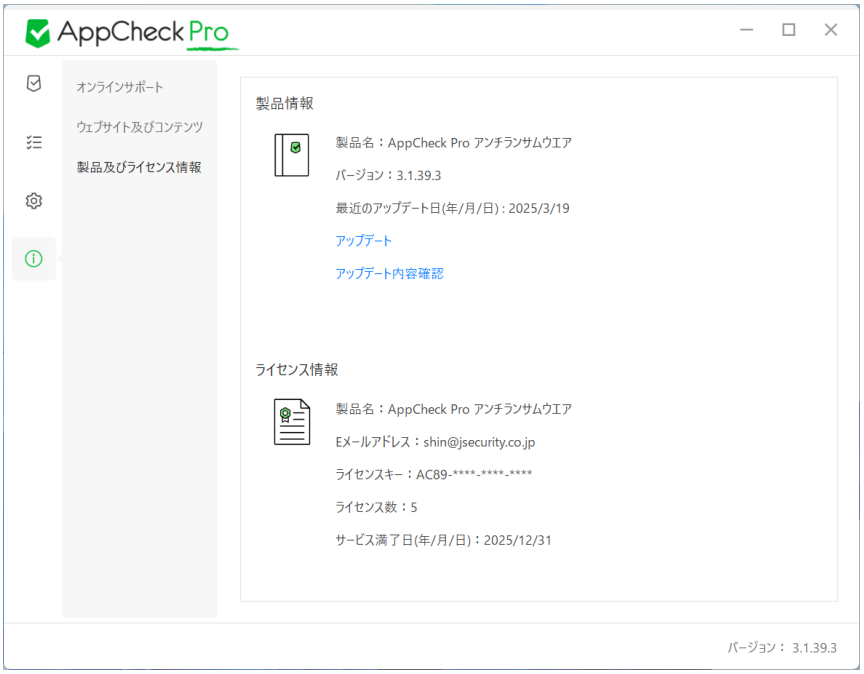
(6) **「Eメールアドレス」**と**「ライセンスキー」**を入力し、確認ボタンを押すと評価バージョンから製品バージョンに更新されます。



※CMS有（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）

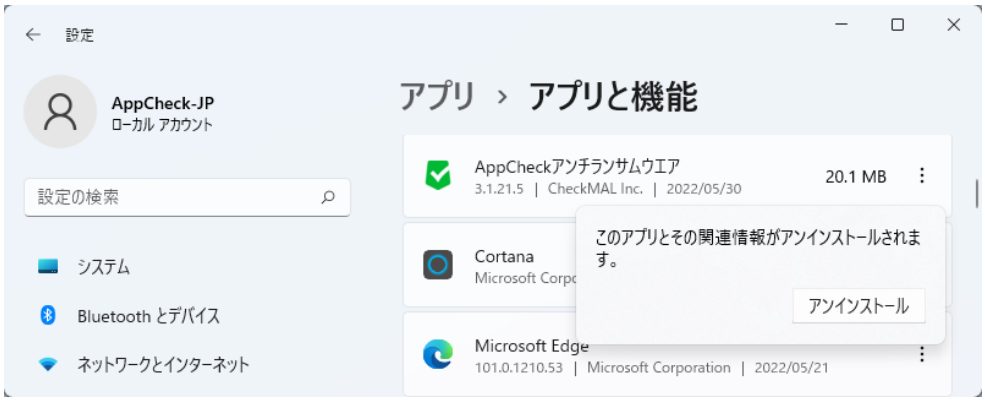
(8) 製品登録が完了すると、「ライセンス情報」に「Eメールアドレス」「ライセンスキー」「満了日」「数量」が表示されますのでご確認ください。



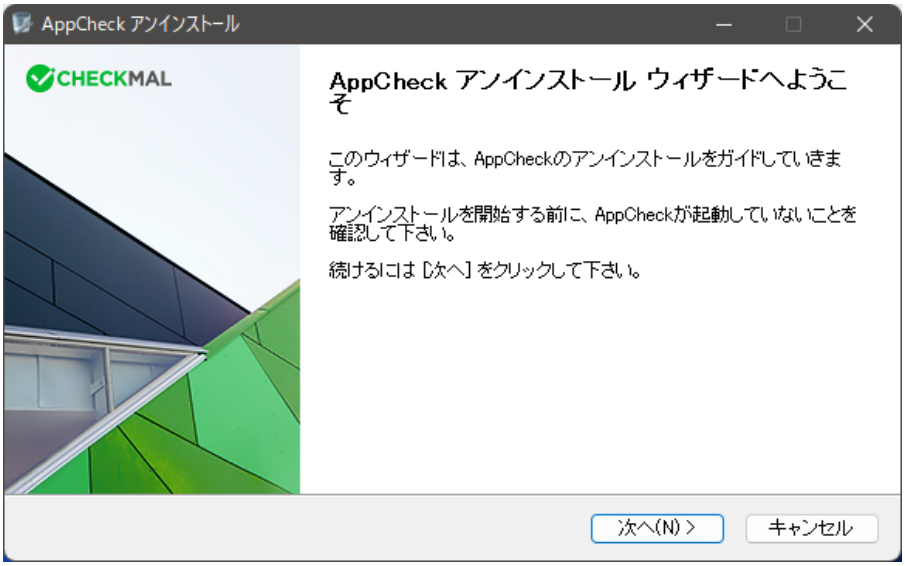
2. アンインストール

※CMS Cloudポリシーの「一般タブ」>「アプリケーション削除許可」がOFF(デフォルト)になっており、エージェント側でのAppCheckアンインストールができない場合は、「エージェント」>「該当エージェントを選択」>「エージェント削除」をクリックし、CMS Cloud側からのAppCheckアンインストールを行うようお願い致します。
エージェント側でAppCheckのアンインストールをしたい場合は、「AppCheckロック設定をOFF」、CMS有は「CMS中央管理ポリシーのアプリケーション削除許可をON」にした状態で、以下手順を参照していただきアンインストールをお願い致します。

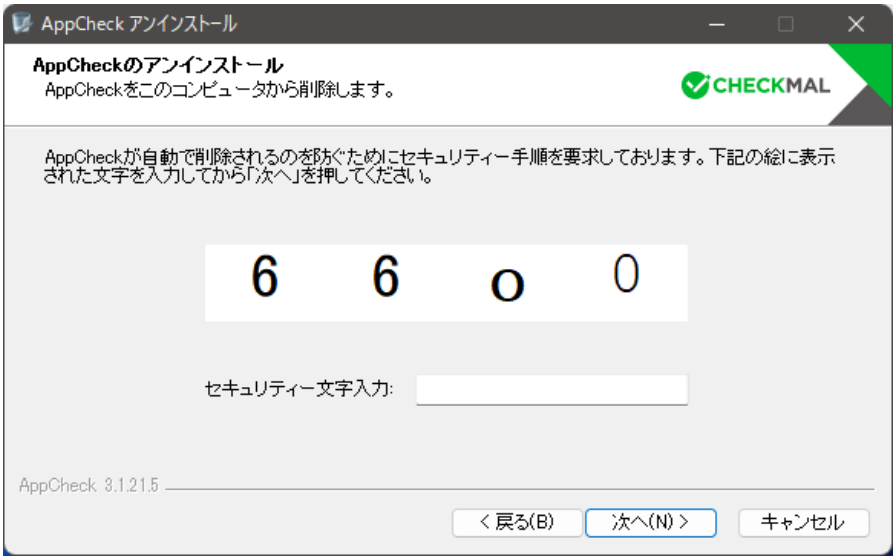
(1) AppCheckのアンインストールは、インターネットと接続されている状態で、「設定」→「アプリと機能」のプログラムリストに登録されている"AppCheckアンチランサムウェア"を選択し アンインストールを実行します。



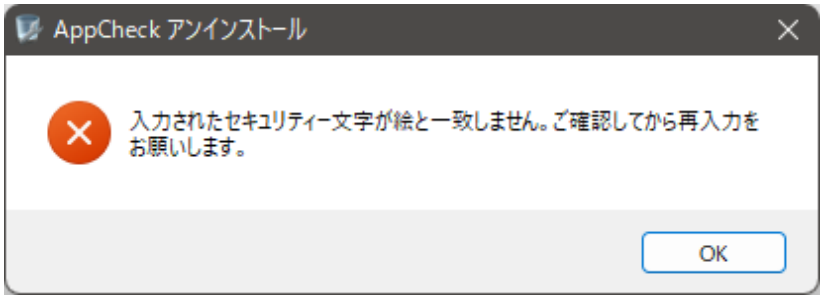
(2)「次へ」をクリックします。



(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。



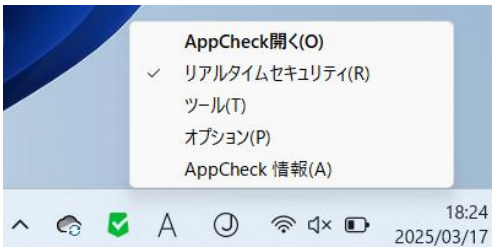
(4) システムからAppCheckを削除する際には、「アンインストール」ボタンをクリックしてください。アンインストール対象は「C:¥ProgramFiles¥CheckMAL¥AppCheck」フォルダ及びその他の関連ファイルとなります。

(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される場合がございます。

3. AppCheck Proの各機能について

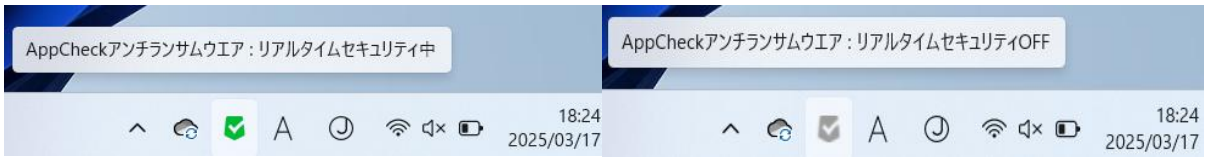
3.1 AppCheckのアイコンメニュー

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が適用されている場合は、「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

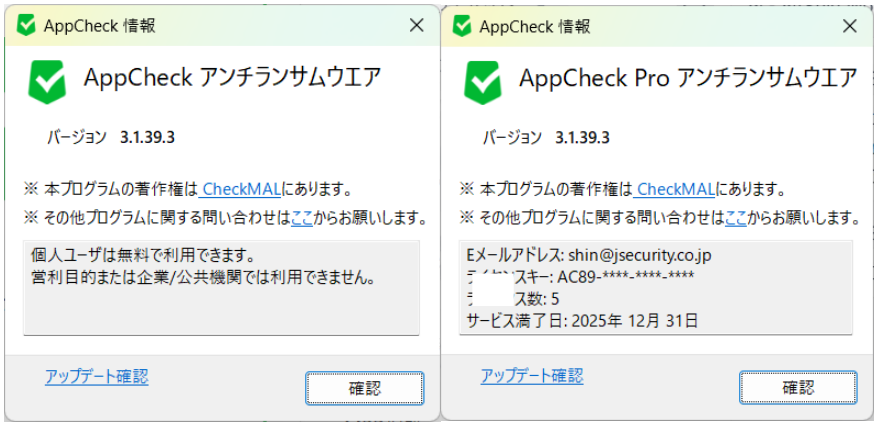


- **緑色のアイコン ：** リアルタイムセキュリティ機能が「ON」の状態
- **グレー色のアイコン ：** リアルタイムセキュリティ機能が「OFF」の状態

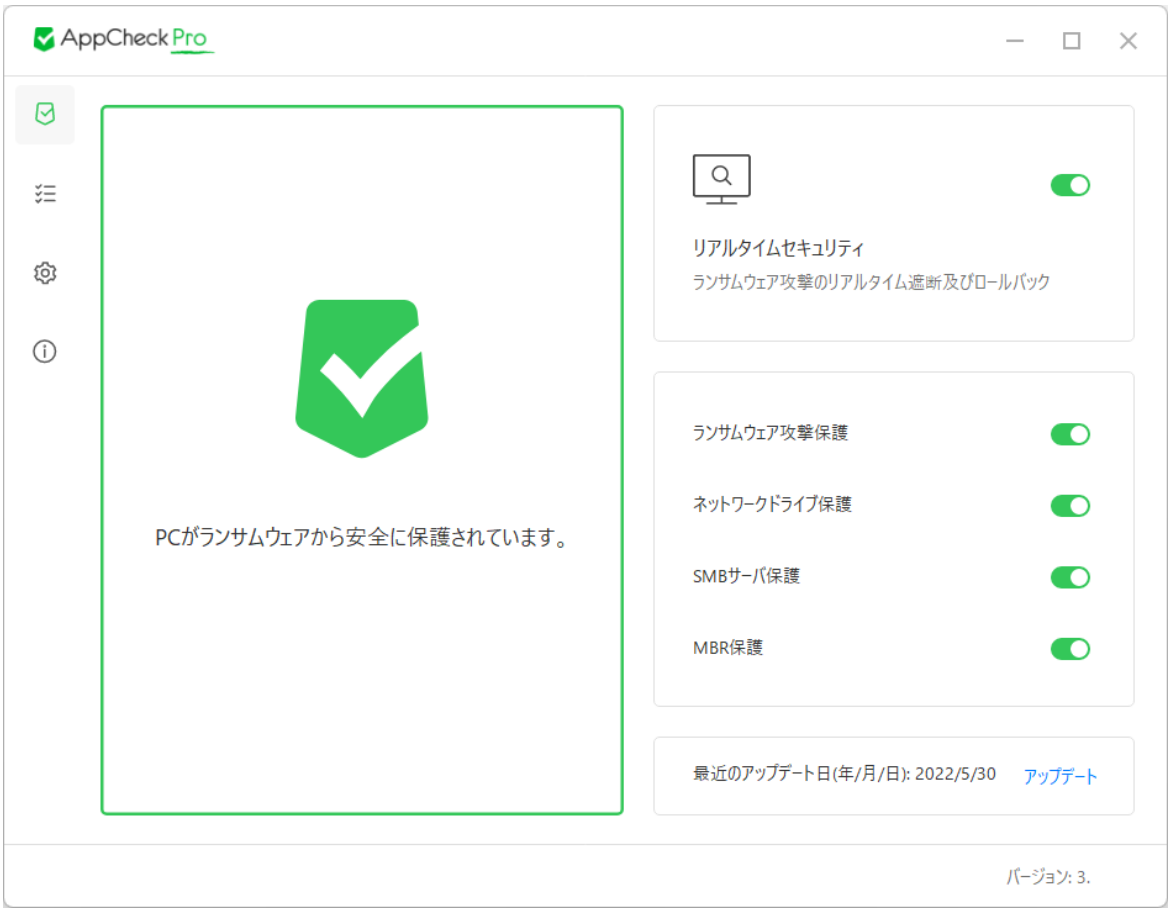
⊙ **ツール ：** 一般ログ、脅威ログ、検疫ログの画面表示

⊙ **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



3.2 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・非活性化ができます。

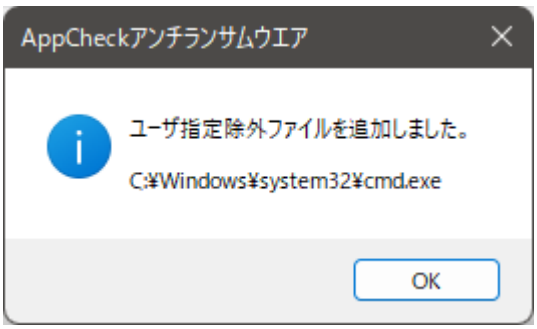
- **リアルタイムセキュリティ「ON」：** ランサムウェアの脅威から安全に保護されています。
- **リアルタイムセキュリティ「OFF」：** ランサムウェアの脅威にさらされています。

⊙ **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。

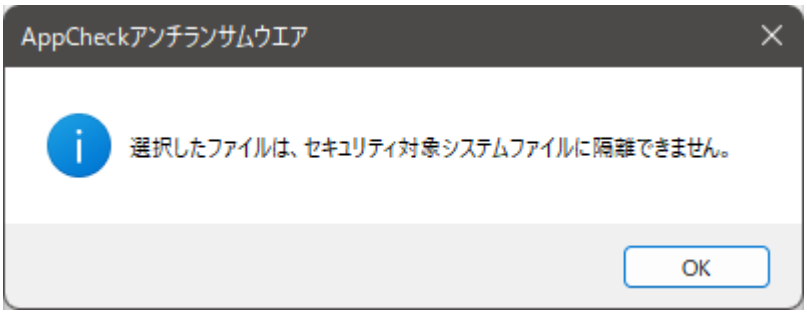
- **プログラム名 ：** ファイル毀損行為により遮断されたファイル名
- **プログラム名（詳細）：**「ツール」 –「脅威ログ」画面に移動
- **プログラム説明 ：**「ランサムウェア動作探知」されたファイルのプロパティ内容
- **プログラム発行者 ：**「ランサムウェア動作探知」されたファイルのデジタル署名
- **ホワイトリスト登録 ：**「ランサムウェア動作探知」されたファイルの中、正常なプログラム行為を誤検知した場合、「ユーザー指定除外ファイル登録」を行うことができます。 除外ファイルとして登録されたファイルは、「オプション」-「例外設定」-「ユーザー指定除外ファイルリスト」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有の場合、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、「ユーザー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。

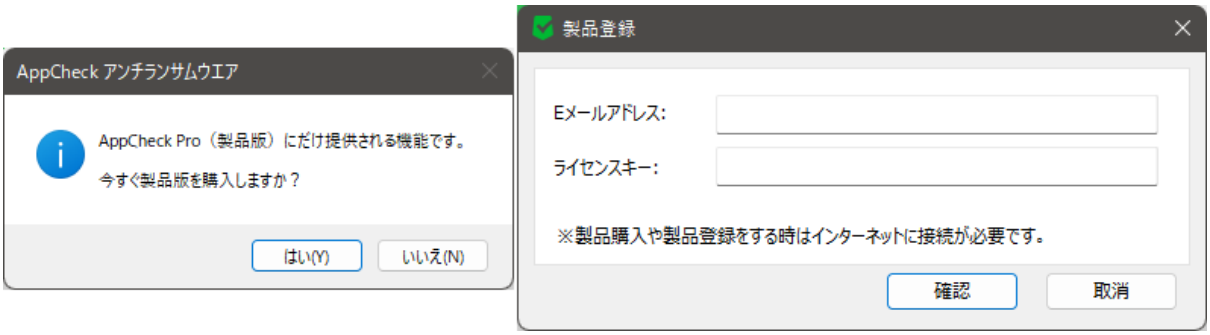
- **ファイルを隔離する ：** ランサムウェアとして検知されましたが、権限などの理由によって自動削除できなかった場合は、検疫所フォルダに格納することができます。



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。

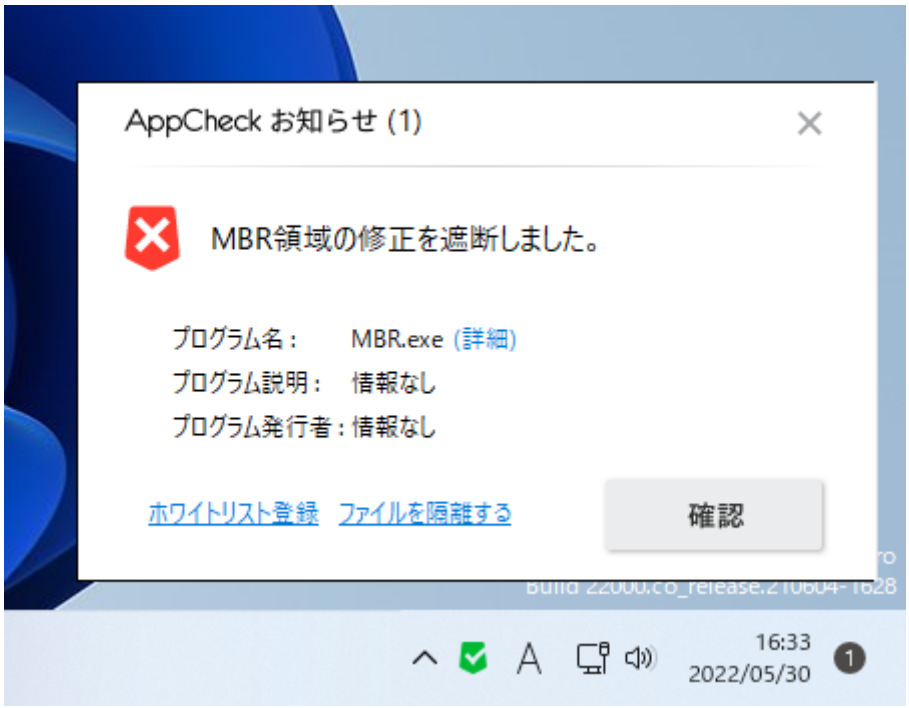
AppCheck評価版で保護機能を活性化すると、「AppCheckProバージョンで提供される機能です。 今すぐ製品版を購入しますか?」という通知メッセージが表示されます。



「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（製品版）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。

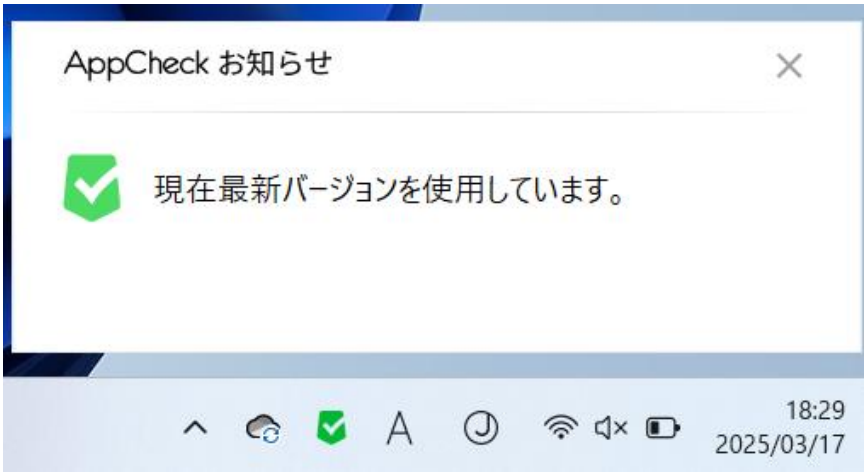


- **プログラム名 ：** MBR領域の毀損で検知、遮断されたファイル名
- **プログラム名（詳細）：**「ツール」－「脅威ログ」画面に移動
- **プログラム説明 ：** MBR領域の毀損で検知、遮断されたファイルのプロパティ内容

- **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有の場合、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。

⊙ **最近のアップデート日 ：** 自動(もしくは手動)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。

3.3 ツール

3.3.1 一般ログ

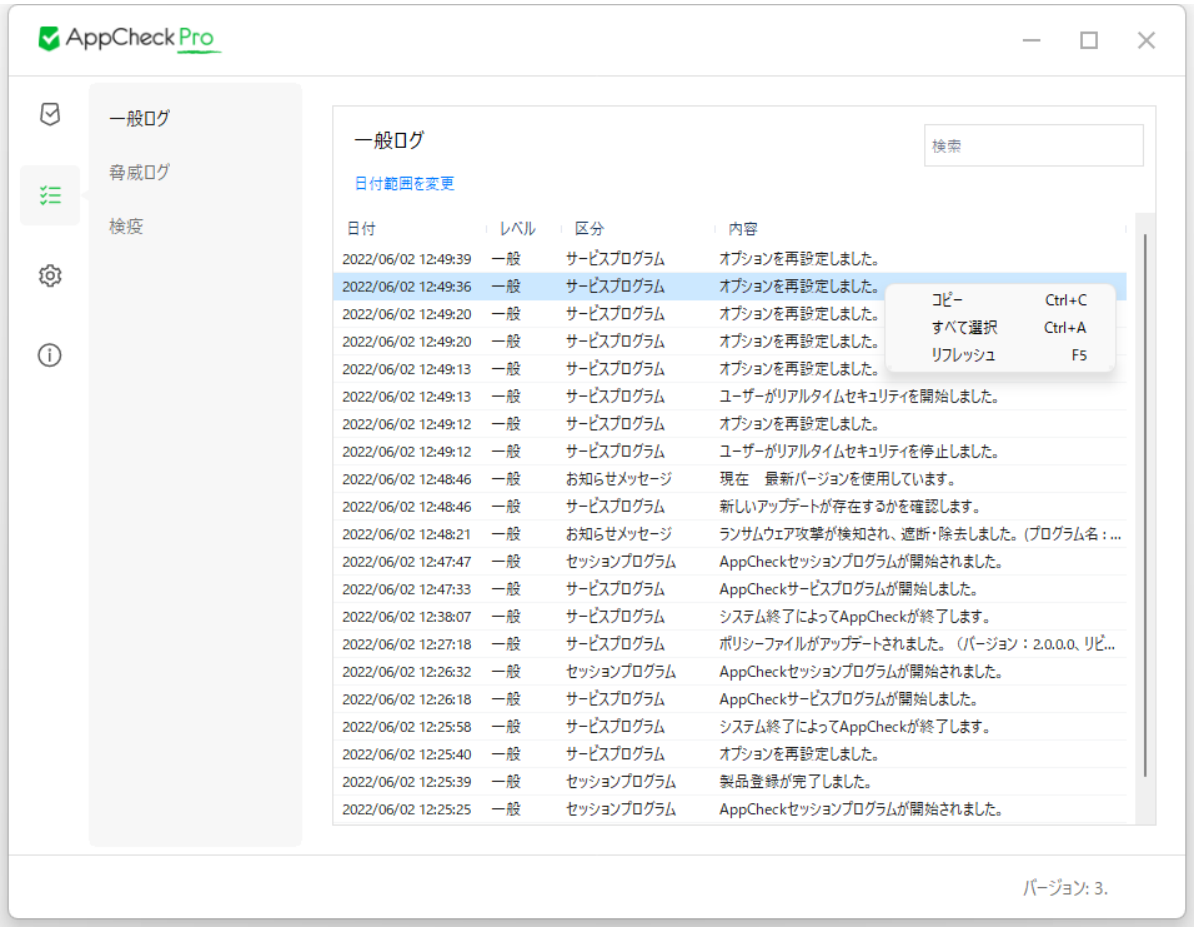
一般ログには、AppCheckの動作中に発生するセッションプログラム、サービスプログラム、自動バックアップ、通知メッセージなど多様な情報が表示されます。

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/昇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。

⊙ **すべて選択（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。

3.3.2 脅威ログ

脅威ログには、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。

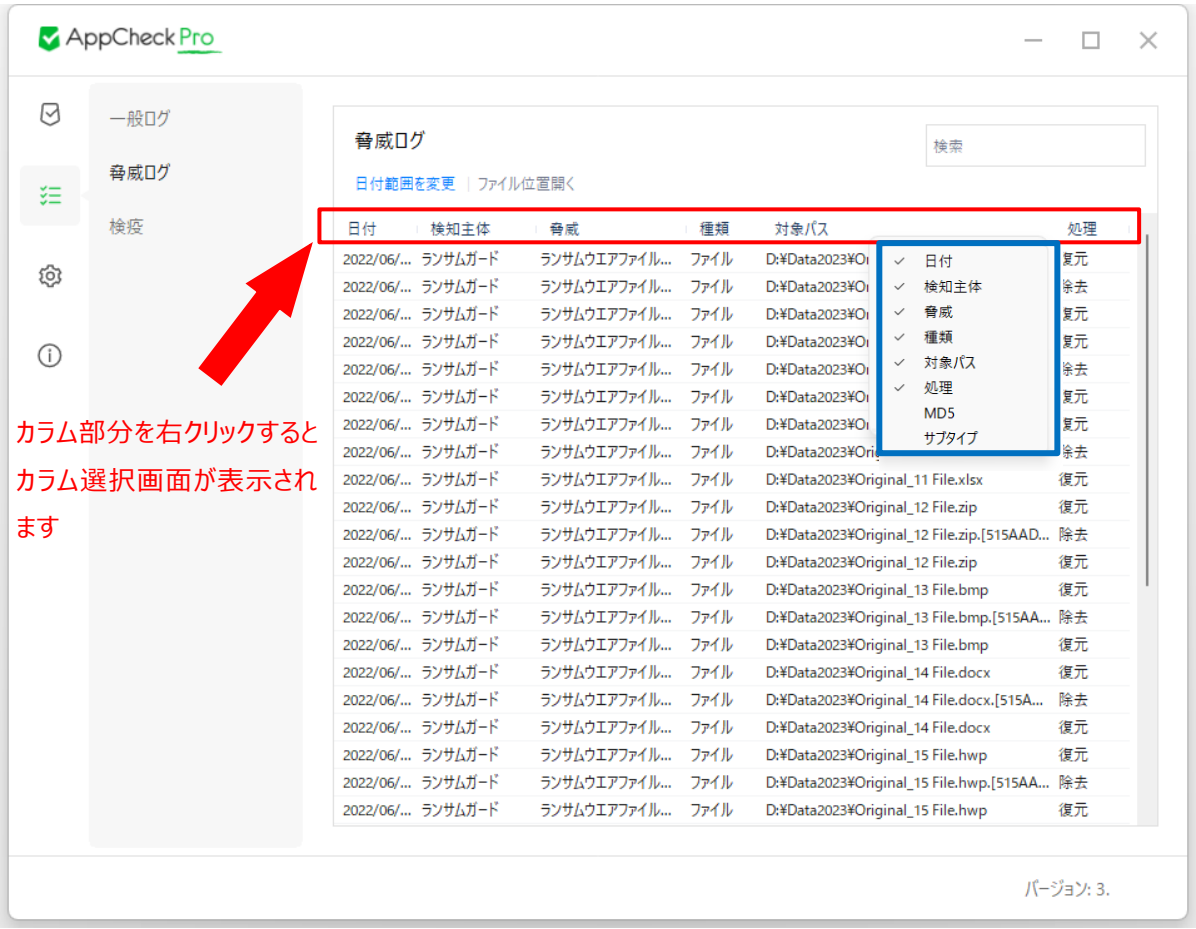
脅威ログの「日付範囲を変更」メニューにより、特定期間内に記録された脅威ログをフィルタリングして確認することができます。

- **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、対象パス、処理、MD5(デフォルト:無効化)、サブタイプ(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。

・MD5とはハッシュ値を作成する際のアルゴリズム(作り方)の名称であり、ハッシュ値は主にデータの整合性チェック及びデジタル著名に利用されます。
(例：改ざんの有無・正規ファイルか悪性ファイルかの判断、等)

・サブタイプとは、AppCheckの検知した機能名が表示されます。
(表示例：N/A(MBR検出・脆弱性ガード等)、ランサムガード、ゴースト、スマート、システムの脅威、ネットワークドライブ、SMBサーバ)

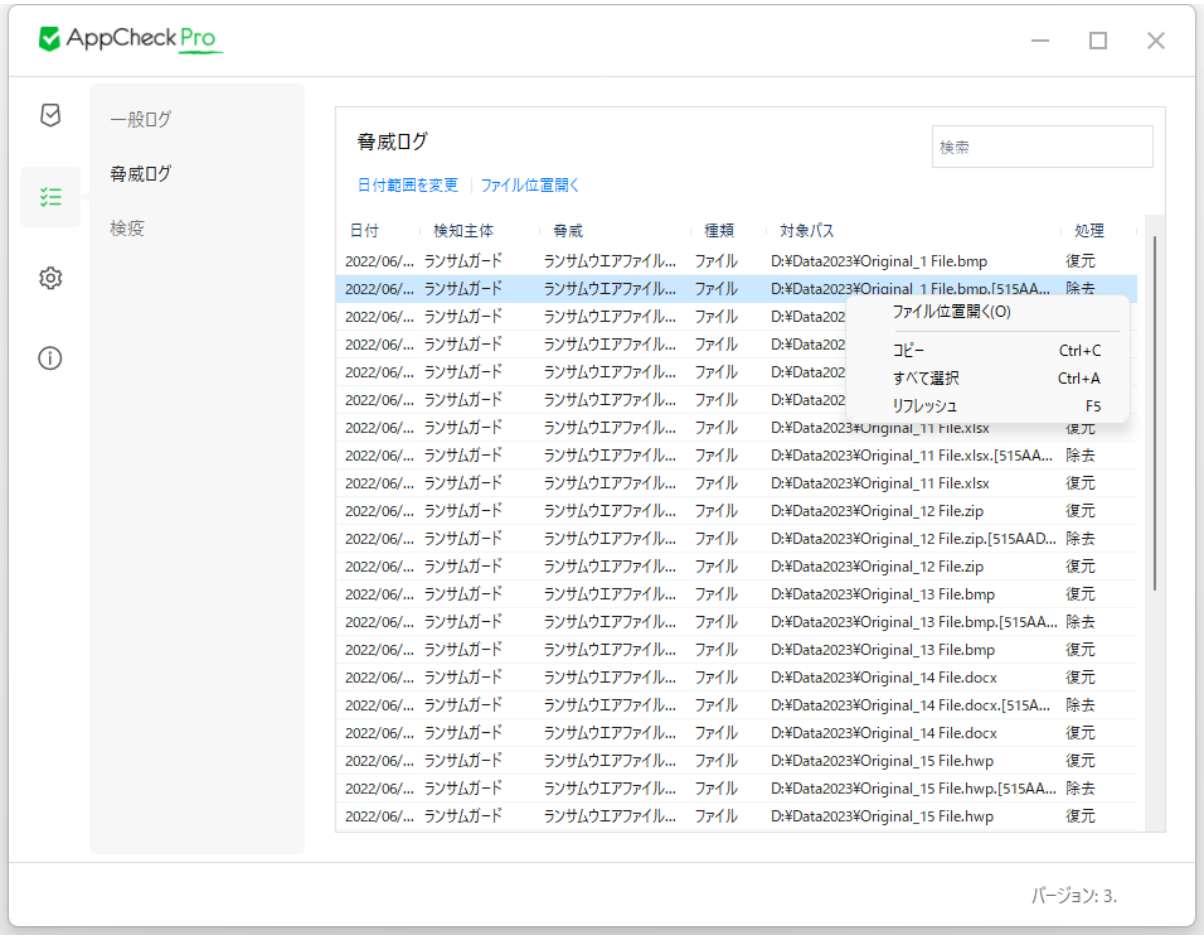


⊙ **遮断 ：** ランサムウェア動作検知、MBR保護で検知されたプロセス(ファイル)とIPアドレス、脆弱点ガードで検知された応用プログラムを遮断します。

⊙ **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いるか、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。

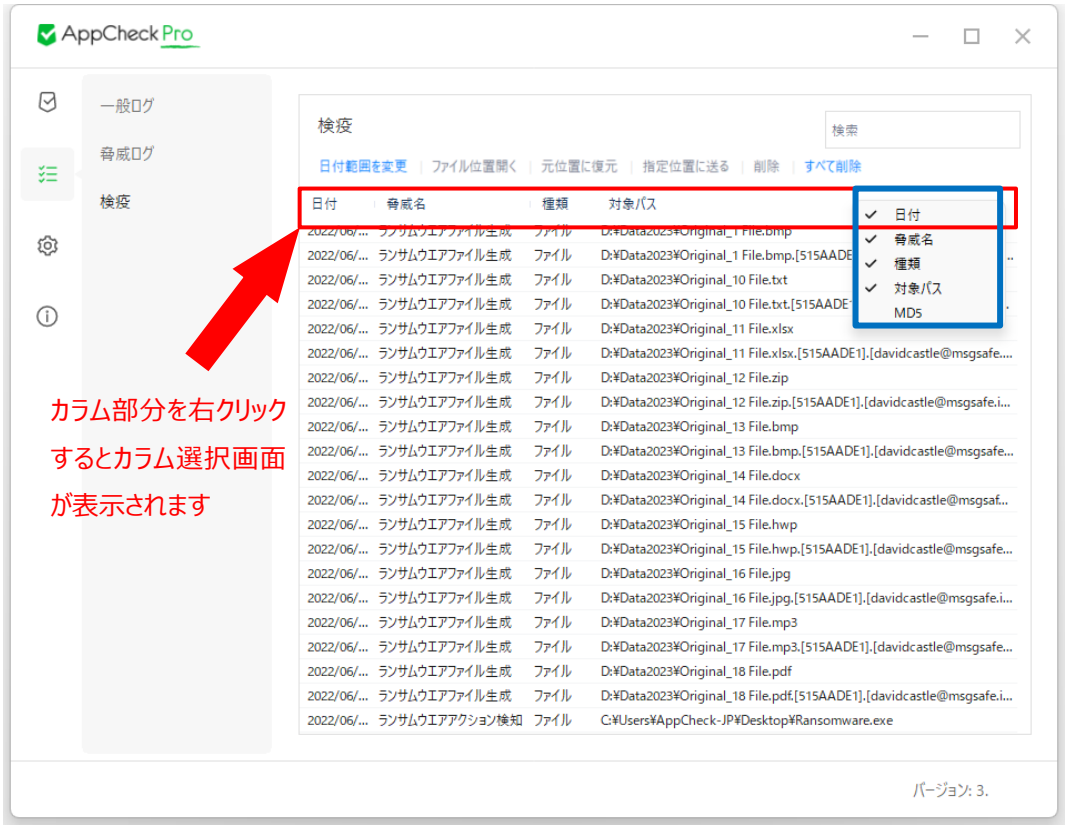
3.3.3 検疫ログ

検疫は、ランサムウェア動作検知により除去され、検疫フォルダ(C:¥ProgramData¥CheckMAL¥AppCheck¥Quarantine)に隔離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に隔離された項目を復元することができます。

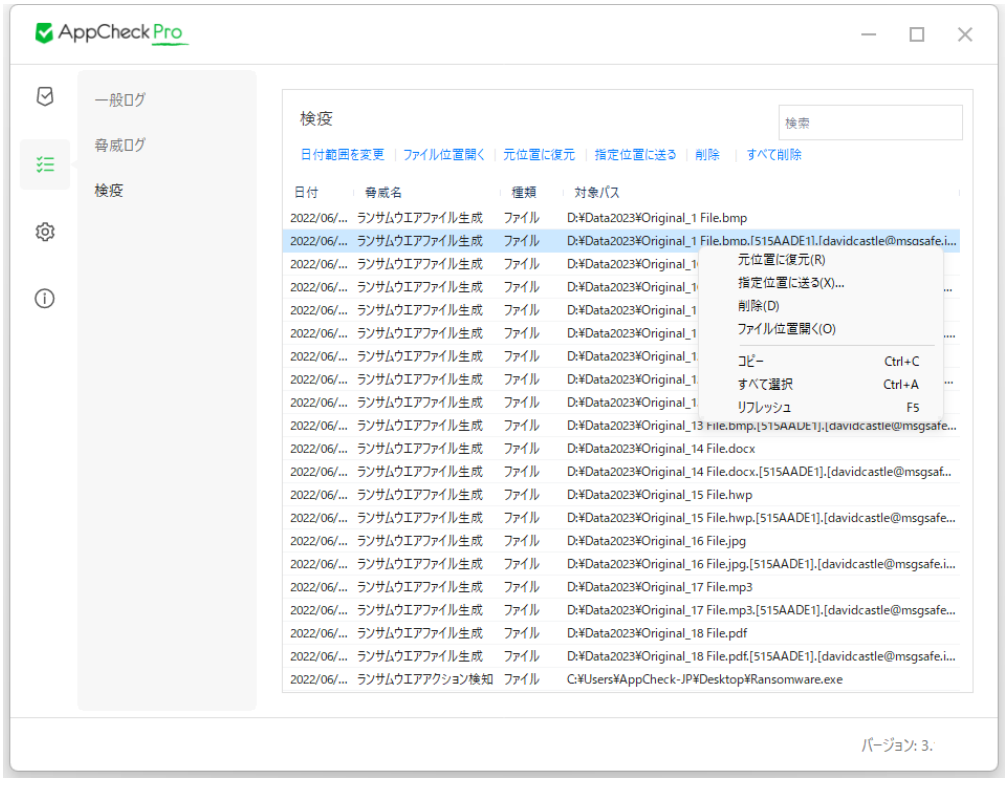
検疫の「日付範囲を変更」メニューにより、特定期間内に記録された検疫ログをフィルタリングして確認することができます。

- **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/昇順に整列できます。



検疫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。

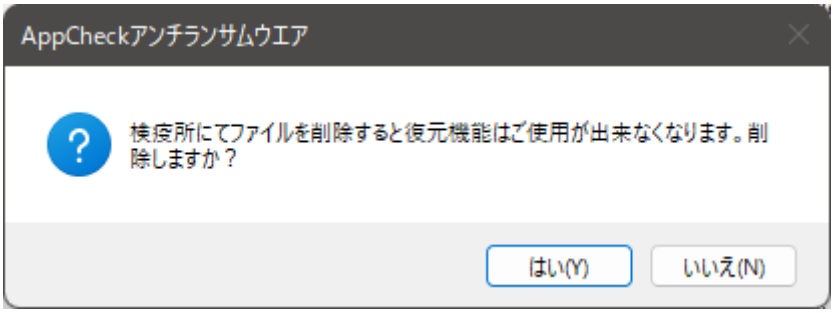


⊙ **元位置に復元 ：** 選択したファイルを元の位置（フォルダ）に復元します。

⊙ **指定位置に送る ：** 選択したファイルをユーザーが指定した位置（フォルダ）に保存します。

⊙ **削除 ：** 検疫フォルダに隔離されているファイルを削除します。

⊙ **すべて削除 ：** 検疫フォルダに隔離されているファイルをすべて削除します。



検疫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。

※「検疫」ログには、ランサムウェア動作検知により隔離されたファイルや日時などの情報が記録されます。
また、検疫所フォルダ(C:¥ProgramData¥CheckMAL¥AppCheck¥Quarantine)には隔離されたファイルの情報がHASH値として保存されており、大量のファイルが検疫されることでディスク容量を圧迫する可能性があります。
そのため、状況に応じて検疫ログから削除し、必要に応じて元の場所へ復元することで、フォルダの管理を適切に行っていただきますようお願いいたします。

⊙ **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。

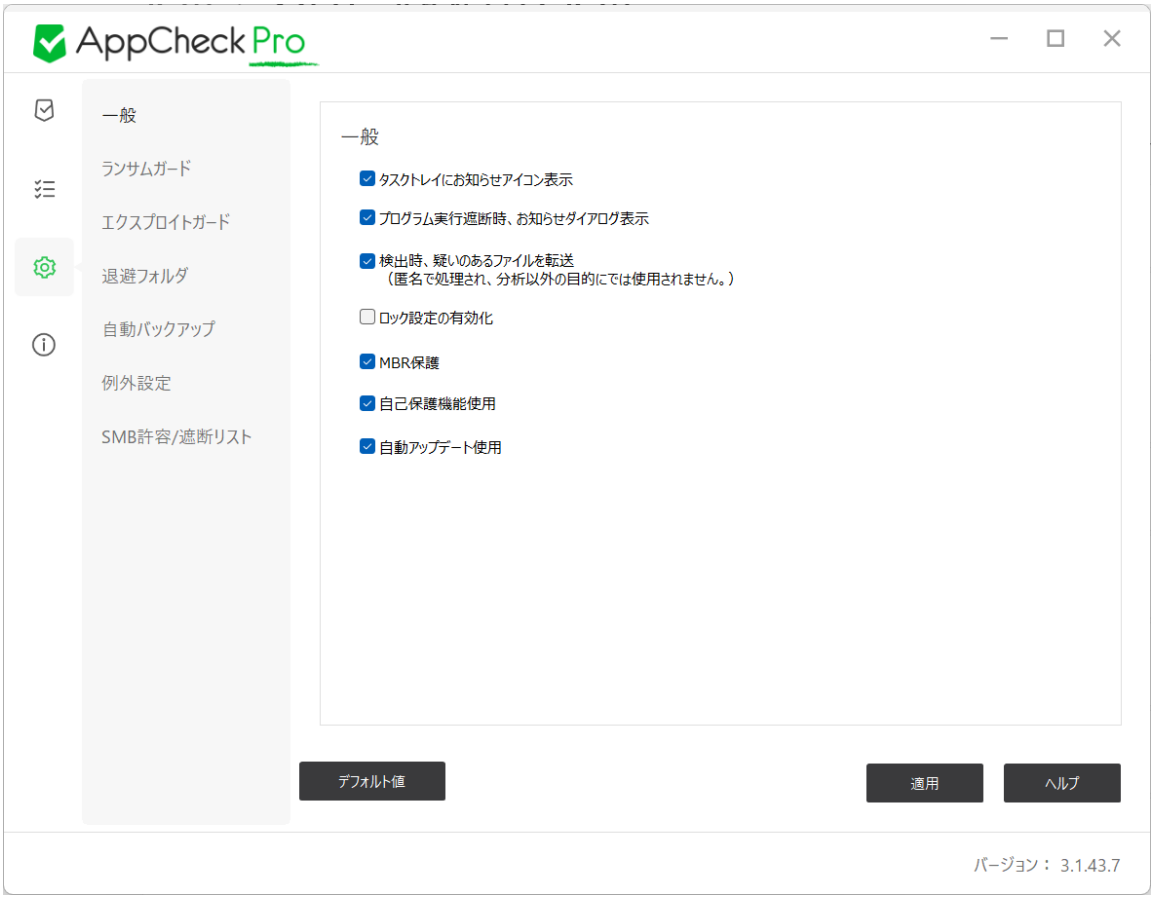
⊙ **コピー（Ctrl+C）：** 選択した項目の検疫ログの詳細情報をコピーします。

⊙ **すべて選択（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。

3.4 オプション

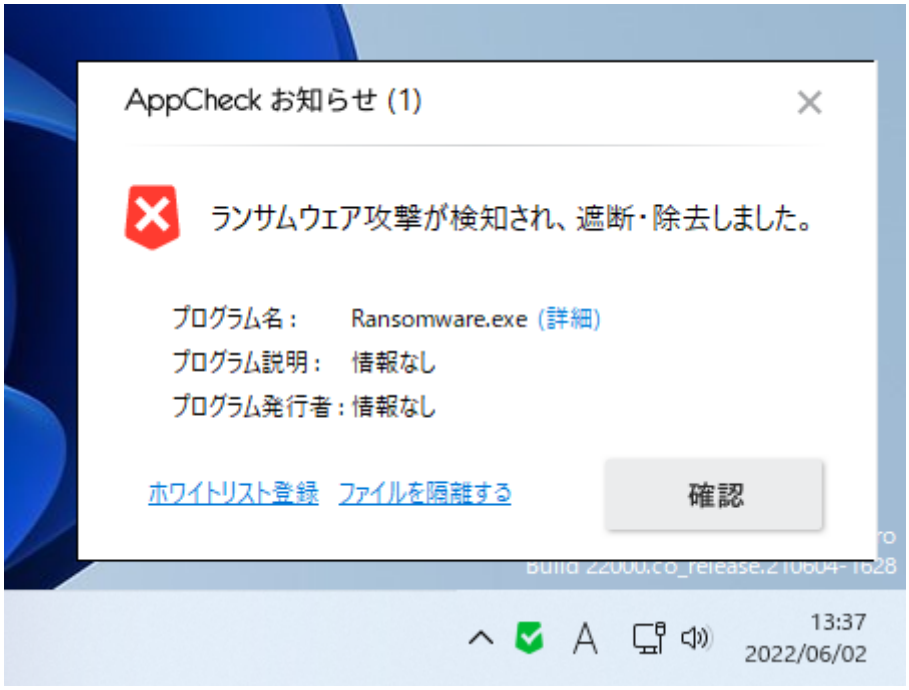
3.4.1 一般



⊙ **タスクトレイにお知らせアイコン表示 ：** 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、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転送(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

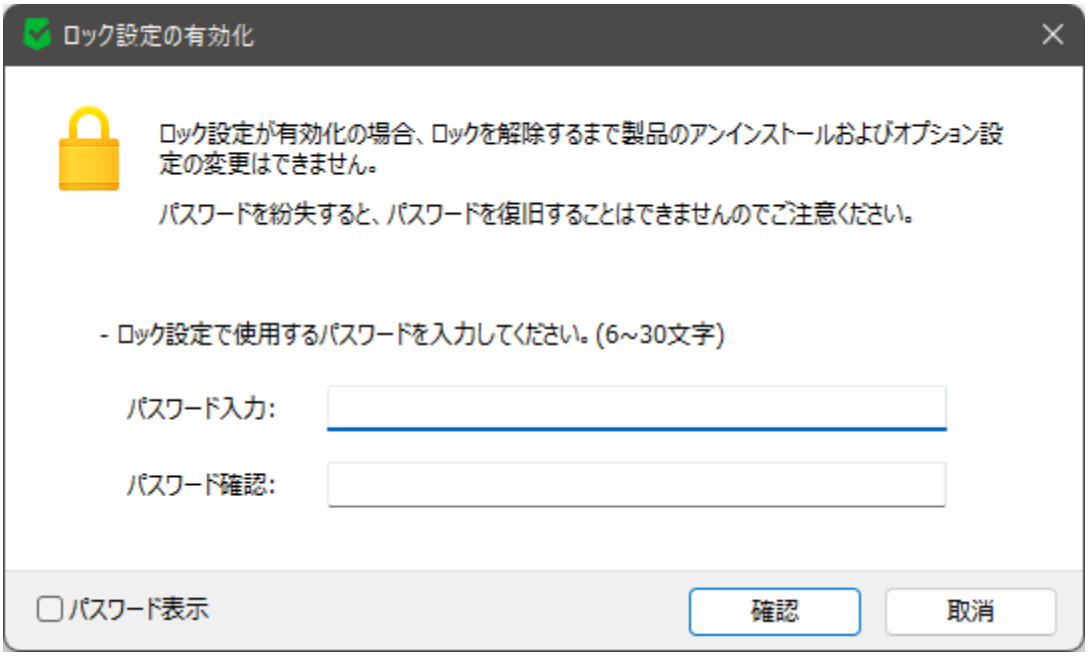
⊙ **MBR保護 ：** MasterBootRecord(MBR)領域内のファイルを毀損しようとするファイルの実行遮断(検知されたファイルは遮断のみ行い、再度実行されたら削除する

⊙ **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）
※権限奪取によるアプリ機能停止・アンインストール等の攻撃に対応できるように、「ロック設定」を有効化にして設定しておくことを推奨しております。

ただし、CMS有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。

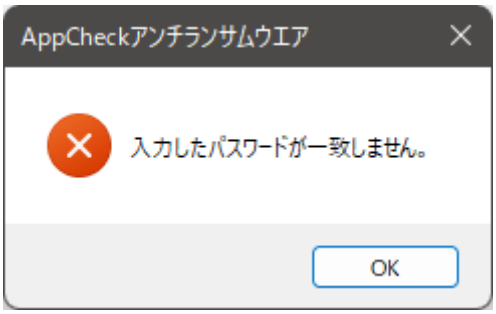
ロック設定の際には「6~30桁の暗証番号」の設定が必要であり、パスワードを紛失した場合は復旧できません。



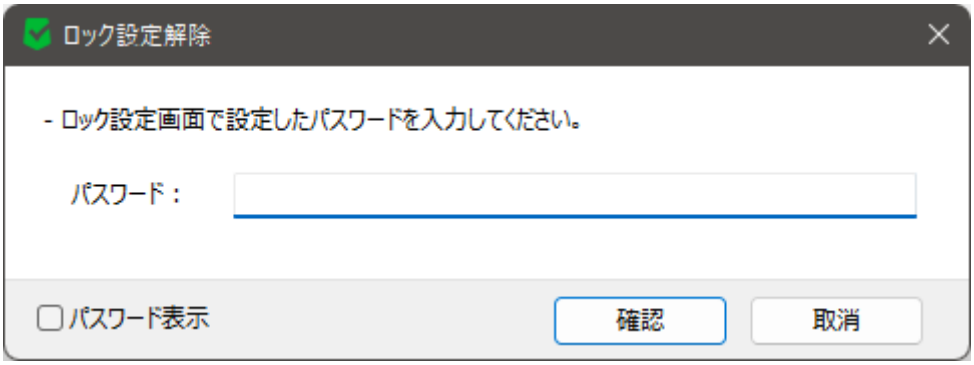
入力したパスワードを確認するためには、「パスワード表示」ボックスにチェックし、「確認」を押してください。

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。

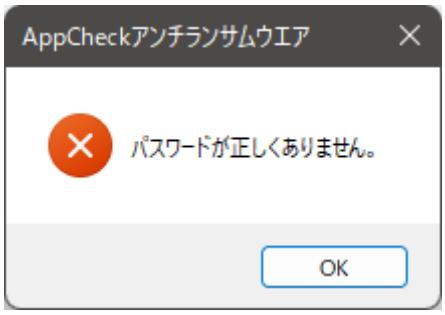
ロック設定に使用するパスワードを入力した後、パスワード確認欄に再入力したパスワードが異なる場合、「入力したパスワードが一致しません。」という通知メッセージが表示されます。



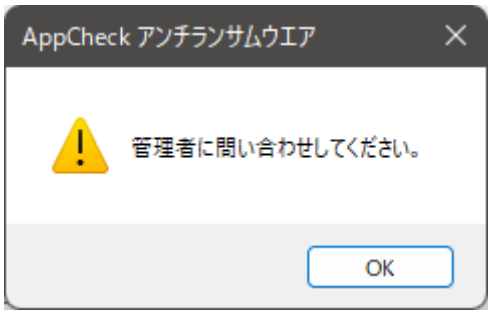
ロック設定が適用された環境でAppCheckオプションメニュー接続時にロック設定解除のためのパスワード入力ウィンドウが表示されます。



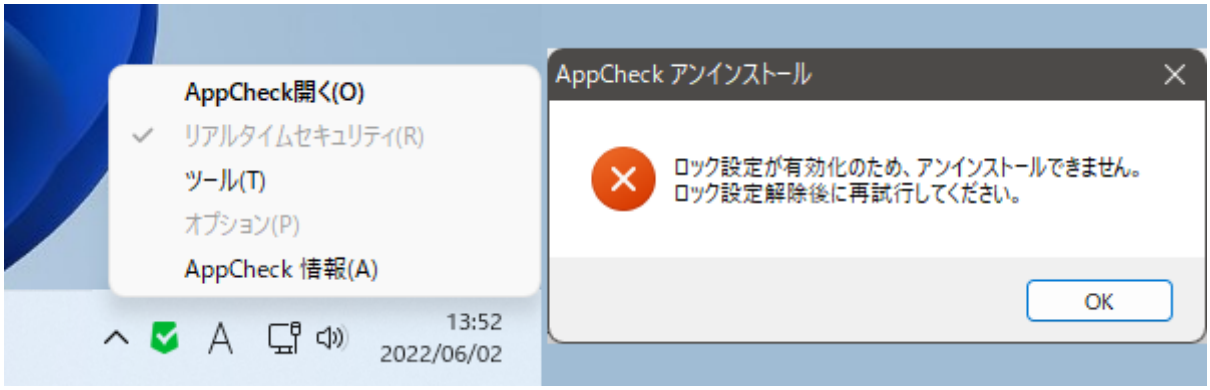
入力したパスワードが間違った場合は、「パスワードが正しくありません。」という通知メッセージが表示されます。



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、「管理者に問い合わせしてください。」という通知メッセージが表示されます。



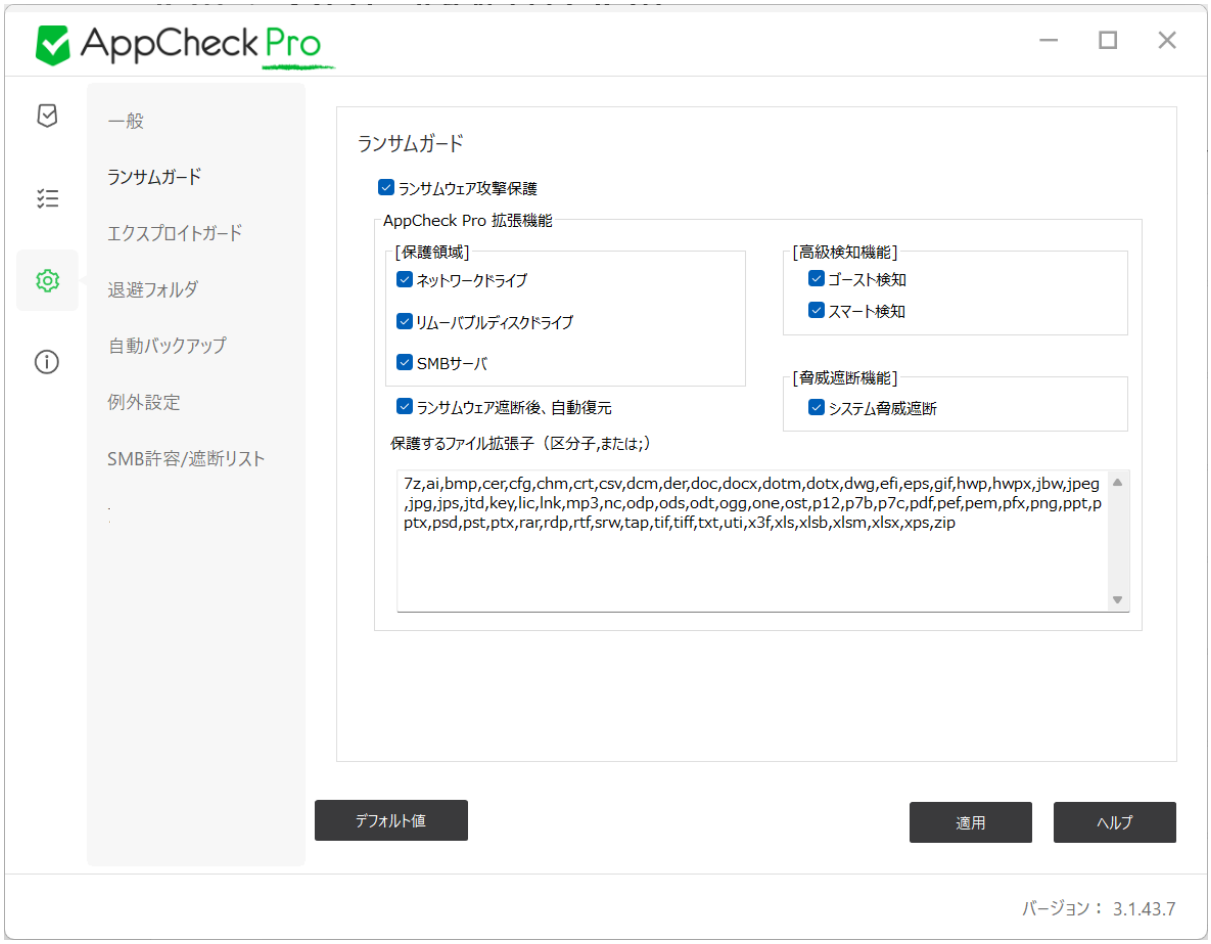
ロック設定の使用またはCMS有は、リアルタイムセキュリティのOFFと、AppCheckProのアンインストールができません。（※CMS中央管理ポリシーで、「アプリケーション削除許可」設定により、AppCheck削除許可設定可能）



- **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。

3.4.2 ランサムガード



⊙ **ランサムウェア攻撃保護：** 保護するファイル拡張子に該当するファイルが毀損された場合、毀損を行ったプロセスを遮断します。

⊙ **AppCheck Pro拡張機能 ： ネットワークドライブ**

AppCheckがインストールされている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(マウントされている)ドライブ内のファイルを毀損した場合、該当プロセスを遮断し、毀損されたファイルの復元を行います。

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

AppCheckがインストールされているPCで実行されたランサムウェアが、USBポートで繋がっているリムーバブルディスク内のファイルを毀損した場合、該当プロセスを遮断し、毀損されたファイルの復元を行います。

⊙ **AppCheck Pro 拡張機能 ： SMBサーバ**

AppCheckがインストール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として繋がっているAppCheckインストール済みPC内のファイルを毀損した場合、遠隔地のIPアドレスを1時間の間遮断し、毀損されたファイルは復元します。

⊙ AppCheck Pro拡張機能 ： ランサムウェア遮断後、自動復元

ランサムウェア検知後、該当行為を行った悪性ファイルを削除します。 ただし、有効なデジタル署名を持つファイル、もしくはシステムフォルダに存在するファイルは削除しません。

⊙ AppCheck Pro 拡張機能 ： 高級検知機能 - ゴースト検知

AppCheckがインストールされているPCのメモリ内に「ゴーストファイル」を配置し、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、より早い段階で検知が行われるようにする機能です。

⊙ AppCheck Pro 拡張機能 ： 高級探知機能 - スマート検知

ランサムウェアの中で、毀損プロセスを実行し、少数のファイルのみ暗号化して終了、再実行を繰り返す動作をするものも正常に検知、復元を行う検知方式となります。

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

Windowsのロールバック（復元）機能関連ファイルを、ランサムウェア攻撃から保護する機能です。

⊙ AppCheck Pro 拡張機能 ： 保護するファイル拡張子(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子は、総65種となります。

(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。

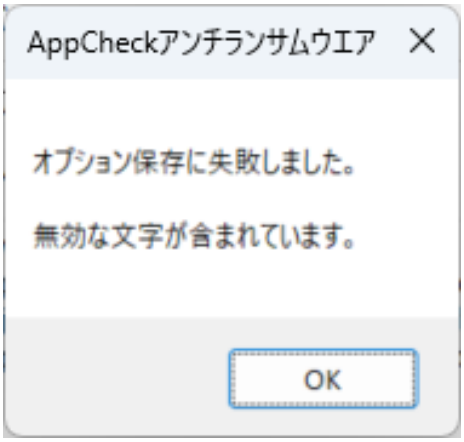
※注意事項

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、「無効な文字が含まれています。」という通知メッセージが生成され、適用することができません。

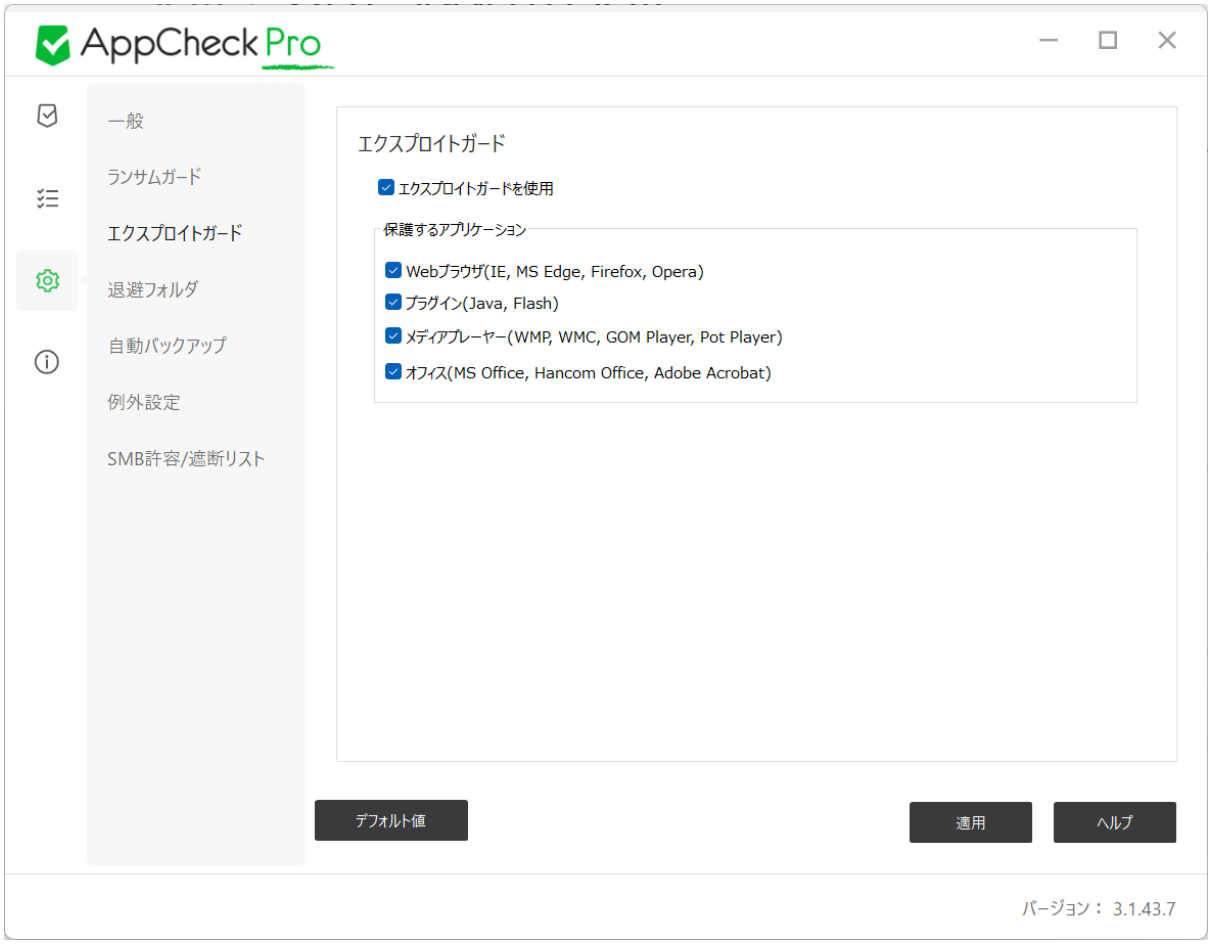


⊙ **デフォルト値 ：** ランサムガード内の設定内容を全て初期値に戻します。

3.4.3 エクスプロイトガード

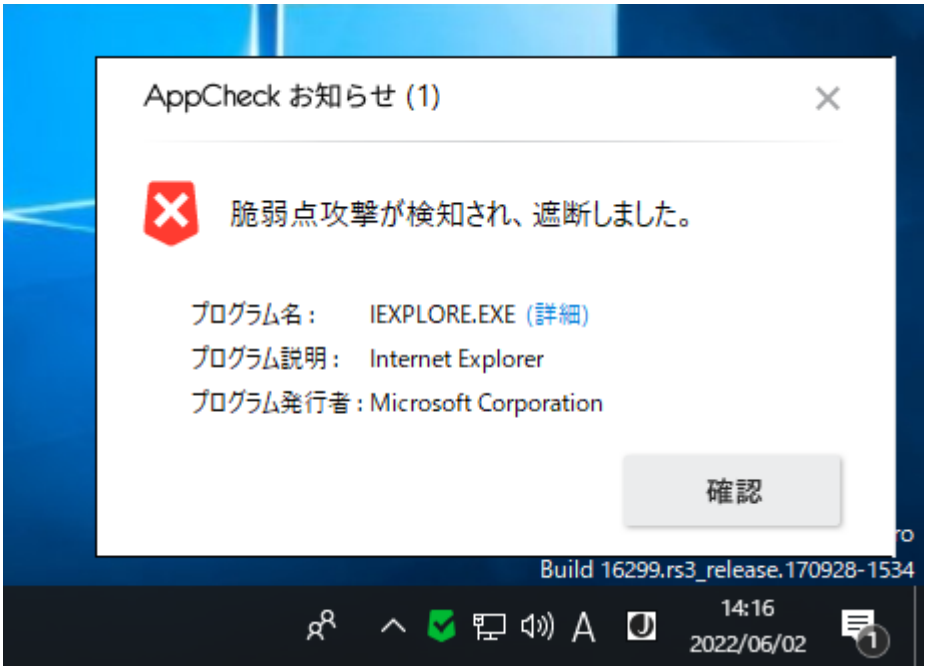
エクスプロイトガードは保護対象にするアプリケーションの脆弱性攻撃が行われる場合、脆弱性攻撃を事前に遮断し、予防する保護機能です。

対象にするアプリケーションのうち、オフィス(Microsoft Office)プログラムはAppCheck Pro有償版でのみ有効化にすることができます。



ウェブブラウザ	Internet Explorer, Microsoft Edge, Firefox, Opera
プラグイン	Java, Flash
メディア再生機	Windows Media Player, Windows Media Center, GomPlayer, PotPlayer
オフィス	Microsoft Office, ハンコムオフィス, Adobe Acrobat

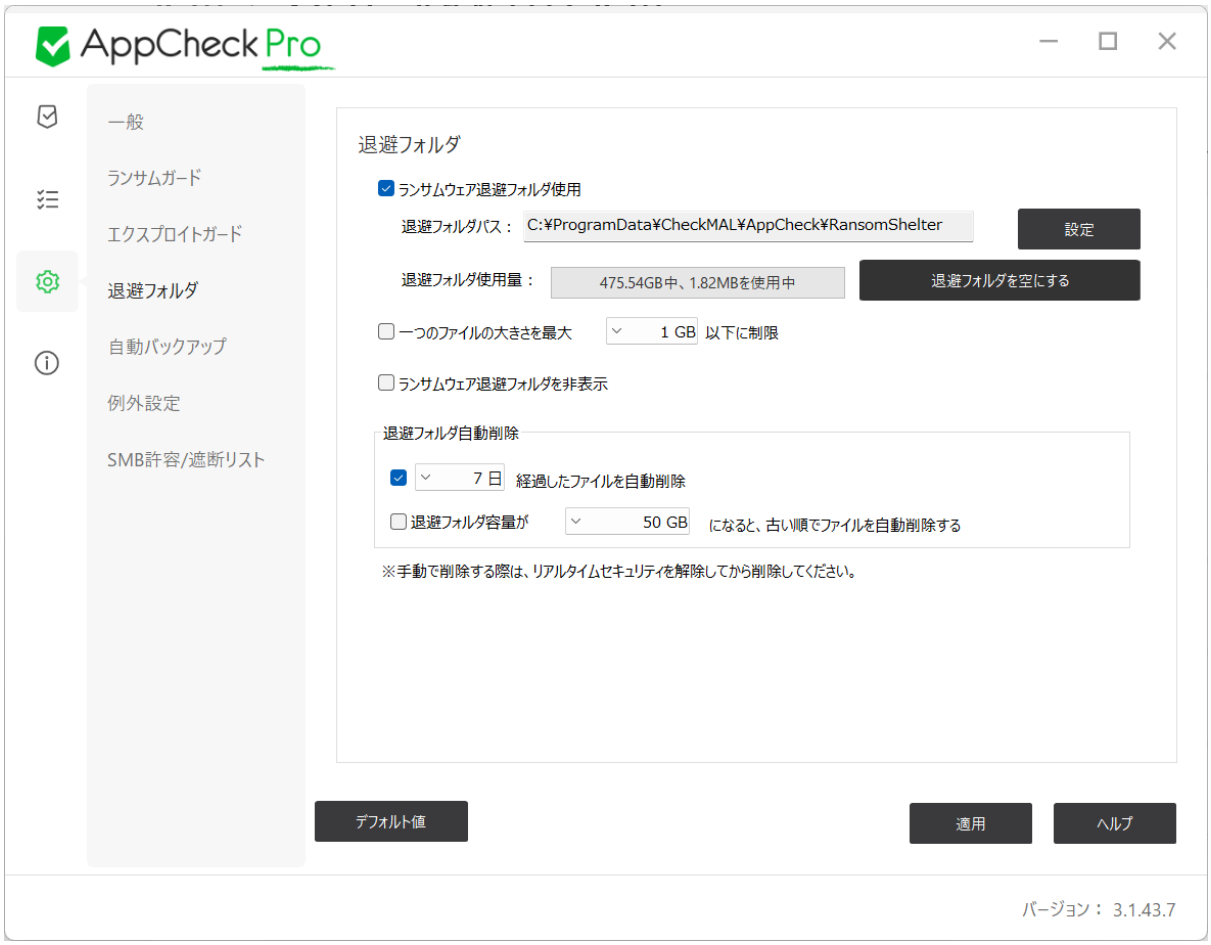
脆弱性攻撃検知が発生した場合、検知されたアプリケーションをご確認ください。Windowsアップデート等を通じて、最新のセキュリティパッチ適用および各アプリケーションの最新バージョンを確認して最新にバージョンにアップデートして脆弱性をなくすようにしてください。



- **プログラム名 ：** 脆弱性攻撃を検知して遮断された保護するアプリケーションの実行ファイル名
- **プログラム名(詳細) ：** 「ツール - 脅威ログ」メニューに自動接続
- **プログラム説明 ：** 脆弱性攻撃を検知して遮断されたファイル属性に表示されたファイル説明値
- **プログラム発行者 ：** 脆弱性攻撃を検知して遮断されたファイルのデジタル署名

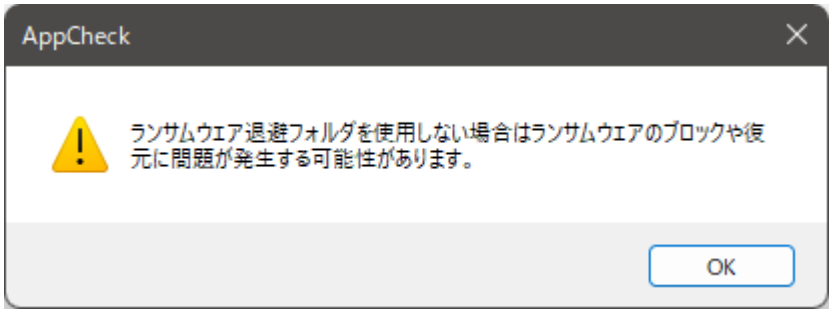
⊙ **デフォルト値 ：** エクスプロイトガード内の設定内容を全て初期値に戻します。

3.4.4 退避フォルダ



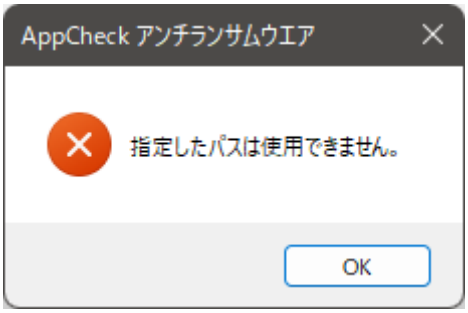
⊙ **ランサムウェア退避フォルダ使用 ：** 保護するファイル拡張子に該当するファイルが、特定条件によって変更、削除される場合、処理直前に変更前の正常状態として「退避フォルダ」に該当ファイルをバックアップしておきます。その後、ランサムウェアの検知、遮断後に「退避フォルダ」から元の場所に自動復元を行います。

「ランサムウェア退避フォルダ」機能をOFFにすると、「ランサムウェア退避フォルダを使用しない場合はランサムウェアのブロックや復元に問題が発生する可能性があります。」という警告メッセージが表示されます。

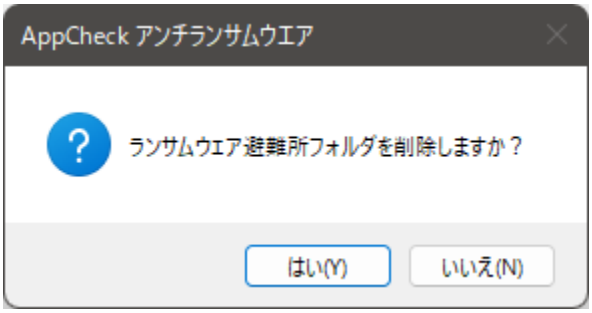


- **退避フォルダパス ：** 退避フォルダの基本パスは、「C:¥ProgramData¥CheckMAL¥AppCheck¥RansomShelter」となり、他の経路への変更も可能です。 ただし、場合によって設定できない経路もございますので

ご了承ください。（「指定されたパスは使用できません。」というメッセージが表示され、他のパスへの変更が必要）



- **退避フォルダ使用量 ：** 退避フォルダパスとして指定されているドライブの全容量の中、退避フォルダに格納されているバックアップファイルの総容量確認ができます。
- **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完全削除します。



「退避フォルダ」内のファイルを手動で削除するには、「AppCheckオプション - 一般 – 自己保護機能使用」のチェックを一時的に解除する必要がございます。

- **1つのファイルの大きさを最大「」以下に制限:** 退避フォルダにバックアップされるファイル一個単位の容量を制限することができます。(100MB, 200MB, 500MB, 1GB, 2GB, 5GB)
- **ランタイムウェア退避フォルダを非表示 ：** 退避フォルダを非表示にすることができます。
- **「○日」経過したファイルを自動削除:** 退避フォルダにバックアップされるファイルが保存され、一定時間「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」経過したら自動削除を行います。(デフォルト：7日)
- **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 ：** 退避フォルダにバックアップされるファイルの全体容量が「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%」に達した場合、古い順で自動削除を行います。(デフォルト：50GB)

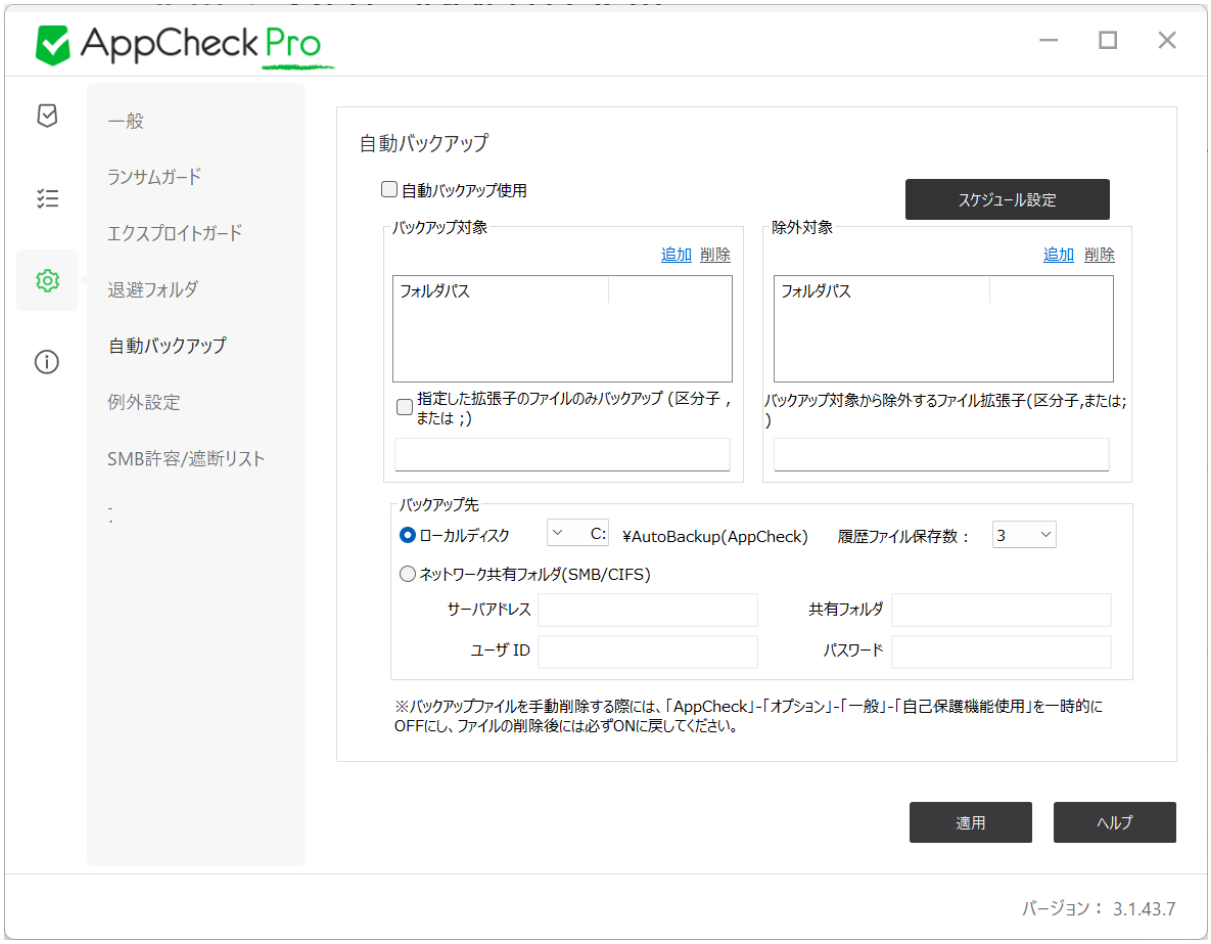
⊙ **デフォルト値 ：** 退避フォルダ内の設定内容を全て初期値に戻します。

3.4.5 自動バックアップ

自動バックアップ機能は、バックアップ対象フォルダを事前指定し、該当フォルダ内の全てのファイルをスケジュール設定によって<AutoBackup(AppCheck)>フォルダにバックアップする機能となります。

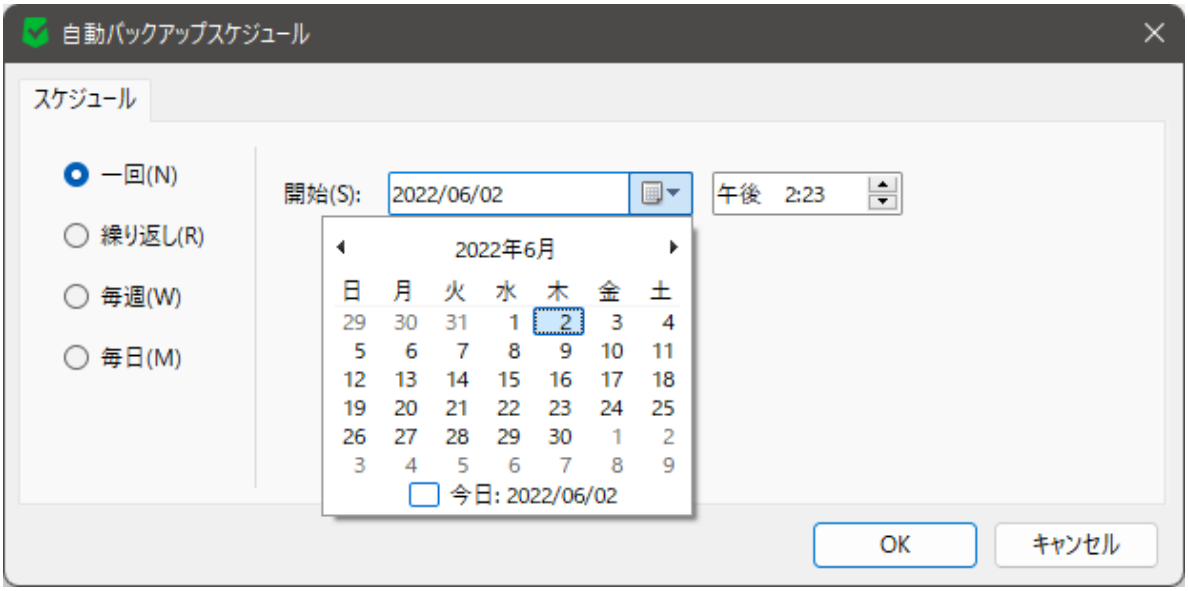
ファイルをヒストリーベースで自動バックアップし、<AutoBackup(AppCheck)>フォルダ内のファイルはランサムウェア攻撃から保護されます。

より安全なバックアップ設定としては、バックアップ先を原本ファイルの元場所とは異なるドライブ上に設定することをお勧めいたします。

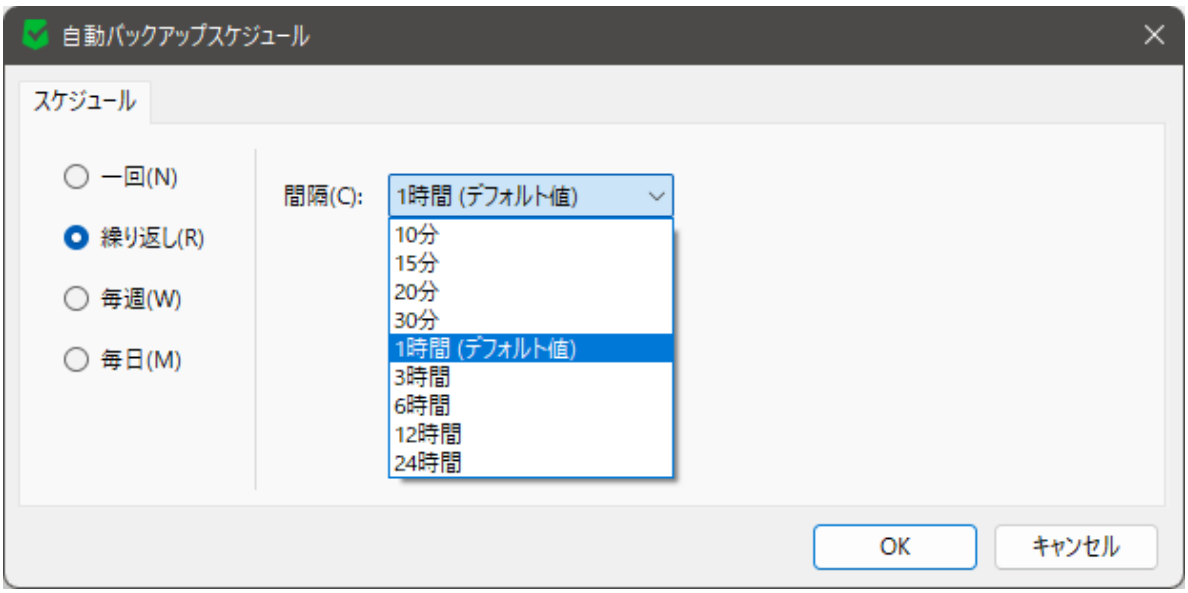


⊙ **スケジュール設定 ：** 一回、繰り返し、毎週、毎月単位で自動バックアップできます。

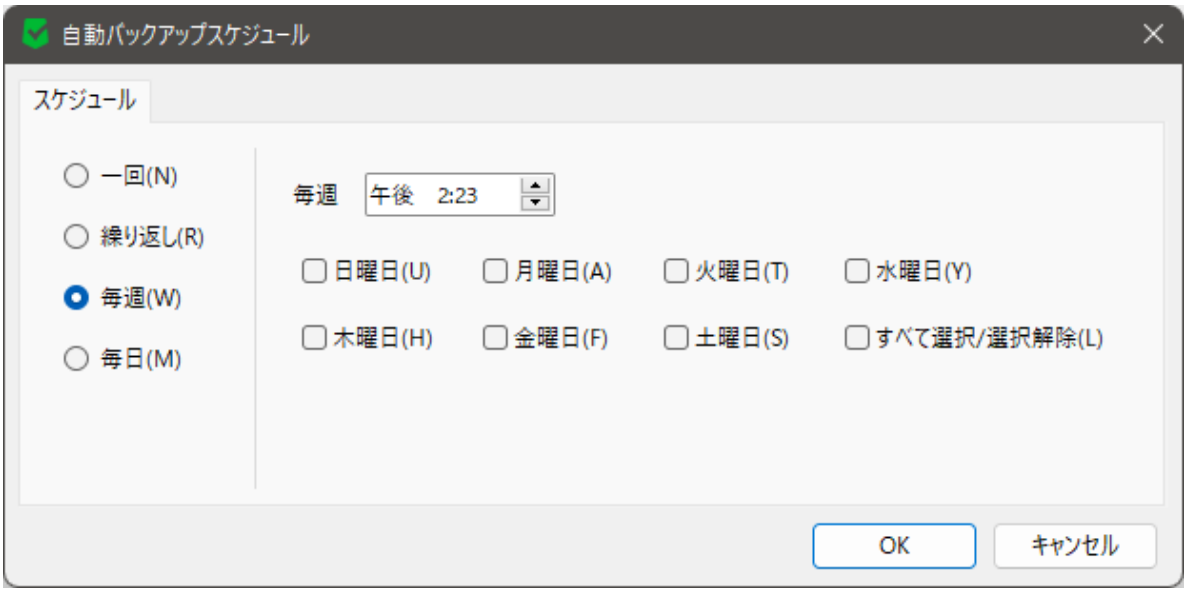
- **一回 ：** 指定した日付と時間に、一回のみの自動バックアップが行われます。



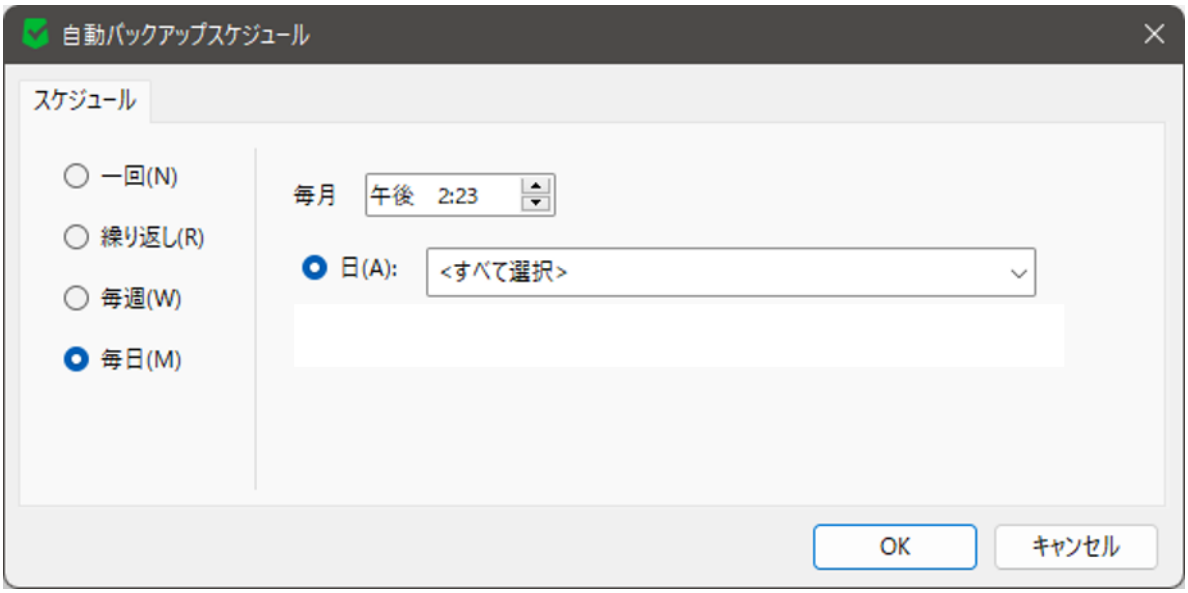
- **繰り返し ：** 10分、15分、20分、30分、1時間（デフォルト）、3時間、6時間、12時間、24時間単位で、定期的な自動バックアップが行われます。



- **毎週 ：** 毎週指定した曜日、時間に定期的な自動バックアップが行われます。



- **毎日 ：** 毎月指定した日、時間に定期的な自動バックアップが行われます。



⊙ **バックアップ対象 ：** バックアップしたいフォルダの追加・削除ができます。

⊙ **指定した拡張子のみバックアップ(区分字,または;) ：** バックアップ対象フォルダ内で、特定した拡張子に該当するファイルのみバックアップを行います。

⊙ **除外対象 ：** バックアップ対象フォルダの下位で、特定したフォルダを指定し、該当フォルダと中のファイルはバックアップされなくすることができます。

⊙ **バックアップ時に除外するファイル拡張子(区分字,または;) :** バックアップ対象フォルダ内のファイルの中、バックアップ対象から除外したいファイルの拡張子を登録することができます。

⊙ **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)から指定できます。

⊙ **ローカルディスク :** PCと物理的に連結されている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ます。選択されているディスクはユーザー様にて変更ができます。

⊙ **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た場合、既存のバックアップファイルは履歴ファイル(.history)に変更されます。履歴ファイル数は0~10個の範囲で設定変更ができます。（デフォルト：3個）

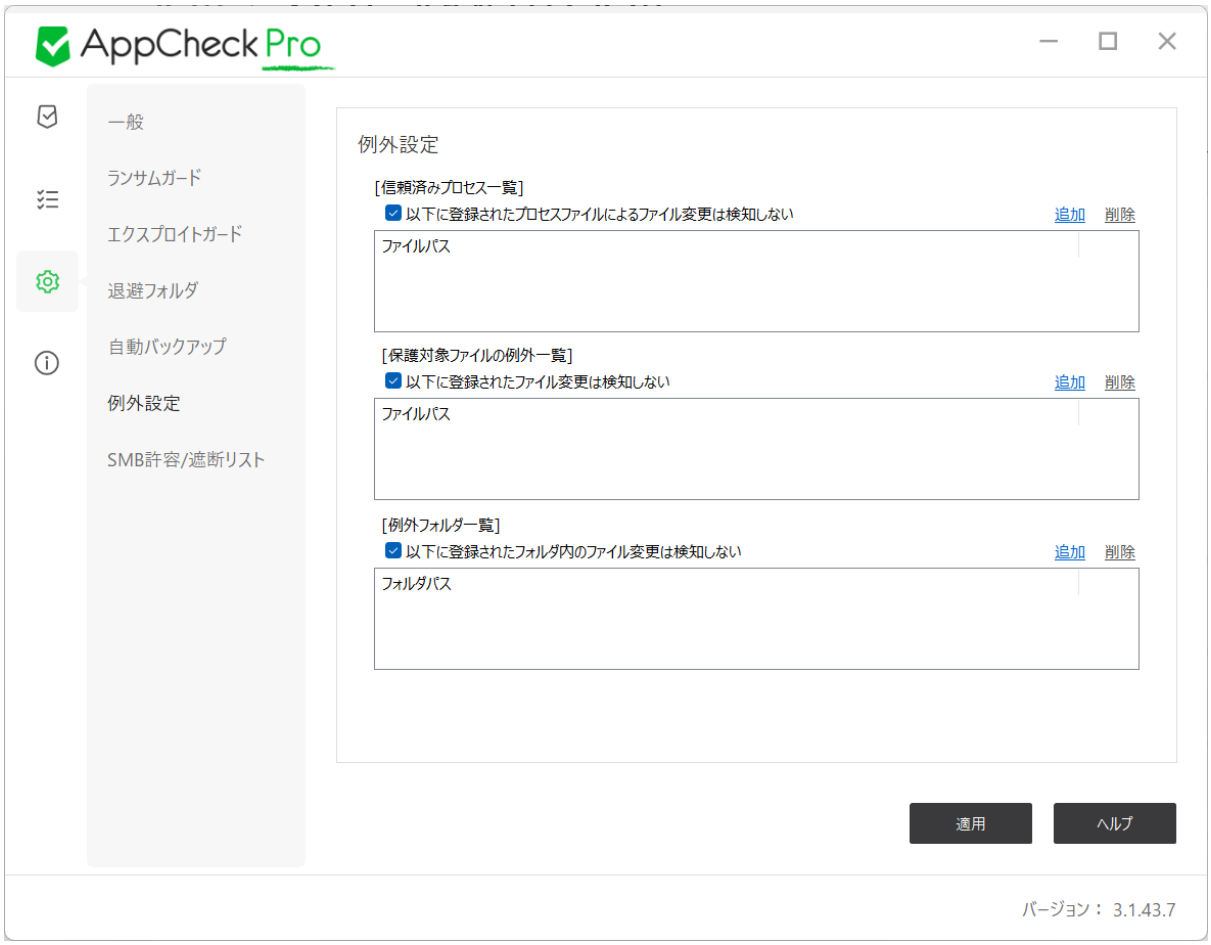
また、履歴ファイルの個数を超える場合は、最も古い履歴ファイルから自動削除されます。

⊙ **ネットワーク共有フォルダ(SMB/CIFS) :** サーバアドレス(IPアドレスまたは遠隔PCのデバイス名)、共有フォルダ(共有設定が行われた遠隔ドライブ/フォルダ名)、ユーザーID、パスワード入力が必要です。

ネットワーク共有フォルダをより安全に運用するためには、常に Windows 最新アップデートを行い、SMB 脆弱性に関する最新セキュリティパッチが適用されるようにしてください。また、共有フォルダへのアクセス権限設定及びアカウント、パスワード管理に気を付けてください。

尚、自動バックアップフォルダ<AutoBackup(AppCheck)>や内部ファイルを削除する際には、"オプション – 一般 – 自己保護機能使用"のチェックを解除し、削除してください。

3.4.6 例外設定



⊙ 信頼済みプロセス一覧

信頼済みプロセス一覧に追加されたファイルに関しては、保護対象となるファイルに変更を行ったとしてもランサムウェアの攻撃として検知されなくなります。ただし、特定した検知条件によっては検知される場合がございます。

注意点としては、一部のランサムウェアは、Windowsシステムファイル(Explorer.exe、svchost.exeなど)をファイル毀損に利用する場合がございますので、システムファイルはなるべく登録しないか、誤検知が発生する一部の端末のみ登録するようにお願いいたします。

・以下に登録されたプロセスファイルによるファイル変更は検知しない ： プロセス登録後には、必ずこちらにチェックを入れるようお願いいたします。

⊙ 保護対象ファイルの例外一覧

保護する拡張子に該当するファイルの中、保護対象ファイルの例外一覧に追加されたファイルに関しては変更されてもランサムウェア攻撃として検知されません。行ったとしてもランサムウェアの攻撃として検知されなくなります。

※検知されないため、退避フォルダへのバックアップ、復元も行われません。

・以下に登録されたファイルは検知しない ： ファイル登録後には、必ずこちらにチェックを入れるようお願いいたします。

⊙ 例外フォルダー一覧

例外フォルダー一覧に登録されているフォルダ内のファイルに関しては、変更されてもランサムウェア攻撃として検知されません。

※検知されないため、退避フォルダへのバックアップ、復元も行われません。

ただし、ネットワークドライブ内のフォルダについては例外設定されないため、検知が行われます。

・以下の登録されたフォルダ内のファイル変更は検知しない ： フォルダ登録後には、必ずこちらにチェックを入れるようお願いいたします。

「保護対象ファイルの例外一覧」または「例外フォルダー一覧」に登録されているファイル、フォルダについては AppCheck の「自動バックアップ機能」として定期的なバックアップを行いますと、より安全なデータ管理ができます。

・登録できる各例外設定パスについて

「信頼済みプロセス一覧」に登録できるプロセスはローカルパスもしくはドライブ文字を付与したネットワークドライブ上の絶対パス(例：¥¥192.168.x.x¥test¥test.exe → Y:¥test¥test.exe)になります。

「**保護対象ファイルの例外一覧**」に登録できるファイルパスはローカルパスのみになります。(ネットワークドライブパスは登録できません。※ドライブ文字を付与しても無効になります。)

「**例外フォルダー一覧**」に登録できるフォルダパスはローカルパスのみになります。(ネットワークドライブパスは登録できません。※ドライブ文字を付与しても無効になります。)

3.4.7 SMBサーバ保護

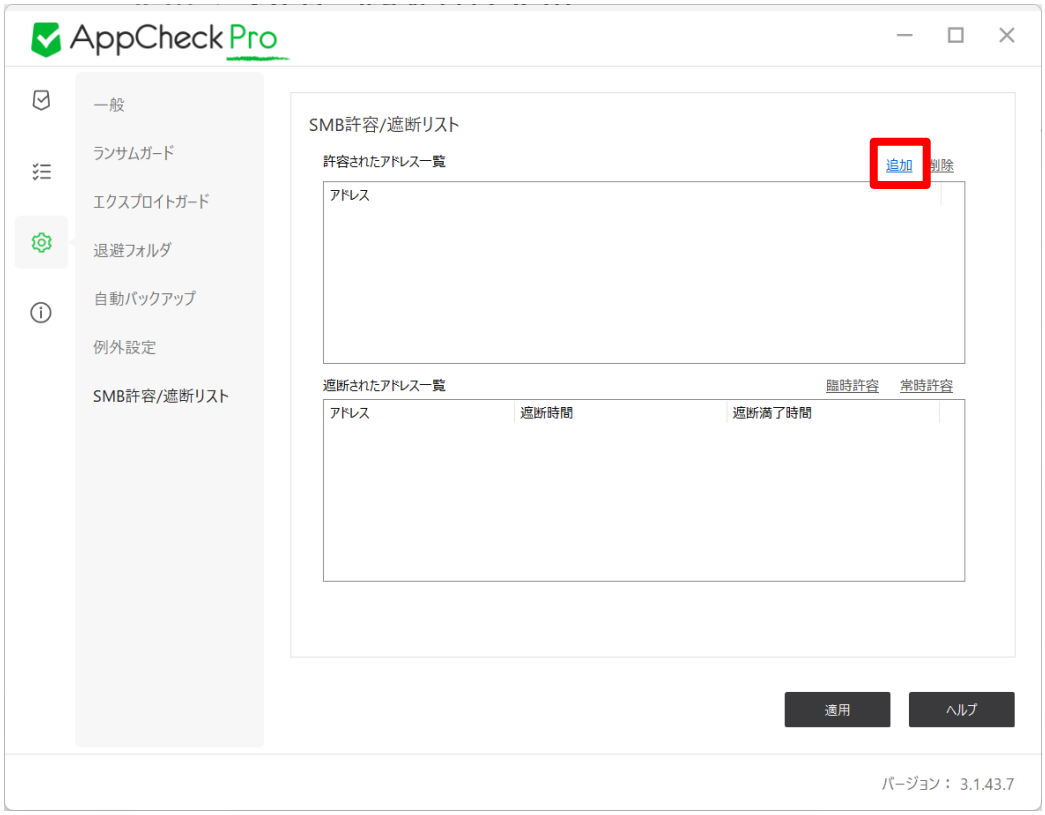
SMBサーバ保護機能は、ネットワークドライブを通じて接続された遠隔地PCからのファイル変更処理を検知し、該当IPアドレス(IPv4、IPv6)からのアクセスを遮断、許容することができます。

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が表示され、該当IPアドレスからのアクセスを一時間の間臨時遮断し、毀損されたファイルに関しては自動復元を行います。

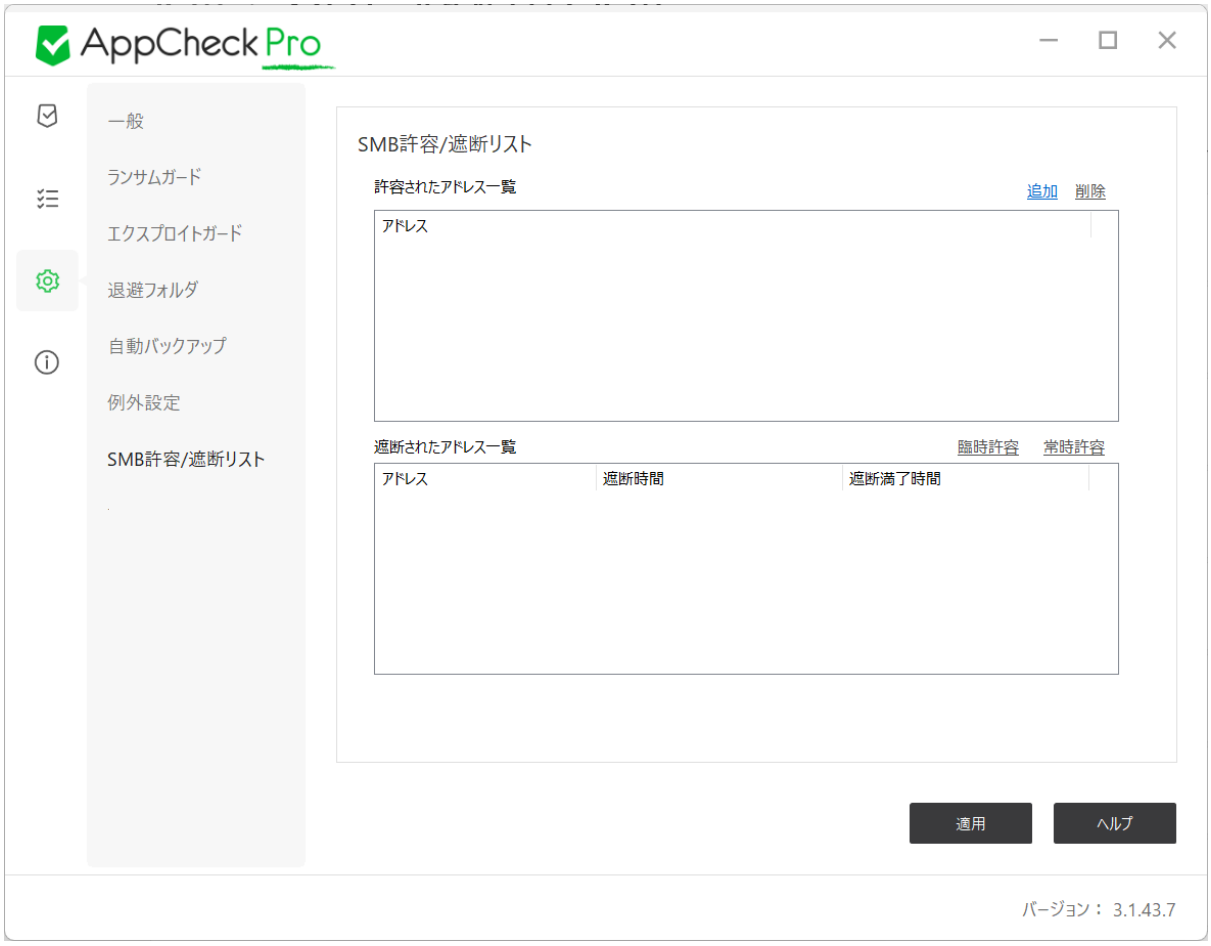
- **IPアドレス(詳細) :** "ツール - 脅威ログ"メニューに移動
- **常時許容 :** 遮断された遠隔地IPアドレスを「常時許容」する(ホワイトリストとして常に許容)
- **臨時許容 :** 遮断された遠隔地IPアドレスを「臨時許容」する(再度検知が発生するまで許容)

※「ロック設定」またはCMS中央管理ポリシーの「ロックモード」が適用されている環境では"常時許容"、"臨時許容"メニューが表示されません。

⊙ 許容されたアドレス一覧



「許可されたアドレス一覧」に直接IPアドレスを追加する際には、追加ボタンをクリックし、IPv4またはIPv6アドレスを個別、順次、全体規則に従って追加するようお願いいたします。



「許可されたアドレス一覧」に追加済みのIPアドレスからのアクセス、ファイル変更に対し、遮断は行われませんが、退避フォルダへの「リアルタイムバックアップ」は行われる場合がございます。

⊙ 遮断されたアドレス一覧

SMB保護機能にて遮断が行われ、「遮断されたアドレス一覧」に登録されたIPアドレスは「1時間のみ」臨時アクセス遮断が行われます。1時間後にはアクセス遮断が解除され、またアクセスが可能となります。

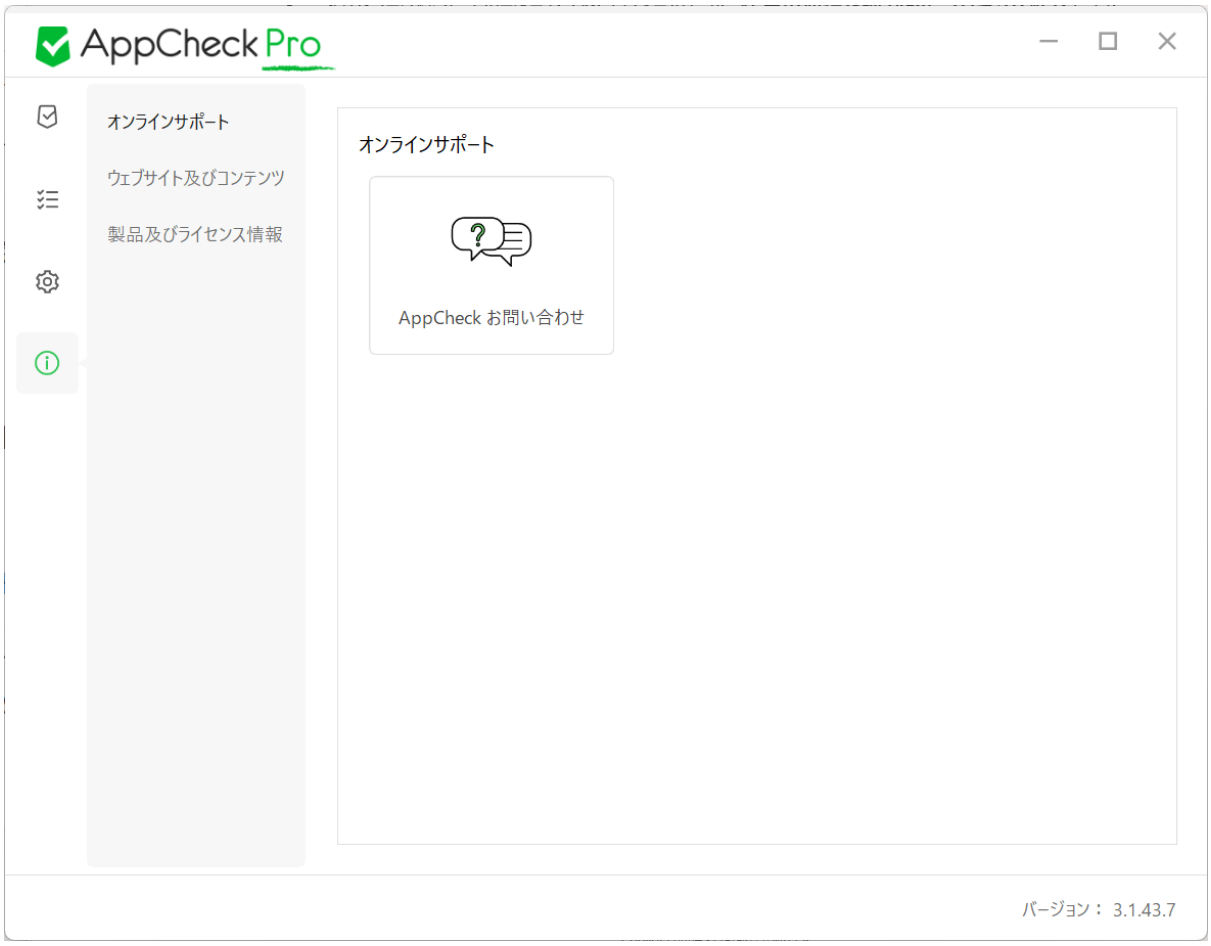
- **追加 ：** 特定したIPアドレスを"許可されたアドレスリスト"に追加し、該当IPアドレスに関しては検知、遮断が行われません。
- **削除 ：** 登録されたIPアドレスを削除することができます。

「遮断されたアドレス一覧」に IP アドレスが追加された状態で、「リアルタイムセキュリティ」機能を OFF にすると、遮断された IP アドレスが許可されます。また、「リアルタイムセキュリティ」を ON にすると、遮断満了時間まで IP アドレスが遮断されるようになります。

ただし、Windows が再起動されたら、遮断満了時間にかかわらず遮断された IP アドレスは自動削除されます。

3.5 カスタマーセンター

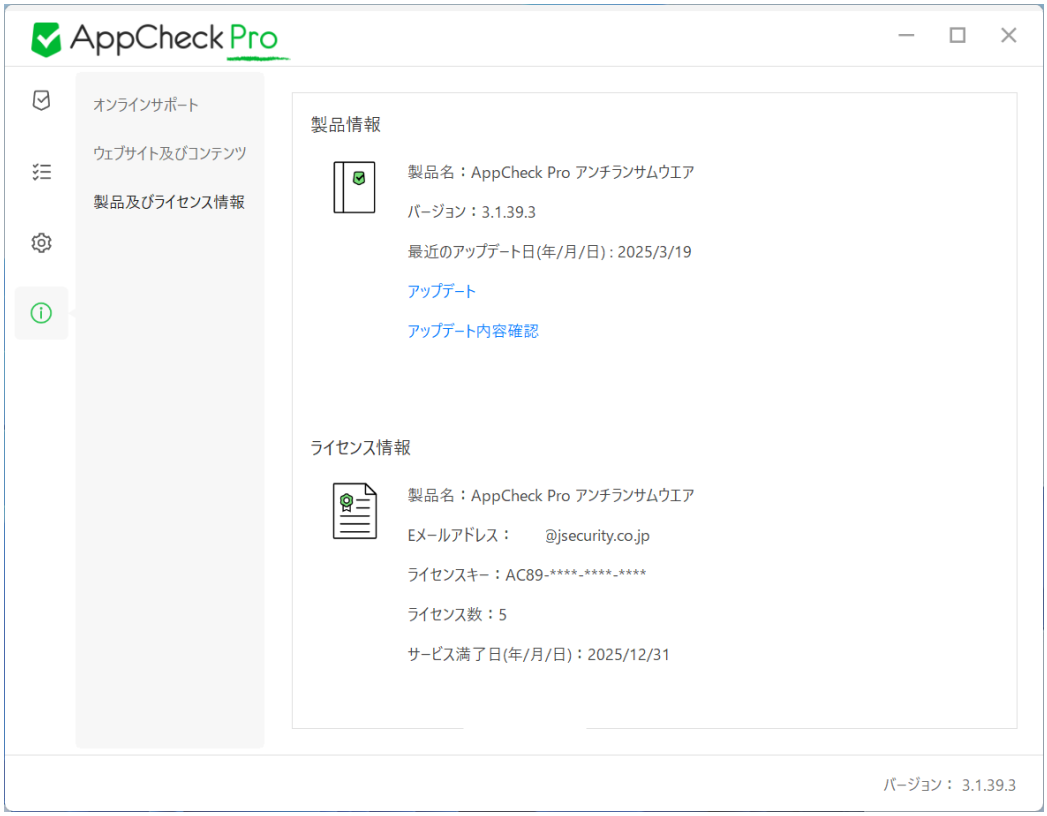
3.5.1 オンラインサポート



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

3.5.2 製品及びライセンス情報

⊙ **製品情報**

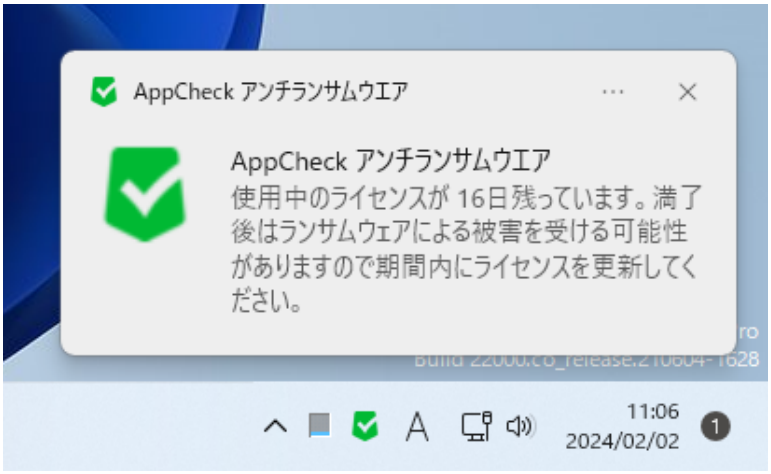


- **製品名 ：** ライセンス登録可否により、AppCheckまたはAppCheckProとして表示
- **バージョン ：** 現在インストールされているAppCheckバージョンが表示
- **最新のアップデート日 ：** 現在インストールされているAppCheckの最新アップデート日を表示
- **アップデート ：** AppCheck最新アップデートの手動実行
- **アップデート内容確認：** AppCheckのリリースノートページに移動

⊙ **ライセンス情報**

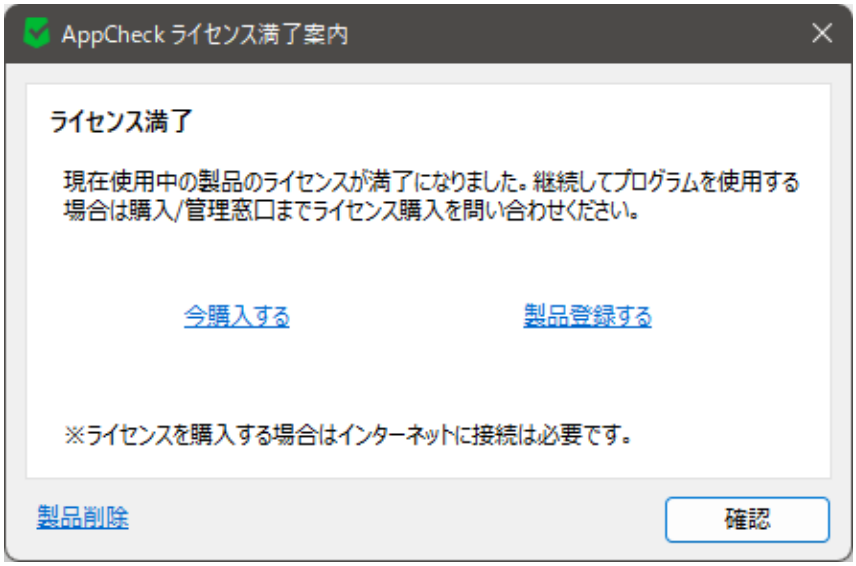
- **製品名 ：** AppCheck Pro アンチランサムウェアとして表示
- **Eメールアドレス ：** ライセンスが付与されたメールアドレスを表示
- **ライセンスキー ：** ライセンスキーを表示
- **ライセンス数 ：** 該当ライセンスキーに付与されているAppCheckPro用ライセンス数(端末数)を表示
- **サービス満了日 ：** 該当ライセンスの満了日を表示

ライセンス満了日の30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。



ライセンスが満了されると、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：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 有である場合は、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・ライセンスキーを登録
- **製品削除 ：** AppCheck をアンインストールする