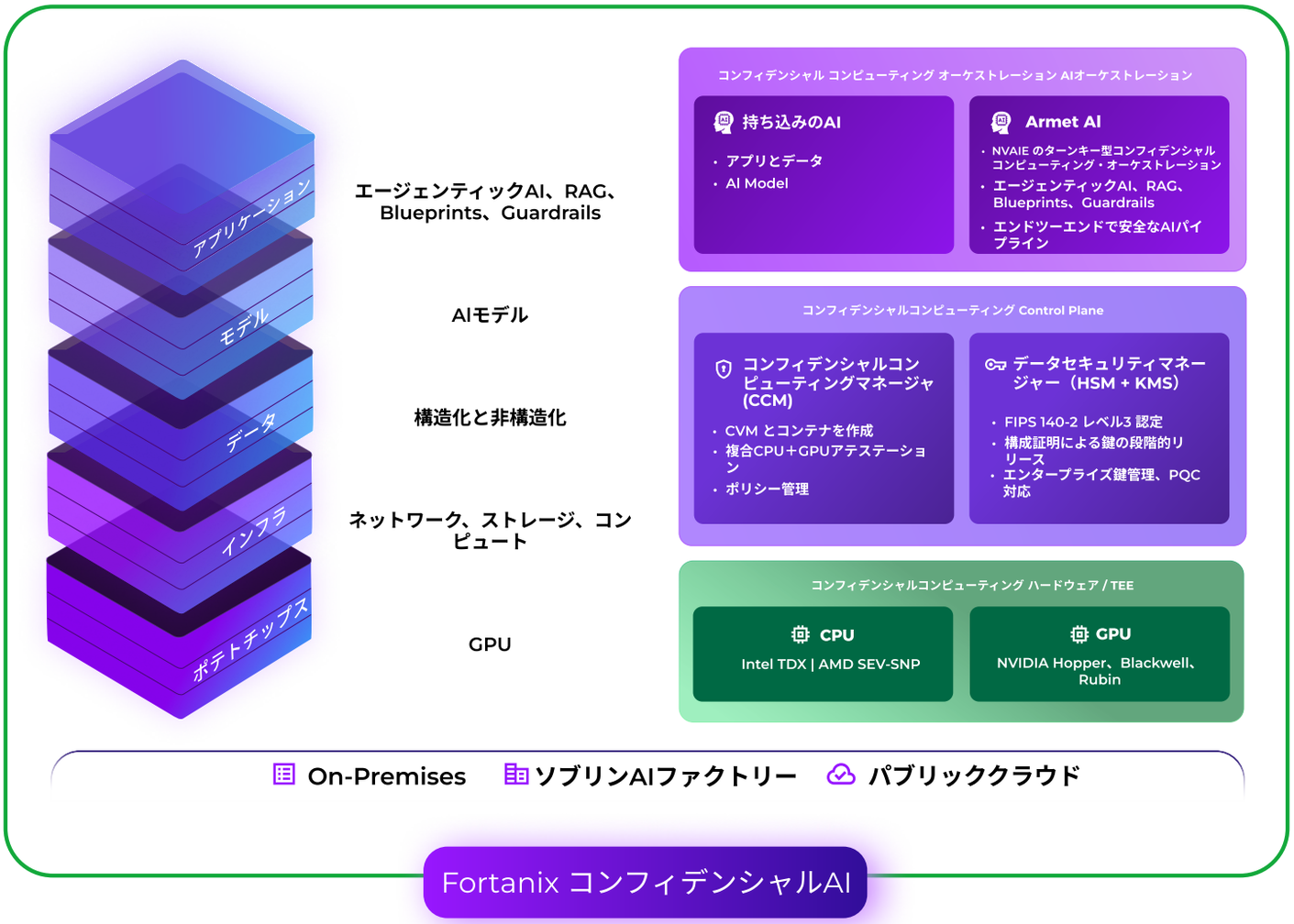
Fortanix コンフィデンシャルAI

AIライフサイクル全体でAIモデルと機微データを保護する

データ漏えいと知的財産の窃取は、企業や各国におけるAI導入を阻んでいます。企業のITリーダーの半数超が、データセキュリティ上のリスクをAI導入の根本的な障壁として挙げる一方で、AIモデルの所有者は、AIファクトリー、クラウドプラットフォーム、エッジインフラなどの第三者環境で自らの価値ある知的財産を展開することに慎重です。従来型のインフラ環境では、管理者アクセスによりデータとAIモデルの双方が処理中に完全に可視化され、推論や学習の際には機微なデータがメモリ上で暗号化されないまま存在し、AIモデルも抽出攻撃に対して脆弱なままです。ゆえにジレンマは残ります——最も貴重な資産を危険や露出にさらすことなく、いかにAIイノベーションを前進させるのか。

Fortanix コンフィデンシャルAI

Fortanix コンフィデンシャルAI は、機密性、信頼性、主権を損なうことなく AI の革新を加速するために、稼働中の専有 AI モデルと機微データの両方を保護し、AI 導入の障壁を取り除くのに役立ちます。NVIDIA と Fortanix の共同ソリューションは、セキュアでハードウェア的に分離された環境で計算を実行することにより、稼働中の AI モデルとデータを保護するために設計された専用のコンフィデンシャル・コンピューティング対応 GPU 上に構築されています。これらの Trusted Execution Environment（TEE：信頼実行環境）は、ほかのハードウェアやオペレーティングシステムから分離されています。これにより、特権を持つ内部者からであっても、機微データや専有モデルの機密性が維持されることを暗号学的に保証しながら、AI ワークロードを実行できます



Fortanix コンフィデンシャルAI の仕組み

セキュアエンクレーブ管理

ntel TDX と AMD SEV-SNP の CPU に加え、NVIDIA Hopper、Blackwell、そして今後登場する Rubin の機密計算対応 GPU を活用し、Fortanix Confidential Computing Manager（CCM）で安全なエンクレーブを作成・管理できます。AI ワークロードを OS、ハイパーバイザー、管理者から分離できます。Trusted Execution Environment（TEE）のポリシーを制御し、適用できます。

AIワークロードを持ち込もう

Bring Your OwnAIモデル、またはFortanix Armet AIを含むサードパーティ提供のモデル（エージェンティックAIのオーケストレーションを実現するターンキー・プラットフォーム）を活用し、貴社のAI戦略とニーズを支援します。

構成証明 検証

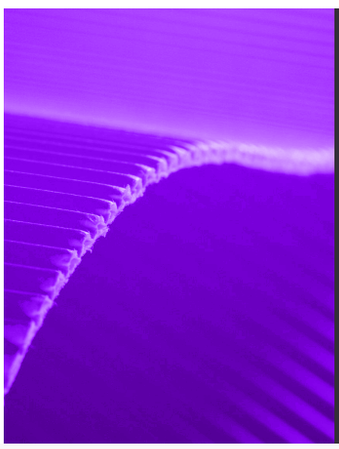
暗号化されたアセットやアーティファクトを送信する前に、Fortanix CCM による暗号学的アテステーションでリモートの TEE を検証してください。実行中のコードが正確に一致していること、そしてハードウェアの分離が本物で改ざんされていないことを確認します。

セキュアキーリリース

暗号鍵は、検証・証明済みのTEEにのみ送信されます。Fortanix データセキュリティマネージャ(DSM) という、KMSを内蔵したFIPS 140-2 レベル3のHSMを用いて、厳格な鍵の保管管理と役割ベースのアクセス制御を適用し、データやモデルが使用中もメモリ上で暗号化されたまま維持され、TEEの外部にいる者からはアクセス不可能であることを確実にします。

包括的なAIライフサイクル保護のメリット

- **モデルの知的財産を保護する:** AIモデルを、知的財産を開示することなく、サードパーティの環境やクラウドプラットフォーム、エッジ環境にデプロイできます。
- **コンフィデンシャル推論:** 機密性の高い入出力を、インフラ提供事業者に公開せずに処理します
- **データ漏えいを防ぐ:** AIワークロードで使用するデータが、処理中であっても常に暗号化されたままであることを確保してください。
- **複数者間の協働:** 基盤となる資産を開示することなく、組織間でデータ共有とモデルへのアクセスを可能にします。
- **ゼロトラスト・アーキテクチャ:** 保護は、ソフトウェア方針ではなく、CPU と GPU のシリコンに対する証明付きの暗号学的検証によって裏付けられており、クラウド事業者、インフラ運用者、または管理者を信頼する必要性を排除します。
- **コンプライアンス対応:** Cloud Act、PII、PHI、機微（センシティブ）データ保護に関する規制要件を満たす



AIは、私たちが製薬の研究開発を具体的に変革するために立ち上げた各種イニシアチブの基盤となっています。しかし、モデルには、しばしば機微情報や個人情報を含む非常に大量のデータが必要です。FortanixとNVIDIAのコンフィデンシャルコンピューティングは、そうしたプライバシーとセキュリティに関する懸念を本質的に解消すると同時に、モデルの精度も向上させます。これは業界全体にとってウィンウィンの状況となるでしょう。」

Hiroki Makiguchi
CTO at Xeureka.

Xeureka

About Us

FortanixはデータとAIセキュリティのグローバルリーダーであり、コンフィデンシャルコンピューティングの先駆者として、オンプレミスおよびマルチクラウド環境で保存時・転送時・使用時の機密データ、AIモデル、アプリケーションを保護する統合プラットフォームを提供しています。ハードウェアで強制されたセキュリティを基盤に、Fortanixはワークロードを改ざん不可能な分離エンクレーブ内で実行可能にし、特権を持つ内部者からであっても、データ漏えい、モデル抽出、不正アクセスから保護します。