

EX AntiMalware v7 Manager ユーザガイド



株式会社フーバーブレイン

—目次—

はじめに	1
アイコンの説明.....	1
注意事項	1
1. 基本コンセプト	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. 管理者設定をする	7
5. ライセンス状況を確認する	9
6. 環境設定をする	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. 一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. 未知のランサムウェア除外を設定する.....	23
8. ユーザ情報を確認する	24
8.1. 検索する	24
8.2. ユーザ情報を表示する	24

8.3.	各ユーザ別のユーザ詳細情報を表示する	26
8.3.1.	ユーザ情報を表示する	26
8.3.2.	処理ログを表示する	27
8.3.3.	ログのみ記録を表示する	28
8.3.4.	除外ログを表示する	28
8.3.5.	キャンセルログを表示する	29
8.3.6.	復旧ログを表示する	29
9.	ログを表示する	30
9.1.	マルウェアログ一覧を表示する	30
9.2.	検知されたディレクトリ情報を表示する	31
9.3.	アクセスログ一覧を表示する	31
9.4.	カテゴリ別の分析を表示する	32
9.5.	マルウェア別の分析を表示する	32
9.6.	ユーザ別の分析を表示する	33
9.7.	月別マルウェアレポートを表示する	34
9.8.	月別検知レポートを表示する	34
9.9.	検知推移分析	35
9.10.	マルウェア侵入状況分析を表示する	35
9.11.	アップデートを表示する	35
10.	クライアントプログラムについて	37
11.	サポートについて	38
12.	Basic、for Server、Light ポリシーのデフォルト設定（確認）	38

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
	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。

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

Web ブラウザ環境	Windows OS: Google Chrome (推奨)、Internet Explorer 11.0 以降、Microsoft Edge 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。

まず、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すが、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います。

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。

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。



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。

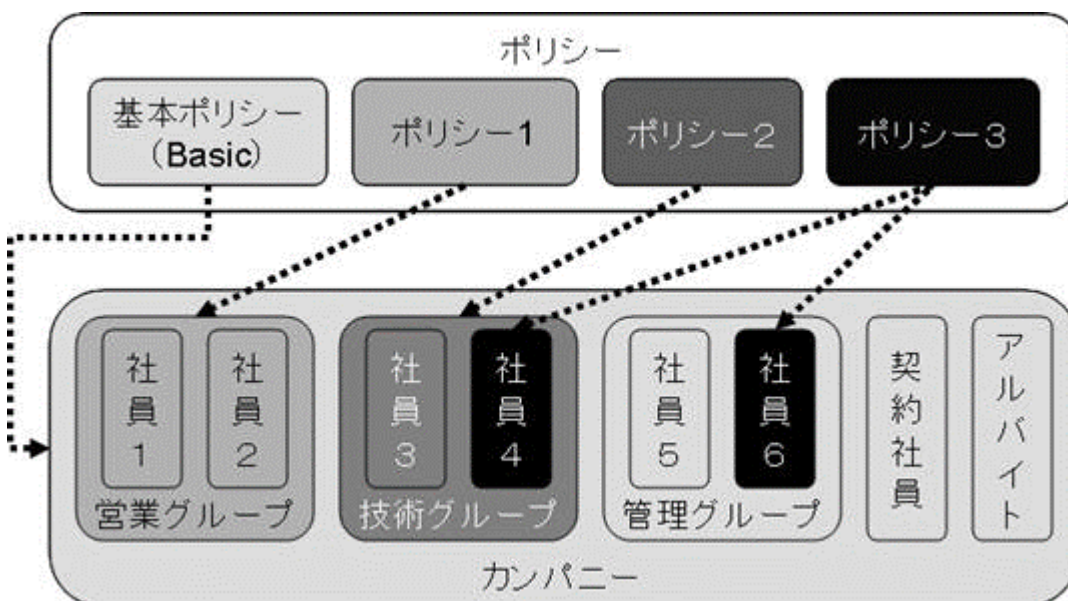


リアルタイム監視設定	
<input checked="" type="checkbox"/>	リアルタイム監視使用(Win/Mac)
監視モード	<input type="radio"/> 軽快(Win) <input checked="" type="radio"/> 標準(推奨)(Win)
<input checked="" type="checkbox"/>	未知のランサムウェア検知使用(Win)

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。



ワークグループを指定するためには対象ワークグループにクライアントプログラムが最低 1 台インス
トールされている必要があります。



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。

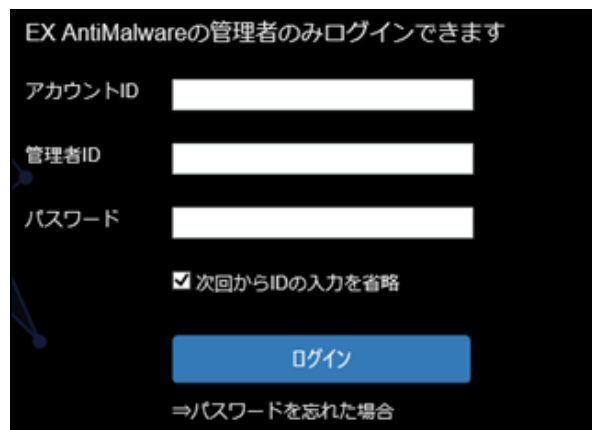
2.1. ログインする

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

<https://exam7.ahkun.jp/akam7>



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。



<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。

<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。



「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。



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。



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(グレースツール)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。

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。

管理者作成数の上限はありません。

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。

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。

The screenshot displays the '管理者情報' (Administrator Information) configuration page. It includes input fields for '管理者ID', '新しいパスワード', 'パスワード確認', '管理者権限', '管理者名', and 'メール'. A list of permissions is shown with red 'X' marks indicating they are disabled. At the bottom, a note reads: '※ 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。'

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。

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。

The screenshot shows the 'ライセンス' (License) page in the EX AntiMalware v7 Manager interface. The page includes a sidebar with navigation options: 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, and ログ. The main content area displays the following information:

- ライセンス: AAEYK-59CR5- [redacted]
- クライアント数: 100 クライアント
- 開始日: 2018-06-01
- 有効期間: 7年 [残り日数: 2119日]
- サーババージョン: V7.0.6.1

At the bottom of the page, there is a note: (株)フーバーブレインが発行した正規ライセンスキーをご使用ください。ライセンスキーをすべて半角で正しく入力してください。(大文字/小文字を識別します。) ライセンスキーの未設定やライセ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。 There are '設定を保存' (Save Settings) buttons next to the license key and the note.

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の保存期間	<p>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す。</p> <p>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。</p>
メール設定	<p>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。</p>

<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。

The screenshot displays the '環境設定' (Environment Settings) page in the EX AntiMalware v7 Manager interface. The left sidebar contains navigation links for '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', and 'ログ'. The main content area is titled '編集設定' (Edit Settings) and includes a '設定を保存' (Save Settings) button. The settings are organized into sections: '検知されたディレクトリ情報の保存期間' (Retention period for detected directory information) with a dropdown set to '6ヶ月'; 'メール設定' (Email Settings) with fields for '送信元アドレス', 'SMTPサーバ', 'ポート番号', 'ユーザ名', and 'パスワード'; and radio button options for 'SMTP over SSL', 'STARTTLS', and 'SMTP認証'. The '件名' (Subject) field contains '[EX AntiMalware v7] マルウェア検知報告' and the '本文' (Body) field contains a detailed alert message in Japanese.

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。

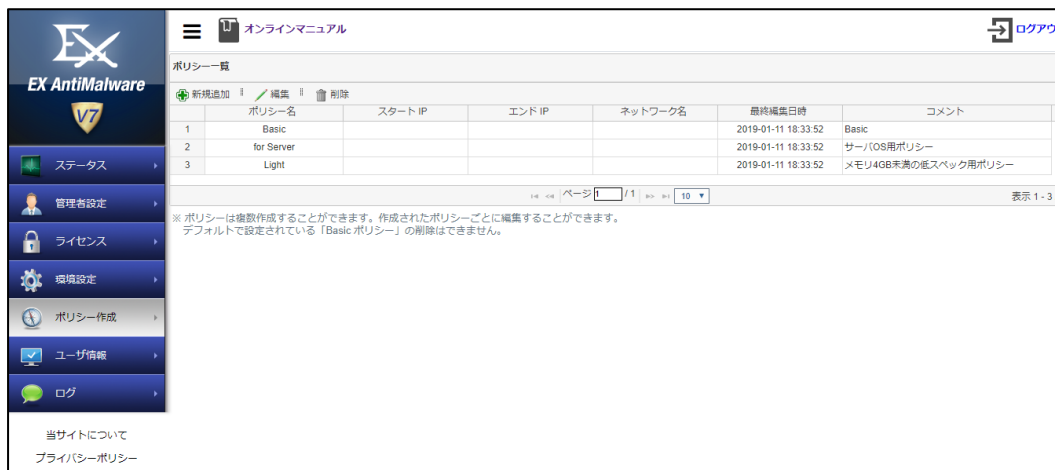
[ポリシー作成]ボタンをクリックします。

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一覧で確認します。

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。

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。

<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。

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」に処理されません。検出時に「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			
<input checked="" type="checkbox"/> バ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)			
<input type="checkbox"/> 結果画面表示			

「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。

「低」に設定するとセキュリティレベルは低くなりますが、スキャン速度は高速になります。

セキュリティレベル	設定内容
高	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なります。

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

エック状態	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 ※1	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。



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。

まず、「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時に自動処理	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「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がシャットダウンされます。
スキャン時に電源OFFの場合、翌日に実行	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。



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

<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。

「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に戻ります。
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。
ユーザ	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。



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 ユーザに設定権限がある場合は、クライアント 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 (推奨)	アプリケーションが実行される前に検知します。 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使用	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メモリ、DVDメディア)挿入時の処理	クライアント PC にリムーバブルディスクを接続したとき、そのリムーバブルディスクをスキャンします。	
	スキャンを行う前に確認ダイアログを表示する	ON にすると自動でスキャン開始はせずに確認ダ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。

	検知時に自動処理	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。
--	----------	--

<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。



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。

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 起動時アップデート」、「周期」、「曜日」、「毎月」の中からアップデートする日時を選択します。	
	PC 起動時アップデート	PC 起動時にプログラムのアップデートを実行します。
	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に詳細情報を表示	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・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/ ポリシー関連アラートを表示	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、任意のクライアント 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同一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。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。

- ◆「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
- ・インターネット一時ファイルの削除
- ・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。



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

- | | |
|-----------------------------------|--|
| <input type="checkbox"/> ウイルス/ワーム | <input type="checkbox"/> トロイの木馬/ハッキングツール |
| <input type="checkbox"/> アドウェア | <input type="checkbox"/> スパイウェア |
| <input type="checkbox"/> ハイジャッカー | <input type="checkbox"/> Hosts ファイル改変マルウェア |
| <input type="checkbox"/> その他 | |

グレートール

- | | |
|---|--|
| <input type="checkbox"/> ファイル交換ソフト(P2P) | <input type="checkbox"/> インスタントメッセンジャー |
| <input type="checkbox"/> ポップアップ広告 | <input type="checkbox"/> 偽セキュリティソフト |
| <input type="checkbox"/> その他 | |

「カテゴリ別処理設定および一括設定」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ト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。

「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。

- | | |
|---------------------------------------|--|
| <input type="checkbox"/> スキャン実行中の中止制御 | <input type="checkbox"/> 除外ボタンの非表示設定 |
| <input type="checkbox"/> 処理実行中の中止制御 | <input type="checkbox"/> ログのみ記録ボタンの非表示設定 |
| <input type="checkbox"/> トレイアイコンの終了制御 | <input type="checkbox"/> リアルタイム監視の終了制御 |
| <input type="checkbox"/> 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」を入力して、[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

<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。



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。

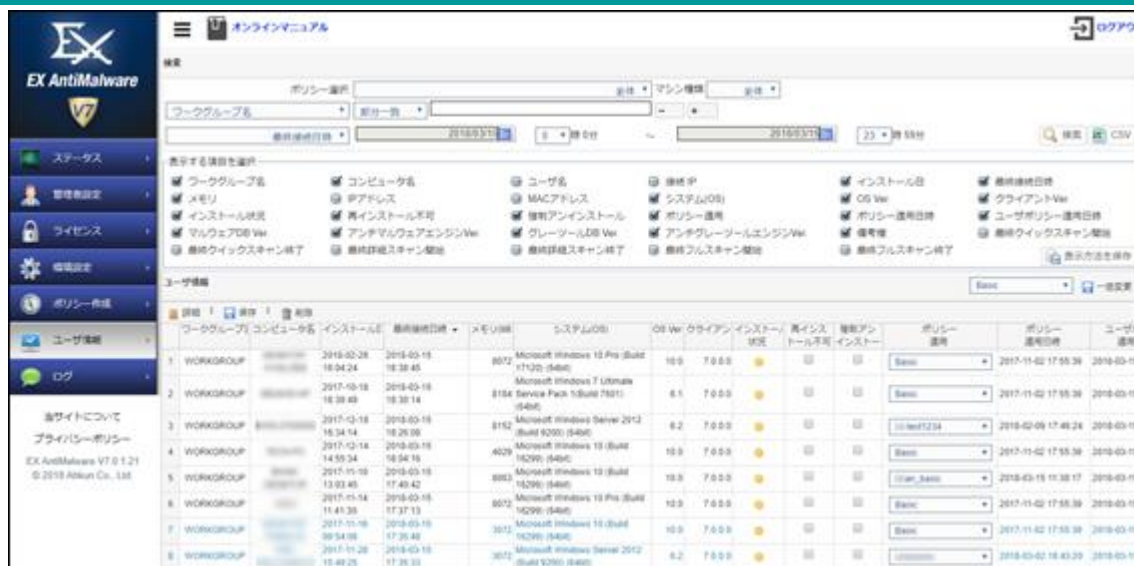
8.2. ユーザ情報を表示する

「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。

各ユーザ情報から下記の設定や確認ができます。

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

	<p>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。</p>						
再インストール不可	<p>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。</p>						
強制アンインストール	<p>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設定です。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。</p>						
ポリシー適用	<p>「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。</p>						
ユーザ情報の削除(アンインストール)	<p>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。</p> <div data-bbox="459 981 1286 1375" data-label="Image"> <p>The screenshot shows the 'User Information' window with the following data:</p> <table border="1"> <thead> <tr> <th>コンピュータ名</th> <th>ユーザ名</th> <th>最終接続日時</th> </tr> </thead> <tbody> <tr> <td>WIN-...</td> <td>Administrator</td> <td>2017-10-06 14:15:20</td> </tr> </tbody> </table> </div>	コンピュータ名	ユーザ名	最終接続日時	WIN-...	Administrator	2017-10-06 14:15:20
コンピュータ名	ユーザ名	最終接続日時					
WIN-...	Administrator	2017-10-06 14:15:20					
アンインストールユーザの確認方法	<p>強制アンインストール、または任意でクライアントプログラムをアンインストールしたユーザを確認する場合は、「アンインストール日」と期間を設定して検索します。</p>						
最終スキャン日時	<p>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。</p>						



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」、「グレースーツール DB バージョン」、「アンチグレース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。



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一覧を確認できます。

「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。

The screenshot shows the 'ユーザー詳細情報' (User Detailed Information) window with the '処理ログ' (Processing Log) tab selected. The log displays a list of detected malware and files with the following columns: 'カテゴリ' (Category), 'マルウェア名' (Malware Name), '処理日' (Processing Date), '処理方法' (Processing Method), and '検知されたディレクトリ' (Detected Directory).

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(P2P)	PP2P.BitSpirit	2018-03-15 11:40:01	処理	h:\bev3.6.0.500.mu.exe
2	ファイル交換ソフト(P2P)	PP2P.Mesh	2018-03-15 11:40:01	処理	h:\マルウェア検体\iMeshV9.exe
3	ファイル交換ソフト(P2P)	PP2P.BitSpirit	2018-03-15 11:40:01	処理	h:\マルウェア検体\bev3.6.0.500.mu.exe
4	ファイル交換ソフト(P2P)	PP2P.Mesh	2018-03-15 11:40:01	処理	h:\MeshV9.exe
5	インスタントメッセージャー	E MSG MirandaM	2018-03-15 11:40:01	処理	h:\マルウェア検体\miranda-im-v0.9.10-unicode.exe
6	インスタントメッセージャー	E MSG MirandaM	2018-03-15 11:40:01	処理	h:\miranda-im-v0.9.10-unicode.exe
7	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 16:17:53	処理	c:\Users\ihari\Desktop\eicar\eicar.com
8	トロイの木馬	K.KLG.natsume	2018-03-14 16:17:37	処理	c:\Users\ihari\Desktop\グレーツール検体\ウイルス検体\natsume.exe
9	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 16:17:37	処理	c:\Users\ihari\Desktop\グレーツール検体\ウイルス検体\eicar.com
10	ファイル交換ソフト(P2P)	PP2P.BitSpirit	2018-03-14 16:17:29	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\bev3.6.0.500.mu.exe
11	ファイル交換ソフト(P2P)	PP2P.Mesh	2018-03-14 16:17:29	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\iMeshV9.exe
12	インスタントメッセージャー	E MSG MirandaM	2018-03-14 16:17:29	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
13	ファイル交換ソフト(P2P)	PP2P.BitTorrent	2018-03-14 16:17:24	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\bittorrent-6.4.exe
14	ファイル交換ソフト(P2P)	PP2P.BitTorrent	2018-03-14 16:00:22	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\bittorrent-6.4.exe
15	ファイル交換ソフト(P2P)	PP2P.BitTorrent	2018-03-14 16:00:22	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\bittorrent-6.4.exe
16	ファイル交換ソフト(P2P)	PP2P.BitSpirit	2018-03-14 16:00:17	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\bev3.6.0.500.mu.exe
17	ファイル交換ソフト(P2P)	PP2P.Mesh	2018-03-14 16:00:14	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\iMeshV9.exe
18	インスタントメッセージャー	E MSG MirandaM	2018-03-14 16:00:11	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
19	インスタントメッセージャー	E MSG MirandaM	2018-03-14 16:00:08	処理	c:\Users\ihari\Desktop\グレーツール検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
20	トロイの木馬	K.KLG.natsume	2018-03-14 16:00:02	処理	c:\Users\ihari\Desktop\グレーツール検体\ウイルス検体\natsume.exe
21	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 15:37:47	処理	c:\Users\ihari\Desktop\グレーツール検体\ウイルス検体\eicar.com
22	トロイの木馬	K.KLG.natsume	2018-03-14 15:37:44	処理	c:\Users\ihari\Desktop\グレーツール検体\ウイルス検体\natsume.exe

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一覧を確認できます。「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。

ユーザ詳細情報					
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	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 14:30:10	ログのみ記録	c:\Users\lhan\Desktop\eicar\eicar.com
2	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 14:30:10	ログのみ記録	c:\Users\lhan\Desktop\グレースール検体\ウイルス検体\eicar.com
3	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 14:30:10	ログのみ記録	h:\bitorrent-6.4.exe
4	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 14:30:10	ログのみ記録	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\bitorrent-6.4.exe
5	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 14:30:10	ログのみ記録	h:\bvs3.6.0.500.mu.exe
6	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 14:30:10	ログのみ記録	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\bvs3.6.0.500.mu.exe
7	インスタントメッセージャー	EMSGMirandaM	2018-03-14 14:30:10	ログのみ記録	h:\miranda-im-v0.9.10-unicode.exe
8	インスタントメッセージャー	EMSGMirandaM	2018-03-14 14:30:10	ログのみ記録	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
9	ファイル交換ソフト(P2P)	PP2PIMesh	2018-03-14 14:30:10	ログのみ記録	h:\MeshV9.exe
10	ファイル交換ソフト(P2P)	PP2PIMesh	2018-03-14 14:30:10	ログのみ記録	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\MeshV9.exe
11	トロイの木馬	K.KLG.natsume	2018-03-14 14:30:10	ログのみ記録	h:\natsume.exe
12	トロイの木馬	K.KLG.natsume	2018-03-14 14:30:10	ログのみ記録	c:\Users\lhan\Desktop\グレースール検体\ウイルス検体\natsume.exe
13	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 14:30:10	ログのみ記録	h:\eicar.com
14	トロイの木馬	K.KLG.natsume	2018-03-14 11:50:11	ログのみ記録	h:\ウイルス検体\natsume.exe
15	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 11:50:11	ログのみ記録	h:\マルウェア検体\bitorrent-6.4.exe
16	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 11:50:11	ログのみ記録	h:\マルウェア検体\bvs3.6.0.500.mu.exe
17	ファイル交換ソフト(P2P)	PP2PIMesh	2018-03-14 11:50:11	ログのみ記録	h:\マルウェア検体\MeshV9.exe
18	インスタントメッセージャー	EMSGMirandaM	2018-03-14 11:50:11	ログのみ記録	h:\マルウェア検体\miranda-im-v0.9.10-unicode.exe
19	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 11:50:11	ログのみ記録	h:\ウイルス検体\eicar.com
20	ランサムウェア	RANSOMWARE	2018-03-07 10:04:55	ログのみ記録	c:\users\lhan\desktop\グレースール検体

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一覧を確認できます。「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。

ユーザ詳細情報					
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(P2P)	PP2PBitTorrent	2018-03-14 14:43:52	除外	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\bitorrent-6.4.exe
2	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 14:43:52	除外	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\bvs3.6.0.500.mu.exe
3	ファイル交換ソフト(P2P)	PP2PIMesh	2018-03-14 14:43:52	除外	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\MeshV9.exe
4	インスタントメッセージャー	EMSGMirandaM	2018-03-14 14:43:52	除外	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
5	トロイの木馬	K.KLG.natsume	2018-03-14 14:43:52	除外	c:\Users\lhan\Desktop\グレースール検体\ウイルス検体\natsume.exe
6	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 14:43:52	除外	c:\Users\lhan\Desktop\グレースール検体\ウイルス検体\eicar.com
7	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-13 12:00:49	除外	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\bitorrent-6.4.exe
8	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-13 11:57:13	除外	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\bitorrent-6.4.exe
9	インスタントメッセージャー	EMSGMirandaM	2018-02-09 12:18:28	除外	c:\Users\lhan\Desktop\グレースール検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
10	インスタントメッセージャー	EMSGMirandaM	2017-11-15 16:36:28	除外	C:\Users\lhan\Desktop\miranda-im-v0.9.10-unicode.exe
11	インスタントメッセージャー	EMSGTrillian	2017-11-15 16:36:28	除外	C:\Users\lhan\Desktop\trillian-v4.2.0.23.exe
12	インスタントメッセージャー	EMSGMirandaM	2017-11-15 16:33:28	除外	c:\Users\lhan\Desktop\miranda-im-v0.9.10-unicode.exe
13	インスタントメッセージャー	EMSGMirandaM	2017-11-15 16:33:25	除外	c:\Users\lhan\Desktop\miranda-im-v0.9.10-unicode.exe
14	インスタントメッセージャー	EMSGTrillian	2017-11-15 16:30:36	除外	c:\Users\lhan\Desktop\trillian-v4.2.0.23.exe
15	インスタントメッセージャー	EMSGTrillian	2017-11-15 16:30:35	除外	c:\Users\lhan\Desktop\trillian-v4.2.0.23.exe
16	ファイル交換ソフト(P2P)	PP2PBitTorrent	2017-11-15 16:23:50	除外	c:\Users\lhan\Desktop\bitorrent-6.4.exe
17	ファイル交換ソフト(P2P)	PP2PBitTorrent	2017-11-15 16:23:50	除外	c:\Users\lhan\Desktop\bitorrent-6.4.exe
18	ファイル交換ソフト(P2P)	PP2PBitTorrent	2017-11-14 15:27:18	除外	c:\Users\lhan\Desktop\eicar\bitorrent-6.4.exe
19	マルウェア	EICAR-Test-File (not a virus)	2017-11-14 12:27:56	除外	c:\Users\lhan\Desktop\eicar\eicar.com
20	マルウェア	EICAR-Test-File (not a virus)	2017-11-14 12:23:12	除外	c:\Users\lhan\Desktop\eicar\eicar.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一覧を確認できます。「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。

ユーザ詳細情報					
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
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	インスタントメッセージャー	E.MSG.MirandaIM	2018-03-14 16:04:20	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\miranda-unicode.exe
2	トロイの木馬	K.KLG.natsume	2018-03-14 16:04:20	キャンセル	c:\Users\hannote\Desktop\デスクツール\ウイルス検体\ウイルス検体\natsume.exe
3	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 16:04:20	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bittorrent
4	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 16:04:20	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bsv3.6
5	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 16:04:20	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\Mesh
6	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 16:04:20	キャンセル	c:\Users\hannote\Desktop\デスクツール\ウイルス検体\ウイルス検体\eicar.com
7	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 15:40:43	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\BitTorrent
8	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 15:38:48	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\BitTorrent
9	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 15:38:46	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bsv3.6
10	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 15:38:46	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bittorrent
11	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 15:38:43	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\Mesh
12	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 15:38:43	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bsv3.6
13	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 15:38:41	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\Mesh
14	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 15:38:41	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\Mesh
15	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 15:38:41	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\Mesh
16	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 15:38:36	キャンセル	c:\Users\hannote\Desktop\デスクツール\ウイルス検体\ウイルス検体\eicar.com
17	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 15:38:12	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\Mesh
18	マルウェア	EICAR-Test-File (not a virus)	2018-03-14 15:34:01	キャンセル	c:\Users\hannote\Desktop\デスクツール\ウイルス検体\ウイルス検体\eicar.com
19	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 15:11:51	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\Mesh
20	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 15:11:51	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bittorrent
21	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 15:11:51	キャンセル	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bsv3.6

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一覧を確認できます。「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。

ユーザ詳細情報					
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
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	インスタントメッセージャー	E.MSG.MirandaIM	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
2	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\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)	PP2PBitMesh	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\VMeshV9.exe
4	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bsv3.6.0.500.mu.exe
5	ファイル交換ソフト(P2P)	PP2PBitSpirit	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bsv3.6.0.500.mu.exe
6	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bittorrent-6.4.exe
7	ファイル交換ソフト(P2P)	PP2PBitTorrent	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\bittorrent-6.4.exe
8	トロイの木馬	K.KLG.natsume	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\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	復旧	c:\Users\hannote\Desktop\デスクツール\ウイルス検体\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	復旧	c:\Users\hannote\Desktop\デスクツール\ウイルス検体\ウイルス検体\eicar.com
11	インスタントメッセージャー	E.MSG.MirandaIM	2018-03-14 16:08:58	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
12	インスタントメッセージャー	E.MSG.MirandaIM	2018-03-14 15:44:23	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\miranda-im-v0.9.10-unicode.exe
13	ファイル交換ソフト(P2P)	PP2PBitMesh	2018-03-14 15:44:23	復旧	c:\Users\hannote\Desktop\デスクツール\マルウェア検体\マルウェア検体\VMeshV9.exe

<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	「マルウェアログ一覧」と「アクセスログ一覧」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. マルウェアログ一覧を表示する

マルウェアログ一覧では各クライアント PC で処理されたマルウェアログ一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。

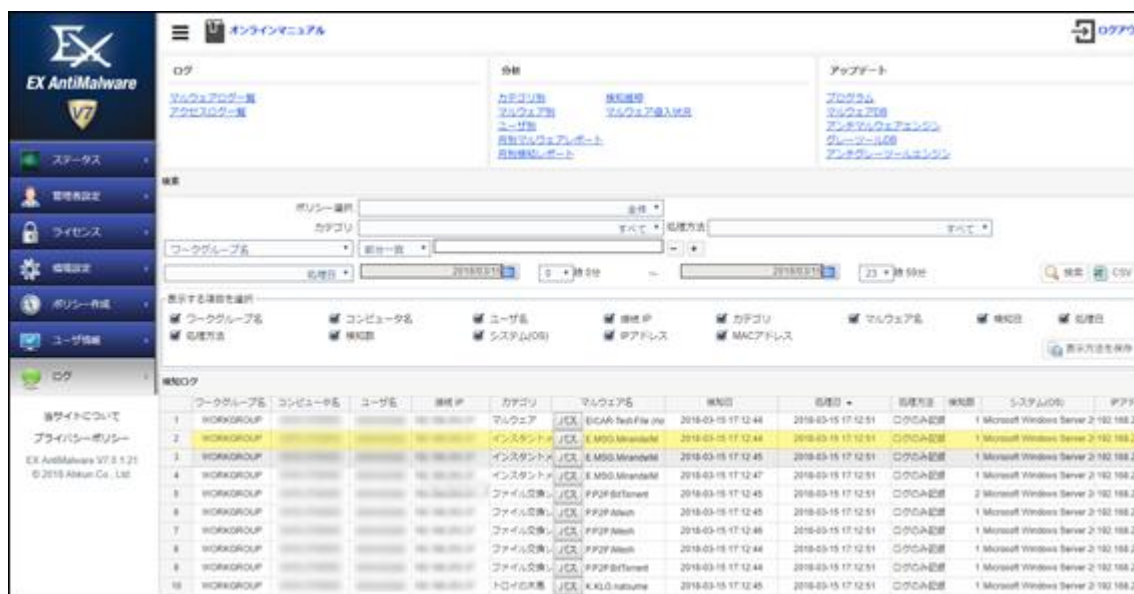
プルダウンメニューから絞り込む項目を選択、または入力項目にキーワードを入力して、**[検索]**ボタンをクリックします。

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むことが可能です。

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。



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。



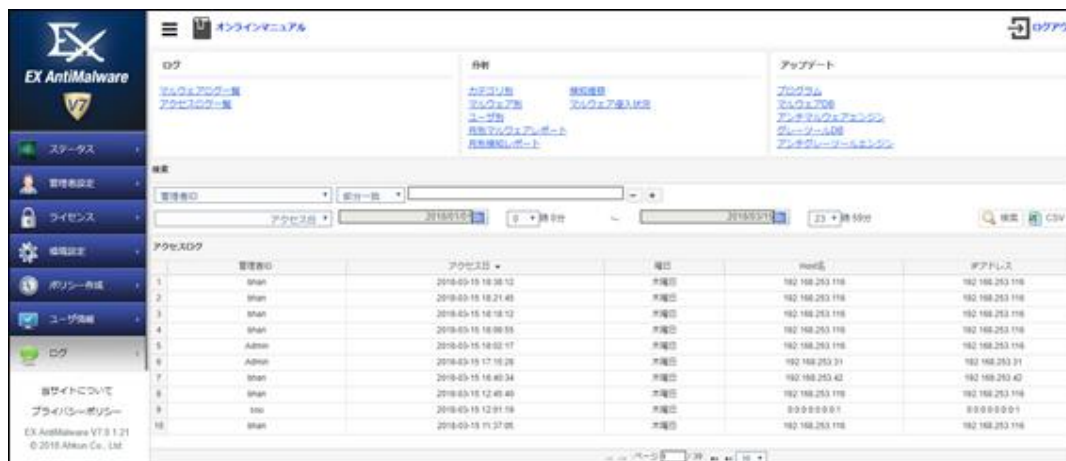
9.3. アクセスログ一覧を表示する

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。



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。



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。

カテゴリー	マルウェア名	コンピュータ数
マルウェア	EX-Test-File (not a virus)	14
ファイルの複製ソフト	PDF Split	14
ファイルの複製ソフト	PDF Merge	7
インストールセッション	EMSG Mhantam	7
ファイルの複製ソフト	PDF Split	7

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。

ユーザ名	コンピュータ名	接続 IP	IP アドレス	検知されたマルウェア数
...	...	192.168.253.88	192.168.253.88	0
...	...	192.168.253.91	192.168.253.91	0
...	...	192.168.253.48	192.168.253.48	0
...	...	192.168.253.37	192.168.253.37	0
...	...	192.168.253.78	192.168.253.78	0
...	...	192.168.240.219	192.168.253.29	2
...	...	192.168.253.918	192.168.253.918	1
...	...	192.168.253.81	192.168.253.81	1
...	...	192.168.253.81	192.168.253.81	1
...	...	192.168.253.84	192.168.253.84	1

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。

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	合計
1 EICAR-Test-File (not a virus)	マルウェア	2018-01-18 18:10:52	2018-05-15 17:12:44	16	4666
2 E-MSG-Malware	インストールメッセージ	2018-01-18 17:07:30	2018-05-15 17:12:47	7	474
3 E-MSG-Skype	インストールメッセージ	2018-01-01 04:57:59	2018-05-15 09:36:13	3	425
4 FPKI-PC-Malware	セキュリティソフト	2018-02-01 18:14:25	2018-05-06 19:30:13	2	34
5 E-MSG-TeamTalk	インストールメッセージ	2018-02-01 18:34:09	2018-02-09 20:13:47	2	30
6 E-MSG-ICQ	インストールメッセージ	2018-03-05 18:46:33	2018-03-08 09:04:42	2	21
7 E-MSG-KanakaTalk	インストールメッセージ	2018-02-01 18:30:06	2018-02-01 18:30:06	1	1
8 E-MSG-CheCase	インストールメッセージ	2018-03-13 17:56:24	2018-05-13 18:16:12	1	2
Application-Bundle-Installation-A	その他	2018-03-12 14:23:28	2018-05-12 18:11:29	1	2
18 AADV-Virus	アドウェア	2018-02-01 18:46:57	2018-02-01 18:46:57	1	1
計 検知されたマルウェア数					7366

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。

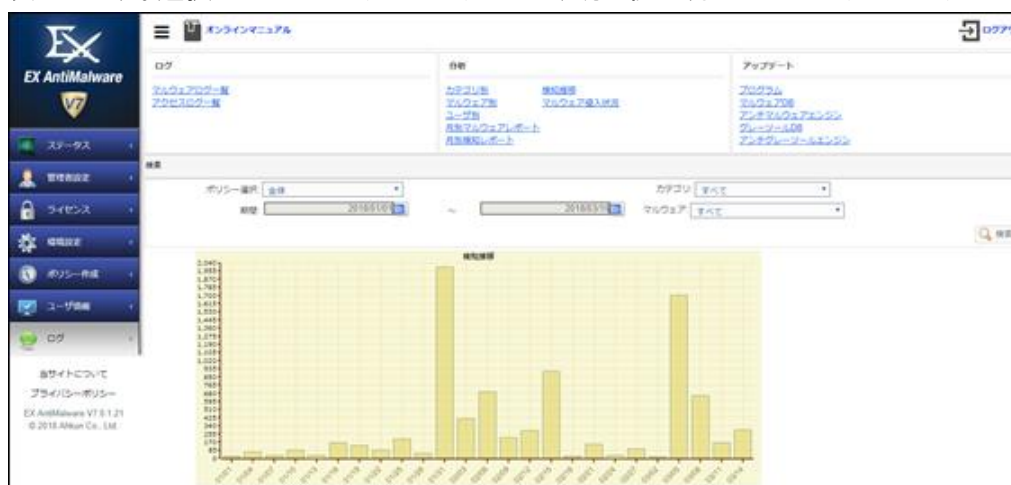
また、[CSV]ボタンをクリックすると、表示した情報を CSV 形式で保存できます。

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。

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
1 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-02-18 18:17:37	マルウェア	EICAR-Test-File (not a virus)
2 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-02-15 17:18:46	マルウェア	EICAR-Test-File (not a virus)
3 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-02-15 17:02:01	マルウェア	EICAR-Test-File (not a virus)
4 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-02-15 17:21:01	マルウェア	EICAR-Test-File (not a virus)
5 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-02-15 17:20:05	マルウェア	EICAR-Test-File (not a virus)
6 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-01-31 13:35:38	マルウェア	EICAR-Test-File (not a virus)
7 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-02-15 17:18:52	マルウェア	EICAR-Test-File (not a virus)
8 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-01-31 13:19:29	マルウェア	EICAR-Test-File (not a virus)
9 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-01-31 14:37:47	マルウェア	EICAR-Test-File (not a virus)
10 WORKGROUP	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	192.168.1.100	192.168.1.100	2018-02-07 18:46:06	マルウェア	EICAR-Test-File (not a virus)
計 検知されたマルウェア数						10

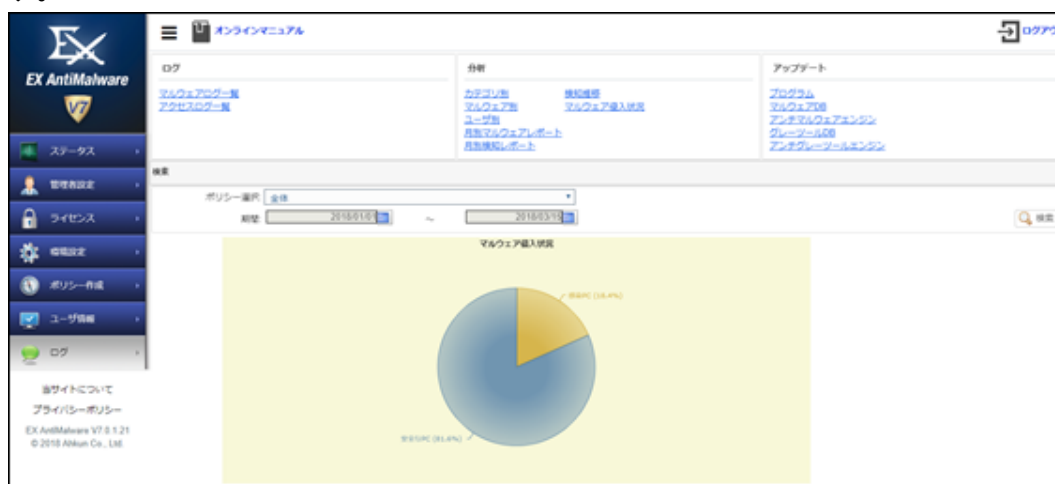
9.9. 検知推移分析

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。



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。

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。
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。
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す。



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。

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。

<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○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】	
バックグラウンドスキャンの設定	
バ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)	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
結果画面表示	<input type="checkbox"/> Y <input type="checkbox"/> N
セキュリティ設定	<input type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input type="checkbox"/> 低
スキャン速度の設定	<input type="checkbox"/> 高速 <input checked="" type="checkbox"/> 標準 <input type="checkbox"/> 低速
その他	
グレーツールの検知時にチェック状態	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
右クリックスキャン	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
圧縮ファイルスキャン	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
スキャン上限サイズ	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
	0
	<input checked="" type="checkbox"/> MB <input type="checkbox"/> GB
スタートページの設定	
確認ダイアログを表示	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
スタートページとして使用する URL :	

【スケジュール】	
フルスキャンスケジュール	<input type="checkbox"/> 設定しない <input type="checkbox"/> 周期:()日 <input type="checkbox"/> 曜日:()曜日 <input checked="" type="checkbox"/> 毎月:(8)日 <input checked="" type="checkbox"/> スキャン開始時間:(12) 時 (00)分 <input type="checkbox"/> スケジュールスキャン時に自動処理 <input checked="" type="checkbox"/> 処理後にプログラム終了 <input type="checkbox"/> 処理後にシステム終了 <input type="checkbox"/> 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	<input type="checkbox"/> 設定しない <input checked="" type="checkbox"/> 周期:(1)日 <input type="checkbox"/> 曜日:()曜日 <input type="checkbox"/> 毎月:()日 <input checked="" type="checkbox"/> スキャン開始時間:(12) 時 (00)分 <input type="checkbox"/> スケジュールスキャン時に自動処理 <input checked="" type="checkbox"/> 処理後にプログラム終了 <input type="checkbox"/> 処理後にシステム終了 <input type="checkbox"/> 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	<input checked="" type="checkbox"/> 基本実行モード(推奨) <input type="checkbox"/> 最小実行モード
管理モード	<input checked="" type="checkbox"/> 管理者 <input type="checkbox"/> 管理者(GUI 非表示) <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
監視モード	<input type="checkbox"/> 軽快 <input checked="" type="checkbox"/> 標準(推奨) <input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input checked="" type="checkbox"/> スキャンを行う前に確認ダイアログを表示する <input type="checkbox"/> 検知時に自動処理
【アップデート】	
アップデートの設定	<input checked="" type="checkbox"/> 自動アップデート <input type="checkbox"/> 手動アップデート <input type="checkbox"/> スケジュールアップデート <input checked="" type="checkbox"/> PC 起動時アップデート
	<input type="checkbox"/> 周期:()日 <input type="checkbox"/> 曜日:()曜日 <input type="checkbox"/> 毎月:()日
	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
アップデート/ ポリシー関連アラートを表示	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N

スマートアップデートを使用	<input checked="" type="checkbox"/> Y <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
インターネット一時ファイルの削除	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
Cookie の削除	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
インターネット/オートコンプリート履歴を削除	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
最近使用したドキュメントのリストを削除	<input checked="" type="checkbox"/> Y <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
指定日数後に削除(クリア)する	<input type="checkbox"/> Y: (14)日 <input checked="" type="checkbox"/> 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	<input type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ウイルス/ワーム	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
アドウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ハイジャッカー	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
トロイの木馬/ハッキングツール	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
スパイウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
Hosts ファイル変更マルウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
その他	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
グレーツール:一括設定	<input type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ファイル交換ソフト(P2P)	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
インスタントメッセージ	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ポップアップ広告	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録

偽セキュリティソフト	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
その他	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> 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	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
処理実行中の中止制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
トレイアイコンの終了制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
処理ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
除外ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
ログのみ記録ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
リアルタイム監視の終了制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
除外設定	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
オプション	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
アンインストール	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
隔離	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> 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	<input type="checkbox"/> 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○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】	
バックグラウンドスキャンの設定	
バ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)	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
結果画面表示	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
セキュリティ設定	<input type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input type="checkbox"/> 低
スキャン速度の設定	<input type="checkbox"/> 高速 <input checked="" type="checkbox"/> 標準 <input type="checkbox"/> 低速
その他	
グレーツールの検知時にチェック状態	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
右クリックスキャン	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
圧縮ファイルスキャン	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
スキャン上限サイズ	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
	0
	<input checked="" type="checkbox"/> MB <input type="checkbox"/> GB
スタートページの設定	
確認ダイアログを表示	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
スタートページとして使用する URL :	
【スケジュール】	
フルスキャンスケジュール	<input type="checkbox"/> 設定しない <input type="checkbox"/> 周期:()日 <input type="checkbox"/> 曜日:()曜日 <input checked="" type="checkbox"/> 毎月:(8)日 <input checked="" type="checkbox"/> スキャン開始時間:(2)時(00)分 <input checked="" type="checkbox"/> スケジュールスキャン時に自動処理 <input checked="" type="checkbox"/> 処理後にプログラム終了 <input type="checkbox"/> 処理後にシステム終了 <input type="checkbox"/> スキャン時に電源 OFF の場合、翌日に実行
	<input type="checkbox"/> 設定しない <input checked="" type="checkbox"/> 周期:(1)日 <input type="checkbox"/> 曜日:()曜日 <input type="checkbox"/> 毎月:()日 <input checked="" type="checkbox"/> スキャン開始時間:(2)時(00)分 <input checked="" type="checkbox"/> スケジュールスキャン時に自動処理 <input checked="" type="checkbox"/> 処理後にプログラム終了 <input type="checkbox"/> 処理後にシステム終了 <input type="checkbox"/> 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	<input type="checkbox"/> 設定しない <input checked="" type="checkbox"/> 周期:(1)日 <input type="checkbox"/> 曜日:()曜日 <input type="checkbox"/> 毎月:()日 <input checked="" type="checkbox"/> スキャン開始時間:(2)時(00)分 <input checked="" type="checkbox"/> スケジュールスキャン時に自動処理 <input checked="" type="checkbox"/> 処理後にプログラム終了 <input type="checkbox"/> 処理後にシステム終了 <input type="checkbox"/> 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	<input checked="" type="checkbox"/> 基本実行モード(推奨) <input type="checkbox"/> 最小実行モード
管理モード	<input checked="" type="checkbox"/> 管理者 <input type="checkbox"/> 管理者(GUI非表示) <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
監視モード	<input type="checkbox"/> 軽快 <input checked="" type="checkbox"/> 標準(推奨) <input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> スキャンを行う前に確認ダイアログを表示する <input checked="" type="checkbox"/> 検知時に自動処理
【アップデート】	
アップデートの設定	<input checked="" type="checkbox"/> 自動アップデート <input type="checkbox"/> 手動アップデート <input type="checkbox"/> スケジュールアップデート
	<input checked="" type="checkbox"/> PC 起動時アップデート
	<input type="checkbox"/> 周期:()日 <input type="checkbox"/> 曜日:()曜日 <input type="checkbox"/> 毎月:()日 <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
アップデート/ ポリシー関連アラートを表示	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
スマートアップデートを使用	<input checked="" type="checkbox"/> Y <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
インターネット一時ファイルの削除	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
Cookie の削除	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
インターネット/オートコンプリート履歴を削除	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
最近使用したドキュメントのリストを削除	<input checked="" type="checkbox"/> Y <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
指定日数後に削除(クリア)する	<input type="checkbox"/> Y: (14)日 <input checked="" type="checkbox"/> 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	<input type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ウイルス/ワーム	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
アドウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ハイジャッカー	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録

トロイの木馬/ハッキングツール	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
スパイウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
Hosts ファイル変更マルウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
その他	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
グレーツール:一括設定	<input type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ファイル交換ソフト(P2P)	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N <input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
インスタントメッセージ	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N <input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ポップアップ広告	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N <input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
偽セキュリティソフト	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N <input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
その他	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N <input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> 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	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
処理実行中の中止制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
トレイアイコンの終了制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
処理ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
除外ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
ログのみ記録ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
リアルタイム監視の終了制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
除外設定	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
オプション	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
アンインストール	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
隔離	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> 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	
	<input type="checkbox"/> 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○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】	
バックグラウンドスキャンの設定	
バ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)	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
結果画面表示	<input type="checkbox"/> Y <input type="checkbox"/> N
セキュリティ設定	<input type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input type="checkbox"/> 低
スキャン速度の設定	<input type="checkbox"/> 高速 <input type="checkbox"/> 標準 <input checked="" type="checkbox"/> 低速
その他	
グレーツールの検知時にチェック状態	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
右クリックスキャン	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
圧縮ファイルスキャン	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
スキャン上限サイズ	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
	0
	<input checked="" type="checkbox"/> MB <input type="checkbox"/> GB
スタートページの設定	
確認ダイアログを表示	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
スタートページとして使用する URL :	
【スケジュール】	
フルスキャンスケジュール	<input type="checkbox"/> 設定しない
	<input type="checkbox"/> 周期:()日 <input type="checkbox"/> 曜日:()曜日 <input checked="" type="checkbox"/> 毎月:(8)日
	<input checked="" type="checkbox"/> スキャン開始時間:(12) 時 (00)分
	<input type="checkbox"/> スケジュールスキャン時に自動処理

	<input checked="" type="checkbox"/> 処理後にプログラム終了 <input type="checkbox"/> 処理後にシステム終了 <input type="checkbox"/> 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	<input type="checkbox"/> 設定しない <input checked="" type="checkbox"/> 周期:(1)日 <input type="checkbox"/> 曜日:()曜日 <input type="checkbox"/> 毎月:()日 <input checked="" type="checkbox"/> スキャン開始時間:(12) 時 (00)分 <input type="checkbox"/> スケジュールスキャン時に自動処理 <input checked="" type="checkbox"/> 処理後にプログラム終了 <input type="checkbox"/> 処理後にシステム終了 <input type="checkbox"/> 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	<input checked="" type="checkbox"/> 基本実行モード(推奨) <input type="checkbox"/> 最小実行モード
管理モード	<input checked="" type="checkbox"/> 管理者 <input type="checkbox"/> 管理者(GUI 非表示) <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
監視モード	<input checked="" type="checkbox"/> 軽快 <input type="checkbox"/> 標準(推奨) <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> スキャンを行う前に確認ダイアログを表示する <input type="checkbox"/> 検知時に自動処理
【アップデート】	
アップデートの設定	<input checked="" type="checkbox"/> 自動アップデート <input type="checkbox"/> 手動アップデート <input type="checkbox"/> スケジュールアップデート <input checked="" type="checkbox"/> PC 起動時アップデート <input type="checkbox"/> 周期:()日 <input type="checkbox"/> 曜日:()曜日 <input type="checkbox"/> 毎月:()日 <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
アップデート/ ポリシー関連アラートを表示	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
スマートアップデートを使用	<input checked="" type="checkbox"/> Y <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N

インターネット一時ファイルの削除	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
Cookie の削除	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
インターネット/オートコンプリート履歴を削除	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
最近使用したドキュメントのリストを削除	<input checked="" type="checkbox"/> Y <input type="checkbox"/> 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	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
指定日数後に削除(クリア)する	<input type="checkbox"/> Y: (14)日 <input checked="" type="checkbox"/> 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	<input type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ウイルス/ワーム	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
アドウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ハイジャッカー	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
トロイの木馬/ハッキングツール	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
スパイウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
Hosts ファイル変更マルウェア	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
その他	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input type="checkbox"/> ユーザ選択 <input checked="" type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
グレーツール:一括設定	<input type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ファイル交換ソフト(P2P)	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
インスタントメッセージ	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
ポップアップ広告	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
偽セキュリティソフト	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> ログのみ記録
その他	<input checked="" type="checkbox"/> Y <input type="checkbox"/> N
	<input checked="" type="checkbox"/> ユーザ選択 <input type="checkbox"/> 隔離 <input type="checkbox"/> 除外 <input type="checkbox"/> 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	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N

処理実行中の中止制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
トレイアイコンの終了制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
処理ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
除外ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
ログのみ記録ボタンの非表示設定	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
リアルタイム監視の終了制御	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N
除外設定	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
オプション	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
アンインストール	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> パスワード設定()
隔離	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 無効化 <input type="checkbox"/> 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	<input type="checkbox"/> Windows の System プロセスを除外する