

# Originator Profile 技術のご紹介

Originator Profile 技術研究組合 (OP CIP)

<https://originator-profile.org/ja-JP/>



# 現在のOPの対象領域

---

- Webで展開されるメディアの偽誤情報(Misinformation/disinformation) 対策
  - 新聞、テレビ
- アドフraud等、デジタル広告における問題の低減化

# WebにOPがもたらすもの

---

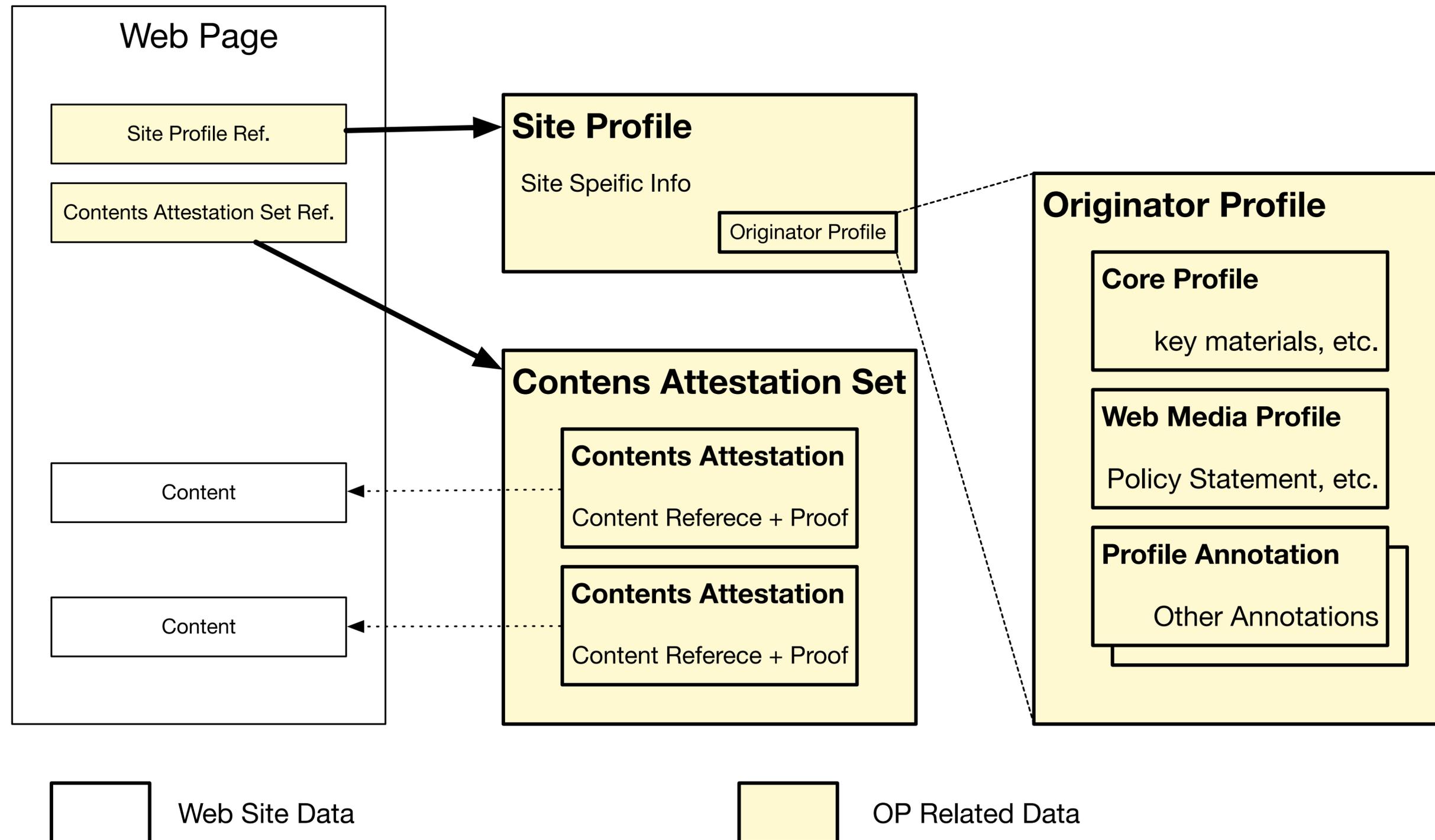
- テキストやメディアの断片 — Content (コンテンツ) — に対し **Content Attestation (CA - コンテンツ証明)** を付与、CAにより、発信元(Originator)と、真正性を確認できる
- Content(+CA)の発信元(Originator)が《**だれか**》そして《**どのような者か**》を検証可能とする情報を **Originator Profile (OP - オリジネータプロフィール)** として表現
  - OP、すなわち発信元についての情報は、デジタルアイデンティティ

# 構成要素

---

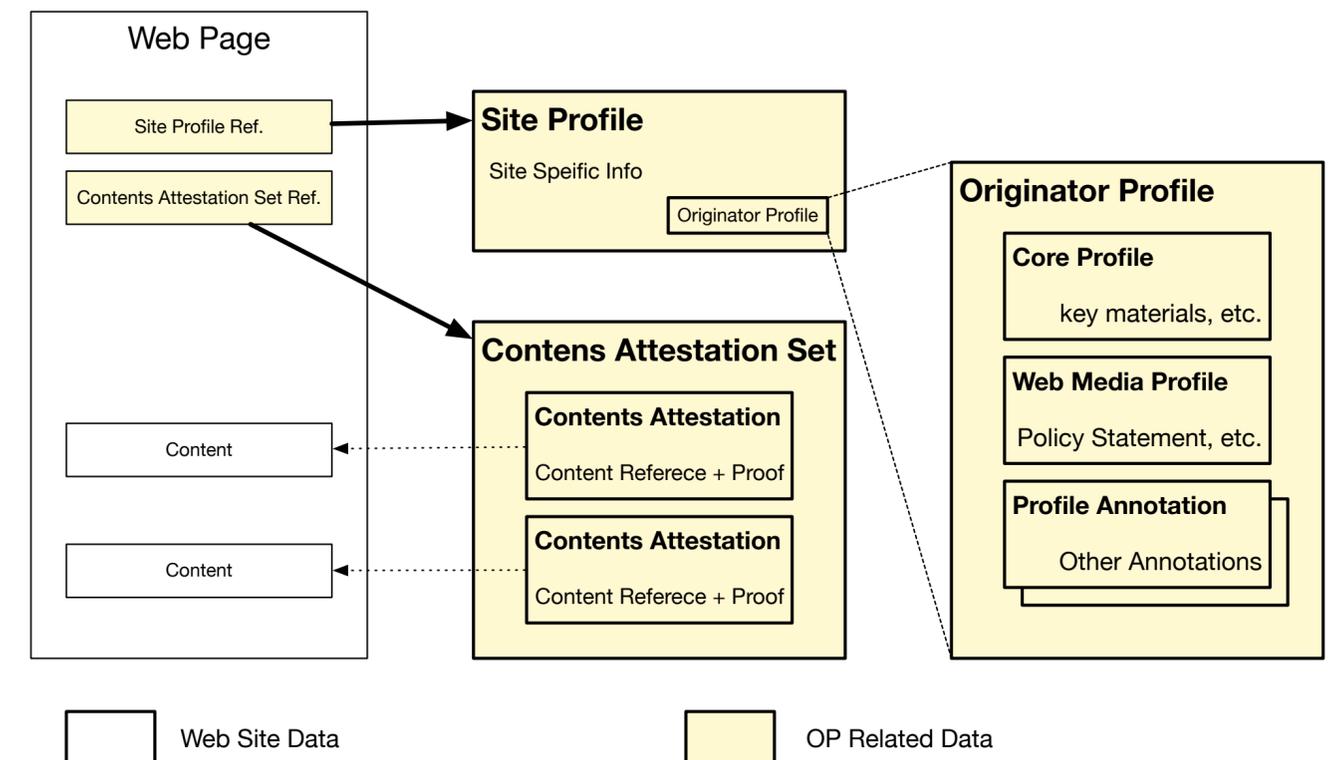
- 共通仕様と実装（対象アプリケーションに非依存）
  - アイデンティティ
  - データモデル
  - ガバナンスモデルのベースデザイン
- 対象アプリケーション領域向けの固有の仕様と実装
  - ウェブコンテンツの真正性確認
  - ウェブコンテンツ向けのユーザインターフェース（プレゼンテーション）

# ウェブコンテンツの真正性確認におけるデータモデル



# ウェブコンテンツの真正性確認におけるデータモデル

- **Originator Profile** には、Core Profile、Web Media Profile、加えて、1つ以上の Profile Annotation で構成される
- 保護される各コンテンツには、**Content Attestation** (CA - コンテント証明) を付与する
- それぞれの情報は柔軟に配置・配信できる



# アイデンティティ

- Originator Profileには、情報発信元についての、人が読むため及び機械解釈に向けた情報を、検証可能な形で格納している。
  - すなわち、検証可能なデジタルアイデンティティ (Verifiable Identity<sup>[1]</sup>)を提供
  - ウェブメディアなどのユースケース固有のプロファイルは、コアと分離され、拡張が容易
- 以下の要素で構成される:
  - **Core Profile:** 発信者がコンテンツ発信に使用する**公開鍵等の基本情報**
    - 最小化されており、DNS RRに保存することも可能
  - **Web Media Profile:** ウェブメディアのユースケースのための付加情報
    - 例えば発信者のポリシー声明、連絡先の情報等
  - **Profile Annotation:** 追加情報、潜在的に第三者によって発行されたもの（抽象モデル）
    - エンティティ実在証明（発信者についての情報）
    - 様々な認証機関によって付与される認証についての情報
    - 様々な組織の会員資格証明
    - その他、あらゆる種類のタグ・ラベル付与

[1] Trusted Webホワイトペーパー Ver.3.0 実装編

<https://trustedweb.go.jp/documents/>

# ウェブ向けのユーザインターフェース

---

- 現在、ブラウザ拡張として実装
- ブラウザ拡張は、拡張のボタンを押すと動作を開始
  - 現在のバージョンでは、ボタンを押すまではOPの処理は行わない

# ガバナンスの基礎を提供するフレームワーク

---

- 初期展開段階におけるOP発行者
  - Core Profile、Web Media Profile、Organization Profile（実在性検証を含む）は、OP立ち上げ時は、OP技術研究組合から発行
  - 日本の新聞については、会員証明を日本新聞協会から発行
  - ユースケースごとに認証機関を追加
    - 例えば、地方自治体プロフィールについては政府（例えば総務省等）の発行が考えられる
- 注意: ガバナンスフレームワークはデザインとして提供するが、将来にわたってOP技術研究組合が権威をもって発行を担うことは目指していない

# 発信者に対する情報付与と機械処理

- OPは《どのような発信者か》を柔軟に付与し、機械処理に用意に使えるフレームワーク
  - Profile Annotationは、誰でもコアプロファイル（対象組織）に対して発行できる
  - 対象組織（コアプロファイルの所有者）は OP配布時に含むProfile Annotationを選ぶことができる（署名はOPの要素ごとでありOP全体が署名されているわけではない）
- OPを活用する者は、以下のような手順でOPで示される情報発信者の情報を受け入れるか拒否するかを決定することができる → ある種のシグナリングメカニズム
  - 事前に、活用するProfile Annotationを検討する
    - どのProfile Annoation発行者を受け入れるのかを決める（例: 新聞協会）
    - 当該発行者による、どのようなProfile Annotationを受け入れるか決める（例: 新聞協会の会員証明）
  - OPを検証し、かつ、活用するProfile Annotationが付与されていることを確認し、必要に応じて活用する

# OPが埋める穴

---

- OP vs X.509 PKI
  - X.509 はガバナンスに関してスケーラビリティや柔軟性を提供しない
    - 通常、様々なポリシーがX.509ツリーの根元に適用される
    - 小規模グループではポリシーの微調整が不可能であるため不向き
      - コミュニティ規模のスケーラビリティが無い
  - スケーラビリティの課題 (OCSP?)

# 開発状況

---

- 初期開発完了、機能調整中
- 展開フェーズ1：少数のメディアからの発信で実用化
  - 2025年初頭
- 展開フェーズ2：アグリゲーター経由のアウトレット、デジタル広告
  - 2025年
  - 追加機能
    - IDの柔軟性を上げる（キーローテーションむ）
    - OPデータ配置の柔軟性の向上
    - 静的ウェブサイト向けの機能が完成
- 展開フェーズ3：地方自治体の情報発信
  - 2025年

...

# お話ししたこと

---

- 現在のOPの対象領域
- 部品:
  - 共通技術（アイデンティティ/データモデル/ユーザインタフェース）  
+ 基本ラインガバナンスモデル
  - ウェブコンテンツの特定コンポーネント
- 発信者に対する情報付与と機械処理
- OPが埋めるギャップ
- 開発状況