



AppCheck CMS Cloud

マニュアル

株式会社 JSecurity

第28版 2025/6/3



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 エージェント現況	
2.1.3 24時間内上位5位脅威	
2.1.4 エージェントバージョン	
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 部署別ポリシー適用	
2.2.2 ポリシーの追加・削除、ファイルの出力・検索	
2.2.3 ポリシー管理 : 一般	
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 ポリシー管理 : 退避フォルダ	
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	
2.2.10 退避フォルダ設定	29
2.2.11 自動バックアップ設定	
2.3 エージェント	
2.3.1 部署別ポリシー適用	
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	
2.3.5 エージェント削除	
2.3.6 エージェントのライセンス変更	
2.4 配布管理	

JSecurity

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	
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	
2.4.2.3 イメージ添付	
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	
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	51
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	57
2.8 ユーザ管理	
	58
2.8.3 ユーザ情報	
2.9 設定	
	61
2.9.1 6.2 $-2.5.1$ 6.2 $-2.5.1$	63
2.9.3 アラーム設定	
2 10 パスワードを忘れた場合	65
	UJ
2.10.1 ハスノート友丈について	00



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 V1.1.37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
	•Microsoft Edge
ブラウザ	•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
```

 使用するにはログインしてください 日本語 エメール エメール ブスワード ご参考ください。 	CMS CLOUD	
管理者初期登録	使用するにはログインしてください 日本語 ✓ Eメール ズ パスワード Dを記憶する パスワードを忘れた場合 管理者初期登録	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。

CMSCloud	•					• • ***
NEW NEVIGATION	ダッシュボード 2025-02-05 15:50:00 * 2025-02-05	15:55:00				6 Rom > ダッシュボード
● ダッシュポード	全体エージェント数	安全	ランワムウェア検知	エクスプロイトガード情報	通うイセンス数	
■ ポリシー管理	5 FX2FoT4/T-R1	✓ ³	• • •		デスクトップロ / サールS	
□ エージェント						
▼ NeBH	e 時間別株和 (unitationed					- / *
■ ログ管理			拉爾伯迪和 尔尔			
■ レポート	- C -					
□ 新餐務課	с.					
▲ ユーダ開展						
× 82		• • • • • •	· · · · · ·	· · · · ·		
	i i i i i i i i i i i i i i i i i i i					
	tales tales	talas talso talse telos telos	valno valno valno valno valno	value value value value	16/86 16/00 16/06 16	10 1615
			◆ ランサムウェア検知 ◆ エクスプロイトガード活動			
	エージェント現況		- = 24時間内上位5位筹成			- *
	全体インストール済エージェント					
	1 (201) 5 (20) (20) (20) (20) (20)					
		4	1			
			1			
	エージェント状況					
	展観エージェント		8	0 Videos		
	\$75451-515F		0	- 発展なし		
	エージェントパージョン		- × Linuxエージェントバージョ	32		- ×
	最新エージェントパージョン:3.1.39.3		最新エージェントパージョン: 1.	0.3-51		
	3.1.36.2 1 3.1.39.3 3		1.0.4511			
https://ip.cms.checkmal	Lcom/agent					



CMS Cloud の各機能について

2.1 ダッシュボード

G922xF.F. Backet 1889: 38646 1830 Image: 120228 Image: 120228 Image: 120228 Image: 120228 Image: 120228 Image: 12028 Image: 120					
	ダッシュボード 2025-02-05 15:	:00 * 2025-02-05 15:55:00			
C P23/92/17-03 P23/92/17-03	全体エージェント数 5	S# 5	ランサムウェア検知 0	エクスプロイトガード情報	
PRESERVE LANCE 4	F29F974/9-73			~	デスクトップ:1 / サーバ:5
Image: Participation of the state of the	時間別検知 (unitralinute)				
Improved provide and the state the stat					
Image: State Stat			時無別執知状況		
1 1					
1 100 101		• • • • • •			· · · ·
No. No. <td>Ĥ</td> <td></td> <td></td> <td></td> <td></td>	Ĥ				
108 1					
NA <					
3dt/JR-/MZ922/h Page Image Image	エージェント現況		- = 24時間内上位5位時	ġ.	
Image:	全体インストール済エージェント				
Image: Section 1 Image: Section 2	1998 5 19975 0 (0%) 197521977 4 (80%)		1		
x->zz/ktk 0 ##1-912/b 0 739/21-912/b 0 X->zz/b(-/52/b) - * ##1-912/b - * ##1-912/b - *			5		
SEL-9121+ 0 4 4 1737-1212+ 0 3 3 4 SEL-912-912+ 0 3 3 6 T-922/MI-922+ - * 8 8 6 6 SEL-912+ - * 8 8 6					
(オブダンユージェント (ナブダンント・コント (ナブダンント (ナブダンン (ナブダンン (ナブダンン (ナブダンン (ナブダンン (ナブダンン (ナブダンン (ナブダン (ナブダン (ナブダン (ナブダ (ナブダ (ナブダ (ナブダ (ナブダ (ナブ ((((((((((((((((((()))))))))	エージェント状況				
I_9I2>N/(-92> - • #II_9I2>N-92> 1.01 ■ 133()	エージェント状況 線ボエージェント		0	a Vitas	
##2-9/20/1-0/20/11.R.1 ■ 1383/10 1383/10	エージェント状況 振校エージェント オフラインエージェント		0	a Values Malau J	
R32311	エージェント状況 厳モニジェント オフラインエージェント エージェントパージョン		0	a Vana Mittar	
	エージェント状況 厳ロニジェント オフラインエージェント エージェントパージョン 総数ニージェントパージョン: 1.1.3.1		0	u Vices ■ Mitto	
	エージェント状況 解乳-ジュント オフマインエージェント エージェントパージョン 解乳-ジュントパージョン 解乳-ジュントパージョン 副乳-ジュントパージョン 副乳-ジュントパージョン		0 0	a vaues ■ Mildot	
	エージエント状況 酸モニジュント オフラウンコージェント エージェントパ(ージョン 酸モニージェントパ(ージョン 酸モニージェントパージョン 11.8.1 13.83);		0 0	ausa Mitatu	
	エージェント状況 第12-0120ト オフラインス-0120ト エージェントパージョン 第12-0120トパージョン 11311		0 0	s toos ■ Meto	

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)

・エージェント現況(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)

・24時間内上位5位脅威(2.1.3をご参照ください)

・エージェントバージョン(2.1.4をご参照ください)

・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: ランサムウエア検知が発生していないエージェント数

・ランサムウェア検知 : ランサムウエア検知が発生した数

・エクスプロイトガード情報:保護対象アプリケーションに対しての脆弱性攻撃遮断数

・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 エージェント現況



エージェント現況では、インストールー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 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。



2.1.4 エージェントバージョン



エージェントバージョンでは、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。

2.1.5 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

CMS Cloud	Ξ 🖉 🖉 Administrator.
MAIN NAVIGATION	脅威ログ & Home > 脅威ログ
@ ⁶ /9951#-1 ^k <	☆ 育成ログ ●検疫所 ■一般ログ ■システムログ
■ ポリシー管理 く	
□ I-ÿI>ト	04/02/2020 15:28:16 - 04/09/2020 15:28:16
▲ 配布管理 〈	Export Basic Y 検索 🗘 III - Ž - Y
■ 四管理 く	IPアドレス キ エージェント日付 キ 受信日付 キ ユーザ名 キ 部署名 キ 木スト名 キ 検知主体 キ 脅威 キ 種類 キ 対象パス キ 処理 キ
■ レポート <	
口 部署管理 〈	
▲ 그-ザ管理 〈	

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

CMS Cloud	≡									e 4	Administrato
MAIN NAVIGATION	ポリ	シー管理								@ Hon	ma > #ilis_#i
월 ダッシュボード <											NC > 1(7)- B.
■ ポリシー管理 く		ポリシー管理									
■ ポリシー管理		Export Basic	٣	□ 部署別一括ポリ	シー適用 + 追加	- 削除			給委	g	A. V
▲ SMB 設定										~~ ~	
査 退避フォルダ 設定		◎ ポリシー名 🔅	Туре 🕴	初期作成時間	最終変更時間	最終適用時間	グージョン 0	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 <mark>ン</mark> ト数	♦ 説明 ♦
■ エージェント <		基本ポリシー	Windows	2019-10-28 16:39:33	2020-04-09 14:34:37	-	2	-	-	ロボリシー ID	A
▲ 配布管理 <		営業部ポリシー	Windows	2020-04-06	2020-04-09 14:39:10	2020-04-06	4	0	0	✓ ホリシー名 ✓ Type	営業部
■ ログ管理 <		JJS基本	Windows	2019-10-28	2020-04-09	2019-11-21	3	0	0	☑ 初期作成時	
レポート <				17:22:53	14:38:59	11:50:56				[6]	
口 部署管理 《		howing 1 to 2 of	F 2 rows							✓ 最終変更時 間	•
▲ ユーザ管理 く		1000 ng 1 to 2 0	210/03							✓ 最終適用時間	
🗲 設定 🗸										✓ バージョン	*

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。

<u>※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。</u>

<u>※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</u>ント数」は表示されません。

<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</u> <u>定後「個別ポリシー適用」ボタンを押してください。</u>

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)

- ・タイプ: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 部署別ポリシー適用

「ポリシー管理」⇒「部署別ポリシー」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。





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。

	=		Administrato
MAIN NAVIGATION	-	e	
📾 ダッシュボード 🗸	ポリシー管理		🙆 Home > ポリシー管理
□ ポリシー管理 く	■ポリシー管理		
□ ポリシー管理			
▲ SMB 設定	Export Basic V DEEM-MAS-A + AL + AL - KR	sharkonetest@gmail.com 🗘 🚦	I- <u>Z</u> - →
★ 退避フォルダ 設定			
🖵 エージェント 🔹 🤞	■ 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 ≑ 対象工	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
▲ 配布管理 <	基本ポリシー Window jp.cms.checkmal.com の内容 2 ポリシーをを入力してください パリシーをを入力してください 2		-
➡ 口グ管理 <	■ 営業部ポリシー Window 4	0 0	0
■ レポート く	」 JJS基本 Window OK キャンセル 3	0 0	0
□ 部署管理 <			-
ユーザ管理 <			ł
▶ 設定 く	Showing 1 to 2 or 2 rows		



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―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

. 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-	一説明:					
Enter	·					
🗸 リア	ルタイムセキュリティ	ィを常に設定する。				
Lock Mo	ode : ON	•				
🗌 個別	コージェントオプショ	ョン変更許容(CMSポリシー無	視)			
ライブラ	チェック周期: 15分	∂毎(デフォルト値) ・				
□ アブ ☑ タス ☑ プロ ☑ 自動 ☑ MBR(パリケーション削除許す クトレイにお知らせて ログラム実行遮断時、す ロアップデート使用 呆護	可 アイコン表示 6知らせダイアログ表示				
 ✓ 自己 ○ 検出 (匿 	保護機能使用 1時、疑いのあるファ・ 名で処理され、分析り	イルを転送 以外の目的では使用されませ	huo)			
			ſ-	般」初期化全体初期	化保存する	取消

・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: OFFにすると、ユーザがAppCheckProのオプション変更ができるようになります。

・個別エージェントオプション変更許容(CMSポリシー無視) : 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、チェックされていません。(アンインストール不可)

・タスクトレイにお知らせアイコン表示: 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: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)

1. 基本ポリシー 🖋					\times
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	
 マランサムウェア攻撃保護 AppCheckPro拡張機能 「保護領域」 マネットワークドライ マリムーバブルディス マSMBサーバ マランサムウェア遮断 保護するファイル拡張子 	(ブ ペクドライブ (後、自動復元 		 [高級検知機能] ゴースト検知 スマート検知 スマート検知 ※AppCheck Pro foi 直接設定する必要か 【脅威遮断機能】 ジステム脅威遮断 	r Windows Server エージェントはオプションで べあります。 断	
ランサムウェア検知後の動作 疑わしいファイル毀損検知回 SMBサーバー保護検出回数 :	F: ブロック及び治療 回数: 10 10	•			
			נקו	パサムガード」初期化 全体初期化 保存する	取消

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。

・ネットワークドライブ: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: 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: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、「リポート先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。

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

・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 - スマート検知

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。

※高級探知機能について、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

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,chm,crt,csv,dcm,der,doc,docx,dotm,dotx,dwg,efi,eps,gif,hwp,hwpx,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。

システム側で「保護するファイル拡張子」が新たに登録される場合がございますが、

その際に、既にご利用されている「保護するファイル拡張子」の一覧上に自動追加はされませんので、該当メニュ ー内の「初期化」ボタンをクリックし、新しい保護対象拡張子が追加されたことを確認頂き、「保存する」をクリック して反映頂くようお願い致します。

※お客様側で直接追加頂いた保護対象拡張子に関しては「初期化」の際に削除されますので、該当拡張子 に関しては再度登録を行うようお願い致します。

・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。





[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ございます。



 \times

2.2.5 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	自動バックアップ	例外設定		
□ エク 保 び W び つ び ク び ク	フスプロイトガードを付 護するアプリケーシ ebブラウザ(IE, MS Ed プラグイン(Java, Flas 〈ディアプレーヤー(WM tフィス(MS Office, H	使用 ge, Firefox, Opera) h) P, WMC, GOM Player, Pot P ancom Office, Adobe Acrob	layer) at)				
			[II]	フスプロイトガード」 初期化	全体初期化	保存する	取消

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<u>「エクスプロイトガードを使用」</u>のチェックボックスと <u>「保護するアプリケーション」</u>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」を有効にしてい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, Firefox, Opera					
プラグイン	Java、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					



2.2.6 ポリシー管理 : 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	
✓ ランサムウェア退避フォ. 	ルダ使用				
退避フォルダパス : D	:¥ProgramData¥CheckMAL¥Ap	pCheck¥RansomShel	ter		設定
□ -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.	ルダを非表示				
- 退避フォルダ自動削除	×				
✓ 7日	▼ 経過したフ	ァイルを自動削除			
□ 退避フォルダ容量が	50GB	▼ になると、き	い順でファイルを自動削	除する	
※バックアップファイルを を一時的にOFFにし、ファ・	手動削除する際には、「Apr イルの削除後には必ずONに戻	oCheck」-「オプシ」 してください。	ョン」-「一般」-「自己係	<護機能使用」	

・ランサムウェア退避フォルダ使用: AppCheckProのランサムウェア退避フォルダ機能を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: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

⊥基本ポリシー♂			×
ー般 ランサムガード エクスプロイトガード 逃避フォルダ 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			
バックアップ対象(フォルダ指定)	追加 除去	除外対象(フォルダ指定)	追加 除去
SUSERPROFILESWDesktop NUSESPROFILESWDesments NUSESPROFILESWDest NUSESPROFILESWDest NUSESPROFILESWDest NUSESPROFILESWDest	۸ ۲		۵ ۲
□ 指定した施張子のファイルのみバックアップ(区分子,または;)		パックアップ対象から除外するファイル拡張子(区分子,または;)	
パックアップ先		10月 ファイル(27万数· 2 -	
○ ネットワーク共有フォルタ(SMB/CIFS) サーバアドレス		出有フォルダ	
		7H / 1///	
ユーザID		バスワード	
※バックアップファイルを手動削除する際には、「AppCheck」-「オブション」-「一般」-「自己	呆護機能使用」を一時的にOFFに	し、ファイルの削除後には必ずのに戻してください。	
		「自動バックアップ」初期化 全体初期化	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ー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。

・バックアップ対象(フォルダ指定):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)

・指定した拡張子のファイルのみバックアップ (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)

・除外対象(フォルダ指定):「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。



・バックアップ対象から除外するファイル拡張子 (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。

・バックアップ先: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	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	退避フォルタ	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							
							*		
							Ψ.		

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「信頼済みプロセス一覧」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 登録するようにお願いいたします。

・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>

1.基本才	^{ピリシー}				>
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
[信頼泳 ☑ 以下	みプロセス一覧] 「に登録されたプロセス	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 ☑ 以下	す象ファイルの例外一覧 「に登録されたファイル	記 レ変更は検知しない 追加 修	正 削除		v
					•
[例外]	フォルダ一覧]				Ŧ
🗹 以下	「に登録されたフォルタ	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	四期化 全体初期化	保存する 取消

⊙ 信頼済みプロセス一覧

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 登録するようにお願いいたします。

・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 : プロセス登録後には、必ずこちらにチェックが入っていることを確認お願いいたします。(デフォルトチェック有)

○ 保護対象ファイルの例外一覧

保護する拡張子に該当するファイルの中、保護対象ファイルの例外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変更は検知しない:ファイル登録後には、必ずこちらにチェックが入っていることを確認お願いいたします。(デフォルトチェック有)

○ 例外フォルダー覧

例外フォルダー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。

・以下の登録されたフォルダ内のファイル変更は検知しない : フォルダ登録後には、必ずこちらにチェックが入っていることを確認お願いいたします。(デフォルトチェック有)

「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。

※ワイルドカード(*・?)の設定について

すべての一覧(プロセス・ファイル・フォルダ)で利用することができます。利用する際は適切に設定を行ってください。

例)

信頼済みプロセス一覧	C:¥Users¥nanashi¥Desktop¥Fire¥*¥setup.exe
例外ファイル一覧	C:¥Users¥nanashi¥Desktop¥Fire¥*¥test.jpeg
例外フォルダ一覧	C:¥Users¥nanashi¥Desktop¥?¥test



2.2.9 SMB設定

CMS Cloud	≡		¢ ⁰ #
MAIN NAVIGATION	SMB設定	🙆 Home	a > SMB ₿
🙆 ダッシュボード 🛛 <			
■ ポリシー管理 く			
■ ポリシー管理			
▲ SMB 設定			-
▲ 退避フォルダ 設定			
■ 例外設定			
▲ 自動バックアップ設定			
□ エージェント <			Ψ.
▲ 配布管理 <			
こので管理 く			
■ レポート く			
ロ部署管理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			
▲ 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	Ξ e Δ ^e shin
MAIN NAVIGATION	SMB設定 @ Have > 38 設定
😤 ダッシュボード <	共通
■ ポリシー管理 く	
■ ポリシー管理	Search C III · ·
▲ SMB 設定 棄 退職フォルダ 設定	□ Asent ID IPアドレス WACアドレス ホスト名 05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 <u>ツール</u>
□ エージェント <	
之 配布管理 <	Showing 1 to 1 of 1 rows
ログ管理 く	
■ レポート く	
□ 部署管理 〈	
📥 그 ザ管理 <	
▶ 設定 <	

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



CMS Cloud	Ξ 🖉 Δ ¹ shin
MAIN NAVIGATION	SMB設定 A Rose > 38 設定
ダッシュボード	く
■ ポリシー管理	
■ ポリシー管理	Bearch C III · ·
■ SMB 設定 査 退避フォルダ 設定	□ Asent ID IPアドレス MACアドレス ホスト名 0S情報 ユーザ名 部署名 インストールバージョン 単 現状態 最終オンライン時間 ツール
🖵 エージェント	
▲ 配布管理	Showing 1 to 1 of 1 rows
■ ログ管理	c
📼 レポート	e de la construcción de la constru
D 部署管理	e de la construcción de la constru
🛓 ユーザ管理	
▶ 設定	c

・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

	≡	a 🖉 🖉 Administra
MAIN NAVIGATION	退避フォルダ設定	& Home > SMB
📾 ダッシュボード <		_
■ ポリシー管理 く		
■ ポリシー管理 ▲ SMR 設定	Search	S ⊞- ≛- ¥
▲ 退避フォルダ 設定	Agent ID ÷ IPアドレス ÷ MAC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	
↓ エージェント く		=
▲ 配布管理 <		=
■ ログ管理 <		=
■ レポート		=
□ 部署管理 〈		
📥 ユーザ管理 🛛 <		
▶ 設定 く	Showing 1 to 5 of 5 rows	
	退避フォルダ設定	
	■ フノブムウェア必避ノオルタ使用 3日時コナルボバフ・ DYDrearsePot+XfkackWHX4aafkackWDaacaafkaltar	-1
		axAE
	 □ 一つのファイルの大きさを最大 □ 16B □ 」 ↓ 以下に制限 □ 」 □ 」 	
	- 退避フォルダ自動削除	
	 ✓ 7 日 	
	□ 逃避フォルダ容量が 50GB ・ になると、古い順でファイルを自動削除する	
	※バックアップファイルを手動削除する際には、「AppCheck」-「オプション」-「一般」-「自己保護機能使用」を一時的にOFF にし、ファイルの削除後には必ずONに戻してください。	
	(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)	



2.2.11 自動バックアップ設定

CMS cloud				# 🖓 ##R
MATH NAVIGATION	自動バックアップ設定		at Ho	ee - 白銀パックアップ設定
ダッシュボード く	★ 「日間バックアップ」初期化		kurokunati secur i	S ⊞• Q
■ ポリシー管理	エージェントID 1Pアドレス 0 MKCアドレス 0 ホスト名	◎ 05情報 ◎ ユーザ名 部署名 ◎	インストールパージョン リ 現状態 日 最終オンライン時間) ツール
▲ 548 設定 ★ 送迎フォルダ 設定				8 -
A 6800070-789				ŝ =
■ I=910F (8 🕒
▲ 配布管理 <	Showing 1 to 4 of 4 rows			
■ ログ管理 く				
 ▲ ユーザ管理 				
+ 82 ×				
・自動バック	アップ設定: エージェント別のバックアップ	設定が可能です。		
	自動バックアップ設定	-	X	
	自動バックアップ使用 スケジュール設定			
	バックアップ対象(フォルダ指定) 追加	除去 除外対象(フォルダ指定)	追加 除去	
	SUSERPROFILES/EDesktop		*	
	%USERPROFILE%¥Favorites			
	%USERPROFILE%#Pictures %USERPROFILE%#Music			
	%USERPROFILE%#Videos			
	•		w	
	□ 指定した拡張子のファイルのみバックアップ(区分子,または	;) バックアップ対象から除外する	5ファイル拡張子(区分子,または;)	
	バックアップ先			
	● ローカルディスク C:¥ AutoBackup(AppCheck)	履歴ファイル保存数: 3		
		□ WORMストレージモード		
	○ ホットワーク共有フォルタ(SMB/CIFS) サーバアドレス	出有フォルダ		
		7519 2 9 10 3		
	ユーザID	パスワード		
	※バックアップファイルを手動削除する際には、「AppCheck」-「オ 必ずのいこ同してください」	プション」-「一般」-「自己保護機能使用」	を一時的にOFFにし、ファイルの削除後には	
	a source of success			
			All danse 7	
			1米1子9 合 职(2月)	
	(設定内容については ※2.2.)	7 「自動バックアップ」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

<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、ホストネーム、 OS情報、OSプラットホーム、ユーザ名、部署名、部署名(最終部署)、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、ライセンスメールアドレス、ライセン ス、ライセンス満了日、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

JSecurity

・**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
- ・ホスト名: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
- ・部署名: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

・部署名(最終部署):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

及び上の階層もすべて表示

・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: 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)

- ・ポリシーバージョン:エージェントに適用されたポリシーバージョン
- ・最新ポリシーバージョン: CMS Cloudに登録されたポリシー名の最新ポリシーバージョン
- ・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。
- ・リアルタイムセキュリティ:現在のリアルタイムセキュリティのステータスを表示できます。
- ・最終オンライン時間:オンライン状態の最終時間

・ライセンスメールアドレス:ライセンスに紐づくメールアドレスを表示します。

- ・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。





2.3.1 部署別ポリシー適用

CMC	_						
	=						
MAIN NAVIGATION	エージェン	F 8888	2002222222				
🙆 ダッシュボード <		- 2000	~~~~~				
	ユージェン	トリスト					
□ ホリシー管理 <	Even et Ber			• /0090+**112		46-27-28	パックフップフィルガキがにオス
↓ エージェント く	Export Bas	SIC P	□ 部者別ホリシー週月	ב ליאועימואו 🛎		報一括変更	F バックアップフォルタを空にする
	_						
		部署別ポリ	シー適用			\times	
		k 📼 🙉 u	PANCOFT				
		4	000000000			Î	
		a 📰 🧣) グロ パール0EM チーム 技術チーム				
		L 6	🛄 営業チーム				
			』海外事業部] 営業チーム				
			🧾 技術チーム			*	
				Filter		III -	
		10	ポリシー名前	÷	リビジョン	۵	
		6	ポリシーテスト		1		
		© 5	テストポリシー		1		
		Image: 4	ポリシーミ		1		
		3	基本 ポリシー		1		
		0 2	TEST2		1		
		Showing 1 to	5 of 6 rows 5 _ rows per	page	< 1	2 >	
					適用	取言道	
	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

CMS Cloud	=						
MAIN NAVIGATION	エージェント 🕅		88				
89 ダッシュボード <	□ エージェントリス	(F					
■ ポリシー管理 く	Export Basic	~ 0	5 部署	別ポリシー適用	▲ 個別ポリシー適用	田 情報一括変更	パックアップフォルダを空にする
エージェント く					/		
					Filter		
				غذيني والع		111202-21	
			10	ホリン~名前	Ť	96237	
		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	
		Showin	g 1 to	5 of 6 rows 5 🔺	rows per page	< 1 2 >	
						通用 取消	

個別ポリシー適用では、部署別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
📾 ダッシュボード 🛛 🔇	ロエージェントリスト
ペ ポリシー管理 <	
□ エージェント 〈	Export Basic V 口部者別ホリソー週用 ● 御知ホリシー通用 ■ 情報一指変更 アバックアップフォルタを空にする ×.
	情報一括変更 ×
	Notice! アップロード時必ずファイル部株子は.x1sで型内ま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: フォーマットダウンロード アップロード:
	Drag & drop files here
	🖀 Browse
	間じる

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1	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、 **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

P :	エージェント!	リスト						
	Export Basic	· · D	「部署別一括ポリ	シー適用	👗 個別ポリシー適用	■ 情報→括変更	パックアップフォルダを空にする × エージェント削除	
						Ļ		
X Ba	ickupフォルダを空	ミにする				★ Backupフォル	ダを空にする	
₫空(i	こする領域を選択してくださ	εU1				◎ 空にする領域を選択し	ってください	
目前	動バックアップフォルダ(Aut アルタイムバックアップフォルダ	toBackup)を空にす (Backup(AppCh	る eck))を空にする			 自動バックアップフォル リアルタイムバックアップ 	ダ(AutoBackup)を空にする ウォルダ(Backup(AppCheck))を空にする	
» I	ロージェント別を空にする	» 部署別を一括空	<u> </u>			» エージェント別を空に	する » 部署別を一括空にする	
						部署を選択してく	ださい	
	1₽アドレス 🕴	масアドレス 🝦	ホストネーム 🖕	os情報 🝦	osプラットホーム 🖕		N SOFT ******	
	xxxxxxxxxx 2			Windows 10	x64 (AMD or Intel)		ロバールOEMチーム 』技術チーム	
				Windows 10	x64 (AMD or Intel)	·····································	3 営業チーム 外事業部	
	*******		00000000000	Windows 10	x64 (AMD or Intel)		◎ 営業チーム 〕 技術チーム □ 技術チーム	
	xxxxxxxxxxxxx g		222222222222222	Windows 7	x64 (AMD or Intel)		キュリティ事業部 IRANSOFT JAPAN	
	00000000000000		20000000000	Windows	x64 (AMD or	3a		

自動バックアップ(2.2.7 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

CMS Cloud	E
MAIN NAVIGATION	
 かりシュボード く 	
■ ポリシー管理 く	↓I-ジェンドリスト
₽ 1-91% <	Export Basic
	cms.checkmal.com の内容 エージェント削除時すべての情報が同時に削除されます。現けますか? のK キャンセル 都用 回 情報一括実更 グ パックアップフォルダを空にする X エージェント削厚来

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

クライアント配布							
Tip! AppOheck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 Wi	ndows Server				現在の最新バージ	∃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	Email	
300000000000000000000000000000000000000		171	2024-12-31	📥 AppCheck V3	📥 AppCheck V3	🖂 Email	
AppCheck Pro					現在の最新「一ジ	ヨン: 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	Email	
		5 / 5	2024-12-31	📥 AppCheck V3	📥 AppCheck V3	🖂 Enail	

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。

・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が表示されない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

ユーザ選択

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)	
■ メールタイトル AppCheckエージェントブログラム配布メ	ールです。	
★ ☆ ● 월 ☶ 클 \$ 월 9/-ス B :: スタイ	ιL -	
	AppCheck Proインストール	

💼 基本内容呼び出し 📑 EXCELでメール送信 🖂 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		×
Q 検索する 受信都Eメール(複数の時は(,)で区分してください)		
■ 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。		
◆ / ● □ 田 書 済 回 ソース B == スタイル ・		
		Î
AppChack Bro Z > Z h - II		
		· ·
★ 其未供加速率(14)	DA EXOSI アメール送信	ロモノール祥信
ユーザ選択	×	
Tip!		
部署やユーザを選択してください。部署選択時に下位部署の時は合わせて送信! す。	Lā	
個人 部署 再任业		
216-4		
JIRANSOFT	^	
88888888 グロバール0EMチーム → 追加		
技術ナーム 営業チーム ← 削除		
海外事業部 営業チーム	-	
技術ナーム・		
確認	取消	

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

◆ → ● 口面目 X Bソース B II 291/k -	8
AppCheck Pro インストール	
	▲ 基本内容符び出し
インストール案内EXCEL形式アップロード	×
Tip! 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。	
ダウンロード: インストール案内EXCEL形式ダウンロード アップロード:	
Drag & drop files here	×
🕿 Вгомяе .	
जित्त 12 वि. सि. सि. सि. सि. सि. सि. सि. सि. सि. स	5

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。

インストール案内EXCEL形式アップロード ×	jp.cms.checkmal.com の内容
Tip!	インストールEXールを送信しました。
エクセルファイルをアップロードし、下鉄の「アップロード」ボタンをクリックす ると、インストール案内メールが自動送信されます。	ОК
ダウンロード: インストール案内EXCEL形式ダウンロード	
アップロード:	
(25.5 KB) 8- wis	
100%	
🖹 🗮 🐨 Upload 🗁 Browse …	
閉じる	



2.4.2.3 イメージ添付

ユーザ選択



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。

Tipl AreOned 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。 現在の見形// フィセンス インストール認証キー 残余数量 / 数量 満了日 配布 Silent 配布 1 / 1 2024-12-31 ▲ AppCheck V3 ▲ AppCheck V3 ▲ AppCheck V3 ▲ AppCheck V3 ↓ DE Email 現在の見形// 本 AppCheck Pro ライセンス インストール認証キー 残余数量 / 数量 満了日 単 元 AppCheck V3 ▲ AppCheck V3 ▲ AppCheck V3 ▲ AppCheck V3 ↓ DE Email 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 Email	クライアント配布 & Hose → 配布管理							
AccOrect エージョントインストールファイルアドレス EE メールで送信して献布できます。 AppCheck Pro for Windows Server ライセンス インストール認証キー 残余数量 / 数量 1 / 1 2024-12-31	Tipl							
現在の見知い 現在の見知い 現在の見知い こここここここここここここここここここここここここここここここここここ	AppOheck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。					
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 Email ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	AppCheck Pro for Wir	ndows Server				現在の最新バー	ジョン:2.5.57.2/3.1.37.4	
AppCheck Pro インストール認証キー 残余数量 / 数量 /	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	Email	
AppCheck Pro 現在の最新 「ション: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 Email	**********		171	2024-12-31	📥 AppCheck V3	📥 AppCheck V3	🖂 Enail	
AppCheck Pro 現在の取材 (ーンヨン:2.5.5/.2/.3.1.3/.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 Email						現在本見がよう	N - N	
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 Email	AppCheck Pro					現住の最新、(一)	シヨン: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	满了日	配布	Silent 配布	Email	
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX			5 / 5	2024-12-31	📥 AppCheck V3	📥 AppCheck V3	🖾 Enail	

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 S erver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)			
S 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。

S 4	AppCheckPro		_		×
i S S	オンラインサポート ウェブサイト及びコンテンツ 刺45.00パライセンフ情報	製品情報 製品名 : AppCheck Pro アンチランサムウエア			
©	☆Ш/X0 / 1 C/ X IB tX	 パージョン: 3.1.25.1 最近のアップデート日(年/月/日): 2022/12/1 アップデート アップデート内容確認 			
		ライセンス情報 製品名: AppCheck Pro アンチランサムウエア Eメールアドレス: ライセンスキー: ライセンス数: 5 サービス満了日:(年/月/日): 2022/12/31			
			パージ	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。



・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	Ξ
MAIN NAVIGATION	- 一般ログ & Home > 一般ログ
 	
■ ポリシー管理 く	
₽ I-ÿi>h <	E 04/02/2020 16:21:15 - 04/09/2020 1
🛓 配布管理 💦 🗸 🗸	Export Basic *
言 பげ管理 く	IPアドレス
■ レポート <	
口 部署管理 〈	
▲ ユーザ管理 〈	
▶ 設定 く	
	Showing 1 to 10 of 161 rows 10 + rows per page < 1 2 3 4 5 17 >

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

・部署名(最終部署): 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 及び上の階層もすべて表示

・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。

・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10,00 0行単位で自動削除されます。

脅威パスに一部リンク付きファイルパスが記載され、クリックすると、【すべてのポリシーの信頼済みプロセス一覧】に登録 するかどうかのポップアップが表示されます。【OK】を選択した場合、対象パスが信頼済みプロセス一覧に登録されます。





2.5.2 検疫所

CMS Cloud	Ξ Administrator.
MAIN NAVIGATION	検疫所
必 ダッシュボード く	● 育成ログ ● 検疫所 ■ 一般ログ ■ システムログ
■ ポリシー管理 く	
₽ I-ÿi>ŀ <	
▲ 配布管理 〈	Export Basic 🔻 🖉 🏭 🗸 🗸 🗸
雪 ログ管理 く	IPアドレス
■ レポート <	
口 部署管理 〈	
▲ ユーザ管理 〈	
▶ 設定 <	

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」ログには、ランサムウェア動作検知により隔離されたファイルや日時などの情報が記録されます。

また、検疫所フォルダ(C:¥ProgramData¥CheckMAL¥AppCheck¥Quarantine)には隔離されたファイルの 情報がHASH値として保存されており、大量のファイルが検疫されることでディスク容量を圧迫する可能性がありま す。そのため、状況に応じてエージェント画面の検疫ログから削除し、必要に応じて元の場所へ復元することで、フォ ルダの管理を適切に行っていただきますようお願いいたします。

(検疫フォルダ内のファイル削除や復元はエージェント画面からのみ可能になります)

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

・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

・部署名(最終部署): 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

及び上の階層もすべて表示

・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、古い順に10,00 0行単位で自動削除されます。



2.5.3 一般ログ

CMS Cloud	🗏 🧧 🖧 Administrator.
MAIN NAVIGATION	一般ログ & Home > 一般ログ
@ \$y>j_1k=1 <	● 音频ログ ● 桂枝所 ■ 一般ログ ■ システムログ
■ ポリシー管理 く	
□ I-91>ト ·	04/02/2020 16:34:11 - 04/09/2020 1
▲ 配布管理 〈	Export Basic *
■ 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 ◎ ホスト名 ◎ レベル ◎ 区分 ◎ 内容 ◎
■ レポート <	
口 部署管理 〈	
▲ 그-ザ管理 〈	
/ 30克 〈	Showing 1 to 10 of 161 mere 14 - over 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

・部署名(最終部署): 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

及び上の階層もすべて表示

・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10,00 0行単位で自動削除されます。



2.5.4 システムログ

CMS Cloud	≡ Ø Administrato
MAIN NAVIGATION	システム・ログ & Home > システム
必須 ダッシュボード く	☆ 豊成ログ ● 検疫所 ■ 一般ログ ■ システトログ
■ ポリシー管理 <	
□ I-ジェント	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 + ログ内容
■ レポート <	
日、部署管理のないので、	
🛓 그-ザ管理 💦 <	
▶ 設定 く	
	Showing 1 to 10 of 240 rows 10 + rows per page < 1 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)ではログ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。

- ・ログ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、ランサムウエア感染情報メニューで分類されています。

1	2/17	/2016	5 00:	00:00)		1 0	1/17	/201	7 23:	59:5	9		Today
0	0	•:	00	•:	00	v	0	23	•	59	•	59	¥	Yesterday
<	Dec	;	T	2016	•	>	<	Jan	1	T	2017	•	>	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

						_			06/02/2017	17:24:04 - 0	6/02/2017 1	7:44:04	
	12.3	5		_		7	イセンス状況						
riday, Jun 2, AppCheck	17:30 kPro for V	Windows Serv	ライセンス数量	10									
	1	· •											
「「」	7.5	5											
Н Ч	1	5											
	2.5	5											
	(

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

検知状況			
		Ê	03/12/2024 13:26:12 - 03/12/2024
	期間別検知状況		
1 1 1 1 1 1 1 1 1 1 1 1 1 1	•		•
Ή.			
13:30	13:35		13:40
	🔶 ランサムウェア検知 🛛 🔶 エクスプロイトガード情報		

期間別検知状況では、ランサムウエ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。

				144.00	v =	
#7FF2 0	4218	0 4444 0	#7ラットホーム	ユーザき	75-78	*
18.6.2.15	DESET IP-16 SECO	Minister 11	sid. (Alb ar Intel)	a johte	미동율	5
192, 168, 0, 118	DESCTIP-11 ERUCS	Nincous 11	s84 CAMD or TitleE	N.F	904	
16.6.2.15	1 HAM-RD	Sinton Y	494 GAB or Level)	J1588	미물목	57
13, 82, 2, 137	DESITIP-COSTD:	Tindout 10	std (AMD or Treat)	249	이동조	
99, 52, 1, 15	SALOFERINEPE	Nintos 7	sid (Alb or Tittel)	Arreweater	지정복	
102, 138, 1, 85	BUTP-RW70	Mincoup 11	st4 GMD or Tribell	201	지금목	
192, 105, 295, 112	N1791	findour 10	est (AMD or Treat)	ie.)	지동전	
13. 52. 2. 131	L-189-FC	Ninteet 7	sid. (Alb or Letel)	Lynx	164	

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 トールされたデバイス情報です。

エージェントリストカラム(Column)には エージェントID、外部IPアドレス、IPアドレス、MACアドレス、ホスト名、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、現状態、最終オンライン時間、受信日付、感染日付、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		ブラットホーム	設置数
Windows 10		x64 (AMD or Intel)	5
Windows 7		x64 (AMD or Intel)	3
솜탉			8
サーバ運用体制			
運用体制		ブラットホーム	設置数
	No matching records found		
송카			

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 Basic 🔻				Search		C		<u>.</u> .	*
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	÷	Ę	惑 注 日 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、ユーザ名、IPアドレス、ホスト名、部署名(最終部署)、エージェント ID、対象パス、ファイル名、受信日付、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、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

	ł	=						Ĺ
MAIN NAVIGATION		٦.	ザ管理					Home
👧 ダッシュボード	<	-			_			
🔦 ポリシー管理	<		Export Basic 🔹 🔍	ユーザ追加 单 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(局終部署)	יב	ーザ情報
🛓 配布管理	<						G	ğ Edit
📰 ログ管理	<		100000000000000000000000000000000000000	*****			G	ğ Edit
■ レポート	<						G	ä Edit
17 - 当要登理				******			G	ğ Edit
				*******			G	2 Edit
	<						G	2 Edit
▶ 設定	<					******	C	2 Edit
							C	2 Edit
			***********	*******		*****	G	2 Edit
			**********	*****		******	G	2 Edit
		Show	ving 1 to 10 of 27 rows 10	x 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

ユーザ管理 Export Basic ● ユーザ追加 ● ユーザ削除 ▲ ユーザExcelアップロード	
ユーザ清報 × 夢景: JIRANSOFT ・ 名前: E メール:	「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。
###73 取消 jp.cms.checkmal.comの内容 選択したユーザを削除しますか? OK キャンセル	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 ユーザExcelアップロード

ユーザ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: ユーザEXCELダウンロード アップロード:	
Drag & drop files here	
閉	ジる

部署内の多数のユーザを一括登録するためには、「ユーザ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:		
EX-11:		
備考(メモ):		
		//
	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	≡
MAIN NAVIGATION	● 管理者
🚳 ダッシュボード 🛛 🔇	
■ ポリシー管理 🔹 🗸	+ 通加 - 削除 ◆ ログインオブション ◆ ライセンスオブション 検索
□-ゔı>ト	名前 ・
▲ 配布管理 <	意み/書き Jsecurity Jsecurity 区 Edit
いまた こう	意动/書き Jsecurity Jsecurity 区 Edit
■ レポート <	Edit
口 部署管理 人	Showing 1 to 3 of 3 rows
▲ ユーザ管理 <	
▶ 設定 🗸	
管理者	
◎ パフーム設定	

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
管理グループ:	
Jsecurity	*
部署:	
Jsecurity	•
名前:	
EX-JJ:	
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:	
==邏択==	۳
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。

※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ございます。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	
パスワード変更案内メッセージ(日):	
9999	
	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。

パスワード期限は3ヶ月間で固定されています。また、パスワード期限変更機能はありません。

- ・ 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。

・ パスワード変更案内メッセージ(日):パスワードの変更案内メッセージを表示する周期を設定します。

ライセンスオプション	<
エージェントリスト表示期間(日):	
0	
「エージェントの満了期間中、オフライン状態に維持される場合、エージェントのライセンスが自動回収 されます。 (0日:ライセンスを回収しない)	
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。

- ・ エージェントリスト表示期間(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	= 🧧 🗘 Administrator.			
MAIN NAVIGATION	ライセンス & Home > 設定 > ライセンス			
鉛 ダッシュボード く				
■ ポリシー管理 く	+ 追加 37亿次更新			
₽ 1-ÿ1>ŀ <	会社 + Eメール + 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 く	AppCheck Pro 5 2020-10-27 00:00:00			
■ レポート <	AppCheck Pro for Windows Server 1 2020-05-07 00:00:00			
口 部署管理 《	Showing 1 to 3 of 3 rows			
▲ ユーザ管理 <				
▶ 設定 〈				
▲ 管理者				
⇒ ライセンス				
 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。

ライセンス追加		×
EX-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。

administrator アラーム設定 B Home > 設定 > アラーム設定 ダッシュボード ₽アラーム設定 ■ ポリシー管理 Tip! 🕹 配布管理 □ Eメール追加 □ Eメール削除 11 ログ管理 S III-💷 レポート ツール アラーム設定 □ 部署管理 修正 削除 Eメ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。) 💄 ユーザ管理 Showing 1 to 1 of 1 row ▶ 設定 🛔 管理者 ■ ライヤンス ◎ アラーム設定 ◉ 15分 ◎ 1時間 ◎ 1日 ○ 1週間 適用 取消 <mark>管理者</mark>検知お知らせメールです。 🦇 😤 📾 🕬 8 C 4月19日(土) 3:01 ☆ ∽ : :msadmin@mg.checkmal.com 心自分 ▼ AppCheck CMS <mark>管理者</mark>検知お知らせメールです。 JsecurityのCMS 検知履歴の通知メールです。 総3件を検知しました。 スト名 (CMS 後、該当リン 遮断

* 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×- <i>\</i> /
パスワード
✓ IDを記憶する
 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.5 8)」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

	CMS CLOUD		
玛	見在のパスワ ―ド	ライセンスキ ー	仮パスワード
	現在のパス を変更	ワードを利用して、 『することが可能で	パスワード うす。
	E X — M		×
	現在のパスワ	— K	a
	パスワード		a
	パスワード確	-77 77	÷
	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 てパス?	た CMS ライセンスキー フードを変更すること; す。	を利用し が可能で
E×ル		×
ライセンス	(キー	a
パスワード	:	a
パスワード	確認	÷D
ログインペー	- 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 M I I I I I I I I I I I I I I I I I I	

・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。