SaAT Personal

製品仕様説明書 Rev.1.00

更新履歴

日付	Rev 番号	更新内容	ページ
2014-01-20	1.00	新規作成	文書全体

目次

はじめに

本書は、SaAT Personal（サート・パーソナル） の外部動作に関する仕様を、SaAT Personal をエンドユーザーに提供する事業者のご担当者様向けに説明したものです。内部動作に関する仕様については、別途お問合せいただければ、開示できる範囲で回答をさせていただきます（セキュリティ上、お答えできかねる場合があります)。また、本書に記載した内容は予告なく仕様やデザイン、文言等の修正がある場合があります。

本書は機密文書となりますので、取り扱いについては十分にご注意願います。全体、または一部の無断複製、頒布は禁止となりますので予めご了承願います。

用語及び略語

以下、本書の中で利用されている、用語・略語を示します。

用語集

用語	意味
HOME 画面	SaAT Personal の本体となる画面。
機能ステータス画面	HOME 画面に対し、表示を切り替えた画面。
環境設定画面	各種機能の使用状況や動作方法を設定する画面。
事業者	SaAT Personal のサービス提供事業者。
サービス提供ページ	SaAT Personal のサービス提供を行うページ。
分析サーバー	SaAT Personal と連携し、セキュリティ上の脅威に関する報告の受付や、分析結果の提供を行うサーバー。
パターン	悪性コードや不正通信の定義情報。既知の脅威に対する検知に使用される。
レピュテーション	プログラムや Web サイトに関して収集した情報からの測定に基づく、危険性の判定内容。主に未知の脅威に対する検知に使用される。
ビヘイビア	プログラムやパケットの挙動に基づく、危険性の判定内容。主に未知の脅威や通信異常に対する検知に使用される。
アンチウイルス	ファイル操作時、該当ファイルの感染をリアルタイムでスキャンする機能。ビヘイビアや分析サーバーからの提供情報に基づく検知、レピュテーションに基づくプログラム実行の遮断も可能。
Active Defense	アンチウイルスによるプログラムのスキャン時、疑わしい動作の有無を分析する機能。分析結果に基づき、プログラム実行の遮断も設定可能。

略語集

略語	意味
QS	クイックスキャン
FS	指定スキャン
SS	スケジュールスキャン
ES	エクスプローラースキャン
US	USB デバイススキャン
AV	アンチウイルス
FW	ファイアウォール
BS	有害サイト遮断
IP	ネットワーク侵入遮断
BP	ビヘイビア侵入遮断
TN	チューニング
FD	ファイル完全削除
LG	ログ
BC	バックアップセンター

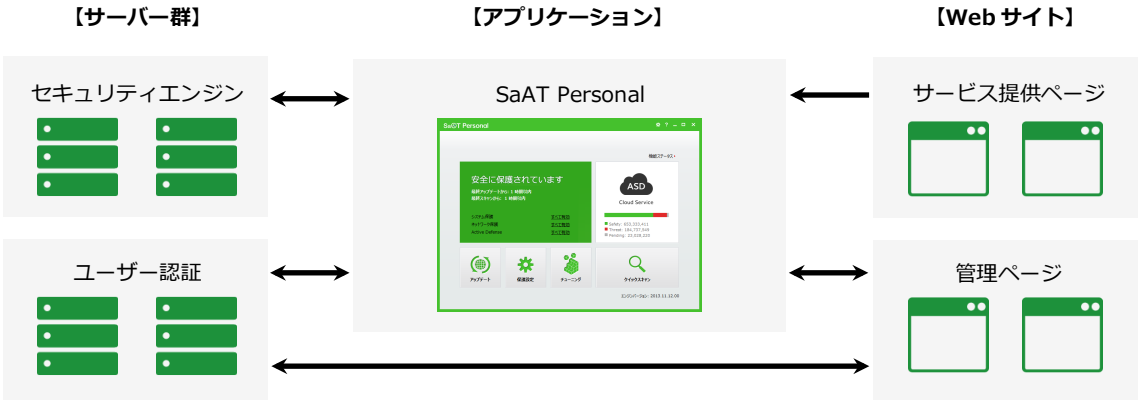
製品概要

SaAT Personal のサービスとは？

SaAT Personal とは、セキュアな環境の確保を目的とした、パソコン向けセキュリティ・ソリューションです。ウイルスなどの悪性コードに代表される多様な不正行為に対抗するため、常時動作による保護を主体とする、先進の各種セキュリティ機能を搭載しています。ファイル・通信の挙動判定や、クラウド上での分析技術と連携した検知により、未知の脅威からもパソコンを効果的に保護します。

サービスシステム概要

SaAT Personal のサービスは、パソコンで動作するアプリケーション、サービス運営用の Web サイト、アプリケーションとの連携動作を担うサーバー群で構成されます。



- **【サーバー群】**セキュリティエンジン配布やユーザー認証などを担う、各種サーバー群で構成。
- **【アプリケーション】**SaAT Personal 本体で構成。
- **【Web サイト】**SaAT Personal のサービス提供ページと、管理ページで構成。

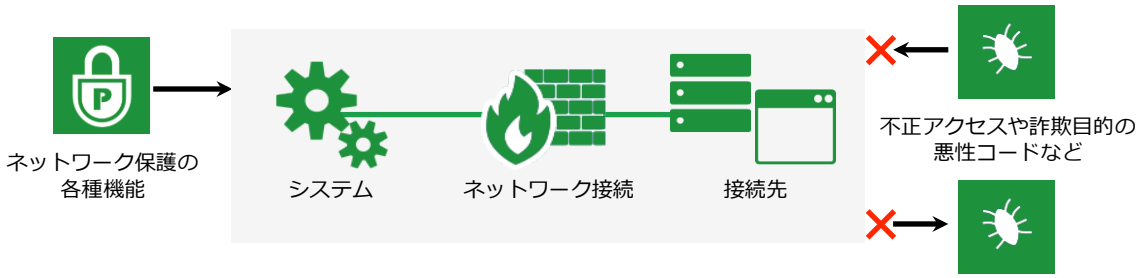
セキュリティ機能

保護機能と動作

SaAT Personal の保護機能は、パソコンのシステム内部を対象とした「システム保護」と、ネットワーク接続を対象とした「ネットワーク保護」で構成されます。

システム保護では各種スキャン機能の実行により、パソコンが感染した悪性コードを駆除できます。さらに、パソコン起動中に常時動作（リアルタイム）で検知する「アンチウイルス」機能を使用することで、パソコンのセキュリティ状態を最大限に高められます。

ネットワーク保護はリアルタイムで動作し、各種機能でシステム内・外への不正なアクセスを遮断します。これにより、情報漏えいや不正侵入、異常通信や有害サイトによる被害の発生を防ぎます。



さらに、SaAT Personal では積極的な防御機能として、疑わしいプログラム動作の有無を分析し、結果に応じ実行遮断の設定を可能とする「Active Defense」機能も搭載しています。

検知方式

SaAT Personal は悪性コードなどの脅威を特定するため、複数の検知方式を採用しています。

既知の悪性コードや不正通信の定義（パターン）は、アップデート時に更新されます。定義にないファイルに対しては、クラウド上の分析サーバーと連携し（クラウド検知）、駆除対象の判定を行います。

さらに、プログラムやパケットの挙動から判定する「ビヘイビア」検知と、プログラムに関して収集した情報に基づいて危険性を測定する「レピュテーション」検知を併用し、未知の脅威に対しても駆除や遮断を可能としています。

システム保護の各種機能

システム内部を対象に、悪性コードの不正活動からパソコンを保護します。

- **【クイックスキャン（QS)】**パソコンのプロセス、ブート領域、重要システム領域をスキャンして、悪性コードを検知します。
- **【指定スキャン（FS)】**パソコンから任意の領域を指定して、スキャンを実行します。
- **【スケジュールスキャン（SS)】**任意の実行日時と領域を設定して、自動的にスキャンを実行します。
- **【エクスプローラースキャン（ES)】**Windows のエクスプローラーから、スキャンを実行します。
- **【USB デバイススキャン(US)】**USB デバイスの接続時､自動的にデバイスへのスキャンを実行します。
- **【アンチウイルス（AV)】**パソコン上のファイル操作をリアルタイムでスキャンします。

機能	保護対象	防御先（脅威）	処理	動作条件	検知方式
QS	システム（特定）	悪性コード	駆除	任意実行	パターン、レピュテーション
FS	システム（指定）	悪性コード	駆除	任意実行	パターン、レピュテーション
SS	システム（指定）	悪性コード	駆除	自動実行（スケジュール日時）	パターン、レピュテーション
ES	ファイル（指定）	悪性コード	駆除	任意実行	パターン、レピュテーション
US	USB デバイス	悪性コード	駆除	自動実行（USB 接続時）	パターン、レピュテーション
AV	ファイル（操作時）	悪性コード	駆除、遮断	常時動作	パターン、ビヘイビア（駆除） レピュテーション（駆除、遮断）

ネットワーク保護の各種機能

ネットワーク接続を対象に、システム内・外の不正アクセスからパソコンを保護します。

- **【ファイアウォール（FW)】**データの送受信やプログラムによるネットワーク接続を制御し、不正アクセスや情報漏えいなどの危険からパソコンを保護します。
- **【有害サイト遮断（BS)】**フィッシングサイトや悪性コードを配布する有害サイト、その他指定したサイトへの接続を遮断します。
- **【ネットワーク侵入遮断（IP)】**ネットワークを介したワームやスパイウェアなどの侵入を検知し、パソコンへの感染を阻止します。
- **【ビヘイビア侵入遮断（BP)】**ネットワーク上の通信状況を監視して異常を検知し、パソコンへの不正な接続を遮断します。

機能	保護対象	防御先（脅威）	処理	動作内容	検知方式
FW	ネットワーク接続	不正アクセスや情報漏えいなど	遮断	常時動作	対象指定、ビヘイビア
BS	サイトへのアクセス	フィッシングサイトや有害サイトなど	遮断	常時動作	有害サイト情報、対象指定
IP	ネットワーク接続	ワームやスパイウェアなどの侵入	遮断	常時動作	対象指定
BP	ネットワーク接続	異常通信やスプーフィング攻撃	遮断	常時動作	ビヘイビア

Active Defense 機能 / ツール機能

未知の脅威への積極的な防御や、各種管理などを行います。

- **【Active Defense（AD)】**アンチウイルスによるプログラムのスキャン時、疑わしい動作の有無を分析します。分析結果に応じプログラムの実行遮断を設定することで、積極的な防御を可能とします。
- **【チューニング（TN)】**パソコンの一時ファイルやメモリなどを整理し、使用状況を改善します。
- **【ファイル完全削除（FD)】**指定したファイルやフォルダを完全に削除し、復元不可能な状態にします。
- **【ログ（LG)】**SaAT Personal の動作履歴（ログ）を確認します。
- **【バックアップセンター（BC)】**各種スキャンで駆除した、感染ファイルのバックアップを管理します。

セットアップ

動作環境

対応 OS（日本語版）

- Windows XP SP3 以上（64 ビット版除く）
- Windows Vista SP1 以上
- Windows 7
- Windows 8 / 8.1（Windows RT 除く）

※上記はバージョンやエディション違い、Windows Vista 以降は 32 ビット版と 64 ビット版を含みます。

※Windows 8 / 8.1 ではデスクトップ画面での動作に対応しています。Windows 8 スタイルには対応しておりません。

※上記の日本語版以外、サーバー版、β版や評価版、ならびに上記以外の OS には対応しておりません。

※インストールには Administrator（管理者）権限が必要です。

システム要件

- CPU：Intel Pentium4 1GHz 以上
- メモリ：1GB 以上
- ハードディスク：300MB 以上の空き容量
- ディスプレイ：解像度 800×600 ピクセル 256 色以上

※リモート接続や仮想マシン環境での動作はサポートしておりません。

ブラウザ

- Internet Explorer 7～11

※上記のβ版や評価版には対応しておりません。

※拡張保護モードが有効化された Internet Explorer や上記以外のブラウザでは、一部機能が正常に動作しない場合があります。

接続環境

- インストール、起動時ともにインターネット接続が利用可能であること。

※ADSL や光ファイバーなど、常時接続が可能な環境を推奨します。

※企業内ネットワークなどインターネット接続環境設定によっては、ご利用いただけない場合があります。

※VPN 環境では動作が不安定になる場合がありますので、その場合はご利用を控えてください。

※SaAT Personal のご利用対象は日本国内在住の方のみです。

インストール

SaAT Personal のサービス提供ページの案内に従い、インストールを開始します。

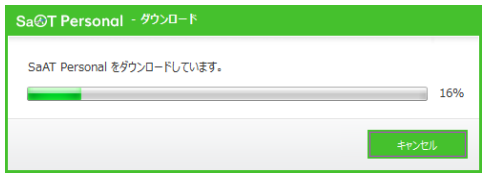
※ご利用開始の方法やサービス提供ページは、事業者により異なります。

※Windows 8 / 8.1 では、デスクトップ画面からサービス提供ページにアクセスしてください。SaAT Personal のインストールと起動はデスクトップ画面にのみ対応しており、Windows 8 スタイルには対応しておりません。

※インストールには Administrator（管理者）権限が必要です。

① サービス提供ページの案内に従い、SaAT Personal のインストール用ファイルをダウンロードします。ダウンロードを開始すると、ダイアログで確認されます。

② ダイアログから「保存」を選ぶと、ファイルがダウンロードされます。ダウンロードしたファイルを実行し、インストーラーを起動します。ダイアログから「実行」を選ぶと、ファイルのダウンロード後、自動的にインストーラーが起動します。



③ インストーラーの指示に従い、インストールを完了します。

※インストール時、ユーザーアカウント制御が有効に設定されていると、コンピューターへの変更許可をダイアログで確認されます。続行するには、ダイアログから許可してください。

④ インストールが完了すると、自動的に SaAT Personal の HOME 画面が表示されます。Windows のタスクトレイ内には SaAT Personal のアイコンが表示されます。

※インストール後、パソコンの再起動が必要となる場合があります。

アンインストール

Windows の以下操作でアンインストールします。

アンインストールの開始後は、画面の指示に従って操作します。

- **【Windows XP】**デスクトップ画面から「スタート」→「設定」→「コントロールパネル」→「プログラムの追加と削除」→「SaAT Personal」の順に選択し、「削除」を実行します。
- **【Windows Vista / 7】**デスクトップ画面から「スタート」→「コントロールパネル」→「プログラムのアンインストール」→「SaAT Personal」の順に選択し、「アンインストール」を実行します。
- **【Windows 8 / 8.1】**デスクトップ画面から「設定」チャーム→「コントロールパネル」→「プログラムのアンインストール」→「SaAT Personal」の順に選択し、「アンインストール」を実行します。

※アンインストール時、ユーザーアカウント制御が有効に設定されていると、コンピューターへの変更許可をダイアログで確認されます。続行するには、ダイアログから許可してください。

※一部のファイルは、エクスプローラー（Explorer.exe）を再起動しないと完全に削除されません。アンインストールを正常に行うには、ダイアログの指示に従ってエクスプローラーを再起動してください。

起動

インストール後、SaAT Personal はパソコンとともに自動的に起動し、Windows のタスクトレイ内にアイコンが表示されます。

※パソコンがセーフモードで動作中の場合、使用できる機能が制限されます。

アイコンの表示

- 【  】アンチウイルスが ON。
- 【  】アンチウイルスが OFF。
- 【  】アンチウイルスが ON で、スケジュールスキャンが実行中。
- 【  】アンチウイルスが OFF で、スケジュールスキャンが実行中。

アップデート

SaAT Personal のアップデートは、自動と手動の 2 種があります。

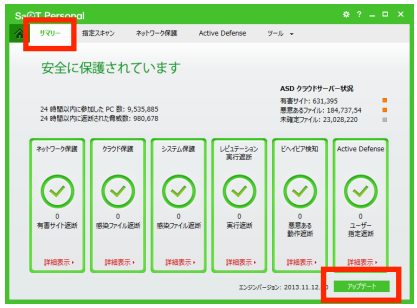
アップデートの対象は、セキュリティ機能のエンジンと SaAT Personal 自身のパッチファイルです。アップデートの動作方法は、環境設定画面から設定できます。

自動アップデート

環境設定画面の「使用環境」→「アップデート設定」で設定できます。設定内容に応じ、パソコンの起動後や設定時間に自動アップデートが実行されます。

手動アップデート

以下の操作で、手動アップデートを実行できます。



- **【HOME 画面から】**「アップデート」を選択します。
- **【機能ステータス画面から】**「サマリー」の「アップデート」を選択します。
- **【タスクトレイメニューから】**「アップデート」を選択します。

UI 仕様

SaAT Personal は以下の画面より構成されます。

HOME 画面（デフォルト）

SaAT Personal の本体となる画面です。セキュリティ状態の確認や主要機能の実行などができます。

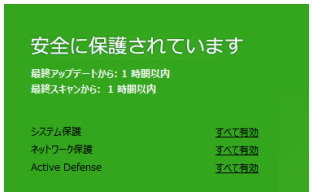
Windows のタスクトレイから SaAT Personal のアイコンを選択するか、タスクトレイメニューから「SaAT Personal を開く」を選択すると、表示されます。

※初期の表示位置は、Windows のデスクトップ中央です。

※画面ウィンドウに対し、タイトルバーをドラッグすると移動、縁をドラッグすると表示サイズの変更ができます。

セキュリティ状態

SaAT Personal のリアルタイム保護機能の使用状況に基づいた、パソコンのセキュリティ状態が表示されます。



リアルタイム保護機能は、システム保護、ネットワーク保護、Active Defense の 3 種で表示されます。各種機能の使用状況（「すべて有効」「一部有効」「無効」）を選択すると保護設定画面が表示され、使用の ON / OFF を切り替えられます。

セキュリティ状態は色で区分されます。イエローやレッドの場合には「解決する」が表示され、選択すると自動的にグリーンの状態に変更できます。

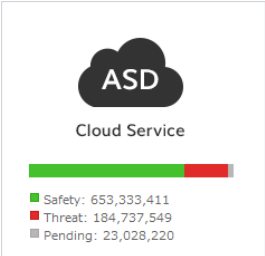
- **【グリーンの状態】**リアルタイム保護機能が「すべて有効」に設定され、安全な状態です。
- **【イエローの状態】**リアルタイム保護機能が「一部有効」「無効」に設定され、注意が必要な状態です。
- **【レッドの状態】**システム保護のアンチウイルスが OFF のため、危険な状態です。

クラウド分析状況

分析サーバーに報告された、ファイルの分類状況です。

報告されたファイルは「Safety（正常なファイル）」「Threat（悪性コード）」「Pending（未確定）」で分類され、現在の各ファイル数が表示されます。

※インターネット接続に問題が発生した場合、クラウド分析状況は表示されません。



メインメニュー

SaAT Personal の主要機能を実行できます。

「アップデート」「チューニング」「クイックスキャン」を選択すると、メニュー内に実行状況が表示されます。実行表示中にメニュー内から「×」を選択すると、実行を中止できます。

- **【アップデート】**手動アップデートを実行します。
- **【保護設定】**保護設定画面が表示されます。
- **【チューニング】**チューニングを実行します。実行表示中に再選択すると、チューニング画面に表示が切り替わります。
- **【クイックスキャン】**クイックスキャンを実行します。実行表示中に再選択すると、スキャン画面に表示が切り替わります。

「クイックスキャン」では状況に応じ、メニュー内に「！」マークが表示されます。マークは色で区分されます。

- **【イエローのマーク】**SaAT Personal のインストール直後か、前回のスキャンから 30 日が経過した場合に表示されます。スキャンを実行するとマークが消えます。
- **【レッドのマーク】**悪性コードを検知した場合に表示されます。メニューを選択するとスキャン画面に表示が切り替わり、HOME 画面に戻るとマークが消えます。

保護設定画面

SaAT Personal のリアルタイム保護機能に対し、使用の ON / OFF を切り替える画面です。

HOME 画面から「保護設定」を選択するか、リアルタイム保護機能の使用状況（「すべて有効」「一部有効」「無効」）を選択すると、表示されます。

- **【ON / OFF】**各種機能に対し、使用の ON / OFF を切り替えられます。
- **【  （環境設定）】**環境設定画面が表示され、該当機能の動作方法を設定できます。
- **【初期値】**使用の ON / OFF を初期化します。初期化の前にダイアログで確認されます。
- **【閉じる】**画面を閉じます。

※アンチウイルス、ネットワーク侵入遮断、ビヘイビア侵入遮断を OFF に切り替える場合、ダイアログで確認されます。

※アンチウイルスが OFF の場合、ビヘイビア検知、レピュテーション実行遮断、Active Defense は使用できません。

※ASD ネットワーク参加を初めて ON に切り替える場合、ダイアログで許諾への同意を確認されます。表示された内容を確認し、「同意する」を選択すると、ON に切り替えられます。

機能ステータス画面

SaAT Personal の HOME 画面に対し、表示を切り替えた画面です。セキュリティ状態や各種機能の動作状況を確認したり、HOME 画面外の機能を実行できます。

HOME 画面から「機能ステータス」を選択すると、表示されます。

※HOME 画面の初期表示は、環境設定画面の「使用環境」→「ユーザー設定」から設定できます。「デフォルト画面」と「機能ステータス画面」から、初期表示を選択します。

セキュリティ状態

SaAT Personal のリアルタイム保護機能の使用状況に基づいた、パソコンのセキュリティ状態が表示されます。

セキュリティ状態はメッセージとその文字色で区分されます。文字色がオレンジやレッドの場合には「解決する」が表示され、選択すると自動的にグリーンの状態に変更できます。

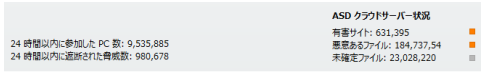
- **【グリーンの文字色】**リアルタイム保護機能が「すべて有効」に設定され、安全な状態です。
- **【イエローの文字色】**リアルタイム保護機能が「一部有効」「無効」で設定され、注意が必要な状態です。
- **【レッドの文字色】**アンチウイルスが OFF のため、危険な状態です。

タブメニュー

ネットワーク保護やActive Defenseに関する動作状況を確認したり、指定スキャンや各種ツールを実行できます。

クラウド分析状況

分析サーバーに報告された、サイトとファイルの分類状況が表示されます。



画面左側には 24 時間以内で、分析サーバーのネットワークに参加したパソコン数と、サーバー上での分析に基づき遮断された脅威（悪性コードや有害サイトなど）の数が表示されます。

画面右側のサーバー状況では、報告されたサイトやファイルの内、「有害サイト」や「悪意あるファイル（悪性コード）」、「未確定ファイル」に分類された数が表示されます。

※インターネット接続に問題が発生した場合、クラウド分析状況は表示されません。

各種機能の動作状況

SaAT Personal によるリアルタイム保護機能に対し、現在の動作状況が表示されます。

リアルタイム保護機能は、ネットワーク保護、クラウド保護、システム保護、レピュテーション実行遮断、ビヘイビア検知、Active Defense の 6 種で表示されます。各種機能の表示は使用状況に応じ、色で区分されます。

- **【グリーンの状態】**該当機能がすべて ON で、安全な状態です。
- **【グレーの状態】**該当機能に OFF が含まれている状態です。

各種機能の表示内には、該当機能が遮断した脅威数が表示されます。「詳細表示」を選択すると、該当機能の使用状況や脅威数などの詳細がダイアログで表示されます。

動作状況の詳細表示

「詳細表示」のダイアログでは、以下の内容が表示されます。

- **【ネットワーク保護】**有害サイト遮断、ネットワーク侵入遮断、ビヘイビア侵入遮断の使用状況と、データ送受信状況、機能別の遮断数やスキャン数が表示されます。
- **【クラウド保護】**アンチウイルスとクラウド保護の使用状況と、スキャンファイル数や遮断ファイル数が表示されます。
- **【システム保護】**アンチウイルスの使用状況と、エンジンアップデート情報が表示されます。
- **【レピュテーション実行遮断】**アンチウイルスとレピュテーション実行遮断の使用状況と、検知数や遮断したファイル数が表示されます。
- **【ビヘイビア検知】**アンチウイルスとビヘイビア検知の使用状況と、遮断したファイル数が表示されます。
- **【Active Defense】**アンチウイルス、Active Defense、クラウド自動分析の使用状況と、サーバーからの分析結果に応じ、信頼または遮断したファイル数が表示されます。

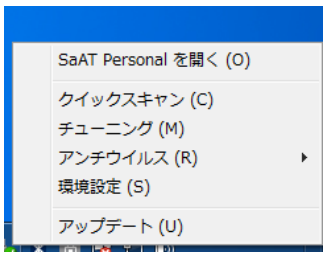
※「クラウド保護」の ON / OFF は、環境設定画面の「詳細設定」→「レピュテーション」から「クラウド検知機能を使用する」を選択すると、切り替えられます。

アップデート

手動アップデートを実行します。

選択すると、ボタン内に実行状況が表示されます。実行表示中にボタン内から「×」を選択すると、実行を中止できます。

タスクトレイメニュー

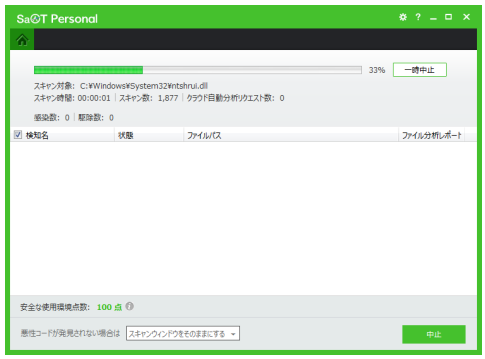


SaAT Personal への各種操作を行うメニューです。主要機能の実行や、リアルタイム保護機能の使用状況を設定できます。

Windows のタスクトレイから SaAT Personal のアイコンを右クリックすると、表示されます。

- **【SaAT Personal を開く】**HOME 画面が表示されます。
- **【クイックスキャン】**クイックスキャンを実行します。選択すると、スキャン画面がウィンドウで表示されます。
- **【チューニング】**チューニングを実行します。選択すると、チューニング画面がウィンドウで表示されます。
- **【アンチウイルス】**SaAT Personal のリアルタイム保護機能に対し、使用状況を設定します。サブメニューを選択すると、該当機能の ON / OFF を切り替えられます。
- **【環境設定】**環境設定画面が表示されます。
- **【アップデート】**手動アップデートを実行します。選択すると、アップデート画面がウィンドウで表示されます。

スキャン画面



各種スキャンの実行画面です。スキャンの種類に応じて、画面の表示方法が変わります。

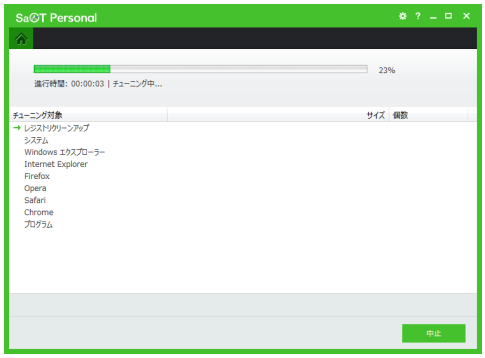
- **【ウィンドウで表示】**エクスプローラースキャン、USB デバイススキャン、タスクトレイメニューからのクイックスキャンは、画面がウィンドウで表示されます。
- **【HOME 画面を切り替えて表示】**HOME 画面からのクイックスキャンは、実行表示中にメニューを再選択すると、画面を切り替えて表示されます。

  画面左上には HOME 画面への切り替えボタンが表示されます。
- **【機能ステータス画面を切り替えて表示】**機能ステータス画面からの指定スキャンは、スキャン開始後に画面を切り替えて表示されます。

  画面上部には、HOME 画面への切り替えボタンとタブメニューが表示されます。

チューニング画面

チューニングの実行画面です。実行方法に応じて、画面の表示方法が変わります。



- **【ウィンドウで表示】**タスクトレイメニューからのチューニングは、画面がウィンドウで表示されます。
- **【HOME 画面を切り替えて表示】**HOME 画面からのチューニングは、実行表示中にメニューを再選択すると、画面を切り替えて表示されます。

  画面左上には、HOME 画面への切り替えボタンが表示されます。

環境設定画面

SaAT Personal の各種機能や使用環境に対し、詳細を設定する画面です。

HOME 画面や機能ステータス画面から環境設定ボタンを選択すると、ウィンドウで表示されます。

- **【設定メニュー】**画面左側に表示されるメニューです。設定の大分類を選択します。
- **【タブメニュー】**「設定メニュー」の選択に応じ、画面上部に表示されるメニューです。設定の小分類を選択します。
- **【すべて初期値】**すべての設定を初期化します。
- **【初期値】**表示中の設定を初期化します。
- **【OK】**設定した内容を保存して、画面を閉じます。
- **【キャンセル】**設定した内容を破棄して、画面を閉じます。
- **【適用】**設定した内容を保存します。画面は閉じません。

※初期化の対象は、各種機能の ON / OFF や動作方法の設定です。各種リストの設定は初期化されません。

システム保護機能

クイックスキャン

機能と動作

パソコンのプロセス（動作中のプログラム）、ブート領域、重要システム領域（OS と、各ユーザーやパブリックのフォルダ）をスキャンして、悪性コードを検知します。

※クイックスキャンでは、悪性コードに感染しやすい領域に限定してスキャンします。パソコン全体をスキャンするには、指定スキャンやスケジュールスキャンを実行する必要があります。

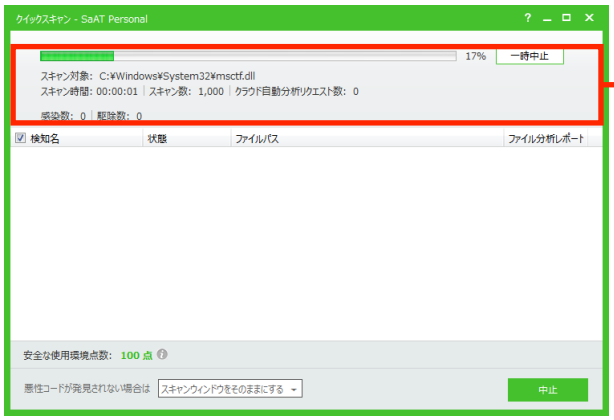
スキャンの実行

以下の操作で実行できます。操作に応じて、スキャン画面の表示方法が変わります。

- **【HOME 画面から】**「クイックスキャン」を選択すると、メニュー内に実行状況が表示されます。実行表示中にメニューを再選択すると、スキャン画面に切り替わります。
- **【タスクトレイメニューから】**「クイックスキャン」を選択すると、スキャン画面がウィンドウで表示されます。

スキャン画面の表示

スキャンを実行すると、実行状況の詳細が表示されます。



- **【スキャン状況】**スキャンの対象、実行状況、分析サーバーへの分析要求やスキャン後のファイル数などが表示されます。
- **【一時中止 / 再開】**スキャンの一時中止と再開を切り替えます。
- **【検知リスト】**悪性コードを検知した場合、その検知名、状態（駆除内容の説明）、ファイルパス（感染ファイルの位置）、ファイル分析レポート（レポートをブラウザの画面内に表示）が表示されます。
- **【悪性コードが発見されない場合は】**スキャン完了後の動作を、画面を維持する、画面を閉じる、パソコンを終了するから切り替えます。
- **【中止】**スキャンを中止して完了します。

スキャンの完了

スキャンが完了すると、スキャン画面の表示が切り替わります。

悪性コードを検知しなかった場合の表示

検知した場合の表示

- **【駆除する】**悪性コードを検知した場合に表示され、駆除を実行します。リストの悪性コードをチェック→「駆除する」を選択します。駆除後、リスト内の「状態」に結果が表示されます。
- **【終了（閉じる）】**画面を閉じます。駆除が完了していない場合、ダイアログで確認されます。

※SaAT Personal は設定に応じ、駆除したファイルを自動的にバックアップします。バックアップの管理はバックアップセンターで行います。

指定スキャン

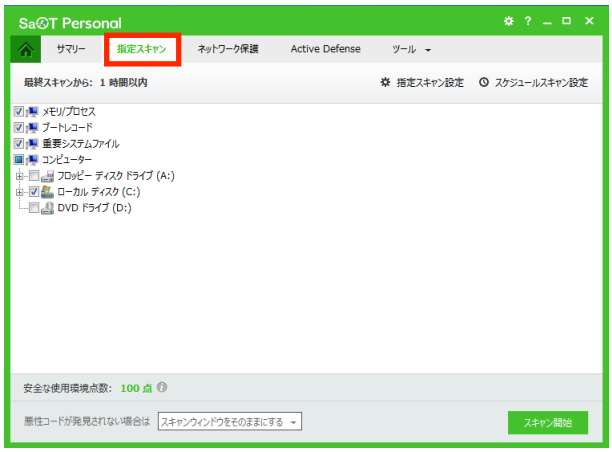
機能と動作

パソコンから任意の領域を指定して、スキャンを実行します。

本機能は機能ステータス画面から実行できます。環境設定画面からは、スキャン対象の詳細や駆除方法などを設定できます。

スキャンの実行

機能ステータス画面の「指定スキャン」から、スキャン領域を指定して実行します。

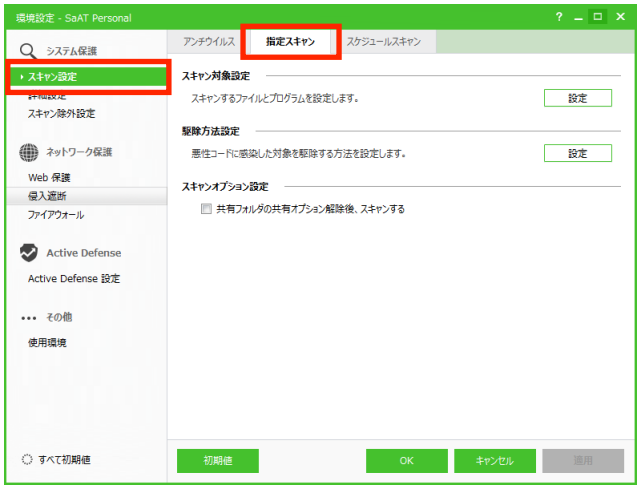


- **【指定スキャン設定】**環境設定画面の「スキャン設定」→「指定スキャン」が表示されます。
- **【スケジュールスキャン設定】**環境設定画面の「スキャン設定」→「スケジュールスキャン」が表示されます。
- **【スキャン対象リスト】**ドライブやフォルダなどを選択して、スキャン領域を指定します。
- **【悪性コードが発見されない場合は】**スキャン完了後の動作を、画面を維持する、画面を閉じる、パソコンを終了するから切り替えます。
- **【スキャン開始】**スキャン画面に切り替わります。指定に応じ、スキャンが実行されます。

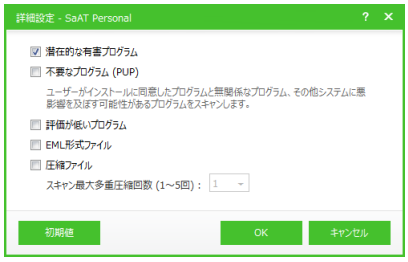
※スキャン画面の表示はクイックスキャンと同様です。

スキャン対象の詳細設定

環境設定画面の「スキャン設定」→「指定スキャン」から、スキャン領域のプログラムとファイルに対し、スキャン対象の詳細を設定できます。



「スキャン対象設定」の「設定」を選択すると、ダイアログが表示されます。スキャン対象に含めるプログラムやファイルを選択し、「OK」を選択します。



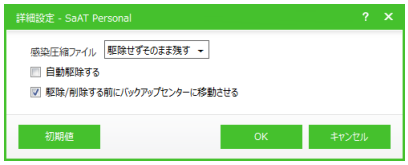
- **【潜在的な有害プログラム】**キーロガーやリモート接続ツールなど、有害プログラムとして分類されたファイルをスキャンします。
- **【不要なプログラム（PUP)】**インストールに同意したものとは無関係のプログラムや、システムに悪影響を及ぼすおそれのあるプログラムをスキャンします。
- **【評価が低いプログラム】**分析サーバーのレピュテーション情報を参照し、評価が低いファイルをスキャンします。
- **【EML 形式ファイル】**拡張子が eml のメールファイルに対し、メール本文と添付ファイルをスキャンします。添付ファイルの感染を検知すると、駆除方法設定に応じた駆除と再添付を行います。（再添付したファイルが多重 EML ファイルの場合、再スキャンは行われません）
- **【圧縮ファイル】**圧縮ファイルをスキャンします。チェックを入れると、「スキャン最大多重圧縮回数（スキャン時に多重圧縮ファイルを解凍する回数の上限）」の設定が可能になります。

駆除方法の設定

環境設定画面の「スキャン設定」→「指定スキャン」から、悪性コードに感染したファイルに対し、駆除の動作方法を設定できます。

「駆除方法設定」の「設定」を選択すると、ダイアログが表示されます。動作方法を設定し、「OK」を選択します。

※指定スキャンの駆除方法は、クイックスキャン/エクスプローラースキャン/USB デバイススキャンにも適用されます。



- **【感染圧縮ファイル】**悪性コードに感染した圧縮ファイルの駆除方法を、残す、削除するから選択します。
- **【自動駆除する】**感染ファイルを自動的に駆除します。駆除時は確認されません。(指定スキャンの場合のみ設定可)
- **【駆除/削除する前にバックアップセンターに移動させる】**駆除したファイルを自動的にバックアップします。バックアップの管理はバックアップセンターで行います。

スキャンオプションの設定

環境設定画面の「スキャン設定」→「指定スキャン」から、スキャンの動作方法に対し、オプションを設定できます。

「スキャンオプション設定」の「共有フォルダの共有オプション解除後、スキャンする」を選択すると、共有フォルダのスキャン時、共有設定を解除します。

※スキャンオプション設定を ON にした場合、解除された共有設定を復帰するには、Windows のファイル共有で再設定する必要があります。

スケジュールスキャン

機能と動作

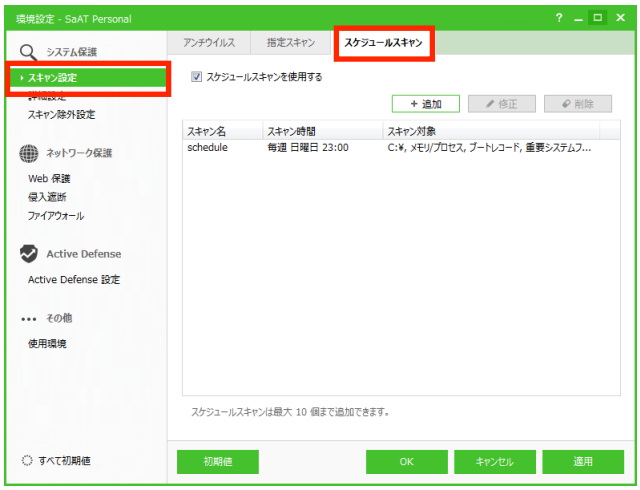
スキャン対象と実行日時のスケジュールを設定して、自動的にスキャンを実行します。

本機能は環境設定画面から、使用の ON / OFF を切り替えられます。スケジュールの追加や修正では、スキャン対象の詳細や駆除方法も設定できます。

使用の ON / OFF

環境設定画面の「スキャン設定」→「スケジュールスキャン」から、「スケジュールスキャンを使用する」を選択します。選択すると、スケジュールの設定が可能になります。

スケジュールの設定



- **【スケジュールリスト】**スケジュールの識別名、スキャンの実行日時と対象が表示されます。
- **【追加】**リストへスケジュールを追加します。選択すると、ダイアログが表示されます。
- **【修正】**スケジュールの設定内容を修正します。リストのスケジュール→「修正」の順に選択すると、ダイアログが表示されます。
- **【削除】**スケジュールを削除します。リストのプログラム→「削除」の順に選択します。削除前に、ダイアログで確認されます。

※スケジュールは最大 10 個まで追加できます。設定が重複している場合は追加できません。

スケジュールの追加や修正

スケジュールの追加や修正のダイアログでは、識別用の「スキャン名」→「スキャン時間」→「スキャン対象」の順に設定し、「OK」を選択します。

ダイアログでは、スキャン対象や駆除方法の設定もできます。設定内容は、環境設定画面の「スキャン設定」→「指定スキャン」内、「スキャン対象設定」や「駆除方法設定」と同様です。

※「駆除方法設定」の「自動駆除する」は、スケジュールスキャンでは設定できません。

スキャンの実行

実行日時になると、自動的にスキャンが実行されます。

実行中、タスクトレイ内の SaAT Personal のアイコンは、以下の表示に切り替わります。

- 【 】アンチウイルスが ON の場合。
- 【 】アンチウイルスが OFF の場合。

エクスプローラースキャン

機能と動作

Windows のエクスプローラー上でフォルダやファイルを指定し、スキャンを実行します。

本機能は環境設定画面から、使用の ON / OFF を切り替えられます。

使用の ON / OFF

環境設定画面の「使用環境」→「ユーザー設定」内、「エクスプローラーメニュー」から「エクスプローラースキャンを使用する」を選択します。

スキャンの実行

Windows のエクスプローラーからフォルダやファイルを右クリックし、コンテキストメニューから「SaAT Personal スキャン」を選択します。スキャン画面が表示され、右クリックしたフォルダやファイルを対象にスキャンが実行されます。

※スキャン画面の表示はクイックスキャンと同様です。

USB デバイススキャン

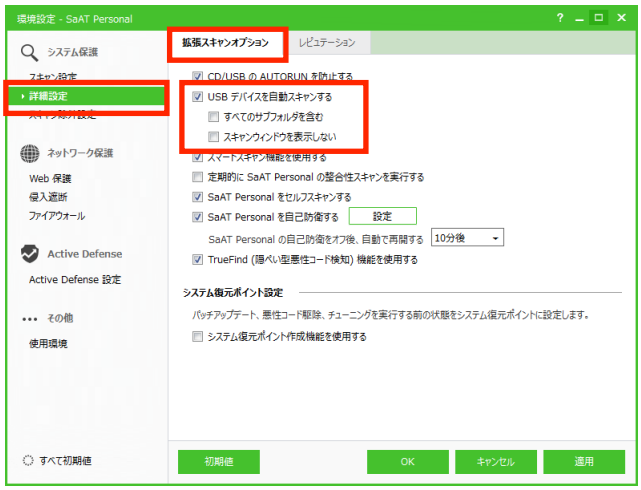
機能と動作

パソコンにメモリやハードディスクなどの USB デバイスが接続された時、自動的にデバイスへのスキャンを実行します。

本機能は環境設定画面から、使用の ON / OFF を切り替えられます。

使用の ON / OFF

環境設定画面の「詳細設定」→「拡張スキャンオプション」から「USB デバイスを自動スキャンする」を選択します。選択すると、「すべてのサブフォルダを含む」と「スキャンウィンドウを表示しない」の設定が可能になります。



スキャンの実行

パソコンに USB デバイスが接続されると、自動的にデバイスへのスキャンが実行されます。設定に応じ、スキャン画面が表示されます。

※スキャン画面の表示はクイックスキャンと同様です。

アンチウイルス

機能と動作

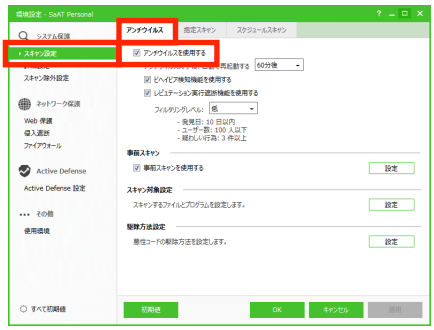
パソコン上のファイル操作をリアルタイムでスキャンし、悪性コードの感染から保護します。

本機能は使用の ON / OFF を切り替えられます。環境設定画面から、動作方法の設定もできます。

スキャンの実行は、ファイルのダウンロード、コピー、移動、実行など、一連の操作時に行われます。感染ファイルを検知すると、設定に応じ駆除します。

使用の ON / OFF

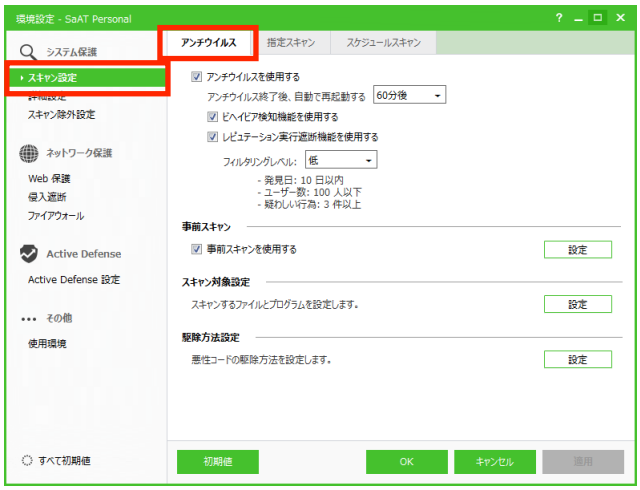
以下の操作で切り替えられます。OFF に切り替える場合、ダイアログで確認されます。



- **【保護設定画面から】**「アンチウイルス」の ON / OFF を選択します。ON に切り替えると、「ビヘイビア検知」と「レピュテーション実行遮断」の設定が可能になります。
- **【環境設定画面から】**「スキャン設定」→「アンチウイルス」を選択し、「アンチウイルスを使用する」を選択します。ON に切り替えると、画面内の他の設定が可能になります。

動作方法の設定

環境設定画面の「スキャン設定」→「アンチウイルス」から、スキャンの動作方法を設定できます。

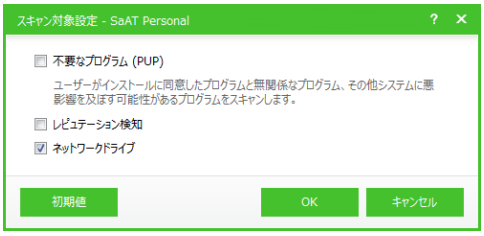


- **【アンチウイルス終了後、自動で再起動する】**使用を OFF にしても、選択した設定で自動的に ON に戻ります。
- **【ビヘイビア検知機能を使用する】**ファイルの実行時、疑わしい動作のセット（ビヘイビア）情報を基準に、悪性コードを検知します。
- **【レピュテーション実行遮断機能を使用する】**分析サーバー上の危険性測定（レピュテーション）情報を基準に、評価が低いプログラムを「疑わしいファイル」として、実行検知の対象とします。検知の度合いは「フィルタリングレベル」から選択できます。チェックを入れると検知が通知され、実行の遮断や許可、ファイル削除を選択できます。
- **【事前スキャン】**ファイルスキャンの前にスキャンする対象を設定します。チェックを入れると、「設定」が選択可能になります。

  「設定」を選択するとダイアログが表示され、事前スキャンの対象をブート領域とメモリ/プロセスから選択できます。
- **【スキャン対象設定】**スキャン対象の詳細を設定します。「設定」を選択すると、ダイアログが表示されます。
- **【駆除方法設定】**駆除方法を設定します。「設定」を選択すると、ダイアログが表示されます。

スキャン対象の詳細設定

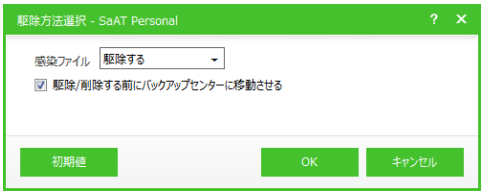
「スキャン対象設定」のダイアログでは、以下の内容を設定できます。



- **【不要なプログラム（PUP)】**インストールに同意したものとは無関係のプログラムや、システムに悪影響を及ぼすおそれのあるプログラムをスキャンします。
- **【レピュテーション検知】**分析サーバーのレピュテーション情報を基準に、脅威や安全性が未検証のファイルをスキャンします。
- **【ネットワークドライブ】**ネットワークドライブ上のファイル実行時もスキャンします。

駆除方法の設定

「駆除方法設定」のダイアログでは、以下の内容を設定できます。



- **【感染ファイル】**悪性コードに感染したファイルの駆除方法を、残す、駆除するから選択します。
- **【駆除/削除する前にバックアップセンターに移動させる】**駆除したファイルを自動的にバックアップします。バックアップの管理はバックアップセンターで行います。

クラウド検知

機能と動作

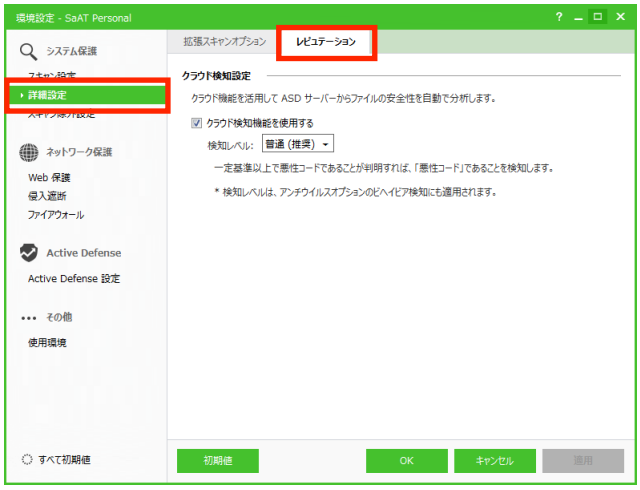
アンチウイルスや、分析サーバー上の情報を参照する各種機能に対し、分析サーバー上のレピュテーション情報に基づく検知（クラウド検知）を適用します。

本機能は環境設定画面から、使用の ON / OFF を切り替えられます。動作方法の設定もできます。

クラウド検知では、分析サーバーに報告された脅威の情報を検知時に活用します。さらに、未報告のファイルを発見するとサーバーに送信し、リアルタイムで分析結果が提供されます。これにより、未知の脅威も迅速に検知し、感染の危険性を減少できます。

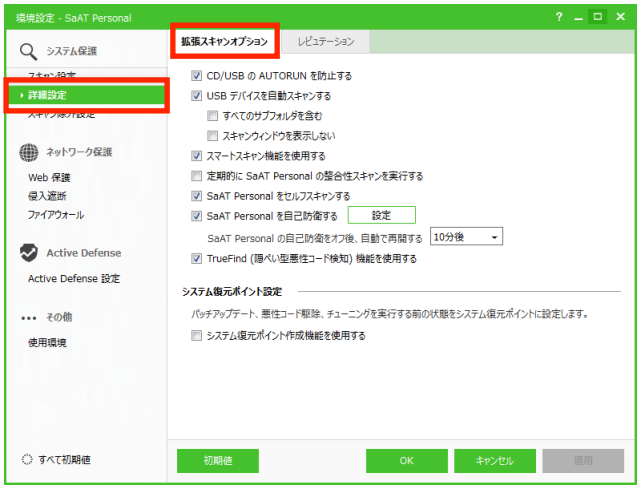
使用の ON / OFF

環境設定画面の「詳細設定」→「レピュテーション」から、「クラウド検知機能を使用する」を選択します。OFF に切り替える場合、ダイアログで確認されます。ON に切り替えると、「検知レベル」の設定も可能になります。



拡張スキャンオプション設定

環境設定画面の「詳細設定」→「拡張スキャンオプション」から、各種スキャンオプションの使用状況を設定できます。



- **【CD/USB の AUTORUN を防止する】**CD 挿入時などの自動実行（AUTORUN）を防止します。
- **【USB デバイスを自動スキャンする】**USB デバイススキャンを設定します。
- **【スマートスキャン機能を使用する】**Windows でインストールしたファイルを安全と判断し、変更が発生するまでスキャン対象から除外します。チェックを入れると、スキャンの速度が向上します。
- **【定期的に SaAT Personal の整合性スキャンを実行する】**SaAT Personal 自身のファイルに対し、デジタル署名の変更有無を確認します。
- **【SaAT Personal をセルフスキャンする】**SaAT Personal 自身のファイルに対し、感染を確認します。
- **【SaAT Personal を自己防衛する】**SaAT Personal のプロセス、レジストリ、ファイル、ボリュームを保護します。選択すると、他の設定が可能になります。

  「設定」を選択するとダイアログが表示され、保護対象を選択できます。自動再開を選択すると、動作を OFF にしても、選択した設定で自動的に ON に戻ります。
- **【TrueFind (隠ぺい型悪性コード検知) 機能を使用する】**自己隠ぺいする悪性コードもスキャンします。検知すると、ブートタイムスキャンにより駆除します。
- **【システム復元ポイント作成機能を使用する】**プログラムのインストール、パッチのアップデート、悪性コードの駆除、チューニング実行前の状態を、Windows のシステム復元ポイントに保存します。

※TrueFind 機能の使用には管理者権限が必要です。64 ビット版 Windows では使用できません。

※Windows 8 / 8.1 では、システム復元ポイントは 1 日に 1 回まで作成できます。セーフモードで起動した場合、システム復元ポイント作成機能は正常に使用できません。

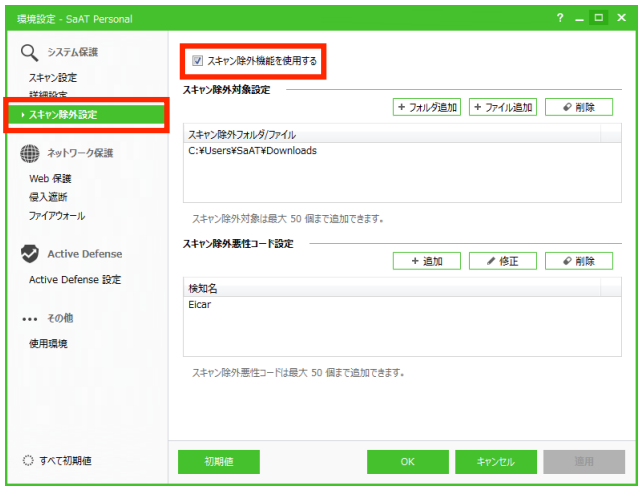
スキャン除外設定

環境設定画面の「スキャン除外設定」から、スキャン機能全般に対し、除外対象を設定できます。

本機能は使用の ON / OFF を切り替えられます。

使用の ON / OFF

環境設定画面の「スキャン除外設定」を選択し、「スキャン除外機能を使用する」を選択します。選択すると、「スキャン除外対象設定」と「スキャン除外悪性コード設定」も可能になります。



フォルダやファイルの除外設定

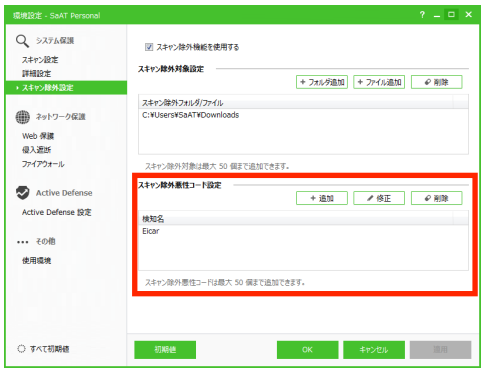
「スキャン除外対象設定」から、除外対象のフォルダやファイルを設定します。

- **【除外リスト】**除外対象のフォルダやファイルのパスが表示されます。
- **【フォルダ追加】**リストへフォルダを追加します。ダイアログが表示されたら、フォルダを選択します。
- **【ファイル追加】**リストへファイルを追加します。ダイアログが表示されたら、ファイルを選択します。
- **【削除】**除外対象を削除します。リストのフォルダやファイル→「削除」の順に選択します。削除前に、ダイアログで確認されます。

※除外対象のフォルダやファイルは最大 50 個まで追加できます。設定が重複している場合は追加できません。

悪性コードの除外設定

「スキャン除外悪性コード設定」から、除外対象の悪性コードを設定します。



- **【除外リスト】**除外対象の悪性コードの検知名が表示されます。
- **【追加】**リストへ悪性コードを追加します。ダイアログが表示されたら、検知名を入力→「OK」を選択します。検知名は、SaAT Personal のスキャン画面で表示される名称を使用します。
- **【修正】**除外対象を修正します。リストの悪性コード→「修正」の順に選択し、ダイアログが表示されたら、検知名を入力→「OK」を選択します。
- **【削除】**除外対象を削除します。リストの悪性コード→「削除」の順に選択します。削除前に、ダイアログで確認されます。

※除外対象の悪性コードは最大 50 個まで追加できます。設定が重複している場合は追加できません。

ネットワーク保護機能

ファイアウォール

機能と動作

データの送受信やプログラムによるネットワーク接続を制御し、不正アクセスや情報漏えいなどの危険からパソコンを保護します。

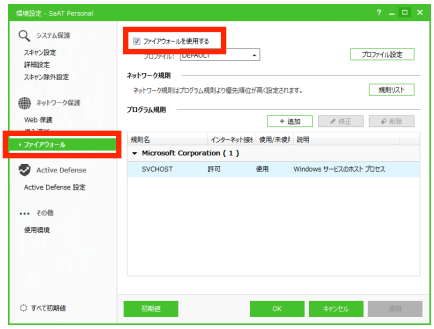
本機能は使用の ON / OFF を切り替えられます。環境設定画面から、動作方法の設定もできます。

本機能の制御下にあるネットワーク接続は制御内容に応じ、自動的に接続が許可または遮断されます。制御下にないプログラムは動作方法の設定に応じ、通知表示や自動処理が行われます。

また、ネットワーク接続の状態は自動的に記録され、機能ステータス画面から確認できます。

使用の ON / OFF

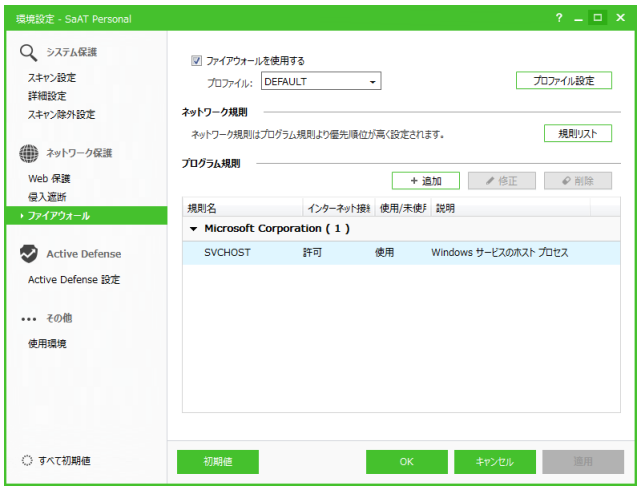
以下の操作で切り替えられます。OFF に切り替える場合、ダイアログで確認されます。



- **【保護設定画面から】**「ファイアウォール」の ON / OFF を選択します。
- **【環境設定画面から】**「ファイアウォール」を選択し、「ファイアウォールを使用する」を選択します。
  ON に切り替えると、画面内の他の設定が可能になります。

動作方法の設定

環境設定画面の「ファイアウォール」から、ネットワーク接続の制御内容を設定できます。



- **【プロファイル】**制御内容の基本設定で、「ネットワーク規則」や「プログラム規則」に優先して適用されます。

  「プロファイル設定」を選ぶとダイアログが表示され、デフォルトの接続処理やオプション機能の使用状況を設定できます。

- **【ネットワーク規則】**ネットワークを通じたデータの送受信に対し、許可または遮断の制御（規則）を設定します。

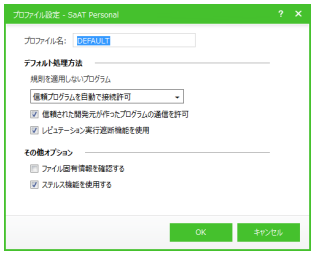
  「規則リスト」を選ぶとダイアログが表示され、規則の確認と設定ができます。

- **【プログラム規則】**パソコン内のプログラムによるネットワーク接続に対し、許可または遮断の制御（規則）を設定します。

  画面から規則の確認と設定ができます。

プロファイルの設定

プロファイル設定のダイアログでは、以下の内容を設定できます。



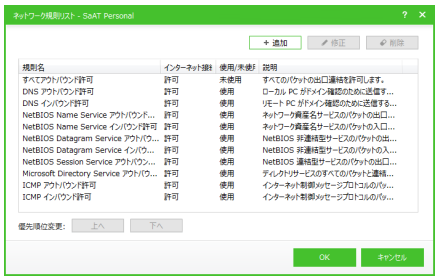
- **【プロファイル名】**プロファイルの表示名を入力します。
- **【デフォルト処理方法】**規則設定外のプログラムによるネットワーク接続に対し、標準の処理方法を選択します。

  処理方法は、接続の許可、遮断、通知から選択、信頼リスト登録済みのプログラム（信頼プログラム）は許可し他は通知、自動決定（信頼プログラムは許可し他は遮断）から選択できます。

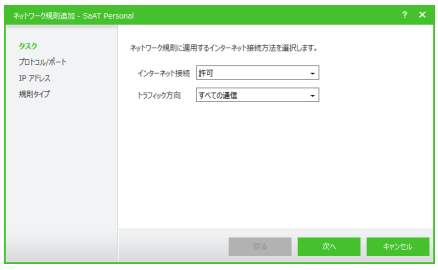
  プログラムのデジタル署名（信頼された開発元）の確認や、レピュテーション情報に基づく遮断処理の ON / OFF も切り替えられます。
- **【その他オプション】**ハッシュ値（ファイル固有情報）に基づくプログラム改ざんの確認や、許可ポート以外への外部からの接続禁止（ステルス機能）の ON / OFF を切り替えます。

ネットワーク規則の設定

ネットワーク規則設定のダイアログでは、以下の内容を設定できます。



ネットワーク規則設定

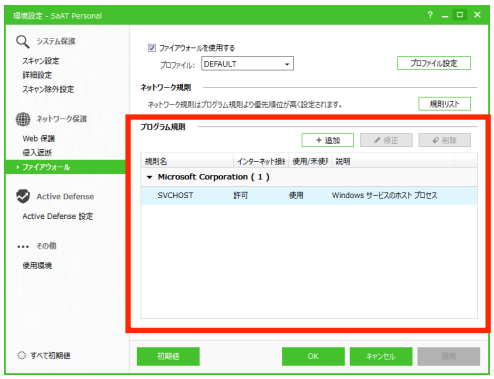


ネットワーク規則の追加/修正

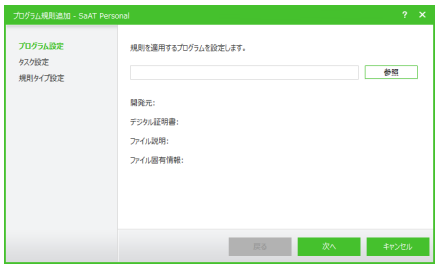
- **【規則リスト】**ネットワーク規則ごとに、名称、接続の許可/遮断、規則の使用/未使用、説明文が表示されます。規則適用の優先順位は、リストの並びに応じます。
- **【追加】**リストへネットワーク規則を追加します。ダイアログが表示されたら、接続の許可/遮断とトラフィック方向→適用するプロトコル/ポート→IP アドレス→規則の名称と説明の順に設定します。
- **【修正】**ネットワーク規則を修正します。リストの規則→「修正」の順に選択し、ダイアログが表示されたら、規則の ON / OFF や、追加時の設定内容を修正します。
- **【削除】**ネットワーク規則を削除します。リストの規則→「削除」の順に選択します。削除前に、ダイアログで確認されます。
- **【優先順位変更】**リストの並びを変更し、規則適用の優先順位を設定します。リストの規則→「上へ」「下へ」を選択します。

プログラム規則の設定

環境設定画面の「ファイアウォール」内、「プログラム規則」から、以下の内容を設定できます。



プログラム規則

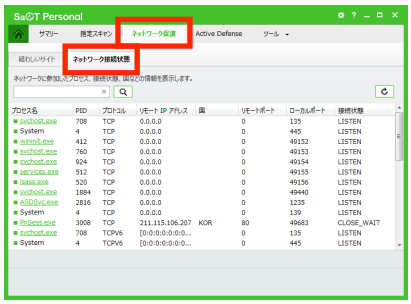


プログラム規則の追加/修正

- 【**規則リスト**】プログラム規則ごとに、名称、接続の許可/遮断、規則の使用/未使用、説明文が表示されます。規則はプログラムの開発元に応じ、グループ化されます。
- 【**追加**】リストへプログラム規則を追加します。ダイアログが表示されたら、対象のプログラム→接続の許可/遮断→規則の名称と説明の順に設定します。
- 【**修正**】プログラム規則を修正します。リストの規則→「修正」の順に選択し、ダイアログが表示されたら、規則の ON/OFF や追加時の設定内容を修正します。
- 【**削除**】プログラム規則を削除します。リストの規則→「削除」の順に選択します。削除前に、ダイアログで確認されます。

ネットワーク接続状態の確認

SaAT Personal はパソコンのネットワーク接続状態を監視し、ネットワークに参加したプロセス（動作中のプログラム）などの情報を自動的に記録します。



機能ステータス画面から「ネットワーク保護」→「ネットワーク接続状態」を選択すると、接続状態のリストが表示されます。

- 【**接続リスト**】接続ごとに、プロセス名、PID（特定ポートを使用するプログラムの Page Identifier）、プロトコル、接続中のリモート IP アドレス、リモートのポート番号、パソコンのポート番号、接続状態が表示されます。

  プロセス名のリンクを選択すると、該当のファイル分析レポートを確認できます。レポートはブラウザの画面内に表示されます。
- 【**検索**】入力したキーワードに応じ、リストの表示を絞り込みます。
- 【**更新**】リストの表示を更新します。

有害サイト遮断

機能と動作

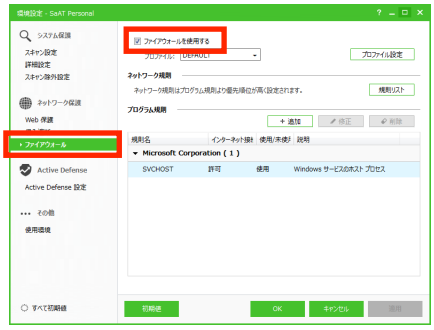
フィッシングサイトや悪性コードを配布する有害サイト、その他指定サイトへのアクセスを遮断します。

本機能は使用の ON / OFF を切り替えられます。環境設定画面から、動作方法の設定もできます。

また、遮断対象の候補は「疑わしいサイト」として自動的に記録され、機能ステータス画面から確認できます。

使用の ON / OFF

以下の操作で切り替えられます。OFF に切り替える場合、ダイアログで確認されます。



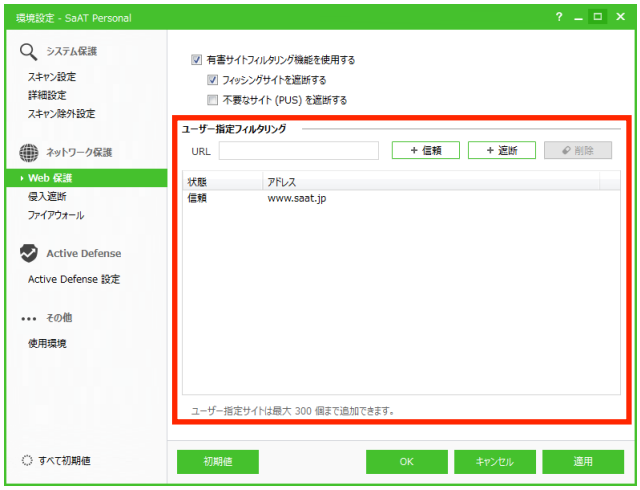
- **【保護設定画面から】**「有害サイト遮断」の ON / OFF を選択します。
- **【環境設定画面から】**「Web 保護」を選択し、「有害サイトフィルタリング機能を使用する」を選択します。ON に切り替えると、画面内の他の設定が可能になります。フィッシングサイトや不要なサイト（PUS）遮断の ON / OFF も切り替えられます。

※不要なサイト（PUS）とは、悪性コードの配布や不要なアプリ（PUP）のインストール、不要なサイトへの誘導を行うサイトです。

※フィッシングサイトや不要なサイトの検知方式は、そのサイトを集積したブラックリスト情報に基づきます。

動作方法の設定

環境設定画面の「Web 保護」内、「ユーザー指定フィルタリング」から、信頼または遮断サイト（アクセスを許可または遮断するサイト）を設定できます。

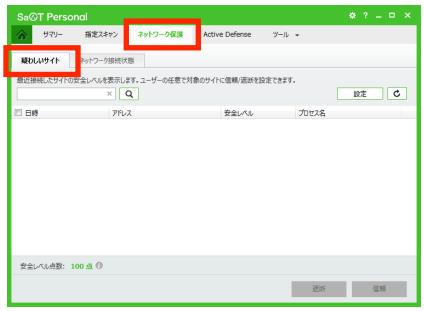


- **【サイトリスト】**サイトごとに、信頼/遮断の状態とアドレスが表示されます。
- **【信頼】**リストに信頼サイトを追加します。URL 入力欄にサイトのアドレスを入力し、「信頼」を選択します。
- **【遮断】**リストに遮断サイトを追加します。URL 入力欄にサイトのアドレスを入力し、「遮断」を選択します。
- **【削除】**信頼/遮断サイトを削除します。リストのサイト→「削除」の順に選択します。削除前に、ダイアログで確認されます。

※信頼/遮断サイトは最大 300 個まで追加できます。設定が重複している場合は追加できません。

※URL の入力は半角文字のみ有効です。全角文字を使用する日本語ドメインのサイトは、信頼/遮断サイトに設定できません。

疑わしいサイトの確認



SaAT Personal はブラウザのアクセス履歴から、有害サイトのおそれがある「疑わしいサイト」を自動的に記録します。

機能ステータス画面から「ネットワーク保護」→「疑わしいサイト」を選択すると、サイトのリストが表示されます。リストから危険性を確認の上、必要に応じ環境設定画面の「Web 保護」内、「ユーザー指定フィルタリング」にサイトを追加できます。

- **【サイトリスト】**サイトごとに、アクセス日時、アドレス、安全レベル（危険なサイトはオレンジ、分析サーバーに情報がないサイトはグレーで表示）、ネットワーク接続中のプロセス名が表示されます。
- **【検索】**入力したキーワードに応じ、リストの表示を絞り込みます。
- **【設定】**環境設定画面の「Web 保護」が表示されます。
- **【更新】**リストの表示を更新します。
- **【信頼】**リストから信頼サイトを設定します。リストのサイト→「信頼」の順に選択すると、環境設定画面の「Web 保護」内、「ユーザー指定フィルタリング」にサイトが追加されます。
- **【遮断】**リストから遮断サイトを設定します。リストのサイト→「遮断」の順に選択すると、環境設定画面の「Web 保護」内、「ユーザー指定フィルタリング」にサイトが追加されます。

ネットワーク侵入遮断

機能と動作

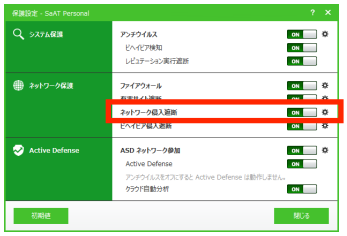
ネットワークを介したワームやスパイウェアなどの侵入を検知し、パソコンへの感染を阻止します。

本機能は使用の ON / OFF を切り替えられます。環境設定画面から、動作方法の設定もできます。

検知方式は、パケット特定の署名情報に基づきます。侵入を検知すると、該当パケットを遮断します。

使用の ON / OFF

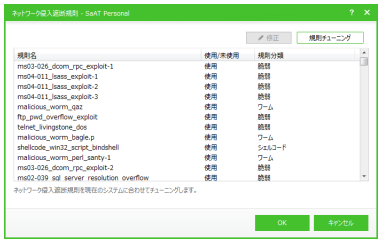
以下の操作で切り替えられます。OFF に切り替える場合、ダイアログで確認されます。



- **【保護設定画面から】**「ネットワーク侵入遮断」の ON / OFF を選択します。
- **【環境設定画面から】**「侵入遮断」→「ネットワーク侵入遮断」を選択し、「ネットワーク侵入遮断機能を使用する」を選択します。ON に切り替えると、画面内の他の設定が可能になります。

  「規則表示」を選ぶとダイアログが表示され、侵入遮断の各制御（規則）の ON / OFF を切り替えたり、規則全体のチューニング（パソコンのシステムアップデートで不要となった規則の一括自動 OFF）が行えます。

  設定した規則は遮断制御の基本設定として、「IP アドレス許可/遮断」に優先して適用されます。



動作方法の設定

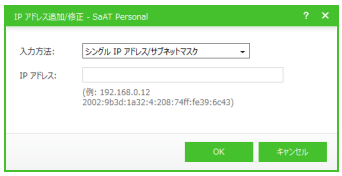
環境設定画面の「侵入遮断」→「ネットワーク侵入遮断」内、「IP アドレス許可/遮断」から、IP アドレスによるネットワーク接続の許可または遮断を設定できます。

- **【IP アドレス許可/遮断を使用する】**IP アドレスによる接続許可/遮断の使用を切り替えます。ON に切り替えると、以下の設定が可能になります。
- **【不正 IP アドレスの一時遮断機能を使用する】**遮断 IP アドレスからパソコン内への接続が発生した場合、一時遮断（30 分間）を行います。一時遮断した IP アドレスは、「遮断 IP アドレス設定」から接続許可や遮断継続への変更ができます。
- **【遮断 IP アドレス設定】**接続を遮断する IP アドレスを設定します。
- **【許可 IP アドレス設定】**接続を許可する IP アドレスを設定します。

遮断 IP アドレスの設定

「遮断 IP アドレス設定」では、以下の内容を設定できます。

遮断 IP アドレス設定/許可 IP アドレス設定



IP アドレスの追加/修正

- **【IP アドレスリスト】**接続を遮断する IP アドレスと、遮断を終了した時間が表示されます。
- **【追加】**リストに IP アドレスを追加します。ダイアログが表示されたら、IP アドレスの入力方法を選択の上、IP アドレスを設定します。
- **【修正】**IP アドレスの設定を修正します。リストの IP アドレス→「修正」の順に選択し、ダイアログが表示されたら設定内容を修正します。
- **【削除】**IP アドレスの設定を削除します。リストの IP アドレス→「削除」の順に選択します。削除前に、ダイアログで確認されます。
- **【接続許可】**IP アドレスを「許可 IP アドレス設定」に移動します。リストの IP アドレス→「接続許可」の順に選択します。
- **【遮断持続】**一時遮断が発生した場合、該当の IP アドレスを継続遮断の対象に変更します。リストの一時遮断済み IP アドレス→「遮断持続」の順に選択します。

許可 IP アドレスの設定

「許可 IP アドレス設定」では、以下の内容を設定できます。

- **【IP アドレスリスト】**接続を許可する IP アドレスが表示されます。
- **【追加】**リストに IP アドレスを追加します。ダイアログが表示されたら、IP アドレスの入力方法を選択の上、IP アドレスを設定します。
- **【修正】**IP アドレスの設定を修正します。リストの IP アドレス→「修正」の順に選択し、ダイアログが表示されたら設定内容を修正します。
- **【削除】**IP アドレスの設定を削除します。リストの IP アドレス→「削除」の順に選択します。削除前に、ダイアログで確認されます。

ビヘイビア侵入遮断

機能と動作

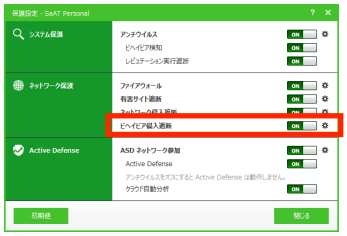
ネットワーク上の通信状況を監視して異常を検知し、パソコンへの不正な接続を遮断します。

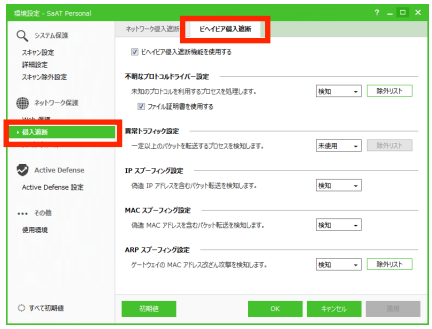
本機能は使用の ON / OFF を切り替えられます。環境設定画面から、動作方法の設定もできます。

検知方式は、パケットの流れに対する異常性の判断に基づきます。異常性を検知すると、動作方法の設定に応じて処理します。

使用の ON / OFF

以下の操作で切り替えられます。OFF に切り替える場合、ダイアログで確認されます。



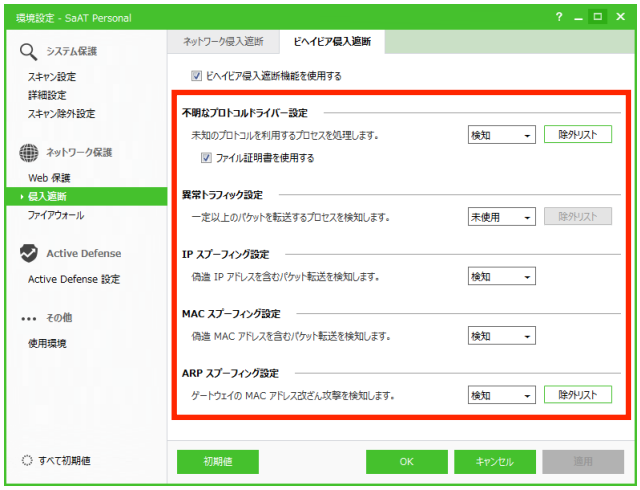


- **【保護設定画面から】**「ビヘイビア侵入遮断」の ON / OFF を選択します。
- **【環境設定画面から】**「侵入遮断」→「ビヘイビア侵入遮断」を選択し、「ビヘイビア侵入遮断機能を使用する」を選択します。ON に切り替えると、画面内の他の設定が可能になります。

動作方法の設定

環境設定画面の「侵入遮断」→「ビヘイビア侵入遮断」から、各種異常性への処理内容を設定します。

処理内容は、検知（検知対象を通知）、遮断（検知対象を遮断）、未使用（通知や遮断をしない）から選択します。



- **【不明なプロトコルドライバー設定】**不明なプロトコルドライバーを対象に、異常パケットへの処理内容を設定します。

  ファイル証明書による遮断除外（初回のみ遮断して証明書を確認し、確認後は許可）の ON / OFF や、「除外リスト」による処理除外対象の設定もできます。

- **【異常トラフィック設定】**動作中のプロセスによるトラフィックを対象に、一定回数以上の送信が発生したパケットへの処理内容を設定します。

  「除外リスト」による処理除外対象の設定もできます。

- **【IP スプーフィング設定】**IP スプーフィング攻撃（攻撃者が自分の IP アドレスを改ざんしてパケットを送信する）への対策として、IP アドレスが実際とは異なるパケットへの処理内容を設定します。

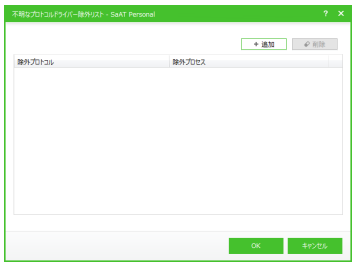
- **【MAC スプーフィング設定】**MAC スプーフィング攻撃（攻撃者が自分の物理アドレスを改ざんしてパケットを送信する）への対策として、物理アドレスが実際とは異なるパケットへの処理内容を設定します。

- **【ARP スプーフィング設定】**ARP スプーフィング攻撃（攻撃者が ARP＝ネットワークアドレスを決めるプロトコルを操作し、自身のパソコンをゲートウェイに偽装してパケットを送信する）への対策として、偽装した ARP 通信への処理内容を設定します。

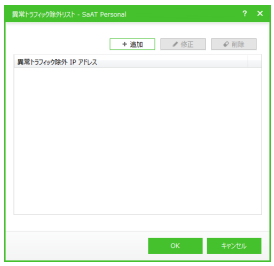
  「除外リスト」による処理除外対象の設定もできます。

除外リストの設定

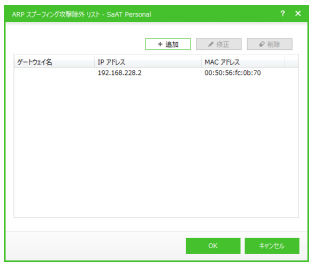
「除外リスト」では、以下の内容を設定できます。



不明なプロトコルドライバー



異常トラフィック



ARP スプーフィング

- **【不明なプロトコルドライバー】**除外するプロトコルのリストが表示されます。

  「追加」を選択するとダイアログが表示され、検知したプロトコルから除外対象を設定できます。リストのプロトコル→「削除」の順に選択すると、設定を削除できます。

- **【異常トラフィック】**除外する IP アドレスのリストが表示されます。

  「追加」を選択するとダイアログが表示され、除外する IP アドレスを設定できます。リストの IP アドレス→「修正」「削除」の順に選択すると、設定の修正や削除ができます。

- **【ARP スプーフィング】**除外するゲートウェイのリストが表示されます。

  「追加」を選択するとダイアログが表示され、除外するゲートウェイの名称、IP アドレス、MAC アドレスを設定できます。リストのゲートウェイ→「修正」「削除」の順に選択すると、設定の修正や削除ができます。

Active Defense 機能

Active Defense

機能と動作

未知の悪性コードから積極的にパソコンを防御するため、アンチウイルスによるプログラムのスキャン時、疑わしい動作の有無を分析します。分析結果を確認し、プログラムの実行許可/遮断を設定できます。

本機能は使用の ON / OFF を切り替えられます。動作方法の設定もできます。また、本機能に関する動作状況は自動的に記録され、機能ステータス画面から確認できます。

本機能を使用するには、アンチウイルスを ON に切り替えた上で、分析サーバーとのネットワーク（ASD ネットワーク）に参加する必要があります。さらにクラウド自動分析を使用することで、未知のファイルであれば分析サーバーに自動送信し、リアルタイムで分析結果の提供を受けることが可能になります。

使用の ON / OFF

Active Defense、ASD ネットワーク、クラウド自動分析の ON / OFF は、以下の操作で切り替えられます。

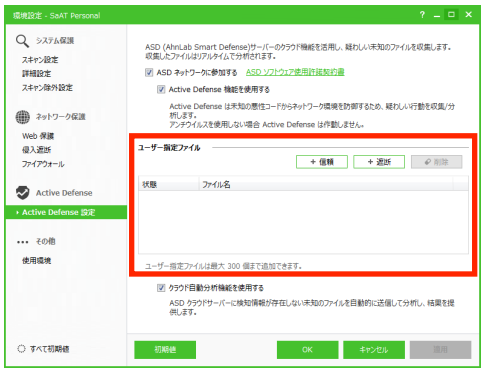
- **【保護設定画面から】**「ASD ネットワーク参加」を ON に切り替えた上で、「Active Defense」「クラウド自動分析」の ON / OFF を選択します。
- **【環境設定画面から】**「Active Defense 設定」を選択し、「ASD ネットワークに参加する」を ON に切り替えた上で、「Active Defense 機能を使用する」や「クラウド自動分析機能を使用する」を選択します。

  「ASD ネットワークに参加する」や「Active Defense 機能を使用する」を ON に切り替えると、画面内の他の設定が可能になります。

※ASD ネットワーク参加を初めて ON に切り替える場合、ダイアログで許諾への同意を確認されます。表示された内容を確認し、「同意する」を選択すると、ON に切り替えられます。

動作方法の設定

環境設定画面の「Active Defense 設定」内、「ユーザー指定ファイル」から、本機能による分析に応じた、プログラムファイルへの信頼（実行許可）/遮断を設定できます。



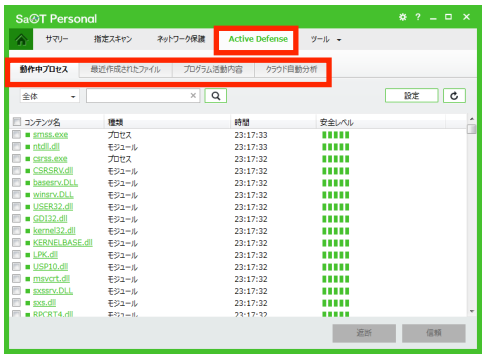
- **【ファイルリスト】**ファイルの信頼/遮断設定の状態と、ファイルパスが表示されます。
- **【信頼】**動作を許可するファイルを追加します。ダイアログが表示されたら、ファイルを選択します。
- **【遮断】**動作を遮断するファイルを追加します。ダイアログが表示されたら、ファイルを選択します。
- **【削除】**ファイルの設定を削除します。リストのファイル→「削除」の順に選択します。削除前に、ダイアログで確認されます。

※信頼/遮断ファイルは最大 300 個まで追加できます。設定が重複している場合は追加できません。

※遮断ファイルに設定すると、指定スキャンやアンチウイルスによる検知時に削除されます。

動作状況の確認

機能ステータス画面の「Active Defense」を選択すると、本機能に関する各種動作状況のリストが表示されます。



リストのタブを選択すると、表示対象を切り替えられます。

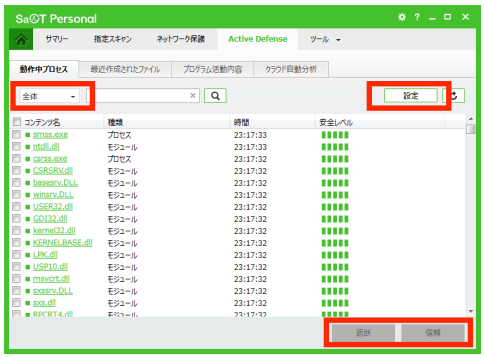
- **【動作中プロセス】**本機能による収集候補となる、動作中のプロセスのリストです。プロセスの名称、種類、実行後の経過時間、分析サーバーのレピュテーション情報による安全レベルが表示されます。
- **【最近作成されたファイル】**本機能による収集候補となる、最近作成されたファイルのリストです。ファイルの作成日時、名称、分析サーバーのレピュテーション情報による安全レベル、ファイルを作成したプロセスのパス（Dropper）が表示されます。
- **【プログラム活動内容】**疑わしいプログラム活動の判断材料となる、パソコン上で動作したプロセスとその活動内容です。活動の日時、プロセスの名称、関連モジュール、動作とその対象が表示されます。
- **【クラウド自動分析】**クラウド自動分析の対象となったファイルと、その分析内容です。分析の要求日時、対象ファイルのパス、進行状態、結果が表示されます。

動作状況のリスト

リストでは、共通で以下の操作を行えます。

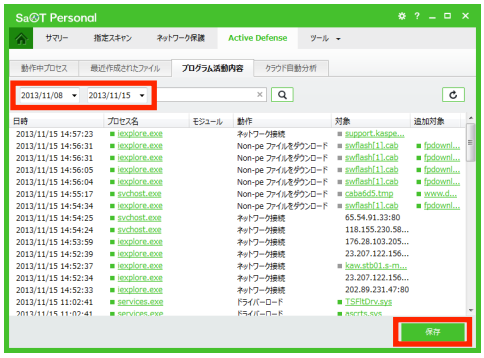
- **【リスト】**リンクを選択すると、該当ファイルの分析レポートを確認できます。レポートはブラウザの画面内に表示されます。
- **【検索】**入力したキーワードで、リストの表示を絞り込みます。
- **【更新】**リストの表示を更新します。

「動作中プロセス」と「最近作成されたファイル」のリストでは、以下の操作を行えます。



- **【未確定/全体】**リストの表示対象を、安全性が未確定のもの/全体から選択します。
- **【設定】**環境設定画面の「Active Defense 設定」メニューが表示されます。
- **【遮断】**リストからファイルをチェック→「遮断」を選択すると、該当ファイルを遮断ファイルとして、環境設定画面の「Active Defense 設定」内、「ユーザー指定ファイル」に追加できます。
- **【信頼】**リストからファイルをチェック→「信頼」を選択すると、該当ファイルを信頼ファイルとして、環境設定画面の「Active Defense 設定」内、「ユーザー指定ファイル」に追加できます。

「プログラム活動内容」と「クラウド自動分析」のリストでは、以下の操作を行えます。



- **【日付指定】**選択した日付の期間で、リストの表示を絞り込みます。
- **【保存】**リストの内容を CSV 形式で保存します。ダイアログが表示されたら、保存するファイル名と場所を入力します。

ツール機能

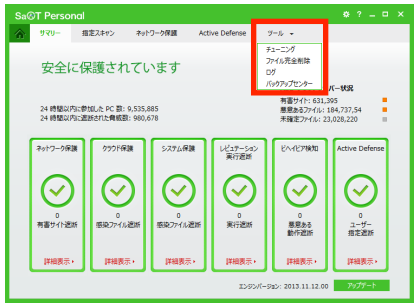
チューニング

機能と動作

パソコンの一時ファイルやメモリなどを整理し、使用状況を改善します。

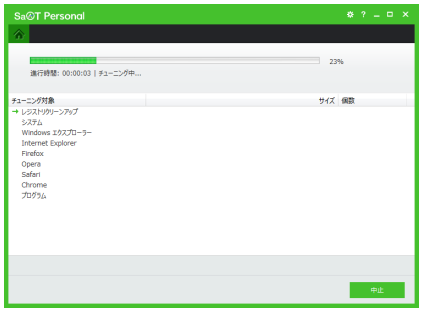
チューニングの実行

以下の操作で実行できます。機能ステータス画面からは、動作方法の設定もできます。



- **【HOME 画面から】**「チューニング」を選択すると、メニュー内に実行状況が表示されます。実行表示中にメニューを再選択すると、チューニング画面に切り替わります。
- **【機能ステータス画面から】**「ツール」→「チューニング」を選択すると、動作方法の設定が表示されます。「チューニング開始」を選択すると、チューニング画面に表示が切り替わります。
- **【タスクトレイメニューから】**「チューニング」を選択します。選択すると、チューニング画面がウィンドウで表示されます。

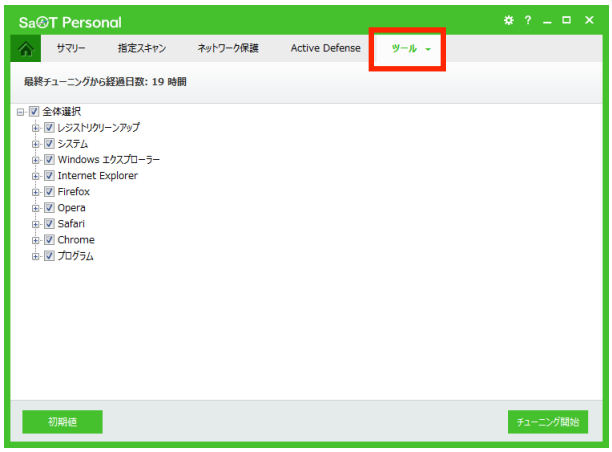
  チューニング画面では、実行状況やチューニング対象の情報が表示されます。



動作方法の設定

機能ステータス画面から「ツール」→「チューニング」を選択すると、動作方法を設定できます。

リストから候補を選択して、チューニングの対象を選択します。



- **【全体選択】**候補すべての選択を切り替えます。
- **【レジストリクリーンアップ】**Windows のレジストリから、使用しない情報などをクリーンアップします。
- **【システム】**パソコンのシステムから、一時ファイルや使用情報などを削除します。
- **【Windows エクスプローラー】**スタートメニューや検索内容などの使用情報を削除します。
- **【Internet Explorer/Firefox/Opera/Chrome】**各ブラウザから、キャッシュや Cookie などを削除します。
- **【プログラム】**各種プログラムから、最近使ったファイルリストなどを削除します。

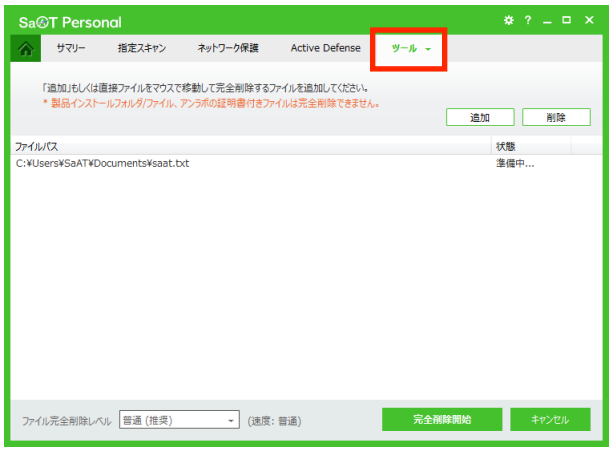
ファイル完全削除

機能と動作

指定したファイルやフォルダを完全に削除し、復元不可能な状態にします。

完全削除の実行

機能ステータス画面から「ツール」→「ファイル完全削除」を選択すると、削除対象の設定が表示されます。対象を設定の上、完全削除を実行します。



- **【ファイルリスト】**削除対象のファイルパスと、削除の実行状態が表示されます。
- **【追加】**リストにファイルを追加します。ダイアログが表示されたら、ファイルを選択します。
- **【削除】**リストからファイルを削除します。リストのファイル→「削除」の順に選択します。
- **【ファイル完全削除レベル】**完全削除のレベルを 5 段階から選択します。レベルに応じ、完全削除の実行速度が変化します。
- **【完全削除開始】**リストのファイルに対し、完全削除を開始します。開始前に、ダイアログで確認されます。完了すると、ボタンは非表示になります。
- **【キャンセル/終了】**削除対象の設定をリセットします。実行前の「キャンセル」では、ダイアログで確認されます。

ログ

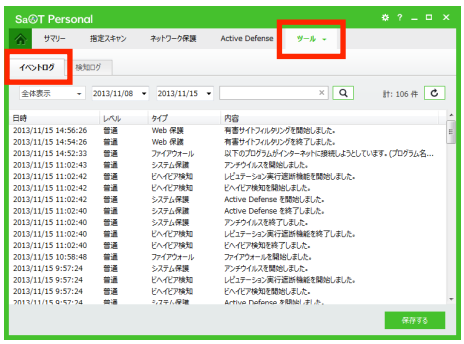
機能と動作

SaAT Personal の動作履歴（ログ）を確認します。

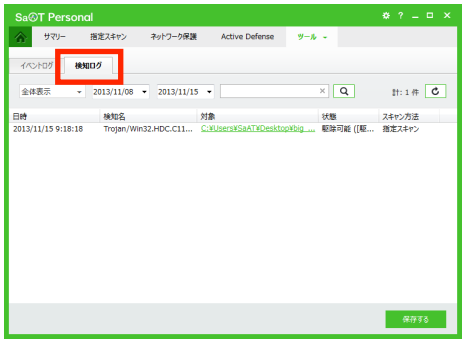
各種機能の動作履歴や、悪性コードなどの検知履歴が表示されます。

ログの確認

機能ステータス画面から「ツール」→「ログ」を選択すると、ログのリストが表示されます。リストのタブを選択すると、表示対象を切り替えられます。



イベントログ



検知ログ

- **【イベントログ】**リストの表示を、各種機能の動作（イベント）履歴に切り替えます。
- **【検知ログ】**リストの表示を、悪性コードや有害サイトの検知履歴に切り替えます。
- **【ログリスト】**切り替えた種類のログが表示されます。「イベントログ」では、イベントの発生日時、危険レベル（普通、警告、エラー）、機能名などのタイプ、イベント内容が表示されます。

  「検知ログ」では、検知の発生日時、対象となった悪性コードや遮断サイトのアドレス、駆除や遮断結果の状態、検知した機能名が表示されます。リスト内のリンクを選択すると、該当のファイル分析レポートを確認できます。レポートはブラウザの画面内に表示されます。
- **【全体表示/システム保護/ネットワーク保護など】**リストの表示対象を、全体/機能別から選択します。
- **【日付指定】**選択した日付の期間で、リストの表示を絞り込みます。
- **【検索】**入力したキーワードで、リストの表示を絞り込みます。
- **【更新】**リストの表示を更新します。
- **【保存する】**リストの内容を CSV 形式で保存します。ダイアログが表示されたら、保存するファイル名と場所を入力します。

バックアップセンター

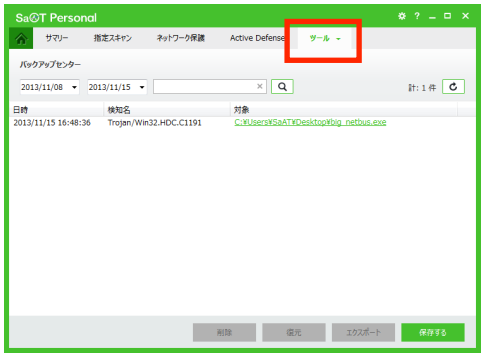
機能と動作

各種スキャンで駆除した、感染ファイルのバックアップを管理します。

バックアップされたファイルは元の位置から退避され、SaAT Personal の管理下に置かれます。本機能ではバックアップの確認、削除、復元ができます。

バックアップの管理

機能ステータス画面から「ツール」→「バックアップ」を選択すると、バックアップセンター（バックアップのリスト）が表示されます。



- **【バックアップリスト】**ファイルのバックアップ日時、検知時の名称、バックアップ元の位置（対象）が表示されます。リスト内のリンクを選択すると、該当のファイル分析レポートを確認できます。レポートはブラウザの画面内に表示されます。
- **【日付指定】**選択した日付の期間で、リストの表示を絞り込みます。
- **【検索】**入力したキーワードで、リストの表示を絞り込みます。
- **【更新】**リストの表示を更新します。
- **【削除】**バックアップを削除します。リストのファイル→「削除」の順に選択します。削除前に、ダイアログで確認されます。
- **【復元】**バックアップを元の位置に戻します。リストのファイル→「復元」の順に選択すると、ダイアログで確認されます。確認時、スキャンからの除外化を選択できます。確認後、結果がダイアログで通知されます。

  除外化したファイルは、環境設定画面の「スキャン除外設定」メニュー内、「スキャン除外対象設定」に追加されます。
- **【エクスポート】**ファイルを元とは違う位置に戻します。リストのファイル→「エクスポート」の順に選択すると、ダイアログで確認されます。確認時、スキャンからの除外化を選択できます。確認後、戻し先を選択すると、結果がダイアログで通知されます。
- **【保存する】**リストの内容を CSV 形式で保存します。ダイアログが表示されたら、保存するファイル名と場所を入力します。

使用環境設定

ユーザー設定

HOME 画面の表示内容やログの保管期間など、SaAT Personal 全般の動作方法を設定します。

環境設定画面から「使用環境」→「ユーザー設定」を選択すると、設定が表示されます。

- **【HOME 設定】**HOME 画面に対し、初期状態での表示を「デフォルト画面」と「機能ステータス画面」から選択します。
- **【保管期間設定】**各種ログとバックアップに対し、保管する日数を設定します。
- **【ロック設定】**SaAT Personal のアンインストールや環境設定の変更に対し、パスワードロックの使用可否を設定します。使用を ON にすると、「パスワード設定」と「ロック除外設定」が有効になります。

  「パスワード設定」を選択すると、ダイアログからパスワードを設定できます。パスワードは、英数字と特殊文字すべてを含む、10～30 文字以内で設定します。

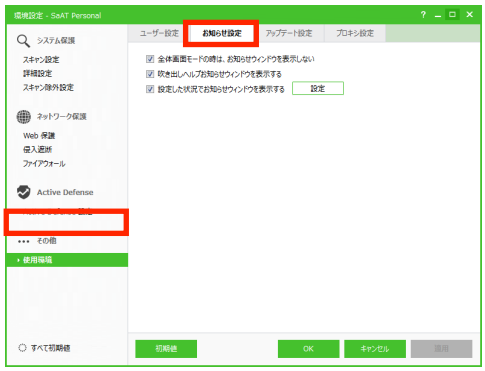
  「ロック除外設定」を選択すると、スケジュールスキャンやファイアウォールに対し、ロック対象からの除外を設定できます。
- **【エクスプローラーメニュー】**Windows エクスプローラーのコンテキストメニューに対し、SaAT Personal の機能メニューを追加します。エクスプローラースキャン、ファイル完全削除、ファイル分析レポートから、追加するメニューを選択します。

  選択に応じ、Windows 上でファイルやフォルダ、ドライブを右クリックすると、該当機能のメニューが表示されます。

お知らせ設定

SaAT Personal による通知表示の動作を設定します。

環境設定画面から「使用環境」→「お知らせ設定」を選択すると、設定が表示されます。

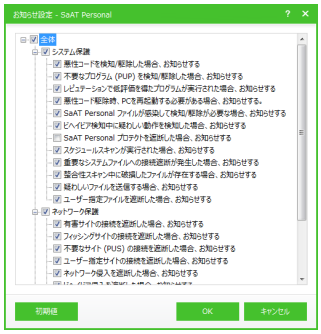


- **【全体画面モード時は、お知らせウィンドウ表示しない】**
  全画面表示中、通知表示を禁止します。
- **【吹き出しヘルプお知らせウィンドウを表示する】**タスクトレイからのバルーン通知表示を使用します。
- **【設定した状況でお知らせウィンドウを表示する】**設定した状況で通知を表示します。表示を ON にすると、「設定」が有効になります。

  「設定」を選択するとダイアログが表示され、通知表示する状況を設定できます。

通知表示の状況

通知表示状況のダイアログでは、以下の内容を設定できます。



- **【全体】**すべての状況で通知を表示します。
- **【システム保護/ネットワーク保護/アップデート】**各種機能の動作から、通知を表示する状況を選択します。

システム保護の通知表示状況

各種の検知/駆除/遮断、駆除時のパソコン再起動、スケジュールスキャンの実行や整合性スキャンの警告が発生した状況で構成されます。

ネットワーク保護の通知表示状況

有害サイトなどへのアクセスやネットワーク接続の遮断、プログラムによる接続発生時で構成されます。

アップデートの通知表示状況

アップデートの失敗や必要性の発生時で構成されます。

アップデート設定

SaAT Personal のアップデートに関し、動作方法を設定します。

環境設定画面から「使用環境」→「アップデート設定」を選択すると、設定が表示されます。

- **【自動アップデートを使用する（推奨)】**パソコンが起動して 5～30 分の間に、自動的にアップデート情報を確認します。その後は「アップデート周期」の時間に応じ、確認が繰り返されます。
- **【スケジュールアップデートを使用する】**実行日時のスケジュールを設定して、自動的にアップデート情報を確認します。
- **【アップデート時に SaAT Personal パッチファイルもダウンロードする】**アップデート時、セキュリティ機能のエンジンに加えて、SaAT Personal 本体のパッチファイルもダウンロードの対象とします。
- **【アップデートファイルの整合性スキャンを実行する】**アップデート時、ダウンロードしたファイルの損傷や感染の有無をスキャンします。
- **【安定（Stable）エンジンを使用する】**アップデート時、最新から一つ前のエンジンをダウンロードの対象とします。
- **【アップデートに失敗した場合、再実行する回数（1～99)】**アップデートの失敗時、自動的に再実行する回数を設定します。

プロキシ設定

SaAT Personal のアップデートや分析レポートの閲覧に関し、プロキシサーバーやポート番号を設定できます。

環境設定画面から「使用環境」→「プロキシ設定」を選択すると、設定が表示されます。

- **【プロキシサーバー設定】**アップデート時、プロキシサーバー経由でネットワークに接続します。

  プロキシーサーバーの使用を ON にすると、サーバーのアドレス、ポート番号、サーバー名、パスワードの設定が可能になります。

- **【レポートサーバー設定】**ファイルやサイトの分析レポートをエクスポートする、レポートサーバーのポート番号が表示されます。該当のポートが使用中の場合、その番号を変更できます。