報道関係者 各位

2025 年 10 月 1 日
株式会社 SHIFT

AI の開発・運用ライフサイクル全体のセキュリティを担保する「セキュア AI 開発プロセス構築支援サービス」の提供を開始

AI システムの要件定義から開発、テスト、運用までの全プロセスのセキュリティ対策を網羅

お客様の売れるソフトウェアサービス／製品づくりを支援する株式会社 SHIFT（本社：東京都港区、代表取締役社長：丹下 大、プライム市場：3697、以下 SHIFT）は、AI を搭載したシステムや、AI と連携するシステムの要件定義から開発、テスト、運用に至るまで、開発・運用ライフサイクルのプロセス全体にわたるセキュリティ対策を支援する「セキュア AI 開発プロセス構築支援サービス」の提供を開始します。

AI エンジンの設計、モデルの脆弱性への対応、トレーニングデータの取扱い、挙動の監視など、AI システム特有のセキュリティ観点にもとづき、設計・開発・運用の全工程にわたって実施すべきセキュア開発プロセスを体系化したガイドを策定します。また、策定したガイドを開発チームに定着させるため、開発メンバーの教育や開発プロセスの運用支援を行い、セキュアな AI システムの開発・運用を実現します。

＜提供開始の背景＞

機械学習や深層学習（ディープラーニング）をはじめとする AI 技術の急速な進化と普及により、生成 AI や AI 技術を活用したアプリケーション、さらには自律的に意思決定を行う「Agentic AI（エージェンティック AI）」など、さまざまな分野に特化した AI システムが次々と誕生しています。しかし、これらの AI システムは、プロンプトインジェクションやトレーニングデータの悪用など、新たなセキュリティリスクを伴うため、開発プロセス全般にわたる AI 特有のセキュリティ課題への対応が不可欠となっています。

セキュアな AI システムの開発に関しては、各種ガイドラインが発行されているものの、企業が自社の開発プロセスに適合した形でこれらのガイドラインを実践するには、メインの開発業務に加え、セキュリティエンジニアの配置や育成が必要となります。このような追加の負担により、AI システムのセキュリティ対応は多くの企業にとって高いハードルとなっているのが現状です。

SHIFT はこれまで、さまざまな業界・業種の企業に対し、AI システム開発支援や AI 特化型品質保証をはじめとする AI システムの開発プロセスを支援するソリューションと、生成 AI 活用システム診断や SOC 導入支援をはじめとする運用プロセスを支援するソリューションの提供を進め、AI システムの開発・運用において数多くの実績を積み重ねています。また、システムのセキュア開発・運用支援や、脅威モデリング等のセキュリティソリューションの提供実績も豊富であり、システム開発の上流工程からセキュリティ対策を取り入れるシフトレフトアプローチの実践ノウハウを蓄積してきています。

このような背景から、AI システム開発・運用に対する深い知見と、システムのセキュア開発・運用支援の豊富な実績を活かし、この度、AI システムの開発・運用ライフサイクル全般に渡るセキュリティ対策を支援する「セキュア AI 開発プロセス構築支援サービス」を新たに提供します。

＜「セキュア AI 開発プロセス構築支援サービス」について＞

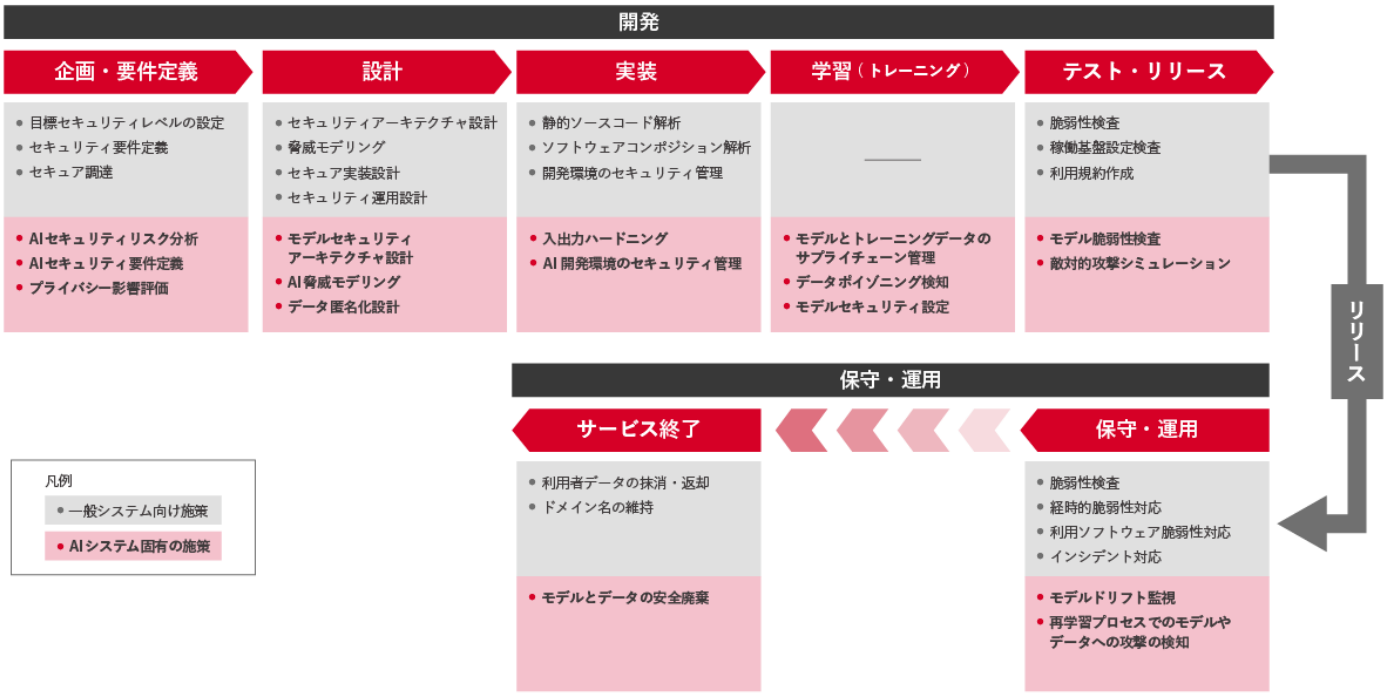
セキュア AI 開発プロセス構築支援サービスでは、お客様の AI システムの開発・運用ライフサイクル全般にわたって、アプリケーション、モデル、インフラストラクチャー、データなどの観点から全方位的にセキュリティ対策を定義し、それらの実践を支援します。

・サービスに関するお問い合わせ：https://service.shiftinc.jp/contact/

■セキュア AI システム開発・運用プロセスを構築するステップ

STEP1 開発・運用プロセス定義フェーズ

お客様の現行の AI システムの開発・運用プロセスを把握し、セキュアな AI システムを開発する上で実施すべきセキュリティ対策を通常のセキュア開発プロセスに追加する形でガイド化します。SHIFT が定めたセキュア AI システム開発・運用プロセスに基づき、実施すべき対策を体系的に整理し、ガイドを作成します。



セキュア AI システム開発・運用プロセス

＜主な支援内容＞

・開発している AI システムの特性や開発プロセス・開発環境などに関する現状分析

・現状分析に基づくセキュア AI システム開発・運用ガイドの策定

STEP2　運営体制整備フェーズ

STEP1 で策定したセキュア AI システム開発・運用ガイドについて、トライアルを通じてフィージビリティを検証すると共に、一連のプロセスを組織内で運営していくための体制・ルール・環境の整備を支援します。

＜主な支援内容＞

・STEP1 で策定したセキュア AI システム開発運用ガイドの最適化

・パイロットシステムでのトライアルによるフィージビリティ検証

・セキュア AI システム開発・運用プロセスに基づく、デザインレビューなどの運営ルールを体系化したマニュアルの策定

・運営体制や運営環境の整備

STEP3　開発・運用プロセス定着化フェーズ

策定・構築したセキュア AI システム開発・運用プロセスの組織定着を支援するとともに、セミナー等を通じて開発メンバーのスキル向上を図ります。

＜主な支援内容＞

・セキュア AI システム開発・運用プロセスに基づくデザインレビュー等の運営トライアル

・デザインレビュー等をおこなう運営事務局業務

・セキュア AI システム開発・運用プロセスや AI 脅威モデリング等に関するセミナー

・サービスに関するお問い合わせ：https://service.shiftinc.jp/contact/

＜SHIFT が提供する主な AI システム開発・運用支援ソリューション＞

SHIFT は、AI システムの開発プロセスの上流から下流までをカバーする、さまざまなソリューションを提供し、多様な業界における高品質な AI システム開発・運用をサポートしています。

■AI 脅威モデリング

脅威モデリングに関する豊富な提供実績に基づき、AI システムアーキテクチャ（アプリケーション層、モデル層、インフラストラクチャー層、データ層）の観点から、AI システムの設計上の脅威を洗い出し、対策案の抽出をおこないます。

■AI システム開発支援

豊富なシステム開発実績と、自社での AI プロダクト開発ナレッジを活かし、お客様のビジネス成功に貢献する AI システムの開発を行います。

■AI 駆動開発

AI エージェントや SHIFT 独自の標準化ノウハウを活用することで、高い開発生産性を発揮しながら、システムの開発・モダナイゼーションを効率的に行います。

■AI 特化型品質保証

AI 固有の品質特性を考慮した、独自の「AI テスト標準観点」と「AI 品質保証フレームワーク」にもとづき、専門チームが、AI／機械学習モデルの開発プロセス全体にわたるコンサルティングを提供。AI システムの開発プロセスにおける品質課題を解決します。

■生成 AI 活用システム診断

生成 AI を活用した Web サービスやシステムの脆弱性を診断します。従来の Web アプリケーション診断では検出できない、生成 AI 固有の脆弱性を、OWASP Top10 for Large Language Model Applications に沿った診断で検出し、セキュリティリスクを可視化し

ます。

＜株式会社 SHIFT について＞

SHIFT は、金融機関などのエンタープライズ領域におけるミッションクリティカルな基幹システムから、EC サイト、スマートフォン向けのアプリ・ゲーム検証まで幅広い分野のお客様に対するソフトウェアの品質保証・テストサービスで事業基盤をつくり成長をつづけてまいりました。現在は、「無駄をなくしたスマートな社会の実現」を目指し、ビジネスの構築からシステムの企画、開発、運用、セキュリティやマーケティング領域、さらには DX 推進まで、お客様の IT にまつわるあらゆるビジネス課題の解決を支援しています。

名　　称	株式会社 SHIFT
代　　表	代表取締役社長　丹下　大
住　　所	東京都港区麻布台 1-3-1　麻布台ヒルズ森 JP タワー
U　R　L	コーポレートサイト https://www.shiftinc.jp/　サービスサイト https://service.shiftinc.jp/

【本プレスリリースに関するお問い合わせ】
株式会社 SHIFT　広報 IR 部　広報室　　Email：pr_info@shiftinc.jp