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

法人版スターターガイド

第 4 版

PC Matic PRO

Enterprise Customer Starter Guide

【はじめに】ファイアウォール装置の設定・確認

PC Matic PROは、クラウド型アプリケーション稼働ログ、稼働プロセススナップショットなどのEDR機能により、外部通信を行います。このため、ファイアウォール装置のIPS機能により、通信が停止されるのが一般的です。以下のIPアドレスをルーター直下のファイアウォール装置へ必ずホワイトリスト指定してください。設定しなければ正常に稼働しません。
詳しくは、FAQ「PC Maticで利用しているIPアドレスを教えてください」を参照ください。

また、一部の中国、ロシアなど日米欧と政治的に対立している国で製造されたファイアウォール装置は、Amazon S3への通信を停止するIPS機能を実装した機種があるようです。PC Matic PROでは、各端末にて検地された未監査の検体をAmazon S3へ検体をアップロードしていますが、送信されなかった場合は、マルウェア分析官によるデジタルフォレンジック(科学捜査)を行うことができないため、アプリケーション・ホワイトリスティングへの登録はなされません。このため、お客様の手によってローカルホワイトリストに登録してください。他社エンドポイントと併用される際はFAQ「他社エンドポイント保護と共用は可能か」を参照ください。

端末への導入

管理ポータル(pcmatic.jpのMyPage)よりログインします。
「端末」-「+端末追加」を押します。

グループを指定することで、そのインストーラーを使い導入すると、その組織にアサインされます。組織の設定は、マニュアル本編の3-2「部署の作成」を参照ください。

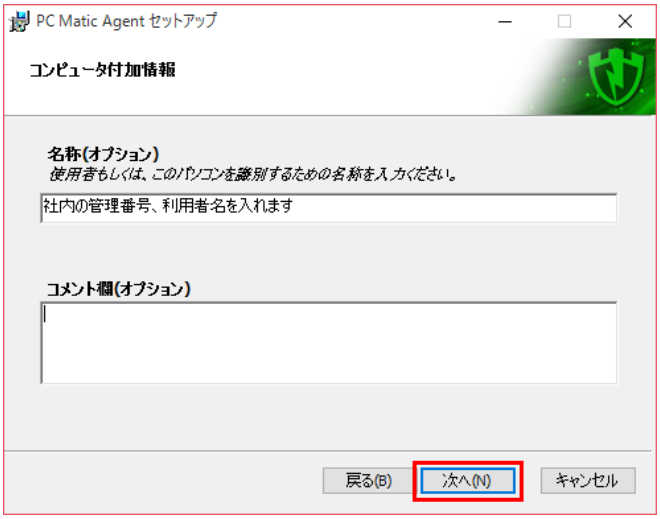
Windows、macのタブを指定します。

インストール直後のエンドポイント保護機能における設定を指定します。これらの設定は、管理ポータルから後で「会社単位」「グループ(組織)単位」「端末」の各レベルにて設定変更も可能です。

システムトレイメニュー「無効」
Javaランタイム「防御」
USB大容量デバイス「許可」
脆弱性適用「有効」
起動阻止ファイル通知「初心者/社内」
を推奨します。

リモートデスクトップは、PC Matic独自のリモートデスクトップ機能になります。

WebShieldは、ブラウザ保護機能ですので、チェック印を入れてください。



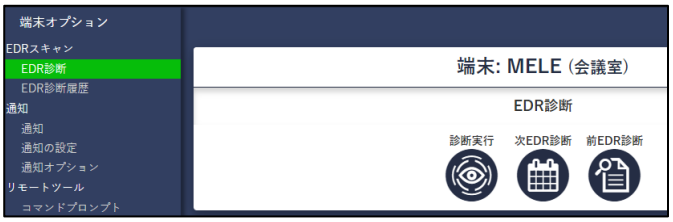
端末に他社セキュリティソフトが導入されていないことを確認し、インストールします。

インストールの際に「名称(オプション)」が表示された箇所に**社内管理番号**や**利用社員名**などを記入すると、端末一覧にそれらが表示され管理しやすくなります。

インストール完了後、WindowsのProfessional系の場合は、Microsoft Defender APTから切り替わるまで5分程度かかりますので、端末をしばらく放置します。

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、管理ポータルにてアイコンが黄色から緑色に変わるまで端末を放置ください。

初期スキャンの実施



「端末」を選択し、導入した端末の詳細を表示します。緑ステータスになるまで30分程要することがあります。

「EDR診断」の項目から「診断実行」を選択し、EDRスナップショットを含む各種診断を実施します。

PC Matic PROを利用して社内へ導入を展開する前に、社内で共通して利用している業務アプリケーションがPC Maticマルウェア分析官によるデジタルフォレンジックを経ていない場合も想定し、「次EDR診断」の項目から「add　スケジュール」にて、「頻度」を「1回」に設定し10分後くらいの時刻で一旦「保存」します。

「編集」にて、先程のスケジュールを開き、マルウェア除去の項目を「完全スキャン」に指定して実行させます。本作業により、パソコン内に格納されている全ての実行可能ファイルが検査され、グローバルホワイトリストに掲載されていないマルウェア分析官によるデジタルフォレンジックが実施されていない実行可能ファイルが分析されます。2～3日経過しても、善良にも悪質にも分類されていない場合は脆弱性を抱えていることが推測されます。

脆弱性を抱えているアプリケーションは、「SuperShield許可リスト」へ追加することにより起動が可能になりますが、セキュリティホールにより悪意あるものによる端末乗っ取りの危険性を伴います。

アプリケーション起動の確認

業務で利用するすべてのアプリケーショが起動するかを確認します。

起動が阻止されるアプリケーションがある場合、PC Maticマルウェア分析官によるデジタルフォレンジックによる結果を24時間程度待ちます。

以上までが社内配布端末での導入手順です

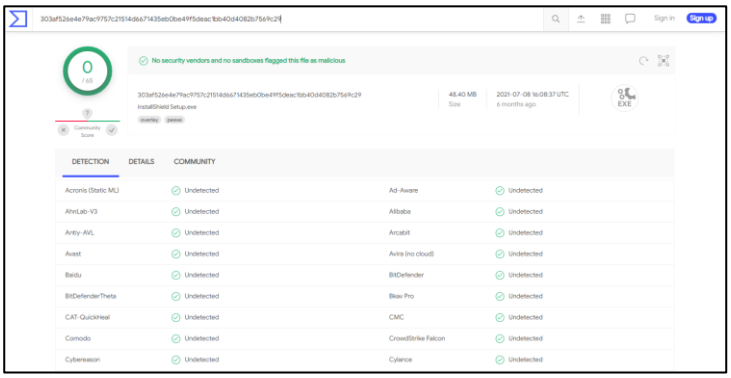
起動阻止されたアプリケーションへの対処方法

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。

「通知」-「セキュリティ」での表示から簡便なローカルホワイトリストへの追加

このタブを開くと起動阻止されたアプリケーションのMD5ハッシュ値が表示されます。こちらの方法ではスクリプトは登録できませんが、アプリケーションファイルはホワイトリストへ簡単に追加できます。

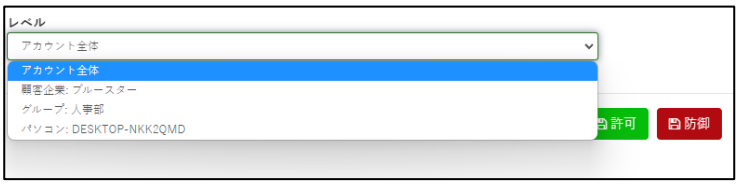
起動阻止されたアプリケーションのファイルハッシュ値がクリック可能となっているため、そちらをクリックすると、VirusTotalが開きます。



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。



「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。

プロセス稼働管理からの登録

先程の「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「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「  」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】

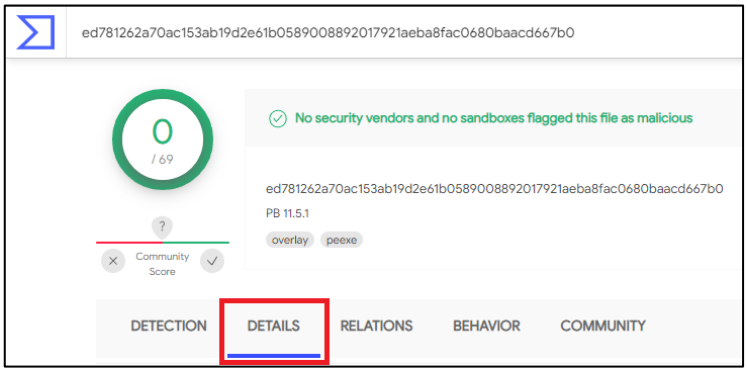
大 危険度 小

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。

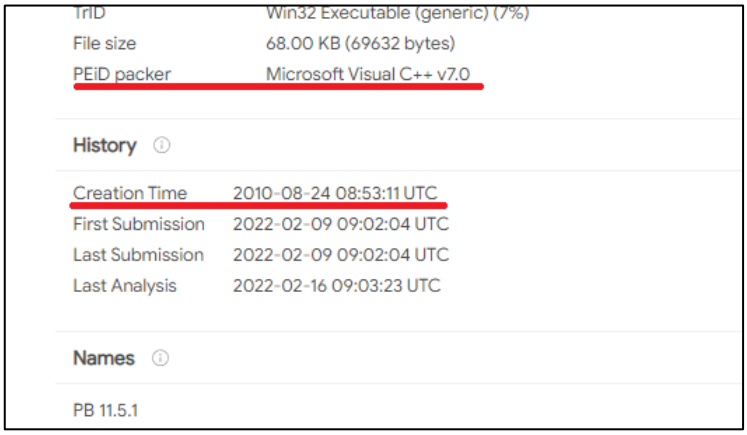
VirusTotalでセキュリティホールがないか詳細を確認する



ウイルスがなくても、深刻なセキュリティホールがある場合、PC Maticではアプリケーション・ホワイトリストへは追加されません。

脆弱性により、パソコンが乗っ取られる危険性があるためです。この有無を日付から推測します。

先程のVirusTotalで、「DETAIL」タブ選択します。



PEiDで、どのコンパイラーで制作されたかを確認することができます。

HistoryのCreation Timeは、VirusTotalがこのプログラムを一番最初に検出した日付であり、提供時期を推測することに役立ちます。

2009年以前のアプリケーションの大半には、Microsoft ATL 脆弱性が含まれています。
Packerが以下の場合はほぼ深刻な脆弱性が含まれます。
Visual C++ 2005
Visual C++ 2008

このようなアプリケーションに関し、利用者へ「最新のVisual Cで開発されたバージョンが先方よりリリースされていないかの確認」とお伝えして最新版の入手を促していただければ幸いです。脆弱性を含む場合は、一般的にベンダーよりセキュリティパッチや最新版が提供されていますが、そうしたことに無頓着なベンダーも過半数存在しているのも確かです。

このようなアプリケーションは、利用者やグループを限定してホワイトリストへ追加し、注意喚起によりパッチ適用や最新版への更新をしていただくことで、パソコンへの不正侵入抑制に貢献します。