ORIGINATOR PROFILE | Tech Community

Originator Profile Tech Meetup #01

動き出した Originator Profile

新聞社・自治体・CMSの実装事例と
実装を支えるサービス



2026.10.27 (Tue)

#optech

ORIGINATOR PROFILE | Tech Community



Originator Profile Tech Meetup #01

#optech

Originator Profile 技術概要

Originator Profile Tech Meetup #01

2026/10/27, ASAI Tomoya, WebDINO Japan

「デジタル空間にもっと信頼を。」の技術概要

エンジニア目線で見る「デジタル空間の信頼確保技術提案」

- 本セッションではエンジニア目線での技術概要をお話しします
  - エンジニア(個人の)視点で見る **Web 技術動向と OP 技術への期待**
  - 提案者・仕様設計者として概説する **OP 技術の仕組みと設計**
- OPの目指すデジタル空間、解決する課題などは軽く触れるのみとします
  - 本日は **"Tech"** Meetup であり社会課題や社会的ビジョン説明は以下を参照
  - **OPのある社会**「信頼できる情報社会」を目指して
    https://originator-profile.org/ja-JP/vision/
  - **Originator Profile が解決する課題**
    https://originator-profile.org/ja-JP/problem-solving/

詳細設計の判断、応用技術の想定、他技術連携など、深掘りトピックは別の機会に

Vision & Potential











報道機関を装った偽のニュースや 偽の広告
広告詐欺、フィッシング詐欺などの拡散を抑止するなど

OPが解決する課題: https://originator-profile.org/ja-JP/problem-solving/

OPによって実現できること

現実社会では、私たちは「誰が言っているか」「その人は誰にどう認識されているか」を重視し、その内容を判断します。
OPは、これを情報空間でも実現します。



- **社会の中で認識されている組織が コンテンツ作成者の実在を確認（太鼓判）**
- **コンテンツ作成者が誰か、どのような者か**
- **コンテンツが改変や切り取りされていないか**



偽・誤情報が
判別しやすい！

コンテンツ作成者が加盟する業界団体等、社会の中で認識されている組織が発信者の実在を示し、その情報を誰もが確認できるようになります。また、情報に基づく自動処理も可能になります。
OP技術の浸透により信頼が可視化・価値化される情報空間が構築されます。

© 2026- Originator Profile Collaborative Innovation Partnership.

ORIGINATOR PROFILE

OPのある社会: https://originator-profile.org/ja-JP/vision/

ネットメディアとOP



❖ 情報ソース・発信者の明確化

ネットの情報が社会に対して一定の影響力を持つなか、偽情報への接触や意図しない改ざんなどをOPにより抑制できます。

- ❑ 不確かな情報・フェイク情報等への接触
- ❑ 不法サイトなどへの広告誘導
- ❑ 詐欺的広告や闇バイト広告

- ❑ ニュースサイトや動画サイト運営者などと連携
- ❑ 他の業界団体と連携し、画像・動画の撮影・作成から表示まで一貫した安全性を目指す

© 2026- Originator Profile Collaborative Innovation Partnership.

OPの適用領域セクション https://originator-profile.org/ja-JP/vision/

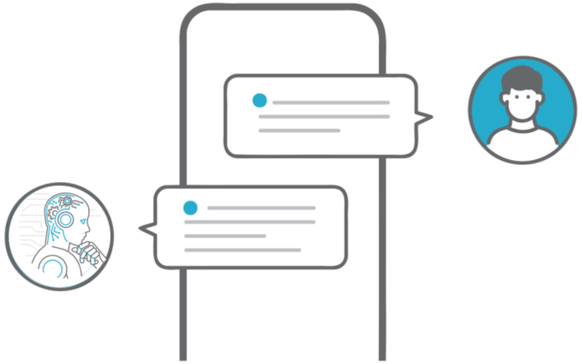
AIを支えるOP

人が情報やサービスに直接接する時も、エージェントが人に代わり情報の収集・分析や手続きをするときも、情報・サービスの出所と信頼性の確認は欠かせません。
ブラウザやAIエージェントによる自動化が進むからこそ、発信者の証明やサービスの使い方を正確にAIに伝えられる技術が重要になります。
OPはウェブ技術と共に、AIによるコンテンツとサービスに対する、より正確な理解を支えます。

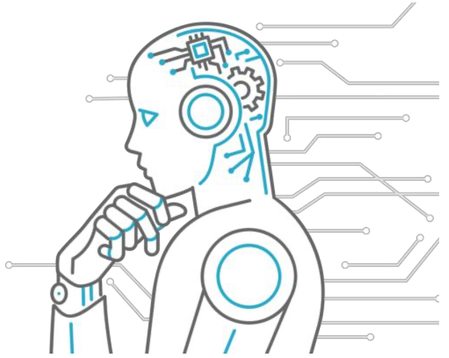
ネット情報をブラウザで調べる
(発信者の信頼性をOPで確認)



ネット情報を対話型AIで調べる
(信頼性は情報源をOPで確認)



AIエージェントが利用者に
代わり信頼性判断と処理



© 2026- Originator Profile Collaborative Innovation Partnership.

OPの適用領域セクション https://originator-profile.org/ja-JP/vision/

ユースケース

目指す「OPのある社会」の例として、「生命・健康・安全の確保」「経済的損失と詐欺被害の防止」「民主主義への寄与、公正な社会に貢献」に関わる5つのユースケースを想定しました。

OPがあることにより、発信者に関する情報をユーザーが確認できるようになります。

OPが無ければ、より注意深い確認をユーザーに喚起することを意味し、結果として真偽を見分けられる可能性も高まります。

どのようなユーザーも、必要な情報に安心してアクセスでき、悪意のある情報にほだされることがないなど、情報格差がなくなる社会でもあります。

- **生命・健康・安全の確保**
  1. 第三者による発信者確認
  2. 行政発の情報
  3. 公的機関のサイトの真正性
- **経済的損失と詐欺被害の防止**
  4. フィッシング詐欺対策
- **民主主義への寄与、公正な社会に貢献**
  5. 選挙に関する情報の真正性

© 2026- Originator Profile Collaborative Innovation Partnership.

ユースケース https://originator-profile.org/ja-JP/vision/

ユースケース	生命・健康・安全の確保

第三者による発信者確認

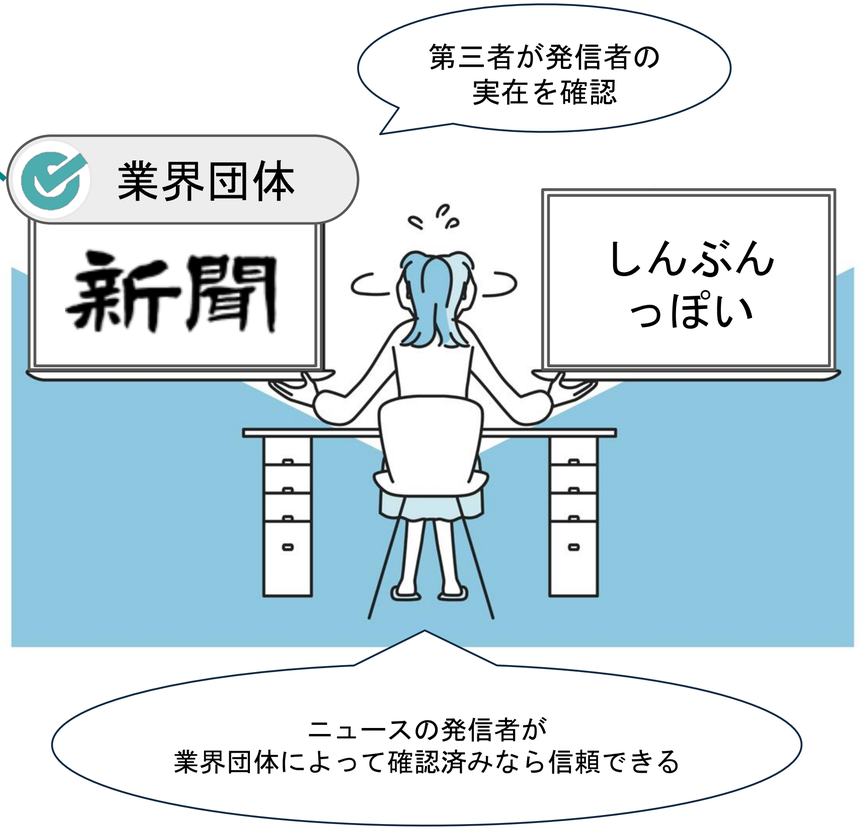
報道機関を偽装したサイトが存在する中、誰が発信した情報か、責任ある団体が発信した情報なのか、業界団体などの第三者が確認したうえで付与されるOP情報が、信頼の担保になります。

OPが正常表示

目視で
真正性を確認

情報の整理に
OPを活用

AI、外部情報とも
連携



OP情報で情報発信者の実在、性質を表示。
ユーザーの判断の助けとなる

OPを活かした検索結果表示や
絞り込みが可能になるなど、
情報収集の入り口でも活用

検索、AI、SNSなどが広くOPを活用し、
発信者確認済みの回答生成や
連携先確認済みのエージェント連携へ

現在

一歩先

将来の
スコープ

© 2026- Originator Profile Collaborative Innovation Partnership.

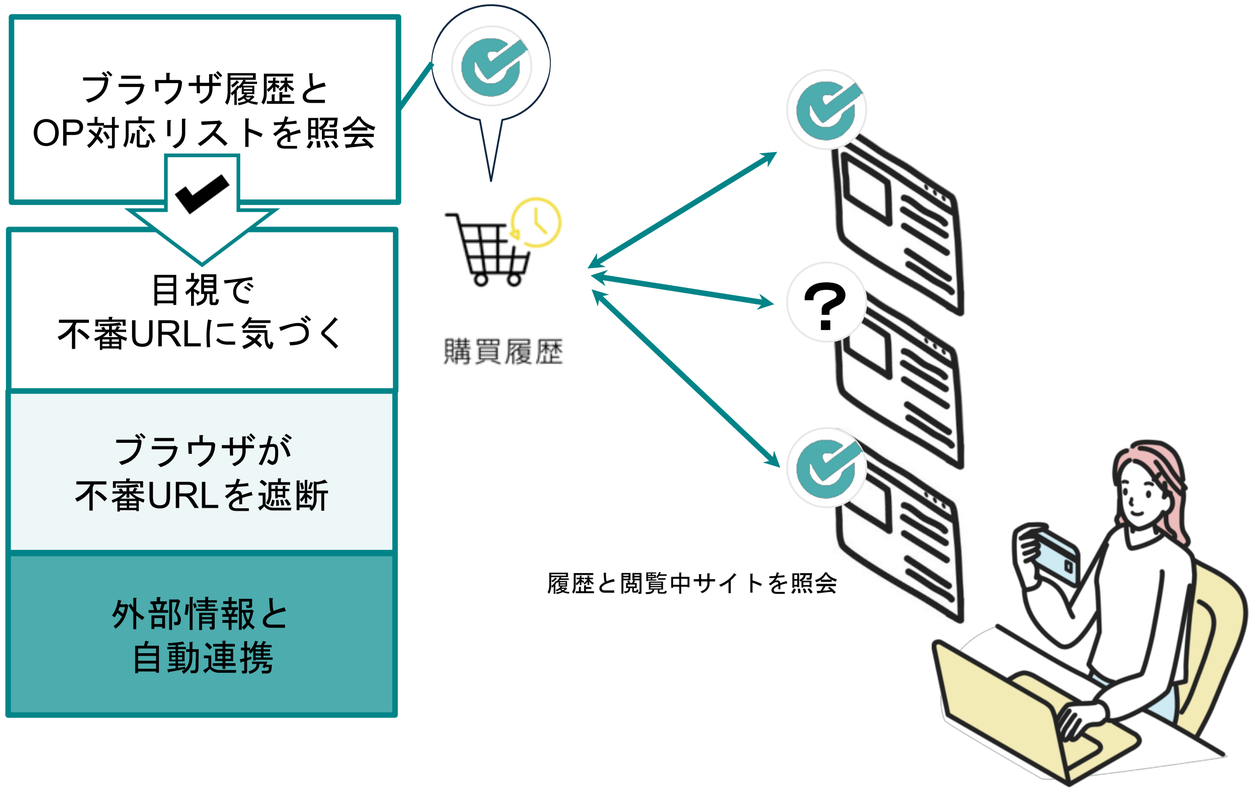
ORIGINATOR PROFILE

ユースケース https://originator-profile.org/ja-JP/vision/

ユースケース	経済的損失と詐欺被害の防止

フィッシング詐欺対策

OP対応ブラウザでは詐欺サイトの多い業界のOP対応企業リストに加え、ユーザのアクセスしたOP対応サイトの履歴を保持します。ブラウザとAIがOP対応のリストと履歴を参照しつつ、偽サイト・フィッシングサイトへのアクセスを自動的にブロックします。



フィッシング詐欺には、ユーザー自身によるサイトのOP情報確認が重要

端末の履歴から不審と判断したサイトは遮断するようブラウザやメーラーに設定

決済業界のOPガバナンスと自動連携し、不審サイトにアクセスしない、AIエージェントがクロールしない等の措置

現在

一歩先

将来のスコープ

© 2026- Originator Profile Collaborative Innovation Partnership.

ORIGINATOR PROFILE

ユースケース https://originator-profile.org/ja-JP/vision/

本動画はこの場のみ(実悪性サイトの社名等の表示があるため)



2026 年にTurnt Up Technologiesが観測した実悪性サイトより

Background & Trends

OP 技術を必要とする背景

ブラウザと TLS が放棄した「身元確認」の実現が求められる

- TLS 証明書の役割は「身元/安心」から「接続」に絞られた

1990s	2007	2015	2017	2019
SSL → TLS	**EVの登場**	**Let's Encrypt**	**"Stripe, Inc"**	**EV表示の撤去**
Netscapeが導入し、TLS 1.0（1999）として標準化。証明書が身元と暗号化を兼ねる	CA/Browser ForumがEVガイドラインを策定。アドレスバーに緑の組織名	無償・自動のDV証明書。HTTPSは「信頼の印」から「当然の前提」に	別の州で同名会社を設立しEVを取得。組織名は一意ではない	Chrome 77・Firefox 70。表示を消しても利用者行動はほぼ不変

- ブラウザはCT, CRLite などで強化を続けるがあくまで暗号化通信サーバ証明書
  - しかし eMudhra (エムドラ) インシデントなど発生してしまう...
  - Safe Browsingに加えてAIでの危険なサイト検知実装も増えているが...

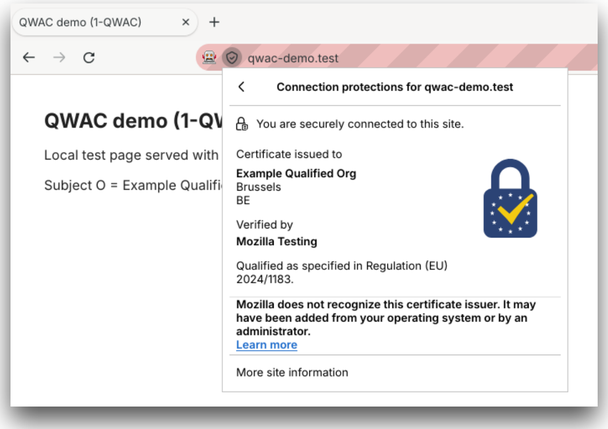
身元情報を支える関連技術の広がり

信頼は1枚の証明書でなく要素技術の組み合わせで築く

- 組織の法的身元の保証
  - eIDAS の QWAC (Qualified Website Authentication Certificates) など
- コンテンツの真正性・完全性
  - CSP, SRI などハッシュ固定から sbSRI や WEBCAT など署名ベースへ
    (親を配るサーバの乗っ取りに無力で polyfill.io 事件では 10万超のサイトに影響)
  - Web アプリ単位での署名や透明性ログの
    (CA/TLSに依存せず全員に同一コードが配付されていることを第三者監査まで可能に)
- 検証済みブランド表示
  - メールでの BIMI+VMC による登録商標表示、電話での STIR/SHAKEN による着信画面表示...

QWAC: EUにおける身元情報の表示

身元情報のブラウザ表示を義務づける法規制の例



- 2027年からはブラウザの対応・表示の義務が発生
  - 証明書情報に EU トラストマークを表示するなどの実装

ブラウザ提供者（第45・45a条）

- QWACを認識し、相互運用性を確保する
- 証明された身元を分かりやすく表示（可能ならEUトラストマーク）
- 義務に反する措置は禁止。根拠ある予防措置のみ可、欧州委員会等へ書面で通知
- QWACに独自の必須要件は課せない。零細・小規模企業は最初の5年間除外

ウェブサイト運営者

- QWACの利用は任意（PSD2の決済APIなど個別法の義務は別）
- 1-QWAC：QWACをそのままTLS証明書として設置
- 2-QWAC：TLS証明書とは別にQWACを取得し、バインディングを公開

QTSP（発行者）

- 附属書IVの要件と参照規格（ETSI EN 319 411-2など）で発行
- 監督機関の審査を受け、EUトラストリストに掲載される
- 1-QWACはブラウザのルートストア入りも必要、2-QWACは不要

2014
eIDASでQWACを定義

2021.06
表示義務を提案

2024.05.20
改正eIDAS発効

2025.12.16
実施規則 2025/2527 採択

2027.01.06
適用開始：基準（ETSI TS 119 411-5）が法的に確定

24年から義務はあったが実施規則の適用で実質的な義務化が法的に確定

真正性保証はハッシュから署名へ

配信サーバ自体を信用せず、TLS/CAと独立した署名技術へ

- 保証根拠は HTML記載ハッシュ → HTML記載署名鍵 → 鍵と公開ログへ

ハッシュ・ポリシー型（親ページが固定）　署名・透明性型（鍵と公開ログが保証）　事件

2004–2012

CSP
2004年に提案、Firefox 4で初実装、2012年にW3C勧告候補

2016–2019

SRI
2016年6月W3C勧告。親ページがハッシュを指定

SXG
Chrome 73（2019）。応答に署名、ただし鍵はCA依存

2022–2024

Code Verify
2022年3月。Metaがハッシュを公開、Cloudflareが監査

パッケージ署名
npm（2023）・PyPI（2024）がSigstoreで来歴を証明

polyfill.io
2024年6月。10万サイト超に悪性コード

2025

署名ベースSRI
2月に試験提供、Chrome 141で出荷。Ed25519鍵で検証

WAICT
10月公開。マニフェスト＋透明性ログ＋ウィットネス

2026

WEBCAT
8月にアルファ版。Sigstore＋透明性ログ、Firefox拡張

SXGの終了
9月末、GoogleがSXG証明書の発行を終了

ChromeOSで署名鍵=OriginとするIsolated Web Appsも同じ方向性

コンテンツの出どころが分かるWebへ

OPは他技術で足りない/適さない/補完する技術を開発・標準化提案

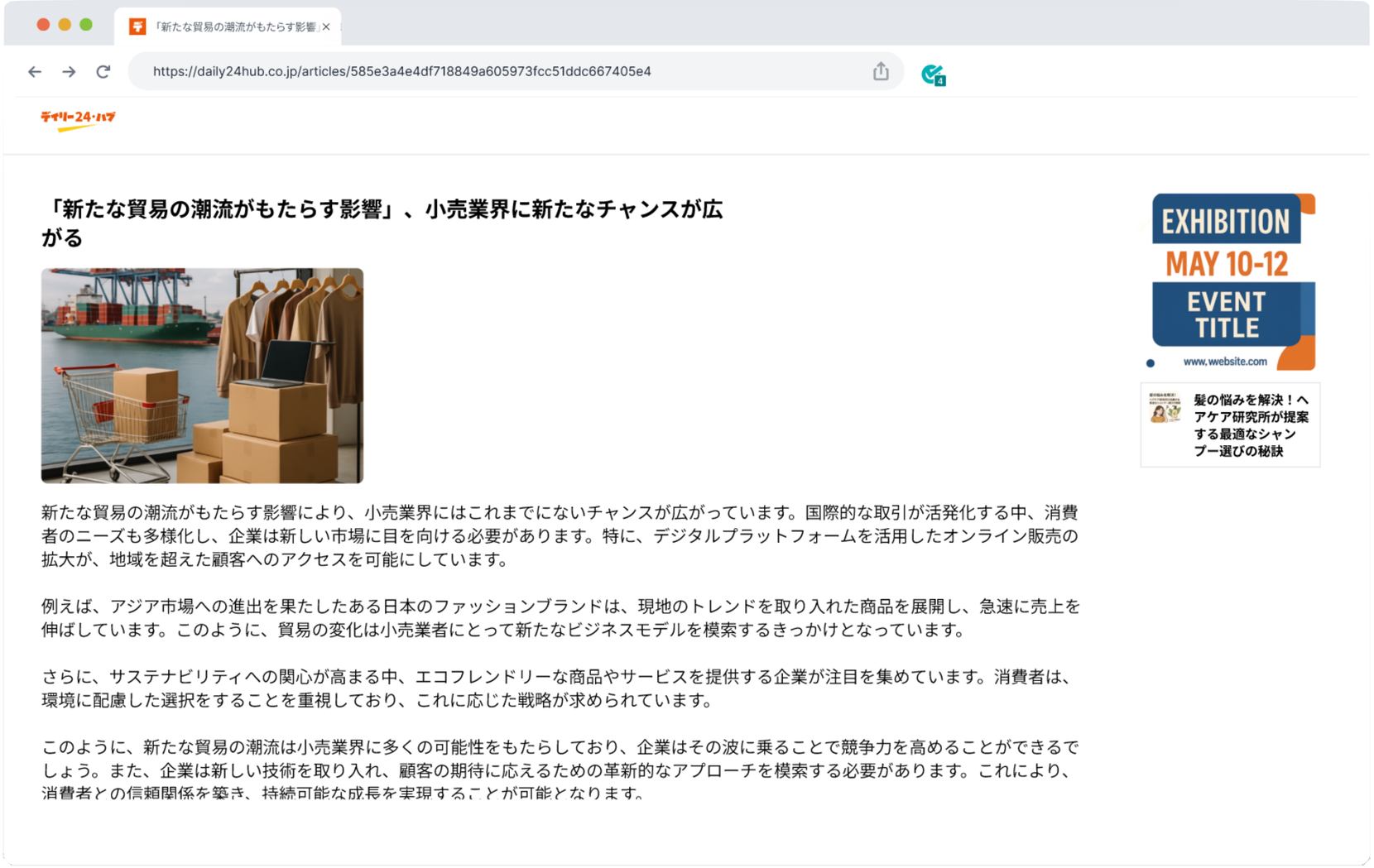
- 組織の**身元情報を柔軟に表現**する技術
  - 組織が誰か、どのようなものか、第三者発行の証明書 (VCベース)で示す
  - トラストリスト形式ではない /「編集履歴」より「責任者の明確化」
- **Webコンテンツのための署名**技術
  - ファイル単位ではなくHTML内の記事本文への署名と検証・表示
  - ファイルやアプリ単位での署名は他技術との連携も想定
- オンライン広告の信頼性を向上させる技術
  - 広告主と媒体が双方を確認できる仕組みや広告取引の信頼性指標など

これ以降、Web開発者が直接関わるコンテンツの出処証明

OP Overview

OP Lens (仮) 拡張機能の利用イメージ

OP対応サイト閲覧時の自動検証、記事の出処もワンクリックで



サイトの運営者や記事の作成者が第三者確認済み組織であることを**自動検証し概要情報を表示**します

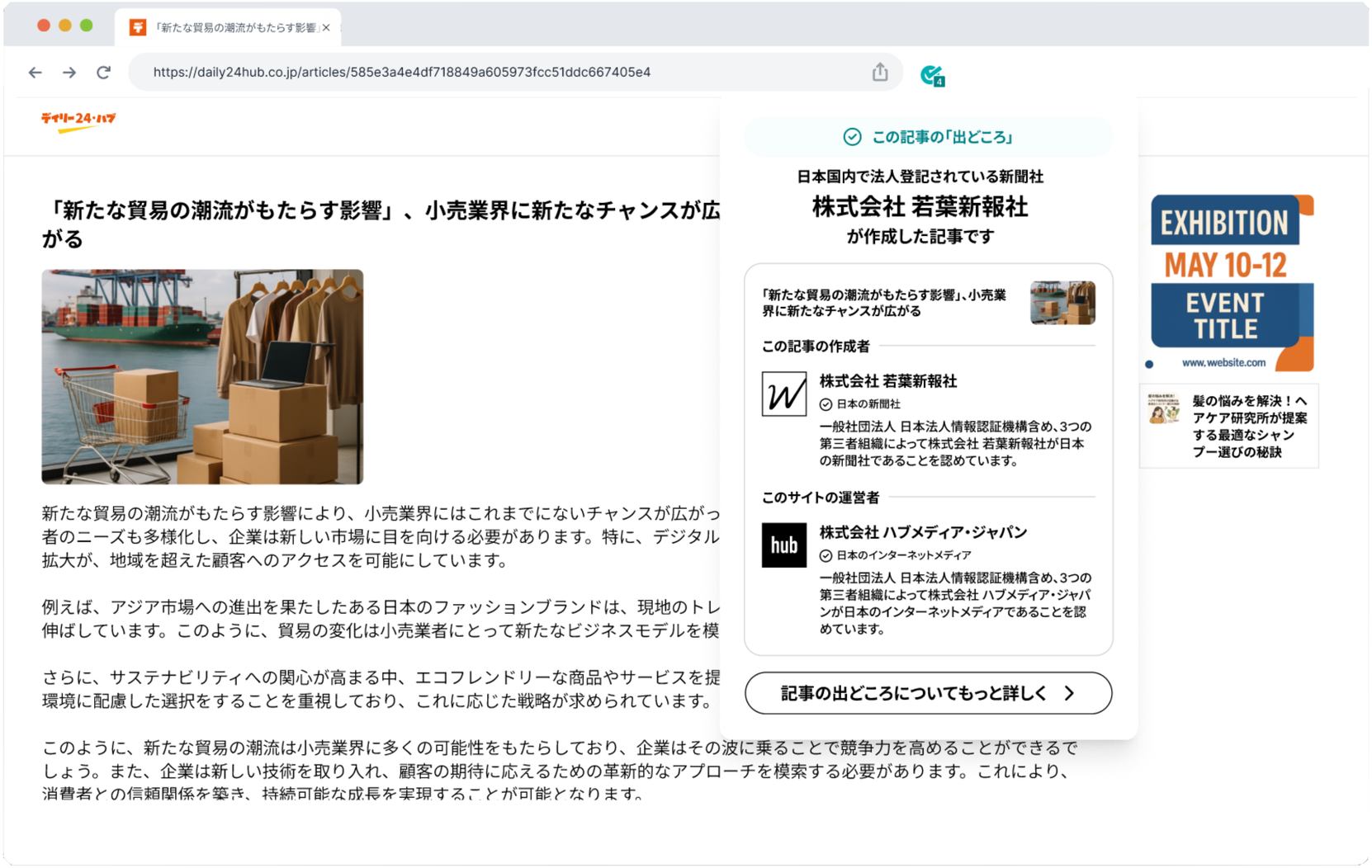
ユーザ向けの拡張機能OP Lensは UI/名称の検討・順次実装中(実装・公開済みの拡張機能OP Inspectorは開発者向けツール)

UIや機能は将来的にブラウザで実装されるまでには変わります(ブラウザ毎の実装になる)

10月時点での Figma プロトタイプ/拡張機能実装は進行中

OP Lens (仮) 拡張機能の利用イメージ

OP対応サイト閲覧時の自動検証、記事の出処もワンクリックで



サイトの運営者や記事の作成者が第三者確認済み組織であることを**自動検証し概要情報を表示**します

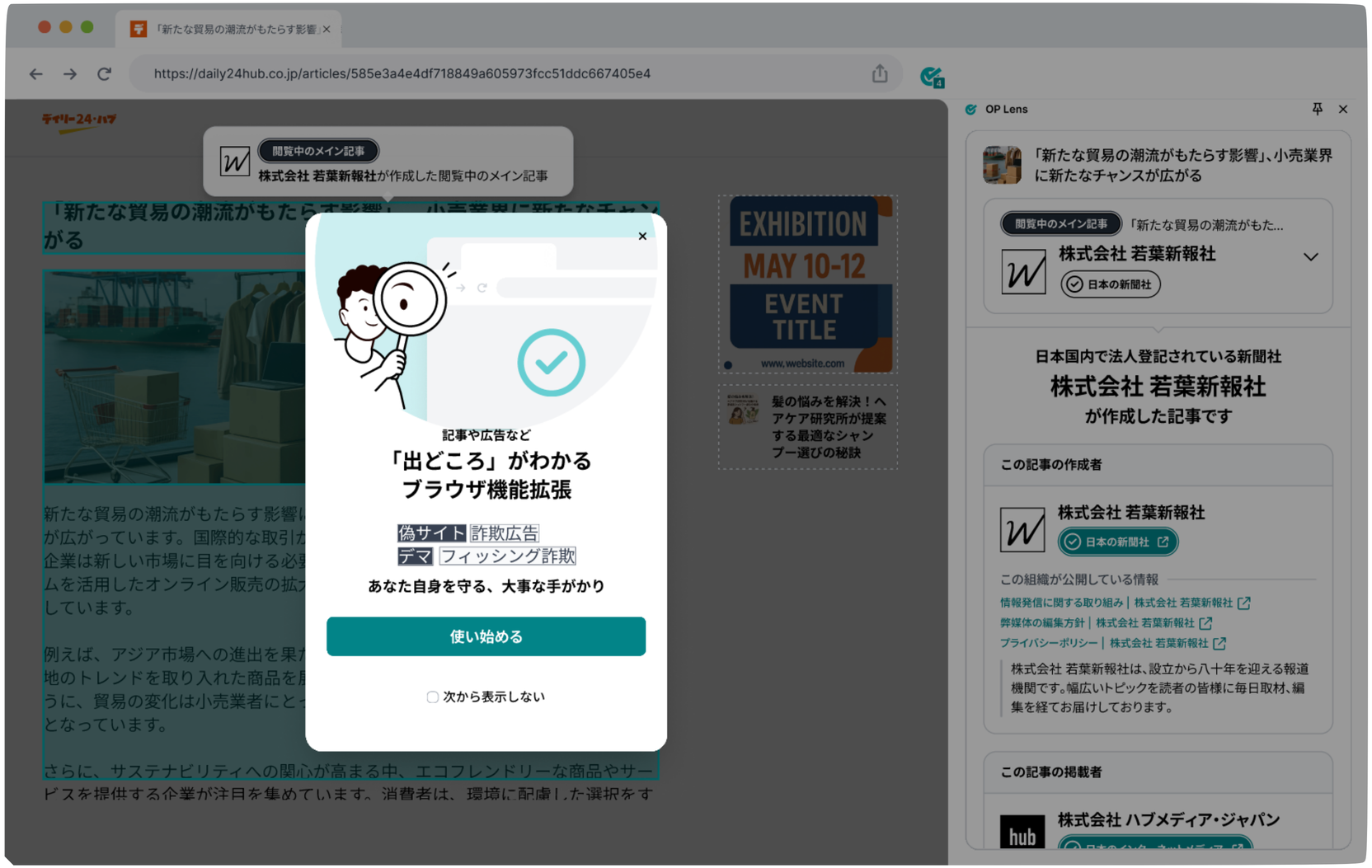
ユーザ向けの拡張機能OP Lensは UI/名称の検討・順次実装中(実装・公開済みの拡張機能OP Inspectorは開発者向けツール)

UIや機能は将来的にブラウザで実装されるまでには変わります(ブラウザ毎の実装になる)

10月時点での Figma プロトタイプ/拡張機能実装は進行中

OP Lens (仮) 拡張機能の利用イメージ

どの部分が、誰による記事か、それはどのような組織か確認できる



サイトにOP,SP,CAの3つの**署名データ**を追加します

OP (Originator Profile) で**どのような組織か**分かる
(第三者確認済みの組織情報)

SP (Site Profile) を設置すると**サイト運営者が誰か**分かる
(HTTPS暗号化通信の証明書とは別途、身元情報を示す)

CA (Content Attestation) を記事に付与すると**どの部分の作成者が誰か**分かる

10月時点での Figma プロトタイプ/拡張機能実装は進行中

OP Lens (仮) 拡張機能の利用イメージ

どの部分が、誰による記事か、それはどのような組織か確認できる



サイトに**OP,SP,CA**の3つの**署名データ**を追加します

OP (Originator Profile) で**どのような組織か**分かる
(第三者確認済みの組織情報)

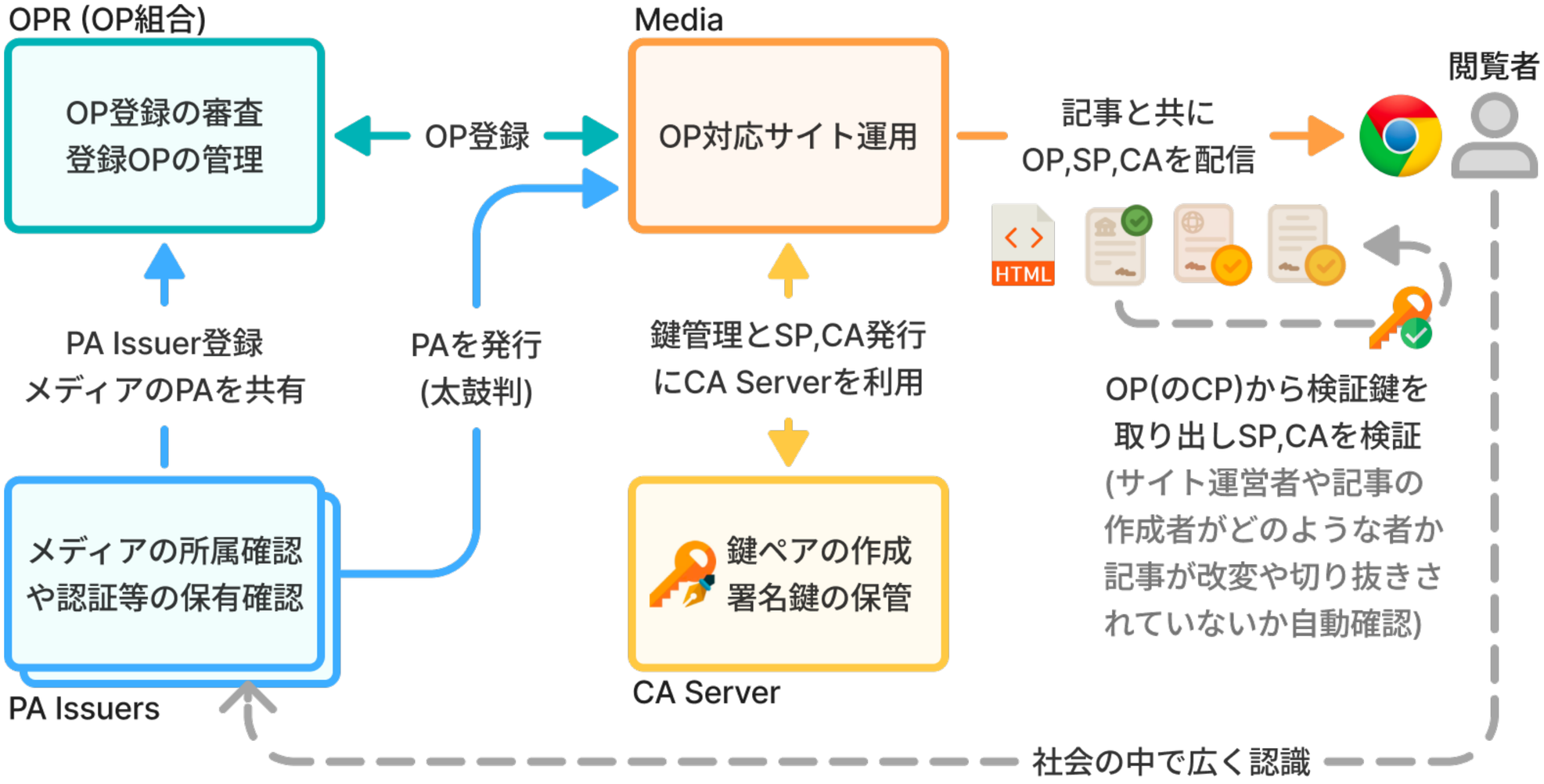
SP (Site Profile) を設置すると**サイト運営者が誰か**分かる
(HTTPS暗号化通信の証明書とは別途、身元情報を示す)

CA (Content Attestation) を記事に付与すると**どの部分の作成者が誰か**分かる

10月時点での Figma プロトタイプ/拡張機能実装は進行中

OPの仕組み(全体イメージ)

第三者確認済みの記事作成者情報 + 改ざんや切り抜きがない証明



注: "Media"は業種のメディアではなく情報/コンテンツ作成/発信主体の意

OP 技術の署名データ
OP, PA, SP, CA

OP, (PA), SP, CA の役割

組織の証明書・コンテンツの証明書・サイト情報の証明書

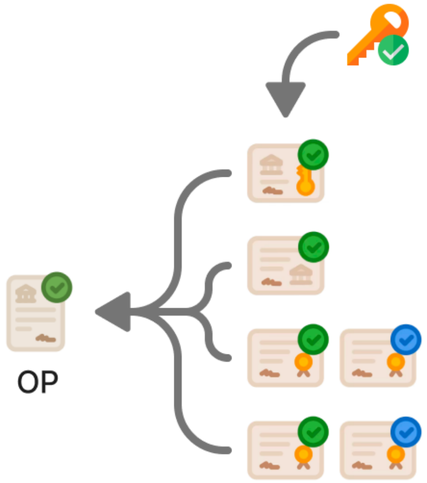
- **Originator Profile** (OP, 組織の証明書) = CP + WMP + PAs
  - Core Profile (CP): OP ID と検証鍵など、署名検証に必要最小限のデータ
  - Web Media Profile (WMP): ポリシー情報などを含む組織基本情報の証明書
  - **Profile Annotation** (PA): 実在性確認・所属団体や認証・許認可などの証明書
- **Site Profile** (SP, サイト情報の証明書)
  - サイトの名称などの基本情報とサイト運営者(など)の OP を含む
- **Content Attestation** (CA, コンテンツの証明書)
  - 記事・コンテンツのタイトルなどの基本情報と、対象範囲を特定する参照情報、非改竄を確認するハッシュ値、掲載先 URL 制限などを含む

OP(に含むPAなど)は第三者確認に基づく発行、SP,CAは本人による発行

OP,SPの役割 (OP,SPに含むもの)

OP=組織証明書(第三者確認情報含む)、SP=サイト証明書(OP同梱)

OPに含めるもの



CPにはMedia検証鍵(公開鍵)を含む (1つ以上)

CIP発行のCP (1つ)

CIP発行のWMP (1つ)

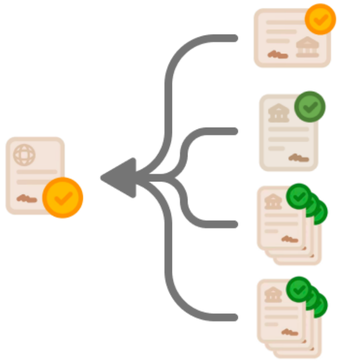
CIP発行の登録証と、CIP発行の実在証PA (1ペア)

CIP発行の登録証と、第三者発行の登録PA (1つ以上のペア)

ブラウザはMediaのOPにWMP, 実在証PA, 登録PAペアが含まれている場合
そのOPが信頼出来る情報発信者と判断し、CPに含む検証鍵を利用する

情報発信者信頼性があると判断するのに的確な団体所属・認証・認可
などと認めるPAについて、CIPがPA登録証PA(登録証)を発行する
検証者は登録証とペアとなっているPAの保有を信頼性判断に用いる
(登録証のないPAもOPに同梱可能だが信頼性判断に使われない)

SPに含めるもの



サイト管理者のWSP (1つ)

サイト管理者のOP (1つ)

PA issuerのOP (保有PA数)

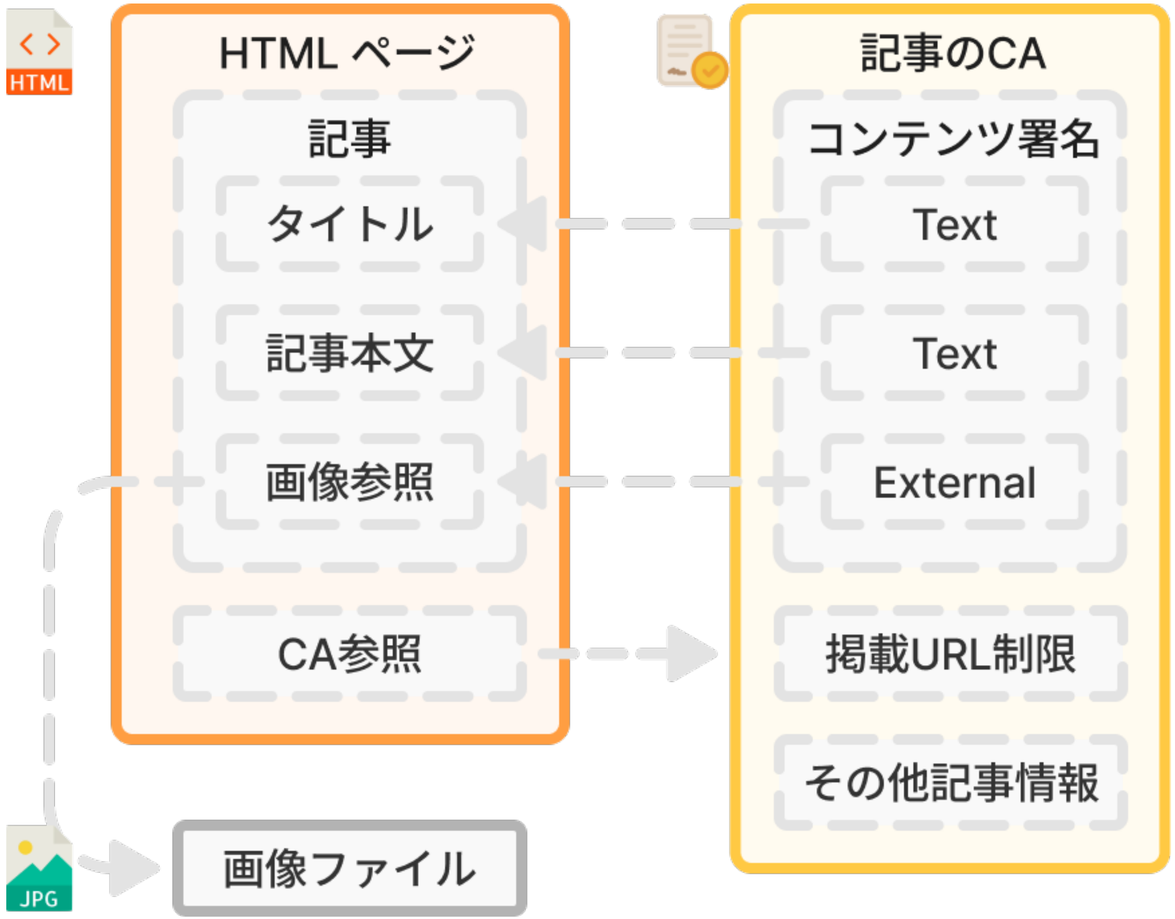
第三者のOP (任意)

ブラウザはサイト管理者のOPを検証し、
そのCPから検証鍵を入手しWSPを検証
OPの検証には保有PA IssuerのOP検証を
必要とするためPA IssuerのOPも同梱

その他に外部配信CA検証などで頻繁に
必要な第三者OPも同梱可能

CAの役割 (URL/HTMLとの関係)

タイトル・本文・画像などへの署名や掲載URL制限

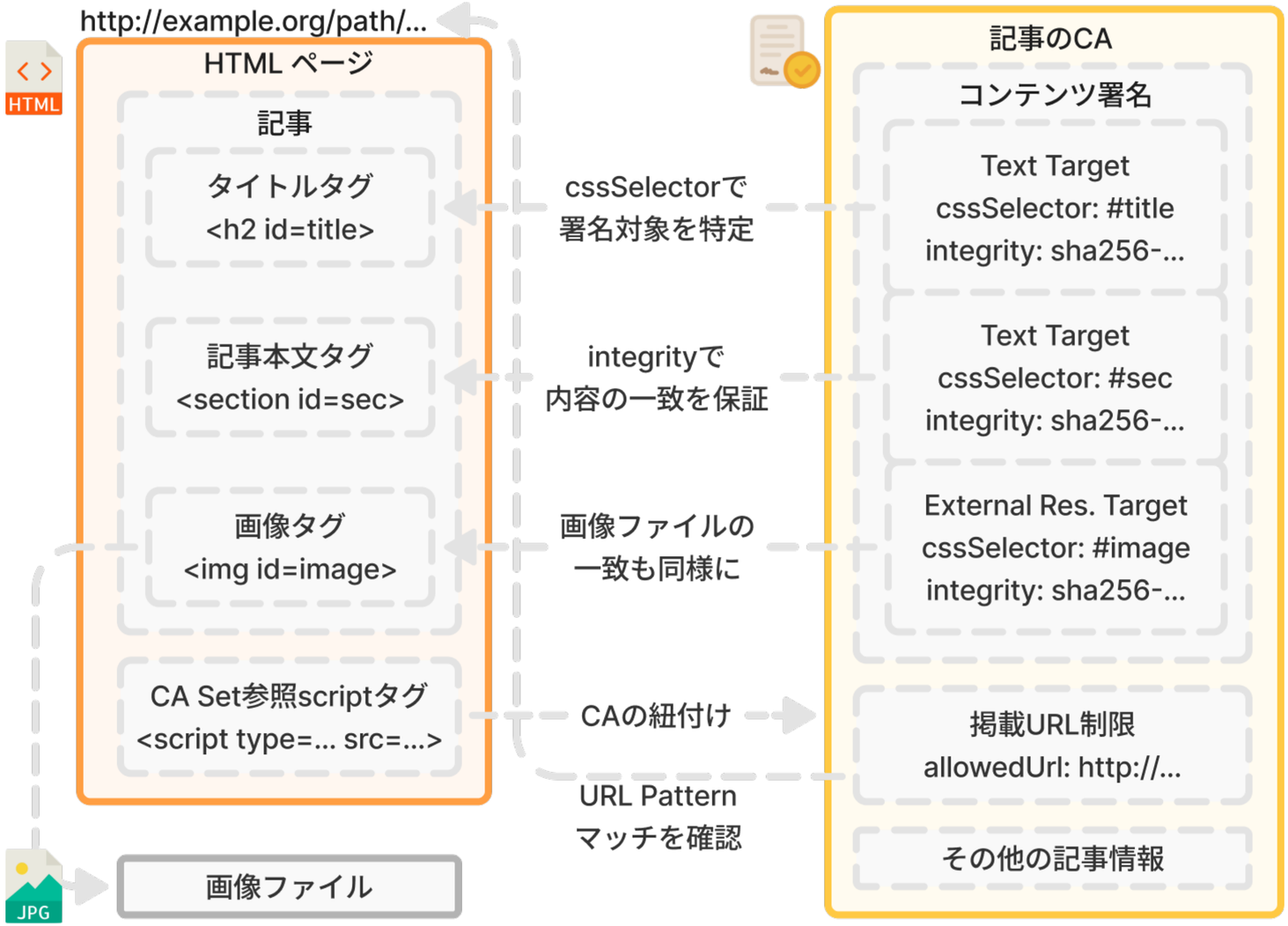


- コンテンツ署名
  - HTML中の記事部分(タイトル・本文・画像など)を指定して署名
  - 署名時との一致を保証
- 掲載URL制限
  - 偽サイトに丸コピしても無効！
- その他記事情報
  - タイトル、サムネイル、概要などコンテンツの基本情報を記載します

詳しくは https://docs.originator-profile.org/ja/tutorial/ca-target/ も参照

CAの役割 (URL/HTMLとの関係) 詳細版

cssSelector指定対象のハッシュ値や掲載許可URL Patternを記載

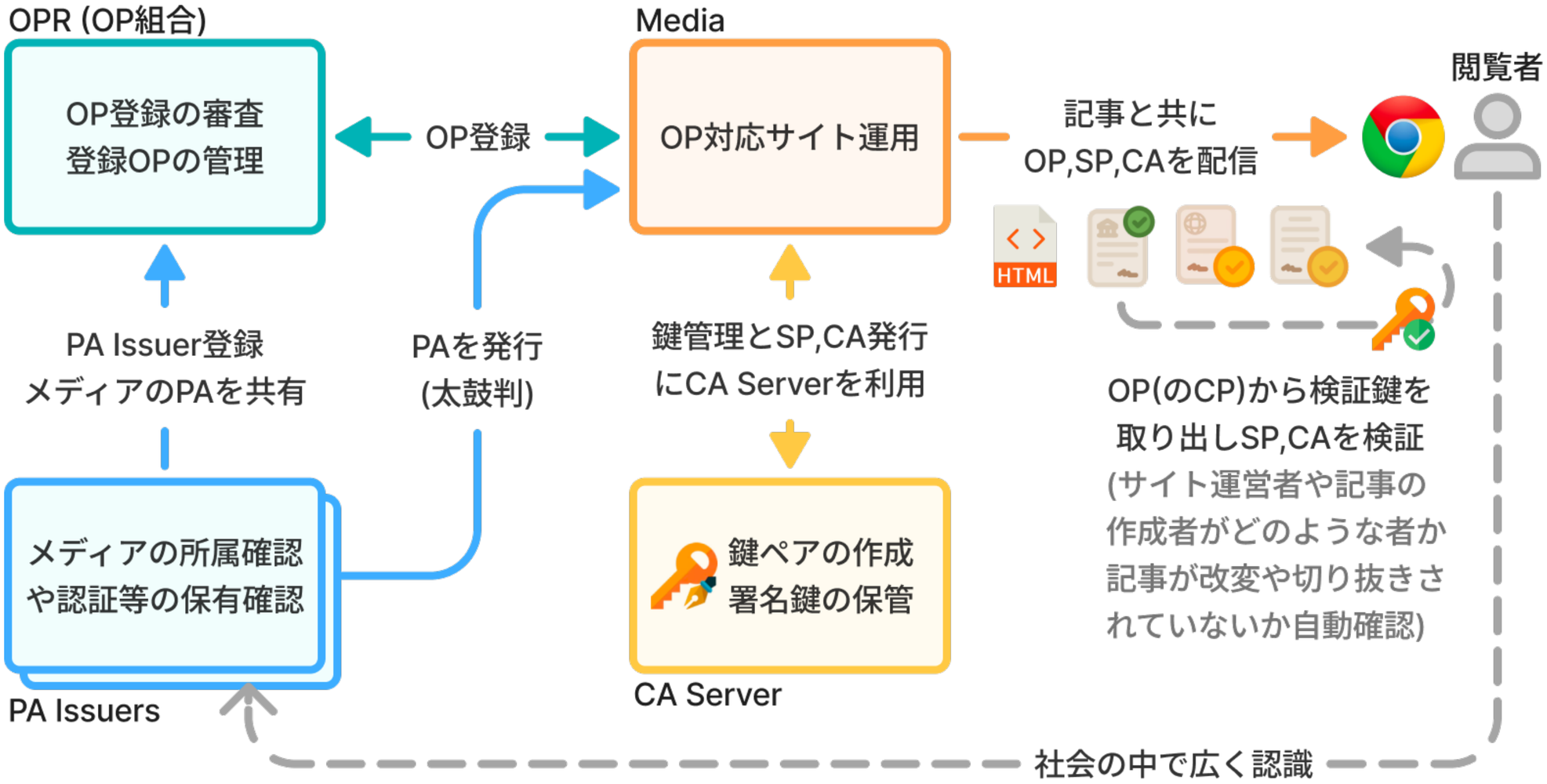


- 下記のハッシュ計算はCA Serverに委ねられます (ブラウザが読み込むものと一致するデータは必要)
- Text Target
  - cssSelectorでマッチした要素内のテキストノードを連結してハッシュ計算
- External Resource Target
  - cssSelectorでマッチした要素のsrc属性などが参照する外部ファイルに対してハッシュ計算

詳しくは https://playground.originator-profile.org/#tag/ca も参照

再掲: OPの仕組み(全体イメージ)

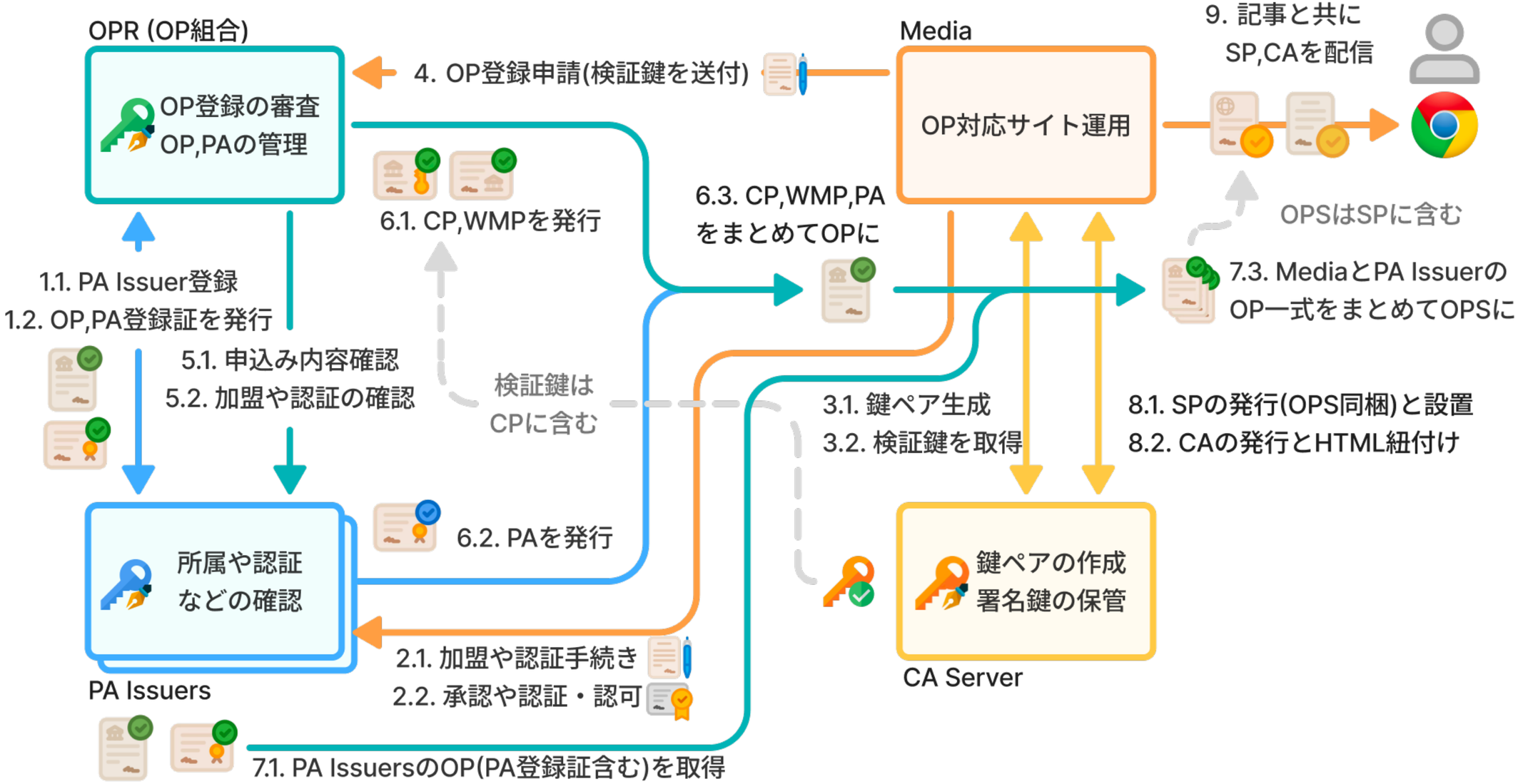
第三者確認済みの記事作成者情報 + 改ざんや切り抜きがない証明



注: "Media"は業種のメディアではなく情報/コンテンツ作成/発信主体の意

Originator Profile 対応 =
OP登録しサイトに SP,CA を設置

OP対応手順・ブラウザへの配信までの流れ



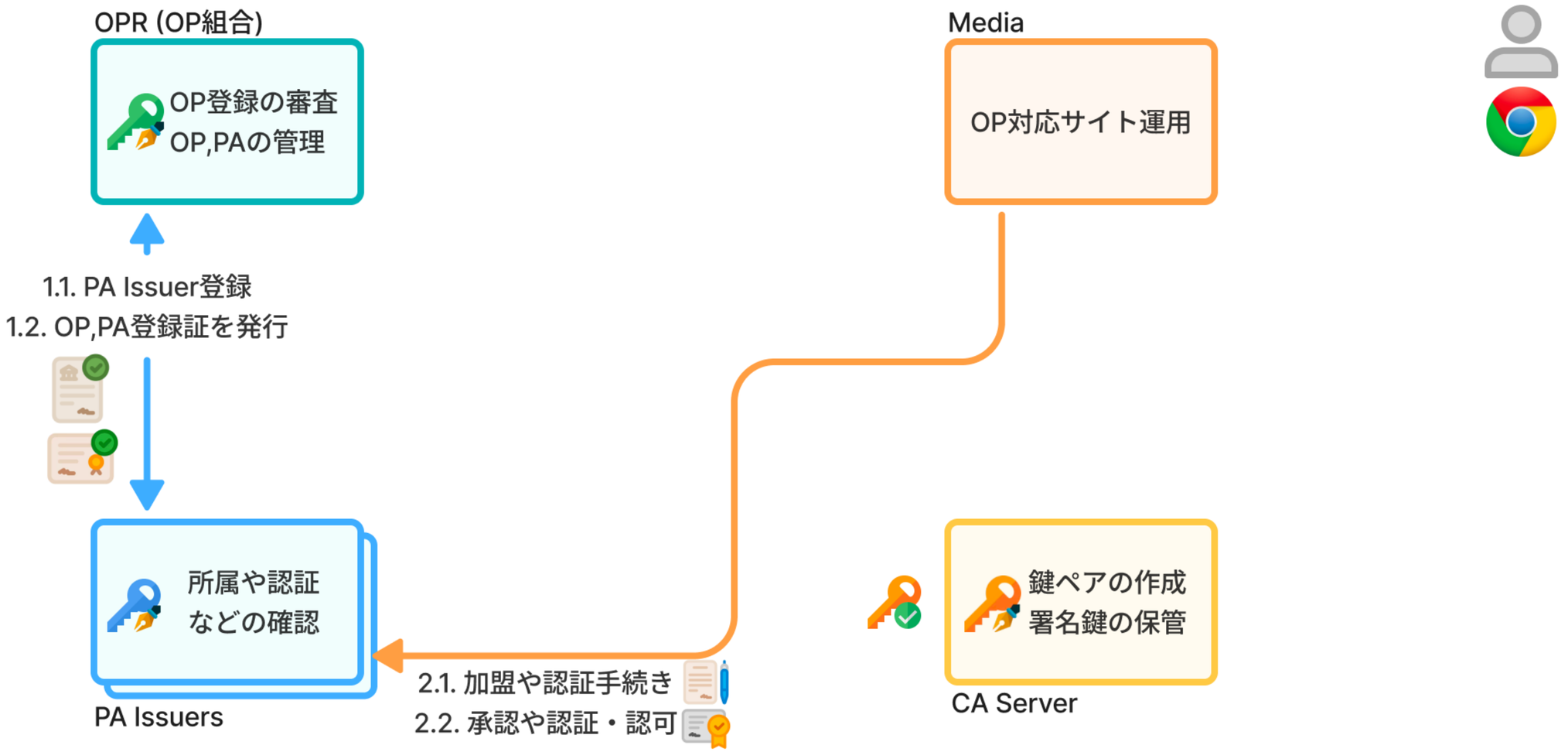
こちらは全体の大まかな流れで一部簡易化 / 詳細は個別パート説明にて

OP登録から SP・CA の作成・配信までの流れ

Originator Profile（OP）技術：登録 → 発行 → 設置 → ブラウザでの検証

OPR（OP組合） PA Issuers Media CA Server 閲覧者のブラウザ

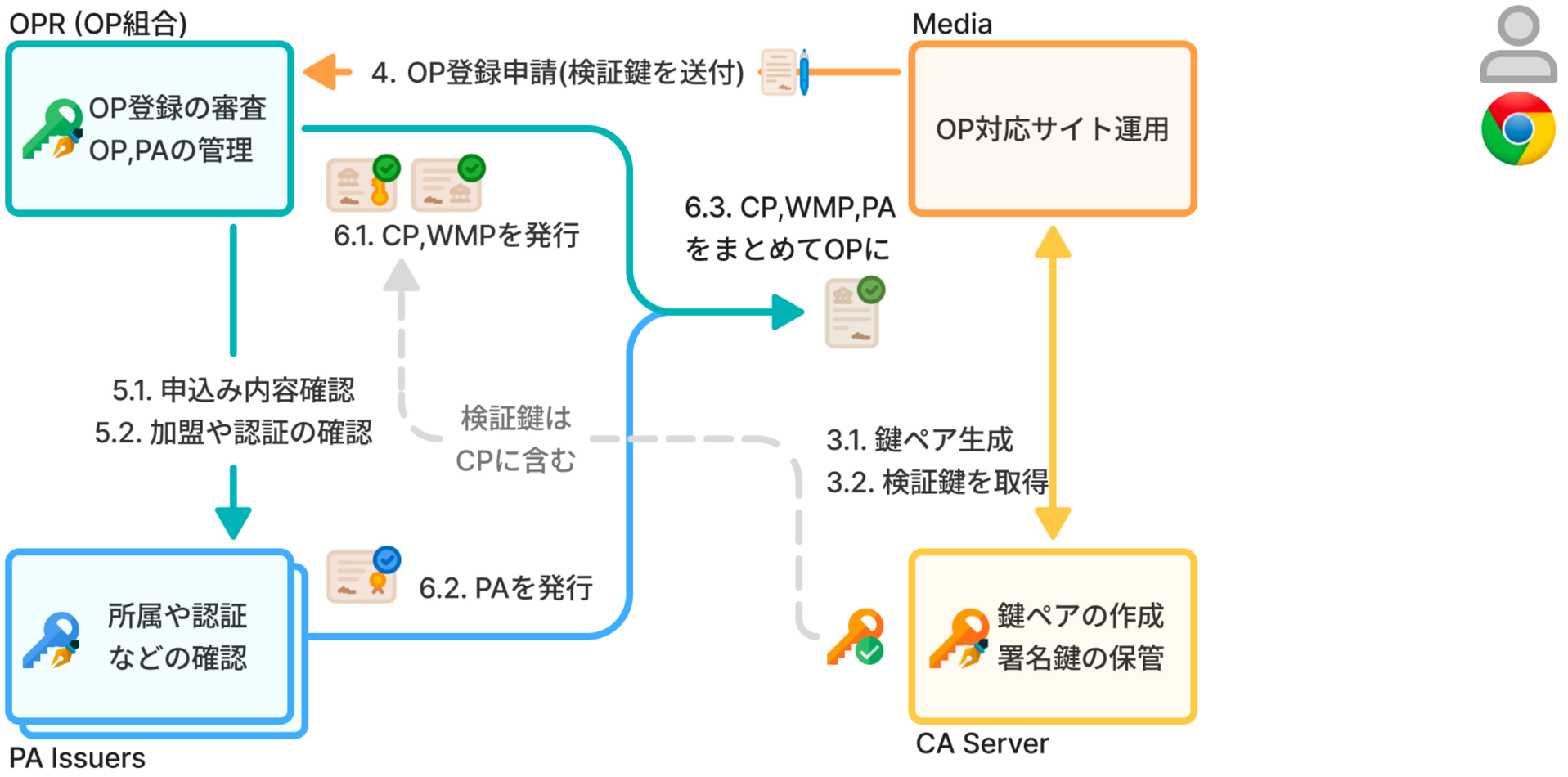
メディアのOP登録以前の流れ(PA Issuer登録とPA保有資格の取得)



メディア側の皆さんが意識する必要はない前提パート(仕組みの理解・説明用)です

実装者側は気にしなくてもOKな事前・前提パート (前提理解用の参考)

OP登録の流れ(OP登録からOPの発行まで)

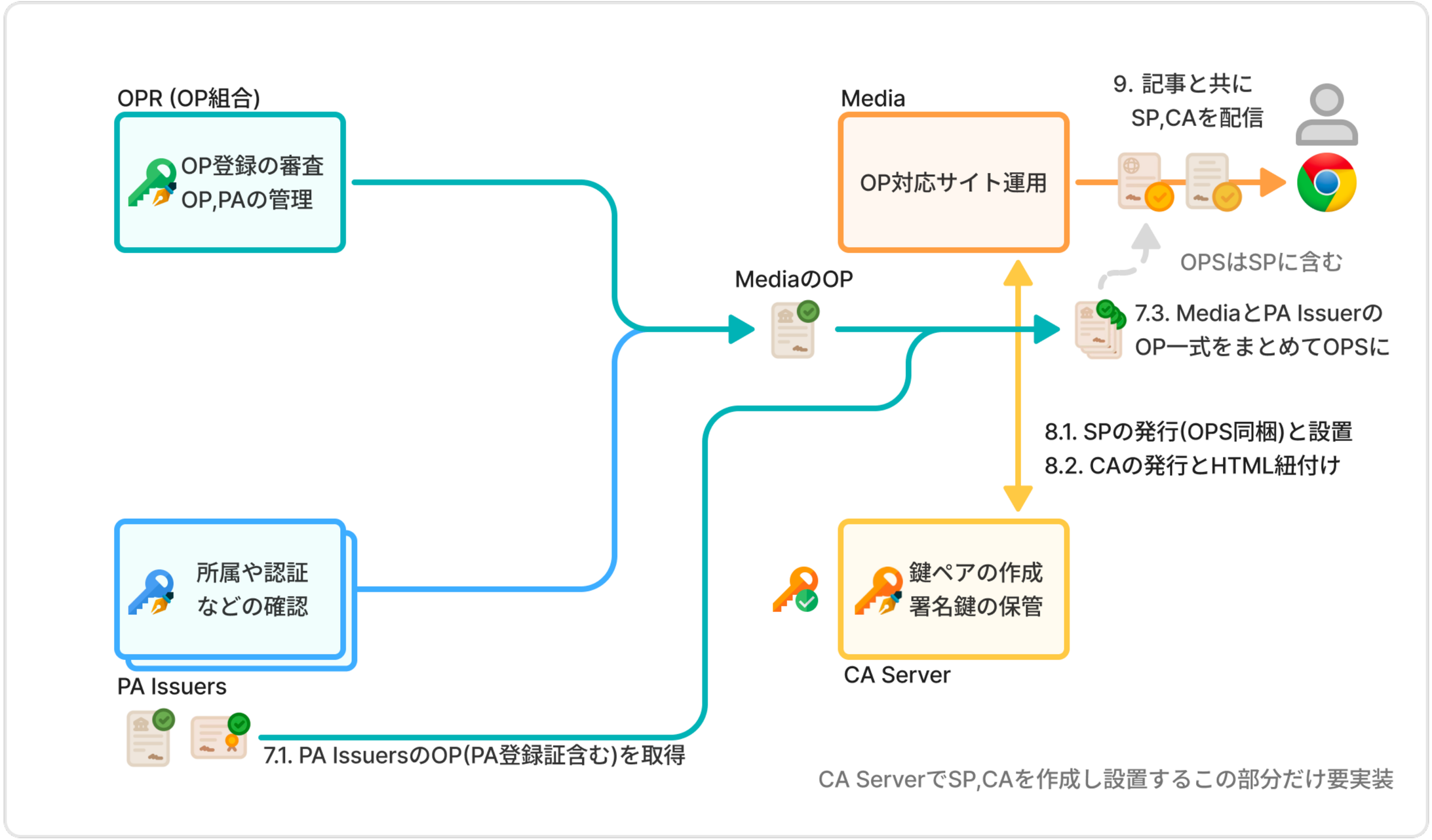


OPRとPA IssuerからそれぞれCP,WMP,PAを取得する流れになっているが、実際にはOPR側でPAおよびPAのOPまで
MediaのOPに必要なもの一式が入ったOPSの形で用意します(GUIでDLまたは固定URLから取得)

このパートはマニュアルに従ってGUIでの「手続き」で済ませられるパート

SP(OPS含む),CAの作成と配信

ORIGINATOR PROFILE CIP



最後のこの部分がサイト側での実装を伴う所です！

Originator Profile 対応の進め方

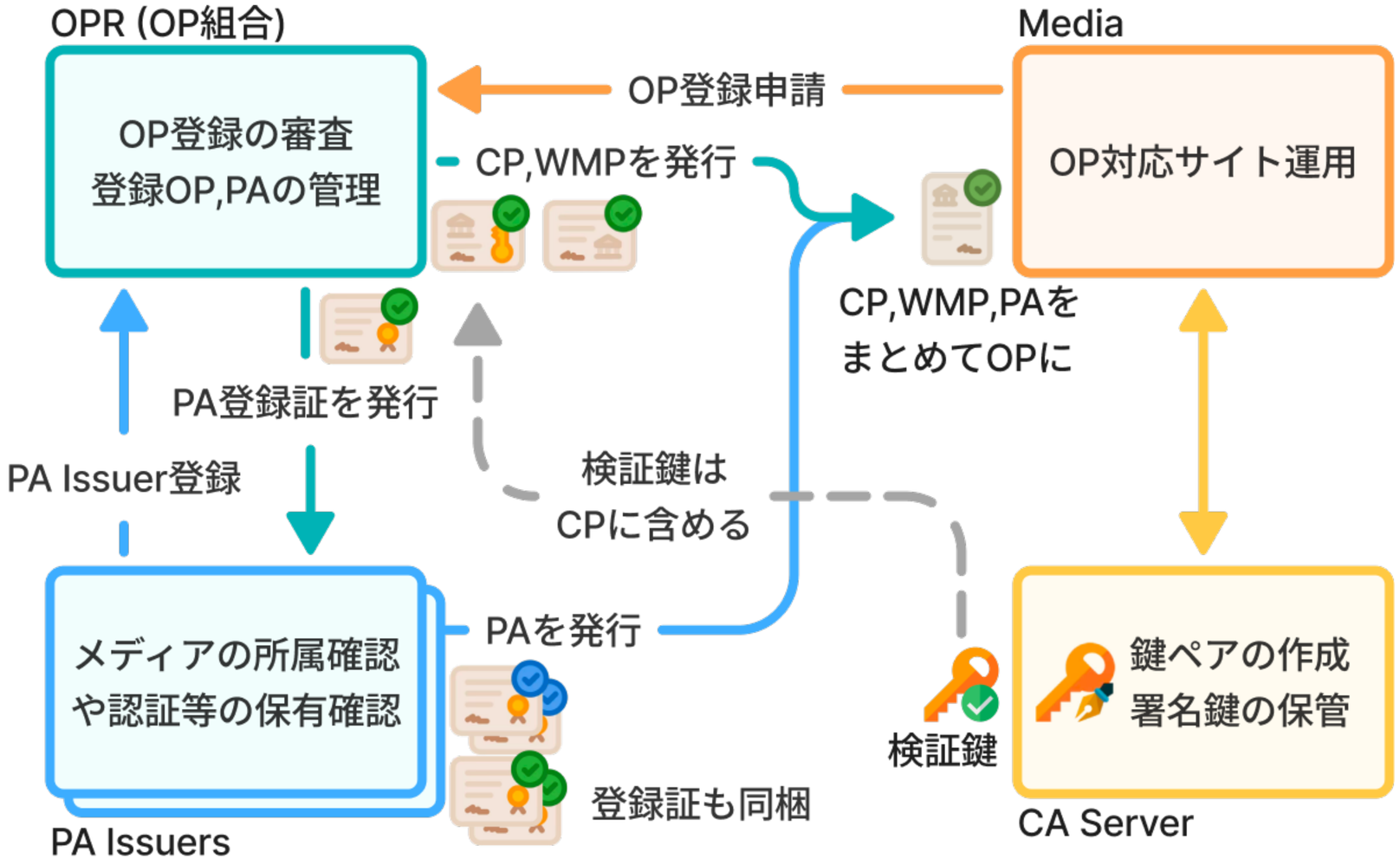
既存 Web サイトを OP 利用サイトにするためには

1. OP 登録 (事前手続き)
   - 検証鍵(公開鍵)と組織情報などをレジストリ (OPR) に登録し、組織の証明書 (OP、第三者確認証明書 PA 含む) を受け取る
2. サイトプロファイルの設置 (サイト毎に一度)
   - サイト毎にサイト証明書 (SP) を作成し /.well-known 配下に設置
3. コンテンツ証明書の発行 (記事/コンテンツ毎に一度)
   - 記事に対応するコンテンツ証明書 (CA) を作成し HTML に紐付ける
   - CA の発行処理・署名鍵管理・有効期限管理などは支援サービスあり

https://docs.originator-profile.org/ja/tutorial/

OP登録とOP(CP,WMP,PA)の発行

OPR (レジストリ)サイトにログインして申請手続きします

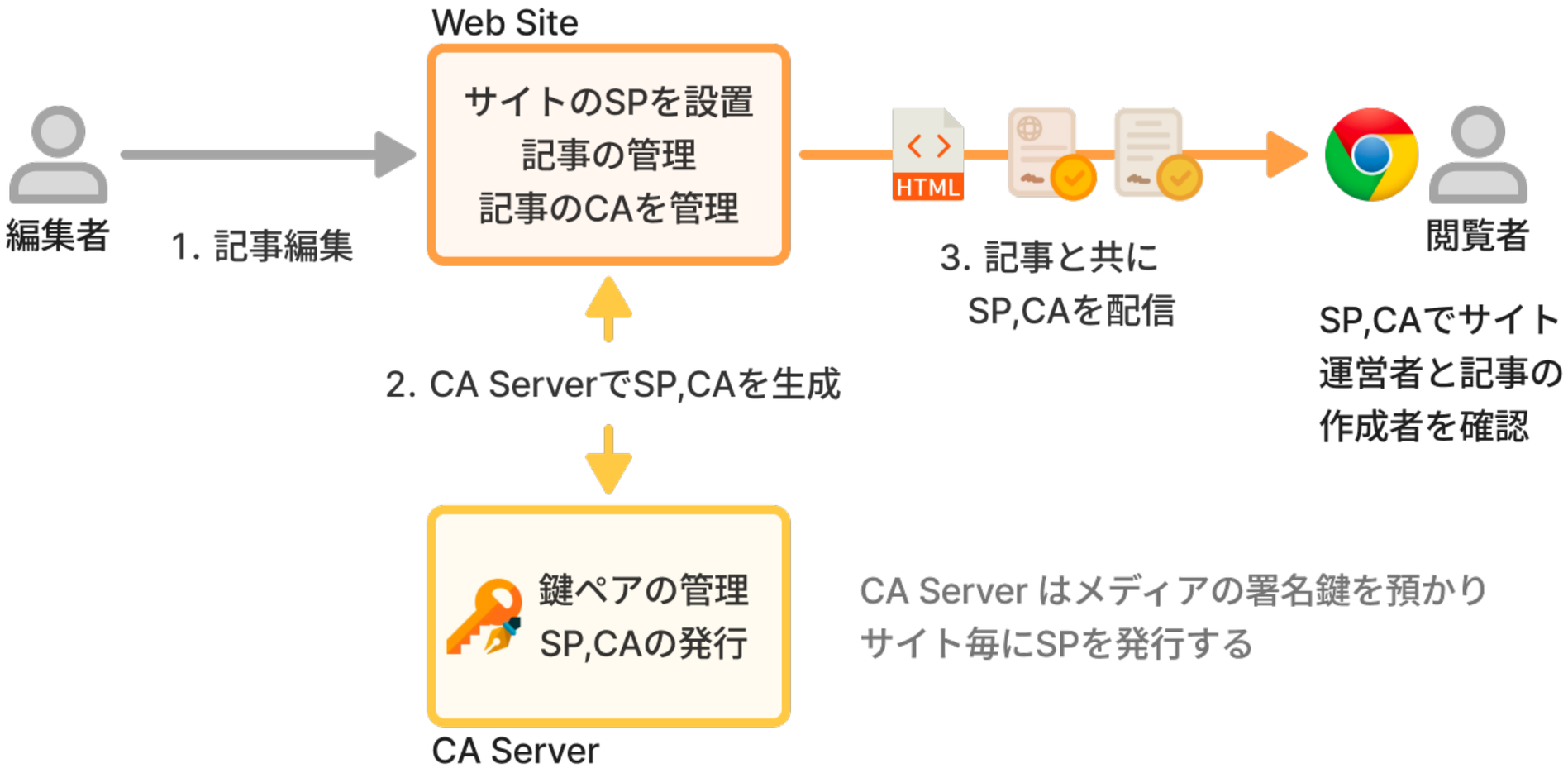


- メディアがすること:
  - 鍵ペア作成
  - OPRへの登録申請
- 緑/青矢印は組合側での対応
- 簡単のためOPと記載しているがメディアのSP,CA検証に必要なOP一式をOPRが作成
- 申請後は固定URLからいつでもOP一式を取得可能

マニュアルに沿ってアカウント登録、OP登録申請する部分

CA ServerによるSP,CAの作成

記事編集時に自動的にCAを発行する実装が必要



CA Server はメディアの署名鍵を預かり
サイト毎にSPを発行する

SP発行はGUI操作でも可
ですがCA発行はAPI連携
で発行する実装が必要

SPは /.well-known/sp.json
に設置するだけでブラウザ
(拡張機能)が自動読み込み

CAはHTMLの<script>タグ
で紐付けると読み込まれます

いずれも非対応ブラウザ
には影響しません
(scriptタグといってもJS
が実行される訳ではない)

https://docs.originator-profile.org/ja/tutorial/sp-setup-guide/
https://docs.originator-profile.org/ja/tutorial/cas-setup-guide/

技術課題と導入・実装の容易化

技術課題と対応

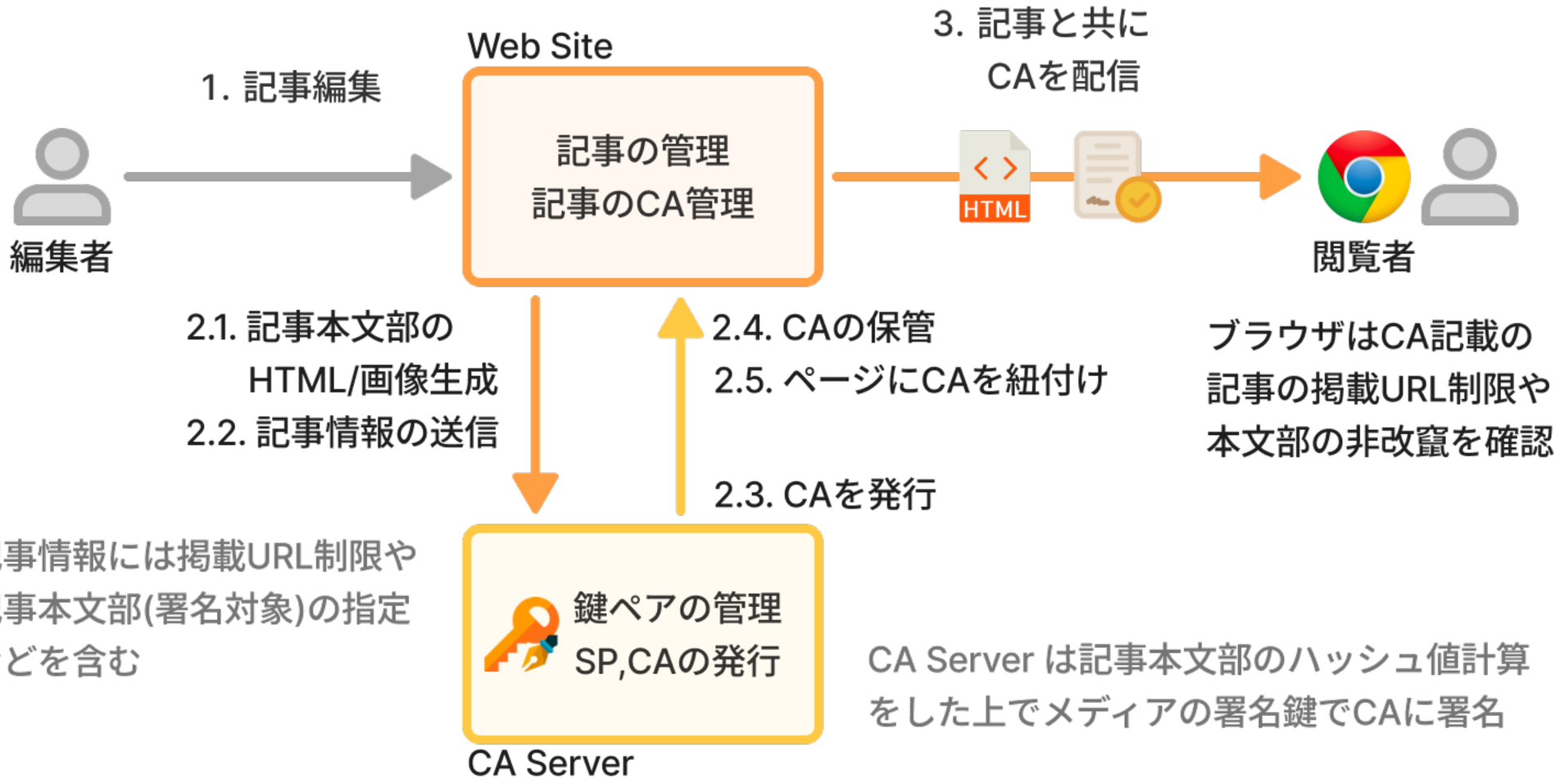
現行仕様での実装ポイント・導入容易化サービスなど

- 導入・設定だけで対応したい
  - ⇒ OSS CMS にはプラグイン、CDN 利用者にはリバプロ型サービスなどを提供
- 商用 CMS/headlessCMS
  - ⇒ 各ベンダーと連携・実装支援を進行中
- 仕組みの理解・お試し
  - ⇒ Playground サービスを含むドキュメント・リファレンス・参照実装の公開
- 開発・デバッグ
  - ⇒ Inspector や Debugger などの検証ツール・デバッグツールを提供中
- CA (コンテンツ証明書) の作成
  - ⇒ 署名サーバ (CA Server) を提供中
- 有効期限管理/自動更新
  - ⇒ 自動更新 CDN を提供予定
- 発行済みデータの確認
  - ⇒ モニターツールを提供予定
- 疑問解消・お悩み相談・仕様議論
  - ⇒ OP Tech Meetup!!!

サービス提供や採用を検討頂く方、気軽にご相談・お問い合わせください

CA ServerによるCA作成

HTML(の一部)と記事情報を送ってCAを生成

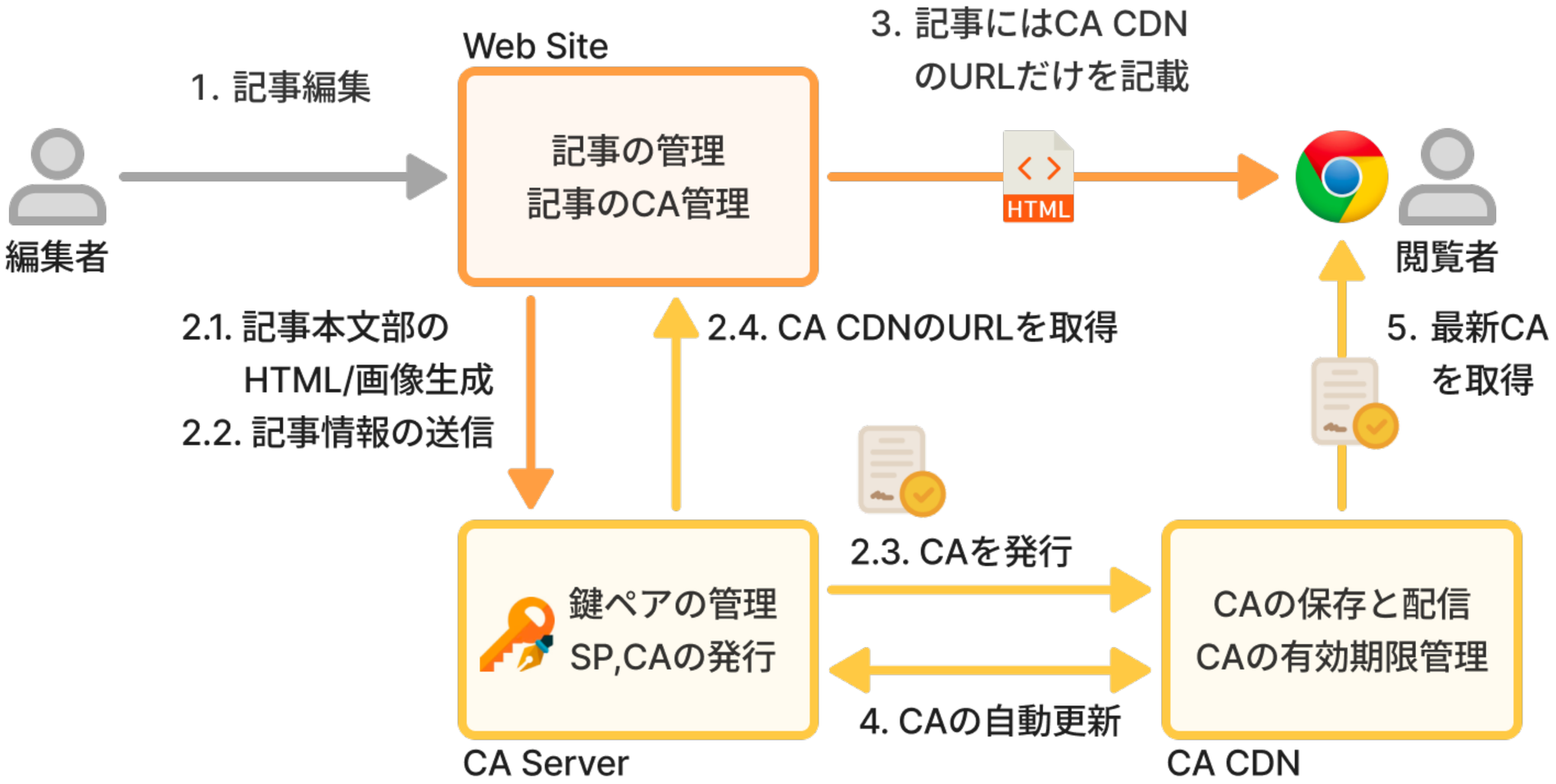


- CA記載内容(記事情報)JSON作って送るREST API
- HTMLなど送信してコンテンツハッシュ値計算も任せられる
- 細かな仕様変更追従もCA Serverが吸収
- 勿論利用は任意/詳しくは電通総研様のセッションにて

API利用には事前にアクセストークンの発行が必要です (詳細はマニュアル参照)

SP,CAの有効期限問題とCA CDN

署名データ＝有効期限があるのは自動更新サービスで解決



- **CA有効期限内の再発行実装は丸投げ可**
- CA CDNは現在詳細設計中。利用可能になる段階で告知
- SPは容易に再発行出来るので対象外(継続検討中)
- 勿論利用は任意/詳しくは電通総研様のセッションにて

ORIGINATOR PROFILE CIP

デジタル空間に、もっと信頼を。

デジタル空間に、もっと信頼を。

是非皆さんご一緒に！