



AppCheck Pro

誤検知対応マニュアル

株式会社 JSecurity

v202609

目次

1. ログデータ抽出方法	3
1.1. CMS有	3
1.1.1 ログデータ抽出	3
1.1. CMS無	5
1.1.2 ログデータ抽出	5
2. 検疫されたファイル/プロセスの復元手順	7
3. 例外設定(プロセス)手順	9
3.1. CMS有	9
3.1.1 ポリシー適用手順	9
3.1.2 エージェント適用手順	12
3.2. CMS無	15
3.2.1 エージェント適用手順	15
4. SMB例外設定(IPアドレス)手順	16
4.1. CMS有	16
4.1.1 全体適用	16
4.1.2 エージェント適用手順	19
4.2. CMS無	22
4.2.1 エージェント適用手順	22
5. 補足	24

1. ログデータ抽出方法

AppCheckでは、検知が発生した際、製品のログ情報欄に該当する検知ログが記載されます。
また、以下の方法でログデータを取得できます。

1.1. CMS有

1.1.1 ログデータ抽出

「脅威ログ」および「検疫所」の2種類のログ抽出方法となります。

(1) CMS Cloud（管理画面）にアクセスします。

<https://jp.cms.checkmal.com>



(2) 画面左側のメニューより「ログ管理」を選択してください。



(3) 脅威ログのタブで下記①～③を順に設定してください。

- ① 日付範囲：検知発生日 ～ 本日
- ② プルダウンより「Export ALL」を選択
- ③ 出力形式で CSVまたはMS-Excelを選択（いずれでも可）

(4) ③番を設定した段階で、該当ファイルがエクスポートされます。



(5) 画面上部のタブを「検疫所」に切り替え、上記(3)の手順を同様に実施します。



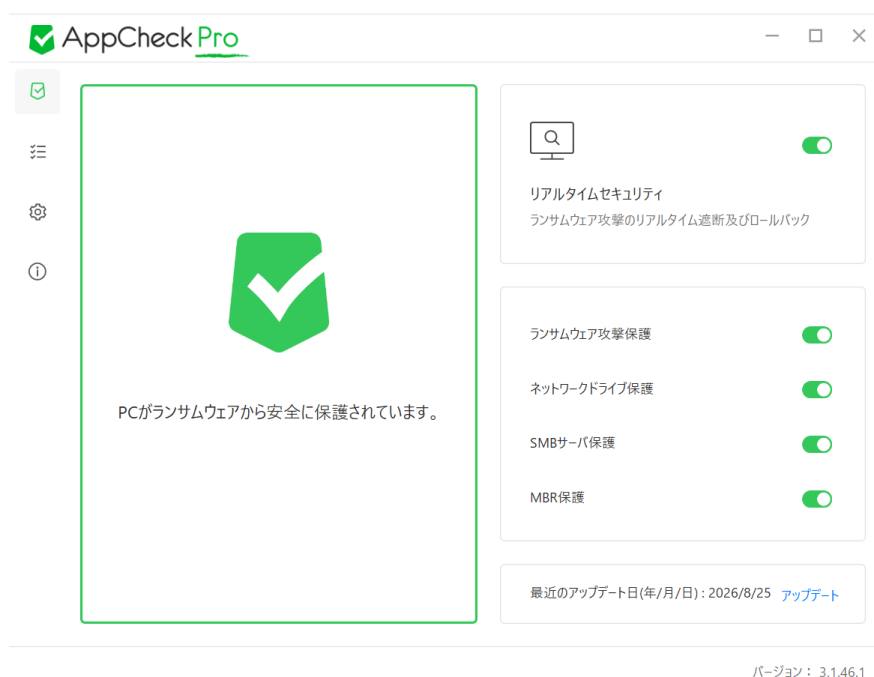
(6) 検知・遮断がありお問い合わせの際は上記で取得したログデータを「solution@santec.com」宛にメールへ添付してご送信いただきますようお願いいたします。

1.1. CMS無

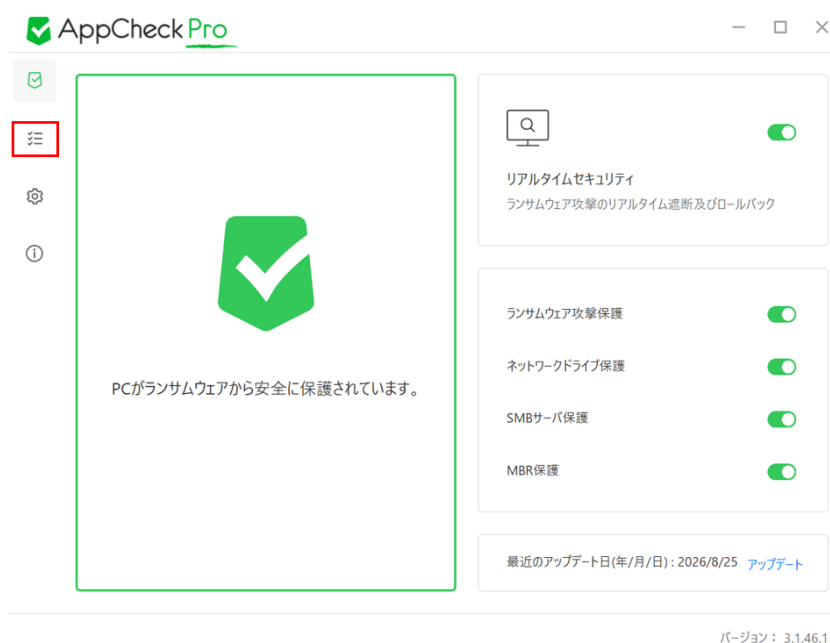
1.1.2 ログデータ抽出

「脅威ログ」および「検疫」の2種類のログ抽出方法となります。

(1) AppCheck を起動します。

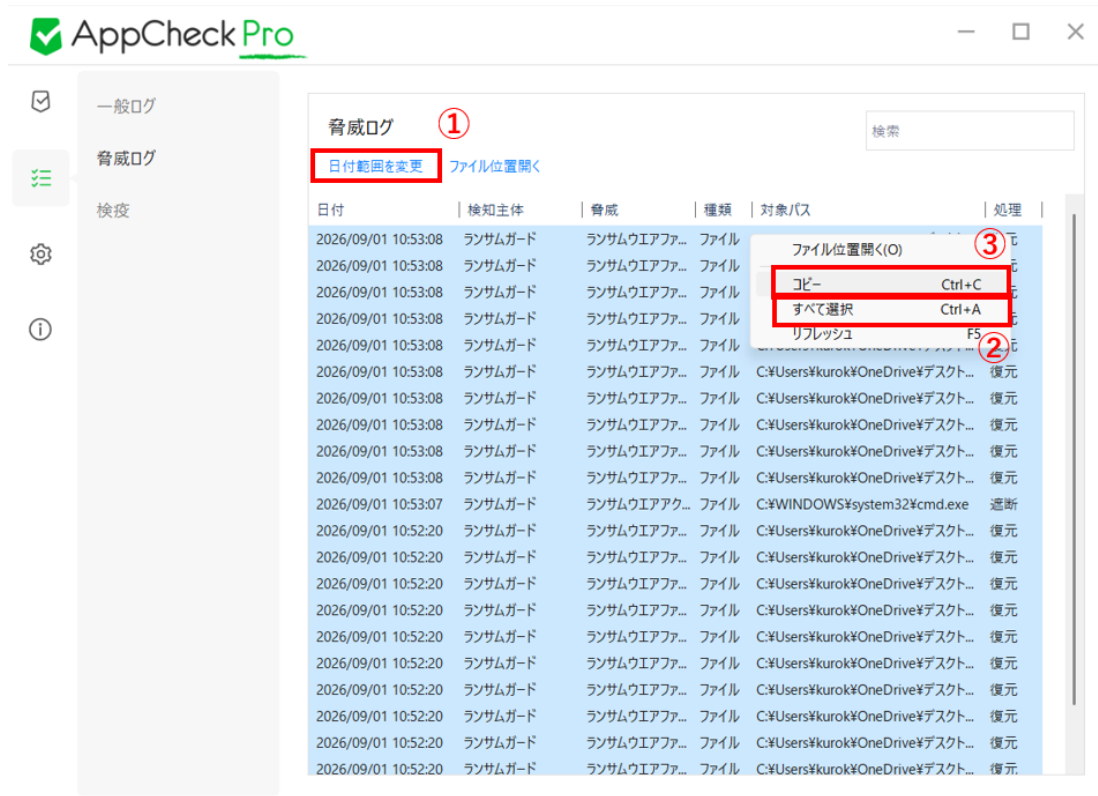


(2) 画面左側のメニューより「ツール」を選択します。



(3) 脅威ログのタブで下記①～③を順に設定してください。

- ① 「日付範囲を変更」から、検知発生日～本日までを指定
- ② 表示されているいずれかのログを右クリックし、「すべて選択」を選択
- ③ 選択したログを Excel にコピー & 貼り付け



バージョン： 3.1.46.1

- 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。

(4) コピー／貼り付けした Excel ファイルを保存します。

(5) 画面左側のタブを「検疫」に切り替え、上記 1～4 の手順を同様に実施します。

(6) 検知・遮断がありお問い合わせの際は上記で取得したログデータを

「solution@santec.com」宛にメールへ添付してご送信いただきますようお願いいたします。

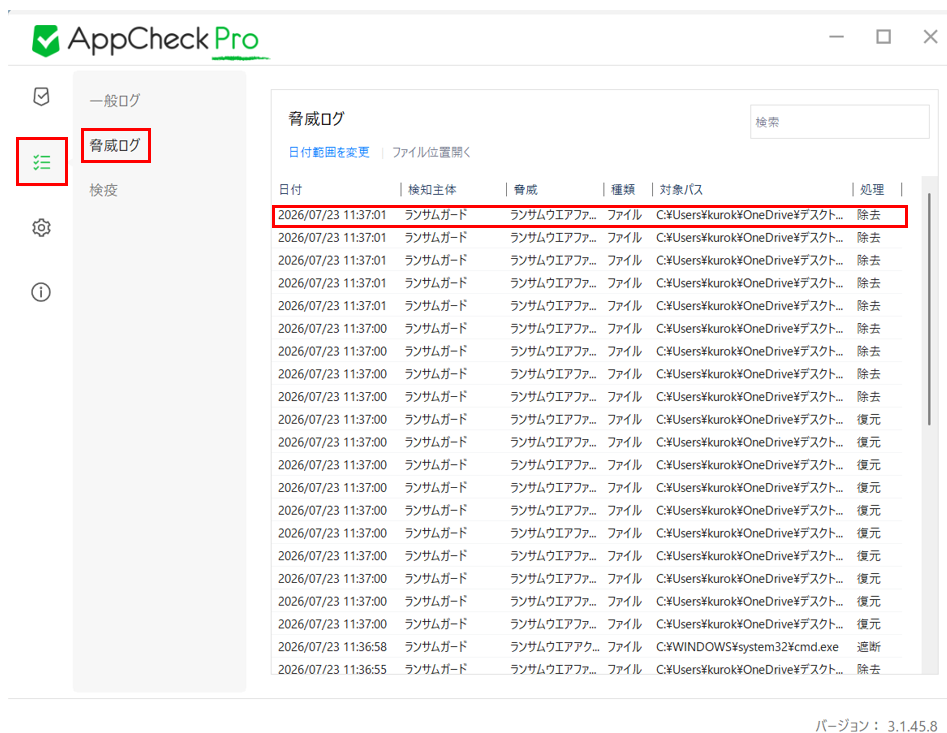
2. 検疫されたファイル/プロセスの復元手順

(1) Windows右下のAppCheckのアイコンをダブルクリックし、AppCheckProを開いてください。

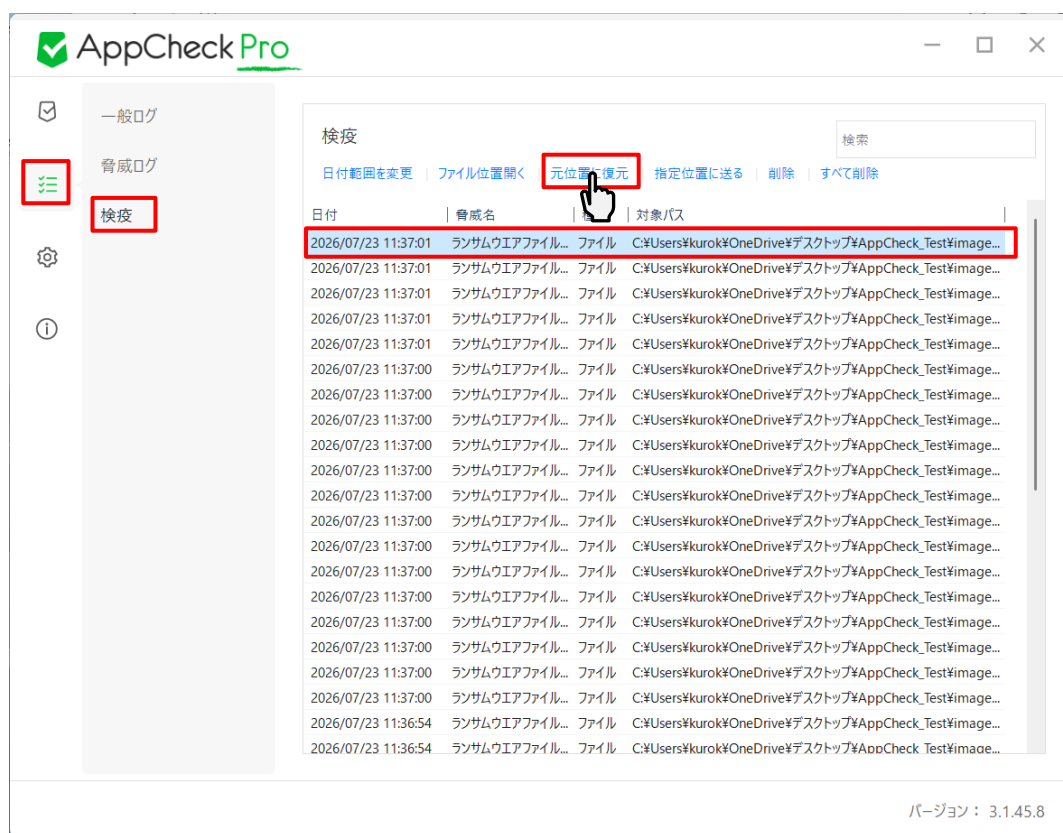


(2) 「ツール」>「脅威ログ」から、誤検知により「除去」されたプロセス/ファイルをご確認ください。

※ Windowsシステムが提供するプロセス、及びデジタル署名を取得しているプロセスは遮断で留まり、AppCheckにより検疫/隔離されません。(例：Windows標準プロセスcmd.exe等)



(3) 「ツール」>「検疫」から、誤検知により除去されたプロセス/ファイルを選択し、「元位置に復元」で復元してください。



3. 例外設定(プロセス)手順

・誤検知により「遮断」されたプロセスを、AppCheckの例外設定(ホワイトリスト)機能を利用し検知対象外に設定することで、再度誤検知してしまう動作を防ぐことができます。

※CMS Cloud ……【ポリシー別設定】、【エージェント別】の2パターンで設定可能
AppCheck (CMS無) ……【エージェント別】のみの1パターンで設定可能

3.1. CMS有

3.1.1 ポリシー適用手順

(1) 下のURLにアクセスし、CMSにログインします。

<https://jp.cms.checkmal.com>



(2) 「該当エージェント」>「ツール」>「ログビュー」ボタンをクリックします。



(3) 「脅威ログ」から「ランサムウェアアクション検知」として誤検知、遮断されているプロセスを確認してください。

ログビュー

検知主体	脅威	種類	対象パス	処理
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Filmora\Download\Temp\TitleV1_Credit_1_45\TempData\thumbnail.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Filmora\Download\Temp\TitleV1_Credit_1_45\TempData\thumbnail.png	復元
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Filmora\Download\Temp\TitleV1_Opener_1\TempData\thumbnail.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Filmora\Download\Temp\TitleV1_Opener_1\TempData\thumbnail.png	復元
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Filmora\Download\Temp\TitleV1_Default_LowerThird\TempData\thumbnail.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\kshin\Documents\Wondershare\Filmora\Filmora\Download\Temp\TitleV1_Default_LowerThird\TempData\thumbnail.png	復元
ランサムガード	ランサムウェアアクション検知	ファイル	C:\Users\kshin\AppData\Local\Wondershare\Filmora\Filmora\11-8.7.752\Filmora\Filmora 11.exe	遮断

Showing 1191 to 1197 of 1197 rows 10 rows per page

閉じる

(4) 「ポリシー管理」>「ポリシー管理」> ご利用されているポリシー(基本ポリシーなど)を選択してください。

CMS Cloud

ポリシー管理 (共通)

Export Basic

ポリシー名	タイプ	初期作成時間	最終変更時間	最終適用時間	バージョン	対象エージェント数	適用されたエージェント数	オンラインエージェント数	説明
基本ポリシー	Windows	2019-10-28 16:39:33	2026-06-30 16:06:11	-	287	-	-	-	

(5) 「例外設定」>「信頼済みプロセス一覧」>「追加」をクリックし、(3)で確認した誤検知プロセス(ファイルのパスまで含めた形)を入力し、「OK」を押してください。

1. 基本ポリシー

一般 ランサムガード エクスプロイトガード 回避フォルダ 自動バックアップ 例外設定

【信頼済みプロセス一覧】

☒ 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 **追加** 修正 削除

【保護対象ファイルの例外一覧】

☒ 以下に登録されたファイル変更は検知しない **追加** 修正 削除

【例外フォルダー一覧】

☒ 以下に登録されたフォルダ内のファイル変更は検知しない **追加** 修正 削除

「例外設定」初期化 全体初期化 保存する 取消

(6) 「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」にチェックを入れ、「保存する」ボタンをクリックしてください。

1. 基本ポリシー

一般 ランサムガード エクスプロイトガード 回避フォルダ 自動バックアップ 例外設定

【信頼済みプロセス一覧】

☒ 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 **追加** 修正 削除

C:\Users\...\AppData\Local\Wondershare\Filmora\Filmora11.6.7.752\Wondershare Filmora 11.exe

【保護対象ファイルの例外一覧】

☒ 以下に登録されたファイル変更は検知しない **追加** 修正 削除

【例外フォルダー一覧】

☒ 以下に登録されたフォルダ内のファイル変更は検知しない **追加** 修正 削除

「例外設定」初期化 全体初期化 **保存する** 取消

3.1.2 エージェント適用手順

(1) 以下のURLにアクセスし、CMSにログインします。

<https://jp.cms.checkmal.com>



The image shows the CMS Cloud login interface. At the top, it says 'CMS CLOUD'. Below that, a message says '使用するにはログインしてください' (Please log in to use). There are three input fields: a language dropdown set to '日本語', an email field with an envelope icon, and a password field with a lock icon. Below these fields are two checkboxes: 'IDを記憶する' (checked) and a 'ログイン' (Login) button. At the bottom, there is a link for 'パスワードを忘れた場合 管理者初期登録' (If you forgot your password, administrator initial registration).

(2) 「該当エージェント」>「ツール」>「ログビュー」ボタンをクリックします。



(3) 「脅威ログ」から「ランサムウェアアクション検知」として誤検知、遮断されているプロセスを確認してください。

ログビュー

脅威ログ 検疫所 一読ログ

検索

検知主体	脅威	種類	対象パス	処理
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\Kshin\Documents\Wondershare\Filora\Filora\Download\Temp\TitleV1_Credit_I_A5WTempData\Thumbnail.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\Kshin\Documents\Wondershare\Filora\Filora\Download\Temp\TitleV1_Credit_I_A5WThumbnail.png	復元
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\Kshin\Documents\Wondershare\Filora\Filora\Download\Temp\TitleV1_Opener_VTempData\Thumbnail.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\Kshin\Documents\Wondershare\Filora\Filora\Download\Temp\TitleV1_Opener_VThumbnail.png	復元
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\Kshin\Documents\Wondershare\Filora\Filora\Download\Temp\TitleV1_Default_LowerthirdVTempData\Thumbnail.png	削除
ランサムガード	ランサムウェアファイル生成	ファイル	C:\Users\Kshin\Documents\Wondershare\Filora\Filora\Download\Temp\TitleV1_Default_LowerthirdVThumbnail.png	復元
ランサムガード	ランサムウェアアクション検知	ファイル	C:\Users\Kshin\AppData\Local\Wondershare\Filora\Filora\11-5.7.752\Wondershare_Filora_11.exe	遮断

Showing 1191 to 1197 of 1197 rows 10 rows per page

閉じる

(4) 「ポリシー管理」>「例外設定(個別)」から、誤検知が発生したエージェントの「ツール」ボタンをクリックしてください。

CMS Cloud

例外設定(個別)

「例外設定」初期化

Search

	エージェントID	IPアドレス	NACアドレス	ホスト名	OS情報	ユーザ名	部署名	インストールバージョン	現状態	最終オンライン時間	ツール
☐											
☐											
☐											
☐											

Showing 1 to 4 of 4 rows

(5)「信頼済みプロセス一覧」>「追加」をクリックし、(3)で確認した誤検知プロセス(ファイルのパスまで含めた形)を入力し、「OK」を押してください。

例外設定

【信頼済みプロセス一覧】

☒ 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 **追加** 修正 削除

【保護対象ファイルの例外一覧】

☒ 以下に登録されたファイル変更は検知しない 追加 修正 削除

【例外フォルダー一覧】

☒ 以下に登録されたフォルダ内のファイル変更は検知しない 追加 修正 削除

保存する 取消

(6)「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」にチェックを入れ、「保存する」ボタンをクリックしてください。

例外設定

【信頼済みプロセス一覧】

☒ 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 追加 修正 削除

C:\Users\shin\AppData\Local\Wondershare\Filmora\Filmora11.6.7.752\Filmora 11.exe

【保護対象ファイルの例外一覧】

☒ 以下に登録されたファイル変更は検知しない 追加 修正 削除

【例外フォルダー一覧】

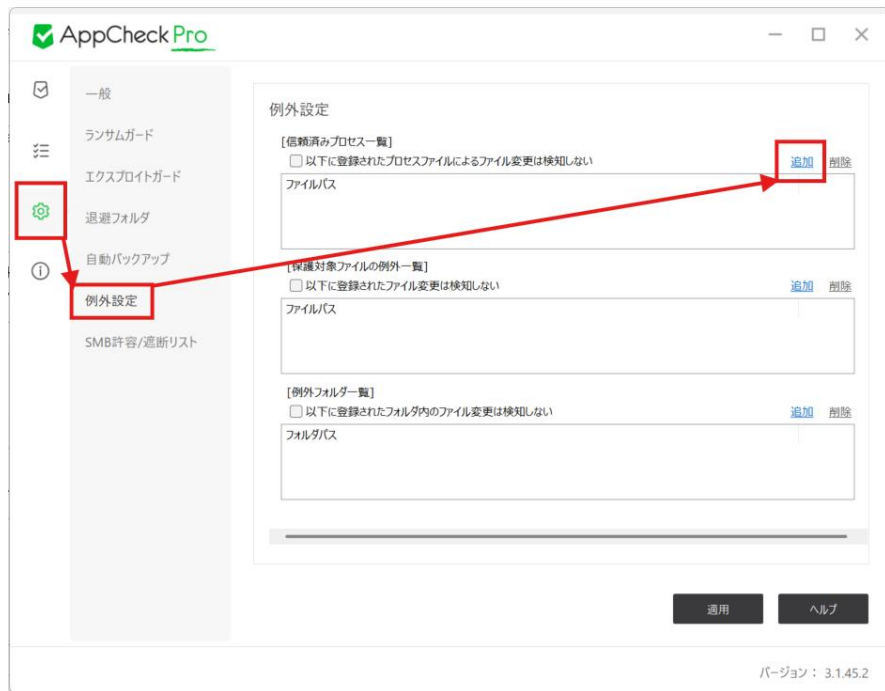
☒ 以下に登録されたフォルダ内のファイル変更は検知しない 追加 修正 削除

保存する 取消

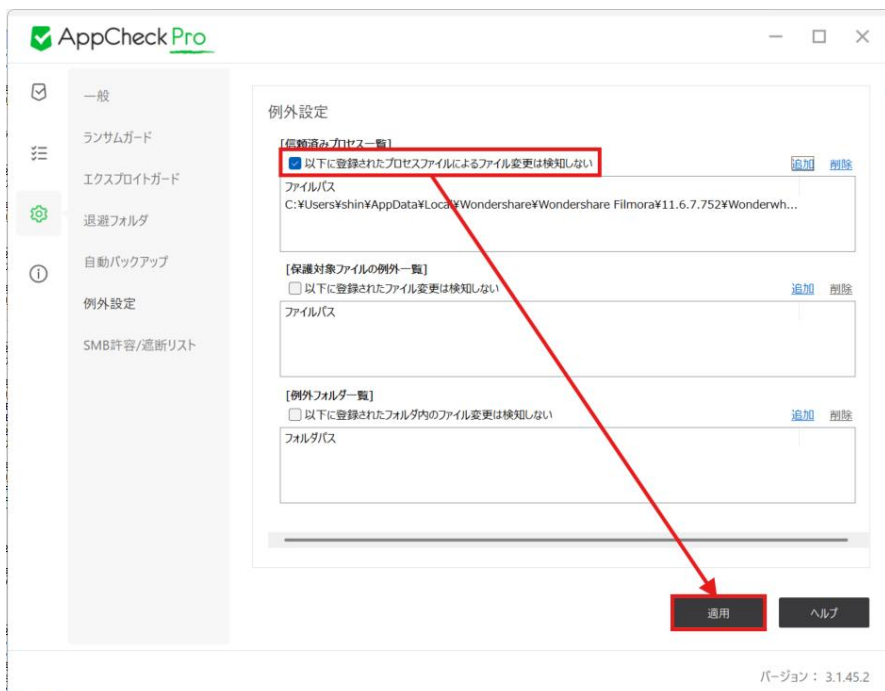
3.2. CMS無

3.2.1 エージェント適用手順

- (1) 「オプション」>「例外設定」>「信頼済みプロセス一覧」>「追加」により、誤検知プロセスファイルを入力し、追加してください。



- (2) 「登録されたファイルはチェックしない」にチェックを入れ、「適用」を押してください。



4. SMB例外設定(IPアドレス)手順

・誤検知により「遮断」されたIPアドレスを、AppCheckのSMB例外設定(ホワイトリスト)機能を利用し検知対象外に設定することで、再度誤検知してしまう動作を防ぐことができます。

※CMS Cloud ……【全体設定】、【エージェント別】の2パターンで設定可能
AppCheck (CMS無) ……【エージェント別】のみの1パターンで設定可能

4.1. CMS有

4.1.1 全体適用

(1) 以下のURLにアクセスし、CMSにログインします。

<https://jp.cms.checkmal.com>



(2) 「SMB設定」>「共通」>「許可されたアドレス一覧」の「追加」をクリックしてください。



(3) 追加するIPアドレスを入力し、「保存する」をクリックしてください。

許可されたアドレス一覧 ×

IP v4

- 個別 : 192.168.1.1
- 順次 : 192.168.1.1-10 (192.168.1.10 ~ 192.168.1.10 まで許可)
- 全体 : 192.168.1.0/24 (192.168.1.1 ~ 192.168.1.255 まで許可)

IP v6

- 個別 : 2001:0DB8:1000:0000:0000:1111:2222
- 順次 : 2001:0DB8:1000::1111:2222-3333
(2001:0DB8:1000::1111:2222 ~ 2001:0DB8:1000::1111:3333 まで許可)
- 全体 : 2001:0DB8::/32
(2001:0DB8:0000:0000:0000:0000:0000 ~ 2001:0DB8:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF まで許可)

保存する 閉じる

(4)「許可されたアドレス一覧」に入力したIPアドレス記載されていることを確認してください。



4.1.2 エージェント適用手順

(1) 以下のURLにアクセスし、CMSにログインします。

<https://jp.cms.checkmal.com>



The image shows the CMS Cloud login interface. At the top, it says 'CMS CLOUD'. Below that, a message reads '使用するにはログインしてください' (Please log in to use). There are three input fields: a language dropdown menu set to '日本語', an email field with an envelope icon, and a password field with a lock icon. Below these fields are two buttons: 'IDを記憶する' (Save ID) with a checkmark icon, and a blue 'ログイン' (Login) button. At the bottom, there is a link for 'パスワードを忘れた場合 管理者初期登録' (If you forgot your password, administrator initial registration).

(2) 「ポリシー設定」>「SMB設定」をクリックしてください。



(3) 「エージェント」>「ツール」をクリックし、「SMB許可/遮断リスト」を表示してください。



(4) 「遮断されたアドレス一覧」にあるIPアドレスを選択し、「常時許可」をクリックしてください。



- 常時許可：遮断された遠隔地IPアドレスを「常時許可」する(ホワイトリストとして常に許可)
- 臨時許可：遮断された遠隔地IPアドレスを「臨時許可」する(再度検知が発生するまで許可)

(5)「許可されたアドレス一覧」に追加されていることを確認してください。

SMB許可/遮断リスト	
許可されたアドレス一覧 追加 削除	
132. 132. 132. 132	
遮断されたアドレス一覧 臨時許可 常時許可	

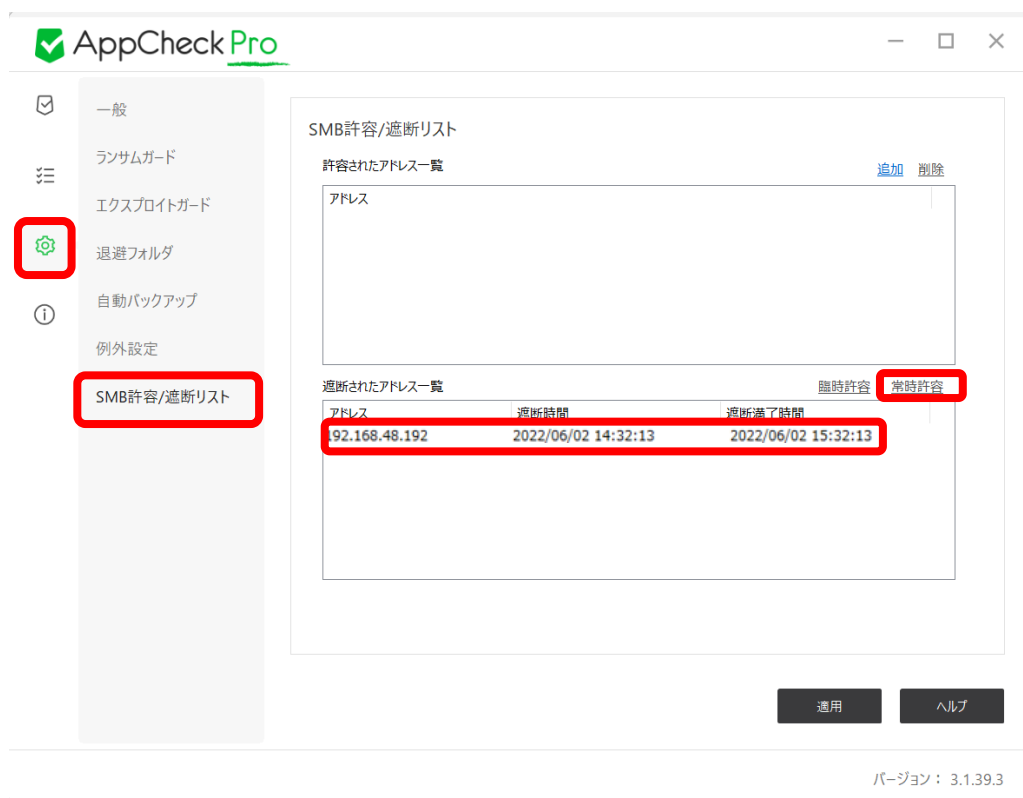
4.2. CMS無

4.2.1 エージェント適用手順

(1) Windows右下のAppCheckのアイコンをダブルクリックし、AppCheckProを開いてください。



(2) 「オプション」>「SMB許可/遮断リスト」を表示し、「遮断されたアドレス一覧」に記載されているアドレスを選択し「常時許可」をクリックしてください。



(3) 「許可されたアドレス一覧」に追加されていることを確認してください。

AppCheck Pro

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許可/遮断リスト

SMB許可/遮断リスト

許可されたアドレス一覧

追加

削除

アドレス
192.168.48.192

遮断されたアドレス一覧

臨時許可

常時許可

アドレス	遮断時間	遮断満了時間
------	------	--------

適用

ヘルプ

バージョン： 3.1.39.3

5. 補足

(1) CMS有且つ、サーバ版のみご契約の場合について

・CMS Cloudをご契約しており、サーバ版のみのAppCheck導入の下、SMBサーバ保護機能により誤検知（IPアドレス遮断）が発生した場合は、以下の3つの対応策がございます。

- ① お客様側にて一度に処理するファイル数の削減を行ってください。
- ② 検知された際に都度「臨時許容」をしてください。
- ③ SMBサーバ保護機能における誤検知を軽減するため、CMS Cloudのポリシー設定において「SMBサーバ保護検出回数」の値を調整してください。

※SMBサーバ保護検出回数の設定変更につきましては、お客様の運用状況に依存いたします。サーバ経由での処理内容や、ファイルサーバ利用時における一度のファイル書き換え数が大きく影響します。そのため、SMBサーバ保護検出回数の値を増やすことで誤検知の発生を抑制できるかと考えられます。

<SMBサーバ保護検出回数の変更手順>

- 1.CMS Cloud を開く <https://jp.cms.checkmal.com/login>
- 2.「ポリシー管理」→「ポリシー管理（共通）」を選択
- 3.該当のポリシーを選択
- 4.「ランサムガード」タブをクリック
- 5.画面下部の「SMBサーバ保護検出回数」の値を増やす

1. 基本ポリシー

一般 ランサムガード エクスプロイトガード 遠隔フォルダ 自動バックアップ 例外設定

☒ ランサムウェア攻撃保護

AppCheckPro拡張機能

【保護領域】

- ☒ ネットワークドライブ
- ☒ リムーバブルディスクドライブ
- ☒ SMBサーバ

【高速検知機能】

- ☒ ゴースト検知
- ☒ スマート検知

※AppCheck Pro for Windows Server エージェントはオプションで直接設定する必要があります。

【脅威遮断機能】

- ☒ システム脅威遮断

ランサムウェア遮断後、自動復元 ☒

保護するファイル拡張子（区分子、）

7z, ai, bmp, cer, cfg, chm, crt, csv, doc, der, docx, dotm, dotx, dwg, efi, eps, gif, h17, hwp, hwpk, jbm, jpeg, jpg, jos, jtd, key, li, c, link, md, mp3, nc, odp, ods, odt, ogg, ome, ovt, p12, p7b, p7c, pdf, pef, pem, pfx, png, pot, potx, psd, pst, ptx, rar, rdp, rtf, srm, tar, tif, tiff, txt, uti, x3f, xls, xlsx, xlsb, xlsm, xlsx, xps, zip

ランサムウェア検知後の動作： ブロック及び治療

疑わしいファイル数検知回数： 10

SMBサーバ保護検出回数： 10

「ランサムガード」初期化 全件初期化 保存する 取消

(2) プロセスの例外設定(誤検知が行われるプロセスの登録)時のメリット・デメリットについて

- ・メリット：正規プロセスから行われた正常なファイル処理がAppCheckにて誤検知されることを防ぐことができます。

- ・デメリット：該当プロセスから行われるファイル処理を全て許可することになるため、もし設定した該当プロセスからファイル毀損が行われても検知されなくなります。

※汎用的なプログラム等は、場合によってはランサムウェア攻撃に悪用されるプロセスがある為、安易に例外設定を行うことは推奨できません。どうしても、誤検知が頻発してしまう場合は、エージェント別の例外設定されることを推奨いたします。

(3) SMB例外設定(誤検知が行われるIPアドレスの登録)時のメリット・デメリットについて

- ・メリット：遠隔地PCから行われた正常なファイル処理がAppCheckにて誤検知されることを防ぐことができます。

- ・デメリット：遠隔地PCの該当IPアドレスから行われるファイル処理を全て許可することになるため、もし設定したIPアドレスからファイル毀損が行われても検知されなくなります。

※上記のデメリットがあるため、誤検知対策として、SMB例外設定は行わず、運用方法(例：ファイル一括削除の数を少なくする等)の変更で対応して頂くことが望ましいです。

(4) SMBサーバ保護機能の各設定パターンによる挙動について

	挙動	遠隔地からのアクセス遮断
SMB サーバ保護機能が「ON」状態	変更を受けるサーバ側のファイルが「保護するファイル拡張子」に該当すれば、ランサムウェアの攻撃として判断し、検知・遮断・リアルタイムバックアップ(サーバ側)による 自動復元を行います。 ※「脅威ログ」と「検疫」にて詳細確認可能	遮断される
SMB サーバ保護機能が「ON」状態で、遠隔地の IP アドレスが「例外設定」に登録済み	変更を受けるサーバ側のファイルが「保護するファイル拡張子」に該当すれば、遠隔地(登録 IP アドレス)からのアクセスは遮断・検知しないが、リアルタイムバックアップ(サーバ側の退避フォルダ内)は行うため、 手動作業による復元が可能です。 ※ログは残らない	登録 IP アドレスからのアクセスのみ遮断されない
SMB サーバ保護機能が「OFF」状態	変更を受けるサーバ側のファイルが「保護するファイル拡張子」に該当すれば、遠隔地からのアクセスは遮断・検知しないが、リアルタイムバックアップ(サーバ側の退避フォルダ内)は行うため、 手動作業による復元が可能です。 ※ログは残らない	遮断されない
補足説明	手動復元の方法としては、エクスプローラー上で「退避フォルダ」から、元場所への上書きコピーとなります。	※1 時間の間、該当 IP アドレスからサーバへのアクセスが遮断されます。遮断後「臨時許容」や「常時許容」機能によりアクセス許可ができます。