PC Matic

第 29 版

ユーザーガイド
macOS 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

PC Matic for macOS は、macOS High Sierra バージョン 10.13.2 以降に対応しています。
CPU は、Intel、Apple Silicon 両方に対応しています。

PC Matic は、次世代エンドポイント保護製品であるため、操作ダッシュボードはアプリケーションではなく、ブラウザーを用いて操作を行います。お客様による定期的な手動スキャンは必要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します。

一般的なセキュリティソフトが端末内で監査を行うのに対し、PC Matic は監査をクラウド上のスーパーコンピュータで実施します。一般製品の数百倍～数万倍の監査をクラウド上で実施しています。

NIST SP 800-167 に準拠したアプリケーション・ホワイトリスティング方式により、米国防総省による政府や外交・軍などの機密情報のような機密性ではないが公開や漏えいすると政府などに大きな影響がある情報を管理するセキュリティ成熟度情報である、NIST CMMC レベル 5(最高)に対応したセキュリティを macOS でも実現いたしました。

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。

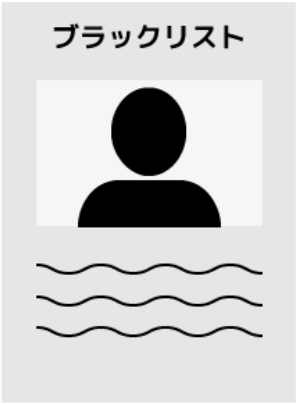
またフリーソフトウェアなど脆弱性を抱えているものも多いアプリケーションを利用することができる一般的なセキュリティソフトと同一の保護レベル(NIST CMMC Level 3)であるブラックリスト方式では、セキュリティホールを抱えるフリーソフトウェアなどもご利用頂けます。またアプリケーション・ホワイトリスティング方式では PC Matic 社のマルウェア分析官によるデジタルフォレンジックが２４時間程度でなされるまで待たなければアプリケーションやスクリプトを稼働させることができませんが、このモードでは稼働させることが可能です。

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ニングや、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。



指名手配レベル

広く知られているセキュリティソフト

空港保安レベル

AI 型 NGAV 製品

軍事レベル

PC Matic PRO

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。

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。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 Google Chrome 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

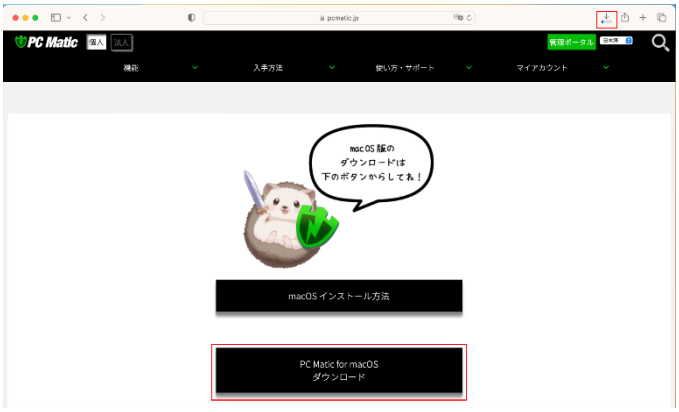
ブラウザー経由でのマルウェアの侵入を多段で防ぐことができる他、前述の悪質な行為を可能な限り阻止します。

3 インストール

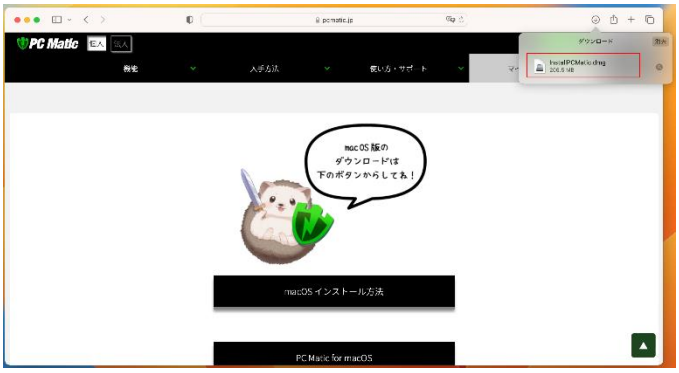
PC Matic のインストール方法からセキュリティ有効までの手順を記載しています。

3.1 インストール手順

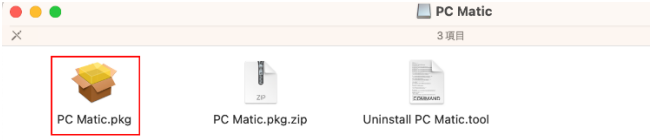
1. PC Matic のインストールを行います。
   https://pcmatic.jp/dl/mac/の
   ダウンロードページより macOS 版の「ダウンロード」ボタンを押します。



2. ダウンロードしたインストーラを開きます。
   Safari の場合は、右上のダウンロードを押して表示されたファイル名を押すと、ダウンロードしたファイルが開きます。



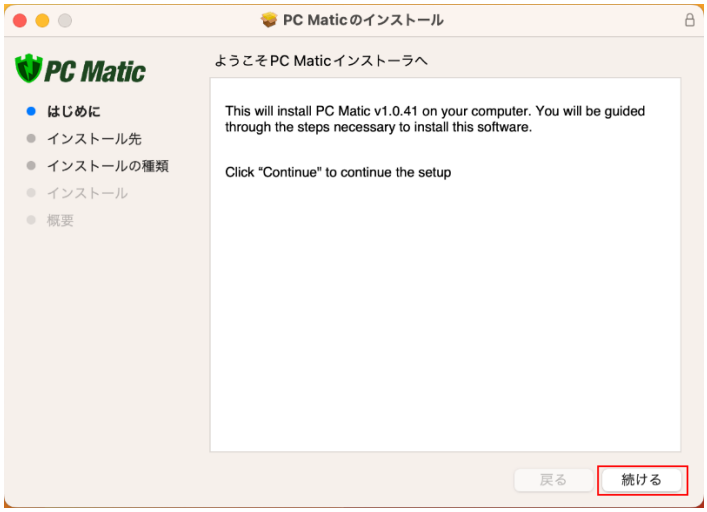
3. 「PC Matic.pkg」をダブルクリックしてインストーラーを起動します。



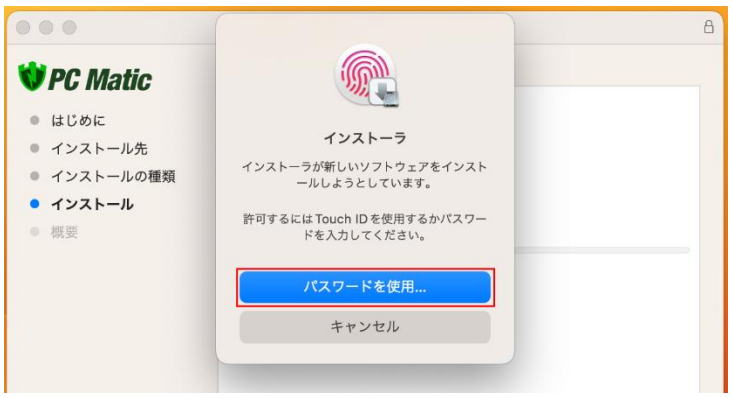
4. メッセージが表示されたら、「インストール」を押します。

5. Touch ID、もしくはパソコンにログインする際のパスワードを入力します。

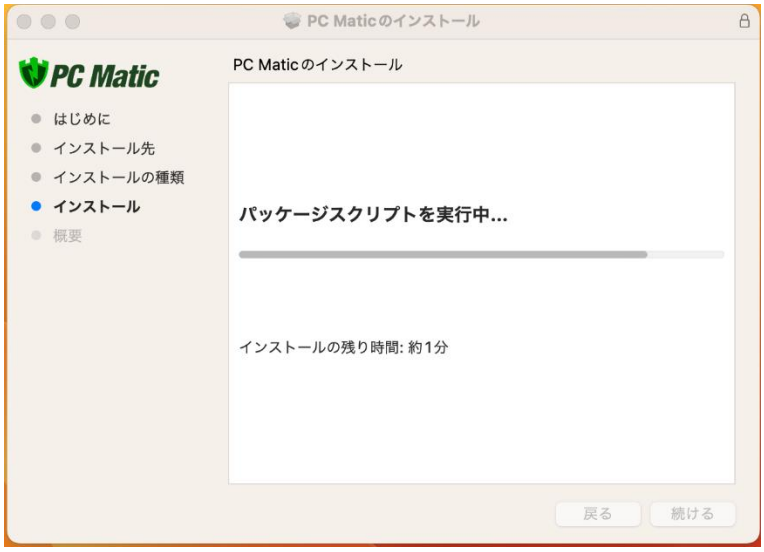
6. インストーラーが起動したら、「続ける」を押します。



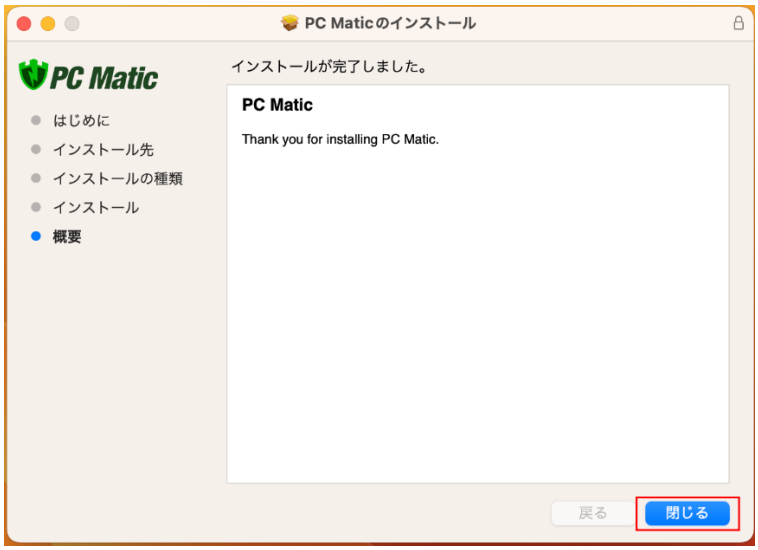
7. Touch ID、もしくはパソコンにログインする際のパスワードを入力します。



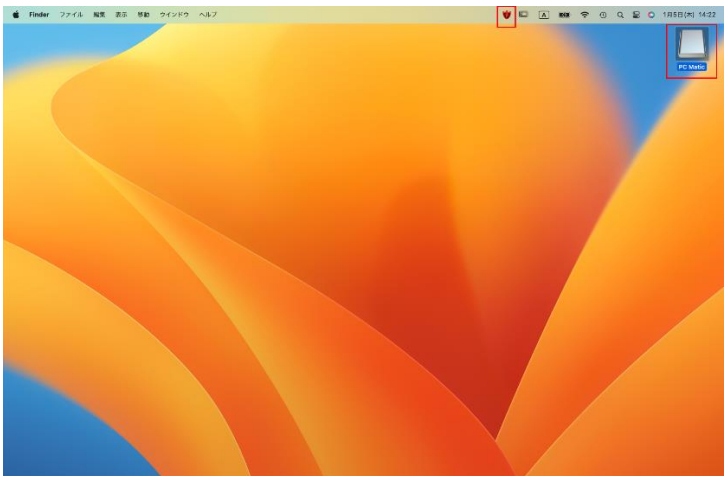
8. インストールが始まります。



9. インストールが完了しましたら、「閉じる」を押します。

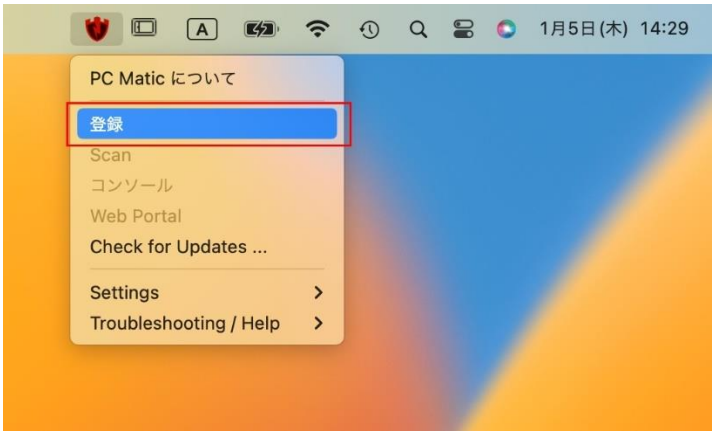


10. デスクトップの右上に PC Matic の SuperShild マークが表示されます。



11. デスクトップの右上に PC Matic とある場合は「"PC Matic"を取り出す」を行ってください。

12. デスクトップの右上にある SuperShild マークを右クリックして「登録」を選択します。



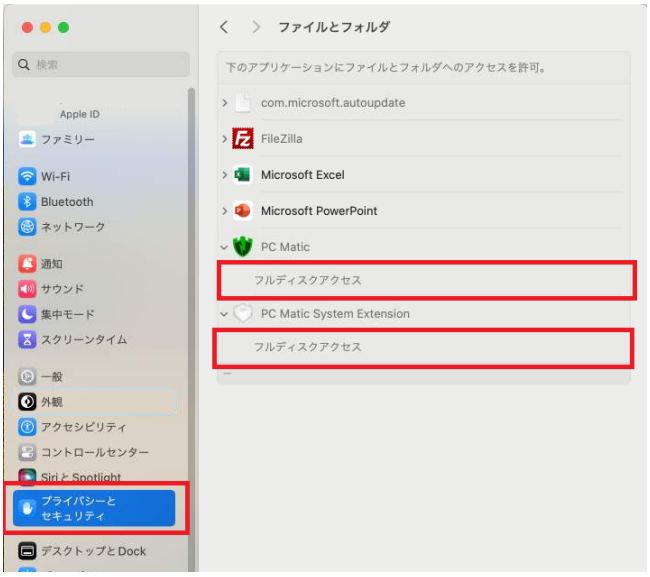
13. PC Matic のアカウントを作成している場合は、メールアドレスとパスワードを入力して「OK」ボタンを押すとライセンス認証が完了します。

アカウントを作成していない場合は、「Create a PC Matic Account」を押してアカウントを作成してください。

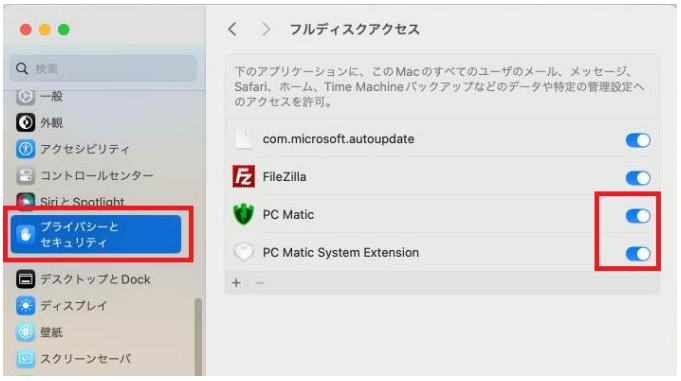
※パスワードが入力できない場合は、Safari の自動入力機能をオフにすると入力できるようになります。

14. 機能拡張がブロックされました」と表示されたら「システム設定を開く」を押します。

15. macOS にて表示された画面から「許可」を押して「プライバシーとセキュリティ」の「ファイルとフォルダ」にある「PC Matic」と「PC Matic System Extension」に「フルディスクアクセス」を与えます。

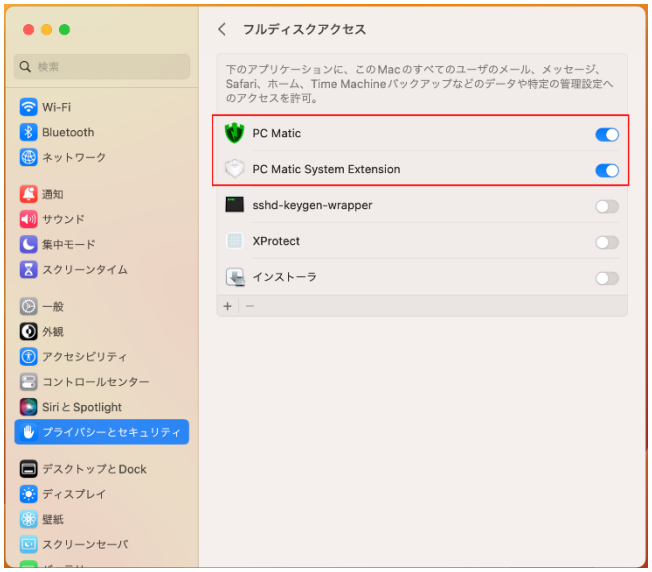


16. 「プライバシーとセキュリティ」-「フルディスクアクセス」から「PC Matic」と「PC Matic System Extension」を右にスライドして有効にします。



17. 上記設定の際は、Touch ID、もしくはパソコンにログインする際のパスワードを入力します。

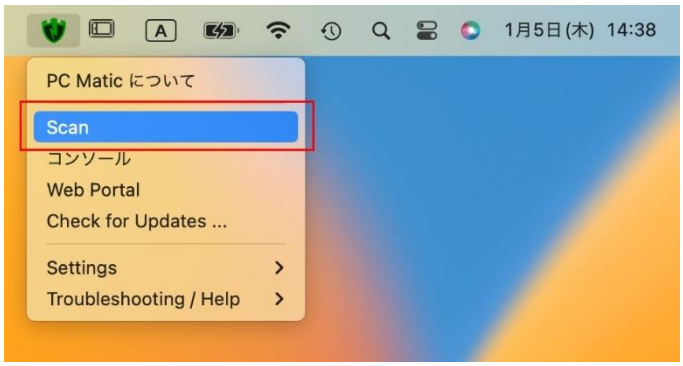
18. 「PC Matic」と「PC Matic System Extension」のフルディスクアクセスが許可されている形（バーが青色）になっていれば、インストール完了です。



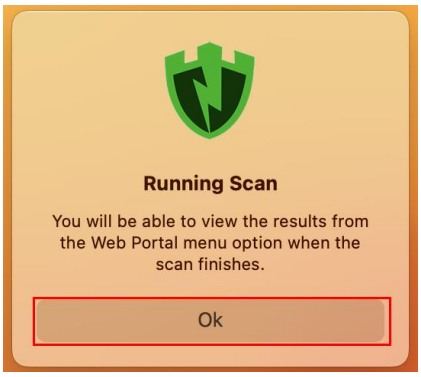
4 初期診断する

インストール後は初期診断を行う必要があります。

1. Mac のメニューバーに PC Matic の SuperShield アイコンが追加されています。
   右クリックして「scan」を選択し、初期診断を実施します。



2. ポップアップが表示されたら「OK」ボタンを押します。
   スキャン中は特に画面等表示されません。

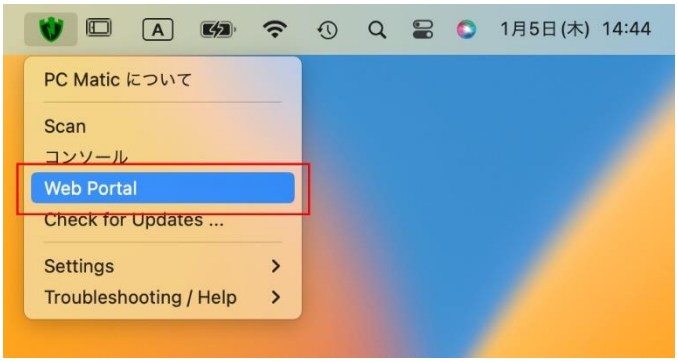


4.1 診断結果画面について

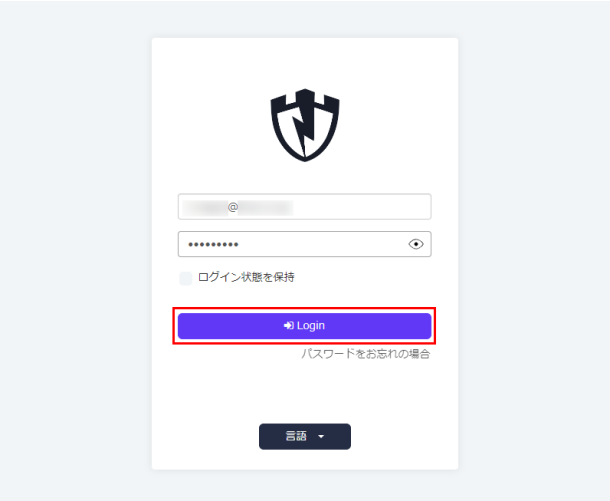
診断結果は管理ポータルで確認できます。

1. メニューバーの SuperShield アイコンを右クリックし、「Web Portal」を選択します。PC Matic は次世代エンドポイント保護であるため、この画面で PC Matic を操作・管理します。

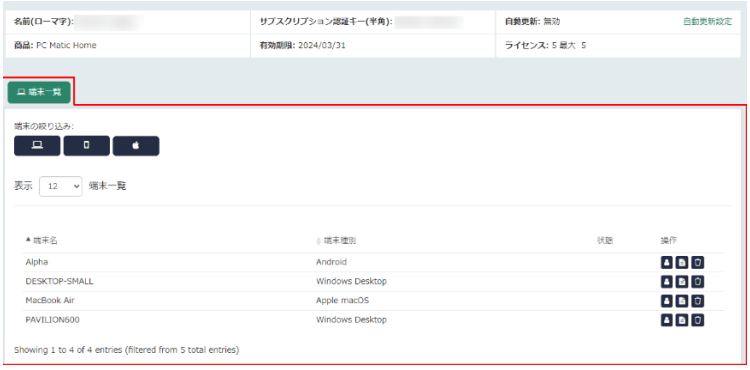
   自動更新であるため「Check for updates」は基本的に操作する必要はありませんが、サポートから指示があった場合に実行してください。



2. ログイン画面が表示されますので、「電子メール」「パスワード」を入力して「ログイン」を押します。



3. ログインすると、端末情報が表示されます。
（ログイン後に違うページを開いて閉じた場合は、次回ログイン時に閉じた際に表示していたページが表示されます。



4. 端末情報の左メニューから「EDR 診断履歴」を選択します。

5. 履歴から見たい診断結果を選択します。

6. 診断結果が表示されます。

4.2 スケジュールを設定する

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。

1. 左側のメニューから「アカウント設定」を選択して、表示されたメニューから「包括スケジュール設定」を選択し、「Add スケジュール」ます。

2. 表示された画面で設定項目を確認します。
   また、頻度を「毎週」に変更し、開始日、開始時刻を設定して、「保存」ボタンを押します。

3. 登録したスケジュールが表示されます。

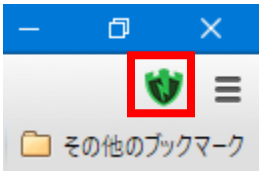
5 詐欺対策(ブラウザー保護)

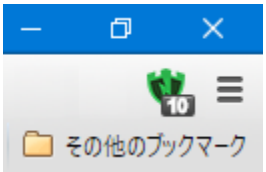
ブラウザーに Google Chrome を使用している場合は、詐欺対策を行うことができるブラウザー保護機能を使用する事ができます。Safari には現時点では対応していいません。

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に広告を非表示にします。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ございません。

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。灰色の状態で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。

5.1 インストールについて

ブラウザー保護機能を使用する場合は、それぞれのブラウザー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 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。

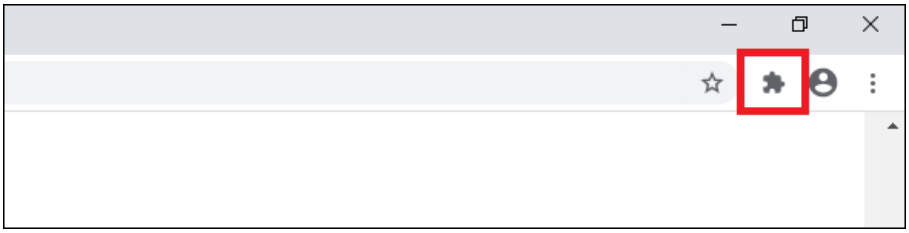
ブラウザー保護機能導入方法:https://pcmatic.jp/faq/webshield/03/

5.1.1 Google Chrome の場合

1. ここをクリックして、Chrome ストアにアクセスしてインストールします。

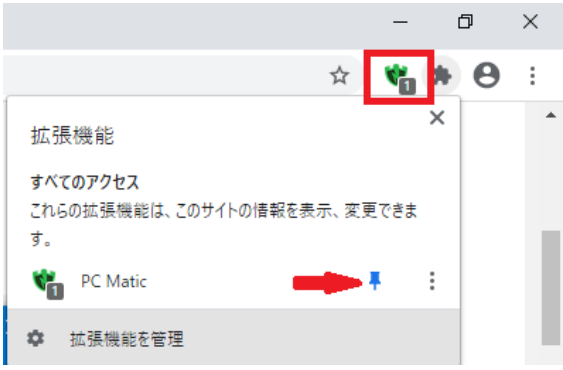
アイコンが非表示になっていないか確認

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、その先の画鋲マークがオン(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

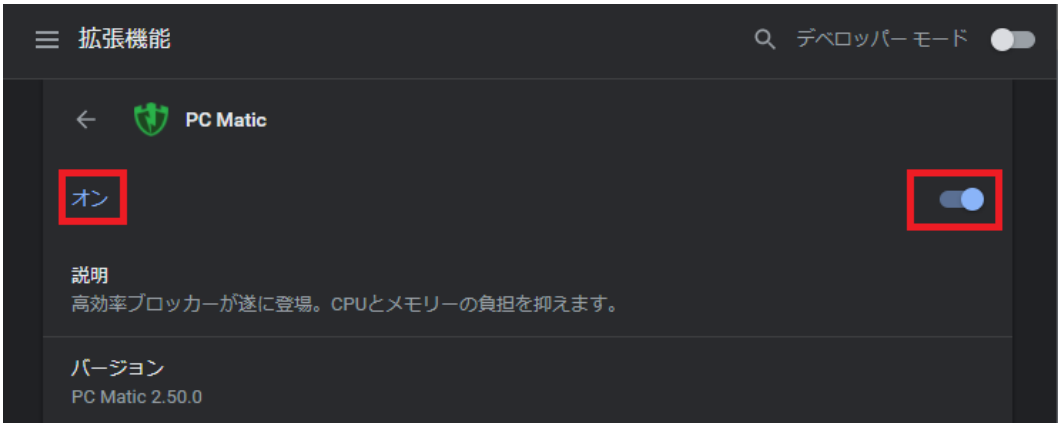


Chrome 導入済で機能がオフの場合

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。

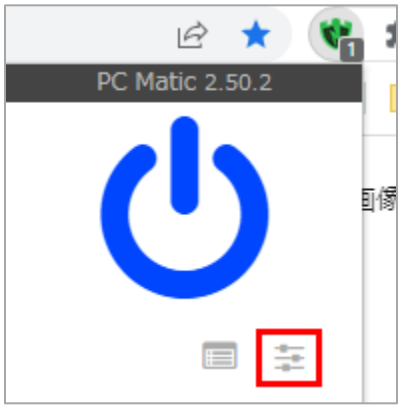
3. 開いた画面の上部にあるスライダーを「オン」にします。



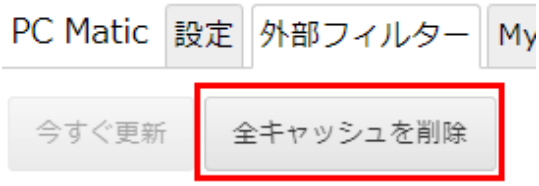
5.2 ブラウザー保護機能を有効にしているのに広告が表示される場合

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。

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



2. 「外部フィルター」タブにある「全キャッシュを削除」を押してください。



3. 「今すぐ更新」を押してください。この操作でフィルターの更新が完了しました。

6 管理ポータル

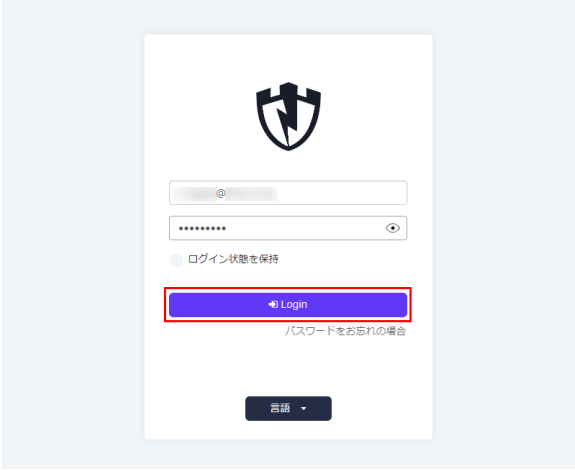
PC Matic は次世代エンドポイント保護製品であるため、本セキュリティクラウドサービスは、ブラウザーを利用して操作します。

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して頂く、または http://portal.pcmatic.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、インストーラーのダウンロード、ローカル・ホワイトリストの定義やアラートの確認、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。

6.1 ログイン

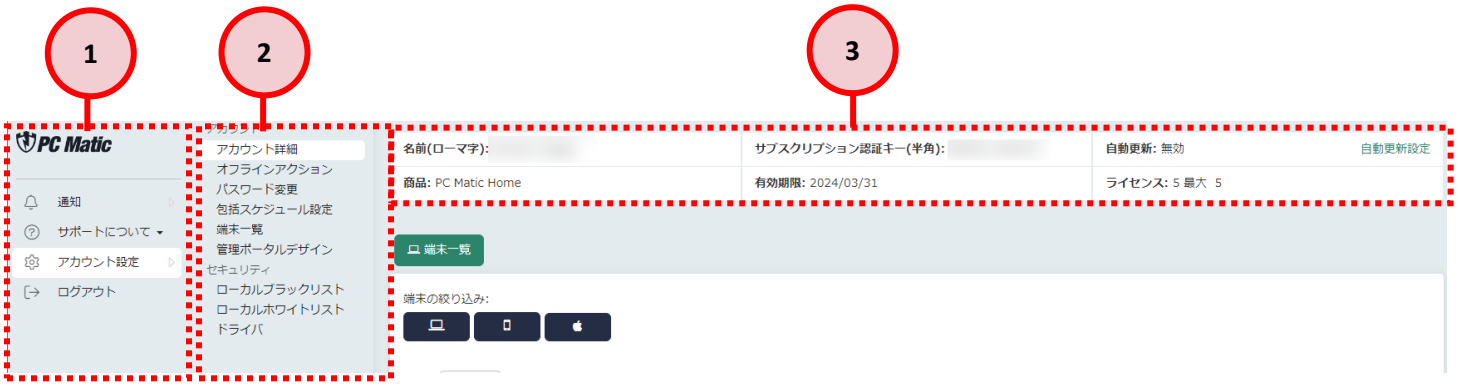
1. PC Matic でアカウントを作成した際の電子メールアドレス、パスワードを入力し、「ログイン」を押します。



6.2 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。

6.3 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。

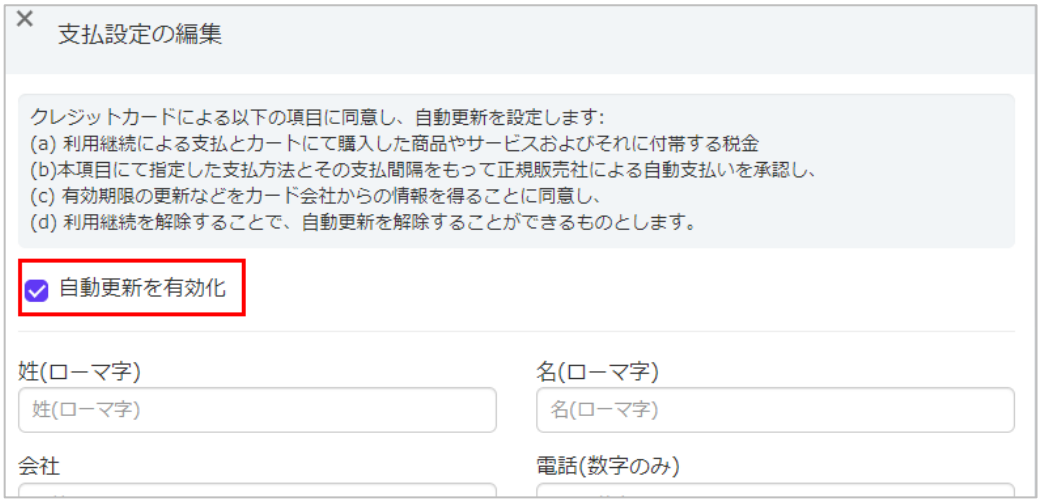
③ 利用者の名称や PC Matic の利用状況が確認できます。またここで自動カード払い設定を行う事ができます。

6.4 自動カード払い設定の解除

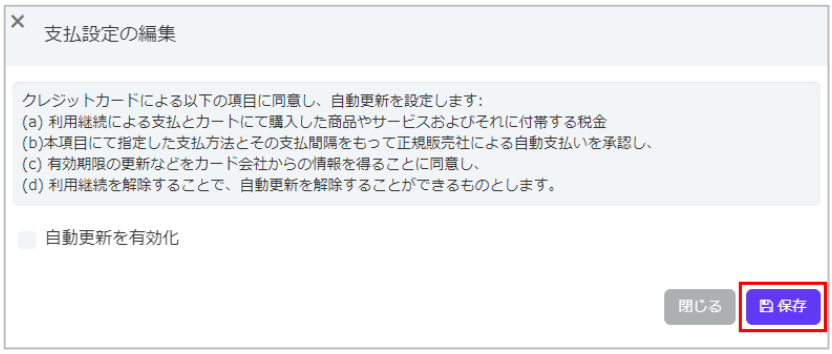
PC Matic を直営店でクレジットカード購入をされた場合は支払いが自動で更新されるようになっています。自動更新を解除する場合は以下の設定を行ってください。

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。



③ 「保存」を押します。



6.5 包括スケジューラの設定

包括スケジューラの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と、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。

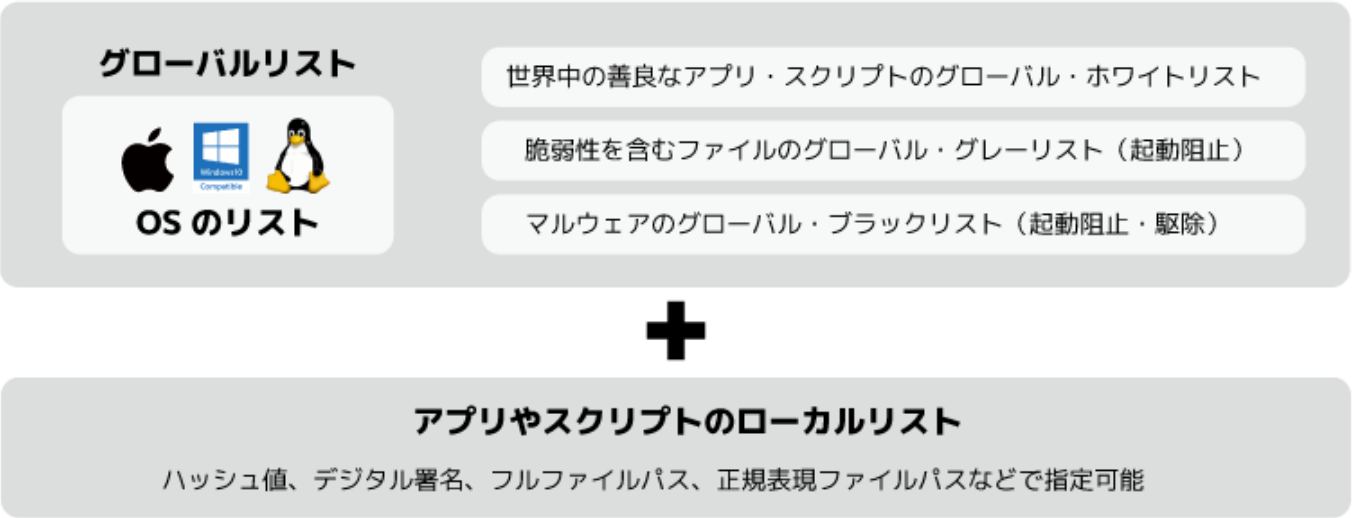
1. 管理画面でメニューの「アカウント設定」－「包括スケジューラ」を選択し、表示された画面の「Add スケジュール」を押します。

2. 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。

6.6 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り、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。

この機能は基本的に自ら開発したアプリケーションや著名ベンダー製品のみに活用し、フリーソフトなどの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。



1. 管理画面のメニューから「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。

6.7 アラートの確認

管理画面の「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。

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。

6.8 パソコン管理

ライセンスに登録されているパソコンが表示されます。ここでは各パソコンに表示されているアラートの確認や、枠の右上の削除ボタンを押すことでライセンスからパソコンを削除する事ができます。

6.9 スーパーシールド稼働ログからローカル・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」－「パソコン」タブを選択し、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。

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、追加したい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・ホワイトリストへの登録レベルを「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。

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。

「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。

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

7 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。

7.1 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。

2. 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

7.1.1 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

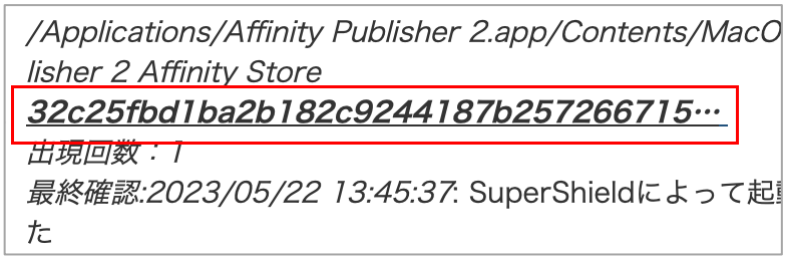
- パソコン利用者がインターネットに接続していない環境でファイルを実行させようとした
- このファイルを多く人がいま起動させ、マルウェア分析官が優先して分類した
- ファイアウォール装置などによりグローバルリストを端末がうまく受信できなかった

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。

7.1.2 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 SHA-256 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。

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。

7.1.3　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。

7.1.4　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。

7.1.5　ファイル名がスクリプト形式の調査方法

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。

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 繝VE 繧、繝ｫ繝我ｻ穂ｺ狗畑\讌ｽ螟ｩ\笆｡繧ｹ繝ｾ繝代・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。

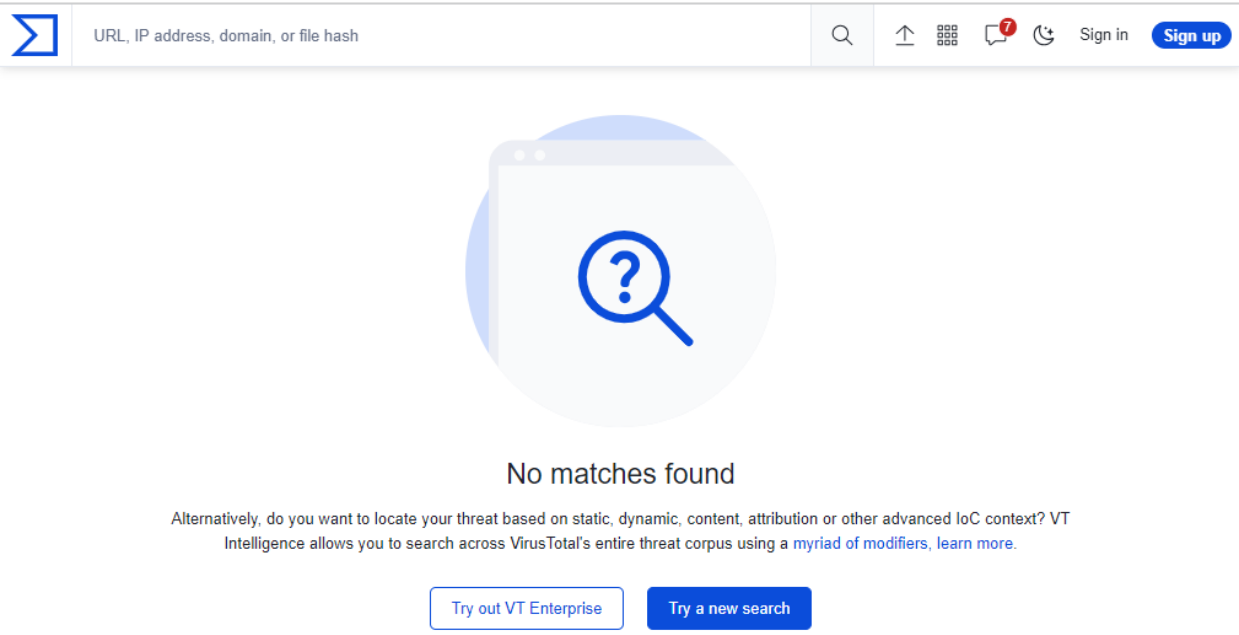
なお、スクリプトも PC Matic 社のマルウェア分析官によってデジタルフォレンジックが行われ、問題のないファイルであれば、グローバル・ホワイトリストへ追加され起動許可が与えられます。

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。

7.2 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。

7.2.1 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メモ帳などにコピー＆ペーストをしてメモしておきます。

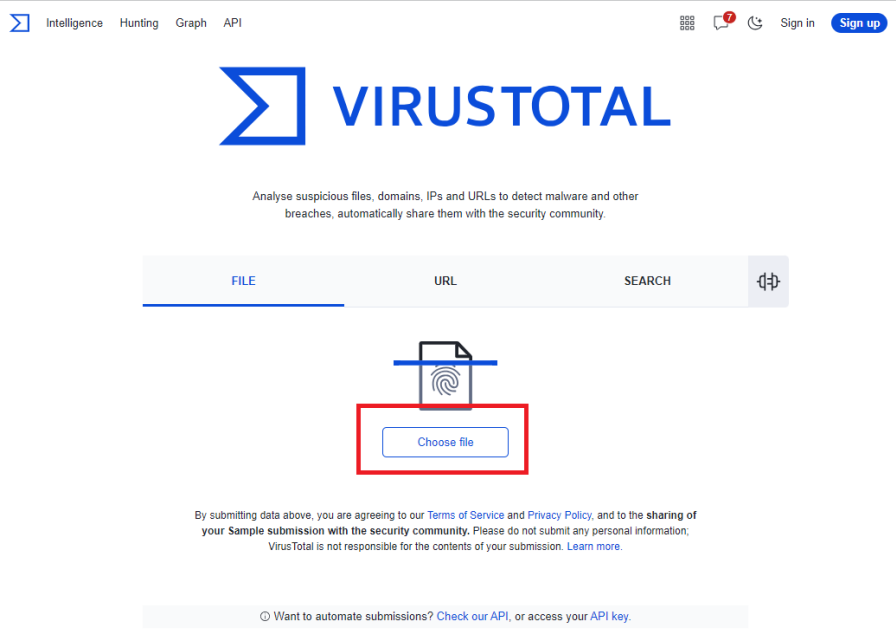
7.2.2 起動阻止されたファイルの探索

「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、Finder にてそのファイルを探します。

7.2.3 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

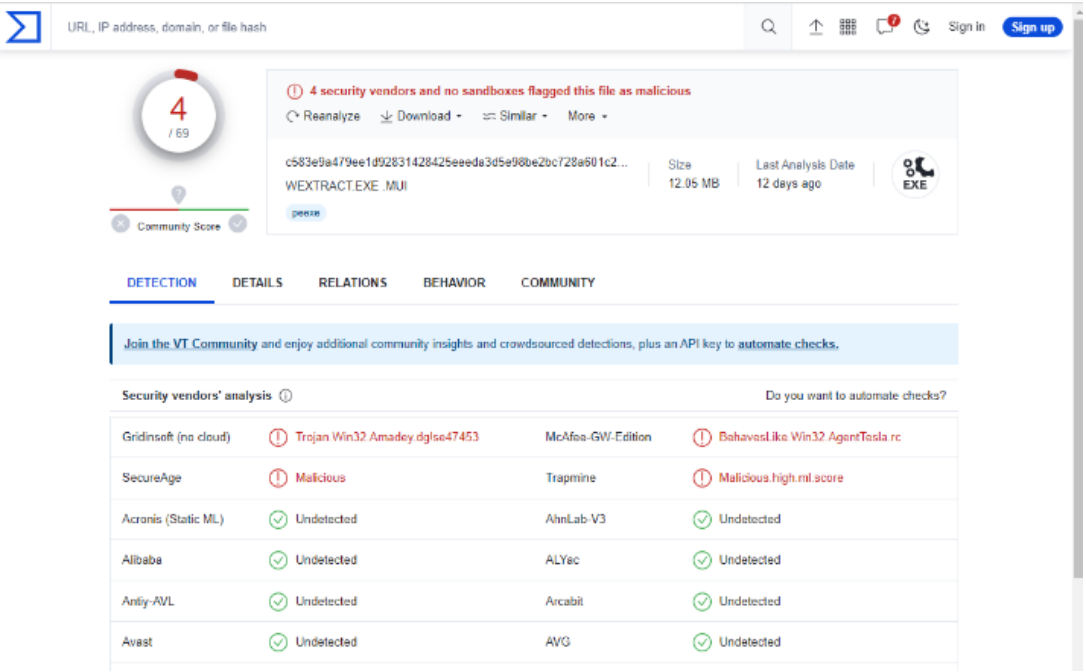
開いた画面の「Choose File」ボタンを押して起動阻止されたファイルをアップロードします。



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。



7.2.4 Behavior タブで素性や問題がないか確認

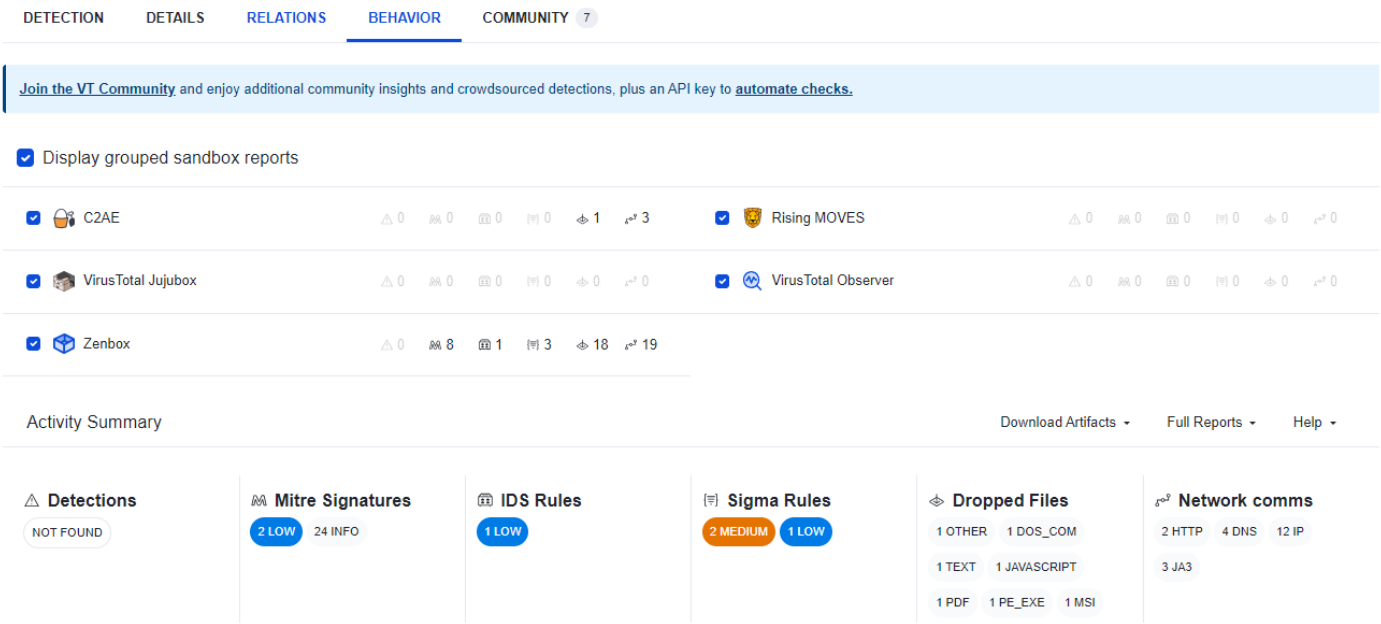
続いて「BEHAVIOR」タブをクリックして表示してください。

「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。



7.2.5 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 タ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	077a9997c4f3f95b80ff0d2b6e24ef87645b8a0747436722d1317d61df950057
?	?	file	23853ecd5459ff99d51b65e70e2b2848347ab5d26c3d9cd69073d69c8d4986d8
?	?	file	475b5c523f2661fc6633b9217613ff47839eaf9a689fed3ac27bfdc6e44f08b3
?	?	file	5fea85a1177a25b5c69ab4a0cad87e382dfc66eccbda2587ad69b41f026c55ed
?	?	file	8102e8f36020bc462853046a4bef51de3fb8f2bc3ed24d96e42ce397a6003ea0

7.2.6 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)がかなり過去である場合は、macOS では互換性の観点から稼働しない可能性が高いファイルです。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。

7.3 管理ポータル「通知」－「セキュリティ」から追加

7.3.1 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. ファイル名がスクリプト形式の場合は、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。

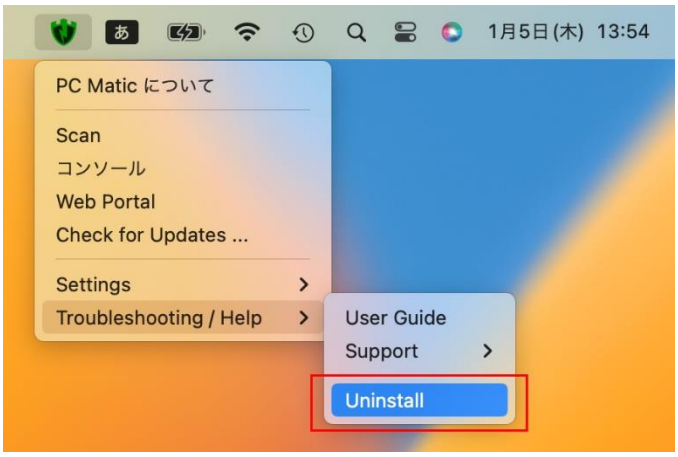
3. 起動阻止されたアプリケーションの「アクション」にある「操作」を押すと下のような画面が表示されます。

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。

8 アンインストール

PC Matic のアンインストール方法を記述します。

1. Mac のメニューバーに PC Matic の SuperShield アイコンをクリックして「Troubleshooting/help」－「Uninstall」を選択します。

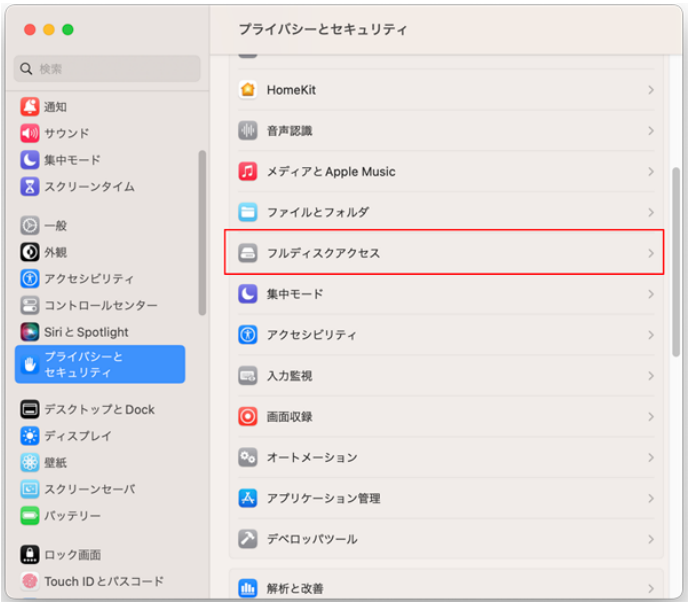


2. PC Matic のログインメールアドレス、パスワードを入力し、「アンインストール」を選択します。

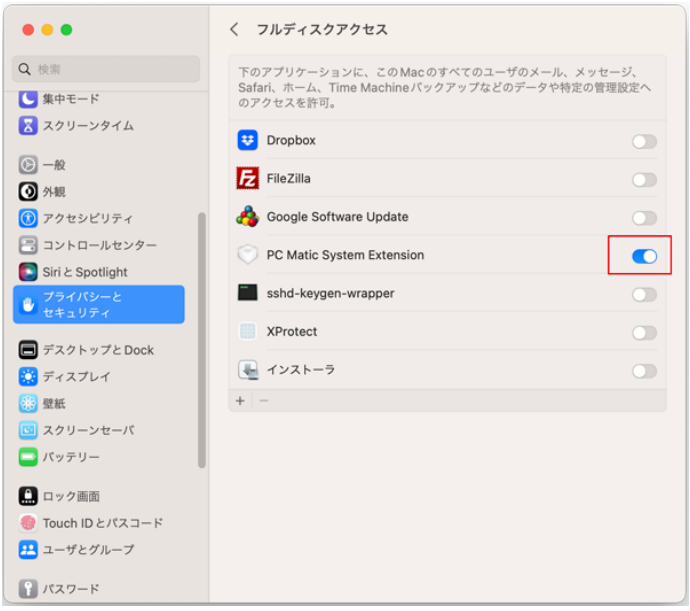
3. Mac にログインする際のユーザ名、パスワードを入力し「OK」を押します。

4. Mac のメニューバーから PC Matic がなくなったことを確認しつつ、数分待ちます。この間、バックグラウンドでアンインストール作業が実行されています。

5. macOS の「設定」-「プライバシーとセキュリティ」-「フルディスクアクセス」を選択します。



6. フルディスクアクセスから「PC Matic」がなくなった事を確認します。
なくなっていない場合は、「PC Matic」が出なくなるまで待ちます。
次に「PC Matic System Extension」を左にスライドして無効化します。



7. プライバシーとセキュリティの画面が表示されたら、Touch ID かパスコードを使用して許可を行ってください。

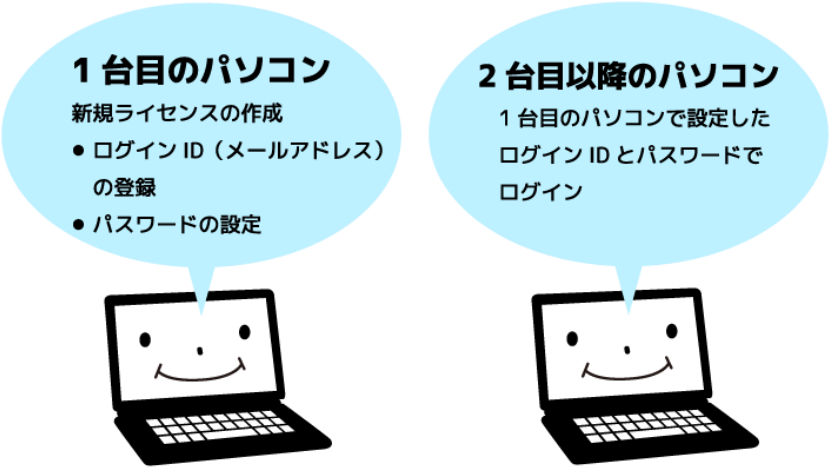
8. パソコンを再起動します。再起動すると「設定」-「プライバシーとセキュリティ」-「フルディスクアクセス」から「PC Matic System Extension」の表示がなくなります。
これでアンインストールは完了です。

9 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ありましたらご一読ください。

9.1 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

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。

9.2 ファイアー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 等のファイアー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 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 IP アドレス を利用しています。ポート番号は、80 と 443 です。以下は日本国内からアクセスする際のアドレスです。海外や衛星回線の場合は異なります。

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

9.3 ウイルス、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、以下を準ウイ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に持つ
- 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、ウイルスか、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変わりに、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。

【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