Kaspersky AI Protect

kaspersky bring on the future

Kaspersky AI Protectは、AIを介した脅威と従来型の脅威の両方を検知する業界最高クラスのソリューションです。ほぼあらゆるアプリケーションに統合できます。

Kaspersky AI Protect（KAIP）は、Webポータルやアプリケーション、プロキシサーバー、NAS（ネットワーク接続ストレージ）、メールゲートウェイを包括的に保護します。HTTPおよびICAPを介して、スタンドアロンサービス、スケーラブルなクラスター、Dockerコンテナとして容易に導入・管理できます。

Kaspersky AI Protectには、LLMファイルやAIエージェントに悪意のある機能が含まれていないかをチェックする新機能が搭載されています。

主な機能

Kaspersky AI Protectは、Linux環境において次の2つのモードのいずれかで動作します。

- **REST-likeサービス：**クライアントアプリからHTTPリクエストを受信し、リクエストに含まれるオブジェクトをスキャンして、スキャン結果をHTTPレスポンスとして返します。
- **ICAPサーバー：**プロキシサーバー／NAS／Webアプリケーションファイアウォール／NGFWなど、ICAPプロトコルで通信するあらゆるソリューションを通過するHTTPトラフィックをスキャンします。この統合モデルでは、ユーザーがリクエストしたURLのスキャンも可能で、悪意のあるコンテンツ、フィッシング、アドウェアを含むWebページを除外します。

Kaspersky AI Protectは、Linux Dockerコンテナ（HTTPモード／ICAPモード）としても提供されます。単体のコンテナとして、またはDocker Swarm、Kubernetes、AWS EKSなどのクラウド環境にデプロイできます。

Kaspersky AI ProtectにはWebベースのGUIが搭載されており、製品動作の設定やサービスイベント、スキャン結果の確認を容易に行えます。

統合シナリオ



AIが今日のビジネスにもたらす脅威

LLMの脆弱性

- .pth、.pt、.pkl、.kers、.ckptなどの形式の大規模言語モデル（LLM）ファイルには、悪意のあるコードが含まれている可能性があります
- 感染したLLMの悪意ある機能が実行されると、パスワードや銀行カード番号などの個人データが漏洩するおそれがあります

不正なAIエージェントとスキル

- マルウェアは、AIエージェントを装っていることが多くあります
- 2026年上半期、カスペルスキーはAIサービスを装った92,000件を超える悪意のある攻撃を検知しました
- 2026年2月以降、システム上のOpenClawスキルのアクティビティはKaspersky Scan Engine 2.2によってスキャンされています。現在、悪意のあるOpenClawスキルのアクティビティが毎月2万件以上検知されています。

Kaspersky AI ProtectのAIモデル／AIエージェント向けセキュリティ機能

LLMモデルファイルのディープスキャン

- .pth、.pt、.pkl、.kers、.ckptなどのモデルファイルをスキャンし、悪意のあるコードやバックドアの埋め込みを検知します。

AIエージェントのセキュリティ検知

- エージェントスキルに対し、クロスプラットフォームで悪意のある挙動を検知する機能を提供します。
- 悪意のあるプラグインを検知し、デバイスの乗っ取りやボットネットへの組み込みを防ぎます。APIキーの漏洩、認証情報の窃取、機密データの持ち出し、悪意のあるコマンド実行といったリスクの回避に役立ちます。

包括的なマルウェア対策

- ヒューリスティック検知と機械学習を組み合わせ、クラウドベースの脅威インテリジェンスと連携してミリ秒単位で対応します。
- 高度なアンパック、多層パッカー検知、インテリジェントな駆除／修復を実行します。
- フィッシングサイトや悪意のあるURLを高精度にフィルタリングします。

主な利点

- クラスターモードによる水平スケーリングで、大容量ファイルも負荷なくスキャン。
- HTTP REST-like／ICAPの2つのプロトコルに対応し、既存システムとシームレスに統合。
- オフラインアップデートに対応し、物理的に隔離された環境や低速ネットワーク環境にも最適。
- LLMファイルおよびスキルファイルのセキュリティスキャンに対応。

サイバー脅威ニュース： www.securelist.com
ITセキュリティニュース： business.kaspersky.com

www.kaspersky.com

©2026 AO Kaspersky Lab. All rights reserved.
登録商標およびサービスマークは、それぞれの所有者に帰属します。

Technology Alliances

カスペルスキーのテクノロジーは、サードパーティ製のハードウェア／ソフトウェアのセキュリティ製品・サービスへの統合向けに提供されています。すべてのソリューションに、専門のテクノロジーパートナーシップサポートが付帯します。

詳細はこちら：www.kaspersky.com/oem