戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

戦略的イノベーション創造プログラム（SIP）第2期／
ビッグデータ・AIを活用したサイバー空間基盤技術／
パーソナルデータ実証研究

トラストサービスに関するアーキテクチャとしての共通API仕様策定とその有効性に関する実証研究

2020年3月18日

セコムトラストシステムズ株式会社
セイコーソリューションズ株式会社

１．研究開発の背景と目的

①狙い

Society5.0やData Free Flow with Trust を実現するために、流通するデータの信頼性を確保する必要がある。

アプリケーションサービスは、その信頼性について、ユーザが特に意識せず安全安心に利用できる環境が必要である。そのため、データの発出やアクセス先を確実に認証、認可し、なりすましを無くし、流れるデータの完全性を担保するためのトラストサービスを、アプリケーションサービスが簡便に利活用できる環境を用意することが重要となる。

そのためトラストサービスの相互運用性を確保し開発効率の向上をねらい共通API仕様を策定、実証し、具現化に向けて課題を整理する。

②背景

最近の国際的なデジタルエコノミー推進の動きの中で、2018年7月「日EU経済連携協定（EPA）」の電子商取引において「署名が電子形式であるという理由だけで署名の法的有効性を否定してはならない」とされ、2019年1月の世界経済フォーラム年次総会（「ダボス会議」）にて国際間で「信頼ある自由なデータ流通（DFFT：データ・フリー・フロー・ウィズ・トラスト）」の確立が最重要課題であるべきことがわが国から提唱されている。

インターネットを利用したパーソナルデータなどの高機密情報が大量に流通しているが、ID、パスワードによる認証だけでは、「なりすまし、詐取、改ざん」に対して十分ではない犯罪事例も日常的に生じてきている。

また、Society5.0においては人を介さずにマシンtoマシン間の情報流通も加速度的に増加することが予想されDFFTの考え方はデータ連携を行う相手の認証だけでなく、流通するデータそのものの真正性担保が必要となる。

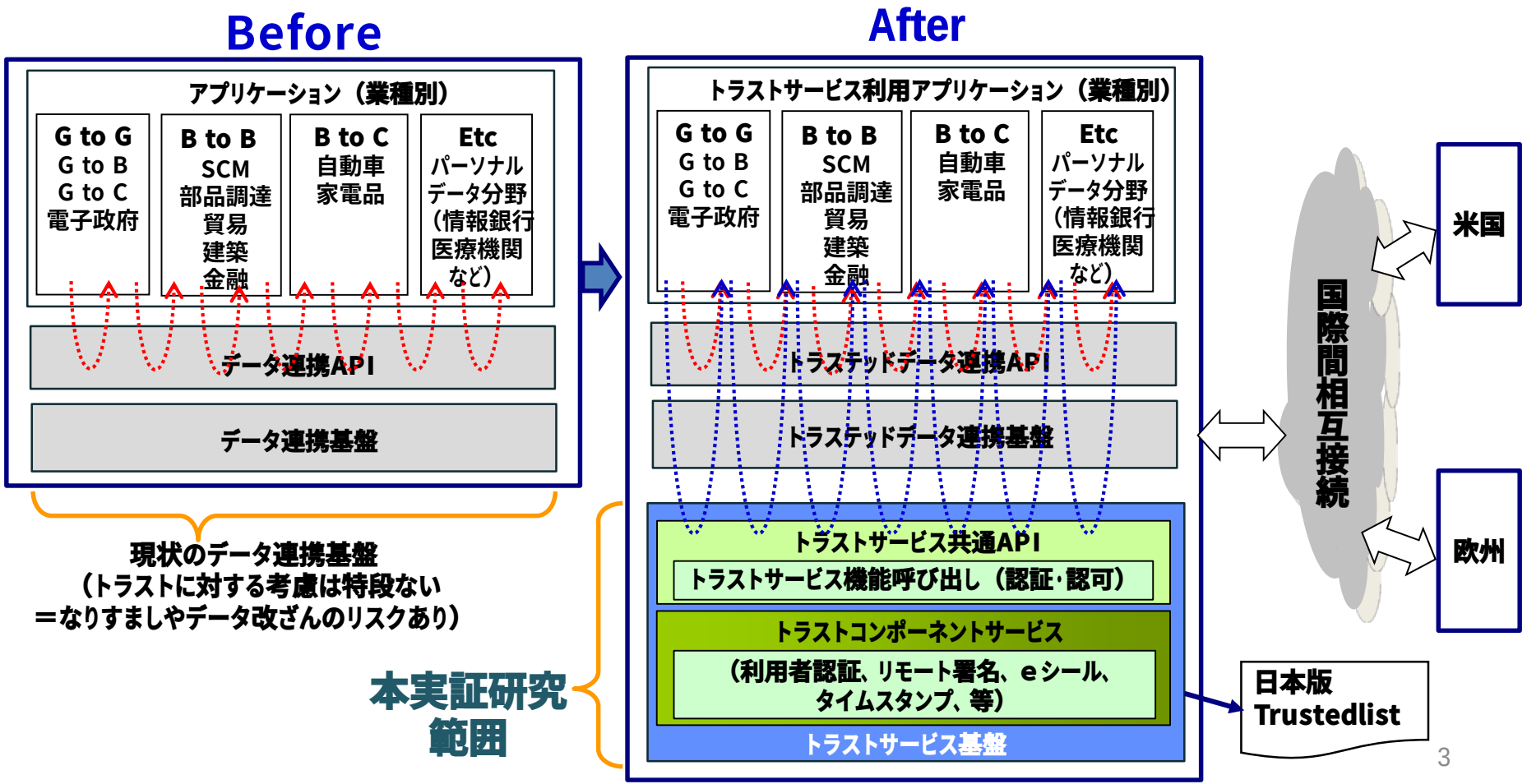
従って健全なData Driven Economyの発展を支え、EUなど国外との情報連携を可能とするためDFFTを支えるトラストサービス基盤として送信元のなりすましやデータの改ざん等を防止するための基盤づくりが求められている。

③課題・目的

現在、トラストサービス事業者が提供しているサービスは、それぞれ独自のインターフェイスを採用しており、上位アプリにとって必ずしも利用しやすく、相互運用が容易に実現できる仕様となっていない。また、トラストサービス事業者が信頼できること（トラストアンカー）を確認するしくみを機械可読可能な形で公開することが求められるが、わが国ではまだ十分に実現できていない。

従って、上記の課題解決のため、トラストサービスとのインターフェースを簡便に連携する共通API（トラストサービス共通APIという）を、トラストアンカーの検証を含み仕様を策定し実証を行い、アーキテクチャへの組み込みと課題を整理する。

2．トラステッドデータ連携構想におけるトラストサービス基盤の位置付け



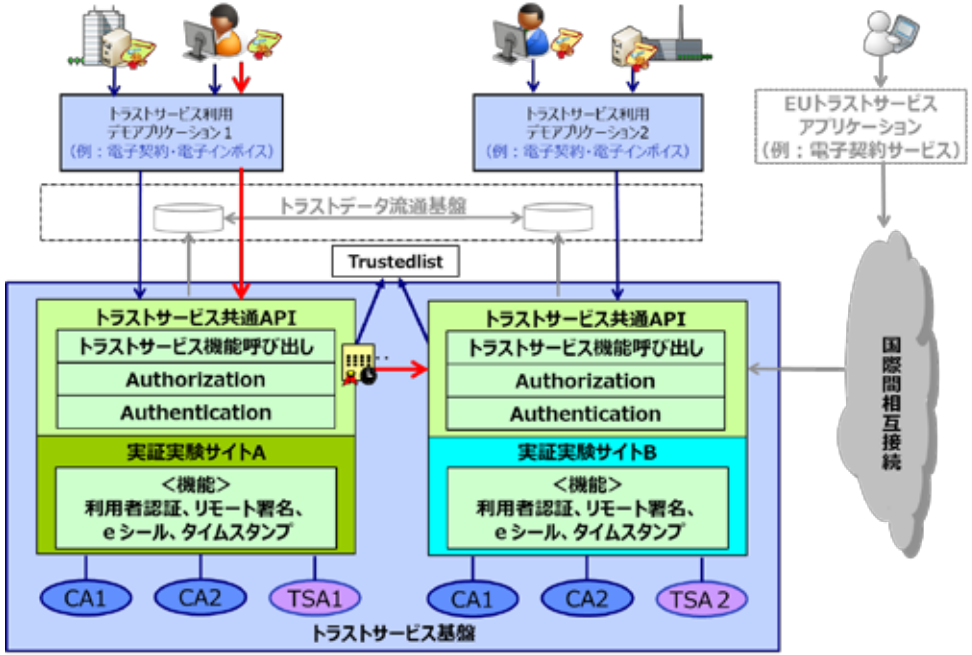
3．研究開発の内容

技術的課題と研究内容

現在、各トラストサービスは、サービス業者毎にAPIのインターフェース仕様やサービス利用時のユーザ認証仕様が異なるため、アプリケーション側は利用するサービス毎にそれらを実装する必要があり、**複数のトラストサービスと簡便に連携する環境が整っているとはいえない**。
そこで今回の実証研究では、**複数のトラストサービスと連携可能な共通APIを開発、検証することで、課題解決の実証を図る**。
研究期間の制約もあるため、共通APIとして整備するのは次ページに示す、鍵管理と、リモート署名、リモートシールについての共通APIに絞って整備を行なう。整備したAPIの実証の具体的なユースケースとして、実証実験サイトAと実証実験サイトBという異なるトラストサービス間でリモート署名を活用した電子契約とリモートシールを活用した電子インボイスのサービス関連系についての実証実験を行なう。

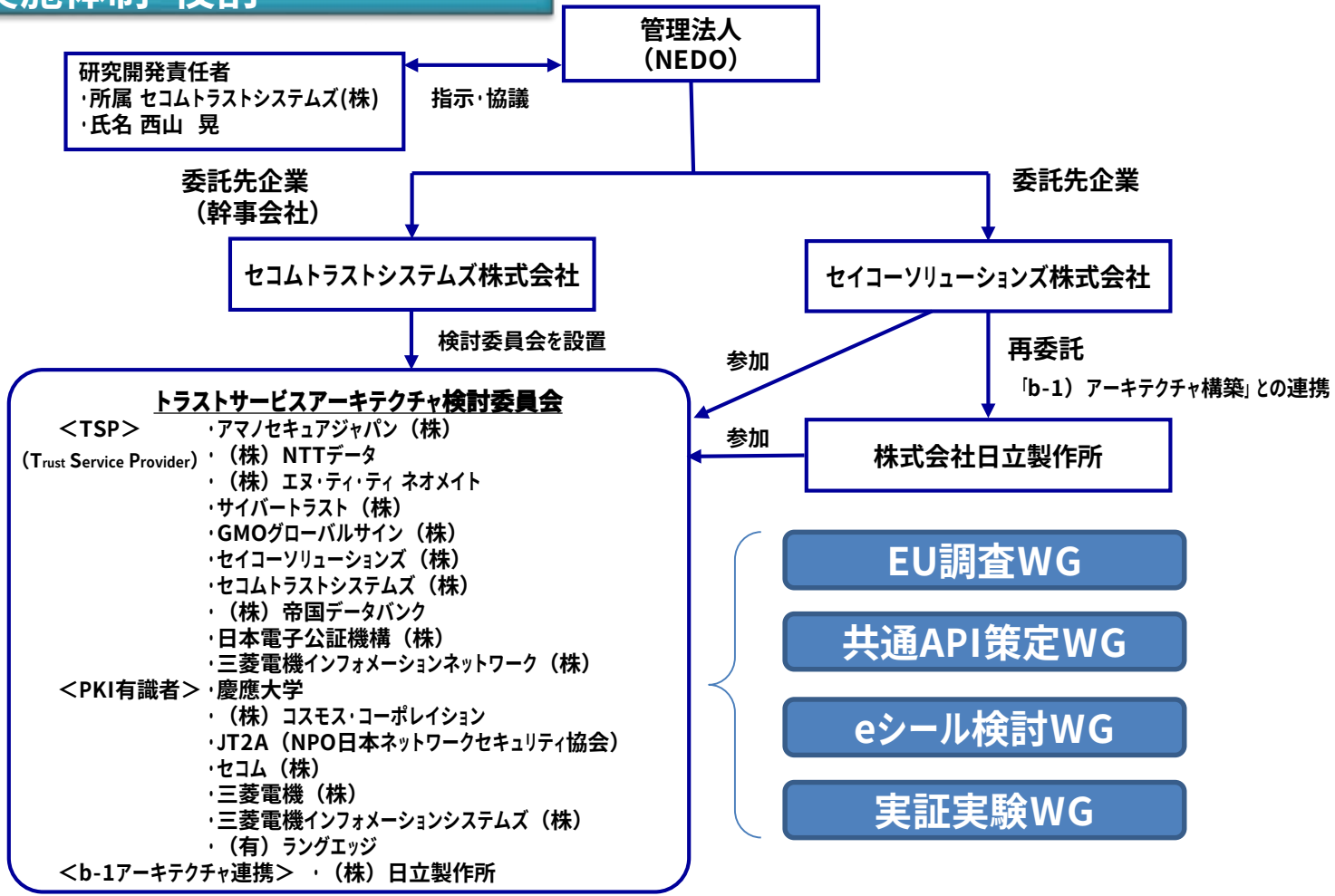
共通API導入前
異なる電子契約サービスの利用者間で電子契約ができない。

共通API導入後
システム間連携が可能となるため、異なる電子契約サービスの利用者間で電子契約が可能となる。



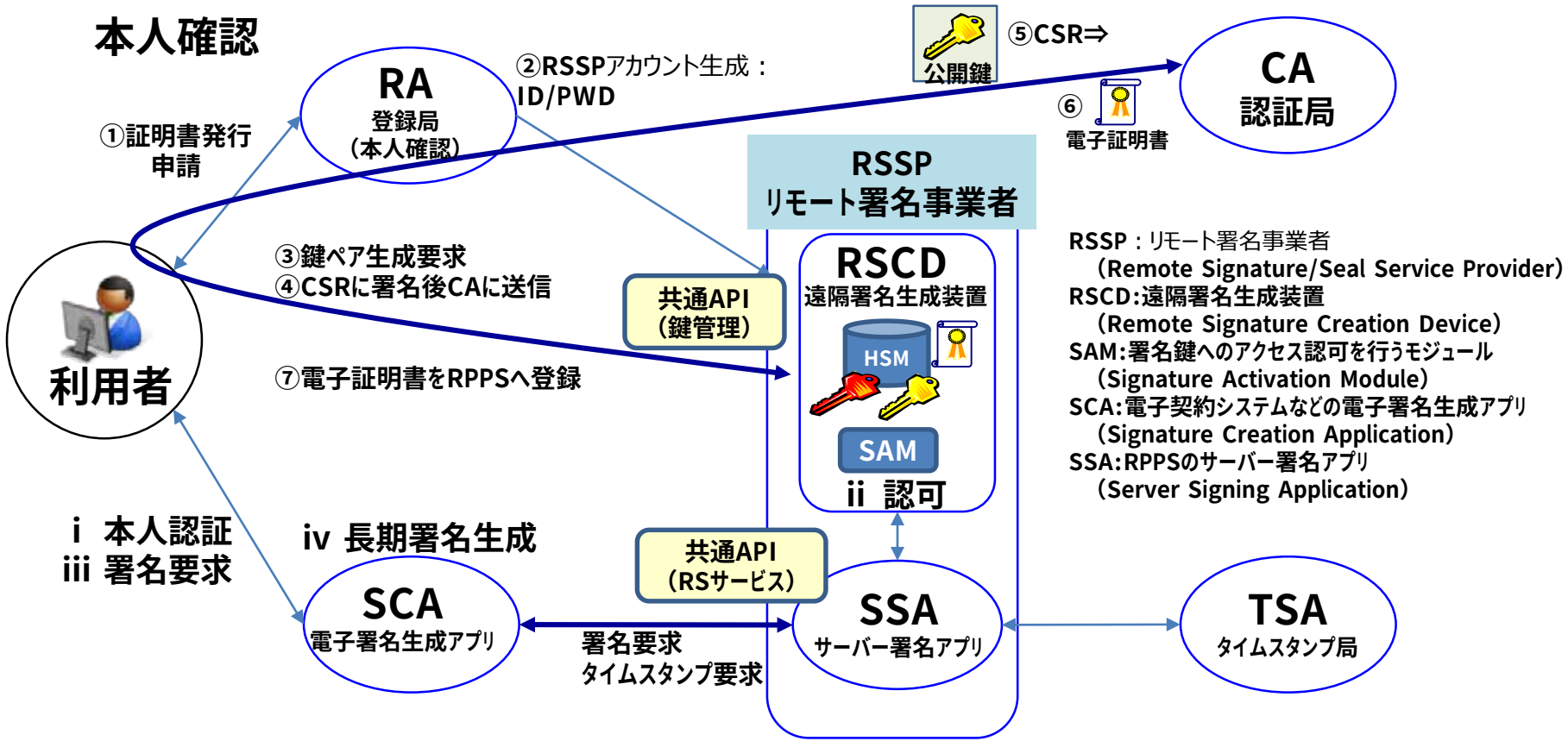
*Trusted List
トラストサービス事業者が認定された適格事業者であることなどを機械可読な形で確認するしくみを公開

4．実施体制･役割


管理法人
（NEDO）
研究開発責任者
･所属 セコムトラストシステムズ(株)
･氏名 西山　晃
指示･協議
委託先企業
（幹事会社）
委託先企業
セコムトラストシステムズ株式会社
セイコーソリューションズ株式会社
検討委員会を設置
参加
再委託
「b-1）アーキテクチャ構築」との連携
参加
株式会社日立製作所
トラストサービスアーキテクチャ検討委員会
＜TSP＞
（Trust Service Provider）
･アマノセキュアジャパン（株）
･（株）NTTデータ
･（株）エヌ･ティ･ティ ネオメイト
･サイバートラスト（株）
･GMOグローバルサイン（株）
･セイコーソリューションズ（株）
･セコムトラストシステムズ（株）
･（株）帝国データバンク
･日本電子公証機構（株）
･三菱電機インフォメーションネットワーク（株）
＜PKI有識者＞
･慶應大学
･（株）コスモス･コーポレイション
･JT2A（NPO日本ネットワークセキュリティ協会）
･セコム（株）
･三菱電機（株）
･三菱電機インフォメーションシステムズ（株）
･（有）ラングエッジ
＜b-1アーキテクチャ連携＞
･（株）日立製作所
EU調査WG
共通API策定WG
eシール検討WG
実証実験WG

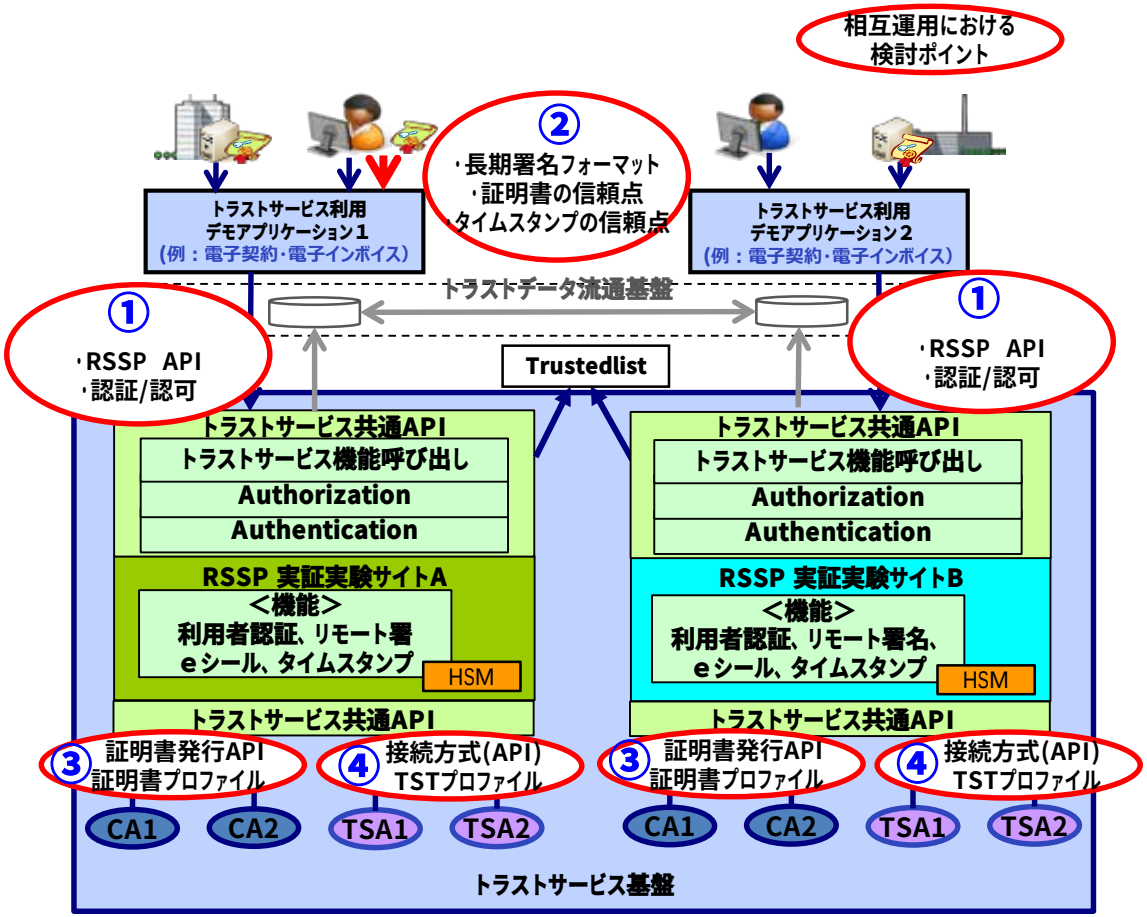
5．トラストサービス共通APIの全体スキーム

CSR:電子証明書発行要求（Certificate Signing Request）
Cert：電子証明書（Certificate）



RSSP：リモート署名事業者
（Remote Signature/Seal Service Provider）
RSCD:遠隔署名生成装置
（Remote Signature Creation Device）
SAM:署名鍵へのアクセス認可を行うモジュール
（Signature Activation Module）
SCA:電子契約システムなどの電子署名生成アプリ
（Signature Creation Application）
SSA:RPPSのサーバー署名アプリ
（Server Signing Application）

6．相互運用実証実験における検討ポイント



①RSSPとの連携

・共通API
- リモート署名業務に必要な共通APIの定義

・認証/認可の相互運用
＝＞ CSC-APIをベースとして追加もしくは修正が必要なAPIの検討。

②アプリケーション間でのデータ流通

・長期署名フォーマットの相互運用
- 署名付与、タイムスタンプ付与、署名検証

＝＞ 長期署名フォーマットプロファイルの必要性につながる。

・EE証明書およびTSA証明書の相互運用
- EE証明書パス検証、TSA証明書パス検証
- トラストアンカおよび失効情報の取得

＝＞ Trusted ListとCAリポジトリの関係や要件の洗い出しにつながる。

③CAとの連携

・証明書発行方式の相互運用性
- CSRのフォーマット
- API（RESTful ,SOAPなど）

・証明書プロファイルの相互運用性
- 鍵/署名/ハッシュ/アルゴリズム、鍵長
- KeyUsage、ExtendedKeyUsage

＝＞ 認証事業者の間での差異、国際標準への準拠（CAB/FのBaseRequirementなど）

④TSAとの連携

・タイムスタンプ取得方式の相互運用性
- API(認証含む)

・TSTの相互運用性
- プロファイル、証明書パス

＝＞ 認証事業者の間での差異

7．結果の評価

【最終目標】：トラストサービスに関するアーキテクチャとしての国際的に通用する共通API仕様策定とその有効性に関する実証研究の実施

【達成度】：100%

【実施事項】

1. 共通API策定WG：従来、リモートモート署名では電子署名に用いるユーザーの電子証明書の発行を受けられるのが１つの認証局に限定されていた。本実証研究では複数の認証局からの証明書発行を可能とし、またタイムスタンプ局も複数利用とするトラスト共通API仕様案を設計した。また、複数利用者と紐づけて利用できる組織による電子署名（ｅシール）用のAPIも合わせて検討した。
2. eシール検討WG：EU標準規格をベースに日本語入力を拡張したeシールプロファイル/発行ポリシ案策定
3. EU調査WG：海外調査3回、CSCおよびTSP事業者とのFace to Face打合せによる情報交換
   - イタリア、ドイツ、ポーランドのTSPのe-インボイス等のユースケースの調査を実施、eシール用証明書のサンプルを収集した
   - ETSI規格であるCSC※のAPIへ、複数TSPをサポートするAPI群の追加提案を実施→提案を歓迎された
   - EU委員会（DG Connect)、ETSIとの意見交換→日EUパイロットプロジェクト（Twin project）の必要性で一致
4. 実証実験WG：RSSP実証実験サイトおよびデモアプリケーション（SCA）サイトの構築･実証
   - 実証実験（基本シナリオ）
     ① 共通APIを利用して電子契約（２者間）のユースケースが実施できることを確認。
     ② 共通APIを利用してeシールのユースケースが実施できることを確認。
   - 実証実験（相互運用シナリオ：一つのSCA-RSSPで複数のTSPの利用確認）
     ① 複数のタイムスタンプ局（セイコー、アマノ）からタイムスタンプが取得可能であることをタイムスタンプの署名検証を通じて確認。
     ② 複数のCA（GMO,ジャパンネット、サイバートラスト、セコム）の署名用証明書を利用し電子署名が可能であることを署名検証を通じて確認。
     ③ 複数のCAのeシール用証明書を利用しeシール付与が可能であることを署名検証を通じて確認。
     ④ ２つの署名アプリサイトから同一のRSSPサイトを利用して電子署名(２者間)が実施できることを署名検証を通じて確認。

※CSC：Cloud Signature Consortium
グローバル市場で採用するに適したクラウドベースのデジタル署名の共通の技術標準を構築することを目標とする業界および学術団体の協議会。
https://cloudsignatureconsortium.org/

【研究成果で期待される波及効果】

様々なアプリケーションが、簡便にトラストサービスを利用できる環境を提供することで、流通するデータに「信頼」を付与するハードルを下げ、安全･安心なSociety5.0実現に寄与できる。

【事業化、実用化、社会実装に向けた出口戦略】：社内体制として、実用化に向けた措置を適宜講じているとともに、国内TSPとの協議を進めている。

８．課題の整理と今後の対応

【課題】

1．複数CAのサポート

今回は各CAの証明書プロファイルに応じてCSR（証明書発行要求）を作成するのはRSSP側で行った。しかしながら広くCAをサポートするためにはCSRの作成はCA、RA側で行う方が拡張性がある。今後、以下の項目等への対応を検討する。

- リモート署名サービスが複数の認証局の証明書をサポートする際のフロー詳細の共通理解。
- リモート署名サービスプロバイダが生成する鍵ペアと持ち主ユーザの関連付け方法。

2．相互運用範囲の明確化

署名鍵への認可情報をHSM内に組み込んだSAM（Signature Activation Module）に直接、2要素認証の情報をインプットする必要があるが、HSMの製品依存があり使える機種が限られる。また、SAMの仕様や2要素認証の方法は様々であるため、相互運用には一定の制限がある。

3．標準化

- 策定した共通APIは、CSCのAPI仕様と差分があり、今後も国際相互運用を考慮した認識合わせと詳細な仕様調整が必要である。
- ユニークな署名鍵を複数のユーザが利用するeシールのリモート署名での利用は世界的にも未整理であり検討の継続が必要である。
- 現時点では国際相互運用ができるトラストサービスであることを実証、検証できる環境が無いため、今後の整備が望まれる。

【成果の対外的発信、国際的取り組み・情報発信】

- トラストサービスの国際相互運用にむけて、EU標準化団体ETSIと連携しているCSCのAPIに組み込むべく協議を継続中
- 本実証研究で策定したAPI仕様を国内の主要TSPへ開示、バージョンアップなどの意見交換を継続して進めて行く。

【連携状況】

パーソナルデータ分野アーキテクチャ構築テーマに対し、共通APIを活用したサービスへの実装およびサービスの普及に向けて共通理解を深める