

# PC Matic PRO

## Zero Trust Application Allowlisting Proactive Endpoint Security Suite

- EPP:エンドポイント保護
- EDR:エンドポイント検出応答
- RMM:端末運用管理
- Fraud prevention:詐欺対策
- Performance:パソコン快適化



### EPP:エンドポイント保護

- ゼロトラスト・アプリケーション型エンドポイント保護
- 稼働モード:グローバルリスト、ローカルリスト限定運用(適応、標準、厳格)
- 想定外挙動検知応答ヒューリスティックエンジン
- OS API,各種スクリプト,通信ソケットの標準拒否
- ファイルレス・マルウェア制御
- エクスプロイト攻撃防御
- Java 有効/無効 制御
- 起動阻止情報のsyslogサーバ送信
- トラッキングcookie削除
- ブラウザ保護 拡張機能(Edge,Firefox,Chrome対応)
  - 詐欺広告、バナー広告、動画広告スキップ機能
  - WEBスキミング阻止、仮想通貨マイニングスクリプト阻止 など



### EDR:Endpoint Detection & Response

- (予防:記録) ドライバ自動更新と実施記録
- (予防:記録) 著名アプリケーション自動更新と実施記録
- (予防:記録) 起動された脆弱なアプリのMITRE CVE情報を通知
- (記録) 起動アプリケーション稼働ログ(クラウド記録24h+端末内7日)
- (記録) 端末導入済サービス一覧取得
- (記録) 端末導入済プロセス一覧取得
- (記録) 稼働プロセスのスナップショット取得
- (記録) セキュリティ状況モニター
- (記録:制御) Windows RDP接続制御・接続ログ
- (記録:制御) 全稼働プロセス詳細把握(端末/日時等)と稼働制御
- (記録:制御) ソフトウェア資産管理(ローカルリスト限定運用リスト作成)
- (制御) ファイルレス・ランサムウェアが利用するOS内部暗号機能制御
- (制御) 各種スクリプト言語によるファイル外部送受信制御
- (制御) USBストレージ装置利用可否
- (制御) Windowsアカウントロック制御
- (制御) 組織別のホワイトリスト/ブラックリスト管理
- (記録:駆除) アドウェアや迷惑アプリ削除
- (記録:駆除) 悪質なブラウザアドオン削除
- (記録:駆除) 悪質ファイル検索・駆除

### RMM:端末運用管理

【端末情報】

- ソフトウェア資産管理 (SAM)
- ハードウェア資産管理 (HAM)
- CPU負荷状況、RAM・ストレージ利用率監視
- リソース・セキュリティ関連 アラート通知
- 世界ランクによる端末陳腐化評価
- SIEM連携API (IBM BigFix, Syslog等)
- 運用状況レポートのPDF自動送信
- Windows Server稼働監視



【端末操作】

- 管理者用ゼロタッチ・リモートデスクトップ (管理→遠隔)
- ファイルマネージャー (遠隔↔管理)
- コマンドプロンプト (管理→遠隔)
- Windows RDP 機能 オン・オフ
- 再起動
- スリープ制御 (常時オン維持)
- 管理者端末 2FA (Google, Microsoft Authenticator等)

【端末快適化】 **Windowsのみ**

- レジストリ最適化
- TCP/IPパケット長 最適化
- 不要スタートアップ削除
- 一時ファイル削除

### 対応OS・リソース

- Microsoft Windows 11 / 10 / 8.1 / 8 / 7
- 上述のWindows Embedded 各版
- Windows Server 2022/2019/2016/2012R2/2012/2008R2 (Server版対応)
- macOS 10.13.2以降 (Intel, Appleシリコン)
- iOS 13以降
- iPadOS 13以降
- Linux (Red Hat, Debian, Ubuntu, OpenSUSE)
- ハードディスク容量: 150 MB 以上
- セキュリティ対策エージェントメモリ使用量: 50 MB
- インターネット回線: ブロードバンド・インターネット




EPP+EDR遠隔運用管理(RMM)が統合した法人向けエンドポイント保護スイート製品



政府・軍隊向けオンプレミス型エンドポイント保護スイート製品




PC Matic PROのマルチテナント版事務機器販売店、大企業向け製品



PC Matic PROの産業機器組込版オフライン・オンライン両対応

PC Matic PROホームページ  
<https://pcmatic.jp/pro/>  
導入事例も掲載しています。

日本地区総ディストリビューター



〒105-0003  
東京都港区西新橋1丁目6-12 AIOS虎ノ門 4階

### 個別対応

脆弱性検査 / 悪質なファイル分析 / セキュリティ状況監視 / 感染時の現地分析と対応策提案 など、別途ご利用頂けます。

販売代理店



法人版

---

組込版

---

政府版

対応OS: Windows 11/10/8.1/8/7、Windows Server 各版、macOS、iPhone、iPad、Linux

# 貴社がサイバー犯罪者の標的にならないために

ゼロトラスト・セキュリティモデル NIST SP800シリーズに準拠したアプリケーション・ホワイトリスト方式で、万が一にも感染しない安心安全を手にしよう。

## ZERO TRUST STARTS from PC Matic



<https://www.cisa.gov/stopransomware>

米CISA庁とFBIは、特設サイト「STOP RANSOMWARE」の「初期アクセスベクトル: 前駆体マルウェア感染」セクションで、エンドポイント保護方式を解説。一般的な保護方式ではなく、PC Maticが採用する新たな保護方式である「アプリケーション・ホワイトリスト方式」の実装を推奨しています。

**政府のセキュリティ基準**  
アメリカ合衆国政府の高いセキュリティ要求を満たした、ゼロトラスト・セキュリティ搭載

**詐欺対策もバッチリ**  
PC Magazine誌による悪質URL対策調査で、No. 1と評価された詐欺対策を装備

**ブラウザ経由の侵入阻止**  
邪魔なバナー広告を非表示にして、業務効率UP。不正なスクリプトによるパソコンへの侵入なども阻止

## 7つの特長

- ① 新種による被害者がゼロ  
従来製品は、新種マルウェアに感染することでワクチンを作成し他者を守るという設計思想。全実行ファイルをマルウェア分析官による人手での監査を経て善良としたものしか起動させないため、新種を見逃さない
- ② グレーゾーンを起動保留  
疑わしきは罰せずが従来製品。PC Maticは、ホワイトリストであるため善良のみで疑わしいものも起動させない
- ③ 深刻な脆弱性を持つ場合起動せず  
実行することでセキュリティ上の脅威が発生するアプリをPC Maticは起動保留。従来製品は起動許可
- ④ 脆弱性自動更新とCVE通知  
悪意ある者に悪用されやすい著名アプリを最新版へ自動更新。脆弱性を含むアプリの起動をCVE番号付きで通知
- ⑤ 多層保護  
複数のホワイトリスト保護方式を多層実装し、いくつかをパスしてしまっても他層で阻止される安心設計
- ⑥ 膨大なサーバーリソース  
膨大なサーバーリソースで、静的及び動的に分析を行い、多数のスコアリングにてマルウェア分析官により最終判定
- ⑦ 同盟国製品  
日本の同盟国であるアメリカ国内で研究開発し運用されている唯一の製品。国家安全保障のため、一切オフショアなし

## 歴史に裏付けられたユニークな技術



### アプリケーション・ホワイトリスト方式

デフォルト拒否でバイナリー形式、スクリプト形式の両実行ファイルを強固に端末を保護。多種多様な端末や利用体系に対応しています。

端末内で善悪を判断するのではなく、未監査の実行ファイルは、マルウェア分析官へ即座に送られ分析にかけられます。



### ニューラルネットワーク型AI

複数のアルゴリズムによるAIスコアや検体のソースコード、バージョンアップ差分などがマルウェア分析官に提示されます。

それらの情報を基に、新種マルウェアなどが潜んでいないかをデジタルフォレンジックし、善・悪・脆弱に手作業で分類します。



### 経験豊富なマルウェア専門家集団

FBIサイバー捜査官出身者や、セキュリティ業界で長年の経験を積んだマルウェア専門家集団が、新種マルウェアを科学捜査手法を用い見逃しません。

顧客企業で生じた事象に対し迅速に対応する体制を敷いており、高い支持を頂いております。



### 220億以上の検証

PC Maticは、220億以上のアプリケーションと端末を診断し、検証してきました。



### 300万以上の顧客

300万人以上のお客様がPC Matic製品を使用し、ご満足いただいています。



### 10万以上の法人端末

PC Matic PROは 10万以上の法人端末で利用され、社内外のITインフラの安全性を確保し、運用を最適化しています。

## 私たちは NIST でゼロトラスト・セキュリティモデルを策定しています。

NIST NCCoE構成企業 PC Matic。真のゼロトラストはPC Maticから始まります。  
※NISTは、米商務省管轄の産業標準化組織です。



"アプリケーションのホワイトリスト化は、徹底した防御のためのソリューションに不可欠な要素です。"

—アメリカ国土安全保障省



アプリケーションのホワイトリスト化やEDRを使用して、承認済ソフトウェアのみ実行可能として、未承認はブロックされるようにします。

—CISA, STOP RANSOMWARE Guideline



"アプリケーションのホワイトリスト化は、特定のプログラムのみをコンピュータ上で実行できるようにするものです。これにより、悪意のあるプログラムがコンピュータ上で実行されるのを防ぐことができます。"

—USA Today



"アプリケーション・ホワイトリスト化は、指定されたプログラムのみ実行させ、悪意のソフトウェアを含むその他のプログラムをすべて起動阻止するため、最高のセキュリティ戦略の1つです。"

—米国コンピュータ緊急事態対策チーム



## Zero Trust - Globally Automated Application Allowlisting

PC Maticは、アメリカ政府と、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である、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新たなエンドポイント保護方式を採用しています。

基本モデルでは、利用者が作成した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、リスト作成の手間がかかるため、PC Maticは長年の経験をもつマルウェア分析官がAIを助手として活用し、ひとつずつ善良なアプリケーションを指定しています。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%を網羅するホワイトリストを用意しています。



### No Victims

従来のセキュリティ製品とは異なり、ゼロトラストで端末を保護するため顧客に感染の心配は一切なく、過去6年間あらゆる感染被害はありません。



### Stress-Free

運用管理者はホワイトリスト登録などの運用は一切不要です。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自動的に利用可能となります。



### Standards

米標準技術研究所(NIST)は、アプリケーション・ホワイトリストリング方式による標準化を策定し、それに準拠しました。



### Up-To-Date

ホワイトリストの更新は迅速で、定義ファイルを更新しなくても保護レベルは低下しないため、最高のセキュリティを維持したまま、オフラインでも使用することができます。



### Lightweight

端末内で監査しないため、セキュリティ保護は端末性能に影響を与えることなく、軽快に動作します。競合他社製品と比較して多くの賞を受賞しています。



### Economical

アプリケーション・ホワイトリストリングを追加導入することで、マルウェア検出の対処に必要な労力とIT資源を、大幅に減少させることができます。



## 添付ファイルで感染しない安心感

ウイルス付きメールは、送信元を取引先のメールアドレスに偽装する事があり、専門家でも添付ファイルの安全性を判断する事は非常に困難になっています。

PC Maticなら、ランサムウェアや標的型攻撃を完全に防御することができるので、安心して添付ファイルを開くことができます。業務を遂行した従業員に「なぜ怪しいメールを開封したんだ」と責めることは止めましょう。情報システム部門がそのようなリスクを排除することができるのですから。



## 様々なホワイトリスト保護による多層防御

グローバルリストとローカルリストの2つの制御リストで、アプリやスクリプトの実行がコントロールされます。グローバルリストは、PC Matic社のマルウェア分析官によって、静的・動的分析をAIの手助けを得ながらデジタルフォレンジックを全件実施し、最終的に手作業で「善良・グレー(脆弱,不明,嫌疑)・悪質」に分類されます。

グローバル・ホワイトリストには、2023年3月時点で1億3千万個が登録済みであり、ホワイトリスト保護方式でありながら、従来のブラックリスト方式製品と同様の使い勝手を実現しています。

自社開発した業務アプリケーションは、様々なローカル・ホワイトリストを活用することで、従来のホワイトリスト型製品と比較し、運用の手間を大幅に削減することに成功しました。



### グローバル・ホワイトリスト

世界中の利用者が検知したアプリケーションから善良なものを共通リスト化したものです。世界中のPC Matic顧客へ即時提供し、善良確認済のアプリ・スクリプトのみ起動を許可します。



### ローカル・ホワイトリスト

アプリケーション・ホワイトリストを補完するため、お客様が独自のアプリケーションを指定端末・組織・企業全体に適用することができます。



### 署名ホワイトリスト

自社開発したデジタル署名済みのアプリケーションは、デジタル署名により包括的に許可され、アプリケーション毎にホワイトリストへ登録する必要がありません。



### スクリプト・ホワイトリスト

ランサムウェアはOS標準機能のスクリプトを介して展開されるため、当社は業界唯一のスクリプティングホワイトリストを作成し、実装しました。



### Windows RDP 認証ホワイトリスト

ハッカーはRDPを利用して端末を乗っ取ります。PC Matic PROは、このセキュリティを強化するため、利用端末へ様々な追加認証の仕組みを提供しています。



### 端末認証ホワイトリスト

Windows RDP接続端末のペアを限定する機能を提供。しかも接続時に追加の接続認証は不要としました。



### Microsoft Office ホワイトリスト

マルウェアは、Officeのマクロを介して活動を開始することがあります。このため、Office専用別途起動可能なマクロやスクリプトのホワイトリストを多段実装しました。



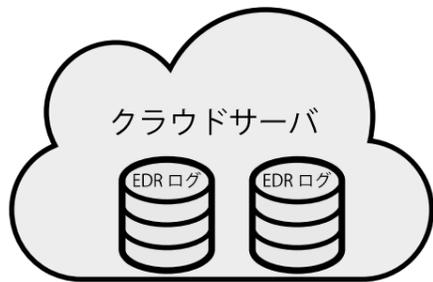
### ファイル拡張子ホワイトリスト

マルウェアは、危険なファイル拡張子を使って実行されます。悪意あるファイル拡張子によるアプリケーションの起動を無効化するホワイトリストを装備しています。



### ローカルディレクトリ・ホワイトリスト

特定ディレクトリをホワイトリストに登録することができ、社内アプリケーションを開発、試験、配布とその利用許可を容易に行うことができます。



- 稼働ログはクラウド上に3ヶ月分保管。悪意ある者に改ざんさせない
- 組織内端末の稼働プロセス一覧を取得でき、起動制御が可能
- 導入アプリ・サービス・ドライバ・稼働中プロセス等のスナップショット
- 起動された脆弱なアプリのMITRE CVE情報を通知
- 著名アプリケーション自動更新機能による脆弱性対策を装備

EDR機能は、万が一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。標準で、米国のマルウェア分析官による監視サービスが付帯しています。

バイナリ形式、スクリプト形式の稼働ログとスナップショットは、クラウド上に保存され、改ざんリスクを回避できます。



- IT資産管理機能で、生産性の落ちているパソコンを把握可能
- ソフトウェア資産管理(ISAM)
- 独自リモートデスクトップ機能で管理者が画面共有
- 遠隔端末のファイル送受信、コマンドプロンプト実行
- USBストレージの利用制限
- Windows RDP利用制限(接続元限定、時間帯など)、接続履歴
- SIEM連携API (IBM BigFix, Syslog等)

EPP, EDRだけではなく、社内端末の運用管理機能(RMM)も統合し、標準料金にてご利用頂けます。複数のソリューションを横断する必要がなく、統合により利便性が向上します。



予防・記録

- ドライバ自動更新と実施記録
- 著名アプリケーション自動更新と実施記録 (NIST SP 800-40)
- 起動アプリケーション稼働ログ
- ブラウザ侵入防止機能
- 端末導入済サービス一覧取得
- 端末導入済プロセス一覧取得
- 稼働プロセスのスナップショット
- セキュリティ状況モニター
- 利用アプリのMITRE CVEを通知



制御

- Windows RDP制御・接続ログ
- 組織別の全稼働プロセス詳細把握(端末/日時等)と稼働制御
- ランサムウェアが利用するOS内部暗号化機能制御
- 各種スクリプト言語によるファイル外部送信機能制御
- USBストレージ装置利用可否
- Windowsアカウントロック制御
- 組織別のホワイトリスト/ブラックリスト管理



駆除

- アドウェアや迷惑アプリ削除
- 悪質なブラウザアドオン削除
- 悪質ファイル検索・駆除



端末情報

- ソフトウェア資産管理 (SAM)
- ハードウェア資産管理 (HAM)
- CPU、RAM、Storage利用率監視
- 資源・セキュリティアラート通知
- 世界ランクによる端末陳腐化評価
- 運用状況レポートを自動的送信
- Windows Server稼働監視
- SIEM連携 (syslog, IBM BigFix)



端末操作

- 管理者用リモートデスクトップ (管理→遠隔)
- ファイルマネージャー (遠隔←→管理)
- コマンドプロンプト (管理→遠隔)
- 再起動
- スリープ制御
- 管理者端末 二要素ログイン認証 (Google, Microsoft等)



端末最適化

- レジストリ最適化
- TCP/IPパケット長最適化
- 不要スタートアップ削除
- 一時ファイル削除



社員が不正に導入したアプリも制御

インターネット上には、無償のソフトウェアが豊富にあります。しかし、アプリケーションの中には、会社に脅威をもたらすものも少なくありません。

全社員が利用したアプリケーション一覧から、いつ、誰が、何を起動したのか容易に把握でき、ふさわしくないアプリケーションを今後起動阻止することが、クリックひとつで行えます。



日本人による日本国内MDR監視センターを利用可能



クライアントライセンスとは別契約にて「感染監視・即時応答」をビジネス時間帯や365日24時間対応するMDRサービスをご利用頂けます。京都三条セキュリティ・オペレーションセンターにて、日本人スタッフが運用監視応答を実施。

端末だけでなく監視が必要な通信装置にも対応可能です。ホワイト運用による安心安全を業界最低価格で提供します。