

生成AI・AIエージェントの利用リスクを無償で確認する

『AI Security Check 2026』の提供を開始

グローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、国内企業を狙うサイバー攻撃が増加し、ランサムウェア被害・個人情報漏えいが相次ぐ中、企業におけるAI活用の拡大を踏まえ、生成AI・AIエージェントの利用状況とセキュリティ上の課題を専門家が簡易的に確認する『AI Security Check 2026』を、先着10社に無償で提供します。

相次ぐサイバー攻撃への不安を、具体的な点検・対策へ

AI利用リスクを無償で確認 「AI Security Check 2026」 先着10社に提供

セキュリティ見直しの機運が高まる今、
生成AI・AIエージェントという新たな『守るべき領域』も点検

当社は、相次ぐ企業の情報漏えいやサイバー攻撃を受け、2026年10月6日、初動相談・初期調査に無償で対応する「緊急セキュリティ相談窓口」を開設しました。

企業を取り巻くセキュリティリスクが多様化する中、生成AIやAIエージェントなどの業務利用が急速に広がり、従来のIT環境だけでなく、AIの利用状況や接続先、取り扱うデータについても把握・管理する必要性が高まっています。今回、企業のセキュリティ見直しを支援する取り組みの一環として、業務におけるAIの利用実態とリスクを把握し、優先的に確認・対応すべき課題を整理する『AI Security Check 2026』を提供します。

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 広報：さりー（井野部）Mobile: 080-4486-0029

TEL: 03-6416-9996 E-Mail: pr@cscloud.co.jp FAX: 03-6416-9997

■ 『AI Security Check 2026』 提供の背景

国内では、不正アクセスや情報漏えい、ランサムウェア被害などの公表が相次ぎ、企業が自社のセキュリティ対策を見直す必要性が高まっています。

同時に、AI活用の進展に伴い、企業が守るべき対象も広がっています。ChatGPTなどの生成AIに加え、社内データを参照するRAGや、業務システムと連携して処理を実行するAIエージェント、AIと外部ツール・データを接続するMCPなど、AIの利用は情報の入力・生成にとどまらず、社内のデータや業務プロセスに深く関わるものへと変化しています。

独立行政法人情報処理推進機構（IPA）が公表した「情報セキュリティ10大脅威2026」でも、「AIの利用をめぐるサイバーリスク」が組織向け脅威の第3位に初めて選出されました。AIへの不十分な理解に起因する意図しない情報漏えいや、AIの悪用によるサイバー攻撃の容易化・巧妙化など、多様なリスクが指摘されています。

こうした中、企業には従来のIT環境に加え、業務で利用するAIについても、誰がどのように利用し、どのような情報を扱い、どのシステム・サービスと接続しているのかを把握することが求められます。

「自社のAI利用は安全なのか」「どこから対策すべきか」といった不安を具体的な点検・対策につなげるため『AI Security Check 2026』を通じて、企業のAI利用実態と優先的に取り組むべき課題の整理を支援します。

出典：IPA「[情報セキュリティ10大脅威 2026](#)」

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 広報：さりー（井野部）Mobile: 080-4486-0029

TEL: 03-6416-9996 E-Mail: pr@cscloud.co.jp FAX: 03-6416-9997

■『AI Security Check 2026』とは



専門家によるオンラインヒアリングを通じて、主に以下の観点から、企業におけるAIの利用状況とセキュリティ上のリスクを簡易的に確認します。

- 利用実態：社内で利用している生成AI・AIエージェントと、その利用者・利用目的
- 取り扱う情報：AIに入力・連携している機密情報や個人情報
- アクセス権限：AIがアクセスできる社内データ・システムと、付与されている権限
- ルールの運用：AI利用ルールの整備状況と、実際の利用状況とのギャップ
- 外部との接続：MCPなどを介した外部ツール・サービスとの接続状況
- 管理・対応体制：AI利用ログの取得・管理、監査、インシデント対応の体制

誰が、どのAIを、何のために利用し、どのデータやシステムと接続しているのかを確認し、優先的に改善すべき事項を整理します。

■AIを安全に活用できる環境づくりを支援

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 広報：さりー（井野部）Mobile: 080-4486-0029

TEL: 03-6416-9996 E-Mail: pr@csccloud.co.jp FAX: 03-6416-9997

株式会社サイバーセキュリティクラウド

当社は、AIの活用を推進するうえで、利用実態とリスクを把握し、それぞれに応じたルールや技術的な管理の仕組みを整えることが重要だと考えています。

本チェックを通じて、より詳細な確認・対策が必要と判断された場合には、課題に応じて『AI ガバナンスアセスメントサービス』による詳細評価や、AIガバナンスプラットフォーム『AI MONBAN』による技術的な統制を支援します。

また、自社サービスや業務システムにLLM、RAG、AI エージェント、MCP 等を組み込んでいる企業には『AI アプリケーション脆弱性診断サービス』も提供しています。

企業が「使う AI」を守る。企業が「つくる AI」を守る。

当社は、AIの導入・利用から開発・運用まで、AI活用のライフサイクル全体にわたるセキュリティを支援してまいります。

■『AI Security Check 2026』概要

項目	内容
対象	生成AI・AI エージェントを業務利用、または導入を検討している法人
内容	AIの利用状況、取り扱う情報、アクセス権限、利用ルール、外部接続、ログ管理・対応体制などの簡易チェック
費用	無償
実施方法	専門家によるオンラインヒアリング
対象企業数	先着10社

■『AI Security Check 2026』のお申し込みフォーム

お申し込みフォーム：<https://lp.cscloud.co.jp/ai-governance-quick-assessment/inquiry/>

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 広報：さりー（井野部）Mobile: 080-4486-0029

TEL: 03-6416-9996 E-Mail: pr@cscloud.co.jp FAX: 03-6416-9997

報道関係者各位

PRESS RELEASE



2026年10月7日

株式会社サイバーセキュリティクラウド

株式会社サイバーセキュリティクラウド (<https://www.cscloud.co.jp>)

所在地 : 〒141-0021 東京都品川区上大崎3-1-1 JR東急目黒ビル13階

代表者 : 代表取締役社長 兼 CEO 小池 敏弘

設 立 : 2010年8月

「世界中の人々が安心安全に使えるサイバー空間を創造する」をミッションに掲げ、世界有数のサイバー脅威インテリジェンスを駆使したWebアプリケーションのセキュリティサービスを軸に、脆弱性情報収集・管理ツールやクラウド環境のフルマネージドセキュリティサービスを提供している日本発のセキュリティメーカーです。私たちはサイバーセキュリティにおけるグローバルカンパニーの1つとして、サイバーセキュリティに関する社会課題を解決し、社会への付加価値提供に貢献してまいります。

【報道関係者各位の問い合わせ先】

株式会社サイバーセキュリティクラウド 広報:さりー(井野部) Mobile: 080-4486-0029

TEL: 03-6416-9996 E-Mail: pr@cscloud.co.jp FAX: 03-6416-9997