政府・軍基準を搭載した
新方式の統合型セキュリティスィート

法人版ユーザーガイド

第 104 版

PC Matic PRO

本書は法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 内容

2　はじめに

PC Matic 法人版は、「エンドポイント保護(EPP)」と「EDR」、「MDR 有人監視サービス」、「遠隔運用管理(RMM)」が統合したセキュリティスイート製品です。端末を強固に守りながら軽快に利用し続けられるようにパソコンメーカー出身者たちの手により、様々な斬新な設計がなされています。これはセキュリティ製品が社員の労働生産性を低下させてはいけないという、PC Matic, Inc.経営者たちの強い意志によるものです。

PC Matic 法人版は、クラウドサービスであるため、運用は管理ポータルを通じて行いいます。専用サーバーの導入は不要であり、初期費用はゼロで年間サブスクリプションライセンスのみで即座に導入できます。

様々なダッシュボードや、強力なレポート機能も特長のひとつです。セキュリティ状況、端末の状況(ディスク空容量、負荷状況)、端末の陳腐化状況などを定期的かつ自動的に配信する機能を実装しています。ウイルス感染や運用上の問題点などを管理者や利用者へメールで自動通知する機能もあり、必要に応じて柔軟な運用を行うことができます。

エンドポイント保護は、「ゼロトラスト・セキュリティモデル」に準拠した今までと異なるアプリケーション・ホワイトリスティング方式を用いています。

EDR はすべてクライアント・サーバモデルにて稼働しています。端末での全稼働プロセスは、すべてクラウド上に記録され、ログを削除することで証拠隠滅を図ろうとするサイバー攻撃を無力化し、感染調査を可能としました。端末状況のスナップショット記録はもちろん、組織内のどの端末がどのアプリケーションを起動したか、どのようなスクリプトファイルが実行されたかを日時と共に 3 か月間クラウド上に記録し閲覧できます。感染など異常時には、専門家の力を借りずにクリック数回で活動記録を閲覧することができます。

MDR 監視サービスは、FBI サイバー捜査官を務めた人物などを中心に、365 日 24 時間無休で全顧客を監視し、異常が検出された際には顧客へ即座に通知を行い、不正なプロセスを停止させます。

遠隔運用管理(RMM)では、ハードウェア・ソフトウェア資産管理はもちろんのこと、遠隔の端末に対し、独自のゼロタッチ・リモートデスクトップ機能、ファイルマネージャー、コマンドプロンプト、再起動など豊富な運用ツールをご利用頂けます。

こうした多くの機能を実装した PC Matic PRO ですが、操作は日本的な直感による操作が可能なユーザインターフェースを採用しています。スライダーによる「オン/オフ」やグラフなどにマウスオーバーするだけで詳細な数値が表示されるなど、お客様からの改善要望を積極的に取り入れ、機能追加や使い勝手を日々向上させています。

PC Matic 法人版の最大の特長は、エンドポイント保護の方式です。アプリケーション・ホワイトリスティング方式というゼロトラスト・セキュリティモデルの中核をなす NIST SP 800-167 を更に厳格に運用方法で、数年間に渡り全顧客にマルウェア感染実績を出さずに提供を続けています。

2022 年は 1620 億個のマルウェアが全世界でばら撒かれました。これは、全世界の人が利用する様々な有功なアプリケーション数を大きく上回っています。そのうち 1.5 億個は新たなワクチンが必要な新種マルウェアでした。このような時代がやってくるのではないかと 2010 年頃より PC Matic 経営陣は予測し、「OS のもつ API をすべてロックし、私たちがデジタルフォレンジックを実施した上で、有効なアプリケーションやスクリプトのみ活動できるようにしてはどうか」という従来の「悪質なアプリケーションやスクリプトを学習させマルウェアを補足する」と逆のアプローチで開発を進め、様々な国際特許を取得致しました。

この方式の違いを分かりやすく比喩表現すると、アプリケーション・ホワイトリスティング方式は、身元確認を事前に行った上で軍事基地のセキュリティクリアランスが必要な特別施設へ入館が許可される「事前入館許可制」のような仕組みです。アポなしで施設に入れないのと同様です。

従来の仕組みは、新型コロナウイルスのように新種には誰かが感染してしまうものの、そのウイルスを調査してワクチンを全顧客に配布することで他の顧客を守るという仕組みです。このため新種や亜種には感染を許してしまいます。AV-TEST や家電量販店でのキャッチコピーで「100%守れる」と謳っていることがありますが、これは完全なる錯誤であり誇大広告です。実際には毎日非常に多くの顧客が感染しており、その顧客からの情報のおかげで他顧客を守れているのです。しかし、この仕組みは、年間 1620 億個がばら撒かれている現状からも推測できるように，既に崩壊しているのです。

このような背景から、アメリカ国防総省(DoD)および政府機関のセキュリティを管掌している国土安全保障省(DHS)が主導して「国家(軍)が関与し高度化するサイバー攻撃」「端末を遅くさせず業務効率を悪化させない」ことを目標に、商務省(DoC)管轄の NIST(米国国立標準技術研究所/日本の JIS に相当)にて民間企業２０社ほどが参加し検討委員会で策定が進められています。PC Matic, Inc.はその構成企業の一社です。

ゼロトラスト・セキュリティモデルは、2020 年頃にドラフト版を定め、現在も広く国民から意見を募集しています。

PC Matic のエンドポイント保護(EPP)は、OS のすべての API をデフォルト拒否設定しています。実行ファイルのハッシュ値などにより起動の是非をサーバー参照し、許可されている場合のみ実行されます。

これにより、ゼロデイ攻撃や N デイ攻撃を受けてもデフォルト拒否で完全ロックされているため、PowerShell スクリプトなどの内部コマンドを用いたものや DLL サイドローディングなど従来のセキュリティソフトによって防御が困難なマルウェアでも、デフォルト拒否により実行が許可されません。

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。

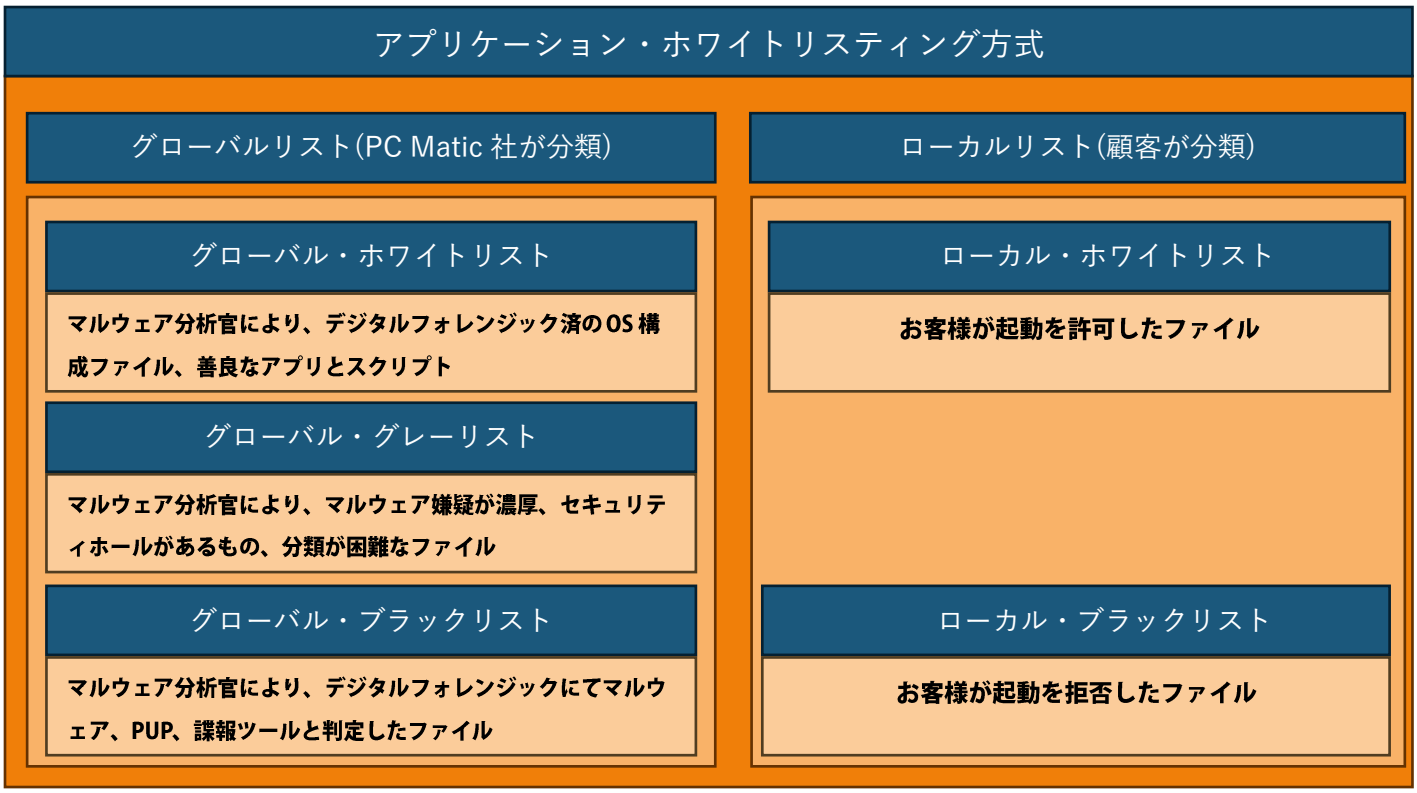
昔からあるホワイトリスト方式は、いわゆるローカルリストのみで、システム管理者がホワイトリストを作成しない限り、アプリケーションの実行が許可されませんでした。しかし、それでは膨大にある社内利用アプリケーションが更新するたびにリストを再生成して配布するという膨大な手間が必要でした。

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が、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」「デジタル署名」で指定することができます。



PC Matic PRO はお客様と共に作り上げていくセキュリティスイート。これさえあれば、端末のセキュリティと運用管理はすべて満足のいくレベルになり、様々な報告書も楽々。これが PC Matic PRO が描いている製品像です。

2.1　PC Matic Pro とは

PC Matic PRO はセキュリティ保護方式として、従来アーキテクチャの延長線上にあるブラックリスト保護方式とは全く異なる、アプリケーション・ホワイトリスティング方式を採用しているのが一番の特長です。

英語:Application Allowlisting)は、NIST SP 800-167 で規定されたゼロトラスト・セキュリティモデルに基づき、指定した信頼できる実行ファイルを指定した許可リストあるファイルのみ実行可能とした方式です。それ以外のファイルはすべて実行拒否されるため指定外のマルウェアなどは一切実行することができません。

この方式は、アメリカ国防総省、国土安全保障省、商務省、FBI と、PC Matic 社を含む民間企業 24 社が中心となり、対サイバー攻撃能力に優れる次世代のセキュリティガイドライン策定している、ゼロトラスト・セキュリティモデルとして作成されたマルウェアなどに影響されないエンドポイント保護の仕組みです。

同方式の基本モデルでは、利用者が作成した「許可リスト」(ホワイトリスト)に指定したファイルのみ実行可能としていますが、許可リスト作成の手間がかかるため、PC Matic は元 FBI サイバー捜査部門に長年従事した分析官を始めとした分析チームが AI を助手として活用し、複数のマルウェア専門分析官による検査経て、ひとつずつ善良なアプリケーションを指定。これをグローバル・ホワイトリストとして全顧客に提供。世界中で利用される善良なアプリケーションの 99%を網羅する許可リストを用意しています。

このグローバル・ホワイトリストによりホワイトリスト方式でありながら、従来のブラックリスト方式の製品と同じ使い勝手で、マルウェアによる影響を一切排除することに成功しました。

もちろん、従来のような厳格に利用可能なアプリケーションを限定させるローカル・ホワイトリスト保護モードも有しています。この保護モードでも、OS が更新される度にホワイトリストを再作成する手間から解放されることはもちろん、起動許可や禁止も管理者がクリックひとつで制御することができます。ホワイトリストの差し替えは不要で運用の利便性を大きく高めています。

同方式を 2016 年に提供開始して以来、全顧客にマルウェア・ランサムウェアによる感染を与えていません。アメリカ連邦政府調達認証 FedRAMP に登録された製品です。日本でも社会基盤企業での採用はもちろん、個人版は 2010 年から市販され、2016 年からは日本のパソコンメーカー様の購入時付帯品として採用されています。

PC Matic PRO は、会社のパソコンを 1 か所から遠隔管理し、保護するためのものです。各端末に操作ソフトはなく、IT 管理者が専用管理コンソールを利用し、端末をフル制御できるようになっています。

PC Matic PRO は、下記で構成されています。

- EPP(SuperShield)でのアプリケーション・ホワイトリスティング方式を使用したリアルタイムマルウェア保護
  - SuperShield 保護が、標的型攻撃をも対処し強固に端末を保護
  - ファイルレスマルウェアへ対応
  - EDR アプリケーション稼働ログをクラウド上に記録。問題発生時の調査が可能
  - EDR を統合し、管理者が社内で不審なアプリケーションの起動がないか包括的に管理することが可能
- ブラウザー保護機能
  - Google Chrome (Windows, macOS)、Edge、Firefox (Windows)の拡張機能として提供
  - EPP と併用することでブラウザーからのマルウェア侵入を多段に防御
  - 不必要な広告バナーを非表示とすることでモバイル環境にて回線負荷を低減。業務効率が向上
- 各端末を定期的にスキャンし最適化を実施
  - スキャン間隔を 1 回、毎日、毎週、または毎月などで、スケジュール設定可能。
    スキャンにより、パソコンに関する問題点の診断・把握と修正が行えます。稼働中のプロセス、サービス、ドライバーなどのスナップショットを取得
    また、電子メールアドレスを設定しておくと、スキャン完了後にレポートを受信可能
- 遠隔運用管理機能を統合
  - 独自リモートデスクトップ機能搭載。VNC をベースに暗号キーなどの仕組みを改修し、セキュリティ性能を高めた独自の通信情報で制御を実施
  - 遠隔ファイルマネージャで、管理端末内のファイルを送受信可能
  - コマンドプロンプトにより、遠隔端末内のアプリケーション削除・導入を始め、あらゆることが可能
  - Windows PRO 版以上に標準搭載される Windows RDP を詳細に制御可能

2.2 注意:Syslog, HCL BigFix, ローカル・ホワイトリスト限定保護モード

以下の拡張機能は標準にて管理ポータルに現れてきません。ご利用の際はサポートまでご連絡ください。

●SYSLOG 送信

TCP/UDP 514 (RFC 3164)などを用いて端末の syslog を特定のサーバーへ送信することができます。

●HCL BigFix 連携

BigFix 端末へ Fixlets を用いてデプロイができ、BigFix と連携を行うことでエンドポイント管理の範囲が大きく拡張されます。

●ローカル・ホワイトリスト限定保護モード

1 億件以上の善良と分類済のアプリケーションリストがグローバルリストとして顧客が利用できることで、従来のブラックリスト方式のエンドポイント保護製品と遜色ない運用の手軽さを提供しつつも NIST SP 800-167 に準拠したゼロトラストの強固さを実現しています。しかし、業務上必要なアプリケーションやスクリプト以外は、一切端末で実行させることのできない、より強固な運用方式を求め

る方のために、OS を構成するファイルのみ利用するローカル・ホワイトリスト限定保護モードを 3 種類用意しております。OS を構成するファイルを提供することで、OS の定期アップデートの際のホワイトリスト作成の手間から解放されます。

●インストール時の通信帯域は 64Kbps 以上必要

プロキシサーバー方式による通信ロギングにより通信速度が低下している場合および、マルウェア感染対策として LAN から WAN への通信帯域を絞っている場合、インストール時は通信帯域として 64Kbps 以上確保してください。推奨値は 1Mbps 以上です。インストーラーは必要なプログラムのダウンローダーでしかないため、インストールの際は、インターネット回線を通じて PC Matic サーバーから動作に必要な最新のプログラムを自動取得して実行されます。また動作に必要な端末情報を取得するなどして多くの通信帯域を必要とします。

2.3 スキャン項目

- ディスク最適化：完全または部分的な最適化を選択します（SSD ドライブはデフラグを行いません。）
- マルウェアスキャン（クイック、フルを選択）：マルウェア（ウイルス）および/または PUA（迷惑なアプリケーション）を除去するように選択します。
- ベンチマーク：他のすべての端末に対するプロセッサー速度、メモリ速度、およびディスク速度をベンチマークし、ワールドランクを算出します。これは、世界中の PC Matic 利用者との比較で、パソコンの買い替え時期などの参考となります。
- ドライバー：必要に応じてドライバーを最新バージョンに強制更新します。
- 脆弱なアプリケーション自動更新：プログラムのセキュリティを維持するために、約 30 個のサードパーティアプリケーションを強制的に更新し、最新のバージョンに保つようにします。（Java、Adobe、iTunes、Skype など）
- Windows のシステム復元ポイントを縮小：Windows のシステム復元ポイントのうち、かなり古い不要な復元ポイントを削除します。
- 不必要なファイルを削除：ごみ箱と一時ファイルをクリーンアップします。
- レジストリの修正：レジストリ内の不必要なエントリを削除します。
- インターネット設定：レジストリ設定を変更して、インターネット応答速度を向上させ、セキュリティを強化します。
- パフォーマンスの微調整：Windows の稼働がスムーズになるように Windows の設定を調整します（例：スタートメニューでアニメーションを削除など）。
- サービス：不要と思われるサービスの自動起動を停止します。
- スケジュールされたタスク：不要と思われるスケジュールタスクをオフにします。
- スタートアッププログラム：必要がないスタートアッププログラムをオフにします。

2.4 脆弱性対策

PC Matic Pro はでは悪意のある者から狙われやすく、利用者が多いアプリケーションを自動更新し、セキュリティホールを塞ぐことでアタック・サーフェス(攻撃対象領域)を極小化します。利用者は脆弱性情報（セキュリティ上の欠陥の情報）を定期的に確認したり、悪意ある攻撃を心配する必要から開放されます(NIST SP 800-40 準拠)。また、ディスプレイ、ネットワーク等のドライバー類も自動的に更新します。これらの著名アプリケーションは必要に応じて追加されます。

1. 7-Zip
2. Adobe AIR
3. Adobe Flash Player ActiveX
4. Adobe Flash Player Plugin
5. Adobe Flash Player PPAPI
6. Adobe Reader
7. Adobe Reader MUI
8. Adobe Reader XI
9. Adobe Shockwave
10. FileZilla
11. Foxit Reader
12. Google Chrome
13. iTunes
14. Java 32
15. Java 64
16. Microsoft Exchange Server 2013
17. Microsoft Exchange Server 2016
18. Microsoft Exchange Server 2019
19. Mozilla Firefox
20. Mozilla SeaMonkey
21. Mozilla Thunderbird
22. OpenOffice
23. Opera
24. PDF Creator
25. PDF XChange Viewer
26. QuickTime
27. Real Player
28. Safari
29. Skype
30. VLC Media Player
31. Winamp
32. WinRAR
33. WinRAR5.X
34. WireShark

これらアプリケーションの個々の更新可否やバージョンアップさせずに固定させる制御は、「アカウント設定」-「脆弱性適用」にて包括的に指定できます。

2.5 管理ポータルへのアクセス

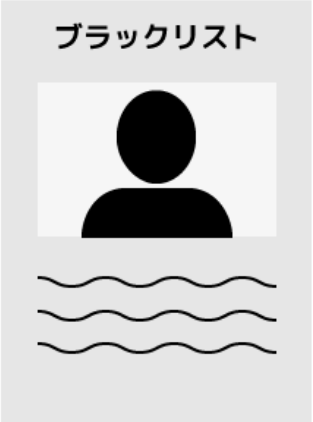
https://portal.pcmatic.com の管理ポータルにアクセスし、パソコンやスマートフォンでいつでも PC Matic で管理している情報をどこでもご覧頂けます。

なお、管理ポータルはフル HD 画質で表示して操作を行ってください。

2.6　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を採用しています。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を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。

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。



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	

3　アカウントの作成とインストール

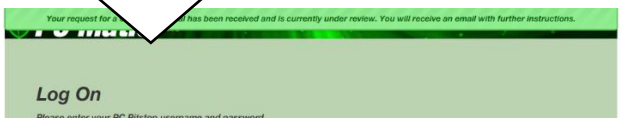
まずアカウントを作成し、その後 PC Matic PRO を設定したいパソコンに PC Matic PRO をインストールします。

3.1　アカウントの作成

1. https://pcmatic.jp/pro/　にアクセスし、「お問い合わせ」からサポートに連絡をします。

2. サポートより通知されたリンクをクリックし、必要事項を記載しパスワード等をフォームに入力し、「利用を申請します」を押します。なお、こちらで入力したメールアドレスに請求書が毎月自動的に送信されます。

ご利用開始月は無料というメッセージと、登録したメールアドレスにメールが送られたという旨のメッセージが表示されます。



3. サポートへアカウント作成が完了した旨および、検証に利用したい台数を連絡します。

※ご利用開始月無料には利用可能台数に制限はありませんので、必要台数をサポートまでご連絡ください。

3.2 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。

3.3 部署の作成

作成したアカウントにログインし、部署を作成します。

1. https://portal.pcmatic.com/ にアクセスします。
2. 登録したメールアドレスと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。

3. ログインしましたら、左側のメニューから「アカウント設定」を選択し、表示されたメニューから「グループ編集」を選択します。

4. 部署を登録します。部署名を入力して「追加」を押してください。登録が終わりましたら「閉じる」を押します。

3.4 インストールの前に

3.4.1 ファイアウォール装置の IPS 機能への除外設定、他社エンドポイント保護(EPP)と併用の場合

事前にファイアウォール装置の IPS へ PC Matic サーバーへの IP アドレス除外指定を

ファイアウォール装置の IPS による通信パケット破棄防止のため、以下をホワイト IP アドレスとして除外指定ください。NAT ルーター、Proxy サーバー、家庭用ルーターでは基本的に除外設定の必要はありません。Cloudflare 社による CDN を利用しており、日本以外では IP アドレスは異なります。他社 EPP, EDR 製品同様、PC Matic サーバー側の IP アドレスをファイアウォール装置の IPS にて破棄されないよう、除外指定する必要があります。最近の IPS には、SSL 監査機能(SSL inspection)が実装されています。このため、ファイアウォール装置を利用している場合は、エンドポイントをインストールする前に、ファイアウォール装置へ指定された IP アドレスもしくは、FQDN を除外指定する必要があります。

ヤマハ製 VPS ルーターも、IPS 類似機能もっているモデルがあるため、解除指定が必要です。

ASUS 製など家庭用 Wi-Fi ルーターには、トレンドマイクロ社の「for Home Network」「Trend Micro Smart Home Network」「AiProtection」と呼ばれる IPS 機能が通信を阻害することが確認されていますので、これらの機能を無効化してからエンドポイントのインストールを行ってください。

なお、IP アドレスは、CDN を利用している関係から、国により異なるため、日本以外の国で利用する際は、ping などで FQDN から IP アドレスを確認ください。

PC Matic にて利用される IP アドレスに関する説明はこちら

事前に他社製エンドポイント保護(EPP)へ PC Matic のファイルや通信先の除外指定を

他社製エンドポイント保護(EPP)と併用される際は、PC Matic エージェントをインストールする前に必ず PC Matic のファイルを除外指定してください。指定しない場合は、PC Matic のエンドポイント保護機能が正常に導入されず、またアンインストールがうまくできない事象も確認されています。

TrendMicro APEX ONE など、ファイルだけでなく通信先も除外指定する必要がある製品もあります。通信先の除外指定設定があるソリューションである場合は、通信先の除外指定も併せて行ってください。

他社エンドポイント保護と併用する場合の説明はこちら

過去のすべての OS セキュリティアップート(Windows update)を適用

PC Matic PRO は、.NET Framework にパッチが適用された状態や最新の暗号アルゴリズムなど Microsoft など OS ベンダーが提供しているパッチが適用された状態での稼働にあわせてプログラムを提供しています。パッチが適用されていない状態では、インストールに失敗したり、正常に稼働しないことがあります。セキュリティソフトは、OS がもつ全ての API をフックします。そのためレジストリクリーナーによって破損している OS や不具合修正のための OS アップデートが適用されていない環境では正常に稼働しないことがあります。

3.4.2　リファレンス機の準備・ローカル・ホワイトリスト作成

PC Matic は、アプリケーション・ホワイトリスティング方式を採用しており、世界中の PC Matic 利用者にて善良なアプリケーション情報であるグローバル・ホワイトリストを顧客同士で共有しています。広く利用されているアプリケーションに関するプログラムは既にグローバル・ホワイトリストに追加されているため、お客様がローカル・ホワイトリストに追加していただく必要はございませんが、自社開発した業務系アプリケーションは、事前のクラウド監査が終了していないため、PC Matic の監査サーバーへ情報を投げ、マルウェア分析官による判定を経て善良であると判断させる必要があります。自社開発アプリケーションに深刻な脆弱性が発見された場合は、unknown(未知)や bad(悪質)と判定されることがあります。開発にあって気をつけて頂くポイントは別途以下の URL をご参照ください。

https://pcmatic.jp/faq/supershield/22/

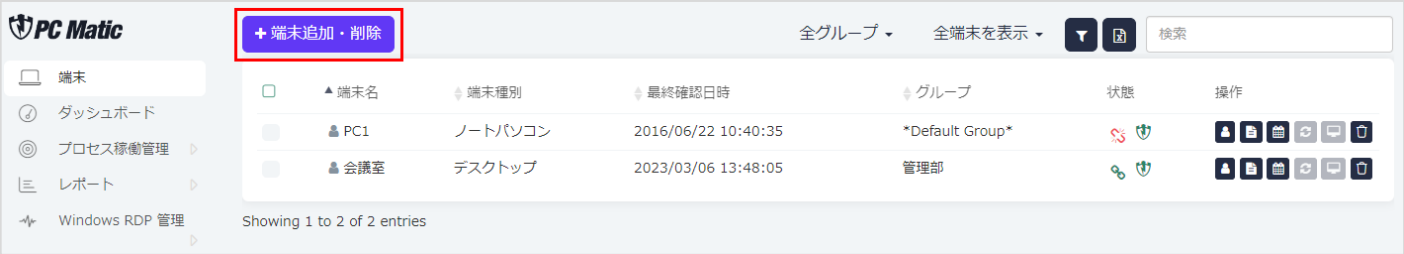
PC Matic を利用するには、各部署(営業・管理・開発など)で標準としているソフトウェア構成のパソコンを社内導入する数日前に**リファレンス機**として予備機などを用いて、事前に導入パソコンにおけるアプリケーションが善良・悪質を PC Matic のサーバーに識別させておく必要があります。

実運用中のパソコンにいきなり導入してもかまいませんが、世界中の PC Matic 利用者がまだ遭遇したことのない、未知のアプリケーションが発見された場合は、一般的には 15 分、最長では監査が終了するまで 24 時間をお待ちいただくことになります。このため業務効率が悪くなりますので、リファレンス機を用いて業務上必要なアプリケーションが起動可能な状態であるかを PC Matic のクラウドサーバへ識別させておいてください。

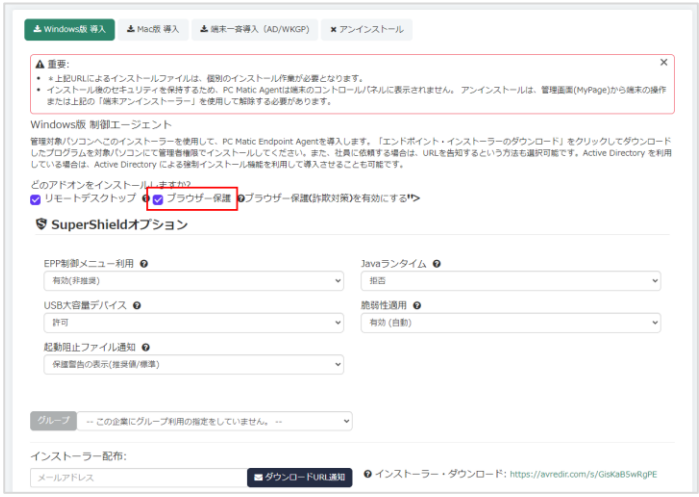
リファレンス機の作成・社内導入までの流れは次のようになります。

1. 既存セキュリティソフトをアンインストールします。
2. https://portal.pcmatic.com/　にアクセスし、管理ポータルにログインします。
3. メインメニューの「SWAM ファイルレーダー」(SWAM: Software Asset Management Dashboard)を選択します。右上にあるスライダーをクリックして右に動かし「緑色」にさせ有効化してください。

4. 自社専用 PC Matic をリファレンス機にインストールします。「端末」を選択し、表示された画面の「端末追加・削除」を押します。



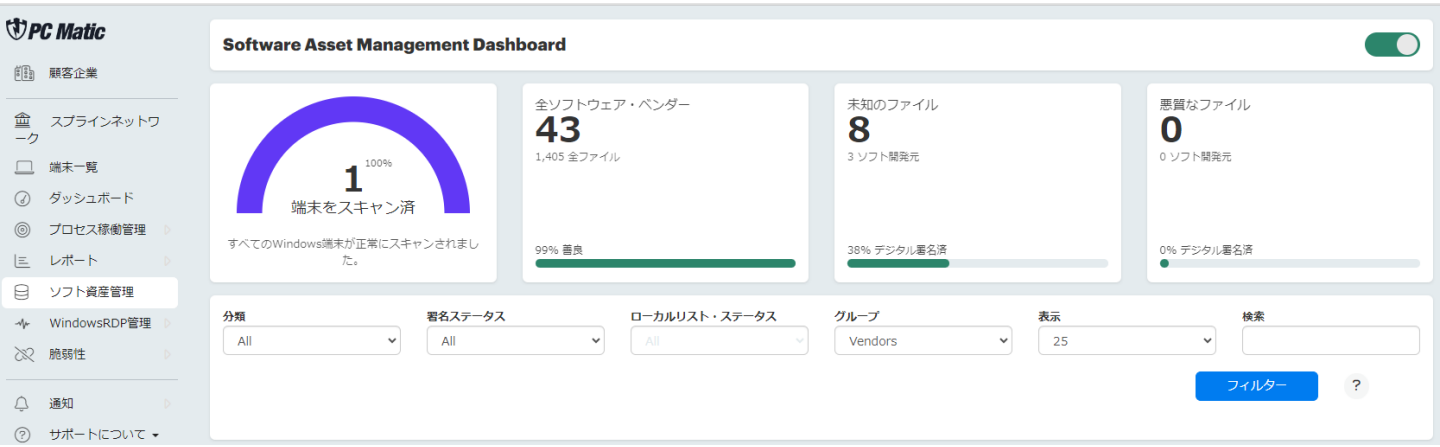
5. リファレンス機にインストールする場合は、「ブラウザー保護」をチェックし、他はデフォルトのまま変更せずに、右下にある URL をクリックして、インストーラーのダウンロードを行ってください。「Microsoft Defender」の項目は「有効化」をお勧めします。「無効化」にすると『Windows セキュリティ』の『ウイルスと脅威の防止』にて、PC Matic SuperShield が保護セキュリティエンジンとして識別されます。有効化にすると Microsoft Defender 等と他社法人版セキュリティエンジンと二重保護モードとなります。



6. リファレンス機にダウンロードしたインストーラーを実行しインストールを完了します。インストール完了後も電源を入れたままにしてください。

7. 「端末一覧」にやがて導入した端末が表示され、「状態」の箇所のアイコンが黄色で表示されます。黄色の状態は、PC Matic の稼働に必要なアプリケーションが PC Matic のサーバー側よりダウンロードされ残りのインストールがバックグラウンドにて実行中であることを表しています。

8. 1 時間ほど経過して SWAM のための初期診断が完了したら、メインメニューの「SWAM ファイルレーダー」(SWAM: Software Asset Management Dashboard)を選択します。SWAM 初期診断が完了した端末の数が表示されているはずです。



3.4.3　運用モードの決定:グローバル・ホワイトリスト保護モード、ローカル・ホワイトリスト保護モード

PC Matic マルウェア分析官によるゼロトラスト・セキュリティモデルに準拠した最終的な判定によって善良と判断されたアプリケーションを利用し、従来のブラックリスト方式のような運用の容易性を実現するグローバル・ホワイトリスト保護モードと、指定したアプリケーション以外は一切に利用しないローカル・ホワイトリスト保護モードが利用できます。

法人版は、グローバル・ホワイトリスト及びローカル・ホワイトリストの利用レベルを変更することでき、より厳格なホワイト運用が可能です。３つのローカル・ホワイトリスト運用による保護モードは、グローバル・ホワイトリストのうち OS 構成ファイル以外のホワイトリストを利用しない保護モードとなります。起動可能なファイルを限定することで、攻撃面を極小化することができ、サイバー攻撃に対する耐性をより高めることができます。全ての保護モードはホワイト運用であるため、OS のもつ全機能を標準でロックし、未知のサイバー攻撃や脆弱性への耐性が強固になります。

【PC Matic のローカル・ホワイトリスト運用モードの特長】
ローカル・ホワイトリスト運用モードのうち『適用』と『標準』は、マルウェア分析官により善良と判定された OS 構成ファイルの更新情報(OS に関連したグローバル・ホワイトリスト)を利用でき、その手間から解放されます。USB メモリに入れたホワイトリストファイルを端末へ適用する手間から完全に解放されます。

【利用推奨シーン】
産業機械の制御用コンピューター、デジタルサイネージ、POS レジ、インフラ企業等の高い脅威耐性が必要なシステムなど

【保護モード設定レベル】
保護モードの変更は「SuperShield オプション」メニューより、「端末」「グループ」「顧客企業」レベルにて設定して頂けます。

【本機能の背景】
最近は、セキュリティ企業が善良と認定済の比較的利用者が多いアプリケーションの脆弱性や汎用性を悪用し、マルウェアとして実行させるケースが急増してきています。これに対処するには、世の中で善良は判定されているアプリケーションであっても、組織内で利用させないことで、リスクを大幅に低減もしくは撤廃させることができます。

グローバル・ホワイトリスト保護モードで運用される方は、SWAM: Software Asset Management Dashboard の画面にて「未知のファイル」と表示されている箇所がゼロでない場合は、「分類」で「Unknown」をグループで「Files」を選択し、「ローカルリスト・ステータス」で「Not on Allowlist」を押してから「フィルター」を押します。ゼロである場合は特にアクションは必要ありません。

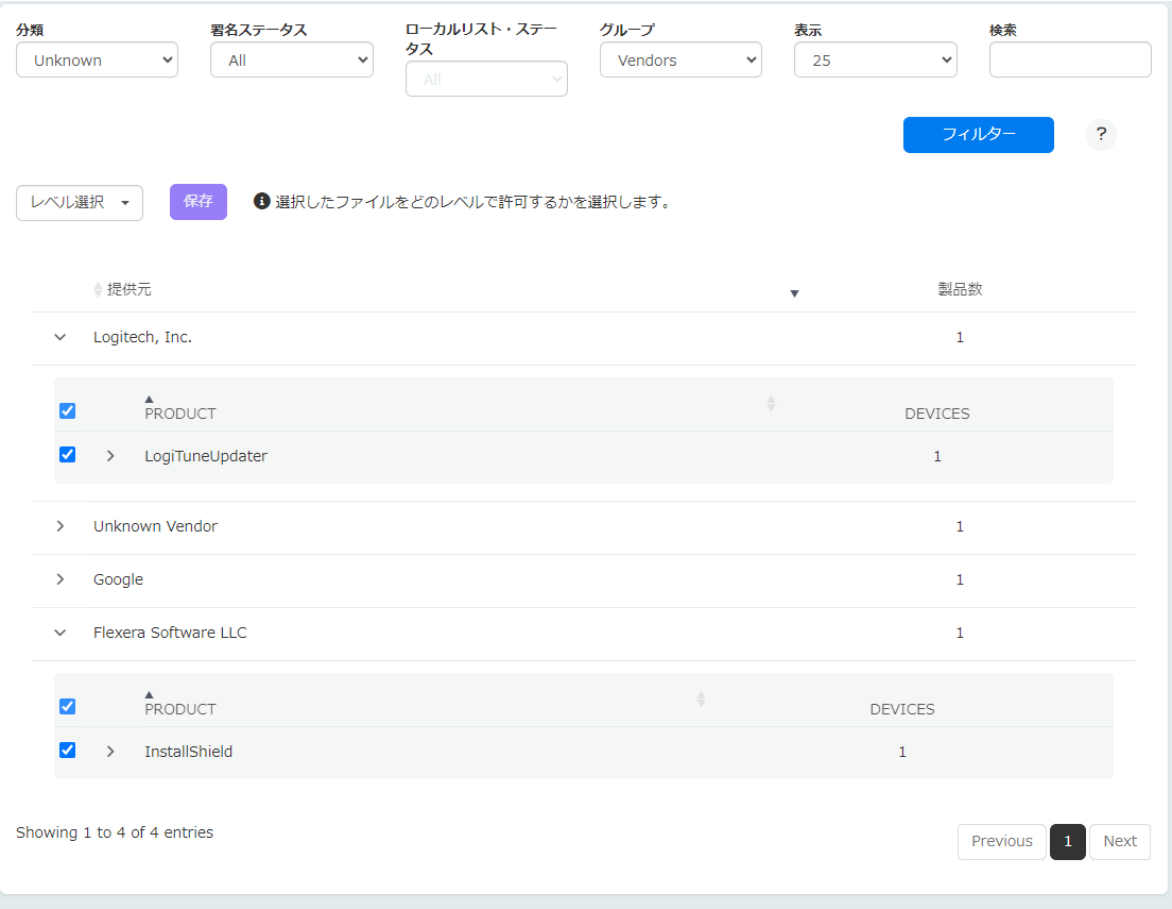
ローカル・ホワイトリスト保護モードで運用される方は、悪質なファイルがゼロであることを確認の上で、「分類」で「all」を選択して「フィルター」を押します。

3.4.4　ローカル・ホワイトリストへの追加

フィルターにて表示された開発元名からプルダウン展開するとアプリケーション名が表示されます。ファイル名の左横にある□にチェックをいれるとローカル・ホワイトリストへ追加選択が行えます。業務上必要なアプリケーションを全て選択していきます。

レベルの選択を展開し、どの組織レベルで該当アプリケーションを利用可能とするか選択します。アカウント作成時の初期段階では端末のみの指定で結構です。後程、ローカル・ホワイトリストの管理画面よりレベルを変更して頂けます。
レベルを選択し、「保存」を押すと、ローカル・ホワイトリストへ追加されます。

PC Matic マルウェア分析官により、まだ未判定を表す「UNKNOWN」である場合は、表示されているファイルを更に開くと「HASH」が表示されます。このハッシュ値をクリックすると VirusTotal に飛びます。善悪の判定を VirusTotal によって分析を行います。詳細は後述の「Unknown となっている場合」をご参照ください。



3.5　システム本稼働後、起動阻止されたファイルの扱い方

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。

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。

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ためローカル・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 Categorization 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

3.5.1 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

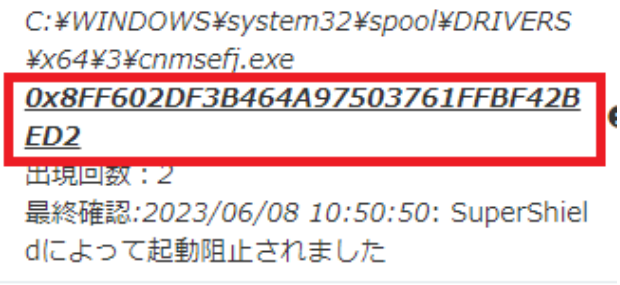
などが推測されます。１回程度であれば放置してください。

同じ端末にて同じファイルを起動阻止した事象が数日に渡って発生した場合は、ローカルリストの再取得ボタンを押してください。先程の通知画面から「端末 PATH」の一番右端にある端末名称をクリックし、端末操作のサブメニューを開きます。サブメニューの下のほうに「ローカルリストの再取得」というメニューがありますので、そちらを選択して開いた画面から「ローカルリストの再取得」ボタンを押します。

3.5.2 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。

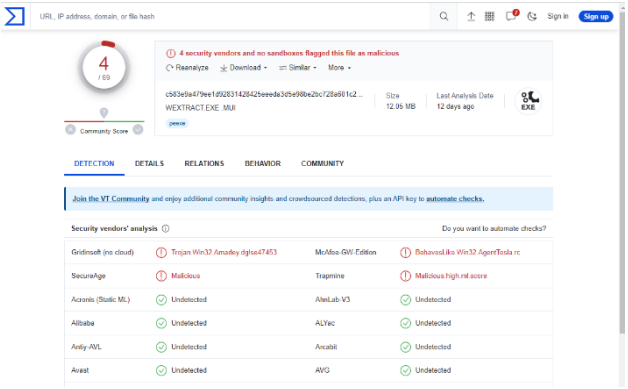
「通知」-「セキュリティ」画面の「説明」の項目に表示されている MD5 ハッシュ値をクリックすると、VirusTotal によるセカンドオピニオンが表示されます。



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。

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。



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。

3.5.3　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)

顧客企業の「プロセス稼働管理」を選択します。標準設定の「プロセス起動阻止」より起動阻止されたファイルを探します。
ファイル一覧の左側にある「 」を押して表示を展開します。メニューの「拒否/許可」タブを押します。
「ファイルハッシュ値」-「アカウント全体」を指定した上で赤色の「拒否のファイル」を押します。

これで、このファイルは、企業全体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、Bad となっている場合の手順に従い、ローカル・ブラックリストへ追加します。

3.5.4　他社セキュリティソフトが問題ないとしている場合(ローカル・ホワイトリスト追加)

顧客企業の「プロセス稼働管理」を選択します。標準設定の「プロセス起動阻止」より起動阻止されたファイルを探します。ファイル一覧の左側にある「 」を押して表示を展開します。メニューの「拒否/許可」タブを押します。

種類のプルダウンにて「デジタル署名」が選択できる場合は、デジタル署名を指定し「レベル」にて「顧客企業名」を選択し緑色の「許可のファイル」を押し、ローカル・ホワイトリストへ追加します。

同じファイルと思われるものが頻繁に起動阻止される際は、「ファイルパス」を指定して追加します。

その他、通常の作業としては、「ファイルハッシュ値」を選択して追加します。

デジタル署名のないバイナリー形式の同じファイル名のファイルが同一顧客で定期的に阻止される際は、ディレクトリ単位や正規表現による包括的なファイル指定を行うのが効率的です。詳しくはこちらをご参照ください。

3.5.5　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既にグローバル・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。顧客企業へ、起動阻止された端末名と共に連絡を行います。

「プロセス稼働管理」-「端末詳細」タブより、どの端末にて起動日時がいつ発生したかをメールもしくは電話など契約内容により、顧客企業へ通知を行います。

顧客企業がマルウェアによって感染しなかったものの、該当パソコンを操作した人に対し、必要であればセキュリティ教育を実施する機会が与えられることになります。

3.5.6　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、プロセス稼働管理より指定を行います。顧客企業の「プロセス稼働管理」を選択します。標準設定の「プロセス起動阻止」より起動阻止されたファイルを探します。regsvr32 が dll を呼び出しているケースは、マルウェアの可能性が高いものになります。

ファイル一覧左の「 」を押して表示を展開します。

「プロセス詳細」タブより「実行ファイルバリエーション」を閲覧し、どのファイルが起動しようとしたのか確認します。

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。

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 繧､綱ｫ綱我ｻ穂ｺ狗畑\謫ｽ蜈ｭ\笆ﾛ繧ｹ綱ｼ綱代・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、顧客企業へ連絡をして、「このディレクトリにあるスクリプトが実行しようとしているのですが、こちらは利用許可が必要ですか。不要ですか」と問い合わせてください。

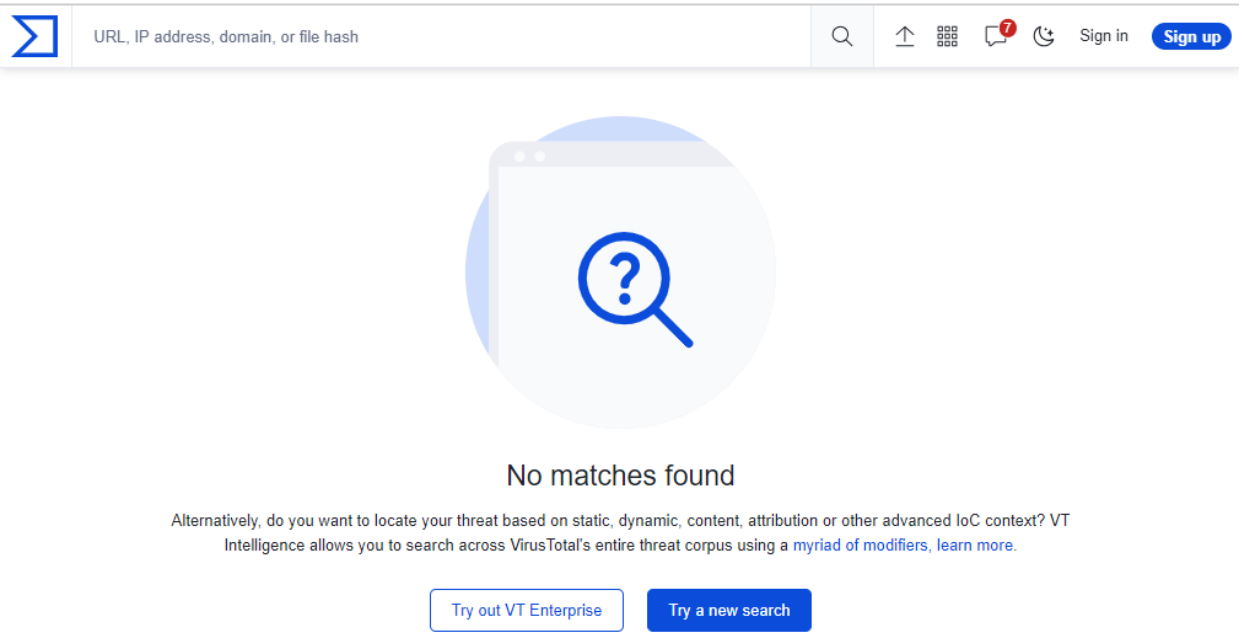
なお、スクリプトも PC Matic 社のマルウェア分析官によってデジタルフォレンジックが行われ、問題のないファイルであれば、グローバル・ホワイトリストへ追加され起動許可が与えられます。

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。

3.6 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、PC Matic の顧客端末にて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ダウンロードし、VirusTotal にアップロードします。パソコンからダウンロードするため、そのパソコンの電源が入っている必要があるため、電源が入っていない時は、作業を行う必要はありません。次回検出された際にパソコンに電源が入っていれば作業を行います。

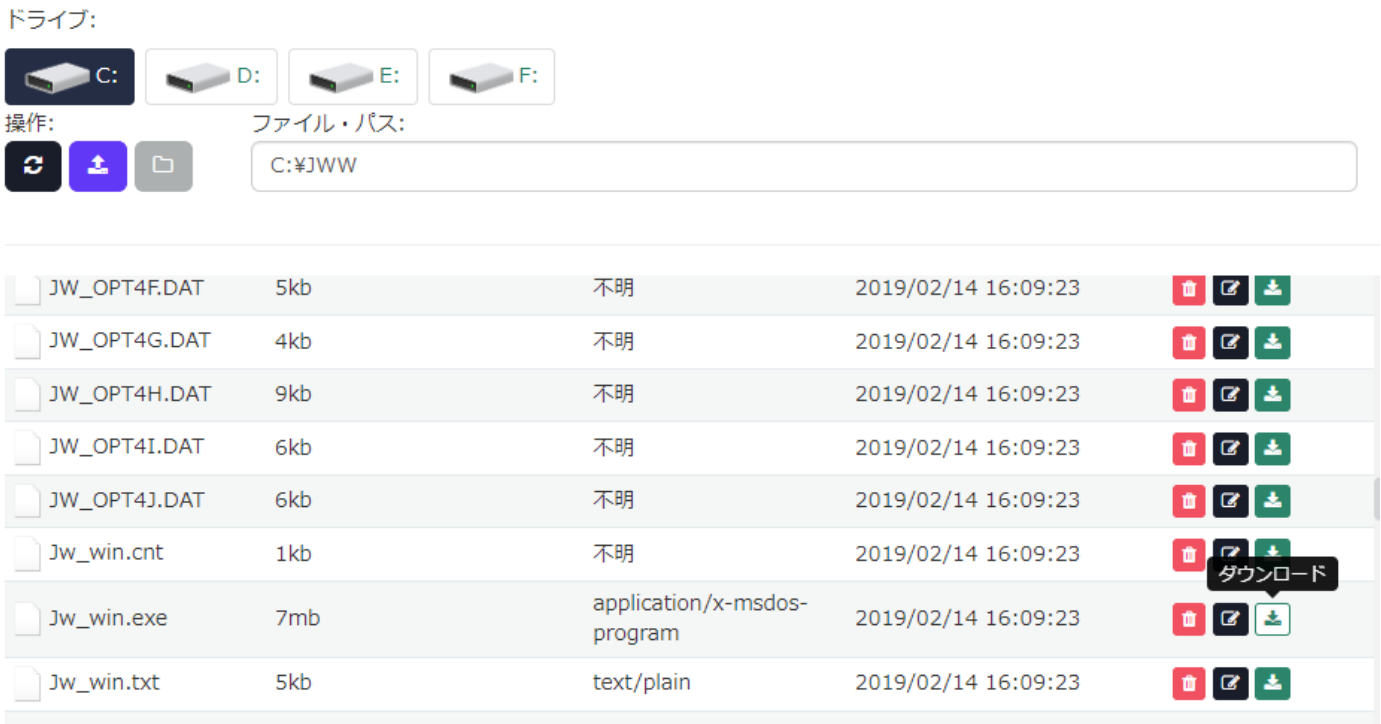
3.6.1 VirusTotal へのアップロードと検証手順

「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。

3.6.2 パソコンのファイルマネージャーを利用してダウンロード

「通知」-「セキュリティ」にて、起動阻止されたファイルの「端末 PATH」の一番右側より、端末名称をクリックして該当端末のサブメニューに入ります。パソコンに電源が入っている状態であれば、「リモートツール」の項目に「ファイルマネージャー」が現れます。先程のファイルパスとファイル名から該当ファイルを探します。

該当ファイル一覧の一番右にある緑色のダウンロードボタンを押します。

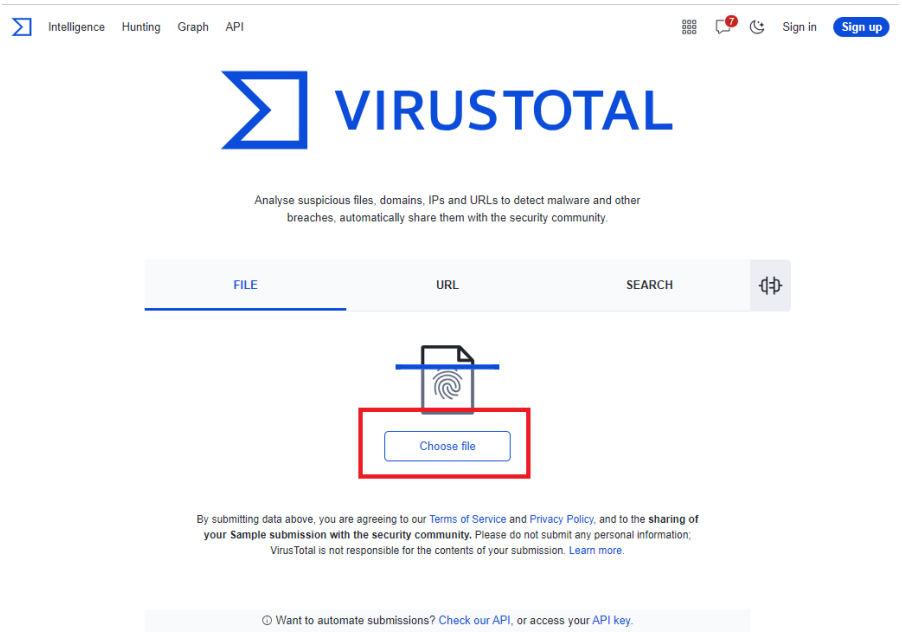


操作しているセキュリティオペレーションセンターのパソコンのブラウザーにて指定されているダウンロード先へファイルがダウンロードされます。

3.6.3 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

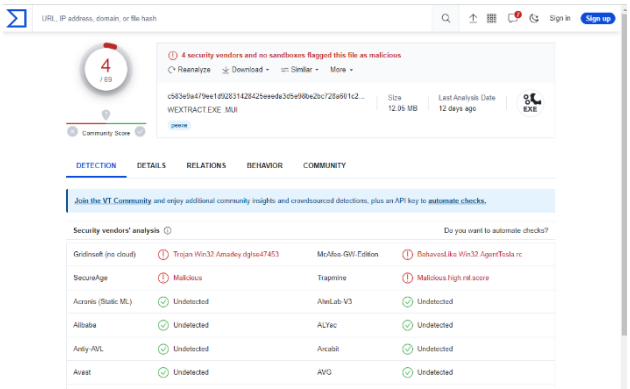
開いた画面の「Choose File」ボタンを押してダウンロードしたファイルをアップロードします。



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。



3.6.4 Behavior タブで素性や問題がないか確認

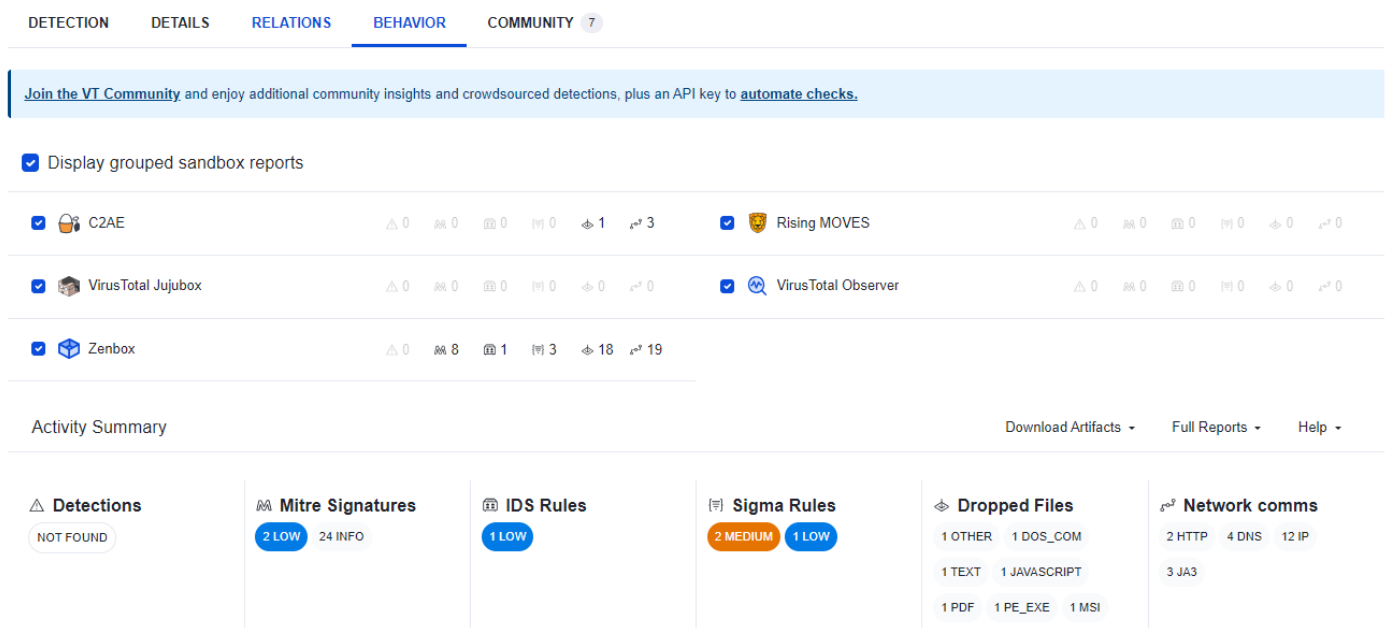
続いて「BEHAVIOR」タブをクリックして表示してください。

「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。



3.6.5 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

3.6.6 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ていま。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。

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。

4　ローカル・ホワイトリストへ追加方法

ローカル・ホワイトリストへの追加の追加方法は複数の指定方法があります。

デジタル署名がされておらず、バイナリー形式のファイルが比較的良く差し変わる際は、ファイルパス指定を利用ください。ファイルパス指定は、バイナリー形式のみ対応しており、スクリプト形式のファイルには対応していません。本手順の解説については、FAQ も参照ください。

4.1　ハッシュ値での指定

デジタル署名がないプログラムを個別に登録していく方法になります。その実行ファイルのみ起動許可が与えられます。デジタル署名が付与されているアプリケーションについては次の項目で実施してください。

4.1.1　通知－セキュリティからハッシュ登録

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。

4.1.2　プロセス稼働管理からハッシュ登録

左メニューの「プロセス稼働管理」から「プロセス起動阻止」を選択すると起動が阻止されたアプリケーションが表示されます。起動阻止されたアプリケーションを選択し、タブを「拒否/許可」に切り替え、指定レベルを選択します。「許可のファイル」を押すと指定レベルにてローカル・ホワイトリストへ追加されます。

4.2　デジタル署名での指定

デジタル署名を用いると複数のファイルで構成されているアプリケーションを包括的に指定することができ、アプリケーションの起動阻止数を大幅に削減することができることがあります。また該当アプリケーションがバージョンアップした際にも有効なことがありますので、可能な限りデジタル署名でローカル・ホワイトリストへ追加することをお勧めします。

ローカル・ホワイトリストへの追加は「プロセス稼働管理」からのみ行えます。

4.3 ファイルパスでの指定

ファイルパス指定には、「ディレクトリ単位包括指定」「ファイル単位フルパス指定」「正規表現指定」の 3 種類の指定方法があります。それぞれに特長があります。

ディレクトリ単位包括指定は、そのディレクトリ(ファイルパス)傘下に複数のバイナリー形式ファイルがある場合や、顧客企業内にプログラマーがいて、新たなバイナリー形式ファイルをたくさん生成する場合に利用します。プログラマーがソフト開発して、いつも試験的に起動をかけるディレクトリを指定することで起動阻止されなくなります。

指定箇所:「アカウント設定」-「ローカル・ホワイトリスト」

ファイル単位フルパス指定は、ファイルパスとファイル名の組み合わせが合致する場合のみ、起動が許可されます。セキュリティ性はディレクトリ単位で指定しまうよりも高まります。同じディレクトリ構造で比較的頻度高くバージョンアップされるバイナリー形式のファイルがある際に活用します。デジタル署名がなされているバイナリー形式の場合は、デジタル署名にてローカル・ホワイトリストへ追加ください。あくまでもデジタル署名がないファイルにのみ利用してください。

指定箇所:「アカウント設定」-「ローカル・ホワイトリスト」

「通知」-「セキュリティ」

「プロセス稼働管理」

正規表現指定は、Windows で管理されたユーザ名が含まれるディレクトリ下にてバイナリー形式の実行ファイルがある際に活用します。C:\Users\mick\App\program.exe のようなログインユーザ名が含まれるマイドキュメント傘下のディレクトリ下にある場合に現れることがあります。プログラムはマイドキュメント傘下には基本的に格納することはマイクロソフトによって非推奨となっていますが利用されることもあります。企業組織の複数人でこのようなディレクトリ下にある業務アプリケーションを利用する際は、ファイルパスが異なって同じ実行ファイルを起動させることがあります。exe などの実行ファイルをハッシュ値にてローカル・ホワイトリストへ指定すれば起動は行えますが、ファイルが頻繁に差し替えられる際は、この正規表現にて指定します。

指定箇所:「アカウント設定」-「ローカル・ホワイトリスト」

ドライブ指定	[a-z]:\\	# Drive
フォルダ指定	(?:[^\\/:*?"<>|\r\n]+\\)*	# Folder
ファイル指定	[^\\/:*?"<>|\r\n]*	# File

Regex 指定例: ^[a-zA-Z]:[\\\/](?:[a-zA-Z0-9]+[\\\/])*([a-zA-Z0-9]+\\Monos\.Client\.(exe))$

Monos.Client.exe のファイル名を持つユーザ名が変化する指定に活用できます。

参照:.NET 正規表現

4.3.1 「アカウント設定」-「ローカル・ホワイトリスト」にて指定手順

フルパス指定および、ディレクトリ単位指定での包括指定をご利用いただけます。多数の実行ファイルがあるゲームソフトでは包括指定が便利です。端末への同期には 5 分程度要します。

管理ポータルへログイン後、「アカウント設定」-「ローカル・ホワイトリスト」を選択します。

「ファイルパス追加」ボタンを押すと下に入力欄が表示されます。

ディレクトリ単位包括指定:

C:\Program Files (x86)\PCMatic

PC Matic 配下の全てのバイナリー形式の実行ファイルを起動許可します。

ファイル単位フルパス指定:

C:\Program Files (x86)\PCMatic\ReinstallService.exe

ReinstallService.exe のみ実行許可します。

正規表現指定:

正規表現で様々な指定が可能です。例:^C:\\Users\\[^\\]+\\AppData\\Local\\Apps\\app.exe

C:\Users\mick\AppData\Local\Apps\app.exe などユーザ名が変化する指定に活用できます。

【説明】は、どのアプリケーションであるかを自分のメモとして記載します。

【レベル】と【プラットフォーム】を指定し、右の「保存」ボタンを押します。正規表現の際はチェック印を。

ファイルパス追加に成功すると、下の欄に追加されます。

4.3.2 プロセス稼働管理からファイル単位フルパス指定

左メニューの「プロセス稼働管理」から「プロセス起動阻止」を選択すると起動が阻止されたアプリケーションが表示されます。起動阻止されたアプリケーションを選択し、タブを「拒否/許可」に切り替え、ファイルパスを選択し、指定レベルを選択します。「許可のファイル」を押すとローカル・ホワイトリストへ追加されます。

4.4 社内展開インストール

インストーラーは、Active Directory(AD)の有無により 2 種類があります。標準で表示されるものは、AD なしのものになっています。

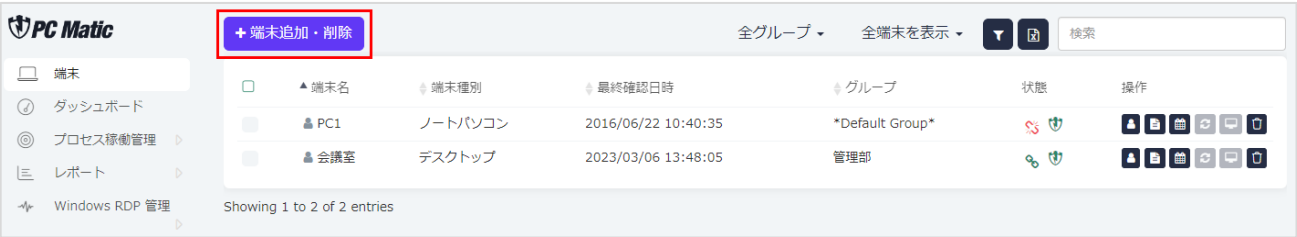
AD なしの「エンドポイントインストーラー」をインストールする場合は、「4.4.1Windows エンドポイントインストーラーをインストールする」をご参照ください。

AD ありの「デバイスマネージャー」を導入する場合は、「4.4.2Active Directory 利用時の導入方法 Active Directory 利用時の」をご参照ください。

4.4.1 Windows エンドポイントインストーラーをインストールする

1. https://portal.pcmatic.com/ にアクセスし、管理ポータルにログインします。

2. 左側のメニューから「端末」を押し、表示された画面で「端末追加・削除」を選択します。



3. インストーラーは、Active Directory(AD)の有無により 2 種類あります。標準で表示されるものは、AD なしのものになっています。AD ありのものを選択する場合は、上部タブを「Windows 版導入」または「Mac 版導入」を選択ください。
なお、AD を利用してインストールを行うと、AD 管理下のパソコンへ一斉インストールをすること可能になります。インストール後に、管理ポータルにしばらくすると自動的にパソコンが表示されます。また、アンインストールを AD 経由で行った後に、管理ポータルより削除してください。

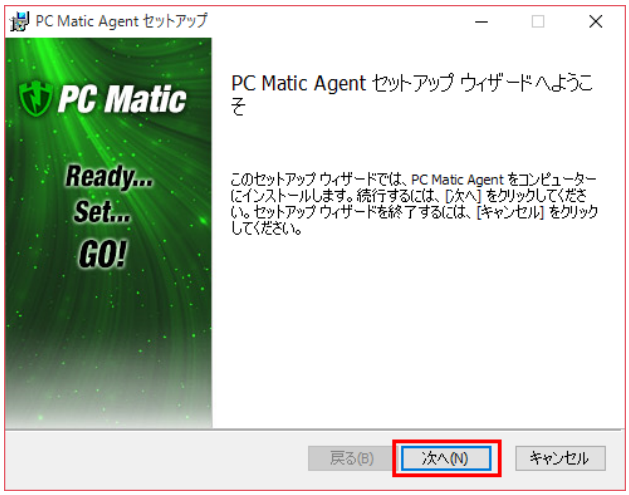
4. リファレンス機で作成したローカル・ホワイトリストをグループやアカウント全体レベルなどに変更し、複数の端末へリファレンス機のローカル・ホワイトリストが自動展開されるように設定します。

5. インストーラーの画面が表示されましたら、オプションやどの部署用のものをインストールするかを設定します。オプション設定は、新規インストール時の標準値です。導入後は管理ポータルより設定変更します。

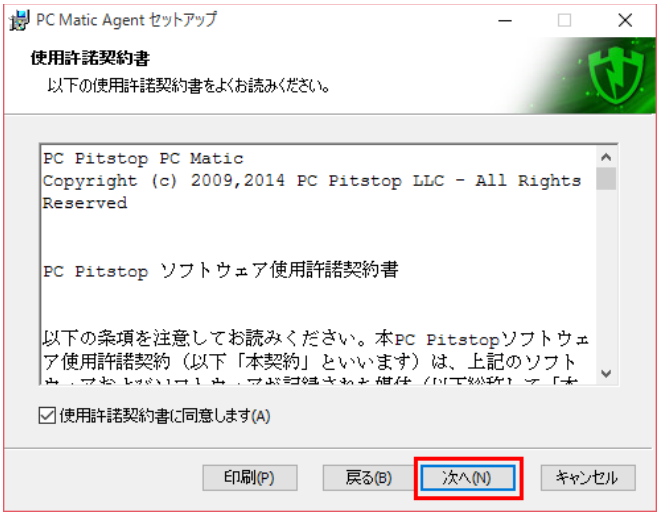
- リモートデスクトップは、遠隔操作機能のオプションですので社内のセキュリティポリシー上解除したい場合は「リモートデスクトップ」のチェックを外してください。
- 「ブラウザー保護」のチェックを入れる事を推奨しています。
- SuperShield オプションの「EPP 制御利用」を「無効(推奨)」にすると、インストールしたパソコンのタスクトレイに PC Matic のアイコンが表示されなくなります。こちらにチェックを入れる事をお勧めしております。なお、グループ未定義を含めて 1 部署に 100 台までインストールする事ができます。
- 起動阻止ファイル通知を「保護警告非表示(初心者/社内)」にすることを推奨しています。
- 「Microsoft Defender」の項目は「有効化」をお勧めします。「無効化」にすると、PC Matic SuperShield が保護セキュリティエンジンとして識別されます。「有効化」にすると Microsoft Defender 等と他社法人版セキュリティエンジンと二重保護モードとなります。

6. インストーラーの設定ができましたら、右下にある「インストーラー・ダウンロード」の URL を押して「Windows 版」および「Mac 版」のインストーラーをダウンロードしてください。

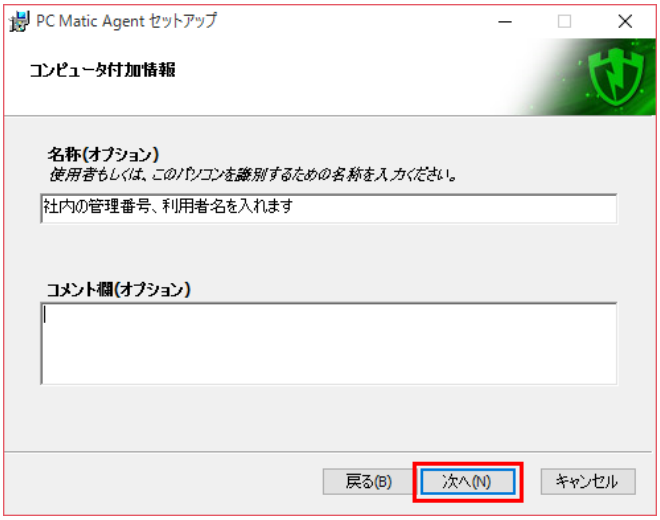
7. インストールは管理者権限で Windows を利用している状態で行ってください。ユーザー権限では正常にインストールが行えません。ダウンロードしたインストーラーを開き「次へ」を押します。



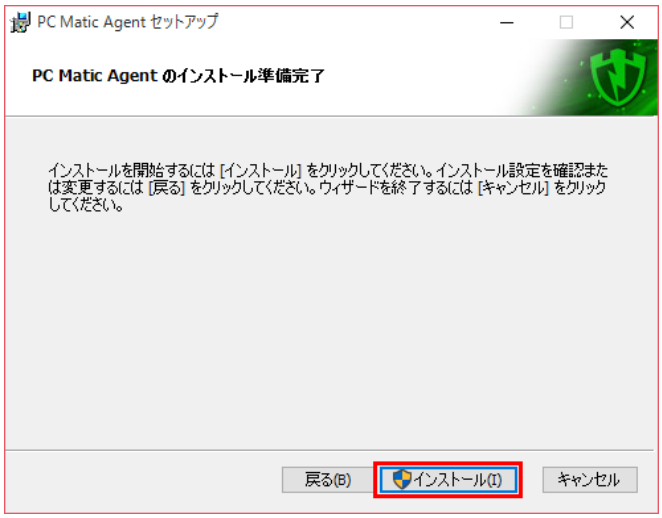
8. 「次へ」を押します。



9. 必要に応じて**端末管理番号**や**利用者名**等の「コンピューターの付加情報」を入力して「次へ」を押します。

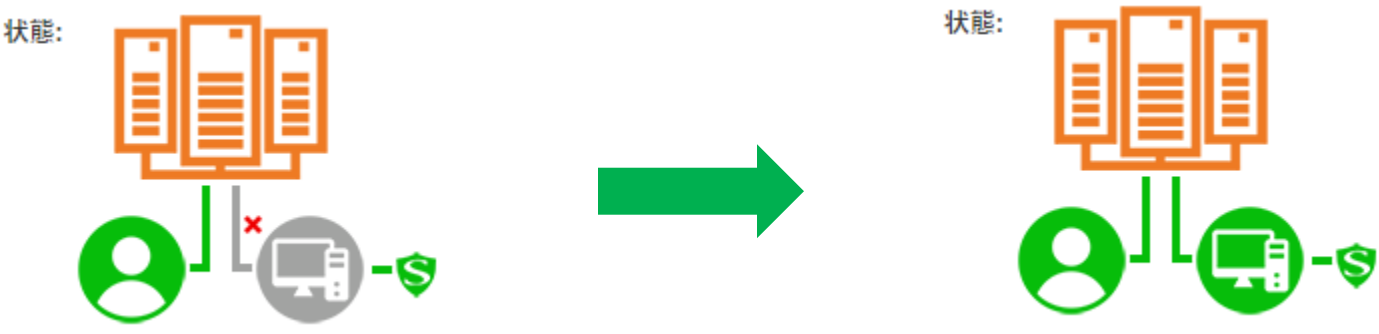


10. 「インストール」を押します。



11. インストールが終わりましたら「完了」を押します。インストーラー終了後に、最大 4700 ファイルを PC Matic Cloud Platform より取得して端末登録と同期を行いますので、管理ポータルにて端末のアイコンが黄色から緑色になるまで端末を放置ください。

12. 管理ポータルの「端末」-「端末の状態」にて、アイコンがオフラインからオンライン状態になるまでインストーラーが終了後、お待ちください。

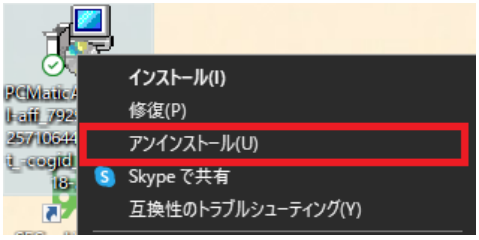


オフライン状態　　オンライン状態

13. スーパーシールド・オプション「ユーザーによるオプション設定オフ」のチェックを外してインストールを行った場合は、タスクトレイに PC Matic のアイコンが表示され、シグネチャをダウンロードしている際は黄色くなり、ダウンロードが完了すると緑

色になります。管理ポータルの端末一覧にて新規導入した端末が緑色ステータスになるまで 30 分程度要します。これは、初期状態において、端末の識別情報をサーバーに伝送し登録処理を行うためです。

インストールに失敗した場合は、インストーラーをマウスで右クリックして表示される「アンインストール」にて、アンインストールし、再度インストールを行います。



4.4.2 Active Directory 利用時の導入方法

デバイスマネージャーのインストーラーを使用すると、Active Directory やワークグループを使用して簡単に PC Matic Pro を端末にインストールできます。サーバー上の GPO と共に PowerShell を使用するプッシュインストール方法により、再起動することなくクライアントを各エンドポイントにインストールすることができます。
なお、端末一斉導入方式でインストールするには下記の環境が必要となります。

- サーバー：PowerShell 3.0 以上が必要
- エンドポイント：PowerShell 2.0 以上が必要

1. https://portal.pcmatic.com/ にアクセスし、管理ポータルにログインします。
2. 「インストーラー」を選択します。

3. 画面右上の「端末追加」を選択します。
4. リモート PowerShell GPO の作成：このオプションを使用すると、リモートの PowerShell 実行を有効にするアクティブディレクトリネットワーク用の GPO が作成されます。インストーラーを使用するには、このオプションを選択したままにするか、選択したコンピューターのリモート PowerShell 実行を有効にする GPO をご自分で作成する必要があります。
   端末一斉導入方式のインストーラーでは、この AD ネットワークを関連付けるグループを選択できるようになりました。これは、複数の AD ネットワークをプッシュインストールする場合に便利です。

5. オプションを設定したら、ダウンロードボタンを選択してインストーラーをダウンロードします。
   このオプションを選択した場合、デバイスマネージャーをインストールして GPO を構成するには、これをアクティブディレクトリサーバー上で実行する必要があります。

6. インストール後、デバイスマネージャーは AD ネットワーク上のコンピューターを見つけ、[ネットワーク端末]タブに表示します。特定のグループを選択した場合は、ポータルホームページのグループドロップダウンを使用して、[ネットワークデバイス]タブが表示されるようにしてください。

ネットワーク端末

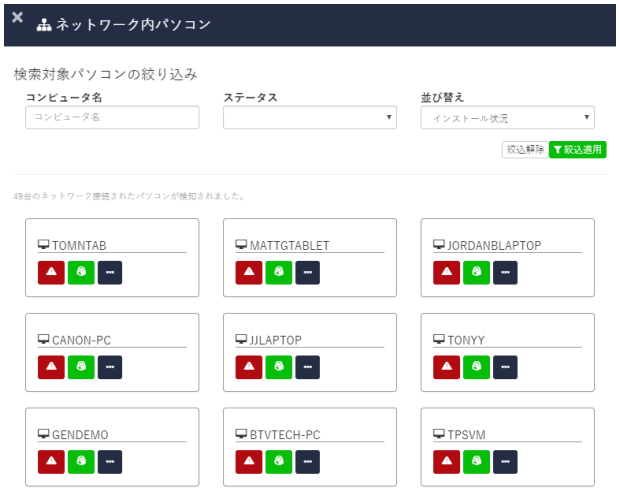
サーバー経由でのインストールが完了したら、「ネットワーク端末」にアクセスできるようになります。 これにより、アクティブディレクトリネットワーク上にあるすべてのパソコンへアクセスできます。 このような観点から、私たちは一括インストールやパソコンへのアンインストール、または個別にインストールとアンインストールが可能です。

この画面では、ネットワーク上のすべてのコンピューターを表示する「端末」タブと、インストール用の管理者資格情報を保存できる「認証情報」の 2 つのタブがあります。

「端末」タブでは、左側のチェックボックスを使用して一括選択ができます。各端末の右側にあるアイコンは、端末に関するさまざまな情報を示しています。

端末状況

- インストール済み：PC Matic Pro が現在エンドポイントにインストールされています。
- アンインストール：PC Matic Pro は現在エンドポイントにインストールされていません。
- 保留中のインストール：PC Matic Pro は、サーバー上のスケジューラーサービスが実行されるときに端末にインストールされます。
- 保留中のアンインストール：PC Matic Pro は、サーバー上のスケジューラーサービスが実行されるときに端末でアンインストールされます。



端末の詳細

- エンドポイント AD ネットワークに関する情報、およびインストール後の現在の PC Matic 構成を表示します。
- **端末へソフトウェアのインストール、アンインストール**
  緑のアイコン：インストールをエンドポイントにプッシュします。
- 赤いアイコン：クライアントをエンドポイントから引き出す（アンインストール）。

アカウントから削除する

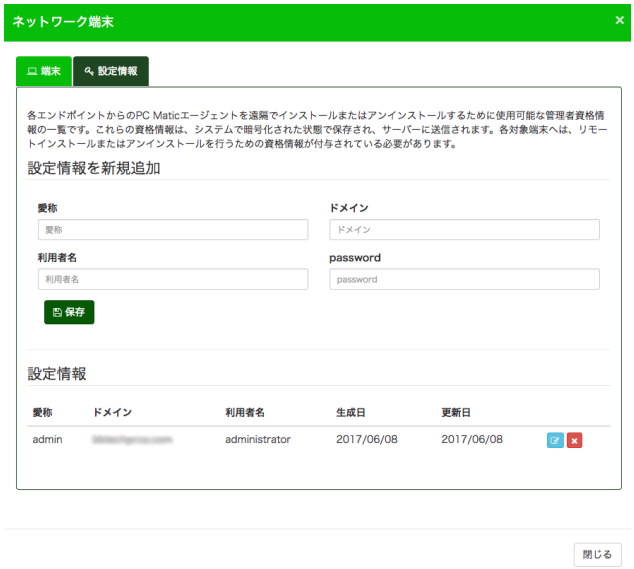
インストールする前に、デバイスマネージャーの画面からデバイスが削除され、インストールをプッシュできなくなります。

手動で端末の追加

現在アクティブなディレクトリネットワーク上にない端末があるが、デバイスマネージャーがインストールされているサーバーがそれらを見ることができる場合は、IP アドレスまたはコンピューター名で追加することができます。「端末」タブでは、その端末名または IP アドレスを入力してマシンを追加し、そのエンドポイントにプッシュインストールを行うことができます。

認証情報

「ネットワーク端末」ウィンドウの「設定情報」タブでは、暗号化された管理者資格情報を保存してインストールできます。 認証情報は、各エンドポイントに一括してまたは個別に割り当てることができます。 これにより、ユーザーがコンピューター上で管理者アクセス権を持っていなくても、各エンドポイントにインストールをプッシュできます。



暗号化された認証情報を追加するときは、将来、各管理者の認証情報を覚えておくのに役立つニックネームを設定してください。 ニックネームは、インストールをプッシュアウトする前に、各認証情報を端末に割り当てるために使用されます。

4.4.3 コマンドラインからのサイレントインストール方法

すべての必要なパラメーターは、ファイル名、コマンドライン、またはその両方の組み合わせで渡す必要があります。コマンドライン引数は、ファイル名から渡された引数を上書きするために使用することができます。

(使用例) msiexec /i PCMaticAgent.MUI.msi /quiet AFF=1234 UID=12345678987654321 GROUP=12345 OPTIONS=11282

必要パラメーター:

AFF	Affilate ID			
UID	UID			
COMPANY	CompanyID	または	GROUP	CompanyGroupID

オプション・パラメータ:

OPTIONS

インストール設定を指定するために使用するビット単位の値です。

1 つのインストーラーで複数の機能を追加するには、機能に対応する各番号を加算する必要があります。

2	SuperShield 導入
16	リモートデスクトップの利用
32	SuperShield トレイアイコンの無効化
512	起動阻止通知の無効化
1024	許可・拒否リスト追加画面表示
2048	Java 許可
4096	脆弱性対策 OFF
8192	脆弱性対策 ON
16384	USB 大容量装置の無効化
32768	ブラウザー保護導入

4.4.4 AWS、VMWare ESX、Windows Terminal Service 仮想環境(VDI モード)への適用方法

PC Matic は、ハードウェア構成情報をベースに端末固有の識別を行っています。仮想環境においては、ハードウェア構成が仮想的に構成されるか同一であるため、PC Matic をインストールする際は、「VDI モード」をグループ単位で設定します。

「アカウント設定」-「VDI モード管理」から、仮想環境を適用するグループを指定します。仮想環境で運用する端末のみ、このグループへ指定ください。

【注意点】

- 複数の仮想環境を利用する際は、複写したイメージにて Windows が管理するコンピュータ名を個々に異なるものへ変更ください。この名称を識別子として PC Matic が利用します。
- 仮想環境へ PC Matic をインストールした後に仮想環境イメージを複写したものを複数起動して利用しないでください。同一端末が複数あると識別し、クライアントサーバ通信に不具合が発生し正常稼働しません。複写後にコンピュータ名を変更し、PC Matic をインストールしてください。
- 仮想環境での利用において VDI モードに設定しなかった場合は、仮想的なハードウェア識別が共通の際は複数台の端末が 1 つの端末として識別されたり、仮想的なハードウェア識別が変化するため 1 つの端末が複数台となって現れるようになります。これらの場合は、すべて正常に稼働しませんのでご注意ください。

4.5 ブラウザー保護(各種詐欺対策)インストール

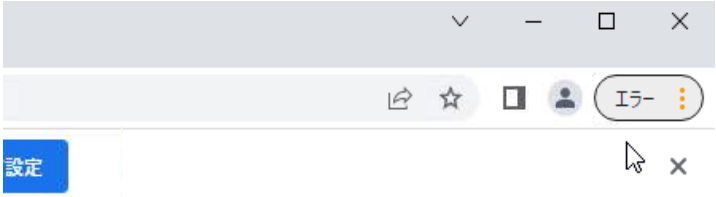
ブラウザー保護機能として、詐欺対策、オンラインバンキング保護、不正なスクリプト実行拒否などの機能を Google Chrome, Edge, Firefox へ拡張機能として導入頂けます。

PC Matic のインストーラー作成時に「ブラウザー保護」へチェック印をいれた場合は、この拡張機能が一緒に導入されます。

チェック印をいれなかった場合は、端末がオンライン状態の際に「ブラウザー保護」タブを選択し、「ブラウザー保護機能 導入」ボタンを押すことで遠隔インストールしていただけます。

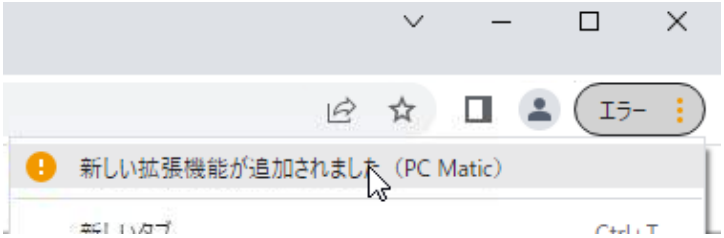
4.5.1 Google Chrome

1. PC Matic インストール後や、「ブラウザー保護」を管理ポータルより導入指令を出した後に、端末にて Google Chrome を立ち上げると画面右上に添付のような「エラー」が表示されます。

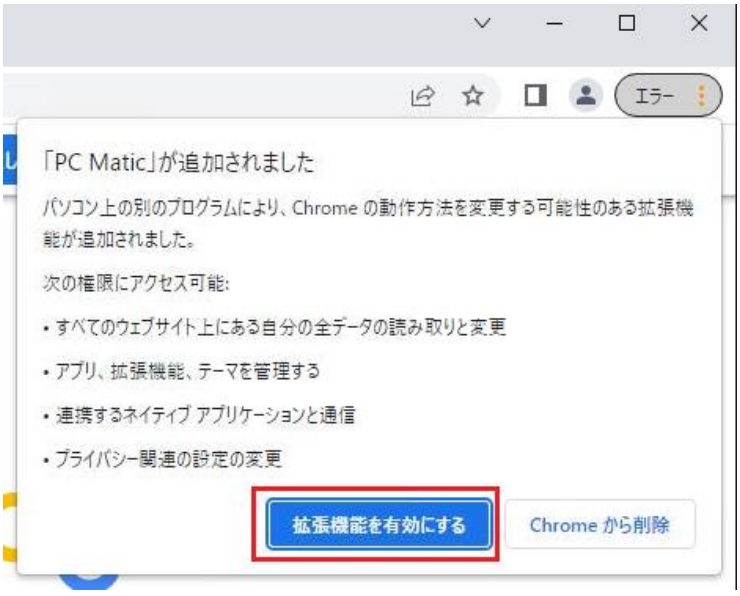


2. エラーをクリックすると、「新しい拡張機能が追加された」と画面が表示されます。

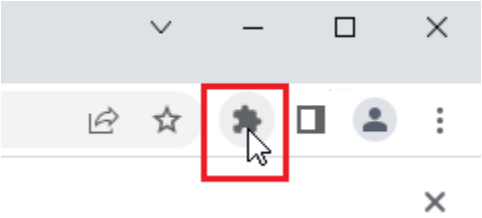
3. 「PC Matic」の箇所をクリックします。



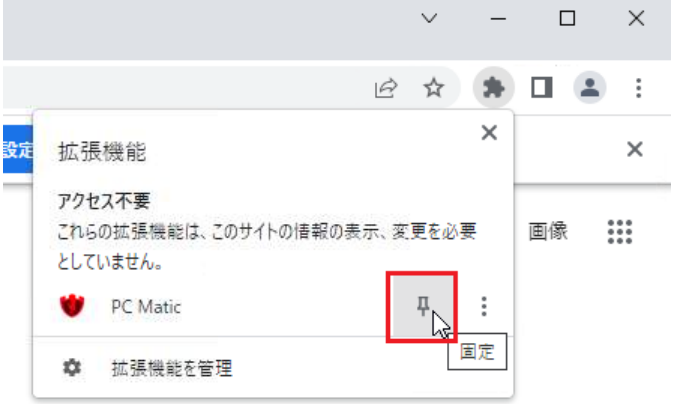
4. 開いた画面で「拡張機能を有効にする」を選択します。



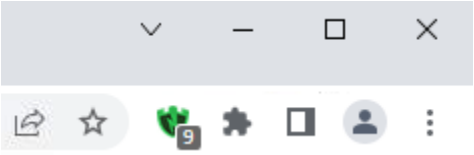
5. 「拡張機能」アイコンを押します。



6. 表示された画面の「PC Matic」の横にあるピンのアイコンをクリックします。

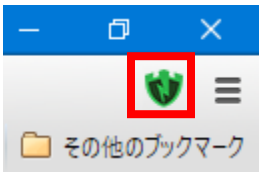


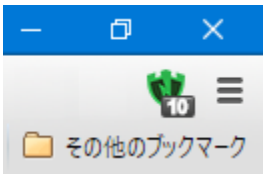
7. ブラウザー上に PC Matic のアイコンが常時表示されるようになります。インターネット上のホームページを表示していない時や、保護解除をした場合はアイコンが赤色で表示されます。



4.5.2 Edge

広告ブロック機能が有効になっている場合は、ブラウザの右上に 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。



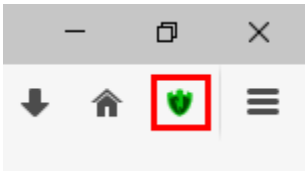


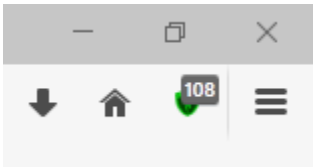
SuperShield アイコンを選択し、表示される画面の をクリックすると広告ブロック機能を解除することができます。
解除すると、 が灰色になり、そのドメインの広告が表示されます。灰色の状態でアイコンを選択すると広告ブロック機能が有効になります。

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広告ブロック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。

4.5.3 Firefox

広告ブロック機能が有効になっている場合は、ブラウザの右上に 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。

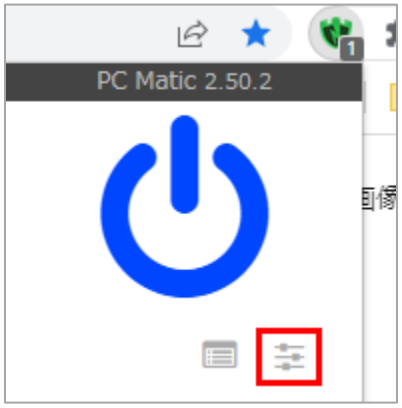




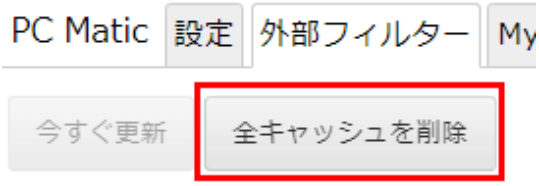
4.5.4 広告ブロック機能を有効にしているのに広告が表示される場合

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。

5　スキャンと最適化

本機能はパソコン内にあるウイルスなどの悪質なファイルを検疫区画へ移動する重要な役割を担っています。週に一度実行されるように設定をお願いいたします。

スキャン最適化は、個々の端末に対して指定するのではなく、顧客企業や部署ごとなど包括的に設定することができます。お昼休みなど業務に支障がない時間に実行されるようにすることをお勧めいたします。

定期スキャンでは、「編集」を押して、「マルウェア監査」を「クイック」へ変更してください。標準のフルスキャンでは、膨大な時間を要するのとストレージへの負担が大きくなります。また、スケジュール実行時にパソコンの電源が入っていない場合は当日中に実行されます。

パソコンが高負荷状態にある場合は、スキャン最適化は実行されずに待機状態になります。負荷が下がった際に実行されるようになります。

1. 管理ポータルで「端末一覧」を押します。
2. スキャンを行いたい端末名を選択します。
3. 端末がオンライン状態になっているのを確認し、「診断実行」を押します。

4. 診断を押すと、様々な診断のオプションが表示されます。

5. オプションを選択し、「即時診断をいま実施」ボタンを押します。EDR 診断が始まり、診断が実行中と右側の画面に表示されます。初回スキャンの場合は、ファイル検査とディスク検査を大量に行いますので 2 ～ 3 時間要します。
Proxy サーバーが導入されている場合は、5 時間以上要することもあります。

6　エンドポイント保護の稼働モードと稼働確認

6.1　4 つのエンドポイント保護稼働モード

エンドポイント保護は、４つの稼働モードを装備しています。グローバルリストを利用することができる「通常稼働モード」と３つの「ローカルリスト稼働モード」です。通常稼働モードでは、マルウェア分析官が１億件以上善良と判定済のグローバル・ホイトリストとローカル・ホワイトリストを併用して利用することができ、一般的なブラックリスト方式のエンドポイント保護と同じ使い勝手でありながら強固な防御能力を実現します。

グローバル・ホワイトリスト及びローカル・ホワイトリストの利用レベルを変更することでき、より厳格なホワイト運用が可能です。３つのローカル・ホワイトリスト運用による保護モードは、グローバル・ホワイトリストのうち OS 構成ファイル以外のホワイトリストを利用しない保護モードとなります。起動可能なファイルを限定することで、攻撃面を極小化することができ、サイバー攻撃に対する耐性をより高めることができます。全ての保護モードはホワイト運用であるため、OS のもつ全機能を標準でロックし、未知のサイバー攻撃や脆弱性への耐性が強固になります。

【PC Matic のローカル・ホワイトリスト運用モードの特長】

ローカル・ホワイトリスト運用モードのうち『適用』と『標準』は、マルウェア分析官により善良と判定された OS 構成ファイルの更新情報(OS に関連したグローバル・ホワイトリスト)を利用でき、その手間から解放されます。USB メモリに入れたホワイトリストファイルを端末へ適用する手間から完全に解放されます。

【本機能の背景】

最近は、セキュリティ企業が善良と認定済の比較的利用者が多いアプリケーションの脆弱性や汎用性を悪用し、マルウェアとして実行させるケースが急増してきています。これに対処するには、世の中で善良は判定されているアプリケーションであっても、組織内で利用させないことで、リスクを大幅に低減もしくは撤廃させることができます。

【利用推奨シーン】

産業機械の制御用コンピューター、デジタルサイネージ、POS レジ、インフラ企業等の高い脅威耐性が必要なシステムなど

【保護モード設定レベル】

保護モードの変更は「SuperShield オプション」メニューより、「端末」「グループ」「顧客企業」レベルにて設定して頂けます。

6.1.1 標準（SuperShield 保護モード/グローバル＋ローカルリスト運用）

グローバルリストにて 1 億 3 千万件のアプリケーションのホワイトリスト提供あり。
ホワイト運用ながらも業界標準のブラックリスト方式エンドポイント保護製品と遜色ない使い勝手を実現
ローカル・ホワイトリストのファイル、スクリプト、デジタル署名、ファイルパス
グローバル・ホワイトリストのファイル、スクリプト

6.1.2 ローカルホワイトリスト運用 - 適応

グローバルリストにてアプリケーションのホワイトリスト提供なし。
ローカル・ホワイトリスト内のバイナリー形式アプリケーションの更新ファイル自動付与
ローカル・ホワイトリストのファイル、スクリプト、デジタル署名、ファイルパス
グローバル・ホワイトリストのスクリプト
グローバル・ホワイトリストの OS 構成ファイル
ローカル・ホワイトリストのファイルに関連する更新ファイル

6.1.3 ローカルホワイトリスト運用 - 標準

グローバルリストにてアプリケーションのホワイトリスト提供なし
ローカル・ホワイトリストのファイル、スクリプト、デジタル署名、ファイルパス
グローバル・ホワイトリストのスクリプト
グローバル・ホワイトリストの OS 構成ファイル

6.1.4 ローカルホワイトリスト運用 - 厳格（組込用途）

グローバルリストで OS,アプリケーションの提供なし。
OS 更新ファイルも阻止されるため運用には注意が必要です
ローカル・ホワイトリストのファイル、スクリプト、デジタル署名、ファイルパス
グローバル・ホワイトリストのスクリプト

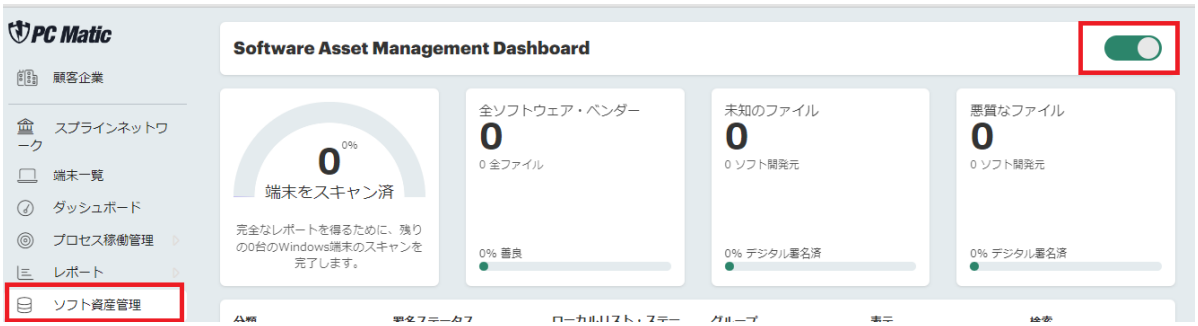
6.2 SWAM ファイルレーダー

端末内にある実行ファイルを社内利用者が起動阻止され業務に支障をきたすことがないよう、業務上実行が必要なファイルが未監査状態で残っていないか把握することができる機能になります。

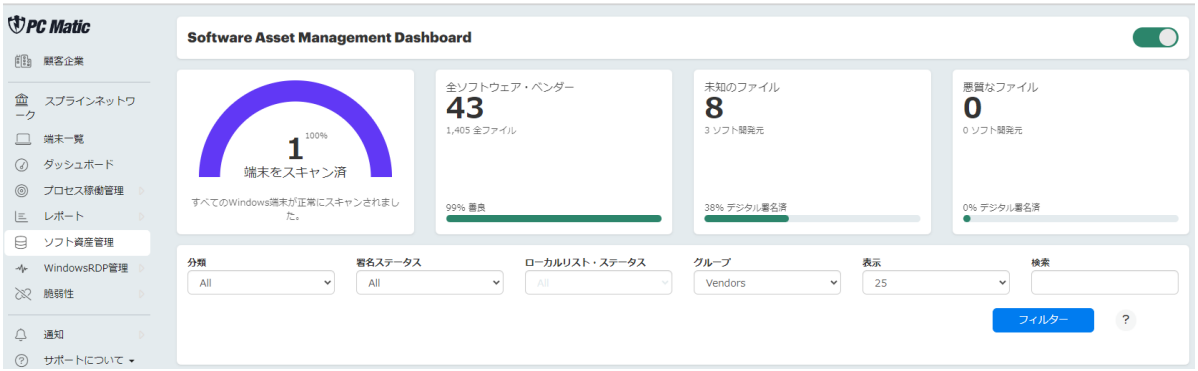
許可したアプリケーションのみに限定して、社内利用を許可する、ローカル・ホワイトリスト保護モードという厳格な運用を行う際は、本機能により起動を許可するファイルを全てローカル・ホワイトリストへ追加し許可リストを作成する必要があります。

本リストを作成するためには、本機能を事前に有効にした上で、端末にエージェントをインストールするか、スケジュールスキャン(定期 EDR 診断)にてファイルの情報を取得しておく必要があります。

メインメニューの「SWAM ファイルレーダー」(SWAM: Software Asset Management Dashboard)を選択します。右上にあるスライダーをクリックして右に動かし「緑色」にさせ有効化してください。



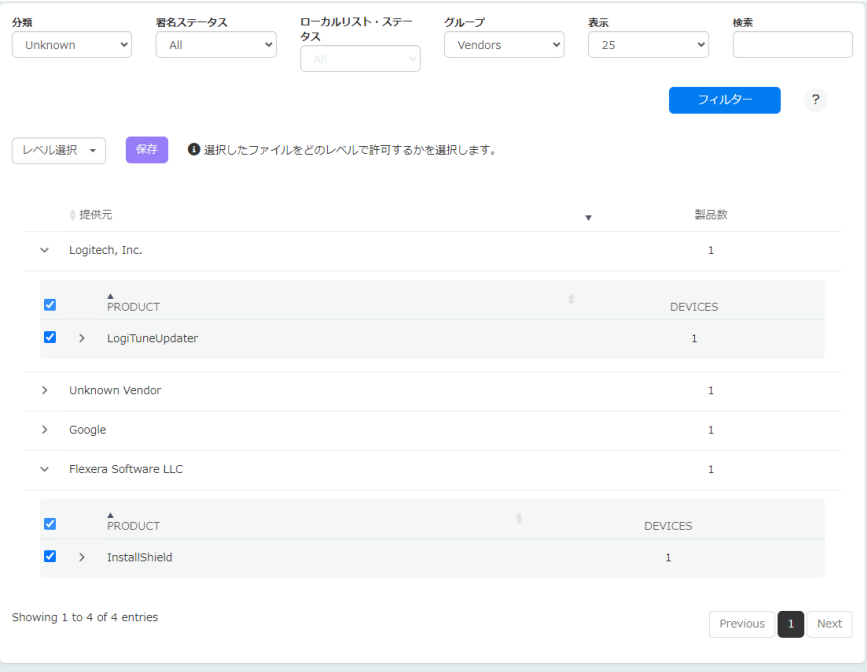
定期スケジュールスキャンが実行されると取得された情報がダッシュボード上で利用可能となります。



フィルターにて表示された開発元名からプルダウン展開するとアプリケーション名が表示されます。ファイル名の左横にある□にチェックをいれるとローカル・ホワイトリストへ追加選択が行えます。業務上必要なアプリケーションを全て選択していきます。

グローバル・ホワイトリスト保護モードで運用する際は、「分類」で「Unknown」をグループで「Files」を選択し、「ローカルリスト・ステータス」で「Not on Allowlist」を押してから「フィルター」を押します。このリストには、未分類である他に、フリーソフトウェアや 2014 年以前の Microsoft Office(Word,Excel, Powerpoint 等)など深刻な脆弱性が含まれているものを分類されています。

このため表示されているファイルを更に開くと「HASH」が表示されます。このハッシュ値をクリックすると VirusTotal に飛びます。善悪の判定を VirusTotal によって分析を行います。詳細は前述の「Unknown となっている場合」を参照の上、VirusTotal にて他社がマルウェアと指定していないか、Behaivor タグにてサイバー攻撃に利用される攻撃方法が含まれていないかを MITRE ATT&CK 項目を参照して調べてください。



レベルの選択を展開し、どの組織レベルで該当アプリケーションを利用可能とするか選択します。アカウント作成時の初期段階では端末のみの指定で結構です。後程、ローカル・ホワイトリストの管理画面よりレベルを変更して頂けます。

レベルを選択し、「保存」を押すと、ローカル・ホワイトリストへ追加されます。

ローカル・ホワイトリスト保護モードの場合は、「分類」の絞り込みを「all」にして必要なアプリケーションを同様に指定しローカル・ホワイトリストを作成します。

6.3 SuperShield 稼働確認

インストールした SuperShield が稼働しているか確認してください。

1. https://portal.pcmatic.com/ にアクセスし、ログインします。
2. 「端末」を選択し、SuperShield をインストールしたパソコンを選択します。

3. 「SuperShield ログ」を選択します。


PC Matic
端末一覧
ダッシュボード
プロセス稼働管理
レポート
WindowsRDP管理
脆弱性
通知
サポートについて
アカウント設定
ログアウト
端末オプション
EDRスキャン
EDR診断
EDR診断履歴
通知
通知
通知の設定
通知オプション
リモートツール
コマンドプロンプト
ファイルマネージャ
リモートデスクトップ
レポート
Windows RDP接続履歴
サイズの大きなファイル
システムスペック情報
パフォーマンス
メンテナンス概要
導入済ソフト
端末の状態
セキュリティ
SuperShield
SuperShieldオプション
SuperShieldログ
ローカルブラックリスト
端末: DESKTOP-Q9QDA57 (会議室)
SuperShieldログ
SuperShieldログ絞込条件
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
全て
検出時の識別状態
全て
検索種別
全項目
絞込解除
絞込適用
Search:

4. 標準では稼働が阻止されたもののみ表示されるように絞り込み設定がされています。
それ以外の稼働ログを確認する場合は、「絞り込み」ボタンを押し、「起動の是非」を「全て」にして「絞込適用」を行ってください。
タイムスタンプの日付を確認しながら、何らかのログが記録されているか確認してください。ログが記録されている場合は、SuperShield が正常に稼働しています。

ログの右にあるアイコンから簡単に「ローカル・ホワイトリスト」へ追加することができます。

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。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。

6.3.1 アプリケーションの起動をブロックする場合

PC Matic SuperShield は、マルウェア分析官により善良と判断されていないアプリケーションは全てブロックします。通常 24 時間程度で善良・マルウェアへ分類されます。深刻な脆弱性が含まれるアプリケーションは遠隔操作されるなどマルウェア同様の脅威となるため、SuperShield では起動が阻止されます。Office 2000 など古いアプリケーションの多くがそれに該当します。

- **ブロックされた場合は、基本的に放置ください**
- マルウェア分析官により、原則として 24 時間でグローバル・ブラックリスト／グローバル・ホワイトリストへ分類されます。
- SuperShield は、定義情報の更新ファイルをリアルタイムに取得します。業務上必要なアプリケーションであると判断できている場合は、管理ポータルの「ローカルホワイトリスト」へ「SuperShield 稼働ログ」「プロセス稼働管理」「通知-セキュリティ」から追加することで、管理者が追加していただくことで即座に利用して頂けます。

・ **最新版がないか再確認ください**

PC Matic のアプリケーション・ホワイトリスティング方式は、脆弱性というセキュリティホールを抱えているアプリケーションは、米国連邦政府基準である NIST SP 800-167 にて起動を拒否されるべきと定義されているため起動が許可されません。セキュリティホールには、深刻なものから軽微なものまで様々な種類がありますが、まずは脆弱性対策がなされた新しいアプリケーションが提供されていないか確認されることをお勧めいたします。

2009 年以前のアプリケーションは、Microsoft 社の開発言語によって生成されたすべてのアプリケーションは深刻な脆弱性を抱えているため、2009 年以前のアプリケーションの大半はこの脆弱性によりご利用いただけないことをご理解ください。

・ **世界中の誰かが、過去起動したことがあ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。実は日本製のフリーソフトウェアもほとんど過去、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です。

6.3.2 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、ホワイトリストもしくは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 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)

6.3.2.1　何故ローカル･ホワイトリストに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**

　残念なことですがここ数年、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。

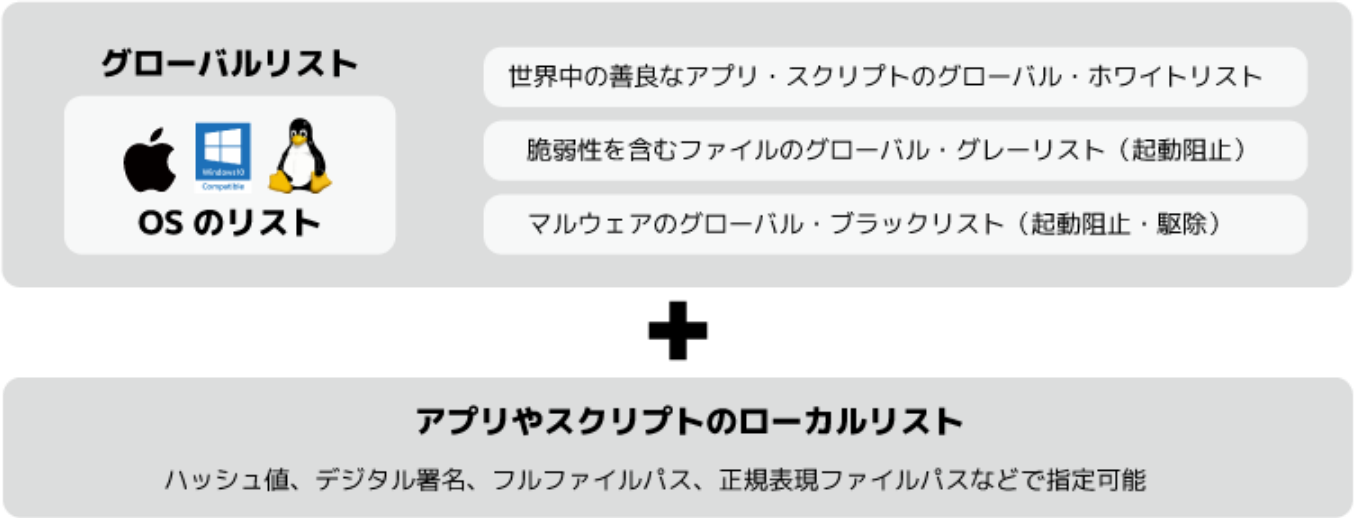
6.3.3　ブロックされたアプリケーションを該当パソコンからローカル・ホワイトリストへ追加

6.3.2.1 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 などで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。

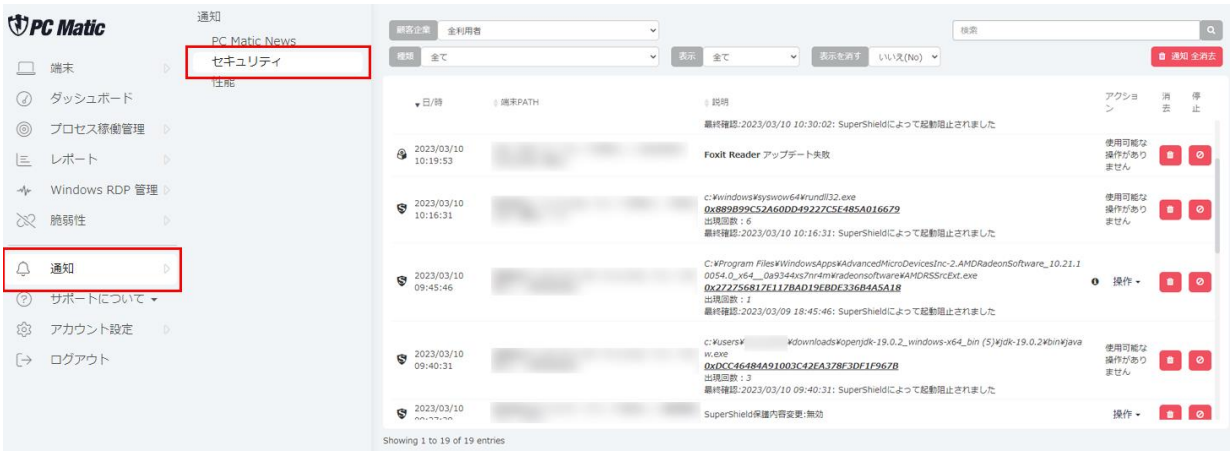
!!! ウイルスに感染、または情報流出の危険性があります!!!



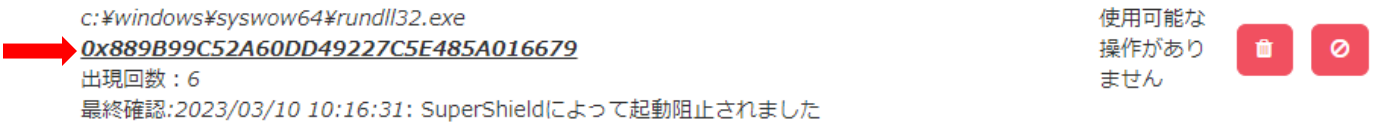
6.3.4 「通知」-「セキュリティ」からローカル・ホワイトリストへ追加

アプリケーションが起動阻止された場合は、以下の簡便な方法で迅速に登録することができます。
基本的にはアプリケーションもスクリプトも「プロセス稼働管理」より詳細を把握した上で登録します。

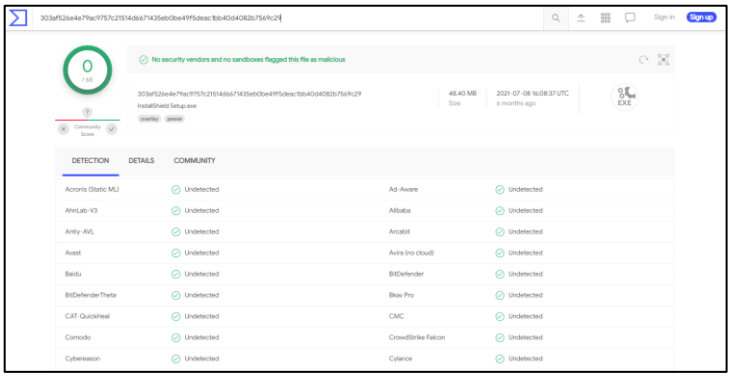
1. 管理ポータルの「通知」-「セキュリティ」には、起動阻止されたすべてのアプリケーション・スクリプトに関する情報が表示され、アカウント全体で起動阻止されたファイルの把握が迅速に行えます。



2. 起動阻止されたファイルのうち、バイナリー形式のものはここから迅速に追加することがでます。まず、太字で表示されている MD5 ハッシュ値をクリックするとそちらをクリックすると、VirusTotal が開きます。Cmd.exe, Wscript.exe, powershell.exe,run32dll.exe はスクリプト形式ですので、「プロセス稼働管理」から行います。(後述)



3. 開いた VirusTotal をセカンドオピニオンとして活用します。



マルウェア疑いがある場合は、3 つ程度のセキュリティソフトが警告を表示することがありますので、参考にしてください。

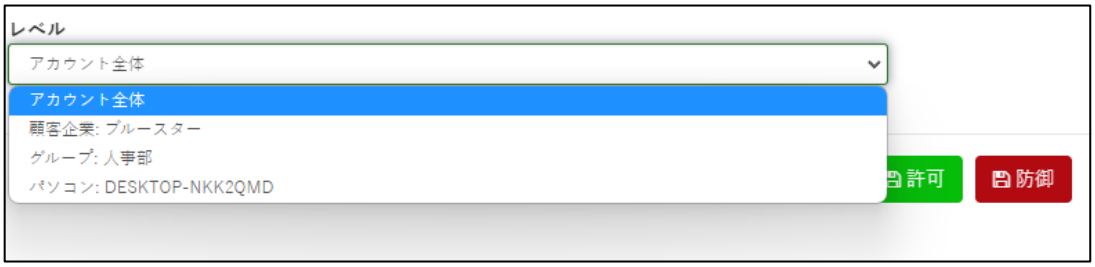
ここに掲載されているセキュリティソフトは、新種マルウェアの検知能力は高くありません。

またセキュリティホール(脆弱性)はウイルスでないため、Undetected と表示されますが悪意あるものにパソコンを乗っ取られるリスクがあります。

これらのセカンドオピニオンにより、個別ホワイトリストへ追加するかを判断します。

4. 「アクション」のプルダウンで、適用を行う組織の範囲を決定します。組織の範囲を大きくすることで、アタックサーフェスが大きくなりますので、全社員など大きなレベルでの許可は極力避けてください。

この操作で、適用範囲のレベルにある端末へ即座に起動許可がなされます。ただし、マルウェアと認定済ファイルの場合は、追加が許可されず「PC Matic サポートへ連絡してください」という主旨のメッセージが画面上部に表示されます。誤検知であると思われる場合は、PC Matic サポートへ至急ご連絡ください。



6.3.5 「EDR プロセス稼働管理」を用いてアプリケーション・スクリプトを詳細に把握し、起動許可する

「通知」-「セキュリティ」の画面から、起動阻止されたアプリケーションやスクリプトの起動可能制御を行う際、企業名などをクリックし、該当企業を選択した後、メニューの「プロセス稼働管理」タブを押し、二段目メニューの「EDR プロセス起動阻止」を選択して、起動阻止されたファイルの一覧を取得します。

一覧の一番左にある「緑の十字」アイコンを押すと情報が拡大表示されます。

現在の識別状態が「不明」となっているものが、まだ PC Matic マルウェア分析官によるデジタルフォレンジックが完了していないファイルとなります。「悪質」はマルウェアと認定済のものです。
「善良」となっているものは、健全と分類済ですのでホワイトリストへ追加する必要はありません。

「拒否/許可」タブを選択し、ホワイトリストへ追加します。「レベル(全社/組織/端末)」およびホワイトリストの制御方法を指定することが可能です。

スクリプトファイルの場合は、「スクリプト」のみ選択が可能となります。

【バイナリー形式のホワイトリストの制御方法】

大

危険度

小

ファイルパス指定:デジタル署名がされていない頻度が高く改変されるプログラム

デジタル署名指定:デジタル署名にて許可を包括指定できます。社内開発アプリに便利です。

MD5 指定:バージョンアップされるたびに MD5 は変化しますので強固な守りになります。

7　保護レベルの包括管理設定

保護レベルは社員個々に行うとウイルスに感染する危険性がありますので、設定は管理者に限定して運用されることを強く推奨いたします。

7.1　SuperShield のオプションを管理者が包括して行う場合

1. https://portal.pcmatic.com/　にアクセスし、ログインします。
2. 「アカウント設定」を押し、表示されたメニューから適応対象の部署があれば選択し、「SuperShield オプション」を押します。

3. 社内で利用する場合は下記の設定をお勧めいたします。

保護モード:SuperShield 保護

脆弱性適用：有効（自動）

EPP 制御の利用：無効(推奨)

起動阻止ファイル通知：保護警告非表示（初心者/社内）

Java ランタイム: 拒否

USB 大容量デバイス：許可

Windows Defender: 許可

社内で USB メモリや SD カードなどの USB デバイスの使用を禁止している場合は、「USB 大容量デバイス」を「利用」にすると、USB マスストレージデバイス(Windows でドライブ名が付与される記録装置)を使用できなくすることができます。

この画面にて設定変更を行った場合は、パソコンを再起動して変更箇所を有効化してください。

8 ソフトウェア制御(プロセス稼働管理・脆弱性対策)

8.1 プロセス稼働管理

1. https://portal.pcmatic.com/ にアクセスし、ログインします。
2. 表示された画面で「プロセス稼働管理」－「全プロセス」を選択します。

3. デジタル署名の有無などから絞込も可能です。悪質なアプリケーションの多くはデジタル署名やカタログ署名がなされていませんので、絞り込むことで悪質なものを発見しやすくなることもありますが、悪質なものもカタログ署名されていることもありますので注意が必要です。
4. プロセス名の緑色の「+」アイコンをクリックすることで、そのプロセスの詳細、「プロセス詳細(MD5)」「端末詳細」「拒否/許可」を閲覧することができます。

5. 「プロセス詳細」では、MD5 や署名状況などを把握することが可能です。MD5 を用いて VirusBulettin にて悪質なプロセスであるかのセカンドオピニオンを取得可能です。

6. 「端末詳細」では、実際に起動させた端末を把握することが可能で、粗悪なフリーソフトウェアなどをダウンロードして実行しやすい従業員を把握し、セキュリティ教育を行うべきかなどの判断指標にも役立ちます。

7. 「阻止/許可」では、社内で利用するのにふさわしくない場合に、「阻止」へ追加することができます。ファイルハッシュ(MD5)によって指定する方法と、特定のディレクトリにて稼働する実行可能ファイルを指定する方法から選択できます。ファイルハッシュであれば、特定のバージョンのみ指定され、ファイルパス指定であれば、更新されたものも起動阻止に指定することが可能です。デジタル署名を持つものは、ここでデジタル署名による包括ホワイトリスト指定が可能です。社内開発アプリケーションが起動阻止されることがなくなります。
なお、マルウェア分析官によって既にマルウェア指定されているものは追加することができません。その旨のメッセージが表示された際は、詳細な情報を PC Matic サポートまでご連絡ください。

8.2 脆弱性適用

著名アプリの自動更新を行うかをアプリ毎に設定する事ができます。また、自動アップデートを行いたくないバージョンがある場合は、そのバージョンに自動でアップデートしないようにする事もできます。

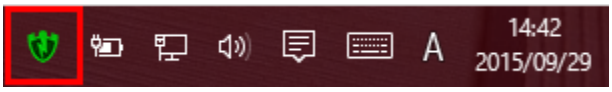
1. https://portal.pcmatic.com/ にアクセスし、ログインします。
2. 表示された画面で「アカウント設定」を押し、表示されたメニューで「脆弱性適用」を選択します。

3. 自動更新しないアプリがある場合は、「Toggle」を選択すると灰色になり、自動更新がされなくなります。また、「最大バージョン値」に更新しないアプリのバージョンを入力するとそのバージョンのアプリは更新されなくなります。

9　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。なお、こちらの設定を行うとウイルスに感染するリスクが増加しますので、社員の方には設定を変更しないように告知をお願いいたします。

- 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・ブラックリスト、ローカル・ホワイトリストの管理



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。

- 制御ファイルを取得中です。
  制御ファイルのダウロードには、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。

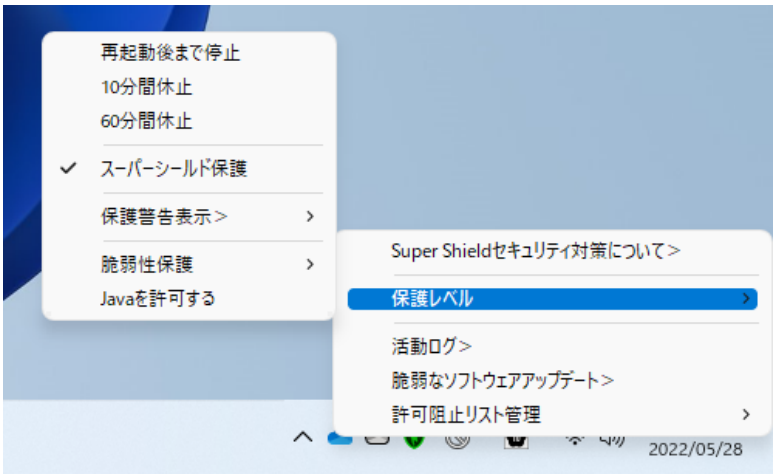
- 再起動が必要な場合
  セキュリティエンジンの自動更新により再起動が必要です。再起動を行ってください。
- ライセンスの期限が切れている場合
  ライセンスの更新を行ってください。

9.1 保護レベルの設定(非推奨)

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るモードを選択することが可能です。ウイルス感染リスクがあるため、本機能を法人で利用することは非推奨としています。

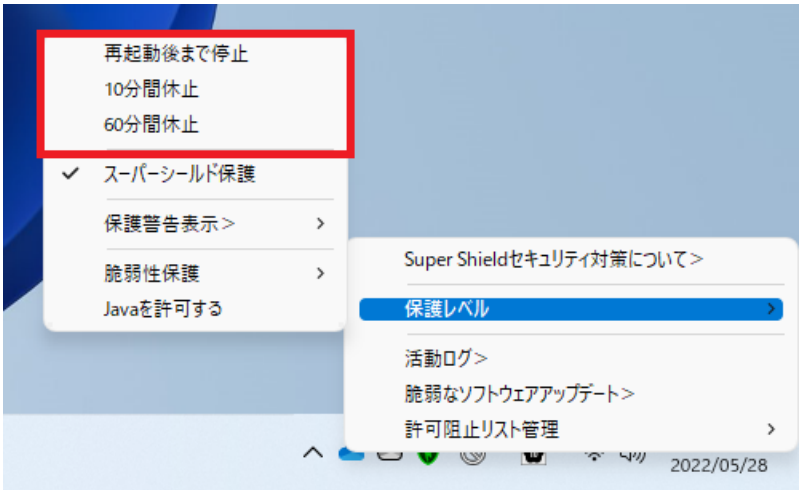
保護レベルの設定では、SuperShield の一時休止を行うことや、保護警告の表示の設定、脆弱性保護の設定の設定が行えます。社内用途ではデフォルトで設定されている「スーパーシールド保護」のご利用を強くお勧めいたします。

なお、これらの設定変更は社員の方が行えないようにしておくことをお勧めいたします。(後述のオプションにて設定可能です)



9.1.1 SuperShield の一時休止

基本的に本モードは使用しないようにしてください。

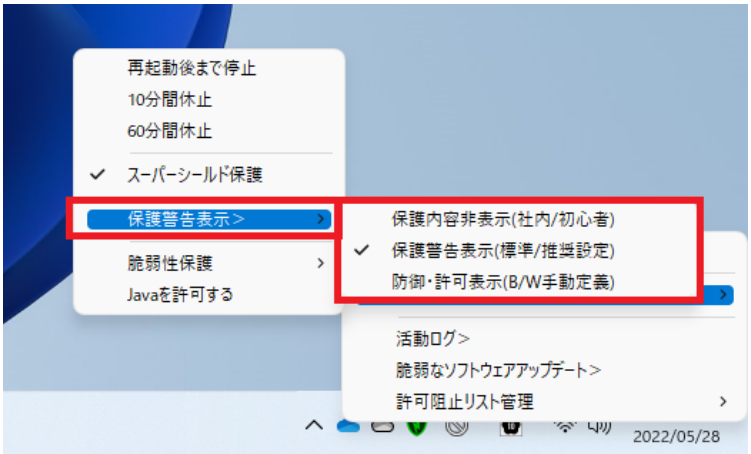


9.1.2　保護警告表示

企業内で利用する場合は、「保護内容非表示（社内/初心者）」をご使用ください。社内問い合わせによるシステム部門の手間が減少します。

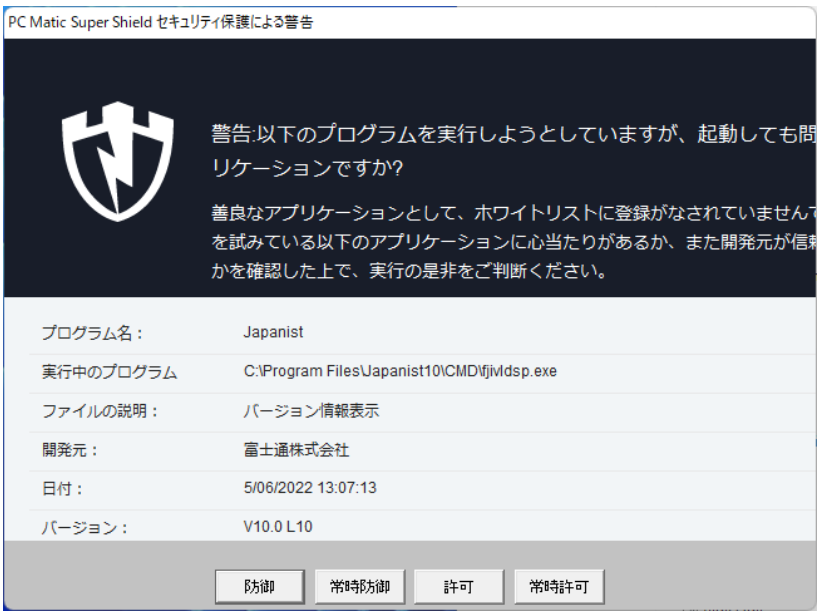
「防御・許可表示（B/W 手動定義）」を選択すると、手動でローカル・ホワイトリスト、ローカル・ブラックリストへ追加する事ができます。こちらは、自作ソフトや社内で利用されているオリジナルアプリケーションを使用する際にご使用ください。

「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すすめいたします。



「実行・阻止の表示」を選択している場合は、グローバル・ホワイトリストやグローバル・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 時間以内にグローバル・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ます。
ご自分で開発したアプリケーションや信頼のおける発売元が出荷している CD-ROM などで配布される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。

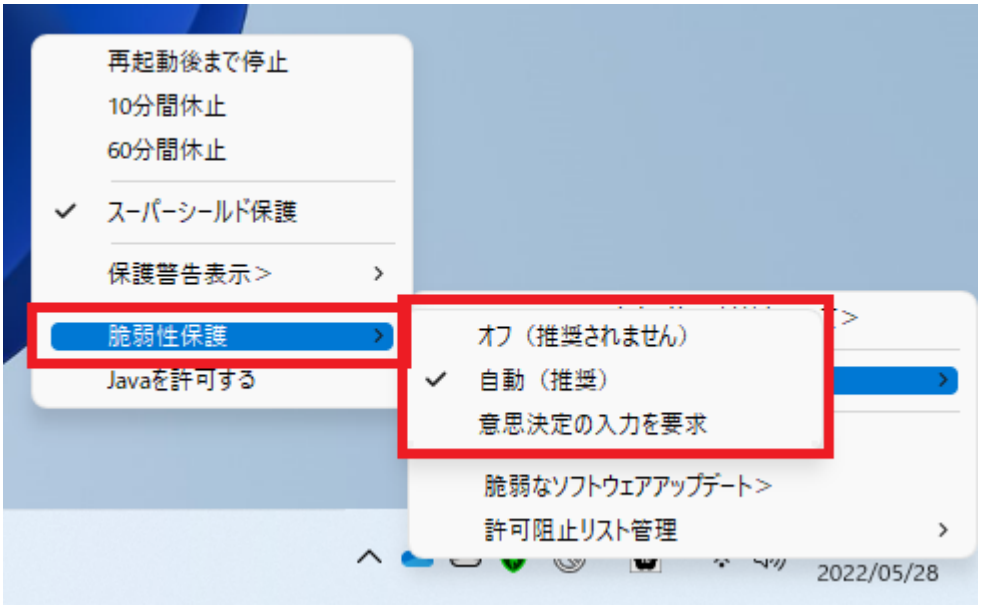


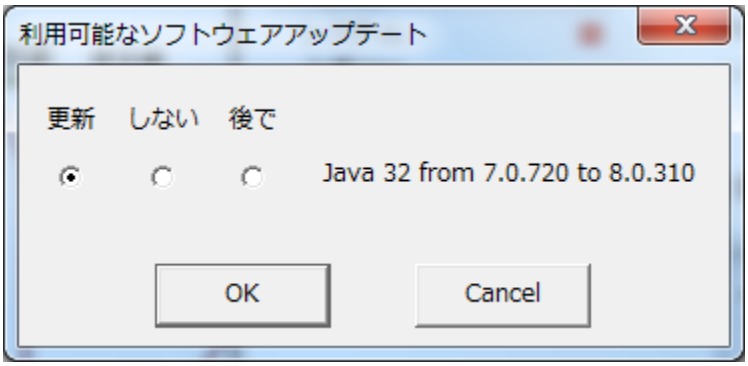
9.1.3　脆弱性保護

通常はデフォルトで設定されている「オン」をご使用ください。

特定のバージョンの Adobe AIR 等でしか動かない社内アプリケーションがある場合は「オフ」を選択してください。ただしセキュリティホールが発生いたしますので、社内でファイアウォールの整備が行われている環境でのみご使用ください。

「意思決定の入力を要求」を選択すると、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。





10 ライセンスの確認・副管理者の追加（アカウント情報）

ライセンスが正しく投入されていて、日付が合っているかをご確認ください。もし日付等が間違っている場合は、ご購入元にご確認ください。

ライセンスは 1 年から 5 年の範囲でお買い求め・更新いただけます。複数年次の場合は長期割引が適用されます。

また、副管理者の追加では、追加した管理者の権限を選択した部署のみ閲覧や編集できる等の細かい設定を行う事ができます。

支払設定・マスター管理者の追加画面を表示するには、管理ポータルより「アカウント設定」－「アカウント詳細」を選択してください。

10.1 ライセンスの確認

「ライセンス認証キー」の箇所でライセンスが正しく投入されていて、日付が合っているかをご確認ください。もし日付等が間違っている場合は、ご購入元にご確認ください。

10.2 副管理者の追加

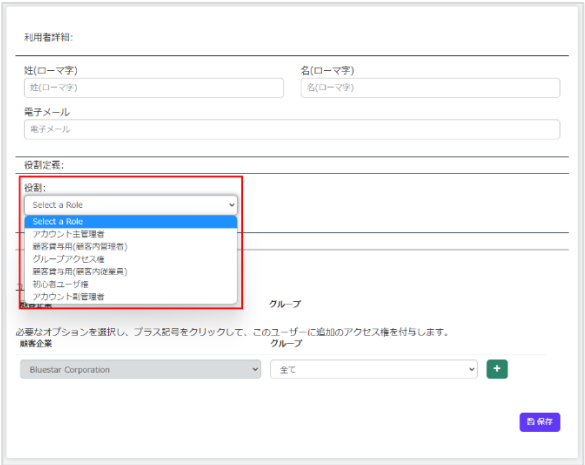
管理者毎に必要なアクセス権限を指定して運用を任せることができます。

PC Matic コンシューマ版および法人版等においてアカウントを作成済の場合には追加を行うことができません。その際は別のメールアドレスにて管理をお願い致します。追加の有無が不明な場合は、パスワードの再発行を依頼し、アカウント作成の有無を確認することができます。https://pcmatic.jp/faq/run/08/

1. 管理ポータルで「アカウント設定」を押し、表示されたメニューで「管理者登録」を選択し、右側の画面で「ユーザー追加」を押します。

2. 「ユーザー追加」を押します。

3. 姓名や電子メールを入力します。
役割定義を行っている場合は、どの役割を管理者に追加するかを選択し、「保存」を押してください。



4. 追加が完了するとユーザーが管理者リストに追加されます。管理者二要素認証(2FA)をオンにすると、その事業所およびその端末でのみ管理ポータルへのアクセスが可能となりセキュリティ性が高まります。ただし、端末が破損した場合は管理ポータルへのアクセスが一切行えなくなりますので、複数の管理者登録を行った上でご利用ください。

10.3 副管理者の期限日が経過した際

副管理者のアカウントにて 90 日以上ログインがない場合はアカウントが無効化されます。アカウントの主管理者により、該当の副管理者のアカウントにある「有効」のスライダーを有効にして再度アカウントを有効化してください。

10.4 管理者二要素認証(2FA)

「アカウント設定」-「管理者二要素認証(2FA)」にて、管理者二要素認証(2FA)を有効化にすると、管理ポータルへログインする際に、Google Authenticator, Microsoft Authenticator 等を用いて認証を 2FA 化させることができ、セキュリティ性が高まります。また接続情報が記録されます。マスター管理者アカウントへは、二要素認証(2FA)を有効化して運用されることをお勧めします。

【導入ステップ】

① 「アカウント設定」→「二要素認証(2FA)」→「二要素認証(2FA)を有効化」ボタンを押す
② ポップアップした QR コードを「Google Authenticator」「Microsoft Authenticator」の「QR コード読込」で読み込みます。
③ 認証アプリで表示された認証コードを PC Matic 側の画面に入力します。

11 管理ポータル

https://portal.pcmatic.com/にアクセスすると管理ポータルが表示されます。この画面では下記の事が行えます。

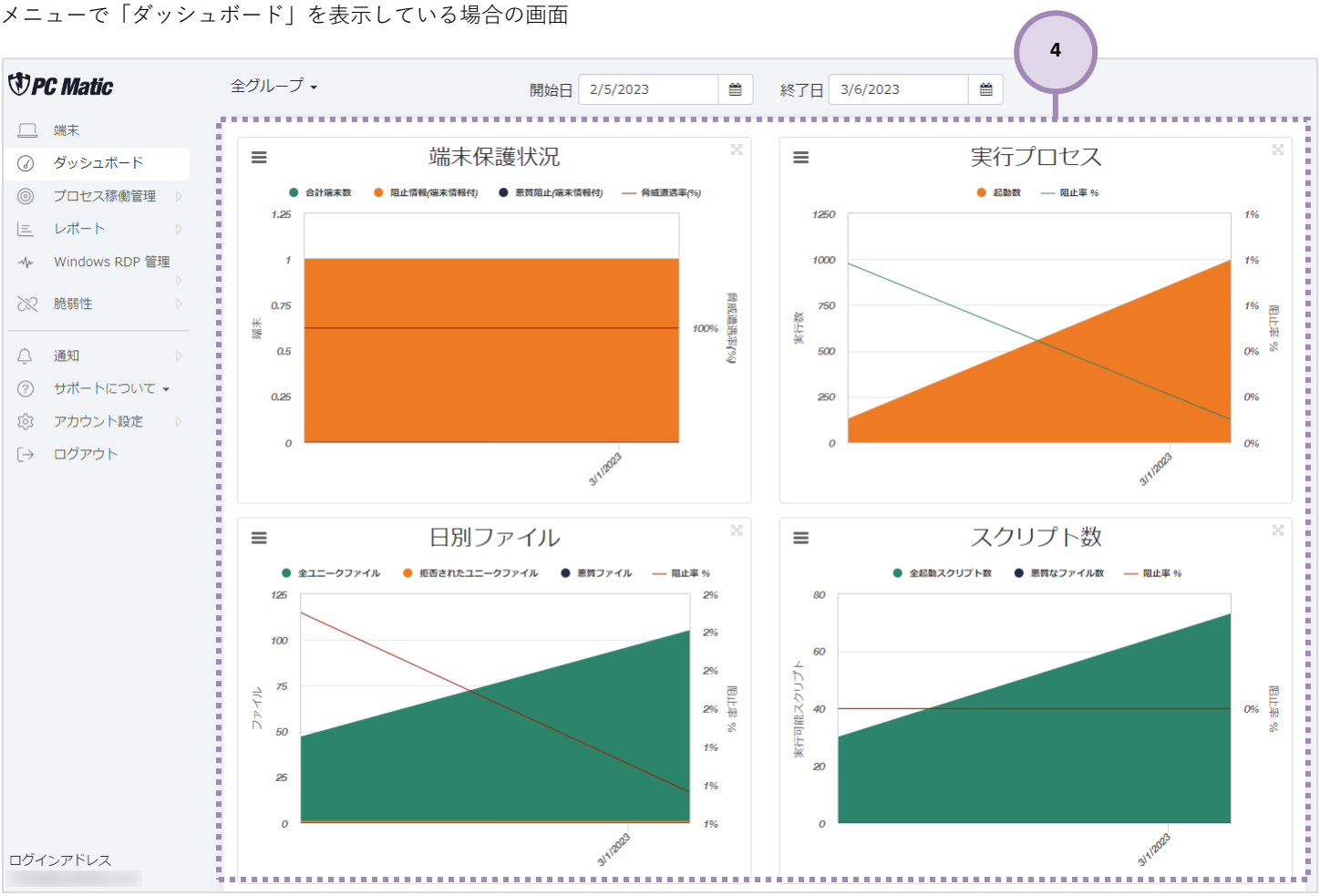
◆「端末」ページ場合

メニューで端末ページを表示している場合の画面

① メニュー。緑色になっているところが、現在表示されているページです。
② 登録されている端末が表示されます
③ 検索窓に端末名を入力して、端末を探しやすくなります。

◆「ダッシュボード」ページの場合

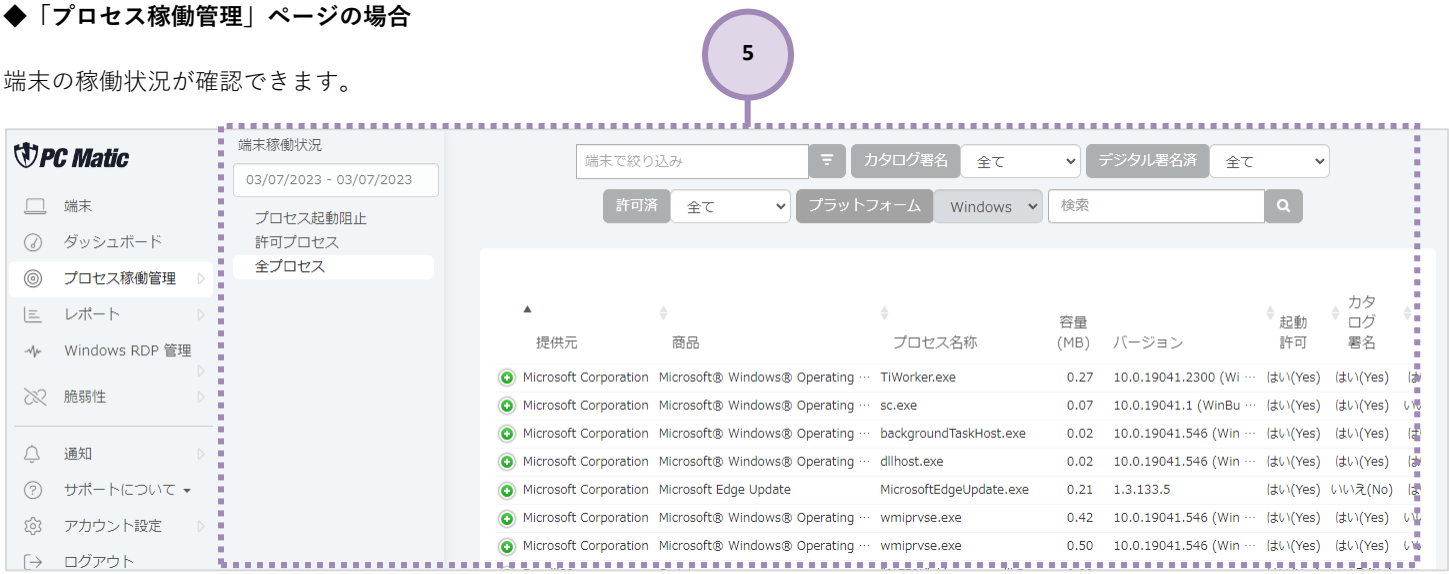
メニューで「ダッシュボード」を表示している場合の画面



④　実施内容（画面はセキュリティ状況タブの場合）端末保護状況、実行プロセス、日地別ファイル、悪質なスクリプト数をグラフで確認できます。

◆「プロセス稼働管理」ページの場合

端末の稼働状況が確認できます。



⑤　左側のメニューを押すと、最新プロセス、直近の阻止プロセス、直近の許可プロセス、過去のプロセス、過去の阻止プロセス、過去の許可プロセスを確認する事ができます。

◆「レポート」ページの場合

メニューで「レポート」を表示している場合の画面

⑥　レポートを PDF 形式で出力

⑦　レポートの Excel 形式での出力

⑧　管理対象にしている各パソコンの利用状況が把握できます。デフォルトでは全期間を表示しています。レポート日を選択すると、指定した期間のレポートを表示する事ができます。

◆「Windows RDP 管理」ページの場合

Windows Professional 版以上に標準搭載されている「Windows RDP」は、昨今悪意のある者からの攻撃対象にさらされているため、PC Matic はこの機能を「無効化」しておくことを強く推奨しております。

業務上やむを得ない場合は、利用が想定される時間や特定の接続元端末に限定して接続を許可されることをお勧めします。これらの特定端末の指定および時間帯による接続は、こちらの機能より設定していただけます。

接続が想定されない端末については、必ず「無効化」してあることを再確認ください。

また、接続された際の接続履歴を本機能でご覧いただけます。覚えがない接続があった場合は、悪意のある者からの接続の可能性があるため、至急パスワードを変更するとともに、Windows RDP による運用を見直してください。

⑨　RDP ライフラインの設定やログの確認等をする事ができます。
　　「有効なセッション？」の「？」は接続されているとマークが変わります。

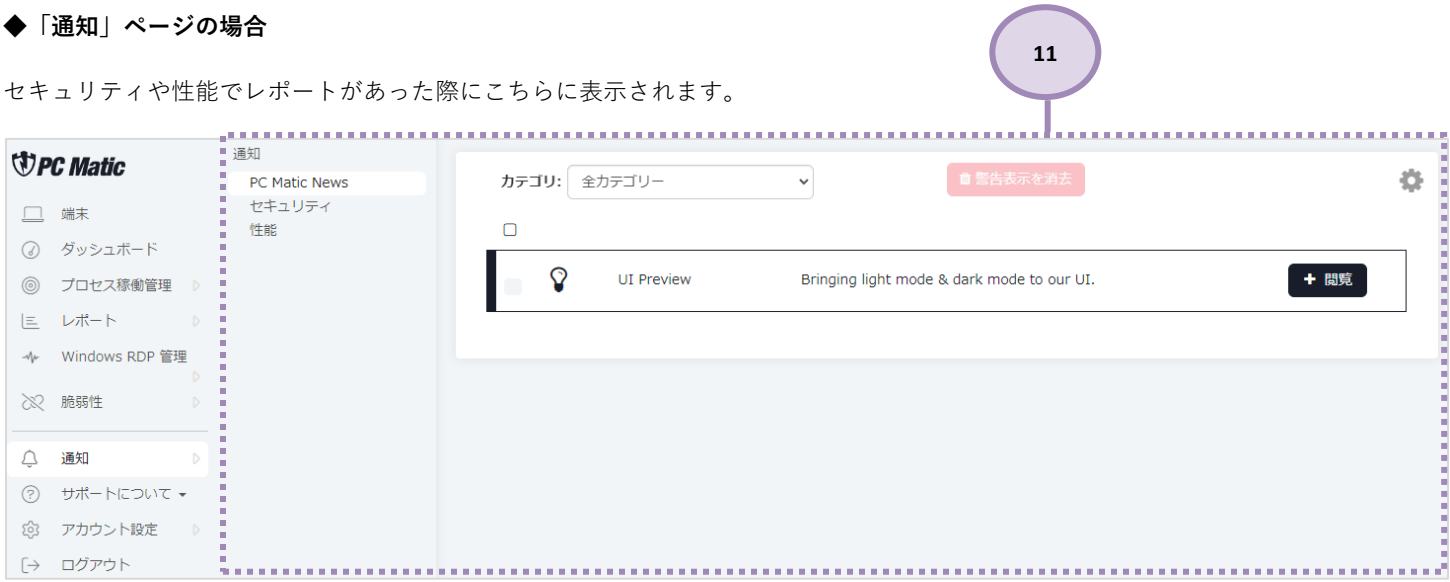
◆「脆弱性」ページの場合

メニューで「脆弱性」を表示している場合の画面

⑩　脆弱性のある端末があった場合にこちらで表示されます。

◆「通知」ページの場合

セキュリティや性能でレポートがあった際にこちらに表示されます。



⑪　アラートがある場合、こちらに表示されます。ウイルス報告などの主要なアラートに関しては、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。

11.1 管理対象 PC レポート

管理対象にしている各パソコンの利用状況が把握できます。デフォルトでは全期間を表示しています。レポート日を選択すると、指定した期間のレポートを表示する事ができます。

11.1.1　セキュリティ概要

管理しているパソコンでどのようなセキュリティ関連の動作が行われたかを記載しています。
項目名をクリックすると、項目毎に昇順、降順に並べ替えられます。

11.1.2　メンテナンス概要

　管理しているパソコンでどのようなメンテナンスが行われたかを機能ごとに記載しています。
項目名をクリックすると、項目毎に昇順、降順に並べ替えられます。
こちらの概要はスキャンを行わないと情報が追加されません。毎週スキャンを行うことを推奨いたします。

11.1.3　ハードウェア資産管理

　組織で利用している端末メーカーやモデルを一覧形式で確認する事ができます。本機能は、EDR 診断(スキャン)を実施した際に更新されます。
左側の「＋」ボタンを押すと利用者などの詳細を確認することができます。左上の EXCEL アイコンを押すとデータを CSV 形式で出力することができます。この情報は過去スキャンした情報が反映されるため、初期スキャンが行われていない端末は表示されません。

11.1.4　ソフトウェア資産管理

PC Matic は、「ソフトウェア資産」という機能を 2 つ装備しています。

一つは、「レポート」-「ソフトウェア資産リスト」(SAM)という項目にて、OS にて管理されているアプリケーション一覧を把握する機能です。インストーラーを利用しないフリーソフトウェアなどはこちらの一覧には表示されないことがありますが、この機能は、主に有料ソフトウェアのライセンス管理や社内未確認のソフトウェアを容易に発見するために用います。

もう一つは、メインメニューにある「ソフト資産管理」というタブで SWAM と呼んでいます。これは、端末内にある全ての実行可能ファイルを把握・制御する機能になります。グローバル・ホワイトリスト保護モード運用時は、潜在的に起動阻止される実行ファイルを把握するもの、ローカル・ホワイトリスト保護運用モード時は、ローカル・ホワイトリスト作成のために用います。

本機能では、組織内の端末にインストールされているソフトウェアの一覧表をご覧いただけます。本項目のソフトウェア資産管理にリストアップされるソフトウェアは、Windows の「設定」-「アプリ」-「インストールされているアプリ」に表示されているソフトウェア一覧で EDR 診断(スキャン)を実施した際に最新情報へ更新されます。インストールを必要としないフリーソフトウェアやパソコン内に直接複写するなどして保管された実行可能ファイルは、こちらでは検出されませんのでご注意ください。実稼働を確認することができる「EDR プロセス稼働管理」と併せて利用することで組織内でのアプリケーション利用実態を完全に把握することが可能です。

一覧表のアプリケーション名称左側にある「＋」ボタンを押すとインストール済のパソコン名などの詳細が表示されます。
この情報はスキャンを行うことで更新されるため、アンインストールやインストールをしても EDR スキャンを実施しなければ更新されません。このため、毎週 1 度のスキャンを実施して、本情報の更新をお勧めいたします。

ソフトウェア資産管理

NAME	QUANTITY	# OF VERSIONS
Google Chrome	1	1
Microsoft Edge	1	1
Microsoft Edge Update	1	1
Microsoft Edge WebView2 Runtime	1	1
Microsoft Update Health Tools	1	1
PC Matic Ad Blocker 1.4.3.0	1	1
PC Matic Agent 1.2.18.0	1	1
PC Matic Super Shield 3.0.47.0	1	1
PushController 1.4.44.0	1	1
Windows PC 正常性チェック	1	1

Showing 1 to 10 of 10 entries

11.2 登録した端末の管理

1. 管理ポータルで「端末」メニューを押すと登録されている端末が表示されます。

2. 表示されたパソコンをクリックすると詳細な情報を表示する事ができます。
画像は「端末の状態」を選択した場合です。表示されている CPU、RAM、DISK のメーターは、数値がおおよそリアルタイムで更新されています。

11.2.1　一覧 表示時のアイコンの説明

各パソコンに表示されているアイコンの説明は下記の通りです。

ステータス

パソコンの電源が OFF になっています

パソコンの電源が ON になっています

SuperShield がインストールされていません

SuperShield のシグネチャを更新しています

SuperShield がインストールされています

アラートがあります

アラートはありません

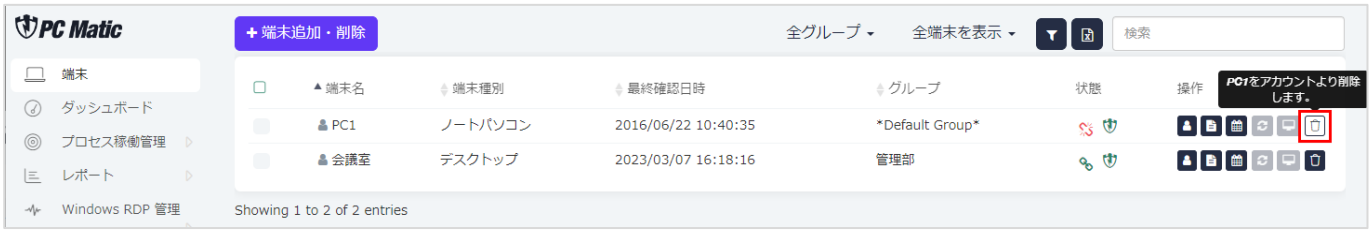
11.2.1　端末操作

操作メニューを選択すると、右側の窓に操作が表示されます。なお、遠隔操作に関連する機能を行う際は、ログインしたいパソコンの電源が入っていないと、操作メニューに「リモートデスクトップ」メニューが表示されませんのでご注意ください。電源オンの識別は、ほぼリアルタイムで行われます。

11.2.2　登録したパソコンを削除する

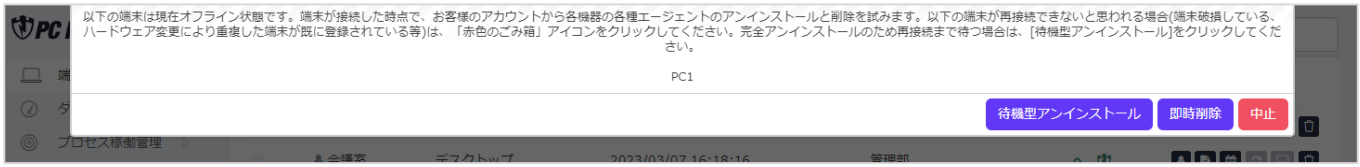
端末一覧より削減します。削除することでライセンス枠が空きます。

1. 左側メニューの「端末」をクリックし、端末一覧画面を表示します。先ほどアンインストールを行った端末をもう利用しない場合は、端末管理上から削除し、ライセンスを開放します。
2. 日本のお客様は、アンインストール作業実施中にシャットダウンしたり、再起動したりするケースが多数見受けられ、正常にアンインストールされない事象がございます。管理ポータルから端末が即座に消去されますが、アンインストール作業はバックグラウンドにてサーバーからアンロックキーを入手しながら 15 分程度かけてアンインストールが実行されます。



3. 「実施してよろしいですか？」と聞かれたら、「了解」を押してください。

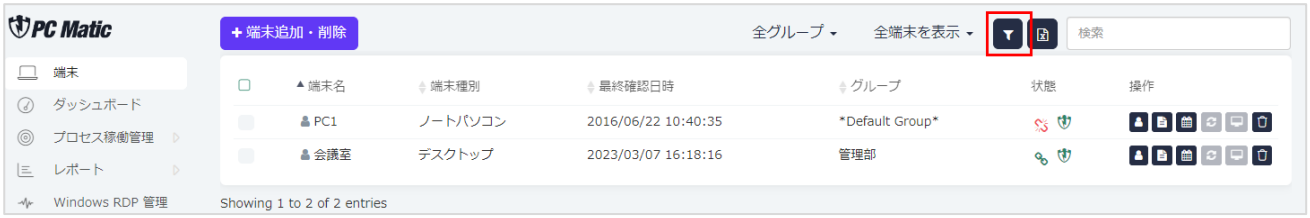
4. オフライン時は、以下の画面が表示されます。
「待機型アンイントスール」は、端末の電源が次回投入された際に、PC Matic PRO に関連するプログラムをアンイントスールし、続いてライセンスを開放します。
「端末解除」は、破棄したパソコンのライセンスが即座に開放されますが、アンインストールは実施されません。



11.2.3　パソコン一覧からの絞り込み

1. 導入アプリケーションの把握、Windows update の最新版が適用されているかなど、様々な条件で調査対象となるパソコンの絞り込み表示を行うことが可能です。
   絞り込み情報は、最新の EDR 診断結果を反映しています。しばらく診断が実施されていな場合は、現状と異なることがあります。また、EDR 診断が実施されていないパソコンは絞り込み表示にて表示されませんので、ご注意ください。

   管理ポータルで「端末」メニューを押すと登録されているパソコンが表示されます。
   端末が表示されたら「　　」ボタンを押します。



2. 表示された「端末の絞り込み」画面で絞り込みたい項目を入力し、「絞り込み適用」ボタンを押します。
   下記の画像の場合は、OS ビルドが最新のものではないものと、OS が Windows 10 のものを AND 検索し、最新にアップデートしていないパソコンを絞り込んで表示しようとしています。

11.2.4　端末リスト表示時のアイコン

端末をリスト表示している際のアイコンの意味は下記の通りです。


管理名称を指定します。


メモを入力できます。


定期診断のスケジュールの確認、追加、削除ができます。


電源がオンの場合に、リモートデスクトップでログインできます。


アカウントより端末を削除します。

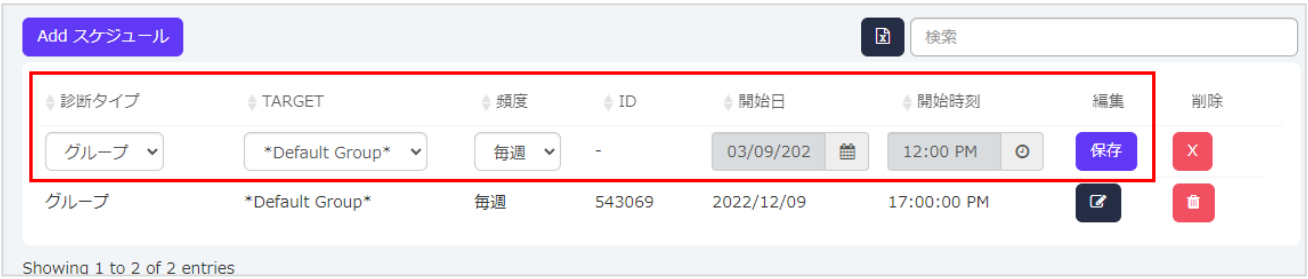
12 アカウントの包括的な EDR 診断スケジュール作成

アカウントの包括的なスケジュールを作成します。EDR 診断は、毎週 1 回程度実施されるよう設定することをお勧めしています。毎日実施すると端末のストレージへの負担が大きく、パソコン寿命を早く迎える可能性が高まります。指定時刻は、EDR 診断実施トリガーの一要素であり、端末の負荷が高い状態など様々な要因でその指定時刻から 30 分、平均 15 分程度の範囲内で実施が開始されます。実施中は、端末の「端末の状態」において、オレンジの PC Matic サーバーと緑色のパソコンが表示されている右下のアイコンにおいて、緑色のパソコン上部に黒色で目玉のようなアイコンが表示されます。このアイコンが表示されるまでは、1 分程度要します。

1. 管理ポータルで「アカウント設定」を押し、表示されたメニューから適用対象を選択し、「包括スケジュール設定」を押します。

2. 「Add スケジュール」ボタンを押します。

3. 診断タイプ、Target、頻度等を設定し、「保存」ボタンを押します。



13 ローカルホワイトリストの管理

新たなアプリケーションが起動阻止された場合は、1 日お待ちください。マルウェア分析官によるデジタルフォレンジック終了後に自動的に起動できるようになります。

自社開発したアプリケーションで監査が必要ない場合は、こちらに登録してください。

なお、社内ツールを作成する際は、Windows コンパイル時にアプリケーション開発名とベンダーシグネチャを入力してください。入力されていない場合は、unknown となり、審査に時間がかかります。

※インターネットからダウンロードしたソフトをこちらから登録することは、ウイルス感染リスクが非常に高まりますので、行わないでください。

※信頼のおけるアプリケーション（市販ソフト）で起動阻止された場合は、ローカル・ホワイトリストへ追加しで起動してください。

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。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。

13.1 設定方法

1. 管理ポータルから「アカウント設定」を押し、表示されたメニューから適用企業と「ローカルホワイトリスト」を選択します。（防御されたものを許可する場合は、「ローカルブラックリスト」を選択します。）

2. ローカル・ホワイトリストから除外したいものを「削除」ボタンを押します。

13.2 ローカルリストのアルゴリズム解説

PC Matic SuperShield エンドポイント保護(EPP)は、端末内のキャッシュファイルを参照し、そこにファイルの MD5 が存在していない場合、PC Matic サーバー参照を行います。オンライン状態で参照に成功した場合は、その分類をキャッシュファイルに登録します。オフラインの場合は、サーバー参照が行えないためキャッシュファイルにない MD5 を参照しようとした場合は、起動が拒否されます。

サーバーにて「Good(善良)」「Bad(悪質サーバー判定したものは、24 時間端末内のキャッシュのみ参照し、サーバー参照は行いません。「Unknown(未知・脆弱性含)」は、1 時間端末内のキャッシュのみ参照し、サーバー参照は 1 時間経過後に参照を行います。

管理者が管理ポータルよりローカル・ホワイトリストやローカル・ブラックリストへの追加した場合、その情報は端末へプッシュ通知にて即座に送信され、通常は 5 秒以内に起動が可能となります。即座に反映されない場合は、ファイアウォール装置によるパケット破棄か PC Matic サーバーが定期保守中であることが想定されます。端末から通信リクエストがないプッシュ通知であるためファイアウォール装置の IPS で外部からの通信として遮断される場合があるため、他社エンドポイント保護製品と同様に PC Matic サーバーが利用している IP アドレスをファイアウォール装置の除外 IP として登録する必要があります。

標準モードで長年運用していると、ローカル・ホワイトリストやローカル・ブラックリストが大きくなり管理がしづらくなることがあります。その場合は、ローカル・ホワイトリストであれば「現在の識別状態」に「Good」と表示されているリストを選択し「削除」を押してリストから除外し整理してください。除外したものは端末へ即座に通知されず、24 時間経過しキャッシュ有効期限が切れた際に参照されます。

このため、マルウェアを「ローカル・ホワイトリスト」に、善良なものを「SuperShield 防御リスト」へ追加してしまったものをリストから削除しても、24 時間はサーバー参照されないため誤登録したものはキャンシュ内で有効となったままとなります。

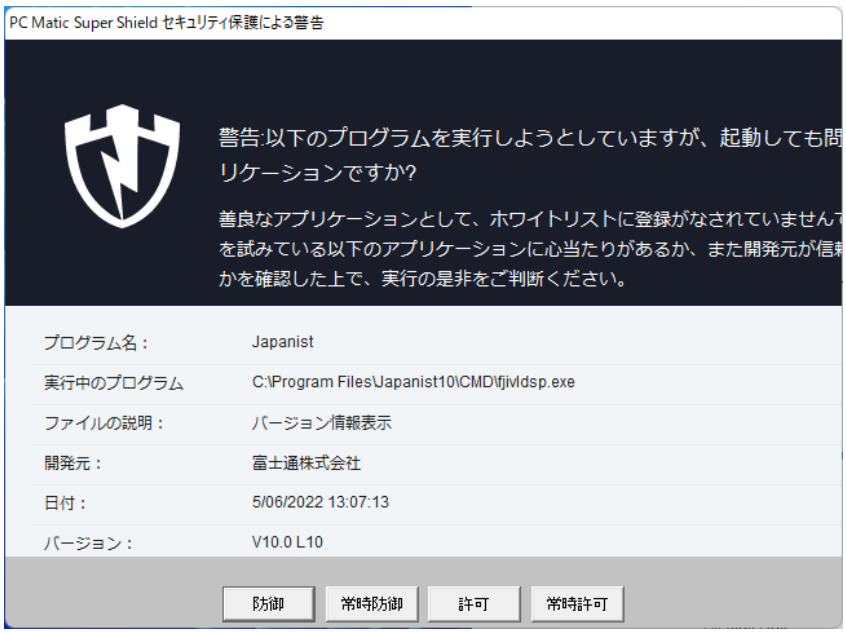
その際は、端末一覧の右にある「B/W 制御情報の再取得」を押すことで強制的に端末内のキャンシュ有効期限を無効化させて全件をサーバー参照させることができます。

13.3 ファイアウォール装置の制御がうまくいかず、個別のローカル・ホワイトリスト制御がうまく取得できない場合

PC Matic サーバーとの通信が正常に行えるよう、ファイアウォール装置へ除外 IP を登録していただくことが大前提ですが、緊急の場合は以下の方法にて端末内にキャッシュを作成することが可能です。

1. 管理ポータルより、該当端末を選択します。端末がオンライン状態の際に表示される「SuperShield オプション」を選択して「保存」を押します。以下の画面より「起動阻止ファイル通知」にて「許可・拒否リスト追加機能（B/W 手動定義）」に一時的に設定します。設定は即座に端末へ反映されます。

2. 起動がなされないアプリケーションを起動させます。以下の画面が表示されます。



「許可」を押すと一時的に起動許可がなされアプリケーションやスクリプトの利用が可能となります。「常時許可」を押すと端末内のローカル・ホワイトリストへ追加され、管理ポータル上の「ローカル・ホワイトリスト」に該当端末のみの許可が現れます。

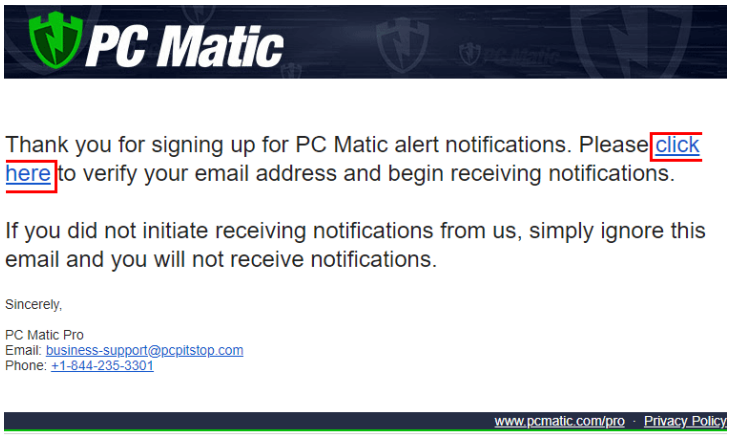
14 アラート送信先

管理関係者のアドレス帳の登録・修正等を行います。アラート通知先に登録する事によってアラートが送られるように設定する事ができます。

1. 「アカウント設定」を押し、表示されたメニューから設定を行いたい企業を選択し、「警告送信管理者」－「連絡先新規追加」を押します。

2. 「利用者名」と「メールアドレス」を入力して「保存」を押します。

3. 入力したメールアドレスにメールが届きますので、「click here」を押してメールアドレスを認証させてください。
承認させると、一覧に表示されている「認証状況」の項目が から になります。



14.1 アドレス帳の編集

アドレス帳に登録されている内容を編集する場合は、下記手順を行ってください。

1. アラート送信先の一覧より内容を変更したい項目で を押します。
2. 編集する項目を変更し、「保存」を押します。

14.2 アドレスの削除

アドレス帳に登録されている内容を削除する場合は、下記手順を行ってください。

1. アラート送信先の一覧より内容を削除したい項目で を押します。
2. 本当に削除してもいいかとメッセージが表示されますので、「OK」を押してください。

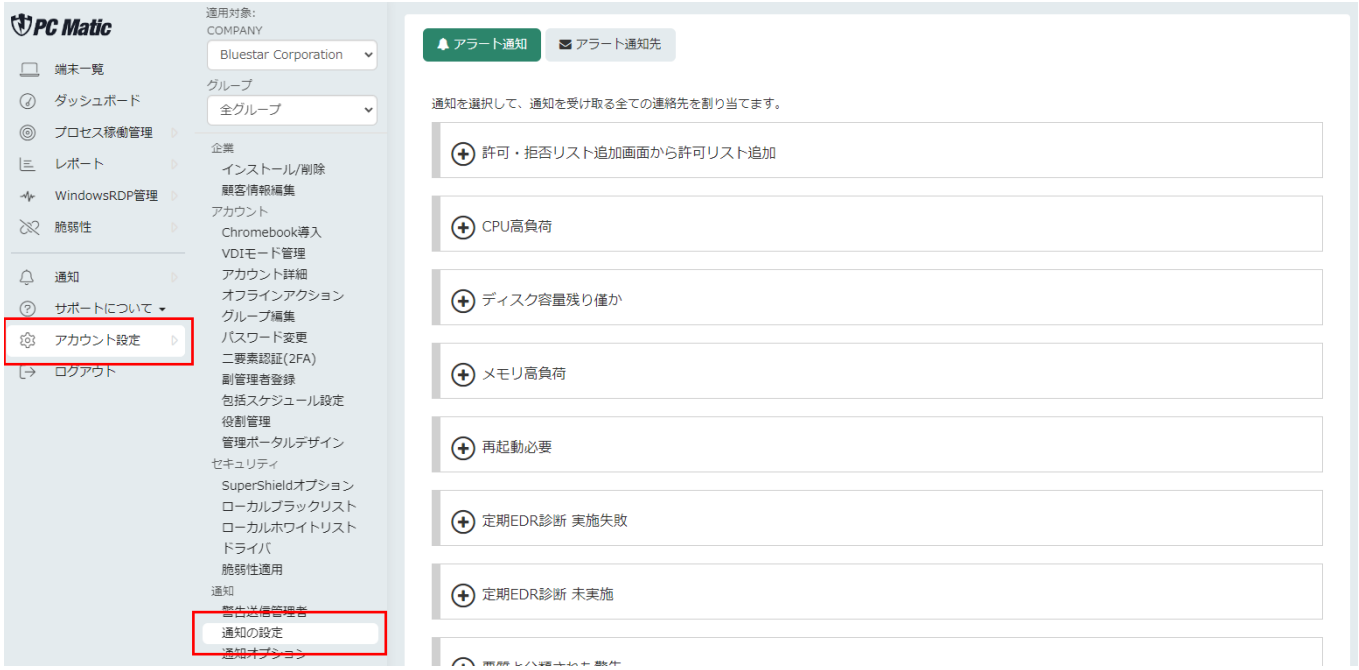
15 アラート通知

アラートの通知で以下の場合にメールでお知らせが届くように設定できます。

- CPU 高負荷状態　（高負荷）
- HDD の空き容量が少ない場合　（ディスク空間残少）
- メモリ使用率が高い場合　（高メモリ負荷）
- 再起動の必要性がある場合　（再起動必要）
- スケジュールスキャンが失敗した場合　（スケジュール実施失敗）
- スケジュールスキャンが動かなかった場合　（スケジュール未実施）
- ウイルスが検知された場合　（ウイルス検知）
- 古いアプリケーションのアップデートに失敗した場合　（脆弱性対策失敗）
- ファイアウォール装置にて通信が阻害されている可能性がある場合（SuperShield 制御ファイルが未完了）
- （管理対象として識別不能）
- （サーバーオンライン/オフライン）
- 未監査、もしくは悪質なものが検知された場合（SuperShield による起動阻止）
- SuperShield の通信がインターネットに接続しているが、サーバーと通信不良の場合（SuperShield 状況変更）

15.1 アラートを設定する

1. 管理ポータルのメニューで「アカウント設定」を押し、表示されたメニューから「通知設定」を選択します。



2. 通知方法を選択します。（画面の場合は、CPU 高負荷で追加しています）

3. アラートの送り先のメールアドレスを選択し、「連絡先を選択してください」を押します。
送り先は増やす場合は、  を押して追加してください。

4. 連絡先に先ほど選択した連絡先が追加されますので、通知間隔を選択し、「保存」を押します。

15.2 アラートの一時的な有効・無効 およびしきい値の変更を行う

1. 管理ポータルで「アカウント設定」－「通知オプション」を選択し、変更を行いたいアラートを設定し、「保存」ボタンを押します。

16 オフラインアクション

「アカウント設定」-「オフラインアクション」の項目には、オフラインであった端末への指示をいつ実施したかの履歴が記録されます。

- 「待機型アンインストール」を行った際、実際に適用された日時
  端末から PC Matic に関連するモジュールが自動的にアンインストールされます。

- 「端末の移動」を行い、組織やグループの変更指定が実際に端末へ適用された日時
  組織やグループの移動に伴い、ローカルホワイトリストの情報が変化することがあります。その変化した日時の把握にご利用ください。

- Windows RDP の有効化/無効化に関する日時
  本項目の設定変更には、端末の再起動や起動が必要になります。設定変更が適用された日時が記録されます。

17 リモートツール

ここでは、実際に PC Matic Pro を運用する際によく使用する操作について記述しています。

操作時は、該当パソコンの電源が入っている必要があります。電源が入っていない場合は表示されません。また電源投入時から実際の操作が可能になるまで 10 分程度を要します。

17.1 リモートツールの利用可否制御

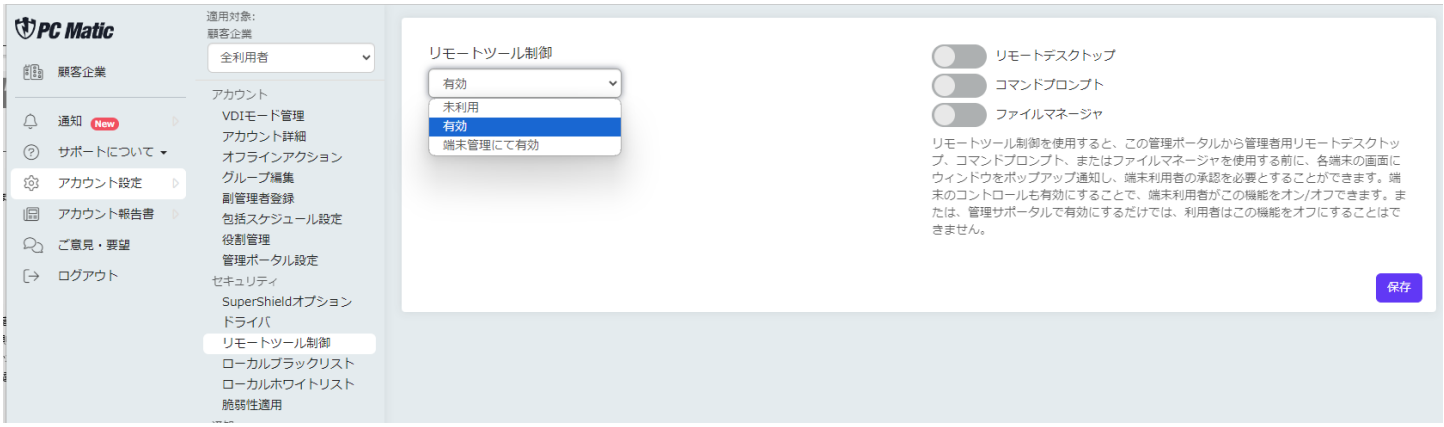
リモートツールは、デジタルサイネージや POS システムなどを集中運用することを念頭においており、管理者が端末に対して即座にリモート運用を行うことができる仕様となっています。しかし事務室での利用などの環境によっては、端末側の利用者により許可を得なければ運用上の問題が起きることがあります。そのような包括的な設定を「アカウント設定」-「リモートツール制御」よりコントロールの状態を「未利用」「有効(ポータルのみ制御可)」「端末からも有効(端末とポータルにて制御可)」から選択することができます。

「なし」を選択すると、端末へ即座にリモートツール利用することができます。

「有効」を選択すると端末側からも管理ポータルからもプロンプト表示の是非が制御できるようになります。

「端末からも有効」を選択すると端末側から「許可を得る、得ない」の選択がタスクトレイ上の SuperShield アイコンよりできるようになります。

なお、これらのプロンプト表示有無は、各端末のセクションからも個別指定が可能です。社長の端末のみプロンプト表示をさせるといった運用方法も良いかもしれません。



17.2 リモートデスクトップの使い方

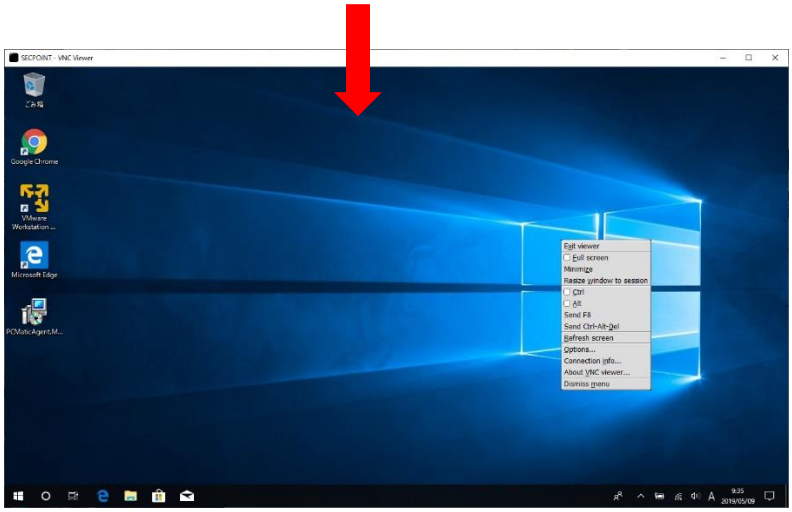
管理者用リモートデスクトップを行うには、操作するパソコン、操作されるパソコンの両方に PC Matic pro がインストールされている必要があります。PC Matic Agent にホスト側とクライアント側の機能が組み込まれているためです。このため操作する側のパソコンは、Windows である必要があります。ポート番号は 443 番ポートを利用しています。

リモートデスクトップの開始方法は下記の通りです。

1. 管理ポータルから「端末」メニューを選択し、リモートデスクトップで動作させたいパソコンの状態がオンかを確認します。
   オンの場合は、状態の鎖マークが緑色になっています。
   画像の場合は、端末名「会議室」の電源が入っている状態ですので、「会議室」を選択しています。

2. 「  リモートログイン」ボタンを押してリモートデスクトップを開始します。

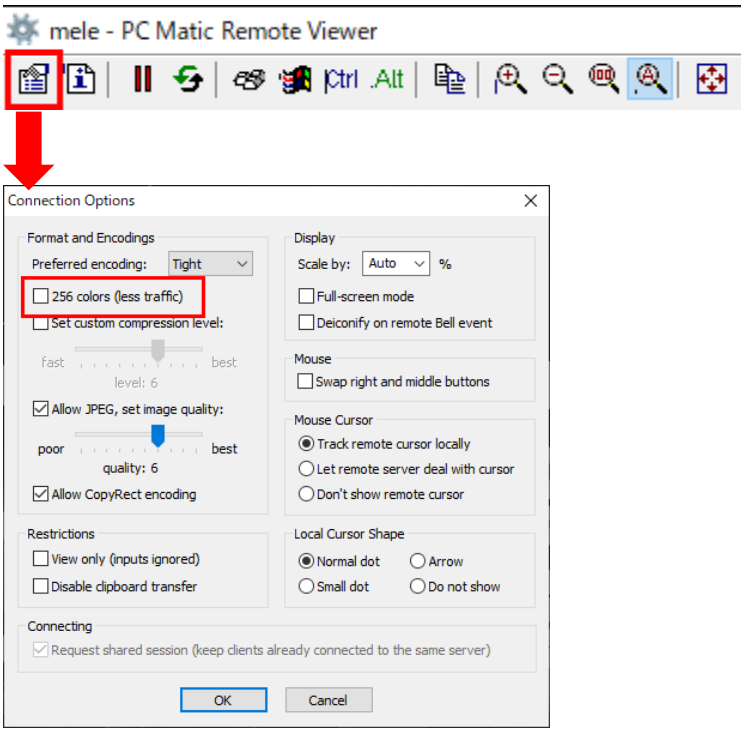
3. メッセージが表示されますので、「アプリケーションの起動」を押すとリモートデスクトップを行う事ができます。



フルスクリーン状態を解除するには、[Ctrl]+[Alt]+[Shift]+[F]を同時に打鍵してください。

17.3 リモートデスクトップの機能

リモートデスクトップが起動して、画面表示が重いと感じた場合は、ボタンを押して、表示された画面で「256 colors(less traffic)」にチェックを入れて「OK」ボタンを押してください。

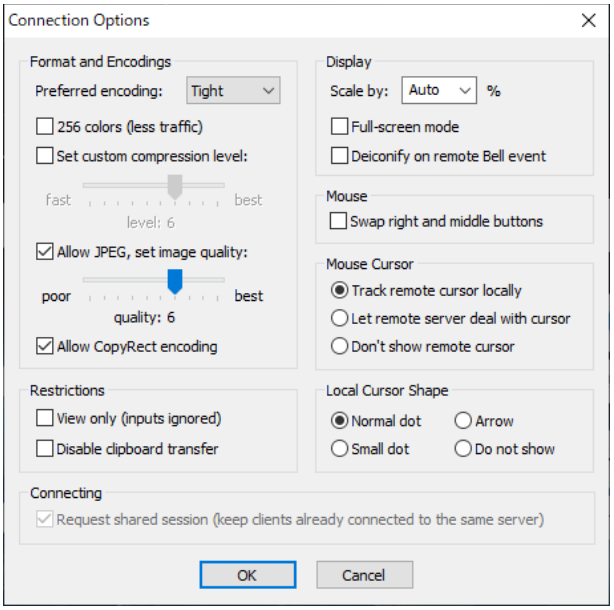


Ctrl + Alt + Del 信号は、Ctrl + Alt + Del + Shift

17.4 リモートデスクトップの設定

メニューから「Options...」を選択することで、リモートデスクトップをより快適にご利用頂ける設定変更ができます。

描画方法を変更することで、より微細な表現が可能な RAW なども選択もできます。Color level を 8 色の低画質にしたり、Custom compressopn level を「１」にしたりすることによって圧縮率が上がり、LTE 回線などでも快適にご利用いただけます。



17.5 パソコンの再起動

「再起動」を選択し、「端末名の再起動」ボタンを押すことでパソコンを再起動させることができます。

17.6 SuperShield の遠隔アンインストールとインストール

「B/W 制御情報の再取得」を選択し、「B/W 制御情報の再取得」ボタンを押すことで該当パソコンの導入済エンドポイントセキュリティ(SuperShield)をアンインストールや、未導入の場合はインストールを行うことができます。エンドポイントを再インストールする際にご利用ください。

17.7 コマンドプロンプトの実行

「コマンドプロンプト」を選択することで該当パソコンへのコマンドプロンプトを実行させることができます。サービスの削除、新しいプリンタドライバのインストールなどにご利用いただけます。

コマンドプロンプトは、32bit 系コマンド実行を前提としていますので、64bit 系のコマンドを実行する場合は、%SystemRoot%\sysnative\wuauclt.exe /resetauthorization /detectnow のように入力ください。

コマンド	説明
ipconfig	端末の IP 情報を確認
“dir /w”	ディレクトリを表示
cd	ディレクトリを移動
sc start	サービスを開始 (例: sc start “PCPitstop Realtime”)
sc stop	サービスを停止 (例: sc stop “PCPitstop Realtime”)
ping	IP アドレスへの PING
ver	Windows バージョンの確認
tasklist.exe	稼働中のタスクの確認
Taskkill /IM <taskname.exe> /F	タスクを強制停止
schtasks /delete /tn “task name” /f	タスクスケジューラーの削除
powershell -Command “restart-service ‘PCPitstop Scheduling’ -force”	PC Matic スケジューラの強制再起動（スケジュール実行がうまく稼働していない場合）
%SystemRoot%\Sysnative\msg.exe * Message goes here.	64bit 端末にメッセージを表示
%SystemRoot%\System32\msg.exe * Message goes here	32bit 端末にメッセージを表示

17.8 ファイルマネージャ

対象端末と操作端末の間でファイルのアップロード・ダウンロードを行う事ができます。なお、アクセス権限により、標準ではマイドキュメント傘下のディレクトリへアクセスは行うことができません。

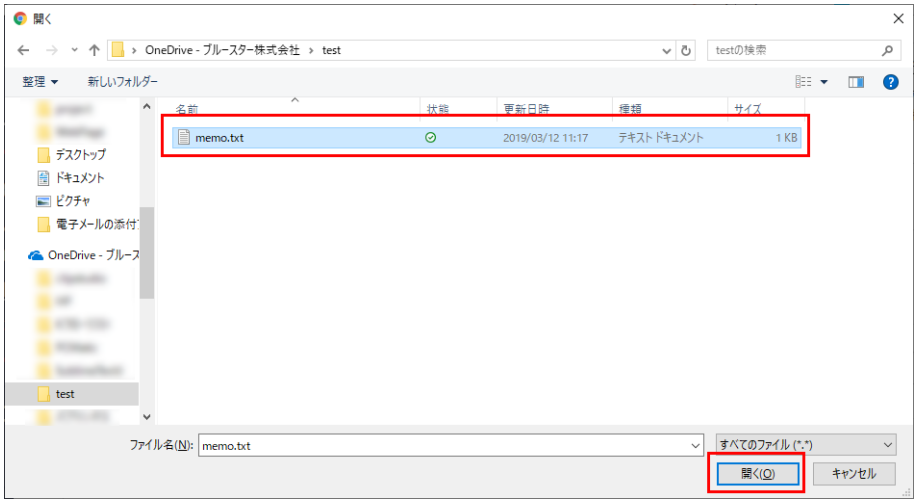
17.8.1　アップロード

1. ファイルをアップロードしたい端末に入ります。
2. 操作から「ファイルマネージャ」を選択します。

3. ファイルのアップロード先は、下に表示されているディレクトリになりますので、アップロードしたいディレクトリに移動します。

4. 「ファイルアップロード」を選択します。

5. アップロードするファイルを選び、「開く」を押します。選択したディレクトリにファイルがアップロードされます。



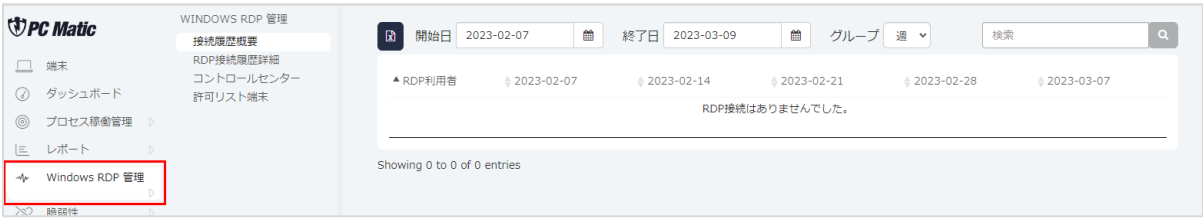
17.8.2 ダウンロード

1. ファイルをダウンロードしたい端末に入ります。
2. 操作から「ファイルマネージャ」を選択します。

3. 下の画面でダウンロードしたいファイルの右側にある「ダウンロード」ボタンを押すと、ファイルがダウンロードされます。

17.9 Windows RDP 管理（Windows RDP 有効化時刻制御・稼働履歴レポート）

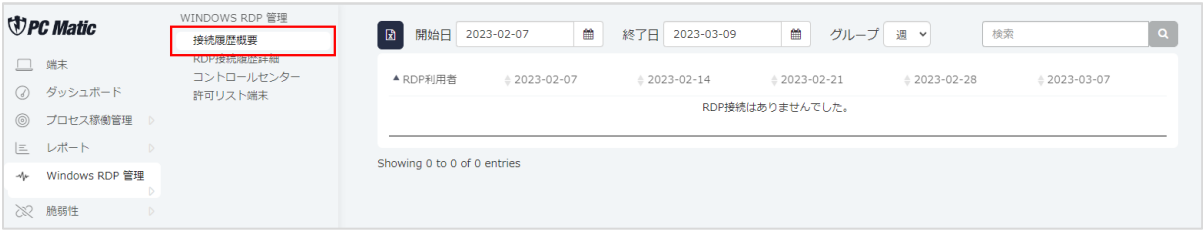
PC Matic PRO では、Windows RDP 有効化時刻制御 や稼働履歴レポートを管理する事ができます。
Windows RDP 有効化時刻制御・稼働履歴レポートを確認するには、管理ポータルの左側のメニューで「Windows RDP 管理」を選択します。



Windows RDP 有効化時刻制御・稼働履歴レポートでは「RDP 接続履歴概要」「コントロールセンター」「RDP 接続履歴詳細」「ホワイトリスト端末」を確認でき、端末リストや各端末のページなどを管理する事ができます。

17.9.1 接続履歴概要

接続履歴概要では、名前の通り接続履歴の概要を確認できます。



17.9.2　コントロールセンター

「コントロールセンター」では、現在アカウントにあるすべてのデバイスと各デバイスの RDP ステータス、スケジュール情報が表示されています。

管理ポータルの説明をします（上記画像）

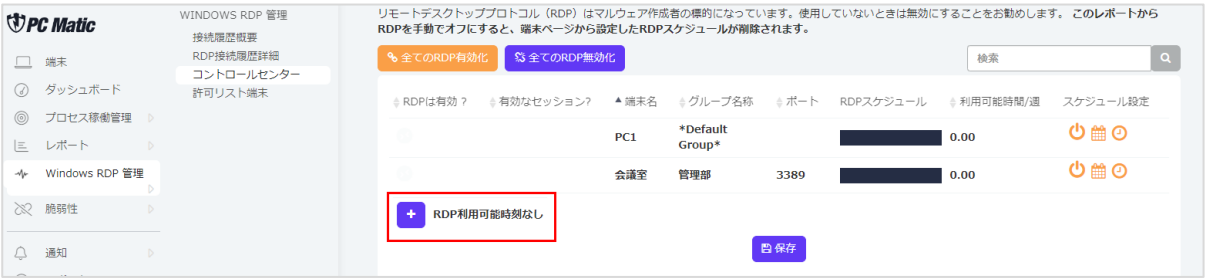
RDP は有効	アイコンがオレンジになっている場合は、RDP が有効になっている事を意味します。
有効なセッション	有効な場合は、緑色の目のアイコンが表示され、クリックすると現在のセッションに関する情報を表示されます。また、現在のセッションを終了する事もできます。
端末名	端末名が表示されます。
ポート	RDP が構成されているポートが有効・向こうに関わらず表示されます。
RDP スケジュール	各端末の RDP のスケジュールが表示されます。
利用可能時間/週	RDP が有効利用できる時間を表示します。
スケジュール設定	スケジュール設定が確認できます。

- **スケジュールの設定**

スケジュールの設定ではバーをオンにして緑色にすると RDP が有効になり、時計マークを押すと仮スケジュールが設定できます。定期的にスケジュールの設定を行いたい場合は、下記の設定を行ってください。

1. 右側にあるカレンダーのマークを押します。

2. 「RDP 利用可能時刻なし」の左側にある「＋」マークを押します。



3. まずは開始時刻を設定しますので、左側の入力欄の右側にある時計マークをクリックします。

4. 表示されたダイアログで矢印を押して開始時刻にします。時刻を合わせると、自動的に左枠の開始時刻が入ります。

5. 開始時刻と同様に終了時刻を設定し、「保存」ボタンを押します。

6. 保存されたメッセージが表示され、スケジュールにあるカレンダーが緑色になります。

17.9.3 RDP 接続履歴詳細

RDP 接続履歴詳細では、概要より詳細な履歴が確認できます。

17.9.4 ホワイトリスト端末

RDP に接続できる管理者の端末を登録します。設定後は接続される側の端末を再起動する必要があります。

RDP セキュリティを有効にし、端末のホワイトリストを制御できます。ソフトウェアを各端末にインストールすると、その端末を RDP ホワイトリストに追加して、ネットワーク上の任意の端末に RDP できるようになります。デフォルト拒否アプローチを使用すると、ホワイトリストにない端末や RDP セッションを開始しようとする端末がブロックされます。

また、リアルタイムでアラートを受信する事もできます。アラートの項目で必要であれば設定してください。

18 macOS 版

PC Matic PRO が macOS 版に対応いたしました。Windows で使い慣れた機能が mac でも使用できます。
macOS ではインストーラーを導入端末上の Safari からダウンロードした pkg を利用しない限り、マスター管理者の ID,パスワードの入力が求められます。このため、macOS への以下の方法にて実施ください。

事前に PC Matic PRO を導入し従業員に配布する場合

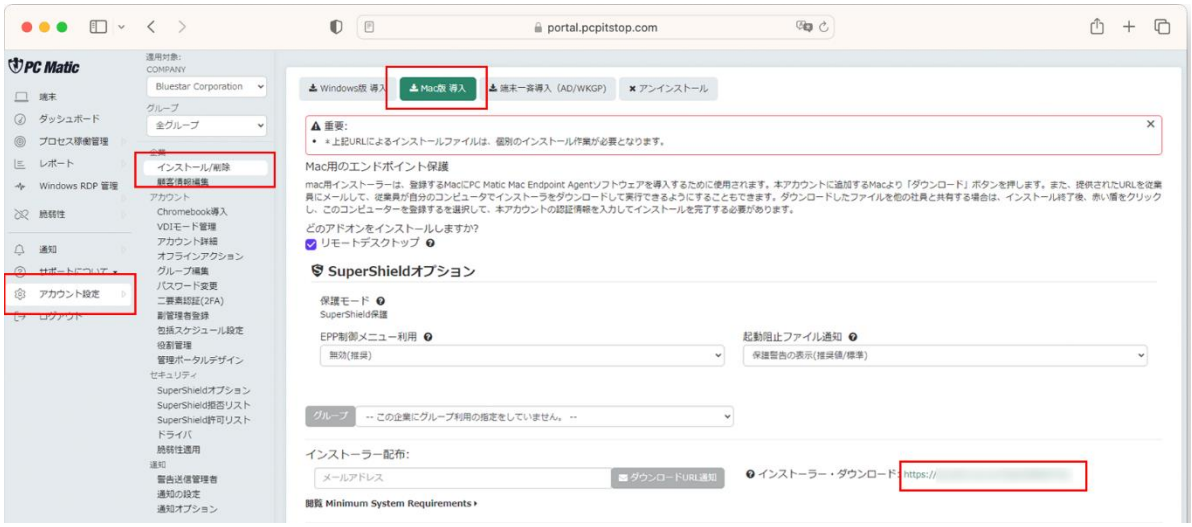
1. USB メモリにダウンロード URL を記載した TXT ファイルを格納し、その URL を USB メモリから Safari ブラウザーを開いてインストーラーパッケージを各導入端末にダウンロードし実行します。

従業員に PC Matic PRO を導入してもらう場合

1. 従業員へ事前に PC Matic PRO 導入のための手順を記した FAQ の URL を告知します。
2. インストーラー生成画面にあるショート URL を従業員に通知します。
3. 従業員により、インストール作業が行われているか管理ポータルより確認します。
4. 正しく導入されているか、「SuperShield ログ」の「起動阻止」を「全て」にして稼働状況を確認します。

18.1 インストール

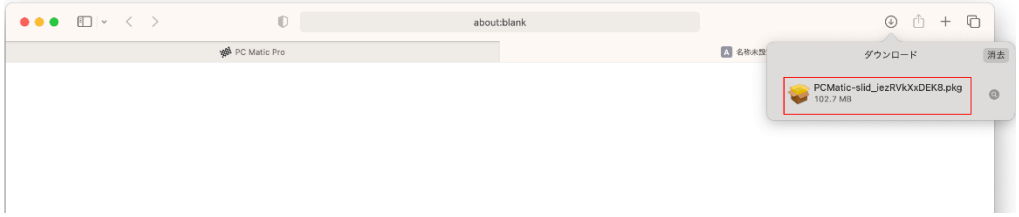
1. 管理ポータルを Safari で表示し、左側のメニューから「アカウント設定」－「インストール/削除」を選択します。
2. 表示されたダイアログで「Mac 版 導入」タブを押し、インストーラーをダウンロードさせたい企業と組織を選択して「インストーラー・ダウンロード」の URL を押して、pkg ファイルを mac にダウンロードします。



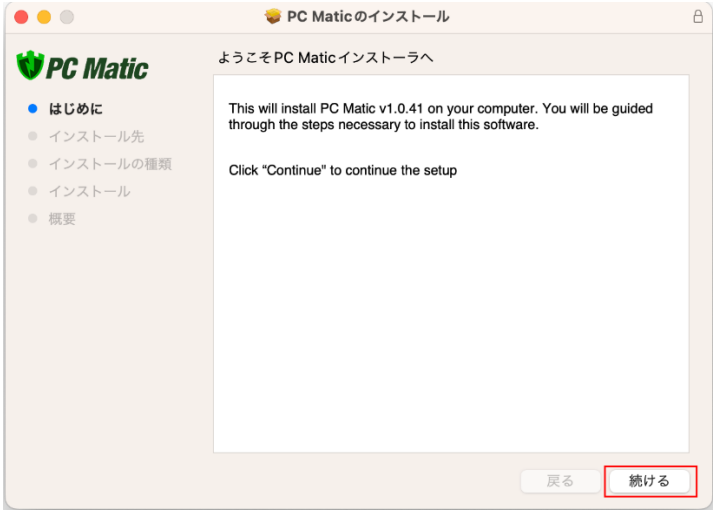
※Safari 以外のブラウザー、Chrome や Firefox で開くと正しくダウンロードできませんので、必ず Safari で行ってください。

※この URL をクリックせずに、PC Matic インストーラーを実行した際は、PC Matic アカウントの ID とパスワードの入力が求められます。

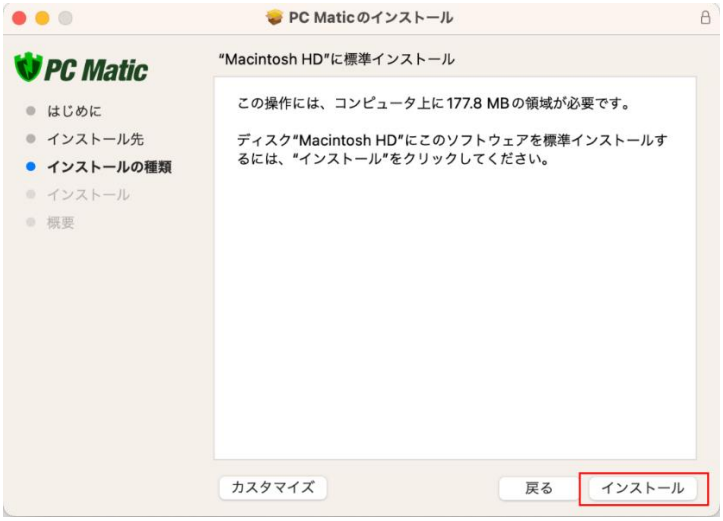
3. Safari の「ダウンロードを表示します」のボタンをクリックして、表示された pkg ファイルをクリックします。



4. インストーラーが起動します。
「続ける」を押します。



5. 「インストール」を押します。

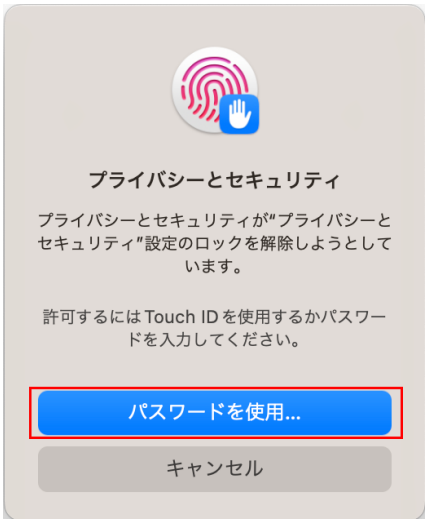


6. 「インストーラーが新しいソフトウェアをインストールしようとしています。」と画面が表示されたら、Touch IDかパスコードを使用して許可を行ってください。

7. 「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。

8. 「アプリケーション”PC Matic Tray.app”のシステムソフトウェアの読み込みがブロックされました。」の箇所にある「許可」を押します。

9. 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。

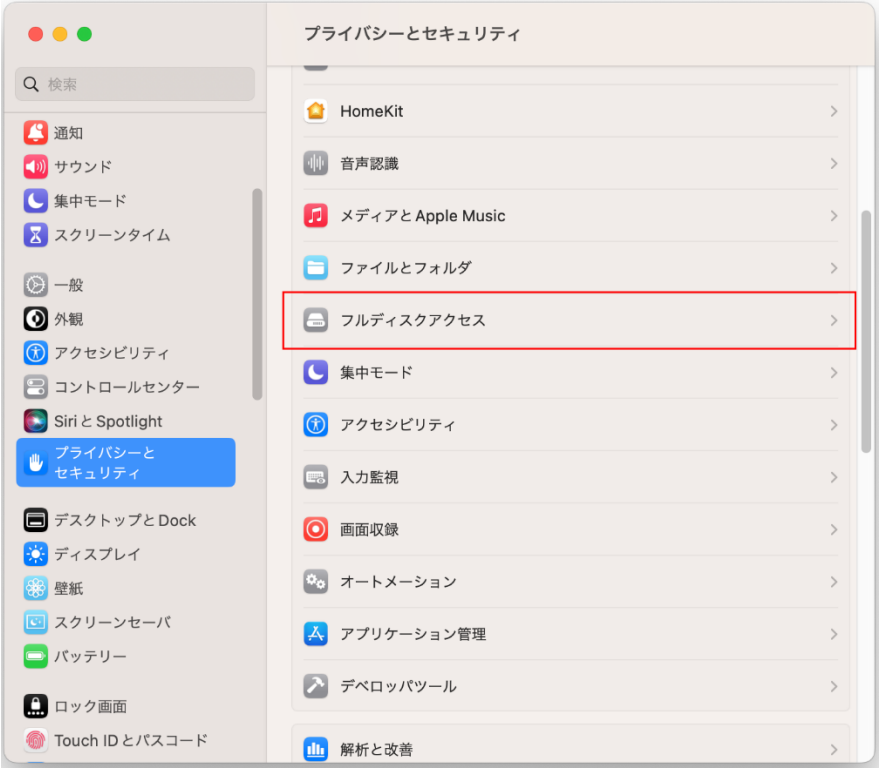


10. 「インストールが完了しました」と表示されたら、インストーラーの「閉じる」を押します。

11. インストーラーをゴミ箱に入れるか表示された場合は、「ゴミ箱に入れる」を押します。

12. デスクトップの通知は×マークを押して非表示にしてください。
また、インストールが完了すると、PC Matic の SuperShield アイコンがメニューバーに表示されます。

13. Mac の設定－「プライバシーとセキュリティ」を表示し、「フルアクセス」を選択します。



14. 「PC Matic System Extension」を右にスライドして有効にします。

15. 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。

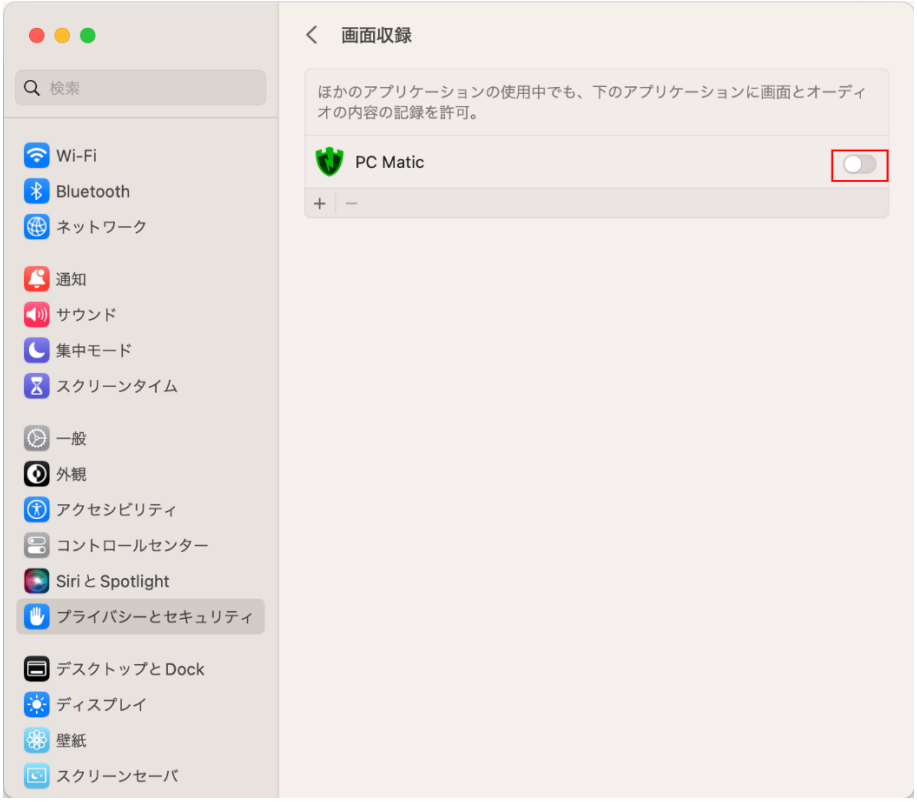
16. 管理ポータルにログインし、インストールした端末が表示されているかを確認します。

18.2 リモートデスクトップ時の許可

PC Matic PRO で macOS にリモートデスクトップを行う場合、プライバシー設定を有効にする必要があります。
以下の手順でプライバシー設定を有効にしてください。

1. スクリーンの記録についてプライバシー設定画面が表示されたら「システム情報を開く」を選択します。

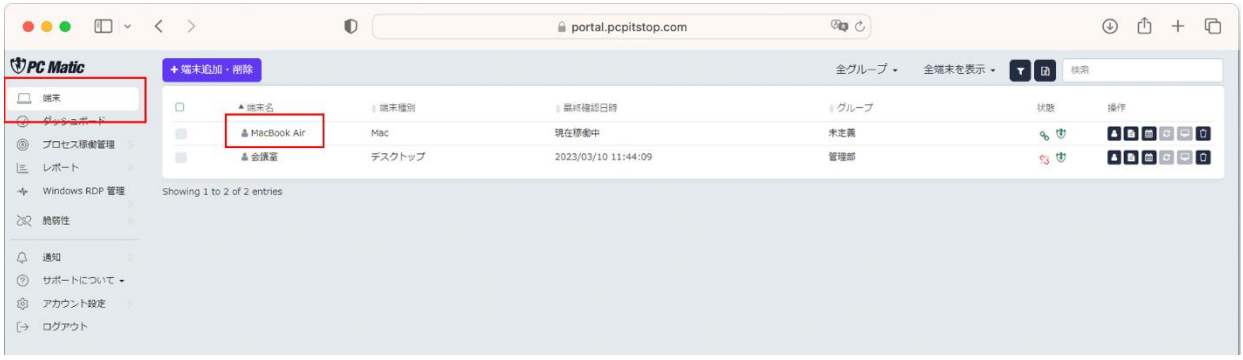
2. 「PC Matic」を右にスライドして有効にします。



3. 「終了して再度開く」を押します。メニューバーにある PC Matic の SuperShield アイコンが 1 度消えて再度表示されれば設定は完了です。

18.3 アンインストール

1. 管理ポータルを表示して、表示された画面で「端末」を選択し、アンインストールを行いたい端末名を選択します。

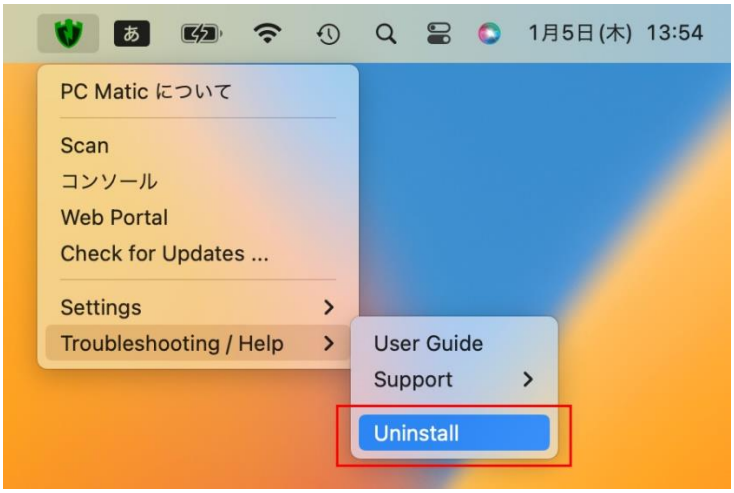


2. 「SuperShield オプション」を押します。

3. 「EPP 制御利用」の「無効（推奨）」を押して表示されたメニューで「有効（非推奨）」を選択します。

4. 「保存」を押します。

5. 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。

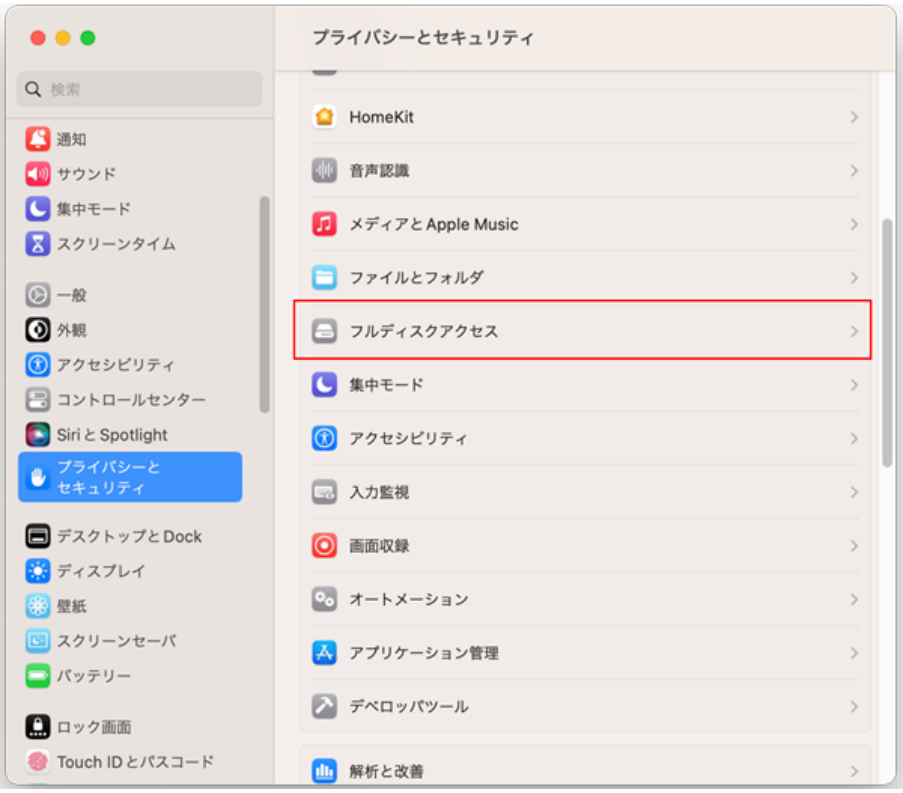


6. PC Matic のログインメールアドレス、パスワードを入力し、「アンインストール」を選択します。

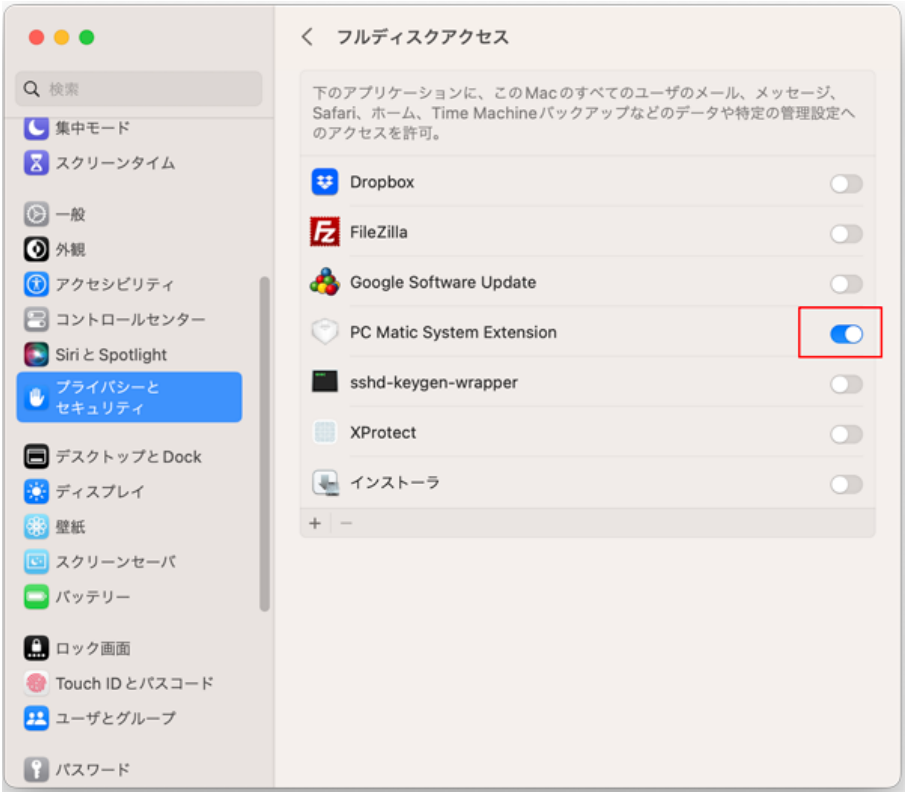
7. Mac にログインする際のユーザー名、パスワードを入力し「OK」を押します。

8. 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。

9. 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。



10. 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。



11. 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。

12. 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。

19 iPhone, iPad へのインストール

iPhone, iPad へのインストールは、App Store より事前にアプリケーションをインストールしておき、アカウント認証情報が含まれた URL を電子メールなどからクリックすることで、自動的に認証が実施されアプリケーションが利用できるようになります。
また、アカウント認証情報へは、企業アカウントおよび、グループの指定情報が含まれており、認証に成功すると管理ポータル上で端末が表示されます。

1. 管理ポータルで「端末」を選択し、表示されたメニューから「+端末追加/削除」をクリックします。表示された画面から「iOS インストール」タブを選択します。

2. 「グループ」を選択すると、「インストーラー・ダウンロード」のセクションに専用 URL が生成され表示されます。

3. 従業員へ導入手順の手引きなどを記載した FAQ や PDF と共に、この URL を従業員へ通知します。

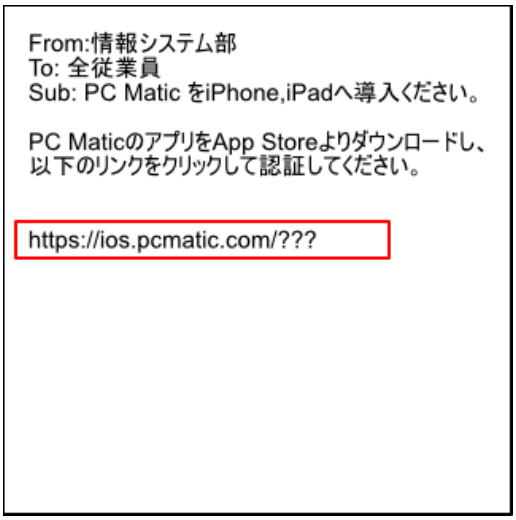
19.1 iPhone, iPad 導入ステップ

1. App Store から、PC Matic アプリケーションをダウンロードします。

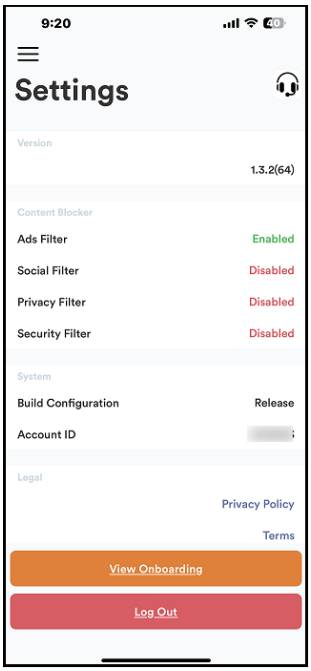
2. App Store から、PC Matic アプリケーションをダウンロードします。

3. 「拡張機能」にある「PC Matic」をスライドして有効化します。

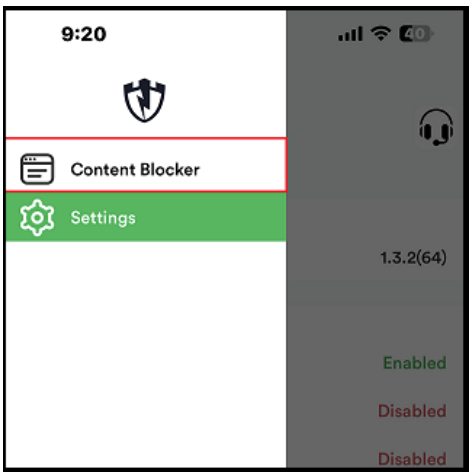
4. 管理者より連絡を受けた電子メールにある専用 URL「https://ios.pcmatic.com/???」を電子メールアプリよりクリックします。ブラウザーへコピペはしないでください



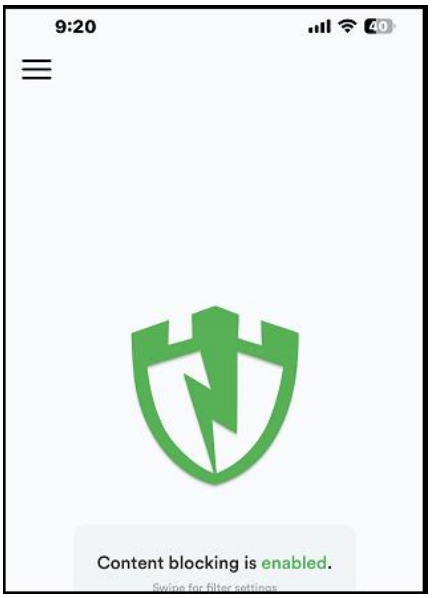
5. PC Matic の画面が開きます。画面を左から右へスワイプしてメニューを表示します。



6. 開いたメニューで「Content Blocker」をタップして選択します。

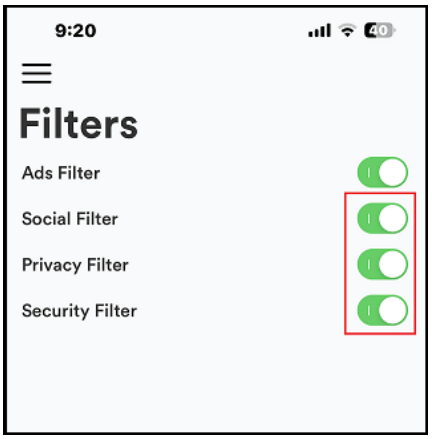


7. この画面を左から右へスワイプして設定の画面に移ります。

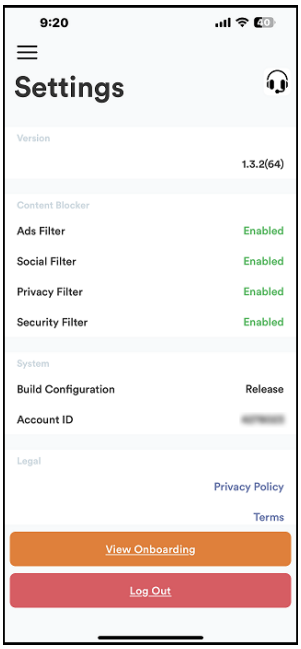


8. 「Social Filter」など必要な機能を有効化します。

広告フィルター : ブラウジング中に発見された、いくつかの形式の広告や詐欺広告を非表示にします。
ソーシャルフィルター : ソーシャルメディアのコンテンツ、ウィジェット、ボタンなどを非表示にします。
プライバシーフィルター : ウェブ解析ツールやトラッキングスクリプトをブロックします。
セキュリティフィルター : マルウェアが含まれている可能性が高いと特定された URL などをブロックします。



9. 画面を左スワイプして、「Setting」に戻り、各機能が有効になっているか確認します。



20 Windows アンインストール

PC Matic PRO をアンインストールする場合は、端末からはアンインストールできませんので、下記手順でアンインストールを行ってください。

電源オフの状態で、端末削除を先に行ってしまった場合は、緊急アンインストールツールを使用してください。

● 端末一覧から削除する

端末一覧から削除を行う際は、端末に電源が投入されていない状態で削除を行った場合は、SuperShield とエージェントを端末で削除を行わなければいけなくなります。一覧から削除を行う際は、削除をする端末の電源を投入した状態で作業を行うか、削除を行う際以外では利用しないようにお願いいたします。

1. 左側メニューの「端末」をクリックし、端末一覧画面を表示します。端末の電源が投入されているか確認し、投入されている場合は、削除を行いたい端末で「削除」ボタン（ゴミ箱マーク）を押します。
   電源が投入されている際に削除を行うことで、SuperShield とエージェントの削除と端末の削除を行います。

20.1 緊急アンインストールツール

アンインストールは、基本的に管理ポータルから各端末に向けて行いますが、万が一、先に端末を削除してしまった場合は、緊急アンインストールツールを使用し強制アンインストールしてください。

こちらは緊急用のため**基本的に使用しない**でください。また、こちらのツールを社員に配布すると、勝手にアンインストールをされてしまう危険があります。**絶対に社員に配布を行わない**でください。

4. 管理ポータルで「端末」を選択し、表示されたメニューから「インストール/削除」を押します。

5. 表示された画面で「アンインストール」タブを選択します。S

6. 「ダウンロード」を選択し、緊急アンインストールツールをダウンロードしてください。ZIP がダウロードされます。この zip 内にある bat を対象端末上で管理者権限にて実行し、アンインストールを行います。この bat は、各顧客企業専用のコードが含まれており、他の顧客企業では利用することができない仕様となっていますのでご注意ください。

21 EDR

EDR 機能は、万が一にも標的型攻撃やランサムウェアによって影響を受けた場合、どの端末がどの時点で感染したかを調査することに役立つ機能です。エンドポイントセキュリティ以外の予防措置も EDR 機能には含まれます。

21.1 予防

PC Matic シリーズは、パソコンへの侵入や権限を奪うなどしてパソコンを乗っ取ることができるセキュリティホールを抱えた脆弱なアプリケーションを強制的に更新することで、侵入ポイントをなくします。Adobe Flash, PDF リーダー, Air。Oracle Java や Filezilla など社内で比較的よく利用される著名アプリケーションを、バックグラウンド処理で強制的に自動更新させることで、社内管理者は社員に通達を出し、実際に更新されたかを確認する作業から解放されます。

21.1.1　著名アプリケーション・ドライバ自動更新

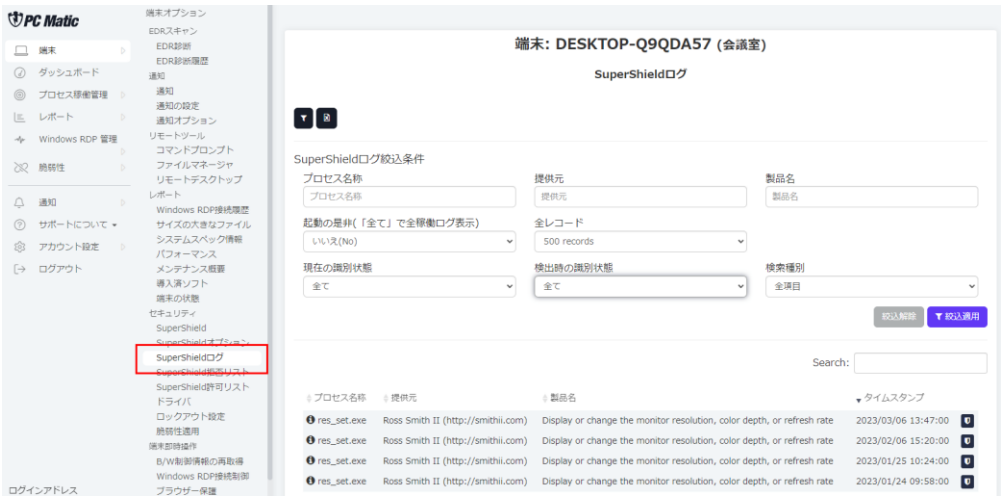
本ガイドの「9　アカウントの包括的なスケジュール作成」を参照して設定します。「アプリケーション更新」と「ドライバー更新」を「オン」にすることで脆弱性対策が実施されます。スケジュール実施の頻度は、「毎週」を推奨しています。実施時刻は昼休みの時刻に設定すると良いでしょう。また設定時刻に厳密に開始するのではなく、パソコンの負荷状態をみて利用中と判断した場合は、延滞させる仕様となっています。利用していないパソコンが同一ネットワーク内に多くあると判断した場合は、順に延滞実施されます。またその時刻に稼働していなくてもその日であれば原則的に実施します。

21.2 記録

21.2.1　アプリケーション起動のログ

PC Matic シリーズは、「SuperShield ログ」から起動した全アプリケーションのログを確認して頂けます。標準では起動阻止されたアプリケーション一覧が絞込表示されています。ログ保持期間は以下のとおりです。

未知・悪質ファイル:36 カ月、全起動ログ:最終利用から 24 時間分を目安にしております。



詳しくは、ホームページの「SuperShield ファイル監査状況の確認」を参照ください。

21.2.2　パソコン情報のスケジュール記録

スケジュールにてパソコンを診断する機能にて、以下の情報を記録可能です。この情報を記録しておくことで、万が一、ウイルス感染した場合は、どの時点から影響を受けていたかを後日調査することが可能となります。

●導入済アプリケーション

●導入済ドライバー

●パソコン情報　(製造メーカー、モデル、BIOS バージョン、メモリ、HDD 等)

●稼働中のプロセス

●稼働中のサービス

●スケジュールタスク

●スタートアップ起動アプリケーション

21.3 分析

世界中の PC Matic 利用者でまだ誰もが遭遇したことのない実行可能ファイル(MD5)が発見された場合は、直ちに多面的な監査がなされます。通常は 1 時間で 95%のもの分類が完了します。残りは、24 時間ほどお待ち頂きます。

また前項目の「記録」を行うことで、万が一、ウイルス感染した場合は、どの時点から影響を受けていたかを後日調査することが可能となります。

21.3.1　パソコン内の分析

以下の情報を指定したスケジュール間隔で PC Matic のクラウドシステムにより善悪の分析が行われます。分析の結果、悪質とされた場合は、警告を表示するか必要な場合は駆除します。

- 導入済アプリケーション
- 導入済ドライバー
- 危険なサービス
- アドウェア
- 危険なブラウザ・アドオン
- 悪質なファイル

21.4 駆除

21.4.1　脆弱性のあるアプリケーション自動更新および不要アプリケーション駆除

前項目の「分析」にて最新版があると判断されたアプリケーションやドライバーは自動的に強制更新されます。また、問題が発生したものは、診断画面にて悪質であると表示されます。この他、危険であるファイルやアドオンは自動的に駆除されます。

- 強制更新:導入済アプリケーション
- 強制更新:導入済ドライバー
- 駆除:アドウェア
- 駆除:危険なブラウザ・アドオン
- 駆除:悪質なファイル

22 「通知」－「セキュリティ」

22.1 セキュリティホールのあるアプリ起動が通知

「通知」-「セキュリティ」のタブにて、各種必要な通知がなされますが、その中で「セキュリティホールのあるアプリケーションが起動された」という通知がなされることがあります。

セキュリティホールのあるアプリケーションは、原則として起動許可がなされませんが、いままで利用許可されており、最近セキュリティホールが発見され、非常に多くの人が利用しているアプリケーションに関しては、BCP(事業継続性)の観点から起動保留を暫くのあいだ行わない処置をとっています。(しばらくすると起動は許可されません)

このようなアプリケーションが利用されている社内利用者に対し、電話やメールにて、脆弱なアプリケーションを利用しているため、最新版へ至急アプリケーションのアップデートを行うことを連絡してください。

昨今のサイバー攻撃では、脆弱なアプリケーションを悪用し端末を乗っ取るケースが大半となっています。脆弱なアプリケーションを対策がなされた最新版にすることで、乗っ取り、ランサムウェアや情報スティーラーなどの脅威から解放されます。アプリケーション・ホワイトリスティング方式だけでは完全でないことをご理解ください。

23 よくある質問

23.1 ライセンス削除に関して

ライセンスは即座に解除していただくことが可能で、社内にて利用されているパソコン台数のみに請求がなされます。パソコンの解除（アンインストール）は、ActiveDirectory を通じて行うことで端末のエージェントを削除していただけます。その後、PC Matic の管理上から削除してください。

コンシューマ版のような最終利用日から 60 日間のロック期間はありません。

23.2 PC Matic のインストールが正常に行われなかった場合

以下の手順にて確認と対処を行ってください。不完全にインストールされてしまった PC Matic のプログラムは、緊急アンインストールツールにてアンインストールしてください。

23.2.1 ファイアウォール装置にて、ホワイトリスト IP アドレスとして除外指定を行ったか確認

ファイアウォール装置の IPS(侵入防止システム)が PC Matic の通信を阻害することがあります。PC Matic サーバーへの IP アドレスを除外指定する必要があります。また、PC Matic は CDN を利用しているため、指定すべき IP アドレスはアクセスする国や回線により異なります。ping などで利用回線での確認作業が必要な場合もあります。

23.2.2 他社セキュリティソフトと併用していないか確認

併用する場合は、他社セキュリティソフトの設定画面にて、PC Matic に関連するフォルダやプロセスを除外指定する必要があります。

23.2.3 セキュリティ関連ツールや、システム関連ユーティリティは導入していないか確認

富士通 InfoBarrier などのセキュリティ関連ツールでは、PC Matic に関連するフォルダやレジストリを除外指定してください。

WiseCare 365(中国), Glary Utilities(中国), CCleaner(英国), Speccy(英国),Spybot Anti-Beacon (英国), Security Reviver(米国)などの Windows のマルウェア対策スキャン インターフェイス (AMSI)を利用しているシステムユーティリティを利用している場合は、アンインストールしてください。

CCleaner などのレジストリツールを Windows 11/10 で稼働させていた場合は、Windows のシステムが破損している可能性が高いため、Windows をクリーンインストールしなおす必要があります。PC Matic は Windows の全てのバイナリーAPI、スクリプトをフックしていますが、それらが破損していると正常に稼働しません。また、Windows が破損している状態では、Windows update が正常に適用されない状態となる等、正常な状態にはなっておらず、セキュリティ面でも問題がありますので、クリーンインストールでの OS 修復が必要です。

23.2.4　過去のすべての OS セキュリティアップート(Windows update)を適用

PC Matic PRO は、.NET Framework にパッチが適用された状態を前提とし、その状態に適合するプログラムを配信して提供しています。OS のセキュリティアップデートを適用しない場合は、サイバー攻撃に対するリスクが大きく増加します。また、脆弱な暗号通信の廃止と、最新の暗号アルゴリズムの配信なども機能アップデートも OS アップデートには含まれています。

パッチが適用されていない状態では、最新暗号アルゴリズムが利用できないためインストールに失敗したり、更新されていない.NET Framework では正常に稼働しないことがあります。

23.2.5　vmware player と Windows の新規導入で競合原因を調査

通信環境によるものか、導入済アプリケーションによるものか原因を切り分けるために、端末に vmware player を導入し、そこへ Windows を導入します。

次に PC Matic PRO をインストールし、問題が発生するか確認します。その状態で問題が発生している場合は、再度「ファイアウォール装置」による通信設定を確認ください。

その状態で問題が発生しない場合は、導入済アプリケーションのうち、システム関連ソリューションが影響している可能性が高いため、資産管理ソフト(SAM)などを導入し、競合が発生するか確認ください。競合が発生したソリューションにて、他アプリケーションの挙動確認などを除外設定する仕組みがあれば、そちらを適用ください。

このような形で競合業務アプリケーションを探して共存の設定を行ってください。

23.2.6　通信プロトコル制御装置やソリューションへの除外指定を確認

ファイアウォール装置やセキュリティ関連ツールでは、Web チャットやテレビ会議などを禁止する仕組みが、セキュリティソフトとは別に導入されている場合があります。PC Matic PRO は、web Sock Secure プロトコルと呼ばれる Web チャットやテレビ会議と同じ通信プロトコルを利用しているため通信が遮断されることがあります。それらの装置で、PC Matic サーバーへの通信を除外指定してください。

23.2.7　他社 EDR ソリューションとの併用は非推奨です。

PC Matic PRO はクラウド型ログ記録の EDR を標準装備しています。このため他社 EDR ソリューションと併用する場合は、他社セキュリティソフトと同様に除外指定を行う必要があります。また、2 つの EDR を稼働させることは端末への負荷が高くなります。

23.2.8　SIEM との併用について

MOTEX LANSCOPE、Splunk、IBM BigFix などの SIEM と併用されるケースがありますが、特段問題は報告されていません。IBM BigFix とのシームレス連携は PC Matic PRO にて標準装備されています。

23.2.9　端末ではインストールに成功したように見えるが管理ホータルに端末情報が上がってこない

該当端末にて WMI が破損している可能性があります。以下のページより WMI 修復ツールを利用して Windows の WMI を修復してみてください。

https://pcmatic.jp/faq/install/07/

修復後、緊急アンインストールツールを用いてアンインストールし、再度インストールを行ってください。

23.3 法人版と MSP 事業者版の違いに関して

MSP 版は、マネージド事業者様が管理対象会社別に管理できるようなマルチテナント機能が装備されておりますが、セキュリティ対策、PC チューニング機能や資産管理機能などは同一でございます。

23.4 特定ドライバーやアプリケーションを自動更新対象外にすることは可能ですか

特定のアプリケーションまたは、ドライバーのバージョンアップの保留は可能です。すべてバージョンアップを停止させる以外にバージョンアップの除外指定が可能でございます。

23.5 管理コンソールの利用者数に制限はありますか

管理コンソールへのアクセス可能者は柔軟に追加可能です。設定変更が可能な admin 権限設定者以外にレポートなどを閲覧することのみが可能な権限者も設定可能です。
また、グルーピング機能にて部署ごとに管理対象パソコンを管理するようになっておりますが、グルーピングは 100 台が上限となっております。グルーピング数は豊富に作成可能です。例えば、営業部門が 250 人いる場合は、営業部門の課単位にて作成いただくと便利です。
また管理権限者は、部門単位でも設定が可能で、例えば学校ではパソコンルームにおける権限者を別途設定するという運用が可能となります。

23.6 リモートデスクトップ機能は別のローカルネットワークでも利用できますか

異なるプライベートネットワークから、複数の管理者が、別のローカルネット可能です。遠隔地の PC を操作可能です。ただし、現在ポートは VNC が利用するポートを利用しており、ファイアウォール装置にて防御されてしまいます。このためポート番号を 443 へ変更する作業を年内に終了させるべく着手に努めております。

23.7 IT 資産管理で各クライアントアプリケーションやドライバーを確認できますか

各クライアントでのインストールされているアプリケーションやドライバー等の種類とそのバージョンを詳細にご確認頂けます。
また脆弱性対策による著名アプリケーションの自動更新機能によって更新された状況もパソコン毎にもご覧頂けます。

23.8 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 を利用しています。CDN を利用しているため、国や回線(通信衛星)により IP アドレスは異なる場合があります。PING を用いて確認ください。

【必須】(日本国内)

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

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

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
utilities.pcpitstop.com	●	●	制御プログラム
switchboard.pcpitstop.com	●		EDR制御プログラム(法人版)
switchboard.pcmatichome.com		●	EDR制御プログラム(個人版)
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
push.pcpitstop.com	●	●	クラサバ制御Keep-aliveサーバ
defs.pcpitstop.com	●	●	SuperShield制御ファイル
drivers.pcpitstop.com	●	●	Driver更新用サーバ
software.pcpitstop.com	●	●	著名ソフトウェア自動更新サーバ
files.pcpitstop.com	●	●	PC Matic プログラムファイル格納サーバ
samples.pcpitstop.com	●	●	バイナリー検体受領サーバ
scriptuploads.pcpitstop.com	●	●	スクリプト検体受領サーバ
android-samples.pcpitstop.com	●	●	android検体受領サーバ
logfiles.pcpitstop.com	●	●	テクニカルサポート用ログ格納
satellite1.pcpitstop.com	●	●	EDR診断実行時の制御サーバ
satellite2.pcpitstop.com	●	●	EDR診断実行時の制御サーバ
satellite3.pcpitstop.com	●	●	EDR診断実行時の制御サーバ
satellite4.pcpitstop.com	●	●	EDR診断実行時の制御サーバ

【法人版でリモートデスクトップ機能を利用する場合】

54.209.29.142 (vncproxy. pcpitstop.com) Port:5500,5900 (IN/OUT)

PC Matic のリモートデスクトップは、オープンソースの VNC をベースに暗号キーなどの仕組みを改修し、セキュリティ性能を高めた独自の通信情報で制御を行っております。このため、NGFW におけるアプリケーション制御機能にて、VNC のシグネチャでは制御できませんのでご注意ください。

【注意】

ウイルスバスター for Home Network、ASUS 無線 Wi-Fi ルーター RT-AC シリーズの AiProtection 機能(トレンドマイクロ製)をご利用の場合は、PC Matic SuperShield 利用状況ログが転送されなくなることが確認されております。SuperShield の利用に問題はございませんが、感染調査を行う EDR の記録機能をご利用になる際には、同装置や機能をオフにしての運用をお願い申し上げます。

【YAMAHA ルーターでの設定例】

評価順	番号	タイプ	プロトコル	送信元アドレス 送信元ポート番号	宛先アドレス 宛先ポート番号
14	200104	pass	*	104.20.82.39	*
				*	*
15	200105	pass	*	104.20.83.39	*
				*	*
16	200106	pass	*	*	104.20.82.39
				*	*
17	200107	pass	*	*	104.20.83.39
				*	*
18	200108	pass	*	34.229.217.50	*
				5500,5900	*
19	200109	pass	*	*	34.229.217.50
				*	5500,5900

23.9 他社エンドポイント保護と併用方法

他社エンドポイント保護(EPP)と併用される際は、他社 EDR 製品同様に、併用する他社エンドポイント保護の設定機能にて以下のファイルを『除外設定』ください。Microsoft Defender, Microsoft Endpoint では除外設定は必要ございません。

【Windows】

● ディレクトリ単位で指定可能な場合(推奨)

C:\Program Files (x86)\PCMatic
C:\Program Files (x86)\PCPitstop

インストーラーパッケージ:PCMaticAgent.MUI-(個別識別子).msi

● プロセスを除外する場合(こちらも登録推奨)

以下のプロセスを全て除外してください。

PCMaticRT.exe
node.exe
pcmaticpushcontroller.exe
PCPitstopScheduleService.exe
WinSW-x86-2.11.exe
pcmconnectnotification.exe
ScriptFileUploader.exe
SampleUploader.exe
PCPitstopRTService.exe
pcmaticrt-wsc.exe
SuperShieldProcessHooker64.exe
SuperShieldProcessHooker32.exe
ElamInstaller.exe
ElamInstaller64.exe
PCMaticRemoteDesktopViewer.exe (管理者リモートデスクトップ機能を利用する場合)
PCMaticRemoteDesktopServer.exe (管理者リモートデスクトップ機能を利用する場合)

【macOS】

macOS では、他社エンドポイント保護製品(EPP)と PC Matic PRO/MSP を併用することはできません。ご了承ください。

他社エンドポイント保護設定情報

23.9.1 Trend Micro APEX ONE

ディレクトリ単位で指定可能であるため、それらを APEX ONE 側にて除外設定します。
除外設定は、こちらの APEX ONE 除外設定ページをご覧ください。

PC Matic の管理ポータルより「アカウント設定」-「ローカルホワイトリスト」へ、「ファイルパス指定」にて、以下 2 点を PC Matic により起動阻止されないよう起動許可を指定します。これより APEX ONE と共存してご利用いただけます。

- ファイルパス: C:¥Program Files (x86)¥Trend Micro
- プラットフォーム: Windows

23.9.2 Symantec Endpoint Protection

ディレクトリ単位で指定可能であるため、それらを Symantec Endpoint Protection 側にて除外設定します。
除外設定は、こちらの「Symantec Endpoint Protection - スキャンからのファイルまたはフォルダの除外」をご覧ください。

PC Matic の管理ポータルより「アカウント設定」-「ローカルホワイトリスト」へ、「ファイルパス指定」にて、以下 2 点を PC Matic により起動阻止されないよう起動許可を指定します。これより Symantec Endpoint Protection と共存してご利用いただけます。

- ファイルパス: C:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protection
- プラットフォーム: Windows

23.9.3 Microsoft Defender for Endpoint

Windows 内蔵の Microsoft defender を拡張した法人向けサービス「Microsoft Defender for Endpoint」を契約しているケースにおいて、PC Matic SuperShield を導入しても Microsoft Defender for Endpoint や Microsoft defender が停止せず、併用できる機能が標準実装されています。Defender は、アクティブモードと呼ばれるフル機能を利用できるモードで動作します。

23.10 社内端末のうち 1/3 や 2/3 が管理ポータルにうまく識別されない

ファイアウォール装置の IPS 機能などによって PC Matic サーバー側と通信が正常に行えていない状態です。前項に従い、ファイアウォール装置へ PC Matic サーバーの IP アドレスを除外指定してください。

23.11 ローカル・ホワイトリストへ登録されているのに起動阻止される

ローカル・ホワイトリストへ登録されているのにも関わらず、オンライン状態で 1 時間程度経過しても起動が阻止される際は、以下を確認ください。

23.11.1 組織内の多くの端末で起動阻止などが発生している

ファイアウォール装置の IPS もしくは、併用しているセキュリティソフトによって PC Matic サーバーとの間でローカル・ホワイトリストの同期処理に問題が発生している事象となります。ファイアウォール装置に PC Matic サーバーへのホワイトリスト指定を行ってください。また、他社セキュリティソフトと併用している際は、他社セキュリティソフトにおいて PC Matic を除外指定する必要があります。

23.11.2 特定の端末のみ起動阻止が発生している

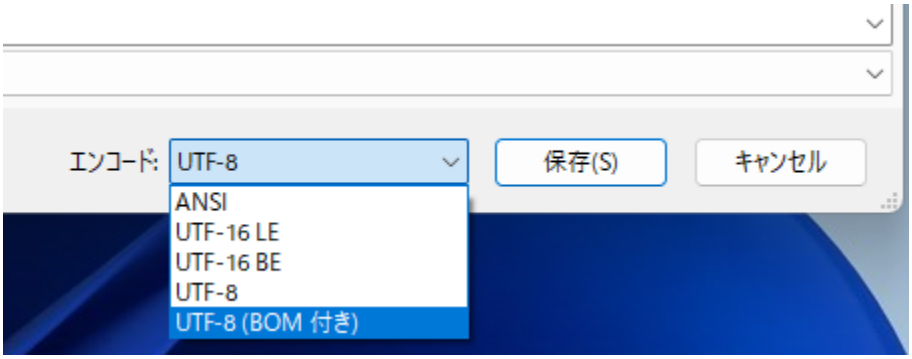
EDR 診断履歴を確認ください。レポート内の「プロセス報告」「サービス診断」「タスクスケジューラー」「スタートアップ・アプリケーション診断」や「導入済ソフトウェアレポート」の項目にて、正しく情報が取得できていない場合は、他社セキュリティソフトがアンインストール後も稼働し続けているために PC Matic サーバーとの通信が妨害されている状態を表しています。

この場合は、Antivirus Removal Tool を用いて残存しているセキュリティソフトを検出し、残存しているセキュリティソフトのベンダーが提供している公式アンインストールツールを用いて完全にアンインストールしてください。

23.12 CSV ファイルを読み込んだら文字化けした

PC Matic は、文字列の扱いに国際標準フォーマット UTF-8 を利用しています。EXCEL の CSV は、シフト JIS の読み込みを行うためエンコードが異なります。シフト JIS は、JIS 第 2 水準までの漢字コードしか扱えませんが、UTF-8 では JIS 第三水準、第四水準以降の文字も扱うことができ、WEB で入力された漢字を文字化けさせずに扱うことができます。

EXCEL で、UTF-8 の CSV を読み込むには、一度 CSV ファイルを Windows 標準の「メモ帳」で開きます。保存する際に「UTF-8(BOM 付)」で上書き保存します。EXCEL で UTF-8 のまま開くことができます。



24 運用 TIPS 集

24.1 端末へ強制的に Windows update を適用

usoclient [オプション] を利用します。

オプション	説明
StartScan	更新プログラムのチェック
StartDownload	更新プログラムのダウンロード
StartInstall	更新プログラムのインストール ※ScanInstallWait の実行後に使用する
RefreshSettings	WindowsUpdate の設定の反映
StartInteractiveScan	ユーザーの入力を求めるダイアログ、進行状況またはエラーの表示
RestartDevice	デバイスの再起動（更新プログラムのインストールの完了） ※Windows 10 バージョン 1803（以降）では何も表示されない
ResumeUpdate	起動時に更新インストールを再開する

STEP 1. usoclient StartScan で、更新ファイルの有無を実行します。

STEP 2. UsoClient StartDownload で、更新プログラムをダウンロードします。

STEP 3. UsoClient StartInstall で、ダウンロードした更新プログラムをインストールします。

STEP 4. UsoClient RestartDevice で、更新プログラムのインストール後にデバイスを再起動します。

これらのコマンドを PC Matic のコマンドプロンプトにて実施することで、対象端末へ遠隔にて Windows update を適用させることが可能です。デジタルサイネージなど無人端末への運用に適しています。

24.2 端末ローカルキャッシュの有効期限

端末で未知の MD5 を検知した場合は、サーバーへ参照を行います。その際にサーバーより「Good」「Bad」へ既に振り分けられていた場合は、それがキャッシュに格納されます。「Good」「Bad」のキャッシュに分類済もしくは、端末/グループ/顧客企業/全アカウントにて「SuperShield 許可」「SuperShield 拒否」に指定されていた場合は、端末内に格納されたキャッシュファイルが 24 時間有効となり、サーバーへは再参照を行いません。これは企業からの通信量削減とサーバー負荷低減のための処置です。

サーバーにて「Unknown」が返された場合は、1 時間再参照を行いません。理由は、通信量削減とサーバー負荷低減のためです。

Unknown にて起動阻止された MD5 のアプリケーションを「SuperShield 許可」もしくは、「SuperShield 拒否」に追加すると、直ちに指定された端末/グループ/顧客企業/全アカウントへキャッシュ情報がサーバーから端末へプッシュ配信されます。このため 1 時間経過することなく起動許可やマルウェア指定が可能になります。

WAN から LAN へのプッシュ通知であるため企業のファイアウォール装置にて IPS が稼働していて、PC Matic のサーバーの IP アドレスがファイアウォール装置のホワイトリストに登録されていない場合は、プッシュ通知がドロップされ、このキャッシュ情報が端末に格納されないことがあります。その場合は、企業のファイアウォール装置へ PC Matic のサーバーIP アドレスを IPS の除外指定することによって正常に動作するようになります。

また、「SuperShield 許可」に個別追加していた MD5 を削除し「SuperShield 拒否」に登録しても、削除情報はプッシュ通知され端末キャッシュから削除されるという処理は行わないため、新たに登録した情報はプッシュされるものの、キャッシュ登録がなされてから 24 時間は挙動が変化しません。先に許可、次に拒否が端末キャッシュに登録された状態となり、キャッシュタイムスタンプが古いものが優先されます。

このため、端末にて正しい判定状況を直ちに反映させたい場合は、「端末一覧」にて対象端末を表示させた後、一覧表示にて右のほうにある「SuperShield キャッシュ更新」を押すことで最新の情報に反映されます。(オンライン時のみ有効)

PC Matic PRO マニュアル

完