



Research



SPDX 3.0 を用いた AI部品表 (AI BOM) の実装

AIおよびデータセット部品表の作成に関する
包括的ガイド

著者

Karen Bennet, Gopi Krishnan Rajbahadur,
Arthit Suriyawongkul, Kate Stewart

2024年10月

目次

概要.....	4	name (必須)	47
なぜSPDXが重要なのか:その重要性和影響.....	5	buildTime (必須).....	47
AI BOMをAIプロファイルとデータセットプロファイルに分ける動機	6	downloadLocation (必須)	47
SPDX AIおよびデータセット プロファイルの開発	7	packageVersion (必須)	48
AI BOMフレームワークの定義	8	primaryPurpose (必須)	48
ワーキンググループの結成と初期目標	8	releaseTime(必須)	48
方法論.....	8	suppliedBy (必須).....	48
データシートとの比較	9	relationshipType = hasConcludedLicense (必須).....	49
モデルカードとの比較.....	13	relationshipType = hasDeclaredLicense (必須).....	49
ファクトシートとの比較.....	16	特定のAIPackageフィールドの詳細.....	50
SPDXを使用して国際標準および規制フレームワークに準拠する	21	autonomyType (任意).....	50
EU人工知能法 (EU AI法) へのコンプライアンスの確保	21	domain (任意).....	50
医療機器に関するFDAおよびEMAの要件への適合の確保	24	energyConsumption (任意)	50
IEEE倫理技術規格 (P70xxシリーズ) への準拠の確保	27	energyQuantity (任意)	51
進行中の改訂および更新	39	energyUnit (任意).....	51
プロファイルの主要要素	40	finetuningEnergyConsumption (任意).....	52
必須なAIPackageのフィールド (AIプロファイル)	42	hyperparameter (任意)	52
任意のAIPackageのフィールド (AIプロファイル)	43	inferenceEnergyConsumption (任意)	52
必須のDatasetPackageフィールド (Datasetプロファイル)	44	informationAboutApplication (任意)	53
任意のDatasetPackageフィールド (Datasetプロファイル)	45	informationAboutTraining (任意).....	53
AIおよびDatasetパッケージ フィールド詳細.....	46	limitation (任意)	54
spxId (必須).....	47		

metric (任意).....	54
metricDecisionThreshold (任意).....	55
modelDataPreprocessing (任意).....	55
modelExplainability (任意).....	55
safetyRiskAssessment (任意).....	56
standardCompliance (任意).....	56
trainingEnergyConsumption (任意).....	56
typeOfModel (任意).....	57
useSensitivePersonallInformation (任意).....	57
特定のDatasetPackageフィールドの詳細.....	58
anonymizationMethodUsed (任意).....	58
confidentialityLevel (任意).....	58
dataCollectionProcess (任意).....	58
dataPreprocessing (任意).....	59
datasetAvailability (任意).....	59
datasetNoise (任意).....	60
datasetSize (任意).....	60
datasetType (必須).....	60
datasetUpdateMechanism (任意).....	60
hasSensitivePersonallInformation (任意).....	61
intendedUse (任意).....	61
knownBias (任意).....	61
sensor (任意).....	62

現実世界のエビデンスの例.....	63
手書き文字認識アプリケーション (SimpleHTR).....	63
SimpleHTR Overview.....	63
SimpleHTRのAIプロファイルを含むSPDXシステムBOM.....	63
CO2データセット.....	64
今後の方向性.....	65
選定された標準および参考文献.....	66
謝辞.....	69
著者について.....	70

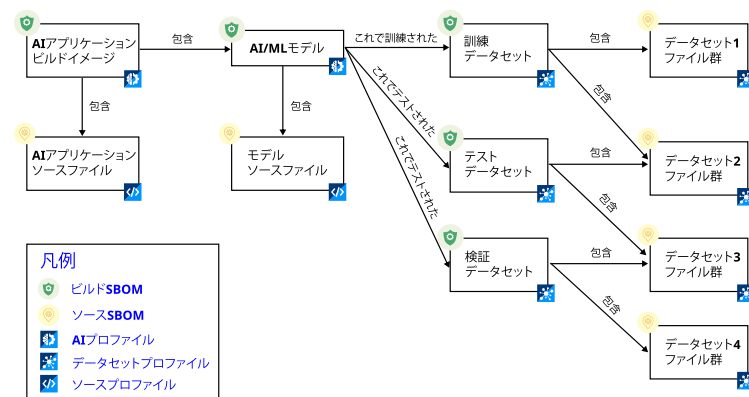
概要

人工知能 (AI) アプリケーション、特にオープンソース ソフトウェアや自由に利用可能なデータを統合するものは、イノベーションの推進、協働の促進、透明性の確保、AI技術へのアクセスの民主化において重要な役割を果たします。これらのアプリケーションは、社会の進歩に大きく貢献し、責任あるAIの実践を広める一助となっています。しかし、それらはしばしば異なる環境向けに設計された多くのサードパーティ コンポーネントを組み込んでおり、セキュリティ上の脆弱性を抱えていたり、データが危殆化していたり、ライセンス条件が不明確である場合があります。

従来のソフトウェアリスクに加えて、AIやデータ集約型アプリケーションには特有の課題も存在します。これには、同意や意図を無視したデータの不適切な利用によるデータ セキュリティ侵害、モデル改ざんや敵対的攻撃といったAIセキュリティの脅威が含まれます。また、設計上の判断、既知のバイアス、エネルギー消費、基本的権利への影響評価といった、非従来型のソフトウェア エンジニアリング要素を文書化する規制義務は、AIリスク管理を著しく複雑化させる可能性があります。さらに、データセットやモデルに対するオープン ライセンスの普及が進む中で、複雑な行動利用条項を伴う場合が多く、新たなAIリスク管理上の考慮事項が生じています。

このような背景において、従来のソフトウェア部品表 (SBOM) の範囲を拡張したAI部品表 (AI BOM) は、ますます複雑化するシステムの管理やAIの普及において重要性を増しています。AIシステムの開発において、関連する設計上の決定や開発依存関係をすべて記録することは、現在ではベスト プラクティスと見なされており、規制機関や業界標準によって義務付けられることも少なくありません。AI BOMを活用することで、組織はこれらの決定や依存関係を体系的に特定・追跡し、技術的セキュリティ、機能的安全性、知的財産、規制遵守に関するリスクを事前に特定・管理・軽減することが可能になります。その結果、AIアプリケーションは潜在的な脅威に対して安全性と回復力を維持することができます。

システム パッケージ データ交換仕様 バージョン3.0 (System Package Data Exchange; SPDX 3.0) は、システム コンポーネントと文書の機械可読な一覧を提供することを目的としています。SPDX 3.0内のAI部品表 (AI BOM) は、関連するSPDXプロファイルを取り入れ、アルゴリズム、データ収集方法、ライブラリ、フレームワーク、ライセンス情報、規格準拠、セキュリティ対策、そしてAIアプリケーションの開発、テスト、展開に関わるその他のツールを包括的に文書化します。さらに、SPDXプロジェクト自体は、AIやデータセットにおけるライセンスの必要性や著作権法の適用性について立場を示していませんが、SPDXのメタデータ フィールドを利用することで、部品表の作成者や利用者が、AIやデータセットの提供者が提示するライセンス関連情報を記録し、共有することが可能です。











なぜSPDXが重要なのか:その重要性和影響

SPDX AIおよびデータ セット プロファイルは、サプライチェーンにおける透明性と責任を促進するための重要な構成要素として機能し、脆弱性、潜在的な危害、リスクの追跡を可能にします。AIシステムの設計、能力、および制約に関する標準化された文書を提供することで、SPDXメタデータを使用したAIプロファイルは、ユーザー間の信頼と理解を深め、システムに関する安全で情報に基づいた意思決定を可能にします。つまり、これらのプロファイルは、AIシステムの信頼性と追跡可能性を向上させるだけでなく、その責任ある利用にも貢献します。

これらの文書は、開発者、ユーザー、弁護士、規制当局、倫理学者にとって非常に重要です。なぜなら、AIの社会的影響を取り扱い、管理するための協力的な環境を促進するからです。これらのプロファイルは、モデルを開発した組織によって作成・維持されており、AI技術が倫理的基準

や法的要件を満たすことを保証する重要な役割を果たします。標準化された文書を提供することにより、AIエコシステム内での責任ある研究と展開を促進し、サプライチェーン全体で透明性と責任を推進します。

SPDX 3.0は、異なる情報に対するプロファイルを作成するために再設計されました。私たちは、AIおよびデータセットプロファイルに焦点を当てています。

	セキュリティ情報 - ソフトウェアに関連する脆弱性の詳細
	ビルド関連情報 - 来歴と再現可能なビルド
	AIモデルに関する情報 - 倫理的、セキュリティ、及びモデルデータ
	データセットに関する情報 - AIおよびその他のデータ利用事例
	業界のサプライチェーンワークフローをサポートするための最小限のサブセット
	著作権およびライセンスに関する情報 - コンプライアンスのサポート
	ソフトウェアに特化した情報
	すべてのプロファイルで使用される情報

AI BOMをAIプロファイルとデータセットプロファイルに分ける動機

SPDX (System Package Data Exchange; システム パッケージ データ 交換) では、AIプロファイルとデータセット プロファイルを分けること で、AIモデルの作成に使用された来歴 (プロヴェナンス) と訓練方法を 明確にすることを目的としています。

AIプロファイルは、機械学習 (ML) の利用事例も含むよう考慮されてい ます。AI/MLモデルにおけるソフトウェア コンポーネントの識別と分類 は、モデルの訓練や更新に使用されるデータセットによって影響を受け ます。特定のデータセットと特定のモデルとの間には必ずしも直接的な 関係はなく、それぞれが別々に取得されることもあります。AIプロファイル は、従来の機械学習アルゴリズム、ニューラル ネットワーク、大規模 言語モデル (LLM)、およびその他の前処理や評価コンポーネントなど、 人工知能機能に直接関連するソフトウェア コンポーネントを指す場合 があります。これらのコンポーネントには、他の種類のソフトウェア コンポーネントとは異なるライセンスに関する考慮事項、使用制限、または セキュリティ上の影響がある場合があります。

AIプロファイルとは異なり、データセット プロファイルは、主にデータ 処理、保存、または管理に関わるコンポーネントを表します。これには、

処理されたデータで構成されるデータベースやファイルが含まれます。 これらのプロファイルを分けることにより、ソフトウェアのデータに関連 する側面をより良く理解でき、そのプライバシー、コンプライアンス、ま たはセキュリティに対する潜在的な影響を明確にすることができます。

AIとデータセット プロファイルを分けることにより、SPDXで構成され たAI部品表 (AI BOM) は、ソフトウェアの構成についてより詳細かつ包 括的な視点を提供し、利害関係者が関連するリスク、義務、および依存 関係を評価・管理しやすくします。ただし、読者は、AI部品表がAIおよ びデータセット プロファイルのフィールドだけで構成されているわけでは ないことに留意する必要があります (モデルやデータセットのみを記 述することが目的でない限り)。AIソフトウェアはソフトウェア コンポー ネント、AIモデル、データセットの組み合わせであるため、包括的なAI 部品表は、AIシステムを完全に記述するために他の多くのプロファイル (例: コア、ソフトウェア) を活用します (詳細については「例」のセク ションを参照してください)。



SPDX AIおよびデータセット プロファイルの開発

この取り組みの大きな目標は、AIコンポーネントを含むソフトウェア システム全体を記述できる、包括的でありながら自動化され、容易に採用可能なAI部品表 (AI BOM) を確立することです。これにより、トレーサビリティの向上、ライセンス コンプライアンス、透明性、規制遵守を実現し、テクノロジー業界におけるAIの文書化と管理の新たな基準を設定することを目指しています。

この体系的なアプローチを通じて、ワーキング グループは標準化されたAIおよびデータセット プロファイルのための堅固な基盤を築き、AIシステムの管理とガバナンスにおける現在および将来の要件を満たすこと

を保証しました。必要なフィールドが既存のSPDXプロファイル (ソフトウェアやコアなど) にすでに含まれている場合には、それらを再定義するのではなく再利用を試みました。これは、SPDX標準における冗長性を回避し、他の標準との緊密な統合を可能にすることで、ソフトウェア エンジニアリングの実践者による迅速かつ広範な採用を促進するためです。ただし、これらのフィールドは他のプロファイルから借用されたものであっても、AIプロファイルまたはデータセット プロファイルの一部と見なされます。



AI BOMフレームワークの定義

ワーキンググループの結成と初期目標

2021年、業界と学術界の専門家からなる多様性に富んだワーキンググループを結成し、AI部品表 (AI BOM) の開発に取り組みました。このグループには、AIやソフトウェア工学を含むさまざまな分野の研究者、教授、最高技術責任者 (CTO)、プロダクト マネージャー、AI開発者、弁護士、ライセンス専門家が参加しており、主に参加者のプロフェッショナルネットワークを通じて招集されました。このオープンな作業グループは、週1回、1時間の会議を開催し、各セッションで最低6名が参加する形で継続的に活動しました。その目標は、AIシステムにおいて透明性を提供するだけでなく、トレーサビリティ、説明責任、来歴、系譜、および自動化を強化する標準を策定することでした。

方法論

私たちの最初の作業は、AI BOMに必要な基本的なフィールドを特定することでした。そのため、最初の数か月間、ワーキンググループはそれぞれの専門知識と多様なバックグラウンドを活かして、AI BOM標準で重要とされる初期のフィールド セットを作成しました。その後、モデルカード、データシート、ファクトシートなどの既存のツールを分析し、この初期リストを拡充することを目指しました。

このような分析の目的は、これらのツールがカバーしているすべてのフィールドを網羅的に取り込むことではなく、AI部品表 (AI BOM) の文脈で必須とされるフィールドを特定することにあります。さらに、作業グループが重要視したもう一つの点は、AI BOM標準が実務者にとって適応性の高いものとなるようにすることでした。

そのため、関連する詳細をできる限り多く取り込むという意欲と、採用や使用が過度に煩雑にならないようにすることのバランスを取ることが

重要でした。その結果、一部のフィールドは将来のバージョンで追加することを決定し、必須とされたフィールドは非常に少数 (この文書の後半で説明) に限定されました。

最後に、既存のSPDXの他のプロファイルにおいて、AIソフトウェアのAI BOMを作成するために必要な情報を表現できる場合には、AIおよびデータセット プロファイルに新たなフィールドを追加することを避けました。上記の考慮事項を踏まえ、作業グループ内で慎重なレビューと民主的な議論を通じて、これらの文書で提案された103のフィールドを分析しました。各フィールドの採用基準は以下の通りです：

- AI BOMの要件への関連性
- フィールドの表現方法の存在
- そのフィールドの追加に関するグループ内での合意

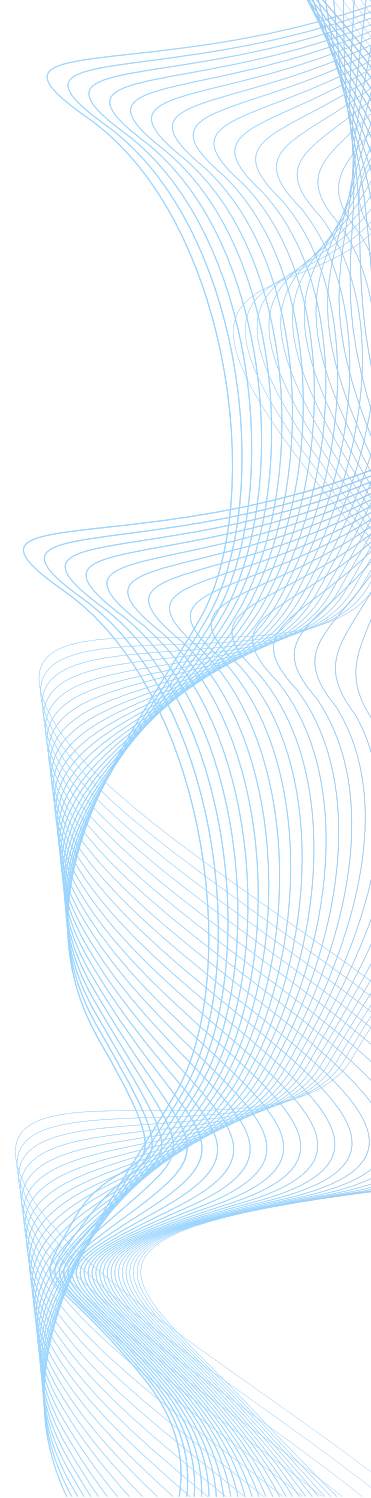
この反復的なプロセスにより、36のフィールドが選定されました。AIプロファイルのAIパッケージには20のフィールド (そのうち5つは必須フィールド)、データセット プロファイルのデータセット パッケージには18のフィールド (そのうち6つは必須フィールド) が含まれ、全員一致の合意に基づいて決定されました。必要に応じて、報告書の著者が決定権を持つ形で合意が形成されました。

データシートとの比較

以下の表は、従来のデータシートのフィールド（元の論文[r]に提供されたデータシートのフィールド）と、私たちが提案するAI部品表に組み込まれたフィールド（AIプロフィール、データセット プロファイル、およびSPDXの他のプロフィールから）の比較を詳細に示しています。

カテゴリ	サブカテゴリ	AI BOMに存在するか？	AI BOM内での対応するフィールド（またはリレーションシップ）または含めなかった理由	SPDX プロファイル
動機	データセットは何の目的で作成されたか？	✓	intendedUse	Dataset
	データセットは誰が作成し、どの団体のために作成されたか？	✓	originatedBy	Core
	データセットの作成に資金提供したのは誰か？	✗	comment フィールドはその代わりに使用できます。ただし、ワーキンググループは、このフィールドはBOMの文脈では関連性がないと判断しました。	N/A
構成	データセットを構成するインスタンスは何を表しているか（例：文書、写真、人々）？	✓	datasetType	Dataset
	総インスタンス数はいくつか（該当する場合は各タイプごとにそれぞれ）？	✓	datasetSize	Dataset
	各インスタンスはどのようなデータで構成されているか？	✓	datasetType	Dataset
	個々のインスタンスに欠けている情報はるか？	✓	datasetNoise	Dataset
	推奨されるデータ分割はあるか？	✓	trainedOn 、 testedOn リレーションシップ	Core
	データセットにエラー、ノイズの原因、または冗長性はあるか？	✓	datasetNoise	Dataset

カテゴリー	サブカテゴリー	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリレーションシップ) または含めなかった理由	SPDX プロファイル
構成	データセットは自己完結型か、それとも外部リソースに依存しているか?	✓	downloadLocation 、 datasetUpdateMechanism	Software 、 Dataset
	データセットには機密と見なされる可能性のあるデータが含まれているか?	✓	confidentialityLevel	Dataset
	データセットには攻撃的、侮辱的、脅迫的、または不安を引き起こす可能性のあるデータが含まれているか?	✓	knownBias	Dataset
	データセットは特定の下位集団を識別しているか?	✓	knownBias	Dataset
	個人を直接的または間接的に識別することは可能か?	✓	hasSensitivePersonalInformation	Dataset
	データセットには何らかの形でセンシティブと見なされるデータが含まれているか?	✓	hasSensitivePersonalInformation	Dataset
	データセットにはすべての可能なインスタンスが含まれているか、それともサンプルか?	✗	ワーキンググループは、このフィールドはBOMの文脈では関連性がないと判断しました。さらに、この情報は dataCollectionProcess フィールドで捕捉できます。	N/A
	各インスタンスにラベルやターゲットが関連付けられているか?	✗	ワーキンググループは、このフィールドはBOMの文脈では細かすぎると判断しました。	N/A
	個々のインスタンス間の関係は明示されているか?	✗	ワーキンググループは、このフィールドはBOMの文脈では細かすぎると判断しました。	N/A
	データセットは人々に関連しているか?	✗	hasSensitivePersonalInformation フィールドはこの側面を捕捉できますが、将来のバージョンでこの情報をより適切に捕捉できるようにフィールドを改善する予定です。	N/A
収集プロセス	各インスタンスに関連付けられたデータはどのように取得されたか?	✓	dataCollectionProcess	Dataset



カテゴリ	サブカテゴリ	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリリースシップ) または含めなかった理由	SPDX プロファイル
収集プロセス	データを収集するために使用されたメカニズムや手順は何か?	✓	dataCollectionProcess	Dataset
	データはどの期間にわたって収集されたか?	✓	builtTime 、 releaseTime	Core
	データは対象となる個人から収集したか、それとも第三者を通じて取得したか?	✓	dataCollectionProcess	Dataset
	対象となる個人にデータ収集について通知されたか?	✓	dataCollectionProcess	Dataset
	対象となる個人は、自分のデータの収集および使用に同意したか?	✓	dataCollectionProcess	Dataset
	データセットがより大きなセットからのサンプルである場合、サンプリング戦略はどのようなものだったか?	✗	ワーキンググループの議論後に含まれないこととなりました。 dataCollectionProcess フィールドでこの情報を捕捉できるためです。	N/A
	データ収集プロセスには誰が関与し、どのように報酬が支払われたか?	✗	ワーキンググループは、このフィールドはBOMの文脈では関連性がないと判断しました。	N/A
倫理的なレビュー プロセスは実施されたか?	✗	このバージョンのAI BOMには含まれていません。ワーキンググループは、今後のバージョンでこれを検討することに決定しました。	N/A	
前処理	データの前処理は行われたか?	✓	dataCollectionProcess	Dataset
利用	データセットはすでに何らかのタスクで利用されたか?	✓	intendedUse	Dataset
	データセットを利用する論文やシステムへのリンクを提供するリポジトリはあるか?	✓	downloadLocation	Software

カテゴリ	サブカテゴリ	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリレーションシップ) または含めなかった理由	SPDX プロファイル
利用	データセットはどのようなタスクに利用できるか?	✓	intendedUse	Dataset
	データセットには利用すべきでないタスクがあるか?	✗	このバージョンのAI BOMには含まれていません。ワーキンググループは、今後のバージョンでこれを検討することに決定しました。	N/A
配布	データセットはどのように配布されるか?	✓	downloadLocation	Software
	データセットは著作権やその他の知的財産権ライセンス、または適用される利用規約の下で配布されるか?	✓	hasDeclaredLicense 、 hasConcludedLicense リレーションシップ	Core
	第三者がインスタンスに関連するデータに対して、知的財産権に基づく制限やその他の制限を課したか?	✓	hasConcludedLicense リレーションシップ	Core
	データセットは、作成を依頼した団体以外の第三者に配布されるか?	✗	ワーキンググループは、このフィールドはBOMの文脈では関連性がないと決定しました。	N/A
メンテナンス	データセットの所有者・キュレーター・管理者にはどのように連絡できるか?	✓	originatedBy	Core
	データセットのサポート・ホスティング・維持は誰が行うか?	✗	ワーキンググループの議論の結果、 supportLevel フィールドがこの情報を捕捉できるため、含めないことに決定されました。	N/A

表1 - SPDX 3.0とデータシートと比較

モデルカードとの比較

以下の表は、従来のモデルカードのフィールド（元の論文[p]で提供されたモデルカードのフィールド）と、提案するAI部品表に組み込まれたAIプロファイル、データセット プロファイル、その他のSPDXプロファイルのフィールドを比較したものです。

カテゴリー	サブカテゴリー	AI BOMに存在するか?	AI BOM内での対応するフィールド（またはリレーションシップ）または含めなかった理由	フィールドに関連したSPDXプロファイル
モデル詳細	モデルを開発した個人または組織	✓	suppliedBy	Core
	モデルの日付	✓	releaseTime	Core
	モデル バージョン	✓	packageVersion	Software
	モデル タイプ	✓	typeOfModel	AI
	トレーニング アルゴリズム、パラメータ、公平性の制約、その他の適用されたアプローチや特徴に関する情報	✓	informationAboutTraining 、 informationAboutApplication	AI
	詳細情報のための論文やその他のリソース	✓	hasDocumentation	Core
	ライセンス	✓	hasDeclaredLicense 、 hasConcludedLicense	Core
モデルに関する質問やコメントを送る場所	✓	suppliedBy	Core	

カテゴリー	サブカテゴリー	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリレーションシップ) または含めなかった理由	フィールドに関連したSPDXプロファイル
モデル詳細	引用の詳細	✗	ワーキンググループの議論の結果、 hasDocumentation リレーションシップがこの情報を捕捉できるため、含めないことに決定されました。ただし、より具体的な関係については、将来のバージョンで検討することができます。	N/A
意図された利用	主な意図された利用方法	✓	primaryPurpose	Software
	範囲外のユースケース	✓	limitation	AI
	主な意図された利用者	✗	ワーキンググループの議論の結果、このフィールドはBOMの文脈では関連性がないと決定されました。さらに、 intendedUse フィールドがタスクの観点からこの情報を捕捉できると考えられます。	N/A
ファクター	関連するファクター	✓	informationAboutTraining 、 hyperparameter	AI
	評価ファクター	✓	informationAboutApplication	AI
メトリックス	モデルのパフォーマンス指標	✓	metric	AI
	決定閾値	✓	metricDecisionThreshold	AI
	バリエーションアプローチ	✗	ワーキンググループの議論の結果、このフィールドはBOMの文脈では関連性がないと決定されました。	N/A
評価データ	データセット	✓	DatasetPackage クラス; trainedOn 、 testedOn リレーションシップ	Dataset
	動機	✓	intendedUse	Dataset

カテゴリー	サブカテゴリー	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリレーションシップ) または含めなかった理由	フィールドに関連したSPDXプロファイル
評価データ	前処理	✓	dataPreprocessing	Dataset
訓練データ	訓練されたデータ	✓	trainedOn	Core
定量分析	単一の結果	✗	ワーキンググループは、このフィールドがBOMの文脈では関連性がないと決定しました。	N/A
	交差的結果	✗	ワーキンググループは、このフィールドがBOMの文脈では関連性がないと決定しました。	N/A
倫理的考慮	N/A	✓	knownBias	Dataset
推奨事項と注意点	N/A	✓	limitation	AI

表2 - SPDX 3.0とモデルカードの比較

この表は、提案するAI BOMがAIモデルのドキュメントにおけるさまざまな重要な側面にどれだけ詳しく対応しているかを示しており、既存の慣行と一致している場所や、特定の改善や調整が行われた場所を明確にしています。

ファクトシートとの比較

以下の表は、従来のファクトシートのフィールド（元の論文[q]で提供されたファクトシートのフィールド）と、IBMがそれ以降進化させた形式[u]の情報を、私たちが提案するAI部品表（AI BOM）に組み込まれたAIプロファイル、データセットプロファイル、およびその他のSPDXプロファイルと比較したものです。

カテゴリ	サブカテゴリ	AI BOMに存在するか?	AI BOM内での対応するフィールド（またはリレーションシップ）または含めなかった理由	フィールドに関連したSPDXプロファイル
一般	「あなた」（供給者）とは誰で、（この特定のサービス以外に）通常どのようなサービスを提供しているのか？	✓	suppliedBy サービスの種類は含まれていません。ワーキンググループは、このフィールドがBOMの文脈では関連性がないと判断したためです。	Core
	このサービスは何についてのものか？	✓	informationAboutApplication 、 primaryPurpose	AI 、 Software
	このサービスの出力を説明せよ。	✓	informationAboutApplication	AI
	このサービスはどのようなアルゴリズムや技術を実装しているか。	✓	typeOfModel ; AIプロファイル	AI
	このファクトシートを以前に更新したことがあるか？	✓	releaseTime	Core
	開発チームの特徴は何か？	✗	ワーキンググループは、この項目はBOMの文脈では関連性がないと判断しました。	N/A
利用方法	このサービスの出力の意図された利用目的は何か？	✓	primaryPurpose 、 domain 、 informationAboutApplication	AI 、 Software
	このサービスを利用する際に従うべき主な手順は何か？	✓	dataCollectionProcess 、 dataPreprocessing 、 informationAboutTraining 、 informationAboutApplication	AI 、 Dataset

カテゴリー	サブカテゴリー	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリレーションシップ) または含めなかった理由	フィールドに関連したSPDXプロファイル
ドメインとアプリケーション	このサービスがテストされた、または利用された分野やアプリケーションは何か?	✓	domain 、 metric 、 metricDecisionThreshold ; testedOn リレーションシップ	AI
	顧客やユーザーはこのサービスをどのように利用しているか?	✓	primaryPurpose	Software
	その他コメントは?	✓	comment	Core
	過去にこのサービスが使用されたアプリケーションをリストアップせよ。	✗	ワーキング グループは、この項目はBOMの文脈では関連性がないと判断しました。	N/A
基本的なパフォーマンス - サービス提供者によるテスト	サービスがテストされたデータセットはどれか? (例えば、テストに使用されたデータセットへのリンクと対応するデータシート)	✓	testedOn リレーションシップ	Core
	テスト方法論を説明せよ。	✓	informationAboutApplication 、 metric 、 metricDecisionThreshold ; testedOn リレーションシップ	AI
基本的なパフォーマンス - 第三者によるテスト	テスト結果を説明せよ。	✓	metric 、 metricDecisionThreshold	AI
	パフォーマンス指標を検証する方法はあるか (例えば、サービスAPIを通じて)?	✓	metric	AI
	その他コメントは?	✓	comment	Core
	サービス提供者以外に、このサービスは第三者によってテストされたか?	✗	このバージョンのAI BOMには含まれていません。ワーキング グループは今後のバージョンで検討することにしました。	N/A
安全性 - 一般	このサービスの利用によるバイアス、倫理的問題、またはその他の安全リスクの可能性について認識しているか?	✓	knownBias 、 standardCompliance	AI 、 Dataset

カテゴリー	サブカテゴリー	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリレーションシップ) または含まなかった理由	フィールドに関連したSPDXプロファイル
安全性 - 一般	個人または個人グループからデータを使用したり、推論を行ったりしているか? その同意を得ているか?	✓	knownBias , standardCompliance , confidentialityLevel , limitation	Dataset
安全性 - 説明可能性	サービスの出力は説明可能または解釈可能か?	✓	modelExplainability	AI
安全性 - 公平性	サービスで使用される各データセットについて: そのデータセットはバイアスがチェックされたか? 公平で代表的であることを確認するためにどのような努力がなされたか?	✓	knownBias , datasetNoise , standardCompliance	AI , Dataset
安全性 - コンセプトドリフト	あなたのシステムは、新しく取り込んだデータに基づいて動作を更新するか?	✓	datasetUpdateMechanism , informationAboutApplication	AI , Dataset
	そのサービスは、訓練データと使用データの違いを確認することを許可するか?	✓	trainedOn , testedOn リレーションシップ; Dataset プロファイル	Dataset
	その他コメントは?	✓	comment	Core
	サービスはバイアス検出と是正を実施しているか?	✗	ワーキンググループの議論の結果、このフィールドは含まれていません。 knownBias フィールドがこの情報を捕捉でき、バイアスは正が行われた場合は、 dataPreprocessing , dataCollectionProcess , modelDataPreprocessing , informationAboutTraining , informationAboutApplication 及び limitation を通じて捕捉できます。	N/A
	未確認データや異なる分布のデータに対する期待されるパフォーマンスはどのようなものか?	✗	ワーキンググループの議論の結果、この情報は domain , intendedUse , primaryPurpose フィールドでカバーできるとされ、このフィールドはBOMの文脈では推測的であると判断されました。	N/A
サービスは時間の経過とともにモデルやパフォーマンスのドリフトをどのようにテストし、監視しているか?	✗	このバージョンのAI BOMには含まれていません。ワーキンググループは、将来のバージョンで検討することに決定しました。	N/A	

カテゴリー	サブカテゴリー	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリリースシップ) または含めなかった理由	フィールドに関連したSPDXプロファイル
安全性 - コンセプトドリフト	新しいデータが追加された際、サービスが正しい期待通りの出力を生成しているかどうかはどのように確認できるか?	✗	ワーキンググループは、このフィールドがBOMの文脈では関連性がないと判断しました。	N/A
	サービスは定期的にテストされているか?	✗	このバージョンのAI BOMには含まれていません。ワーキンググループは将来のバージョンで検討することを決定しました。	N/A
セキュリティ	このサービスはどのように攻撃や悪用される可能性があるか? 説明せよ。	✓	safetyRiskAssessment	AI
	このサービスが適さないアプリケーションやシナリオを列挙せよ。	✓	intendedUse 、 primaryPurpose 、 informationAboutApplication 、 domain	AI 、 Dataset
	どのようにユーザーや利用データを保護しているか?	✓	anonymizationMethodUsed	Dataset
	その他コメントは?	✓	comment	Core
	サービスは、対立的攻撃に対して堅牢性が確認されたか?	✗	ワーキンググループの議論の結果、この情報は safetyRiskAssessment フィールドで捕捉できるため、含まれていません。ただし、ワーキンググループは今後のバージョンでの検討を決定しました。	N/A
	セキュリティ侵害の潜在的な処理計画はどのようになっていますか?	✗	このバージョンのAI BOMには含まれていません。ワーキンググループは、今後のバージョンで考慮することを決定しました。	N/A
来歴 - 訓練データ	サービスはそのままの (既製の) モデルを提供しているか? サービスはどのデータセットで訓練されたか?	✓	informationAboutTraining 、 informationAboutApplication 、 trainedOn	AI
	各データセットについて: 訓練データセットは公開されているか?	✓	datasetAvailability	Dataset
	そのサービスでは、データシートに記載された変換に加えて、データの変換が必要だったか?	✓	informationAboutTraining 、 informationAboutApplication 、 modelDataPreprocessing 、 dataPreprocessing	AI

カテゴリ	サブカテゴリ	AI BOMに存在するか?	AI BOM内での対応するフィールド (またはリリースシップ) または含めなかった理由	フィールドに関連したSPDXプロファイル
来歴 - 訓練データ	合成データを使用しているか?	✓	dataCollectionProcess	Dataset
	各データセットについて: データセットにはデータシートやデータステートメントがあるか?	✗	このバージョンのAI BOMには含まれておらず、Fact-sheetsに特有すぎるため、ワーキンググループは今後のバージョンで検討することに決定しました。	N/A
Lineage - Trained Models	モデルはどのように訓練されたか?	✓	informationAboutTraining	AI
	モデルは最後にいつ更新されましたか?	✓	releaseTime	Core
	トレーニング前に、事前知識を使用したり、データの重み付けを行ったりしたか?	✓	informationAboutTraining 、 modelDataPreprocessing	AI
	その他コメントは?	✓	comment	Core

表3 - SPDX 3.0とIBM ファクトシートとの比較

この分析は2022年5月に実施されたことをお伝えすることが重要です。その後、モデルカード、ファクトシート、データシートなどのツールはさらに多くのフィールドを持つように進化しており、現在では他にも多くのツールが存在しています。そのため、この分析が最も包括的な比較であるわけではないことに留意すべきです。しかし、私たちはこの分析をあくまで初期の出発点として使用し、その後、収集されたフィールドをさらに進化させました。SPDXのAIおよびDatasetプロファイルは、次回のリリースに向けて強化され、AIに対するコミュニティの考え方の進展を反映し、さまざまな政策立案者、実務者、研究者、開発者からのフィードバックをもとに対応しています。

SPDXを使用して国際標準および規制フレームワークに準拠する

このセクションでは、コンプライアンスのユースケースを示し、私たちのフレームワークが最良の実践および現在のAI標準に合致していることを確認します。私たちは、倫理的なAIの取り扱いに関するISOおよびIEEEの標準と比較を行いました。さらに、私たちのフレームワークは、EU AI法の新たな要件にも対応できるよう設計されており、バージョン3.1での完全準拠を目指しています。また、米国およびEUの医療機器規制とも照合しました。これらの検証を通じて、私たちのAI BOMは広く確立されたガイドラインに沿う形で調整され、将来の規制要件にも対応できるようになっています。

本論文の著者は、EUの人工知能法（EU AI法）、米国食品医薬品局（FDA）の医療機器規制、IEEE P70xxシリーズの倫理的技術に関する標準、そしてISO AI標準を詳細に検討しました。目的は、SPDX 3.0がこれらの規制や標準によって義務付けられた詳細を捕捉できるフィールドを含んでいるかどうかを評価することでした。本論文は、SPDX 3.0のAI BOMが要求される詳細をどの程度表現できるかについての比較分析の結果を示しています。この比較は、提案されたAI BOMが分野における確立された規範およびガイドラインに適合することを確保する上で重要な役割を果たします。関連する国際標準を統合することによって、私たちはAIの倫理的な利用およびそのドキュメンテーション要件に対する包括的かつ一貫したアプローチを開発しようとしています。

EU人工知能法（EU AI法）¹へのコンプライアンスの確保

提示された表は、SPDX 3.0のフィールドとEU人工知能法（EU AI Act）の主要な条項、特にEUデータベースへの登録要件（第49条）の対応を示しています。この登録は、高リスクAIシステムを市場に出す前や実世界でのテストを行う前に必須となります。2024年8月1日から施行される [EU AI Act](#) は、人工知能を規制するために明確なルールを設け、AIシステムが既存の法規制や基本的な権利に従って設計・展開されることを確保することを目的としています。この立法は、AIシステムをリスクレベルに基づいて分類し、高リスクのアプリケーションに対しては、透明性と責任を強化するためにより厳しい要件を課しています。SPDX 3.0を活用することで、組織は自社のAIシステムを効果的にマッピングし、ドキュメント化することができ、EU AI Actの規定に準拠し、スムーズな登録プロセスを実現できます。この統合は、規制への遵守を簡素化するだけでなく、安全で倫理的なAI技術の開発を促進します。

1 2024年6月13日に制定された欧州議会および欧州理事会の規則（EU）2024/1689は、人工知能に関する調和的な規則を定め、規則（EC）第300/2008号、（EU）第167/2013号、（EU）第168/2013号、（EU）2018/858号、（EU）2018/1139号、（EU）2019/2144号および指令2014/90/EU、（EU）2016/797号、（EU）2020/1828号を改正しました（人工知能法）。<http://data.europa.eu/eli/reg/2024/1689/oj>

カテゴリー	サブカテゴリー	EU AI法の概要と条項	AI BOMに存在するか?	AI BOMの該当するフィールド	SPDXプロファイル
システム、提供者、導入者の識別	システムユニークID	「実世界条件でのテストに関するEU全域で一意的の単一識別番号」 - Annex IX (1) 「提供者によるEUデータベース内のAIシステムエントリのURL」 - Annex VIII Section C (3) 「AIシステムの識別と追跡を可能にする追加の明確な参照」 - Annex VIII Section A (4) - Annex VIII Section B (4)	✓	Package 内の spdxId 、 externalIdentifier 、 externalRef 、 packageUrl	Core
	システム名	「AIシステムの商標名」 - Annex VIII Section A (4) - Annex VIII Section B (4)	✓	Package 内の name (そしてそのサブクラスの AIPackage)	Core
	提供者の連絡先	「提供者の名前、住所、連絡先の詳細」 - Annex VIII Section A (1) - Annex VIII Section B (1) - Annex VIII Section C (1)	✓	CreationInfo の createdBy 、および Person かつ/または Organization における externalIdentifier	Core
	導入者の連絡先	「導入者の名前、住所、連絡先の詳細」 - Annex VII Section C (1)	✓	suppliedBy 、および Person かつ/または Organization における externalIdentifier	Core
システムの詳細	意図された目的	- Annex VIII Section A (5) - Annex VIII Section B (5) - Annex IX (3)	✓	primaryPurpose 、 informationAboutApplication	Core
	システムによって使用される情報	「システムによって使用される情報(データ、入力) およびその動作ロジック」 - Annex VIII Section A (6)	✓	informationAboutApplication 、 informationAboutTraining 、 testedOn 、 trainedOn リレーションシップ; Dataset プロファイル	AI 、 Dataset
	システムステータス	「AIシステムの状態(市場に出ている、またはサービス中; もはや市場に出ている/サービス中でない、リコールされた)」 - Annex VIII Section A (7)	✓	validUntilTime 、 supportLevel	Core

カテゴリー	サブカテゴリー	EU AI法の概要と条項	AI BOM に存在する か？	AI BOMの該当するフィールド	SPDXプロファイル
システムの詳細	システム分類	「AIシステムが高リスクではないと見なされる根拠についての簡潔な概要(第6条第3項に基づく手続きの適用において)」 - Annex VIII Section B (7)	✓	informationAboutApplication ; hasDocumentation リレーションシップ	AI 、 Core
	使用説明書	「導入者向けの使用説明書、および導入者に提供されるユーザーインターフェースの基本的な説明(該当する場合)」 - Annex IV (1)(h)	✓	informationAboutApplication ; hasDocumentation リレーションシップ	AI 、 Core
システムの詳細	影響評価	「第27条に基づいて実施された基本的権利影響評価の結果の概要」 - Annex VIII Section C (4) 「この規則の第26条第8項に規定されたように、規則(EU)2016/679の第35条または指令(EU)2016/680の第27条に従って実施されたデータ保護影響評価の結果の概要(該当する場合)」 - Annex VIII Section C (5)	✓	hasDocumentation リレーションシップおよび description リレーションシップが 使われることもある	Core
	認証	「第47条に記載されたEU適合宣言のコピー」 - Annex IV (8) 「通知機関によって発行された証明書の種類、番号、期限、およびその通知機関の名前または識別番号(該当する場合)」 - Annex VIII Section A (8)	✓	standardCompliance 、 validUntilTime 、 hasDocumentation リレーションシップおよび description リレーションシップが 使われることもある	AI 、 Core
検証の詳細	テスト計画	「実際の条件でのテスト計画の主な特徴の概要」 - Annex IX (4)	✓	hasDocumentation リレーションシップおよび description リレーションシップが 使われることもある	Core

カテゴリー	サブカテゴリー	EU AI法の概要と条項	AI BOMに存在するか?	AI BOMの該当するフィールド	SPDXプロファイル
検証の詳細	テストに参加したユーザー	「実際の条件でのテストに関与した提供者または見込み提供者、ならびに導入者の名前と連絡先詳細」 - Annex IX (2)	✗	このための特定のリレーションシップタイプは存在しない。ただし、リレーションシップ「to」として Agent (Person) および/または Organization と「 relationshipType 」として「other」を使用し、標準化された description 値を併用することができる。 連絡先詳細はPerson および Organization内の externalIdentifier で保持される	Core
アプリケーション詳細	市場	「AIシステムが市場に出され、サービスに投入され、または欧州連合内で利用可能にされたすべての加盟国」 - Annex VIII Section A (10)	✓	Organization が利用可能で、標準化された国コードの externalIdentifier を利用する	Core

表4 - EU AI法（一部）とSPDX 3.0の適合

医療機器に関するFDAおよびEMAの要件への適合の確保

米国食品医薬品局 (FDA) は、医療機器のサイバー セキュリティ リスクを評価し、製造業者のリスク管理プロセスを評価するためにソフトウェア部品表 (SBOM) を活用しています。同様に、欧州医薬品庁 (EMA) も医療機器のサイバー セキュリティとリスク管理の重要性を強調しています。

AIおよびDataset プロフィールと共に、SPDX 3.0で導入されたSourceおよびBuildプロフィールは、医療機器の市場提出プロセスに必要な要件を効果的に特定することができます。さらに、Runtimeプロフィールは、医療機器のサイバー セキュリティ監視と維持をサポートするために重要です。Securityプロフィールは、新たに発見された脆弱性の特定と軽減、ソフトウェアの更新やパッチの実施を支援します。

2024年3月22日現在、関連するFDAガイドラインは [FDA CFR サーチ](#) でアクセスできます。欧州連合の医療機器規制に関するガイドラインは、[MDCG承認文書及びその他のガイダンス](#) でアクセスできます。

カテゴリー	詳細とCIUAW	AI BOM に存在 するか	AI BOMの該当するフィールド	SPDXプロフ ファイル
パッケージ詳細	アプリケーション内のデータおよび情報に関する一般的な理解。[m]	✓	informationAboutApplication, Dataset プロファイル	AI, Dataset
	デバイスが診断、治療、予防、治癒、または軽減する条件の説明、ならびにデバイスが対象とする患者集団の説明。	✓	primaryPurpose	Software
	外国および米国での販売履歴の説明。この説明には、申請者によるデバイスの販売履歴および、もし知られていれば、他の人物によるデバイスの販売履歴を含むものとする。	✓	comment	Core
	デバイスの説明 (画像による表現を含む)。	✓	informationAboutApplication informationAboutTraining	AI
モデル詳細	申請書内のデータおよび情報について読者が全体的な理解を得られるような詳細な要約。	✓	informationAboutApplication informationAboutTraining	AI
	申請書に提出された非臨床試験の概要。	✓	metric	AI
	その機器が販売されたすべての国のリストと、販売が中止されたすべての国のリストを含めること。	✓	comment	Core
モデル詳細	その機器がどのように性能基準を満たしているか、またはどのような逸脱がある場合にはその正当性を示すための十分な情報を提供すること。	✓	comment	Core

カテゴリー	詳細とCIUAW	AI BOM に存在 するか	AI BOMの該当するフィールド	SPDXプロフ ファイル
データ詳細	データがどのように収集および分析されたかの説明、ならびに結果が肯定的、否定的、または結論が出ないものであるかにかかわらず、その概要を記載すること。	✓	dataCollectionProcess	Dataset

表5 - SPDX 3.0を通じた米国FDA医療機器規制への準拠

カテゴリー	詳細と節	SPDXに 存在する か	フィールド名	SPDXプロフ ファイル
パッケージ詳細	<p>第10条 - 製造業者の一般的義務:</p> <ul style="list-style-type: none"> - 第10条第1項: 製造業者は、自社の機器がAnnex Iに定められた基本的な安全性および性能要件を満たしていることを確保しなければならない。 - 第10条第2項: 製造業者は、設計、製造、最終検査を網羅する品質管理システムを確立し、維持しなければならない。 - 第10条第3項: 製造業者は、機器に関する技術文書を作成し、最新の状態に保たなければならない 	✓	<p>spdxId、locator、created、packageVersion、createdBy、originatedBy、suppliedBy、downloadLocation、primaryPurpose、datasetType、verifiedUsing、typeOfModel、informationAboutApplication、informationAboutTraining、metric、comment、description</p> <p>hasConcludedLicense、hasDeclaredLicense、testedOn、trainedOn リレーションシップ</p>	AI 、 Core 、 Dataset 、 Licensing 、 Software

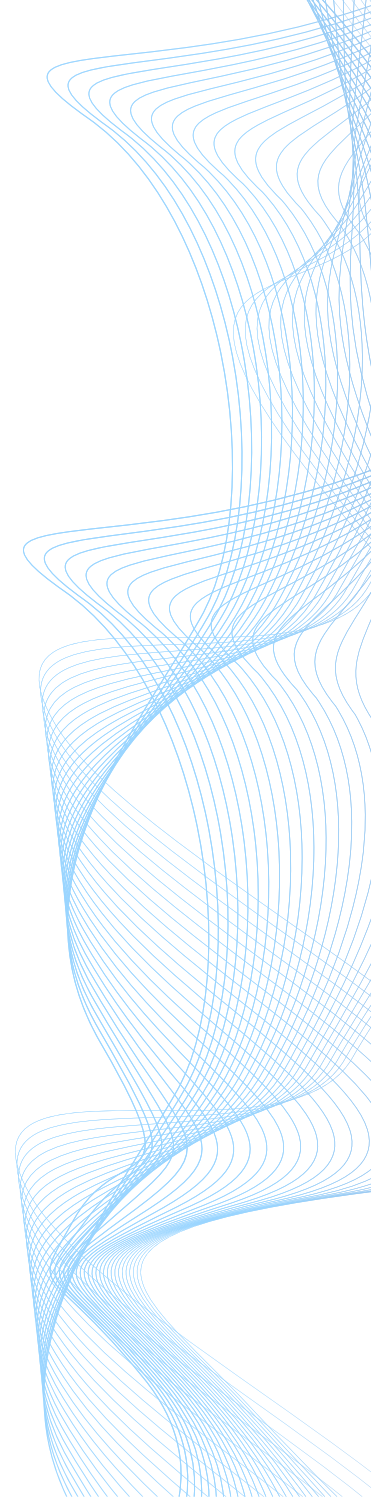
表6 - SPDX 3.0を通じたEU医療機器規則 (MDR) への準拠

IEEE倫理技術規格 (P70xxシリーズ) への準拠の確保

IEEE P70xxシリーズ規格は、準拠を確保するために文書化すべき重要な情報を明示しています。P70xx規格で要求されるすべてのフィールドがSPDXで明示的に義務付けられているわけではありませんが、P70xx規格に従うためには、SPDX 3.0のすべての必要なフィールドを含める必要があります。両規格に準拠し、AIシステムの整合性と信頼性を確保するためには、関連情報を包括的に文書化することが重要です。SPDX 3.0は、必要なすべての情報を文書化するための包括的なフレームワークを提供しており、IEEE P70xxとSPDX規格の両方を満たすことを目指す組織にとって理想的な選択肢となります。

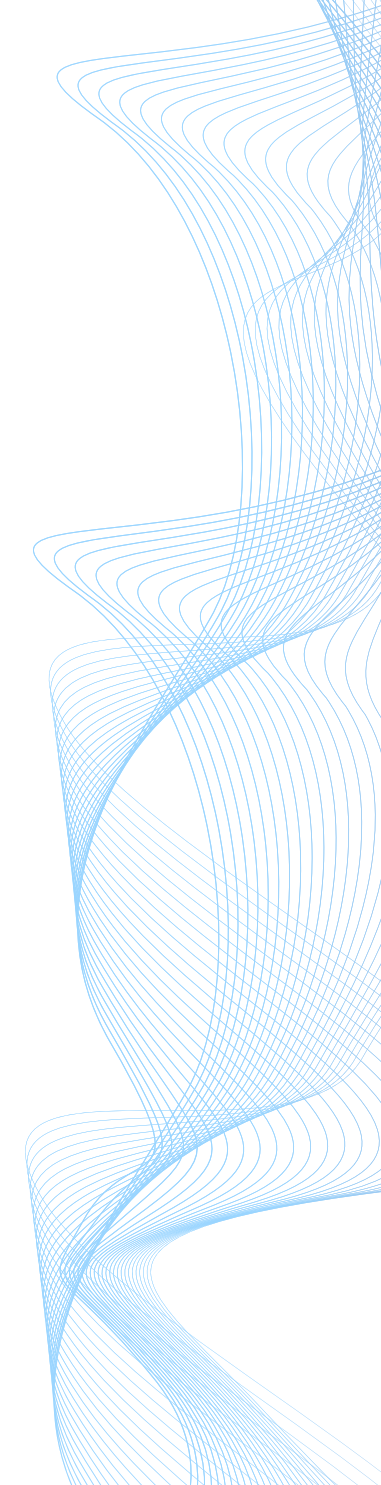
カテゴリー	説明 かつ/または セクション	SPDXに存在するか	フィールド名	SPDXプロファイル
パッケージ詳細	<p>7000 - 条項 1.2: 倫理的価値観と原則は、システム設計プロセス全体で考慮されなければならないと義務付けています。</p> <p>7001 - 条項 2.2: 利害関係者が倫理的考慮や意思決定プロセスに関与することを義務付けています。</p> <p>7002 - 条項 5.2: 監査履歴には、データを作成した人物、作成日時、およびその後の修正に関する情報を含めることを義務付けています。</p> <p>7009 - 条項 1.1: フェイルセーフ設計をサポートするシステムアーキテクチャの原則と所有権を識別する文書を求めています。</p> <p>7014 - 条項 5.1: システムの倫理的設計と運用に責任を持つ人々が責任を負うことを保証するための責任メカニズムの確立を求めています。</p>	✓	createdBy	Core
	<p>7000 - 条項 3.2: 倫理的影響評価を文書化することを義務付けています。</p> <p>7001 - 条項 4.2: 倫理的影響評価を文書化することを義務付けています。</p> <p>7002 - 条項 2.2: プライバシー影響評価では、データの出所を文書化し、データを作成した人物に関する情報を含めることを義務付けています。</p>	✓	impactStatement	Security

カテゴリー	説明 かつ/または セクション	SPDXに存在するか	フィールド名	SPDXプロファイル
パッケージ詳細	<p>7009 - 条項 5.2: 倫理的考慮事項とそれがシステム設計および運用に与える影響を文書化することを義務付けています。</p> <p>7010 - 条項 8.1: ユーザーおよび社会に与える影響を含むウェルビーイング指標の報告を求めています。</p> <p>7014 - 条項 3.2: 倫理的影響評価を文書化し、システム コンポーネントを作成した人物に関する情報を含め、利害関係者によるレビューを求めています。</p>	✓	impactStatement	Security
	<p>7000 - 条項 2.2: 透明性と説明責任の要件を文書化し、システムコンポーネントを提供した人物に関する情報を含めて利害関係者に伝達することを義務付けています。</p> <p>7001 - 条項 1.2: 倫理的原則と価値観をシステムライフサイクル全体で考慮し、システムコンポーネントを提供した人物の情報を含む文書化を求めています。</p> <p>7002 - 条項 4.2: データの来歴の文書化には、データを作成した人物、作成日時、及びその後の変更に関する詳細を含めることを義務付けています。</p> <p>7005 - 条項 5.2: 監査証跡には、データを提供した人物、提供日時、およびその後の変更に関する情報を含めることを義務付けています。</p> <p>7007 - 条項 5.1: システムの倫理的設計と運用に責任を持つ者が責任を負うことを保証するための責任メカニズムの確立を求めています。</p> <p>7009 - 条項 5.2: 責任メカニズムを文書化し、定期的にレビューすることを義務付けており、システムコンポーネントを提供した人物に関する情報を含める必要があります。</p> <p>7010 - 条項 5.1: システムの倫理的設計と運用に責任を持つ者が責任を負うことを保証するための責任メカニズムの確立を求めています。</p> <p>7014 - 条項 5.2: 責任メカニズムを文書化し、定期的にレビューすることを義務付けており、システムコンポーネントを提供した人物に関する情報を含める必要があります。</p>	✓	suppliedBy	Core



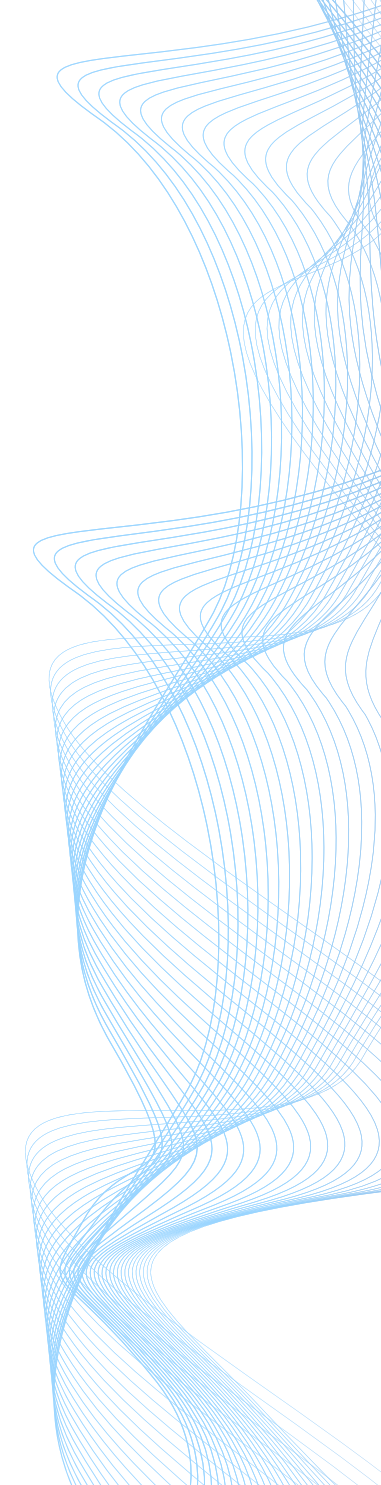
カテゴリー	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDXプロ ファイル
パッケージ詳細	7014 - 条項 11.1: 新たに発生する倫理的課題に対処するため、システムの継続的な監視および保守のプロセスを確立することを求めています。これには、データライフサイクル管理の実践を監視し、データの有効期限ポリシーが遵守されていることを確認することが含まれます。	✓	validUntilTime	Core
	7000 - 条項 5.2: これらの戦略が効果的であることを確保するために、文書化およびレビューを行うことが義務付けられています。 7001 - 条項 3.2: これらの透明性要件を文書化することが義務付けられています。 7002 - 条項 3.2: これらの仕組みには、データ利用の目的や文脈を文書化する規定が含まれる必要があり、アプリケーションやシステムの説明を含む場合があります。 7005 - 条項 2.1: 雇用者データが倫理的かつ責任を持って使用されることを確保するため、透明性および説明責任の仕組みを確立することが求められています。 7009 - 条項 2.2: 障害が発生した場合にシステム機能を回復または安全な状態に移行するための回復機構を開発および実装することが義務付けられています。 7010 -- 条項 7.2: 福祉指標の有効性を評価するための監視および評価プロセスを確立することが義務付けられています。 7014 - 条項 6.2: 必要に応じてステークホルダーや規制当局に提供される文書を作成することが義務付けられており、これにはアプリケーションやシステムの説明が含まれます。	✓	description	Core
	7000 - 条項 5.2: これらの戦略を文書化し、その有効性を確保するためにレビューを行うことが義務付けられています。 7001 - 条項 5.2: これらの戦略を文書化し、その有効性を確保するためにレビューを行うことが義務付けられています。 7002 - 条項 1.2: これらの方針および手順には、データ利用の目的および文脈を文書化する規定を含める必要があり、AIアプリケーションの主要な目的を含む場合があります。	✓	primaryPurpose	Software

カテゴリー	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDXプロ ファイル
パッケージ詳細	<p>7010 - 条項 1.2: 人間の福祉の促進、倫理的配慮、AIの責任ある利用を含む指標の目的を概説しています。</p> <p>7014 - 条項 6.2: ステークホルダーや規制当局が必要に応じて利用できる文書を作成することが義務付けられており、これにはシステムの主要な目的の説明が含まれます。</p>	✓	primaryPurpose	Software
	<p>7000 - 条項 5.2: データまたはシステムコンポーネントのダウンロード元に関する情報を含め、これらのアカウントビリティメカニズムを文書化し、定期的にレビューすることが義務付けられています。</p> <p>7001 - 条項 2.2: データまたはシステム コンポーネントのダウンロード元に関する情報を含め、これらの透明性および説明責任要件を文書化し、ステークホルダーに伝えることが義務付けられています。</p> <p>7002 - 条項 3.2: データの来歴を文書化する規定を含め、これらのメカニズムを構築することが義務付けられています。これにはデータのダウンロード元に関する情報が含まれます。</p> <p>7005 - 条項 5.2: データを提供した人物、提供日時、およびその後の変更に関する情報を含めた監査証跡を作成することが義務付けられています。</p> <p>7007 - 条項 6.2: ステークホルダーや規制当局が必要に応じて利用できる文書を作成することが義務付けられており、これにはデータまたはシステム コンポーネントのダウンロード元に関する情報が含まれます。</p> <p>7014 - 条項 5.2: データまたはシステム コンポーネントのダウンロード元に関する情報を含め、これらのアカウントビリティメカニズムを文書化し、定期的にレビューすることが義務付けられています。</p>	✓	downloadLocation	Software
AI詳細	<p>7014 - 条項 5.2: この基準では、使用されるモデルの種類に関する情報を含め、これらのアカウントビリティメカニズムを文書化し、定期的にレビューすることが義務付けられています。</p>	✓	typeOfModel	AI



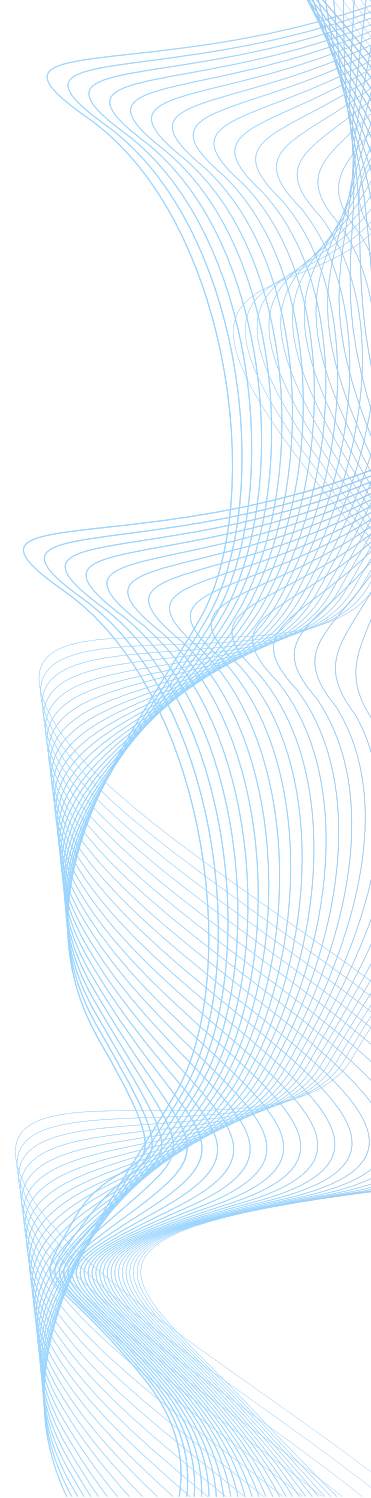
カテゴリー	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDX プロ ファイル
AI詳細	<p>7000 - 条項 5.2: この基準では、これらの戦略を文書化し、その効果を確認するために定期的にレビューすることが義務付けられています。</p> <p>7002 - 条項 2.1: データ処理活動に関連する潜在的なプライバシーリスクを特定するためのプライバシー影響評価の実施が求められています。</p> <p>7010 - 条項 8.2: 報告は、利害関係者にとって透明でアクセス可能で、理解しやすいものでなければならないと義務付けられています。</p> <p>7014 - 条項 4.2: これらの透明性と説明責任の要件は文書化され、利害関係者に伝えられる必要があります。</p>	✓	modelExplainability	AI
	<p>7005 - 条項 5.2: 監査トレイルには、データを提供した人物、提供された日時、およびその後の変更に関する情報が含まれている必要があります。</p> <p>7010 - 条項 7.3: 実装および監視の実践についての文書化が求められています。</p> <p>7014 - 条項 6.2: この文書は、必要に応じて利害関係者および規制当局に提供されなければならないと義務付けられており、AIアプリケーションに関する包括的な情報を含む必要があります。</p>	✓	informationAboutApplication	AI
	<p>7005 - 条項 5.2: 監査トレイルには、データを提供した人物、提供された日時、およびその後の変更に関する情報が含まれている必要があります。</p> <p>7009 - 条項 6.1: システムで使用されるデータの整合性とセキュリティを確保するためのデータ管理実践の実施が求められています。</p> <p>7002 - 条項 1.2: これらの方針と手順には、データの来歴を文書化するための規定が含まれており、データの作成者に関する情報も含まれる必要があります。</p> <p>7014 - 条項 4.2: これらの方針と手順は文書化され、利害関係者に対して、AIアプリケーションのトレーニングに関する包括的な情報を含めて伝達される必要があります。</p>	✓	informationAboutTraining	AI

カテゴリー	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDXプロ ファイル
AI詳細	<p>7001 - 条項 8.2: 検証およびバリデーションのプロセスは文書化され、利害関係者によってレビューされる必要があります。</p> <p>7009 - 条項 2.3: 故障検出および回復メカニズムは、その効果と制限を含めて文書化される必要があります。</p> <p>7014 - 条項 5.2: これらの戦略は文書化され、効果を確保するためにレビューされる必要があります。</p>	✓	limitation	AI
	<p>7000 - 条項 6.2: 検証およびバリデーション プロセスは文書化される必要があります。</p> <p>7001 - 条項 8.2: 検証およびバリデーション プロセスは文書化される必要があります。</p> <p>7009 - 条項 3.2: システムは安全要件を満たしていることを確認するために検証およびバリデーションされる必要があります。</p> <p>7010 - 条項 2.2: 物理的、精神的、社会的、環境的なウェルビーイングのさまざまな指標を文書化する必要があります。</p> <p>7014 - 条項 10.1: システムは定義された倫理的および透明性の要件を満たしていることを確認するために検証およびバリデーションされる必要があります。</p>	✓	metric	AI
	<p>7014 - 条項 10.2: システムが期待される品質指標を満たしていることを確認するために、検証およびバリデーションが必要です。</p>	✓	metricDecisionThreshold	AI
	<p>7000 - 条項 7.2: サポート プロセスは文書化され、定期的にレビューされることが義務付けられています。</p> <p>7001 - 条項 9.2: これらのプロセスは文書化され、定期的にレビューされることが義務付けられています。</p> <p>7009 - 条項 3.3: この規格では、発生するリスクや脆弱性に対応するために、継続的な監視およびメンテナンス プロセスの確立が求められています。</p>	✓	supportLevel	Core
	<p>7000 - 条項 10.2: 法律および規制への遵守は文書化され、レビューされることが義務付けられています。</p> <p>7001 - 条項 11.2: 法律および規制への遵守は文書化され、レビューされることが義務付けられています。</p>	✓	standardCompliance	AI



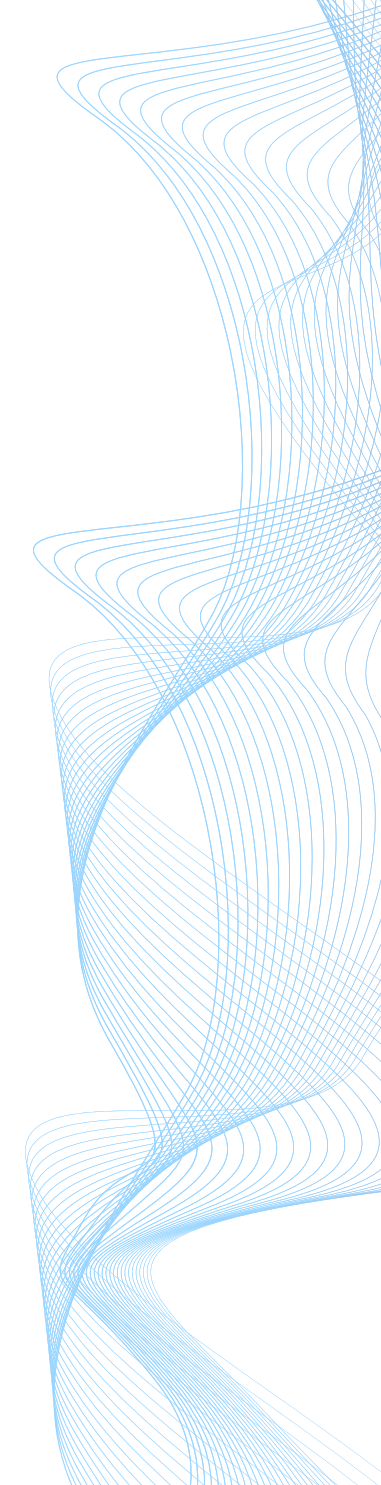
カテゴリー	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDXプロ ファイル
AI詳細	<p>7002 - 条項 2.2: これらの透明性および説明責任の要件は文書化され、利害関係者に対して説明されることが義務付けられており、関連する法律および規制への遵守に関する情報も含まれます。</p> <p>7005 - 条項 6.2: この文書は必要に応じて利害関係者および規制当局に提供され、関連する法律および規制への遵守に関する情報も含まれます。</p> <p>7007 - 条項 4.2: これらのポリシーおよび手順は文書化され、利害関係者に対して説明されることが義務付けられており、関連する法律および規制への遵守に関する情報も含まれます。</p> <p>7009 - 条項 8.2: 法律および規制への遵守の文書化が義務付けられています。</p> <p>7010 - 条項 5.2: ウェルビーイング指標を測定するために使用されるデータは、安全に管理され、関連する規制に遵守していることが義務付けられています。</p>	✓	standardCompliance	AI
	<p>7000 - 条項 4.2: これらの倫理的要件はシステムの設計および開発プロセスに組み込まなければならないことが義務付けられています。</p> <p>7009 - 条項 3.1: 潜在的な故障モードとその影響を特定するためのリスク評価の実施が義務付けられています。</p> <p>7014 - 条項 4.1: 共感を模倣するシステムの設計および運用に関連する潜在的なリスクを特定することが義務付けられています。</p>	✓	safetyRiskAssessment	AI
ソフトウェア詳細	<p>7000、7001、7002、7005、7007、7010、7014 - これらの条項は、特定のアプリケーションドメインの文脈におけるドメインタイプの要求を含みます。</p>	✓	domain	AI
	<p>7000、7001、7002、7005、7007、7010、7014 - 条項 6.1: これらの条項は、エミュレートされた共感の使用に関して、ユーザーからのインフォームド Consent (事前の同意) を得るためのメカニズムの確立を要求します。</p>	✓	comment	Core

カテゴリー	説明 かつ/または セクション	SPDXに存在するか	フィールド名	SPDXプロファイル
ソフトウェア詳細	<p>7005 - 条項 3.2: データの来歴の文書化が、データの供給者、供給日時、及びその後の変更についての詳細を含むべきことが要求されています。</p> <p>7009 - 条項 6.1: システムで使用されるデータの整合性とセキュリティを確保するためのデータ管理の実施が要求されています。</p> <p>7010 - 条項 5.1: 倫理的で透明なデータ収集方法の確立が要求されています。</p> <p>7014 - 条項 8.2: すべてのデータポリシーと手順が文書化されることが義務付けられています。</p>	✓	modelDataPreprocessing	AI
	<p>7014 - 条項 5.2: 機密データが文書化されるべきことが義務付けられています。</p>	✓	useSensitivePersonalInformation	AI
	<p>7005 - 条項 3.2: データの来歴の文書化には、データを提供した人物、提供された日時、及びその後の変更に関する詳細が含まれるべきことが義務付けられています。</p> <p>7009 - 条項 6.1: データの整合性とセキュリティを確保するためのデータ管理方法の実施が要求されています。</p> <p>7010 - 条項 5.3: データ収集および管理方法の文書化が義務付けられています。</p> <p>7014 - 条項 6.2: これらのメカニズムがユーザーの自律性を尊重し、ユーザーがエミュレートされた共感のレベルを制御するためのオプションを提供するべきことが義務付けられています。</p>	✓	autonomyType	AI
	<p>7009 - 条項 7.1: システムの環境への影響を評価することが要求されています。これには、エネルギー消費や廃棄物管理が含まれます。および条項 7.2: システムがさまざまな環境条件下で安全に動作するように設計されることが義務付けられています。</p> <p>7014 - 条項 4.2: これらの方針と手順が文書化され、利害関係者に通知されるべきことが義務付けられています。これには、エネルギー使用に関する考慮が関連する場合も含まれる可能性があります。</p>	✓	energyConsumption	AI
データ詳細	<p>7005 - 条項 3.2: データの来歴を文書化する際に、データの提供者、提供日時、およびその後の変更に関する詳細を含めることが義務付けられています。</p>	✓	anonymizationMethodUsed	Dataset



カテゴリ	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDXプロ ファイル
データ詳細	<p>7009 - 条項 6.1: システムで使用されるデータの完全性とセキュリティを確保するためのデータ管理手法の実施が要求されています。</p> <p>7014 - 条項 8.2: すべてのデータに関する方針と手続きが文書化されることが義務付けられています。</p>	✓	anonymizationMethodUsed	Dataset
	<p>7001 - 条項 6.2: データガバナンスの方針と手続きを文書化し、利害関係者に伝達することが義務付けられています。</p> <p>7002 - 条項 1.2: これらの方針と手順には、データの来歴を文書化するための規定を含む方針と手続きが義務付けられており、データ作成者に関する情報も含まれることを求めています。</p> <p>7005 - 条項 3.2: データの来歴に関する文書化が、データ提供者、提供日時、及びその後の変更に関する詳細を含むことが義務付けられています。</p> <p>7009 - 条項 6.1: システムで使用されるデータの完全性とセキュリティを確保するためのデータ管理手法の実施が要求されています。</p> <p>7010 - 条項 5.3: データ収集および管理手法を文書化することが要求されています。</p> <p>7014 - 条項 8.2: すべてのデータに関する方針と手続きが文書化されることが義務付けられています。</p>	✓	dataCollectionProcess	Dataset
	<p>7002 - 条項 1.2: これらの方針と手順には、データの来歴を文書化するための規定を含む方針と手続きが義務付けられており、データ作成者に関する情報も含まれることを求めています。</p> <p>7005 - 条項 3.2: データの来歴に関する文書化が、データの提供者、提供日時、およびその後の修正に関する詳細を含むことが義務付けられています。</p> <p>7009 - 条項 6.1: システムで使用されるデータの完全性とセキュリティを確保するためのデータ管理手法の実施が要求されています。</p> <p>7010 - 条項 5.3: データ収集および管理手法を文書化することが要求されています。</p> <p>7014 - 条項 8.2: すべてのデータに関する方針および手続きが文書化されることが義務付けられています。</p>	✓	dataPreprocessing	Dataset

カテゴリー	説明 かつ/または セクション	SPDXに存在するか	フィールド名	SPDXプロファイル
データ詳細	<p>7002 - 条項 1.2: これらの方針と手順には、データの来歴を文書化するための規定を含む方針と手続きが義務付けられており、データ作成者に関する情報も含まれることを求めています。</p> <p>7009 - 条項 6.1: システムで使用されるデータの完全性とセキュリティを確保するためのデータ管理手法の実施が要求されています。</p> <p>7014 - 条項 8.2: すべてのデータに関する方針および手続きが文書化されることが義務付けられています。</p>	✓	datasetAvailability	Dataset
	<p>7002 - 条項 1.2: これらの方針と手順には、データの来歴を文書化するための規定を含む方針と手続きが義務付けられており、データ作成者に関する情報も含まれることを求めています。</p> <p>7005 - 条項 3.2: データの来歴に関する文書が、データの提供者、提供日時、およびその後の修正に関する詳細を含むことが義務付けられています。</p> <p>7009 - 条項 6.1: システムで使用されるデータの完全性とセキュリティを確保するためのデータ管理手法の実施が要求されています。</p> <p>7010 - 条項 5.3: データ収集および管理手法を文書化することが要求されています。</p> <p>7014 - 条項 8.2: すべてのデータに関する方針および手続きが文書化されることが義務付けられています。</p>	✓	datasetNoise	Dataset
	<p>7002 - 条項 1.2: これらの方針と手順には、データの来歴を記録するための規定が含まれることが義務付けられています。この記録には、データを作成した人物に関する情報が含まれる必要があります。</p> <p>7005 - 条項 3.2: データの来歴を記録する際には、データを提供した人物、提供された時期、およびその後の変更に関する詳細を含むことが義務付けられています。</p> <p>7009 - 条項 6.1: システムで使用されるデータの完全性と安全性を確保するためのデータ管理手法の実施が義務付けられています。</p> <p>7014 - 条項 8.2: すべてのデータ方針と手順が文書化されることが義務付けられています。</p>	✓	datasetSize	Dataset



カテゴリー	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDXプロ ファイル
データ詳細	<p>7002 - 条項 1.2: これらの方針と手順には、データの来歴を記録するための規定が含まれることが義務付けられています。この記録には、データを作成した人物に関する情報が含まれる必要があります。</p> <p>7005 - 条項 3.2: データの来歴を記録する際には、データを提供した人物、提供された時期、およびその後の変更に関する詳細を含むことが義務付けられています。</p> <p>7009 - 条項 6.1: システムで使用されるデータの完全性と安全性を確保するためのデータ管理手法の実施が義務付けられています。</p> <p>7014 - 条項 8.2: すべてのデータ方針と手順が文書化されることが義務付けられています。</p>	✓	datasetType	Dataset
	<p>7009 - 条項 6.1: システムで使用されるデータの完全性と安全性を確保するためのデータ管理手法の実施が求められています。</p> <p>7010 - 条項 5.3: データ収集および管理手法の文書化が求められています。</p> <p>7014 - 条項 8.2: すべてのデータ方針と手順が文書化されることが義務付けられています。</p>	✓	datasetUpdateMechanism	Dataset
	<p>7000 - 条項 6.2: 意図された使用方法の文書化が義務付けられています。</p> <p>7001 - 条項 6.2: データ ガバナンスの方針と手順の文書化が義務付けられています。</p> <p>7002 - 条項 5.2: これらの実践は、データの意図された使用方法の文書化およびその使用に対する明示的な同意を得るための規定を含むことが義務付けられています。</p> <p>7005 - 条項 5.2: 監査証跡には、雇用主データの意図された使用方法に関する情報が含まれていることが義務付けられています。</p> <p>7007 - 条項 6.2: この文書は、利害関係者および規制当局が必要に応じて、システムの意図された使用方法に関する情報を含めて利用できるようにされることが義務付けられています。</p> <p>7009 - 条項 6.2: サイバー脅威からシステムを保護し、サイバーセキュリティ対策を確立することが義務付けられています。</p> <p>7010 - 条項 1.2: システムのライフサイクル全体を通じて、これらの倫理的原則と価値観が考慮されることが義務付けられており、システムの意図された使用方法の文書化が含まれます。</p> <p>7014 - 条項 8.1: エミュレートされた共感システムでのデータの倫理的かつ責任ある使用を確保するためのデータ ガバナンス方針と手順の確立が求められています。</p>	✓	intendedUse	Dataset

カテゴリー	説明 かつ/または セクション	SPDXに 存在する か	フィールド名	SPDXプロ ファイル
データ詳細	7001- 条項 6.2: データ ガバナンスの方針と手順の文書化が義務付けられています。 7002 - 条項 1.2: これらの方針と手順には、データの来歴を文書化するための規定が含まれ、データを作成した者に関する情報が含まれることが義務付けられています。 7009- 条項 6.1: システムで使用されるデータの整合性とセキュリティを確保するためのデータ管理実践の実施が求められています。 7010 - 条項 5.3: データ収集および管理実践の文書化が求められています。 7014 - 条項 7.2: 公平性の原則がシステムの設計と運用に組み込まれることが義務付けられています。	✓	knownBias	Dataset
	7014 - 条項 5.2: 共感的/敏感なデータの文書化が義務付けられています。	✓	hasSensitivePersonalInformation	Dataset
	7014 - 条項 8.2: すべてのデータ ポリシーおよび手順の文書化が義務付けられています。	✓	sensor	Dataset

表7 - IEEE P70xxの公開されている標準とSPDX 3.0の比較

この表は、公開されている複数のIEEE P70xx倫理技術標準と、SPDXが遵守する必要がある分野を比較しています。さらに、私たちは現在、米国の行政命令14028コンソーシアム、EU AIオフィス、カナダ、日本、英国のAIおよびデータ委員会、さらには複数の国際標準化機関（IEEEおよびISO）と協力して、SPDX 3.0のカバレッジの検証を行っています。

進行中の改訂および更新

AI分野が進展し続ける中、私たちのワーキンググループは新しい分野や考慮事項を特定し、AI部品表 (AI BOM) に統合することに努めています。定期的な更新および改訂は私たちのプロセスに不可欠であり、AI BOMが最新の状態を保ち、倫理的なAIの利用と文書化の最高基準に準拠することを保証します。例えば、EU AI法に基づく新たに浮上したニーズを考慮に入れています。

同様に、私たちは [Hugging Faceの最新のモデルカード](#) [s]には、「fine-tuned from model (モデルからの微調整)」、「funded by (資金提供者)」、「language (言語)」、「demo (デモ)」、「bias recommendations (バイアスに関する推奨)」、「testing factors (テスト要因)」、「model examination (モデルの検証)」、および環境への影響やコンピュータ インフラの把握に関する豊富なフィールドが含まれていることを認識しています。これらのフィールドを次回の改訂で標準に組み込むことを目指しており、その際、これらのフィールドがどれほど関連性があり、有用で実用的であるかについてコミュニティと十分に議論する予定です。これらの文書化標準の目的は、私たちのものとは異なるためです。



プロフィールの主要要素

SPDX AIおよびデータセット プロファイルの主要要素は何か

ライセンスの詳細: SPDXライセンスは、ソフトウェアやその他のコンテンツに関するライセンス情報を標準化して伝える方法を提供し、私たちの場合、AIモデルやデータセットのライセンス情報を含むことで、組織がオープンソースソフトウェアのサプライチェーンを管理し、AIシステムのライセンス義務を遵守するのを容易にします。さらに、AIモデルやデータセットには、ライセンス条項が不明確なライセンスが付いていることが一般的です。SPDXプロフィールの、宣言されたライセンスおよび結論に達したライセンスに関する情報を捕捉する機能は、実務者がライセンス遵守リスク要因を管理するのに役立ちます。AIおよびデータセット プロファイルで使用されるSPDX 3.0フィールドは、relationshipType = hasConcludedLicense および relationshipType = hasDeclaredLicense です。

モデルの詳細: AI特有のアプリケーションに必須のモデルに関する基本情報、すなわち名前、バージョン、タイプ。SPDX 3.0の特定フィールドは、spdxId、name、suppliedBy、downloadLocation、packageVersion、primaryPurpose、releaseTimeです。

モデルアーキテクチャ: モデルの構造に関する説明、例えばレイヤーの数と種類、ハードウェアの特性、およびその他の主要なアーキテクチャの選択肢。SPDX 3.0のフィールドは、typeOfModel、informationAboutTraining、informationAboutApplication、safetyRiskAssessment、standardCompliance、domain、autonomyTypeです。

トレーニングデータと方法論: モデルのトレーニングに使用されたデータに関する情報、例えばデータセットのサイズ、データソース、使用された前処理やデータ拡張技術など。また、トレーニング方法論に関する詳細、例えば使用されたオプティマイザー、損失関数、および調整されたハイパーパラメータなども含まれます。SPDX 3.0のフィールドは、modelDataPreprocessing、modelExplainability、hyperparameter、energyConsumption、

useSensitivePersonalInformation、および トレーニング データへのリレーションシップです。

パフォーマンスおよび検証指標: モデルのさまざまな指標におけるパフォーマンスに関する情報、例えば精度、適合率、再現率、F1スコアなど。また、モデルがデータの異なるサブセットでどのようにパフォーマンスを発揮するかに関する情報も含まれる場合があります。例えば、SPDX 3.0には次のフィールドがあります: metrics、metricDecisionThreshold。

バイアスと制限: モデルの潜在的なバイアスや制限についてリストアップしたもの、例えばトレーニングデータの不均衡、過学習、またはモデルの予測におけるバイアスなど。また、モデルの制限に関する情報も含まれます。例えば、新しいデータへの一般化能力や特定の使用ケースへの適性、遵守状況やリスクレベルに関する情報です。例えば、SPDX 3.0には次のフィールドがあります: knownBias、limitation。

責任あるAIの考慮事項: モデルに関連する倫理的または責任あるAIの考慮事項、例えばプライバシーの懸念、公平性、透明性、またはモデルの利用が社会に与える潜在的な影響や標準の遵守に関する情報です。SPDX 3.0のフィールドは、knownBias、primaryPurposeです。

気候変動に関する考慮事項: 主な環境問題は、AIモデルのトレーニングおよび運用に必要なエネルギー消費です。例えば、大規模な言語モデルはかなりの計算能力を必要とし、これが多大なエネルギー使用につながるがよくあります。特にこれらのモデルが再生可能エネルギー源に頼らないデータセンターでトレーニングされる場合です。このエネルギー使用は二酸化炭素排出に寄与し、気候変動に影響を及ぼす可能性があります。もう一つの考慮事項は、データセンターの冷却に使用される水などの物理的資源です。私たちは、開発者がエネルギー効率の良いAIアルゴリズムや、再生可能エネルギー源を使用したデータセンター、そしてハードウェアの循環型経済の原則を促進することをコメント欄で記録することを奨励しています。SPDX 3.0のフィールドは、

energyConsumption、commentsです。

データセットの詳細: データセットに関する基本情報、例えば名前、バージョン、ライセンスなど、および意図された使用ケース。SPDX 3.0の特定フィールドは、spxId、name、suppliedBy、downloadLocation、packageVersion、primaryPurpose、releaseTimeです。

データセットアーキテクチャ: データの構造やデータの種類に関する説明、例えばデータの数など。SPDX 3.0の特定フィールドは、datasetTypeです。

データセットのバイアスと制限: データセットの潜在的なバイアスや制限をリストアップしたもの、例えばトレーニングデータやプロダクションデータの不均衡など。SPDX 3.0の特定フィールドは、knownBias、limitationです。

データセットの責任あるAIの考慮事項: データに関連する倫理的または責任あるAIの考慮事項、例えばプライバシーの懸念、公平性、透明性、またはデータの使用が社会に与える潜在的な影響など。また、モデルのさらなるテスト、検証、または監視に関する推奨事項も含まれる場合があります。SPDX 3.0の特定フィールドは、metric、knownBias、useSensitivePersonalData、hasSensitivePersonalDataです。

AIおよびデータセットプロファイルで使用される主要なリレーションシップ

- relationshipType = contains
- relationshipType = hasConcludedLicense
- relationshipType = hasDeclaredLicense
- relationshipType = testedOn
- relationshipType = trainedOn

AIプロファイルは、AIシステムおよびモデルの成果物に関連する情報を文書化し、共有するための標準化された方法を提供することを目的と

しています。これらの成果物は、AI開発プロセスの具体的な成果物であり、ソフトウェアパッケージ、モデル、データセットなどです。このプロファイルは、SPDXのCoreおよびSoftwareプロファイルにモデル固有の追加フィールドを重ねる形で構築されています。

主な課題は、オープンソースのモデルとデータにソフトウェアのベストプラクティスを適応させ、自動化ツールの作成を可能にすることです。現在、監査人に必要な重要な情報、例えばライセンス、バージョン管理、検証などが、オープンモデルやデータをホスティングしているリポジトリには欠けていることが多いです。

1. **ライセンス:** 各AI成果物に関連するライセンスを明確に記載し、適切な使用と配布を確保するとともに、創作者や貢献者の権利を尊重すること。
2. **バージョン管理:** AI成果物の一貫したバージョン管理スキームを実施し、更新、バグ修正、改善の追跡をより効果的に行えるようにすること。
3. **検証:** AI成果物のパフォーマンスと信頼性を評価するために使用された検証およびテスト プロセスに関する情報を提供すること。
4. **来歴:** AI成果物の起源と履歴を文書化し、創作者、貢献者、および時間の経過に伴う変更点を含めること。
5. **メタデータ:** AI成果物に関連する適切なメタデータを記録し、再利用リスクの理解を深めるために目的、データ使用、パフォーマンスなどを明示すること。

必須なAIPackageのフィールド (AIプロファイル)

以下の表のフィールドは、[AIPackage](#) tがAIプロファイルに準拠していると見なされるために必須です (profileConformance = ["ai", "core", "software"])

フィールド	カーディナリティ	プロファイル	定義
buildTime	Required(1..1)	Core	成果物のビルド日時を指定
downloadLocation	Required(1..*)	Software	成果物がどこにあるかを指定
name	Required(1..1)	Core	作成者によって指定された成果物の名前を識別
packageVersion	Required(1..1)	Software	成果物のバージョンを識別
primaryPurpose	Required(1..1)	Software	ソフトウェア成果物の主な目的を識別 (例:「モデル」)
releaseTime	Required(1..1)	Core	成果物がリリースされた日時を指定
spdxId	Required(1..1)	Core	成果物のグローバルに一意的な識別子
suppliedBy	Required(1..*)	Core	成果物を提供した人物、組織、またはツールを識別
relationshipType = hasConcludedLicense	Required(1..1)	Core	すべてのAIPackageには、必ず一つの「has-ConcludedLicense」タイプのリレーションシップが存在し、その要素が「from」プロパティとして、AnyLicenseInfoが「to」プロパティとして設定されている「必要がある」
relationshipType = hasDeclaredLicense	Required(1..1)	Core	すべてのAIPackageには、必ず一つの「has-DeclaredLicense」タイプのリレーションシップが存在し、その要素が「from」プロパティとして、AnyLicenseInfoが「to」プロパティとして設定されている「必要がある」

表8 - AIプロファイルからのAIPackageに必須なフィールド

任意のAIPackageのフィールド (AIプロファイル)

フィールド	カーディナリティ	プロファイル	定義
autonomyType	Optional(0..1)	AI	意思決定のループに人間が必要かどうかをリスト
domain	Optional(0..1)	AI	AIシステムが属するドメインの種類を指定
energyConsumption	Optional(0..1)	AI	AIシステムで使用されるAIモデルのトレーニング、推論、およびファインチューニングのエネルギー消費を識別
energyQuantity	Optional(1..1)	AI	energyQuantityプロパティは、消費されたエネルギーの量を保存する
energyUnit	Optional(1..1)	AI	energyUnitプロパティは、測定に使用された単位を保存する
hyperparameter	Optional(0..*)	AI	トレーニングプロセス前に定義された、学習アルゴリズムの挙動を制御する関連する設定
information-AboutTraining	Optional(0..1)	AI	モデルのトレーニングに関する関連する特徴や情報
information-AboutApplication	Optional(0..1)	AI	アプリケーションに関する関連する特徴や情報
limitation	Optional(0..1)	AI	システムに関する既知の関連する制限事項
metric	Optional(0..*)	AI	どのようにテストされたかに関する関連する情報
metricDecision-Threshold	Optional(0..*)	AI	アプリケーションがベンチマークに達しているかどうかに関する関連する情報
modelDataPre-processing	Optional(0..*)	AI	データ準備フェーズのすべてのステップのリスト
modelExplainability	Optional(0..*)	AI	一般ユーザーに対してモデルの動作をどのように説明するかに関する関連情報
safetyRiskAssessment	Optional(0..1)	AI	モデルのリスク分類を指定

フィールド	カーディナリティ	プロファイル	定義
standardCompliance	Optional(0..*)	AI	遵守されている関連する標準
typeOfModel	Optional(0..*)	AI	モデルのタイプを指定
useSensitivePersonalInformation	Optional(0..1)	AI	アプリケーションは敏感な個人データを使用しているか
relationshipType = testedOn	Optional(0..1)	Core	テスト目的およびデプロイ検証目的のためのデータセットを指定
relationshipType = trainedOn	Optional(0..1)	Core	トレーニング目的のためのデータセットを指定

表9 - AIプロファイルからのAIPackageに任意なフィールド

必須のDatasetPackageフィールド (Datasetプロファイル)

以下の表のフィールドは、[DatasetPackage](#) がDataset Profileに準拠していると思なされるために必須です (profileConformance = ["core", "dataset", "software"])。

フィールド	カーディナリティ	プロファイル	定義
buildTime	Required(1..1)	Core	成果物のビルド日時を指定
datasetType	Required(1..1)	Dataset	データセットに含まれるデータのタイプの説明
downloadLocation	Required(1..*)	Software	成果物がどこにあるかを指定
originatedBy	Required(1..*)	Core	データセットを作成した人物、組織、またはツール
packageVersion	Required(1..1)	Software	成果物のバージョンを識別

フィールド	カーディナリティ	プロファイル	定義
primaryPurpose	Required(1..1)	Software	ソフトウェア成果物の主な目的を識別
name	Required(1..1)	Core	作成者によって指定された成果物の名前
releaseTime	Required(1..1)	Core	成果物がリリースされた日時を指定
spdxId	Required(1..1)	Core	成果物のグローバルに一意的な識別子
relationshipType = hasConcludedLicense	Required(1..1)	Core	すべてのDatasetPackageには、必ず1つの「hasConcludedLicense」タイプのリレーションシップが存在し、その要素が「from」プロパティとして、AnyLicenseInfoが「to」プロパティとして設定されている「必要がある」
relationshipType = hasDeclaredLicense	Required(1..1)	Core	すべてのDatasetPackageには、必ず1つの「hasDeclaredLicense」タイプのリレーションシップが存在し、その要素が「from」プロパティとして、AnyLicenseInfoが「to」プロパティとして設定されている「必要がある」

表10 - DatasetプロファイルからのDatasetPackageに必須なフィールド

任意のDatasetPackageフィールド (Datasetプロファイル)

フィールド	カーディナリティ	プロファイル	定義
anonymization-MethodUsed	Optional(0..1)	Dataset	使用された匿名化方法を説明
confidentialityLevel	Optional(0..1)	Dataset	データセットに含まれるデータポイントの機密性レベルを説明
dataCollectionProcess	Optional(0..1)	Dataset	データセットがどのように収集されたかを説明

フィールド	カーディナリティ	プロファイル	定義
dataPreprocessing	Optional(0..1)	Dataset	生データに適用された前処理手順を説明し、与えられたデータセットを作成した方法を説明
datasetAvailability	Optional(0..1)	Dataset	データセットが公開されており、直接ダウンロードできるかどうかを示す。それ以外の場合は、クリックを通じてアクセスするか、登録フォームを記入することでのみアクセスできることを示す
datasetNoise	Optional(0..1)	Dataset	データセットに含まれる可能性のあるノイズの種類を説明
datasetSize	Optional(0..1)	Dataset	データセットのサイズを示す
datasetType	Optional(0..1)	Dataset	データセットに含まれるデータの種類を説明
datasetUpdate-Mechanism	Optional(0..1)	Dataset	データセットを更新するためのメカニズムを説明
hasSensitivePersonalInformation	Optional(0..1)	Dataset	データセットにセンシティブな個人情報が含まれているかどうかを説明
intendedUse	Optional(0..1)	Dataset	与えられたデータセットが何のために使用されるべきかを説明
knownBias	Optional(0..1)	Dataset	データセットが包含していることが知られているバイアスを記録
sensor	Optional(0..1)	Dataset	データ収集に使用されたセンサーについて説明

表11 - DatasetプロファイルからのDatasetPackageに任意なフィールド

AIおよびDatasetパッケージ フィールド詳細

このセクションでは、AIおよびDatasetプロファイルからのAIPackageおよびDatasetPackageに共通する、かつ必須のフィールドについて説明します。各フィールドには、その説明、タイプ、使用例、およびJSON-LDシリアライゼーションの例が含まれます。なお、ドキュメント内のすべてのJSON-LDの例は説明用であり、SPDXドキュメント内で有効なオブジェクトと見なされるためには追加のフィールドが必要な場合があることにご注意ください。

spdxId (必須)

概要: spdxIdは、他の要素によって参照される可能性のある要素を一意に識別します。これらの参照は、内部または外部のものかもしれませんが、同じ要素の複数のバージョンが存在する可能性があります。各バージョンは一意に参照できる必要があります。これにより、要素間の関係を明確に表現することができます。

タイプ: xsd:anyURI

例: spdxIdは、エージェント、パッケージ、ファイル、またはその他の要素を識別するために使用できます。グローバルに一意であることを確保するため、spdxIdには標準化された一意の識別子（例えば、ユニバーサルユニーク識別子 (UUID)）を組み込むことができます。

構文:

```
{
  "type": "ai_AIPackage",
  "spdxId": "https://spdx.org/spdxdocs/Person/AS-1000e6a2-0229-4875-baa7-c99be213b6e1"
}
```

name (必須)

概要: 作成者によって指定された要素の名前を識別します。

タイプ: xsd:string

例: nameフィールドは、SPDXドキュメント内のさまざまな要素（ドキュメント自体、パッケージ、ファイル、またはファイル内の特定のコードスニペットなど）を識別するために使用できます。

構文:

```
{
  "type": "ai_AIPackage",
  "name": "An example SPDX document"
}
```

buildTime (必須)

概要: アーティファクトがビルドされた時刻を指定します。

buildTimeは、ビルド時刻を特定の日付と時刻の文字列表現で示します。精度は秒単位で、常にUTCタイムゾーンで表現されます。ISO-8601形式は、YYYY-MM-DDThh:mm:ssZです。

タイプ: DateTime (xsd:dateTimeStampのサブクラス)

例: Package、File、Dataset、Artifact のビルド時刻。

構文:

```
{
  "type": "ai_AIPackage",
  "buildTime": "2024-04-24T12:00:00Z"
}
```

downloadLocation (必須)

概要: downloadLocationは、ドキュメントが作成された時点でのパッケージのダウンロード用リソース識別子 (URI) を特定します。参照される正確なパッケージをどこで、どのようにダウンロードするかを明確にすることは、検証とデータ追跡において重要です。

タイプ: xsd:anyURI

例: downloadLocationは、直接ダウンロードリンク、リポジトリのURL、またはバージョン管理システム内の特定のパスなど、さまざまな種類のリソースを指すことができます。

構文:

```
{
  "type": "ai_AIPackage",
  "downloadLocation": "https://example.com/download/anotherexamplepackage.tar.gz"
}
```

packageVersion (必須)

概要: packageVersionは、識別目的やパッケージバージョンの後続の変更を示すために役立ちます。使用されるバージョンニング方式には制限がありません。

タイプ: xsd:string

例: 有効な例としては、“3.14159”、“1.0.0-alpha”、“2.4_13”、“24.04”、“1.2.1.2”、“2024H”、“961219 ASIA”、“3.6:1:0123abcd:x86_64”などがあります。

構文:

```
{  
  "type": "ai_AIPackage",  
  "packageVersion": "3.14159"  
}
```

primaryPurpose (必須)

概要: primaryPurposeは、ソフトウェアアーティファクトの主な意図された機能に関する情報を提供します。その値は、SoftwarePurposeデータ型で定義されたエントリの1つから選択する必要があります。

タイプ: SoftwarePurpose (以下のリストから1つ選

択: application、archive、bom、configuration、container、data、device、deviceDriver、diskImage、documentation、evidence、executable、file、filesystemImage、firmware、framework、install、library、manifest、model、module、operatingSystem、other、patch、platform、requirement、source、specification、test)

例: “application”はソフトウェアアーティファクトがソフトウェアアプリケーションであることを示します。“library”はソフトウェアアーティファクトがソフトウェアライブラリであることを示します。“model”はソフトウェアアーティファクトが機械学習または人工知能モデルであることを示します。

構文:

```
{  
  "type": "ai_AIPackage",  
  "primaryPurpose": "model"  
}
```

releaseTime(必須)

概要: releaseTimeは、アーティファクトがリリースされた日時を指定します。releaseTimeはリリース時刻の特定の日付と時間を文字列形式で表現します。秒単位の精度を持ち、常にUTCタイムゾーンで表現されます。ISO-8601形式はYYYY-MM-DDThh:mm:ssZです。

タイプ: DateTime (xsd:dateTimeStampのサブクラス)

例: Package、File、Dataset、Artifactのリリース時刻。

構文:

```
{  
  "type": "dataset_DatasetPackage",  
  "releaseTime": "2023-10-06T17:00:00Z"  
}
```

suppliedBy (必須)

概要: suppliedByは、アーティファクト (例: スニペット、ファイル、AI、データセットパッケージ、脆弱性) の実際の配布元を識別します。

タイプ: Agent (組織または個人)

例: suppliedByフィールドは、ソフトウェアコンポーネントの供給元を追跡するのに役立ちます。これにより、各コンポーネントの出所を特定し、正しい供給者にクレジットを与えることが容易になります。これは、ライセンス条項への準拠や監査目的において重要です。

構文:

```
{
  "type": "ai_AIPackage",
  "suppliedBy": {
    "type": "Organization",
    "name": "Example AI Co-op"
  }
}
```

relationshipType = hasConcludedLicense (必須)

概要: hasConcludedLicenseリレーションシップは、SPDXデータの作成者がソフトウェア アーティファクトを規定すると合理的に結論づけたライセンスを識別します。この結論は、ソフトウェア アーティファクト内のライセンス情報やその他の関連データの分析に基づいています。AIパッケージやデータセットパッケージのようなソフトウェア アーティファクトには、複数の結論付けられたライセンスが存在する場合があります。

タイプ: Relationship

例: Relationshipオブジェクト内の「to」フィールドに含まれるライセンスは、[NoAssertionLicense](#)、[NoneLicense](#)、[LicenseExpression](#)、または [SPDXライセンスリスト](#) に記載された任意のライセンスを含む、AnyLicenseInfoクラスの任意のオブジェクトとすることができます。

構文:

```
{
  "type": "Relationship",
  "relationshipType": "hasConcludedLicense",
  "from": "https://spdx.org/spdxdocs/AIPackage/EX-a09c4e3e-df9a-48e7-9a2a-
```

```
38ca15cd2ea7",
  "to": [
    "https://spdx.org/licenses/Apache-2.0"
  ]
}
```

relationshipType = hasDeclaredLicense (必須)

概要: hasDeclaredLicenseリレーションシップは、ソフトウェア アーティファクト内で実際に発見されたライセンス情報を識別します。例えば、これは自動化ツールを使用して検出されたライセンス情報です。AIパッケージやDatasetパッケージのようなソフトウェア アーティファクトには、複数の宣言されたライセンスが存在する場合があります。

タイプ: Relationship

例: Relationshipオブジェクト内の「to」フィールドに含まれるライセンスは、[NoAssertionLicense](#)、[NoneLicense](#)、[LicenseExpression](#)、または [SPDX License List](#)に記載された任意のライセンスを含む、AnyLicenseInfoクラスの任意のオブジェクトとすることができます。

構文:

```
{
  "type": "Relationship",
  "relationshipType": "hasDeclaredLicense",
  "from": "https://spdx.org/spdxdocs/DatasetPackage/DS-d170dabb-fe05-4c98-b41d-5f62dc6d606a", "to":
  [
    "https://spdx.org/licenses/CC-BY-4.0"
  ]
}
```

特定のAIPackageフィールドの詳細

このセクションでは、AI ProfileのAIPackageに特有のフィールドについて説明します。各フィールドには、その説明、タイプ、例、およびJSON-LDのシリアライズ例が含まれています。

autonomyType (任意)

概要: システムが人間の関与や指導なしに意思決定や行動を実行できるかどうかを示します。

タイプ: PresenceType (以下のリストから1つを選択: yes、no、noAssertion)

例: 「yes」は、AIシステムが潜在的に人間なしで意思決定を行えることを示します (例: 自動運転車、無人航空機、ロボット、バーチャルアシスタント)。

「no」は、人間がAIの意思決定を検証するために関与していることを示します (例: 住宅ローン承認、金融投資、司法制度)。

「noAssertion」は、利用可能な情報から自律性のタイプが不明であることを示します。モデルが文書化されている時点での情報に基づいています。

構文:

```
{  
  "type": "ai_AIPackage",  
  "ai_autonomyType": "yes"  
}
```

domain (任意)

概要: AIソフトウェアに含まれるAIモデルが正常に機能することが期待されるドメインを記述する自由形式のテキストです。

タイプ: xsd:string

例: コンピュータビジョン (computer vision)、自然言語処理

(natural language processing) など

構文:

```
{  
  "type": "ai_AIPackage",  
  "ai_domain": "natural language  
  processing"  
}
```

energyConsumption (任意)

概要: AIモデルのトレーニングにかかる既知または推定されるエネルギー消費を記録します。エネルギー消費が不明な場合、推定値は使用された計算リソース (例えば、浮動小数点演算回数)、トレーニング時間、処理ユニットの種類と数量、その他トレーニングに関連する詳細に基づくことができます。もしenergyConsumptionに値が設定されている場合、energyQuantityおよびenergyUnitは必須です。

タイプ: EnergyConsumption

例: 自然言語処理 (NLP) タイプの大規模言語モデルは、機械翻訳、テキスト生成、感情分析に使用されるアプリケーションであり、トレーニングに膨大な計算リソースを必要とします。エネルギー消費は重要で、単一の大規模言語モデルがその全生涯で5台の車と同じ量の炭素を排出する可能性があるとして推定されています。そのため、NLPモデルのトレーニングのエネルギー効率を改善する方法の開発への関心が高まっており、これにより開発者がトレーニングアルゴリズムを最適化し、より効率的なハードウェアを活用する能力が向上するでしょう。

構文:

```
{
  "type": "ai_AIPackage",
  "ai_energyConsumption":
  {
    "type": "ai_EnergyConsumption",
    "ai_trainingEnergyConsumption":
    [
      {
        "type": "ai_
EnergyConsumptionDescription",
        "ai_energyQuantity": "36.5",
        "ai_energyUnit":
        "kilowattHour"
      },
      {
        "type": "ai_
EnergyConsumptionDescription",
        "ai_energyQuantity": "0.4",
        "ai_energyUnit":
        "kilowattHour"
      }
    ],
    "ai_inferenceEnergyConsumption":
    [
      {
        "type": "ai_
EnergyConsumptionDescription",
        "ai_energyQuantity": "0.042",
        "ai_energyUnit":
        "kilowattHour"
      }
    ]
  }
}
```

```
]
}
```

energyQuantity (任意)

概要: エネルギーの数量情報を提供します。

タイプ: xsd:decimal

例: トラフィックパターンなどの各センサーの電力使用量。

構文:

```
{
  "type": "ai_EnergyConsumptionDescription",
  "ai_energyQuantity": "0.042",
  "ai_energyUnit": "kilowattHour"
}
```

energyUnit (任意)

概要: エネルギーの単位情報を提供します。

タイプ: EnergyUnitType (以下のリストから1つを選択:
kilowattHour、megajoule、other)

例: 「kilowattHour」はキロワット時 (kW.h) を示します。

「megajoule」はメガジュール (MJ) を示します。「other」はその他のエネルギー測定単位を示し、必要に応じて「comment」フィールドで詳細を指定します。

構文:

```
{
  "type": "ai_EnergyConsumptionDescription",
  "ai_energyQuantity": "0.042",
  "ai_energyUnit": "kilowattHour"
}
```

finetuningEnergyConsumption (任意)

概要: AIシステムで使用されるAIモデルの微調整時に消費されるエネルギー量を指定します。

タイプ: EnergyConsumptionDescription

例: 画像分類のための深層学習ニューラルネットワークのファインチューニング段階で、ファインチューニングモジュール自体が15 kWh (キロワット時) のエネルギーを消費したと報告されています。

構文:

```
{
  "type": "ai_EnergyConsumption",
  "ai_finetuningEnergyConsumption":
  [
    {
      "type": "ai_
      EnergyConsumptionDescription",
      "ai_energyQuantity": "2.4",
      "ai_energyUnit": "kilowattHour"
    }
  ]
}
```

hyperparameter (任意)

概要: ハイパーパラメータ値を記録します。ハイパーパラメータは、学習アルゴリズムの動作を制御するためにトレーニングプロセス前に定義される設定です。これらは、トレーニング中にデータから学習されるモデルパラメータとは異なります。開発者は通常、ハイパーパラメータを手動で設定するか、ハイパーパラメータチューニング (いわゆる試行錯誤) のプロセスを通じて設定します。

タイプ: /Core/DictionaryEntry

例: 学習率、バッチサイズ、ニューラルネットワークの層の数。

構文:

```
{
  "type": "ai_AIPackage",
  "ai_hyperparameter":
  [
    {
      "type": "DictionaryEntry",
      "key": "cnn_kernel_vals",
      "value": "[5, 5, 3, 3, 3]"
    },
    {
      "type": "DictionaryEntry",
      "key": "beam_search_scoring_
      mode", "value": "Words"
    }
  ]
}
```

inferenceEnergyConsumption (任意)

概要: 推論時にAIシステムで使用されるAIモデルによって消費されるエネルギーの量を指定します。

タイプ: EnergyConsumptionDescription

例: 画像分類のためのディープラーニングニューラルネットワークの推論段階で、トレーニングモジュール自体が80ワット時のエネルギーを消費したと報告されています。

構文:

```
{
  "type": "ai_EnergyConsumption",
  "ai_inferenceEnergyConsumption": [
    {
```

```

    "type": "ai_
    EnergyConsumptionDescription",
    "ai_energyQuantity": "0.042",
    "ai_energyUnit": "kilowattHour"
  }
}

```

informationAboutApplication (任意)

概要: ソフトウェア内でAIモデルがどのように使用されているかの説明。これには、前処理の手順、サードパーティAPI、その他の関連する詳細が含まれるべきです。AIモデルがソフトウェアアプリケーション内で提供する機能には、実行するために設計された特定のタスクや決定、入力データがAIモデルに渡される前に適用される前処理手順（データ クリーニング、正規化、特徴抽出など）、およびAIモデルと併用されるサードパーティAPIやサービス（データソース、クラウドサービス、他のAIモデルなど）が含まれます。また、AIモデルをソフトウェアアプリケーション内で実行するために必要な依存関係や要件（特定のハードウェア、ソフトウェア ライブラリ、サードパーティAPI、オペレーティングシステム、その他の関連する詳細）についても説明します。

タイプ: xsd:string

例: このモデルの設計、開発、展開において行われた特定のタスクや決定。

構文:

```

{
  "type": "ai_AIPackage",
  "ai_informationAboutApplication": "A
  vehicle identification system utilizes XYZ
  Cloud's object classification service in
  conjunction with a custom-AI model designed
  for vehicle make and model classification. The
  system is designed to process 1600x1200 pixel

```

```

images captured by a consumer-grade camera
equipped with automatic lighting adjustment."
}

```

informationAboutTraining (任意)

概要: 訓練プロセスの詳細な説明、使用された特定の技術、アルゴリズム、方法を含みます。

タイプ: xsd:string

例: AIモデルを訓練するために使用された訓練データに関する関連情報、例えば、データのソースや品質、使用された測定基準/ベンチマークなど。具体的な例としては、テキストを肯定的、否定的、または中立的に分類する感情分析モデルの訓練プロセスを説明することが挙げられます。

構文:

```

{
  "type": "ai_AIPackage",
  "ai_informationAboutTraining": "The
  sentiment analysis model was trained using
  a supervised learning approach with the
  following details: The training data was
  sourced from a combination of public datasets
  such as the IMDb movie reviews dataset
  and the Sentiment140 dataset. The data was
  preprocessed to remove duplicates, handle
  missing values, and normalize text. The
  quality was measured using metrics such as
  accuracy, precision, recall, and F1 score

```

on a held-out validation set. The model was trained using a deep learning approach with a Bidirectional LSTM (Long Short-Term Memory) network. The network architecture included an embedding layer, two bidirectional LSTM layers, and a dense output layer with softmax activation. The model was optimized using the Adam optimizer with a learning rate of 0.001. The model achieved an accuracy of 85% on the test set, with an F1 score of 0.84 for positive sentiment, 0.82 for negative sentiment, and 0.80 for neutral sentiment.”

```
}
```

limitation (任意)

概要: AIパッケージ (またはAIパッケージ内のAIモデル) の制限を記録します。これは網羅的であることは保証されておらず、AIパッケージ (またはその中のAIモデル) の制限に関するものではありません。

タイプ: xsd:string

例: モデルやアプリケーションの使用に関する地域制限。トレーニングデータセットにおけるデータの多様性の欠如 (例えば、白人の人物が多く含まれている画像の偏り)。アルゴリズムの制限 (例えば、ノイズに対する感度)。ドメイン固有の制限 (例えば、クレジットカード詐欺を検出するモデルの訓練は、他の金融取引での詐欺検出と比較して異なる課題があります)。

構文:

```
{  
  "type": "ai_AIPackage",  
  "ai_limitation": "The dataset used for  
model training was largely collected under  
clear weather conditions, which may limit the  
model's ability to predict accurately in other
```

```
weather types.”
```

```
}
```

metric (任意)

概要: AIモデルが評価された際の測定基準を記録します。これにより、予測の質に関する声明を行うことができ、例えば不確実性、精度、テストされた集団の特性、質、公平性、説明可能性、堅牢性などが含まれます。

タイプ: DictionaryEntry

例: 精度、適合率、再現率、F1スコア、ROC曲線、AUC、MSE、MAE、RMSE、R二乗、リストベンチマーク、ペルソナ。

構文:

```
{  
  "type": "ai_AIPackage",  
  "ai_metric": [  
    {  
      "type": "DictionaryEntry",  
      "key": "precision",  
      "value": "0.94"  
    },  
    {  
      "type": "DictionaryEntry",  
      "key": "F1",  
      "value": "0.91"  
    }  
  ]  
}
```

metricDecisionThreshold (任意)

概要: 指標フィールドで説明されている指標の計算に使用されたしきい値を記録します。予測モデルの出力に基づいて意思決定を行うために使用される事前定義されたしきい値です。このしきい値は、モデルの出力スコアまたは確率に適用され、与えられた入力の予測されたクラスやカテゴリを決定します。metricDecisionThresholdの選択はAIシステムのパフォーマンスに重大な影響を与える可能性があります。低いしきい値は偽陽性が多くなる可能性があり、高いしきい値は偽陰性が多くなる可能性があります。そのため、アプリケーションの特定の要件とトレードオフに基づいて適切なしきい値を慎重に選択することが重要です。

タイプ: DictionaryEntry

例: 入力为正か負かに分類されるかを決定するために使用される値。確率スコアがしきい値より大きければ入力は正として分類され、それ以外の場合は負として分類されます。

構文:

```
{
  "type": "ai_AIPackage",
  "ai_metricDecisionThreshold": [
    {
      "type": "DictionaryEntry",
      "key": "precision",
      "value": "0.20"
    }
  ]
}
```

modelDataPreprocessing (任意)

概要: 機械学習モデルに入力データを与える前に実行される操作のセットです。modelDataPreprocessingの目的は、生データをモデルが使用できる適切な形式に変換し、モデルの精度、効率、堅牢性を向上させることです。

タイプ: xsd:string

例: データクレンジング、データ正規化、データ変換、データ分割、データ拡張

構文:

```
{
  "type": "ai_AIPackage", "ai_
modelDataPreprocessing": "lower casing all
text, punctuation marks removed, text shorter
than 10 characters removed, leave-one-out
cross-validation applied"
}
```

modelExplainability (任意)

概要: AIモデルからの結果をどのように説明できるか、その異なる説明メカニズムをリスト化した自由形式のテキストです。このフィールドは、モデルがどのように予測、決定、推奨を行ったか、またその選択がなぜ行われたのかを理解するための洞察を促進します。モデルの説明可能性の目的は、AIシステムをより透明で信頼性が高く、説明責任のあるものにすることです。

タイプ: xsd:string

例: 特徴量の重要度、部分依存プロット、入力特徴量と予測の関係可視化、SHAP (SHapley Additive exPlanations)、LIME (Local Interpretable Model-Agnostic Explanations)、ルールベースの説明。標準化された手法名を使用することが推奨されますが、値に制限はありません。手法がモデルにどのように適用されたかの詳細は、追加で「description」フィールドに記載することができます。

構文:

```
{  
  "type": "ai_AIPackage",  
  "ai_modelExplainability": "feature_important",  
  "description": "The AI package utilizes a random forest model for image classification. Feature importance is calculated using permutation importance to determine the most influential pixels in the images."  
}
```

safetyRiskAssessment (任意)

概要: AIシステムの一般的な安全リスク評価の結果を記録します。

評価は、[EU一般リスク評価方法論](#)に基づいてカテゴリー化されます。この方法論は、規則 (EC) 第765/2008号の第20条を実施し、当局が一般的な製品安全性の遵守を評価する際に役立つことを目的としています。米国FDAもこれらの定義を使用していますが、このカテゴリー化はEU AI法の暫定合意で提案されているものとは異なることに注意が必要です。

タイプ: SafetyRiskAssessmentType (以下のリストから選択: serious、high、medium、low)

例: serious (例: 自動運転車)、high (例: 適応型教育)、medium (例: 銀行ローンの承認)、low (例: ショッピング推奨)。開発者は、EUで販売されるアプリケーションのように、対象となるオーディエンスに応じて安全リスク評価を分類します。

構文:

```
{  
  "type": "ai_AIPackage",  
  "ai_safetyRiskAssessment": "serious"
```

```
}
```

standardCompliance (任意)

概要: AIソフトウェアが準拠している標準を記録します。これには、ISO、IEEE、ETSIなどによって開発された公表済みおよび未公表の標準が含まれます。これらの標準は法的または規制上の要件を満たしている場合もありますが、それが必須であるとは限りません。Core Profile内の「standardName」という別フィールドでは、準拠を取得していないが遵守されている他の標準を記録できます。

タイプ: xsd:string

例: DIN、ETSI、IEC、IEEE、ISO、ITU、JISC、NIST、OASIS、W3Cなどの関連する標準。例: ISO/IEC 5962:2021、ISO/IEC TS 4213:2022、IEEE 7014-2024、FGAI4AD-02。

構文:

```
{  
  "type": "ai_AIPackage",  
  "ai_standardCompliance": "IEEE 7002-2022 Data Privacy Processing"  
}
```

trainingEnergyConsumption (任意)

概要: AIシステムで使用されるAIモデルをトレーニングする際に消費されたエネルギー量を指定します。

タイプ: EnergyConsumptionDescription

例: 深層学習ニューラルネットワークによる画像分類のトレーニング段階で、トレーニングモジュール自体が980 kWh (キロワット時) のエネルギーを消費したと報告されています。

構文:

```
{
  "type": "ai_EnergyConsumption",
  "ai_trainingEnergyConsumption":
  [
    {
      "type": "ai_EnergyConsumptionDescription",
      "ai_energyQuantity": "980",
      "ai_energyUnit": "kilowattHour"
    }
  ]
}
```

typeOfModel (任意)

概要: ソフトウェアで使用されているAIモデルの種類を記録します。

タイプ: xsd:string

例: 教師ありモデル (Supervised model)、教師なしモデル (unsupervised model)、強化学習モデル (reinforcement learning model)、またはそれらの組み合わせ。もしくは、ニューラルネットワーク (neural network)、線形モデル (linear model)、サポートベクターマシン (support vector

machines)、ベイジアンモデル (Bayesian models) など。

構文:

```
{
  "type": "ai_AIPackage",
  "ai_typeOfModel": "reinforcement
learning"
}
```

useSensitivePersonalInformation (任意)

概要: 個人データが、文脈に応じた目的限定の方法で使用される場合を記録します。この際、ユーザーの好み、期待、同意が考慮されます。機微な個人情報は、AIシステムの動作をユーザーのニーズ、好み、文脈に適合させるために使用されることがあります。

タイプ: PresenceType (次のリストから選択: yes、no、noAssertion)

例: 位置データ、健康データ、生体認証データ、行動データなどの機微な個人データが使用される場合、値は「yes」、使用されない場合は「no」。

構文:

```
{
  "type": "ai_AIPackage",
  "ai_useSensitivePersonalInformation": "yes"
}
```

特定のDatasetPackageフィールドの詳細

このセクションでは、Dataset ProfileにおけるDatasetPackageに特有のフィールドについて詳述します。各フィールドには、その説明、タイプ、例、およびJSON-LDシリアル化の例が含まれています。

anonymizationMethodUsed (任意)

概要: データセットまたはデータセット内のフィールドに適用された匿名化手法を記述する自由形式のテキストです。

タイプ: xsd:string

例: 擬似匿名化 (pseudonymization)、k-匿名性 (k-anonymity)、l-多様性 (l-diversity)、t-近接性 (t-closeness)、差分プライバシー (differential privacy)、その他の方法。標準化された手法名を使用することが推奨されますが、値に制限はありません。データセットに適用された方法の詳細や、匿名化関連の前処理手順については、追加で「description」フィールドに記載できます。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_anonymizationMethodUsed":
    "pseudonymization",
  "description": "replace direct identifiers
(such as name or social security number)
with artificial identifiers to prevent the
data from being directly linked back to the
individual"
}
```

confidentialityLevel (任意)

概要: トラフィックライトプロトコル (Traffic Light Protocol) によって定義された異なる機密性レベルを記述します。

タイプ: ConfidentialityLevelType (以下のリストから1つを選択: red、amber、green、clear)

- red: データセット内のデータポイントは非常に機密性が高く、指定された受信者のみと共有可能
- amber: データセット内のデータポイントは特定の組織およびそのクライアントと必要に応じてのみ共有可能
- green: データセットは、同業者やパートナーのコミュニティ内で共有可能
- clear: データセットは制限なく自由に配布可能

例: データセットは、redとしてマークされる場合、機密性の高い財務情報が含まれていることを示します。amberのデータセットには、独自の事業データ、顧客リスト、または競争情報が含まれる可能性があります。greenのデータセットには一般的な事業データが含まれる可能性があります。clearのデータセットには公開されているデータが含まれる可能性があります。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_confidentialityLevel": "clear"
}
```

dataCollectionProcess (任意)

概要: データセットがどのように収集されたか (すべてのソースを含む) を記述します。

タイプ: xsd:string

例: データセットがどのソースからスクレイピングされたか、またはデータ収集に使用されたインタビューのプロトコルなどが含まれます。このフィールドには、データセットが別のデータセットのサブセットである場合や、複数のデータセットを組み合わせで作成された場合についても記録できます。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_dataCollectionProcess":
  "Collected by scraping data from https://
  example.com"
}
```

dataPreprocessing (任意)

概要: 生データに適用されたさまざまな前処理ステップを記述します。

タイプ: xsd:string

例: 標準化、正規化、重複排除、トークン化、データがAIモデルに入力される前に適用されるデータクリーニング、正規化、特徴量抽出などの前処理ステップが含まれます。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_dataPreprocessing": "z-score
  standardization",
  "description": "each data point is re-
  scaled based on the mean and standard
  deviation of the dataset."
}
```

datasetAvailability (任意)

概要: 一部のデータセットは公開されており、直接ダウンロードできますが、他のデータセットはクリック同意後や登録フォームの記入後にアクセス可能です。このフィールドでは、データセットの利用可能性をその視点から記述します。

タイプ: DatasetAvailabilityType (以下から1つ選択: clickthrough、directDownload、query、registration、scrapingScript)

- clickthrough: データセットは公開されておらず、クリック同意ページで利用規約に同意した後のみアクセス可能。
- directDownload: データセットは公開されており、直接ダウンロード可能。
- query: データセットは公開されているが、一度にすべてのデータを取得することはできず、クエリを通じて一部のデータを取得可能。
- registration: データセットは公開されておらず、利用者はメール登録を行うことでアクセス可能。ただし、利用規約への同意は必要ない。
- scrapingScript: データ提供者は元のデータを公開していないが、提供されたスクレイピング スクリプトを使用してデータセットを再構成する必要がある。

例: クリック同意タイプの例として、OpenStreetMap (OSM) が挙げられます。OSMは、世界中の地図を自由に編集できる共同プロジェクトであり、道路、建物、観光名所などの地理的な特徴が含まれています。データをダウンロードするには、ユーザーがOSMのウェブサイトにアクセスして利用規約に同意する必要があります。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_datasetAvailability": "
  clickthrough"
}
```

datasetNoise (任意)

概要: データセットが含む可能性のあるノイズの種類を記述します。

タイプ: xsd:string

例: 一貫性のないデータは、均一で標準化されていないデータを指します。欠損データは、データセットに存在しないデータポイントを指します。関連性のないデータは、AIモデルが解決しようとする問題に対して関連性がないデータを指し、人為的なエラーもデータセットにノイズを導入することがあります。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_datasetNoise": "Human error.
  Since manually entered into the system,
  errors such as typos or incorrect data
  entry can occur."
}
```

datasetSize (任意)

概要: データセットのサイズをバイト単位で記録します。サイズはバイトで測定されるべきです。

タイプ: xsd:nonNegativeInteger

例: データセットのサイズは様々であり、このフィールドは実際のバイト数を記録します。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_datasetSize": 2689
}
```

datasetType (必須)

概要: データセットに含まれるデータタイプを指定します。データセットには複数のデータタイプが含まれている場合があります。

タイプ: DatasetType (以下のリストから選択: audio、categorical、graph、image、noAssertion、numeric、other、sensor、structured、syntactic、text、timeseries、timestamp、video)

例: 「structured」は、表形式で整理されたデータや、リレーショナルデータベースから取得されたデータを指します。「timestamp」は、各エントリにタイムスタンプが含まれているデータを指しますが、特定の順序で記録されていたり、特定の間隔で記録されたりすることを保証するわけではありません。「noAssertion」は、データタイプを特定できない場合に使用します。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_datasetType":
  [
    "structured",
    "timestamp"
  ]
}
```

datasetUpdateMechanism (任意)

概要: データセットを更新するメカニズムを記述する自由形式のテキストです。

タイプ: xsd:string

例: 「Batch」、「real-time」(株価などのリアルタイムで更新されるデータ)、「incremental」(ソーシャルメディアデータやニュース記事など、段階的に更新されるデータ)、「manual」(人間の判断が必要なデータで、検証のために手動で更新されるもの)。

構文:

```
{  
  "type": "dataset_DatasetPackage",  
  "dataset_datasetUpdateMechanism":  
    "Batch. Updated annually."  
}
```

hasSensitivePersonalInformation (任意)

概要: 個人の識別情報に関する結論を導き出すことを可能にするセンシティブな個人データまたは情報の有無を示します。

タイプ: PresenceType (以下のリストから1つ選択: yes、no、noAssertion)

例: 「yes」は、バイオメトリクスデータや個人の人種、民族に関する情報のようなセンシティブな個人情報が使用されていることを示します。「no」は、トレーニング、テスト、またはプロダクションでセンシティブな個人情報が使用されていないことを示します。

構文:

```
{  
  "type": "dataset_DatasetPackage",  
  "dataset_hasSensitivePersonalInformation":  
    "no"  
}
```

intendedUse (任意)

概要: 与えられたデータセットの使用目的について説明する自由形式のテキストです。データセットが意図された目的以外で使用されると、脆弱性や法的問題を引き起こす可能性があります。

タイプ: xsd:string

例: もしデータセットが研究目的で収集された場合、それを商業目的で使用することは知的財産権やその他の法的契約を侵害する可能性があります。また、特定の人口統計から収集された医療データは、その人口統計向けに機械学習モデルをトレーニング

する目的にのみ適用される場合があります。このような場合、intendedUseフィールドはその情報を捕捉します。

構文:

```
{  
  "type": "dataset_DatasetPackage",  
  "dataset_intendedUse": "To make the  
  research about greenhouse gas emissions  
  accessible."  
}
```

knownBias (任意)

概要: データセットに含まれるさまざまなバイアスについて説明する自由形式のテキストです。

タイプ: xsd:string

例: i) 選択バイアス: 収集されたデータが研究されている集団を代表していない場合に発生します。

ii) 測定バイアス: たとえば、調査質問が回答に影響を与えるように表現されている場合や、特定のグループに対して測定が他のグループよりも正確である場合。

iii) ラベルバイアス: データを分類するために使用されるラベルにバイアスがある場合、たとえば、特定のラベルが特定のグループにより頻繁に適用される場合です。

構文:

```
{  
  "type": "dataset_DatasetPackage",  
  "dataset_knownBias": "Data in some  
  geographical areas are more complete  
  than the others."  
}
```

sensor (任意)

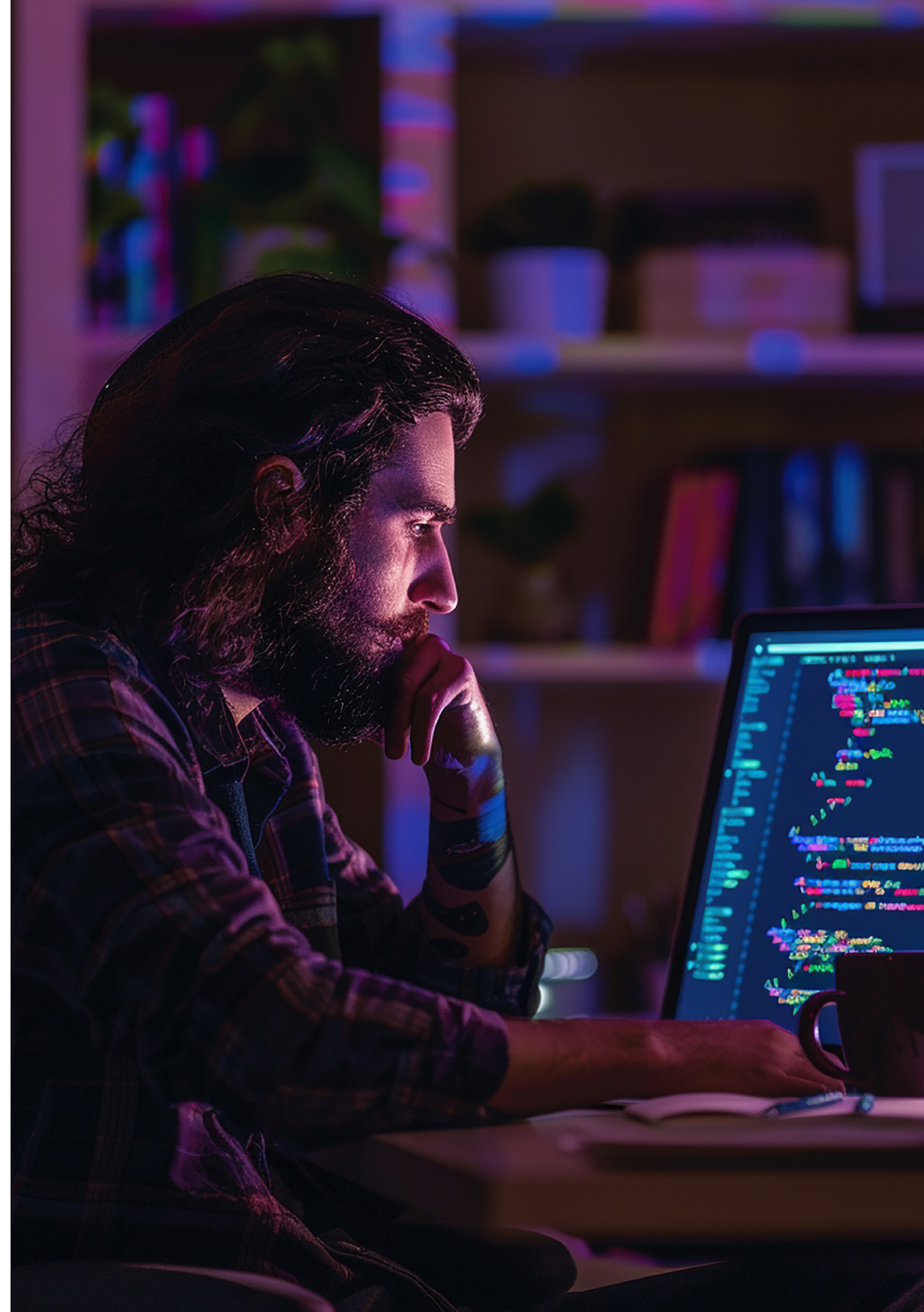
概要: データ収集に使用されたセンサーとそのキャリブレーション値について説明します。値はキーと値の形式で保存されます。

タイプ: DictionaryEntry

例: キーにはカメラ、ライダー、レーダー、マイクロフォン、温度、圧力、接近センサー、生体認証センサーなど、関連するタイプが含まれます。値は標準化されたモデルおよびメーカーコードが推奨されますが、使用するキーや値に関する制限はありません。

構文:

```
{
  "type": "dataset_DatasetPackage",
  "dataset_sensor":
  [
    {
      "type": "DictionaryEntry",
      "key": "lidar",
      "value": "Acme A-5.2M"
    },
    {
      "type": "DictionaryEntry",
      "key": "lidar-calibration-
distance-offset",
      "value": "0.05"
    }
  ]
}
```



現実世界のエビデンスの例

以下は、異なるタイプのAIシステムとそれに対応するSPDX 3.0ファイルのいくつかの例です。将来的に追加される例も含めた包括的な例のコレクションは、次のリンクで確認できます: <https://github.com/spdx/spdx-examples>.

手書き文字認識アプリケーション (SimpleHTR)

AI BOMの複雑さは、いくつかの理由で中程度に複雑なAIシステムでも大幅に増加する可能性があります。第一に、AIシステムはしばしば多数の依存関係を持っており、特にTensorFlowのような人気のあるオープンソースのフレームワークを利用する場合に顕著です。第二に、AIモデルの複雑さが増すにつれて、例えばOpenAIのGPT-4のようなモデルを使用する場合、表現がますます冗長になり、読者が追うのが難しくなります。高度に複雑なシステムのAI BOMを作成することは完全に可能ですが、そのような例を使用すると可読性と理解性に影響を与えるため、目的を達成できなくなります。

実世界のAI BOMの簡単でありながら非自明な例を提供するために、依存関係が管理可能な公開されているオープンソースAIシステムを選択することにしました。高い品質を確保するために、GitHubで1,000以上のスターを持つプロジェクトに限定して検討しました。論文の著者たちによる綿密な分析と議論を経て、デモンストレーションの目的でSimpleHTRプロジェクトを選択しました。

SimpleHTR Overview

SimpleHTRはHarald Scheidlによって開発された手書き文字認識システムです。TensorFlowを使用して実装され、IAM手書き文字認識データセットでトレーニングされています。このシステムのAIモデルは、単一の手書き単語や複数行の手書き単語の画像を処理し、認識されたテキストを出力します。行レベルおよび単語レベルのモデルは、5つのCNN層と2つのRNN (LSTM) 層からなるニューラル ネットワーク ベースで、コネクショニスト テンポラル ロスおよびデコード方式を使用しています。

SimpleHTRは、モデルのトレーニング、データの読み込み、およびデータ前処理のためのソースコードを提供しており、これらの機能を実現するためにさまざまなオープンソースのパッケージを使用しています。モデル、データセットの前処理、および推論プロセスに関する詳細な情報については、[開発者のブログ記事](#) [t]を参照してください。

SimpleHTRのAIプロファイルを含むSPDXシステムBOM

SimpleHTRのAI BOMは、AIモデル、トレーニングに使用されるデータセット、これらの機能をサポートするパッケージ、それらの依存関係、およびこれらのパッケージのライセンス情報に関するすべての関連情報を記録します。また、AI BOMドキュメント自体の来歴に関する情報も含まれています。

例えば、SimpleHTRの単語モデルに関する情報はAIPackage内に記録され、IAM Handwriting Databaseに関する情報はDatasetPackage内に記録されます。relationshipType: “trainedOn”のRelationshipインスタンスは、これら2つのパッケージ間に意味的なリンクを定義します。

```
AIPackage(name="word-model")
```

```
    trainedOn DatasetPackage(name="IAMdataset")
```

完全なAI BOMは、[公式の例のリポジトリ](#) で利用可能です。AI BOMの作成に関する詳細なマニュアルは本論文の範囲を超えていますが、そのようなチュートリアルを近い将来公開する予定です。

CO2データセット

実際のデータセットBOMの例を示すために、Our World in Dataから「CO2および温室効果ガス排出データセット (CO2データセット)」を選択しました。この選択は、データセットの構造のシンプルさと、そのドメインが一般の人々にとってアクセスしやすいことの2つの重要な要因によるものです (ニュースメディアは長年にわたり温室効果ガス排出に関する報道を行っています)。CO2データセット全体は、2つのファイル (データとコードブック) から構成されており、<https://github.com/owid/co2-data/> で無料で利用できます。

そのシンプルな構造にもかかわらず、データセットの基になるデータはさまざまなソースから取得されており、ライセンスの違いなどの複雑さを引き起こす可能性があります。本書では、特定のフィールドと関係に焦点を当てます。完全なデータセットBOMは、<https://github.com/spdx/spdx-examples/tree/master/dataset/example01> で確認できます。

このデータセットは、2つのプレーンテキストファイルから構成されています: data.csvとcodebook.csvの両方がCSV (カンマ区切り値) 形式です。data.csvには、国別の年次排出データが含まれており、80列がヘッダーで定義されています。データのほとんどは数値 (例: 人口、GDP、CO2排出量) であり、一部はカテゴリカルデータ (例: 国名) です。codebook.csvは、data.csvの各列の詳細 (説明、単位、データソース) を記載しています。

BOMでは、data.csvとcodebook.csvは、primaryPurpose: “data”およびcontentType: “text/csv;charset=UTF-8”としてファイルインスタンスとして定義されています。また、relationshipType: “describes”のRelationshipインスタンスがこれら2つのファイル間に意味的なリンクを定義しています。

```
codebook.csv describes data.csv
```

BOMのrootElementはDatasetPackageインスタンスです。relationshipType: “contains”のリレーションシップが、data.csvおよびcodebook.csvのファイルをDatasetPackageインスタンスにリンクするために使用されています。

```
DatasetPackage1 contains [data.csv, codebook.csv]
```

relationshipType: “hasDeclaredLicense”のリレーションシップインスタンスは、データセットパッケージのライセンスを記述するために使用されます。

```
DatasetPackage1 hasDeclaredLicense CC-BY-4.0
```

DatasetPackageクラスには、データセットの特性を記述するためのいくつかのプロパティがあります。例えば、hasSensitivePersonalInformationは「no」に設定され、knownBiasは「一部の地理的地域のデータが他の地域よりも完全である」といった文字列に設定されています。



今後の方向性

現在、システムはますます多くのトレーニングされたAI/MLモデルを製品に組み込んでいます。これらのプロファイルは、リスクを評価できるようにシステム分析に組み込むことができる形で関連するメタデータをキャプチャするための出発点です。しかし、安全が重要なアプリケーションでは、他の「成分」も効果的なナレッジグラフにリンクされる必要があり、これにより分析を適用することができます。

SPDXの進化は、より広範なコンポーネントを網羅することでシステム分析とリスク評価を変革する準備が整っています。共通の要素およびアーティファクトクラスを特徴とする確立されたSPDX基盤モデルを活用し、この取り組みは、ハードウェア、サービス、テスト、振る舞い分析、運用のための追加のプロファイルを導入する準備をしています。この包括的な戦略は、ソフトウェア、ハードウェア、モデル、サービス間の複雑なリンクを促進し、システムの安全分析を強化するとともに、システムの振る舞いや文脈についての精緻な理解を可能にします。

さらに、運用および脅威/損害に関するプロファイルの開発は、SPDXツールキットを強化し、複雑なシステムにおけるリスク評価と軽減の能力を向上させます。今後、SPDXはISOおよびIEEEの標準とのさらなる整合性を目指し、世界中の政府法令に対するコンプライアンスを検証することで、慎重な文書化を通じて透明性と説明責任を確保することを目指しています。

この戦略的方向性は、AI/ML統合システムの信頼性と安全性を強化するだけでなく、業界全体および他の文書化されたリスクシナリオにおけるより包括的で効果的なリスク管理の実践への道を切り開くこととなります。



選定された標準および参考文献

[a] The System Package Data Exchange® (SPDX®) Specification Version 3.0 - <https://spdx.dev/use/specifications/>

[b] [IEEE 7000-2021 Model Process for Addressing Ethical Concerns during System Design](#) は、システム設計時に倫理的懸念を特定し対処するためのモデルプロセスを提供するベストプラクティス標準です。文書化すべき情報には、システムの制限、AIシステムに関する一般的な情報、関連するステークホルダー/意図された使用法、バイアス因子の特定、説明責任、実行時モニタリング、および説明可能性が含まれます。

[c] [IEEE 7001-20210 Transparency of Autonomous Systems](#) は、透明なAIシステムを開発するためのガイドラインを提供するベストプラクティス標準です。コンプライアンスのために文書化すべき情報には、アプリケーション、制限、意図された使用法、使用データ、採用されたアルゴリズムおよび特定の決定の根拠、システムの出力と行動の説明（関連するステークホルダーに理解できる方法で）などが含まれます。さらに、メトリクス（精度）、バイアス/公正性、アプリケーションのガバナンス、責任者、システムのセキュリティおよびプライバシー対策（潜在的な脆弱性やリスクを含む）も文書化する必要があります。

[d] [IEEE 7002-2022 Data Privacy Processing](#) は、自治およびインテリジェントシステムの設計におけるバイアスに対処するためのガイドラインを提供するベストプラクティス標準です。文書化すべき情報には、システム内のデータ、アルゴリズム、および人間の意思決定を含む潜在的なバイアスの源を特定すること、バイアスがシステムのパフォーマンス、公平性、安全性に与える潜在的な影響、識別されたバイアスの源を軽減または排除する方法、バイアスに関する懸念を関連するステークホルダーに説明することが含まれます。

[e] [IEEE 7005-2021 Transparent Employer Data Governance](#) は、自治およびインテリジェントシステム (A/IS) の設計における倫理的懸念を特定し対処するためのプロセスモデルを提供するベストプラクティス標準です。文書化すべき情報には、すべての関連するステークホルダー（セクション6.2.1）、プライバシー、公平性、透明性、説明責任に関連する問題など、A/ISに関連する倫理的懸念が含まれます。

[f] [IEEE 7007-2021 Ethically Driven Robotics and Automation Systems](#) は、ロボティクスおよびオートメーションシステムの設計、開発、展開における倫理的懸念を特定し対処するために使用できるオントロジーモデルの開発に関するガイダンスを提供するベストプラクティス標準です。文書化すべき詳細には、ロボティクスおよびオートメーションシステム (RAS) によって影響を受ける可能性があるすべての関連ステークホルダー（直接的および間接的なユーザー、そしてその運用によって影響を受ける可能性がある者）を特定することが含まれます。

[g] [IEEE 7010-2020 - Impact of Autonomous and Intelligent Systems on Human Well-Being](#) は、ベストプラクティス標準です。評価には、人間の福祉に対するリスクを軽減するための戦略を記録し、懸念に対処するための保護措置や政策、手続きの策定が含まれます。また、影響および軽減戦略を評価し、その効果を評価した上で、必要に応じて調整を行うことが求められます。

[h] [IEEE 7014-Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems](#) は、共感的なA/ISの設計に関するさまざまな考慮事項をカバーする標準であり、ユーザー体験、アクセシビリティ、フィードバックメカニズム、データプライバシーなどが含まれます。また、共感的A/ISに関連する潜在的な倫理的リスクを特定するためのリスク評価の実施、およびそれらのリスクを軽減するための戦略の開発に関するガイダンスも提供しています。

[i] [IEEE 7009-2024 - IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems](#) は、自治および半自治システムのフェイルセーフ設計のための包括的なフレームワークを提供する標準です。この標準は、潜在的な故障モードに対処し、リスクを軽減するための戦略を実施することで、これらのシステムの安全性、信頼性、および堅牢性を確保することを目的としています。標準は、システムアーキテクチャ、障害検出および回復メカニズム、安全保証プロセスなど、フェイルセーフ設計のさまざまな側面をカバーしています。

[j] [ISO/IEC 5962:2021 Information technology SPDX® Specification V2.2.1](#) は、ソフトウェアコンポーネントおよびその関係に関する情報をサプライチェーン内で伝達するためのフォーマットです。この標準は、ソフトウェアコンポーネントのライセンス、著作権、セキュリティ脆弱性、その他のメタデータを含む、ソフトウェアコンポーネントを記述するための共通の言語と構造を提供します。また、組織や個人間でソフトウェアコンポーネントの情報交換を円滑にするために使用できるSPDX文書を作成・共有するためのベストプラクティスも定義しています。

[k] [ISO/IEC FDIS 5338 Information technology – AI – AI system life cycle processes](#) は、人工知能 (AI) システムのライフサイクルプロセスに焦点を当てています。これは、AIシステムの設計、開発、展開、運用、保守、および廃止に関するフレームワークを提供し、安全、効果的、倫理的なAIの使用を促進することを目指しています。AIシステムの要求事項：開発者は、AIシステムの機能的、性能的、安全性に関する要求事項に加えて、倫理的および社会的考慮事項を文書化する必要があります。文書化された評価には、使用されたアーキテクチャ、アルゴリズム、およびデータが含まれます。文書にはまた、AIシステムが透明性、説明可能性、公平性、堅牢性などの倫理的および社会的考慮事項にどのように対応しているかについての情報が含まれているべきです。さらに、AIシステムがどのようにテストされたか、およびその結果や指標に関する情報も含まれるべきです。開発者は、AIシステムの展開および運用に関する情報を文書化し、システムがどのように監視、保守、および更新されるかについても記録する必要があります。AIシステムの廃止については、AIシステムライフサイクル中に実施されたリスク評価を文書化する必要があり、倫理的および社会的リスクの評価を含みます。リスクがどのように識別され、評価され、軽減されたかに関する情報も含まれるべきです。AIシステムの設計および開発における説明責任および責任のメカニズムについても文書化する必要があり、明確な責任の分担、設計決定の文書化、および倫理的および社会的懸念への対応プロセスが含まれるべきです。また、AIシステムの継続的な改善のためのプロセス（倫理的および社会的考慮事項の継続的な監視と評価を含む）およびフィードバックと学習のメカニズム、規制の遵守に関するプロセスも記録する必要があります。

[l] [ISO 13475 - Medical](#) は、医療機器業界に特化した品質管理システムの要求事項を定めた国際的に合意された標準です。この標準は、医療機器の設計、製造、設置、納品に関わる組織が、顧客および規制要件を一貫して満たす医療機器および関連サービスを提供する能力を示すためのフレームワークを提供します。標準の主要な特徴は次のとおりです。規制遵守：医療機器がFDA、欧州連合、その他の世界的な当局によって設定された規制要件を満たすことを保証します。リスク管理活動を製品実現中に組み込み、医療機器の安全性と有効性を確保します。医療機器に関連するリスクを特定、分析、評価、管理、監視するための支援を行います。組織が包括的な文書を保持することを要求し、品質マニュアル、文書化された手順、および記録を含みます。トレーサビリティを確保し、遵守と有効性の証拠を提供します。QMS（品質管理システム）が定期的にレビューおよび更新され、その有効性を維持することを保証します。また、データの分析と意思決定のためにSPDXを使用することは、良い解決策となります。ISO 13485:2016は医療機器業界にとって重要な標準であり、安全性、有効性、および規制遵守を保証する品質管理のための堅牢なフレームワークを提供します。ISO 13485の要求事項に従うことにより、組織は評判を高め、顧客満足度を向上させ、世界市場へのアクセスを得ることができます。

[m] [Code of Federal Regulations \(CFR\) Part 814 – Premarket Approval of Medical Devices](#) は、医療機器が市場に出る前にその安全性と有効性を確保するための重要な規制です。これらの要求事項を遵守することにより、製造業者は自社の機器がFDAの厳格な基準を満たしていることを示し、公共の健康を守るとともに、市場へのアクセスを促進することができます。

[n] [FDA Rules and Regulations](#) - 米国FDAの規則および規制は、製品が高い品質、安全性、および有効性基準を満たしていることを確保することによって、公共の健康と安全を維持するために不可欠です。包括的なガイダンスを提供し、検査を実施し、遵守を強制することにより、FDAは消費者を保護し、医療および食品業界での革新を促進する重要な役割を果たしています。FDAのウェブサイトは、これらの規制を理解し遵守するための豊富なリソースを提供しており、業界の専門家、研究者、および一般の人々にとって貴重なツールとなっています。SPDXは、製品およびAIインベントリの管理ツールとして推奨されています。

[o] Data, Analytics, and Artificial Intelligence Adoption Strategy. US Department of Defense. https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

[p] Mitchell, Margaret, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, and Timnit Gebru. “Model cards for model reporting.” In Proceedings of the conference on fairness,

accountability, and transparency, pp. 220-229. 2019.

[q] Arnold, Matthew, Rachel KE Bellamy, Michael Hind, Stephanie Houde, Sameep Mehta, Aleksandra Mojsilovič, Ravi Nair et al. “FactSheets: Increasing trust in AI services through supplier’s declarations of conformity.” IBM Journal of Research and Development 63, no. 4/5 (2019): 6-1.

[r] Gebru, Timnit, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé Iii, and Kate Crawford. “Datasheets for datasets.” Communications of the ACM 64, no. 12 (2021): 86-92.

[s] Hugging Face Model Card Template https://github.com/huggingface/huggingface_hub/blob/v0.24.6/src/huggingface_hub/templates/modelcard_template.md

[t] Build a Handwritten Text Recognition System using TensorFlow <https://towardsdatascience.com/build-a-handwritten-text-recognition-system-using-tensorflow-2326a3487cd5>

[u] IBM Face Sheet Introduction <https://aifs360.res.ibm.com/introduction>





謝辞

著者は、[AI & Dataset Profileワーキンググループ](#)のメンバーに対し、建設的な意見と有用なAI BOMフィールドを作成するための支援に感謝の意を表します。また、著者は、本論文のドラフトに対するコメントをいただいた以下のレビューアーにも感謝の意を表します。

- Alexios Zavras
- Gary O’Neill
- Matt White
- Michael Dolan
- Robert Martin
- Victor Liu
- Ibrahim Haddad
- Scott Bennet
- Michael Hind
- Steve Winslow

本訳文について

この日本語文書は、[Implementing AI Bill of Materials \(AI BOM\) with SPDX 3.0](#)の参考訳として、The Linux Foundation Japanが便宜上提供するものです。英語版と翻訳版の間で齟齬または矛盾がある場合（翻訳版の提供の遅滞による場合を含むがこれに限らない）、英語版が優先されます。

翻訳協力：小笠原徳彦

著者について

Karen Bennet

Karenは、オープンソースとクローズドソースの両方のソリューションにおいて、30年以上のソフトウェア開発の経験を持つシニア エンジニアリング リーダーです。彼女は、自動運転車、ヘルスケア、金融、ロボティクス、リテール推奨業界において、大規模なAIプラットフォームの展開に成功しています。以前はRed Hat、IBM、Yahoo、および複数のスタートアップで、AIプラットフォーム/ツール分野のシニア エンジニアリング リーダーとして活躍していました。KarenはAI分野の専門家として、ISO、IEEE、Linux Foundation、NIST、CISA、EU AI Act、Canada AI Actに関与しており、AI & Dataset Profileの共同リーダーを務めています。彼女はAI分野で14件の特許を保有しており、AIに関連するさまざまな技術的問題に関する技術論文を発表しています。

Gopi Krishnan Rajbahadur

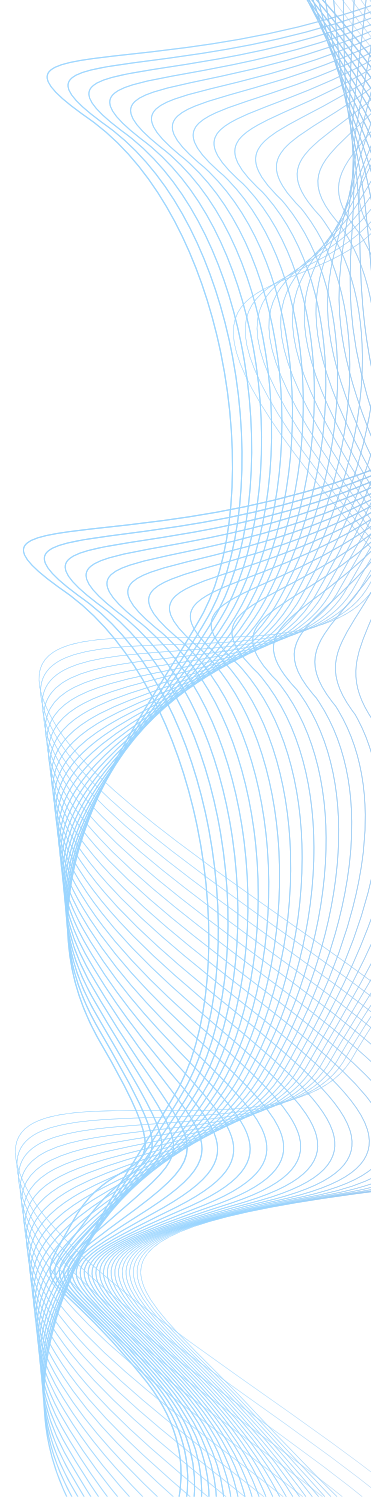
Gopi Krishnan Rajbahadurは、カナダのHuaweiのソフトウェア エクセレンス センターでシニア スタッフ リサーチャーを務めています。現在、Large Language Modelsのソフトウェア エンジニアリングとAIデータセットのガバナンスに取り組んでおり、研究分野にはAIのためのSE、SEのためのAI利用、規制可能なAIソフトウェアの開発が含まれます。また、ISO SPDX標準でAI & Dataset Profileの共同リーダーとして、SEおよびAIの標準分野にも積極的に貢献しています。さらに、オープンソースイニシアティブ「OpenDataology」の共同設立者であり、Open Source Summitで頻繁に発表しています。彼の研究は、TSE、TOSEM、EMSE、ICSEなどの著名なSEの出版物に取り上げられています。

Arthit Suriyawongkul

Arthit Suriyawongkulは、ダブリンのトリニティ カレッジで、Science Foundation Ireland Research CentreのAI駆動型デジタルコンテンツ技術 (ADAPT) とデジタル強化現実のSFI研究センターの博士研究者です。彼のシステム アカウンタビリティ オントロジー研究は、ソフトウェア エンジニアリングの標準と法的枠組み、特にEU AI Actとの交差点に焦点を当て、責任あるAI開発の促進を目指しています。ArthitはISOのSPDX標準への提出に積極的に貢献しており、学術的な活動に加えて、タイ ネットワーク (民権団体) の共同設立者としても活動しています。

Kate Stewart


Kate Stewartは、Linux FoundationでDependable Embedded SystemsのVPを務めています。ソフトウェア業界で30年以上の経験があり、カナダ、オーストラリア、アメリカで開発者として働き、過去20年間は世界中のオープンソース ソフトウェア開発チームと共に活動しています。KateはSPDXの創設者の一人で、現在はこのプロジェクトの技術的リーダーの一人です。また、NTIA SBOM formats and toolingワーキンググループの共同リーダーであり、CISA SBOM tooling and implementationワーキンググループの共同リーダーも務めています。現在は、組み込み市場で使用されるオープンソース プロジェクトが、安全性、セキュリティ、ライセンス遵守のベスト プラクティスを採用する手助けを行っています。2015年にLinux Foundationに参加して以来、Real Time Linux、Zephyr、ELISAプロジェクトなどを立ち上げました。







Linux Foundation Researchについて


2021年に設立された **Linux Foundation Research** は、拡大するオープンソースコラボレーションを調査し、新たな技術トレンド、ベストプラクティス、オープンソースプロジェクトのグローバルな影響に関する洞察を提供しています。プロジェクトのデータベースやネットワークを活用し、定量的・定性的手法のベストプラクティスに取り組むことで、Linux Foundation Research は、世界中の組織にとって有益なオープンソースの知見を提供するライブラリを構築しています。

 x.com/linuxfoundation

 youtube.com/user/TheLinuxFoundation

 facebook.com/TheLinuxFoundation

 GITHUB.COM/LF-ENGINEERING

 linkedin.com/company/the-linux-foundation



Copyright © 2024 [The Linux Foundation](#)

本レポートは [Creative Commons Attribution-NoDerivatives 4.0 International Public License](#) のもとでライセンスされています。

この著作物を参照する際には、以下のように引用してください: Karen Bennet, Gopi Krishnan Rajbahadur, Arthit Suriyawongkul, and Kate Stewart, “Implementing AI Bill of Materials (AI BOM) with SPDX 3.0: A Comprehensive Guide to Creating AI and Dataset Bill of Materials,” The Linux Foundation, October 2024.