

# **AppCheck CMS Cloud**

## マニュアル

株式会社 JSecurity

第四版 2021/03/05

## 目次

1.1 CMS Cloudのログイン方法	5
各機能詳細	6
2.1 ダッシュボード	6
2.1.1 時間別検知	
2.1.2 エージェントバージョン	8
2.1.3 エンジンアップデート状況	9
2.1.4 24時間内上位 5位脅威	
2.1.5 ポリシー適用状況	
2.1.6 ログ統計	
2.2 ポリシー管理	
2.2.1 ポリシー追加および削除	
2.2.2 ポリシー管理 : 一般	14
2.2.3 ポリシー管理 : ランサムガード	
2.2.4 ポリシー管理 : エクスプロイトガード	
2.2.5 退避フォルダ	
2.2.6 ポリシー管理 : クリーナー	
2.2.7 ポリシー管理 :自動バックアップ	
2.2.8 ポリシー管理 : ユーザ指定除外ファイル	
2.2.9 SMB設定	
2.3 エージェント	
2.3.1 部署別一括ポリシー適用	
2.3.2 個別ポリシー適用	
2.3.3 情報一括変更	
2.3.4 バックアップフォルダを空にする	
2.4 配布管理	
2.4.1 クライアント配布 : インストール情報	
2.4.2 クライアント配布 : Eメール送信	

2.4.2.1 Eメール検索	
2.4.2.2 エクセルでメール送信	
2.5 ログ管理	
2.5.1 脅威ログ	
2.5.2 検疫所	
2.5.3 一般ログ	
2.5.4 システムログ	
2.6 レポート	
2.6.1 ライセンス	
2.6.2 検知状況	
2.6.3 運営体制情報	
2.6.4 製品情報報告書	
2.6.5 ランサムウエア感染情報	
2.6.6 エクスプロイトガード情報	
2.7 部署管理	
2.8 ユーザ管理	
2.8.1 ユーザ追加と削除	
2.8.2 部署別ユーザ追加	
2.8.3 ユーザ情報	
2.9 設定	
2.9.1 管理者	
2.9.2 ライセンス	
2.9.3 アラーム設定	
2.10 パスワードを忘れた場合	
2.10.1 パスワード変更について	54
2.10.2 仮パスワードについて	

#### はじめに

このたびは、CMS Cloud 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、ご使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 AppCheck のホーム ページ (https://www.appcheck.jp/support/) でご確認ください。

#### 著作権について

本書は AppCheck Pro for Windows Server 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 V1.1.22を参考に作成しています。

## 1.1 CMS Cloudのログイン方法

下記の URL にアクセスします。

https:/	/cms.checkmal.com/

<b>CMS</b> CLOUD	
使用するにはログインしてください  日本語  レ レ レ レ レ レ レ レ レ レ レ レ レ レ レ レ レ レ	言語:「日本語」を選択します。 管理者の E メールアドレスとパスワードを入力し、 「ログイン」ボタンをクリックます。

※管理者の E 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 E メールアドレスとパスワードになります。

※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。

ログインが成功すると「ダッシュボード画面」が表示されます。

🕑 CMS 📾																						🖉 지명권
MALK MANTGRETON	ダッシュボー	- 15																		8	Home > 12	ッシュボード
<ul> <li></li></ul>	28.	エージェント	飲				93						10					数ライセン3 100	æ			
≪ ポリシー管理 く							× '										Ċ	<u> </u>				
₽ I-9IYF <	PRESENT ALLOS	- Shout										_										6.4
± 626933 <	ed Budd borb (orm																					
■ ログ培理 <											約税	阴検知状况										
≡ L#-► <																						
C) 278993 <																						
▲ 그~····································	#1																		-	~		
× 88 <	101	••		•	•	•			•	•	•	•		•	•	•	•	~				
	н																					
		•	00	22.00	28.00	11. May	01.00	02.00	01.00	04.00	00.00	06.00	07.00	00.00	08.00	18:00	11.00	12.00	16.00	14.00	18.00	16.00
											+ 7	e + 80										
																						_
	エージェントバ	ージョン									- ×	エンジンアッ	ブテート状況									- x
	全体設置エージ	エント										最新エージェン	トバージョンには	E.O. 1. 15								
	9295 7 9~75 0 (220)	デスクトゥ	7 (1020																			
	0																					
	エージェント状	22																800.0819	20.08.9			
	接続エージェン	F.									0											
	自体エージェン	٢									0											
	24時間内上位5년	2角斑									- ×	ポリシー適用	状況									- x
												TEST2: 通問:(1)	不適用::(0)				1979					
												TEST: MATE:(1)	不適用::(D)									
	1											_					103					
	obje																					
						×	0 Anas															
						<b>=</b> 8s	NGC-															

## 各機能詳細

2.1 ダッシュボード

🕑 CMS 😡																						3333
HREN NRVEGATION	ダッシュ	ボード	*																	B Hos	e> 55	シュボード
		全体エー 7	ジェント数				安全						efa					残ライセンク 103	激			
ペ ポリシー管理 <							× (*					l i i					2	100				
↓ エージェント	R中日日日 (北京市)	(Linit Ho	art)			_																4 4
▲ £2%@13 <																						-
■ ログ管理 <											時間別	検知状況										
■ UR=F <																						
□ ##### • >																				-		
- 1-9802 (	# 																	/	-			
7 RE (	16-1	4		•	•	•	•	•	•	•	•	•	•	•	•	•	•	-				
		0	21:00	22:00	28:00	al. May	01:00	02:00	00:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	18:00	14:00 15	00	16:00
												+ 秋知										
	T-877 N	ыл <u>-</u> з	con Na									T1602/70										
	1-919	197(=:									- x	ANT-OF	(b) section of the	0.1.15								- ×
	全体設置工 全体設置工	-91)	21									2.0.1.15	111 9 2011									
	サーバ 0 0	(010 😏	291-77 7 (1000																			
	_													6								
	エージェン	下状况									0						6	938.00				
	Ren	T UN									0											
	1894T-5	1.71																				
	24時期内 ト	រកសាផ	a att									ポロシー達日	31+19									-
	2440 1007 3.1		104									IISIZ: WE:(	1) 不過用::(0)									
																	1065					
												TEST: 道用:(()	) 不適用::(0)									_
	bộ ci Pa																PULCE					
	0																					_
																						_
																						_
						Values																_
	-																					

ダッシュボードでは、全体エージェント数/残ライセンス数などの他、次の項目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および状態) (2.1.2を参照ください)

- ・エンジンアップデート状況(2.1.3を参照ください)
- ・24時間内上位 5位脅威(2.1.4を参照ください)
- ・ポリシー適用状況(2.1.5を参照ください)
- ・ログ統計(2.1.6を参照ください)



・ 全体エージェント数: CMS Cloudを通じて配布されインストールされたAppCheck Pro for Windows Server AppCheck Pro全体エージェント数

・安全: ランサムウエア検知がないエージェント数

・検知:ランサムウエ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うち、残ライセンス数

#### 2.1.1 時間別検知



時間別検知状況では、日単位または1時間単位、1分単位で安全なエージェント数とランサムウエア検知で対処が

必要なエージェント数をリアルタイムグラフで表示します。

管理者確認が必要な特定位置にマウスを位置する場合時間と安全または検知された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

• 3	x
4	
0	
(	4

エージェントバージョンでは全体インストール済エージェント(サーバ、デスクトップ)情報とエージェント状況(接続エージェ ント、危険エージェント)数を表示します。

全体インストール済エージェントでは AppCheck Pro for Windows Server製品(サーバ)と AppCheck Pro 製品(デスクトップ)で分類します。

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うちオンライン状態のエージェント数を表示します。

危険エージェントは、ランサムウエア検知が発生したエージェント数を表示します。

#### 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、インストールされたエージェント別AppCheck Proのバージョン情報を円グラフで表示します。

特定バージョンのエージェントを表示するには、左側上段に表示されたバージョンをクリックして状況を確認することができます。

#### 2.1.4 24時間内上位 5位脅威



24時間以内にランサムウエア検知が行われたファイルパス(Object Path)のエージェント数(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します。各ログをクリックすることで、エージェントごとの詳細なログを確認することが

可能です。

CMS Cloud	≡ Administrator.									
MAIN NAVIGATION										
<b>@</b> ∮y>ュホ−ド <	全有成ログ ●検疫所 ■一般ログ ■ システムログ									
■ ポリシー管理 く										
□ I-9I>h										
▲ 配布管理 〈	Export Basic Y 検索 🛛 🗰 - 💆 - 🗸									
■ ログ管理 く	IPアドレス									
■ レポート <										
口 部署管理 〈										
▲ 그-ザ管理 <										

#### 2.2 ポリシー管理

CMS Cloud	Ξ									<b>e</b> (	Administrato
MAIN NAVIGATION	ポリシ	レー管理								ø	Home > ポルシー管
	▶シュポード < □										
□ ポリシー管理 く		リンー官理									
m dis. tre		Export Basic	•	□ 部署別一括ポリシ	·-適用 + 追加	一削除			検索	S	<u>a</u>
▲ SMB 設定		ポリシー名 💧	Type 🗄	初期作成時間	最終変更時間	最終適用時間		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	教 合 副規制 合
□ I-ジェント		基本ポリシー	Windows	2019-10-28	2020-04-09	-	2	-	-	-	
▲ 配布管理 <				16:39:33	14:34:37					ロボリシーコ	D
■ ログ管理 〈		営業部ポリシー	Windows	2020-04-06 15:53:39	2020-04-09 14:39:10	2020-04-06 16:08:09	4	0	0	☑ ポリシー名 ☑ 初期作成時	業部
■ レポート <		JJS基本	Windows	2019-10-28 17:22:53	2020-04-09 14:38:59	2019-11-21 11:50:56	3	0	0	<ul><li>☑ 最終変更時</li><li>☑ 最終適用時</li></ul>	na) na)
口 部署管理 〈	4 Ch	owing 1 to 2 of	2 10000							<ul> <li>マ バージョン</li> <li>マ 対象エージ ント数</li> </ul>	ж. — — — — — — — — — — — — — — — — — — —
▲ 그─ザ管理 <	50	owing 1 to 2 of	210/05								
▶ 設定 く											

ポリシー管理では多様なポリシーを管理でき、各ポリシーを適用されたエージェントは自動で AppCheck Proのオプ ション機能が設定されます。

※実際に適用されるまで、CMS Cloudサーバとエージェント間において一定時間の通信時間が必要となります。

※デフォルト設定では「基本ポリシー」となります。

「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」には表記されません。

<u>※個別ポリシーを各エージェントに適用するには、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</u>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。

ポリシー管理に表示されるカラム(Column)には ポリシーID、ポリシー名、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、説明に分類されており、 選択した各項目を表示します。

・ポリシーID:自動採番で各ポリシーに番号を付与します。

・ポリシー名:任意で記入できます。 (2.2.1 ポリシーの追加および削除 を参照ください)

- ・初期生成時間:ポリシーを登録した時間を表示します。
- ・最終変更時間:既存ポリシーを修正した時間を表示します。

・最終適用時間:CMS Cloud上で設定したポリシーを対象エージェントに適用した最終時間を表示します。

・バージョン:登録した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:登録したポリシーを適用するエージェント数

(「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:登録したポリシーを適用されたエージェント数

(「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

(「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:各ポリシー内容を自由に記入できます。

#### 2.2.1 ポリシー追加および削除

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

CMS Cloud	E	2	4 Administrator
MAIN NAVIGATION	ポリシー管理		<b>の</b> Home > ポリシー管理
🙆 ダッシュボード 🛛 🗸			
■ ポリシー管理 <			
■ ホリシー管理	Export Basic • Creat-adu-adu • att	sharkonetest@gmail.com	<b>∷</b> - <b>∠</b> - <b>∨</b>
<ul> <li>SMB 設定</li> </ul>	■ ポリシー名 ▲ Type ▲ 20期代成時期 ▲ 長線空雨時期 ▲ 長線造田時期 ▲ パージョン ▲ 対象エ	ージェント数 💧 油田されたエージェント数	オンラインエージェン
□ I-ÿI>ト			-
▲ 配布管理 <	cms.checkmal.com の内容:		
■ ログ管理 く	■ 営業印ポリシー Windo ポリシー名を入力してください	0 0	0
■ レポート 〈	DIS基本 Windo	0 0	0
			Þ
	Showing 1 to 2 of 2 rows		

cms.checkmal.com の内容:		×
削除しますか?削除されたポリシーは復旧できません ジェントは基本ポリシーに変換されます。	。ポリシー変更が	完了してないエー
	OK	キャンセル

既に登録されたポリシーを削除する場合には、該当ポリシーを選 択後、「削除」ボタンをクリックします。 削除されたポリシーに適用されたエージェントは基本ポリシーに自 動変換されます。

また登録されたポリシーをExcel様式またはCSVでExportし、内容を確認することも可能です。



#### 2.2.2 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	クリーナー	自動バックアップ	ユーザ指定除外ファイル				
ポリシー	説明:									
Ente	r									
🗹 リアハ	レタイムセキュリティ	を常に設定する。								
Lock N	Mode: OFF		•							
口個別	コーザポリシー変	更許可								
ライブチ	エック周期: 1	5分毎(デフォルト値)	-							
✓ I-:	ジェントアンインスト	~-ル許可								
✓ お知	らせ領域アイコン化	使用								
ע דם?	グラム実行遮断時	にお知らせダイアログ実行								
	リバッファート使用									
□ 検出	は時、疑いのあるフ 「名で処理され、分	アイルを転送する 分析以外の目的にでは使用	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: AppCheck Pro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AppCheckのオプションの変更できないようLockします。

・個別ユーザポリシー変更許容 : エージェントユーザがインストールされたAppCheck Proのオプション機能に よって、個別に詳細設定を変更できるように許可します。

・ライブチェック周期:15分(デフォルト)、20分、30分、1時間周期で適用されたエージェントに対するポリシー 設定を確認します。

・エージェントアンインストール許可:個別エージェント毎による AppCheck Proアンインストールを許可します。 デフォルト設定では、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: AppCheck Pro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:ランサムウエア行為検知時タスクバー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 AppCheck Pro CARBエンジンのアップデートを自動確認します。

・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)

#### 2.2.3 ポリシー管理 : ランサムガード



・ランサムウエアアクション遮断実行:ランサムウエア感染でファイル毀損の動作が発見された時に、"ランサムウエア動作検知"お知らせダイアログを作成し、プロセスを遮断します。

・毀損動作検知実行:ランサムウエアによる元のファイルを復旧不可能状態に削除する動作を検知して遮断します。

・MBR保護 : Master Boot Record (MBR)領域を改ざんしようとするファイルの実行アクションを遮断す
 る機能

・ランサムウエア遮断後自動治療 : ランサムウエア事前防御使用時に、検知されたランサムウエアを自動治療 (削除)します。

・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 計49種(7z,ai,bmp,cer,crt,csv,der,doc,docx,dwg,eps,gif,hwp,jpeg,jpg,key,lic,lnk,mp3,nc,o ds,odt,ogg,one,p12,p7b,p7c,pdf,pef,pem,pfx,png,ppt,pptx,psd,ptx,rdp,rtf,srw,tap,tif,tiff, txt,uti,x3f,xls,xlsx,xps,zip)で、ファイル拡張子名の登録および修正ができます。

・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のローカル ディスクからランサムウエアによって毀損されないよう、ランサムウエアの毀損行為を遮断する機能

・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エアによって暗号化された場合、遮断および自動復元される機能

\*USB接続HDDは「ランサムウエアアクション遮断機能」により保護されます。

・SMBサーバ保護: AppCheckがインストールされたPCやサーバ内のドライブにある共有フォルダがランサムウエアに感染しないように、ランサムウエアに感染したPCからのネットワークアクセスを一時的に遮断します。

・疑わしいファイル毀損検知:ランサムウエアと判断するファイル毀損検知回数を選択することができます。

\*ファイル毀損検知回数を少なく設定すると、ランサムウエアではない正規プログラムを過検知するケースがあります。

#### <ネットワークドライブ保護>



#### [ご注意]

ネットワークドライブ保護およびSMBサーバ保護を有効にするためには、共有フォルダを提供するサーバのネットワーク設定で「TCP/IPv6」のチェックを解除することで正常に遮断が行えます。

#### [ご注意]

バックアップフォルダ<Backup(AppCheck)>削除のためにはAppCheckリアルタイムセキュリティを一時的に解除して削除するよう願います。

#### 2.2.4 ポリシー管理 : エクスプロイトガード

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				
<ul><li>」 エクジ</li></ul>	スプロイトガードを使用	Ð								
- 保調	豊するアプリケーショ	i>								
✓ w ✓ プ	<ul> <li>✓ Webブラウザ(IE, MS Edge, Chrome, Firefox, Opera)</li> <li>✓ プラグイン(Java, Flash)</li> </ul>									
✓ ×5	ディアプレーヤー(WM	P, WMC, GOM Player	, Pot Player)							
⊻ л.	MACIMS Office, H	ancom Office, Adobe	e Acrobat)							

Web ブラウザやマイクロソフトオフィスの他、各種プラグインなどのアプリケーションの脆弱性を突く、悪意のある攻撃から PC やサーバを保護します。

※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 両方を有効にして下さい。また「エクスプロイトガードを使用」を off に した場合、「保護するアプリケーション」を有効にしていても機能は適用いたしませんので、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 Ofiice, Hancom Office, Adobe Acrobat

#### 2.2.5 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 クリーナー 自動バックアップ ユーザ指定除外ファイル								
✓ リアルタイムバックアップ実行								
退避フォルダパス: C:¥ProgramData¥CheckMAL¥AppCheck¥RansomShelter	設定							
□ 一つのファイルの大きさを最大 1GB - 以下に制限								
□ ランサムウェア退避フォルグ非表示								
- 退避フォルダ自動削除								
2 7 日 ▼ 経過したファイルを自動削除								
□ 退避フォルグ容量がディスクの 50GB - 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								

・リアルタイムバックアップ実行: AppCheckのリアルタイムバックアップ機能のon/offを設定します。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する:リアルタイムバックアップの対象ファイルの容量を設定します。
 100MB、200MB、500MB、1GB (デフォルト)、2GB、5GB単位で設定が可能です。デフォルト設定では
 「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 的に削除します。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日単位で設定が可能です。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))になると、古い順でファイルを自動削除):指定した設定値になった場合、退避フォルダを自動削除します。退避フォルダのディスク容量に合わせて設定してください。 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。

### 2.2.6 ポリシー管理 : クリーナー

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       自動パックアップ       ユーザ指定除外ファイル          変造されたシステム検査 <t< th=""><th>1.基本ポ</th><th>リシー 🖋</th><th></th><th></th><th></th><th></th><th></th></t<>	1.基本ポ	リシー 🖋					
<ul> <li>変造されたシステム検査</li> <li>ネットワーク環境検査</li> <li>悪性プログラム検査</li> <li>広告プログラム検査</li> <li>ブラウザー拡張プログラム検査</li> <li>ショットカット悪性 URL検査</li> <li>ランサムウェアノート除去</li> <li>臨時ファイル/フォルダー除去</li> </ul>	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
	◎ 変 マネ 悪 マ 広 マシラ 『	造されたシステム ットワーク環境検 性プログラム検査 ラウザー拡張プロ コットカット悪性 ンサムウエアノー 時ファイル/フォ	▲検査 塗査 至 コグラム検査 主 URL検査 - ト除去 ルダー除去				

変造されたシステム検査、ネットワーク環境検査、悪性プログラム検査、ブラウザー拡張プログラム検査、ショットカット 悪性 URL 検査、ランサムウェアノート削除、臨時ファイル/フォルダー除去機能を提供します。

#### 2.2.7 ポリシー管理 :自動バックアップ

-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
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
%USERPROFILE %USERPROFILE %USERPROFILE %USERPROFILE %USERPROFILE	96¥Desktop 96¥Documents 96¥Favorites 96¥Pictures 96¥Music 96¥Music	*			•
□ 指定した拡張子名	だけバックアップ (区分子 ,る	または ;)	バックアップ時	除外するファイル拡張	張子名 (区分子 ,または ;)
□ 指定した拡張子名 バックアップする箇所	だけバックアップ (区分子 , a	ttti ;)	バックアップ時間	徐外するファイル拡き 数:3	振子名 (区分子 ,または ;)
<ul> <li>□ 指定した拡張子名</li> <li>パックアップする箇所</li> <li>● □-カルディスク</li> <li>○ ネットワーク共有ファ</li> </ul>	だけバックアップ(区分子 , a	ŧta;) heck)	バックアップ時間 「加速ファイル保存 WORMストレ	除外するファイル拡き 数: 3 ージモード	振子名 (区分子 ,または ;) ▼
<ul> <li>□ 指定した拡張子名</li> <li>パックアップする箇所</li> <li>● ローカルディスク</li> <li>○ ネットワーク共有ファ サーバアドレス</li> </ul>	だ <b>けバックアップ(区分子 ,</b> ま C:¥ AutoBackup(AppC tルグ(SMB/CIFS)	ŧta;) heck)	バックアップ時間 「「「」」 「「」」 「「」」 「」」 「」 「」」 「」」	除外するファイル拡き 数: 3 ージモード	振子名 (区分子 ,または ;)

自動バックアップは指定したバックアップ対象フォルダを定期的に自動バックアップフォルダ

<AutoBackup(AppCheck)>に増分バックアップできます。デフォルト設定では「機能off」の状態となります。

・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 時間単位で設定が可能です。デフォルト設定では機能offとなっております。

・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追加および削除が可能です。

(※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、指定したファイル拡張子名だけをバックアップするように設定可能です。

(※例: doc、hwp、jpg または doc;hwp;jpg)

・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、自動バックアップを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可能です。

デフォルトでは bak、tmp拡張子名が追加されています。

・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)>の指定を選択します。ローカルディスク、ネットワーク共有フォルダ(SMB/CIFS)の中から1つ選択できます。

・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として保存します。 デフォルト設定では「3」となっております。

・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。 デフォルト設定では「設定off」となっております。

#### 2.2.8 ポリシー管理 :ユーザ指定除外ファイル

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	
口以下	に登録されたファイノ	しは常に許可 追加 削除					
							*
							-

ユーザ指定除外ファイルは、ランサムガード、マルチエンジン、システム検知により検知(遮断)されたファイルのうち、 お客様の判断により常に検査実行を行わないように設定許可したファイルを記入します。

#### [ご注意]

基本的にAppCheck Pro製品では特定プログラムに対するホワイトリストが含まれていますが、正常的なexplorer. exeまたはsvchost.exeシステムファイルを利用しファイル暗号化行為を実行するランサムウエアが存在するため、シス テムファイルをユーザ信頼ファイルに勝手に追加しないでください。

#### 2.2.9 SMB設定

CMS Cloud		Administrator.
MAIN NAVIGATION	SMB 設定 。	Home > SMB 設定
🛚 ダッシュボード		
■ ポリシー管理	テリュー エークレフト 許容されたアドレスリスL Add Del	
■ ポルシー管理		
▲ SMB 設定		<b>^</b>
	<	
▲ 配布管理	<	
こ ログ管理 ・		-
▣ レホート		
口 部署管理		
▲ ユーザ管理		
▶ 設定		

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

CMS Cloud	= 🖉 Administra
MAIN NAVIGATION	SMB設定 @ Home > SMB;
の ダッシュボード く	
■ ポリシー管理 く	
■ ポルシー管理	search Search Start Z- Y
📥 SMB 設定	Agent ID 参 IPアドレス 参 MACアドレス 参 ホスト名 参 OS情報 参 ユーザ名 部署名 参 インストールバージョン 参 現状態 参 最終オンライン時間 参 ツール
प्रान्ट्रेग्रोन् <b>र</b>	
▲ 配布管理 〈	
■ ログ管理 く	=
≣ ∪ಸ−ト <	=
○ 部率管理 〈	
▶ 設定 く	Showing 1 to 5 of 5 rows

・SMB設定 → 「エージェント」: ユーザ毎にSMB許容/遮断が可能です。

#### 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

<u>※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</u> 「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プラットホーム、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プラットホーム: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

・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。



#### 2.3.1 部署別一括ポリシー適用

	Ξ								
MAIN NAVIGATION	エージェン	<b>ト</b>							
🖚 ダッシュボード 🖌	ユニージェン	->>リスト							
< ポリシー管理 <									
□ エージェント	Export	в∨	□ 部署別一括ポリシー適用	目 🔺 個別ボ	リシー適用	圓 一括ユーザ登	録 ■ バックアップフォルダを空に	する	
	Г	部審別ポリ	シー適田			$\times$			
		LIPE // 111							
		dan 📄 🚑 d	IRANSOFT			<b>^</b>			
			■ 2000000000000000000000000000000000000						
		E	📄 🔊 技術チーム						
			二 単 営業チーム   二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二						
		- Fi	🔜 🧾 営業チーム						
			🔜 🛄 技術チーム			*			
				Filter		· · · ·			
		10	ポリシー名前	\$	リビジョン	\$			
		6	ポリシーテスト		1				
		0 5	テストポリシー		1				
		4	ポリシーミ		1				
		© 3	基本 ポリシー		1				
		2	TEST2		1				
		Showing 1 to	5 of 6 rows 5 🛓 rows	per page	< 1	2 >			
					適用	取注道			
	L								

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に選択して適用できます。

#### 2.3.2 個別ポリシー適用

	=							
MAIN NAVIGATION	エージェント							
<ul> <li>● ダッシュボード く</li> <li>◆ ボリシー管理 く</li> <li>□ エージェント く</li> </ul>								
				Filter		]		
		ID	ポリシー名前	÷ IJ	ະິ⊇ັ∋ນ ∳			
		0 6	ポリシーテスト		1			
		0 5	テストポリシー		1			
		0 4	ポリシー2		1			
		0 3	基本 ポリシー		1			
		0 2	TEST2		1			
		Showing 1 t	o 5 of 6 rows 5 🔔 rows p	er page	< 1 2 → 適用 取消			

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

CMS Cloud	=
MAIN NAVIGATION	エージェント
<b>8</b> 8 ダッシュボード <	<b>ロ</b> エージェントリスト
ペ ポリシー管理 <	Fxnort Basic V DI 想電知一括ポリシー油目 島 個別ポリシー油目 冊 佐紹一括安西 オ バックアップフォルグを空にする ¥
<b>₽</b> エージェント 〈	
	「情報一括変更 × Notice! アップロード時後がファイル境界刊は.x1sで登切さたxcel.97-2003に保存した。 アップロード: フォーマットがウンロード アップロード: Drag & drop files here ■ Brows

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。

						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



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。

#### 2.4 配布管理

#### 2.4.1 クライアント配布 : インストール情報

CMS Cloud	≡
MAIN NAVIGATION	- クライアント配布 & Home > 配布管理
<b>鉛</b> ダッシュボード く	インフトール清報 FV-11送信
■ ポリシー管理 く	
□ I-91>F <	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。
🛓 配布管理 💦 🗸 🗸	
言 ログ管理 く	インストールファイル 🎍 ダウンロード
≡ レポート <	Silent インストールファイル
口 部署管理 〈	インストール総理正キー
▲ ユーザ管理 〈	保有ライセンス
▶ 設定 く	
	インストール認証キー詳細内容は[設定>ライセンス]で確認可能です。
	回다ーば

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ヘ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。

・インストールファイル: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する方式です。

・Silentインストールファイル: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ない方式です。

・インストール認証キー: CMS Cloudからダウンロードしたファイル名を変更しない場合、自動的にインストール認証 キーが登録された状態で、インストールします。

・保有ライセンス: CMS Cloudランセンス情報に登録された製品とライセンス数量を表示します。

#### [ご注意]

ファイル名を変更した場合、インストールする際に、認証キーを手動で入力する必要がありますので、ダウンロードしたフ ァイル名を変更しないことをおすすめします。

#### 2.4.2 クライアント配布 : Eメール送信

CMS Cloud	=	4	Ac	
MAIN NAVIGATION	クライアント配布	<b>19</b> 8 H	ome > i	配布管理
<b>鉛</b> ダッシュボード く	インストール情報 Eメール決信			
■ ポリシー管理 く				
₽ I-ÿi>ŀ <	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在できます。			
▲ 配布管理 〈				
こ の ご 「 こ こ こ こ う う う う う う う う う う う う う う う	Q 検索する 受信者Eメール(複数の時は(,)で区分してください)			
≣レホート <	■ メールタイトル AppCheckエージェントプログラム配布メールです。			
口 部署管理 〈	♠ ≫ ♥ ☑ ☶ 블 X № 소스 B :: 스타일 •			
▲ 그─ザ管理 〈				
▶ 設定 〈	AppCheck Pro インストール			
				•
	童 基本内容許が出し ■ EXCELでメ	一儿送信	⊠ EX–II	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

◆ → ● 回 亜 目 第 回 ソース B Ⅲ スタイル ・
AppCheck Pro インストール
▲ 基本内容呼び出し 🛛 EXCELでメール送信 🛛 EX ール送信
インストール案内EXCEL形式アップロード ×
<b>Tip!</b> EXCELファイルをアップロードするとEXCEL内のEメールアドレスにインストール案 内Eメールが送信されます。
<b>ダウンロード</b> : インストール案内EXCEL形式ダウンロード <b>アップロード</b> :
Drag & drop files here
FFI じる

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。

#### 2.5 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。 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。



 ・Export Basic:現在表示されているWeb 画面の内容をExport
 ・Export All:全てのデータをExport

#### 2.5.1 脅威ログ

CMS Cloud	E _ Δ <sup>Q</sup> Administrator.
MAIN NAVIGATION	- 一般ログ & Home > 一般ログ
の ダッシュボード く	
■ ポリシー管理 く	
□ I-ÿI>ト	□□ 04/02/2020 16:21:15 - 04/09/2020 1
▲ 配布管理 〈	Export Basic Y 検索 S III - Z · Y
■ ログ管理 く	IPアドレス 🕴 エージェント日付 💠 受信日付 🌩 ユーザ名 🍦 部署名 🍦 木スト名 🍦 検知主体 🛉 脅威 🍦 種類 💠 対象パス 🌩 処理
■ レポート <	
口 部署管理 く	
▲ 그ザ管理 〈	
▶ 設定 く	
	Showing 1 to 10 or 101 rows 10 + rows per page

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、ランサムウエア情報、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:ランサムウエア行為・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:ランサムウエアによる脅威と思われる行為内容を表示します。

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

・対象パス:ランサムウエア行為・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。

\*脅威ログは基本2ヶ月間、最大50,000ラインまで保存できます。50,000ラインを超過した場合は、古いログから10,000ラインを削除していきます。

#### 2.5.2 検疫所

	Ξ
MAIN NAVIGATION	検疫所
1999 ダッシュボード く	
■ ポリシー管理 く	
□-ゔı>ト	☐ 04/02/2020 16:33:04 - 04/09/2020 16
▲ 配布管理 <	Export Basic *  総索  C  III・  ユ・ ・
言 ログ管理 く	IPアドレス
■ レポート	
口 部署管理 《	
▲ ユーザ管理 <	

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

・脅威:ランサムウエアによる脅威と思われる行為内容を表示します。

「ランサムウエアファイル名変更」「ランサムウエアアクション検知」「ランサムウエアファイル毀損」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

\*検疫所ログは基本1ヶ月間、最大50,000ラインまで保存できます。50,000ラインを超過した場合は、古いロ グから10,000ラインを削除していきます。

#### 2.5.3 一般ログ

CMS Cloud	Ξ 🖉 Administrator.
MAIN NAVIGATION	- 角2日グ & Home > 一般ログ
@ \$\\\\\\ \$	
■ ポリシー管理 く	
₽ I-91>h <	
▲ 配布管理 〈	Export Basic * 総第 🗸 🗰 🕹 🗸 🗸
- U/B-1 (	IPアドレス キュージェント日付 受信日付 ユーザ名 キ 部署名 キ ホスト名 キレベル キ 区分 キ 内容
- V/- I. (	
□ 部署管理 〈	
▲ ユーザ管理 <	
	Showing 1 to 10 of 161 rows 10 + rows per page

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、ランサムウエ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。

\*検疫所ログは基本1ヶ月間、最大50,000ラインまで保存できます。50,000ラインを超過した場合は、古いロ グから10,000ラインを削除していきます。

#### 2.5.4 システムログ

	Ξ 🖉 Administrat
MAIN NAVIGATION	システム・ログ & Home > システム
48 ダッシュボード く	● 音成ログ ● 検疫所 盲 一般ログ ■ システムログ
■ ポジー管理 く	
🖵 I-স্টাস্ 🗸 🗸	m 04/02/2020 16:35:55 - 04/09/2020 16
▲ 配布管理 〈	Export Basic 🔻
言ログ管理く	ログ日付     +     ログレベル     +     アクセス者     +     抽検IP     +     ログ内容
≣ レポート <	
□ 部署管理 〈	
🛓 그 ザ管理 🛛 🔍 <	
▶ 設定 く	
	Showing 1 to 10 of 240 rows 10 + rows per page 24 - 2 - 3 - 4 - 5 24 >

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

\*システムログは基本7日間、最大50,000ラインまで保存できます。50,000ラインを超過した場合は、 古いログから10,000ラインを削除していきます。

#### 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、ランサムウエア感染情報メニューで分類されています。

										/17/2017 23:59:59				
12/17/2016 00:00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00:00     12/17/2016 00     12/17/2016 00     12/17/2016     12/17/2016     12/17/201     12/17/17/201     12/17/201     12/17/201     12/17/17/201     12/17/17/201     12/17/17/201     12/17/17/201     12/17/17/17/17/17/17/17/17/17/17/17/17/17/					<b>m</b> 0	1/17	/201	7 23:	59:59	9		Today		
0	0	•:	00	•	00	¥	0	23	•	59	•	59	¥	Yesterday
<	Dec	:	T	2016	•	>	<	Jan		¥	2017	Ŧ	>	Last 7 Days
Su	Мо	Tu	₩e	Th	Fr	Sa	Su	Мо	Tu	₩e	Th	Fr	Sa	Last 30 Days
27	28	29	30	1	2	3	25	26	27	28	29	30	31	This Month
4	5	6	7	8	9	10	1	2	3	4	5	6	7	Last Month
11	12	13	14	15	16	17	8	9	10	11	12	13	14	Custom Range
18	19	20	21	22	23	24	15	16	17	18	19	20	21	Apply Cancel
25	26	27	28	29	30	31	22	23	24	25	26	27	28	
1	2	3	4	5	6	7	29	30	31	1	2	3	4	

ライセンス、検知状況、ランサムウエ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			■ 05/02/2017 17:24:04 - 05/02/2017 17:44					
iday. Jun 2, AppChec	17:80 ckPro fo	r Window	Serverライセンス数量: 10									
	1	10										
調		7.5										
H-M-H		5										
		2.5										
		0 -										

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。

IP7FLA 0	ホスト名 ()	05倍報 ()	OSブラットホーム	◊ ユーザ名	グループ名	ツール
100000000	000000000	Vindows 10	x64 (AMD or Intel)	b.j.c001	20202020	
3666566	00000000	Vindows 10	x64 (AMD or intel)	bjo	3333333	
2000000	0000000	Windows 7	x64 (AMD or Intel)	JIRAN		
33333333	30000000	Windows 10	x64 (AMD or intel)	Sun	20000000	5
2000000	3000000	Windows 7	x64 (AMD or intel)	SangHeeJon	20000000	
33333333	3000000	Windows 10	x64 (AMD or intel)	joo	20000000	
38888888	33636366	Windows 10	x64 (AMD or intel)	ks j	3333333	
22222222	33333333	Windows 7	x64 (AMD or intel)	Lynx	22222222	
XXXXXXXXXX	200000000	Windows 7	x64 (AMD or intel)	djjung	XXXXXXXXXX	

ライセンス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たデ 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プラットホーム、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ダウンロードできます。

#### 2.6.2 検知状況



期間別検知状況では安全なエージェントとランサムウエア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。



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プラットホーム、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	ホーム	設置数
Windows 10		x64 (AMD o	r Intel)	5
Windows 7		x64 (AMD or	r Intel)	3
솜計				8
運用体制		ブラットホ	設置数	
No mate	ching records found			
솜탉				

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営体制(AppCheck Pro)とサ ーバ運営体制(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 ランサムウエア感染情報



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

Export B	asic V				S	'earch		C	•	<u>.</u>	۷
名前	♦ 部署名(最終部署)	エージェントID	↓ メインボードS/N	±.	対象バス	÷.	ファイル名	÷	厦	轢田付	÷
			No matching records found								

下段ではランサムウエア行為検知が発生した感染日付別で詳細ランサムウエ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



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

CMS CIO	ud	=		Ĺ
MAIN NAVIGATION		フーザ管理		Home
👧 ダッシュボード	<			
🔦 ポリシー管理	<	Export Basic 🔹 🍳 ユーザ追加 🗢 ユーザ削除 🛓 部署別ユーザ追加	Search	
📮 エージェント	<	□ 名前 ♦ Email	部署名(局統部署)	ユーザ情報
📥 配布管理	<		*****	🖾 Edit
111 ログ管理	<		*********************	🗹 Edit
■ レポート	<		***********************	G Edit
□	,			🖸 Edit
<ul> <li>コーザ数理</li> </ul>	Ì			🖸 Edit
	<u> </u>		***********************	🖸 Edit
> 設定	<		*****************	🖾 Edit
			******************	🖸 Edit
				🖸 Edit
			*****	🖾 Edit
		Showing 1 to 10 of 27 rows 10 . rows per page		< 1 2

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 <mark>ザ</mark> 管理				
Export I ~	0 1-9%m	• 1-47RBR		が追加
ユーザ情報			×	
部署:				
JIRANSOFT			*	
ЕХ~И∕:				
		1	業存する 取消	

「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 ×
<b>Notice!</b> 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。
<mark>ダウンロード:</mark> 部署EXCELダウンロード <b>アップロード:</b>
Drag & drop files here …
閉じる

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。

#### 2.8.3 ユーザ情報

ユーザ情報	×
部署:	
Jsecurity	-
ユーザ名:	
Eメール:	
備考(メモ):	
	/i
保存	する 取消

ユーザ管理リストに登録された特定ユーザ情報を修正するためには、Edit(編集)ボタンをクリックして既存に入力された部署、名前、Eメール、備考(メモ)情報を変更できます。

#### 2.9 設定

#### 2.9.1 管理者

CMS Cloud	= 🖉 🖉 Administrator.
MAIN NAVIGATION	管理者
🚳 ダッシュボード 🛛 🗸 <	
■ ポリシー管理 く	+ 追加 - 削除 ● ログインオブション ● ライセンスオブション 検索
	□ 名前
▲ 配布管理 〈	意み/書き Jsecurity Jsecurity 区 Edit
■ げ管理 く	読み/書き Jsecurity Jsecurity 区 Edit
≣ レポート <	D     D     Security     Jsecurity     Jsecurity     G Edit
口 部署管理 《	Showing 1 to 3 of 3 rows
▲ 그ザ管理 <	
▶ 設定 〈	
▲ 管理者	
◎ アラーム設定	

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。

管理者設定	$\times$
∕ணா/ப்ப_ு'.	
育理フルーフ:	
Jsecurity	-
部署:	
Jsecurity	*
名前:	
ЕХ- <i>I</i> /:	
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:	
== 選択==	•
保存する	取消

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。

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		$\times$
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

CMS Cloud	= e 🖉 Administ	trator.
MAIN NAVIGATION	ライセンス & Home > 設定 > 3	ライセンス
🕰 ダッシュボード 🔹 🤇		
■ ポリシー管理 <	+追加 ○ ライセンス更新	
<b>₽</b> I-ÿi>h (	会社 +     EXール +     ライセンス +     製品 +     ライセンス数 +     終了日 +     削除	¢
▲ 配布管理 〈	CMS CLOUD 1 2020-10-27 00:00:00	
■ ログ管理 🔹	AppCheck Pro 5 2020-10-27 00:00:00	
■ レポート く	AppCheck Pro for Windows Server         1         2020-05-07 00:00:00	
い 部署管理 く	Showing 1 to 3 of 3 rows	
▲ 그-ザ管理		_
▶ 設定 <		
▲ 管理者		
ライセンス		
② アラーム設定		

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。

	$\times$
認証する	取消
	認証する

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上で脅威ログが検知されたタイミングでメール通知を行います。

それぞれの設定時間ごとにチェックを行い、メール通知をします。

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。

CMS Cloud	=	🖻 🗘 Administrator.
MAIN NAVIGATION	アラーム設定	<b>必</b> Home > 設定 > アラーム設定
<ul> <li>の グッシュボード く</li> <li>同 ポリシー管理 く</li> </ul>	■アラーム設定	
🖵 I-স্টা>া 🗸	Tip! ランサムウェアアクション後知が発生した場合のみにお知らせメールが以下に登録したメールアドレスに送信されます。	
🛓 配布管理 🛛 🗸 🤇		
		S III -
	■ アラーム設定 ×	ツール 
▲ ユーザ管理 <	EXールを入力して下さい。(複数の場合は、カンマ(,)区切りでEメールを入力して下さい。) Showing 1 to 1 of 1 rows	HURA JIST
▶ 設定 く		
<ul> <li>管理者</li> <li>ライセンス</li> <li>アラーム設定</li> </ul>		
	<ul> <li>● 15分</li> <li>● 1時間</li> <li>● 1日</li> <li>● 1週間</li> <li>通問</li> </ul>	

## 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。

#### 2.10.1 パスワード変更について

CMS CLOUD						
現在のパスワ ード		ライセンスキ ー	仮パスワード			
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。						
	EX-1					
	現在のパスワ	—	<b>a</b>			
	パスワード		<b>A</b>			
	パスワード確	認.	÷			
	ログインページ	に移動	変更			

- ■「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

CMS CLOUD						
現在のパスワ ード	ライセンスキ ー	仮パスワード				
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。						
E メール		⋈				
ライセンス	マキー	<b>a</b>				
パスワート	*					
パスワー	《確認	÷D				
ログインペ-	-ジに移動	変更				

■「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

CMS CLOUD				
現在のパスワ ライセンスキ ード ー	仮パスワード			
Eメールで仮パスワードを送ります。				
E メール	$\bowtie$			
ログインページに移動	送信			

・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。