



AppCheck CMS Cloud

マニュアル

株式会社 JSecurity

第24版

2024/12/3

目次

| | |
|--|-----------|
| 1.1 CMS Cloudへのアクセス、ログイン..... | 6 |
| CMS Cloudの各機能について..... | 7 |
| 2.1 ダッシュボード..... | 7 |
| 2.1.1 時間別検知状況..... | 8 |
| 2.1.2 エージェントバージョン..... | 9 |
| 2.1.3 エンジンアップデート状況..... | 10 |
| 2.1.4 24時間内上位5位脅威..... | 11 |
| 2.1.5 ポリシー適用状況..... | 11 |
| 2.1.6 ログ統計..... | 12 |
| 2.2 ポリシー管理..... | 13 |
| 2.2.1 部署別一括ポリシー適用..... | 14 |
| 2.2.2 ポリシー追加および削除..... | 14 |
| 2.2.2 ポリシーの追加・削除、ファイルの出力・検索..... | 15 |
| 2.2.3 ポリシー管理 : 一般..... | 16 |
| 2.2.4 ポリシー管理 : ランサムガード..... | 17 |
| 2.2.5 ポリシー管理 : エクスプロイトガード..... | 20 |
| 2.2.6 退避フォルダ..... | 21 |
| 2.2.7 ポリシー管理 : 自動バックアップ..... | 23 |
| 2.2.8 ポリシー管理 : 例外設定 (ユーザ指定除外ファイル)..... | 25 |
| 2.2.9 SMB設定..... | 28 |
| 2.2.10 退避フォルダ設定..... | 29 |
| 2.3 エージェント..... | 30 |
| 2.3.1 部署別一括ポリシー適用..... | 32 |
| 2.3.2 個別ポリシー適用..... | 32 |
| 2.3.3 情報一括変更..... | 33 |
| 2.3.4 バックアップフォルダを空にする..... | 34 |
| 2.3.5 エージェント削除..... | 34 |
| 2.3.6 エージェントのライセンス変更..... | 35 |

| | |
|--|-----------|
| 2.4 配布管理 | 35 |
| 2.4.1 各ライセンス毎のインストールファイルダウンロード、配布..... | 35 |
| 2.4.2 クライアント配布 : Eメール送信..... | 36 |
| 2.4.2.1 Eメール検索..... | 37 |
| 2.4.2.2 エクセルでメール送信..... | 38 |
| 2.4.2.3 イメージ添付..... | 39 |
| 2.4.3 ソフトウェア配布ツールを用いたインストールについて..... | 40 |
| 2.5 ログ管理 | 43 |
| 2.5.1 脅威ログ..... | 43 |
| 2.5.2 検疫所..... | 45 |
| 2.5.3 一般ログ..... | 46 |
| 2.5.4 システムログ..... | 47 |
| 2.6 レポート | 48 |
| 2.6.1 ライセンス..... | 49 |
| 2.6.2 検知状況..... | 50 |
| 2.6.3 運営体制情報..... | 51 |
| 2.6.4 製品情報報告書..... | 51 |
| 2.6.5 ランサムウェア感染情報..... | 52 |
| 2.6.6 エクスプロイトガード情報..... | 53 |
| 2.7 部署管理 | 54 |
| 2.8 ユーザ管理 | 55 |
| 2.8.1 ユーザ追加と削除..... | 55 |
| 2.8.2 部署別ユーザ追加..... | 56 |
| 2.8.3 ユーザ情報..... | 57 |
| 2.9 設定 | 58 |
| 2.9.1 管理者..... | 58 |
| 2.9.2 ライセンス..... | 60 |
| 2.9.3 アラーム設定..... | 61 |
| 2.10 パスワードを忘れた場合 | 62 |
| 2.10.1 パスワード変更について..... | 63 |
| 2.10.2 仮パスワードについて..... | 64 |

はじめに

この度は、CMS Cloudをご購入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、ご利用となる前に本書をよくお読みください。

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 Pro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CMS Cloud V1.1.35を参考に作成しています。

動作環境について

[表1] AppCheck CMS Cloud 動作環境

| システム動作環境 | |
|----------|---|
| ブラウザ | <ul style="list-style-type: none">・Microsoft Edge・Google Chrome・Mozilla Firefox |

1.1 CMS Cloudへのアクセス、ログイン

下記 URL にて、CMS Cloud のログインページにアクセスしてください。

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



言語：「日本語」を選択いただき、

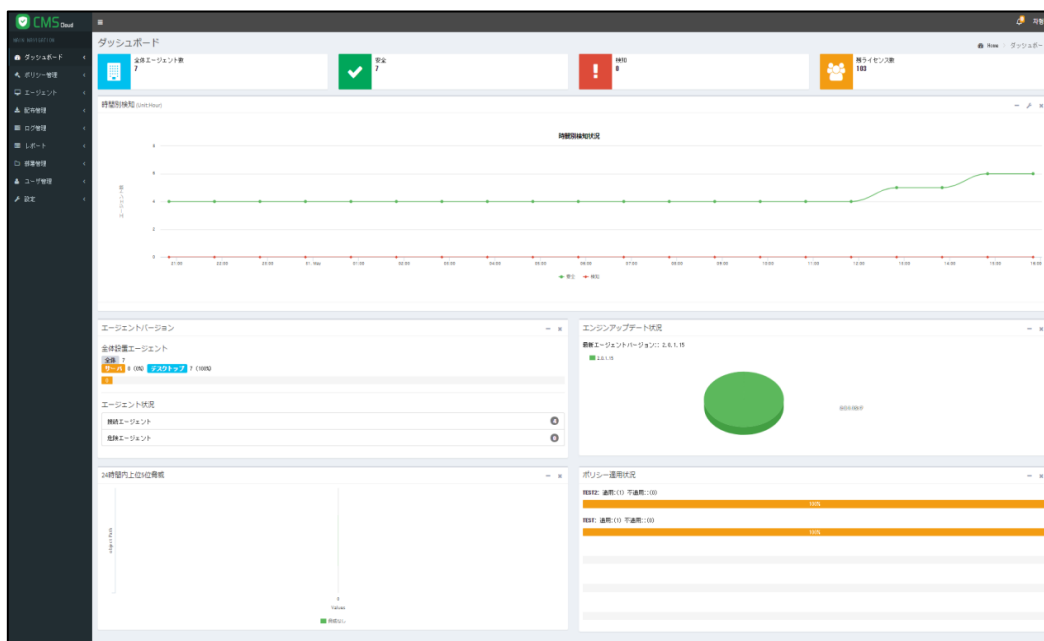
管理者のメールアドレスとパスワードを入力し、

「ログイン」ボタンをクリックしてください。

※管理者初期登録については「AppCheck クイックガイド」をご参考ください。

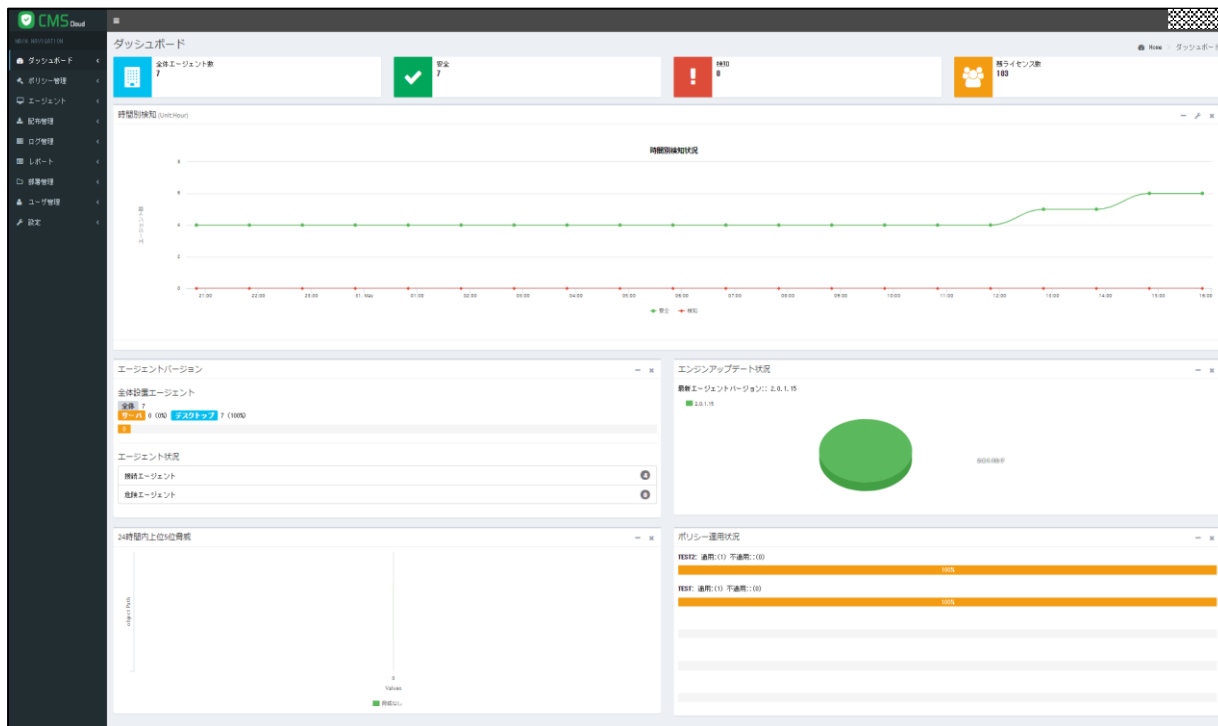
※管理者のメールアドレスとパスワードは、「AppCheck クイックガイド」で登録したメールアドレスとパスワードとなります。

※パスワードを忘れた場合は、「パスワードを忘れた場合」からパスワード変更および仮パスワードを入手して下さい。
(2.10 をご参照ください) 正常にログインできたら「ダッシュボード画面」が表示されます。



CMS Cloud の各機能について

2.1 ダッシュボード



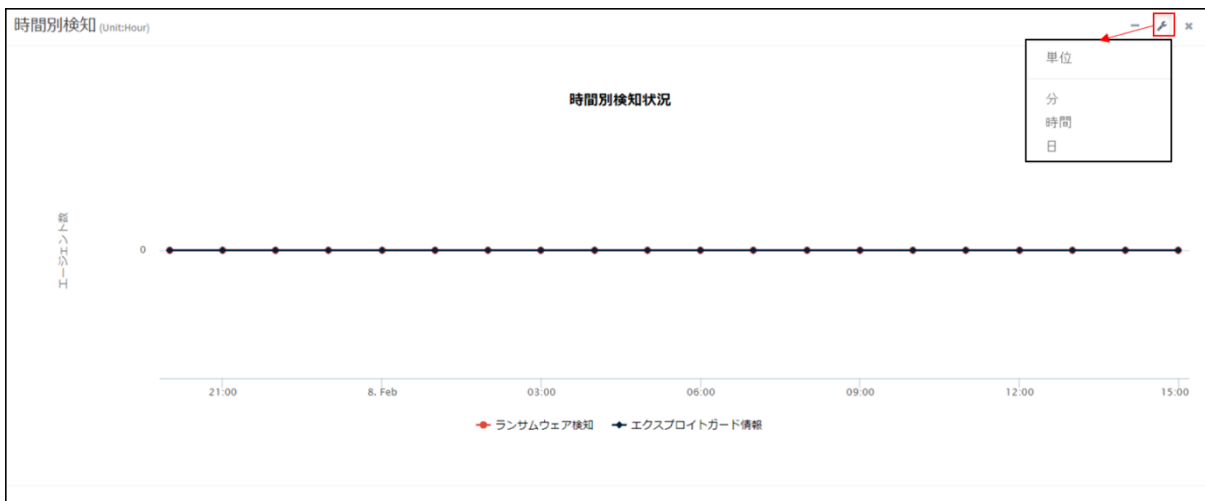
ダッシュボードでは検知状況を含め、様々な情報を一目で確認することができます。

- ・**時間別検知状況** (2.1.1をご参照ください)
- ・**エージェントバージョン(全体インストールエージェント及び状態)** (2.1.2をご参照ください)
- ・**エンジンアップデート状況** (2.1.3をご参照ください)
- ・**24時間内上位5位脅威** (2.1.4をご参照ください)
- ・**Windowsポリシー適用状況** (2.1.5をご参照ください)
- ・**ログ統計** (2.1.6をご参照ください)



- ・**全体エージェント数** : CMS Cloudにて配布、インストールされたAppCheck Pro、AppCheck Pro for Windows Serverの全体体エージェント数
- ・**安全** : ランサムウェア検知が発生していないエージェント数
- ・**検知** : ランサムウェア検知が発生したエージェント数
- ・**残ライセンス数** : 契約ライセンス数の中で、まだ利用されていないライセンス数

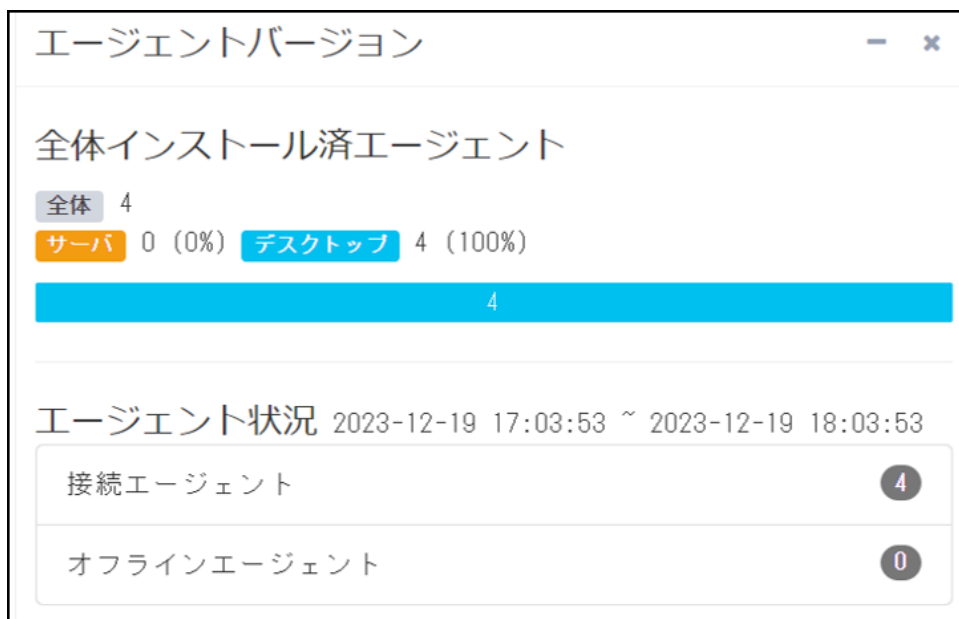
2.1.1 時間別検知状況



時間別検知状況では、日単位、1時間単位、または1分単位で「ランサムウェア検知状況」と「エクスプロイトガード検知情報」が集計され、グラフとして表示されます。

確認したい時間帯にマウスカーソルを置くと、該当時間帯の検知状況(エージェント数)が表示されます。

2.1.2 エージェントバージョン

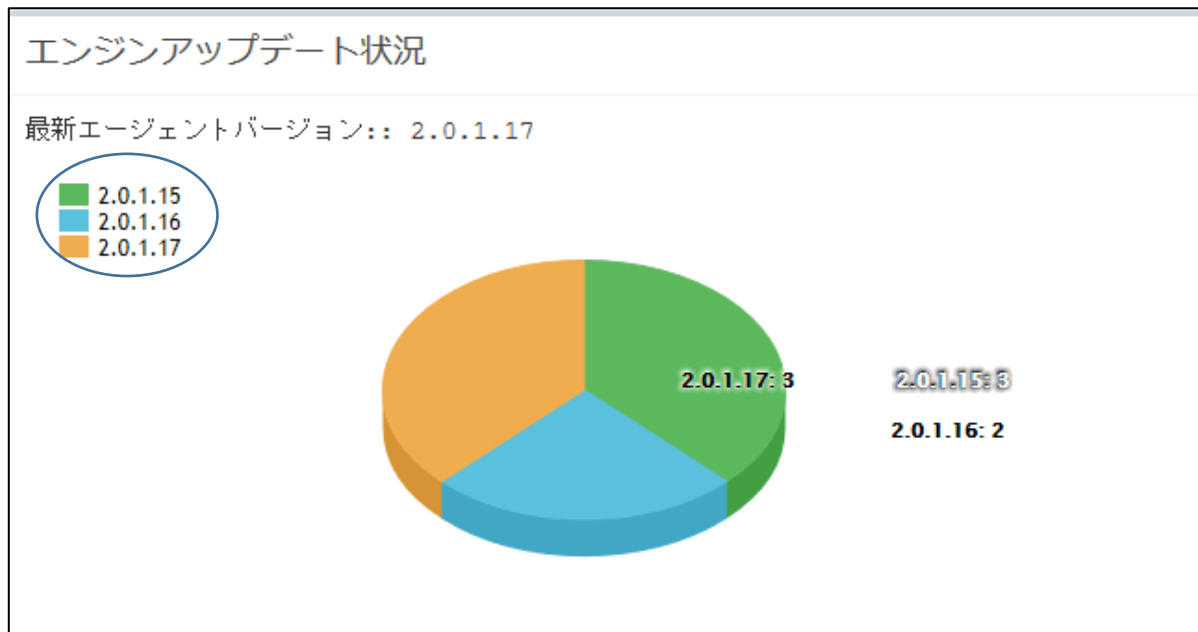


エージェントバージョンでは、インストールされているエージェント全体(PC版、サーバ版)の情報とエージェント状況(接続エージェント、オフラインエージェント)数が表示されます。

全体インストール済エージェントでは、AppCheck Pro(PC版)とAppCheck Pro for Windows Server(サーバ)が分けられて表示されます。

「接続エージェント」は、インストールされたエージェントの中、現在オンライン状態のエージェント数が表示され、「オフラインエージェント」は、現在オフライン状態のエージェント数が表示されます。

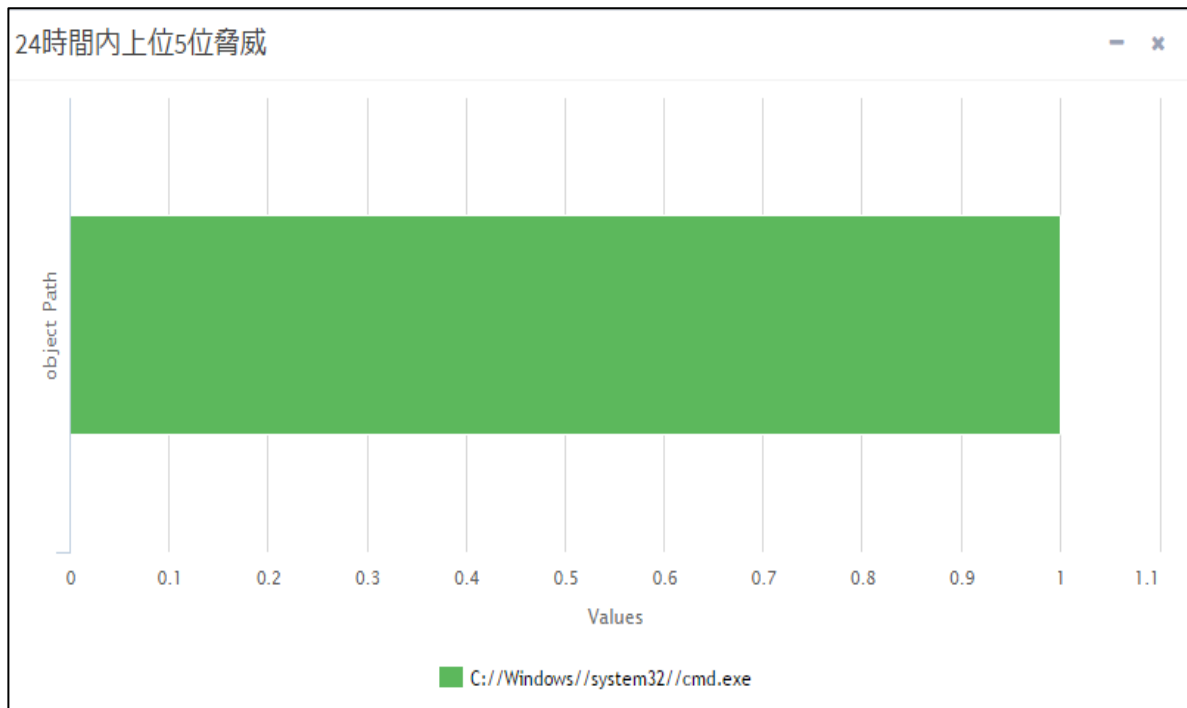
2.1.3 エンジンアップデート状況



エンジンアップデート状況では、各エージェントにインストールされているAppCheckバージョンの割合が円グラフで表示されます。

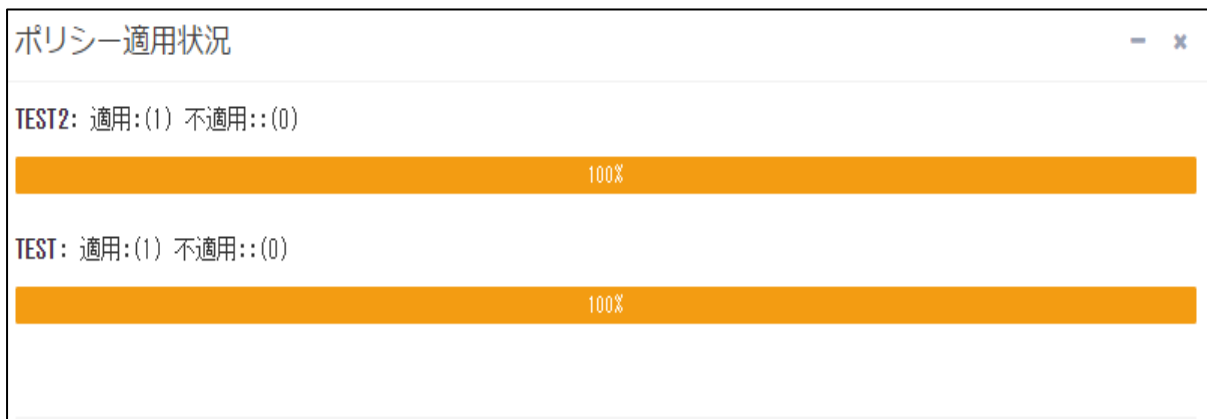
特定バージョンのエージェント数を確認する際には、画面の左上から特定バージョン名をクリックしてください。

2.1.4 24時間内上位5位脅威



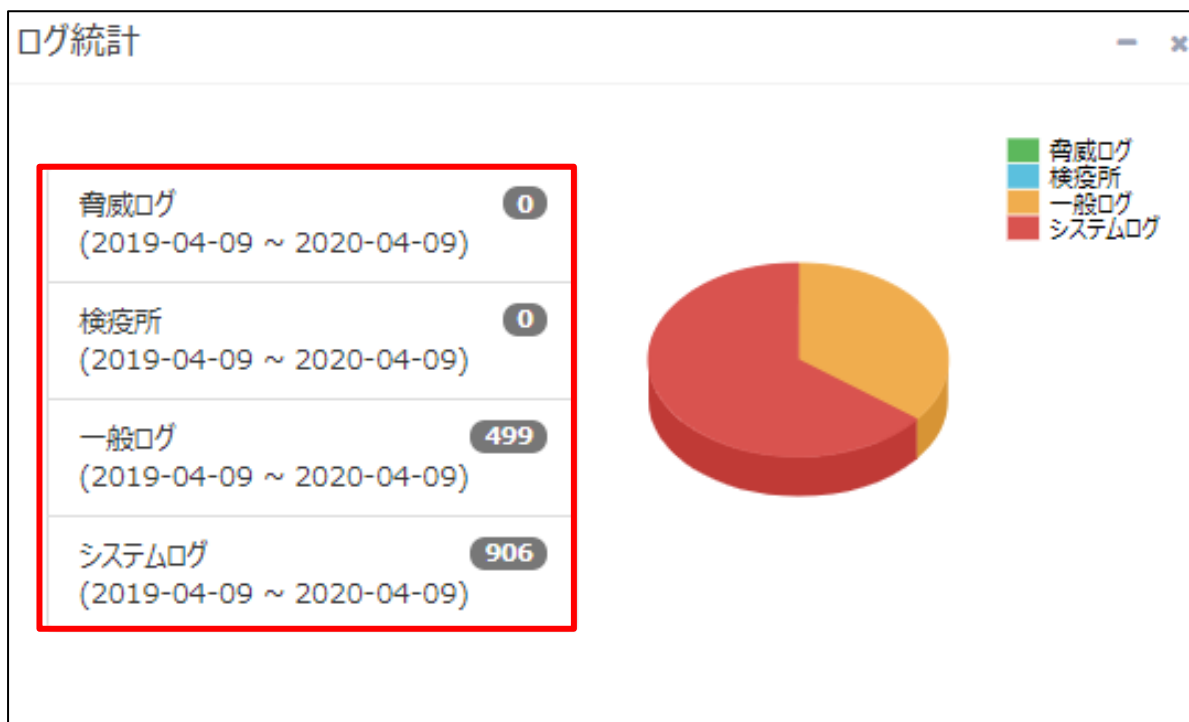
24時間以内に検知された毀損プロセスのファイルパス(Object Path)と該当エージェント数(Values)を表示します。

2.1.5 ポリシー適用状況



ポリシーの適用状況では、登録されたすべてのポリシー名と各ポリシー別適用/不適用エージェント数を表示します。

2.1.6 ログ統計



エージェント全体のログを確認することができます。各ログをクリックすると、エージェントごとの詳細ログが表示されます。

※画面例



ダッシュボードの「ログ統計」から「脅威ログ」を選択し、「ログ管理」の「脅威ログ」画面が表示されています。

2.2 ポリシー管理



ポリシー管理では複数のポリシーの作成・管理ができ、各ポリシーが適用されるエージェントは自動でAppCheckProの設定内容が反映されます。

※ポリシーによる設定内容反映は、CMS Cloudサーバとエージェントの間で同期が必要であるため、約15分程かかります。

※デフォルトポリシーは「基本ポリシー」となり、「基本ポリシー」を適用した「対象エージェント数」・「適用されたエージェント数」は表示されません。

※個別ポリシーを各エージェントに適用する場合は、エージェント画面(2.3を参照)に移行し、対象エージェントを指定後「個別ポリシー適用」ボタンを押してください。

ポリシー管理のカラム(Column)は、ポリシーID、ポリシー名、Type、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、説明があり、フィルターで選択されている項目が表示されます。

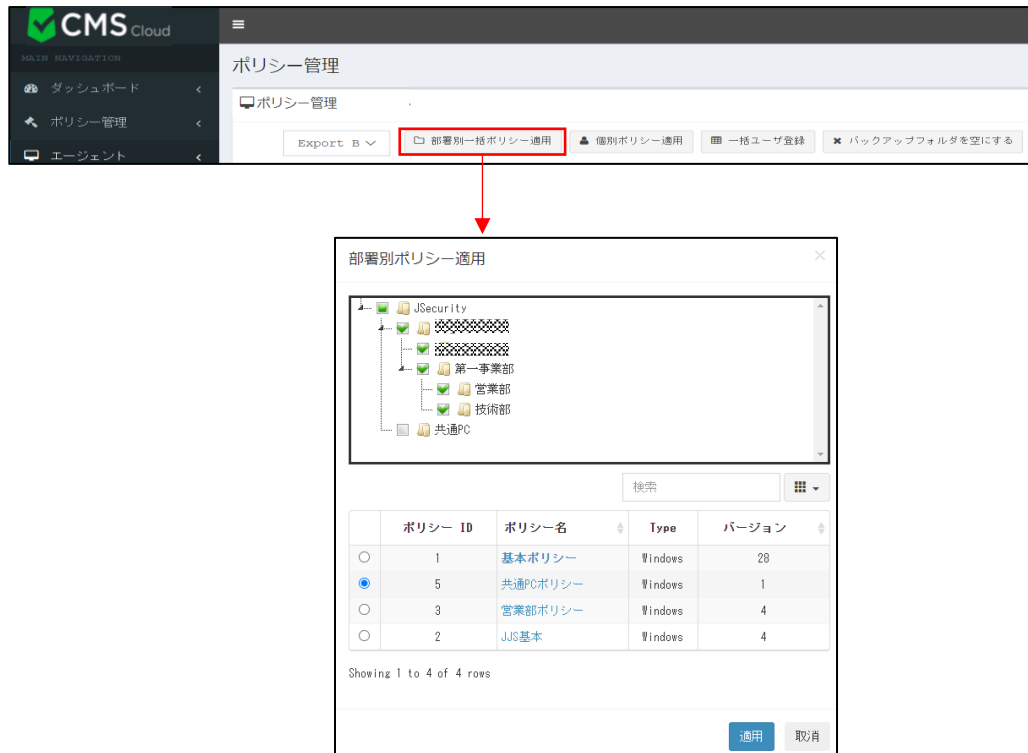
- ・**ポリシーID**：自動採番により、各ポリシーに付与された番号が表示されます。
- ・**ポリシー名**：任意で設定できるポリシーの名称が表示されます。(2.2.1「ポリシー追加および削除」参照)
- ・**Type**：ポリシーのOSタイプ(Windows)が表示されます。
- ・**初期生成時間**：ポリシーを登録した時間が表示されます。
- ・**最終変更時間**：ポリシーを修正した最終時間が表示されます。
- ・**最終適用時間**：ポリシーを対象エージェントに適用した最終時間が表示されます。
- ・**バージョン**：ポリシーの登録、修正回数(ポリシーのバージョン管理)
- ・**対象エージェント数**：ポリシーを適用するエージェント数が表示されます。
(「基本ポリシー」適用エージェント数はカウントされません。)
- ・**適用されたエージェント数**：ポリシーを適用されたエージェント数が表示されます。
(「基本ポリシー」適用エージェント数はカウントされません。)
- ・**オンラインエージェント数**：オンライン状態のエージェント数が表示されます。

(「基本ポリシー」適用エージェント数はカウントされません。)

- ・説明：お客様が自由に記入できるポリシー説明項目となります。

2.2.1 部署別一括ポリシー適用

「ポリシー管理」⇒「部署別一括ポリシー」メニューから部署を指定し、ポリシーを一括適用することが可能です。



The screenshot shows the CMS Cloud interface with the 'Policy Management' page. A red box highlights the 'Deployment Policy Application' button. A red arrow points to a dialog box titled '部署別ポリシー適用' (Deployment Policy Application). The dialog contains a tree view of the organization structure and a table of policies.

Organization Structure:

- JSecurity
 - 第一事業部
 - 営業部
 - 技術部
 - 共通PC

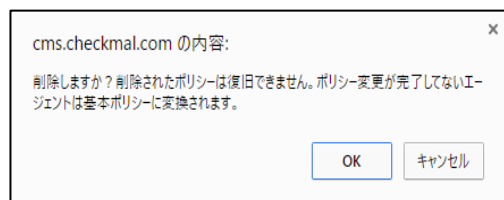
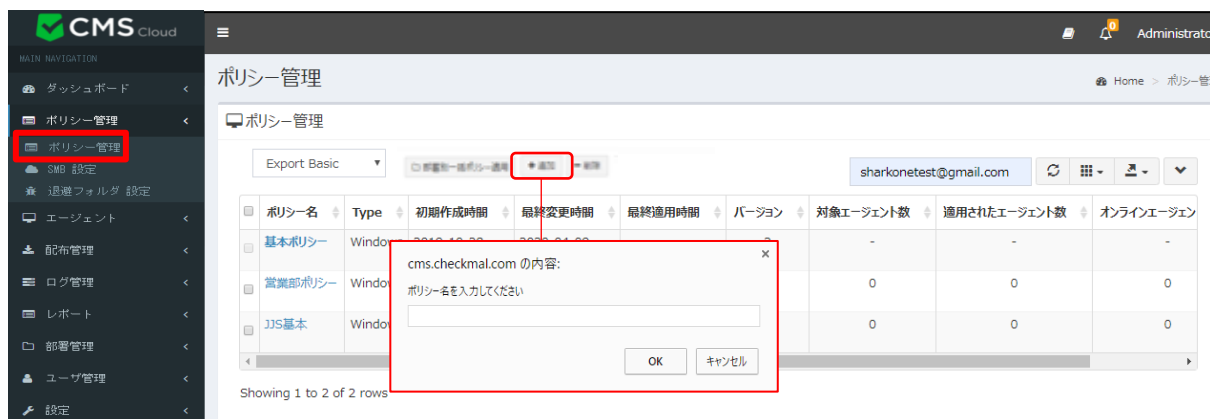
| | ポリシー ID | ポリシー名 | Type | バージョン |
|----------------------------------|---------|----------|---------|-------|
| <input type="radio"/> | 1 | 基本ポリシー | Windows | 28 |
| <input checked="" type="radio"/> | 5 | 共通PCポリシー | Windows | 1 |
| <input type="radio"/> | 3 | 営業部ポリシー | Windows | 4 |
| <input type="radio"/> | 2 | JIS基本 | Windows | 4 |

Showing 1 to 4 of 4 rows

Buttons: 適用 (Apply), 取消 (Cancel)

2.2.2 ポリシーの追加・削除、ファイルの出力・検索

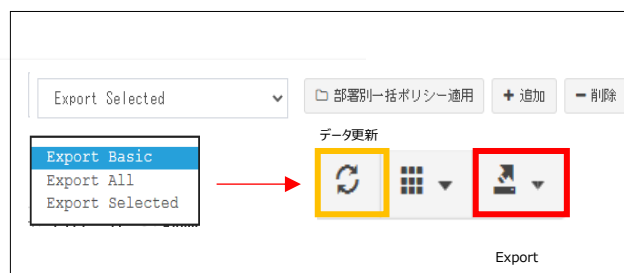
新しいポリシーを追加する場合は、「追加」ボタンをクリックし、ポリシー名を入力してください。



既に登録済みのポリシーを削除する場合は、該当ポリシーを選択し、「削除」ボタンをクリックしてください。

※削除されたポリシーに適用されていたエージェントには、自動的に基本ポリシーが適用されます。

また、ポリシーをCSVやExcelでExportし、詳細内容を確認することも可能です。



- Export Basic : 現在表示されているWeb画面の内容をExportする
- Export All : 全てのデータをExportする
- Export Selected : 選択した部分のみExportする



また「ポリシー名」、「Type」、「説明」でポリシーを検索することも可能です。

2.2.3 ポリシー管理 : 一般

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 退避フォルダ 自動バックアップ 例外設定

ポリシー説明 :

Enter ...

リアルタイムセキュリティを常に設定する。

Lock Mode : OFF

個別ユーザポリシー変更許可

ライブチェック周期 : 15分毎(デフォルト値)

アプリケーション削除許可

お知らせ領域アイコン使用

プログラム実行遮断時、お知らせダイアログ実行

自動アップデート使用

MBR保護

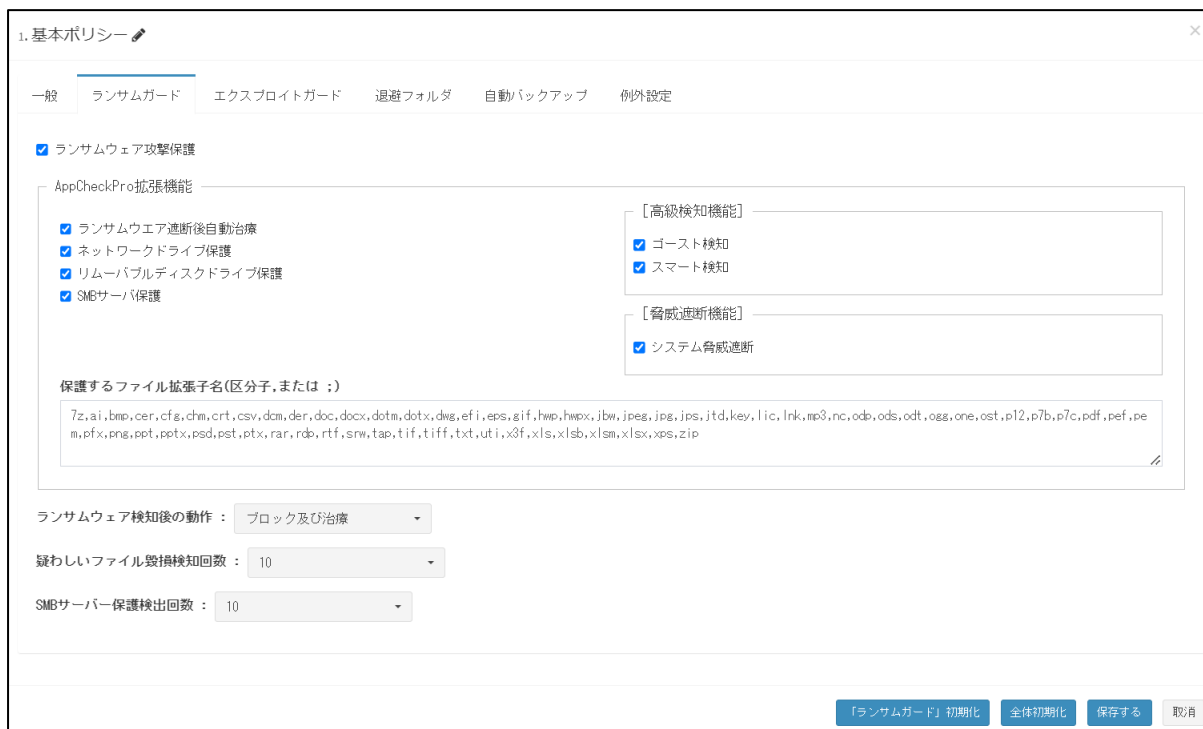
自己保護機能使用

検出時、疑いのあるファイルを転送する
(匿名で処理され、分析以外の目的では使用されません。)

- ・**ポリシー説明** : 該当ポリシーに対する詳細説明を自由に記入できます。
- ・**リアルタイムセキュリティを常に設定する** : AppCheckProエージェントのリアルタイムセキュリティ機能を常に有効にします。
- ・**LockMode** : ONにすると、ユーザがAppCheckProのオプションの変更できないようLockがかかります。
- ・**個別ユーザポリシー変更許可** : エージェントユーザ側から、AppCheckProの設定内容を自由に変更できるようにします。**※ポリシー内容が適用されなくなります。**
- ・**ライブチェック周期** : エージェントにポリシーを適用する際の同期化周期を設定することができます。**※3分、7分、10分、15分(デフォルト)、20分、30分、1時間周期で設定できます。**
- ・**アプリケーション削除許可** : エージェント側で行うAppCheckProアンインストールを許可します。**※デフォルト設定として、チェック(アンインストール許可) 済となっています。**
- ・**お知らせ領域アイコン使用** : AppCheckProアイコンを、タスクバーのお知らせ領域に表示します。
- ・**プログラム実行遮断時、お知らせダイアログ実行** : ランサムウェア検知時、タスクバーのお知らせ領域に遮断お知らせダイアログを表示します。
- ・**自動アップデート使用** : 3時間周期で、AppCheckProのCARBエンジン最新アップデート内容を自動確認し、アップデートを行います。
- ・**MBR保護** : Master Boot Record (MBR)領域を毀損しようとするファイルの実行を遮断します。
- ・**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)、ファイル、レジストリを無力化ツールや悪性攻撃から保護します。
- ・**検出時、疑いのあるファイルを転送する** : ランサムガード、エクスプロイトガードで検出された疑わしいファイルを

Checkmal社へ転送します。(匿名で処理され、分析以外の目的では使用しません)

2.2.4 ポリシー管理 : ランサムガード



・**ランサムウェア攻撃保護** : ランサムウェア攻撃によりファイル毀損が検知されたら、ランサムウェア動作検知お知らせダイアログが表示され、該当プロセスは遮断されます。

・**ランサムウェア遮断後自動治療** : 検知されたランサムウェアを自動治療(削除)します。

・**ネットワークドライブ保護** : ネットワークドライブ内のファイルが、AppCheckがインストールされたPCから実行されたランサムウェア攻撃により毀損されたら検知、遮断、自動復元を行います。

・**リムーバブルディスクドライブ保護** : USBメモリまたはCFメモリに保存されたファイルがランサムウェアによって暗号化された場合、検知、遮断、自動復元を行います。

* USB接続HDDは通常のランサムウェア攻撃保護機能にて保護されます。

・**SMBサーバ保護** : 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、「レポート先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。

・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。

・高級探知機能 - スマート探知

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。

・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。

・**保護するファイル拡張名（区分子,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名は(7z,ai,bmp,cer,cfg,chg,crt,css,dcm,der,doc,docx,dotm,dotx,dwg,efi,eps,gif,hwp,hwpj,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)で総65種となります。

新規拡張子の追加修正も可能です。

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、「保護する拡張名（区分子,または;）」設定画面内の「初期化」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。

・ランサムウェア検知後の動作：ランサムウェアを検知時の動作を設定します。

- ブロック及び治療：ランサムウェアを検知すると、ブロック・削除・復元を正常に行います。（デフォルト値）
- ログのみ残す：ランサムウェアを検知すると、検知ログのみ残し、ブロック・削除・復元は行いません。（リアルタイムバックアップは実施）

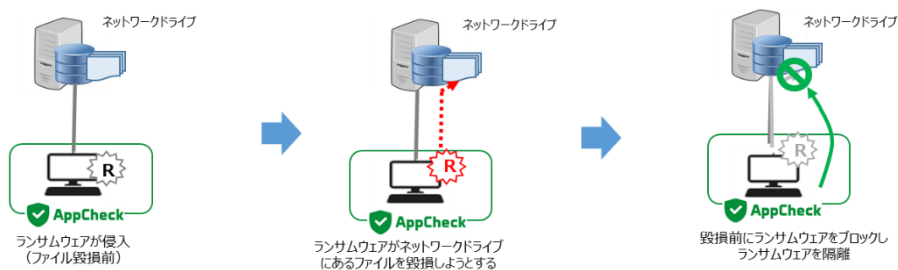
・疑わしいファイル毀損検知回数：ランサムウェアとして判断する「ファイル毀損検知回数」を設定できます。

*デフォルトはファイル10個となっており、1～100まで設定可能です。

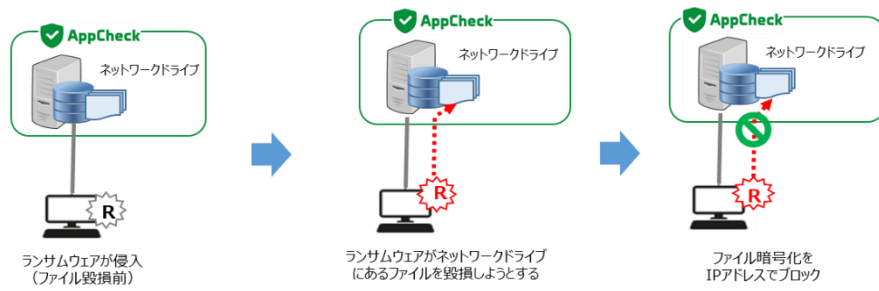
・SMB サーバー保護検出回数：遠隔地 PC からのアクセスによるファイル変更をランサムウェア攻撃として判断する「ファイル毀損検知回数」を設定できます。

*デフォルトはファイル10個となっており、1～100まで設定可能です。

<ネットワークドライブ保護>



<SMBサーバ保護>



[ご注意]

バックアップフォルダ<Backup(AppCheck)>を削除するためには、AppCheckProの「リアルタイムセキュリティ」を一時的に解除する必要があります。

2.2.5 ポリシー管理 : 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。

※エクスプロイトガードを使用する場合、必ず「エクスプロイトガードを使用」のチェックボックスと「保護するアプリケーション」のチェックボックスに両方チェックして下さい。また「エクスプロイトガードを使用」を off にした場合は、「保護するアプリケーション」を有効にしても機能は適用されませんのでご注意下さい。

保護するアプリケーション

| | |
|-----------|---|
| Web ブラウザ | Internet Explorer、Microsoft Edge、Chrome、Firefox、Opera |
| プラグイン | Java、Adobe Flash |
| メディアプレーヤー | Windows Media Player、Windows Media Center、GomPlayer、PotPlayer |
| オフィス | Microsoft Office、Hancom Office、Adobe Acrobat |

2.2.6 退避フォルダ

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 **退避フォルダ** 自動バックアップ 例外設定

リアルタイムバックアップ実行

退避フォルダパス :

一つのファイルの大きさを最大 以下に制限

ランサムウェア退避フォルダ非表示

退避フォルダ自動削除

経過したファイルを自動削除

退避フォルダ容量がディスクの になると、古い順でファイルを自動削除

※手動削除を行う場合は、「AppCheck」 - 「オプション」 - 「一般」 - 「自己保護機能使用」をオフにした後に削除してください。

・リアルタイムバックアップ実行 : AppCheckProのリアルタイムバックアップ機能をon/offにすることができます。

※デフォルト設定は「on」となっております。

退避フォルダパス 

ランサムウェア退避フォルダを指定
(以下のフォルダを除く)

- ?:*
- ?:\Windows
- ?:\Program Files
- ?:\Program Files (x86)
- ?:\Users
- ?:\Windows*
- ?:\Program Files*
- ?:\Program Files (x86)*
- ?:\Users*

- ・**退避フォルダパス**：設定ボタンをクリックし、退避フォルダのパスを指定することができます。
- ・**一つのファイルの大きさを最大〇〇以下に制限**：リアルタイムバックアップの対象ファイル容量を設定できます。100MB、200MB、500MB、1GB（デフォルト）、2GB、5GB単位で設定可能です。
※デフォルト設定は「機能off」となっております。
- ・**ランサムウェア退避フォルダ非表示**：指定した退避フォルダを非表示にします。
※デフォルト設定では「機能off」となっております。
- ・**退避フォルダ自動削除（〇〇経過したファイルを自動削除）**：指定した時間を経過すると退避フォルダを自動削除します。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（デフォルト）、7日単位で設定可能です。
※デフォルト設定では、「機能on」となっております。
- ・**退避フォルダ自動削除（退避フォルダ容量がディスクの〇〇になると、古い順でファイルを自動削除）**：退避フォルダ内の容量が指定した容量になったら、退避フォルダ内のファイルを古い順で自動削除します。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%単位で設定が可能です。
※デフォルト設定は、「機能off」となっております。

2.2.7 ポリシー管理 : 自動バックアップ

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

自動バックアップ使用 スケジュール設定

バックアップする対象 追加 除去

除外する対象 追加 除去

バックアップする場所

ローカルディスク ネットワーク共有フォルダ (SMB/CIFS)

サーバーアドレス

ユーザーID

共有フォルダ

パスワード

履歴ファイル保存数 : 3

FORNストレージモード

※手動削除を行う場合は、「AppCheck」-「オプション」-「一般」-「自己保護機能使用」をオフにした後に削除してください。

印刷 保存する 取消

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。また、ネットワークドライブ上に設定するのであればフォルダへのアクセス時にログイン情報ができるように設定し、アクセスを制限することがお勧めです。もし、アクセスを制限することが難しいのであれば、なるべく自動バックアップ先をAppCheckエージェント端末のローカルディスク内に設定することはより安全であり、どうしてもネットワークドライブ上へのパス設定が必要な場合は重要度が低いファイルだけバックアップするようにしてください。

- ・**自動バックアップ使用** : 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時間単位で設定可能です。
- ・**バックアップする対象** : 管理者の選択によってバックアップする対象フォルダを追加、削除することが可能です。
(※例 : %USERPROFILE%\Documents 、 %USERPROFILE%\Favorites)
- ・**指定した拡張子名だけバックアップ (区分子,または;)** : バックアップする対象フォルダに含まれたファイルのうち、指定した拡張子名に該当するファイルのみバックアップすることができます。
(※例 : 「doc、hwp、jpg」または「doc;hwp;jpg」など)

・**除外する対象**：「バックアップする対象」に含まれるサブフォルダを指定し、自動バックアップから除外するフォルダを指定できます。

・**バックアップ時除外するファイル拡張子名（区分子,または;）**：バックアップする対象フォルダに含まれたファイルのうち、指定したファイル拡張子名はバックアップから除外するように設定できます。

・**バックアップする箇所**：バックアップする対象フォルダを保存する自動バックアップフォルダ<AutoBackup(AppCheck)>の場所を設定できます。ローカルディスク、ネットワーク共有フォルダ(SMB/CIFS)から選択してください。

・**履歴ファイルの保存数**：自動バックアップフォルダ内のファイルを最大10までhistory fileとして保存できます。

※デフォルト設定は「3」となっております。設定個数を超える場合は、古い順で削除されます。

- バックアップタイミング：同一ファイル名で、ファイル内のデータが変更された場合
- バックアップファイルのファイル名形式:[拡張子を含む元のファイル名.14桁の生成時間.history]
(ex: samplefile.txt.20210810111631.history)
- 復元方法：日付とhistoryを削除し、拡張子を含めた元のファイル名に変更してください。

・**ネットワーク共有フォルダ(SMB/CIFS)**：サーバアドレス（リモートIPアドレスまたはリモートPC名）、共有フォルダ（共有設定が行われたリモートドライブ、フォルダ名）、ネットワーク共有フォルダのユーザID、パスワードを正確に入力してください。

・**WORMストレージモード**：WORMディスク（1回記録後、修正不可方式）にファイルをバックアップします。

※デフォルト設定は「off」となっております。

2.2.8 ポリシー管理：例外設定（ユーザ指定除外ファイル）

※CMS Cloudの「配布管理」にてインストールされているエージェントが1台も存在しない場合と、V2.5(旧バージョン)のみインストールされている場合は、旧表記「**ユーザ指定除外ファイル**」として以下画面が表示されます。

<旧表記画面>



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 退避フォルダ クリーナー 自動バックアップ **ユーザ指定除外ファイル**

以下に登録されたファイルは常に許可 [追加](#) [削除](#)

ユーザ指定除外ファイル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。

※新表記の「**信頼済みプロセスリスト**」に該当します。

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お願いいたします。

・**以下に登録されたファイルは常に許可**：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。

<新表記画面>

◎ 信頼済みプロセスリスト

信頼済みプロセスリスト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お願いいたします。

・以下に登録されたファイルは常に許可：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。

◎ 例外ファイル一覧

保護する拡張子に該当するファイルの中、例外ファイル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常に許可：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。

◎ 例外フォルダ一覧

例外フォルダ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。

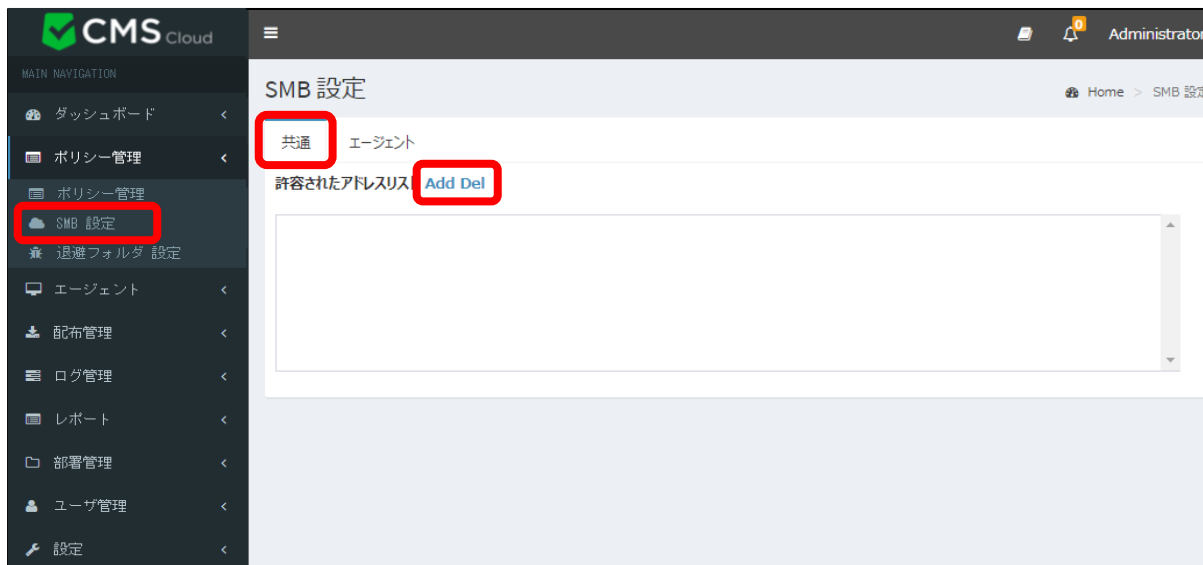
※検知されないため、退避フォルダへのバックアップ、復元も行われません。

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。

・以下の登録済みフォルダへの実行を許可する：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。

「例外ファイル一覧」または「例外フォルダ一覧」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。

2.2.9 SMB設定



- SMB 設定 → 「共通」：許可されたアドレスリストの追加や削除が可能です。

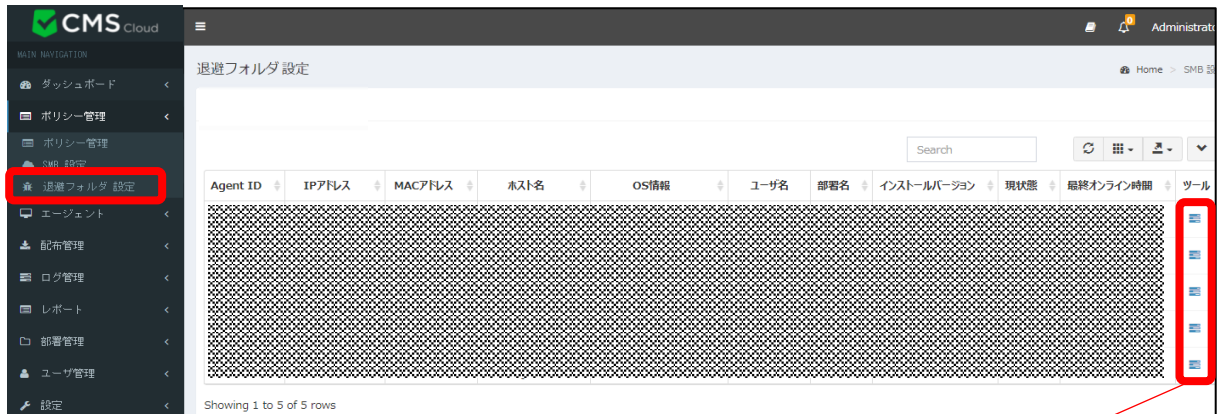


- SMB設定 → 「エージェント」：エージェント別のSMB許可/遮断が可能です。



- SMB設定 → 「エージェント」 → 「SMB設定の初期化」：SMB設定を初期化します。

2.2.10 退避フォルダ設定



- ・退避フォルダ設定： エージェント別の退避フォルダ設定が可能です。

退避フォルダ設定

リアルタイムバックアップ実行
退避フォルダパス：

一つのファイルの大きさを最大 以下に制限

ランサムウェア退避フォルダ非表示

退避フォルダ自動削除

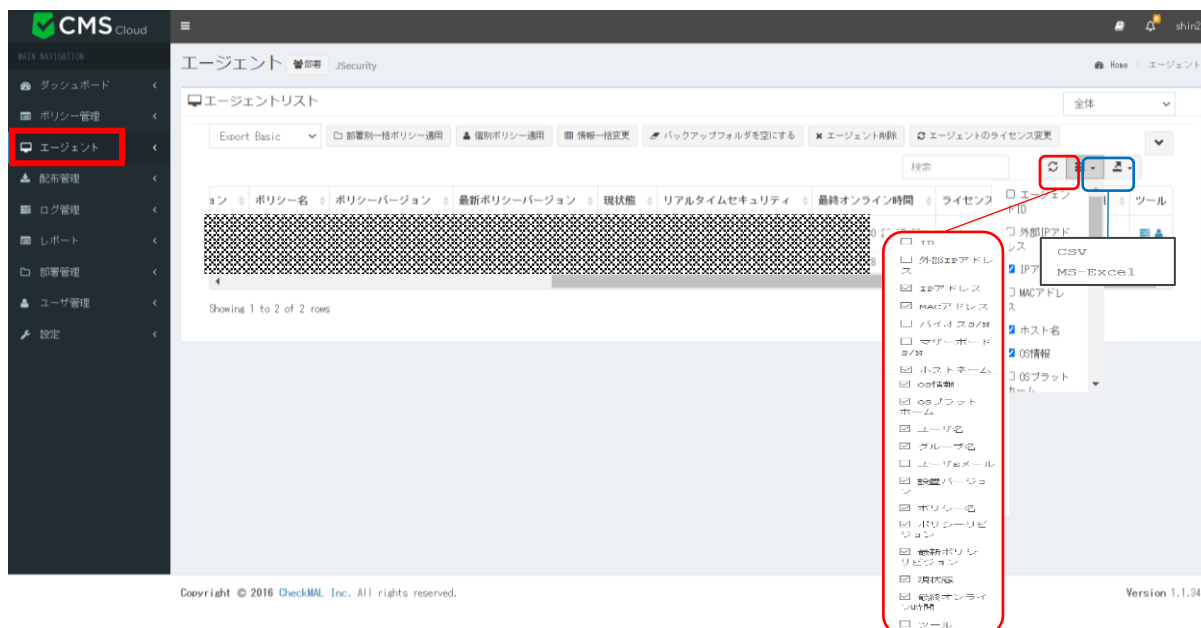
経過したファイルを自動削除

退避フォルダ容量がディスクの になると、古い順でファイルを自動削除

※自動バックアップフォルダを手動で削除する場合は、リアルタイムセキュリティをOffにしてから削除してください

(設定内容については ※2.2.6 「退避フォルダ」をご参考ください)

2.3 エージェント



エージェントは、CMS Cloudを通じて配布され、インストールされた全てのエージェントServer/PCリストを表示し、リストに表示されたエージェントに対する部署別/個別ポリシー適用、エージェント削除および一括ユーザ登録ができます。またエージェントリストデータは "Export data"メニューにより、CSVまたはMS-Excelファイルフォーマットでエクスポートできます。※リストの緑色は、現在、AppCheckエージェントがオンライン(Online)で、実行中の状態を意味します。(リアルタイムではないため、実行中であっても、オフラインだと表示される場合があります。) ※白色：オフライン

※ポリシー（2.2 を参照）を各エージェントに適用するには、エージェント画面に移行し、対象エージェントを指定後「個別ポリシー適用」ボタンを押して頂ければ適用となります。

※個別ポリシーを適用していないエージェントには「基本ポリシー」が適用となります。

エージェントリストに表示されるカラム(Column)には ID、外部 IPアドレス、IPアドレス、MACアドレス、BIOS S/N、マザーボード S/N、ホストネーム、OS情報、OSプラットフォーム、ユーザ名、グループ名、ユーザEメール、インストールバージョン、ポリシー名、ポリシーリビジョン、最新ポリシーリビジョン、現状態、最終オンライン時間、ツールで分類されており、選択した各項目を表示します。

[ご注意]

オフライン端末へのポリシー適用については、一度オンラインにしてから適用してください。

各エージェントのポリシー適用状況は、ポリシー名 およびポリシーリビジョン/最新ポリシーリビジョンにてご確認ください。

- ・ ポリシーリビジョンはエージェントに適用されたポリシー名の改訂リビジョン番号
- ・ 最新ポリシーリビジョンは「ポリシー設定」にて登録されたポリシーの最新リビジョン番号となります。
- ・ 最新ポリシーリビジョンとポリシーリビジョンが異なったリビジョンの場合、最新リビジョンを適用してください。

・**エージェントID**：エージェントがインストールされたPC番号

- ・外部IPアドレス：エージェントがインストールされたPCのグローバルアドレス
- ・IPアドレス：エージェントがインストールされたPCの内部IPアドレス
- ・MACアドレス： エージェントがインストールされたPCのMACアドレス
- ・BIOS S/N： エージェントがインストールされたPCのBIOSシリアルナンバー
- ・マザーボード S/N： エージェントがインストールされたPCのマザーボードシリアルナンバー
- ・ホストネーム： エージェントがインストールされたPC名
- ・OS情報： エージェントがインストールされたPCのOS
- ・OSプラットフォーム： エージェントがインストールされたPCのOSプラットフォーム
- ・ユーザ名： エージェントがインストールされたPCのユーザ名
- ・グループ名： 部署管理（ 2.7 部署管理 を参照ください）で登録された部署名
- ・ユーザEメール： ユーザのEメール（ 2.8 ユーザ管理 を参照ください）
- ・インストールバージョン： インストールされたAppCheck Proのバージョン情報
- ・ポリシー名： CMS Cloudで登録されたポリシー名（ 2.2 ポリシー管理 を参照ください）
- ・ポリシーリビジョン： エージェントに適用されたポリシーリビジョン
- ・最新ポリシーリビジョン： CMS Cloudに登録されたポリシー名の最新ポリシーリビジョン
- ・現状態： エージェントがインストールされたPCのインターネット接続状態。 オンライン・オフラインを確認できます。
- ・最終オンライン時間： オンライン状態の最終時間
- ・ライセンス： 該当エージェントに適用されているライセンスを表示します。
- ・ライセンス満了日： 適用されているライセンスの満了日を表示します。
- ・ツール： エージェントがインストールされたPCとユーザを簡易的に紐づけることが可能です。
またエージェントログビューを表示することが可能です。

ライン時間 ツール

| | | |
|--------------|--|--|
| -02 16:37:13 | | |
| -02 16:27:24 | | |
| -02 16:28:27 | | |
| -25 11:27:20 | | |

<ユーザ紐づけ>

<ログビュー>

ログビュー

| 日付 | 水準 | 区分 | 内容 |
|---------------------|----|-----------|--------------------|
| 2017-10-02 14:52:14 | 一般 | サービスプログラム | オプションを再設定しました。 |
| 2017-10-02 14:52:14 | 一般 | 自動バックアップ | 自動バックアップ処理が開始しました。 |

既存ユーザ検索 新規追加

検索

| | 部署名 | ユーザ名 | Eメール |
|-----------------------|-----------|------|------|
| <input type="radio"/> | JIRANSOFT | | |
| <input type="radio"/> | JIRANSOFT | | |
| <input type="radio"/> | JIRANSOFT | | |
| <input type="radio"/> | | | |

Showing 1 to 5 of 65 rows 5 rows per page

適用 取消

2.3.1 部署別一括ポリシー適用



部署別ポリシー適用では、ポリシー管理から追加されたポリシーを部署別を選択して適用できます。

2.3.2 個別ポリシー適用



個別ポリシー適用では、部署別一括ポリシー適用ではない個別エージェントに対するポリシー適用をサポートし、リストに表示された特定エージェントを選択してポリシーを適用できます。

2.3.3 情報一括変更



情報一括変更では、所定フォーマットをダウンロードしファイル作成しアップロードすることで、多数のインストール済エージェントユーザを一括修正登録することができます。

| 現在設置されたエージェント情報(変更禁止) | | | | | | ユーザ情報 | |
|-----------------------|-------------|----------|------------|------------|------------|-------------|----------|
| Agent ID | MAC Address | Hostname | IP Address | 外部 IP アドレス | エージェントユーザ名 | ユーザEメール(必須) | ユーザ名(必須) |
| 3401 | | | | | | | |
| 3404 | | | | | | | |

変更できる内容は、ユーザEメール、ユーザ名となります。

2.3.4 バックアップフォルダを空にする

The screenshot shows the 'Agent List' page in CMS Cloud. The 'Backup folders to empty' button is highlighted in the top navigation bar. Below, two panels show the 'Backup folders to empty' dialog. The left panel shows the 'Empty by agent' option selected, and the right panel shows the 'Empty by deployment' option selected.

自動バックアップ(2.2.4 ポリシー管理：自動バックアップ)で指定したバックアップフォルダ内のファイルを「空」にすることができます。

また検疫所(2.5.2 検疫所を参照ください)で検知した“Backup (AppCheck) ”フォルダ内のファイルを「空」にすることができます。

対象は、ユーザ毎または部署毎で設定することが可能です。

2.3.5 エージェント削除

The screenshot shows the 'Agent List' page in CMS Cloud. The 'Delete Agent' button is highlighted in the top navigation bar. Below, a confirmation dialog is shown asking if the user wants to delete the agent and its associated information.

エージェント削除をすると、該当のエージェントPCからライセンスの削除をすることができます。

※削除まで約1時間かかります。

2.3.6 エージェントのライセンス変更



エージェントに適用されているライセンスを、同タイプ(PC版かサーバ版)の他のライセンスに変更することができます。

2.4 配布管理

2.4.1 各ライセンス毎のインストールファイルダウンロード、配布



CMS Cloudインストール認証キーが含まれたAppCheck Pro for Windows Server、AppCheck Pro製品はインストールファイルダウンロードまたはEメールを通じてクライアントへインストールプログラムファイルを配布できます。

配布されたAppCheck Proインストールプログラムファイルはインストール完了後、自動で製品登録を行います。管理者はCMS Cloudのエージェントリストを通じてインストールされたエージェント状況を確認できます。

- ・**ライセンス** : CMS Cloudの「ライセンス」に登録されているエージェント用のライセンスが表示されます。
- ・**インストール認証キー** : 該当ライセンスに付与されている認証キーが表示されます。
- ・**残余数量/数量** : 該当ライセンスの残り分/総数量が表示されます。
- ・**満了日** : 該当ライセンスの満了日が表示されます。

- ・**配布**：インストールファイルのダウンロードができます。
- ・**Silent配布**：実行時、インストールウィンドウを表示されない方式のインストールファイルのダウンロードができます。
- ・**Email**：該当インストールファイルをメールにて配布することができます。

[ご注意]

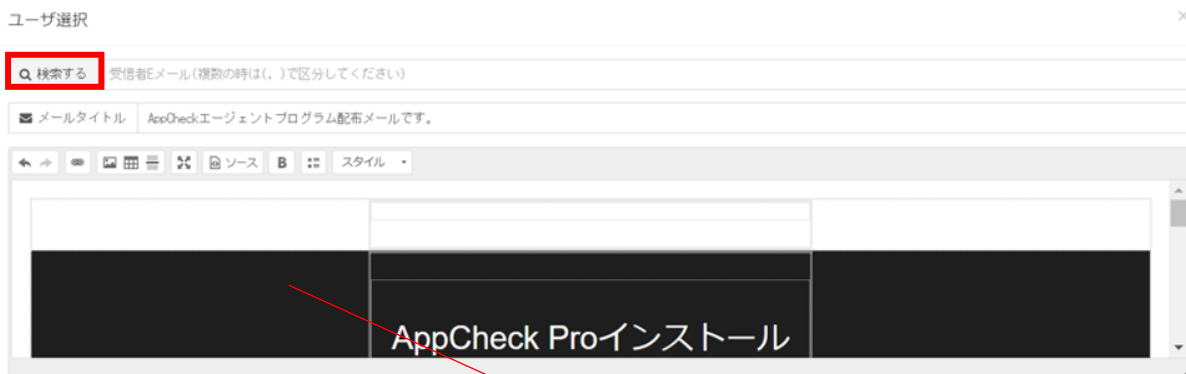
ダウンロードしたインストールファイル名を変更すると、インストールする際に認証キーを手動で入力する必要となりますので、ダウンロードしたインストールファイルはファイル名を変更しないようお願い致します。

2.4.2 クライアント配布：Eメール送信



Eメール方式でクライアントを配布する場合には、インストール認証キーとダウンロードリンクが含まれたEメールを送信できます。メールタイトル(デフォルト)は、「AppCheckエージェントプログラム配布メールです。」となります。管理者がメールタイトルと内容を直接修正して送信することもできます。

2.4.2.1 Eメール検索

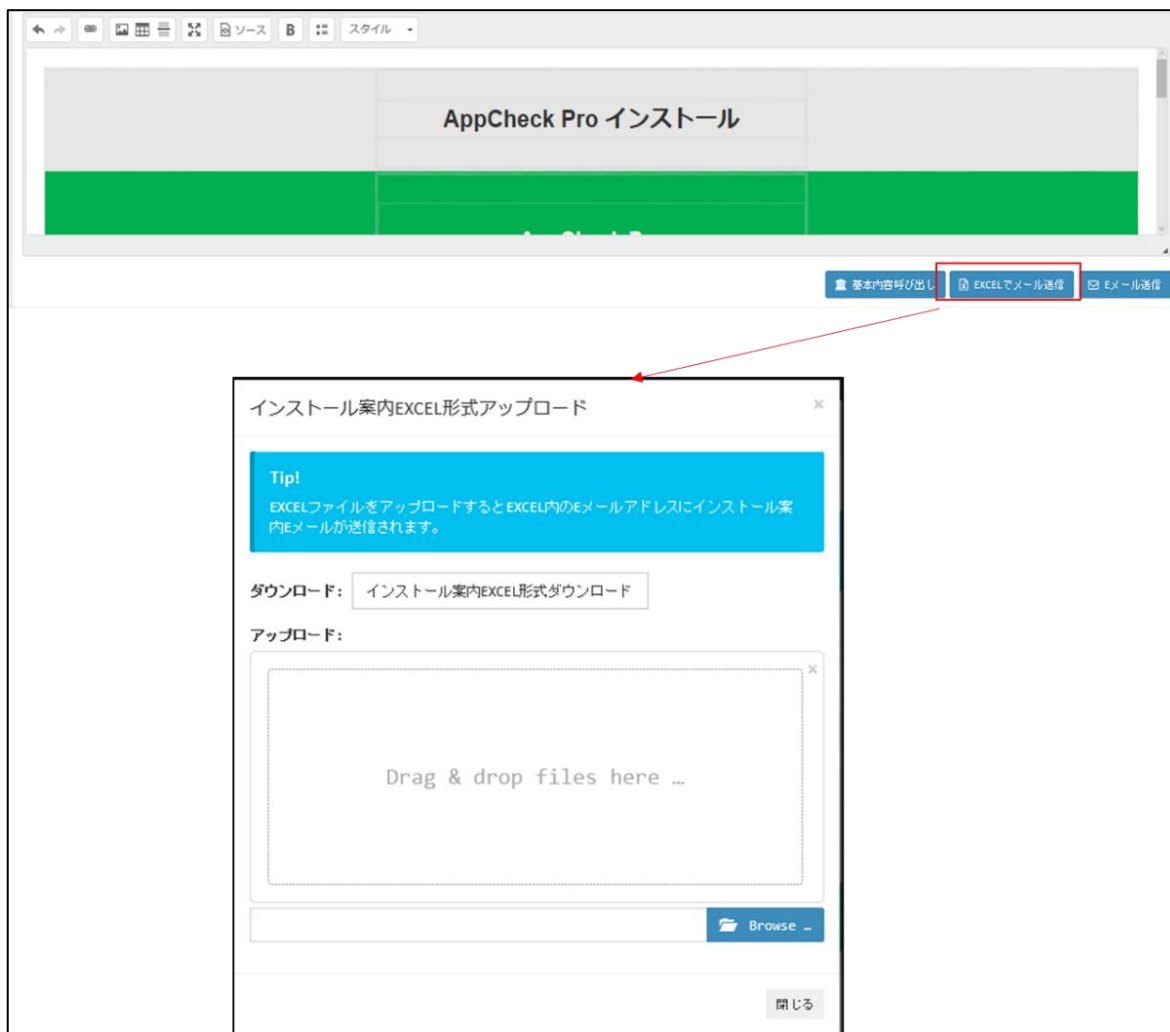


ユーザ選択ではユーザや部署を選択し、クライアントのEメール配布先を指定できます。

事前に部署管理（2.7 を参照）やユーザ管理（2.8 を参照）の登録を行い、適用するユーザを追加または削除することができます。

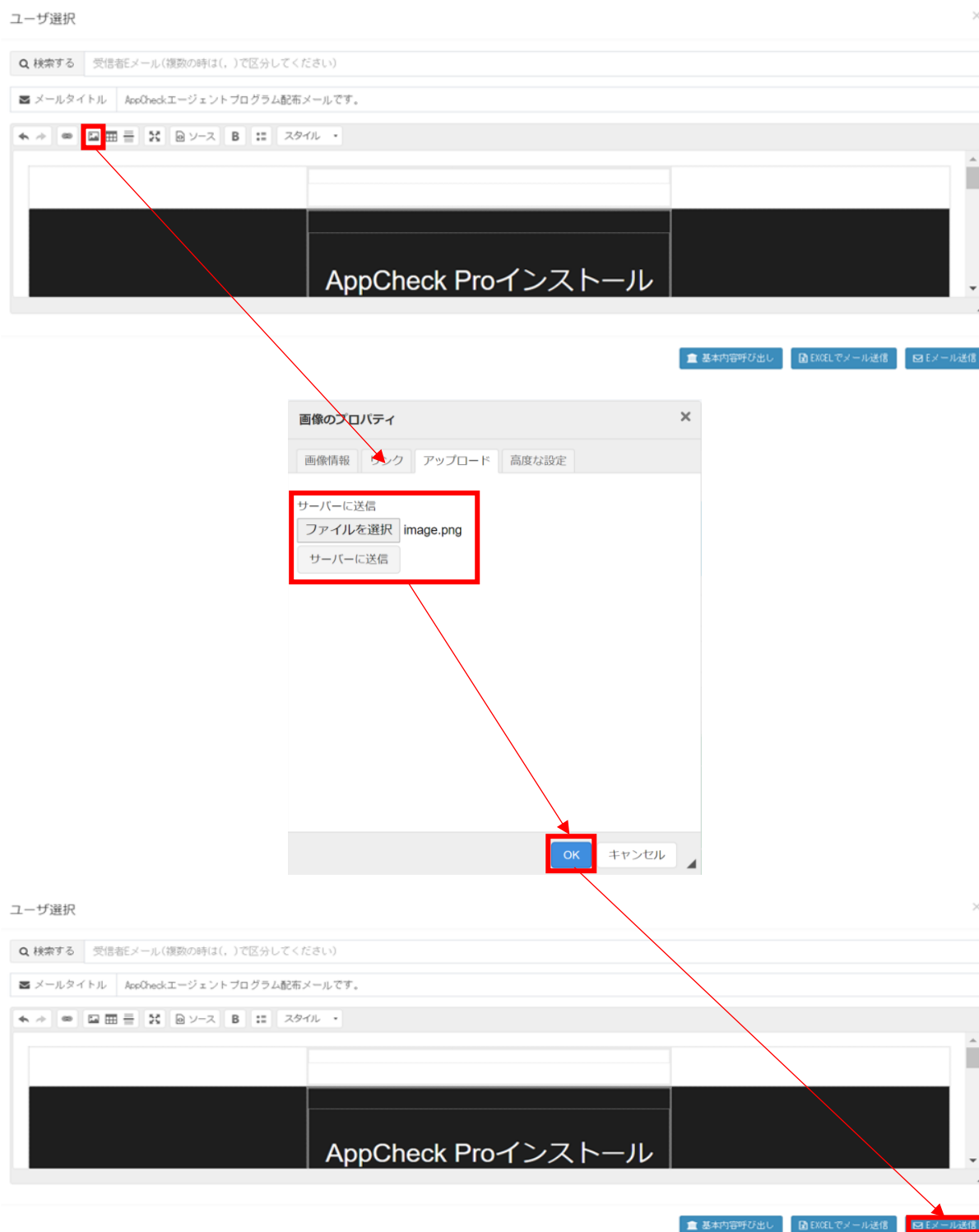
Eメール受信者が多数の場合にはコンマ(,)でメールアドレスを区分して、「検索する」ボタンをクリックし、個人(ユーザ)または部署に登録されたユーザへ送信できます。

2.4.2.2 エクセルでメール送信



事前にユーザ登録されていないクライアントにEメールでインストールプログラムを配布するためには「エクセルでメール送信」ボタンを押し、Excelファイル(.xls)をダウンロードし、ファイルにEメールリストを追加しアップロードした後、Eメールを送信するようにお願いします。

2.4.2.3 イメージ添付



インストーラー配布メールにイメージを添付するためには、「イメージ」>「ファイルを選択」>「サーバーに送信」の手順でファイルを一度サーバーにアップロードする必要があります。

その後「OK」ボタンを押し、「Eメール送信」ボタンでメールを送信してください。

2.4.3 ソフトウェア配布ツールを用いたインストールについて

手順1

・「配布管理」にて「インストールファイル」又は「Silentインストールファイル」をダウンロードしてください。

| クライアント配布 | | | | Home | 配布管理 |
|--|------------|-----------|------------|---------------------------------|-------------|
| Tip! AppCheckエージェントインストールファイルアドレスをEメールで送信して配布できます。 | | | | | |
| AppCheck Pro for Windows Server | | | | 現在の最新バージョン: 2.5.57.2 / 3.1.37.4 | |
| ライセンス | インストール認証キー | 残余数量 / 数量 | 満了日 | 配布 | Silent 配布 |
| XXXXXXXXXX | XXXXXXXXXX | 1 / 1 | 2024-12-31 | AppCheck V3 | AppCheck V3 |
| AppCheck Pro | | | | 現在の最新バージョン: 2.5.57.2 / 3.1.37.4 | |
| ライセンス | インストール認証キー | 残余数量 / 数量 | 満了日 | 配布 | Silent 配布 |
| XXXXXXXXXX | XXXXXXXXXX | 5 / 5 | 2024-12-31 | AppCheck V3 | AppCheck V3 |

注1) インストールファイルとは、ダウンロードしたファイルを実行し、インストールウィンドウを表示してインストールするファイルとなります。Silentインストールファイルはダウンロードしたファイルを実行し、インストールウィンドウを表示せずインストールするインストールファイルとなります。


注2) PC版のAppCheckProもサーバ版のAppCheckPro for Windows Serverも同じインストールファイルです。手順3を実施する際に機器のOSを判別し自動的にAppCheckPro又はAppCheckPro for Windows Serverをインストールします。

手順2

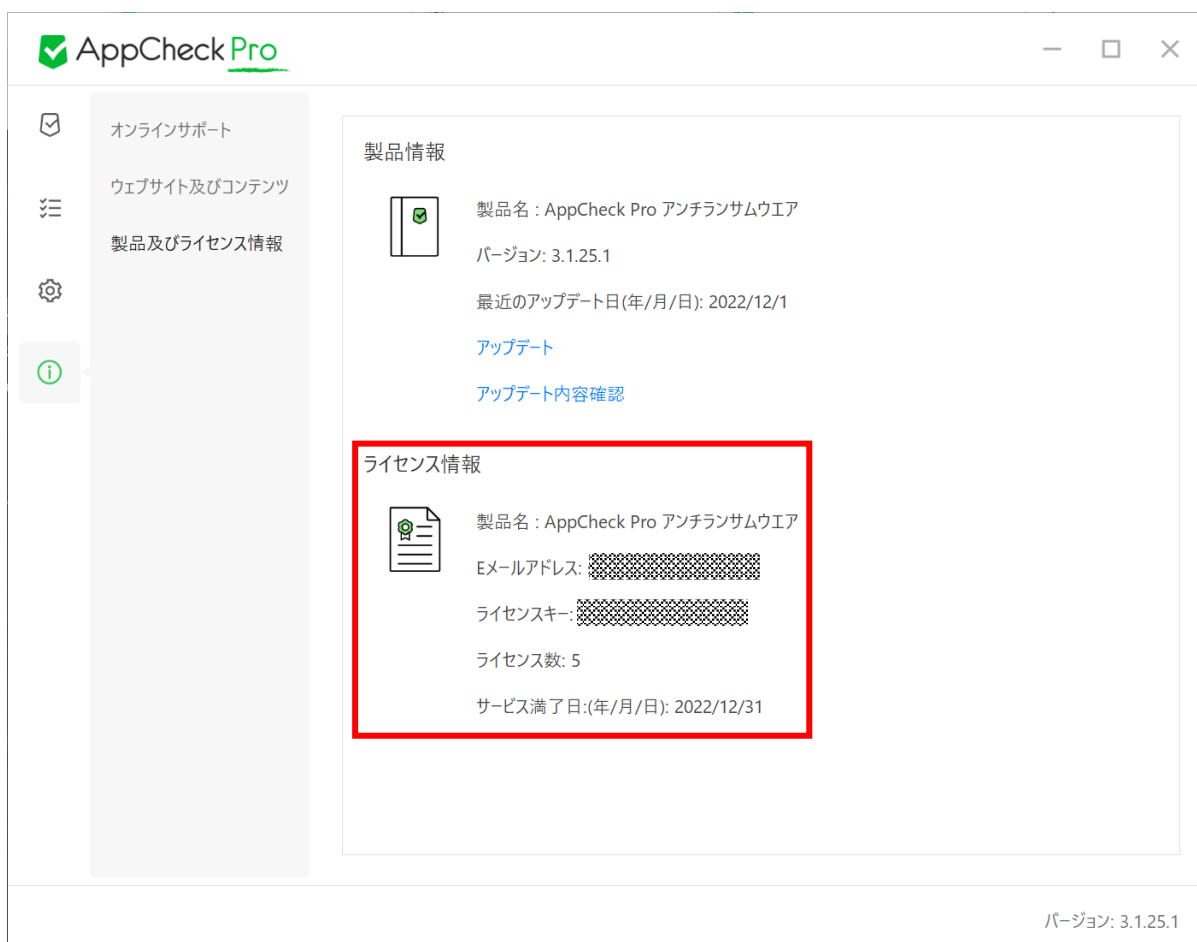
・ダウンロードしたインストールファイルを、ご利用される「ソフトウェア配布ツール」のマニュアルに従い、AppCheckProをインストールする端末に配布してください。

手順3

・配布されたインストーラーを端末内で実行し、AppCheck製品をインストールしてください。

| 名前 | 更新日時 | 種類 | サイズ |
|--|----------------|----------|-----------|
| ▼ 今日 (1) | | | |
|  AppCheckSetupCMS[Company=627896463332... | 2022/12/01 ... | アプリケーション | 15,894 KB |

・インストール完了後、AppCheckのライセンス情報欄に以下項目が表示されているかご確認ください。



The screenshot shows the AppCheck Pro application window. The left sidebar contains navigation options: オンラインサポート, ウェブサイト及びコンテンツ, 製品及びライセンス情報 (selected), and an information icon. The main content area is divided into two sections: 製品情報 and ライセンス情報. The 製品情報 section displays: 製品名: AppCheck Pro アンチランサムウェア, バージョン: 3.1.25.1, 最近のアップデート日(年/月/日): 2022/12/1, with links for アップデート and アップデート内容確認. The ライセンス情報 section, highlighted with a red box, displays: 製品名: AppCheck Pro アンチランサムウェア, Eメールアドレス: [redacted], ライセンスキー: [redacted], ライセンス数: 5, and サービス満了日(年/月/日): 2022/12/31. The bottom right corner of the window shows the version: バージョン: 3.1.25.1.

① インストールしたAppCheckの製品名

- ② ソフトウェア使用権利書に記載のEメールアドレス
- ③ ソフトウェア使用権利書に記載のライセンスキーの一部
- ④ ソフトウェア使用権利書に記載の保有のライセンス数量
- ⑤ ソフトウェア使用権利書に記載のサービス（ライセンス）満了日

※トライアルについて

ソフトウェア配布ツールでのAppCheck製品の配布の実績は多数ございますが、ソフトウェア配布ツールによっては正常に配布されない場合がございます。

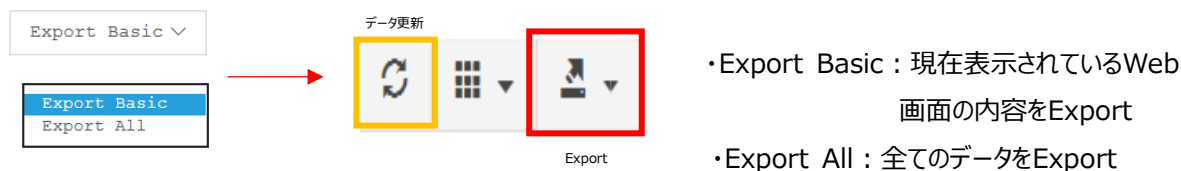
そのため、事前にテスト頂くことを推奨いたします。事前テストをされる場合は、AppCheck Proトライアルライセンス申込書にご記入頂きトライアルライセンスをお申込ください。

2.5 ログ管理

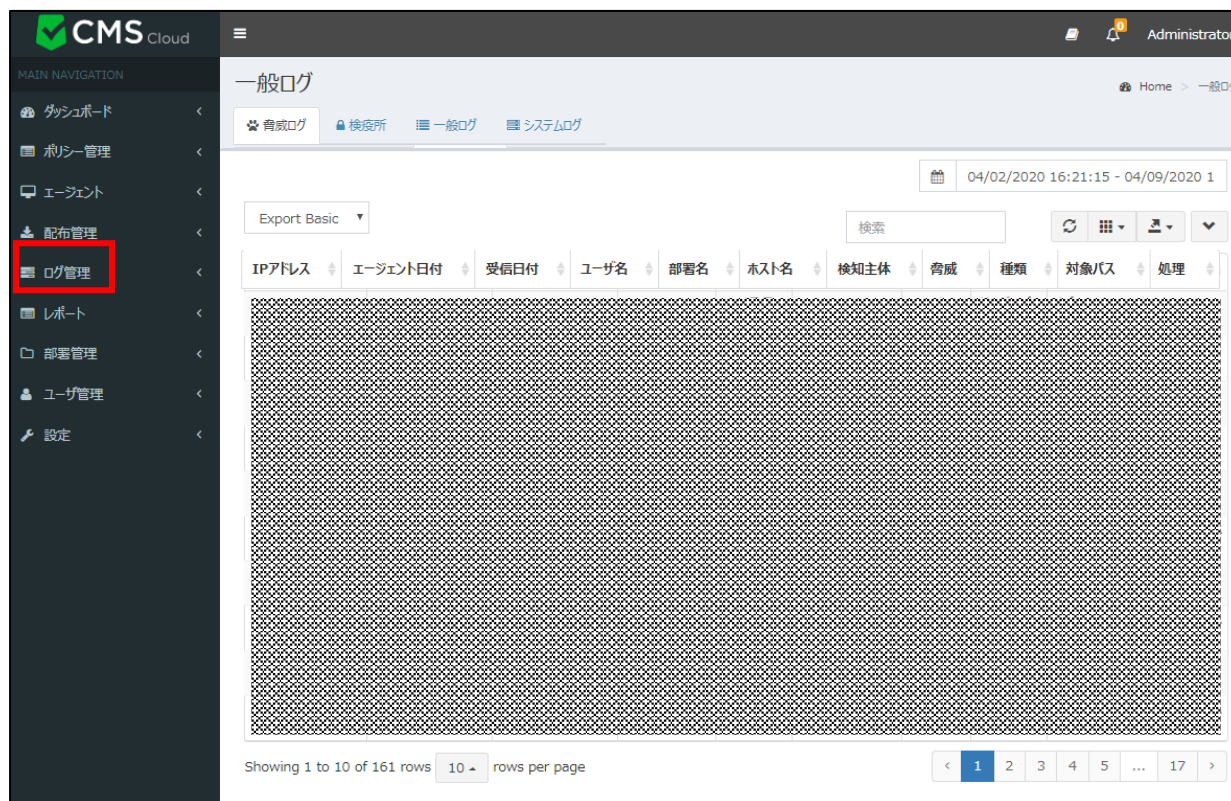
ログ管理ではAppCheckツールに記録される脅威ログ、検疫所、一般ログとシステムログ情報を提供します。

※全てのログデータが表示されるまで、時間がかかる場合がございます。

ログに記録されたデータは"Export data"メニューを通じてCSV、Excelファイルフォーマットでエクスポートできます。



2.5.1 脅威ログ



脅威ログはランサムガード、リアルタイムセキュリティ、システム検査により、遮断および削除された項目に対する情報が累積記録されます。

特にランサムガードで検知した脅威ログには、ランサムウェア情報、一部壊れたファイル自動復元情報、脅迫メッセージ自動削除情報、毀損時変更されたファイル名の自動復元情報が含まれています。

脅威ログカラム(Column) では ログID、エージェントID、外部 IPアドレス、IPアドレス、エージェント日付、受信日付、名前、部署、ホスト名、検知主体、脅威、種類、対象パス、処理で分類されています。

- ・**ログID** : 自動採番で脅威イベントログに番号を付与します
- ・**エージェントID**: エージェントがインストールされたPC番号
- ・**外部IPアドレス** : エージェントがインストールされたPCのグローバルアドレス
- ・**IPアドレス** : エージェントがインストールされたPCの内部IPアドレス
- ・**エージェント日付** : エージェント側で生成したイベントログの時間
- ・**受信日付** : エージェント側で発生したログをCMS Cloud側で受信した時間
- ・**ユーザ名** : ユーザ管理 (2.8 ユーザ管理を参照) にて登録したユーザ名
- ・**部署名** : 部署管理 (2.7 部署管理を参照) にて登録した部署名
- ・**ホスト名** : エージェントがインストールされたPC名
- ・**検知主体** : ランサムウェア行為・ファイル毀損・ファイル名変更脅威等を検知した機能。
「リアルタイムスキャン」「システム検査」「ランサムガード」のうち、いずれかで検知します。
- ・**脅威** : ランサムウェアによる脅威と思われる行為内容を表示します。
「ランサムウェアファイル名変更」「ランサムウェアアクション検知」「ランサムウェアファイル毀損」のうち、いずれかを表示します。
- ・**対象パス** : ランサムウェア行為・ファイル毀損・ファイル名変更脅威をAppCheck Proで検知したファイルパス
- ・**処理** : 脅威に対するアクションを表示します。
「検出」「ブロック」「削除」「復元」「名前を復元」「削除に失敗しました」「ブロックに失敗しました」のうち、いずれかを表示します。

*「失敗」と処理メッセージが出た場合、実行ファイルを “.bak” に変更し、エージェントを再起動した際に、その実行ファイルを自動的に削除いたします。

*脅威ログは1年間の間、最大50,000行まで保存されます。50,000行を超過する場合は、古い順で10,000行単位で自動削除されます。

2.5.2 検疫所



検疫所はランサムガード、もしくはリアルタイムセキュリティにより自動削除されたファイルが隔離されている情報が累積記録されます。

検疫所カラム(Column)には ログID、エージェントID、外部 IPアドレス、IPアドレス、エージェント日付、受信日付、名前、部署、ホスト名、脅威、種類、対象パスで分類されています。

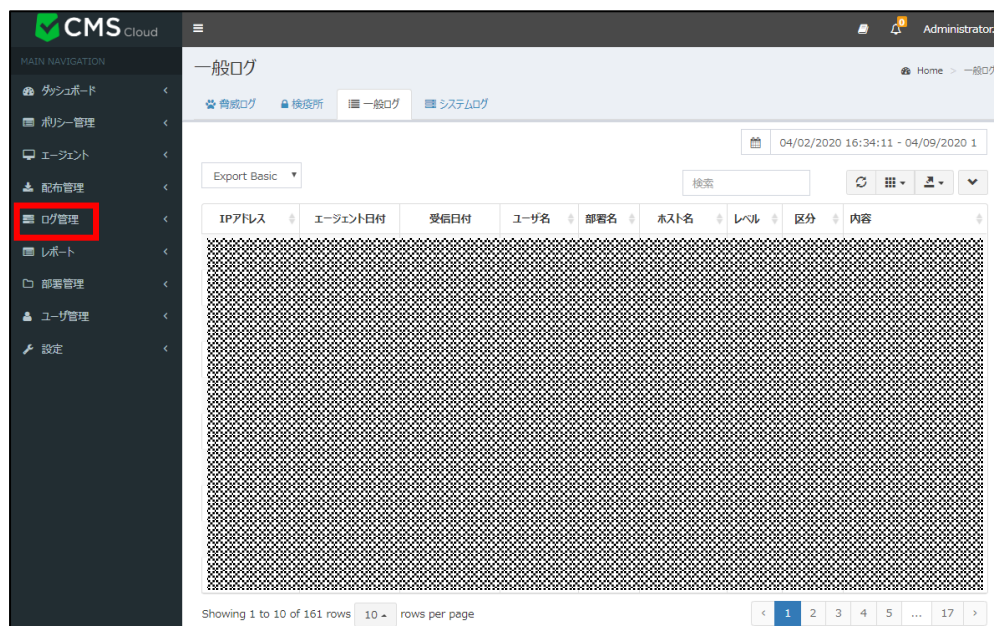
- ・**ログID** : 自動採番で検疫所イベントログに番号を付与します
- ・**エージェントID** : エージェントがインストールされたPC番号
- ・**外部IPアドレス** : エージェントがインストールされたPCのグローバルアドレス
- ・**IPアドレス** : エージェントがインストールされたPCの内部IPアドレス
- ・**エージェント日付** : エージェント側で生成したイベントログの時間
- ・**受信日付** : エージェント側で発生したログをCMS Cloud側で受信した時間
- ・**名前** : ユーザ管理 (2.8 ユーザ管理を参照) にて登録したユーザ名
- ・**部署名** : 部署管理 (2.7 部署管理を参照) にて登録した部署名
- ・**ホスト名** : エージェントがインストールされたPC名
- ・**脅威** : ランサムウェアによる脅威と思われる行為内容を表示します。

「ランサムウェアファイル名変更」「ランサムウェアアクション検知」「ランサムウェアファイル毀損」のうち、いずれかを表示します。

- ・**種類** : 自動削除された内容を表示。「ファイル」「レジストリキー」「レジストリ値」のいずれかを表示
- ・**対象パス** : ランサムガードで検知し、遮断され検疫処理をされたファイルパス

*検疫ログは1年間の間、最大50,000行まで保存されます。50,000行を超過する場合は、古い順で10,000行単位で自動削除されます。

2.5.3 一般ログ



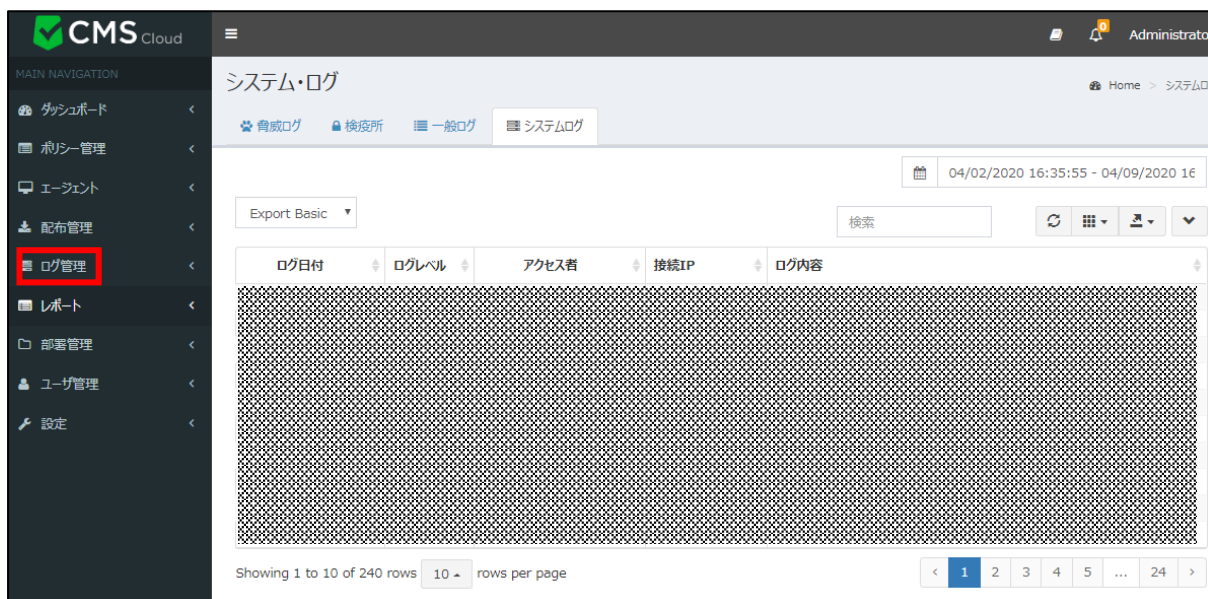
一般ログは AppCheck Pro使用時に発生するプログラム開始/終了、サービス開始/終了、リアルタイムスキャン開始/終了、ランサムガード開始/終了、アップデート、オプション設定、ランサムウェアおよびランサムガードお知らせメッセージ等の情報が累積記録されます。

一般ログカラム(Column)には ログID、エージェントID、外部 IPアドレス、IPアドレス、エージェント日付、受信日付、名前、部署、ホスト名、レベル、区分、内容で分類されています。

- ・**ログID** : 自動採番で一般イベントログに番号を付与します
- ・**エージェントID** : エージェントがインストールされたPC番号
- ・**外部IPアドレス** : エージェントがインストールされたPCのグローバルアドレス
- ・**IPアドレス** : エージェントがインストールされたPCの内部IPアドレス
- ・**エージェント日付** : エージェント側で生成したイベントログの時間
- ・**受信日付** : エージェント側で発生したログをCMS Cloud側で受信した時間
- ・**ユーザ名** : ユーザ管理 (2.8 ユーザ管理を参照) にて登録したユーザ名
- ・**部署名** : 部署管理 (2.7 部署管理を参照) にて登録した部署名
- ・**ホスト名** : エージェントがインストールされたPC名
- ・**レベル** : 危険度を表示します。(一般、注意)
- ・**区分** : 「自動バックアップ」「セッションプログラム」「サービスプログラム」「アップデート」「お知らせメッセージ」のうちいずれかを表示します。
- ・**内容** : 区分の処理内容を表示します。

*一般ログは1年間の間、最大50,000行まで保存されます。50,000行を超過する場合は、古い順で10,000行単位で自動削除されます。

2.5.4 システムログ



システムログにはCMS Cloudシステムログ情報を累積記録して、カラム(Column) ではID、ログ日付、ログレベル、アクセス者、接続IP、ログ内容で分類されています。

- ・**ID** : 自動採番でシステムイベントログに番号を付与します
- ・**ログ日付** : ログ発生日付
- ・**ログレベル** : ログの水準を表示します。(INFO、ERROR)
- ・**アクセス者** : システムログにアクセスしたエージェントのEメール
- ・**接続IP** : システムログにアクセスしたIPアドレス
- ・**ログ内容** : ログの内容を表示

*システムログは1年間の間、最大50,000行まで保存されます。50,000行を超過する場合は、古い順で10,000行単位で自動削除されます。

2.6 レポート

レポートではライセンス、検知状況、運営体制情報、製品情報報告書、ランサムウェア感染情報メニューで分類されています。

The screenshot displays a date range selection interface. At the top, a date range is shown: 12/17/2016 00:00:00 - 01/17/2017 23:59:59. Below this, there are two input fields for the start and end dates, each with a calendar icon. The start date is 12/17/2016 00:00:00 and the end date is 01/17/2017 23:59:59. There are also dropdown menus for the month and year for both dates. Below the input fields are two calendar views. The left calendar shows December 2016, and the right calendar shows January 2017. The date 17 is selected in both calendars. To the right of the calendars are several buttons for predefined date ranges: Today, Yesterday, Last 7 Days, Last 30 Days, This Month, and Last Month. The 'Custom Range' button is highlighted in blue. At the bottom right, there are 'Apply' and 'Cancel' buttons.

ライセンス、検知状況、ランサムウェア感染情報レポートで提供する統計情報は管理者が指定した期間(今日(Today)、昨日(Yesterday)、7日(Last 7 Days)、30日(Last 30 Days)、今月(This Month)、前月(Last Month)、ユーザ指定(Custom Range))によって多様に出力されます。

2.6.1 ライセンス



ライセンス状況では AppCheck Pro、AppCheck Pro for Windows Server製品のライセンス数量および使用状況を日付別で確認できます。

2.6.2 検知状況



期間別検知状況では、ランサムウェア検知もしくはエクスプロイトガード検知が発生したエージェント数をグラフで表示します。

グラフ下の安全、検知項目を選択してクリックするとフィルタリング処理された検知状況を確認できます。

| IPアドレス | ホスト名 | OS情報 | OSプラットフォーム | ユーザ名 | グループ名 | ツール |
|-------------|-------------|------------|------------------|---------------|--------|---------------------------------|
| 10.10.10.10 | SERVER01-01 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.11 | SERVER01-02 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro for Windows Server |
| 10.10.10.12 | SERVER01-03 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.13 | SERVER01-04 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.14 | SERVER01-05 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.15 | SERVER01-06 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.16 | SERVER01-07 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.17 | SERVER01-08 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.18 | SERVER01-09 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |
| 10.10.10.19 | SERVER01-10 | Windows 11 | win (ARM or x64) | Administrator | System | AppCheck Pro |

検知状況に表示された個別エージェントリストは AppCheck Pro、AppCheck Pro for Windows Server製品がインストールされデバイス情報を表示します。

エージェントリストカラム(Column)には ID、外部IPアドレス、IPアドレス、MACアドレス、BIOS S/N、マザーボード S/N、ホストネーム、OS情報、OSプラットフォーム、ユーザ名、グループ名、ユーザEメール、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、現在状態、最終オンライン時間、ツール(脅威ログ、検疫所、一般ログ)で分類されています。

*各カラム内容について前述記載項目と重複するため、ここでは内容説明はいたしません。

エージェントリストに記録されたデータは"Export data"メニューを通して CSV、MS-Excelファイルフォーマットで送信できます。

2.6.3 運営体制情報

2017-06-05 10:59:25

デスクトップ運用体制

| 運用体制 | プラットフォーム | 設置数 |
|------------|--------------------|-----|
| Windows 10 | x64 (AMD or Intel) | 5 |
| Windows 7 | x64 (AMD or Intel) | 3 |
| 合計 | | 8 |

サーバ運用体制

| 運用体制 | プラットフォーム | 設置数 |
|---------------------------|----------|-----|
| No matching records found | | |
| 合計 | | |

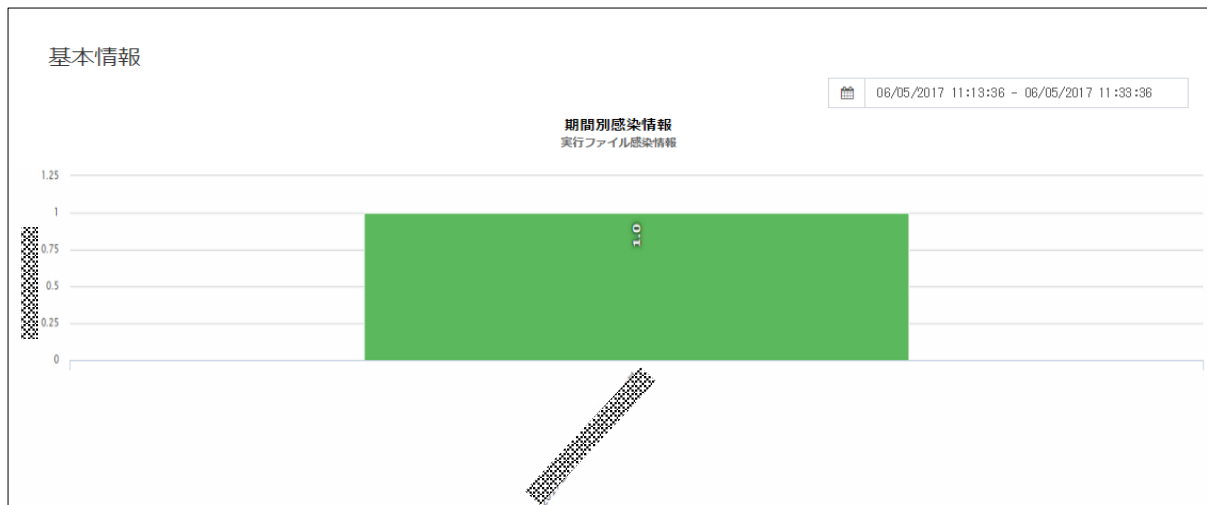
運営体制情報ではCMS Cloudを通じて配布されインストールされたデスクトップ運用体制(AppCheck Pro)とサーバ運用体制(AppCheck Pro for Windows Server)製品数に対する情報を提供します。

2.6.4 製品情報報告書



製品情報ではCMS Cloudを通して配布されインストールされたデスクトップ(AppCheck Pro)製品とサーバ(AppCheck Pro for Windows Server)製品のインストール数を円グラフと表で確認できます。

2.6.5 ランサムウェア感染情報



ランサムウェア感染情報では期間別ランサムウェア行為検知が発生した感染数を確認できます。

| 名前 | 部署名(最終部署) | エージェントID | メインボードS/N | 対象パス | ファイル名 | 感染日付 |
|---------------------------|-----------|----------|-----------|------|-------|------|
| No matching records found | | | | | | |

下段ではランサムウェア行為検知が発生した感染日付別で詳細ランサムウェア感染情報を確認できます。

該当表で提供するカラム(Column)はユーザID、名前、部署名(最終部署)、エージェントID、メインボードS/N、対象パス、感染日付で分類されています。

2.6.6 エクスプロイトガード情報



エクスプロイトガード情報では期間別エクスプロイトガード検知状況を確認できます。

下段では検知が発生した日付別で詳細情報を確認できます。

該当表で提供するカラム(Column)はユーザID、ユーザ名、部署名(最終部署)、エージェントID、メインボードS/N、対象パス、ファイル名、検知日付で分類されています。

2.7 部署管理



Tip!

- ※部署追加 : 選択した部署の下位に新しい部署を追加します。
- ※部署修正 : 選択した部署の部署名を変更します。
- ※部署削除 : 会社名を除外した選択した部署を削除します。
- ※未登録部署はシステムで予約された部署名です。変更不可です。

部署名 :

JIRANSOFT

部署追加 部署修正 部署削除

CMS Cloud製品を通じて配布された多数のエージェント管理を効率的にするために部署別に分類します。

部署追加、部署修正、部署削除機能を通して企業環境に合わせて構成できます。

2.8 ユーザ管理



ユーザ管理は CMS Cloudを通じて配布された AppCheck Pro製品をインストールしたエージェント管理のためにユーザ追加ができます。

ユーザ管理のカラム(Column)にはユーザID、名前、Eメール、部署名(最終部署)、インストールされたエージェント数、ユーザ情報で分類することができます。

2.8.1 ユーザ追加と削除



「ユーザ追加」メニューでは所属部署、名前、Eメールを入力してユーザを登録します。

またユーザ削除は、対象ユーザを選定し「ユーザ削除」を行ってください。

2.8.2 部署別ユーザ追加

部署EXCELアップロード

Notice!
アップロード時必ずファイル拡張子は.xlsで型式はExcel 97-2003に保存したファイルをアップロードしてください。

ダウンロード:

アップロード:

Drag & drop files here ...

部署内の多数のユーザを一括登録するためには、「部署EXCEL」をダウンロードし、ファイルに部署、名前、Eメール、処理方法を作成し、アップロードするようにお願いします。

2.9 設定

2.9.1 管理者



管理者設定メニューではCMS Cloud製品に対する管理者登録および管理権限を指定できます。

管理者設定のカラム(Column)にはID、名前、管理者Eメール、電話番号、管理権限、管理グループ ID、部署名、オプションで分類されています。

管理者追加時には管理グループ、部署、名前、Eメール、パスワード（変更時入力）、パスワードの確認、電話番号、管理権限(読み、読み/書き)情報を入力してください。

※管理権限「読み/書き」を持つ管理者は、必ず1個以上存在する必要があります。もし、「読み/書き」を持つ管理者が1個のみある場合は、該当管理者を削除することはできません。(他にもある場合は削除可能)

既存に登録された管理者情報を修正するためには、Edit（編集）オプションで変更可能です。



ログインオプション

ログイン試行回数:
5

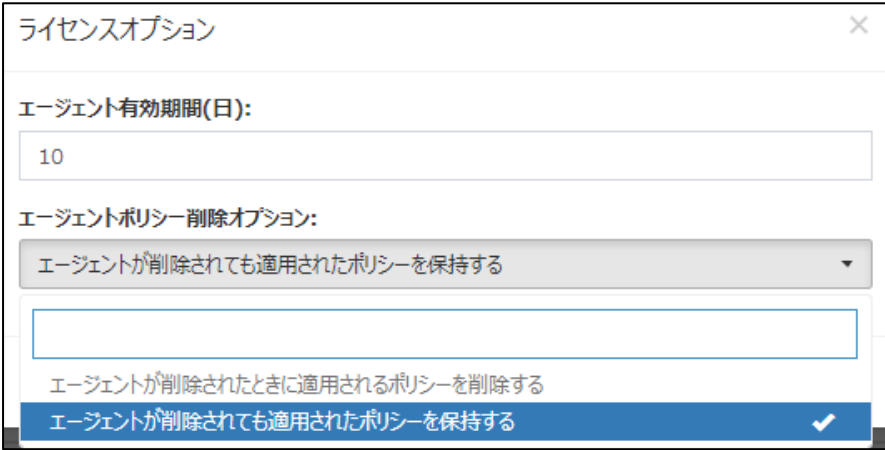
ログイン遮断時間(分):
5

パスワード有効期限(日):
365

保存する 取消

ログインオプションではログインに関する設定を行います。

- ・ ログイン試行回数：ログイン処理をする回数を設定します。
- ・ ログイン切断時間（分）：「ログイン試行回数」で指定した回数以上、ログインに失敗した場合、指定した時間（分）の間、ログインが不可能になります。
- ・ パスワード有効期限（日）：パスワード有効期限を設定します。



ライセンスオプション

エージェント有効期間(日):
10

エージェントポリシー削除オプション:
エージェントが削除されても適用されたポリシーを保持する

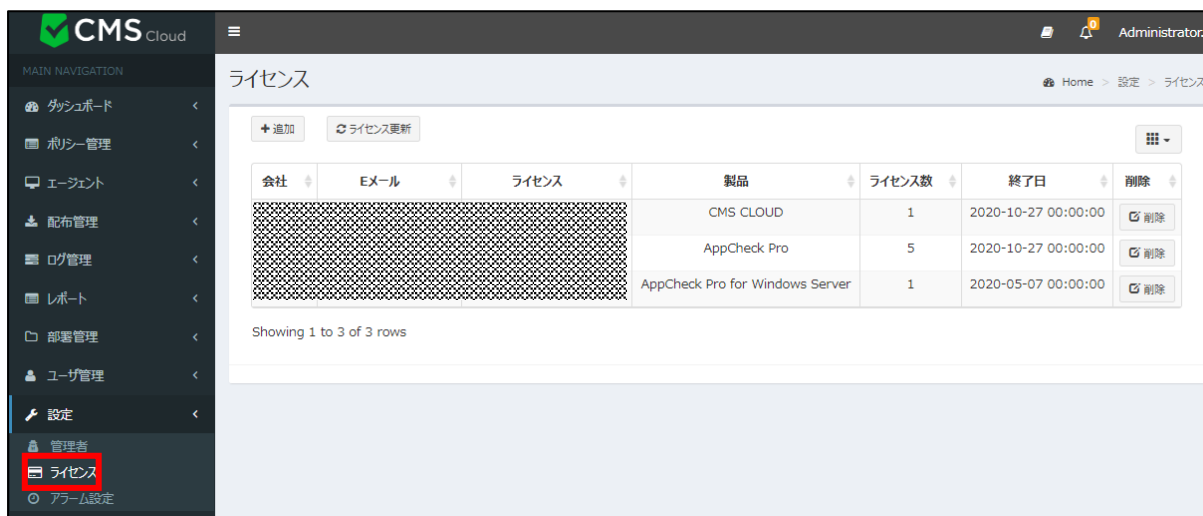
エージェントが削除されたときに適用されるポリシーを削除する

エージェントが削除されても適用されたポリシーを保持する ✓

ライセンスオプションでは CMS Cloud とのセッションを管理します。

- ・ エージェント有効期間（日）：CMS Cloud とのセッション有効期間を設定します。
- ・ エージェントポリシー削除オプション：「エージェント有効期間（日）」で指定した期間中、CMS Cloud との通信がない場合の処理を指定できます。

2.9.2 ライセンス



ライセンス管理メニューは CMS Cloud、AppCheck Pro、AppCheck Pro for Windows Server 製品に対するライセンス登録および削除を管理します。

ライセンス管理メニューのカラム(Column)には ID、会社、Eメール、ライセンス、製品、ライセンス数量、終了日、削除で分類できます。

ライセンス追加

Eメール:

ライセンスキー:

認証する 取消

ライセンス登録のためには購入時登録したEメールアドレスと発行されたライセンスキー情報で認証します。

2.9.3 アラーム設定

CMS Cloudと連動されているAppCheckPro（エージェント）でランサムウェア攻撃が検知されたら、検知ログがリアルタイムでCMSに送信されます。送信された脅威ログはデフォルト**15分**（変更可能）ごとにCMS内で集計され、アラーム設定されているメールアドレス宛に感染通知が送信されます。

アラームが必要ない場合、「Eメール削除」、設定内容を変更したい場合は「修正」ボタンをクリックし、修正することが可能です。

* 脅威ログが検知されなければ、メール通知は行われません。



2.10 パスワードを忘れた場合

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

「パスワードを忘れた場合」からパスワードを変更、仮パスワードを入手することが可能です。

※パスワードは8文字以上で、少なくとも1つの文字、特殊文字、数字を含む必要があります。

※CMS初期登録を行った後、ご要望にて「CMSライセンスに紐づくメールアドレス」を変更された場合でも、ログインIDはそのまま「初期登録されたメールアドレス」になります。もし、ログインIDを変更されたい場合は「2.9.1 管理者(P.58)」ページをご参考いただき、新しいメールアドレスとして管理者を追加してください。

2.10.1 パスワード変更について

The screenshot shows the 'CMS CLOUD' interface for password change. At the top, there are three tabs: '現在のパスワード' (Current Password), 'ライセンスキー' (License Key), and '仮パスワード' (Temporary Password). The '現在のパスワード' tab is selected and highlighted with a red box. Below the tabs, a message states: '現在のパスワードを利用してパスワードを変更することが可能です。' (You can change your password using your current password). A form contains four input fields: 'Eメール' (Email), '現在のパスワード' (Current Password), 'パスワード' (Password), and 'パスワード確認' (Password Confirmation). Each field has an icon on the right: an envelope for email, a lock for the current password, a lock for the new password, and a refresh icon for confirmation. At the bottom left is a link 'ログインページに移動' (Move to login page), and at the bottom right is a blue button labeled '変更' (Change).

■「現在のパスワード」を利用して、パスワードを変更することが可能です。

- ・Eメール：ログイン時のEメールを入力
- ・現在のパスワード：現在のパスワードを入力
- ・パスワード：変更したい新しいパスワードを入力
- ・パスワード確認：変更したいパスワードを再入力

The screenshot shows the 'CMS CLOUD' interface for password change. At the top, there are three tabs: '現在のパスワード' (Current Password), 'ライセンスキー' (License Key), and '仮パスワード' (Temporary Password). The 'ライセンスキー' tab is selected and highlighted with a red box. Below the tabs, a message states: '登録されたCMSライセンスキーを利用してパスワードを変更することが可能です。' (You can change your password using the registered CMS license key). A form contains four input fields: 'Eメール' (Email), 'ライセンスキー' (License Key), 'パスワード' (Password), and 'パスワード確認' (Password Confirmation). Each field has an icon on the right: an envelope for email, a lock for the license key, a lock for the new password, and a refresh icon for confirmation. At the bottom left is a link 'ログインページに移動' (Move to login page), and at the bottom right is a blue button labeled '変更' (Change).

■「ライセンスキー」を利用して、パスワードを変更することが可能です。

- ・Eメール：ログイン時のEメールを入力
- ・ライセンスキー：現在のライセンスキーを入力
- ・パスワード：変更したい新しいパスワードを入力
- ・パスワード確認：変更したいパスワードを再入力

2.10.2 仮パスワードについて

The screenshot shows the 'CMS CLOUD' interface. At the top, there are three tabs: '現在のパスワード' (Current Password), 'ライセンスキー' (License Key), and '仮パスワード' (Temporary Password). The '仮パスワード' tab is selected and highlighted with a red box. Below the tabs, the text 'Eメールで仮パスワードを送ります。' (Send temporary password by email) is displayed. There is an input field for 'Eメール' (Email) with a red box around it and an envelope icon on the right. Below the input field, there is a blue button labeled '送信' (Send) with a red box around it. To the left of the button is a link that says 'ログインページに移動' (Move to login page).

- ログイン時のEメールを入力し、「送信」ボタンをクリックすると、仮パスワードが送信されます。