

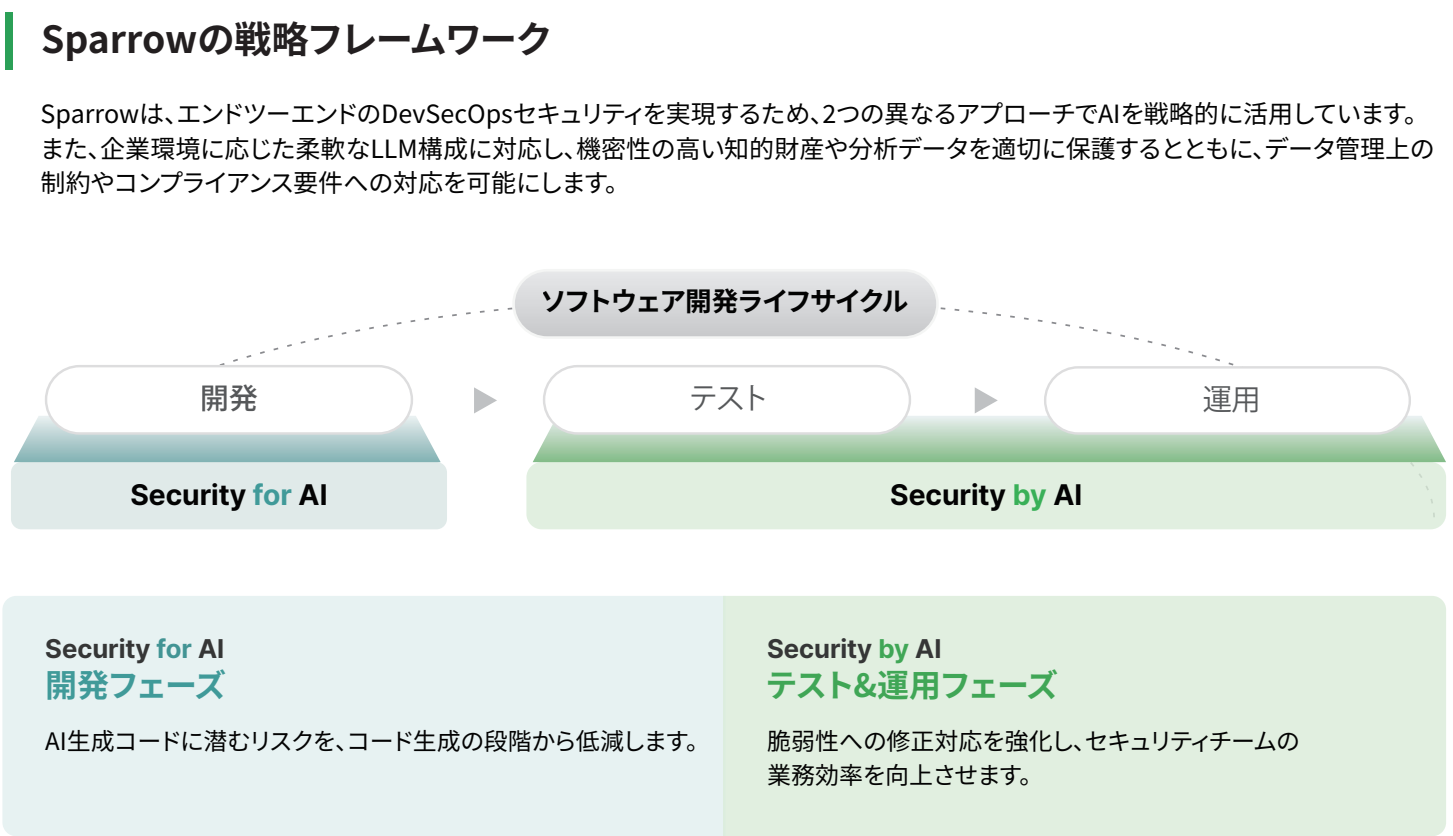
エグゼクティブサマリー

生成AIと大規模言語モデル (LLM) は、ソフトウェア開発ライフサイクル (SDLC) を大きく変革し、コードの生成を飛躍的に加速させています。

従来のセキュリティ対策では、このスピードに対応することが難しくなっており、アプリケーションセキュリティテスト (AST) と企業のリスク管理には、新たなアプローチが求められています。アプリケーションセキュリティには、AI生成コードの安全性を確保すると同時に、AIを活用して防御能力をさらに高めることが求められます。

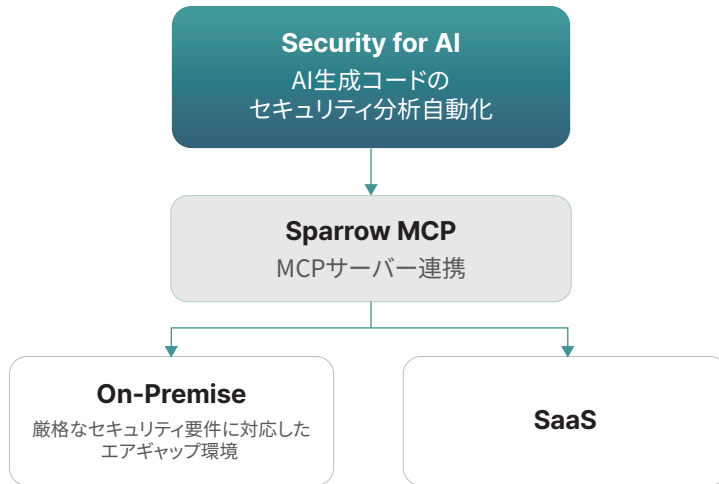
AI時代の主要課題

課題領域	ビジネスへの影響とリスク要因
拡大する攻撃対象領域 (AI生成コード)	AI生成コードは、特有の脆弱性を含んだままデプロイされることがあります。急速に進む開発スピードに対応し、ソフトウェアサプライチェーンへの攻撃を防ぐには、大規模かつ自動化されたセキュリティ検証の仕組みが不可欠です。
修復のボトルネック	脆弱性の検出件数が急増する一方で、多くの組織では、その優先順位付けや修正対応が追いついていません。従来のルールベースの手法では効率的な対応が難しく、脆弱性が修正されないまま放置される期間が長期化しています。



Security for AI: 自動検証とDevSecOpsの統合

プロンプト入力の段階からセキュリティを組み込むことで、Sparrowは開発者の生産性を維持しながら、AI生成コードのセキュリティリスクを根本から低減します。



Sparrow MCP連携

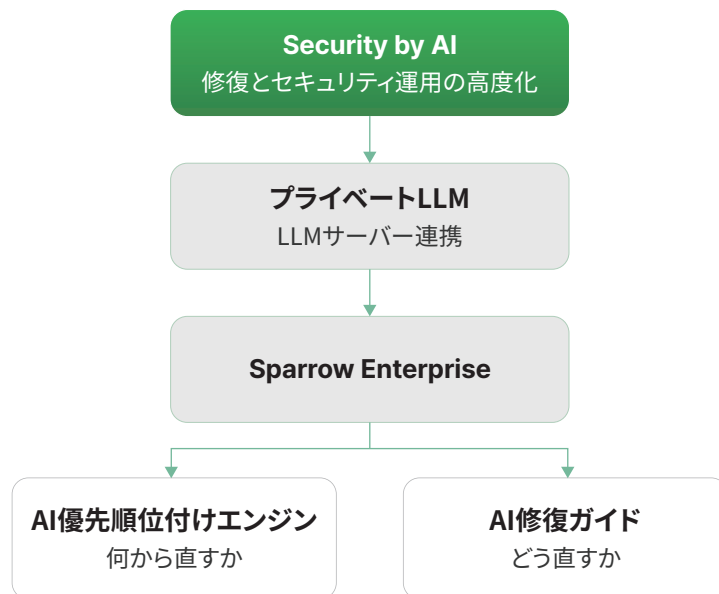
SparrowはModel Context Protocol (MCP) サーバーと連携し、AIコーディングアシスタント上でソースコードの詳細解析やオープンソースの構成解析を直接実行することで、セキュリティテストを自動化します。

ソフトウェアサプライチェーンセキュリティ (SBOM)

AI生成コードに含まれるオープンソースソフトウェアを自動的に識別し、標準形式のソフトウェア部品表 (SBOM) を生成することで、ソフトウェアコンポーネントの可視化を実現します。

Security by AI: インテリジェントな修復と運用効率の向上

Sparrowは、重大度の高い脆弱性に対して適切な修正案を提示し、検出から修正までのプロセスを効率化することで、平均修復時間 (MTTR) を短縮します。



AIによる優先順位付けエンジン

AIが検出した脆弱性を、資産の重要度や企業のリスク特性を踏まえて総合的に分析し、リスクに応じた最適な修正優先順位を提示します。

AI修復ガイド

開発者に安全なコード修正案と状況に応じた修正例を提示し、修正方法の検討や対応にかかる負担を大幅に軽減します。

プライベートLLMとSparrow Enterpriseの連携

ASTの解析結果を企業のプライベートLLMと照合し、検出結果の妥当性を検証することで誤検知を適切に除外し、セキュリティ運用を最適化します。

Sparrow製品 ラインアップ

Sparrow Enterprise



製品資料を
ダウンロード

Sparrow Enterprise AI Package



製品資料を
ダウンロード