ESET AI Security
機能紹介資料

第1版

2026年11月

Canon

キヤノンマーケティングジャパン株式会社

目次

1．はじめに
2．AI エージェントによる課題、リスク
3．ESET AI Securityでの保護

©Canon Marketing Japan Inc.

1. はじめに

昨今、AIエージェントは企業の日常業務に組み込まれることも多くなりました。

一方で、AIの利用拡大は新たな攻撃経路を生み出しており、従来のセキュリティ対策だけでは捉えきれない新たなリスクへの対応が求められています。

ESET AI Securityでは、そのようなAI利用に伴うリスクを可視化し、安全なAI利用を支援いたします。

本資料ではESET AI Securityの以下機能を対象としております。

サービス名	内容
AI Agent Security	AIエージェント自身が扱う・取り込む可能性のある脅威に対応
AI Behavioral Monitoring	自律型AIエージェントの振る舞いを監視 エージェントが稼働を開始した後の動作を制御

- 本資料は、本資料作成時のソフトウェア及びハードウェアの情報に基づき作成されています。
  ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに記載されている機能、名称及び画面などが異なっている場合があります。
  また、本資料の内容は将来予告なく変更することがあります。
- 本製品の一部またはすべてを無断で複写、複製、改変することはその形態に問わず、禁じます。
- ESET、ESET AI Security、AI Agent Security、AI Behavioral Monitoring、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET Server Security for Microsoft Windows Server、ESET Endpoint Security for macOS、ESET Server Security for Linux、ESET Endpoint アンチウイルス for Linux、ESET LiveGrid、ESET PROTECT は、ESET,spol. s r.o. の商標です。
- Microsoft、Windows、Windows Serverは米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。

©Canon Marketing Japan Inc.

1. はじめに

AI活用は「生成」から「実行」へ

生成AIの普及により、企業におけるAI活用は、情報収集や文章作成などの業務を「**支援する**」用途から、
AIが目的に応じて必要な処理を判断し、データやシステムと連携して業務を「**実行する**」用途へと広がりつつあります。

生成AIの活用は、情報収集やコンテンツ生成といった用途だけでなく、社内データや業務システムと連携する領域へと広がっています。
さらに、AIが利用者から与えられた目的に応じて、必要な処理を判断し、実際の業務を実行する使い方も登場しています。

このように、AIがより自律的に業務へ関わるようになる中で、**AIエージェントの活用にも注目が集まっています。**

業務を「支援するAI」

情報を調べる
文章を作成する
情報を要約する

→

業務を「実行するAI」

目的を理解する
必要な処理を判断する
データやシステムと連携する
タスクを実行する

©Canon Marketing Japan Inc.

2. AIエージェントによる課題、リスク

(1) AI エージェントとは？

AIエージェントとは、利用者から与えられた目的に応じて**AIが自ら考え、必要な作業を判断・実行する仕組み**です。
従来の生成AIが利用者からの質問や指示に対して回答を生成することを中心としているのに対し、AIエージェントは目的に応じて複数の処理を組み合わせ、より自律的に行動できることが特徴です。
一方で、AIエージェントが利用できるデータやシステムが増えるほど、**適切な権限管理やセキュリティ対策も重要**になります。
今後、業務での活用拡大が期待される一方で、安全に利用するための仕組みづくりも求められています。

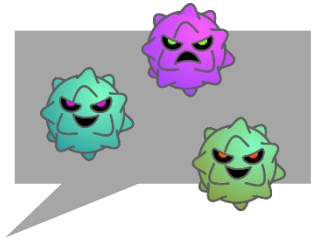


©Canon Marketing Japan Inc.

2. AIエージェントによる課題、リスク

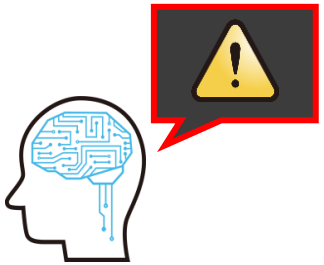
(2) AIエージェントによるリスク

AIエージェントを利用するにあたって、以下のようなリスクが考えられます。



プロンプトインジェクション

悪意のある指示が書かれたプロンプトを読み込むことで、**有害なコマンドが実行**される



悪意のある構成要素の取り込み

AIエージェントが、**悪意のあるスキルや外部コンポーネントを取得・利用**する



機密情報の漏洩

AIエージェントが機密情報へアクセスし、**機密情報が漏洩**するリスク

TIPS

IPAが公開したセキュリティ短信によると、「AIエージェントやその実行基盤を経由した情報窃取や任意コード実行が相次いだ」と報告されている。
その一例として、AIエージェントが300を超える組織の1.3万枚以上の社内画像をGitHub上で公開した事例が紹介されている。
※出典：IPA(独立行政法人情報処理推進機構)「AIセキュリティ短信 2026年10月号」
https://www.ipa.go.jp/digital/ai/security/rcu1hd0000007gji-att/2026-4_1016.pdf

©Canon Marketing Japan Inc.

2. AIエージェントによる課題、リスク

(3) AIエージェントによるリスクから会社を守るために

AIエージェントによるリスクから会社を守るためには以下のような対策が重要です。
※2026年11月時点では、悪意のあるAIスキルファイルの検知が中心です。

リスク	プロンプトインジェクション	悪意のある構成要素の取り込み	機密情報の漏洩
対策	AIエージェントによる ・不審なコマンド実行 ・プロセス・ファイル・レジストリ操作 を監視・検知	・スキルファイル*1 ・パッケージ ・MCPサーバー*2 などを検査 AIエージェントが利用する前に脅威を検知・ブロック	AIエージェントの出力を起点にした ・高リスクなコマンド実行 ・ファイル操作 を監視・検知

上記対策は**ESET AI Security**で実現可能

*1.スキルファイル・・AIエージェントに機能や処理手順を追加するためのファイル。
*2.MCPサーバー・・AIエージェントが外部のデータを取得し、ツールを操作するためのプログラム/サービス

©Canon Marketing Japan Inc.

3. ESET AI Securityでの保護

(1) ESET AI Securityの利用条件

ESET AI Securityのご利用には、以下の条件を満たしている必要があります。なお、各条件を満たす場合、各機能は既定で有効*1 です。

①以下のESETプログラムを利用している
　　Windows向け、Windows Server向け、Mac向け、Linux Desktop向け、Linux Server向け
②以下機能を有効にしている
　　リアルタイム保護、Webアクセス保護、ESET LiveGrid
③ESET PROTECT Advanced、Complete、Elite、MDRのいずれかのライセンスを利用している

※ESET PROTECT Entry ライセンスの場合は基本機能の提供のみ。ESETの既存の防御技術によって提供される機能にとどまる。

プログラム名	概要
ESET Endpoint Security (EES)	Windowsクライアント向け総合セキュリティプログラム
ESET Endpoint アンチウイルス (EEA)	Windowsクライアント向けウイルス・スパイウェア対策プログラム
ESET Server Security for Microsoft Windows Server	Windows Server向けウイルス・スパイウェア対策プログラム
ESET Endpoint Security for macOS	Macクライアント向け総合セキュリティプログラム
ESET Server Security for Linux	Linux Server向けウイルス・スパイウェア対策プログラム
ESET Endpoint アンチウイルス for Linux	Linux Desktop向けウイルス・スパイウェア対策プログラム

*1.2026年11月時点では製品設定にESET AI Securityに関わる項目はございません。

©Canon Marketing Japan Inc.

3. ESET AI Securityでの保護

(2) ESET AI Securityの機能

AI Agent Security は**エージェントが取り込む外部構成要素を保護**し、AI Behavioral Monitoring は**エージェントが稼働を開始した後の動作を制御**します。
両者を組み合わせることで、**予防的な防御と、クライアント上での実行時制御を提供**します。

AI Agent Security

主に**AIエージェントが取り込むものを保護**
悪意のある、または侵害されたAI スキルファイルを、
AIエージェントが利用する前に検知してブロックすることが可能
※2026年11月時点では、悪意のあるAIスキルファイルの検知が中心です。
ユースケース例

- 悪意のあるスキルファイルについて、AIエージェントが**ダウンロードまたは実行する前に検知してブロック**
- AIエージェントが、ディスク上に既に存在する**侵害されたファイルを取り込むことを防ぐ**

AI Behavioral Monitoring

主に**AIエージェントの振る舞いを監視**
不審または悪意のあるファイルへのアクセス検知、コマンド実行や
レジストリへのアクセスなどリスクの高い活動の監視
ユースケース例

- プロンプトインジェクションによる**悪意のある動作実行を検知**
- AIエージェントが認証情報、機密ファイル、ソースコードへ**アクセスまたは流出させようとする動作を検知**
- リスクの高いシェルコマンドの実行やプロセス、ファイル操作、
  レジストリ操作を監視

＊ 検出結果は各種ESETプログラムの検出ログよりご確認いただけます。

©Canon Marketing Japan Inc.