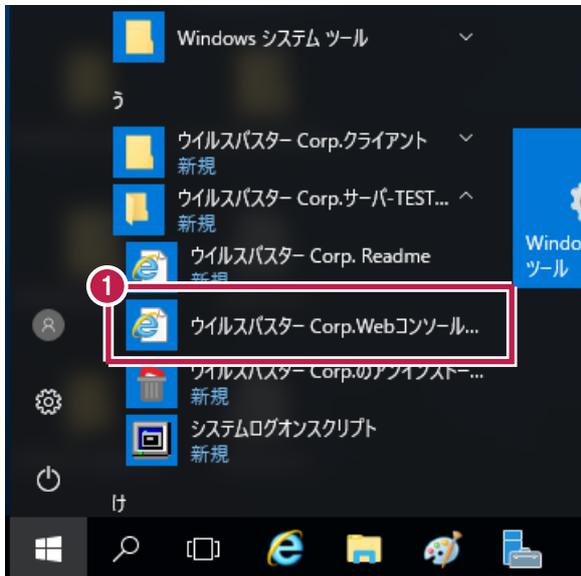


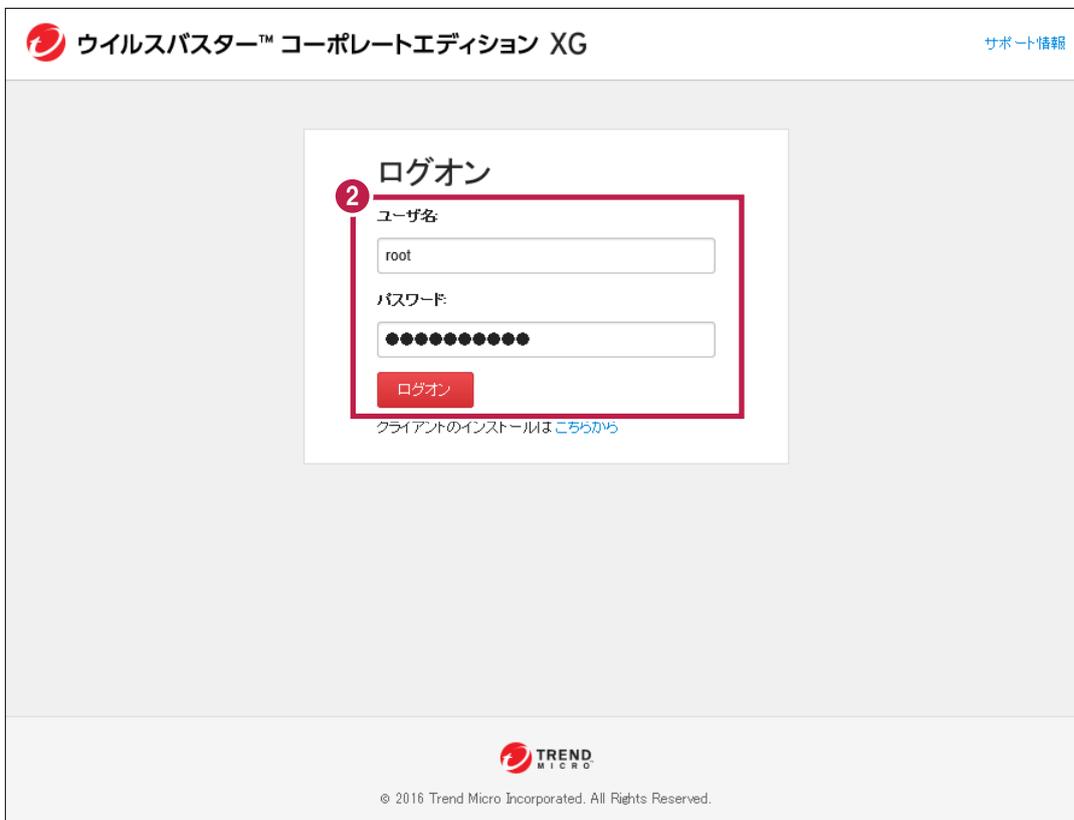
ウイルスバスター コーポレートエディション（サーバーの除外設定）

- 1 Windowsスタートメニューから [ウイルスバスター Corp.Webコンソール (HTML)] をクリックします。

【スタートメニュー】

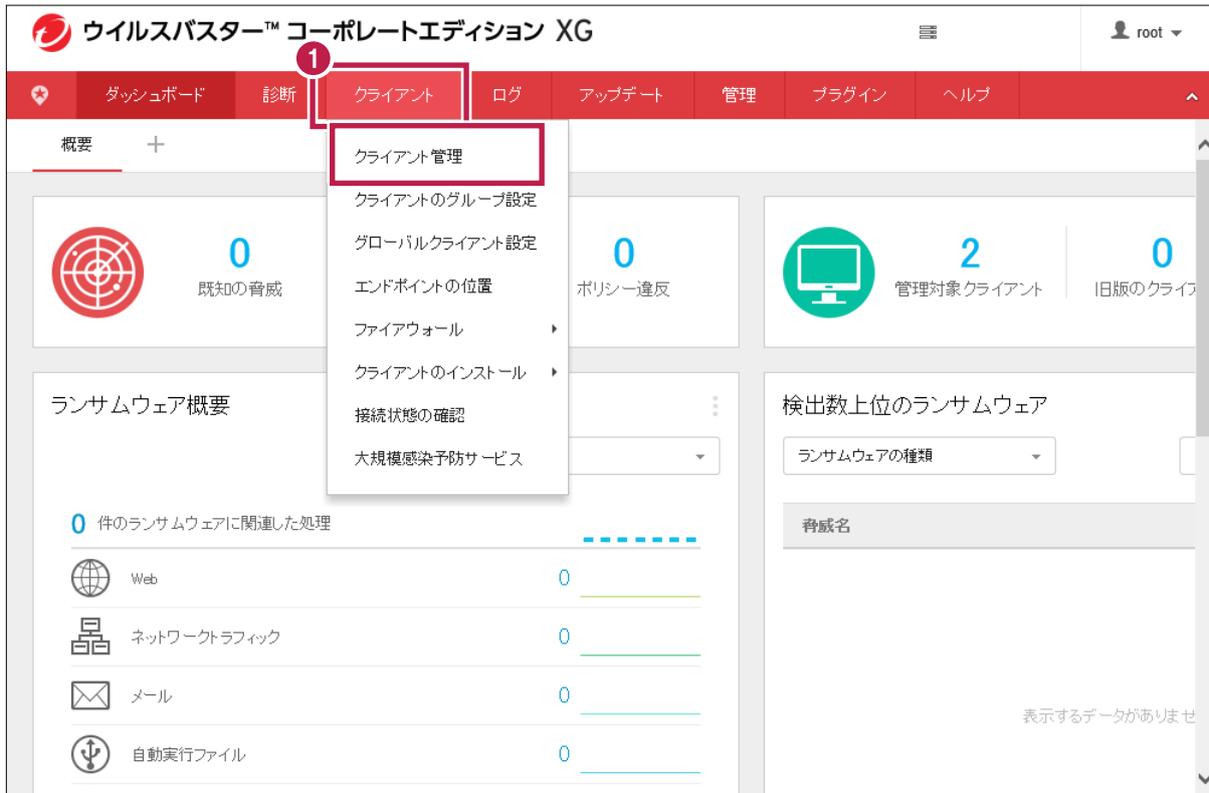


- 2 システム管理者の方がユーザー名とパスワードを入力して、[ログオン] をクリックします。

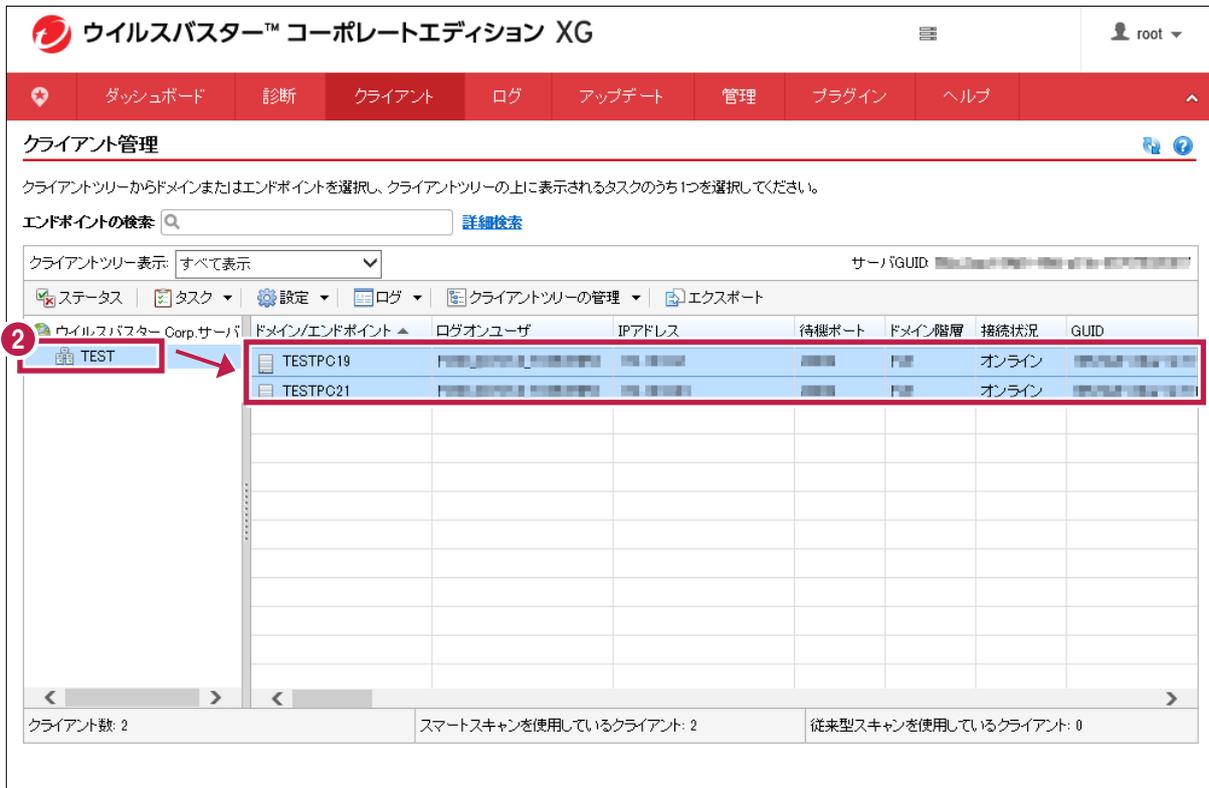


① リアルタイム検索の除外設定

1 [クライアント] - [クライアント管理] をクリックします。



2 除外設定するコンピュータを選択します。(Shift・Ctrlキーで複数選択可)



3 [設定] - [検索設定] - [リアルタイム検索設定] をクリックします。

ウイルスバスター™ コーポレートエディション XG

クライアント管理

クライアントツリーからドメインまたはエンドポイントを選択し、クライアントツリーの上に表示されるタスクのうち1つを選択してください。

エンドポイントの検索 [詳細検索](#)

クライアントツリー表示: **すべて** 3 サーバGUID:

ステータス | タスク | **設定** | ログ | クライアントツリーの管理 | エクスポート

検索方法	待機ポート	ドメイン階層	接続状況	GUID
Webシミュレーション設定	手動検索設定		オンライン	
機械学習型検索設定	リアルタイム検索設定		オンライン	
不審接続監視設定	予約検索設定			
挙動監視設定	ScanNow設定			
デバイスコントロール設定				
サンプル送信				
アップデートエージェント設定				
権限とその他の設定				
追加サービス設定				
スパイウェア/グレーウェアの承認済みリスト				
信頼済みプログラムリスト				

クライアント数: 2 用いているクライアント: 2 従来型スキャンを使用しているクライアント: 0

4 [ウイルス/不正プログラム検索を有効にする] がONであることを確認し、[検索除外] タブをクリックします。

リアルタイム検索設定

ウイルス/不正プログラム検索を有効にする

スパイウェア/グレーウェア検索を有効にする

対象 処理 **検索除外**

ファイルに対するユーザのアクティビティ

次のファイルを検索する: [作成中/変更中および取得中のファイル]

検索対象ファイル

検索可能なすべてのファイル

トレンドマイクロの推奨設定で検索されたファイルタイプ

対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください)

[".ACCDB,ACE,AMG,ARJ,BAT,BIN,BOO,BOX,BZ2,CAB,CDR,CDT,CHM,CLA,CLASS,COM,OPT,OSG,DLL,DOC,DOCM,DOCX,DOT,DTM,DOTX,DRV,DVB,DWG,DWT,EML,EPOC,EXE,GMS,GZ,HLP,HTA,HTM,HTML,HTT,INL,JAR,JPEG,JPG,JS,JSB,JTD,JTT,LNK,LZH,MD,B,MPD,MPP,MPT,MSG,MSI,MSO,MST,NWS,OBD,OCX,OFT,OVL,PDF,PHP,PIF,PL,P.M,PO,T,POTM,POTX,PPAM,PPS,PPSM,PPSX,PPT,PPTM,PPTX,PRG,QPW,RAR,REG,RTF,SCR,

検索設定

シャットダウン時にフロッピーディスクを検索

ネットワークドライブの検索

挿入後にUSBストレージデバイスのシステム領域を検索

リムーバブルストレージデバイスの接続後、その中のすべてのファイルを検索

メモリから検出された不正プログラムの変種を隔離

保存 キャンセル

5 [検索除外を有効にする] がONであることを確認します。

6 弊社製品がインストールされているフォルダパス「C:¥FCAPP」を入力します。
(Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。)
※参照ツリーなどは表示されないの、手入力する必要があります。
※指定したフォルダーのサブフォルダーも除外対象となります。

7 [+] ボタンをクリックします。

リアルタイム検索設定

ウイルス/不正プログラム検索を有効にする
 スパイウェア/グレーウェア検索を有効にする

対象 処理 **検索除外**

検索除外

検索除外を有効にする
 すべての検索タイプに検索除外設定を適用する

検索除外リスト (ディレクトリ)

ディレクトリパスを入力してください (例: C:\temp\ExcludeDir)。

トレンドマイクロ製品がインストールされているディレクトリの除外

C:¥FCAPP

+
-

検索除外リスト (ファイル)

ファイル名またはファイルのフルパスを入力してください (例: ExcludeDoc.hlp, C:\temp\excl\dir\ExcludeDoc.hlp)。

+
-

保存 キャンセル

8 下部のリストに、フォルダパスが追加されたことを確認します。

リアルタイム検索設定

ウイルス/不正プログラム検索を有効にする
 スパイウェア/グレーウェア検索を有効にする

対象 処理 **検索除外**

検索除外

検索除外を有効にする
 すべての検索タイプに検索除外設定を適用する

検索除外リスト (ディレクトリ)

ディレクトリパスを入力してください (例: C:\temp\ExcludeDir)。

トレンドマイクロ製品がインストールされているディレクトリの除外

C:¥FCAPP

+
-

検索除外リスト (ファイル)

ファイル名またはファイルのフルパスを入力してください (例: ExcludeDoc.hlp, C:\temp\excl\dir\ExcludeDoc.hlp)。

+
-

保存 キャンセル

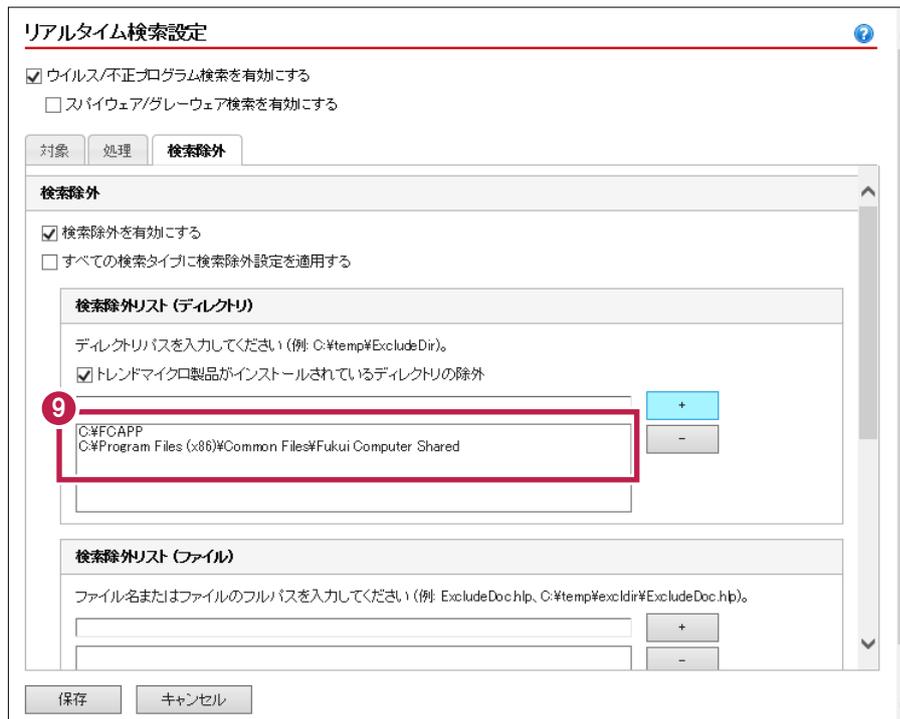
9

以下のフォルダーが存在する場合は、同様な手順で、それぞれリストに追加してください。

※存在しない場合は追加不要です。

・32 ビットOS の場合「C:¥Program Files ¥Common Files¥Fukui Computer Shared」

・64 ビットOS の場合「C:¥Program Files (x86)¥Common Files¥Fukui Computer Shared」



10

追加が終わったら、[保存] をクリックします。



11 [閉じる] をクリックします。



■ ② 手動検索／予約検索の除外設定

- 1 [設定] - [検索設定] - [手動検索設定] または [予約検索設定] をクリックして設定してください。
※設定方法は、前述の「①リアルタイム検索の除外設定」と同様です。



③ 挙動監視の除外設定

- 1 [設定] - [挙動監視設定] をクリックします。

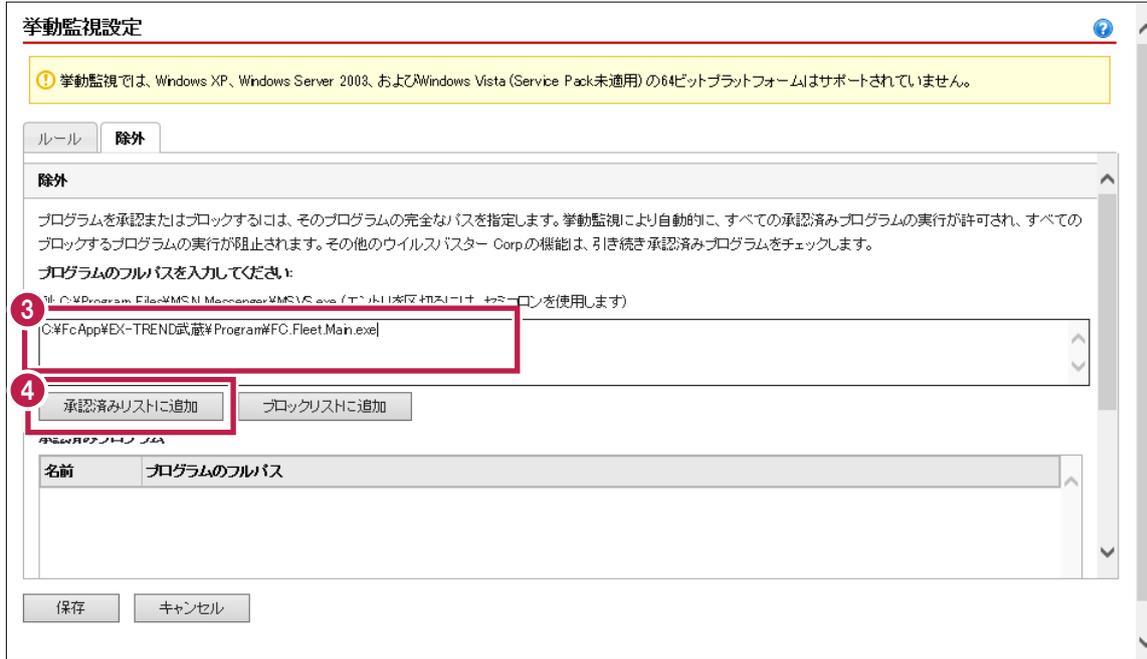
The screenshot shows the VirusBuster Corporate Edition XG web interface. At the top, there is a navigation bar with tabs for 'ダッシュボード', '診断', 'クライアント', 'ログ', 'アップデート', '管理', 'プラグイン', and 'ヘルプ'. Below this is the 'クライアント管理' (Client Management) section. A search bar for 'エンドポイントの検索' is present. A dropdown menu for 'クライアントツリー表示' is set to 'すべて'. A red circle with the number '1' highlights the '設定' (Settings) icon in the top navigation bar. A red box highlights the '挙動監視設定' (Behavior Monitoring Settings) option in the settings dropdown menu. The main area shows a table of clients with columns for IP address, port, domain, connection status, and GUID.

- 2 [不正プログラム挙動ブロックを有効にする] がONであることを確認して、[除外] タブをクリックします。

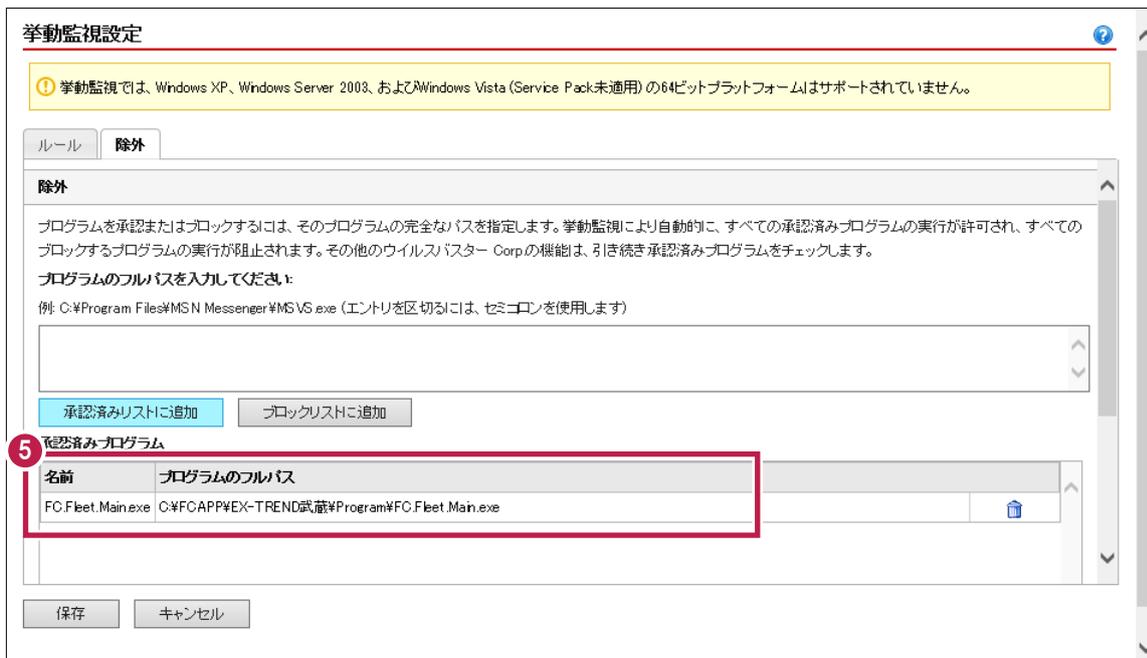
The screenshot shows the '挙動監視設定' (Behavior Monitoring Settings) dialog box. A yellow warning message at the top states: '挙動監視では、Windows XP、Windows Server 2003、およびWindows Vista (Service Pack未適用) の64ビットプラットフォームはサポートされていません。' (Behavior monitoring does not support 64-bit platforms for Windows XP, Windows Server 2003, and Windows Vista (Service Pack not applied)). Below this, the 'ルール' (Rules) section has the '除外' (Exclusion) tab selected. Under the '不正プログラム挙動ブロック' (Block malicious program behavior) section, the checkbox '不正プログラム挙動ブロックを有効にする' (Enable blocking of malicious program behavior) is checked. Below this, there are options for 'ブロックする脅威' (Block threats) and 'ランサムウェア対策' (Ransomware protection). The 'ランサムウェア対策' section includes checkboxes for '不正な暗号化や変更から文書を保護' (Protect documents from unauthorized encryption or modification) and 'プログラム検査を有効にして不正な実行可能ファイルを検出およびブロック' (Enable program scanning to detect and block unauthorized executable files). At the bottom, there is a checkbox for 'HTTPまたはメールアプリケーションを介してダウンロードされた新たなプログラムを監視する' (Monitor newly downloaded programs via HTTP or email applications) and buttons for '保存' (Save) and 'キャンセル' (Cancel).

- 3 ボックスに「C:¥FCAPP」フォルダー内のexeファイルのパスを手入力します。
 例：C:¥FcApp¥EX-TREND武蔵¥Program¥FC.Fleet.Main.exe
 （Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。）
 ※その他の除外設定するexeファイルは、P.10を参照してください。

- 4 [承認済みリストに追加] をクリックします。

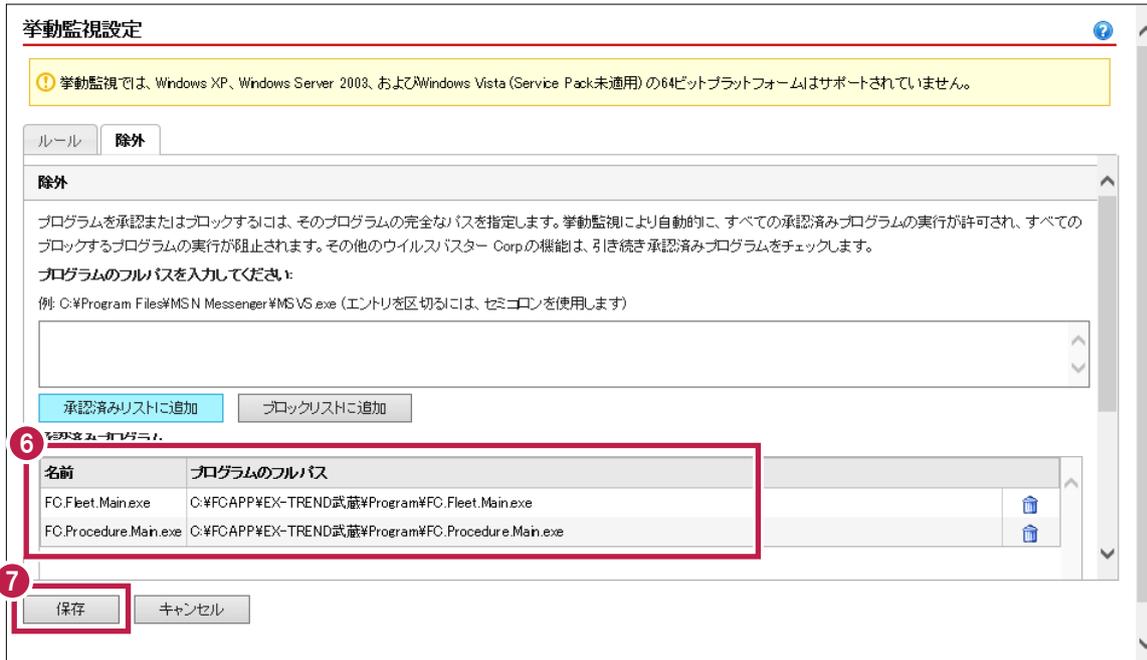


- 5 [承認済みプログラムリスト] に追加されたことを確認します。



6 同様な手順で、必要なファイルをすべてリストに追加してください。
※半角セミコロン（ ; ）で区切ることで、複数のパスを入力可能です。

7 追加が終わったら、[保存] をクリックします。



8 [閉じる] をクリックします。



EX-TREND 武蔵に関して除外設定をおすすめする EXE ファイル一覧

(ウイルスとして誤認識された場合に、除外設定の参考にしてください。)

EX-TREND 武蔵			
No	EXE ファイルが存在するフォルダパス	EXE ファイル名	関係するプログラム
1	C:¥FCAPP¥EX-TREND 武蔵¥Program	FC.Fleet.Main.exe	インデックス
2		FC.Procedure.Main.exe	施工計画書作成支援
3		CCad.exe	建設 CAD
4		FC.Scheduler.exe	工程管理
5		FC.CsManager.exe	原価工程管理
6		ExPhoto.exe	写真管理
7		ExAlbum.exe	アルバム編集
8		ExDeki.exe	出来形管理
9		ExPave.exe	舗装出来形管理
10		ExQual.exe	アスファルト温度管理
11			コンクリート品質管理
12		TrndEnou.exe	電子納品ツール
13	C:¥FCAPP¥FCNCLCenter	FCNCLCenter.exe	ネット認証ライセンスセンター
14	C:¥FCAPP¥FCAccountDesktop	FCAccountDesktop.exe	FC アカウントデスクトップアプリ

※Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。

※弊社の他プログラムでも、ウイルスとして誤認識される場合があります。

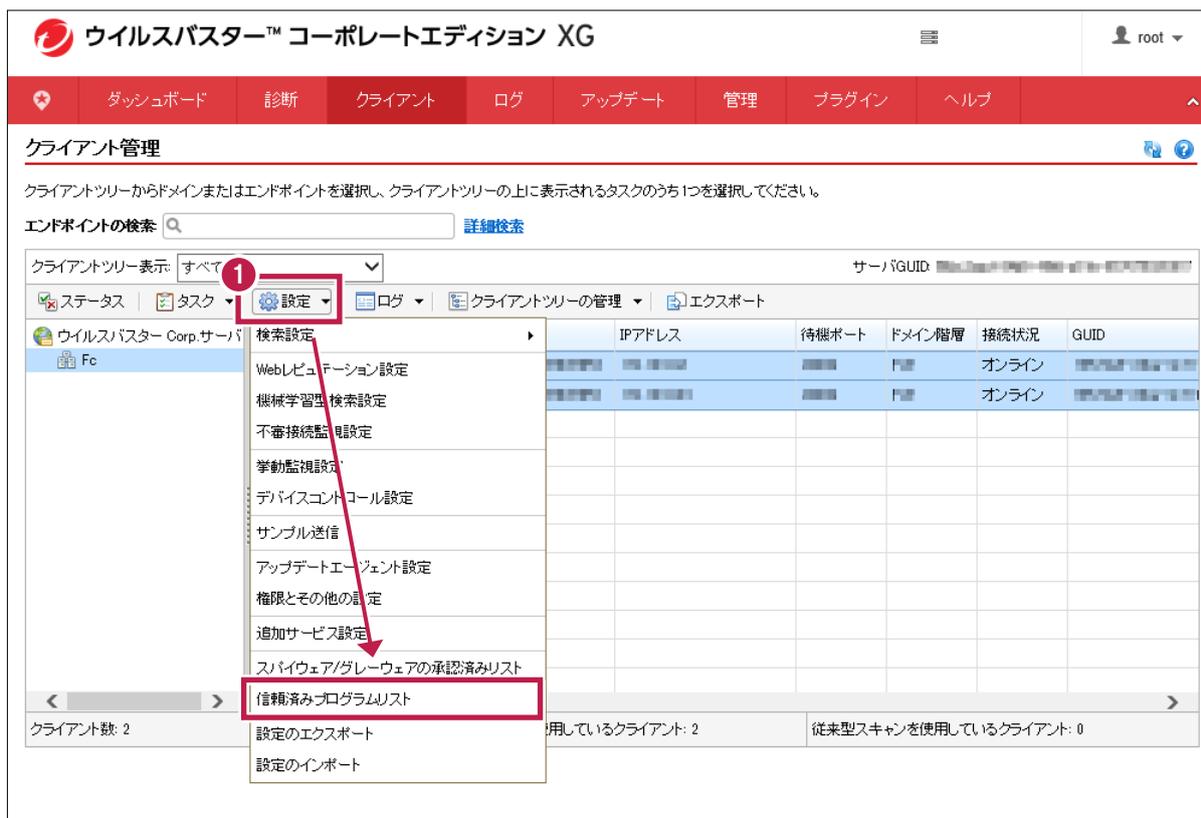
その時は各プログラム (program) フォルダ内の誤認識された EXE ファイルを除外設定して下さい。

例)

- ・TREND-ONE の場合 「C:¥FCAPP¥TREND-ONE¥Program」フォルダ以下の EXE ファイル
- ・BTXA の場合 「C:¥FCAPP¥BTXA¥Program」フォルダ以下の EXE ファイル

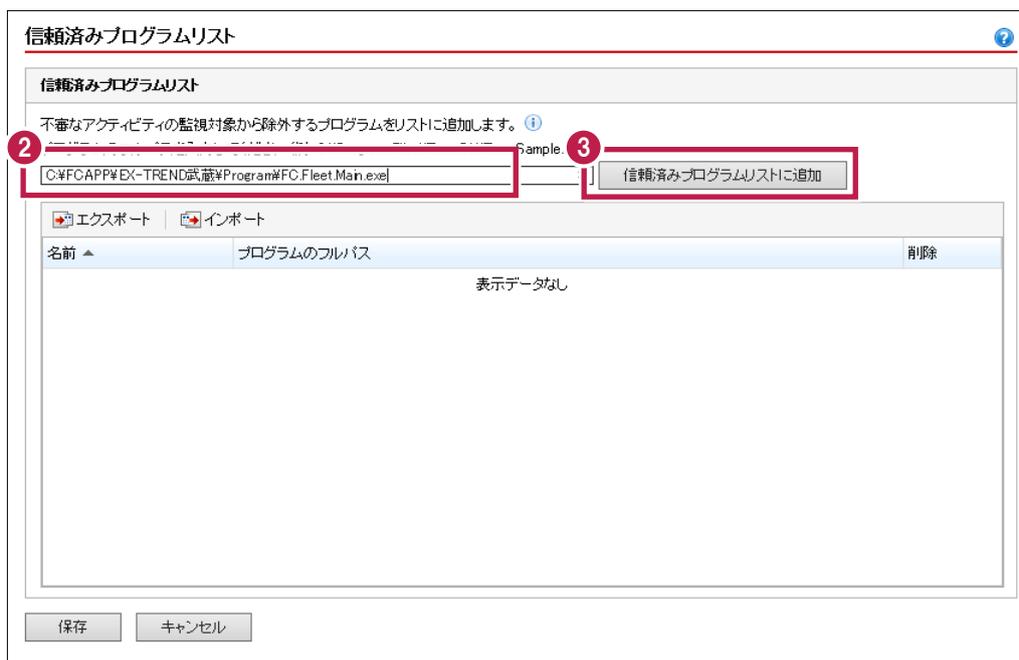
④ 信頼済みプログラムに追加

- 1 [設定] - [信頼済みプログラムリスト] をクリックします。

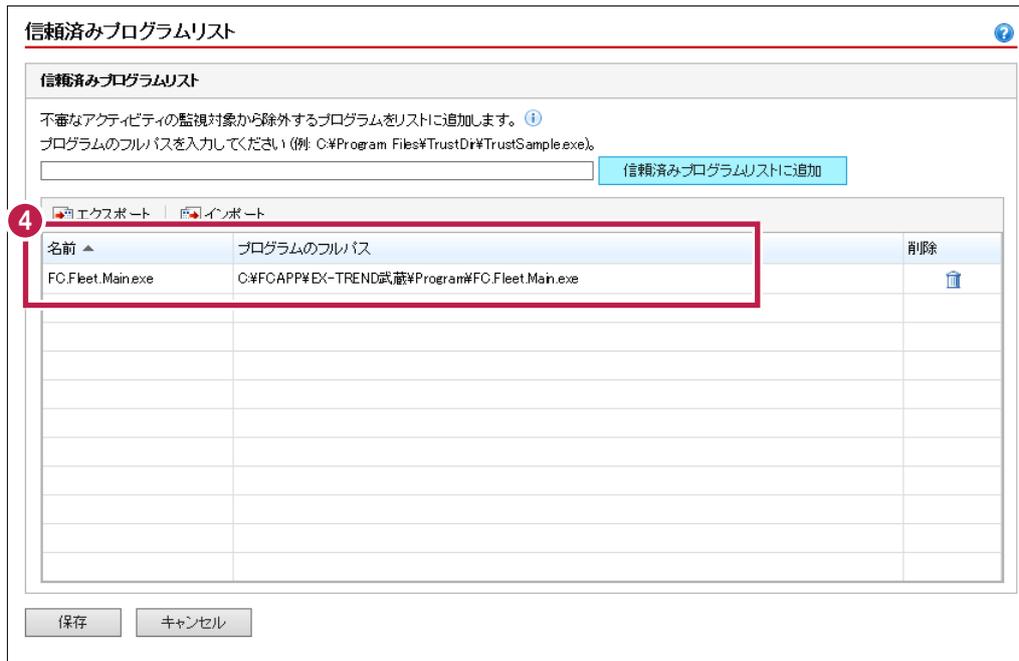


- 2 ボックスに「C:¥FCAPP」フォルダー内のexeファイルのパスを手入力します。
例：C:¥FcApp¥EX-TREND武蔵¥Program¥FC.Fleet.Main.exe
(Cは弊社製品のインストールドライブです。お客様の環境に合わせて読み替えてください。)
※その他の追加するexeファイルは、P.10を参照してください。

- 3 [信頼済みプログラムリストに追加] をクリックします。

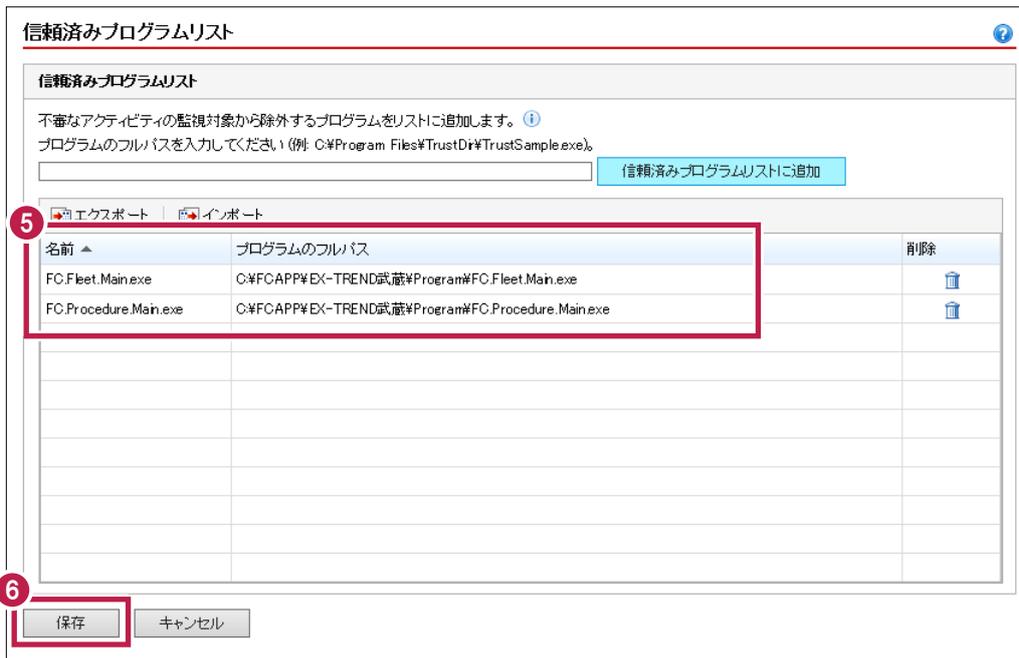


4 [信頼済みプログラムリスト] に追加されたことを確認します。



5 同様な手順で、必要なファイルをすべてリストに追加してください。

6 追加が終わったら、[保存] をクリックします。



7 [閉じる] をクリックします。
以上で終了です。

