AI事業者ガイドライン案に関する
BSA| The Software Allianceからの意見

2024年2月19日

総論

BSA｜The Software Alliance[1]（BSA | ザ・ソフトウェア・アライアンス、以下、BSA）は、AI事業者ガイドライン案に（以下、ガイドライン案）に関し、総務省および経済産業省（以下、経産省）に意見を提出する機会[2]が得られたことに感謝します。我々は、総務省および経産省がAI事業者が責任をもってAIを開発・導入・利用することを支援するために、ガイドライン案をとりまとめたことを高く評価しています。ガイドライン案[3]においては、AIに関連するリスクを最小化するために適切な安全対策を講じながらも、イノベーションとAIの活用を促進するための産業界の自主的な取り組みを支援するリスクベースの、ライフサイクルアプローチの考えが採用されており、我々はこれを支持します。BSAとBSAの会員企業は、日本政府に協力し、この取り組みを支援していきたいと考えています。

BSA は、世界のソフトウェア産業を代表する主唱者です。BSA の会員企業は、AI を含む最先端のサービスを開発する最前線におり、その製品は経済のあらゆる分野でビジネスに利用されています。[4] 例えば、BSA 会員は、クラウド・ストレージやデータ処理サービス、顧客関係管理（CRM）ソフトウェア、人事管理プログラム、ID 管理サービス、サイバーセキュリティ・サービス、コラボレーション・ソフトウェアなど

---

[1] BSAの活動には、Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2]「AI事業者ガイドライン案」に関する意見募集　（2024年1月）：
https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=145210224&Mode=0

[3]「AI事業者ガイドライン案」本文　（2024年1月）
https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000267013
「AI事業者ガイドライン案」別添
https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000267014

[4]「Artificial Intelligence in Every Sector（あらゆる分野における人口知能（AI））」2022年6月13日
https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf　（英文）

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

のツールを提供しています。そのため、デジタルトランスフォーメーション（DX）を促進するテクノロジーの大きな可能性や、AI の責任ある利用を最適にサポートする政策について、独自の見識を持っています。BSA の見解は、会員企業と協力し「バイアスに挑む： AI の信頼性構築に向けた BSA のフレームワーク」（以下、BSA フレームワーク）[5]をまとめた経験に基づいています。このフレームワークは、二年以上前に BSA が発表したリスク管理フレームワークで、AI システムにおける意図しないバイアスの可能性を事業者が軽減するのに役立つものです。膨大な調査に基づき、主要な AI 開発事業者の経験に基づく BSA フレームワークは、影響評価を実施するためのライフサイクルベースのアプローチを概説し、それに対応するベストプラクティスを紹介しています。

以下の提言は、これらの課題に関する我々の経験と、我々が以前提出した、「新AI事業者ガイドライン スケルトン（案）」に対する提言[6]に基づいています。

国際的な調和

[本編 /はじめに 2 頁 および 文書全体]

世界の政策立案者が AI に対する規制に取り組んでいますが、現在のテクノロジーのエコシステムがグローバルな性質を持っていることから、イノベーションを促進するためには、協調的な政策対応が求められています。広島 AI プロセスで示された、国際的な議論を推進していく日本のリーダーシップを BSA は支持します。各国が多様な関係者との対話を通じて相互運用性を追求し、共通の AI 課題に対応するためのリスクベースの政策アプローチのビジョンを共有すること、また、責任ある AI ガバナンスに関する規範（リスクベースのアプローチ、AI バリューチェーンにおける相応かつ役割に応じた責任分担など）を推進することを我々は奨励します。また、イノベーターが有益なアプリケーションのために、自信を持って柔軟にテクノロジーを導入できるように、国際的なパートナー間で AI に関する共通の用語や分類法についても合意すべきと考えます。このような調和のとれたアプローチをガイドライン案に反映することを推奨します。

定義

[本編 /第 1 部 AI とは / 関連する用語 / 9 頁]

ガイドライン案では、AI システムを 「活用の過程を通じて様々なレベルの自律性をもって動作し学習する機能を有するソフトウエアを要素として含むシステムとする（機械、ロボット、クラウドシステム等）」と定義しています。AI システムが国際的な文脈で開発・導入されることを踏まえると、AI に適用される定義は、AI 技術のさ

[5] 「バイアスに挑む：AIの信頼性構築に向けたBSAのフレームワーク」(BSA Framework to Build Trust in AI) 2021年6月8日
https://ai.bsa.org/wp-content/uploads/2021/07/2021bsaaibiasjp.pdf

[6]「新AI事業者ガイドライン スケルトン（案）に対する BSAからの提言」（2023年10月27日）
https://www.bsa.org/files/policy-filings/jp10272023draftaibusiness.pdf

らなる広範な導入・利用を促進するため、異なる法域を超えて運用可能とすべきです。我々は、日本が OECD の AI の定義[7]を採用することを推奨します。OECD の定義のように、国際的に認知された AI システムの定義を用いることで、日本の政策の国際的な整合性が保たれ、本ガイドラインに関する議論や、その採用、遵守を促進することが可能となります。

AI エコシステムにおける AI 主体間の公平で相応な責任分担

[本編 / はじめに 5 頁 /「第 5 部 AI 利用者に関する事項　35-36 頁）。

AI のバリューチェーンは多様であり、責任を遵守する上で最も適した主体に責任を割り当てることが重要です。このことがガイドライン案において認識されていること、また、スケルトン（案）[8]から AI 主体の分類が狭まったことを我々は歓迎します。

しかし、本ガイドラインはさらに改善できると考えます。各々の分類に該当する AI 主体の事例を示し、また、例えば、カスタマイズ可能である場合は、AI 利用者が AI システムを変更できることに言及するなど、説明を追加することも有用です。これにより、AI のバリューチェーンにおける責任が公平で相応であることを確実にすることができます。

現在の定義と指針では、カスタマイズ可能なAIは考慮されていませんが、これは多くのエンタープライズ企業がAI利用者に提供している製品です。AI開発者は、一般的なカスタマイズ可能なAIツールを頻繁に開発していますが、その本来の目的は低リスクです。これらのツールをどのように利用するかは、AI利用者・顧客次第です。企業間取引（B2B）の文脈では、AIに入力するデータを最終的に管理し、AIの設定方法を指示し、AIシステムがいつ、どのような文脈で利用されるかを決定し、また、出力結果がどう利用されるかという最も重要な判断をするのは、多くの場合、顧客なのです。AIシステムの利用法に関する詳細を提供する最も適した立場にあり、データ入力とその結果としての出力、およびシステムの性能に影響を与えるその他の現実の要因について、より深い洞察を持っているのは、AI利用者です。これを踏まえ、「第5部 AI利用者に関する事項」にカスタマイズ可能なAIに関する記述を含めることを推奨します。

---

[7] 更新されたOECDのAIシステムの定義　2023年11月29日
https://oecd.ai/en/wonk/ai-system-definition-update
「AIシステムは、明示的または暗黙的な目的のために推測するマシーンベースのシステムである。受け取った入力から、物理環境または仮想環境に影響を与える可能性のある予測、コンテンツ、推奨、意思決定等の出力を生成する。AIシステムが異なれば、導入後の自律性と適応性のレベルも異なる」

[8] 「新AI事業者ガイドライン スケルトン（案）」https://www8.cao.go.jp/cstp/ai/ai_senryaku/5kai/gaidorain.pdf

リスクベースアプローチ

[本編 / 第 2 部 / C.共通の指針 3）公平性 15-16 頁、別添 1. B. AI による便益 /リスク/ AI によるリスク 13-17 頁]

BSA は、リスク管理プログラムの実施を奨励しています。ガイドライン案において、AI 事業者がガバナンス・ゴールを設定し、そのゴールを達成するために「AI マネジメントシステム」の設計・運用をすることを推奨していることを我々は支持します。効果的なリスク管理プログラムにおいては、組織が AI リスクを管理するために必要な人員、方針、プロセスを特定します。リスク管理プログラムの構成要素には、役割と責任を明確に割り当てること、正式な方針を確立すること、評価システムを採用すること、経営陣の監督を確実にすること、リスクの高い AI について影響評価を実施すること、また、高いリスクをもたらす AI の課題を判断し対応するために、部門間のガバナンス委員会や倫理委員会等、社内における独立した評価制度を設けることなどが含まれます。組織は、こうした実践をより広範な企業リスク管理プログラムの中に組み込んだり、個別の AI プログラムとして確立することもできます。

個人にとって高いリスクをもたらすユースケースに焦点を当てた、リスクベースアプローチをAIポリシーにおいて採り入れること我々は強く奨めています。このリスクベースのアプローチを 採用するために、ポリシー策定においては、高リスクAIとして特定すべきユースケースを部分的に示し定義すべきと考えます。これには、住宅、雇用、信用、教育、医療、保険などに関し、個人の適格性を判断するAIシステムが含まれます。ガイドライン案の別添の「AIによるリスク」において、リスクの事例が示されていますが、リスクの高い利用と低い利用を明確に区別していません。ガイドライン案に、AIの高リスク利用を構成するものの明確な区別または定義、および高リスクのAIを開発または導入する組織が影響評価を実施し、実施したことを公にすることを記すことを推奨します。

外部監査

[別添 2.「第 2 部 E. AI ガバナンスの構築」関連 / 5. 評価 56-59 頁]

ガイドライン案では、各組織が設定した AI ガバナンス・ゴールの達成に向けて、AI マネジメントシステムが適切に機能しているか否かを評価するために、社内のリソース、もしくは外部監査主体を活用することが提案されています。選択肢の一つとして外部監査が示されていることは理解していますが、以前の我々の意見書で指摘した通り、現時点では AI に関する監査可能な基準が成熟していないため、外部監査の活用には慎重であるべきと考えます。現在、以下のいずれかを企業が実施する上で、既存の手順やベストプラクティスはほぼありません。 (1) AI システムを監査できる信頼できる法人を選ぶ (2) そのような監査法人がどのような基準を適用すべきかを決定する。ISO はいくつかの AI 関連規格を発行していますが、多くの規格はまだ開発中です。また、現在、AI システムに対応する十分な自主的コンセンサスに基づく規格が不

足しています。共通の基準がなければ、監査の質は大きく異なります。監査によって異なるベンチマークで測られる可能性があり、客観的なベンチマークに基づく評価を得るという目標が損なわれます。

また、BSA は透明性を促進する必要性を理解していますが、機密情報や専有情報を含む監査結果を事業者に公表することを求めないことを推奨します。公表することは、AI システムの厳格な評価を受ける意欲を企業に失わせることになります。このような理由から、外部監査は AI ガバナンスを達成するための適切な解決策ではなく、このような提案をガイドライン案から削除することを奨めます。

高度な AI システムに関係する事業者に共通の指針と高度な AI システムを開発する組織向けの行動規範

[本編 / 第 2 部 / D. 高度な AI システムに関係する事業者に共通の指針 23-25 頁 /「高度な AI システムを開発する組織向けの広島プロセス国際行動規範」における追加的な記載事項 30-31 頁]

ガイドライン案では、広島AIプロセスで策定された全ての AI 関係者向け[9] 及び高度な AI システムを開発する組織向けの国際指針[10]、また、高度な AI システムを開発する組織向けの国際行動規範[11]を参照しています。我々は、安全・安心・信頼できるAIを促進することを目的とした指針と行動規範の目的を支持していますが、その内容は、以下に記すように、さらに改善できると考えております。

指針と行動規範の適用範囲の明確化

我々は指針と行動規範の適用範囲を明確にすることを推奨します。ガイドライン案は、「高度なAIシステム」に適用されるとしていますが、「高度なAIシステム」の定義が記されていません。我々は、ガイドライン案を修正し、「高度なAIシステム」が、危害のリスクが高い最も能力の高いモデルのみを包含することを明確にし、この用語を説明することを奨めます。これにより、低リスクの場面で利用される可能性のあるAIシステムを対象とした責任を課すことが避けられ、代わりに個人に最も大きな影響を及ぼす領域にリソースを集中させることが可能となります。「高度なAIシステム」という用語も一貫して使用されるべきです。例えば、II)においては、明確に高度なAIシステムに焦点を当てずに、より広範にAIシステムに言及しています。

I) AIライフサイクル全体にわたるリスクを特定、評価、軽減するための措置

*第一に、本項では、内部テストの利用を促進し、外部テストを常に実施すべきと示唆することは避けるべきです。*本項では、AIのライフサイクル全体を通じてのリスクの

[9] 全ての AI 関係者向けの広島プロセス国際指針
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document03.pdf
[10] 高度な AI システムを開発する組織向けの広島プロセス国際指針
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document04.pdf
[11] 高度な AI システムを開発する組織向けの広島プロセス国際行動規範
https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document05.pdf

特定と軽減を取り上げ、組織が実施すべき措置として、内部テストと独立した外部テストの両方を記述しています。我々は、テストがリスクを特定する上で重要であることに同意しますが、組織が常に外部テストを実施すべきと示唆することは避けるべきと考えます。組織が外部テストを実施することを選択する状況もあります。しかし、外部テストでは企業秘密、ネットワークや情報のセキュリティを脅かす可能性のある情報、また、その他の専有情報を共有することへの懸念が生じます。内部テスト（AIシステムの開発担当チームからは独立した従業員のチームにより実施可能）により、このような懸念を生じさせることなく、リスクを特定し、軽減することが可能となります。このことから、本項では内部テストに焦点を絞り、独立した外部テストへの言及を削除することを推奨します。

*第二に、本項は、AIシステムの開発者やAIシステムの導入者など、AIバリューチェーンにおける様々な役割を反映するよう更新されるべきです。*開発者、導入者その他のバリューチェーン内の関係者は、それぞれ異なる種類の情報にアクセスすることができ、リスクを軽減するために異なる行動をとることができます。I)の現行の記述は、AIシステムが他の組織によって取得され、導入された後であっても、AIシステムの開発者が、そのAIシステムに関連するリスクを特定し、評価し、軽減することができると想定しているように読めます。多くの場合は、そうではありません。上述したように、AIに関わるすべての主体がAIライフサイクル全段階において作成されたすべての情報にアクセスできるとみなすのではなく、I)では、ライフサイクルにおける役割に基づいて、異なる組織によるリスクの特定、評価、軽減を奨励すべきです。AIのバリューチェーンにおける、その組織の知識、統制力、及び立場に基づき、特定のリスクに対処可能な、最も適切な役割に、関連する責任と説明責任は割り当てられるべきです。

II) 導入後の脆弱性と悪用の特定と緩和

*II)は、AI システムの開発者と AI システムの導入者の役割の違いを反映するよう更新されるべきです。*I)と同様に、II)は、AI バリューチェーンのすべての関係者が、AI システムのライフサイクルを通じて、AI システムに関するすべての情報にアクセスできるとみなしているように読めます。II)は、導入*後に*発生する脆弱性に焦点を当てているため、適切な役割、すなわち、AI システムを利用する導入者（例えば、AI 利用者）に適用されるように改訂し、システムの開発者など、懸念に対処する立場にない組織にそのような責任を課さないことを強く推奨します。開発者と導入者（例えば、AI 利用者）のような異なる役割を持つ組織の責任を区別することの重要性は、それぞれの役割を持つ組織が利用できる情報の種類を考えれば明らかです。例えば、AI システムの開発者は、そのシステムの学習に使用されるデータの特徴、システムの既知の限界、およびその意図される利用について説明するのに適した立場にありますが、一般に、そのシステムが他の組織によって取得され、導入された後にどのように利用されるかについての洞察はありません。対照的に、導入者（例えば、AI 利用者）は、システムが実際にどのように利用されているか、人によるどのような監督が実施されているか、システムの実際の機能についてどのような苦情が出ているのかを把握するのに適

した立場にあります。組織はまた、既存の AI モデルを組織の製品やサービスに統合するなど、その他の役割を担うこともあります。これらの組織に課される責任も同様に、AI システムを組織の製品やサービスに統合する際の役割を反映したものでなければなりません。

役割に基づく責任を設けることは AI に限ったことではなく、世界中のプライバシーとセキュリティに関する法律においてベストプラクティスと考えられています。[12]

*また、II) では、脆弱性へのアプローチを明確にすべきです。*II)は、脆弱性の特定と緩和、そして必要に応じて悪用されたインシデントやパターンに焦点を当てています。また、これらの取り組みに関連して、他の利害関係者にも言及しています。重要なのは、脆弱性の報告が内密に取り扱われることです。顧客の契約上の合意を妨げたり、専有情報に関する懸念を生じさせたりする可能性があるためです。また、脆弱性に対処する際には、他のセキュリティ上の影響も考慮すべきです。業界内では、脆弱性はパッチやその他の緩和策が適用されるまでは公表せず、それ以上の被害や悪意ある行為者による潜在的な悪用を防ぐのが一般的な慣行となっています。脆弱性報告に関する法律や政策は、リスクに基づき、国際的に認知された基準やベストプラクティスに沿ったものであるべきです。ガイドライン案は、これらのセキュリティ・インシデントに対応する際の秘密保持の重要性を認識すべきです。

III) 高度なAIシステムの能力、限界、適切・不適切な使用領域に関する公表

*我々はIII)を支持します。*III)の透明性に関する責任を、AIのバリューチェーンにおいて異なる役割を担う様々な組織の間でどのように割り当てるべきかをさらに明確にすることを推奨します。III) では、高度なAIシステムに関する重要な情報（能力、限界、適切・不適切な使用領域を含む）を公表することを求めています。我々は、AIシステムに関する透明性を顧客に提供するための様々な新しいリソースをAIシステムの開発者が作成していることを認識しています。その中には、責任あるAI設計の選択に関する情報を提供する文書や、特定のAIサービスを導入し性能を最適化するためのベストプラクティスなどが含まれます。政府は、このような情報を導入者に提供する取り組みを支援すべきですが、その一方で、開示することで企業秘密、秘密保持、サイバーセキュリティ、プライバシーに関する懸念が生じるような基礎的な学習データその他の情報の開示要件は回避すべきです。

IV)責任ある情報共有とインシデント報告への取り組み

*IV）においては、脆弱性に関するどのような報告を指しているのかを明確にすることを推奨します。*脆弱性報告とインシデント対応は、効果的なセキュリティプログラムの重要な構成要素です。IV)で推奨しているインシデント報告の公表は、顧客との契約上の合意や脆弱性に安全に対処するための措置を妨げる可能性があります。上述したように、一般に、企業は、パッチを開発するか他の緩和策を実施するまでは、脆弱性

[12]「AI開発者とAI導入者：重要な違い」（2023年3月16日）
https://www.bsa.org/files/policy-filings/jp04102023aidevdep.pdf

を報告すべきではありません。脆弱性報告に関する法律や政策は、リスクに基づき、国際的に認知された基準やベストプラクティスに沿ったものであるべきです。我々は、政府に対し、こうしたセキュリティ・インシデントへの対応における機密保持の重要性を認識するよう求めます。

V) リスクベースのアプローチに基づくAIガバナンス及びリスク管理方針の策定、実施、開示

組織の説明責任を強化し、責任あるAIを確実にするためのリスク管理方針と実践の重要性を認識するV）を我々は支持します。

V）は、組織がAIのライフサイクル全体を通じてリスクを評価し、軽減するためのリスク管理プログラムを開発し、実施すべきであることを認識しています。効果的なリスク管理プログラムにおいて重要なのは、影響評価の実施であることをガイドライン案において認識することを奨めます。影響評価は、組織がリスクを特定し、軽減することを可能にするものであり、AIシステムのリスクの高い利用について、開発者と導入者が実施すべきです。組織全体の担当者が目的、データ準備、設計の選択、テスト結果を検討できるようにすることで、これらの評価はAI製品やサービスを改良し、組織のリスク管理プログラムの内部変更を推進するのに役立ちます。このような変更を実施することで、組織は既存の懸念事項によりよく対処し、新たなリスクが出現した場合にはそれに適応することが可能となります。

また、V)では、AIガバナンスに関するポリシーや実行するための組織の開示についても言及しています。我々は、影響評価を機密として扱うことをガイドライン案において認識することを奨めます。これにより、幅広い潜在的なリスクを特定し緩和するために、厳格なプロセスを通して影響評価を実施するインセンティブを組織が維持することができます。AIシステムの高リスクの利用に対して評価が実施されているという事実は、外部の利害関係者にとって、組織がAIシステムの徹底的な検証を実施していることを知ることができるため、信頼性を高めることができます。これらの評価は、既存の国内法に基づき、調査の過程で規制当局も入手できるようにするべきです。
我々は、リスク管理ポリシーの実施を確実にするというV)の目的を支持します。V)においては、影響評価がこの目標を達成する上で役立つ重要な説明責任ツールであると言及すべきです。

VII) 信頼できるコンテンツ認証及び来歴メカニズムの開発と導入

*我々はVII）を支持します。*AIが生成したコンテンツをユーザが識別できるような、信頼性の高いコンテンツ認証および来歴メカニズム（電子透かしなど）を開発・導入することは、AIポリシーにおいて注目すべき重要な点です。AIが生成したコンテンツに対するコンテンツ来歴要件は、画像、音声、および動画コンテンツに焦点を当てるべきです。画像や音声や動画コンテンツのラベリング用に開発されたツールが、テキストに有効であるとは考えにくいからです。テキストベースのAIが生成したコンテンツ

の来歴を確保するためには、個人がAIシステムと対話したときにそれを知ることができるような、別の透明性メカニズムに焦点を当てることを推奨します。

我々は、政府に対し、コンテンツの真正性と来歴に関するオープンな業界標準の採用を推進する、Content Authenticity Initiative[13]、 Coalition for Content Provenance and Authenticity[14] の活動を活用するよう奨励します。これにより、撮影者や画像が生成された場所、ソフトウエアを使用して編集されたかどうかなど、画像や動画の出所に関する情報を特定できるようになり、コンテンツの真正性を判断する際に役立ちます。

XI）適切なデータインプット対策と個人データ及び知的財産保護の実施

*本項は不要です。*I)から X) が、既存の規制の枠組みではとり扱われていないシステム・レベルのリスクに対処しているのとは異なり、XI)は、既存の規制が既に有効である課題に関与しています。入力データに関して適切な保護措置を実施することの重要性には同意しますが、新たな AI 指針や行動規範を含めることは、適切なデータガバナンスを維持することが組織に既に求められていることを認識していないことを意味します。加えて、XI)の記述は、データセットの透明性に言及していますが、データセットが機密情報であったり、さまざまな専有情報を含んでいたりする可能性があるため、開示されるべきではないことを認識していません。

ガイドライン内容の実施のための具体的な手法

[別添（付属資料）全体]

ガイドライン（案）の本編で示された内容を実施するための具体的な手法を別添において「実践例」と共に記していることを我々は評価します。加えて、これらの具体的な手法が単なる例として示されており、ガイドライン（案）本編に示された基本的な理念、原則、指針、行動規範を達成するための唯一の手段ではないことを明示することを我々は推奨します。これにより、実践においては、別の選択肢もあることが事業者に明確になります。

結論

今回、意見募集の際に、総務省と経産省において英訳を用意されたことを BSA と BSA 会員企業は感謝しております。特に、今回のように分量の多い文書においては助かります。我々は、効果的な AI ポリシーの策定をしていく、という日本政府の目標を支援するため に、総務省と経産省に協力していけることを期待しています。本提言を共有することに加え、この取り組みを今後どのように支援していけるかについて話し合う機会 を継続的に頂ければ幸いです。

[13] Content Authenticity Initiative: https://contentauthenticity.org/
[14] Coalition for Content Provenance and Authenticity: https://c2pa.org/