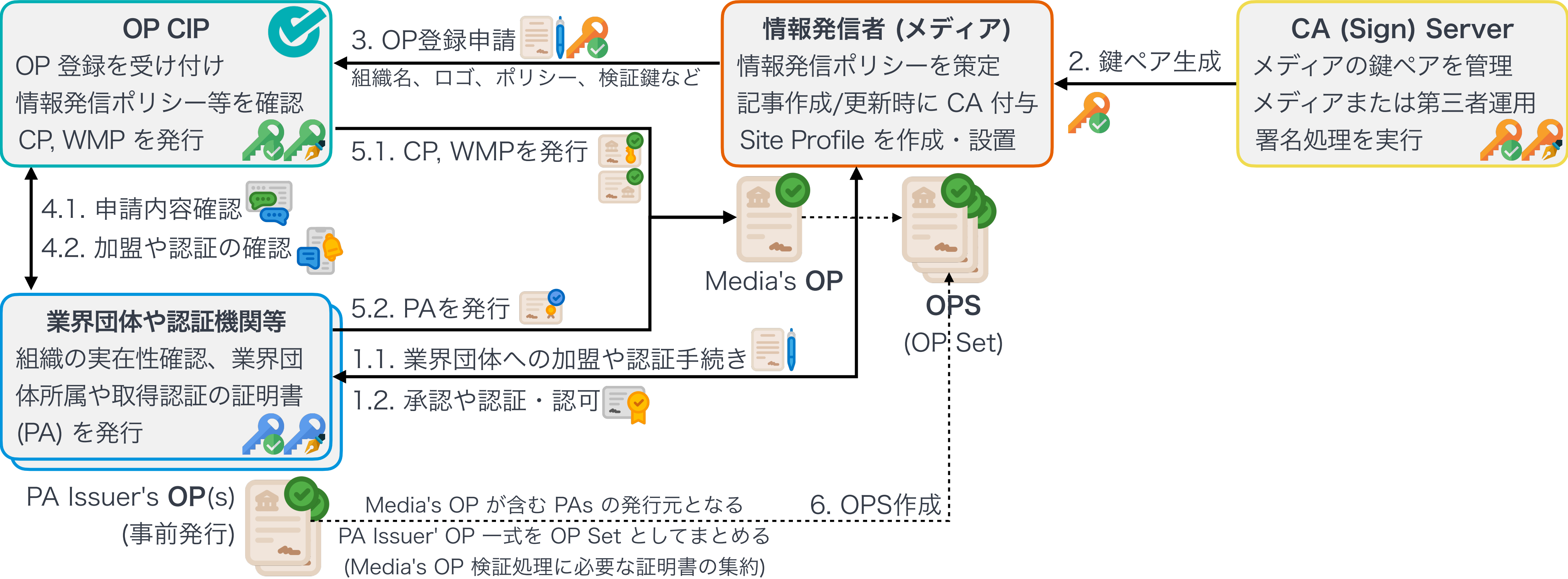


Originator Profile の仕組み

OP の登録と発行手続き



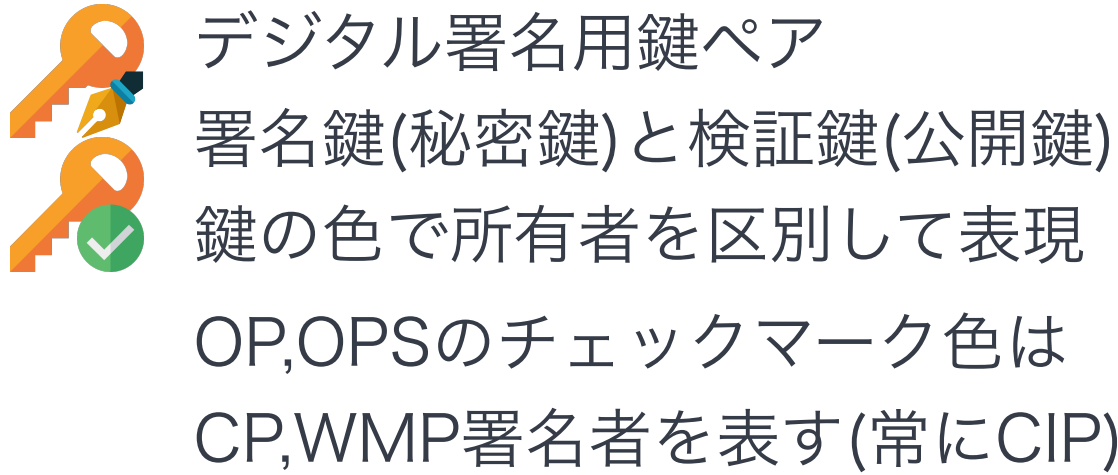
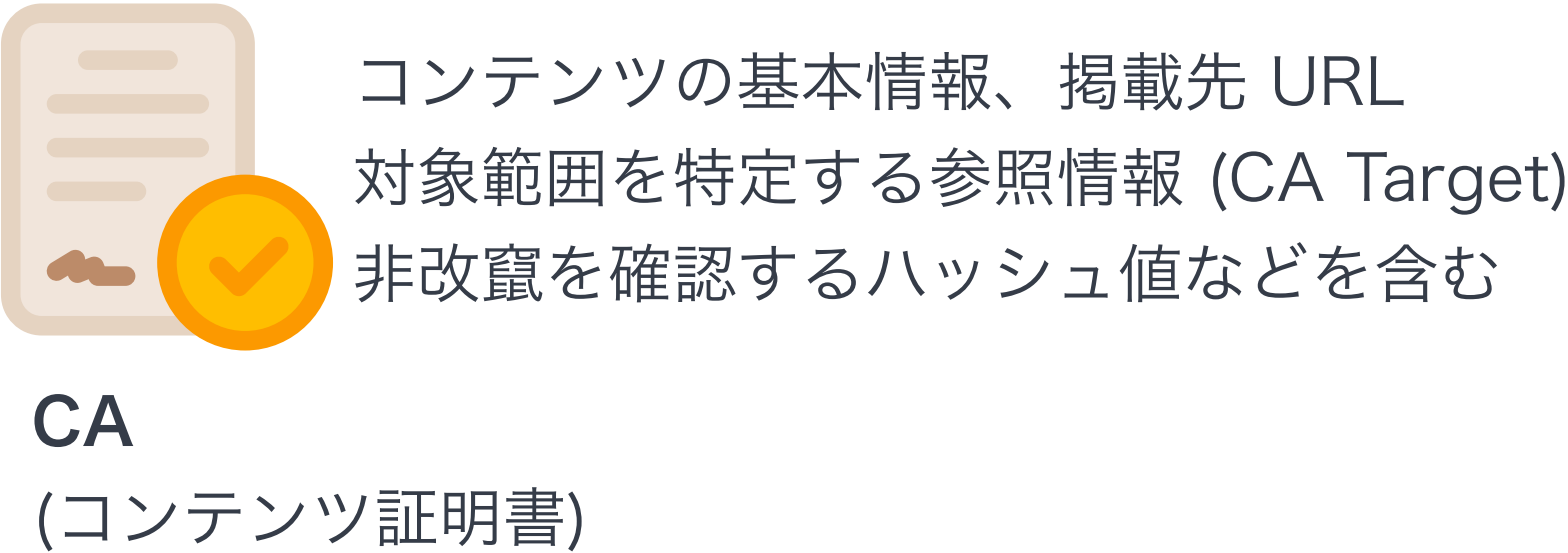
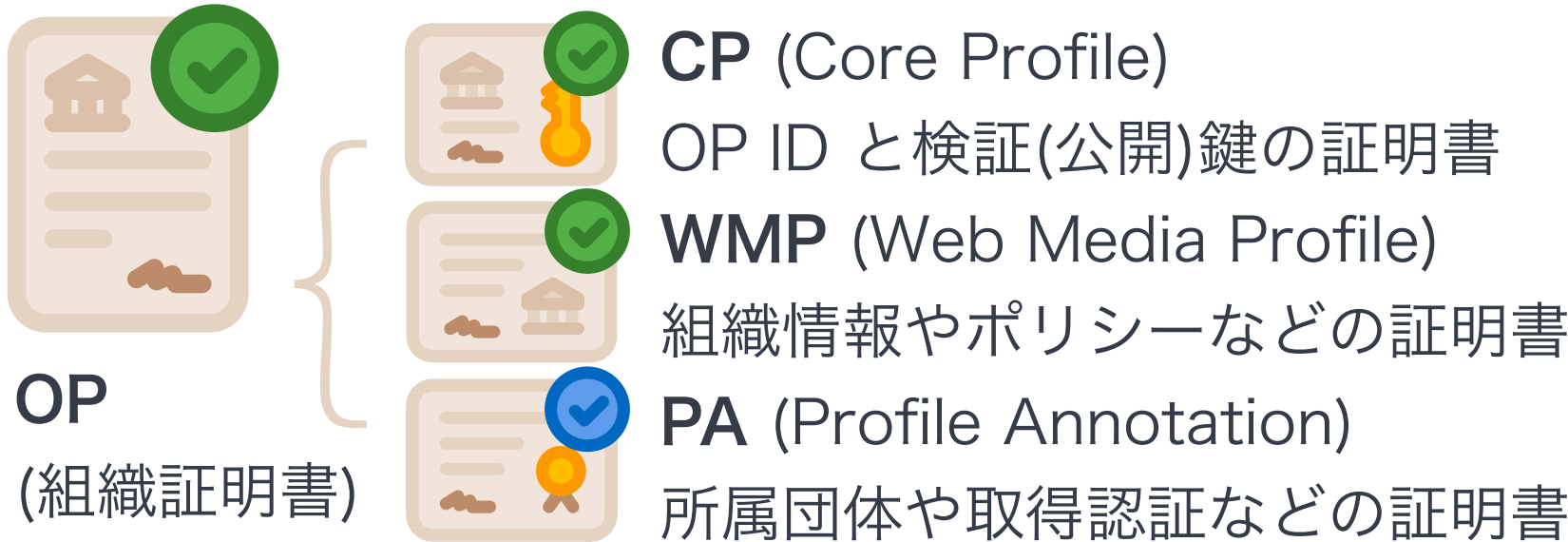
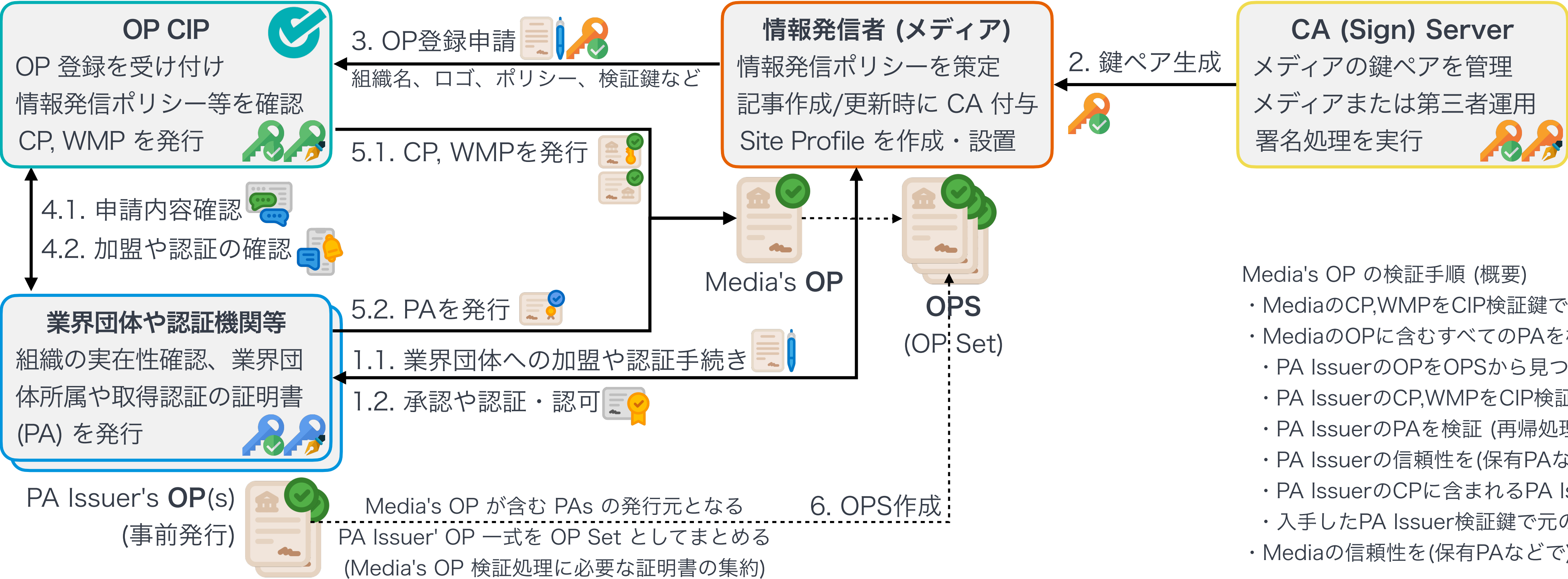
- CP (Core Profile)**
OP ID と検証(公開)鍵の証明書
- WMP (Web Media Profile)**
組織情報やポリシーなどの証明書
- PA (Profile Annotation)**
所属団体や取得認証などの証明書



コンテンツの基本情報、掲載先 URL
対象範囲を特定する参照情報 (CA Target)
非改竄を確認するハッシュ値などを含む

デジタル署名用鍵ペア
署名鍵(秘密鍵)と検証鍵(公開鍵)
鍵の色で所有者を区別して表現
OP,OPSのチェックマーク色は
CP,WMP署名者を表す(常にCIP)

OP の登録と発行手続き



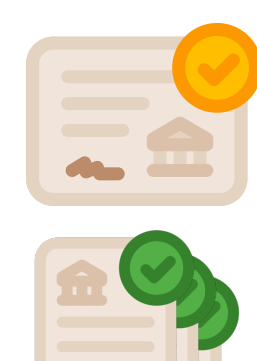
省略や順序無視あり(実運用手順は未定義)

SP (Site Profile) の作成と設置





SP
(サイト証明書)



WSP (Web Site Profile)
サイト情報の証明書



OPS (OP Set)
メディアと PA 発行者の OP



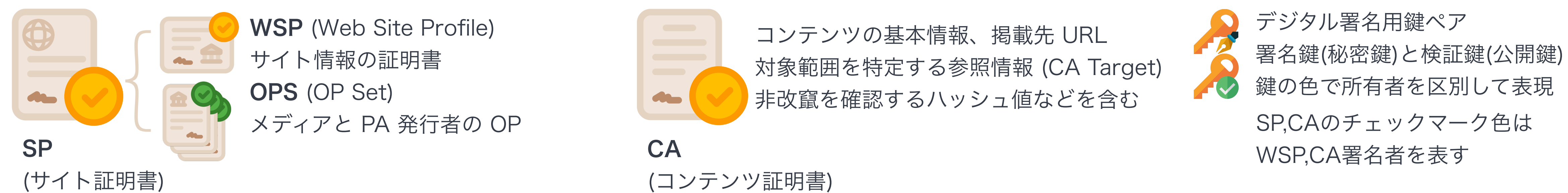
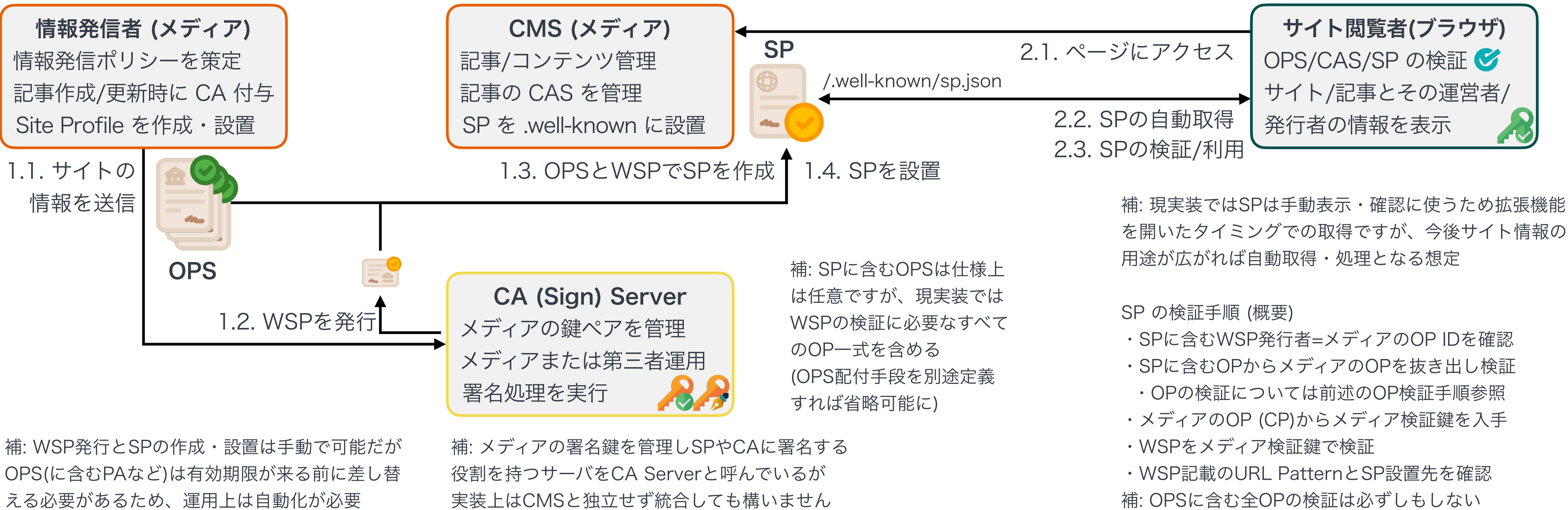
CA
(コンテンツ証明書)

コンテンツの基本情報、掲載先 URL
対象範囲を特定する参照情報 (CA Target)
非改竄を確認するハッシュ値などを含む



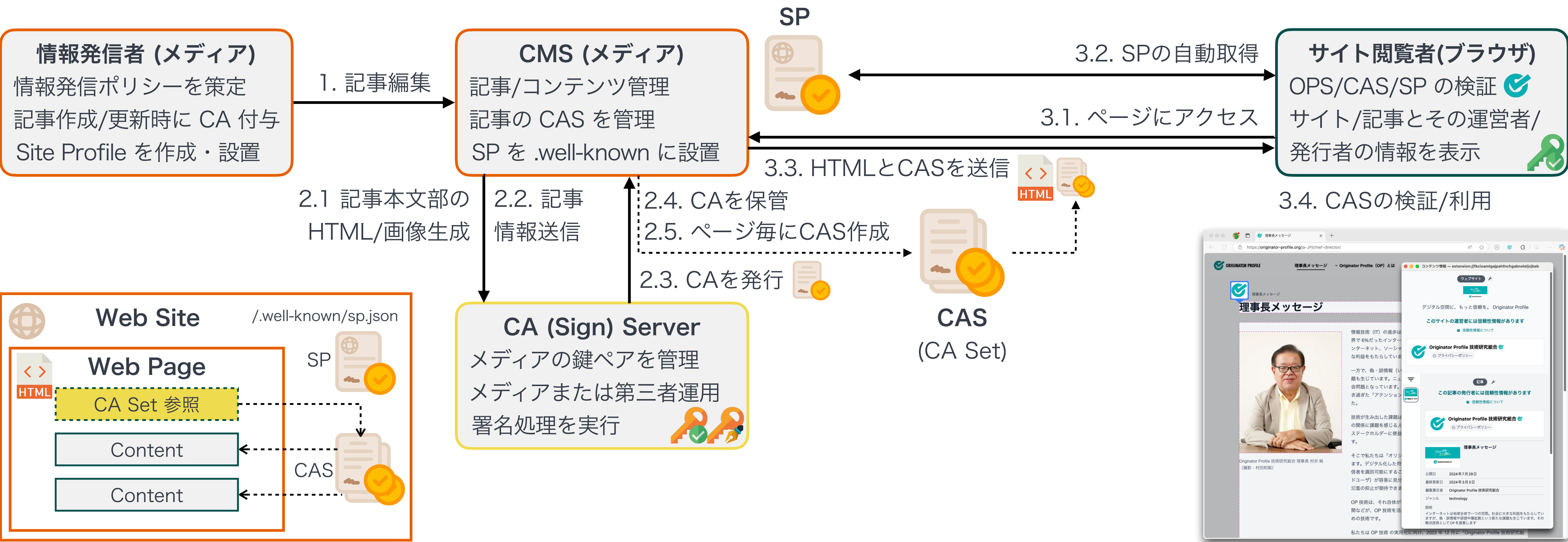
デジタル署名用鍵ペア
署名鍵(秘密鍵)と検証鍵(公開鍵)
鍵の色で所有者を区別して表現
SP,CAのチェックマーク色は
WSP,CA署名者を表す

SP (Site Profile) の作成と設置



サイト情報と共にOPSも送りSPを受け取る方法もあり

CA (Content Attestation) の作成と送信



SP
(サイト証明書)

WSP (Web Site Profile)
サイト情報の証明書

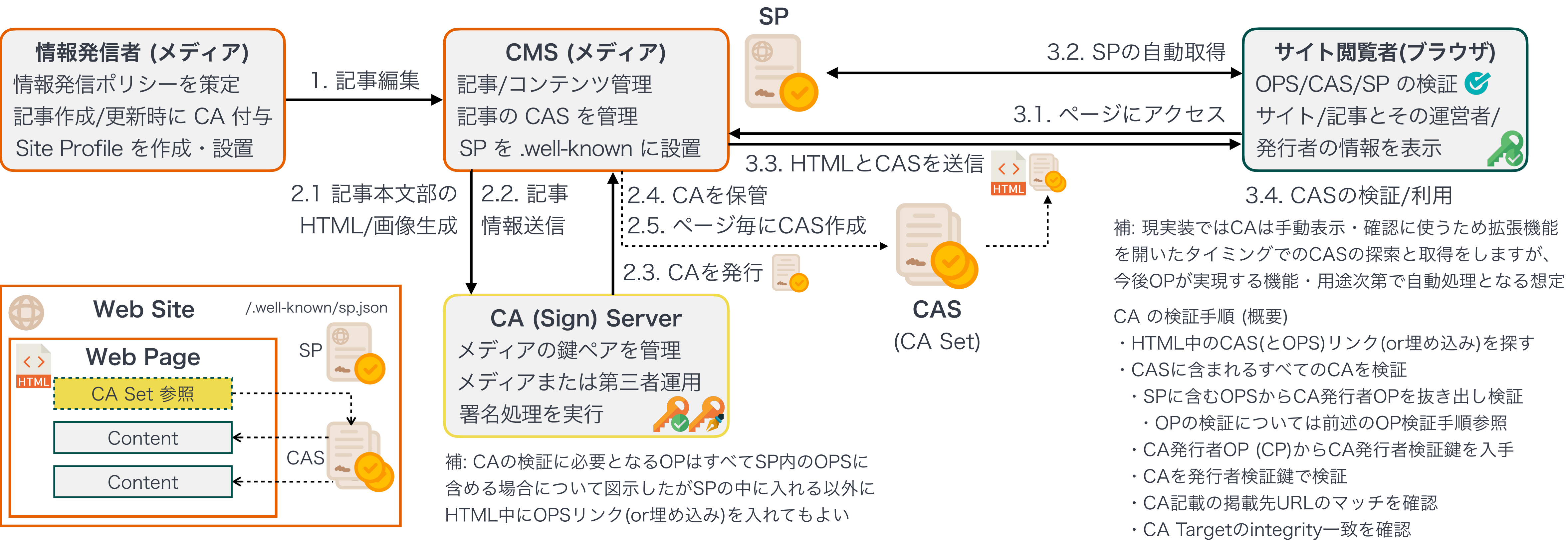
OPS (OP Set)
メディアと PA 発行者の OP

CA
(コンテンツ証明書)

コンテンツの基本情報、掲載先 URL
対象範囲を特定する参照情報 (CA Target)
非改竄を確認するハッシュ値などを含む

デジタル署名用鍵ペア
署名鍵(秘密鍵)と検証鍵(公開鍵)
鍵の色で所有者を区別して表現

CA (Content Attestation) の作成と送信



SP
(サイト証明書)

WSP (Web Site Profile)
サイト情報の証明書

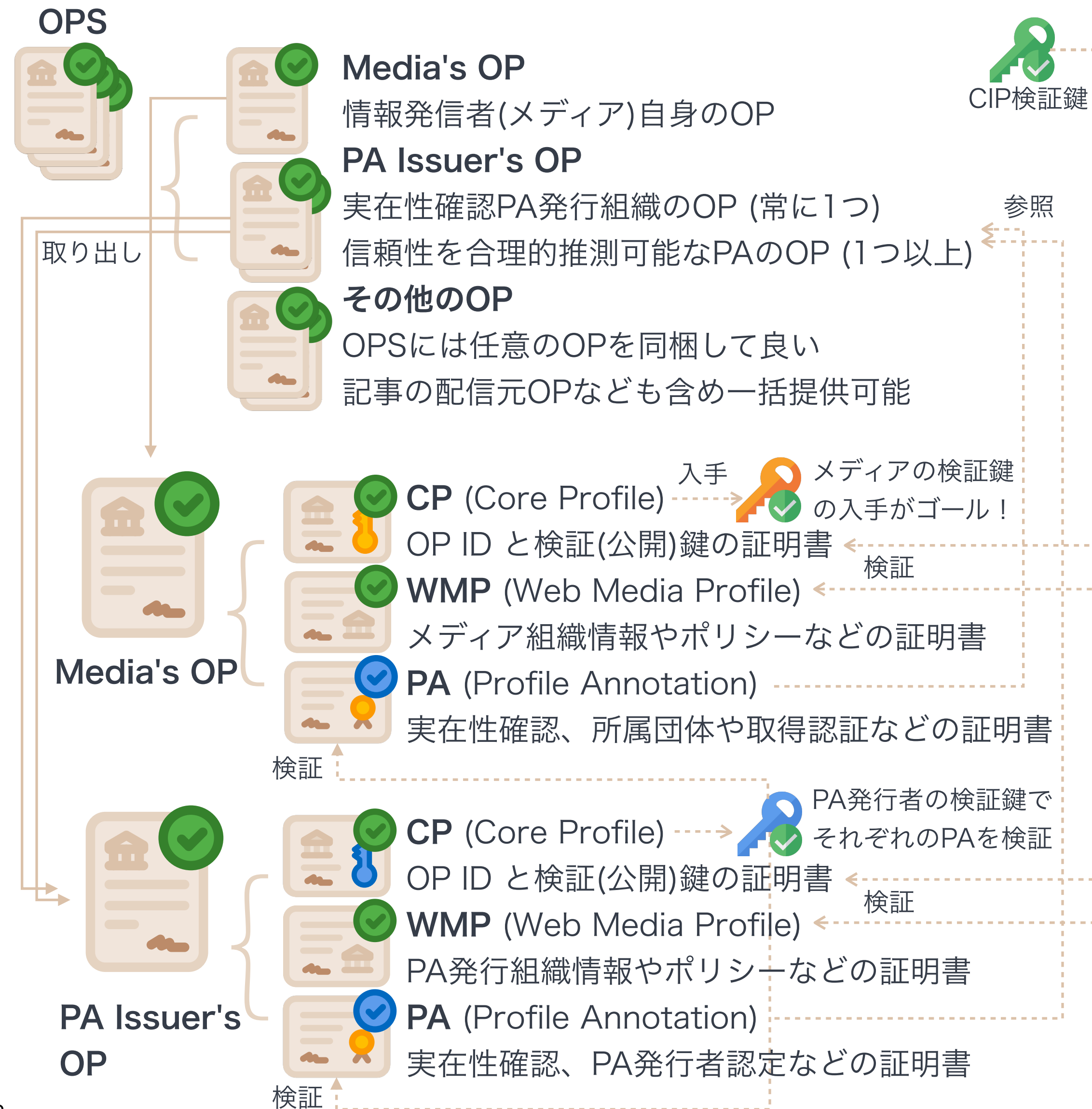
OPS (OP Set)
メディアと PA 発行者の OP

CA
(コンテンツ証明書)

コンテンツの基本情報、掲載先 URL
対象範囲を特定する参照情報 (CA Target)
非改竄を確認するハッシュ値などを含む

デジタル署名用鍵ペア
署名鍵(秘密鍵)と検証鍵(公開鍵)
鍵の色で所有者を区別して表現

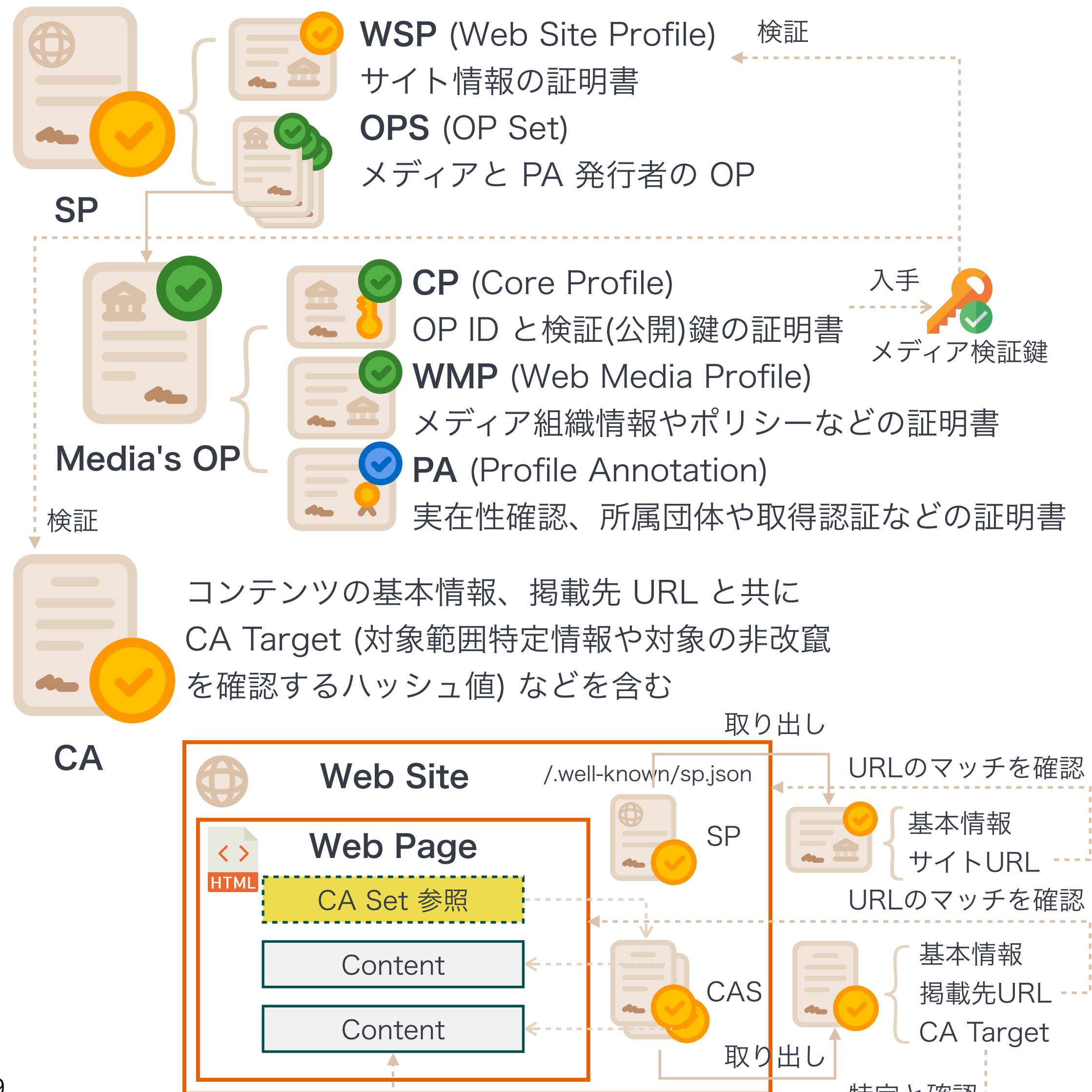
OP の検証処理



1. OPSから対象組織のOPを選択し取り出し
 - ・ 例: SPやCAを検証する(検証鍵が必要な)場合、それらの発行者OP(メディアのOP)が対象
2. 検証組織のCP,WMPをCIP検証鍵で検証
 - ・ CIP検証鍵はブラウザ同梱など別途事前に入手
3. 検証対象OPに含むすべてのPAを検証 (ループ処理)
 - ・ PA IssuerのOPを(OPSから)探しCP,WMP,PAsを入手
 - ・ PA IssuerのCP,WMPをCIP検証鍵で検証
 - ・ PA IssuerのOPに含むすべてのPAを検証 (再帰処理)
 - ・ PA Issuerの信頼性を(保有PAなどで)判断
 - ・ PA IssuerのCPに含むPA Issuer検証鍵を入手
 - ・ 入手したPA Issuer検証鍵で元のPAを検証
4. 対象組織の信頼性を(保有PAなどで)判断

すべてのCP,WMP,PAと鍵の失効確認も行います(未実装/説明割愛)

CA, SP の検証処理



1. SPとCASを取得しWSP,OPS,CAを取り出し
 - ・ SPは.well-known設置なので自動取得
 - ・ CASはHTMLからのリンク(または直接埋め込み)
2. メディア(WSP,CA発行者)のOPを取り出し検証
 - ・ 検証鍵の入手までの手順は「OPの検証処理」を参照
3. WSPの検証
 - ・ メディアの検証鍵でWSPを検証
 - ・ WSP記載のサイトURL Patternのマッチを確認
4. CAの検証
 - ・ メディアの検証鍵でCAを検証
 - ・ CA記載の掲載先URL Patternのマッチを確認
 - ・ すべてのCA Targetのハッシュ値の一致を確認
 - ・ テキストはCSS Selector対象要素のハッシュ値
 - ・ 画像などはバイナリファイル全体のハッシュ値

CA発行者OPをSPに含めない場合は別途OPSをHTMLからリンク(説明割愛)