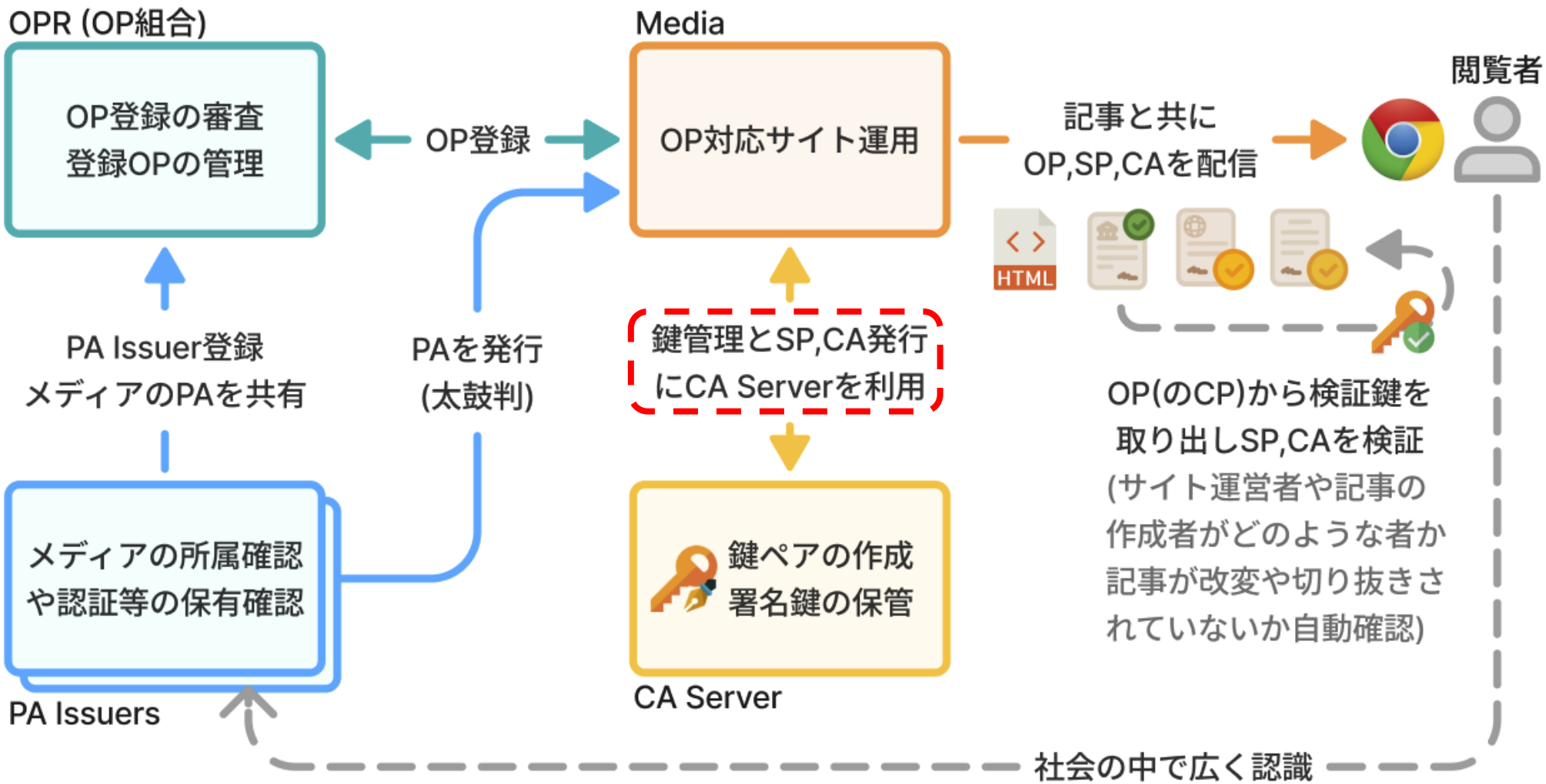
Originator Profile Tech Meetup

CA Server(+CA CDN)
ご説明資料

Originator Profile技術研究組合

2026年10月27日

CA発行の仕組み


OPR (OP組合)
OP登録の審査
登録OPの管理
OP登録
Media
OP対応サイト運用
閲覧者
記事と共に
OP,SP,CAを配信
HTML
PA Issuer登録
メディアのPAを共有
PAを発行
(太鼓判)
鍵管理とSP,CA発行
にCA Serverを利用
OP(のCP)から検証鍵を
取り出しSP,CAを検証
(サイト運営者や記事の
作成者がどのような者か
記事が改変や切り抜きさ
れていないか自動確認)
メディアの所属確認
や認証等の保有確認
鍵ペアの作成
署名鍵の保管
PA Issuers
CA Server
社会の中で広く認識

CAサーバーとは

Originator Profile（OP）におけるCAサーバー（Content Attestation Server）とは、コンテンツの発信者が、自身が発信するWeb記事や広告などのコンテンツに対して、真正性を示す「Content Attestation（CA：コンテンツ証明）」を発行・管理するためのサーバーです。

主な役割

- **鍵ペアの作成・署名鍵の保管**
- **SP（サイトプロファイル）の発行**
- **CA（コンテンツ証明）の発行・更新**
- **CMSとの連携（APIによるCA発行）**

今回ご説明するCA Serverは参加企業様が独自で仕組みを構築せずに導入するための電通総研が提供するサービスです。

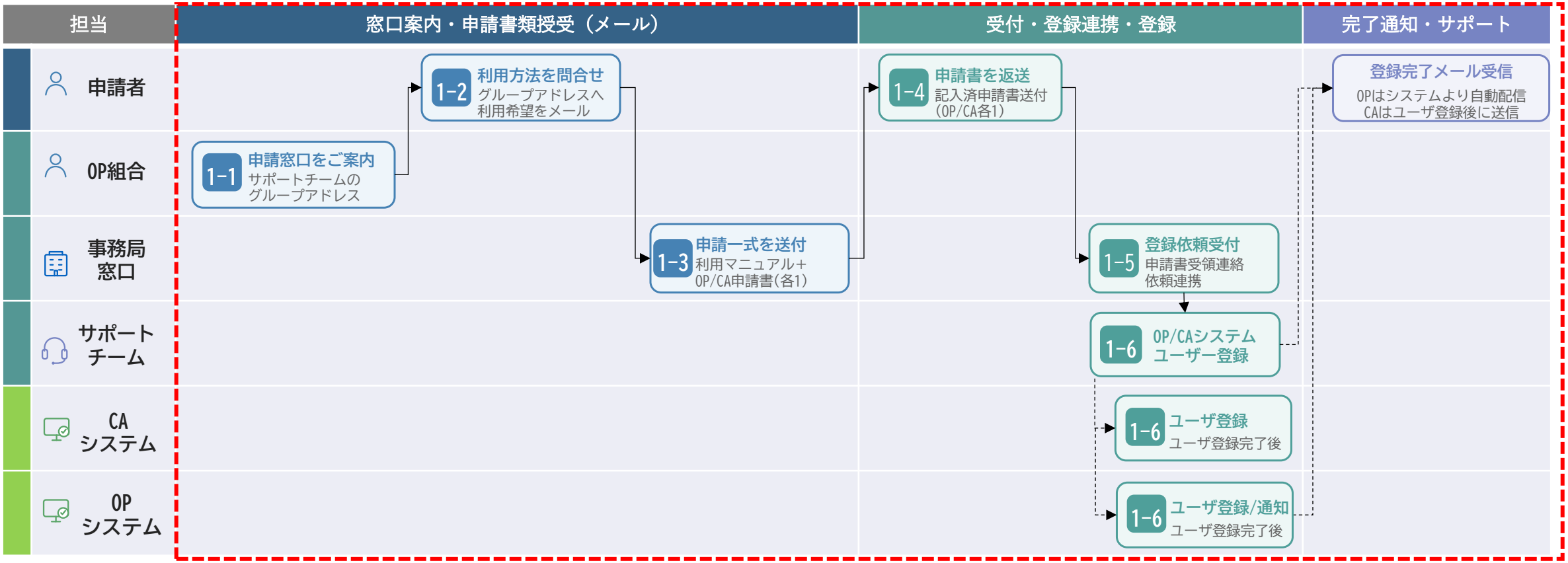
CAサーバー利用のSTEP

OP導入決定後にCAサーバー（Content Attestation Server）によるCA発行に至るまで、６つのステップが必要になります。



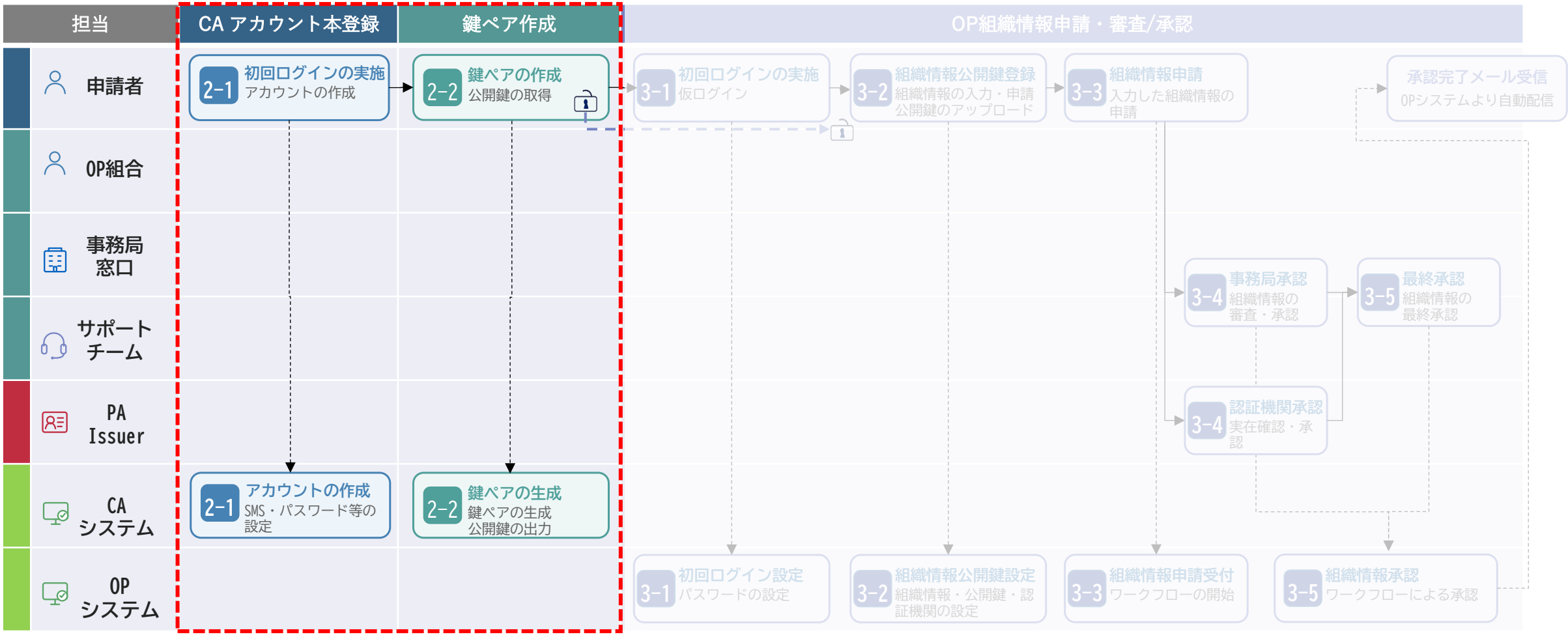
STEP1：利用申請（OP Registory/CA Serverのアカウント作成）

OP組合の窓口より申請書類の授受を行い、OP/CAそれぞれのアカウント申請を行います。



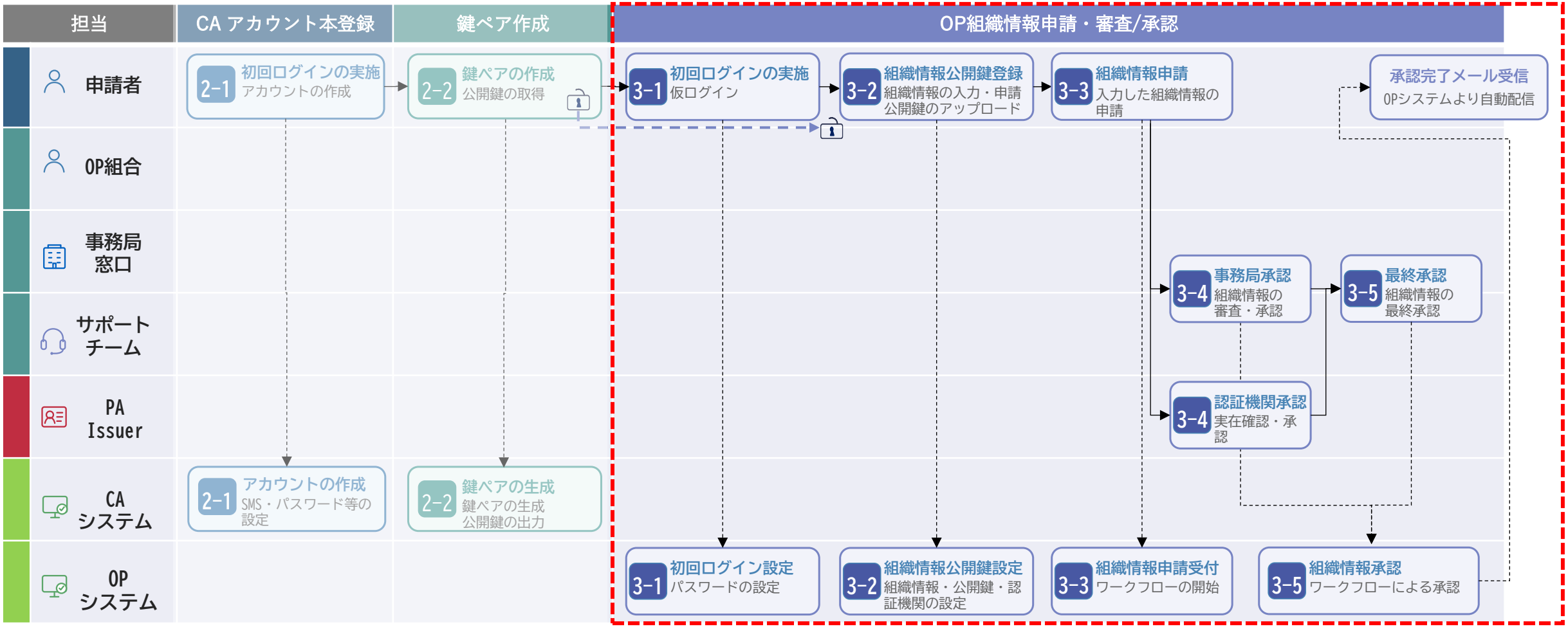
STEP2：鍵ペアの作成

有効化したCAアカウントを使用してCA Serverで鍵ペアを作成します。



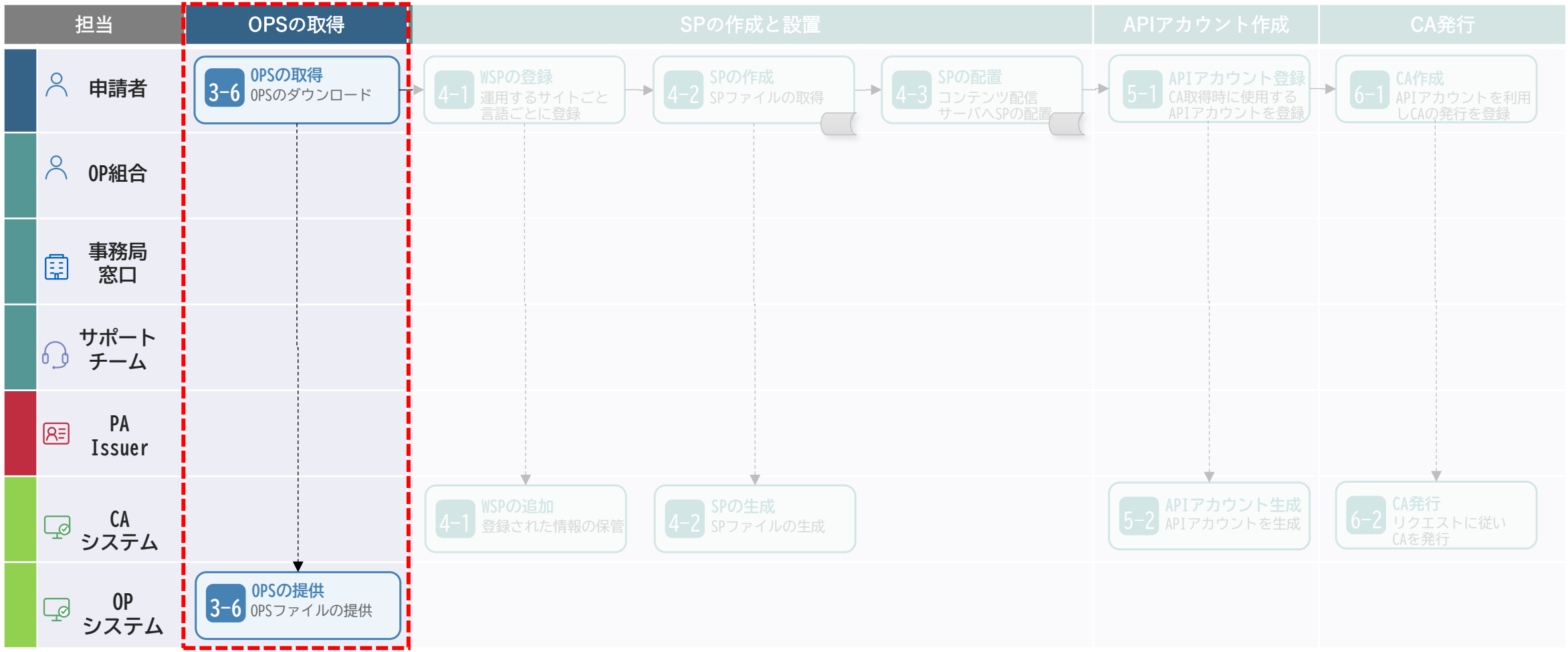
STEP3：組織情報企業情報申請・OPSの発行

申請したアカウントで作成した鍵ペアも付与して組織情報を申請し、OPSを発行します。



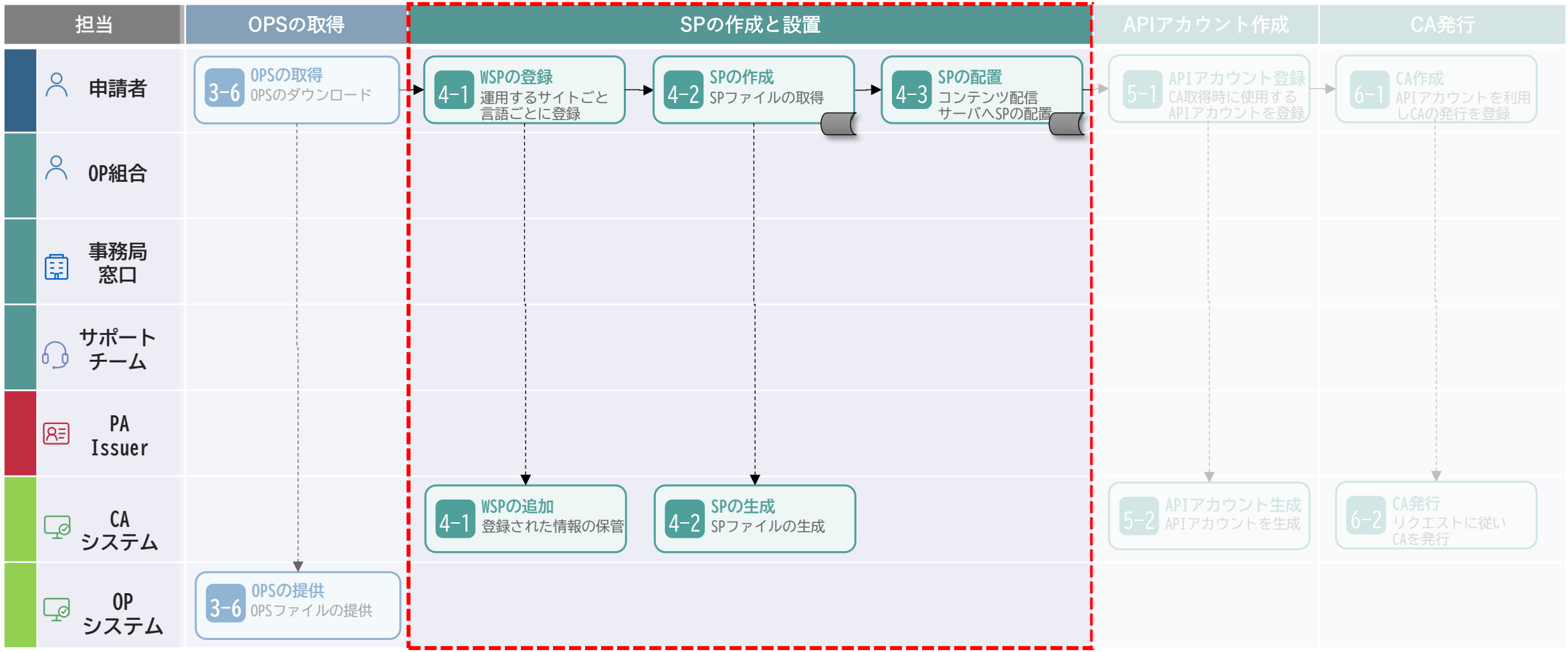
STEP3：組織情報企業情報申請・OPSの発行

申請したアカウントで作成した鍵ペアも付与して組織情報を申請し、OPSを発行します。



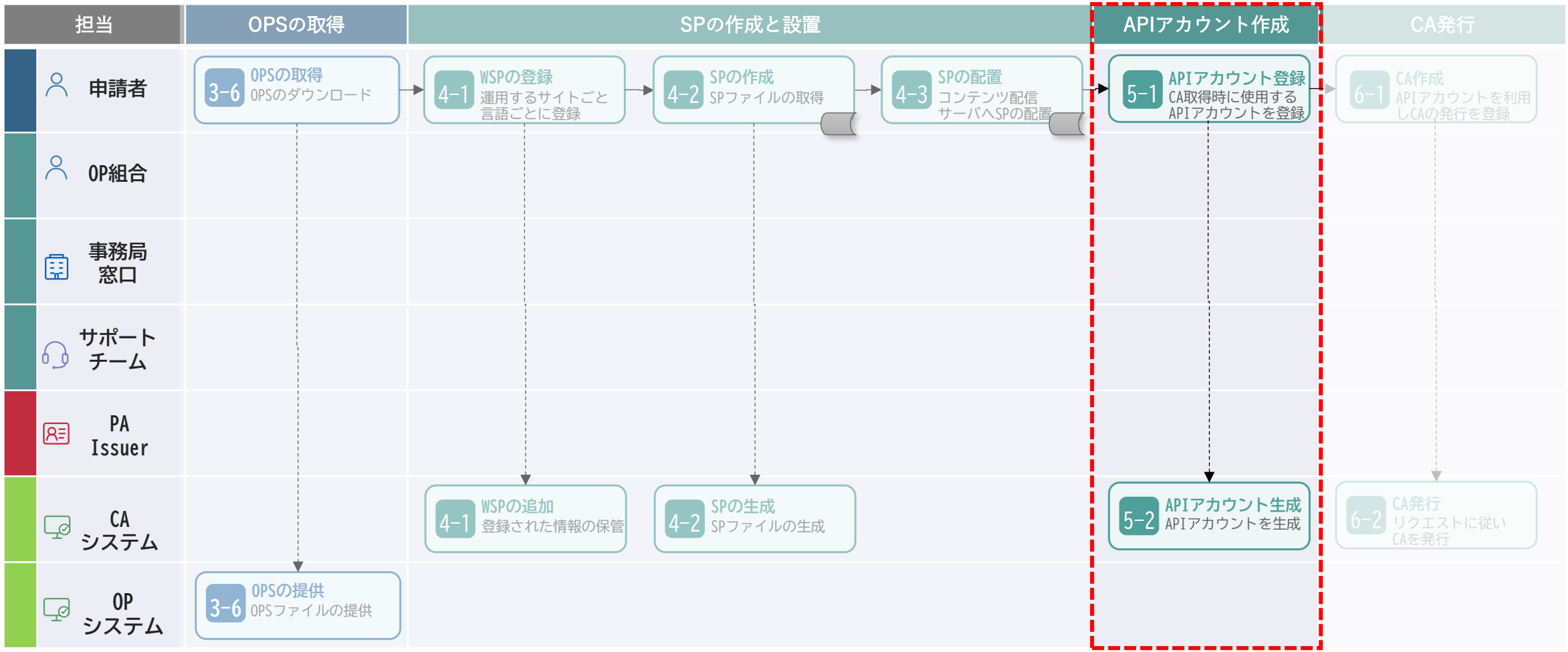
STEP4：SP作成

取得したOPSを使用し、WSPを登録しSPを作成しコンテンツを提供する環境に配置します。



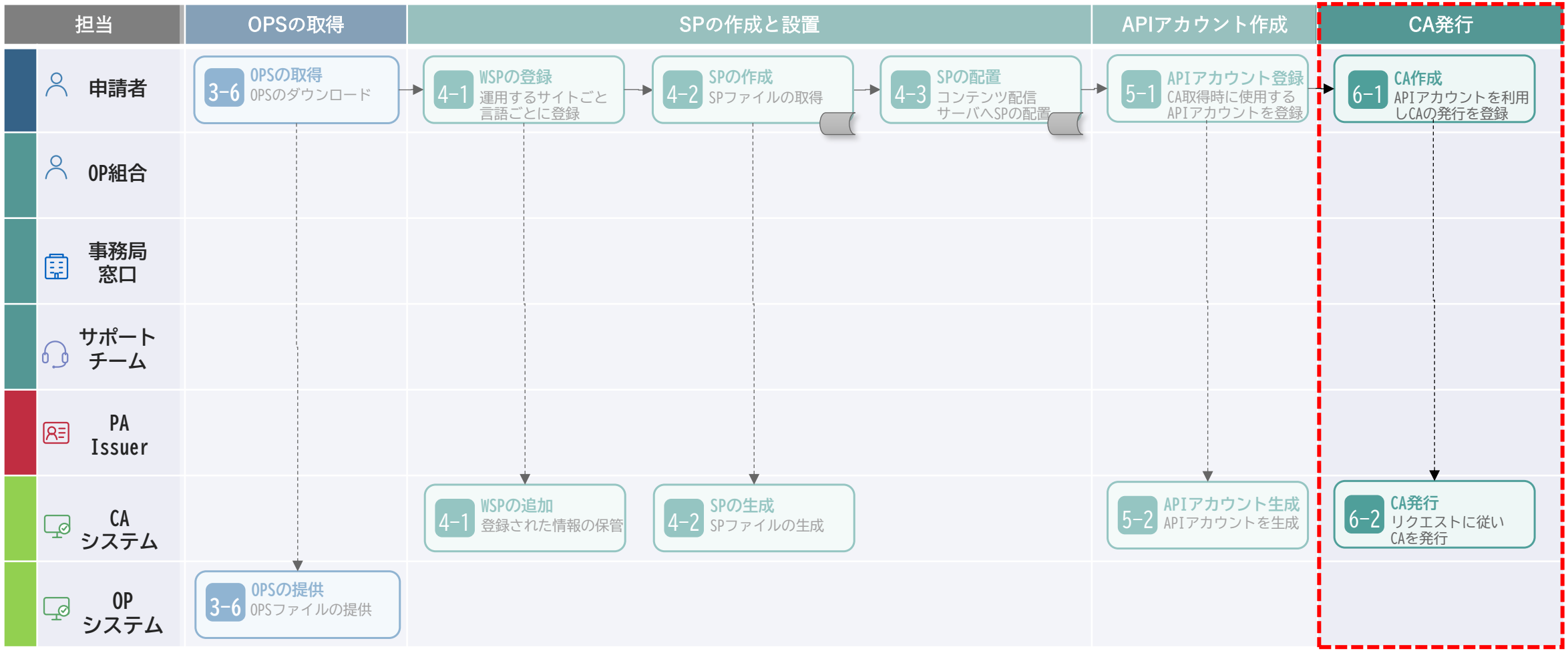
STEP5： APIアカウント作成

コンテンツを配信するCMS等から利用するCA発行用APIアカウントを作成します。



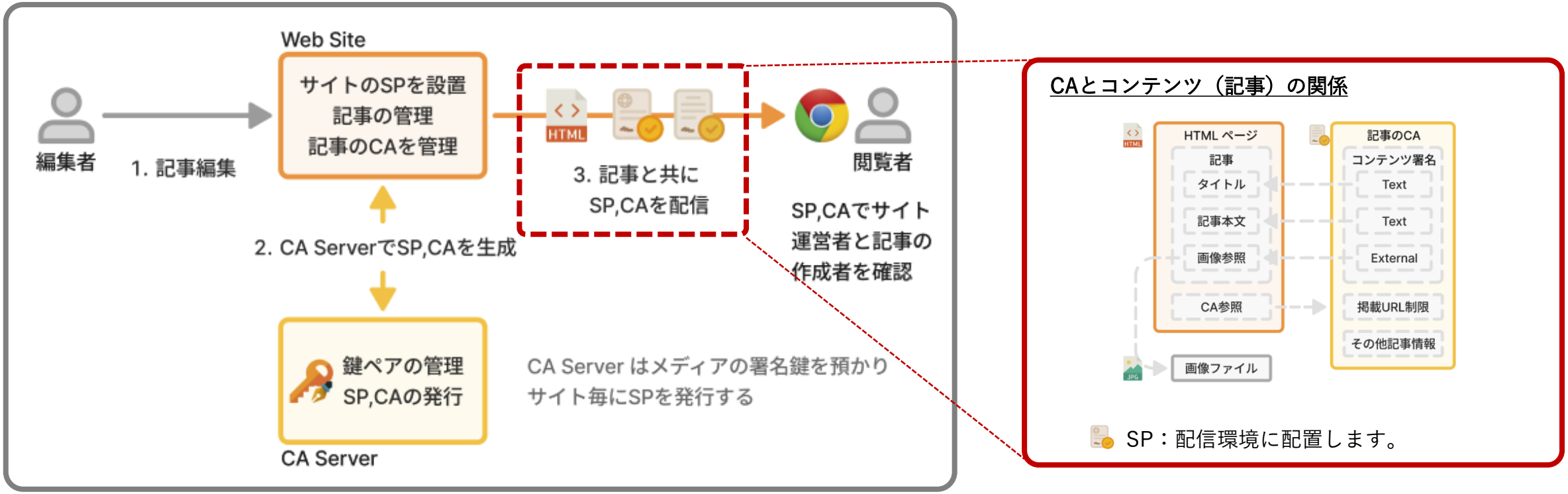
STEP6： CA発行

コンテンツを配信するCMS等から作成したCA発行用APIアカウントを用いてCAを発行します。



ご参考：発行したSP・CAとコンテンツ（記事）の関係

- 発行したSP・CAはコンテンツとともに配信することで閲覧者は、運営者と記事の作成者を確認することができます。



CAの運用について

- コンテンツの発信者が、自身が発信するコンテンツに対して真正性を示す**Content Attestation（CA：コンテンツ証明）には有効期限の設定が必要になります。CA Serverではデフォルト設定を「発行から1年間」**としています。

- また、継続して該当コンテンツの真正性を維持するためには、 CAの有効期限を迎える前に更新が必要になります。

🕒 **有効期限の考え方**

- **発行時の指定**
    - CAの有効期間は、発信者がCAサーバーで発行する際に任意で指定した期間（iat：発行日、exp：満了日）で決まりますが、**通常は1年以下が推奨**されています。

- **署名アルゴリズムの寿命**
    - 将来的な暗号の危殆化や耐量子計算機暗号（PQC）への移行を見据え、2026年時点の指針として、**3〜4年を超える長期の有効期間は推奨されていません。**

- **実質的な有効期間**
    - CAの有効性はそれを発行する組織の「OP（Originator Profile）」に依存するため、**CAの実質的な有効期間は「CA自身の有効期間」と「OPの有効期間」の共通部分（重なる期間）**となります。

CAと各証明書との関係性と運用

🔗 各証明書との関係性

CAは、サイト全体を証明する他のプロファイルと連動して機能します。

- **OP（Originator Profile）との関係**
  - OPと CAの関係性は、「組織証明（大元の身元証明書）」と「記事証明（その組織が発行した個々の成果物）」という関係性にあります。
  - 組織の身元を証明するOPの有効期間が切れると、たとえCAの期限が残っていてもそのCAの検証は失敗になります。

- **SP（Site Profile）との関係**
  - SP（Web Site Profile）と CA（Content Attestation）の関係性は、「サイト全体の証明」と「個々の記事の証明」という“全体と個”の関係性にあります。

⚠ 有効期間を短く保つ理由と運用

- **セキュリティの担保**
  - 個別記事の失効機能がないため、期間を短くしてリスクを軽減します。
- **運用の自動化**
  - 手間を減らすため自動化が推奨されます。

CAの有効期限と更新

- 🕛 **CAの有効期限と更新**
  - 過去の記事であっても、その記事の信頼性証明（検証に成功する状態）を維持し続けたい場合は、**有効期限が切れる前にCAを再発行**し、**Webページ側を更新**する必要があります。
  - 何もしないまま有効期限が満了すると、そのCAは「失効」し、第三者がその記事を検証した際に「無効（証明が切れた状態）」と判定されてしまいます。
  - 更新には、**新しいCA（デジタル署名）の取得と保存とHTML側（CAS）への反映が必要になります。**

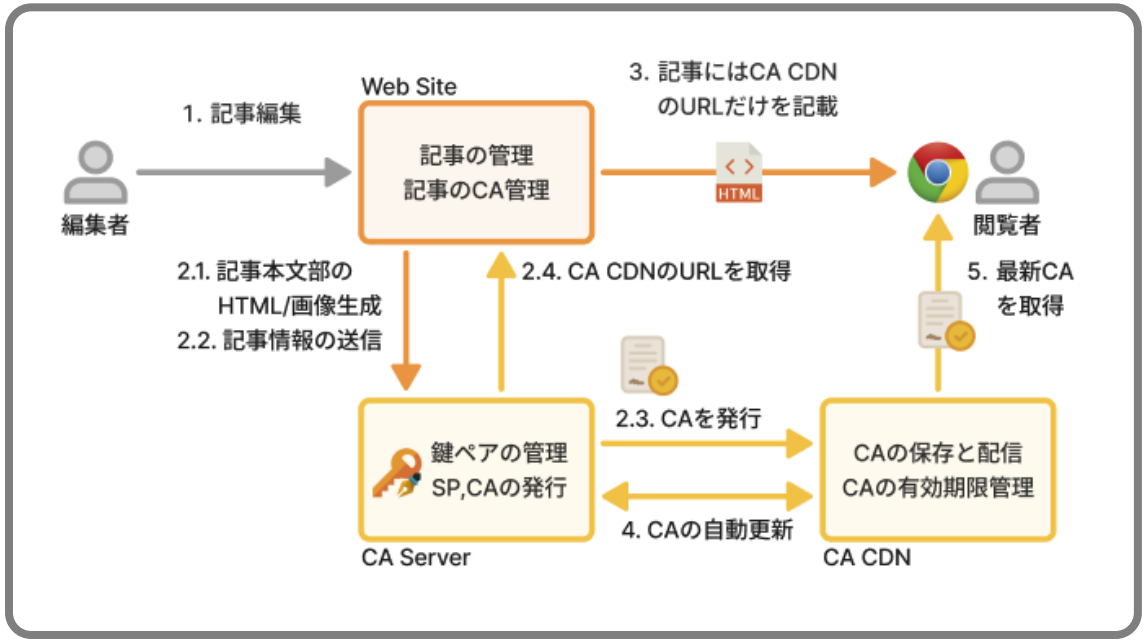
  ※記事を取り下げる場合、CAを再発行せずそのまま有効期限切れ（失効）を待つ運用も可能ですが、必要に応じてCAの公開を取り下げる等の運用が考えられます。

- 💡 **混同しやすい注意点**
  - **「OPの更新」と「CAの更新」について**
    - 組織の証明であるOP（最長398日）が更新されても、署名に使う公開鍵が変わらなければ、過去記事のCAを連動して再発行する必要はありません。
    - あくまで「**CA自身の有効期限（デフォルト1年）」が切れるタイミング**で、CAの再発行が必要になります。

CAの有効期限の課題と今後の方向性

- 🕛 **CAの有効期限の課題**
  - CAの有効期限の対応のための更新には、**新しいCA（デジタル署名）の取得と保存とHTML側（CAS）の反映が必要時なります。**
  - 膨大な量になると想定される過去の記事への更新は、システム的に大きな負荷になることが想定されます。

- 💡 **今後の方向性**
  - CAの更新負荷を低減するため、CA Serverに「**有効期限前に同一内容でCAを再発行しホストする CA CDNサービス**」の実装を検討中です。
  - CMS側でCA発行時にCA CDNのURL（CAの配置場所）を受け取り、記事内（CAS）に有効なCA配置先を指定いただく対応を行うことにより、指定したCAの有効期限の設定に従い、再発行処理の実装が不要となる想定です。





Originator Profile 技術研究組合（OP CIP）