



AppCheck Pro

誤検知対応マニュアル

株式会社 JSecurity

第4版	2025/2/20
-----	-----------

目次

1. 検疫されたファイル/プロセスの復元手順	3
2. 例外設定(プロセス)手順	5
2.1.【CMS有】 ポリシー適用手順	5
2.2.【CMS有】 エージェント別	7
2.3.【CMS無】 エージェント別	10
3. SMB例外設定(IPアドレス)手順.....	11
3.1.【CMS有】 全体適用	11
3.2.【CMS有】 エージェント別	13
3.3.【CMS無】 エージェント別	16
4. 補足	18

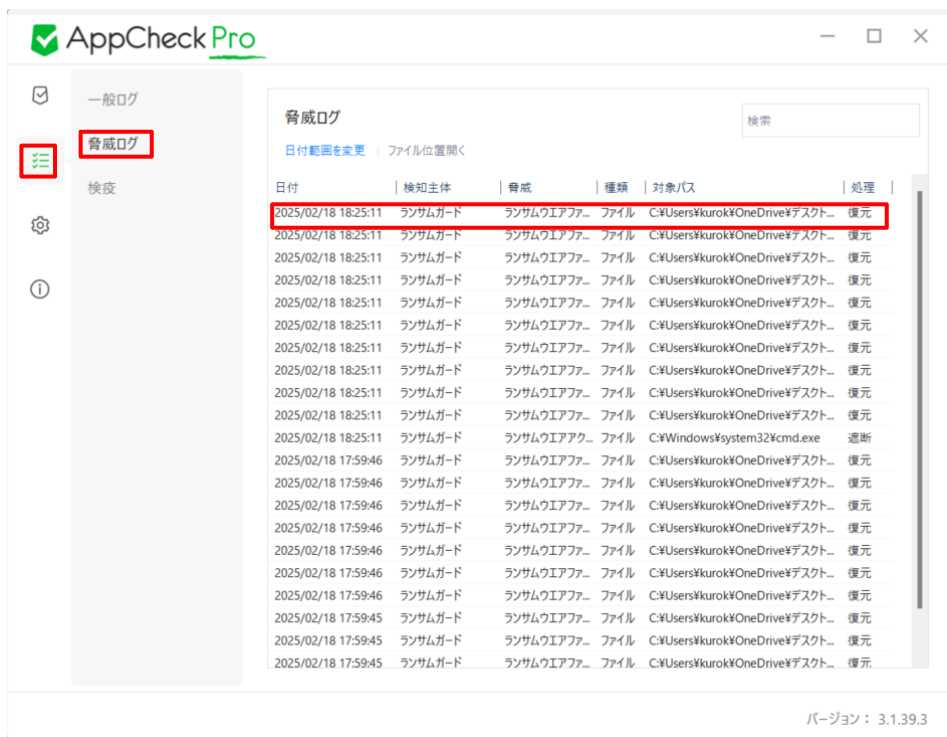
1. 検疫されたファイル/プロセスの復元手順

(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「遮断」されたプロセスファイルをご確認ください。

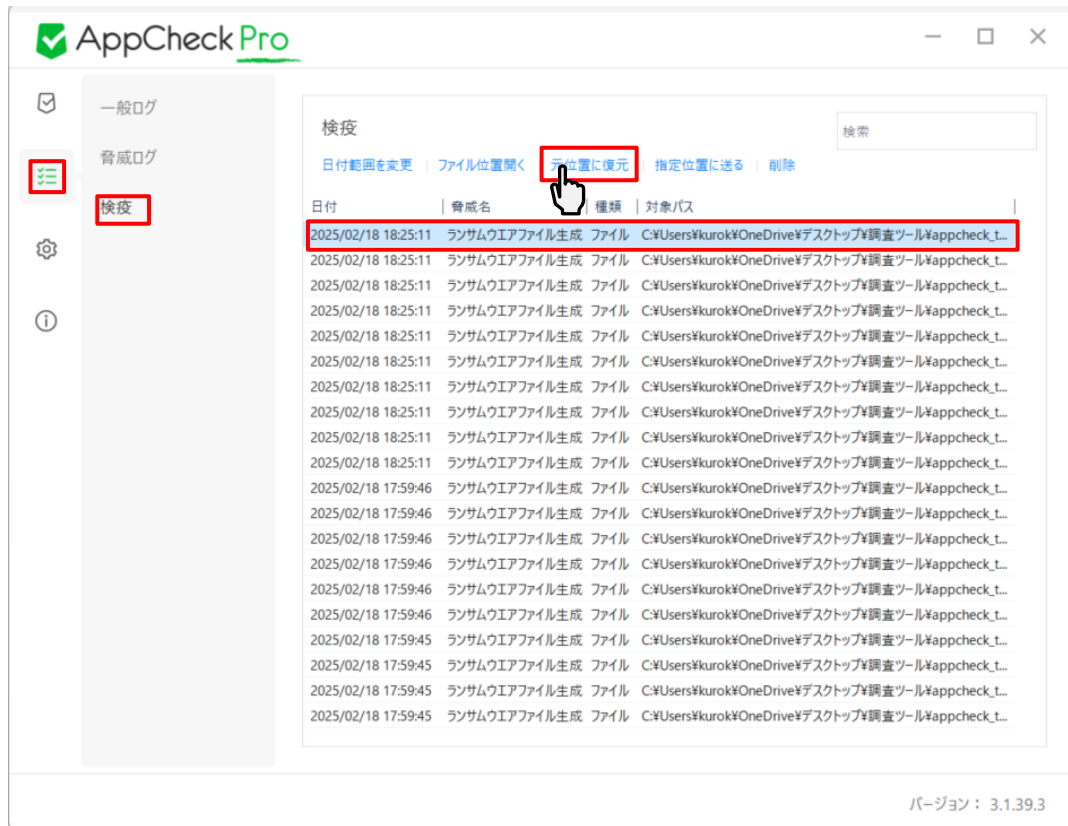
※ Windowsシステムが提供するプロセス、及びデジタル署名を取得しているプロセスは遮断で留まり、AppCheckにより検疫/隔離されません。(例：Windows標準プロセスcmd.exe等)



The screenshot shows the AppCheck Pro application window. On the left sidebar, the '脅威ログ' (Threat Log) icon is highlighted with a red box. The main window displays a table of threat logs with the following columns: 日付 (Date), 検知主体 (Detected by), 脅威 (Threat), 種類 (Type), 対象パス (Target Path), and 処理 (Action). One row is highlighted with a red box, showing a ransomware threat detected by 'ランサムガード' (Ransomware Guard) for the file 'C:\Users#\kurok#\OneDrive#\デスクトップ...'. Another row shows 'C:\Windows\system32\cmd.exe' with the action '遮断' (Blocked).

日付	検知主体	脅威	種類	対象パス	処理
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 18:25:11	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:46	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:46	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:46	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:46	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:46	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:45	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:45	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:45	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:45	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元
2025/02/18 17:59:45	ランサムガード	ランサムウェアファ...	ファイル	C:\Users#\kurok#\OneDrive#\デスクトップ...	復元

(3) 「ツール」>「検疫」から、誤検知により削除されたプロセスファイルとデータファイルを選択し、「元位置に復元」で復元してください。



2. 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

2.1. 【CMS有】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。



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	ポリシー名	ポリシーバージョン	最新ポリシーバージョン	現状態	リアルタイムセキュリティ	最終オンライン時間	ツール
					3.1.32.1	基本ポリシー	-	58	オンライン	アクション	2023-07-05 11:17:35	ログビュー
					3.1.32.1	基本ポリシー	-	58	オンライン	アクション	2023-07-05 11:16:58	
					3.1.32.1	基本ポリシー	-	58	オンライン	アクション	2023-07-05 11:16:52	

- (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 一般ログ

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\shin\Documents\Wondershare\Filaora\Download\Temp\Title\1_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\shin\Documents\Wondershare\Filaora\Download\Temp\Title\1_Credit_1_45\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\shin\Documents\Wondershare\Filaora\Download\Temp\Title\1_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\shin\Documents\Wondershare\Filaora\Download\Temp\Title\1_Opener_1\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\shin\Documents\Wondershare\Filaora\Download\Temp\Title\1_Default_Lowert\rd\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\shin\Documents\Wondershare\Filaora\Download\Temp\Title\1_Default_Lowert\rd\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\shin\AppData\Local\Wondershare\Filaora\11-8-7-752\Wondershare\Filaora_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

Export Basic 部署別一括ポリシー適用 + 追加 + Linux追加 - 削除 shin@iran.com

ポリシー名	Type	初版作成時間	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	2024-12-23 16:21:16	-	88	-	-	-	

Showing 1 to 6 of 6 rows 10 rows per page

- (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。

基本ポリシー

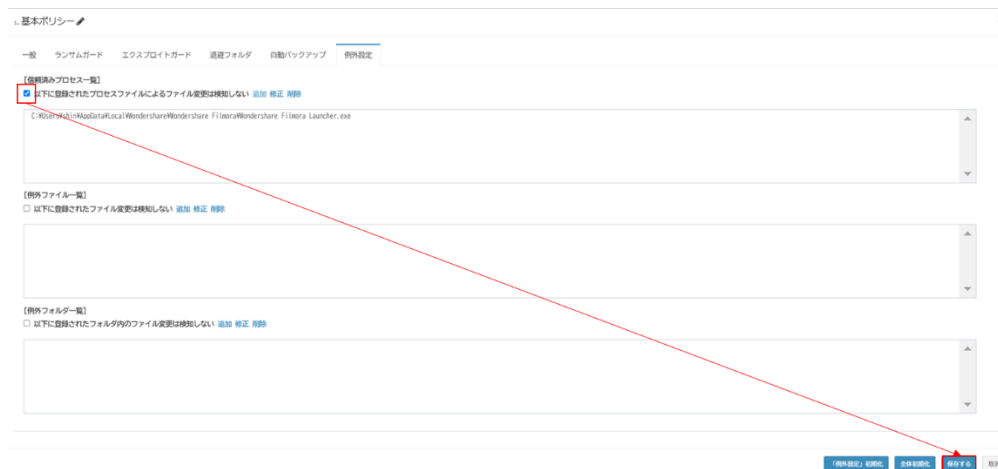
一般 ランサムガード エクスプロイトガード 遠隔フォルダ 自動バックアップ 例外設定

【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

【例外ファイル一覧】
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

- (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。



2.2. 【CMS有】 エージェント別

- (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 screenshot shows the CMS CLOUD login page. The page title is 'CMS CLOUD'. Below the title, it 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: 'Language' (日本語), 'Email' (Eメール), and 'Password' (パスワード). A checkbox 'Remember ID' (IDを記憶する) is checked. A 'Login' (ログイン) button is present. Below the login fields, there is a link for 'Forgot password? Admin initial registration' (パスワードを忘れた場合 管理者初期登録).

(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。



(4) 「ポリシー管理」>「例外設定」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。



- (5) 「信頼済みプロセスリスト」>「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](#)

【例外ファイル一覧】
 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\Yshim\LocalData\Local\Wondershare\Filmora\Wondershare Filmora Launcher.exe

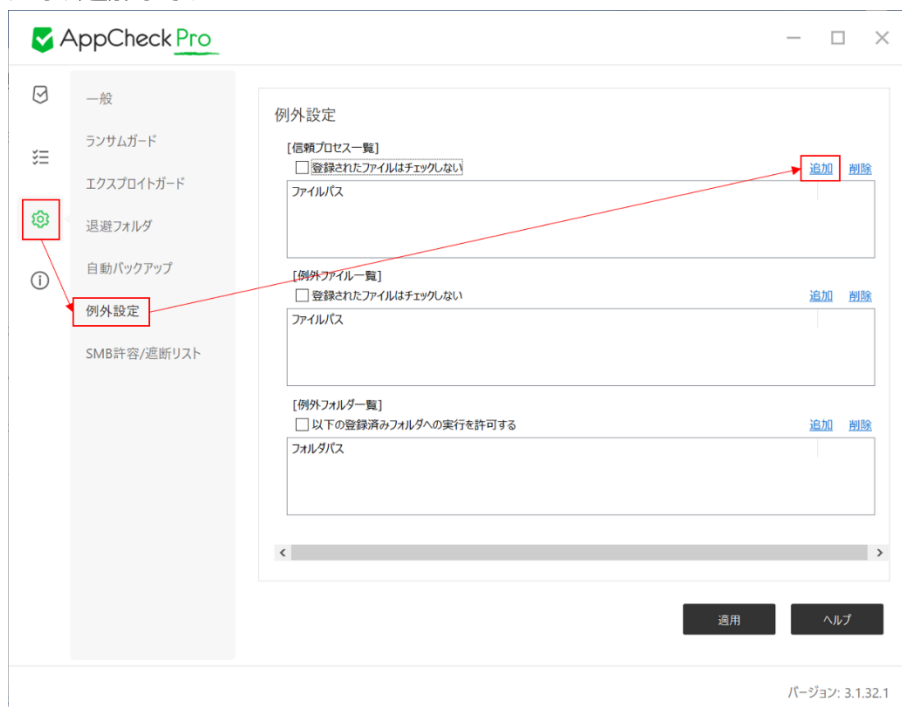
【例外ファイル一覧】
 以下に登録されたファイル変更は検知しない [追加](#) [修正](#) [削除](#)

【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](#)

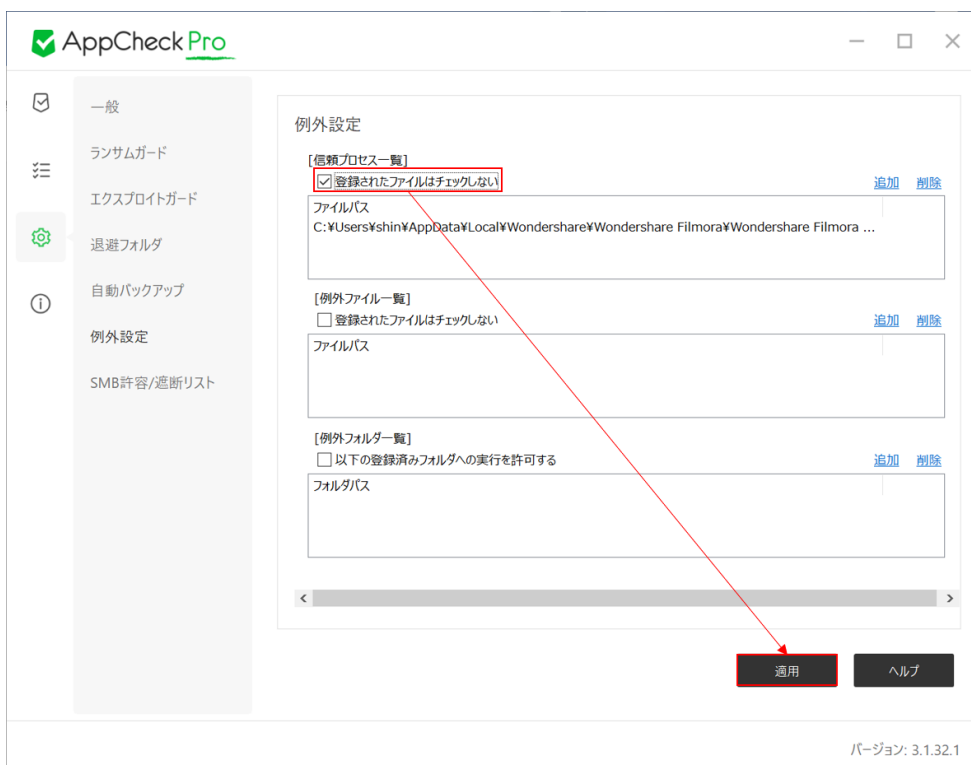
[保存する](#) [取消](#)

2.3. 【CMS無】 エージェント別

- (1) 「オプション」>「例外設定」>「信頼プロセス一覧」>「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。



3. 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

3.1. 【CMS有】 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>

CMS CLOUD

使用するにはログインしてください

日本語

Eメール

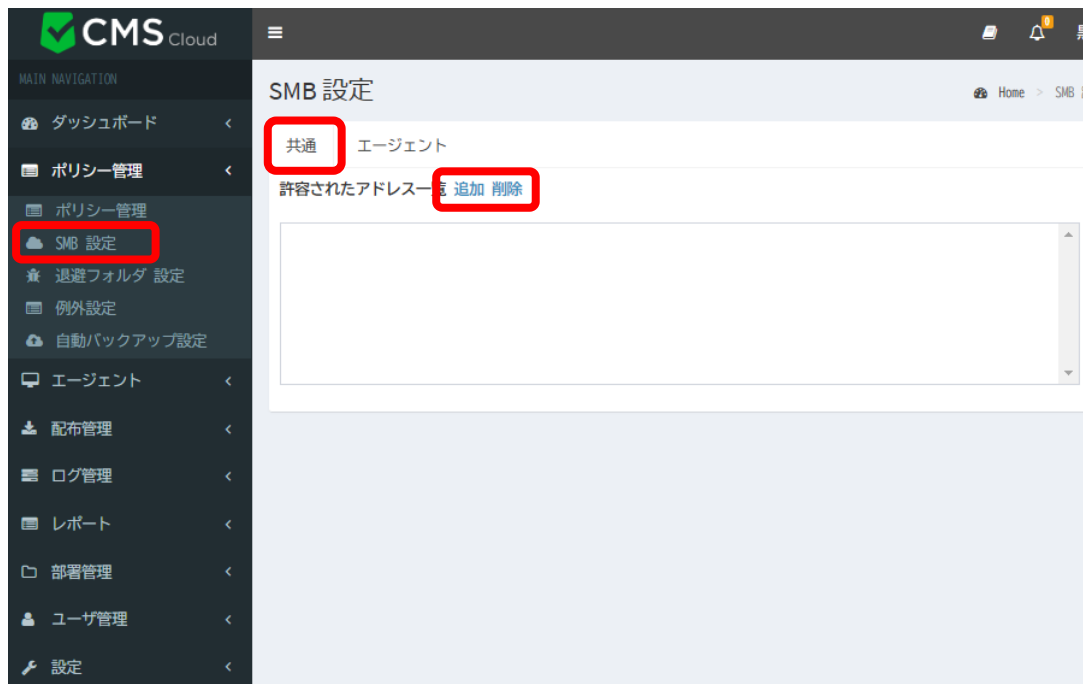
パスワード

IDを記憶する

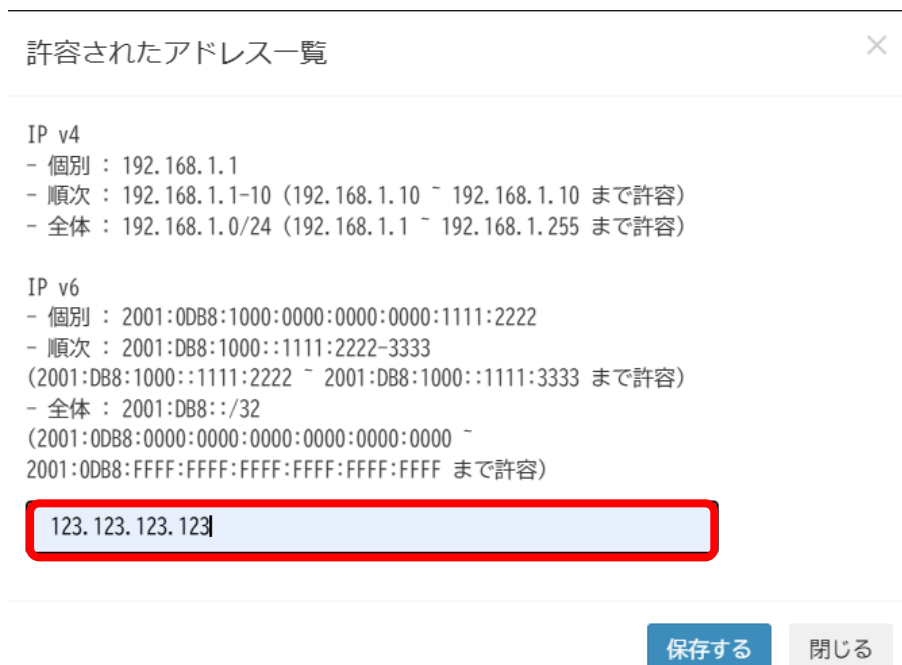
ログイン

パスワードを忘れた場合
管理者初期登録

(2) 「SMB設定」>「共通」>「許容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。



(4) 「許容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。



3.2. 【CMS有】 エージェント別

(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) 「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。

SMB許容/遮断リスト

許容されたアドレス一覧 [追加](#) [削除](#)

--

遮断されたアドレス一覧 [臨時許容](#) [常時許容](#)

--

- 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)

(5) 「許容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許容/遮断リスト

許容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 [臨時許容](#) [常時許容](#)

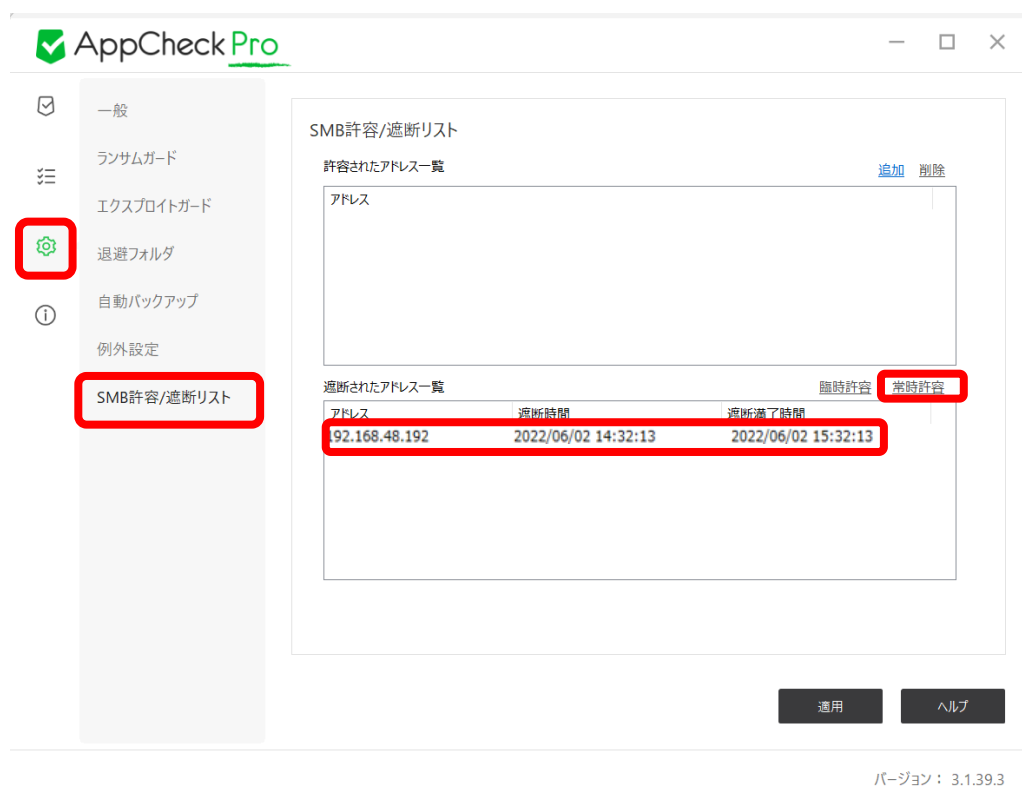
--

3.3. 【CMS無】 エージェント別

(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許容/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「常時許容」をクリックしてください。



(3) 「許容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。

The screenshot shows the AppCheck Pro application window. On the left is a navigation menu with the following items: 一般 (General), ランサムガード (Ransomware Guard), エクスプロイトガード (Exploit Guard), 回避フォルダ (Avoidance Folder), 自動バックアップ (Automatic Backup), 例外設定 (Exception Settings), and SMB許容/遮断リスト (SMB Allow/Block List). The 'SMB許容/遮断リスト' item is selected. The main content area is titled 'SMB許容/遮断リスト' and contains two sections: '許容されたアドレス一覧' (Allowed addresses list) and '遮断されたアドレス一覧' (Blocked addresses list). The '許容されたアドレス一覧' section has a table with one entry: '192.168.48.192', which is highlighted with a red box. Above this table are '追加' (Add) and '削除' (Delete) buttons. The '遮断されたアドレス一覧' section has a table with columns 'アドレス' (Address), '遮断時間' (Block time), and '遮断満了時間' (Block expiration time). Above this table are '臨時許容' (Temporary allow) and '常時許容' (Permanent allow) buttons. At the bottom right of the main area are '適用' (Apply) and 'ヘルプ' (Help) buttons. The footer of the window displays 'バージョン: 3.1.39.3'.

4. 補足

(1) 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お奨めできません。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お奨めいたします。

(2) 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。

(3) 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、遠隔地からのアクセスは遮断しないが、検知・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
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しないが、検知・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。