



第 80 版

ユーザーガイド Windows 版

本書は個人版マニュアルです。個人版と法人版は操作および仕様が異なります。

1 目次

2	はじめに	1
2.1	PC Matic セキュリティエンジンの特長	2
2.2	詐欺対策を装備したブラウザ保護機能	4
3	インストール	5
3.1	他社製セキュリティソフトのアンインストール	5
3.2	インストール手順	6
3.3	SuperShield のインストール	12
3.4	ライセンス認証キーでのライセンス認証方法	13
3.5	SuperShield の稼働確認	14
4	インストーラ管理画面	16
4.1	インストーラ管理画面のアイコン	17
5	初期スキャンを実施	18
5.1	スケジュール設定	20
5.1.1	最適化直後に設定する場合	20
5.1.2	インストーラ管理画面から設定する場合	20
5.2	オプションの設定	21
6	タスクトレイに常駐している SuperShield アイコン	22
6.1	保護レベルの設定	23
6.1.1	SuperShield の一時休止	23
6.1.2	ブラックリスト保護とスーパーシールド保護	24
6.1.3	保護警告表示	24
6.1.4	脆弱性保護	26
6.1.5	アプリケーションの起動がブロックされる場合	27
6.1.6	PC Matic セキュリティエンジン詳細図解	28
6.1.7	未知のアプリケーション監査で 24 時間以上経過しているのにまだブロックされる場合	29
6.2	活動ログ	34
6.3	脆弱なソフトウェアアップデート	34
6.4	許可阻止リストの管理	34
7	詐欺対策(ブラウザ保護)	35
7.1	インストールについて	36
7.1.1	Google Chrome の場合	36
7.1.2	Firefox の場合	38
7.1.3	Chromium Edge の場合 (Windows 11/10 20H2 以降)	40
7.1.4	Old Edge (Windows 10 20H1 以前)	41

7.2	ブラウザ保護機能を有効にしているのに広告が表示される場合	41
8	オプション	42
8.1	最適化実行前に復元	43
8.2	テクニカルサポート用のログファイルのアップロード	44
8.3	スケジューラー	45
8.4	スキャンオプション	45
8.5	ローカル・ホワイトリストの管理	46
8.5.1	スタートアップ・アプリケーション	46
8.5.2	サービス	46
8.6	ユーザー評価	46
8.7	言語	46
8.8	SuperShield	46
9	管理ポータル	47
9.1	ログイン	47
9.2	配色設定	47
9.3	管理ポータル画面	48
9.4	自動カード払い設定の解除	48
9.5	包括スケジュール設定	49
9.6	ローカルホワイトリストの設定	50
9.7	アラートの確認	51
9.8	端末管理	51
9.9	スーパーシールドログからローカルホワイトリスト登録	52
10	ローカル・ホワイトリストへの登録手順	54
10.1	起動阻止されたファイルを管理ポータルより把握	54
10.1.1	Good となっている場合	55
10.1.2	Unknown となっている場合	55
10.1.3	マルウェアであると判断できる場合(ローカル・ブラックリスト追加)	56
10.1.4	Bad となっている場合	56
10.1.5	ファイル名が cmd.exe、wscript.exe、regsvr32.exe のスクリプト形式の調査方法	56
10.2	VirusTotal を用いた検証	57
10.2.1	VirusTotal へのアップロードと検証手順	57
10.2.2	起動阻止されたファイルの探索	57
10.2.3	VirusTotal にアップロード	58
10.2.4	Behavior タブで素性や問題がないか確認	59
10.2.5	Relation タブで通信先、展開ファイルなどを調査	60

10.2.6	Detail タブで最終調査	61
10.3	管理ポータル「通知」－「セキュリティ」から追加	63
10.3.1	通知－セキュリティからハッシュ、スクリプト登録	63
11	よくある質問	64
11.1	2 台目にライセンス認証キーを入力しているのに利用登録できない	64
11.2	起動時にエラーや白か黒の単色画面表示し、PC Matic が起動しませんでした。	64
11.3	削除対象のパソコンから PC Matic 関連のアプリケーションの削除	65
11.4	インストーラ管理画面から削除対象の端末を削除	66
11.5	ファイアウォールに設定するための IP アドレスを教えてください	67
11.6	ウイルス、善良なアプリ、PUP の判定基準について	68

2 はじめに

PC Matic は、Windows パソコンを快適に使い続けるために必要な「**セキュリティ対策**」と「**詐欺対策**」そして「**パソコン快適化**」を1つにまとめたソフトです。

セキュリティ対策では、ゼロトラスト・セキュリティモデルのセキュリティエンジンを搭載しています。セキュリティ対策ソフトがもつ「ブラックリスト」と「ヒューリスティックスキャン」の2つのエンジンに加え、世の中に存在する膨大な数の実行可能ファイル(バイナリー、スクリプト形式)のハッシュを収集することにより、「アプリケーション・ホワイトリスティング方式」によるエンジンを実装しています。この方式は、アメリカ政府によって最近定められた政府機関向けの高いセキュリティ基準を満たした仕組みです。PC Matic では新たなアプローチによって「軽快さ」と「防御力の高さ」を両立しています。

また最近では、マルウェア・ランサムウェアによる脅威のほかに、悪意ある組織による詐欺が社会問題化しています。誰もが自分は詐欺にはひっかからない自身があると考えていますが、実際詐欺にあった人はこうした普通の人たちです。専門家でも見分けるのが困難になりつつあるマルウェア・ランサムウェアや詐欺。これらの防御を統合的に実装し、自動更新やリアルタイム処理で全世界の顧客を守る仕組みを PC Matic は採用しています。

そしてパソコン購入時の快適さを維持するための専用ソフトを内包させたパソコン快適化機能を搭載しています。

PC Matic があれば、Windows パソコンは安心安全かつ快適に使い続けられるという創業メンバーであるパソコンメーカー出身者たちの想いが込められています。

PC Matic は、アプリケーション・ホワイトリスティング方式による新しいセキュリティ製品であるため、操作ダッシュボードはアプリケーションではなく、ブラウザで**管理ポータル**を開いて操作・管理を行います。お客様による定期的な自動スキャンを行う必要はなく、パソコンが低負荷時に自動的に未監査のファイルを探索し、クラウド上で多面監査されマルウェア分析官によりデジタルフォレンジックが実施されます。

【はじめに】

Windows 版は、無料診断機能を持つ**インストール用ミニ管理画面**と、ライセンス保有者が利用する**管理ポータル**によって構成されています。

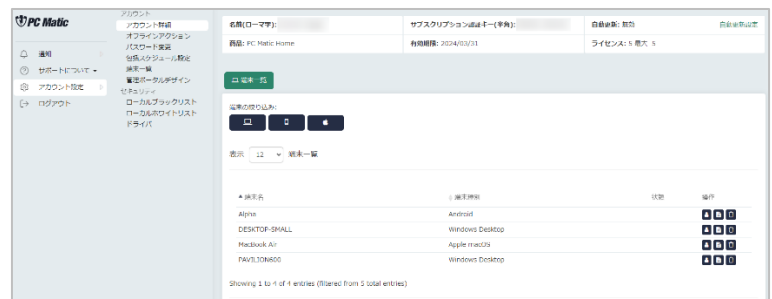
【初期】 インストール用ミニ管理画面

対象:無料診断機能、初期導入、購入更新



【日常】 管理ポータル

対象:ライセンス保有者によるフル操作



2.1 PC Matic セキュリティエンジンの特長

PC Matic のエンドポイント保護機能は、SuperShield 保護レベルと呼んでいる「**アプリケーション・ホワイトリスティング方式**」と、「**ブラックリスト方式**」の**2つの稼働モード**を搭載しています。標準ではアプリケーション・ホワイトリスティング方式に設定されており、この保護モードでは、NIST SP 800-167 で規定され、米国政府調達基準(NIST CMMC Level 5)で運用されている、信頼できるアプリケーションのみ起動可能とした高いセキュリティ保護がなされます。脆弱性を含むものやマルウェアの疑いがあるものを起動させない高い保護レベルのものをご利用いただけます。

またフリーソフトウェアなど脆弱性を抱えているものも多いアプリケーションを利用することができる一般的なセキュリティソフトと同一の保護レベル(NIST CMMC Level 3)であるブラックリスト方式では、**2009 年以前に作成されたセキュリティホール**を抱えるフリーソフトウェアなどもご利用頂けます。またアプリケーション・ホワイトリスティング方式では PC Matic 社のマルウェア分析官によるデジタルフォレンジックが24時間程度でなされるまで待たなければアプリケーションやスクリプトを稼働させることができませんが、このモードでは稼働させることが可能です。

両モードとも端末での監査ではなくクラウド上で監査を行うため、パソコンに負荷をかけないのが特長となっています。

SuperShield 保護モードでは、ゼロトラスト・アプリケーションの方針により、全ての実行可能ファイルを人工知能による複数のコードスキャンや、多様の仮想環境によるサンドボックスなどによりスコアリングされ、それを元 FBI サイバー捜査官も含むマルウェア分析官の手により、善・悪・グレー(嫌疑/脆弱性含)の3つに分類されます。グレーゾーンのものを起動させないことにより、高い安全性を担保しています。

ファイルレス・ランサムウェアと呼ばれるスクリプトによる身代金型マルウェアにも OS がもつスクリプトも標準でロックをかけています。これにより政府調達基準の高いセキュリティ要求基準を満たし、完全に悪意あるアプリケーションやスクリプトの実行ができなくなっています。

ブラックリスト保護モードでは、一般的な次世代セキュリティソフトと同様に脆弱性を含むものも起動可能とし、マルウェア、ランサムウェアそしてスパイウェアなど実被害をもたらすものを駆除します。



判定		SuperShield 保護モード	ブラックリスト 保護モード	ファイル削除
Bad	マルウェア、ランサムウェア	実行 拒否	実行 拒否	削除
Unknown	未監査、グレー、脆弱性含む	実行 拒否	実行 許可	
Good	善良と確認済アプリケーション	実行 許可	実行 許可	

サーバーにて実行の是非が判断されるリストには、「グローバルリスト」と「ローカルリスト」の2種類があります。

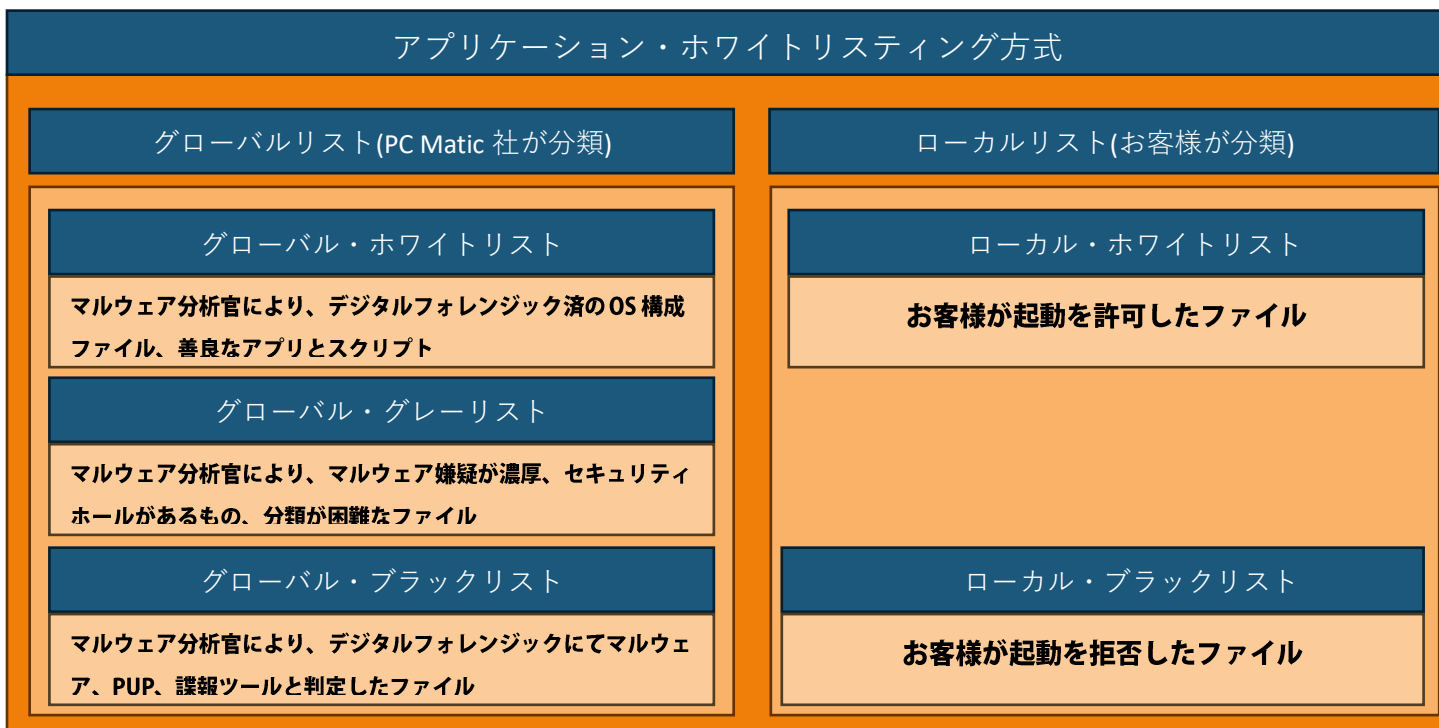
昔からあるホワイトリスト方式は、いわゆるローカルリストのみで、システム管理者がホワイトリストを作成しない限り、アプリケーションの実行が許可されませんでした。しかし、それでは膨大にある社内利用アプリケーションが更新するたびにリストを再生成して配布するという膨大な手間が必要でした。

PC Matic は、OS を構成するシステムファイルも含め、顧客が遭遇した新たなハッシュ値をもつバイナリー、スクリプト形式の両方の全ファイルに対し、デジタルフォレンジックを実施し、グローバルリストへ登録します。

マルウェア分析官が善良と判断した実行ファイルは、グローバルリストで全世界の顧客で共有され起動が許可されます。このためシステム管理者は、Microsoft Office や会計ソフトなどの業務アプリケーションが自動更新した後に、大急ぎでホワイトリストを作成して再配布する手間から解放されました。使い勝手は従来のブラックリスト方式を採用した製品と遜色ありません。このためホワイトリスト製品でありながら、Microsoft からは Windows におけるセキュリティソフトの正式認定を受け、Windows にてエンドポイント保護として特別権限を付与され OS で認識されます。

一方、グローバルリストに登録されないアプリケーションもあります。これは、セキュリティホールを抱えたアプリケーションなどです。ゼロトラスト・セキュリティモデルの定めにより、脆弱性と呼ばれるセキュリティホールがあるアプリケーションを利用することは、サイバー攻撃者に絶好の足場を与えることとなるため、このセキュリティモデルでは利用を直ちにやめるべきと規定されています。このため起動可能リストへ追加されませんが、利用したいこともあるかもしれません。例えば 2009 年以前に VC で作成された Windows アプリケーションは全て脆弱性を抱えています。起動したいこともあるでしょう。その際は、ローカルリストへ追加することで、限定された端末や組織グループにおいて起動を許可させる指示をシステム管理者が追加していただけます。追加した情報は即座に端末へ反映され利用可能となります。

ローカルリストへの追加は、「ハッシュ値」「ファイルパス」で指定することができます。



2.2 詐欺対策を装備したブラウザー保護機能

PC Matic では、先述のエンドポイント保護に加え、詐欺対策などが強化された機能を Edge、Google Chrome、Firefox の拡張機能を提供しています。装備している機能は以下のとおりです。

- バナー広告非表示
- 動画再生中の動画広告スキップ
- テクニカルサポート詐欺サイトへの誘導阻止
- 不正広告ネットワークによるアダルト・違法広告非表示
- 金融機関や有名 EC サイトに似せた詐欺サイトへの誘導阻止
- 不正侵入防止
- 不正スクリプト実行阻止
- SNS, 広告システムによるプライバシー侵害
- 仮想通貨マイニングスクリプト実行阻止
- スクリプト型 Web スキミング防止

ブラウザー経由でのマルウェアの侵入を多段で防ぐことができる他、前述の悪質な行為を可能な限り阻止します。

3 インストール

PC Matic のインストール方法からセキュリティ有効までの手順を記載しています。

3.1 他社製セキュリティソフトのアンインストール

Windows の仕様で Microsoft 認定セキュリティソフトを 2 つ導入することができないため、PC Matic をインストールする前に他のセキュリティソフトを必ずアンインストールする必要があります。

以下の手順で他社セキュリティソフトをアンインストールしてください。一時的にアンインストールしても、ウイルスに感染することはほぼありませんので、ご安心ください。

1. コントロールパネルを開きます。

■Windows 11, 10, 8 の場合

「設定」 - 「アプリケーション」より表示されたアプリケーション一覧より、セキュリティソフトをアンインストールします。マカフィーと Spybot は標準設定のままではアンインストールできませんので、以下のページよりアンインストール手順を参照ください。<https://pcmatic.jp/howto/uninstall/>

■Windows7 の場合

[スタートボタン]をクリック→[コントロールパネル]を選択。

2. プログラムのアンインストールまたは変更を選択します。

3. ご使用のセキュリティソフトで右クリックし、[アンインストール]を選択します。

LinkChecker 9.2		2014/06/16	35.3 MB	
mazec-T for Windows	MetaMoj Corp	2013/07/04	47.5 MB	3.0.3.823
Microsoft Expression SuperPreview 4 Trial	Microsoft Corporation	2015/08/10		4.0.1241.0
Microsoft Office Home and Business 2013 - ja-jp	Microsoft Corporation	2015/08/25		15.0.4745.1002
お使いのセキュリティソフト				
Microsoft Visual C++ 2005 Redistributable	アンインストール(U)	2015/08/19	290 KB	8.0.61001
Microsoft Visual C++ 2008 Redistributable - x64 9...	Microsoft Corporation	2014/06/23	13.2 MB	9.0.30729.6161
Microsoft Visual C++ 2008 Redistributable - x86 9...	Microsoft Corporation	2014/12/04	4.61 MB	9.0.21022
Microsoft Visual C++ 2008 Redistributable - x86 9...	Microsoft Corporation	2014/06/23	500 KB	9.0.30729.6161

3.2 インストール手順

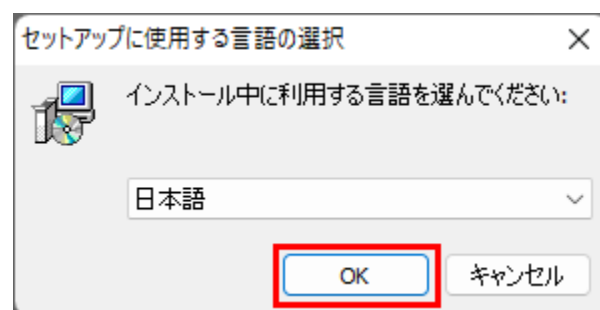
1. PC Matic のインストールを行います。

<https://pcmatic.jp/consumer/> のメニュー「入手方法」－「ダウンロード」からダウンロードしたファイルをダブルクリックします。なお、インストールを行う際は、Windows を管理者権限で利用している状態で行ってください。ユーザー権限では正常にインストールが行えません。

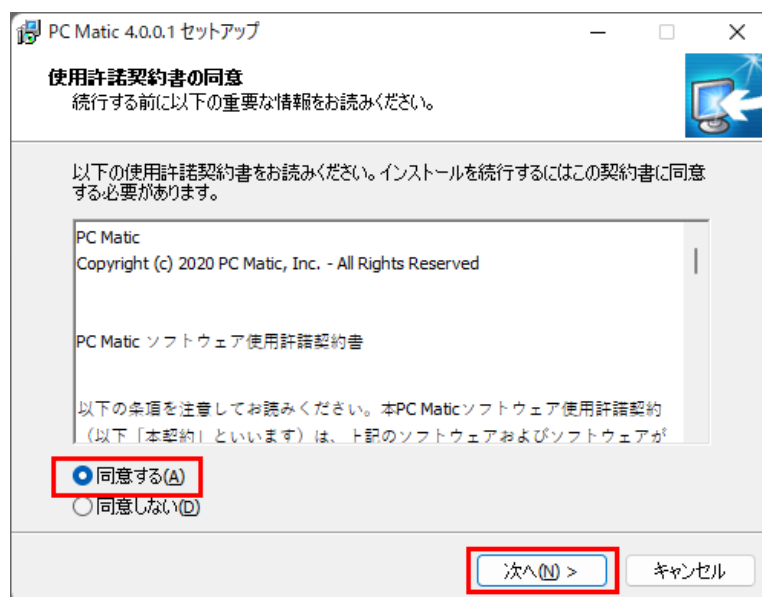
(図の場合はデスクトップに保存した pcmatic-setup-1300.exe を開いています)



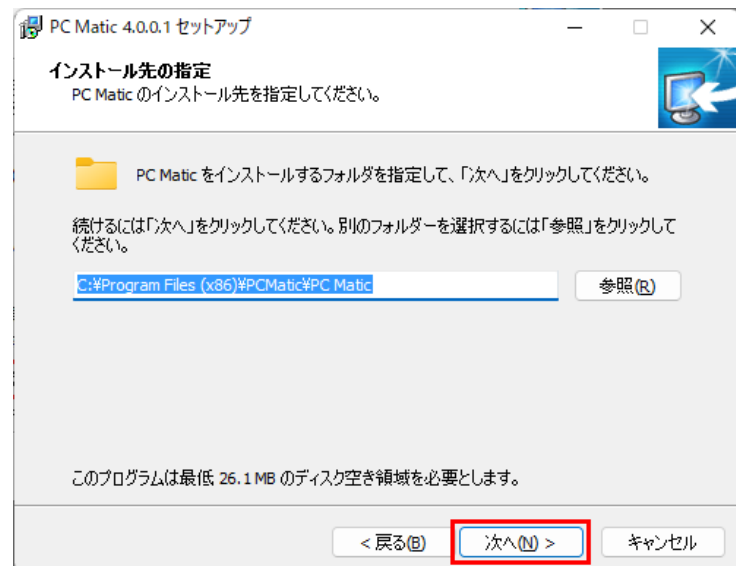
2. 表示された画面で使用する言語を選択します。
ここでは「日本語」を選択して「OK」ボタンを押します。



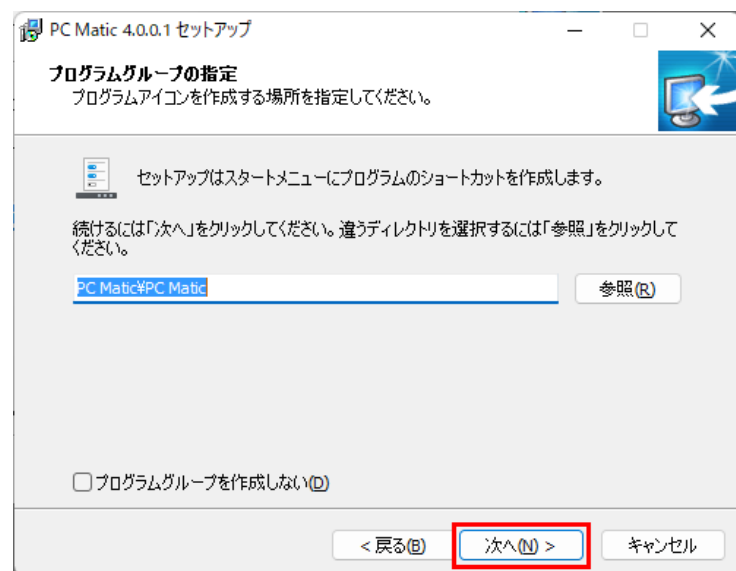
3. 規約に「同意する」を押して「次へ」を選択します。



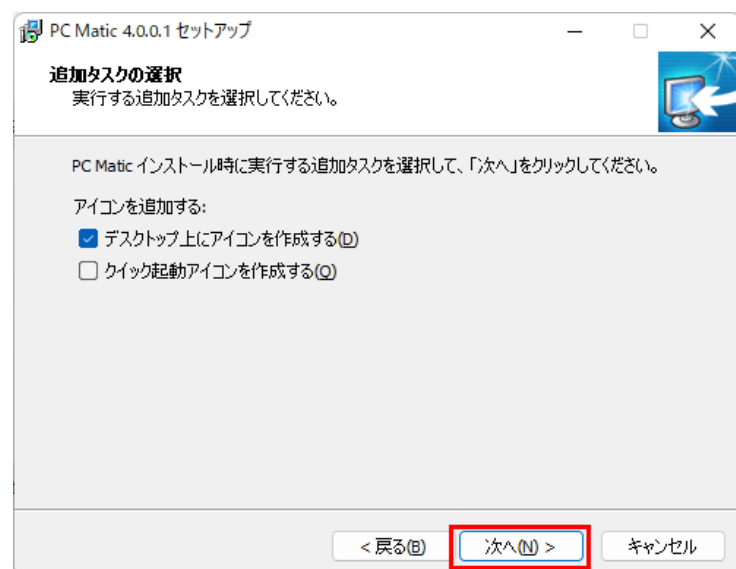
4. インストール先を選択します。
変更する必要がない場合は、この画面では何もしないで「次へ」を押してください。



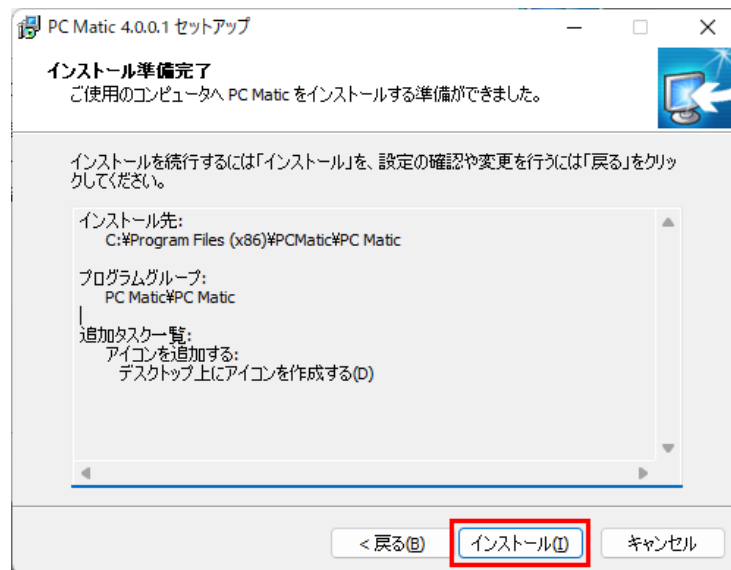
5. プログラムグループを指定します
変更する必要がない場合は、この画面では何もしないで「次へ」を押してください。



6. 追加タスクを選択します。
デスクトップにアイコンを作成するか、クイック起動にアイコンを作成するかを選択してください。選択が完了したら「次へ」を押してください。



7. 選択内容を確認し、よければ「インストール」を押します。



8. インストールが完了したら PC Matic を起動します。
- 「PC Matic を実行する」にチェックが入っているのを確認したら「完了」ボタンを押します。
- 「Active-X コントロール」をインストールするか聞かれた場合は「OK」ボタンを押してください。



9. 開いた画面から「新規にアカウントを作成する」を選択します。



10. 必要事項を入力します。

「パスワード」は、8文字以上で「英大文字」「小文字」「数字」の3要素を必ず含めてください。パスワードは、Windows メモ帳などへ一旦入力し、それを2箇所のパスワード項目へ貼り付けで入力されることをお勧めします。認証キーを保有している場合は、この画面で認証キーを入力します。認証キーは、一度有効化すると電子メールに紐付き、無効化されます。

PC Matic 利用登録

ログイン情報

*電子メール
ログインメールアドレス

*パスワード
パスワードを入力

*メールアドレス(確認)
メールアドレス(確認)

*パスワード確認
パスワード確認

アカウント情報

*姓
姓

*名
名

*電話
電話

携帯
携帯

どこでお知りになりましたか?

商品情報

サブスクリプションキー
サブスクリプションキー

ライセンス条項

PC Matic Copyright (c) 2022 PC Matic, Inc. - All Rights Reserved

NOTICE TO ALL USERS Carefully read the following legal agreement ("agreement"), which sets forth license terms for PC Matic software. BY INSTALLING PC Matic, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. If someone else uses a copy of PC Matic installed by you, he or she may do so only subject to all conditions, obligations and limits described in this Agreement.

☐ PC Maticのライセンス条項に同意します。

☒ 利用を申請します

※ 登録済の方は、こちら

11. 先ほどアカウント作成で入力したメールアドレスとパスワードを入力してログインします。



12. 「スキャン」ボタンを押して初期スキャンを実施してください。
SuperShield をインストールする前にスキャンを実行する必要があります。



13. スキャンが開始されます。
「スキャン」ボタンが「スキャン停止」ボタンに変わり、スキャンボタンの上にスキャン内容が表示されます。
スキャン中に Script エラーが表示されても「OK」を押してそのまま続行してください。
※Script エラーは自動的に修復されます。




14. 初期診断が完了し、無料ユーザーの場合は別ウインドウで購入画面が開きます。
ライセンス利用者は、購入画面は表示されません。インストーラ管理画面を利用するにはキーボードの「F5」を押してください。

15. オンラインでの購入、またはライセンスキー認証をし、有料版にします。

オンライン購入する場合は、「**無料版から有料版へのライセンス購入**」を参考にしてください。


ライセンス認証キーを用いる場合は、「**ライセンス認証キーによるライセンス認証方法**」を参考にしてください。


America's Antivirus

カート

唯一の米国内製のアンチウイルスで家族全員を守りましょう

- ✓ 100% アメリカ製
- ✓ 365日、迅速なメールサポート
- ✓ Windows, Mac, と Androidに対応
- ✓ 30日間 返金保証




請求合計

PC Matic ¥4980

合計 ¥4980

[注文](#)


利用可能なコンピュータ数の選択 5



年間ライセンス

PC Maticの年間サブスクリプションは、自動更新により、常に最新版へ保たれます。
最も人気のある

¥4980




永久版

セキュリティ対策と最適化を半永久的に利用可能なライセンス
ベストバリュー

¥24980

PC Maticの項目を選択します。



PC Maticのパッケージ CDROM (送料込)

¥1300

電子メール

パスワード

名

会社

住所 1

国

Japan

市区町村

電子メール(再入力)

パスワード再入力

姓

電話番号

090

住所 2

都道府県

神奈川県

郵便番号

支払い種別

クレジットカード ☒ コンビニ/ATM ☐

カード種類

MasterCard

カード番号

認証番号(CVV2)

有効期限

10 20

☒ PC Maticから製品の更新情報を含むメールニュースを希望する。

請求合計: ¥4980

[注文](#)

利用規約

Hey there! Do you have questions about PC Matic?

3.3 SuperShield のインストール

1. ホーム画面で「保護されていません」を押します。
他のセキュリティソフトがインストールされている場合は、「SuperShield」をインストールする前にアンインストールしてください。アンインストールについては、「[他社製セキュリティソフトのアンインストール](#)」参照。

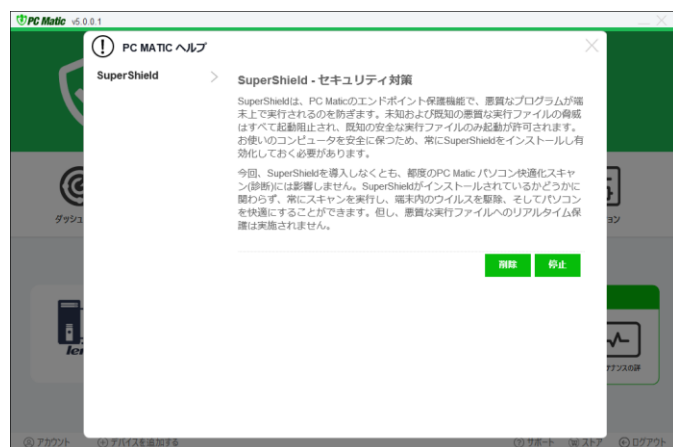
「保護」か「開始中」と表示されている場合は、既に SuperShield がインストールされていますので、この手順は行わないでください。



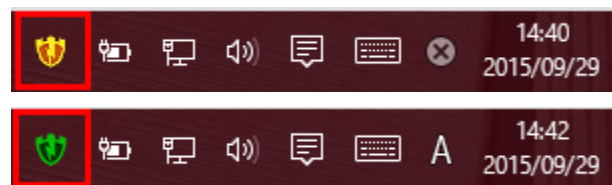
2. 「インストール」ボタンを押します。
無料版ユーザーにもこのボタンが表示されますが、SuperShield によるセキュリティ保護は実施されず、パソコンを再起動する度に購入を促す画面がポップアップで表示されます。



3. 画面が右図のようになりましたら、「SuperShield」のインストールは完了です。
パソコンを再起動してください。セキュリティ機能が有効になります。



- タスクトレイにあるアイコンを確認します。
タスクバーの右側にあるタスクトレイに PC Matic のアイコンがあります。こちらはシグネチャをダウンロードしているので黄色になっていると思いますが、ダウンロードが完了すると緑色になります。



※タスクトレイにあるアイコンが赤色の場合には、ライセンス認証ができていないため保護機能が有効となっておりませんのでご注意ください。

「SuperShield」をインストールすることによって、セキュリティが有効になりました。

有料版にした事によって、最適化機能が使用できるようになります。次は、パソコンのスキャン(最適化)を行って最適化を行いましょう。詳しくは、「5. 診断する」をご参照ください。

3.4 ライセンス認証キーでのライセンス認証方法

本作業を行うことによって、1 台目のパソコンで利用したログイン ID(電子メールアドレス)にライセンス管理が関連づけられます。2 台目以降のパソコンを利用する際には、ログイン ID とパスワードを入力してログインをしていただく事で、ライセンスの範囲内にてご利用いただけます。なお、ライセンス認証キーは、1 台目のパソコンで登録した際に無効化されています。

- PC Matic にログインし、左下の「アカウント」を押します。



2. 「更新用のライセンス認証キーをお持ちですか？」の下欄にライセンス認証キーを入力して「更新」ボタンを押します。



3.5 SuperShield の稼働確認

SuperShield 稼働状況を確認することで、PC Matic でブロックされたアプリケーションなどを確認する事ができます。また、起動が阻止されたアプリケーションはローカル・ホワイトリストをご参照いただき、必要に応じてブラックリスト保護モードへ切り替えるか、ローカル・ホワイトリストへの登録を行ってください。

1. PC Matic を起動し、「SuperShield」ボタンを押します。



2. 表示された画面で絞り込みを行うための「フィルター」ボタンを押します。



フィルター画面では、次の絞り込みを行い確認する事ができます。

- 現在の識別状態
現在 PC Matic を起動しているパソコンにインストールされているアプリケーションの分類状況を確認する事ができます。
- 検知時の識別状況
タスクトレイに常駐している SuperShield がアプリケーション起動時に認識した状態になります。例えば、24 時間クラウド監査するという旨のメッセージが表示された場合は、そのアプリケーションはこちらで「不明」に分類されます。









4 インストーラ管理画面

PC Matic を起動すると表示されるのが PC Matic のインストーラ管理画面です。こちらの画面から PC Matic の様々な操作が行えます。このインストーラ管理画面の説明は以下の通りです。



- ① 操作画面
- ② 現在使用しているパソコンの情報
- ③ スキャン履歴表示、パフォーマンス分析で、前回スキャン時のデータ、メンテナンスの詳細を表で見ることができます。パフォーマンス分析は3回以上スキャン後に表示されるようになります。
- ④ スキャンの開始ボタン

4.1 インストーラ管理画面のアイコン

	<p>スキャンを開始します。</p>
	<p>インストーラ管理画面を表示した際に 1 番最初に表示される画面を表示します。 この画面から様々なメニューを選択する事ができます。</p>
	<p>SuperShield の活動履歴を表示します。 SuperShield のインストール・アンインストール・停止が行えます。</p>
	<p>スケジュールの確認や設定を行う事ができます。</p>
	<p>アカウントの範囲内で使用している端末の情報が表示されます</p>
	<p>スキャン結果を確認する事ができます。</p>
	<p>オプションでは以下の事が行えます。</p> <ul style="list-style-type: none"> ・最適化実行前に復元 ・テクニカルサポート用のログファイル作成 ・スケジューラーの状況確認 ・スキャンおよび最適化を行うための設定オプションを変更・確認 ・ローカル・ホワイトリストの管理 ・コンピューターのユーザー評価 ・言語の選択 ・リアルタイムセキュリティ保護機能の管理 ・検疫

5 初期スキャンを実施

インストール後は、初期スキャンを実施します。

PC Matic は、パソコンの根本的な問題から解決を行っています。スキャンと最適化を 4 回ほど繰り返してください。繰り返す事により、より快適にパソコンを動作させられるようになります。なお、スキャンと最適化を行った後にパソコンを再起動する必要がありますのでご注意ください。



また、スケジュールスキャンを設定しておくと、決められた日時に自動的にスキャンと最適化を行ってくれるようになりますので、週 1 回スキャンを行うように設定ください。スケジュールスキャンの設定により、このインストーラ管理画面を用いてスキャンを実施する必要がなくなります。

スケジュールスキャンの設定をしている時間にパソコンを起動していない場合は、次回パソコン起動時に自動でスキャンが開始されます。

1. PC Matic にログインしてホームにある「スキャン」ボタンを押します。スキャンとは診断の意味です。

※PC Matic を利用するには、アカウント作成が必要です。



2. 「スキャン」ボタンが「スキャン停止」ボタンに変わります。



※最適化が行えるのは有料版のみです。

既に購入されていてライセンスの認証を行いたい場合は「[無料版から有料版へのライセンス購入・更新](#)」をご参照ください。

PC Matic は重要な問題から解決していきますので、3 回ほどスキャンと最適化を繰り返す事によってより問題が解決されていきます。

5.1 スケジュール設定

スケジュールを設定することによって、毎週決まった時間にスキャンと最適化を自動で行うように設定できます。ウイルスを検疫区画に移動する役割を担っていますので、必ず設定を行ってください。

5.1.1 最適化直後に設定する場合

1. 最適化直後の画面で「週ごとのスキャン設定」を押します。



2. 「スケジュールを作成しました」が表示されスケジュールが設定されます。



5.1.2 インストーラ管理画面から設定する場合

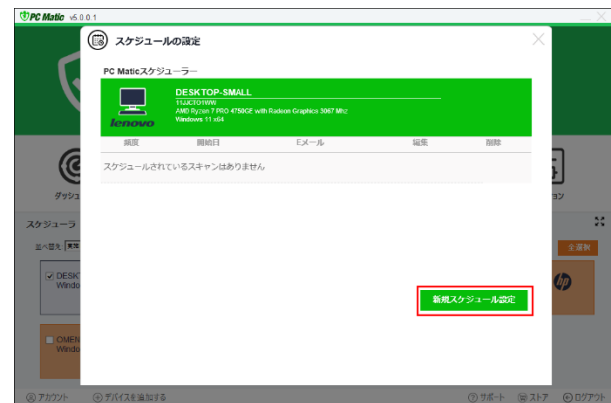
1. インストーラ管理画面の「スケジューラ」を押します。



2. 「個別設定」を押します。



3. 「新規スケジュール設定」を押します。



4. スケジュールの頻度を「毎週」にし、毎週行う曜日、時刻を設定して「保存」ボタンを押します。

時刻を「12:00PM」などのお昼休み時間等にしておくことを推奨しています。



5.2 オプションの設定

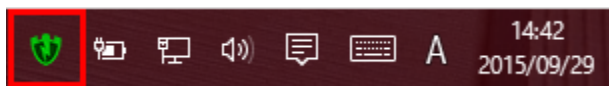
インストーラ管理画面から「オプション」ボタンを押すとスキャンオプションの設定を行うことができます。



6 タスクトレイに常駐している SuperShield アイコン

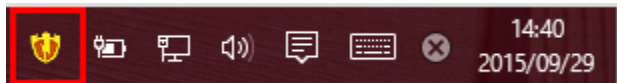
タスクバーの右側にあるタスクトレイには SuperShield アイコンが常駐しています。このアイコンから下記の事が行えます。

- 保護レベルの設定
- 活動ログの設定
- 脆弱性のあるソフトウェアのアップデート
- ローカル・ホワイトリスト、ローカル・ブラックリストの管理
- PC Matic の起動



SuperShield アイコンが黄色になっている場合は下記の事が考えられます。

- 制御情報を取得中
制御情報のダウンロードには、15 分前後要します。しばらくお待ちください。
- 脆弱性のあるアプリケーションがあり、アップデートが必要な場合
SuperShield アイコンを右クリックして表示される「脆弱性ソフトウェアのアップデート」を選択し、アップデートを行ってください。



SuperShield アイコンが赤色になっている場合は下記の事が考えられます。

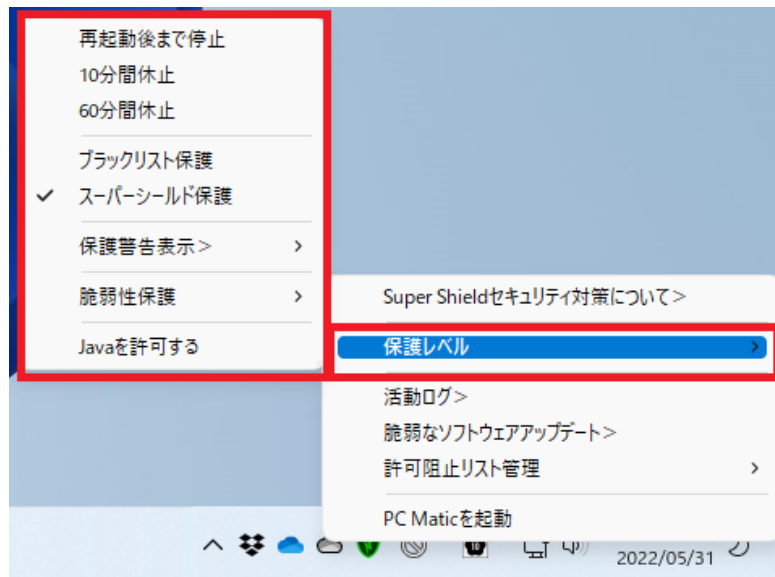
- 再起動が必要な場合
セキュリティエンジンの自動更新により再起動が必要です。再起動を行ってください。
- ライセンスの期限が切れている場合やライセンス認証ができなかった場合
ライセンスの更新を行ってください。



6.1 保護レベルの設定

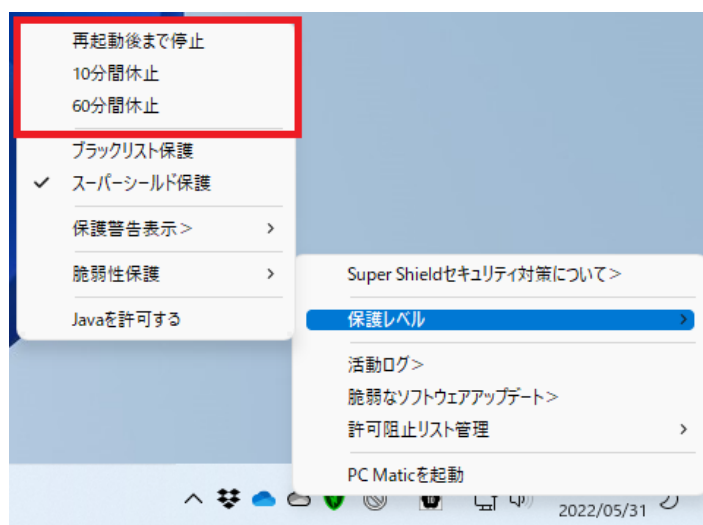
タスクトレイの SuperShield アイコンを右クリックし、表示されたメニューから「保護レベル」を選択すると保護レベル設定が行えます。タスクトレイのアイコンは標準では、「^」を押さなければ表示されませんので、Windows の「設定」-「個人用設定」-「タスクバー」-「その他のシステムトレイアイコン」より「PC Matic Super Shield」を「オン」にさせていただくことでアイコンを表示して頂けます。

保護レベルの設定では、SuperShield の一時休止を行うことや、ブラックリスト保護、スーパーシールド保護の切り替え、保護警告の表示の設定、脆弱性保護の設定、ファイルアクセス監視の設定が行えます。



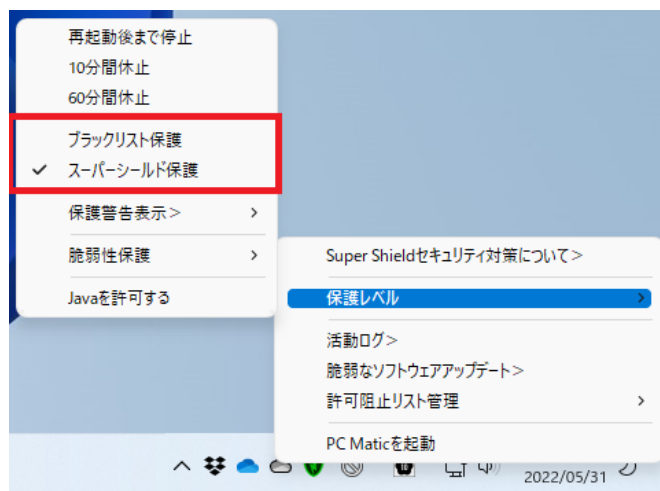
6.1.1 SuperShield の一時休止

Windows の大規模アップデート、Windows7 から 10 にする場合や Windows10 の TH1 から TH2 にアップデートする場合にご利用ください。停止や休止を行わなくてもアップデートは行えます。



6.1.2 ブラックリスト保護とスーパーシールド保護

通常はデフォルトで設定されている「スーパーシールド保護」をご使用ください。ブラックリスト保護は、従来のセキュリティソフトと同様の保護レベルで稼働します。頻繁にアプリケーションがバージョンアップされる際に設定ください。



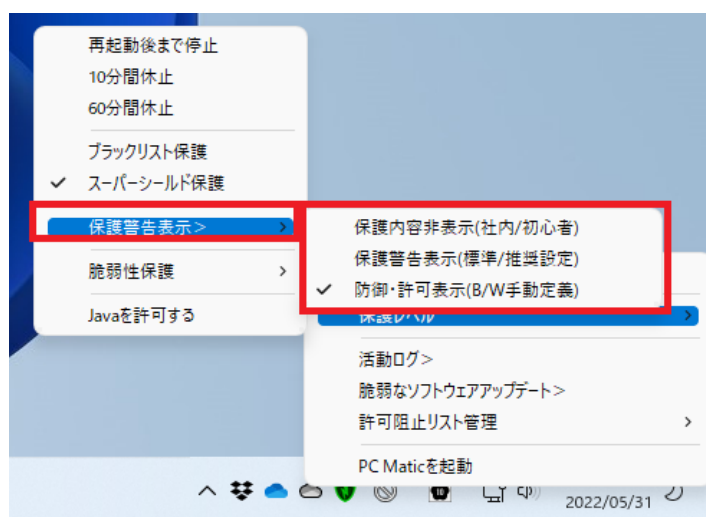
6.1.3 保護警告表示

通常はデフォルトで設定されている「保護警告表示（標準/推奨設定）」をご使用ください。パソコン初心者や企業でご利用の方は「保護内容非表示（社内/初心者）」を選択することをお勧めしています。

「防御・許可表示（B/W 手動定義）」を選択すると、手動でローカル・ブラックリスト、ローカル・ホワイトリストを登録する事ができます。こちらは、自作ソフトや社内で行われているオリジナルアプリケーションを使用する際に使用ください。

未知のアプリケーションで起動がブロックされたものは、PC Matic のクラウド分析サーバーへアプリケーションが転送され、詳細な監査がマルウェア分析官により実施されます。通常は 24 時間でグローバル・ホワイトリスト/グローバル・ブラックリストへの追加が完了し、起動が可能になるか、ウイルスである場合は削除されます。

「防御・許可表示」は、パソコンに詳しい方が利用されることを強くお勧めいたします。



「保護警告表示」を選択している場合は、ホワイトリストやブラックリストに登録されていないアプリケーションで、ヒューリスティックスキャンによる監査にて問題がないアプリケーションである場合は、以下の「PC Matic SuperShield セキュリティによる警告」が表示されます。



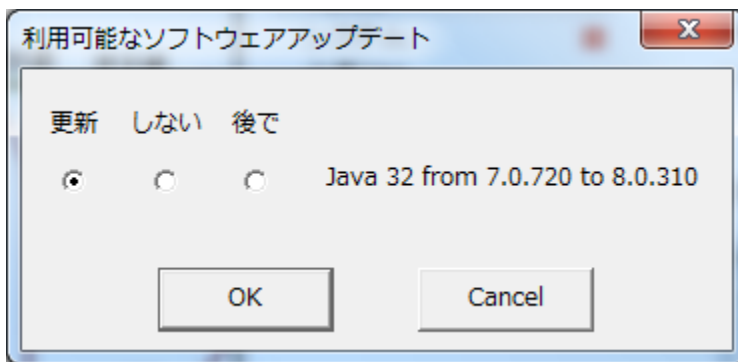
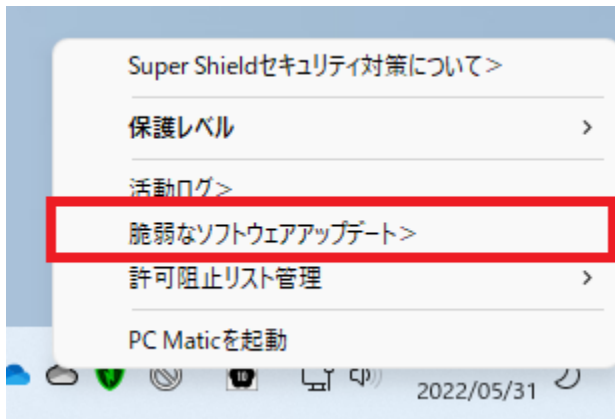
この画面が表示されると共に、PC Matic のクラウド分析サーバーへアプリケーションが転送され、詳細な監査が実施されます。通常は 24 時間でグローバル・ブラックリスト／グローバル・ホワイトリストへの追加が完了します。ご自分で開発したアプリケーションをすぐに利用したい場合は、「常時許可」もしくは「許可」を選択してください。「常時許可」を押すとローカル・ホワイトリストへ追加されます。

判定		SuperShield 保護モード	ブラックリスト 保護モード	ファイル削除
Bad	マルウェア、ランサムウェア	実行 拒否	実行 拒否	削除
Unknown	未監査、グレー、脆弱性含む	実行 拒否	実行 許可	
Good	善良と確認済アプリケーション	実行 許可	実行 許可	

6.1.4 脆弱性保護

脆弱なアプリケーションがある場合は、ここを選択するとダイアログが表示されます。

脆弱性があったソフトウェアがアップデートを行う際に「利用可能なソフトウェアアップデート」が表示され、アップデートを行うか、行わないか、後ほど行うかの選択が行えるようになります。



6.1.5 アプリケーションの起動がブロックされる場合

PC Matic SuperShield は、PC Matic マルウェア分析官により、デジタルフォレンジックを実施していないアプリケーションおよび既にウイルス、脆弱性(セキュリティホール)を含むアプリケーションに認定済のものを起動阻止します。通常 15 分から 24 時間程度でホワイト、グレー、ブラックへ分類されます。拒否リスト上にあるアプリケーションは、スキャンを行うことで検疫区画に移動されます。

- ブロックされた場合は、24 時間お待ちください

通常は、24 時間以内にグローバル・ブラックリスト／グローバル・ホワイトリストへ分類されます。PC Matic では、2003 年以降に日米欧を中心に世界中で使用されている市販アプリケーションやドライバー、シェアウェア、フリーソフトウェアの MD5 を算出したものをデータベース化し、グローバル・ホワイトリストとして 1 億 3 千万個以上登録しています。ウイルスやスパイウェアが、特定の目的のもとに次々と開発され、世界中に拡散している昨今では、「既知のもののみ起動を許可する」というアプリケーション・ホワイトリストティング方式(NIST SP 800-167)が、標的型メールや新種ウイルスも含め、唯一の解決策になります。

- 最新版がないか再確認ください

PC Matic のインストール直後に今まで利用していたアプリケーションが使えなくなった方は、脆弱性を含む Windows 再配布モジュールが含まれていた可能性がありますので、最新版がないかをアプリケーション開発元へご確認ください。10 年以上経過している古いアプリケーションは、ほとんどの場合、深刻な脆弱性(セキュリティホール)を抱えています。

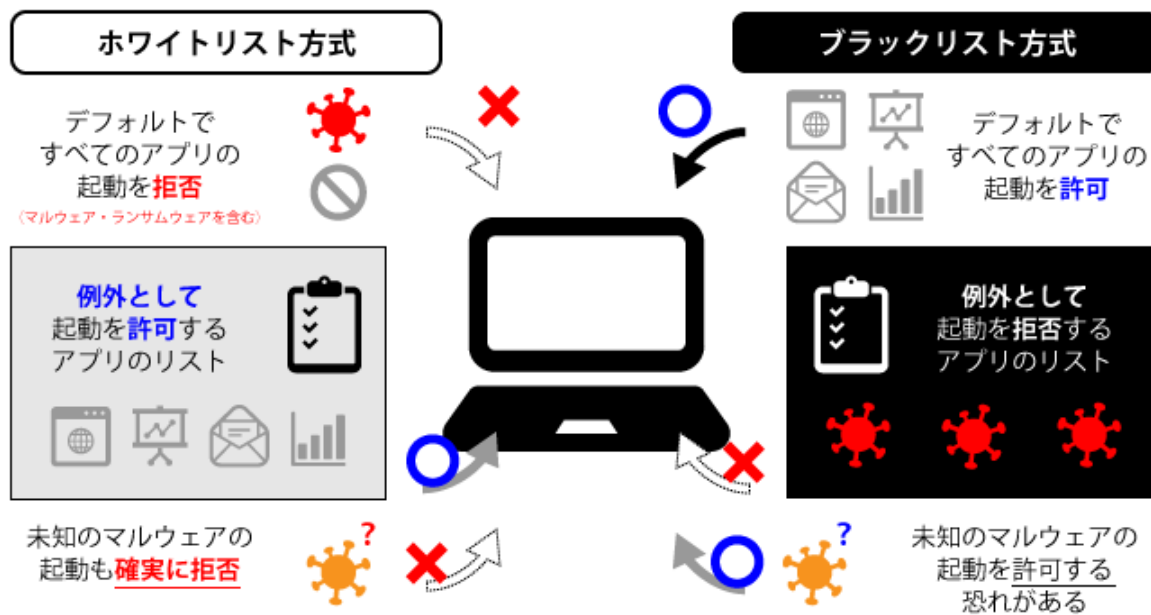
一方で新たに開発されたアプリケーションの出荷直後は、未知のものとして起動を阻止してしまうことになります。PC Matic では、新規にリリースされたソフトウェアの全てを著名ベンダー製、個人製の区別をすることなく、様々なアプローチで脆弱性のある再配布モジュールが組み込まれていないか、悪意があるコードが含まれていないかなどを慎重に多面調査し、原則として 24 時間以内にグローバル・ホワイトリストかグローバル・ブラックリストへの振り分けを行います。

- はやる気持ちを抑えてください。善悪は個人では判断できません

いますぐ起動したい気持ちはわかりますが、未知のアプリケーションが善良であるか、善良でないかの判断は、多面監査でセキュリティ監査を経た上でなければ、誰も判断することができない世の中になっています。特にインターネット上で取得したアプリケーションには、アドウェアや諜報ツールが埋め込まれているものがあります。特に動画ダウンローダー、不正音楽ダウンロードソフト、画像加工ソフトは悪意のあるソフトウェアを含んでいるものが非常に高い確率で存在しています。また著名な作者や企業であっても、ウイルスによって不慮の影響を受けている可能性もあり、実際にそのようなことも多く発生しています。

- 世界中の誰かが、過去起動している場合は、既に分類にかけられています
ご自分のパソコンで目新しいアプリが防止されるのではなく、世界中の PC Matic 利用者が過去遭遇していないアプリケーションが未知のアプリケーションとなります。すでに過去、誰かが PC Matic にて検知されていれば、原則的にブラックかホワイトに分類されています。日本製のフリーソフトウェアは、ほとんど分類にかけられています。古いフリーソフトウェアがブロックされた場合は、グレー判定により起動阻止されている可能性が濃厚となります。

6.1.6 PC Matic セキュリティエンジン詳細図解



6.1.7 未知のアプリケーション監査で 24 時間以上経過しているのにまだブロックされる場合

PC Matic SuperShield は、グローバル・ホワイトリストもしくはグローバル・ブラックリストに登録されていない、未知のアプリケーションが検知された場合、クラウド上の分析サーバーに即時転送され解析作業が開始されます。通常 15 分から 24 時間以内にホワイト、ブラックへ分類されますが、以下のようなケースではグレーもしくは更に時間を要します。

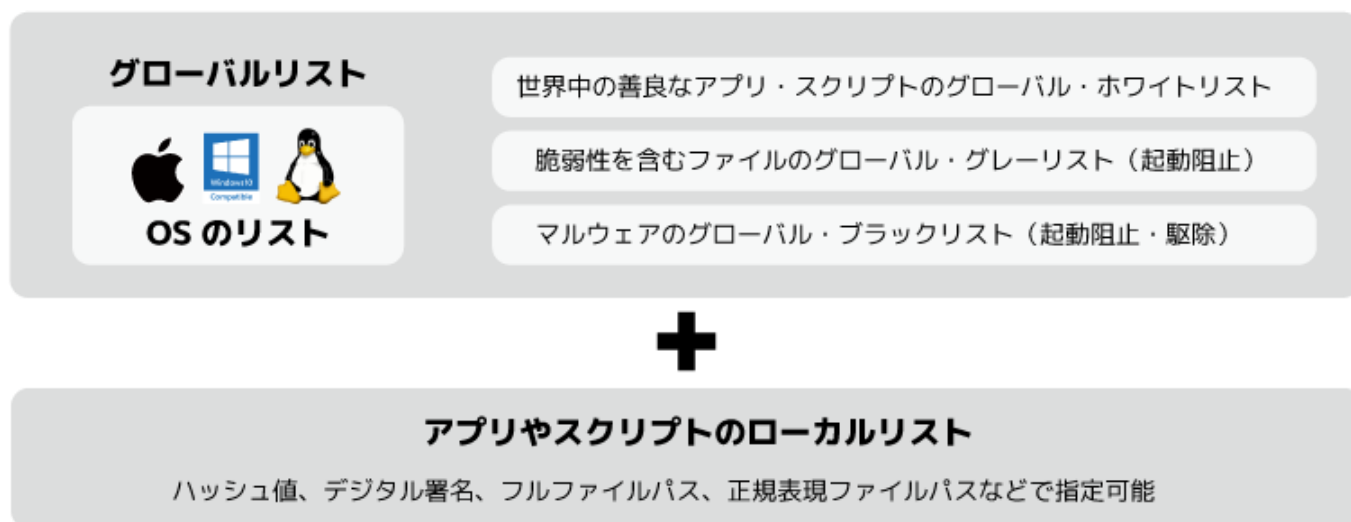
判定		SuperShield 保護モード	ブラックリスト 保護モード	ファイル削除
Bad	マルウェア、ランサムウェア	実行 拒否	実行 拒否	削除
Unknown	未監査、グレー、脆弱性含む	実行 拒否	実行 許可	
Good	善良と確認済アプリケーション	実行 許可	実行 許可	

【グレー(保留扱い)】とされ、グローバル・ホワイトリストにもグローバル・ブラックリストにも追加されないアプリケーション

- 古い開発言語で記述され、脆弱性を抱える(侵入可能なセキュリティホールがある)
 - 「アプリケーション名」「開発元」へ ASCII または UTF-8 で認証局によるデジタル署名がない(未署名)
 - プログラムが暗号化され解読されないようになっている(国家諜報機関製の嫌疑)
 - ウイルスの一部である可能性(合体型ウイルスの嫌疑)
 - 短期間に頻繁な改版がされていることを確認(悪意の嫌疑)
- など他にも多岐にわたります。

監査にさらに時間が必要と判断されたアプリケーション

- 時限タイマー型のウイルスが含まれている疑いがある(判明時に拒否リスト化)



6.1.7.1 何故ローカル・ホワイトリストへ安易に追加してはいけないのか

- 急増するオープンソースへの悪質なコードの組み込み

残念なことです、ここ数年オープンソースソフトウェアには、犯罪組織や国家諜報機関が作成した悪質なコードが含まれていることが急増しています。オープンソースプロジェクトにおいて、悪意のある組織がキーロガーを仕掛けたり、悪質なウイルスやアドウェアを読み込むコードを仕込んだりする事が急増しています。

- 昔からある著名なフリーソフトが悪質な組織へ売却される

昔から利用しているフリーソフトも作者はいつまでもボランティアでいることに疲れたからなののでしょうか。多額の支払いを持ち掛けられ売却をする作者や法人が国際的に増加しています。売却された著名なフリーソフトは、犯罪組織や国家諜報機関によって人々の情報取得をするツールとして活用されている事例も多く発見されています。不必要な通信が見受けられるためです。

DVD リッピング、音楽や動画ダウンロードや共有、画像加工の分野のソフトウェアにこうした傾向が多く見受けられますので特に注意が必要です。丁寧な説明ページや Wikipedia にバージョンの説明があっても信用してはいけません。資金力のある犯罪組織は多くの人員を割いて行動しています。

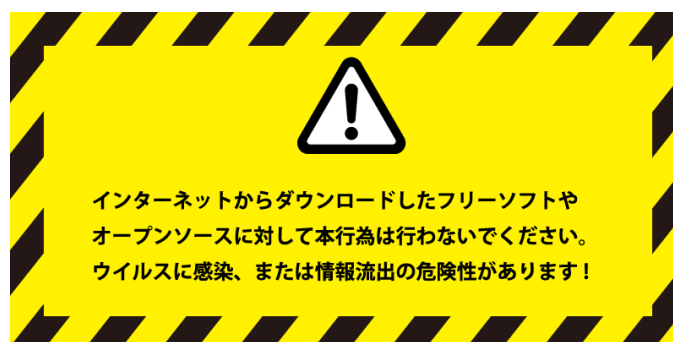
6.1.7.2 ブロックされたアプリケーションを該当パソコンからローカル・ホワイトリストへ追加

6.1.7.1 の内容を理解したうえで、ブロックされたアプリケーションをローカル・ホワイトリストへ追加し、即時起動を許可することができます。

こちらはご自分で開発したアプリケーションをすぐに利用したい場合や、信頼のおける発売元が出荷している CD-ROM など配布されているアプリケーションを利用したい場合に行ってください。

インターネットからダウンロードしたフリーソフトやオープンソースに対して本行為は行わないでください。

!!! ウイルスに感染、または情報流出の危険性があります!!!



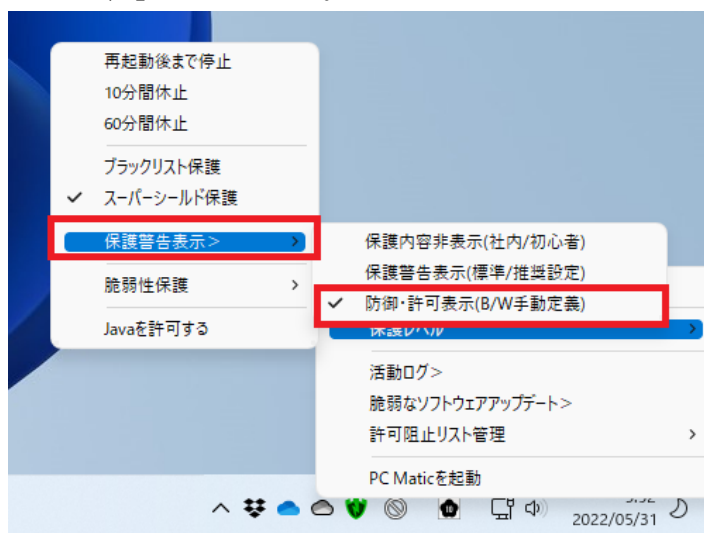
● 該当パソコンからローカル・ホワイトリストへ追加

こちらの設定は、パソコンに詳しい方が利用されることを強くお勧めいたします。新規に検知したアプリケーションで未分類の場合に、こちらで「許可」または「常時許可」を押しますと、アプリケーションがウイルスやランサムウェアであった場合は感染することがあります。(インターネットより取得したアプリは追加しないでください)

ローカル・ホワイトリストへ追加しても、実行されないことがあります。グローバル・ホワイトリストやローカル・ホワイトリストはエンドポイント保護(EPP)に対して働きますが、二重のセキュリティ保護として EDR 機能により、既知の不正 C&C サーバーへの通信、不正な挙動を防御します。起動警告表示がされないものの、利用できない場合は、この EDR により阻止されている可能性があります。善良と思われるものが本事象となりました際は、サポートまでご連絡ください。

※管理ポータルを通じて、実行を許可するローカル・ホワイトリストを管理することができます。

1. タスクバーにある SuperShield アイコン（緑色の盾マーク）を右クリックし、「保護レベル」－「保護警告表示」－「防御・許可表示 (B/W 手動定義)」を選択します。



2. 必要なアプリケーションを起動した際に表示される SuperShield の警告表示で「常時許可」もしくは「許可」を選択することでアプリケーションの起動が可能となります。



● 管理ポータルにてローカル・ホワイトリストへ追加

信頼のおけるベンダーによって提供されたアプリケーションが、24 時間以上経過しても起動が阻止される場合は、その監査状況を以下の方法にて確認することができます。(インターネットより取得したアプリは追加しないでください)

また、PC Matic のライセンスは家族や友人と共有可能となっていますので、遠隔にいる同一アカウント利用者のローカル・ホワイトリストへ追加をクラウド越しに指定して頂くことが可能です。設定が各パソコンへ反映されるまで数分要します。

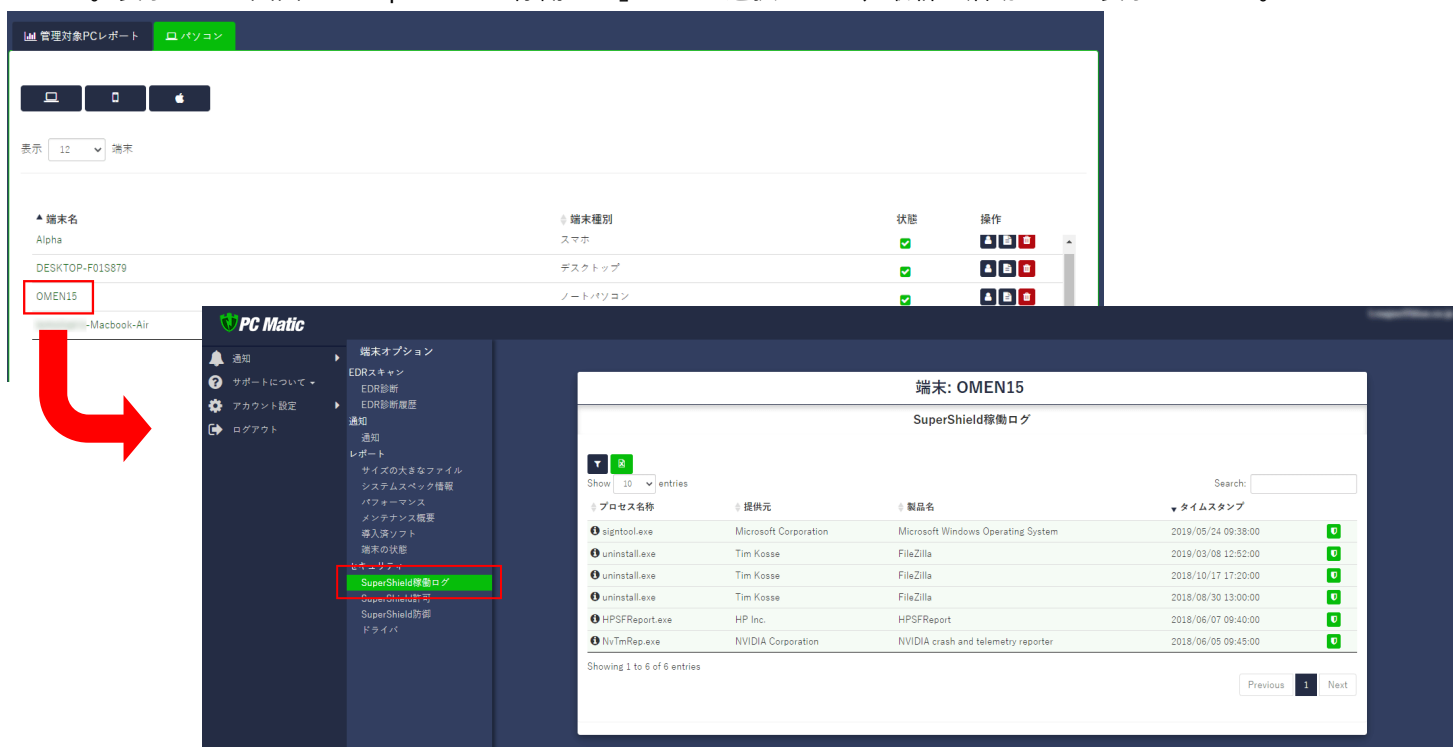
1. 管理ポータルにログインし、「アカウント設定」－「アカウント詳細」－「パソコン」タブを選択します。




名前	サブスクリプションキー	自動更新: 無効	自動更新設定
商品: PC Matic Home	有効期限: 2023/03/31	ライセンス: 4 台/最大 5	

端末名	端末種別	状態	操作
Alpha	スマホ	✓	[Icons]
DESKTOP-F01S879	デスクトップ	✓	[Icons]
OMEN15	ノートパソコン	✓	[Icons]
-Macbook-Air	Mac	✓	[Icons]

2. 表示された画面でアプリケーションの起動がブロックされたなど、活動ログを調査したいパソコン名を選択します。表示された画面で「SuperShield 稼働ログ」タブを選択すると、最新の活動ログが表示されます。



プロセス名	提供元	製品名	タイムスタンプ	状態
signtool.exe	Microsoft Corporation	Microsoft Windows Operating System	2019/05/24 09:38:00	✓
uninstall.exe	Tim Kosse	FileZilla	2019/03/08 12:52:00	✓
uninstall.exe	Tim Kosse	FileZilla	2018/10/17 17:20:00	✓
uninstall.exe	Tim Kosse	FileZilla	2018/08/30 13:00:00	✓
HPSFReport.exe	HP Inc.	HPSFReport	2018/06/07 09:40:00	✓
NvTmRep.exe	NVIDIA Corporation	NVIDIA crash and telemetry reporter	2018/06/05 09:45:00	✓

左上にある「絞り込み」を選択して表示される画面で「起動の是非」の項目を「いいえ」を選択すると起動がブロックされたアプリケーション一覧が絞り込んで表示されます。標準では起動しなかったアプリケーションが表示されています。



端末: OMEN15

SuperShield稼働ログ

SuperShield稼働ログ絞り込み条件

プロセス名称:

提供元:

製品名:

現在の識別状態:

検出時の識別状態:

起動の是非(ブランクで全稼働ログ表示):

検索種別:


絞り込み解除

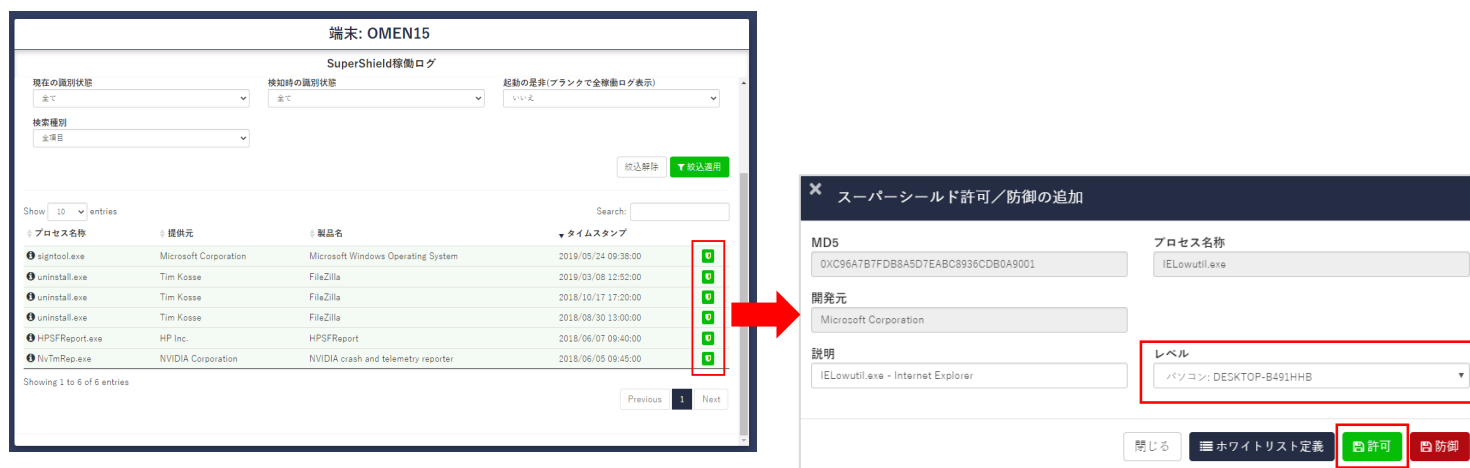
Show: 10 entries

Search:

プロセス名称	提供元	製品名	タイムスタンプ	
signtool.exe	Microsoft Corporation	Microsoft Windows Operating System	2019/05/24 09:38:00	
uninstall.exe	Tim Kosse	FileZilla	2019/03/08 12:52:00	
uninstall.exe	Tim Kosse	FileZilla	2018/10/17 17:20:00	
uninstall.exe	Tim Kosse	FileZilla	2018/08/30 13:00:00	

「現在の識別状態」が「未知」は、非分類（脆弱性を含むものもある）のアプリケーションで、「悪い」は、ウイルスや PUP として判定されたアプリケーションになります。

黄色や赤色に分類され、自身や社内で作成したアプリケーションをローカル・ホワイトリストに追加したい場合は、追加したいアプリケーションの右側にある  マークを押し、表示された画面でローカル・ホワイトリストの登録レベルをこのパソコン本体のみに設定するか、「全アカウント」にするかを選択し「許可」を選択します。



端末: OMEN15

SuperShield稼働ログ

現在の識別状態:

検出時の識別状態:

起動の是非(ブランクで全稼働ログ表示):

検索種別:

絞り込み解除

Show: 10 entries

Search:

プロセス名称	提供元	製品名	タイムスタンプ	
signtool.exe	Microsoft Corporation	Microsoft Windows Operating System	2019/05/24 09:38:00	
uninstall.exe	Tim Kosse	FileZilla	2019/03/08 12:52:00	
uninstall.exe	Tim Kosse	FileZilla	2018/10/17 17:20:00	
uninstall.exe	Tim Kosse	FileZilla	2018/08/30 13:00:00	
HPSFReport.exe	HP Inc.	HPSFReport	2018/06/07 09:40:00	
NvTmRep.exe	NVIDIA Corporation	NVIDIA crash and telemetry reporter	2018/06/05 09:45:00	

Showing 1 to 6 of 6 entries

Previous 1 Next

スーパースールド許可/防御の追加

MD5: 0XC96A7B7FDB8A5D7EABC8936CDB0A9001

プロセス名称: IELowutil.exe

開発元: Microsoft Corporation

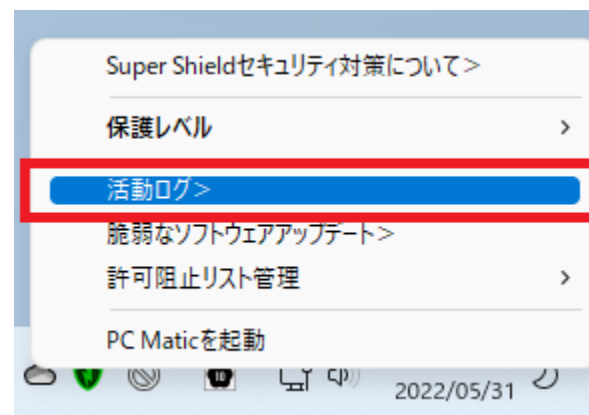
説明: IELowutil.exe - Internet Explorer

レベル: パソコン: DESKTOP-B491HHB

閉じる

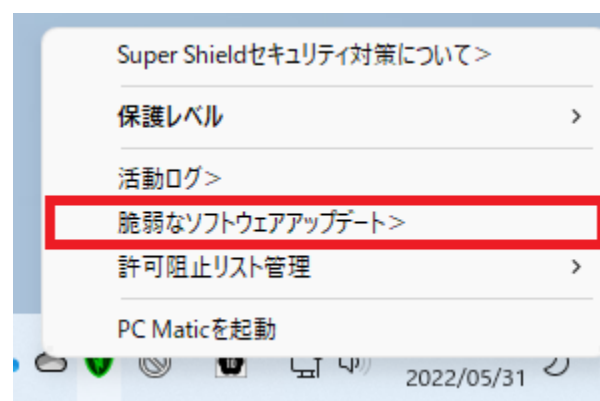
6.2 活動ログ

活動ログをご覧いただくことによって、SuperShield のセキュリティ保護機能の監査結果を確認することができます。



6.3 脆弱なソフトウェアアップデート

PC Matic では、スケジュールスキャンによって脆弱性のあるソフトの自動アップデートを行っていますが、脆弱性があるソフトがあった場合に SuperShield アイコンが黄色になります。「脆弱なソフトウェアアップデート」を選択する事で対象アプリケーションのアップデートを行えます。



6.4 許可阻止リストの管理

「保護レベル」の「保護警告表示」を「実行・阻止の表示」を選択している場合は、警告表示がされ実行を許可した場合は「ホワイトリスト」に表示され、阻止にした場合は「ブラックリスト」に表示されます。



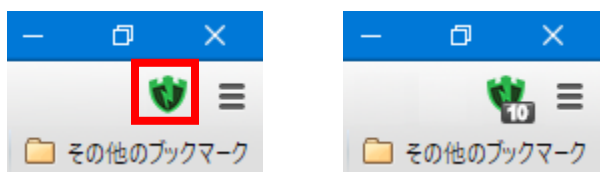
7 詐欺対策(ブラウザー保護)


ブラウザーに Google Chrome、Firefox、Chromium Edge、Old Edge、IE11 を使用している場合は、詐欺対策を行うことができるブラウザー保護機能を使用する事ができます。


ブラウザー保護機能を使用するには、下記手順でインストールを行う必要があります。これに付帯する広告ブロック機能では、現在表示しているホームページに広告がある場合、非表示にします。また、動画広告も非表示になります。

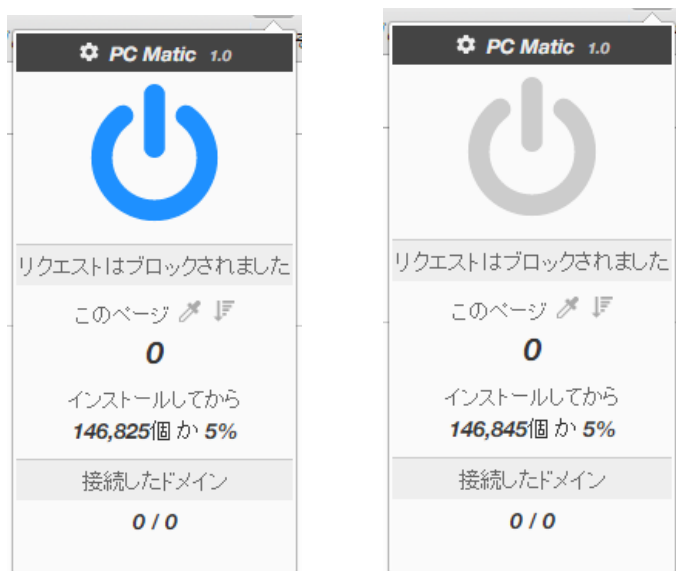
本拡張機能は、ブラウザー経由での端末侵入防止機能(IPS)および、詐欺広告を配信する不正な広告ネットワークによる広告表示を阻止する機能を装備しています。操作パネルは uBlock Origin を利用していますが、実装機能や表示阻止対象は同一ではありません。

ブラウザー保護機能が有効になっている場合は、ブラウザーの右上に SuperShield アイコンが緑色で表示されます。また、アイコンに非表示にしている広告数が表示されます。



SuperShield アイコンを選択し、表示される画面の  をクリックするとブラウザー保護機能を解除することができます。

解除すると、 が灰色になり、そのドメインの広告が表示されます。灰色の状態アイコンを選択すると広告ブロック機能が有効になります。



例：pcmatic.blue.co.jp のドメインを表示している際に有効にした場合は、そのページの全てにブラウザー保護機能が適応されます。www.blue.co.jp は別ドメインであるため、広告はブロックされません。

7.1 インストールについて

ブラウザ保護機能を使用する場合は、それぞれのブラウザでインストールを行う必要があります。

下記リンク先に Google Chrome、Firefox、Chromium Edge、Old Edge のインストール方法が記載されていますので、ご参照ください。

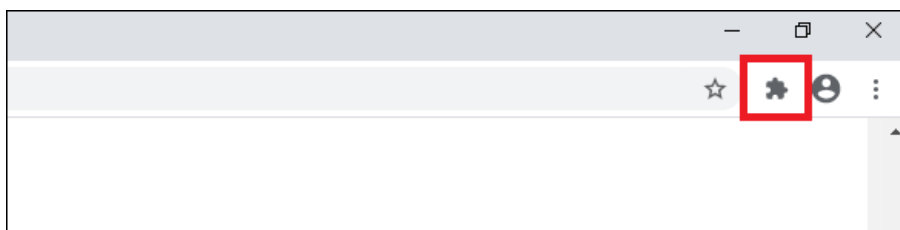
ブラウザ保護機能導入方法:<https://pcmatic.jp/faq/webshield/03/>

7.1.1 Google Chrome の場合

Chrome ストアをクリックして、Chrome ストアより WebShield を入手してください。

アイコンが非表示になっていないか確認

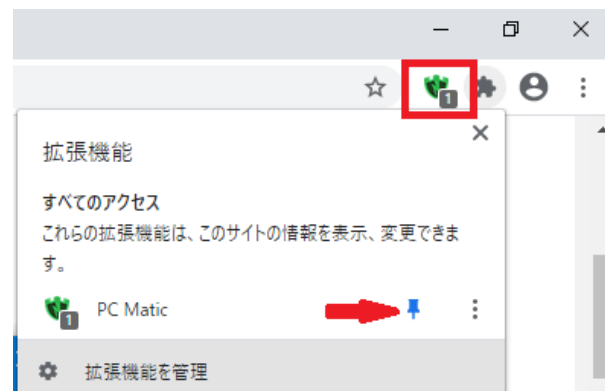
1. Chrome の右上にある「拡張機能」ボタンを押します。



2. 開いた画面に「PC Matic」があり、その先の画鋏マークがオン(青色)になっていなければ、導入されているもののアイコンが非表示になっているだけです。オンにします。



3. アイコンが表示されれば成功です

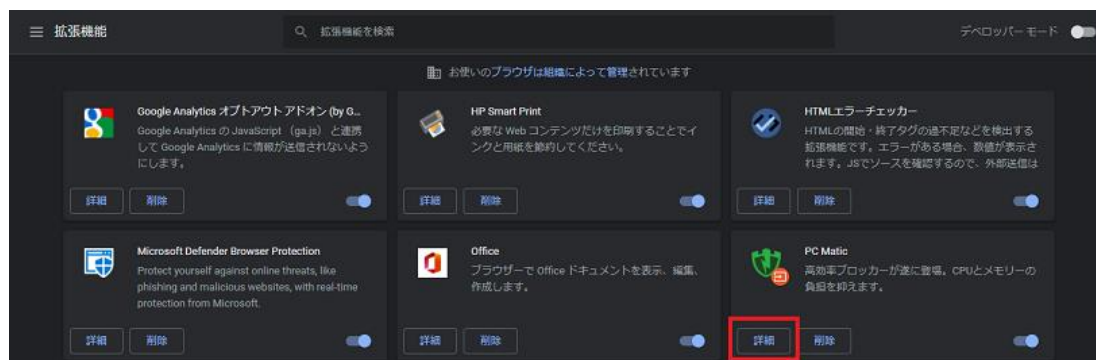


Chrome, Chromium Edge 導入済で機能がオフの場合

1. 画面右上のメニューから「その他のツール」から「拡張機能」を選択します。



2. 導入済の拡張機能一覧から「PC Matic」の「詳細」を選択します。

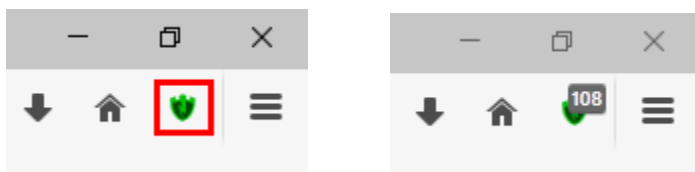


3. 開いた画面の上部にあるスライダーを「オン」にします。

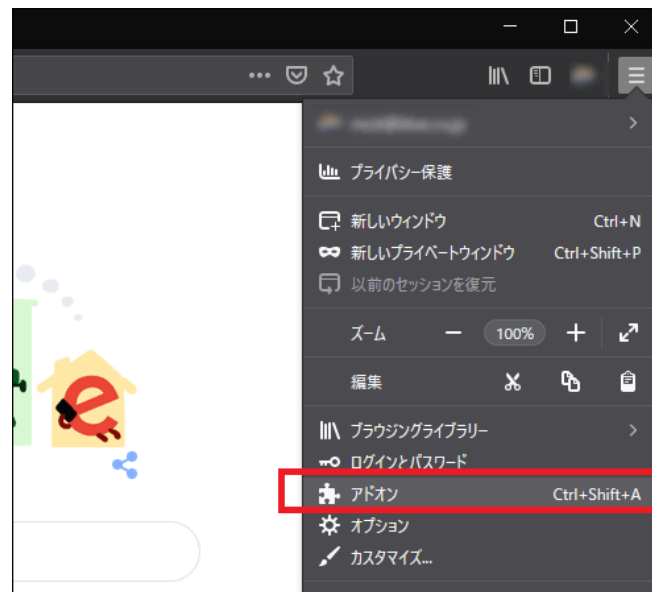


7.1.2 Firefox の場合

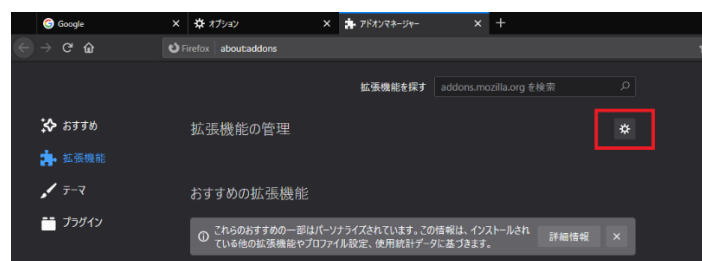
ブラウザー保護機能が有効になっている場合は、ブラウザーの右上に SuperShield アイコンが緑色で表示されます。また、アイコンに非表示にしている広告数が表示されます。



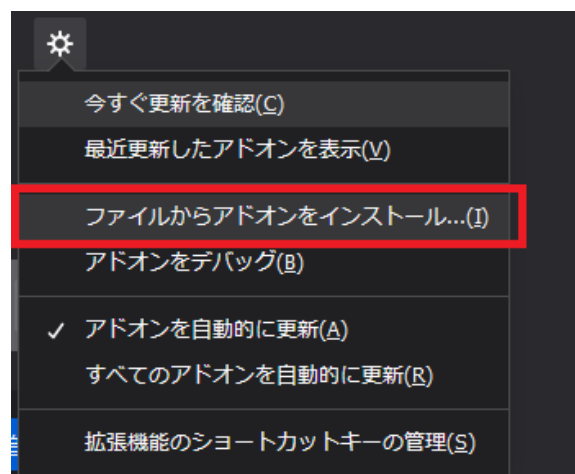
1. 画面右上のメニューから「アドオンとテーマ」を選択します。



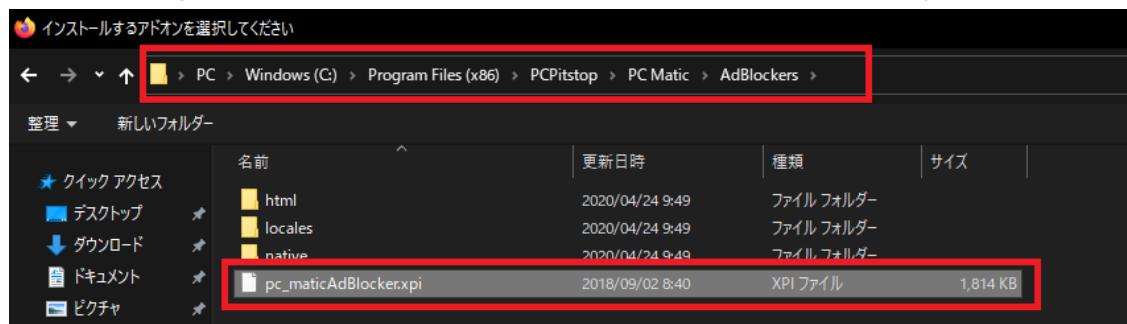
2. 開いたタブの左側にある「ギア状のアイコン」を選択します。



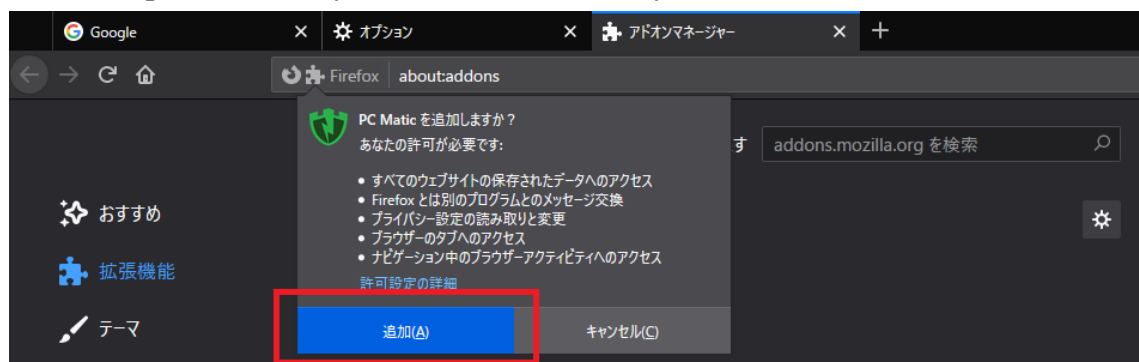
3. 「ファイルからアドオンをインストール」を選択します。



4. 「C:\ProgramFiles(x86)\PCMatic\PC Matic\AdBlockers」 内にある「pc_maticAdBlocker.xpi」を選択します。

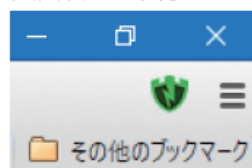


5. 「追加」を選択します。これで導入が完了します。

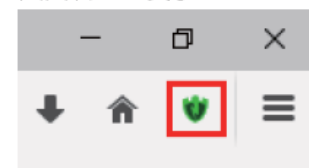


6. ブラウザーにある PC Matic のアイコンをクリックします。

Google Chrome
画面右上に表示



Firefox
画面右上に表示



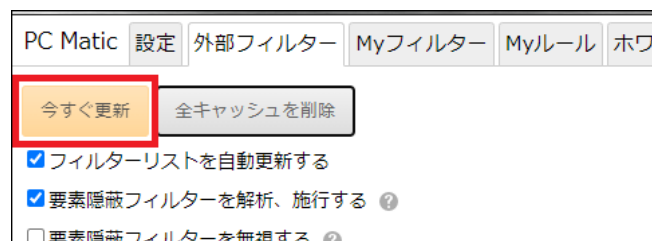
7. 電源アイコンの下にグレーで4つあるアイコンの右端を選択します。



- 「外部フィルター」タブの上部にある「全キャッシュを削除」をクリックします。



- 隣の「今すぐ更新」を押すことができるようになりますので、押して最新のシグネチャーを受信します。即時にダウンロードされます。設定画面を閉じて終了です。

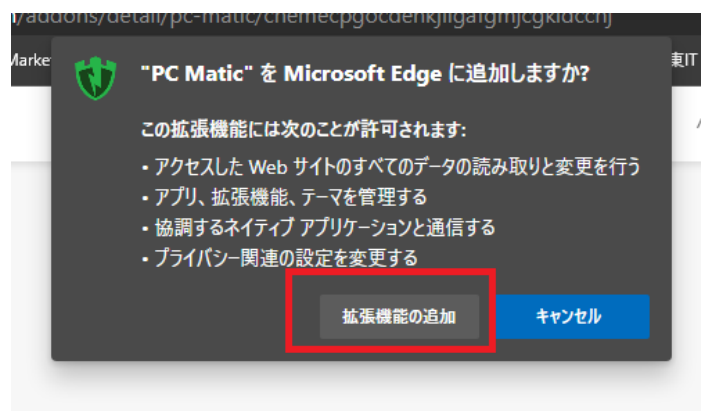


7.1.3 Chromium Edge の場合 (Windows 11/10 20H2 以降)

- ここをクリックして Edge アドオンにアクセスしてください。
- 「インストールを押します。」



- 「拡張機能の追加」を押します。拡張機能のインストールが行われます。



- インストールが終了すると、ブラウザーに下のような画面が表示され、ブラウザーにアイコンが追加されます。




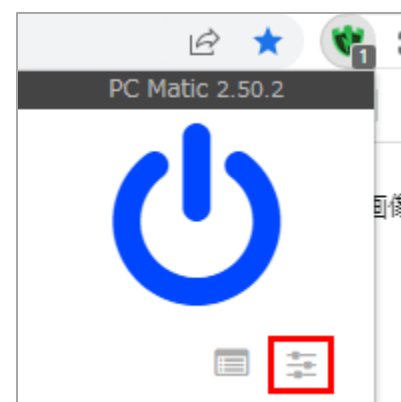
7.1.4 Old Edge (Windows 10 20H1 以前)

- ここをクリックして [Microsoft Store](#) から拡張機能入手します。
- マイクロソフトストアで「インストール」を押します。
- ブラウザーに導入されアイコンが表示されます。

7.2 ブラウザー保護機能を有効にしているのに広告が表示される場合

Google Chrome、Firefox を使用している場合は、フィルターを更新する事ができます。

- SuperShield マークを押し、表示された画面の  マークを押します。



- 「外部フィルター」タブにある「全キャッシュを削除」を押します。



- 「今すぐ更新」を押します。この操作でフィルターの更新が完了しました。



8 オプション

オプションでは下記の事が行えます。

- 最適化実行前に復元
- テクニカルサポート用のログファイルのアップロード
- スケジューラーの状況確認
- スキャンおよび最適化を行うための設定オプションを変更・確認
- ローカル・ホワイトリストの管理
- コンピューターのユーザー評価
- 言語の選択
- SuperShield の削除・停止

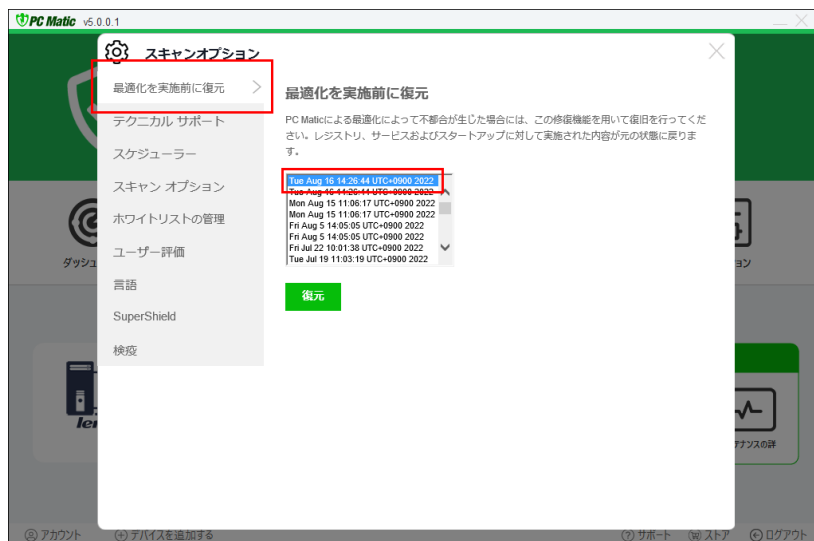
オプションを起動するには、インストーラ管理画面の「オプション」を押します。



8.1 最適化実行前に復元

PC Matic の最適化によって不都合が生じた場合には、この修復機能を用いて復旧を行ってください。レジストリ、サービスおよびスタートアップに対して実施された内容が元の状態に戻ります。

1. どの最適化実行前に戻りたいのかを選択し、「復元」を押します。



2. 「本当に復元してもよろしいですか？」と表示されますので、「はい」ボタンを押します。



8.2 テクニカルサポート用のログファイルのアップロード

テクニカルサポートに問い合わせを行った際に、「PC Matic のログをアップロードしてください」と依頼されたらこの操作を行ってください。なお、「テクニカルサポート用のログ」には、パソコンの利用状況に関する情報が含まれていて、個人を特定する情報は含まれておりませんので、ご安心ください。

1. オプション画面を表示し、左側のメニューから「テクニカルサポート」を選択し、「ログを作成」ボタンを押します



2. 「Successfully uploaded」と表示された場合は、正常にアップロードされています。

一部の.NET バージョンによりアップロードができない場合があります。その場合には、「PC Matic-Support.zip」という圧縮フォルダがデスクトップ上に作成されますので、これを電子メールに添付してサポートに問い合わせを行います。



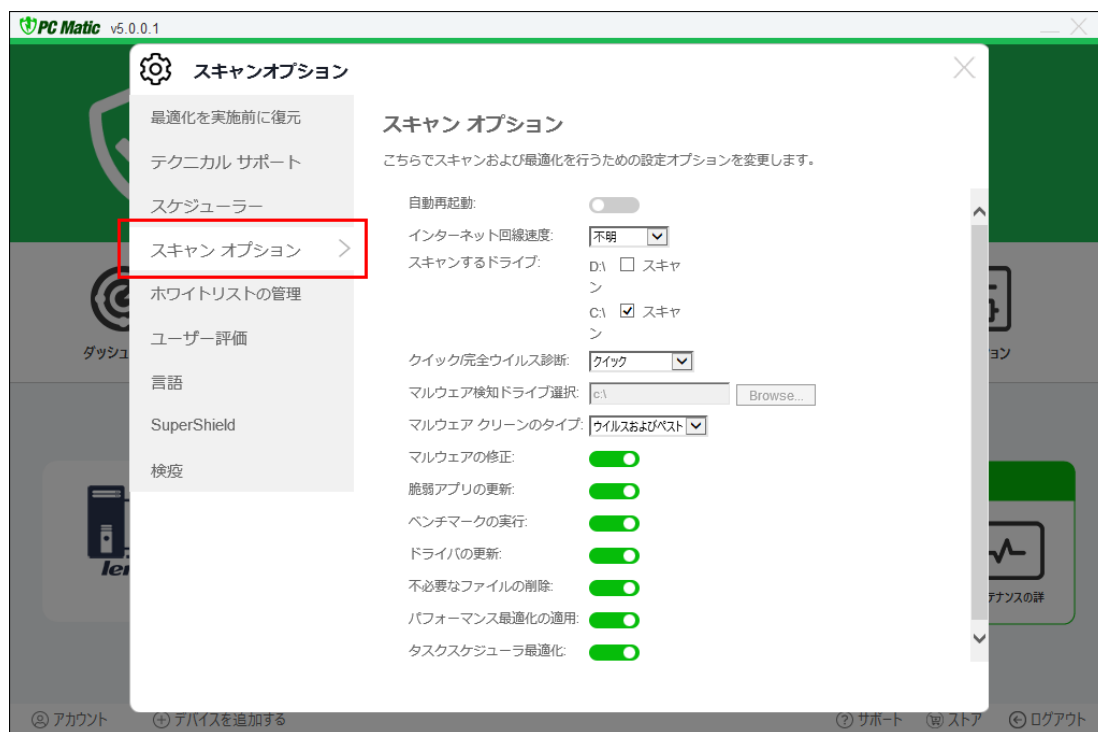
8.3 スケジューラー

スケジュールの作成やスケジュールの停止を行う事ができます。また、スケジュールを設定している場合は、前回のスケジュールスキャンをいつ行ったかを確認する事ができます。

パソコンの電源を切らずにスタンバイモードで使用している方は「スケジューラーを停止」を行ってください。スタンバイモードが解除されなくなります。

8.4 スキャンオプション

スキャンや最適化を行うための設定オプションを変更できます。変更したい項目を編集してください。



8.5 ローカル・ホワイトリストの管理

8.5.1 スタートアップ・アプリケーション

このリストより除外をしたい場合は、アプリケーションを選択し「スタートアップ起動を除外する」ボタンを押してください。

8.5.2 サービス

一覧よりサービスを除外する場合は、対象とするサービスを選択し、「サービスの除外」ボタンを押してください。

8.6 ユーザー評価

現在お使いおパソコンの評価を収集するためにお手伝いいただける場合は、こちらに記入して「送信」してください。

8.7 言語

ご使用の PC Matic の言語を変更する場合は、こちらより変更したい言語を選択して「言語の変更」を押してください。

8.8 SuperShield

セキュリティ対策の実施が必要ない場合は、「削除」または「停止」を押してください。

9 管理ポータル

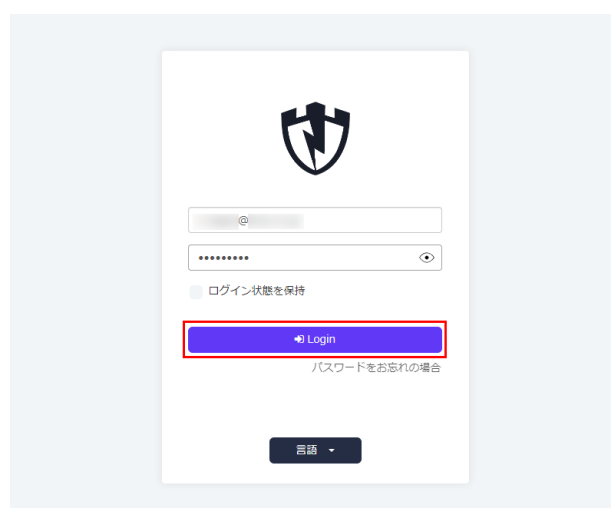
PC Matic のホームページ (<https://pcmatic.jp/>) から「管理ポータル」と書かれたリンクを押す、または <https://portal.pcpitstop.com/> にアクセスして頂くと、管理ポータルを表示する事ができます。

管理ポータルでは、スケジュールの設定、インストーラのダウンロード、ローカル・ホワイトリストの追加・削除などの指定やアラートの確認、利用状況詳細レポート、メンテナンス概要、パソコンの状況を確認することができます。画面表示はパソコンのほか、タブレットやスマートフォンにも対応しています。

9.1 ログイン

PC Matic でアカウントを作成した際の電子メールアドレス、パスワードを入力し、「Login」を押します。

※ログイン状態を保持などの言葉が日本語で表示されていない場合は、「言語」「Language」など表示されているボタンを押して「日本語」を選択してください。



9.2 配色設定

「アカウント設定」 - 「管理ポータルデザイン」の「配色テーマ」を押して「Dark Mode」を押すとダークモードで表示することができます。



9.3 管理ポータル画面



- ① メニューが表示されています。
- ② ①で選択したメニュー内容に応じたサブメニューが表示されます。
- ③ 利用者の名称や PC Matic の利用状況が確認できます。またここで自動カード払い設定を行う事ができます。

9.4 自動カード払い設定の解除

PC Matic を直営店でクレジットカード購入をされた場合は支払いが自動で更新されるようになっています。自動更新を解除する場合は以下の設定を行ってください。

1. 管理ポータル画面で「アカウント設定」－「アカウント詳細」を選択し、表示された画面で「自動更新設定」を押します。



2. 「自動更新を有効化」を選択してチェックを外します。

×

支払設定の編集

クレジットカードによる以下の項目に同意し、自動更新を設定します：

(a) 利用継続による支払とカートにて購入した商品やサービスおよびそれに付帯する税金

(b) 本項目にて指定した支払方法とその支払間隔をもって正規販売社による自動支払いを承認し、

(c) 有効期限の更新などをカード会社からの情報を得ることに同意し、

(d) 利用継続を解除することで、自動更新を解除することができるものとします。

☒ 自動更新を有効化

姓(ローマ字)

名(ローマ字)

姓(ローマ字)

名(ローマ字)

会社

電話(数字のみ)

3. 「保存」を押します。

×

支払設定の編集

クレジットカードによる以下の項目に同意し、自動更新を設定します：

(a) 利用継続による支払とカートにて購入した商品やサービスおよびそれに付帯する税金

(b) 本項目にて指定した支払方法とその支払間隔をもって正規販売社による自動支払いを承認し、

(c) 有効期限の更新などをカード会社からの情報を得ることに同意し、

(d) 利用継続を解除することで、自動更新を解除することができるものとします。

☐ 自動更新を有効化

閉じる

保存

9.5 包括スケジュール設定

包括スケジュール設定を行うと登録しているすべてのパソコンを包括してスキャンを実施します。スキャンは毎週 1 回実施する事をおすすめします。このスケジュールを設定しておく、新しいパソコンを追加してもパソコンで個別にスケジュール設定を行う必要がなくなります。

1. 管理ポータルでメニューの「アカウント設定」－「包括スケジュール設定」を選択し、表示された画面の「Add スケジュール」を押します。



通知

サポートについて

アカウント設定

ログアウト

アカウント

アカウント詳細

オフラインアクション

パスワード変更

包括スケジュール設定

端末一覧

管理ポータルデザイン

セキュリティ

ローカルブラックリスト

ローカルホワイトリスト

ドライバ

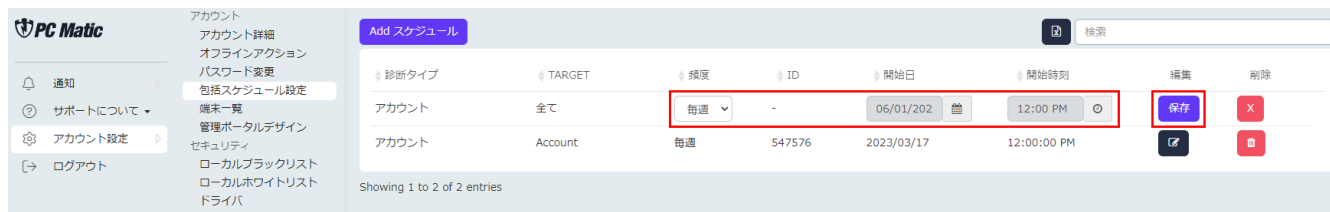
Add スケジュール

検索

診断タイプ	TARGET	頻度	ID	開始日	開始時刻	編集	削除
アカウント	Account	毎週	547576	2023/03/17	12:00:00 PM		

Showing 1 to 1 of 1 entries


- 表示された画面で頻度、開始日、開始時刻を設定し、「保存」を押してください。
送信先アドレスを設定している場合はスキャン完了後に設定したメールアドレスにメールが送られてきます。



9.6 ローカルホワイトリストの設定

ローカルホワイトリストを設定する事によって必要なソフトが動作しない場合に動作させるように設定する事ができます。

この機能は自ら開発したアプリケーションのみに活用し、第三者が作成したアプリケーションに対しては基本的に利用しないでください。

- 管理ポータルメニューから「アカウント設定」 - 「ローカルブラックリスト」を選択し、除外したいものを選び、「 除外」ボタンを押します。



ローカルホワイトリストに追加されているものを除外する場合は、「ローカルホワイトリスト」を選んでください。

ローカルホワイトリストに設定を行っても PC Matic 側のサーバーが悪質であると判断している場合は、赤色で警告し続けられます。お客様へ再考を促すためです。

9.7 アラートの確認

管理ポータル内の「通知」を押して表示される「セキュリティ」「性能」では、登録しているパソコンにアラートがあった場合の通知が表示されます。



通知

PC Matic News

セキュリティ

性能

種類 全て

表示 全て

表示を消す いい!

通知 全消去

▼ 日/時	◆ 端末PATH	◆ 説明	アクション	消去	停止
2023/01/30 15:14:19	未定義 / DESKTOP-SMALL	C:\Users#\OneDrive\Desktop\GetuGamen.exe 0x0B00DBD013E765C73CD83BB2B21885E7 出現回数: 1 最終確認: 2023/01/30 00:14:17: SuperShieldによって起動阻止されました	操作	消去	停止

ウイルス報告などの主要なアラートに対しては、ウイルスの無力化は行われておりますので、特に対処の必要はございません。

9.8 端末管理

ライセンスに登録されている端末が表示されます。ここでは各端末に表示されているアラートの確認や、端末名の右にある削除ボタンを押すことでライセンスから端末を削除する事ができます。



アカウント

アカウント詳細

オンラインアクション

パスワード変更

包括スケジュール設定

端末一覧

管理ポータルデザイン

セキュリティ

ローカルブラックリスト

ローカルホワイトリスト

ドライバ

名前(ローマ字):

サブスクリプション認証キー(半角):

自動更新: 無効

自動更新設定

商品: PC Matic Home

有効期限: 2024/03/31

ライセンス: 5 最大 5

端末一覧

端末の絞り込み:

表示 12 端末一覧

▲ 端末名	◆ 端末種別	状態	操作
Alpha	Android		🔍 🗑️ 🔄
DESKTOP-SMALL	Windows Desktop		🔍 🗑️ 🔄
MacBook Air	Apple macOS		🔍 🗑️ 🔄
PAVILION600	Windows Desktop		🔍 🗑️ 🔄

Showing 1 to 4 of 4 entries (filtered from 5 total entries)

9.9 スーパーシールドログからローカルホワイトリスト登録

管理ポータルで「アカウント設定」－「アカウント詳細」－「端末一覧」を選択し、表示された画面でアプリケーションの起動がブロックされたなど、活動ログを調査したいパソコン名を選択します。最新の活動ログが表示されます。



端末の絞り込み:

表示 12 端末

▲ 端末名

- Alpha
- DESKTOP-SMALL**
- DESKTOP-SMALL
- MacBook Air
- PAVILION600

Showing 1 to 5 of 5 entries (filtered from 6 total entries)

端末オプション

- EDRスキャン
- EDR診断
- EDR診断履歴
- 通知
- レポート
- サイズの大きなファイル
- システムスเปック情報
- パフォーマンス
- メンテナンス概要
- 導入済ソフト
- 機体の状態
- セキュリティ
- SuperShieldログ
- ローカルブラックリスト
- ローカルホワイトリスト
- ドライバ

端末: DESKTOP-SMALL

SuperShieldログ

SuperShieldログ絞り込み条件

プロセス名称

提供元

製品名

起動の是非(「全て」で全稼働ログ表示)

いいえ(No)

全レコード

500 records

現在の識別状態

検出時の識別状態

検索種別

全項目

絞り込み解除


絞り込み適用

Search:

プロセス名称	提供元	製品名	タイムスタンプ
ctest.exe	unknown vendor	unknown product	2023/05/23 10:05:00
crashpad_handler.exe	unknown vendor	unknown product	2023/05/23 10:05:00
photo.exe	Serif (Europe) Ltd	Photo 2	2023/05/22 13:06:00

標準で起動阻止されたアプリケーション一覧が絞り込み表示されます。

「現在の識別状態」が「未知」は、非分類(脆弱性を含むものもある)のアプリケーションで、「悪い」は、ウイルスやPUPとして判定されたアプリケーションになります。

黄色や赤色に分類され、自身や社内で作成したアプリケーションをローカル・ホワイトリストに追加する際は、追加するアプリケーションの右側にある  マークを押し、制御画面を表示します。

プロセス名称	提供元	製品名	タイムスタンプ	
FnKey.exe	unknown vendor	FnKey	2023/02/22 14:35:00	
foobar2000.exe	Piotr Pawlowski	foobar2000 Application	2023/02/10 13:46:00	
foobar2000.exe	Piotr Pawlowski	foobar2000 Application	2023/02/10 11:46:00	
Aoiro.exe	unknown vendor	aoiro	2023/02/06 13:31:00	
photo.exe	Serif (Europe) Ltd	Photo 2	2023/01/31 10:22:00	
GetuGamen.exe	unknown vendor	NewGetu	2023/01/30 15:14:00	
Aoiro.exe	unknown vendor	aoiro	2023/01/19 13:09:00	

ローカル・ホワイトリストの登録レベルを「パソコン」で、このパソコン本体のみに設定するか、「全アカウント」で、自分が管理するパソコンすべてに適用させるルールとするかを選択し、「許可」を押します。

×

SuperShield許可か拒否リストへ追加

提供元

Piotr Pawlowski

プロセス名称

foobar2000.exe

ファイルハッシュ値

0XA0AF04C0DF2FDFEAF6D28CB3F634189C

説明

foobar2000.exe - foobar2000 Application

レベル

アカウント全体

閉じる

許可リストの編集

許可

拒否

次に、「アカウント設定」-「ローカルホワイトリスト」を押して自分専用の「ローカルホワイトリスト」画面を表示します。

PC Matic

通知

サポートについて

アカウント設定

ログアウト

アカウント

アカウント詳細

オフラインアクション

パスワード変更

包括スケジュール設定

端末一覧

管理ポータルデザイン

セキュリティ

ローカルブラックリスト

ローカルホワイトリスト

ドライバ

ファイルハッシュ追加

デジタル署名追加

ファイルパス追加

Script追加

エクセル形式で出力

ファイルアップロード

CSVテンプレートのダウンロードはこちら。

検索

説明	端末登録日	詳細	レベル	プラットフォーム	現在の判定状況
foobar2000.exe - foobar2000...	2023/06/01	0xa0af04c0df2fdfeaf6d28cb3f634189c	アカウント全体	Windows	Unknown
CPUBooster.exe - Chris-PC C...	2022/07/25	0x3bf53504c71341945bc14f13ae0773...	アカウント全体	Windows	Unknown
CPUBooster.exe - Chris-PC C...	2022/07/25	0x3bf53504c71341945bc14f13ae0773...	パソコン: THINKCENTRE_MT	Windows	Unknown

「ローカルホワイトリスト」に先程追加したアプリケーションのハッシュ部分をクリックすると、セカンドオピニオンとして利用を推奨している「VirusTotal」の該当ファイルに関するページへ直接アクセスされます。

PC Matic

通知

サポートについて

アカウント設定

ログアウト

アカウント

アカウント詳細

オフラインアクション

パスワード変更

包括スケジュール設定

端末一覧

管理ポータルデザイン

セキュリティ

ローカルブラックリスト

ローカルホワイトリスト

ドライバ

ファイルハッシュ追加

デジタル署名追加

ファイルパス追加

Script追加

エクセル形式で出力

ファイルアップロード

CSVテンプレートのダウンロードはこちら。

検索

説明	端末登録日	詳細	レベル	プラットフォーム	現在の判定状況
foobar2000.exe - foobar2000...	2023/06/01	0xa0af04c0df2fdfeaf6d28cb3f634189c	アカウント全体	Windows	Unknown
CPUBooster.exe - Chris-PC C...	2022/07/25	0x3bf53504c71341945bc14f13ae0773...	アカウント全体	Windows	Unknown
CPUBooster.exe - Chris-PC C...	2022/07/25	0x3bf53504c71341945bc14f13ae0773...	パソコン: THINKCENTRE_MT	Windows	Unknown

VirusTotal による調べ方は、[VirusTotal](#) を用いた検証をご覧ください。

10 ローカル・ホワイトリストへの登録手順

PC Matic は、PC Matic 社のマルウェア分析官が静的・動的なデジタルフォレンジックを実施し、マルウェアでないものおよび、悪意ある行為を行うことができない実行ファイル(バイナリー形式・スクリプト形式)をグローバル・ホワイトリストとして分類し、全顧客でホワイトリスト登録することなく、ホワイト運用にてアプリケーションを起動許可することができる仕組みです。

このため、PC Matic の全世界の顧客が、いまだ遭遇していないファイル、脆弱性というセキュリティホールを含むもの、悪意ある行動をさせることができるアプリケーションに関しては起動を行うことができません。

起動できなかったファイルのうち、最近配信された新しい業務系アプリケーションなどは起動阻止されてから問題がなければ 24 時間以内に起動可能となりますが、自分で開発したアプリケーションなどはローカル・ホワイトリストへ登録しなければ利用できない場合があります。

また、政府が作成したアプリケーションをいますぐ利用したい際にもローカル・ホワイトリストへ登録することで即座に利用することができますが、基本的にはローカル・ホワイトリストへ登録する必要はありません。

10.1 起動阻止されたファイルを管理ポータルより把握

1. 起動阻止されたファイルは、管理メニューの「通知」-「セキュリティ」を選択します。起動阻止されたファイルなど該当するものが表示されているはずです。

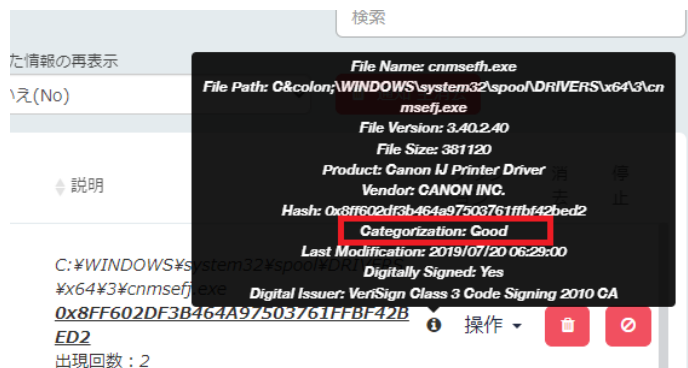


日/時	端末PATH	説明	アクション	消去	停止
2023/06/08 10:50:50	C:\WINDOWS\system32\spool\DRIVERS\x64\3\cnmself.exe	0x8FE602DF3B464A97503761FFBF42BED2 出現回数: 2 最終確認: 2023/06/08 10:50:50: SuperShieldによって起動阻止されました	操作		
2023/06/06 17:56:25		SuperShield保護内容変更:無効	操作		

ファイル名が「cmd.exe」「Wscript.exe」となっている場合は、スクリプト形式のファイルであるためスクリプト形式の調査方法を参照してください。

2. 起動ファイル名が「regsvr32.exe」となっている場合は、マルウェアの可能性があるのでローカル・ホワイトリストへ追加しないでください。(既に Good としている Windows 内部コマンドですが、不正な起動は阻止されます)

ハッシュ値と「操作」の間にある「i」印にマウスオーバーします。すると黒いポップアップが表示されます。



まず「脅威カテゴリー」の表示に着目します。

「Good」: グローバル・ホワイトリストへ追加済

「Unknown」: 未着手・脆弱性含む

「Bad」: マルウェア

10.1.1 Good となっている場合

PC Matic 社のマルウェア分析官によって既にグローバル・ホワイトリストへ追加されているため、基本的には起動可能となっています。本事象が発生するのは

- パソコン利用者がインターネットに接続していない環境でファイルを実行させようとした
 - このファイルを多く人がいま起動させ、マルウェア分析官が優先して分類した
 - ファイアウォール装置などによりグローバルリストを端末がうまく受信できなかった
- などが推測されます。

パソコンを再起動して再度起動を試してください。

10.1.2 Unknown となっている場合

このステータスの場合は、まだマルウェア分析官によって分類されていないか脆弱性が含まれているファイルになります。

「通知」-「セキュリティ」画面の「説明」の項目に表示されている MD5 ハッシュ値をクリックすると、VirusTotal によるセカンドオピニオンが表示されます。

VirusTotal は世界中のセキュリティソフトがどう検出しているかを知ることができるサイトです。

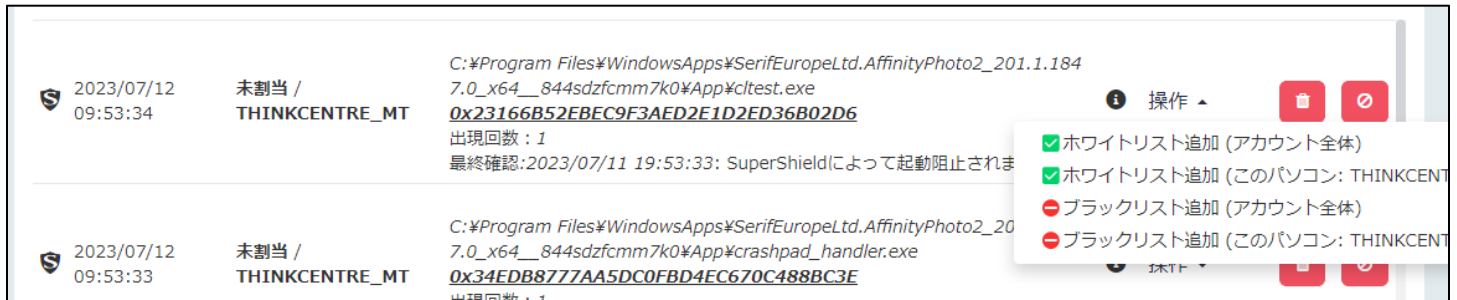
C:\WINDOWS\system32\spool\DRIVERS\x64\cnmseff.exe
0x8FF602DF3B464A97503761FFBF42BED2
 ED2
 出現回数: 2
 最終確認: 2023/06/08 10:50:50: SuperShield
 によって起動阻止されました

他の項目も確認しますが、詳しい解説は、VirusTotal を利用しての検証手順セクションをお読みください。

10.1.3 マルウェアであると判断できる場合(ローカル・ブラックリスト追加)

管理メニューの「通知」-「セキュリティ」から、起動阻止されたファイルの右の「▲」から「アカウント」にてローカル・ブラックリストへ追加します。

これで、このファイルは、アカウントで起動が完全に拒否されるようになり安全性が高まります。



このようにマルウェアと思われるファイルを追加した際はローカル・ブラックリストへ追加します。

10.1.4 Bad となっている場合

PC Matic 社のマルウェア分析官によってマルウェア判定済みであり、グローバル・ブラックリストへ追加されているため、無害化され、検疫区画へ移動されます。誤検知であると思われる場合はサポートまでご連絡ください。

10.1.5 ファイル名が cmd.exe、wscript.exe、regsvr32.exe のスクリプト形式の調査方法

スクリプト形式の場合は、ps1、wsf などのスクリプト形式の場合は、VirusTotal にバイナリー形式と同様の手順で調査を行うことができます。多数ある bat ファイルは VirusTotal に乗っていないことが多く、またアップロードしても正しい検査結果はあまりでないようです。

Bat は、MS-DOS 時代のバッチファイルと呼ばれるもので、Windows11/10 時代での利用は推奨されていませんが、後方互換性のために実行は可能です。このため不明の際はローカル・ホワイトリストに追加しないほうが安全です。

ps1 は、PowerShell スクリプトで最近はこの方式を用いたマルウェアが急増しています。ただしすべてがマルウェアという訳ではありません。

起動阻止される形式のスクリプトファイルは多くあります。起動をかけているディレクトリ、この例であれば、

C:\Users\PC10\Dropbox\new 綱VE 纒、綱ヲ綱我ヲ穂コ狗畑\譚ス蜈ハ\笆罎纒ケ綱シ綱代・SALE\2023SS

というクラウドストレージや会計ソフトなどの無害と推測されるディレクトリに格納されているファイルであれば、ローカル・ホワイトリストへ追加し、起動許可を与えてください。

判断がつかないものは、ローカル・ホワイトリストへ登録しないことをお勧めします。

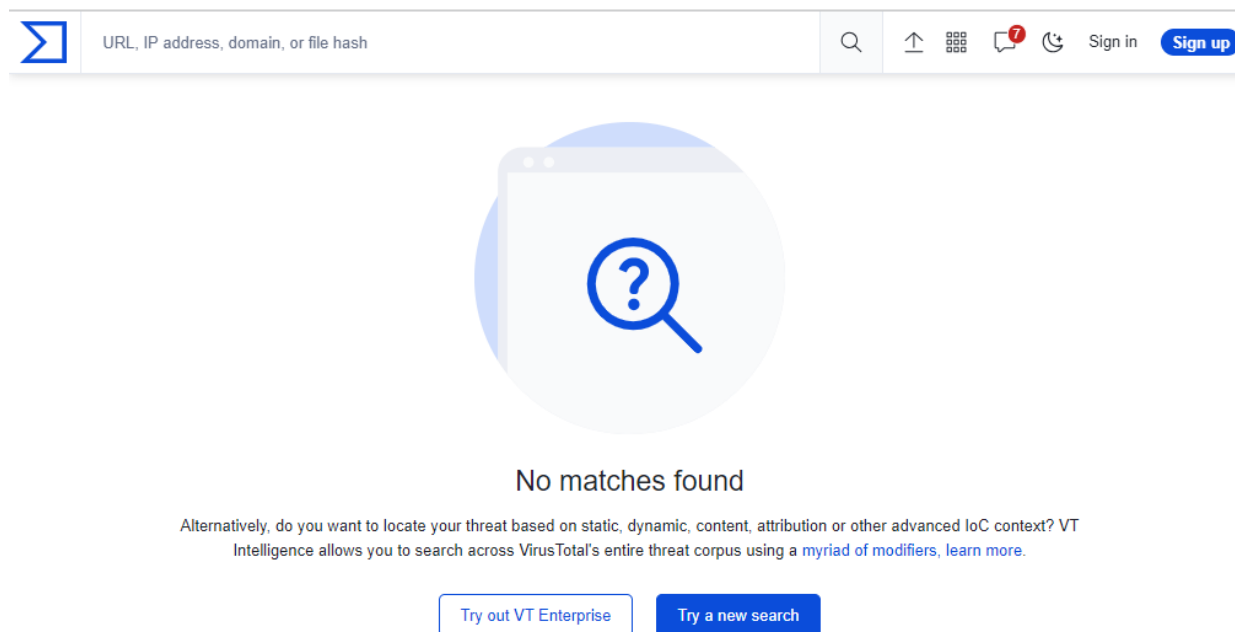
なお、スクリプトも PC Matic 社のマルウェア分析官によってデジタルフォレンジックが行われ、問題のないファイルであれば、グローバル・ホワイトリストへ追加され起動許可が与えられます。

スクリプトの場合、判断がつかない場合はローカル・ホワイトリストへ追加しないほうが良いでしょう。

10.2 VirusTotal を用いた検証

VirusTotal は、世界中の従来型セキュリティソフトを用いたセカンドオピニオンとして有効な分析サイトです。

VirusTotal には、過去誰かが手作業で検体ファイルをアップロードした際にのみ表示されます。このため、自社開発アプリケーションや比較的新しいファイルは、VirusTotal では表示されないことがあります。このため、検出されたファイルが必ず VirusTotal にて分析内容が表示される訳ではありません。



この場合は、該当パソコンから起動阻止されたファイルを VirusTotal にアップロードします。

10.2.1 VirusTotal へのアップロードと検証手順

「通知」-「セキュリティ」にて、起動阻止されたファイルの「説明」にあるファイルパスとファイル名を Windows メモ帳などにコピー & ペーストをしてメモしておきます。

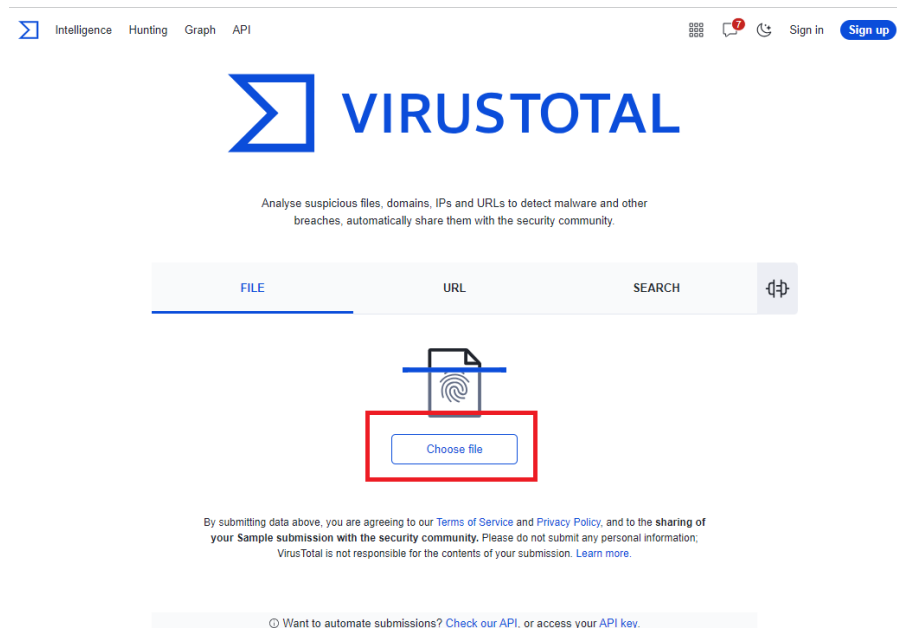
10.2.2 起動阻止されたファイルの探索

「通知」-「セキュリティ」にて、起動阻止されたファイルのファイルパスとファイル名を調べ、Windows エクスプローラーにてそのファイルを探します。

10.2.3 VirusTotal にアップロード

右のリンクより VirusTotal を開きます。 <https://www.virustotal.com/gui/home/upload>

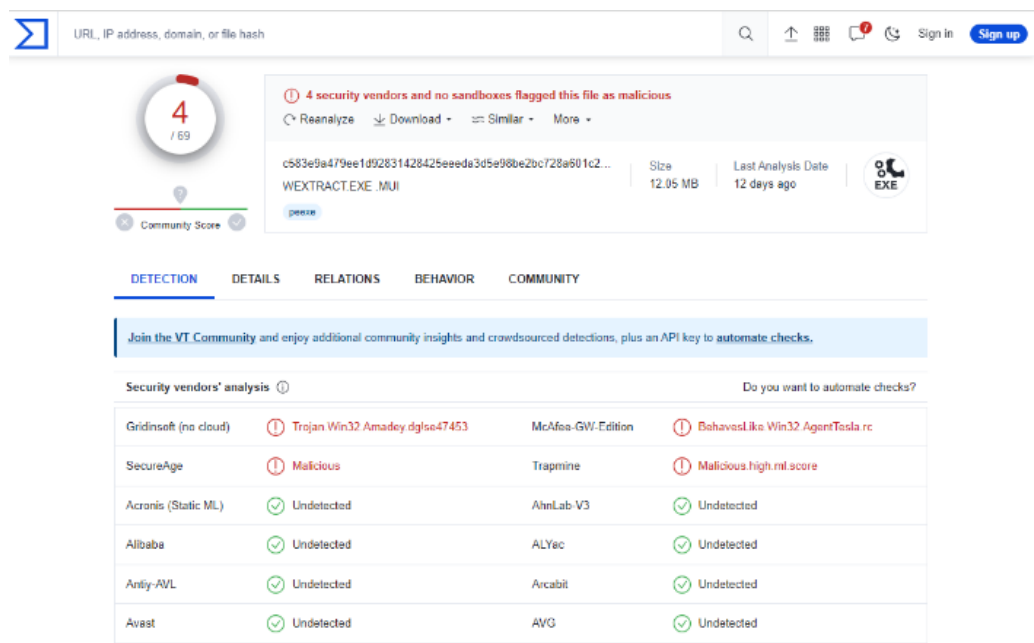
開いた画面の「Choose File」ボタンを押して起動阻止されたファイルをアップロードします。



しばらくするとアップロードされたファイルの検査結果が表示されます。

70 程度のセキュリティソフトのうち何個が悪質と判定しているかが表示されます。SecureAge、MaxSecure、Bkav pro、Jiangmin、Zillya は、いつも誤検知を表示しますので参考にしないでください。

10 個程度が検出していれば明らかにマルウェアですので、ローカル・ホワイトリストへ追加するなどして起動許可を与えず、ローカル・ブラックリストへ追加してください。



10.2.4 Behavior タブで素性や問題がないか確認

続いて「BEHAVIOR」タブをクリックして表示してください。

「Activity Summary」にて、過去マルウェアが利用したハッキング手法に該当するものが、この実行ファイルに含まれている場合は表示されます。

下記事例では、Mitre Signature に HIGH が 2 件含まれていますが、1 件でも HIGH の扱いがあった場合は、マルウェアの可能性が高いと言えます。ブラックリストへ追加ください。Sigma Rules も注意が必要です。

Dropped Files は、展開されたファイルの情報になりますが、マルウェア展開されるとここに警告が表示されます。警告された場合は、マルウェアを展開するローダーという種類のマルウェアである可能性があります。

Network comms には、悪意あると識別されている既知の C&C サーバー(マルウェアを展開させるなど実行指示をさせるサーバー)との通信があるかを警告します。下の例では 1 件の通信が確認されていますので危険となります。

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 7

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

☒ Display grouped sandbox reports

<input checked="" type="checkbox"/> C2AE <div> 0 0 0 0 1 3 </div>	<input checked="" type="checkbox"/> Rising MOVES <div> 0 0 0 0 0 0 </div>
<input checked="" type="checkbox"/> VirusTotal Jujubox <div> 0 0 0 0 0 0 </div>	<input checked="" type="checkbox"/> VirusTotal Observer <div> 0 0 0 0 0 0 </div>
<input checked="" type="checkbox"/> Zenbox <div> 0 8 1 3 18 19 </div>	

Activity Summary
Download Artifacts
Full Reports
Help

Detections
NOT FOUND

Mitre Signatures
2 LOW
24 INFO

IDS Rules
1 LOW

Sigma Rules
2 MEDIUM
1 LOW

Dropped Files
1 OTHER
1 DOS_COM
1 TEXT
1 JAVASCRIPT
1 PDF
1 PE_EXE
1 MSI

Network comms
2 HTTP
4 DNS
12 IP
3 JA3

10.2.5 Relation タブで通信先、展開ファイルなどを調査

Contacted URLs には、このプログラムによる通信先が表示されます。PDF 変換など有用な機能をもっているフリーソフトウェアが、不必要に外部通信を行うことなど目的外の挙動を行うものがあります。その際には、この項目に注意する必要があります。悪意あると識別されている既知の C&C サーバー(マルウェアを展開させるなど実行指示をさせるサーバー)との通信があるかを警告します。この例では、90 のセキュリティソフトのうち 12 製品が「危険」と判定しているサイトへ通信していることを示しています。

Contacted URLs (2) ⓘ				
Scanned	Detections	Status	URL	
2023-05-10	0 / 89	-	https://ardownload3.adobe.com/pub/adobe/reader/win/AcrobatDC/2300120174/AcroRdrDCUpd2300120174_MUI.msp	
2023-07-07	12 / 90	404	http://62.233.57.136/	

Execution Parents には、このプログラムがどのようなファイルから実行されたか親を示しています。下の例では html ファイルから Windows Installer が起動し、このプログラムが実行されたことを表しています。21 の製品が html を危険だとし、34 の製品がインストールプログラムをマルウェアと判定しています。

Execution Parents (2) ⓘ			
Scanned	Detections	Type	Name
2023-07-12	34 / 60	Windows Installer	tuncxwfw
2023-07-12	21 / 59	HTML	202305 Indicative Planning RELEX.html

Bundled Files には、このプログラムに同梱されていたファイルの情報が示されます。下の例では、RoboForm.dll という Windows ダイナミックリンクライブラリ(サブプログラムのようなもの)が 33 の製品で危険であると判定しています。

Bundled Files (2) ⓘ			
Scanned	Detections	File type	Name
✓ 2023-07-06	33 / 70	Win32 DLL	RoboForm.dll
✓ 2023-06-19	0 / 71	Win32 EXE	robotaskbaricon.exe

Dropped Files には、このプログラムから展開・外部通信によってダウンロードされたファイルの情報が示されます。

下の例では、マルウェアと確定するにふさわしいファイルが展開されていることがわかります。

Dropped Files (12) ⓘ			
Scanned	Detections	File type	Name
✓ 2023-07-06	33 / 70	Win32 DLL	RoboForm.dll
✓ 2023-05-09	0 / 59	PDF	202305 Indicative Planning RELEX.pdf
✓ 2023-07-12	34 / 60	Windows Installer	tuncxwfw
✓ 2023-06-19	0 / 71	Win32 EXE	robotaskbaricon.exe
✓ ?	?	file	02ba16481a349b54284b5ea37f211f60bb8243100db362122cffe9a2577e43db
✓ ?	?	file	077a9997c4f3f95b80f0d2b6e24ef87645b8a0747436722d1317d61df950057
✓ ?	?	file	23853ecd5459ff99d51b65e70e2b2848347ab5d26c3d9cd69073d69c8d4986d8
✓ ?	?	file	475b5c523f2661fc6633b9217613ff47839eaf9a689fed3ac27bfdc6e44f08b3
✓ ?	?	file	5fea85a1177a25b5c69ab4a0cad87e382dfc66eccbda2587ad69b41f026c55ed
✓ ?	?	file	8102e8f36020bc462853046a4bef51de3fb8f2bc3ed24d96e42ce397a6003ea0

10.2.6 Detail タブで最終調査

このタブでは、まず History の項目に着目します。

Creation Time (制作年月日)が 2009 年以前の日付である場合、Microsoft Visual C にてコンパイルされたアプリケーションが持つ、Microsoft ATL (Active Template Library) 脆弱性に影響されている可能性が濃厚です。このため、アプリケーション利用中は端末に侵入されるリスクが高まります。この脆弱性の深刻度は高く、可能な限り利用しないことが推奨されます。このため、ローカル・ホワイトリストへは極力登録しないでください。

日付が現在よりも未来になっていることがあります。マルウェアが比較的によく利用する手法であるためローカル・ホワイトリストへは登録しないでください。

History ⓘ	
Creation Time	2023-05-09 07:29:26 UTC
First Submission	2023-05-09 09:59:48 UTC
Last Submission	2023-05-09 13:25:44 UTC
Last Analysis	2023-07-12 00:29:06 UTC

次に **Signature info** でデジタル署名が付与されているかを確認します。善良なアプリケーションであれば、デジタル署名やカタログ署名がなされています。マルウェアの大半は、こうした署名がない状態で配布されることが一般的です。

Signature info ⓘ

Signature Verification

✔ Signed file, valid signature

File Version Information

Copyright	Copyright 2013-2022 KING JIM CO.,LTD.
Product	SR5900P Status Monitor
Description	Status Monitor
File Version	5,5,0,0
Date signed	2022-10-31 16:36:00 UTC

Signers

- + 株式会社キングジム
- + DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
- + DigiCert Trusted Root G4
- + DigiCert

Counter Signers

- + DigiCert Timestamp 2022 - 2
- + DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA

署名がない場合は、ファイル名でインターネット検索を行ってください。どの企業が作成して配布しているかの目安を得ることができます。

以上の作業で善良であるか、グレーであるか、マルウェアであるかの判断がつきます。マルウェアであると推測される際は、ハッシュ値でローカル・ブラックリストへアカウント全体のレベルにて追加してください。

10.3 管理ポータル「通知」－「セキュリティ」から追加

10.3.1 通知－セキュリティからハッシュ、スクリプト登録

1. 「通知」－「セキュリティ」を選択します。起動阻止されたファイルなど該当するものが表示されているはずです。



2. ファイル名が「cmd.exe」「Wscript.exe」となっている場合は、スクリプト形式のファイルであるためスクリプト形式の調査方法を参照してください。善良なスクリプトはここから登録できます。

3. 起動阻止されたアプリケーションの「アクション」にある「操作」を押すと下のような画面が表示されます。



4. 必要なレベルを選択してポップアップした画面で「確認」を押すとローカル・ホワイトリストへ追加されます。

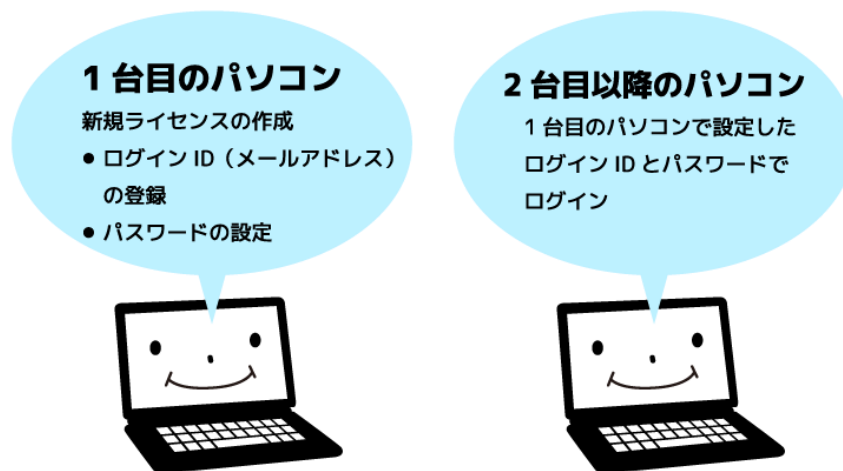
11 よくある質問

ホームページに掲載しているよくある質問の中から特に質問の多いものをご紹介します。なお、ホームページのよくある質問は、随時更新中ですのでご不明な点がございましたらご一読ください。

11.12 台目にライセンス認証キーを入力しているのに利用登録できない

ライセンス認証キーは、1 台目のパソコンで登録された際に無効化されております。

PC Matic は、クラウドアプリケーションであるため、1 台目のパソコンで利用したログイン ID(電子メールアドレス)にライセンス管理が関連づけられます。2 台目以降のパソコンをご利用する際は、ログイン ID とパスワードを入力してログインしていただく事で、ライセンスの範囲内にてご利用いただけるようになります。



11.2 起動時にエラーや白か黒の単色画面表示し、PC Matic が起動しませんでした。

PC Matic はクラウドアプリケーションであるため、インターネット上から必要な最新のアプリケーションモジュールをダウンロードして起動します。

このため、PC Matic より起動されるアプリケーションが Internet Explorer のセキュリティ設定、もしくはセキュリティソフトによって起動が阻止されている場合、このような現象が発生いたします。このような現象が発生した場合には、以下の設定を見直していただきますようお願い申し上げます。

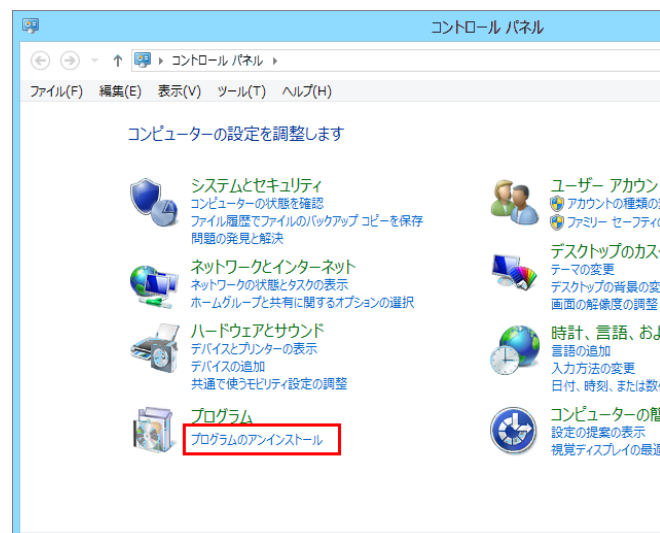
(1)Internet Explorer の「インターネットオプション」-「セキュリティ」において、インターネットのセキュリティゾーンを「中」もしくは「中低」に設定し、「既定」ボタンを押して JavaScript の設定/Cookie 受入を有効化してください。

(2)ウイルス対策等のセキュリティソフトによって起動が阻止されている可能性がありますので、セキュリティソフトの「ホワイトリスト」に、PC Matic を追加ください。

PC Matic はセキュリティ関係者の業界会合へ参加しており、相互にセキュリティエンジンで誤検知が起きないよう連携を深めておりますが、一部の古いセキュリティ対策エンジン、もしくは業界会合に参加していないベンダー製品は、PC Matic の起動を阻止してしまう可能性があるためです。

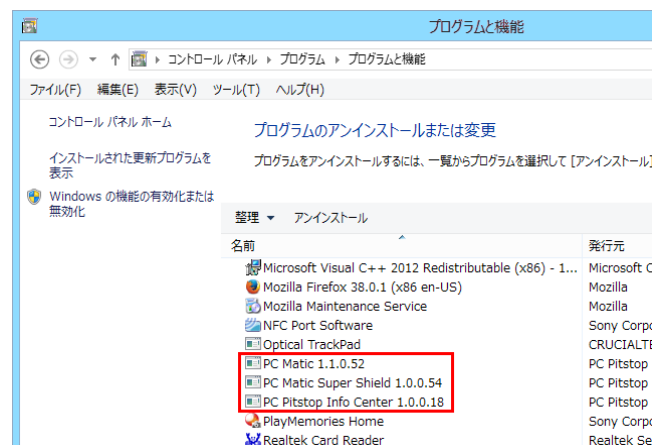
11.3 削除対象のパソコンから PC Matic 関連のアプリケーションの削除

1. Windows の「コントロールパネル」を起動し、「プログラムのアンインストール」もしくは「プログラムの追加と削除」を選択します。

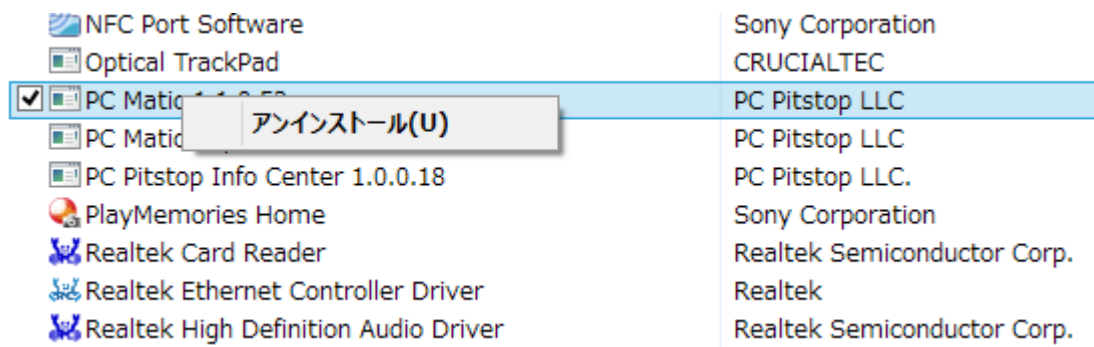


2. リストの中から、下記 3 つを探し以下の順番にてアンインストールを行ってください。3 番目の"Info Center"は基本的に自動的に削除されます。

1. 【インストーラ管理画面】PC Matic Info Center
2. 【本体】PC Matic
3. 【アンチウイルス】PC Matic SuperShield



3. 削除するプログラムを選択して右クリックをし、アンインストールを選択してください。



11.4 インストーラ管理画面から削除対象の端末を削除

1. PC Matic を起動しインストーラ管理画面を表示させます。
ログインしていない場合は、電子メールアドレスでログインしてください。

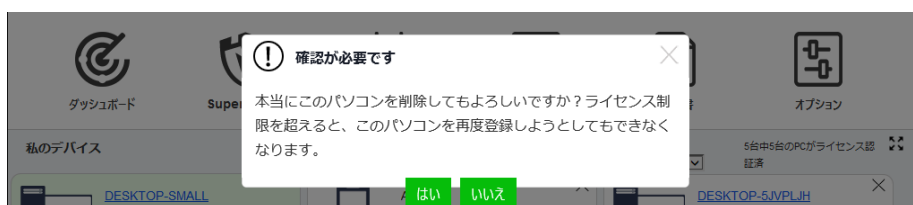
「私のデバイス」を押します。



2. 削除したい端末の右上にあるバツマークをクリックします。(赤枠で囲まれた箇所)



3. 表示されたダイアログで「はい」を押すと情報が削除され利用可能ライセンス枠が1つ増加します。



11.5 ファイアウォールに設定するための IP アドレスを教えてください

PC Matic に限らずエンドポイントセキュリティが必要とする制御情報の更新や機能改善のためのセキュリティエンジン更新時は、ウイルスの特徴を表すコードが含まれています。これにより、UTM 等のファイアウォール装置が持つアンチウイルス機能によるパケット監査において、ウイルスそのものであると誤検知される事により通

信が阻止されることや、パケット監査のために通信速度が極端に低下することがあるとの報告を頂いております。このような症状が発生している場合には、PC Matic の開発元である PC Matic 社が現在利用している以下の FQDN もしくは、IP アドレスを監査除外へ設定をしてください。

PC Matic では、以下の FQDN を利用しております。またそれぞれの IP アドレスは以下のとおりです。ポート番号は、80 と 443 です。以下は日本国内から利用する際のアドレスです。

IPv4 回線

通信先	Source IP	Port	Destination IP	Port
宛先 OutBound 1	(LAN)	* もしくは any	104.20.238.118	80,443
宛先 OutBound 2	(LAN)	* もしくは any	104.20.237.118	80,443
送信元 InBound 1	104.20.238.118	80,443	(LAN)	* もしくは any
送信元 InBound 2	104.20.237.118	80,443	(LAN)	* もしくは any

IPv6 回線 (フレッツ光)

通信先	Source IP	Port	Destination IP	Port
宛先 OutBound 1	(LAN)	* もしくは any	2606:4700:10::6814:ee76	80,443
宛先 OutBound 2	(LAN)	* もしくは any	2606:4700:10::6814:ed76	80,443
送信元 InBound 1	2606:4700:10::6814:ee76	80,443	(LAN)	* もしくは any
送信元 InBound 2	2606:4700:10::6814:ed76	80,443	(LAN)	* もしくは any

収容されている FQDN

FQDN	法人版	個人版	用途
supershield.pcpitstop.com	●	●	SuperShieldログ受電サーバ群
supershield-files.pcpitstop.com	●	●	SuperShieldプログラム
ss-api-v1.pcpitstop.com	●	●	SuperShield制御プログラム
utilities.pcpitstop.com	●	●	制御プログラム
switchboard.default.pcpitstop.com	●		EDR制御プログラム
switchboard.pcmatichome.com		●	EDR制御プログラム
ny.cf.pcpitstop.com	●	●	回線最適化試験
echo.pcpitstop.com	●	●	回線応答速度試験
api.pcpitstop.com	●	●	API接続用途
defs.pcpitstop.com	●	●	SuperShield制御ファイル
drivers.pcpitstop.com	●	●	Driver更新用サーバ
software.default.pcpitstop.com	●	●	著名ソフトウェア自動更新サーバ
files.pcpitstop.com	●	●	PC Matic最新ファイル格納サーバ
logfiles.pcpitstop.com	●	●	テクニカルサポート用ログ格納
satellite2.default.pcpitstop.com	●	●	EDR診断実行時の制御サーバ
satellite3.default.pcpitstop.com	●	●	EDR診断実行時の制御サーバ
satellite4.default.pcpitstop.com	●	●	EDR診断実行時の制御サーバ

11.6 ウィルス、善良なアプリ、PUP の判定基準について

PC Matic SuperShield は、他社と比較して厳しい分類基準になっています。

一般的なセキュリティ対策ソフトの基準に加えて、以下を準ウィルスとして駆除対象としています

- アンインストールをしても広告を表示する(PUP, Adware)
- ブラウザーの[HOME]を特定サイトに固定する機能をインストーラー等を持つ
- 各国の政府関係機関により、政府関係機関にて利用が禁止されているアプリケーション
- ゲームソフトでありながら EXCEL 等のファイル転送を行うなど、目的外の動作を行う
- 対外的に認識されているアプリケーションの目的外と思われる通信を実施
- 特定の IP アドレスにおいて異なる挙動を行うコードの内包

など

【困難な判断基準。PC Matic は厳しい基準で対応】

アプリケーションが迷惑なアプリケーション(PUP)であるか、ウィルスか、善良なアプリケーションなのかの線引きは利用者によって判断基準が異なり、私たちセキュリティベンダーにとっても基準作りはひとつの大きな課題です。

利用者にとってどのようなアプリケーションが広告などを表示して迷惑なアプリケーションなのか、広告は表示するものの使い勝手のよい機能を提供してくれるアプリケーションなのか。また、とても使い勝手の良いかな漢字変換機能を提供する代わりに、キーボードから入力された全ての文字や単語をクラウドに転送するアプリケーションを善良と判断して良いのか。その判断基準を作成するのはとても難しいものがあります。

一般的にウイルスとされていないアプリケーションであっても、西側諸国の政府にて、政府関連機関において導入しないことを推奨するアプリケーションリスト(政府非推奨アプリケーションや機能)が存在しています。

また、迷惑な広告を表示し続ける広告や、検索エンジンを特定のものに固定する機能などは、一般的なセキュリティソフトでは、ウイルスとされないのが(PUP:迷惑なアプリケーション)一般的です。これらをウイルスとしていないのは、セキュリティ評価機関がウイルスとしていないため、ウイルスと指定すると誤検知と判断され認証マークが取得できなくなるからです。しかし、利用者にとってはとても迷惑なものです。

【各国政府による不適切ソフトもウイルス指定】

PC Matic は、米国政府機関にて採用されている背景から、ウイルスとされていないものの、西側諸国の政府にて導入しないことが推奨されているアプリケーションや PUP をウイルスや望まないアプリケーションとして削除対象としています。一般的なセキュリティソフトは確実に黒判定されていないグレーのものは、疑わしくても起動を許可します。しかし、PC Matic は「疑わしきは許可せず」（グレーはブラック）という軍事レベルの判定基準により、厳格に悪意のある可能性をもつアプリケーションを起動阻止しています。昨今においては、マニアが面白半分に作成するウイルスよりも、1 万倍もの差で国家諜報機関がある意図をもってウイルスや諜報ツールを作成しています。このような背景から、軍事レベルの

【古いアプリケーションは脆弱性を抱え終焉を迎えます】

また、ウイルスではないものの、Windows XP 時代に作成された古いアプリケーションは、残念ながらセキュリティホールを抱えていることが一般的です。コンパイラにて作成されたものに深刻なセキュリティホールが発見されたからです。こうしたアプリケーションを利用することで、パソコンへの侵入を許したり、悪質なコード実行を許したりしてしまうものが多くあります。長年愛したアプリケーションが利用できないことは、とても残念ですが、セキュリティホールを抱えているアプリケーションを利用することは、セキュリティリスクを極端に高めるため、「グレー判定」としています。グレー判定したアプリケーションは、削除しないものの PC Matic は

判定基準をもって怪しいアプリケーションは、起動を阻止し削除するべきと考えているのが PC Matic です。お客様の視点にたち、保護を優先することがお客様の役に立つと考えているからです。

一般的にはウイルスではないものの、PC Matic ではウイルスや PUP として判定されているものには、こうした政府勧告や ISP 指定のものがあります。PC Matic は日本の大手 ISP より提供を受けた、迷惑な広告を表示しパソコンに変調を来すアプリケーション、150 本以上を PUP として登録し、駆除対象としています。高水準でのセキュリティを実現するために欠かせない基準であると私たちは考えています。

起動を阻止し続けます。グレー判定された場合は、同様な機能を提供する新しいアプリケーションへの乗り換えを検討する時期としての判断を行って頂ければ幸いです。使い慣れたアプリケーションを止めることは残念ですが、ポンコツなものを長く使い続けることには、大きなリスクが伴うのです。どんなものにも寿命があると考え、新しい環境で作られたアプリケーションのご利用ください。

古い自動車を誰かがメンテナンスをしなければ乗り続けられないのと同様です。動くから良いのではなく、動かし続けることで危険性は増します。

【疑わしきは罰することで高い安全性を確保】

PC Matic が世界中のセキュリティベンダーから絶賛されている理由は、この厳しめのセキュリティ判断基準にあります。安全性を高めるために、疑わしいアプリケーションは標準状態では起動できない処置をし、安全性の低下を警告しております。PC Matic では、これらをすべて準ウイルスとして駆除対象や起動を阻止する処置をしています。

PC Matic 個人版マニュアル

完