

# AI を活用したソリューションで AI がもたらすリスクに対応

「Black Duck の導入後、  
手動コード・レビューにかかる  
時間が大幅に短縮され、  
検出されたセキュリティ問題が  
迅速に解決されるようになり、  
効率性と開発者の満足度が  
共に向上しました。」

Black Duck SCA によって、  
セキュリティ、ライセンスへの  
準拠、当社のソフトウェア・  
サプライ・チェーンの質に  
対する自信が高まりました。  
これは単なるツールではなく、  
安全なアジャイル開発を  
戦略的に実現する手段です。」

—Dan Mazor,  
ITAM / Black Duck SME,  
CGI Group

AI によって、ソフトウェアの開発と構築のパイプラインが劇的に変化しています。しかし、開発ワークフローに AI が急速に導入されたため、セキュリティへの対応が遅れています。Black Duck の「世界の DevSecOps の現状 2024」レポートによると、AI によって生成されたコードをセキュアにする能力に自信がないと回答した人の 93% は、不安を抱えながらも一部の開発業務で AI を利用し続けています。このため、技術的負債の増大、セキュリティの低下、知的財産 (IP) が危険にさらされるといったリスクが生じています。

この新たな状況では、AI によって実現するソフトウェア開発の高速化と大規模化に対応できるように、先進的なアプリケーション・セキュリティ・テストのアプローチが求められています。このアプローチにより、AI 時代の DevSecOps のために回復力と柔軟性を備えた基盤を築くことができます。

**48%** Black Duck の顧客は、本稼動環境に混入する重大度の高い不具合が  
**48% 低下**したことを確認しました。<sup>1</sup>

**22%** Black Duck の導入後、開発者が問題を管理するための時間が短縮され、  
新しいコードの記述に充てることができる時間が **22% 増加**しました。<sup>2</sup>

## AI がもたらす新たなリスクの状況

AI によって新たなソフトウェア・リスクが生じており、既存のセキュリティ・ワークフローでは対応が困難です。GitHub Copilot のような AI コーディング・アシスタントを利用しているか、コードに AI を組み込んでいるかにかかわらず、開発チームは、新たな一連のリスクを管理するために役立つツールを必要としています。

## セキュアでないコードの大規模な拡散

開発チームは、通常、AI コーディング・アシスタント・モデルのトレーニングに使用されたトレーニング・データセットを確認できません。AI ツールを無条件に信頼している開発者は、脆弱性があり、セキュアでないコードを知らぬ間にコードベースに混入させ、大規模に複製してしまうおそれがあります。このため、統合され、自動化された静的アプリケーション・セキュリティ・テスト (SAST) の重要性が高まっています。これは、開発者によって記述されたコードと同様に、AI 対応のパイプラインによって決定づけられる量と規模の AI によって生成されたコードを解析します。

## ライセンス違反および知的財産の価値の毀損

大量の公開データセットでトレーニングされた AI ツールにより、オープンソース・プロジェクトから直接抽出されたコード断片 (「スニペット」) が含まれるコードが生成されることは少なくありません。開発者がコードの出所や関連するライセンスについて直接把握していなければ、ライセンス違反のリスクにさらされ、知的財産の所有権に対して異議が申し立てられる可能性が生じます。

<sup>1</sup> Black Duck の「世界の DevSecOps の現状 2024」レポート

<sup>2</sup> 「Black Duck が開発の生産性を高め、リスクを低減し、顧客のコストを低下させる方法 (How Black Duck Drives Development Productivity, Lowers Risk, and Decreases Cost for Customers)」2025 年

## AI 時代に 不可欠なツール

### Black Duck SAST

- AI によって生成されたコードがセキュアで、高品質で、法規を遵守していることを検証します。
- セキュアでない LLM データハンドリングの問題 (OWASP LLM05) を特定します。

### Black Duck SCA

- AI で生成されたコードによって生じるオープンソースのライセンス違反や知的財産リスクを検出します。
- API ベースのオープンソースのスニペット検出を使用して、すべてのコミットでコンプライアンスを徹底します。
- プロジェクト内のオープンソース AI モデルの詳細とリスクに関する知見を得ます。

### Black Duck Assist

- AI によって生成される問題の要約と自動生成されるコード修正の推奨によって修正作業を効率化します。

## Black Duck: 統合された AI 対応のセキュリティとコンプライアンス

Black Duck のソリューションは、AI の規模に対応するよう構築され、業界をリードしている SAST およびソフトウェア・コンポジション解析 (SCA) ソリューションを含み、AI を活用して修正を簡素化および迅速化する機能を備えています。このため、急速に変化している AI 支援開発のリスクに独自の方法で対応することができます。開発チームがセキュリティ、品質、コンプライアンスの問題に対応する準備を整えながら、自信をもってイノベーションを推進してください。

### AI コーディング・アシスタントが生成するコードの検証

AI コーディング・アシスタントでは、かつてないほどスピードで大量のコードが生成されますが、一貫した品質とセキュリティの標準を適用する必要があります。Black Duck Polaris™ Platform、Coverity® 静的解析、Black Duck® SCA を使用して、コミットするたびにスキャンを自動的に実行してください。

- AI が生成するコードにセキュリティや品質上の不具合が混入することを防ぐ
- AI が生成するコードをセキュリティとコーディングの標準に確実に準拠させる
- AI が生成するコードによって知的財産や著作権が侵害される可能性を防ぐ

### AI を活用して安全なコードをより迅速に構築する

AI を活用した当社のセキュリティ・アシスタント Black Duck Assist™ は、セキュリティ上の不具合を速やかに修正し、よりセキュアなコードを記述できるように開発者を支援します。AI が生成する問題の要約は、開発者が、報告されたセキュリティ問題を理解するのに役立ちます。これには、セキュリティ上の不具合が発生する条件、ハッカーがその不具合を悪用するやり方、その問題を修正して再発を防ぐ方法が含まれます。AI によって生成されるコードの修正案では、コードに簡単に貼り付けることができるカスタマイズされた修正が開発者に提供されるため、試行錯誤が不要になります。

## ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。詳しくは、[www.blackduck.com/jp](https://www.blackduck.com/jp) をご覧ください。

### ブラック・ダック・ソフトウェア合同会社

[www.blackduck.com/jp](https://www.blackduck.com/jp)

©2025 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2025 年 12 月