AppCheck アンチランサムウェア

- CARB(カーブ)エンジン動作確認について -

CHECKMAL

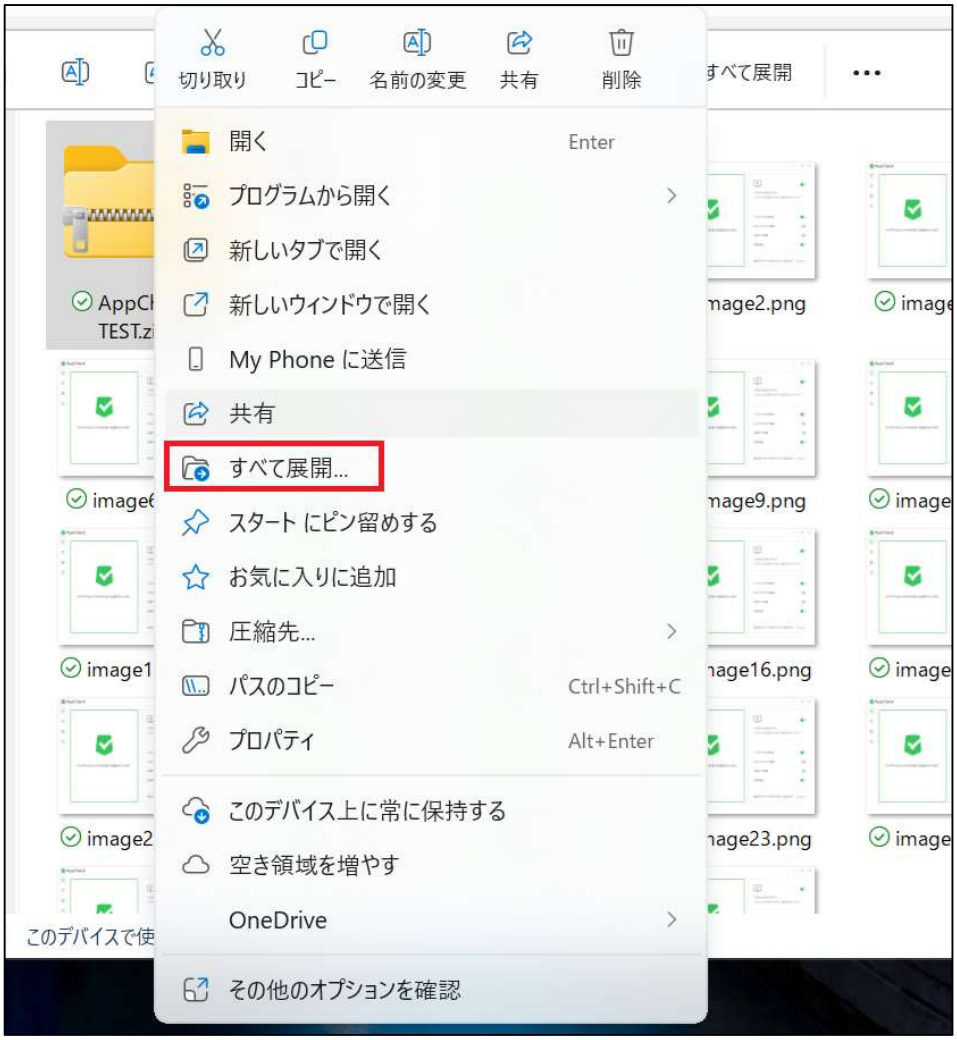
このテストは、AppCheck アンチランサムウェアのCARB(カーブ)エンジンでファイル毀損行為の遮断プロセスをサンプルファイルで行うテストとなります。
このテストは、お客様のシステムに一切影響を与えることはありませんので、どうぞご安心ください。

<用意するもの >

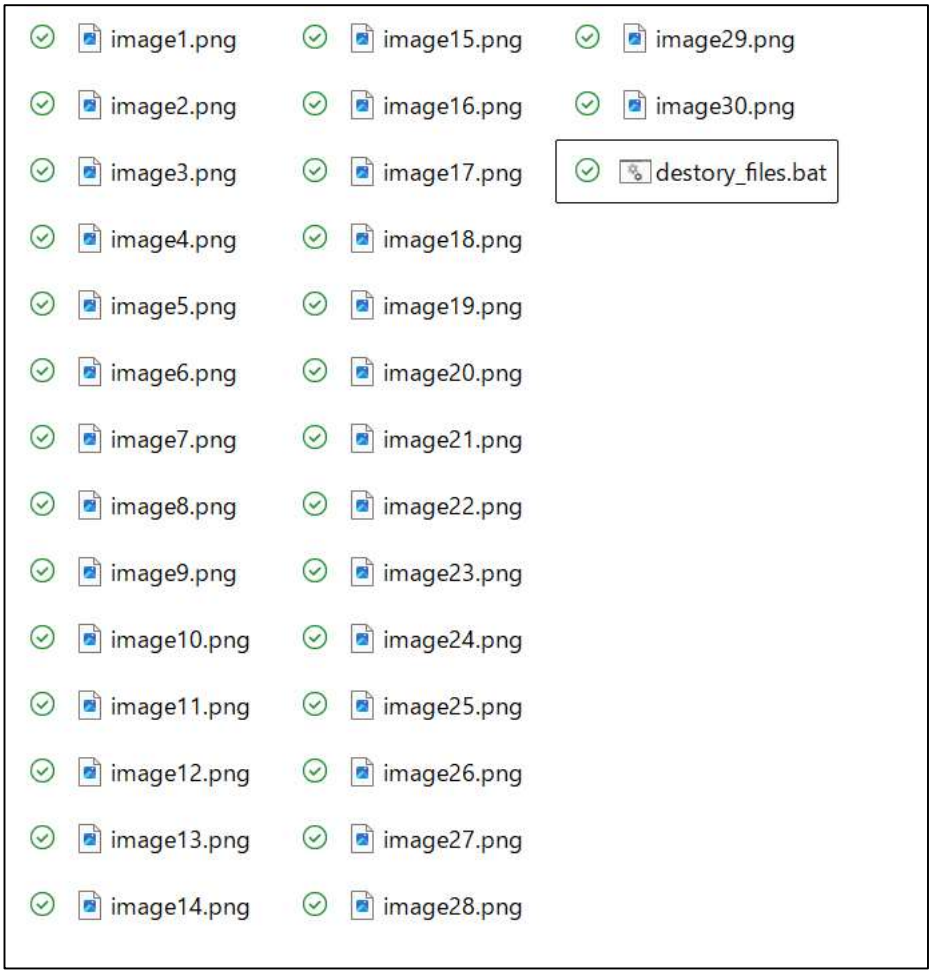
- ✓ **AppCheck Pro アンチランサムウェア**
- ✓ **テスト用ファイル (appcheck_test.zip) :**
  https://www.checkmal.com/download/appcheck_test_jp.zip

1. AppCheck Pro アンチランサムウェアのインストールファイルをダウンロードし、インストールを行ってください。

2. テストファイル(appcheck_test_jp.zip)を任意のフォルダにダウンロードし、解凍してください。



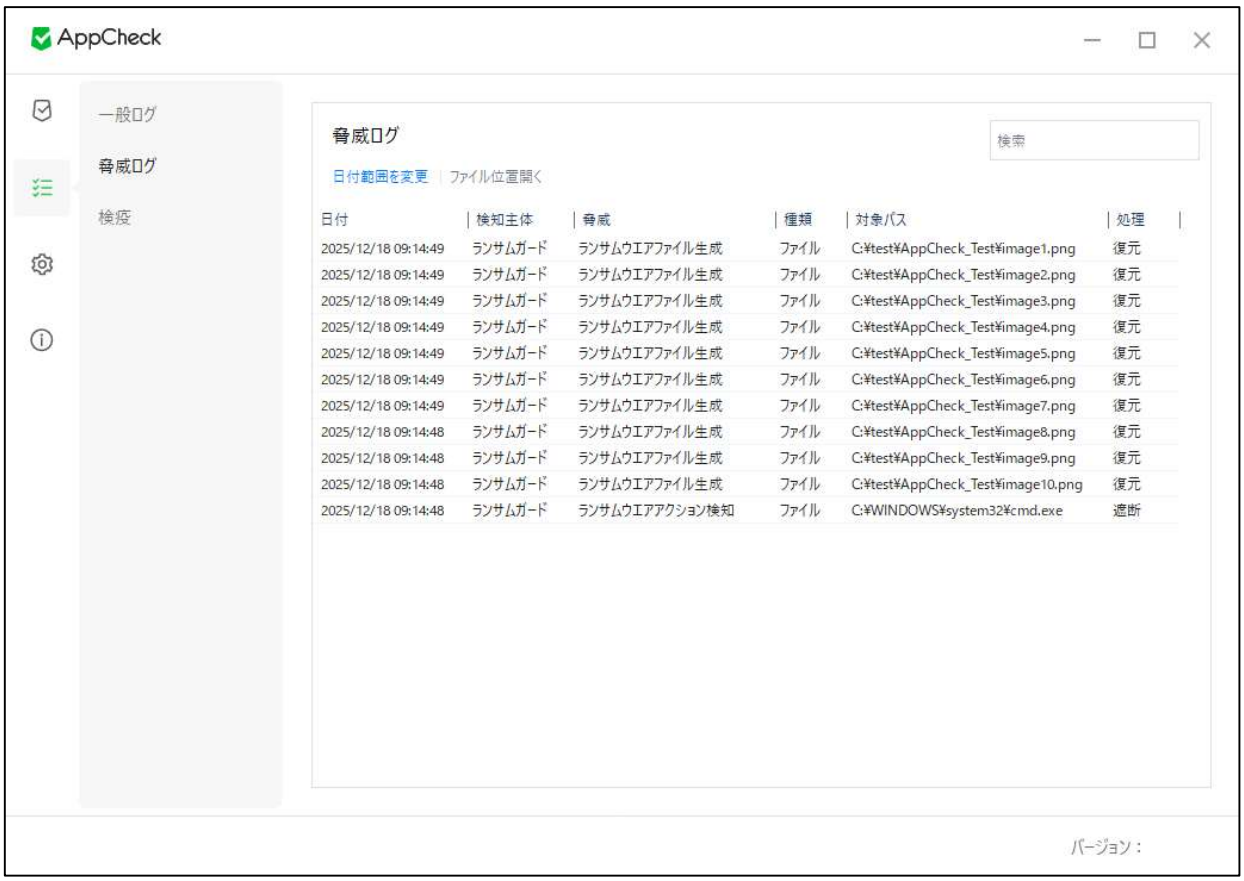
3. 解凍済みのファイルを保存したフォルダには PNG画像ファイル（30個)と「destory_files.bat」バッチファイルが入っています。「destory_files.bat」ファイルは 「echo」の「redirect」コマンドで 30個のPNGファイルを毀損する目的で制作されたものです。

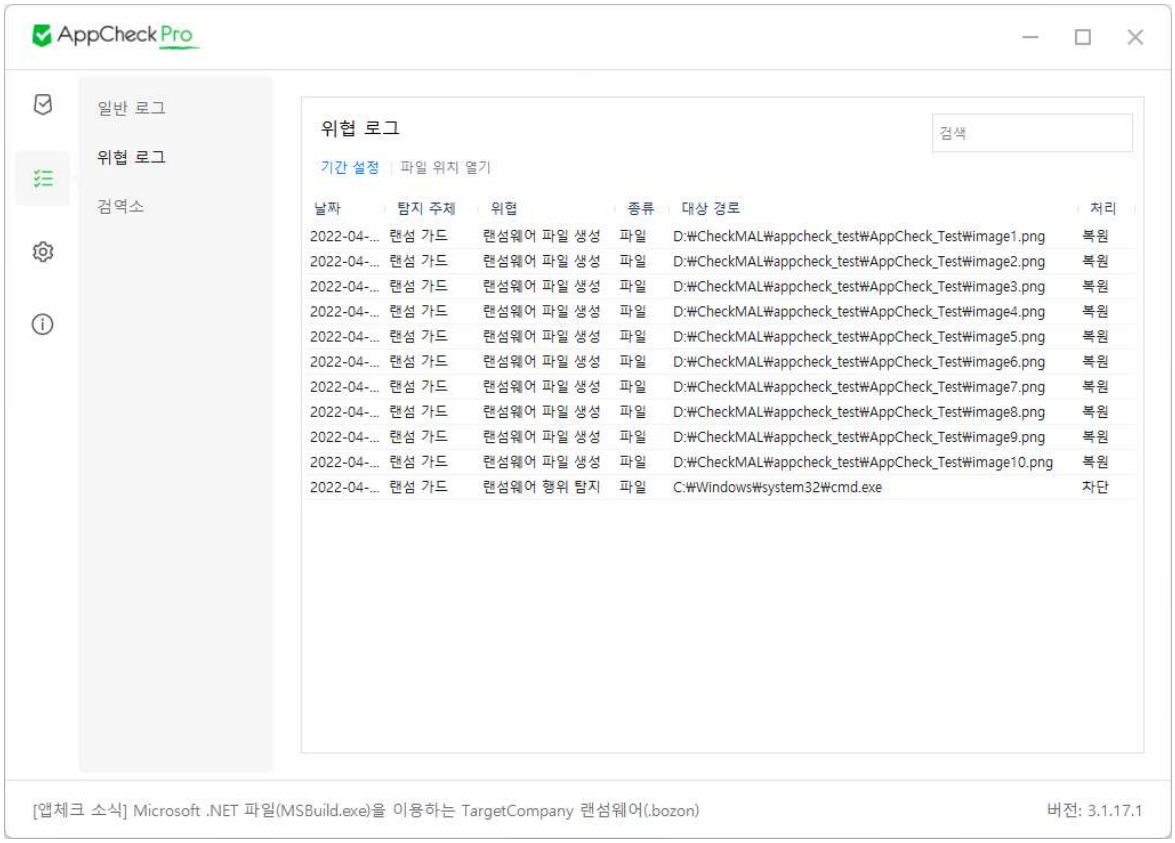


4.「destory_files.bat」ファイルを実行すると、自動で３０個のPNGファイルの毀損行為が行われますが、このタイミングで AppCheck アンチランサムウェアのは、「ランサムウェア攻撃が検知」というお知らせウィンドウを表示し、ファイル毀損行為を遮断します。

ファイル毀損行為が発生するファイル(PNGファイル)のコピーはリアルタイムでランサムウェア退避フォルダ(デフォルトの位置 ： C:¥ProgramData¥CheckMAL¥AppCheck¥RansomShelter)に臨時的にバックアップされ、ランサムウェアの行為検知によりランサムウェアが遮断された場合、ランサムウェアの退避フォルダに臨時バックアップファイルを使って復元を行います。

5. AppCheck ツールの「**脅威ログ**」からランサムウェア行為検知により遮断されたプロセス(ファイル)及び一部壊れたファイルが自動復元されたことに関する詳しい情報を確認出来ます。




AppCheck Pro
일반 로그
위협 로그
검역소
위협 로그
검색
기간 설정
파일 위치 열기
날짜 탐지 주체 위협 종류 대상 경로 처리
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image1.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image2.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image3.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image4.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image5.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image6.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image7.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image8.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image9.png 복원
2022-04-... 랜섬 가드 랜섬웨어 파일 생성 파일 D:₩CheckMAL₩appcheck_test₩AppCheck_Test₩image10.png 복원
2022-04-... 랜섬 가드 랜섬웨어 행위 탐지 파일 C:₩Windows₩system32₩cmd.exe 차단
[앱체크 소식] Microsoft .NET 파일(MSBuild.exe)을 이용하는 TargetCompany 랜섬웨어(.bozon)
버전: 3.1.17.1