

TECHNICAL REPORT ON AI AND MULTIMEDIA AUTHENTICITY STANDARDS

AIとマルチメディア真正性規格に関する技術報告

MAPPING THE STANDARDISATION LANDSCAPE

標準化の現状展望

技術文書

英和対訳
一般財団法人 日本規格協会



TABLE OF CONTENTS

	Executive Summary	04
1	Introduction	05
	1.1 Methodology	
2	Categories of Standards	06
	2.1 Content Provenance	
	2.2 Trust and Authenticity	
	2.3 Asset Identifiers	
	2.4 Rights Declarations	
	2.4.1 General Purpose	
	2.4.2 Opt-Out Mechanisms	
	2.5 Watermarking	
3	Overview of Specifications	08
	3.1 Content Credentials	
	3.2 Content Credentials	
	3.3 JPEG Trust Part 1: Core foundation	
	3.4 JPEG Trust Part 2: Trust profiles catalogue	
	3.5 JPEG Trust Part 3: Media asset watermarking	
	3.6 CAWG Metadata	
	3.7 Originator Profile	
	3.8 PROV	
	3.9 Overview of trustworthiness in artificial intelligence	
	3.10 Framework for trust-based media services	
	3.11 Trust.txt	
	3.12 Chromium Reputation Provider Framework	
	3.13 ISCC: International Standard Content Code (ISCC)	
	3.14 Unique Media Identifier (UMid)	
	3.15 TDM Reservation Protocol	
	3.16 ai.txt	
	3.17 Robots.txt	
	3.18 Vocabulary for Expressing Content Preferences for AI Training	
	3.19 Open Binding of Content Identifiers (OBID)	
	3.20 X.ig-dw: Implementation guidelines for digital watermarking	
	3.21 DRM technology for digital publications Part 1: Overview of copyright protection technologies in use in the publishing industry	

目次

	概要	04
1	はじめに	05
	1.1 方法論	
2	規格の分類	06
	2.1 コンテンツの出所	
	2.2 信頼性と真正性	
	2.3 資産識別子	
	2.4 権利宣言	
	2.4.1 汎用	
	2.4.2 オプトアウトメカニズム	
	2.5 透かし	
3	仕様の概要	08
	3.1 コンテンツ認証情報	
	3.2 コンテンツ認証情報	
	3.3 JPEG Trust 第1部:コア基盤	
	3.4 JPEG Trust 第2部:信頼プロファイルカタログ	
	3.5 JPEG Trust 第3部:メディア資産の透かし	
	3.6 CAWG メタデータ	
	3.7 オリジネータープロファイル	
	3.8 PROV	
	3.9 人工知能における信頼性の概要	
	3.10 信頼に基づくメディアサービスのためのフレームワーク	
	3.11 Trust.txt	
	3.12 クロミウムレピュテーションプロバイダフレームワーク	
	3.13 ISCC:国際規格コンテンツコード (ISCC)	
	3.14 ユニークメディア識別子 (UMid)	
	3.15 TDM予約プロトコル	
	3.16 ai.txt	
	3.17 Robots除外プロトコル (Robots.txt)	
	3.18 AIトレーニング向けコンテンツ選好表現語彙	
	3.19 コンテンツ識別子のオープンバイディング (OBID)	
	3.20 X.ig-dw: デジタル透かしの実装ガイドライン	
	3.21 デジタル出版物のためのDRM技術 第1部:出版業界で使用されている著作権保護技術の概要	

3	3.22 A Review of Medical Image Watermarking Requirements for Teleradiology	
	3.23 MPEG-21 - Part 11: Evaluation Tools for Persistent Association Technologies	
	3.24 IEEE Draft Standard for Evaluation Method of Robustness of Digital Watermarking Implementation in Digital Contents	
	3.25 H.MMAUTH: Framework for authentication of multimedia content	
	3.26 H.274(V4): Versatile supplemental enhancement information messages for coded video bitstreams	
	3.27 H.VADS: Assessment criteria for video authenticity detection services	
	3.28 Credible Web	
	3.29 Technical and Governance Guidelines for Responsible Data Collection	
	3.30 Data Provenance Standards	
	3.31 IEEE Standard for Transparent Human and Machine Agency Identification	
	3.32 IPTC Photo Metadata Standard	
	3.33 DASH - Part 4: Segment Encryption and Authentication	
	3.34 Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies	

4	Standardization Map	20
	4.1 Standards & Specification Map	
	4.2 Media Type Support Map	

5	Related Standards	24
	Blockchain and Distributed Ledger Technologies	
	Identity Standards	
	Rights Declarations	
	Creative Commons	
	Supply Chain Integrity, Transparency, and Trust	

6	Conclusion and next steps	25
----------	----------------------------------	-----------

	Annex A: Table of Standard & Specification Categorization	26
--	--	-----------

	Annex B: Table of Media Type Support	29
--	---	-----------

3	3.22	遠隔放射線診断における医用画像透かしの要件に関するレビュー	
	3.23	MPEG-21 – 第11部: 継続性連合技術の評価ツール	
	3.24	デジタルコンテンツにおける電子透かし実装の堅牢性評価方法に関するIEEE規格案	
	3.25	H.MMAUTH: マルチメディアコンテンツの認証フレームワーク	
	3.26	H.274 (V4): 符号化ビデオビットストリーム用多用途補足拡張情報メッセージ	
	3.27	H.VADS: ビデオ真正性検出サービスの評価基準	
	3.28	信頼できるウェブ	
	3.29	責任あるデータ収集のための専門的およびガバナンスガイドライン	
	3.30	データ出所規格	
	3.31	人間と機械の透過性のあるエージェンシー識別のためのIEEE規格	
	3.32	IPTC写真メタデータ規格	
	3.33	DASH - 第4部: セグメント暗号化および認証	
	3.34	人工知能生成コンテンツ技術のレベルに関する推奨プラクティス	

4	標準化マッピング	20
	4.1	規格と仕様のマップ
	4.2	メディアタイプサポートマップ

5	関連規格	24
	ブロックチェーンと分散台帳技術	
	アイデンティティ規格	
	権利宣言	
	クリエイティブ・コモンズ	
	サプライチェーンの完全性, 透明性, および信頼性	

6	結論と次のステップ	25
	附属書A: 規格および仕様の分類表	26
	附属書B: メディア種別のサポート表	29

EXECUTIVE SUMMARY

This technical paper provides a comprehensive overview of the current landscape of standards and specifications related to digital media authenticity and artificial intelligence. It categorizes these standards into five key clusters: content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking. The report provides a short description of each standard along with link for further details.

By mapping the contributions of various Standard Development Organizations (SDOs) and groups, we aim to identify gaps and opportunities for further standardization. This could serve as a valuable resource for stakeholders seeking to navigate the complex ecosystem of standards at the intersection of artificial intelligence and authenticity in digital media and to implement best practices to safeguard the authenticity of digital assets and the rights assigned to them. The findings underscore the critical role of robust specifications and standards in fostering trust and accountability in the evolving digital landscape.

AI and Multimedia Authenticity Standards Collaboration (AMAS)

The AI and Multimedia Authenticity Standards Collaboration is a global initiative advancing standardization in the rapidly evolving field of AI-generated and altered media. By identifying gaps and driving the development of new standards, we support transparent, privacy-conscious, and rights-respecting practices. Our work also aims at informing policy and regulatory frameworks to promote legal compliance and safeguard public trust.

Led by the World Standards Cooperation, the collaboration serves as a vital forum for dialogue among standards developers, civil society organizations, technology companies, and other key players. Participating organizations include the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), the Coalition for Content Provenance and Authenticity (C2PA), the China Academy of Information and Communications Technology (CAICT), DataTrails, Deep Media, and Witness.

Convened by ITU under the auspices of the World Standards Cooperation, the collaboration was launched at the AI for Good Global Summit in 2024.

Learn more here (<https://aiforgood.itu.int/multimedia-authenticity/>) or contact the Secretariat at amas-secretariat@itu.int

Disclaimer:

This report is a collaborative work prepared by the secretariats of the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO), and the International Telecommunication Union (ITU) under the banner of the World Standards Cooperation (WSC).

The views, observations, and conclusions expressed in this publication are solely those of the authors, including from the respective secretariats. They do not necessarily reflect, nor do they represent, the official positions, policies, or consensus views of the national member bodies, or any other affiliated members of IEC, ISO, or ITU.

This document is intended to provide a technical overview and mapping of the standardization landscape concerning AI and multimedia authenticity for informational purposes. It has not been subject to the formal approval processes of these standards development organizations and should not be construed as an official standard or a formal endorsement by their respective membership.

概要

本技術文書は、デジタルメディアの真正性と人工知能(AI)に関連する規格および仕様の現状について、包括的な概要を提供します。これらの標準規格は、コンテンツの出所、信頼性と真正性、資産識別子、権利宣言、透かしの5つの主要なクラスターに分類されています。本報告書では、各規格の簡単な説明と、詳細情報へのリンクを提供しています。

様々な規格開発団体(SDO)やグループの貢献をマッピングすることで、さらなる標準化に向けたギャップと機会を特定することを目指しています。これは、デジタルメディアにおけるAIと真正性の交差点にある複雑な規格のエコシステムを理解し、デジタル資産の真正性とそれらに付与された権利を保護するためのベストプラクティスを実装しようとする関係者にとって貴重なリソースとなる可能性があります。結果は、進化するデジタル環境において、堅牢な仕様と規格が信頼と説明責任を促進する上で重要な役割を果たすことを強調しています。

AIとマルチメディア真正性規格の連携(AMAS)

AIとマルチメディア真正性規格の連携は、急速に進化するAI生成および改変メディアの分野における標準化を推進するグローバルイニシアチブです。ギャップを特定し、新たな規格の開発を推進することで、透明性、プライバシーへの配慮、そして権利尊重を重視した実践をサポートします。また、法令遵守を促進し、公共の信頼を守るための政策および規制フレームワークの構築にも取り組んでいます。

世界標準協力(WSC)が主導するこの連携は、規格開発者、市民社会組織、テクノロジー企業、その他の主要プレイヤー間の対話のための重要なフォーラムとして機能しています。参加組織には、国際電気標準会議(IEC)、国際標準化機構(ISO)、国際電気通信連合(ITU)、コンテンツの出所と真正性に関する連合(C2PA)、中国情報通信研究院(CAICT)、DataTrails、Deep Media、Witnessなどがあります。

この連携は、世界標準協力(WSC)の後援の下、ITUが招集し、2024年に開催されたAI for Goodグローバルサミットで開始されました。

詳細はこちら(<https://aiforgood.itu.int/multimedia-authenticity/>)をご覧ください、事務局(amas-secretariat@itu.int)までお問い合わせください。

免責事項:

本報告書は、世界標準協力(WSC)の旗の下、国際電気標準会議(IEC)、国際標準化機構(ISO)、国際電気通信連合(ITU)の各事務局が共同で作成したものです。

本書に記載されている見解、所見、および結論は、各事務局を含む著者の見解のみに基づくものです。これらは、IEC、ISO、ITUの各国会員団体またはその他の提携団体の公式見解、方針、またはコンセンサスを必ずしも反映または代表するものではありません。

本文書は、AIおよびマルチメディア真正性に関する標準化の現状について、情報提供を目的として専門的な概要とマッピングを提供することを目的としています。本文書は、これらの規格開発団体による正式な承認プロセスを経ておらず、公式な規格または各会員団体による正式な承認と解釈されるべきではありません。

Section 01

INTRODUCTION

This technical paper provides a comprehensive overview of various standards and specifications related to digital media, focusing on content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking. These standards are essential for ensuring the authenticity of both synthetic and non-synthetic digital content. As generative AI continues to evolve, the need for robust standards becomes increasingly critical to protect the interests of creators, consumers, and organizations.

The standards discussed in this report are developed by various Standard Development Organizations (SDOs) and groups, each contributing to different aspects of AI and authenticity. By adhering to these guidelines, organizations can better maintain the trustworthiness and provenance of their digital assets, ensuring that content remains authentic and traceable throughout its lifecycle.

1.1 Methodology

The approach taken in this report involves a thorough review of known existing standards and specifications related to digital media. The focus was on identifying key areas where standards already exist, and from that, what might still be needed to support the authenticity and integrity of digital content. From that review, we have broken this report into the following categories: content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking.

第1章

はじめに

本技術文書では、デジタルメディアに関連する様々な規格と仕様について、コンテンツの出所、信頼性と真正性、資産識別子、権利宣言、透かしに焦点を当て、包括的な概要を提供します。これらの規格は、合成デジタルコンテンツと非合成デジタルコンテンツの両方の真正性を保証するために不可欠です。生成AIが進化を続けるにつれ、クリエイター、消費者、そして組織の利益を守るために、堅牢な規格の必要性がますます高まっています。

本報告書で解説する規格は、AIと真正性の異なる側面に貢献する様々な規格開発団体(SDO)およびグループによって開発されています。これらのガイドラインを遵守することで、組織はデジタル資産の信頼性と出所をより適切に維持し、コンテンツのライフサイクル全体を通じて真正性と追跡可能性を維持できます。

1.1 方法論

本報告書では、デジタルメディアに関連する既存の既知の規格と仕様を徹底的にレビューしました。焦点は、既に規格が存在している主要分野を特定し、そこからデジタルコンテンツの真正性と完全性を支えるために今後何が必要かを明らかにすることにあります。このレビューに基づき、本報告書を、コンテンツの出所、信頼性と真正性、資産識別子、権利宣言、透かしの5つのカテゴリーに分類しました。

Section 02

CATEGORIES OF STANDARDS

In this technical paper, we have clustered those standards and specifications in the scope of this analysis into five categories: content provenance, trust and authenticity, asset identifiers, rights declaration and watermarking. Rights declaration, in turn, is defined in two inclinations: general purpose and opt-out mechanisms. The general purpose rights declaration addresses a broad scope while the opt-out mechanisms refer to a specific aspect of rights declaration that is of relevance to the scope of this document.

2.1 Content Provenance

Content provenance refers to information on the origin, history, and lifecycle of digital content. This is an important tool for the verification of the authenticity and integrity of digital assets. Provenance information helps in storing information about the creation, modification, and distribution of content, providing a transparent record that can be used to establish trust and authenticity. This is particularly important in use cases and applications where the authenticity and accountability of content is paramount, such as in journalism, scientific research, and digital art.

2.2 Trust and Authenticity

Trust and authenticity represent methodologies for ensuring that digital content is genuine and has not been tampered with. Such mechanisms are essential for maintaining the integrity of digital media, especially in environments where content manipulation is a significant concern. By implementing trust and authenticity measures, organizations can protect their digital assets from unauthorized alterations and help ensure that consumers can rely on the content they receive.

2.3 Asset Identifiers

Asset identifiers are unique codes assigned to digital content to ensure proper management and identification of the asset. These identifiers help in maintaining a clear and organized record of digital assets, making it easier to organize, manage and distribute content. By using asset identifiers, organizations can ensure that their digital media is properly tracked and accounted for, reducing the risk of loss or unauthorized use.

第2章

規格のカテゴリー

本技術文書では、分析対象となる規格と仕様を、コンテンツの出所、信頼性と真正性、資産識別子、権利宣言、透かしの5つのカテゴリーに分類しました。権利宣言は、汎用型とオプトアウト型の2つの定義に分かれています。汎用型の権利宣言は広範な範囲を扱いますが、オプトアウト型の権利宣言は、本文書の範囲に関連する特定の側面を指します。

2.1 コンテンツの出所

コンテンツの出所とは、デジタルコンテンツの起源、履歴、ライフサイクルに関する情報を指します。これは、デジタル資産の真正性と完全性を検証するための重要なツールです。出所情報は、コンテンツの作成、変更、配信に関する情報を保存し、信頼性と真正性を確立するための透明性のある記録を提供するのに役立ちます。これは、ジャーナリズム、科学研究、デジタルアートなど、コンテンツの真正性と説明責任が最も重要となるユースケースやアプリケーションにおいて特に重要です。

2.2 信頼性と真正性

信頼性と真正性は、デジタルコンテンツが真正であり、改ざんされていないことを保証するための方法論を表します。このようなメカニズムは、特にコンテンツの改ざんが大きな懸念事項となる環境において、デジタルメディアの完全性を維持するために不可欠です。信頼性と真正性を確保するための対策を実装することで、組織はデジタル資産を不正な改ざんから保護し、消費者が受け取るコンテンツを信頼できるようにすることができます。

2.3 資産識別子

資産識別子は、デジタルコンテンツに割り当てられた固有のコードであり、資産の適切な管理と識別を保証します。これらの識別子は、デジタル資産の明確で整理された記録を維持し、コンテンツの整理、管理、配付を容易にするのに役立ちます。資産識別子を使用することで、組織はデジタルメディアが適切に追跡および管理され、紛失や不正使用のリスクを軽減できます。

2.4 Rights Declarations

2.4.1 General Purpose

Rights declarations are formal statements that outline the rights and permissions associated with digital content. These declarations help in clarifying the ownership and usage rights of digital assets, providing a clear framework for how content can be used and shared. By establishing clear rights declarations, organizations can protect their intellectual property and ensure that their digital assets are used in accordance with their intended purpose.

2.4.2 Opt-Out Mechanisms

Opt-out mechanisms are a specialized approach to rights declarations that allow users to exclude their content from certain processes, such as data mining or AI training. These mechanisms are essential for protecting the privacy and rights of content creators, ensuring that their digital assets are not used without their consent. By implementing opt-out mechanisms, organizations can provide users with greater control over their content and ensure that their rights are respected.

2.5 Watermarking

Watermarking ensures that digital content is marked in a way that can be used to verify its authenticity, synthetic (or not) nature, and ownership. Watermarking is increasingly used to facilitate the declaration of the rights of content creators and to help ensure that their digital assets are not used without their consent. By implementing watermarking measures, organizations can provide users with greater control over their content and make sure that their rights are respected.

2.4 権利宣言

2.4.1 一般的な目的

権利宣言とは、デジタルコンテンツに関連する権利と許可を概説した正式な声明です。これらの宣言は、デジタル資産の所有権と使用权を明確にし、コンテンツの使用方法和共有方法に関する明確なフレームワークを提供します。明確な権利宣言を確立することで、組織は知的財産を保護し、デジタル資産が本来の目的に沿って使用されることを保証できます。

2.4.2 オプトアウトメカニズム

オプトアウトメカニズムは、権利宣言に対する特殊なアプローチであり、ユーザーがデータマイニングやAIトレーニングなどの特定のプロセスからコンテンツを除外できるようにします。これらのメカニズムは、コンテンツ作成者のプライバシーと権利を保護し、デジタル資産がユーザーの同意なしに使用されないようにするために不可欠です。オプトアウトメカニズムを実装することで、組織はユーザーにコンテンツに対するより高度なコントロールを提供し、ユーザーの権利が尊重されることを保証できます。

2.5 透かし

透かしは、デジタルコンテンツに、その真正性、合成(または非合成)の性質、および所有権を検証できる方法でマークを付けることを保証します。透かしは、コンテンツ作成者の権利宣言を容易にし、デジタル資産が作成者の同意なく利用されることを防ぐために、ますます利用されています。透かし対策を導入することで、組織はユーザーにコンテンツに対するより高度なコントロールを提供し、権利の尊重を確実にすることができます。

Section 03

OVERVIEW OF SPECIFICATIONS

3.1 Content Credentials

- SDO/Group: C2PA
- Link: [C2PA Specification](#)
- Status: Published
- Publication Date: 2025
- Media: Any

Summary: This standard provides guidelines for embedding content credentials in digital media to ensure provenance. It outlines methods for attaching metadata to digital assets, which can include information about the creator, creation date, and any modifications made to the content. This helps in maintaining a verifiable record of the content's history.

3.2 Content Credentials

- SDO/Group: ISO TC 171/SC 2
- Link: [ISO 22144](#)
- Status: In progress
- Media Types: Any

Summary: This ISO standard outlines methods for documenting content credentials to maintain provenance. It specifies the types of metadata that should be included and the formats for storing this information. By following these guidelines, organizations can ensure that their digital content is traceable and its authenticity can be verified.

3.3 JPEG Trust Part 1: Core foundation

- SDO/Group: ISO/IEC JTC 1/SC 29/WG 1
- Link: [ISO 21617-1:2025, second edition in progress](#)
- Status: Published
- Publication Date: 2025
- Media: Any (image focused)

Summary: This standard focuses on trust and authenticity in JPEG images through provenance, detection and fact-checking. It provides a framework for embedding metadata directly into JPEG files in the form of trust indicators. This allows users to decide the degree of trust they can put on a digital assets as a function of their trust profiles. This is particularly useful in contexts where image manipulation is common, such as in social media applications.

第3章

仕様の概要

3.1 コンテンツ認証情報

- SDO/グループ: C2PA
- リンク: [C2PA Specification](#)
- ステータス: 発行済み
- 発行日: 2025年
- メディア: 任意

概要:この規格は、デジタルメディアにコンテンツ認証情報を埋め込むことで出所を保証するためのガイドラインを提供します。デジタル資産にメタデータを添付する方法を概説しており、メタデータには作成者、作成日、コンテンツに加えられた変更に関する情報などが含まれます。これにより、コンテンツの履歴に関する検証可能な記録を維持することができます。

3.2 コンテンツ認証情報

- SDO/グループ: ISO TC 171/SC 2
- リンク: [ISO 22144](#)
- ステータス: 進行中
- メディアタイプ: 任意

概要:このISO規格は、コンテンツの出所を維持するための認証情報を文書化する方法を概説しています。含めるべきメタデータの種類と、その情報を格納するためのフォーマットを規定しています。これらのガイドラインに従うことで、組織はデジタルコンテンツの追跡可能性と真正性の検証を確実に行うことができます。

3.3 JPEG Trust 第1部: コア基盤

- SDO/グループ: ISO/IEC JTC 1/SC 29/WG 1
- リンク: [ISO 21617-1:2025, 第2版進行中](#)
- ステータス: 発行済み
- 発行日: 2025年
- メディア: 任意(画像中心)

概要:この規格は、出所、検出、およびファクトチェックを通じて、JPEG画像の信頼性と真正性に焦点を当てています。信頼インジケータの形でメタデータをJPEGファイルに直接埋め込むためのフレームワークを提供します。これにより、ユーザーは信頼プロファイルに基づいて、デジタル資産に付与できる信頼度を決定できます。これは、ソーシャルメディアアプリケーションなど、画像操作が頻繁に行われる環境で特に役立ちます。

3.4 JPEG Trust Part 2: Trust profiles catalog

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 1
- **Status:** In progress
- **Media:** Any (image focused)

Summary: This standard introduces a series of trust profile snippets that can be used either as is or as starting points to establish profiles for use in specific workflows, use cases and applications such as broadcasting, digital cameras, AI-powered content generation services, etc.

3.5 JPEG Trust Part 3: Media asset watermarking

- **SDO/Group:** ISO/IEC JTC 1/SC 29/WG 1
- **Status:** Initiated
- **Media Types:** Images

Summary: This standard is planned to provide an overview of mechanisms used for watermarking of media assets.

3.6 CAWG Metadata

- **SDO/Group:** Creation Assertions Working Group, as part of DIF
- **Link:** [CAWG Metadata](#)
- **Status:** Published
- **Publication Date:** 2025
- **Media Types:** Any

Summary: This specification provides a framework for expressing metadata that captures detailed information about the content, including ownership and authorship.

3.4 JPEG Trust 第2部:信頼プロファイルカタログ

- **SDO/グループ**: ISO/IEC JTC 1/SC 29/WG 1
- **ステータス**: 進行中
- **メディア**: 任意(画像中心)

概要: この規格では、一連の信頼プロファイルスニペットを導入しています。これらのスニペットは、そのまま使用することも、放送、デジタルカメラ、AIを活用したコンテンツ生成サービスなどの特定のワークフロー、ユースケース、アプリケーションで使用するプロファイルを確立するための出発点として使用することもできます。

3.5 JPEG Trust 第3部:メディア資産の透かし

- **SDO/グループ**: ISO/IEC JTC 1/SC 29/WG 1
- **ステータス**: 開始済み
- **メディアタイプ**: 画像

概要: この規格は、メディア資産の透かしに使用されるメカニズムの概要を提供することを目的として計画されています。

3.6 CAWGメタデータ

- **SDO/グループ**: Creation Assertions Working Group (DIFの一部)
- **リンク**: [CAWGメタデータ](#)
- **ステータス**: 発行済み
- **発行日**: 2025年
- **メディアタイプ**: 任意

概要: この仕様は、コンテンツの所有権や著作者など、コンテンツに関する詳細情報を記述するメタデータを表現するためのフレームワークを提供します。

3.7 Originator Profile

- **SDO/Group:** Originator Profile
- **Link:** [Originator Profile](#)
- **Status:** In progress
- **Media:** Web pages

Summary: This specification provides a framework for documenting the origin of digital content. It includes guidelines for creating and maintaining profiles that capture detailed information about the content's creator and its creation process. This helps in establishing a clear and verifiable record of the content's provenance.

3.8 PROV

- **SDO/Group:** Open Provenance
- **Link:** [PROV](#)
- **Status:** Published
- **Publication Date:** 2013
- **Media:** Any

Summary: This standard offers a model for representing provenance information in digital content. It defines a set of concepts and relationships that can be used to describe the history of a digital asset, including its creation, modification, and distribution. This model can be applied across various types of digital content, providing a flexible and comprehensive approach to provenance documentation.

3.9 Overview of trustworthiness in artificial intelligence

- **SDO/Group:** ISO/IEC JTC 1/SC 42
- **Link:** [ISO/IEC TR 24028:2020](#)
- **Status:** Published
- **Publication Date:** 2020

Summary: This standard offers an overview of trustworthiness in artificial intelligence. It provides guidelines for assessing the reliability and integrity of AI systems, ensuring that they produce trustworthy results. This is crucial in applications where AI is used to generate or manipulate digital content, as it helps in maintaining the authenticity of the output.

3.7 オリジネータープロフィール

- **SDO/グループ:** オリジネータープロフィール
- **リンク:** [Originator Profile](#)
- **ステータス:** 進行中
- **メディア:** ウェブページ

概要: この仕様は、デジタルコンテンツの出所を文書化するためのフレームワークを提供します。コンテンツの作成者と作成プロセスに関する詳細情報を記述するプロフィールの作成および維持に関するガイドラインが含まれています。これにより、コンテンツの出所に関する明確かつ検証可能な記録を確立することができます。

3.8 PROV

- **SDO/グループ:** Open Provenance
- **リンク:** [PROV](#)
- **ステータス:** 発行済み
- **発行日:** 2013年
- **メディア:** 任意

概要: この規格は、デジタルコンテンツにおける出所情報の表現モデルを提供します。デジタル資産の作成、変更、配付などの履歴を記述するために使用できる一連の概念と関係性を定義します。このモデルはさまざまな種類のデジタルコンテンツに適用でき、出所の文書化に対する柔軟かつ包括的なアプローチを提供します。

3.9 人工知能における信頼性の概要

- **SDO/グループ:** ISO/IEC JTC 1/SC 42
- **リンク:** [ISO/IEC TR 24028:2020](#)
- **ステータス:** 発行済み
- **発行日:** 2020年

概要: この規格は、人工知能における信頼性の概要を提供します。AIシステムの信頼性と整合性を評価し、信頼できる結果を生成するためのガイドラインを提供します。これは、AIを用いてデジタルコンテンツを生成または操作するアプリケーションにおいて、出力の真正性を維持する上で非常に重要となります。

3.10 Framework for trust-based media services

- **SDO/Group:** ITU-T
- **Link:** [ITU-T Y.3054](#)
- **Status:** Published
- **Publication Date:** 2018

Summary: is framework provides guidelines for trust-based media services. In particular, it includes methods for establishing and maintaining trust in digital media platforms, ensuring that users can rely on the content they access. This is particularly important in contexts where media services are used to distribute sensitive or high-value content.

3.11 Trust.txt

- **SDO/Group:** JournalList
- **Link:** [Trust.txt](#)
- **Status:** Initiated
- **Media:** Web pages

Summary: This specification outlines methods for establishing trust in digital content. It includes guidelines for creating and maintaining trust.txt files, which can be used to document the trustworthiness of digital assets. This helps in ensuring that users can verify the authenticity of the content they receive.

3.12 Chromium Reputation Provider Framework

- **SDO/Group:** Google's Chrome Team
- **Link:** [Chromium Reputation Provider Framework](#)
- **Status:** Initiated
- **Media:** Web pages

Summary: This framework provides guidelines for reputation management of digital content. It includes methods for assessing and maintaining the reputation of digital assets, ensuring that users can trust the content they access. This is particularly important in contexts where reputation is a key factor in determining the value and reliability of digital media.

3.10 信頼に基づくメディアサービスのためのフレームワーク

- SDO/グループ: ITU-T
- リンク: [ITU-T Y.3054](#)
- ステータス: 発行済み
- 発行日: 2018年

概要:このフレームワークは、信頼に基づくメディアサービスのためのガイドラインを提供します。特に、デジタルメディアプラットフォームにおける信頼を確立・維持するための手法が含まれており、ユーザーがアクセスするコンテンツを信頼できることを保証します。これは、メディアサービスが機密性の高いコンテンツや高価値コンテンツを配信するために使用される状況において特に重要です。

3.11 Trust.txt

- SDO/グループ: JournalList
- リンク: [Trust.txt](#)
- ステータス: 開始済み
- メディア: ウェブページ

概要:この仕様は、デジタルコンテンツにおける信頼を確立するための手法を概説しています。デジタル資産の信頼性を文書化するために使用できるtrust.txtファイルの作成および維持に関するガイドラインも含まれています。これにより、ユーザーは受信したコンテンツの真正性を検証できるようになります。

3.12 クロミウムレピュテーションプロバイダフレームワーク

- SDO/グループ: Google Chrome Team
- リンク: [Chromium Reputation Provider Framework](#)
- ステータス: 開始済み
- メディア: ウェブページ

概要:このフレームワークは、デジタルコンテンツのレピュテーション管理に関するガイドラインを提供します。デジタル資産のレピュテーションを評価・維持するための方法が含まれており、ユーザーがアクセスするコンテンツを信頼できるようにします。これは、レピュテーションがデジタルメディアの価値と信頼性を決定する重要な要素となる状況において特に重要です。

3.13 ISCC: International Standard Content Code (ISCC)

- **SDO/Group:** ISO/TC 46/SC 9
- **Link:** [ISO 24138](#)
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Any

Summary: This standard provides a unique identifier for digital content. It includes guidelines for creating and maintaining ISCC codes, which can be used to track and manage digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.14 Unique Media Identifier (UMid)

- **SDO/Group:** IWA 44
- **Link:** [UMid](#)
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Any

Summary: This specification offers a unique identifier for media content. It includes methods for creating and maintaining UMid codes, which can be used to track and manage media assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.15 TDM Reservation Protocol

- **SDO/Group:** W3C
- **Link:** [TDMRep](#)
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Web pages, EPub, PDF

Summary: This protocol provides guidelines for reserving content from text and data mining. It includes methods for creating and maintaining TDMRep files, which can be used to document the reservation of digital assets. This helps in ensuring that content is not used for data mining without the creator's consent.

3.13 ISCC: 国際規格コンテンツコード (ISCC)

- **SDO/グループ:** ISO/TC 46/SC 9
- **リンク:** [ISO 24138](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** 任意

概要: この規格は、デジタルコンテンツに固有の識別子を提供します。デジタル資産の追跡と管理に使用できる ISCC コードの作成と維持に関するガイドラインが含まれています。これにより、コンテンツが適切に管理され、容易に識別・取得できるようになります。

3.14 ユニークメディア識別子 (UMid)

- **SDO/グループ:** IWA 44
- **リンク:** [UMid](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** 任意

概要: この仕様は、メディアコンテンツに固有の識別子を提供します。UMidコードの作成および維持方法が含まれており、メディア資産の追跡と管理に使用できます。これにより、コンテンツが適切に管理され、容易に識別および取得できるようになります。

3.15 TDM予約プロトコル

- **SDO/グループ:** W3C
- **リンク:** [TDMRep](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** ウェブページ, EPub, PDF

概要: このプロトコルは、テキストマイニングおよびデータマイニングからコンテンツを予約するためのガイドラインを提供します。デジタル資産の予約を文書化するために使用できるTDMRepファイルの作成および維持方法が含まれており、これにより、作成者の同意なしにコンテンツがデータマイニングに使用されないようにすることができます。

3.16 ai.txt

- SDO/Group: Spawning
- Link: [Spawning ai.txt](#)
- Status: Published
- Publication Date: 2023
- Media: Any

Summary: This specification offers a method for opting out of AI training. It includes guidelines for creating and maintaining ai.txt files, which can be used to document the opt-out of digital assets. This helps in ensuring that content is not used for AI training without the creator's consent.

3.17 Robots Exclusion Protocol (Robots.txt)

- SDO/Group: IETF
- Link: [RFC 9309](#)
- Status: Published
- Media: Any

Summary: This standard provides guidelines for excluding content from web crawlers. It includes methods for creating and maintaining robots.txt files, which can be used to document the exclusion of digital assets. This helps in ensuring that content is not accessed by web crawlers without the creator's consent.

3.18 Vocabulary for Expressing Content Preferences for AI

- SDO/Group: IETF
- Link: [ietf-ai-pref-vocab-00](#)
- Status: In progress
- Media: Any

Summary: This document proposes a standardized vocabulary of use cases that can be targeted when expressing machine-readable opt-outs related to Text and Data Mining (TDM) and AI training. The vocabulary is agnostic to specific opt-out mechanisms and enables declaring parties to communicate restrictions or permissions regarding the use of their digital assets in a structured and interoperable manner.

3.16 ai.txt

- SDO/グループ: Spawning
- リンク: [Spawning ai.txt](#)
- ステータス: 発行済み
- 発行日: 2023
- メディア: 任意

概要: この仕様は、AIトレーニングからオプトアウトする方法を提供します。デジタル資産のオプトアウトを文書化するために使用できるai.txtファイルの作成と管理に関するガイドラインが含まれています。これにより、作成者の同意なしにコンテンツがAIトレーニングに使用されないようにすることができます。

3.17 Robots除外プロトコル (Robots.txt)

- SDO/グループ: IETF
- リンク: [RFC 9309](#)
- ステータス: 発行済み
- メディア: 任意

概要: この規格は、ウェブクローラーからコンテンツを除外するためのガイドラインを提供します。デジタル資産の除外を文書化するために使用できるrobots.txtファイルの作成と管理に関するガイドラインが含まれています。これにより、作成者の同意なしにウェブクローラーがコンテンツにアクセスしないようにすることができます。

3.18 AI向けコンテンツ選好表現語彙

- SDO/グループ: IETF
- リンク: [ietf-ai-pref-vocab-00](#)
- ステータス: 進行中
- メディア: 任意

概要: 本文書は、テキスト・データマイニング (TDM) およびAIトレーニングに関連する機械可読なオプトアウトを表現する際に対象とすることができる、ユースケースの標準化された語彙を提案します。この語彙は特定のオプトアウトメカニズムに依存せず、宣言者がデジタル資産の利用に関する制限事項または許可事項を、構造化された相互運用可能な方法で伝達することを可能にします。

3.19 Open Binding of Content Identifiers (OBID)

- SDO/Group: SMPTE
- Link: [SMPTE ST 2112-10:2020](#)
- Status: Published
- Publication Date: 2020
- Media: Audio

Summary: This standard provides guidelines for binding content identifiers to digital media. It includes methods for creating and maintaining OBID files, which can be used to document the binding of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.20 X.ig-dw: Implementation guidelines for digital watermarking

- SDO/Group: ITU-T SG17
- Link: [2413-PLN](#)
- Status: Published, but temporary
- Publication Date: 2024
- Media: Images, Video

Summary: This guideline offers methods for implementing digital watermarking. It includes guidelines for creating and maintaining watermark files, which can be used to document the watermarking of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.21 DRM technology for digital publications Part 1: Overview of copyright protection technologies in use in the publishing industry

- SDO/Group: ISO/IEC JTC 1/SC 34
- Link: [ISO/IEC 23078-1:2024](#)
- Status: Published
- Publication Date: 2024
- Media: EPub, PDF

Summary: This standard provides an overview of DRM technologies for digital publications. It includes guidelines for creating and maintaining DRM files, which can be used to document the DRM of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.19 コンテンツ識別子のオープンバイディング(OBID)

- **SDO/グループ:** SMPTE
- **リンク:** [SMPTE ST 2112-10:2020](#)
- **ステータス:** 発行済み
- **発行日:** 2020年
- **メディア:** オーディオ

概要: 本規格は、コンテンツ識別子をデジタルメディアにバイディングするためのガイドラインを提供します。デジタル資産のバイディングを文書化するために使用できるOBIDファイルの作成および管理方法が含まれています。これにより、コンテンツが適切に管理され、容易に識別および取得できることが保証されます。

3.20 X.ig-dw: デジタル透かしの実装ガイドライン

- **SDO/グループ:** ITU-T SG17
- **リンク:** [2413-PL EN](#)
- **ステータス:** 発行済み (暫定版)
- **発行日:** 2024年
- **メディア:** 画像, ビデオ

概要: このガイドラインは、デジタル透かしの実装方法を示しています。デジタル資産への透かしの記録に使用できる透かしファイルの作成と管理に関するガイドラインも含まれています。これにより、コンテンツが適切に管理され、容易に識別・取得できることが保証されます。

3.21 デジタル出版物のためのDRM技術 第1部: 出版業界で使用されている著作権保護技術の概要

- **SDO/グループ:** ISO/IEC JTC 1/ SC 34
- **リンク:** [ISO/IEC 23078-1:2024](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** EPub, PDF

概要: この規格は、デジタル出版物のためのDRM技術の概要を示しています。本規格には、デジタル資産のDRMを文書化するために使用できるDRMファイルの作成と管理に関するガイドラインが含まれています。これにより、コンテンツが適切に管理され、容易に識別・取得できることが保証されます。

3.22

A Review of Medical Image Watermarking Requirements for Teleradiology

- SDO/Group: NIH
- Link: [Medical Image Watermarking](#)
- Status: Published
- Publication Date: 2012
- Media: Images

Summary: This review outlines the requirements for watermarking medical images for teleradiology. It includes guidelines for creating and maintaining watermark files, which can be used to document the watermarking of medical images. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.23

MPEG-21 — Part 11: Evaluation Tools for Persistent Association Technologies

- SDO/Group: ISO/IEC JTC 1/SC 29
- Link: [ISO/IEC TR 21000-11:2004](#)
- Status: Published
- Publication Date: 2004
- Media: Audio, Video

Summary: This standard provides tools for evaluating persistent association technologies. It includes guidelines for creating and maintaining evaluation files, which can be used to document the evaluation of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.24

IEEE Draft Standard for Evaluation Method of Robustness of Digital Watermarking Implementation in Digital Contents

- SDO/Group: IEEE
- Link: [IEEE P3361](#)
- Status: In progress
- Media: Any

Summary: This draft standard offers methods for evaluating the robustness of digital watermarking. It includes guidelines for creating and maintaining evaluation files, which can be used to document the evaluation of digital assets. This helps in ensuring that content is properly accounted for and can be easily identified and retrieved.

3.22 遠隔放射線診断における医用画像透かしの要件に関するレビュー

- SDO/グループ: NIH
- リンク: [Medical Image Watermarking](#)
- ステータス: 発行済み
- 発行日: 2012年
- メディア: 画像

概要: このレビューでは、遠隔放射線診断における医用画像への透かしの要件について概説します。また、医用画像への透かしの文書化に使用できる透かしファイルの作成と管理に関するガイドラインも含まれています。これにより、コンテンツが適切に管理され、容易に識別・取得できることが保証されます。

3.23 MPEG-21 – 第11部: 継続性連合技術の評価ツール

- SDO/グループ: ISO/IEC JTC 1/SC 29
- リンク: [ISO/IEC TR 21000-11:2004](#)
- ステータス: 発行済み
- 発行日: 2004年
- メディア: オーディオ, ビデオ

概要: この規格は、継続性連合技術を評価するためのツールを提供します。評価ファイルの作成と維持に関するガイドラインが含まれており、デジタル資産の評価を文書化するために使用できます。これにより、コンテンツが適切に管理され、容易に識別および取得できることが保証されます。

3.24 デジタルコンテンツにおける電子透かし実装の堅牢性評価方法に関するIEEE規格案

- SDO/グループ: IEEE
- リンク: [IEEE P3361](#)
- ステータス: 進行中
- メディア: 任意

概要: この規格案は、電子透かしの堅牢性を評価するための方法を提供します。評価ファイルの作成と維持に関するガイドラインが含まれており、デジタル資産の評価を文書化するために使用できます。これにより、コンテンツが適切に管理され、容易に識別・取得できることが保証されます。

3.25

H.MMAUTH: Framework for authentication of multimedia content

- **SDO/Group:** ITU-T SG21/Q9
- **Link:** [H.MMAUTH](#)
- **Status:** In progress
- **Media:** Video

Summary: This Draft Recommendation specifies a technical solution for the verification of multimedia content integrity, enabling users to confirm the authenticity of the content by its creators, such as governments, companies, or news organizations. The solution is based on the digital signing of data streams. The content creator (encoder) uses a private key to sign the content, while the recipient (decoder) uses a corresponding public key to verify the authenticity. The public key, necessary for verification, is not derived directly from the data stream but is obtained through a trusted, independent method, such as a third-party trust center.

3.26

H.274(V4): Versatile supplemental enhancement information messages for coded video bitstreams

- **SDO/Group:** JVET (ITU-T SG21 & ISO/IEC JTC 1/SC 29/ WG5)
- **Link:** [H.274\(V4\)](#)
- **Status:** In progress
- **Media:** Video

Summary: This specification contains changes to the versatile supplemental enhancement information messages for coded video bitstreams (VSEI) standard to specify additional SEI messages that will be useful for the purposes of content provenance, trust and authenticity.

3.27

H.VADS: Assessment criteria for video authenticity detection services

- **SDO/Group:** ITU-T SG21/Q7
- **Link:** [H.VADS](#)
- **Status:** In progress
- **Media:** Video

Summary: This Draft Recommendation provides a comprehensive assessment framework for video authenticity detection services. It specifies the requirements, assessment categories, key metrics, and methods to evaluate the capabilities of video authenticity detection services. By establishing a structured, criteria-based approach, this Draft Recommendation would guide the development, evaluation, and selection of reliable and effective video authenticity detection services.

3.25 H.MMAUTH: マルチメディアコンテンツの認証フレームワーク

- **SDO/グループ:** ITU-T SG21/Q9
- **リンク:** [H.MMAUTH](#)
- **ステータス:** 進行中
- **メディア:** ビデオ

概要: この勧告案は、マルチメディアコンテンツの完全性を検証するための専門的ソリューションを規定し、政府、企業、報道機関などのコンテンツ作成者によるコンテンツの真正性をユーザーが確認できるようにします。このソリューションは、データストリームのデジタル署名に基づいています。コンテンツ作成者（エンコーダ）は秘密鍵を使用してコンテンツに署名し、受信者（デコーダ）は対応する公開鍵を使用して真正性を検証します。検証に必要な公開鍵は、データストリームから直接取得されるのではなく、サードパーティのトラストセンターなどの信頼できる独立した方法を通じて取得されます。

3.26 H.274 (V4): 符号化ビデオビットストリーム用多用途補足拡張情報メッセージ

- **SDO/グループ:** JVET (ITU-T SG21 & ISO/IEC JTC 1/SC 29/WG5)
- **リンク:** [H.274 \(V4\)](#)
- **ステータス:** 進行中
- **メディア:** ビデオ

概要: この仕様は、符号化ビデオビットストリーム用多用途補足拡張情報メッセージ（VSEI）規格に対する変更を含み、コンテンツの出所、信頼性、および真正性の検証に役立つ追加のSEIメッセージを規定します。

3.27 H.VADS: ビデオ真正性検出サービスの評価基準

- **SDO/グループ:** ITU-T SG21/Q7
- **リンク:** [H.VADS](#)
- **ステータス:** 進行中
- **メディア:** ビデオ

概要: この勧告案は、ビデオ真正性検出サービスのための包括的な評価フレームワークを提供します。ビデオ真正性検出サービスの能力を評価するための要件、評価カテゴリー、主要な指標、および手法を規定しています。構造化された基準に基づくアプローチを確立することにより、この勧告案は、信頼性が高く効果的なビデオ真正性検出サービスの開発、評価、および選択の指針となります。

3.28 Credible Web

- **SDO/Group:** W3C
- **Link:** [Cred Web](#)
- **Status:** In progress
- **Media:** Web pages

Summary: The mission of the W3C Credible Web Community Group is to help shift the Web toward more trustworthy content without increasing censorship or social division. We want users to be able to tell when content is reliable, accurate, and shared in good faith, and to help them steer away from deceptive content. At the same time, we affirm the need for users to find the content they want and to interact freely in the communities they choose. To balance any conflict between these goals, we are committed to providing technologies which keep end-users in control of their Web experience.

3.29 Technical and Governance Guidelines for Responsible Data Collection

- **SDO/Group:** Alliance for Responsible Data Collection (ARDC)
- **Link:** [Technical and Governance Guidelines for Responsible Data Collection](#)
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Data

Summary: With the rapid expansion of online digital data, it is critical to establish responsible data collection standards that provide data collectors with guidance on best practices, provide third parties with a reliable means to assess whether the public web data they seek to use has been responsibly sourced, and protect public access to public data. The technical guidelines set forth below are part of a broader framework for responsible data collection that includes important guidelines for data collection governance. As such, all ARDC guidelines must be applied holistically. These standards build upon previous work by the FISD-SIA-Alternative Data Council on Web Data Collection Considerations.

3.28 信頼できるウェブ

- **SDO/グループ:** W3C
- **リンク:** [Cred Web](#)
- **ステータス:** 進行中
- **メディア:** ウェブページ

概要: W3C Credible ウェブコミュニティグループの使命は、検閲や社会の分断を助長することなく、ウェブをより信頼できるコンテンツへと移行させることです。私たちは、ユーザーが、コンテンツが信頼でき、正確で、誠意を持って共有されているかどうかを判断できるようにし、欺瞞的なコンテンツを避けることができるようにしたいと考えています。同時に、ユーザーが希望するコンテンツを見つけ、選択したコミュニティで自由に交流できる必要性を認識しています。これらの目標の両立を図るため、エンドユーザーが自らのウェブ体験をコントロールできる技術を提供することに尽力しています。

3.29 責任あるデータ収集のための専門的およびガバナンスガイドライン

- **SDO/グループ:** 責任あるデータ収集のためのアライアンス (ARDC)
- **リンク:** [Technical and Governance Guidelines for Responsible Data Collection](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** データ

概要: オンラインデジタルデータの急速な拡大に伴い、データ収集者にベストプラクティスに関するガイダンスを提供し、第三者が利用しようとする公開ウェブデータが責任ある方法で収集されたかどうかを評価するための信頼性の高い手段を提供し、公開データへの一般アクセスを保護する、責任あるデータ収集基準を確立することが極めて重要です。以下に示す専門的ガイドラインは、データ収集ガバナンスに関する重要なガイドラインを含む、責任あるデータ収集のためのより広範なフレームワークの一部です。したがって、ARDCのすべてのガイドラインは包括的に適用する必要があります。これらの規格は、FISD-SIA-オルタナティブデータ協議会によるウェブデータ収集に関する考慮事項に関する過去の取り組みに基づいています。

3.30 Data Provenance Standards

- **SDO/Group:** Data & Trust Alliance
- **Link:** [D&TA Data Provenance Standards v1.0.0](#)
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Data

Summary: The Data Provenance Standards are a set of guidelines developed by the Data & Trust Alliance to help organizations assess dataset quality, transparency, and legal usability for AI and traditional data applications. The standards aim to provide essential metadata about a dataset's origin, creation method, and legal usage, with the goal of increasing data trust and reducing risks in AI development.

3.31 IEEE Standard for Transparent Human and Machine Agency Identification

- **SDO/Group:** IEEE
- **Link:** [IEEE 3152-2024](#)
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Images, Audio

Summary: This standard addresses recognizable audio and visual markers that assist humans in distinguishing communication with a human, a machine, or a combination of both. Therefore, the standard defines visual, textual, and auditory marks. This standard does not cover methods to determine whether an interaction is with a machine, such as Turing tests.

3.32 IPTC Photo Metadata Standard

- **SDO/Group:** IPTC
- **Link:** [IPTC Photo Metadata Standard 2024.1](#)
- **Status:** Published
- **Publication Date:** 2024
- **Media:** Images, Video

Summary: This document specifies metadata properties with a focus on usage with photos, some of these properties are also specified by the IPTC Video Metadata Hub.

3.30 データ出所規格

- **SDO/グループ:** データ&トラスト・アライアンス
- **リンク:** [D&TA Data Provenance Standards v1.0.0](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** データ

概要: データ出所規格は、データ&トラスト・アライアンスが開発したガイドライン集であり、組織がAIおよび従来のデータアプリケーションにおけるデータセットの品質、透明性、法的利用可能性を評価するのに役立ちます。これらの規格は、データセットの出所、作成方法、法的利用に関する重要なメタデータを提供することで、データの信頼性を高め、AI開発におけるリスクを軽減することを目的としています。

3.31 人間と機械の透過性のあるエージェンシー識別のためのIEEE規格

- **SDO/グループ:** IEEE
- **リンク:** [IEEE 3152-2024](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** 画像, オーディオ

概要: この規格は、人間が人間、機械、または両者とのコミュニケーションを区別するのに役立つ、認識可能な音声および視覚マーカーを扱っています。したがって、この規格では、視覚、テキスト、および聴覚マーカーを定義します。この規格は、チューリングテストなど、機械とのインタラクションかどうかを判断する方法は扱っていません。

3.32 IPTC写真メタデータ規格

- **SDO/グループ:** IPTC
- **リンク:** [IPTC Photo Metadata Standard 2024.1](#)
- **ステータス:** 発行済み
- **発行日:** 2024年
- **メディア:** 画像, ビデオPTC

概要: この文書は、写真での使用に重点を置いたメタデータプロパティを規定しています。これらのプロパティの一部は、IPTCビデオメタデータハブでも規定されています。

3.33 DASH - Part 4: Segment Encryption and Authentication

- **SDO/Group:** ISO/IEC JTC 1/SC 29
- **Link:** [ISO/IEC 23009-4:2018](#)
- **Status:** Published
- **Publication Date:** 2018
- **Media:** Video

Summary: This standard introduces encryption and authentication mechanisms at the segment level for adaptive video streaming, which enhances content integrity and protects against tampering during media transmission. It complements existing watermarking and trust/authenticity standards, especially for streaming use cases.

3.34 Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies

- **SDO/Group:** IEEE SA
- **Link:** [P3429](#)
- **Status:** Published
- **Publication Date:** 2023
- **Media:** Any

Summary: This recommended practice offers a structured framework for understanding and classifying Artificial Intelligence Generated Content (AIGC). It defines rules and levels of AIGC technologies, outlines recommended practices for their implementation, and provides real-world use cases. This standard is highly relevant to the trust and authenticity domain, as it supports transparent communication of the origin, nature, and reliability of AI-generated content—an increasingly critical aspect of digital media governance.

3.33 DASH - 第4部: セグメント暗号化および認証

- **SDO/グループ:** ISO/IEC JTC 1/ SC 29
- **リンク:** [ISO/IEC 23009-4:2018](#)
- **ステータス:** 発行済み
- **発行日:** 2018年
- **メディア:** ビデオ

概要: この規格は、アダプティブビデオストリーミングにおけるセグメントレベルの暗号化および認証メカニズムを導入し、コンテンツの完全性を高め、メディア伝送中の改ざんを防止します。特にストリーミングのユースケースにおいて、既存の透かしおよび信頼性/真正性に関する規格を補完します。

3.34 人工知能生成コンテンツ技術のレベルに関する推奨プラクティス

- **SDO/グループ:** IEEE SA
- **リンク:** [P3429](#)
- **ステータス:** 発行済み
- **発行日:** 2023年
- **メディア:** 任意

概要: この推奨プラクティスは、人工知能生成コンテンツ(AIGC)を理解し、分類するための構造化されたフレームワークを提供します。この規格は、AIGC技術のルールとレベルを定義し、その実装に関する推奨プラクティスを概説し、実際のユースケースを示しています。この規格は、AI生成コンテンツの出所、性質、信頼性に関する透明性のあるコミュニケーションをサポートするため、信頼性と真正性の領域に非常に関連しています。これは、デジタルメディアガバナンスにおいてますます重要になっている側面です。

Section 04

STANDARDIZATION MAPPING

4.1 Standards & Specification Map

	Content Provenance	Trust Authenticity	Asset Identifiers	Rights Declarations	Watermarking	Other
Content Credentials	●	●			●	
JPEG Trust Part 1: Core foundation	●	●	●	●	●	
CAWG Metadata	●	●		●		
Originator Profile	●	●				
PROV	●	●				
IPTC Photo Metadata Standard	●	●		●		
JPEG Trust Part 2: Trust profiles catalog		●				
Overview of trustworthiness in artificial intelligence		●				
Framework for trust-based media services		●				
Trust.txt		●		●		
Chromium Reputation Provider Framework		●				
MPEG-21 – Part 11: Evaluation Tools for Persistent Association Technologies		●			●	
H.MMAUTH: Framework for authentication of multimedia content		●				
H.273(V4): Versatile supplemental enhancement information messages for coded video bitstreams		●				
H.VADS: Assesment criteria for video authenticity detection services		●				
DASH - Part 4: Segment Encryption and Authentication		●				
Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies		●				
JEPG Trust Part 3: Media asset watermarking					●	
Open Binding of Content Identifiers (OBID)			●		●	

第4章

標準化マッピング

4.1 規格と仕様のマップ

	コンテンツの出所	信頼性と真正性	資産識別子	権利宣言	透かし	その他
コンテンツ認証情報	●	●			●	
JPEG Trust 第1部: コア基盤	●	●	●	●	●	
CAWG メタデータ	●	●		●		
オリジネータープロフィール	●	●				
PROV	●	●				
IPTC写真メタデータ規格		●		●		
JPEG Trust 第2部: 信頼プロフィールカタログ		●				
人工知能における信頼性の概要		●				
信頼に基づくメディアサービスのためのフレームワーク		●				
Trust.txt		●		●		
クロミウムレピュテーションプロバイダフレームワーク		●				
MPEG-21 – 第11部: 継続性連合技術の評価ツール		●			●	
H.MMAUTH: マルチメディアコンテンツの認証フレームワーク		●				
H.274(V4): 符号化ビデオビットストリーム用多用途補足拡張情報メッセージ		●				
H.VADS: ビデオ真正性検出サービスの評価基準		●				
DASH - 第4部: セグメント暗号化および認証		●				
人工知能生成コンテンツ技術のレベルに関する推奨プラクティス		●				
JPEG Trust 第3部: メディア資産の透かし					●	
コンテンツ識別子のオープンバインディング(OBID)			●		●	

4.1 Standards & Specification Map (cont'd)



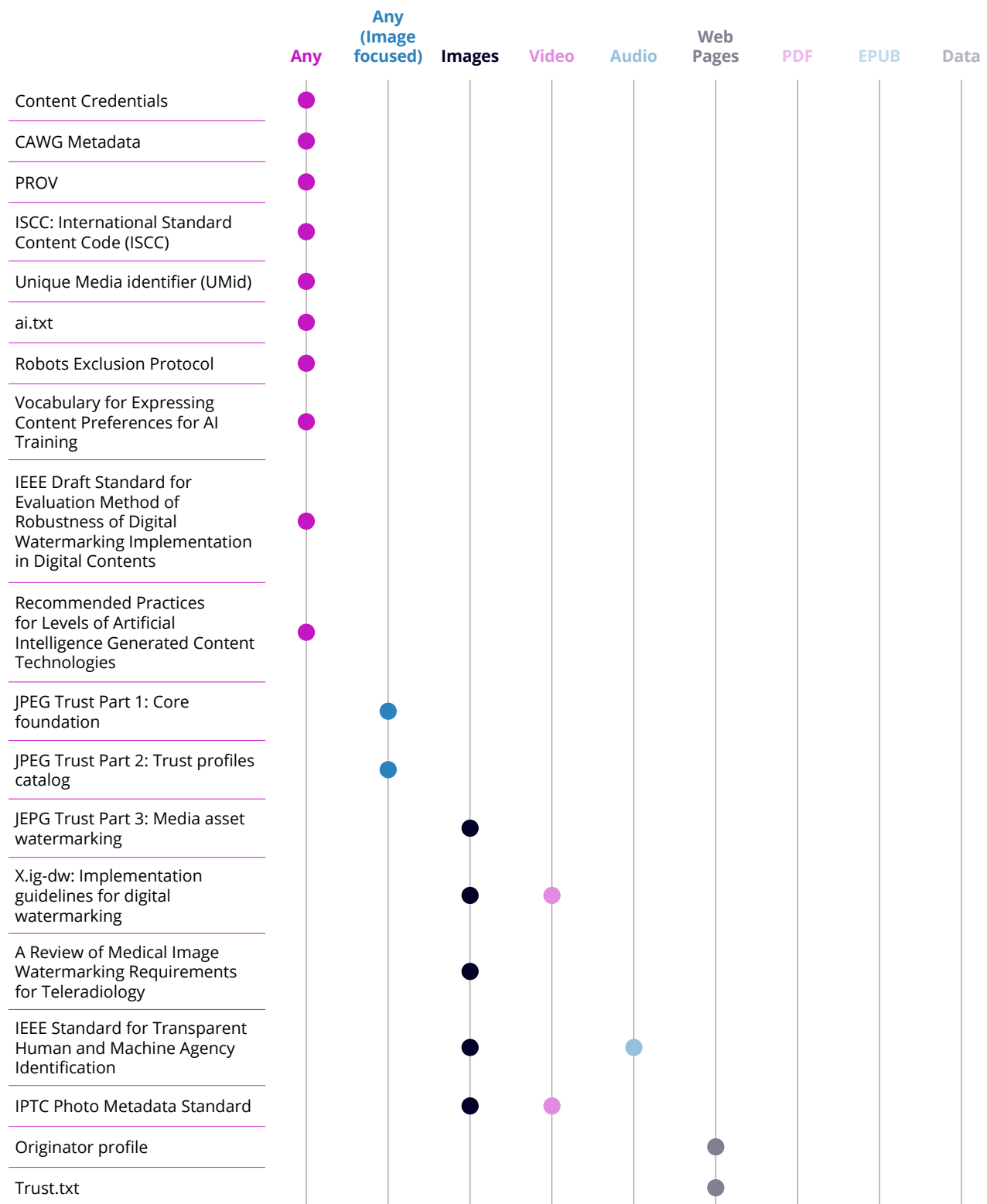
For an accessible table representation of this chart, see Annex A: Table of Standard & Specification Categorization.

4.1 規格と仕様のマップ(続き)

	コンテンツの出所	信頼性と真正性	資産識別子	権利宣言	透かし	その他
X.ig-dw: デジタル透かしの 実装ガイドライン					●	
遠隔放射線診断における医 用画像透かしの要件に関す るレビュー					●	
デジタルコンテンツにおける 電子透かし実装の堅牢性評 価方法に関するIEEE規格 案					●	
人間と機械の透過性のある エージェンシー識別のため のIEEE規格					●	
ISCC: 国際標準コンテン コード (ISCC)			●			
ユニークメディア識別子 (UMid)			●			
TDM予約プロトコル				●		
ai.txt				●		
Robots除外プロトコル				●		
AIトレーニング向けコンテン ツ選好表現語彙				●		
デジタル出版物のための DRM技術 第1部: 出版業界 で使用されている著作権保 護技術の概要				●		
信頼できるウェブ						●
責任あるデータ収集のための 専門的およびガバナンスガイ ドライン						●
データ出所規格						●

この表を分かりやすく表にしたものについては、「附属書A: 規格および仕様の分類表」をご覧ください。

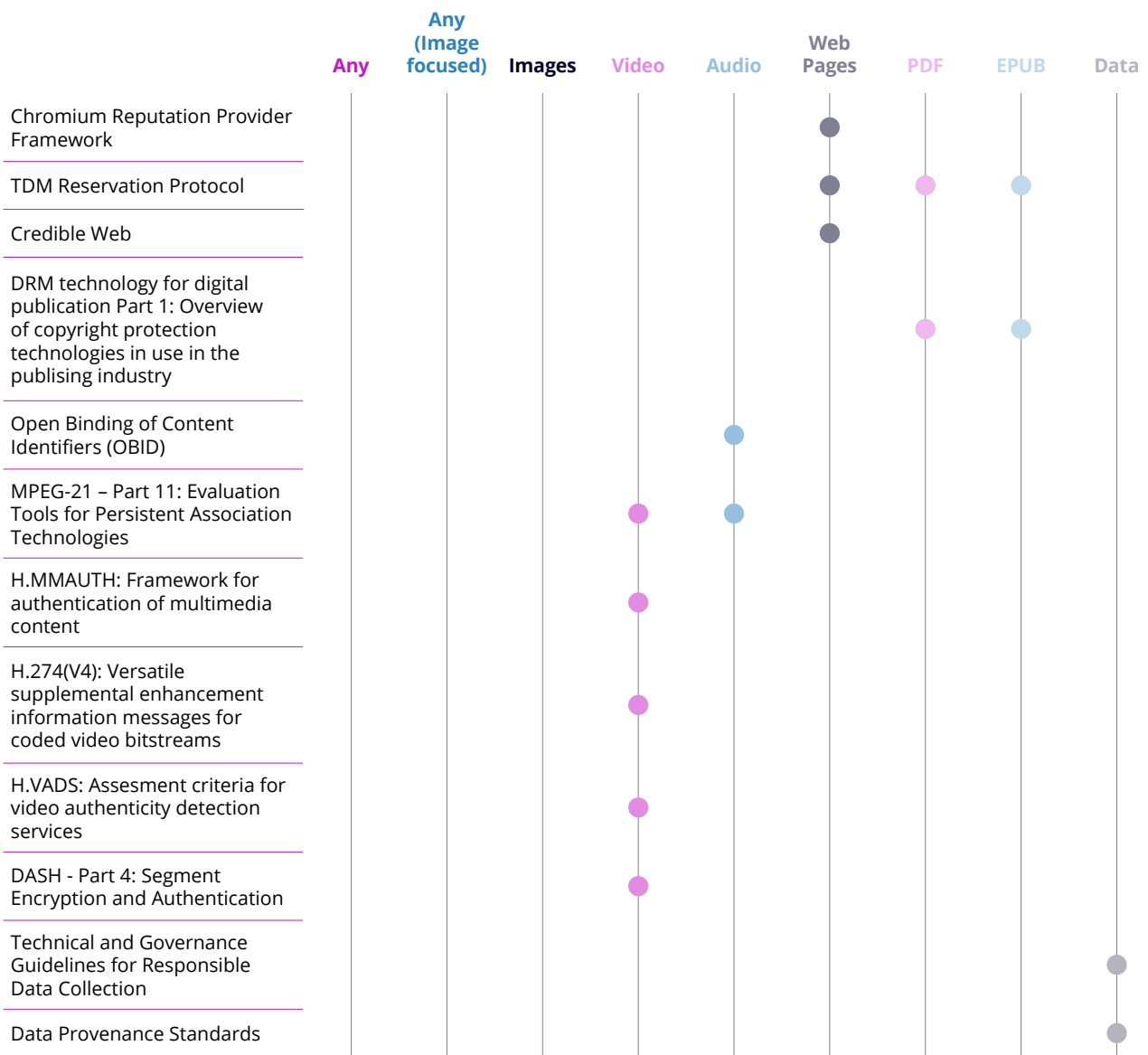
4.2 Media Type Support Map



4.2 メディアタイプサポートマップ

	任意	任意 (画像中心)	画像	ビデオ	オーディオ	ウェブ ページ	PDF	EPUB	データ
コンテンツ認証情報	●								
CAWGメタデータ	●								
PROV	●								
ISCC: 国際標準コンテンツ コード (ISCC)	●								
ユニークメディア識別子 (UMid)	●								
ai.txt	●								
Robots排除プロトコル	●								
AIトレーニング向けコンテン ツ選好表現語彙	●								
デジタルコンテンツにおける 電子透かし実装の堅牢性評 価方法に関するIEEE規格 案	●								
人工知能生成コンテンツ技 術のレベルに関する推奨プ ラクティス	●								
JPEG Trust 第1部: コア基 盤		●							
JPEG Trust 第2部: 信頼プ ロファイルカタログ		●							
JPEG Trust 第3部: メディア 資産の透かし			●						
X.ig-dw: デジタル透かしの 実装ガイドライン			●	●					
遠隔放射線診断における医 用画像透かしの要件に関す るレビュー			●						
人間と機械の透過性のある エージェンシー識別のため のIEEE規格			●		●				
IPTC写真メタデータ規格			●	●					
オリジネータープロフィール						●			
Trust.txt						●			

4.2 Media Type Support Map (cont'd)



For an accessible table representation of this chart, see Annex B: Table of Media Type Support.

4.2 メディアタイプサポートマップ(続き)

	任意	任意 (画像中心)	画像	ビデオ	オーディオ	ウェブ ページ	PDF	EPUB	データ
クロミウムレピュテーション ロバイダフレームワーク						●			
TDM予約プロトコル						●	●	●	
信頼できるウェブ						●			
デジタル出版物のための DRM技術 第1部:出版業界 で使用されている著作権保護 技術の概要							●	●	
コンテンツ識別子のオープン バインディング (OBID)					●				
MPEG-21 – 第11部:継続 性連合技術の評価ツール				●	●				
H.MMAUTH: マルチメディ アコンテンツの認証フレーム ワーク				●					
H.274 (V4): 符号化ビデオ ビットストリーム用多用途補 足拡張情報メッセージ				●					
H.VADS:ビデオ真正性検出 サービスの評価基準				●					
DASH - 第4部:セグメント暗 号化および認証				●					
責任あるデータ収集のための 専門的およびガバナンスガイ ドライン									●
データ出所規格									●

この表のアクセス可能な表形式については、附属書B「メディア種別のサポート表」を参照してください。

Section 05

RELATED STANDARDS

In addition to the core standards discussed in this report, several related areas of standardization play a significant role in supporting digital media authenticity. These standards address foundational technologies and practices that complement the main categories of content provenance, trust and authenticity, asset identifiers, rights declarations, and watermarking.

Blockchain and Distributed Ledger Technologies

Blockchain and Distributed Ledger Technologies (DLT) provide a well-established approach to decentralized, tamper-evident ledgers that can be used to record information about the provenance and integrity of digital assets. By leveraging cryptographic techniques, these technologies enable transparent and immutable records of content creation, modification, and transfer. Standards such as those from ISO TC 307 (Blockchain and distributed ledger technologies) and the W3C (e.g., Verifiable Credentials and DIDs) are increasingly referenced in digital media workflows.

Identity Standards

Robust digital identity standards are essential for establishing the authenticity of content creators, both human and organizational. Efforts emanating from organizations such as the Decentralized Identity Foundation (DIF) and its Creator Assertion Working Group (CAWG, <https://cawg.io/identity/1.1/>) allow for secure and privacy-preserving identification while enabling features such as attribution of digital assets.

Rights Declarations

It is important to establish a flexible, machine-readable framework for expressing permissions, prohibitions, and obligations associated with digital content. Standards such as the Open Digital Rights Language (ODRL), standardized by the W3C, enable rights holders to specify how their content may be used, shared, or restricted, supporting automated rights management and compliance across diverse platforms and services.

Creative Commons

Creative Commons (CC) licenses are widely adopted for the standardized declaration of usage rights for digital content. The CC framework provides a suite of licenses that allow creators to communicate permissions and restrictions in a clear, interoperable manner.

Supply Chain Integrity, Transparency, and Trust

Supply Chain Integrity, Transparency, and Trust (SCITT) is an emerging initiative led by the IETF, focuses on establishing standards for the secure and transparent tracking of digital assets throughout their lifecycle. SCITT aims to provide mechanisms for recording, verifying, and auditing actions taken on digital content, enhancing supply chain integrity and supporting trust in digital ecosystems. This is particularly relevant for complex media workflows involving multiple stakeholders and distribution channels.

第5章

関連規格

本報告書で解説したコア規格に加え、デジタルメディアの真正性を支える上で重要な役割を果たす、いくつかの関連標準化分野があります。これらの規格は、コンテンツの出所、信頼性と真正性、資産識別子、権利宣言、透かしといった主要カテゴリーを補完する基盤技術とプラクティスを扱っています。

ブロックチェーンと分散台帳技術

ブロックチェーンと分散台帳技術(DLT)は、デジタル資産の出所と完全性に関する情報を記録するために使用できる、分散の改ざん防止型台帳への確立されたアプローチを提供します。これらの技術は、暗号技術を活用することで、コンテンツの作成、変更、および転送に関する透明性と不変性のある記録を可能にします。ISO TC 307(ブロックチェーンおよび分散台帳技術)やW3C(検証可能な認証情報やDIDなど)などの標準は、デジタルメディアのワークフローにおいてますます参照されるようになっています。

アイデンティティ規格

堅牢なデジタルアイデンティティ規格は、個人および組織のコンテンツ作成者の真正性を確立するために不可欠です。Decentralized Identity Foundation(DIF)やそのCreator Assertion Working Group(CAWG, <https://cawg.io/identity/1.1/>)などの組織による取り組みにより、安全かつプライバシーを保護した識別が可能になるとともに、デジタル資産の帰属表示などの機能も実現されています。

権利宣言

デジタルコンテンツに関連する許可、禁止事項、義務を表現するための、柔軟で機械可読なフレームワークを確立することが重要です。W3Cによって標準化されたOpen Digital Rights Language(ODRL)などの規格により、権利者はコンテンツの使用方法、共有方法、制限方法を指定でき、多様なプラットフォームやサービスにおける自動的な権利管理とコンプライアンスを実現できます。

クリエイティブ・コモンズ

クリエイティブ・コモンズ(CC)ライセンスは、デジタルコンテンツの使用権に関する標準化された宣言として広く採用されています。CCフレームワークは、クリエイターが明確かつ相互運用可能な方法で許可と制限事項を伝えることができるライセンススイートを提供します。

サプライチェーンの完全性、透明性、および信頼性

サプライチェーンの完全性、透明性、そして信頼性(SCITT)は、IETFが主導する新たなイニシアチブであり、デジタル資産のライフサイクル全体にわたる安全で透明な追跡のための規格を確立することに重点を置いています。SCITTは、デジタルコンテンツに対するアクションを記録、検証、監査するためのメカニズムを提供し、サプライチェーンの完全性を高め、デジタルエコシステムにおける信頼性をサポートすることを目指しています。これは、複数のステークホルダーと配信チャンネルが関与する複雑なメディアワークフローに特に関連しています。

Section 06

CONCLUSION AND NEXT STEPS

Through the categorization of these existing specifications and standards into key areas, we have highlighted their critical role in fostering trust, accountability, and integrity in the digital ecosystem. The findings underscore the importance of continued collaboration among Standard Development Organizations (SDOs), industry stakeholders, and researchers to address existing gaps and emerging challenges.

As next steps, it is essential to focus on the harmonization of overlapping standards and the development of interoperable frameworks that can be widely adopted across industries. Emerging areas of work, such as the integration of decentralized technologies for enhanced provenance management and the exploration of new watermarking techniques for synthetic media, present exciting opportunities for innovation. Additionally, fostering awareness and adoption of these specifications and standards through education, advocacy, and pilot implementations will be crucial in ensuring their effectiveness and impact.

The evolving nature of digital media and AI technologies necessitates a proactive approach to standardization. By staying ahead of technological advancements and fostering a collaborative ecosystem, we can build a robust foundation for the authenticity and trustworthiness of digital content in the years to come.

第6章

結論と次のステップ

これらの既存の仕様と規格を主要分野に分類することで、デジタルエコシステムにおける信頼性、説明責任、そして完全性を促進する上でこれらの重要な役割を明らかにしました。この結果は、既存のギャップと新たな課題に対処するために、規格開発団体(SDO)、業界のステークホルダー、そして研究者間の継続的な協力の重要性を強調しています。

次のステップとして、重複する規格の調和と、業界を超えて広く採用できる相互運用可能なフレームワークの開発に重点を置くことが不可欠です。分散技術の統合による出所管理の強化や、合成メディア向けの新しい透かし技術の探求といった新たな取り組み分野は、イノベーションの刺激的な機会を提供します。さらに、教育、啓発活動、パイロット導入を通じて、これらの仕様や規格の認知度向上と普及を促進することは、その有効性と影響力を確保する上で不可欠です。

デジタルメディアとAI技術は進化を続けているため、標準化への積極的なアプローチが不可欠です。技術革新を先取りし、協調的なエコシステムを構築することで、今後数年間にわたり、デジタルコンテンツの真正性と信頼性を確保するための強固な基盤を構築することができます。

ANNEX A: TABLE OF STANDARD & SPECIFICATION CATEGORIZATION

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking	Other
Content Credentials	x	x			x	
Content Credentials	x	x				
JPEG Trust Part 1: Core foundation	x	x	x	x	x	
JPEG Trust Part 2: Trust profiles catalog		x				
JPEG Trust Part 3: Media asset watermarking					x	
CAWG Metadata	x	x		x		
Originator Profile	x	x				
PROV	x	x				
Overview of trustworthiness in artificial intelligence		x				
Framework for trust-based media services		x				
Trust.txt		x				
Chromium Reputation Provider Framework		x		x		
ISCC: International Standard Content Code (ISCC)						
Unique Media Identifier (UMid)			x			
TDM Reservation Protocol				x		
ai.txt				x		
Robots Exclusion Protocol (Robots.txt)				x		

附属書A: 規格および仕様の分類表

仕様	コンテンツの出所	信頼性と真正性	資産識別子	権利宣言	透かし	その他
コンテンツ認証情報	X	X			X	
コンテンツ認証情報	X	X				
JPEG Trust 第1部: コア基盤	X	X	X	X	X	
JPEG Trust 第2部: 信頼プロファイルカタログ		X				
JPEG Trust 第3部: メディア資産の透かし					X	
CAWG メタデータ	X	X		X		
オリジネータープロファイル	X	X				
PROV	X	X				
人工知能における信頼性の概要		X				
信頼に基づくメディアサービスのためのフレームワーク		X				
Trust.txt		X				
クロミウムレピュテーションプロバイダフレームワーク		X		X		
ISCC: 国際標準コンテンツコード (ISCC)						
ユニークメディア識別子 (UMid)			X			
TDM予約プロトコル				X		
ai.txt				X		
Robots排除プロトコル (Robots.txt)				X		

ANNEX A: TABLE OF STANDARD & SPECIFICATION CATEGORIZATION (CONT'D)

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking	Other
Vocabulary for Expressing Content Preferences for AI Training				x		
Open Binding of Content Identifiers (OBID)			x		x	
X.ig-dw: Implementation guidelines for digital watermarking					x	
DRM technology for digital publications						
Part 1: Overview of copyright protection technologies in use in the publishing industry				x		
A Review of Medical Image Watermarking Requirements for Teleradiology					x	
MPEG-21 — Part 11: Evaluation Tools for Persistent Association Technologies		x			x	
IEEE Draft Standard for Evaluation Method of						
Robustness of Digital Watermarking Implementation in Digital Contents					x	
H.MMAUTH: Framework for authentication of multimedia content		x				
H.274(V4): Versatile supplemental enhancement information messages for coded video bitstreams		x				
H.VADS: Assessment criteria for video authenticity detection services		x				
Credible Web						x

附属書A: 規格および仕様の分類表(続き)

仕様	コンテンツの出所	信頼性と真正性	資産識別子	権利宣言	透かし	その他
AIトレーニング向けコンテンツ選好表現語彙				X		
コンテンツ識別子のオープンバイディング (OBID)			X		X	
X.ig-dw: デジタル透かしの実装ガイドライン					X	
デジタル出版物のためのDRM技術 第1部: 出版業界で使用されている著作権保護技術の概要						
遠隔放射線診断における医用画像透かしの要件に関するレビュー				X		
MPEG-21 – 第11部: 継続性連合技術の評価ツール					X	
デジタルコンテンツにおける電子透かし実装の堅牢性評価方法に関するIEEE規格案		X			X	
H.MMAUTH: マルチメディアコンテンツの認証フレームワーク						
H.274 (V4): 符号化ビデオビットストリーム用多用途補足拡張情報メッセージ					X	
H.VADS: ビデオ真正性検出サービスの評価基準		X				
信頼できるウェブ		X				
AIトレーニング向けコンテンツ選好表現語彙		X				
コンテンツ識別子のオープンバイディング (OBID)						X

ANNEX A: TABLE OF STANDARD & SPECIFICATION CATEGORIZATION (CONT'D)

Specification	Content Provenance	Trust and Authenticity	Asset Identifiers	Rights Declarations	Watermarking	Other
Technical and Governance Guidelines for Responsible Data Collection						x
Data Provenance Standards						x
IEEE Standard for Transparent Human and Machine Agency Identification					x	
IPTC Photo Metadata Standard	x	x		x		
DASH - Part 4: Segment Encryption and Authentication		x				
Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies		x				
Levels of Artificial Intelligence Generated Content Technologies		x				

附属書A: 規格および仕様の分類表(続き)

仕様	コンテンツの出所	信頼性と真正性	資産識別子	権利宣言	透かし	その他
責任あるデータ収集のための専門的およびガバナンスガイドライン						X
データ出所規格						X
人間と機械の透過性のあるエージェンシー識別のためのIEEE規格					X	
IPTC写真メタデータ標準	X	X		X		
DASH - 第4部: セグメント暗号化および認証		X				
人工知能生成コンテンツ技術のレベルに関する推奨プラクティス		X				
人工知能生成コンテンツ技術のレベル		X				

ANNEX B: TABLE OF MEDIA TYPE SUPPORT

Standard	Audio	Data	EPUB	Images	PDF	Video	Web Pages	Others
Content Credentials	x	x	x	x	x	x	x	x
Content Credentials	x	x	x	x	x	x	x	x
JPEG Trust Part 1: Core foundation	x	x	x	x	x	x	x	x
JPEG Trust Part 2: Trust profiles catalog	x	x	x	x	x	x	x	x
JPEG Trust Part 3: Media asset watermarking				x				
CAWG Metadata	x	x	x	x	x	x	x	x
Originator Profile							x	
PROV	x	x	x	x	x	x	x	x
Overview of trustworthiness in artificial intelligence								
Framework for trust-based media services								
Trust.txt							x	
Chromium Reputation Provider Framework							x	
ISCC: International Standard Content Code (ISCC)	x	x	x	x	x	x	x	x
Unique Media Identifier (UMid)	x	x	x	x	x	x	x	x
TDM Reservation Protocol			x		x		x	
ai.txt	x	x	x	x	x	x	x	x

附属書B: メディア種別のサポート表

規格	オーディオ	データ	EPUB	画像	PDF	ビデオ	ウェブページ	その他
コンテンツ認証情報	X	X	X	X	X	X	X	X
コンテンツ認証情報	X	X	X	X	X	X	X	X
JPEG トラスト パート1: コア基盤	X	X	X	X	X	X	X	X
JPEG トラスト パート2: トラストプロファイルカタログ	X	X	X	X	X	X	X	X
JPEG トラスト パート3: メディア資産透かし				X				
CAWGメタデータ	X	X	X	X	X	X	X	X
オリジネータープロファイル							X	
PROV	X	X	X	X	X	X	X	X
人工知能における信頼性の概要								
信頼に基づくメディアサービスのためのフレームワーク								
Trust.txt							X	
Chromiumレピュテーションプロバイダフレームワーク							X	
ISCC: 国際標準コンテンツコード (ISCC)	X	X	X	X	X	X	X	X
ユニークメディア識別子 (UMid)	X	X	X	X	X	X	X	X
TDM予約プロトコル			X		X		X	
ai.txt	X	X	X	X	X	X	X	X

ANNEX B: TABLE OF MEDIA TYPE SUPPORT (CONT'D)

Standard	Audio	Data	EPUB	Images	PDF	Video	Web Pages	Others
Robots Exclusion Protocol (Robots.txt)	x	x	x	x	x	x	x	x
Vocabulary for Expressing Content Preferences for AI Training	x	x	x	x	x	x	x	x
Open Binding of Content Identifiers (OBID)	x							
X.ig-dw: Implementation guidelines for digital watermarking				x		x		
DRM technology for digital publications								
Part 1: Overview of copyright protection technologies in use in the publishing industry			x		x			
A Review of Medical Image Watermarking Requirements for Teleradiology				x				
MPEG-21 — Part 11: Evaluation Tools for Persistent Association Technologies	x					x		
IEEE Draft Standard for Evaluation Method of								
Robustness of Digital Watermarking Implementation in Digital Contents	x	x	x	x	x	x	x	x
H.MMAUTH: Framework for authentication of multimedia content						x		

附属書B: メディア種別のサポート一覧(続き)

規格	オーディオ	データ	EPUB	画像	PDF	ビデオ	ウェブページ	その他
Robots排除プロトコル (Robots.txt)	X	X	X	X	X	X	X	X
AIトレーニング向けコンテ ンツ選好表現語彙	X	X	X	X	X	X	X	X
コンテンツ識別子のオー プンバインディング (OBID)	X							
X.ig-dw: デジタル透かし の実装ガイドライン				X		X		
デジタル出版物のための DRM技術								
第1部: 出版業界で使用さ れている著作権保護技術 の概要			X		X			
遠隔放射線診断における 医用画像透かしの要件に 関するレビュー				X				
MPEG-21 – 第11部: 継 続性連合技術の評価ツ ール	X					X		
IEEEデジタルコンテンツ における電子透かし実装 の堅牢性評価方法に関す るIEEE規格案	X	X	X	X	X	X	X	X
H.MMAUTH: マルチメデ ィアコンテンツの認証フ レームワーク						X		

ANNEX B: TABLE OF MEDIA TYPE SUPPORT (CONT'D)

Standard	Audio	Data	EPUB	Images	PDF	Video	Web Pages	Others
H.274(V4): Versatile supplemental enhancement information messages for coded video bitstreams						x		
H.VADS: Assessment criteria for video authenticity detection services						x		
Credible Web							x	
Technical and Governance Guidelines for Responsible Data Collection		x						
Data Provenance Standards		x						
IEEE Standard for Transparent Human and Machine Agency Identification	x			x				
IPTC Photo Metadata Standard				x		x		
DASH - Part 4: Segment Encryption and Authentication						x		
Recommended Practices for Levels of Artificial Intelligence Generated Content Technologies	x	x	x	x	x	x	x	x
Levels of Artificial Intelligence Generated Content Technologies	x	x	x	x	x	x	x	x

附属書B: メディア種別のサポート一覧(続き)

規格	オーディオ	データ	EPUB	画像	PDF	ビデオ	ウェブページ	その他
H.274(V4): 符号化ビデオビットストリーム用多用途補足拡張情報メッセージ						X		
H.VADS: ビデオ真正性検出サービスの評価基準						X		
信頼できるウェブ							X	
責任あるデータ収集のための専門的およびガバナンスガイドライン		X						
データ出所規格		X						
人間と機械の透過性のあるエージェンシー識別のためのIEEE規格	X			X				
IPTC写真メタデータ標準				X		X		
DASH - 第4部: セグメント暗号化および認証						X		
人工知能生成コンテンツ技術のレベルに関する推奨プラクティス	X	X	X	X	X	X	X	X
人工知能生成コンテンツ技術のレベル	X	X	X	X	X	X	X	X



© 2025 International Electrotechnical Commission (IEC), International Organization for Standardization (ISO), and International Telecommunication Union (ITU), some rights reserved

This publication is made available under the Creative Commons Attribution-NonCommercial 3.0 IGO (CC BY-NC 3.0 IGO) license. The full text of the license is available at <https://creativecommons.org/licenses/by-nc/3.0/igo/deed.en>

You are permitted to:

- Share — copy and redistribute the material in any medium or format.
- Adapt — remix, transform, and build upon the material.

Under the following terms:

- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- NonCommercial — You may not use the material for commercial purposes.

For any use that is not permitted by this license, including all commercial use rights, requests and inquiries should be addressed to the International Telecommunication Union (ITU), which is administering the copyright on behalf of the World Standards Cooperation partners for this publication.



ISBN 978-2-8399-4720-6



© 2025 国際電気標準会議 (IEC), 国際標準化機構 (ISO), 国際電気通信連合 (ITU), 一部の権利は留保されています。

この発行物は、クリエイティブ・コモンズ 表示-非営利 3.0 IGO (CC BY-NC 3.0 IGO) ライセンスに基づいて提供されています。ライセンスの全文は <https://creativecommons.org/licenses/by-nc/3.0/igo/deed.en> でご覧いただけます。

以下の行為が許可されます。

- ・ 共有 — あらゆる媒体または形式で資料を複製および再配付すること。
- ・ 翻案 — 資料をリミックス、変形、および活用すること。

以下の条件に基づきます。

- ・ 帰属表示 — 適切なクレジットを付与し、ライセンスへのリンクを提供し、変更があった場合はその旨を明記する必要があります。これらの行為は、合理的な方法であればどのような方法で行っても構いませんが、ライセンサーがあなたまたはあなたの使用を推奨していると示唆するような方法は禁止されています。
- ・ 非営利 — 本資料を営利目的で使用することはできません。

本ライセンスで許可されていない使用 (商用利用権を含む) については、国際電気通信連合 (ITU) までお問い合わせください。ITU は、本出版物の著作権を世界標準協力のパートナーを代表して管理しています。



本文書は経済産業省の委託事業の成果です。
© JISC/JSA 2025

記載内容の一部及び全てについて無断で編集、
改編、販売、翻訳、変造することを固く禁じます。

ISBN 978-2-8399-4720-6