AI の保護とライセンシング

Wibu-Systems が手掛けるソリューションと研究活動

Nicolai Ruhnau
WIBU-SYSTEMS AG



WIBU SYSTEMS

目次

はじめに 2

AI 資産と、その攻撃対象 3

Wibu-Systems の AI 保護と
ライセンシングソリューション 4

研究プロジェクト 6

サマリー 6

著者

Nicolai Ruhnau は、ミュンヘン専門学校で、分散情報システムを専攻し、学士論文で賞を獲得して、学位（理学）を取得。その後、ルートヴィヒ=マクシミリアン大学（ドイツ・ミュンヘン）の大学院に進学し、自然言語処理の研究で修士号（理学）を取得。

2015 年より、ミュンヘンとカールスルーエにおいて、多種多様な業種や分野で、ソフトウェアエンジニアとして従事。2023 年、WIBU-SYSTEMS AG に入社し、人工知能（AI）分野の最先端研究プロジェクトに参加。

はじめに

2023 年 8 月にガートナーが発表した産業レポート「先進テクノロジのハイプ・サイクル：2023 年」が示すように、コンピュータービジョンをはじめとした人工知能（AI）技術は、研究レベルの黎明期を脱し、今や、実世界のあらゆる分野にて応用が進んでいます。

「AI からの保護」「AI による保護」「AI の保護」はそれぞれ、区別して考える必要があります。革新的なセキュリティ技術を専門に扱う Wibu-Systems もまた、これらの問題に取り組んでいます。ライセンスの管理・バインディング、またはコード保護の強化に、AI を使用できるだけでなく、その AI 自体の保護やライセンシングも可能です。本ホワイトペーパーでは、後者のテーマに焦点を当てることにします。

機械学習（ML）ライフサイクルにおける保護の重要性が、複数の文献より指摘されているように、近年、Wibu-Systems でも、この分野に関する専門知識を深めてきました。

弊社のユーザーが利用する機械学習技術は多種多様であり、中でも、医療診断や工場の品質管理は、その代表的なユースケースと言えるでしょう。これらのアプリケーションは通常、ChatGPT や他のクラウドサービスとは、要件が大きく異なります。

攻撃者がアクセスできるような環境にある AI モデルや、アプリケーションにおける知的財産（IP）は、どのように保護すればよいのでしょうか。また、特定のライセンシング、マーケティング、更新に関する留意事項（例：オフラインマシンにおけるアクセス制御）の対処方法には何があるでしょうか。このように、AI モデルを提供するにあたり、ライセンシングに関しても、新たな課題と機会が生じます。

さらに機械学習には、独自のライフサイクルという特殊性が存在することも理解する必要があります。モデルを本番環境に適応させるには、展開、モニタリング、そして継続的なメンテナンスが不可欠です。こうした問題はしばしば、Model Operation や ML-Ops（Machine Learning Operations）と表現されます。

2023 年のガートナーによる調査結果にもあるように、これらの保護とライセンシング要件に対するソリューションは、未だ発展途上にあります。

間もなく施行予定の、EU による AI 規制法は、倫理面と安全面とを重視し、今後数年間の規制の方向性を定めることでしょう。こうした状況を踏まえても、今から行動を起こし、ML-Ops を戦略的に設計する企業は、産業全体が守るべき新たなコンプライアンス要件との相乗効果を期待することができるはずです。

AI 資産と、その攻撃対象

機械学習アーキテクチャーに含まれる AI 資産

図 1の機械学習アーキテクチャーは、企業が保護またはライセンシングを望む様々な知的財産 (IP) と、その保護目的を示しています。知的財産 (IP) は、モデルそのものに限らず、訓練データ、経験や専門知識に基づくデータの前処理方法など、あらゆるものに含まれています。

スマートなライセンシングソリューションによって、さまざまなユースケースが実現可能となります。

- モデルは、ペイ・パー・ユーズモデルに基づくオンライン販売、またはオフラインの大型マシンの一部としての組み込みも可能です。アクセスは、役割、場所、時間に応じて制御することができます。
- もうひとつの困難な要件として、ユーザー側の AI モデル保護のロジスティクスと、便利で柔軟なライセンスメカニズムの組み合わせが挙げられます。

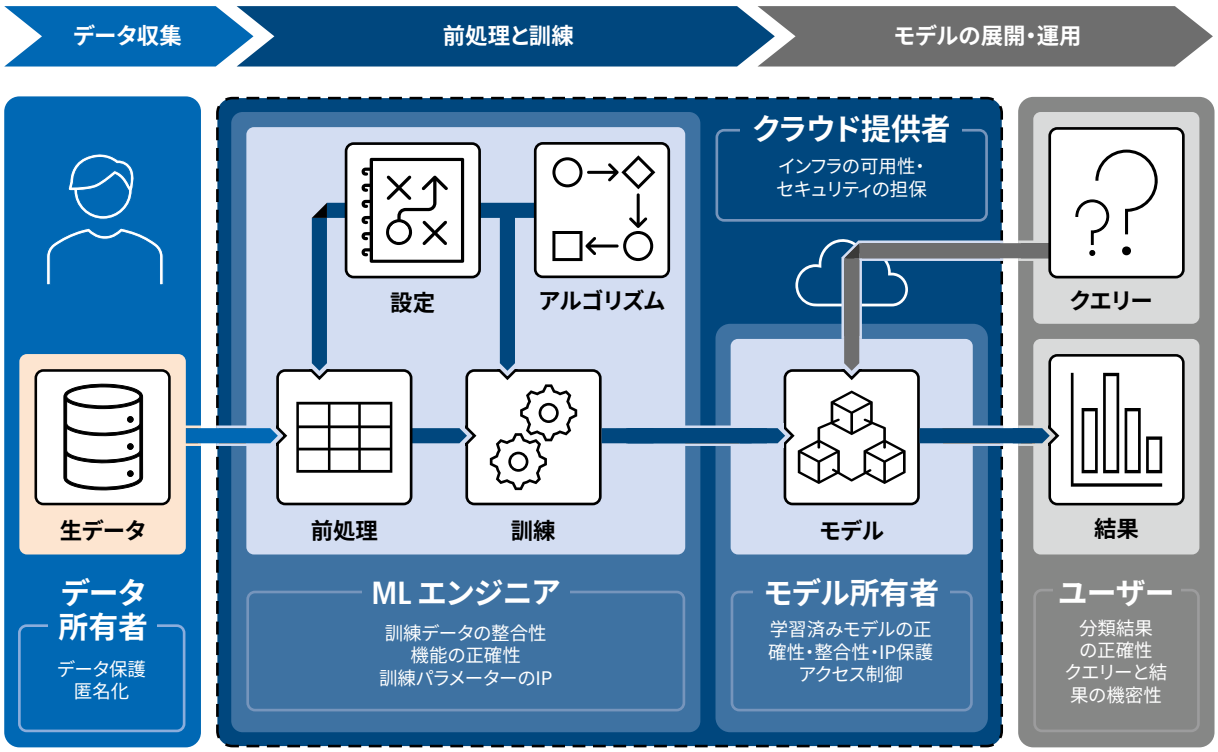


図 1：機械学習ライフサイクル

攻撃対象

機械学習ライフサイクルは、様々な攻撃に対して脆弱であり、その影響は開発と運用の全ての段階に及びます。最終的な予測結果が、安全で信頼できることを保証するためにも、元となる訓練データへの不正アクセスや改ざんを防ぐ必要があります。

また、動的で多くのデータを含む機械学習ライフサイクルは、基礎となるデータやモデルに対する、リバースエンジニアリングの防止、さらには、更新プロセスの管理など、特有の課題を抱えています。

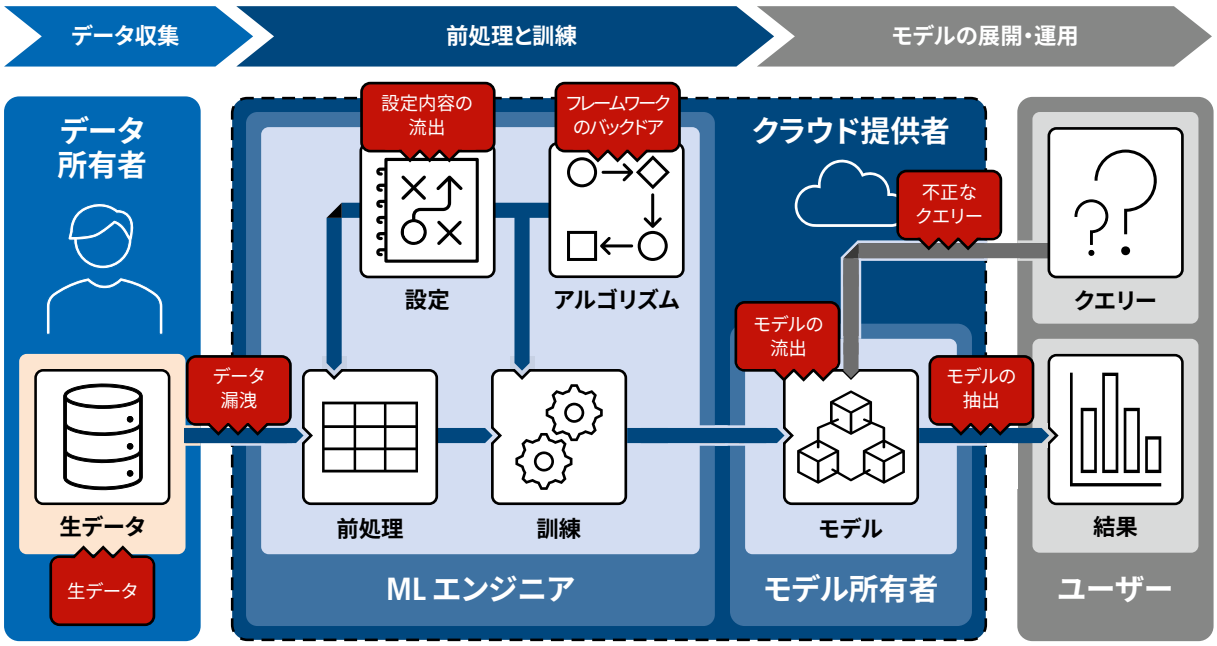


図 2：機械学習アーキテクチャーにおける攻撃対象

Wibu-Systems の AI 保護とライセンシングソリューション

CodeMeter と AxProtector

Wibu-Systems は、CodeMeter と AxProtector によって AI の保護とライセンシングに関する多くの課題を解決します。これにより、C++ や Python で書かれた機械学習ライブラリやプログラムに、柔軟かつ堅牢な保護レイヤーを導入することができます。

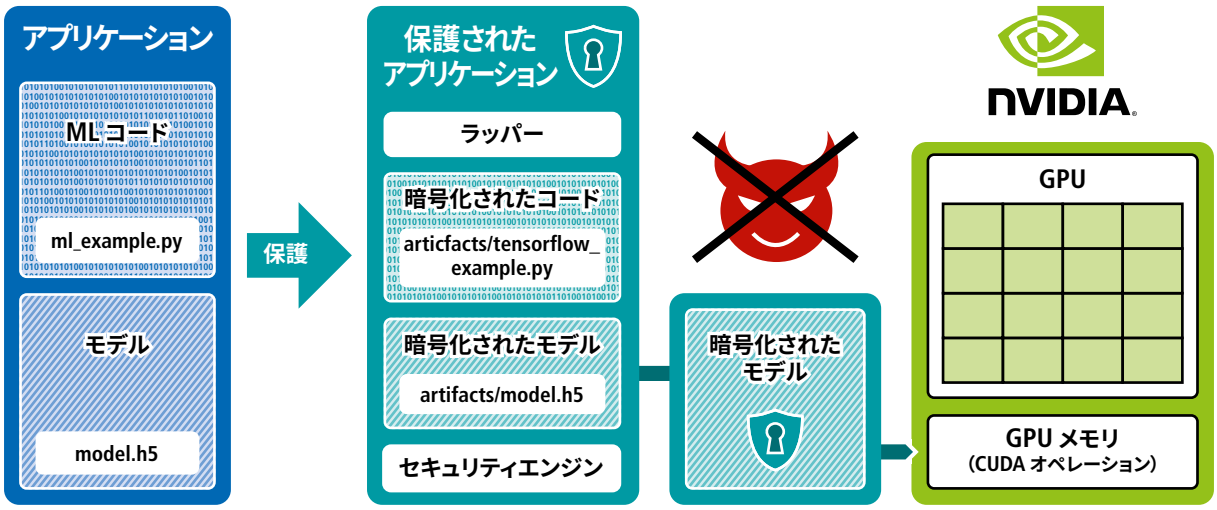


図 3：モデルとコードの暗号化、コンテンツの読み取りと実行は認証ユーザーに限定

Wibu-Systems のライセンシングソリューション

スマートなライセンシングソリューションによって、さまざまなユースケースが実現可能となります。

- ペイ・パー・ユーズモデルに基づく、モデルのオンライン販売
- 大型マシンへの AI の組み込み
- 役割別のアクセス制御

他にも、場所や時間をベースにしたアクセス制御などがあります。

また、ユーザー側の AI モデル保護のロジスティクスも、ライセンシングソリューションの課題に含まれます。

Wibu-Systems は、ビジネスプロセスの実現や改善に役立つ統合型ライセンシングソリューションを提供します。例えば、Python アプリケーションの場合、まず、CodeMeter と、AxProtector Python のライセンスがある AxProtector をオペレーションシステム (OS) (例：Windows、Linux、macOS) にインストールします。その後、ビジネスに応じた特定のライセンス要件に沿う、JSON設定を作成し、暗号化コマンドを実行します。

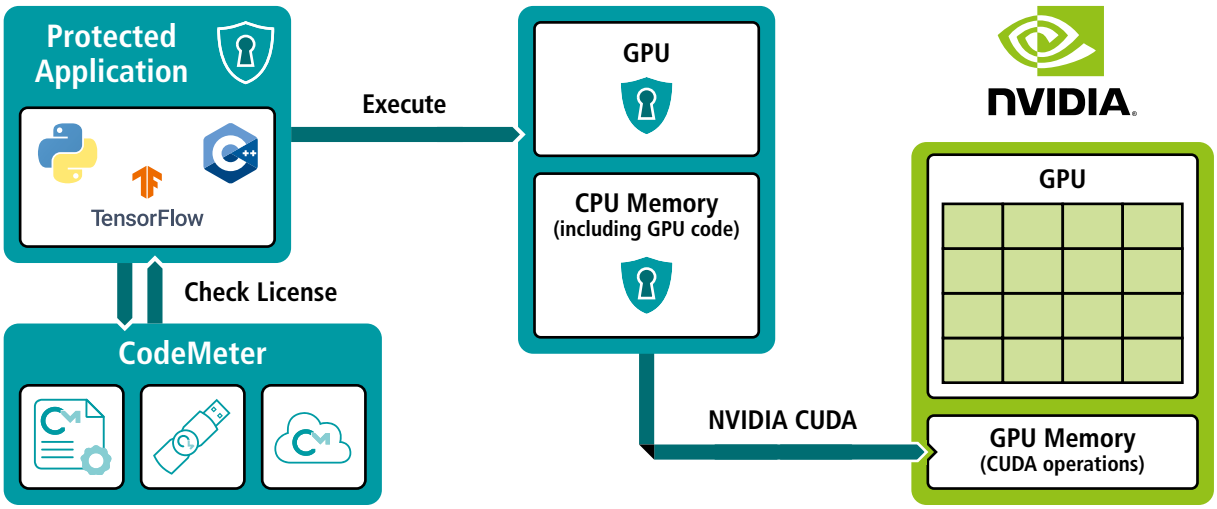


図 4：CodeMeter のランタイムが認証を確認。
CPU メモリを含む CPU 内部の操作の保護、ランタイムの解析・不正アクセス・リバースエンジニアリングに対するプログラムと機械学習モデルの安全性確保。

AxProtector の設定は、機械学習アドオンやその他アクセサリーが不要な標準設計となっています。ビジネスとユースケースの要件は、CodeMeter によって、特定の要件に応じてカスタマイズされるため、「保護・ライセンシング・セキュリティの最適化」が実現できます。ライセンスは、CodeMeter License Central を使用することで、オンプレミスまたはクラウド内で簡単に管理可能です。

プログラムの実行は、認証ユーザーにのみ許可されます。ソリューションのセキュリティをさらに強化したい場合には、CodeMeter ドングルといったセキュアなハードウェア要素の統合をおすすめします。

機械学習プロセスのライセンシングと保護は、このように、簡単なインストールだけで完結します。

通常、NVIDIA GPU が使用され、NVIDIA CUDA 経由で、TensorFlow のような機械学習ライブラリがインターフェイスされることでしょう。かなりの野心的な攻撃者であれば、PCI バスや GPU メモリからコマンドを読み取ることも可能かもしれませんが、その場合、リバースエンジニアリングに関する専門知識が要求されます。また、メモリダンプ時のコマンドと、内部の NVIDIA CUDA マシンオペレーションについても理解しなければ攻撃することは不可能です。

研究プロジェクト

2023 年 8 月、Wibu-Systems をはじめとするプロジェクトの参加メンバーは、SMILE4KMU (Secure Machine Learning Lifecycle) をスタートさせました。プロジェクトの終了は、2026 年 7 月を予定しています。このプロジェクトの中心的なテーマは、特にドイツの中小企業における、機械学習ライフサイクルの保護とライセンシングです。この最先端の研究は、ドイツの連邦教育研究省からの助成を受けています。

プロジェクトのゴールは、機械学習ライフサイクル全体のセキュアかつ革新的な保護とライセンシングのソリューション開発です。

本プロジェクトの統括責任者は、WIBU-SYSTEMS AG と、機械学習を専門とするドイツのスタートアップ、preML GmbH が務めます。preML は、マシンビジョンによる品質管理ソリューションの一部として、実際のユースケースを開発します。そして、オッフェンブルク大学 (ドイツ) もまた、優れた機械学習とITセキュリティの知識、研究能力、実績にて、このプロジェクトに貢献します。

Wibu-Systems は、機械工学や産業工学から、IoT 向けのウェブベースのセキュリティサービスに至るまで、さまざまな業界のユースケースをカバーするために、プロジェクトパートナーに限らず、ドイツの有名機関とも緊密に連携しています。

プロジェクトを通して得られた研究成果は、中小企業の限られたリソースを考慮しつつ、既存および新規のビジネスまたは産業のユースケースに適用される見込みです。弊社が有する暗号化とライセンシングの専門知識とエコシステムが、企業のさらなる競争上の優位性実現に貢献することを期待します。

信頼できる実行環境と、GPU コンテキストにおける AI モデルの整合性保護に関しては、「NVIDIA コンフィデンシャルコンピューティング」のような技術が役立ちます。こうした技術を使うことで、実行時に、セキュアなデータアクセスと暗号化アプリケーションを可能にします。従って、強力な AI モデルの保護に期待されるアプローチは、NVIDIA ソリューションと、Wibu-Systems の CodeMeter テクノロジーとの組み合わせ、そして、Wibu-Systems のライセンシングソリューションへの統合です。



画像 1：ドイツの連邦教育研究省のウェブサイトに掲載された SMILE4KMU 研究プロジェクトの公式画像

サマリー

AI や機械学習の活用が一般化し、ビジネスの成功に欠かせないものとなった今、機械学習の運用やライフサイクルの管理だけでなく、それらに関連する保護やライセンスの要件は、各企業に固有の課題であると同時に、競争上の優位性を獲得するチャンスにもなっています。

では、これらの新たに登場した資産は、どのようにライセンシングし、保護すればよいのでしょうか？ー Wibu-Systems がこの疑問に答えます。Wibu-Systemsは、AxProtector、CodeMeter、CodeMeter License Central といった、堅牢でありながら柔軟性の高いソリューションを提供し、急増するニーズに応えています。この汎用性の高いライセンス管理ソリューションは、クラウドへの統合の有無にかかわらず、幅広く複雑な要件にも対応します。また、EU の AI 規制法をはじめとしたコンプライアンス要件は、信頼できるモデル保護とライセンシングの差し迫った必要性に拍車をかけています。

こうした状況を受け、Wibu-Systems ではすでに、機械学習のライフサイクルと運用における様々な側面を網羅的にカバーするため、既存のソリューションの拡張に挑んでいます。SMILE4KMU プロジェクトのような最先端の研究により、機械学習ソリューションのライセンシングや収益化が期待できるとともに、「NVIDIAコンフィデンシャルコンピューティング」の活用も可能になります。

5062-032-07 / 2026-11-02

Wibu-Systems について

ドイツ本社



WIBU-SYSTEMS AG
Zimmerstrasse 5
76137 Karlsruhe, Germany
Phone: +49 721 93172-0
sales@wibu.com | www.wibu.com

Wibu-Systems は、最先端のサイバーセキュリティとソフトウェアライセンスのライフサイクル管理におけるグローバルリーダーです。当社は、デジタル資産に組み込まれた知的財産を保護し、技術ノウハウの収益化の機会を拡大を目的とした、グローバルで特許取得済みのセキュリティソリューションを提供することに尽力しています。

ソフトウェアパブリッシャーやインテリジェントデバイスメーカーを対象に、当社の包括的な製品群の相互運用可能なハードウェアおよびソフトウェアモジュールは、主要なプラットフォームや多様な業界にわたって、海賊版、リバースエンジニアリング、改ざん、妨害行為、サイバー攻撃から保護します。

Wibu-Systems オフィス

WIBU-SYSTEMS USA, Inc.
米国 +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS (Shanghai) Co., Ltd.
上海 +86 21 5566 1791
北京 +86 10 8296 1560
info@wibu.com.cn

WIBU-SYSTEMS 株式会社
日本
+81 45 565 9710
info@wibu.jp

WIBU-SYSTEMS Korea Ltd.
韓国
+82 2 6206 9490
sales@wibu.co.kr

WIBU-SYSTEMS India Pvt. Ltd.
インド
+91 9632423407
info@wibu.in

WIBU-SYSTEMS BV
オランダ +31 74 750 14 95
ベルギー +32 2 808 6739
sales@wibu.systems

WIBU-SYSTEMS LTD
英国 | アイルランド
+44 20 314 747 27
sales@wibu.systems

WIBU-SYSTEMS SARL
フランス
+33 1 86 26 61 29
sales@wibu.systems

WIBU-SYSTEMS
スペイン | ポルトガル
+34 91 123 0762
sales@wibu.systems

WIBU-SYSTEMS
北欧 | バルト諸国
+46 8 5250 7048
sales@wibu.systems

Wibu-Systems は、プログラムまたはこのドキュメントを事前の通知なしに変更する権利を明示的に留保します。

© 2026 WIBU-SYSTEMS AG – Blurry Box®, CmReady®, CodeMeter®, SmartBind®, SmartShelter®,および Wibu-Systems® は、WIBU-SYSTEMS AG の登録票商標です。このドキュメントで使用されているその他すべてのブランド名および製品名は、それぞれの所有者の商号、サービスマーク、商標、または登録商標です。

WIBU SYSTEMS

SECURITY
LICENSING
PERFECTION IN PROTECTION

www.wibu.com