

2026年9月30日
株式会社サイバーセキュリティクラウド

AIの脆弱性を「見つける」から「直す」へ。 『AIセキュリティ改善・実装支援サービス』を提供開始

「AIの暴走」を仕組みで防ぐ。AIセキュリティとAI開発の専門チームがAIアプリケーションを改修

AI セキュリティ改善・実装支援サービス

見つけたAIの脆弱性を、 「直し方」の設計から 実装まで。

AIセキュリティの専門家とAI開発の専門家が連携し、
課題を具体的な改善策へ落とし込み、設計・実装までを一気通貫で支援。

AIセキュリティの改善を相談する

支援内容を見る

☑ 当社・他社・自社評価の診断結果から相談できます。
内容を確認のうえ、支援範囲を決めます。



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、AIアプリケーションの脆弱性診断などで明らかになったセキュリティ上の問題について、原因分析、改善方針の具体化から設計・実装までを専門チームが一気通貫で支援する『AIセキュリティ改善・実装支援サービス』を、2026年9月30日より提供開始します。

現在、AIの活用は文章生成や検索から、社内データを参照するRAG、外部サービスと連携するMCP、さらにはAI自身が判断して外部システムを操作するAIエージェントへと急速に広がっています。これに伴い、AIセキュリティで考慮すべきリスクも「AIが間違ったことを言うリスク」から「AIが間違ったことをするリスク」へと拡大しています。実際に、AIエージェントが意図しない操作を行うなど、いわゆる「AIの暴走」も国内外で報じられており、AIに与える権限や人による承認、外部システムとの接続など、AIアプリケーションそのものを安全に設計・実装する重要性が高まっています。

当社は2026年7月、こうしたAI固有のリスクを攻撃者の視点で検証する『AIアプリケーション脆弱性診断サービス』を開始しました。一方、診断によって問題を発見しても、実際に改善するためには、改善方針を具体的なセキュリティ要件やシステム設計へ落とし込み、既存システムの構成や性能、利用者の使い勝手なども考慮しながら実装する必要があります。

そこで当社は、AIアプリケーションの脆弱性を「見つける」だけでなく、改善方針を決め、設計し、実際に「直す」ところまでを支援する本サービスの提供を開始します。

■『AIセキュリティ改善・実装支援サービス』概要

AI セキュリティ改善・実装支援サービス 概要図

診断等で見つかったAIの脆弱性を、改善方針の具体化から設計・実装まで一気通貫で支援



AIセキュリティの専門チームが、診断結果をもとに脆弱性の根本原因や想定される攻撃経路を分析し、改善方針とセキュリティ要件を策定します。AI開発の専門チームと設計段階から共同で検討し、既存システムへの影響や性能、使いやすさ、開発負荷を踏まえ、具体的な実装タスク・仕様へ落とし込みます。

個々の指摘への対処にとどまらず、複数の脆弱性に共通する原因まで分析し、リスク低減に向けた設計・実装を支援します。

【サービス提供の流れ】

- 1. 分析：**診断結果・システム構成を確認し、脆弱性の原因や想定される攻撃経路を分析します。
- 2. 方針策定：**分析結果をもとに改善の優先順位を整理し、AIセキュリティ要件を定義します。
- 3. 設計・実装：**セキュリティ要件をAIアプリケーションの設計へ落とし込み、必要な実装・改修を行います。
- 4. セキュリティレビュー：**合意したセキュリティ要件が、設計・実装へ適切に反映されているかを確認します。

※ 改善後のAIアプリケーションを攻撃者の視点で検証し、対策の有効性を確認する再診断は、オプションとして提供します。

【主な改善・実装領域】

標準の支援対象は、以下のAI固有のセキュリティ領域です。対象システムの構成や課題に応じて、必要な対策を選定します。

【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 広報担当：さりー（井野部）
Mobile：080-4486-0029（さりーいのべ） / E-Mail：pr@cscloud.co.jp

- **LLM・プロンプト**
プロンプトインジェクションやシステムプロンプトの漏えいなどに対し、入力・出力の検証や指示構造の見直しを組み合わせた多層防御を実装します。
- **RAG**
利用者の権限に応じた検索制御やデータの分離により、閲覧権限のない情報がAIを通じて開示されるリスクを低減します。
- **AIエージェント**
利用できるツールや権限を必要最小限に絞り、重要な操作には人の承認を組み込むことで、AIによる意図しない操作のリスクを低減します。
- **MCP・外部ツール連携**
接続先の制御、実行時の引数検証、認証情報の管理、実行履歴の記録などにより、AIが生成した指示を無条件で外部システムへ渡さない仕組みを構築します。
- **AIデータ**
個人情報や営業秘密などについて、AIへの入力・参照・出力が許される範囲を整理し、機密情報の検知・マスキングなどを実装します。

※ 上記以外の、Web・APIの認証・認可やクラウド上の権限管理など、周辺領域の改修が必要な場合もオプションにて対応します。

【企業の開発体制に応じた支援方法】

- **実装助言**：お客様の開発チームが実装し専門チームが改善設計や実装上の助言、レビューを支援
- **共同開発**：お客様の開発チームと専門チームが共同で実装
- **実装代行**：専門チームが改善方針の策定から設計・実装までを担当

当社が顧客窓口と全体統括を担い、専門チームと連携して支援します。
具体的な実施内容・成果物は、お客様の開発体制や契約範囲に応じて決定します。

■『AIセキュリティ改善・実装支援サービス』についてのお問い合わせ

株式会社サイバーセキュリティクラウド
戦略事業室

TEL：03-6416-9996

URL：<https://www.cscloud.co.jp/ai-security-remediation/>

■サイバーセキュリティクラウドのAIセキュリティ事業の展開について

AI 活用の全てのシーンに製品・サービス投入を計画



© Cyber Security Cloud, Inc. 2026

当社は2026年より本格的にAIセキュリティ領域へ事業を展開しています。4月にAIガバナンスを推進する専門組織『AI Trust Board』を設置したのを皮切りに、6月にはAIの利用を統制する『AI MONBAN』、7月

【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 広報担当：さりー（井野部）
Mobile：080-4486-0029（さりーいのべ） / E-Mail：pr@cscloud.co.jp

にはAI固有の脆弱性を見つける『AIアプリケーション脆弱性診断サービス』、8月にはAIの管理体制を評価する『AIガバナンスアセスメントサービス』の提供を開始しました。
今回、見つかった問題を「直す」本サービスを加えることで「統制する」「を見つける」「評価する」「直す」の各側面から、企業のAI活用を支援するサービス体制を拡充します。

サービス	対象	役割
AI MONBAN	企業内のAI利用・AIと社内システム間のデータフロー	- 社内システムとAIの間に置くゲートウェイ - 利用中のAIと接続することで、外側から「統制する」
AIアプリケーション脆弱性診断サービス	LLM、RAG、MCP、AIエージェント等を活用したAIアプリケーション	- 専門家による診断と改善・緩和策の提示 - AI固有の脆弱性を「を見つける」
AIガバナンスアセスメントサービス	企業内のAI利用実態・管理体制	- 専門家による調査・評価、改善ロードマップの提示 - AI利用の管理体制を「評価する」
AIセキュリティ改善・実装支援サービス	LLM、RAG、MCP、AIエージェント等を活用したAIアプリケーション	- 専門家による原因分析、改善方針の具体化、設計・実装支援、セキュリティレビュー - 見つかった問題を「直す」

AIは企業競争力を左右する重要なインフラとしてすでに存在感を高めています。当社は企業のAI活用のあらゆるシーンに対応する製品・サービスを計画的に投入し、安心・安全にAIを利活用できる環境を提供することで、企業成長を支援してまいります。

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 広報担当：さりー（井野部）
Mobile：080-4486-0029（さりーいのべ） / E-Mail：pr@cscloud.co.jp