EX AntiMalware v7 Manager ユーザガイド





Copyright © 2019 Fuva Brain Limited. All Rights Reserved.

—目次—

は	はじめに1				
ア・	イコンの	D説明	.1		
注	意事項	Į	.1		
1.	基本	ニコンセプト	. 2		
	1.1.	動作環境	. 2		
	1.2.	設定と運用手順	. 2		
	1.3.	ポリシー作成の基本的な考え方	. 2		
2.	開始	と終了	.4		
	2.1.	ログインする	. 4		
	2.2.	ログアウトする	. 5		
3.	ステ	ータス画面を表示する	. 6		
4.	管理	君設定をする	. 7		
5.	ライ・	センス状況を確認する	. 9		
6.	環境	1設定をする	10		
7.	ポリ	シー作成をする	11		
-	7.1.	基本設定をする	12		
-	7.2.	スキャンオプションを設定する	13		
-	7.3.	スケジュールを設定する	15		
-	7.4.	実行モードを設定する	16		
-	7.5.	リアルタイム監視を設定する	17		
-	7.6.	アップデートを設定する	18		
-	7.7.	ー時ファイル削除を設定する	20		
-	7.8.	ユーザ制御を設定する	21		
-	7.9.	除外	23		
	7.9.1	. 除外を設定する	23		
	7.9.2	れのランサムウェア除外を設定する	23		
8.	고—	ザ情報を確認する	24		
8	3.1.	検索する	24		
8	3.2.	ユーザ情報を表示する	24		

EX AntiMalware v7 Man	nager ユーザガイド	🐼 Fuva Brain
8.3. 各ユーサ	- ゲ別のユーザ詳細情報を表示する	
8.3.1. ユー	−ザ情報を表示する	
8.3.2. 処理	理ログを表示する	
8.3.3. ロク	ブのみ記録を表示する	
8.3.4. 除夕	ハログを表示する	
8.3.5. ++	マンセルログを表示する	
8.3.6. 復日	日ログを表示する	
9. ログを表示す	-2	
9.1. マルウェ	<u>-</u> アログー覧を表示する	
9.2. 検知され	<i>いたディレクトリ</i> 情報を表示する	
9.3. アクセス	、ログー覧を表示する	
9.4. カテゴリ	別の分析を表示する	
9.5. マルウェ	<u>-</u> ア別の分析を表示する	
9.6. ユーザ別	別の分析を表示する	
9.7. 月別マル	レウェアレポートを表示する	
9.8. 月別検知	ロレポートを表示する	
9.9. 検知推利	多分析	
9.10. マルウェ	-ア侵入状況分析を表示する	
9.11. アップデ	[:] 一トを表示する	
10. クライアント	トプログラムについて	
11. サポートに	こついて	
12. Basic、for	Server、Light ポリシーのデフォルト設定 (確認)	

EX AntiMalware v7 Manager ユーザガイド

はじめに

このマニュアルは、EX AntiMalware v7 Manager の操作手順について記述したマニュアルです。

EX AntiMalware v7 Manager は、企業などの組織において、各クライアント PC にインストールされる EX AntiMalware v7 クライアントプログラムを一元管理することができます。

主な機能は、ステータス、管理者設定、ライセンス、環境設定、ポリシー作成、ユーザ情報、ログなどです。

本書に含まれるすべてのテキスト、図表は株式会社フーバーブレインの独占的所有物であり、顧客の個人的か つ非営利目的での使用に供するものです。

弊社からの文書による承諾なしに、本内容のいかなる部分をも、いかようにも修正、複写、配布、送信、展示、実 演、再生、出版、ライセンス、類似物製作、譲渡、使用もしくは販売することはできません。

本書の情報は、通告なしに変更される場合があり、株式会社フーバーブレインに責任あるいは説明義務が生じることはありません。

また、この文書に記載されるその他の登録済みならびに未登録の商標はすべて各々の商標の所有者の財産です。

アイコンの説明

ここでは、本マニュアル内で使用するアイコンについて説明しています。

アイコン	説明
\bigcirc	禁止事項を示しています。
	注意事項や制限事項を示しています。
	補足説明などを示しています。

注意事項

ここでは、EX AntiMalware v7 クライアントプログラムを動作する上での注意事項を説明しています。



他社製品のアンチウイルスソフトと併用する場合、他社製品のアンチウイルスソフトもしくは EX AntiMalware v7 クライアントプログラムが正常に動作できない可能性があります。併用する場合は、 EX AntiMalware v7 クライアントプログラムを「軽快モード」で動作させる必要があります。 EX AntiMalware v7 Manager ユーザガイド

1. 基本コンセプト

この章は大変重要ですので必ずお読みください。

EX AntiMalware v7 Manager は、誰でも簡単に導入、設定、運用ができるように、直感的に理解できる GUIを採用 しています。

ただし、製品の基本コンセプトである下記の「1.2. 設定と運用手順」と「1.3. ポリシー作成の基本的な考え方」を お読みいただくことで、製品についてより深く理解していただけます。

1.1. 動作環境

Wab ゴーウギョ油	Windows OS:Google Chrome(推奨)、Internet Explorer 11.0 以降 、Microsoft Edge
Web ノノリ 境境	Mac OS : Safari
画面解像度	1024 x 768 以上(1280 x 1024 推奨)

1.2. 設定と運用手順

EX AntiMalware v7 Managerの設定と運用の手順は以下になります。

- ・管理者のログイン(アカウント ID、管理者 ID、パスワードが必要です)
- ・ライセンスの確認
- ・管理者パスワードの変更
- ・管理者の追加(作業レベルに応じて複数の管理者を追加できます)
- ・アラート・メールの環境設定を設定
- ・ポリシーの作成(複数作成できます)
- ・EX AntiMalware v7 クライアントプログラムのインストール情報を各クライアント PC に配信
- ・ユーザ情報の確認、または各クライアント PC 別の設定を変更
- ・ログの監視、分析およびアップデート確認と報告書の作成
- ・ポリシーの見直し
- 1.3. ポリシー作成の基本的な考え方

以下の図を例にポリシー作成の基本的な考え方を説明します。

先ず、会社(アカウント)全体に基本ポリシー(Basic)がデフォルトで用意されています。

また、サーバ OS 用(for Server)と低スペック PC 用(Light)用のポリシーもプリセットされていまが、これらは後から個別に適用させることができます。



サーバ OS 用(for Server)と低スペック PC 用(Light)用のポリシーは 2019 年 2 月以降に出荷され たアカウントからプリセットされております。

デフォルト以外に組織内の従業員(クライアント PC)別に IP アドレス範囲またはワークグループを指定した個別のポリシーを作成できます。ここで参照される IP アドレスは接続 IP(グローバル IP)となります。

🐔 Fuva Brai

EX AntiMalware v7 Manager ユーザガイド

そのため、グローバル IP が異なる拠点かつ、グローバル IP が静的 IP の場合に正常に動作します。

この場合、営業グループと技術グループのクライアント PC がインストールされると個々のポリシーに適用されます。

その他のクライアント PC はインストール時に基本ポリシー(Basic)が適用されます。

次に、IP アドレス範囲またはワークグループを「ポリシー1」と「ポリシー2」以外に指定した「ポリシー3」を作成します。

このポリシーを特定グループや人(クライアント PC)に後から個別に適用させることができます。 ここでは「社員 4」や「社員 6」に後から「ポリシー3」を適用しています。

ン ポリシーが適用される優先順位としては、個別適用(=一括変更) > IP アドレス範囲指定 > ワークグループ指定 > 基本ポリシー(Basic)になります。

一括変更した場合も個別変更と同じで優先順位が一番高い設定になります。



Windows OSとMac OSでは使用可能な項目が異 なりますのでご注意ください。(Win)と表示された項 目は Windows OS のみで有効な機能です。 (Win/Mac)はいずれのOSも使用可能です。





EX AntiMalware v7 Manager ユーザガイド

2. 開始と終了

管理者はインターネットに接続できる環境にて、管理者の PC よりブラウザを利用して EX AntiMalware v7 Manager にログインして操作します。

2.1. ログインする

管理者はブラウザを利用して、EX AntiMalware v7 Manager ヘログインできます。

https://exam7.ahkun.jp/akam7

Endpoint mainure protection agence	도 EX AntiMalware 🦁	Ogen and flenklet sensety policies
	EX AntiMalwareの管理者のみログインできます アカウントロ 常理者ロ ノスワード プ 次回からDの入力を書味 ログイン =ノ(スワードをSれた場合	

EX AntiMalware v7 Manager にログインするには、ご契約時に株式会社フーバーブレインまたは弊社代理店から 提供されている、アカウント ID、管理者 ID、パスワードが必要です。

EX AntiMalwa	ireの管理者のみログインできま
アカウントID	
管理者ID	
パスワード	
Δ	✓次回からIDの入力を省略
1	ログイン

くご注意事項>

アカウント ID、管理者 ID、パスワードは、大文字・小文字などを正しく入力してください。

管理者 ID とパスワードを忘れた場合はログイン画面の[管理者 ID、パスワードを忘れた]ボタンをクリックします。 アカウント ID とメールアドレスを入力後[送信する]ボタンをクリックすることで、指定のメールアドレスに EX AntiMalware v7 パスワードアシスタントからメールが届きます。そのメールに従いパスワードを変更してください。

くご注意事項>

上記のメールアドレスは初期設定時に「管理者設定」タブで設定されたメールアドレスになります。メールアドレス が設定されていない場合や入力時にミスがある場合は「入力された情報から、お客様を確認することができませ んでした。」と表示されます。

① 入力された情報から、お客様を確認するこ	とができませんでした	-	
	•		
	パスワードをお	忘れた場合	
· · · ·	アカウントID	480.00 (MK	
	管理者ID	10000	
	メール	the galaxies of	
		送信する 戻る	

「Ex AntiMalware v7 パスワードアシスタント」メール記載の URL にアクセスしパスワードを再設定してください。

🗅 パスワードリセット ×	+ -	×
← → C ▲ 保護されていないえ	通信 https:// /akam7/passwordReset/pwdreset?art=8NJpR5EyAQ44d_CM 🛧 🦉	:
8 m 8 m 8 m	🖀 Taur Barrison. 🔸 P. B. 👌 Hammarka	
	EX AntiMalware v7 パスワードリセット	
	新しぃパスワード	
	Your Password	
	パスワード強度: 未入力 (0%)	
	もう一度パスワードを入力してください Vour Passward	
	1001 Password	
	送信	
	パスワードに関して	
	パスワードは8文字以上の半角英数字記号を設定してください。	
	バスワート強度か50%以上となるように入力してくたさい。 お客様のお名前 Fマールアドレス 生年日日やその他の個人情報	
	の音歌のの名前、ころうのキャンス、エキカロにての他の個人情報	
	簡単に入手できる情報は使用しないでください。	
1		

2.2. ログアウトする

EX AntiMalware v7 Manager 画面の右上にある[ログアウト]ボタンをクリックすることでログアウトできます。



EX AntiMalware v7 Manager の操作が行われないまま一定時間が経過した場合は、自動的にセッションが切れます。この場合は、再度ログインする必要があります。

3. ステータス画面を表示する

EX AntiMalware v7 Manager にログイン後[ステータス]タブが表示されます。 [ステータス]タブでは下記のアカウント状況を確認することができます。

F				
EX AntiMalware	有効 ライセンスステータス V	9 管理者人数 Number of managers	15 ポリシー数 Number of policies	\mathbf{Q}_0^0
🜉 ステータス 🕠	ライセンスステータス	ログ情報	ユーザ情報	
🤱 WEARS -	クライアント数: 150 和用規則: 5年	44 BUSHAUER : 7306 F10098AUER : 2607	ユーザ数: 114 後期アンインストール設定数:0	
🔒 54822 -	ライゼンスステータス: 有効 サーババージョン: V7.0.1.21	NORMANDER: 362 Thermoniate: 24	アンインストール数: 18 仮想マシン数: 83	
🏘 aase 🕓				
🕚 mus-ma 🕠				
🛃 এ-গরম 🕠				
ب الات 🥏				
当サイトについて				
プライバシーボリシー				
EX.AntMalware V7.0.1.21 © 2018 Ahkun Co., Ltd.				

項目	内容
ライセンスステータス	インストールできるクライアント PC 数、有効期間、ライセンスのステータス(有
	効・無効)、サーバのバージョンを確認できます。クライアントPC数(ユーザ数)
	およびライセンス期間が超過した場合は無効と表示されます。また、導入後ク
	ライアント PC にインストール前の状態でも無効と表示され1台目のインストー
	ルから有効に表示が変わります。
管理者人数	[管理者設定]タブで登録している管理者数を確認できます。
ポリシー数	[ポリシー作成]タブで作成したポリシー数(基本ポリシー(Basic)とプリセットポ
	リシー(for Server、Light)を含む)を確認できます。 ※プリセットポリシー(for
	Server、Light)を含む)は 2019 年 2 月以降の出荷分から表示されます。
ログ情報	年間 / 月間 / 週間 / 当日 別の検知マルウェア(グレーツール)数を確認
	できます。
	※年間は1月1日~12月31日まで、月間は1日~月末まで、週間は月曜か
	ら日曜まで、当日は 0 時から 23 時 59 分までの検知数を集計します。
ユーザ情報	ユーザ数、強制アンインストール設定数、アンインストールユーザ数、ユーザ
	数に含まれる仮想マシン台数を確認できます。現在のライセンス消費数は(ユ
	ーザ数-アンインストール数=ライセンス消費数)となります。

🐔 Fuva Brair

4. 管理者設定をする

[管理者設定]タブでは、EX AntiMalware v7 Manager を管理するための管理者の作成、削除や編集などができます。

複数の管理者の作成や管理者別の権限設定ができます。

デフォルトで設定されている「Admin 管理者」の削除はできません。

Admin 管理者には、管理者の追加 / 編集 / 削除とすべてのタブを確認できる、権限があります。



新しい管理者を追加するには、画面左上にある[新規追加]ボタンをクリックします。

新規作成する管理者の「管理者 ID」、「パスワード」と、この管理者が管理できる「管理者権限」を設定し、管理者 名とメールアドレスを入力して[設定を保存]ボタンをクリックします。

保存後は[一覧に戻る]ボタンをクリックして、新しい管理者の登録内容を確認します。

新規作成項目	内容
管理者 ID	24 文字以内で任意の ID を入力します。
	管理者 ID は他の管理者 ID と重複できません。
	重複されている場合は、「管理者 ID は既に使用されています。」と表示されます。
	管理者 ID は「半角大文字・半角小文字」、「半角数字」、「アンダーバー(_)」、「ハイフ
	ン(-)」のみが有効です。
新しいパスワード	4 文字以上 24 文字以内で任意のパスワードを入力します。
	「パスワード」は「半角大文字・半角小文字」、「半角数字」、「アンダーバー(_)」、「ハ
	イフン(-)」のみが有効です。
パスワード確認	先に入力したパスワードと同じものを入力してください。
管理者権限	管理コンソールで管理者がアクセスできるタブの設定です。
	デフォルトではすべてのタブが無効(X)になっています。
	有効にする場合は各項目(X)をクリックします。
管理者名	任意の管理者名を 50 文字以内で入力します。
	管理者名は、半角英数字、全角日本語、アンダーバー(_)、ハイフン(-)のみが有効
	です。
メール	追加される管理者のメールアドレスを入力します。

管理者作成数の上限はありません。

Copyright © 2019 Fuva Brain Limited. All Rights Reserved.

🐔 Fuva Brair

EX AntiMalware v7 Manager ユーザガイド

このメール設定を行っていないと、パスワードを忘れた場合にログイン画面で[管理 者 ID、パスワードを忘れた]ボタンをクリックしても、管理者 ID およびパスワードの情 報がメール送信されません。

$\overline{\nabla}$	≡ "∎*	v74'y7=17%	→ 109791
EX AntiMalware	522556		
V7	69世代10		
■ ステータス	厳しいびスワード		
. TTARE .	パスワード構成		
A SHEAR	6725424	X 管理書設支(規則) X ライセンス(規則) X 由発設支(規則) X ボリシー作成(規則) X ユーザ清朝(規則) X ログ(規則) X 管理書設支(修正) X ライセンス(修正) X 由発設支(修正) X ボリシー作成(修正) X ユーザ清朝(修正)	
🎄 anze 🚽	9226		
🕚 #US-Mit 🕠	×-16		
🛃 1-9988 🕠			
ہ ارم 🥏	× 複数の管理者の デフォルトで設定	9月で客様電防の機能設定だできます。 たされている「Admin 智速者」の展開はできません。	

各管理者を選択して[編集]ボタンをクリックすることで、管理者情報を編集できます。

ただし、管理者 ID は変更できません。

管理者 ID を変更する場合は一度、この管理者を削除してから新規に管理者を作成してください。

EX AntiMalware v7 Manager ユーザガイド

5. ライセンス状況を確認する

[ライセンス]タブでは、ライセンス状況を確認することができます。

株式会社フーバーブレインがアカウントの発行時にライセンスキーを入力された状態でお客様に提供しますので、 お客様がライセンスキーを入力する必要はありません。

お客様のアカウントには、あらかじめクライアント PC(ユーザ)数、開始日、有効期間の情報が設定されていますので、ライセンス画面上からクライアント PC 数、開始日、有効期間(残り日数)、サーババージョンなどを確認できます。

	$\overline{\mathbf{N}}$	টি র>	ラインマニュアル	
EV		ライセンス		設定を保存
EX A	V7	ライセンス	AAEYK-59CR5-	
	· ·	クライアント数	100 クライアント	
	ステータス)	開始日	2018-06-01	
-	管理者設定	有効期間	7年[残り日数:2119日]	
	ライセンス・	サーババージョン	V7.061	
ų,	環境設定	(推) フーパーブレ	インボタント	
	ポリシー作成 🛛 🕨	(株) シーハージレ ライセンスキーをす ライセンスキーの未	インがおけびにしなってビスペイーをこと時かくことで、 ベイギ角で正しく入力してくだきい。(大文字小文字を選別します。) 設定やライゼンス有効期限が終了している場合はEX AntiMalwareクライアントのインストールはできません。	設定を保存
N	ユーザ情報 →			
,	ログ・			

🐔 Fuva Brain

EX AntiMalware v7 Manager ユーザガイド

6. 環境設定をする

[環境設定]タブでは、検知されたディレクトリ情報の保存期間を設定する「検知されたディレクトリ情報の保存期間」や「メール設定」でメール送信サーバ関連の設定を行うことができます。

環境設定項目	内容
検知されたディレクトリ情報	検知されたマルウェアのディレクトリ情報の保存期間を月単位で設定できま
の保存期間	す。
	EX AntiMalware v7 Manager では、検知されたマルウェアの情報をすべてデー
	タベースに保存していますが、検知ディレクトリ情報については、デフォルトで
	保存期間を「6ヶ月」に設定しています。
メール設定	アラートメールの送信元アドレス、SMTP サーバ、ポート番号、ユーザ名、パス
	ワード、SMTP over SSL、STARTTLS、SMTP 認証、件名や本文を設定できま
	す。件名と本文は255文字以内で入力できます。件名と本文には半角英数
	字、全角日本語、アンダーバー(_)、ハイフン(-)のみが有効です。メール設定
	のチェックボックスにチェックして有効にします。その後、各設定を行った後で
	[設定を保存]ボタンをクリックして保存します。アラートメールは、送信条件が
	合致した場合に [ポリシー作成] タブの各ポリシー設定画面にある[基本設定]タ
	ブにて、アラートメール送信先として登録されたメールアドレスへ送信します。

くご注意事項>

アラートメールの送信設定でお客様の社内メールサーバを使用された場合、EX AntiMalware v7 Manager サー バからの SMTP 通信を社内メールサーバで許可する必要があります。SMTP 通信を許可できない場合はアラー トメールを送信できません。

$\overline{\mathbf{N}}$	រា 🛪	ンラインマニュアル		€□₫₽₫₽
	環境設定			1 設定を保存
EX AntiMalware	検知されたディレ	クトリ情報の保存期間		
VZ	期間	6	5月	
7= 67	メール設定 🗹			
× 77−9A →	送信元アドレス			
💂 管理者設定 ,	ѕмтрサーパ		ポート番号	
A 57222 ,				
	ユーザ名		バスワード	
♀ 県現設正				
🚯 ポリシー作成 🕠	SMTP over SSL	●有効●無効		
↓ ユーザ情報 ・	STARTTLS	◎ 自動 ◎ 無効		
- الات	SMTP認証	◎ 自動 ◎ 無効		
	件名	IFX AntiMalware v7l マルウェア検知報告	7	
当サイトについて				
プライバシーポリシー	本文	指定されたしきい値を超える マルウエアを検知しました。 絵和内安の発揮についてけらど素ご聴動ください		
EX AntiMalware V7.0.6.1		安全を期ずために、マルウェアが検知されているPCのネットワーク ケーブルを外したうえで、詳細スキャンを実行してください。		
Copyright © Fuva Brain Limited. All Rights Reserved.		,	e.	

📢 Fuva Brai

EX AntiMalware v7 Manager ユーザガイド

7. ポリシー作成をする

EX AntiMalware v7 クライアントプログラム用のポリシーを作成、編集、削除することができます。

[ポリシー作成]ボタンをクリックします。

新しいポリシーを作成するには、[新規追加]ボタンをクリックします。 ポリシー設定画面が表示されますので各タブで設定を行います。 設定が完了しましたら[設定を保存]ボタンをクリックして保存します。 保存する前に確認ダイアログが表示されますので[OK]ボタンをクリックします。



作成したポリシーを編集するには、編集するポリシー名を選択して[**編集**]ボタンをクリックします。 ポリシー設定画面の各タブで修正を行い、[**設定を保存**]ボタンをクリックして保存します。 その後、[**一覧に戻る**]ボタンをクリックしてポリシーー覧で確認します。

作成したポリシーを削除するには、削除するポリシー名を選択して[**削除**]ボタンをクリックします。 確認ダイアログが表示されますので削除する場合は[OK]ボタンをクリックします。 デフォルトで自動的に作成されている基本ポリシー「Basic」は、削除することができません。



サーバマシンとメモリ 4GB 未満の低スペックマシンは予め用意されているサーバ OS 用(for Server)と低スペック PC 用(Light)のポリシーを適用することで新規作成の手間 を省けます。



リアルタイム監視設定

✓ リアルタイム監視使用(Win/Mac)
 監視モード ● 軽快(Win) ● 標準(推奨)(Win)
 ✓ 未知のランサムウェア検知使用(Win)

Windows OSとMac OSでは使用可能な項目が異 なりますのでご注意ください。(Win)と表示された項 目は Windows OS のみで有効な機能です。 (Win/Mac)はいずれのOSも使用可能です。

📢 Fuva Brai

EX AntiMalware v7 Manager ユーザガイド

7.1. 基本設定をする

「基本設定」では、ポリシー名称、IPアドレスの範囲またはネットワーク名、アラートメールの送信条件や宛先のメ ールアドレスを登録できます。

登録できるメールアドレス数に上限はありません。

ポリシー名称は半角英数字24文字以内、全角日本語は8文字以内で入力します。

コメントは 100 文字以内で入力します。コメントには、半角英数字、全角日本語、アンダーバー(_)、ハイフン(-) のみが有効です。

ポリシー名称は重複できません。

重複している場合は「このポリシー名は既に使用されています。」と表示され、ポリシーを作成することができません。

同様に、IP アドレス範囲とネットワーク名も重複できません。

重複している場合は「IP 範囲またはネットワーク名は既に使用されています。」と表示されます。

🔨 Basic ポリシーでの IP アドレス範囲とネットワーク名の設定はできません。

アラートメールの送信条件についてはデフォルトで1時間に「10」件以上のマルウェアを検出した場合、登録され たメールアドレスへ送信します。

送信条件についてはお客様の運用ポリシーに合わせて設定を変更してください。

∇		
EV AntiMahwara	ポリシー 編集(Basic)	(一一覧に戻る) 💼 設定を保存)
	基本2011 スキャンオブション スケジュール 実行モード リアルタイム監護 アップデート 一時ファイル剤除 ユーザ制御 除外	(Win) (Windows OS)(Mac) (Mac OS)
*	最本證定(Win/Mac)	
→ ステータス →	ポリシー名称: Basic	
🔔 管理者設定 ,	29-hp:	
🔒 5rtexa 🕠	將7/P:	
袋 福境設定 ,	ネットワーク名: 「浙正信し」 *	
● ポリシー作成 ・	コメント: Basic	
ユーザ情報 →	アラート・メール送信(Win/ Mac)	
	1時間に 10 件以上のマルウェアを検出したら管理者へメールを送信	
	メールアドレス: 💦 追加 🔯 修正 📴 クリア	
当サイトについて	范 死先 (0)	
プライバシーポリシー	金進沢(金進沢府除	
EX AntiMalware V7.1.0.2		🖛 一覧に戻る 👔 設定を保存

くご注意事項>

アラート・メール送信については、「環境設定」でメール設定が有効、かつ各項目が正しく設定されている必要があります。

EX AntiMalware v7 Manager ユーザガイド

7.2. スキャンオプションを設定する

スキャンオプションでは、クライアントプログラムのスキャン時や処理時の設定を詳細に設定できます。 「バックグラウンドスキャンの設定」は、スケジュールスキャン時にクライアント PC のスキャン画面を非表示にで きます。スキャン画面を非表示に設定した場合は、スキャン結果画面をクライアント PC に表示するかどうかも選 択できます。また、ログオフ状態でクライアントプログラムのスキャンを実行させる場合、「バックグラウンドでスケ ジュールスキャンを実行」をオンに設定します。スキャン結果画面もオフに設定する必要があります。

通常のスケジュールスキャン時の自動処理は検出時の処理方法が「ユーザ選択」の場合でも 「隔離」処理を行いますが、「バックグラウンドスキャンの設定」では設定が異なりますのでご注 意ください。

バックグラウンドスケジュールスキャンの場合、「ユーザ選択」は「ログのみ記録」に処理されま す。検知時に「隔離」に処理する場合は、ユーザ制御のスキャンするカテゴリの設定で「隔離」を 設定してください。サーバOSのように常時ログオフ状態で運用する場合は、必ず「バックグラウ ンドでスケジュールスキャンを実行」をオンに設定してください。スキャン結果画面もオフに設定 する必要があります。

基本設定	スキャンオプション	スケジュール	実行モード	
バックグラウンドスキャンの設定				

「セキュリティ設定」は、スキャン時のセキュリティ設定を、「高」、「中」、「低」の中から選択できます。

セキュリティレベル	設定内容
山田	すべてのファイルと現在実行中のプロセスをスキャン
中	実行ファイルとその関連ファイル、および現在実行中のプロセスをスキャン
低	実行ファイルと現在実行中のプロセスをスキャン

「スキャン速度の設定」は、スキャン速度を、「高速」、「標準」、「低速」の3段階で調整できます。

クライアントPCユーザが他のプログラムで作業をしているときや、クライアントPCのシステム仕様が低い場合は、 スキャン時間が長くかかります。

このような場合にはスキャン速度を遅くすることで、他の作業に影響を与えないように調整できます。

「その他」は、スキャンに関する上記以外の設定です。「グレーツールの検知時にチェック状態」、「右クリックスキャン」、「圧縮ファイルスキャン」のそれぞれについて、チェックボックスにチェックを入れることでその機能が有効 になります。複数指定可能です。

スキャン設定	設定内容
グレーツールの検知時にチ	EX AntiMalware v7 クライアントプログラムでスキャンを実施し、グレーツールを

🎸 Fuva Brai

X AntiMalware v7 Manager ユーサ	^デ ガイド 🦉 🖯
ェック状態	検知した際に、検知したグレーツールを選択状態にするかどうかを設定できま
	す。チェックボックスにチェックを入れると選択状態になり、チェックしないと非
	選択状態となります。
右クリックスキャン	クライアント PC にあるファイルやフォルダを EX AntiMalware v7 クライアントプ
	ログラムでスキャンするためのオプションです。このチェックボックスにチェック
	を入れるとクライアント PC で「右クリックスキャン」機能が有効になり、チェック
	しないと機能が動作しません。
圧縮ファイルスキャン	圧縮ファイルに対してスキャンするかどうかを指定できます。圧縮ファイルスキ
※ 1	ャンは、スキャン時間を要するため推奨しません。通常のスキャンによりマル
	ウェア・グレーツールが発見されるなど、再度詳細なスキャンを実施する必要
	がある場合にのみ実施してください。このチェックボックスにチェックを入れる
	と、圧縮ファイルもスキャンの対象とし、チェックしないと対象としません。

※1 7z 形式の圧縮ファイルに関してはスキャン上限サイズ 40MB に設定されています。

「スキャン上限サイズ」は、スキャン対象のファイルサイズに上限を設定することができます。 スキャン対象のファイルサイズは「MB」と「GB」に設定して数字を入力して設定します。 このスキャン上限サイズを設定することでスキャン時間を短縮することができます。

「スタートページの設定」は、ハイジャッカーを検知し処理するとき、設定変更されたブラウザのスタートページ(ブ ラウザの起動時に表示されるホームページ)に対して、URLを指定して復旧させるための設定です。 この処理時に確認画面をクライアント PC に表示する場合は「確認ダイアログを表示」を選択します。 ハイジャッカーを処理後に設定する URL を「スタートページとして使用する URL」に設定します。

∇	
	ポリシー編集(Basic) 📻 認定を保存
V	バックグラウンドスキャンの設定(Wini Mac) ヘルプ
ス テータス ・	 ■ パックグラウンドでスケジュールスキャンを実行(GUI)非表示) ■ 結果病面表示
	セキュリティ設定(Win/Mac)
	◎ 鬲 ● 中 ◎ 低
A 51222 ,	スキャン連度の設定(Win)
	◎ 高速 ● 標準 ◎ 低速
W MARKAGE	その他
🕦 ポリシー作成 🕠	 ダ グレーツールの検知時にチェック状態(Win) 愛 右クリックスキャン(Win) 愛 圧縮ファイルスキャン(Win Mac) □ スキャン上限サイズ: 0 MB ◎ GB(Win Mac)
「 ユーザ情報 ・	スタートページの設定(Win)
ر الات 🥏	● 確認ダイアログを表示 スタートページとして使用するURL:
当サイトについて	

🐔 Fuva Brair

7.3. スケジュールを設定する

スケジュールでは、「フルスキャンスケジュール」と「クイックスキャンスケジュール」を設定できます。 これらのスケジュールは重複して予約できます。

同じ条件で「フルスキャンスケジュール」と「クイックスキャンスケジュール」を設定された場合は「フルスキャンス ケジュール」のみが実行されます。

先ず、「設定しない」、「周期」、「曜日」、「毎月」の中から1つを選択してください。

設定項目	詳細
設定しない	スキャンを予約しません。
周期	何日に1回スキャンをするかを日単位で指定します。
曜日	スキャンをする曜日を指定します。つまり、週に1回のスキャンとなります。
毎月	毎月何日にスキャンをするか指定します。つまり、月に1回のスキャンとなります。
スキャン開始時間	チェックを入れると、スキャンを開始する時間を指定できます。
	※チェックを入れない場合は、PC 起動時にスキャン開始設定となります。
スケジュールスキャン	スケジュールスキャン終了時に自動処理するように設定できます。処理の方法は
時に自動処理	「スキャンオプション」で設定した処理方法になります。処理後に「プログラムの終
	了」または「システムの終了」も選択できます。
	※システム終了を選択すると PC がシャッドダウンされます。
スキャン時に電源 OFF	チェックが入っている場合、スキャンスケジュールの設定で指定されている時間に
の場合、翌日に実行	PCの電源がOFFになっているときには、翌日以降、PCの電源がONになった際に
	スキャンが実行されます。

運用の例としては、クイックスキャンは毎日お昼休みに実施し、フルスキャンは月に1回実施するなどの設定が可能です。

PC 起動時にスキャンをする場合は、周期を「1日」に設定し、スキャン開始時間を設定しなければ、PC 起動時に スキャンを行います。ただし、PC 起動時のスキャンは1日に1回のみ実行されます。

$\overline{\mathbf{N}}$	= I x>=1><->	
EV AntiMalwara	ポリシー編集(Basic)	🖛 一覧に戻る 📑 設定を保存
		(Win) (Windows OS)(Mac) (Mac OS)
Ŵ	フルスキャンススケジュール(Win/Mac)	
ステータス →	 ◎ 設定しない ◎ 周期: 1 ▼ 日 ◎ 曜日: 月曜日▼ ● 毎月: 8 ▼ 日 	
🔵 管理者設定 🕠	▼ スキャン開始時間 : 12▼時 00▼ 分	
	■ スクシュールスキャン制に自動処理 ※検出時の対応方法が「ニーザ運行」の場合は、「構態」処理を行います。 ● 処理後にごつびうたます ● 処理後にころステムを了	
** 15480°F	■ スキャン時に電源OFFの場合、翌日に実行	
	クイックスキャンスケジュール(Win/Mac)	
● ポリシー作成 ・	● 設定しない	
🕎 ユーザ情報 🕠	 ● 周問: 1 ▼ 日 ● 曜日: 月曜日▼ ● 毎月: 1 ▼ 日 ● ズスキャン周始時間: [12 ▼時](00 ▼ 分) 	
ە ە 🥏	■ スケジュールスキャン時に自動処理 ※使出曲の対応方法が「ニーゲ選択」の場合は、「痛酷」処理を行います。 ● 処理様にプレプン長下の 処理後にシステム終了	
当サイトについて	■ スキャン時に電源OFFの場合、翌日に実行	
プライバシーポリシー		🖛 一覧に戻る 🔂 設定を保存

🎻 Fuva Brai

EX AntiMalware v7 Manager ユーザガイド

7.4. 実行モードを設定する

「プログラム実行方式」は、基本実行モード(推奨)と、最小実行モードのいずれかを選択します。

実行形式	詳細		
基本実行モード(推奨)	自動で最新バージョンを維持すると共にリアルタイムでマルウェア・グレーツー		
	ルを検知・処理できます。		
最小実行モード	ユーザがプログラムを手動で実行する場合のみアップデートとスキャンが実行		
	できます。		
	リアルタイム監視	使用しない	
	自動アップデート	使用しない	
	スケジュールスキャン	使用しない	

くご注意事項>

最小実行モードを選択すると、ユーザが手動実行時のみセキュリティ機能が動作します。

通常時はユーザの PC が脅威に晒されるため、特別な理由がある場合のみ、このモードを設定してください。

「官理七一ト」は、設定の権限について、「官理者」、「官理者(GUI 非衣示)」、「ユーサ」の中から選択し;	「管理モー	-ド」は、	設定の権限につい	て、「管理者」、	「管理者(GUI 非表示)」、	「ユーザ」の中から選択しま	ミす。
---	-------	-------	----------	----------	-----------------	---------------	-----

管理モード	詳細
管理者	管理者による設定がクライアントPCに反映されます。クライアントPCユーザに
	よる一時的な設定変更はできますが、EX AntiMalware v7 クライアントプログラ
	ムのアップデート時に管理者による設定に戻ります。60 分間隔のポリシー通
	信で設定が戻ります。
管理者(GUI 非表示)	管理者による設定がすべてのクライアントPCに反映されます。クライアントPC
	に GUI が表示されず、また、Windows のスタートメニューやコントロールパネル
	にもソフトウェア名が表示されません。したがって、クライアント PC ユーザでの
	操作、および設定変更はできません。
ューザ	クライアント PC ユーザによる設定がクライアント PC に反映されます。管理者
	はクライアント PC の設定を変更できません。ユーザが直接クライアントプログ
	ラムで修正した設定が優先されます。

「スケジュールスキャン後、実行するプログラムの指定」は、スキャン終了後、任意のプログラムを実行できます。 テキストボックスに、実行プログラム名を入力し、「追加」ボタンをクリックして追加します。

(例) TargetProgram.exe

登録できるプログラム数に上限はありません。また、登録を削除するには、プログラムリストから該当プログラム をチェックして[**クリア**]ボタンをクリックしてください。

🎸 Fuva Brain

EX AntiMalware v7 Manager ユーザガイド

∇		
EX AntiMalware	ポリシー編集(Basic)	🖛 一覧に戻る 🕞 設定を保存
	- 基本設定 スキャンオプション スケジュール 実行モード リアルタイム監視 アップデート 一時ファイル刷除 ユーザ制御 除外	(Win) (Windows OS)(Mac) (Mac OS)
W	プログラムの実行方式(Win/ Mac)	ロ ヘルプ
77-47	● 基本実行モード (推奨) 😡 最小実行モード	
	管理モード(Win/Mac)	
💂 管理者設定 ,	● 管理者 ◎ 管理者(GUI非表示) ◎ ユーザ	
	スケジュールスキャン後、実行するプログラムの指定(Win/ Mac)	
	プログラム: 🛜 追加 💱 修正 📢 クリア	
🔯 環境設定 🕠	- D プログラム (0)	
(1) (1) (1)	全選択(全選択解除	
U AUS-HEAK		🖛 一覧に戻る 📄 設定を保存
ユーザ情報 →		
ب الات 🔵		

7.5. リアルタイム監視を設定する

リアルタイム監視設定では、リアルタイム監視の有効や無効、リアルタイムでマルウェアが検知されたときの自動処理を指定できます。

監視モード	詳細		
リアルタイム監視使用	クライアント PC のリアルタイム監視を実施します。 クライアント PC ユーザに設		
	定権限な	がある場合は、クラ	ライアント PC ユーザによって監視を OFF にすること
	ができま	す。	
監視モード	リアルタ	イム監視では「軽	快」と「標準(推奨)」の2つの監視モードがあります。
	デフォル	トでは「標準(推奨)」に設定されています。
	軽快	実行されているこ	アプリケーションに対して監視を行います。
		他社製品のアン	チウイルスソフトと併用する場合にご利用ください。
	標準	アプリケーション	が実行される前に検知します。
	(推奨)	セキュリティ強度	が高いため、他社製品のアンチウイルスソフトと併
	用する場合は、他社製品のアンチウイルスソフトもしくは、EX		
		AntiMalware v7 ?	クライアントプログラムが正常動作できない可能性が
		あります。	
未知のランサムウェア検知	未知のランサムウェア(新型身代金ウイルス)が、データを不正に暗号化し		
使用	たり、変更したりする挙動を検知し、ブロックします。		
	また、ラ	ンサムウェアによる	る復元ポイント(シャドーコピー)の削除もブロックしま
	す。		
	※ランサムウェア検知使用は監視モードが標準時のみ選択可能です。		
リムーバブルディスク(USB	クライア	ント PC にリムーパ	「ブルディスクを接続したとき、そのリムーバブルディ
メモリ、DVD メディア)挿入	スクをスキャンします。		
時の処理	スキャン	を行う前に確認	ON にすると自動でスキャン開始はせずに確認ダ
	ダイアロ	グを表示する	イアログが表示されます。OFF にすると自動的に
			スキャンが開始されます。

EX	X AntiMalware v7 Manager ユーザガイド 🍯 Fuva B					
	検知時(こ自動処理	リムーバブルディスクのスキャン後に検知したマル			
			ウェアを自動で処理します。処理方法については			
			「7.8. ユーザ制御」のカテゴリ別処理設定に従い			
			処理が行われます。			
			※「ユーザ制御」での検出時の対応方法が「ユー			
			ザ選択」の場合は、「隔離」処理を行います。			

くご注意事項>

- 1. 「軽快」を設定すると、クライアント PC の監視強度は低くなります。他のドライバとのコンフリクトが発生する可能性がある場合のみ、「軽快」を選択してください。
- 2. ランサムウェア検知使用は監視モードが標準時のみ選択可能です。
- 3. ランサムウェア検知使用は Windows Server 2008 では非対応となります。
- 4. 復元ポイントの保護は OS のシステム保護機能が有効になっていて復元ポイントが作成されている場合のみ 正常に動作します。

$\overline{\mathbf{N}}$		
EX AntiMalware	ポリシー編集(Basic)	🖛 一覧に戻る 🕞 設定を保存
	基本設定 スキャンオブション スケジュール 実行モード リアルタイム監視 アップデート 一時ファイル削除 ユーザ制御 除外	(Win) (Windows OS)(Mac) (Mac OS)
W	リアルタイム監視設定	■ヘルプ
→ ステータス →	 ✓ リアルタイム監視使用(Win/Mac) 監視モード ● 軽快(Win) ● 標準(推奨)(Win) 	
💂 管理者設定 🔸	✓ 未知のランサムウェア検知使用(Win)	
	✓ リムーバブルディスク(USBメモリ、DVDメディア)挿入時の処理(Win)	
 ・ ・ ・	■ スキヤノを打つ時に残酷ジオナロジを表示する(Win) ■ 検知時に目録処理(Win) ※機出時の対応方法が「ユーザ選択」の場合は、「隔離」処理を行います。	
● ポリシー作成 ・		🖛 一覧に戻る 🔤 設定を保存
ユーザ情報 >		
الات 👷		

7.6. アップデートを設定する

EX AntiMalware v7 クライアントプログラムのプログラム、マルウェアデータベース、ポリシーなどをアップデートする方法を設定します。

アップデートの方法は、「自動アップデート」、「手動アップデート」、「スケジュールアップデート」から選択できます。

実行形式	詳細
自動アップデート	30 分に 1 回の頻度で自動的にアップデートします。サーバ側にアップデートす
	る情報がある場合に限りそれらをダウンロードします。
	※ポリシー通信は 60 分に1回となります。
手動アップデート	クライアント PC ユーザが任意に手動でアップデートします。

衸 Fuva Brai

EX AntiMalware v7 Manager ユーザガイド

スケジュールアップデート	アップデートを予約します。	スケジュールアップデートを選択した場合は、「PC		
	PC 起動時 どッノナート 	PC 起動時にノロクラムのアッノナートを実行しま		
		す。		
	周期	何日に1回アップデートをするかを日単位で指定し		
		ます。		
	曜日	アップデートをする曜日を指定します。つまり、週		
		に1回のアップデートとなります。		
	毎月	毎月何日にアップデートをするか指定します。つま		
		り、月に1回のアップデートとなります。		
	アップデート開始時間	チェックを入れると、アップデートを開始する時間を		
		指定できます。		
DB アップデート時にユーザ	アップデート終了時にクライアント PC ユーザに新たに追加されたマルウェア・			
に詳細情報を表示	グレーツールデータベース	などの詳細情報を表示します。		
アップデート/ ポリシー関連	EX AntiMalware v7 クライアントプログラムが1週間以上アップデートをしていな			
アラートを表示	い、または、管理者によっ	てポリシーが変更されているのにも拘わらずクライア		
	ント PC に反映されていな	いユーザに対して警告メッセージを表示します。		
スマートアップデートの使用	スマートアップデートは、日	E意のクライアント PC が更新したマルウェアデータベ		
	ースのファイルを自動的に	ローネットワークに所属する周囲のクライアント PC		
	へ配信する機能です。クラ	イアントPC同士でDBを更新するため、インターネッ		
	ト通信負荷が軽減できます	ト。尚、スマートアップデートの設定が有効であって		
	も、同一ネットワーク内にな	あるいずれのクライアントPCも最新DBを持っていな		
	い場合は、従来通りインタ	ーネットへ接続し、フーバーブレインのダウンロード		
	サーバから DB を更新しま	きす。		

スマートアップデート対応 OS:

Windows 10 / 8.1 / 8 / 7 (32bit/64bit) Windows Server 2016 / 2012 / 2012R2 / 2008R2

Windows Storage Server 2016 / 2012R2

スマートアップデートの特徴および注意事項:

- ◆DB 配信はルータを超えて行われませんのでローカルネットワーク以外のコンピュータへ DB を配信することは ありません。
- ◆社外への持出し等で社内 LAN から外れる場合は従来通りインターネットへ接続し、フーバーブレインのダウン ロードサーバから DB を更新します。
- ◆フーバーブレインのダウンロードサーバの最新 DB を常にチェックしますので、古いファイルや壊れたファイル が配信されることはありません。

📢 Fuva Brai

EX AntiMalware v7 Manager ユーザガイド

- ◆「ポート番号」は、クライアント PC がスマートアップデート通信に使用するポート番号を指定します。デフォルト ポート番号「9340」は特に変更する必要はありません。
- ◆本機能のデフォルト設定は「有効」となります。また、管理モードがユーザの場合もデフォルトは有効になります。
- ◆スマートアップデートの有効/無効をクライアントPCから切り替えることはできません。Managerのポリシーから 設定してください。
- ◆スマートアップデートを有効にすると、Windows ファイアウォールへ、通信許可の設定が自動作成されます。 「Windows ファイアウォール受信規則名: AhkunSmartUpdate TCP/UDP」
- ◆Windows 標準以外のファイアウォール製品を導入していて、スマートアップデートを使用するにはポート 9340 の TCP/UDP 受信を許可してください。



7.7. 一時ファイル削除を設定する

「スキャン実行前の削除設定」は、クライアント PC のスキャンを実施する直前に、以下の一時ファイルについて 削除するかどうかを設定できます。

- ・Windows 一時ファイルの削除
- ・インターネットー時ファイルの削除
- ・Cookie の削除
- ・インターネット/オートコンプリート履歴を削除
- ・最近使用したドキュメントのリストを削除

「処理履歴と隔離項目の削除設定」は、「削除せずにそのまま放置」または、「指定日数後に削除(クリア)する」の いずれかを選択します。

「指定日数後に削除(クリア)する」を選択した場合は、ポリシー適用日当日を基準にして、設定されている日数以前のログと隔離済みファイルが、クライアント PC から削除されます。

🐔 Fuva Brai

ЕX	AntiMa	lware	٧7	Manager	ユーザガイ	۴
----	--------	-------	----	---------	-------	---

$\overline{\nabla}$	オンラインマニュアル	
EV AntiMahwara	ポリシー編集(Basic) ゆ	■ 一覧に戻る 📄 設定を保存
	基本設定 スキャンオブション スケジュール 実行モード リアルタイム監視 アップデート	in) (Windows OS)(Mac) (Mac OS)
W	スキャン実行前の剤除設定(Win)	≧ ヘルプ
💻 ステータス 🔹 🖡	全選択(全選択(新 ■ Mndows=特ファイルの削除 ■ インターネット ー時ファイルの削除	
🔒 管理者設定 ,	■ Cookieの削除 ■ インターネット/オートコンプリート履歴を削除	
A 51222 ,	₩ 最近使用したドキュメントのリストを削除	
	処理履歴と隔離項目の削除設定(Win/ Mac)	
· 環境設定 •	● 削除せずにそのまま放置	
	◎ 指定日数後に削除(クリア)する : 2週間 ▼ 日	
● ポリシー作成 →		🖛 一覧に戻る 🔂 設定を保存
ユーザ情報		
ب ارت 🔍		

7.8. ユーザ制御を設定する

「スキャンするカテゴリの設定」は、スキャンの対象にする以下のマルウェアカテゴリを選択して、それぞれのチェ ックボックスにチェックを入れることでスキャンの対象になります。複数選択可能です。

ユーザによるスキャンの際にだけではなく、スケジュールスキャン、リアルタイム監視の際の共通の 設定になります。バックグラウンドスケジュールスキャンの場合、「ユーザ選択」は「ログのみ記録」 に処理されます。

マルウェア

□ トロイの木馬/ハッキングツール

□ Hosts ファイル改変マルウェア

□ アドウェア

- □ スパイウェア
- ロ ハイジャッカー

□ ウイルス/ワーム

- □ その他
- グレーツール
 - □ ファイル交換ソフト(P2P) □ インスタントメッセンジャー
 - ロ ポップアップ広告 ロ 偽セキュリティソフト
 - □ その他

「カテゴリ別処理設定およびー括設定」は、カテゴリ別に検出時の対応方法を選択できます。また、マルウェアや グレーツール全体に対して一括に設定を変更することもできます。本設定はユーザによるスキャンだけではなく、 スケジュールスキャン、リアルタイム監視の際の共通の設定になります。



例外として「スケジュールスキャン時に自動処理」と「リムーバブルディスク挿入時の自動処理」では 検出時の対応方法が「ユーザ選択」の場合でも「隔離」処理を行います。

🐔 Fuva Braiı

EX AntiMalware v7 Manager ユーザガイド

「ユーザ機能制限」は、以下のクライアントPCの機能を制限することができます。制限する機能についてチェック ボックスにチェックを入れます。複数選択可能です。

- □ スキャン実行中の中止制御 □ 除外ボタンの非表示設定
- □ 処理実行中の中止制御 □ ログのみ記録ボタンの非表示設定
- □ トレイアイコンの終了制御 □ リアルタイム監視の終了制御
- □ 処理ボタンの非表示設定

また、「除外設定」、「オプション」、「アンインストール」、「隔離」それぞれの設定について、「許可」、「パスワード 設定」、「無効化」にいずれかを選択できます。

設定項目	設定内容
許可	選択した場合は、その機能をクライアント PC で制限なしに使用することができま
	す。
パスワード設定	選択した場合はパスワードを入力してください。その機能をクライアント PC で使用
	する際、パスワードの入力を要求されます。
無効化	選択した場合は、その機能がクライアント PC で非表示となって使用できません。



7.9. 除外

7.9.1. 除外を設定する

EX AntiMalware v7 クライアントプログラムにおいて検知対象から除外するための設定ができます。

除外できる項目は、「ファイル名」、「拡張子」、「ディレクトリ」、「マルウェア名」です。除外できる項目の追加数に 上限はありません。

各除外設定項目のテキストボックスに除外したい「ファイル名」、「拡張子」、「ディレクトリ」、「マルウェア名」を入 カして、「追加]ボタンをクリックして登録します。

除外登録されている項目をクリア(解除)するには、クリア(解除)したい項目を選択して、[クリア]ボタンをクリックします。

設定項目	設定内容
ファイルの除外設定	ファイル名を入力します。(例) abc.exe
拡張子の除外設定	拡張子名を入力します。(例) exe
ディレクトリの除外設定	ディレクトリ名を入力します。(例) C:¥Program Files¥abc
マルウェアの除外設定	検知したマルウェア名を入力します。(例) P.P2P.BitTorrent

くご注意事項>

「マルウェアの除外設定」テキストボックスに入力するマルウェア名は、ログに表示されているマルウェア名を入 力してください。

7.9.2. 未知のランサムウェア除外を設定する

未知のランサムウェア検知機能で検知対象から除外するための設定ができます。

検知したランサムウェアが正規の暗号化ソフトウェア等の場合はファイル名を入力します。

(例) TestCrypt.exe

□「Windows の System プロセスを除外する」

上記除外項目は、ファイルサーバや共有設定をしている PC で、ランサムウェア検知情報が「ランサムウェア: System」と表示されていて、確実に過剰検知と判断できた場合に、検知対象から「System プロセス」を除外する 設定になります。

<System プロセス除外時の注意事項>

System プロセスの過剰検知が発生した PC のみを対象に除外設定を行ってください。

実際のランサムウェアに感染した場合は、ローカル PC のファイルが暗号化されると共にファイルサーバや共 有設定をしている他の PC のファイルも暗号化の対象になります。

その場合は、「System プロセス」として共有フォルダのファイル暗号化を実施しますので、すべての PC を対象 に除外設定を行うと、実際のランサムウェアが共有フォルダのファイルを暗号化したときに止められなくなる可 能性もあります。

📢 Fuva Brai

EX AntiMalware v7 Manager ユーザガイド

$\overline{\nabla}$,					2 00701
EV AntiMalwara	ポリシー編集(Basic)						🖛 一覧に戻る 🛛 💼 設定を保存
	基本設定 スキャンオプション	スケジュール 実行モード	リアルタイム監視	アップデート	一時ファイル削除	ユーザ制御	(Win) (Windows OS)(Mac) (Mac OS)
<u>v</u>	踪外(Win/Mac)						
ステータス ・	📴 ファイル名 🔚 拡張子 📔	- ディレクトリ 📔 マルウェア名	5				
🔒 管理者設定 🕠	 □ ファイル名 (0) □ 拡張子 (0) □ ボ張子 (0) 						
A 51822 >	- ロマルウェア名(0)						
	全選択十全選択解除	📴 クリア					
· 梁· 编辑定 · ·	未知のランサムウェア除外(Win)						
(の) ポリシー作成)							
<u> </u>	除外するファイル名:				🛛 📷 追加 🛛 📴 🌣	קט	
□ ユーザ情報 →	二〇 ファイル名(0)						
ب الا 🥥	全選択 全選択解除						
当サイトについて	□ WindowsのSystemプロセスを除外!	する(Win)					
プライバシーポリシー							
EX AntiMalware V7.1.0.2							
Copyright @ Fuya Brain							🖛 一覧に戻る 🕞 設定を保存

8. ユーザ情報を確認する

ユーザ情報では、EX AntiMalware v7 クライアントプログラムをインストールしているユーザの情報を項目別で細かく確認できます。

その上、個別の「ポリシー適用」、「強制アンインストール」や「再インストール不可」の設定ができます。

- 8.1. 検索する
- ・デフォルトでは「最終接続日時」の範囲内でポリシー「全体」とマシン種類「全体」から検索された「ワークグルー プ名」、「コンピュータ名」、「ユーザ名」、「インストール状況」、「再インストール不可」、「強制アンインストール」 と「ポリシー適用」項目が表示されています。検索の条件を変更して再検索することもできます。プルダウンメニ ューから絞り込む項目を選択、または入力項目にキーワードを入力して、「検索」ボタンをクリックします。入力 キーワードを「部分一致」、「等しい」、「等しくない」などの条件設定で絞り込みが可能です。
- ・上部の検索に合わせて「表示する項目を選択」で表示したい項目を追加することやその設定を保存することも できます。保存する場合は[表示方法を保存]ボタンをクリックして保存します。表示した項目を CSV 形式でエク スポートする場合は[CSV]ボタンをクリックして任意の場所に保存します。
- 8.2. ユーザ情報を表示する

「ユーザ情報」では上記の検索条件や表示設定で設定されたユーザ情報が一覧表示されます。

項目	内容
一括変更	検索画面から検索した全クライアント PC に対して、同一のポリシーを一括して適
	用することができます。ポリシーを適用するには、対象を検索機能から検索し、表
	示された該当ユーザに対してプルダウンメニューから適用したいポリシー名を選
	択して[一括変更]ボタンをクリックします。
インストール状況	EX AntiMalware v7 クライアントプログラムのインストール状態を確認できます。イ
	ンストール状況からクライアントプログラムの状況を把握して、正確なユーザ管理

各ユーザ情報から下記の設定や確認ができます。

🐔 Fuva Brain

X AntiMalware v7 Manager ユ	ーザガイド 🦉 🖪									
	ができます。正常にインストールされている場合は「黄色」で表示されます。									
再インストール不可	クライアント PC ユーザが EX AntiMalware v7 クライアントプログラムをアンインスト									
	ール後、または管理者により強制アンインストール後に同じマシンで再度インスト									
	ールできないようにするための設定です。設定する場合はチェックボックスを選択									
	して[保存]ボタンをクリックします。									
強制アンインストール	EX AntiMalware v7 クライアントプログラムを強制的にアンインストールするための									
	没定です。強制アンインストールが設定された場合、クライアントプログラムがアッ									
	プデート実行時に自動的にアンインストールされます。必要に応じて「再インスト									
	ール不可」と共に設定します。									
ポリシー適用	ポリシー作成」で作成されたポリシーをクライアント PC 個別に適用するためのも									
	のです。該当ユーザの「ポリシー適用」プルダウンメニューから適用したいポリシ									
	ー名を選択して[保存]ボタンをクリックします。									
ユーザ情報の削除(アン	PCの故障や破棄等で EX AntiMalware v7 クライアントプログラムをアンインストー									
インストール)	ルできない場合は、ユーザを指定して削除することでアンインストール同様、未使									
	用のクライアントライセンスを1つ増やすことができます。まだ使用中のユーザを									
	誤って削除した場合は再インストールが必要ですのでご注意ください。									
	ユーザ情報									
	📃 詳細 📱 📊 保存 📲 💼 削除									
	コンピュータ名 ユーザ名 最終接続日時 最									
	WIN_ 2017-10-06									
	Administrator 14:15:20									
アンインストールユーザ										
の確認方法	1 $ -$									
最終スキャン日時	クライアントPC個別の最後にスキャンした日時を表示します。									

🌮 Fuva Braiı

R/	-	≡ ¹⁰ *>	54>V:												1	0779
44																
EX AntiMalware			1755	-86			210	7554	818	24.1						
V	12	ークグループ名	1. Aliantes	+ #10	n •			-								
			4010047	m + 📖	20	1051	8 + 10 0 11	~ E		- 26	16/13/19	25	- 19 53.11		Q HE	at CSV
37-97 1		FTGREEN														
1 10002 ·	1	0-99%-0	7名	S 3283	-98		■ ユーザ名 ■ MMC 700-7	8 8K	e i inter			# 100	Barrel	3	総統連続日時	
		1-1521-14	6K .	# #-153	()——从常时		● 個利アンインストール	a mus	通用			ぼ ボリラ	一道用日间		ユーザポリシー連邦は	518
a artear a	1	V//92708	Ver.	第 アンテリ	0.0272555 2.5-1.499	Ver	■ グレージールDB Ver	# 75/	ドクレージ	-1435	SVM.	-	1.78	9	創造ウイックスキャン	-9218
ir anne .		◎ 単位クイックスキャンボア ◎ 単純詳細スキャ					a multiplication (277			120417-2411	Garvarae		
	3-	3-746												fier	• • 6	R28-6
Manager and the second		210 1 1 1 H	1. 249													
2 1-9'se		3-951-71	コンピュータ石	-1>21-10	anastos -	×6008	5.3.94.00	OB Ver	00-022	45X7-/ #R	▲イシス ドール不可	後期プラークストー	ポリシー		ポリシー 適用日用	1-1/F 適用
		WORKDROUP		2018-02-28 18:04:24	2018-03-18 18:38-45	0072	Microsoft Hindows 10 Pro (Build 1/1/20: (Million	10.0	7068		U.	-81	Section		2017-11-0217-55.39	2010-02-18
07 .	,	workshour	-	2017-10-18 16:38:49	2018-05-18 18:30:14	8154	Microsoft Itlindows 7 Ultimate Bervice Pack toBuild 76010 (5464)	61	70.00		u	-10	Sec.		2017-11-02 17 95 39	2010-02-18
治サイトについて	3	workskour	-	2017-12-18	2012-03-18	8152	Microsoft mindows betwee 2013 (dward \$200) (54540	6.2	7.000		U.	-10	10 April 12 14	٠	2010-02-09 17:49:24	2010-03-18
7947(5-#05-		WORKDROUP	1000	2017-12-18	2010-00-15	4029	Morealt Hindows 18 (Bull) 16290: Addet	10.0	70.03	•	-0	10	East.	•	2017-11-02 17 15 39	3010-00-10
© 2018 Altikun Co., Ltd.	5	WORKSROUP	-	2017-05-08	2018-03-18	805)	Microsoft Illinitavis 12 (Build 16206) (Materi	19.8	7.000		11	8	(far,bate	+	2018-03-05 0138-07	2010-02-05
		volkskouP		2017-01-54	2018-02-18	8672	Microsoft Introducts 12 Pro. (Suite 142308-142441	12.0	7620	•		10	Baix	+	2017-01-02 17:55.30	2010-03-15
	1	winkanour		2017-11-10	2013-05-18 17-25-48	3673	Microsoft Introduces 10 (Build 10/2010) (Matur	10.0	7.408		.0		Berri.		2017/11/42 17:58 39	2010-02-10
				30x1-bx20	2010-0210		Manhauft minutes a figured 2012					-				

8.3. 各ユーザ別のユーザ詳細情報を表示する

「詳細」は、各ユーザの詳細情報を確認する機能です。

該当ユーザを選択して[詳細]ボタンをクリックするか、または該当ユーザ情報をダブルクリックします。

別画面が表示され、各タブにて選択したユーザの詳細情報として、「ユーザ情報」、「処理ログ」、「ログのみ記録」、「除外ログ」、「キャンセルログ」、「復旧ログ」などを確認することができます。

各ログの表示件数の上限は 5000 件です。それを超える件数がある場合はユーザ詳細情報からは確認できません。

ユーザ詳細情報を閉じる場合は、画面右上の[Close]ボタンをクリックします。

8.3.1. ユーザ情報を表示する

選択したユーザの「インストール」、「アップデート」、「ポリシー適用」などの情報を確認できます。

設定項目	設定内容
インストール	「接続 IP」、「インストール日」、「最終接続日時」、「システム(OS)」、「OS バージ
	ョン」などが表示されます。
アップデート	プログラムバージョン」、「マルウェア DB バージョン」、「アンチマルウェアエンジ
	ンバージョン」、「グレーツール DB バージョン」、「アンチグレーツールエンジン
	バージョン」などが表示されます。
ポリシー適用	「ポリシー適用日時」、「ユーザポリシー適用日時」、「ポリシー名」などが表示さ
	れます。
備考欄	任意の情報をテキスト文で 255 文字まで記入して保存することができます。保
	存する場合は[設定を保存]ボタンをクリックします。備考欄には、半角英数字、
	全角日本語、アンダーバー(_)、ハイフン(-)のみが有効です。

🎸 Fuva Brain

EX AntiMalware v7 Manager ユーザガイド

ューザ	计编辑程								Clos
	ユーザ情報	処理ログ	0/07/28	単外ログ	キャンセルログ	御田ログ 。			
1>7	ar-14	ESKTOP)							1
	酸粧P	インス	h-#8	最终地线日	19	システム(05)		05パージョン	
19	192.168.253.116 2017-11-10 13:03:45			2018-03-15 18	341:11 M	crosoft Windows 10 (Build 162)	99) (64bit)	10.0	
アッフ	グデート(-0	ESKTOP)							
70	グラムバージョン	グレーツール	00/(-9a>	アンチグレーツー	ルエンジンバージョン	マルウェアロリバーション	アンチマルウェン	アエンジンバージョン	
	7.0.0.0 30439.20170501			1	7.0.0.0	11449964.20180315	7.7	\$308.0.0	
ポリシ	>)創川(ESKTOP)							
	30	リシー波用日時			ユーザポリシ			ポリシー名	
	2018	8-03-15 11:38:1	7		2018-03-15	18:41:11		an_basic	
盖 肉根	DESKT	OP)							
					03582				
				8					
									×

8.3.2. 処理ログを表示する

選択したユーザについて、マルウェアが処理されたログー覧を確認できます。

「カテゴリ」、「マルウェア名」、「処理日」、「処理方法」、「検知されたディレクトリ」などが表示されます。

1-5	步詳細情報									Close
	ユーザ情報	の取口グ	ログのみ記録	除外ログ	キャンセル	100	衛田ログ			
	カテゴリ		マルウェア名		処理日	処理方法				検知されたディレクトリ
1	ファイル交換ソフトの	P2P)	P.P2P.BitSpirit	2015	03-15 11:40:01	然理	h1bev3.6.0	500 m	nu e	ree
2	ファイル交換ソフトの	P2P)	P.P2PiMesh	2018	-03-15 11.40.01	処理	れマルウコ	7株4	\$1/A	NeshVG ave
3	ファイル交通ソフトの	P2P)	P P2P BitSpirit	2018	-03-15 11.40.01	処理	81マルウェ	798	T-br	sv3.6.6.500 mu.exe
4	ファイル交換ソフトの	P2P)	PP2P3Mesh	2018	03-15 11 40:01	52	h WeshVS	exe		
.5	インスタントメッセン	57-	E MSG MirandalM	2018	03-15 11 40:01	始度	れつしつる	:79ki	\$ in	iranda-im-v0.9.10-unicode.exe
8	インスタントメッセン	57-	E MSG MrandalM	2015	-03-15 11 40.01	15/2	h Imwanda	-im-v0	9.1	0-unicode exe
7	マルウェア		EICAR-Test-File (not a vi	rus) 2015-	03-14 16:17:53	始建	c/Users/bl	w/De	iskt	op/eicar/eicar.com
.8	トロイの木馬		K.KLG natsume	2018	03-14 16:17:37	然間	c/Usersibl	nan/De	isid	opiグレージール検球Iウイルス検球 eathume exe
.9	マルフェア		EICAR-Test-File (not a vi	rus) 2018-	03-14 16:17:37	然理	c:\Users\bl	an/De	rskå	opiグレーツール検オiウイルス検体Teicar.com
10	ファイル交換ソフトの	P2P)	P P2P BitSpirit	2018-	03-14 16:17:29	始度	c'Usersibl	an/De	eskt	op/グレーツール様体iマルウェア操体ibev3.6.0.500 mu.e:
11	ファイル交換シフトの	P2P)	P/P2P/Mesh	2015	03-14 16:17:29	- 1012	c:Usersibi	an/De	skt	op/グレーツール検洋Iマルウェア検洋WeshV9.exe
12	インスタントメッセン	51+-	E MSG MirandalM	2018	03-14 16:17:29	始理	c/Users/bl	an/De	1983	opiグレーツール検体Iマルウェア映印imiranda-im-v0.9.11
13	ファイルスカソフトの	P2P)	P P2P BitToment	2018	03-14 16:17:24	然理	c:/Users/bl	an/De	tska	opiグレージール検体Iマルウェア操体bittorrent-6.4.exa
-14	ファイル交換ソフトの	P2P)	P.P2P.BitToment	2018	03-14 16:00 22	始建	c.'Usersibl	an/De	iskt	op/グレーツール検洋\マルウェア様体bittorrent-6.4 exe
15	ファイル交換ソフトの	P2P)	P.P2P.BitToment	2018-	03-14 16:00:22	然理	c:\Users\bi	an/De	iskā	opiグレージール検球マルウェア検洋お用orrent-6.4 exe
16	ファイル交換ソフトの	P2P)	P.P2P.BitSpirt	2018	03-14 16:00.17	処理	c'Usersibl	anDe	iskt	opiグレーツール検体iマルウェア検体ibev3.6.0.500 mu e
17	ファイル交換ソフトの	P2P)	PP2PMesh	2018-	03-14 16:00 14	始理	c'Users/bl	an/De	eskt	op/グレーツール様体Iマルウェア様体iMeshV9.exe
15	インスタントメッセン	57-	E MSG MirandalM	2018	03-14 16:00 11	均理	c:Usersibl	an/De	iskt	opiグレージール検体Iマルウェア株体Inivanda-Ini-v0.9.1t
10	インスタントメッセン	57-	E MSG MirandalM	2018	03-14 16:00 01	処理	c/Users/bi	hamDe	1983	opiグレーツール検尔マルウェア除市mranda.im-v0.9.11
20	トロイの木馬		K KLG natsume	2018	03-14 16:00 02	均理	c.'Users/bl	an/De	ska	opiグレージール検体Iのイルス検体Matsume.exe
21	マルウェア		EICAR-Test-File (not a vi	rus) 2015-	03-14 15:37.47	始建	c:Usersibl	an/De	eski	op/グレーツール検知ウイルス検体ieicar com
:22	トロイの大阪		K KI G natione	2015	03-14 15:37-44	100	c/Elsenibi	un/De	144	************************************

EX AntiMalware v7 Manager ユーザガイド

8.3.3. ログのみ記録を表示する

選択したユーザについて、検知されたマルウェアのログのみを記録する処理がされたログー覧を確認できます。 「カテゴリ」、「マルウェア名」、「処理日」、「処理方法」、「検知されたディレクトリ」などが表示されます。 未知のランサムウェア検知使用で検知したログはすべて「ログのみ記録」として表示されます。

-L	ザ詳細情報									Clo
	ユーザ情報 処理	85400D 00	10:	MD7	キャ ン	セルログ	間日ログ			
	カデゴリ	マルウェア名		处理的	1	処理方法			検知されたディレクトリ	
1	マルウェア	EICAR-Test-File (not a v	(rus) 2	018-03-14 1	4:30:10	ログのみ記録	c.'Usersibha	in/Desk	topleicar/eicar.com	
2	マルウェア	EICAR-Test-File (not a v	nus) 2	015-03-14 1	4.38.18	ログのみ記録	c.'Users/bha	n/Desk	top/グレージール検体ウイルス検体elci	ar.com
3	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2	018-03-14 1	4 38 18	ログのみ記録	h bittorrent-	6.4.exe		
4	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2	018-03-14 1	4.38.18	ログのみ記録	c:IUsersibha 6.4 exe	n/Desk	top)グレーツール映体Iマルウェア映体は	ttorrent-
5	ファイル交換ソフト(P2P)	P.P2P.BitSpirit	2	018-03-14 1	4.38.18	ログのみ記録	h1bev3.6.0.5	500 mu	exe	
6	ファイル交換ソフト(P2P)	P P2P BitSpirit	2	018-03-14 1	4 30 10	0708R#	c:IUsersibha Ibsv3.6.0.50	n/Desk 0 mu e	top/グレージール検体(マルウェア狭体 et	
7	インスタントメッセンジャー	E MSG MirandalM	2	018-03-14 1	4 38 18	ログのみ記録	h Imiranda-a	m-v0.9	10-unicode exe	
.6	インスタントメッセンジャー	E MSG MirandalM	2	010-03-14 1	4.38.18	ログの外記録	c:/Users/bh/ v0.9.10-unic	n/Desk ode en	top/グレーツール映体Iマルウェア映体ie s	siranda-im-
9	ファイル交換ソフト(P2P)	PP2PiMesh	2	018-03-14 1	4 38 18	ログのみ記録	h:\MeshV9	exe		
10	ファイル交換ソフト(P2P)	P.P2P:Mesh	2	018-03-14 1	4 38 18	ログのみ記録	c:/Users/bha	n/Desk	top/グレージール検索Iマルウェア検体は	AeshV9.exe
11	トロイの木馬	K KLO natsume	2	018-03-14 1	4 38 18	ログのみ記録	h inatsume r	exe		
12	トロイの木馬	K.RLG.natsume	2	018-03-14 1	4:38:18	ログのみ記録	c/Users/bha	in/Desk	top)グレージール映体(ウイルス映体)vab	sume.exe
13	マルウェア	EICAR-Test-File (not a v	Rus) 2	015-03-14 1	4.38.18	ログのみ記録	It leicar com			
14	トロイの木馬	K KLG natsume	2	018-03-14	11.58.11	ログのみ記録	10112	Ritina .	burne exe	
.15	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2	018-03-14	1.58.11	ログのみ記録	11マルウエン	7株住1	ottoment-6.4 exe	
16	ファイル交換ソフト(P2P)	P.P2P.BitSpirt	2	018-03-14	11.58:11	ログのみ記録	れマルウエン	78km	osv3.6.0.500.mu.exe	
17	ファイル反換ソフト(P2P)	P.P2P.Mesh	2	018-03-14	11 58 11	ログのみ記録	hiマルウエ)	7時(1)	Mesh/V9.exe	
18	インスタントメッセンジャー	E MSG MirandalM	2	018-03-14	1 58 11	ログのみ記録	れてんりエン	7株中	miranda-im-v0 9.10-unicode exe	
19	マルウェア	EICAR-Test-File (not a v	(rus) 2	018-03-14	1.58:11	ログのみ記録	れつくんえき	奥尔 eic	ar com	
20	ランサムウェア	RANSOMWARE	2	018-03-07 1	8.04.55	ログのみ記録	c:users/bha	ndeskt	op/グレージール検体	

8.3.4. 除外ログを表示する

選択したユーザについて、検知されたマルウェアの除外処理がされたログー覧を確認できます。 「カテゴリ」、「マルウェア名」、「処理日」、「処理方法」、「検知されたディレクトリ」などが表示されます。

1-	步祥被情報									Close
	ユーザ情報 処理の	ログ ログのみ足録	緑外ログ	+72	セルログ	期日ログ				
	カテゴリ	マルウェア名	処理	8	処理方法				検知されたディレクトリ	÷.
1	ファイル交換ソフト(P2P)	P.P2P BitTorrent	2018-03-14	14 43 52	1875	c Usersibhania	Deskt	lop/2	プレーツール検中マルウェア様体bittoment-6.4 exe	
2	ファイル交換ソフト(P2P)	P P2P BitSpirit	2018-03-14	14:43:52	3875	c. Wsersibhania Vbsv3.6.0.500.m	Deski nu ex	lop\3	プレージール検体マルウェア映体	
3	ファイル交換ソフト(P2P)	PP2P.Mesh	2018-03-14	14:43:52	1855	c1Users/bhania	Deski	lop!?	ブレージール検体Iマルウェア検体iMeshV9 exe	
4	インスタントメッセンジャー	E.MSG.MirandalM	2018-03-14	14.43.52	1875	c (Usersibhan)2 v0.0.10-unicode	Deskt e.exe	top/C	パレーツール検体マルウェア映印miranda-im-	
5	トロイの木馬	K.KLG.natsume	2018-03-14	14:43:52	1895	c'lUsers/bhar/0	Deskt	lop1/2	プレーツール検知ウイルス検伸inatourne exe	
8	マルウェア	EICAR-Test-File (not a virus)	2018-03-14	14:43:52	28:53	c:\Usersibharid	Deskt	lopi?	パレージール検知ウイルス陳律eicar.com	
7	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2018-03-13	12:00:49	18/5	c1Usersibhan0	Deskt	lop/3	プレージール検洋マルウェア狭体はBorrent-5.4 exe	
8	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2018-03-13	11.57:13	78/95	c Usersibhania	Deski	top/2	パレーツール検知マルウェア映体bittoment-6.4 exe	
9	インスタントメッセンジャー	E.MSQ MirandalM	2018-02-09	12 18 28	3875	c Wersibhand v0.9.10-unicode	Desks e exe	lapi/	プレーツール検体マルウェア映体micanda-in-	
10	インスタントメッセンジャー	E MSG MirandalM	2017-11-15	16:36:28	19:25	C:Usersibhani	Desk	topie	niranda-im-v0.9.19-unicode exe	
11	インスタントメッセンジャー	EMSG Trillan	2017-11-15	16 36 28	1875	C.Usersibhania	Desk	topit	rillian-v5.1.0.20 exe	
12	インスタントメッセンジャー	E MSG MirandalM	2017-11-15	16.33.28	7875	c'Usersibhan/2	Deski	lop/n	niranda-im-v0.9.19-unicode.exe	
13	インスタントメッセンジャー	E MSG MirandalM	2017-11-15	16 33 25	28:91	c Usersibharia	Deskt	lopin	niranda-im-v0.9.19-unicode.exe	
14	インスタントメッセンジャー	E.MSG Trillan	2017-11-15	19:30:36	19:05	c:\Users\bharid	Deski	top/#	Illan-v4.2.0.23.exe	
15	インスタントメッセンジャー	E.MSG Trillan	2017-11-15	16:30:35	18/5	c Usersibhania	Deskt	top/b	illian-v4.2.0.23.exe	
16	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2017-11-15	16.23.50	1875	c Usersibharid	Deski	lopib	ittorrent-6.4.exe	
17	ファイル交換ソフト(P2P)	P.P2P.BitToment	2017-11-15	16:23:50	2853	c Usersibharid	Deskt	lop/b	ittoment-6.4.exe	
15	ファイル交換ソフト(P2P)	P.P2P.BitTonent	2017-11-14	15.27.18	1855	c:\Usersibhan\0	Deskt	lople	icaribittorrent-6.4.exe	
19	マルウェア	EICAR-Test-File (not a virus)	2017-11-14	12:27:56	1895	c Usersibhand	Deskt	top/e	icaneicar.com	
20	マルウェア	EICAR-Test-File (not a virus)	2017-11-14	12:23:12	3835	c:Usersibharid	Deskt	iop/e	icarleicar.com	

8.3.5. キャンセルログを表示する

選択したユーザについて、マルウェアを検知後、処理をせずにプログラムを終了したログー覧を確認できます。 「カテゴリ」、「マルウェア名」、「処理日」、「処理方法」、「検知されたディレクトリ」などが表示されます。

1-1	f詳暗情報					Close
	ユーザ情報 身	6 W CD /2	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	8%D7 #	ヤンセルログ	0x田ログ 。
	カデゴリ		マルウェア名	処理日	処理方法	検知されたディレクトリ
3	インスタントメッセン	977-	E MSG MirandalM	2018-03-14 16:0	H 20 キャンセル	c:Usen/hannote/Desktop/デストジールマルウェア後本マルウェア様本mixand unicode exe
2	トロイの木馬		K KLG natsume	2015-03-14 16:0	4.20 キャンセル	c:Users'hannote/Desktop/デストジールのイルス様体ウイルス様体natsume er
3	ファイル交換ソフトの	P2P)	P P2P.BitTorrent	2018-03-14 16:0	4:20 キャンセル	c:Users/hannote/Desktop/テストツールマルウェア様本マルウェア様体attore
4	ファイル交換ソフトの	P2P)	P.P2P.BitSpirit	2018-03-14 16.0	4:20 キャンセル	c:Users/hannote/Desktop/テストツールマルウェア検ボマルウェア検体bav3.6
5	ファイル交換ソフトの	P2P)	PP2P/Mesh	2018-03-14 16:0	4:20 キャンセル	c'Users'hannote'Desktopiテストツールマルウェア検索マルウェア検体iMeshi
6	マルウェア	1	EICAR-Test-File (not a virus)	2018-03-14 16:0	4:20 キャンセル	c:Users/hannole/Desktop/デストツール/ウイルス検印/ウイルス検印eicar.com
7	ファイルスネソフトは	P2P)	P P2P it tesh	2018-03-14 15:4	ゆ43 キャンセル	CiUsersiAannote/Desktopテストソールマルウェア技体マルウェア技体Mesh
8	ファイル交換ソフトの	P2P)	P.P2P.BitToment	2018-03-14 15:3	8.48 キャンセル	c:UsersithannoteiDesktop/テストジールマルウェア検体マルウェア検体BitTom
9	ファイル交換ソフトの	P2P)	P.P2P.BitSpirit	2018-03-14 15:3	8.46 キャンセル	c:Users/hannole/Desktop/テストシール/マルウェア映体/マルウェア映体bav3.6
10	ファイル交換ソフトの	P2P)	P.P2P.BitTonent	2018-03-14 15:3	はお キャンセル	c'Users/hannote/Desktop/テストジールマルウェア検洋bittone
11	ファイルスタンフトド	P2P)	P.P2P.Mesh	2018-03-14 15:3	あお キャンセル	c:Usersihannote/Desktopiテストツールマルウェア映本マルウェア映体iMeshi
12	ファイル交換ソフトの	P2P)	P.P2P.BitSpirit	2018-03-14 15:3	は43 キャンセル	c'Users/hannote/Desktop/テストツールマルウェア検体マルウェア検体bav3.6
13	ファイル交換ソフトの	P2P)	P P2P Mesh	2018-03-14 15 3	18:41 キャンセル	c ⁻ Users'hannote'DesktopiテストツールIマルウェア映中マルウェア映体Mesh
14	ファイル交換ソフトの	P2P)	P.P2PiMesh	2018-03-14 15:3	は41 キャンセル	c'Users/hannote/Desktop/テストジール/マルウェア狭体/マルウェア狭体/Mesh/
.15	ファイル交換ソフトが	P2P)	P.P2PiMesh	2018-03-14 15:3	8.41 キャンセル	c:Users'hannobe/Desktopiテストジールマルウェア映体マルウェア映体iMeshi
16	マルウェア	1	EICAR-Test-File (not a virus)	2018-03-14 15:3	838 キャンセル	c:/Users/hannote/Desktop/デストジール/ウイルス検知/ウイルス検知eicar.com
17	ファイル交換ソフトの	P2P)	P P2P Mesh	2018-03-14 15:3	8-12 キャンセル	c:/Users/hannole/Desktop/デストツールマルウェア様体マルウェア様体iMesh/
15	マルウェア	1	EICAR-Test-File (not a visus)	2018-03-14 15:3	14:01 キャンセル	c:/Usersihannole/Desktop/デストツール/ウイルス標準/ウイルス標準/eicar.com
10	ファイル交換ソフトが	P2P)	P.P2P.Mesh	2010-03-14 15:1	11.51 中中ン也化	c:/Usersi/hannote/Desktopiテストツール/マルウェア映体マルウェア映体Meshi
-20	ファイル交換ソフトの	P2P)	P.P2P.BitTorrent	2018-03-14 15 1	11.51 キャンセル	c:UsersihannoterDesktopiテストツールマルウェア検体マルウェア検体altions
21	ファイル交換ソフトの	P2P)	P.P2P.BitSpirit	2018-03-14 15 1	1151 キャンセル	c'Users'hannote'Desktop'テストツールマルウェア様中マルウェア様体bav3.6 +

8.3.6. 復旧ログを表示する

選択したユーザについて、処理済みのマルウェアを復旧したログー覧を確認できます。 「カテゴリ」、「マルウェア名」、「処理日」、「処理方法」、「検知されたディレクトリ」などが表示されます。

1-	ザ詳細情報					Clos
	ユーザ情報 処理の	コグ ログのみ記録	除外ログ キャン	セルログ	● 御田ログ →	
	カテゴリ	マルウェア名	処理日	処理方法	検知されたディレクトリ	Â
1	インスタントメッセンジャー	E MSG MirandalM	2018-03-14 16:08:58	(R) B	c:Users'hannote'Desktop/テストツールマルウェア検渉/マルウェア検渉 Vrikanda-im-v0.9.10-unicode.exe	
2	ファイル交換ソフト(P2P)	P.P2P.Mesh	2018-03-14 16:08:58	(R) E	c:Users'hannoteiDesktopiテストツールマルウェア検体\マルウェア検体 VMeshV9.exe	
3	ファイル交換ソフト(P2P)	P.P2P.Mesh	2018-03-14 16:08:58	(R) B	c:Users/hannotelDesktopiテストツールマルウェア検洋\マルウェア検洋 VMeshV9.exe	
4	ファイル交換ソフト(P2P)	P.P2P.BitSpirit	2018-03-14 16:08:58	(10 B	c:Usen/hannoteiDesktop/テストツールマルウェア検体\マルウェア検体 Vosv3.6.0.500 mu exe	
5	ファイル交換ソフト(P2P)	P.P2P.BitSpirit	2018-03-14 16:08:58	(R) B	c:Users/hannote/Desktop/テストツールマルウェア検渉/マルウェア検渉 Vosv3.6.0.500 mulexe	
6	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2018-03-14 16:08:58	(R)E	c:Users'hannote'Desktop/テストツールマルウェア検洋\マルウェア検洋 'billoment-6.4.exe	
7	ファイル交換ソフト(P2P)	P.P2P.BitTorrent	2018-03-14 16:08:58	(R) B	c:Users'hannote'Desktopiテストツールマルウェア検渉マルウェア検渉 'billorren5-6.4.exe	
8	トロイの木馬	K.KLG.natsume	2018-03-14 16:08:58	(RDB)	c:Users'hannote'Desktopiテストツール/ウイルス検体/ウイルス検体 \natsume.exe	
9	トロイの木馬	K.KLG.natsume	2018-03-14 16:08:58	(10 B	c:/Users/hannote/Desktop/デストツール/ウイルス検询/ウイルス検体 \natsume.exe	
10	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 16:08:58	(R)E	c:Users'hannote'Desktop/デストツール/ウイルス検律/ウイルス検律 Veicar.com	
11	インスタントメッセンジャー	E MSG MirandalM	2018-03-14 16:08:58	(R) B	c:/Users/hannote/Desktop/テストツールマルウェア検洋マルウェア検洋 Vmiranda-im-v0.9.10-unicode exe	
12	インスタントメッセンジャー	E.MSG.MirandalM	2018-03-14 15:44:23	(10B	c:Usen/hannoteiDesktopiテストツールマルウェア検体\マルウェア検体 Vmiranda-im-v0.9.10-unicode.exe	
13	ファイル交換ソフト(P2P)	P.P2P.Mesh	2018-03-14 15:44:23	(R) B	c:Wsens'hannote'Desktop/テストツールマルウェア検体マルウェア検体 VMeshV9.exe	
	THE ALL MIRE COLUMNS	0.00011-0	2010/00/00/00/00/00	dan	AIRCOMPTOTION FOR A CONTRACTOR AND A CON	*

EX AntiMalware v7 Manager ユーザガイド

くご注意事項>

マルウェアの復旧は、処理を実行した各クライアント PC で行う必要があります。 また、マルウェアの復旧は、管理者権限のあるユーザアカウントで行ってください。

9. ログを表示する

「ログ」では、各クライアント PC の情報をサーバで集計して閲覧、または、分析してグラフ表示などができます。 基本的に「ログ」、「分析」と「アップデート」の3つのタブに分かれています。

タブ	内容
ログ	「マルウェアログー覧」と「アクセスログー覧」が確認できます。
分析	「カテゴリ別」、「マルウェア別」、「ユーザ別」、「月別マルウェアレポート」、「月
	別検知レポート」、「検知推移」、「マルウェア侵入状況」などの分析結果が確認
	できます。
アップデート	「プログラム」、「マルウェア DB」、「アンチマルウェアエンジン」、「グレーツール
	DB」、「アンチグレーツールエンジン」の各アップデート状況を円グラフによって
	表示できます。

9.1. マルウェアログー覧を表示する

マルウェアログー覧では各クライアント PC で処理されたマルウェアログー覧が処理日を基準に表示されます。 検索の条件を変更して再検索することもできます。

プルダウンメニューから絞り込む項目を選択、または入力項目にキーワードを入力して、[検索]ボタンをクリック します。

入力キーワードを「部分一致」、「等しい」、「等しくない」などの条件設定で絞り込もことが可能です。

上部の検索に合わせて「表示する項目を選択」で表示したい項目を追加することやその設定を保存することもで きます。

保存する場合は、[表示方法を保存]ボタンをクリックします。

表示した項目を CSV 形式でエクスポートする場合は、[CSV]ボタンをクリックして任意のディレクトリに保存します。

🐔 Fuva Brair

EX AntiMalware v7 Manager ユ<u>ーザガイド</u>

F×	≣ 🕅 *>>*	>9=176									-Doard
	07				1948			9979-	Ŕ.		
EX Antimaiware	<u>2002705-8</u> 202305-8				58338 240478 2-98 882403	85.89 3421793	AME .	20024 242x20 225240 00-2-5	0 11713553		
29-92					用制度化。*	t-b-		72992-	9-12555		
	4.8										
Travite .		10/5~#F				8.8.*					
A SHEA		29731	×			TAT *	6/87/h		. 7	NC *	
and the second second	ワークグループ名	,	·新田	<			- +				
dens .		648.		2018	0.011	• M 212	-	23	* M 5915	9	88 🗑 CSV
🕥 RUS-AR	89783058H		32E3-93	8	# 2-76	al and P	₩ カFdV	a 70	2176	# 463	er sata
🕎 -3-9 56 -	# GETA		exce.	200	# 5/3/P.(408)	🖬 97F63	₩ MAC71	12		14	-
. 07	189007										
	2-994-78	39-63-95	コーザモ	1010	7779	742176	9000	640 •	158312 (#	NUE 5-3.9 Li0	0 P293
単分くところいる	1 HORKOROLP			10.00.00.0	71.927	JCX, EICAR text File (no	2018-03-15 17 12 44	2010-02-15 17 12:51	070408	1 Microsoft Windows	Server 2:102.188.25
プライバシーポリシー	3 808060P			-	#3285h#	JCX E MOD Amandade	2010/07/02/08	2018-85-18 17,12:51	COCHER	1 Moreauth Weatowi	Derrer 2, 192, 188,25
EX Antibiativare \$7,8,1,21	1 HORADROLP			-	H208/9517	JCR. E.MSG.MinanderHil	2010-03-15 17:12-45	2010-03-15 12 12 51	COONER.	4 Monault Wedgess	Derver 2: 102:108:35
6 2016 Absur Co., Ltd.	4 HORKOROUP			-	45285 F.F	JCR. E.MOD.Winanda-MI	2018-03-05 17:12:47	2010-00-15 17 12:51	070408	1 Moresell Woodows	Server 2 192 198 25
	1 HORKOROLP				27415395	JCR PPOP Betterwet	2010/02/15/17/12/45	2010-02-15 17 12:51	COCADE	2 Morand Wedness	Server 2 192 188.25
	T HORNOROLP			-	2703285	TUA PERMIT	2010/03/05/05 17:12:45	2010-02-15 17:12:51 Mont 31:45 47 47-44	CARADE	1 Margaret Visions	Server 2 162 168 25
	1 10000000				2441000	ITA PERMIT	NUM AL IN STATE	1000.03.05.07.02.01	CARA DE	A Referenced Management	Barley 2, 162, 168, 25
	 beconder 				The state of the	ALC PROPERTY	Makely in 17-12-44	5555.05.45 17 17.54	COLORED B	1 Manual Manual	
	a someone				the second se	and the second se	and the second sec			The second s	

9.2. 検知されたディレクトリ情報を表示する

検知ログのマルウェア名の[パス]をクリックすると検知されたディレクトリ情報を確認できます。 ※検知されたディレクトリ情報は[ユーザ情報]タブのユーザ詳細情報からも確認できます。

F/	■ ₩ *>>+>+>		-J.07791
EV Antillahuman	07	54	¥97¥-+
V7	2002.202-8 2292.202-8	AFINE MEET RACETE RECEIPTION	20224 26.02.706 7.62.706
. 10.07		/0.	
area .		C User/American/Cestop/7/J/317/818/2/J/327/818	nitranda-ini vit 8 10 unicode are
🗶 weense 🔹	ALL	-	
🔒 энеэх 🕠	ULVER DE LE		(YAT.*)
4 ener -	10-070-7A 1100-0 11		Q an Bicav
0 eus-ma	 第三丁を専用を用き 第二丁クジュージネ 第二コンピュージネ 		wince witche
関 3-998	Winana Winan	*	(Q Renates
2 29	8407		
89416007 794/(5~805-		1 123322 DEC Manual 2013311/1214	HIGH 5-3.7 (200) P271 B 1 Monard Renard Renard 2102 102.70 (Minuted Renard Renard Renard 2102 102.70 (Minuted Renard Rena

9.3. アクセスログ一覧を表示する

EX AntiMalware v7 Manager にアクセスされた管理者情報をアクセスログとして管理しています。 アクセスログでは「管理者 ID」、「アクセス日」、「曜日」、「Host 名」、「IP アドレス」、「操作」が確認できます。 条件を変更して検索することも可能です。

検索した項目を CSV 形式でエクスポートする場合は、[CSV]ボタンをクリックして任意のディレクトリに保存します。

🐔 Fuva Brai

$\overline{\mathbf{N}}$					-E 0770
44	07	64		アップゲート	
	201202-N	カテコリ語 単数 エレウエア語 200 ユーザ語 用語アルヴェアレポート 用語学校にポート	10 21741/12	202324 20222700 204240722255 204204022255 20420404 204204-2442145	
AP-76					
1 BURNE -	Tween the		1		
- SKENK	79628 •	3016010 1 · · 0 · m	- 0	11 + in 50m	Q ## 8 cm
de entre	P98307				
S AN INVESTIGATION OF COMPANY	R480	アクセス日・	40	medi	#アドレス
N 1015-415 1	1 6/14/1	2010-05-10 10:30.12	±180	182 198 263 118	192 198 253 118
	2 that	2010-00-18 18 21 48	1965	162.168.293.118	182,198,253,118
1 3-9/8H +	3 844	2018-85-15-16-18-12	.190	182-188-243-118	192 198 253 116
	4 0141	2010-05-16 16:00:58	780	182 148 253 118	182 165 253 116
- C7 1	5 Alter	2010-00-15 10:02 17		182:188.293.116	162 168 253 114
100	a Abra	2018-03-15 17:10 26	785	102 108 203 21	182 198 213 31
AND A DOWNLOW	P Bhan	2010-03-15 10 40 34	740	190,190,250,42	192 168 210 AD
Bibe tor Source	8	2010/05/15 12:45:40	745	182 188 253 118	192.198.253.119
	2 M 1	200 million and 100 million and			********

9.4. カテゴリ別の分析を表示する

検知されたマルウェアをカテゴリ別に分析することができます。

ポリシー選択と期間を設定して、[**検索**]ボタンをクリックすることでカテゴリ別の一覧を表示します。 また、[CSV]ボタンをクリックすると、検索した情報を CSV 形式で保存できます。

閲覧できる項目は、「カテゴリ」、「検知されたマルウェア数」、「検知率(%)」です。

$\sim $	■ ¹ / ₁ *>>+>+>+>+>		
EV Antillahunna	07	5H	アップジート
V Antomalware	340+707-8 791307-8	カテゴン約 単純成長 スルウェア語 スルウェア違ん状態 ユーザ第 約8554.00エアレポート	2023A 2402208 202720522555 20-2-308
🐺 X7-9X 🕠		RESIDELAT-E	アンチグレージールエンジン
🧕 uutaika 🕠	88		
A SHEDR	ポリシー編尺 金信 時間 2016年1月1日	2816/0319	Q. 88. 🗷 CSV
At anno .	カアゴリ取分析		
9 8	カデゴリ	検知されたマルウェア	B • 8/0=(%)
(i) #US-88	1 7//217	4792	64.36
	2 ファイル交換ソフトP3P	5410	19.30
2-558	3 インスタントメッセンジャ	1001	14.11
	4 ND-Y08.8	116	1.59
👄 nđ 🔹	5 待セキュリティンフト	34	0.47
20, 1	6 9594917	10	0.14
	7 806	2	0.03
首サイトについて	8 7F9±7		0.01
プライバシーポリシー			
EX AntiMalware V7.0.1.21 0.2018 ANkun Co., Ltd.	計機能されたマルウェア	8 7004 	10 *

9.5. マルウェア別の分析を表示する

検知されたマルウェア名別に分析することができます。

ポリシー選択と期間、カテゴリを設定して、[検索]ボタンをクリックすることでマルウェア別の一覧を表示します。 選択できるカテゴリは、既に検知済みのマルウェアのカテゴリに限定されます。

また、[CSV]ボタンをクリックすると、表示した情報を CSV 形式で保存できます。

閲覧できる項目は、「カテゴリ」、「マルウェア名」、「コンピュータ数」です。

🐔 Fuva Brair

EX An	tiMa	lware	v7	Manager	<u></u>	-ザガイ	۴
-------	------	-------	----	---------	---------	------	---

$\overline{\nabla}$	E Server	375							6	
EV Antillaburan	07			64			アップソート			
EX AntiMahware	2622202-N 292302-N			27238 742278 2-28 887422758	カテゴンE 単化相型 スムウェア語 スムウェブ語入びE ユーザ語 第807-01-71-8-5			70795 2522708 758780727255		
25-92				<u>用数据输出。但一下</u>			20#50-V-112050			
	**									
A	100 E	201416	1 ~ E	2018/05/1	カデゴリ すべた				Q.	E R CSV
artor -	750178088				CONTRACTOR INCOME				i sa tina	
N		5730				マルウェア省				· 89-152
*	8	24717			EC4A	fast-file (nut a virus)				. 14
B	2	フナイル交換ソフト	(#2#);			P2PBRown				16
	1.	25-662第221	(737)			P/OP/Medit				1.8
100	4	インスタントメッセン	277	E MSG MAXAMM						1
and the second s	10	ファイルを良いつき	(#2#)		1	# P2P Bitlant				. 1
9 D7 ·						10 as as 1 - 4				
	<>31-A88									
治サイトについて	2-074-78	コンピュータ石	3-96	1010.07	-4532h-68	ACCR401	5-7,9,5,08	1.00 Vec	HESINE.	P7 アレス
プライバシーボリシー	 workowow 	State of the local dist.		182 168 253 116	2017-11-10 13 03 45	2010-02-10 10-41 11	Monard Printed 19-20	10.0	8063	192 108 56 1
EX Antibideness V7.5.1.21	2 WORKDROUP	1010.0104000		142.188.253.37	2017-12-19.1634.14	2018-03-15 10:50:59	Worsald Hindows Sava	c 62	8182	182,188,252,3
@ 2018 Ankun Co., Ltd.	 Workokou# 	processing of		182.586.250.85	2017/12/28 11:18:06	2018-02-09 10 28 42	Michaelt Holdsey 7 Hor	8.1	8109	102.168.253.0
	4 WORKDROUP	100000-00.001	1001000	182 148 253 115	2017-12-08 13:08-45	2010-00-19 19 19 44	Monand Hindard 7 Frd	4 81	29/3	182 108 253 11
	5 WORKDROUP	1010.010800		182 186 280 37	2017-12-12 18:38:38	2018-02-01 10:58:39	Microsoft Hirstones Sarva	r; 82	8192	1021101212121
						12. m m 3. 4				

また、表示項目をクリックして、そのマルウェアが検知されたコンピュータの「インストール情報」を画面の下部で 表示させることができます。

9.6. ユーザ別の分析を表示する

ポリシー選択と期間を設定して、[**検索**]ボタンをクリックすることでユーザ別の一覧を表示します。 また、[**CSV**]ボタンをクリックすると、表示した情報を CSV 形式で保存できます。閲覧できる項目は、「ユーザ名」、 「接続 IP」、「IP アドレス」、「検知されたマルウェア数」です。

\overline{N}	=	4594595376					-100000	
	0.7			64t		7977-1 20234 7402-738 7547300-73100 2010-71-00 2010-71-00 71490-01-1100		
W Antimatiware	742±75 22230	22-18 2-18		22332 0000 240128 750120 24028 00210126-1				
1 25-52				和影響的公式一下				
A	4.8							
A BRANK .		ポリシー 単作 全体		•				
D PHEDA		#12 E	20101012	2010/05/19			🔾 HE 🗑 CSV	
2 auge -	3-17896							
		1-98	コンピュータ名	945 P	デアドレス	MREPLE7.09±7	**	
🚺 mus-ma			ALC: 1000-1	192,108,253,88	192 108 253 88			
Start Mark South A	2	81.05	10,000	182 186 253 51	10.02.15	1		
2-1/64	2	100.000	100.000.000	192 198 253 48	12.0.2.15	1		
	4		1010.010000	192 108 251 37	182.168.253.37	1		
10 57 I		10110		142.948.253.7%	10.0.2 15			
<i><i><i>a</i></i></i>	1.			182 108 248 215	182 556 253 26	4		
WHAT LOT ANT	1			192.108.253.108	192 198 253 118	1		
H D A I W P A I D				102.100.253.01	12.0.2.15			
754/13-2015-			in the second second	100,000,000,000	10.0.2.18			
EX AntiMateory V7.0.1.21 ID 2018 Advant Co., Ltd.	257			112.148.213.84	10.0.2.16	1. 1.		
					(1-1) H + H +			
	6/882							
		カチゴリ	249278	NAULE.		1546.0	687.8	
i	1.0	and an ender some ment	de anna air a ta an			many of the latest	al an and	

また、表示ユーザをクリックして、そのユーザが処理した「処理履歴」を画面の下部で表示させることができます。

9.7. 月別マルウェアレポートを表示する

ポリシー選択と期間を設定して、[検索]ボタンをクリックすることで月別マルウェアの一覧を表示します。 また、[CSV]ボタンをクリックすると、表示した情報を CSV 形式で保存できます。

閲覧できる項目は、「マルウェア名」、「カテゴリ」、「初回の検知日」、「最終検知日時」、「コンピュータ数」、「検知 したマルウェアの合計数」です。

\sim 7	=	W 4>>+>+>+>+>+>					· 군 09791	
EV Antillaburara	07			1940		アップデート		
EX AntiMalware		207-8 107-8		12208 8048 740278 7402780 2428 887402704+5 88804.4-5	R.R.	2022A 74.05.20 72.45.7000 72.45.7000 72.45.7000 72.45.7000 72.45.7000 72.45.7000 72.45.7000 72.45.7000 72.45.7000 72.45.700000000000000000000000000000000000		
A2:20								
👷 wennz 🕠		Million and		+1				
a stepa .		Ref 1010	- 19	2010/02/10			Q HE E CSV	
de esser .	READ	1.76-1						
A REPORT OF A		769176	5930	RECHARG	814504	3261-98.	68	
A 1015-ME +	. 1	EXCAR feet File (not a smull)	74917	2010-01-10-10-10-10	2010-05-15 17 12 44	54	4090	
and the second sec	2	E MISO Minandamine	インスタントメッセント	2010-01-10-12-20	2010-03-15 17:12:47	<i>x</i>	474	
COLUMN 1	1	E.MSG Skype	インスタントラッセンタ	2010-01-01-04:57:59	2818-85-13 88:36:13		425	
	. 4	F FKE PCNIschartic	- 侍世がみ リティリク	P 2018-02-01 1614-26	2010-03-05 19 30 13	2	34	
		E MISG TeamTalk	インスタントメンセンタ	2018-02-01 10:04:09	2010-02-09 20:12-47	2	90.	
8 . WY	1.1	E M50 -CO	インスタンクメッセンタ	17- 2010-03-05 10 at 33	2010-63-08 09-94 42	2	21	
and the second second	7	E MIO Karao felk	インスタントメッセンタ	2018-02-0118-30-00	2018-82-01 18:30:08			
御寺ペトについて		6 MIG ChoCae	ペンスタントメンセンタ	im = 2018-05-15 17 96.24	2010-03-13-10-12		2	
プライバシーボリシー		reprication thander inclutioner A	eos	2010-05-12 14:23:36	2010-03-12 10 17:39	1	1	
EX AntiMateuro V7.8.3.25 E 2018 Aldere Co. Ltd.	.18	A ADV Yorkee	アドウエア	2010-02-01 13,46,57	2010/02-01 15 45:57			
					N = CAP JASER B	B	7306	

9.8. 月別検知レポートを表示する

ポリシー選択と期間、カテゴリとマルウェアを設定して、[検索]ボタンをクリックすることで月別検知レポートの一覧を表示します。

選択できるカテゴリとマルウェアは、既に検知済みのカテゴリとマルウェアに限定されます。

また、[CSV]ボタンをクリックすると、表示した情報を CSV 形式で保存できます。

閲覧できる項目は、「ワークグループ名」、「コンピュータ名」、「接続 IP」、「IP アドレス」、「検知日」、「カテゴリ」、 「マルウェア名」、「検知したマルウェアの合計数」です。

$\overline{\nabla}$	=	T 4>>+>+==P	9.						
	07			08			アップデート		
EX AntiMalware		201700-11 20100-11			第11日日 又ルフェア使入法 アレポート	A.	2022A 2422708 2022708		
				月末時に,一	-b		75900-0-02555		
	**								
A		ポリシー道内 創住			(*)				
a stess i		net C	301640.0	2000	1920 TA	τ	71/217 1952		
de entre ·								Q RR E CIV	
	/1085	L-8-1-							
🚺 (\$25-ft)) 🔹		9-69%-78	3582-98	Bet P	#7FL3	8103	69:30	262126	
		Workcarlouit	design of generation.	10.000	1000.00	2018-02-18 VE 17:37	2/227	EICAR-Text File (not a year)	
💓 3-990 (1	workdkour	ACCOUNT OF ADDRESS	10.000	10101	2018-02-15 17 18-48	7//317	EXCAR-Text-File (not a whee)	
	1.1	WORKOROUP	NUMPER ADDRESS	100.000.000	1002.0	2018-02/15 17 10/01	21/227	(CAR Yes) Fee (not a vise)	
9 09 +		wonkonour	10.0117-01.007864	10.000	100110	2918-42-18.17.21.01	7//017	ECAN Tech File (htt & whee)	
-	1.1	WORKOROUF	contract of specification	10.000	1044.0	2018-62-15 17:20:05	₹1/2≠7	EICAN Test File (rst a vnat)	
あやイトについて		WORKOROUP	The second second	10.00	10101	3018-01-31 12:35:38	2//257	ECAN feet-Frei Init a vinit)	
the sale of the	T	WORKOROUP	stration grades	10.000	1010.0	2016-02-15 17:18.62	マルクエア	EICAA Tep-File (nut a vitut)	
3.54V2m#05m	. 8	wokkakouP	And a second second second	10.100.000	10.01.01	2010-01-21 12:10:20	21/257	ECAR feat Fee (not a virus)	
EX ArtiMalward V7.8 1 21		WORKOROUP	and a series of the	10.100.000.00	10010	2018/01/01 58:37:47	76717	EICAN Tech File (hol a virus).	
8 2018 Alloin Co., LM	18	WORKSROUP	10.0000000	10.000	10010	3518-02-07 16-48-95	7//2±7	ECAR-Tech-File (nut a virus)	
								計 単気された マルウエア目	
					14.14.10	-58 /304			

9.9. 検知推移分析

ポリシー選択と期間、カテゴリ、マルウェアを設定して、[検索]ボタンをクリックすることで検知推移を棒グラフで 表示します。選択できるカテゴリとマルウェアは、既に検知済みのカテゴリとマルウェアに限定されます。



9.10. マルウェア侵入状況分析を表示する

ポリシー選択と期間を設定して、[検索]ボタンをクリックすることでマルウェアの侵入状況を円グラフで表示しま す。

$\overline{\nabla}$	E 1004040174		-2 0979H
EY AntiMahwara	07	5 47	アップデート
V Antumarware	2.02.707-1 7922.07-1	カテゴンE 単位成準 アムウェア語 スルウェア違入状況 ユーザ語 月末マルウェアレポート	70254 2022708 21/92/027252 21/92/0272522
AF-97 +		AB9661/2-1-	Z1#91-9-64192
🔒 weasse 🕠			
a settor 🕠	ボジジー編代 金修 利徒 2858010 1 ~	2018/03/19	Q HE
de enez -		マルウェア最入状況	
ि अप्रध्न-सन्द । जि. व-प्रश्नस ।		(Bar(()L4%)	
1874 FED417 7547 (S=#355= EX Andhalanan V2 5 1 21 0 2018 Ablum Co. UM	92504C (01.4		

9.11. アップデートを表示する

アップデートでは、「プログラム」、「マルウェア DB」、「アンチマルウェアエンジン」、「グレーツール DB」、「アンチ グレーツールエンジン」の各アップデート状況を分析して円グラフで表示できます。ポリシー選択と期間を設定し て、[検索]ボタンをクリックすることで各アップデート状況を円グラフで表示します。

項目	内容
プログラム	期間中に EX AntiMalware v7 クライアントプログラムをアップデートした PC と、
	アップデートしていない PC を円グラフで表示します。
マルウェア DB	期間中に EX AntiMalware v7 クライアントプログラムのマルウェアのデータベー
	スをアップデートした PC と、アップデートしていない PC を円グラフで表示しま
	す。

EX AntiMalware v7 Manager ユーザガイド

X AntiMalware v7 Manager ユーザガイド		🔊 Fuva Brain	
	アンチマルウェアエンジン	期間中に EX AntiMalware v7 クライアントプログラムのマルウェア検出エンジ	ン
		をアップデートした PCと、アップデートしていない PCを円グラフで表示します	o
	グレーツール DB	期間中にEX AntiMalware v7 クライアントプログラムのグレーツールのデータ	べ
		ースをアップデートした PC とアップデートしていない PC を円グラフで表示しま	ŧ
		す。	
	アンチグレーツールエンジン	期間中にEX AntiMalware v7クライアントプログラムのグレーツール検出エン	ジ
		ンをアップデートした PC と、アップデートしていない PC を円グラフで表示しま	Ξ
		す。	



🎻 Fuva Brain

EX AntiMalware v7 Manager ユーザガイド

10. クライアントプログラムについて [EXAMv7_UsersGuide_Client.pdf] をご確認ください。

🐔 Fuva Brair

EX AntiMalware v7 Manager ユーザガイド

11. サポートについて

サポートのお問い合わせは、EX AntiMalware v7 のライセンスおよびソフトウェアサポートをご契約された販売会 社までお願いします。

くご注意事項>

ご購入前のお客様の技術サポートは基本的にお受けしておりません。

サービスやソフトウェアに関する技術的なご質問や、製品評価時のご質問につきましては、

info_antimalware @fuva-brain.co.jp または株式会社フーバーブレインの代理店、および弊社営業担当までお問い合わせください。

12. Basic、for Server、Light ポリシーのデフォルト設定 (確認)

13. 項目	設定	
【基本設定】		
基本設定		
ポリシー名称	Basic	
スタート IP	_	
終了IP	_	
ネットワーク名	指定なし	
コメント	Basic	
アラート・メール送信		
1 時間に〇件以上のマルウェアを検出したら管理者へメールを送信	10	
メールアドレス	-	
【スキャンオプション】		
バックグランドスキャンの設定		
バックグランドでスケジュールスキャンを実行(GUI 非表示)	□Y ■N	
結果画面表示		
セキュリティ設定	□高 ■中 □低	
スキャン速度の設定	□高速 ■標準 □低速	
その他		
グレーツールの検知時にチェック状態	■Y □N	
右クリックスキャン	■Y □N	
圧縮ファイルスキャン	■Y □N	
	□Y ■N	
スキャン上限サイズ	0	
	■MB □GB	
スタートページの設定		
確認ダイアログを表示	□Y ■N	
スタートページとして使用する URL :		

【スケジュール】	
	ロ設定しない
	□周期:()日□曜日:()曜日 ■毎月:(8)日
	■スキャン開始時間:(12)時(00)分
フルスキャンスケジュール	ロスケジュールスキャン時に自動処理
	■処理後にプログラム終了
	口処理後にシステム終了
	ロスキャン時に電源 OFF の場合、翌日に実行
	ロ設定しない
	■周期:(1)日□曜日:()曜日□毎月:()日
	■スキャン開始時間:(12)時(00)分
クイックスキャンスケジュール	ロスケジュールスキャン時に自動処理
	■処理後にプログラム終了
	口処理後にシステム終了
	ロスキャン時に電源 OFF の場合、翌日に実行
【実行モード】	
プログラムの実行方式	■基本実行モード(推奨) □最小実行モード
管理モード	■管理者 □管理者(GUI 非表示) □ユーザ
スケジュールスキャン終了後、実行するプログラムの指定	
【リアルタイム監視】	
リアルタイム監視設定	
リアルタイム監視使用	■Y □N
	口軽快
監視モード	■標準(推奨)
イックスキャンスケジュール 各行モード] コグラムの実行方式 理モード アジュールスキャン終了後、実行するプログラムの指定 アルタイム監視] アルタイム監視設定 リアルタイム監視使用 監視モード リムーパブルディスク(USB メモリ、DVD メディア)挿入時の処理 *ップデート] DB アップデート時にユーザに詳細情報を表示 アップデートボリシー関連アラートを表示	■ランサムウェア検知使用
	■Y □N
リムーバブルディスク(USB メモリ、DVD メディア)挿入時の処理	■スキャンを行う前に確認ダイアログを表示する
	□検知時に自動処理
【アップデート】	
	■自動アップデート
	ロ手動アップデート
	ロスケジュールアップデート
アップデートの設定	■PC 起動時アップデート
	□周期:()日□曜日:()曜日□毎月:()日
	ロアップデート開始時間: 時 分
 DB アップデート時にユーザに詳細情報を表示	
アップデート/ ポリシー関連アラートを表示	

AntiMalware v7 Manager ユーザガイド	🐔 Fux
スマートアップデートを使用	■Y □N
ポート番号	9340
【一時ファイル削除】	
スキャン実行前の削除設定	
Windows 一時ファイルの削除	■Y □N
インターネットー時ファイルの削除	■Y □N
Cookie の削除	□Y ■N
インターネット/オートコンプリート履歴を削除	□Y ■N
最近使用したドキュメントのリストを削除	■Y □N
処理履歴と隔離項目の削除設定	
削除せずにそのまま放置	■Y □N
指定日数後に削除(クリア)する	□Y: (14)日 ■N
【ユーザ制御】	
マルウェア:一括設定	ロユーザ選択 口隔離 口除外 ロログのみ記録
	■Y □N
ウイルス/ワーム	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
アドウェア	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
ハイジャッカー	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
トロイの木馬/ハッキンクツール	□ユーザ選択 ■隔離 □除外 □ログのみ記録
- * / ! -	■Y □N
2/1717	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
Hosts ファイル改変マルウェア	□ユーザ選択 ■隔離 □除外 □ログのみ記録
その他	■Y □N
	□ユーザ選択 ■隔離 □除外 □ログのみ記録
グレーツール:一括設定	ロユーザ選択 口隔離 口除外 ロログのみ記録
	■Y □N
ファイル交換ソフト(P2P)	■ユーザ選択 □隔離 □除外 □ログのみ記録
1 - 7 Fr. 1 Jun 1 - 1 - 2 -	□Y■N
インスタントメッセンジャー	■ユーザ選択 □隔離 □除外 □ログのみ記録
<u></u>	■Y □N
ボッブアップ広告	■ユーザ選択 □隔離 □除外 □ログのみ記録

AntiMalware v7 Manager ユーザガイド	F.
偽セキュリティソフト	■Y □N
	■ユーザ選択 □隔離 □除外 □ログのみ記録
7.0.W	■Y □N
その他	■ユーザ選択 □隔離 □除外 □ログのみ記録
ユーザ機能制限	
スキャン実行中の中止制御	□Y ■N
処理実行中の中止制御	□Y ■N
トレイアイコンの終了制御	□Y ■N
処理ボタンの非表示設定	□Y ■N
除外ボタンの非表示設定	□Y ■N
ログのみ記録ボタンの非表示設定	□Y ■N
リアルタイム監視の終了制御	□Y ■N
除外設定	■許可 □無効化 □パスワード設定()
オプション	■許可 □無効化 □パスワード設定())
アンインストール	■許可 □無効化 □パスワード設定()
隔離	■許可 □無効化 □パスワード設定()
【除外】	
除外	
ファイル名の除外設定	
拡張子の除外設定	
ディレクトリの除外設定	
マルウェア名の除外設定	
未知のランサムウェア除外	
ኲクト 9 るノブイル石	□Windows の System プロセスを除外する

項目	設定	
【基本設定】		
基本設定		
ポリシー名称	for Server	
スタート IP	_	
終了IP	-	
ネットワーク名	指定なし	
コメント	サーバ用ポリシー	
アラート・メール送信		
1 時間に〇件以上のマルウェアを検出したら管理者へメールを送信	10	
メールアドレス	-	

■Y □N
□Y ■N
□高 ■中 □低
□高速 ■標準 □低速
■Y □N
■Y □N
■Y □N
□Y ■N
0
■MB □GB
□Y ■N
ロ設定しない
□周期:()日□曜日:()曜日 ■毎月:(8)日
■スキャン開始時間:(2)時(00)分
■スケジュールスキャン時に自動処理
■処理後にプログラム終了
口処理後にシステム終了
ロスキャン時に電源 OFF の場合、翌日に実行
ロ設定しない
■周期:(1)日□曜日:()曜日□毎月:()
■スキャン開始時間:(2)時(00)分
■スケジュールスキャン時に自動処理
■処理後にプログラム終了
口処理後にシステム終了
ロスキャン時に電源 OFF の場合、翌日に実行
■基本実行モード(推奨) □最小実行モード
■管理者 □管理者(GUI 非表示) □ユーザ

Brain

AntiMalware v7 Manager ユーザガイド	🗧 🖌 👘 🖓 👘 🖓 👘
リアルタイム監視使用	■Y □N
監視モード	■標準(推奨)
	■ランサムウェア検知使用
	■Y □N
リムーバブルディスク(USB メモリ、DVD メディア)挿入時の処理	ロスキャンを行う前に確認ダイアログを表示する
	■検知時に自動処理
【アップデート】	
アップデートの設定	■自動アップデート
	ロ手動アップデート
	ロスケジュールアップデート
	■PC 起動時アップデート
	□周期:()日□曜日:()曜日□毎月:()日
	ロアップデート開始時間: 時 分
DB アップデート時にユーザに詳細情報を表示	
アップデート/ ポリシー関連アラートを表示	■Y □N
スマートアップデートを使用	■Y □N
ポート番号	9340
【一時ファイル削除】	
スキャン実行前の削除設定	
Windows 一時ファイルの削除	■Y □N
インターネットー時ファイルの削除	■Y □N
Cookie の削除	□Y ■N
インターネット/オートコンプリート履歴を削除	□Y ■N
最近使用したドキュメントのリストを削除	■Y □N
処理履歴と隔離項目の削除設定	
削除せずにそのまま放置	■Y □N
指定日数後に削除(クリア)する	□Y: (14)日 ■N
【ユーザ制御】	
スキャンするカテゴリの設定	
マルウェア:一括設定	ロユーザ選択 口隔離 口除外 ロログのみ記録
	■Y □N
ワイルス/ワーム	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
アドウェア	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
ハイジャッカー	

Copyright © 2019 Fuva Brain Limited. All Rights Reserved.

AntiMalware v7 Manager ユーザガイド	File File File File File File File File
	■Y □N
アロコ 50 不局/ ハッオノン ソール	□ユーザ選択 ■隔離 □除外 □ログのみ記録
スパイウェア	■Y □N
	□ユーザ選択 ■隔離 □除外 □ログのみ記録
Hosts ファイル改変マルウェア	■Y □N
	□ユーザ選択 ■隔離 □除外 □ログのみ記録
その他	■Y □N
	□ユーザ選択 ■隔離 □除外 □ログのみ記録
グレーツール:一括設定	□ユーザ選択 □隔離 □除外 □ログのみ記録
コッノル大海ション(D2D)	□Y ■N
ンディル文換フント(F2F)	■ユーザ選択 □隔離 □除外 □ログのみ記録
	□Y ■N
インスタントメリセンシャー	■ユーザ選択 □隔離 □除外 □ログのみ記録
キぃーマぃーナチ	□Y ■N
	■ユーザ選択 □隔離 □除外 □ログのみ記録
	□Y ■N
偽セキュリティソフト	■ユーザ選択 □隔離 □除外 □ログのみ記録
乙 四曲	□Y ■N
ての地	■ユーザ選択 □隔離 □除外 □ログのみ記録
ユーザ機能制限	
スキャン実行中の中止制御	□Y ■N
処理実行中の中止制御	□Y ■N
トレイアイコンの終了制御	□Y ■N
処理ボタンの非表示設定	□Y ■N
除外ボタンの非表示設定	□Y ■N
ログのみ記録ボタンの非表示設定	□Y ■N
リアルタイム監視の終了制御	□Y ■N
除外設定	
オプション	■許可 □無効化 □パスワード設定()
アンインストール	■許可 □無効化 □パスワード設定()
隔離	
【除外】	
 除外	
ファイル名の除外設定	
拡張子の除外設定	
ディレクトリの除外設定	
マルウェア名の除外設定	

EX	AntiMalware v7 Manager ユーザガイド	-	Fuva Brain
	未知のランサムウェア除外		
	际外するファイル名	□Windows の System プロセスを除外する	

項目	設定
【基本設定】	
基本設定	
ポリシー名称	Light
スタート IP	_
終了IP	-
ネットワーク名	指定なし
コメント	メモリ 4GB 未満の低スペック用ポリシー
アラート・メール送信	
1 時間に〇件以上のマルウェアを検出したら管理者へメールを送信	10
メールアドレス	_
【スキャンオプション】	
バックグランドスキャンの設定	
バックグランドでスケジュールスキャンを実行(GUI 非表示)	□Y ■N
結果画面表示	
セキュリティ設定	□高 ■中 □低
スキャン速度の設定	□高速 □標準 ■低速
その他	
グレーツールの検知時にチェック状態	■Y □N
右クリックスキャン	■Y □N
圧縮ファイルスキャン	□Y ■N
	□Y ■N
スキャン上限サイズ	0
	■MB □GB
スタートページの設定	
確認ダイアログを表示	□Y ■N
スタートページとして使用する URL :	
【スケジュール】	
	口設定しない
	□周期:()日 □曜日:()曜日 ■毎月:(8)日
	■スキャン開始時間:(12)時(00)分
	ロスケジュールスキャン時に自動処理

Copyright © 2019 Fuva Brain Limited. All Rights Reserved.

ntiMalware v7 Manager ユーザガイド	E Fi
	■処理後にプログラム終了
	口処理後にシステム終了
	ロスキャン時に電源 OFF の場合、翌日に実行
	口設定しない
クイックスキャンスケジュール	■周期:(1)日□曜日:()曜日□毎月:()日
	■スキャン開始時間:(12)時(00)分
	ロスケジュールスキャン時に自動処理
	■処理後にプログラム終了
	口処理後にシステム終了
	ロスキャン時に電源 OFF の場合、翌日に実行
【実行モード】	
プログラムの実行方式	■基本実行モード(推奨) □最小実行モード
管理モード	■管理者 □管理者(GUI 非表示) □ユーザ
スケジュールスキャン終了後、実行するプログラムの指定	
【リアルタイム監視】	
リアルタイム監視設定	
リアルタイム監視使用	■Y □N
	■軽快
監視モード	□標準(推奨)
リアルタイム監視使用	ロランサムウェア検知使用
リムーバブルディスク(USB メモリ、DVD メディア)挿入時の処理	■Y □N
	□スキャンを行う前に確認ダイアログを表示する
	□検知時に自動処理
【アップデート】	
	■自動アップデート
	ロ手動アップデート
マップニートの乳白	ロスケジュールアップデート
アッフナートの設定	■PC 起動時アップデート
	□周期:()日□曜日:()曜日□毎月:()日
	ロアップデート開始時間: 時 分
DB アップデート時にユーザに詳細情報を表示	■Y □N
アップデート/ ポリシー関連アラートを表示	■Y □N
スマートアップデートを使用	■Y □N
ポート番号	9340
【一時ファイル削除】	
スキャン実行前の削除設定	
Windows 一時ファイルの削除	■Y □N

AntiMalware v7 Manager ユーザガイド	🖌 🖌
インターネットー時ファイルの削除	■Y □N
Cookie の削除	□Y ■N
インターネット/オートコンプリート履歴を削除	□Y ■N
最近使用したドキュメントのリストを削除	■Y □N
処理履歴と隔離項目の削除設定	
削除せずにそのまま放置	■Y □N
指定日数後に削除(クリア)する	□Y: (14)日 ■N
【ユーザ制御】	
スキャンするカテゴリの設定	
マルウェア:一括設定	ロユーザ選択 口隔離 口除外 ロログのみ記録
	■Y □N
ウイルス/ワーム	□ユーザ選択 ■隔離 □除外 □ログのみ記録
アドウェア	■Y □N
	□ユーザ選択 ■隔離 □除外 □ログのみ記録
ハイジャッカー	■Y □N
	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
トロイの木馬/ハッキングツール	□ユーザ選択 ■隔離 □除外 □ログのみ記録
スパイウェア	■Y □N
	□ユーザ選択 ■隔離 □除外 □ログのみ記録
	■Y □N
Hosts ファイル改変マルウェア	ロユーザ選択 ■隔離 口除外 ロログのみ記録
7 o //h	■Y □N
その他	ロユーザ選択 ■隔離 口除外 ロログのみ記録
グレーツール:一括設定	ロユーザ選択 口隔離 口除外 ロログのみ記録
ファイル交換ソフト(P2P)	■Y □N
	■ユーザ選択 □隔離 □除外 □ログのみ記録
	□Y ■N
インスタントメッセンジャー	■ユーザ選択 □隔離 □除外 □ログのみ記録
ポップアップ広告	■Y □N
	■ユーザ選択 □隔離 □除外 □ログのみ記録
	■Y □N
偽セキュリティソフト	■ユーザ選択 □隔離 □除外 □ログのみ記録
その他	■Y □N
	■ユーザ選択 □隔離 □除外 □ログのみ記録
ユーザ機能制限	
スキャン実行中の中止制御	□Y ■N

AntiMalware v7 Manager ユーザガイド		S Fuv
処理実行中の中止制御	□Y ■N	
トレイアイコンの終了制御	□Y ■N	
処理ボタンの非表示設定	□Y ■N	
除外ボタンの非表示設定	□Y ■N	
ログのみ記録ボタンの非表示設定	□Y ■N	
リアルタイム監視の終了制御	□Y ■N	
除外設定	■許可 □無効化 □パスワード設定()	
オプション	■許可 □無効化 □パスワード設定()	
アンインストール	■許可 □無効化 □パスワード設定()	
隔離	■許可 □無効化 □パスワード設定()	
【除外】		
除外		
ファイル名の除外設定		
拡張子の除外設定		
ディレクトリの除外設定		
マルウェア名の除外設定		
未知のランサムウェア除外		
除外するファイル名		
	□Windows の System プロセスを除外する	