資料１１－２

# トラストサービスの在り方を検討するにあたって

2019年10月11日

トラストサービス推進フォーラム

# トラストサービスとは

- トラストサービスは、<u>誰もが信頼できる基準</u>を満足しているサービス


このサービスは利用して大丈夫か？

現状：データの信頼性を技術的に確保するサービスは、既に我が国において始まっているが、自然人の電子署名以外は**<u>信頼できることを公的に保証する仕組み</u>**は無い。

**<u>トラストサービスの信頼性を保証するフレームワーク</u>**が無い

課題1：明確で共通的な信頼性判断基準
・利用者にとって、トラストサービスの信頼性の判断基準がないトラストサービスが存在する（リモート署名，eシールなど）。
・トラストサービスごとに，評価基準・認定の枠組みや信頼できる事業者の公表方法などが異なると，利用者の混乱を招く恐れがある。

課題2：国際的な相互運用
・国際間の取引やルール決めなどでは、国の取り決めでなければ対等な関係になれない。
・場合によっては、相手国のルールを強要され、国の自主性を損なうことになりかねない。

# 「トラストサービスの信頼性を保証するフレームワーク」を考える

- 第三者による評価：オレオレ（自己申告だけ)では信頼できない
  → 第三者が客観的に評価、監査することでトラストサービス事業者の信頼性が確認できる。
- 評価の主体：誰が評価すべきか？
  → 身内や利害関係者は不適切、公平な評価能力、専門性が必要。
  → 第三者たる評価機関の要件を定める基準が必要。
- 評価の基準：評価機関は何に基づいてトラストサービス事業者を評価すべきか
  → 共通的な評価手順・項目等：これらは、トラストサービスの種類によらずに共通的な部分が多い
  → 個別的な技術・運用基準：各トラストサービスに応じた技術・運用の基準が必要。
- 利用者への公開：評価基準を満たした信頼できる事業者であることを利用者はどのように知りえるか？
  → 基準を満たした事業者を認定し、公開する必要がある。
  → 利用者は信頼性の裏付けのあるサービスを望んでいる。そうした裏付けをアプリが自動的に確認できるためには，認定事業者の公開を機械可読な形式で行う必要がある。
  → 利用者があらゆる情報を収集して総合的に信頼性・安全性を判断することは難しく、利用者に代わって情報を収集し判断の材料を提供する仕組みが必要である。
- 公的枠組み：上記、評価、認定のしくみを規定する何らかの公的な枠組みの整備が必要
  → トラストサービス事業者の認定制度や技術基準は、国内で統一的ルールの下での運営が必要（様々な基準の民間認定制度があると混乱を招く恐れがあるため，統一ルールが必要）。
  → 国際的なトラストサービスの相互承認には、国が関与した制度が必要。

“誰もが信頼できる公的な枠組み”を整備することで
課題１「明確で共通的な信頼性判断基準」、課題２「国際的な相互運用」を解決

# 「トラストサービスの信頼性を保証するフレームワーク」を構成する４つの観点

1．トラストサービス提供事業者（TSP）に対する評価・検証体制の確保
- 適合性評価機関が満たすべき基準と、国による適合性評価機関の認定
- 各トラストサービスに対する準拠性評価の実施体制の整備

※タイムスタンプ事業者の認定及び電子署名法上の認証業務の認定については評価機関の整備が進んでいる

２．技術的な基準とその評価体制の整備（技術標準）
- 日本として技術標準を構築・維持していく体制創り

３．トラストアンカーの開示
- 機械可読（Society5.0）な，現在のみならず過去に遡ってトラストを確認できるホワイトリスト

**４．公的な枠組みの整備**
**準拠性/適合性監査の公的枠組みによる責任の明確化**

技術革新、暗号技術などの環境変化に対応できる国家として安全・安心を担保する統一した仕組みのもと、各トラストサービスの基準を設定する。これにより、さまざまな業界で、信頼が裏付けられたサービスが提供できる。

# 1.トラストサービス事業者（TSP）に対する評価・検証体制の確保

**利用者からのニーズの声**：「タイムスタンプが諸外国で認められるか不安」、「リモート署名事業者の安全性が利用用途に適しているか分からない」
**発生している課題**：認証局以外は国の認定制度が無く、タイムスタンプ局は民間制度であり諸外国でその効果が認められるか不透明。リモート署名については技術、運用基準や認定制度も未整備であり事業者のセキュリティレベルに差があり信頼できる事業者かどうかを判断する基準がない。
**課題解決には**：一定の基準を満たしたトラストサービス事業者を認定し公開するには統一的なルール、基準が必要。様々な基準の民間認定制度があると混乱を招く恐れがあり、国際的なトラストサービスの相互承認には、国が関与した公的な仕組みが必要。そのためには以下の施策が必要。
①国の制度に基づいた適合性評価機関を設置
②国際レベルでアップデートされるトラストサービスの技術・運用などの基準の整備、メンテナンス
③その基準への準拠性の適合性評価機関による評価・検証
これらにより、信頼ある事業者であることを認定可能となり、利用者が安心して事業者を選択できるものと考えられる。

■ 適合性評価機関が満たすべき基準と、国による適合性評価機関の認定
- TSPを監査する適合性評価機関に求められる要件は製品認定機関と共通部分が多い。下記ENやISO,JIS※などを参考に，国際標準に準拠して適合性評価機関の要件を規定する標準規格を策定することが考えられる。

  ※ETSI EN 319 403（TSPを評価する適合性評価機関の要件）、ISO/IEC 17065（JIS Q 17065 製品認証機関の認定）
- 適合性評価機関は上記のような一定の基準に従って、国または国が指定する公的認定機関が認定することで公に信頼が担保される。

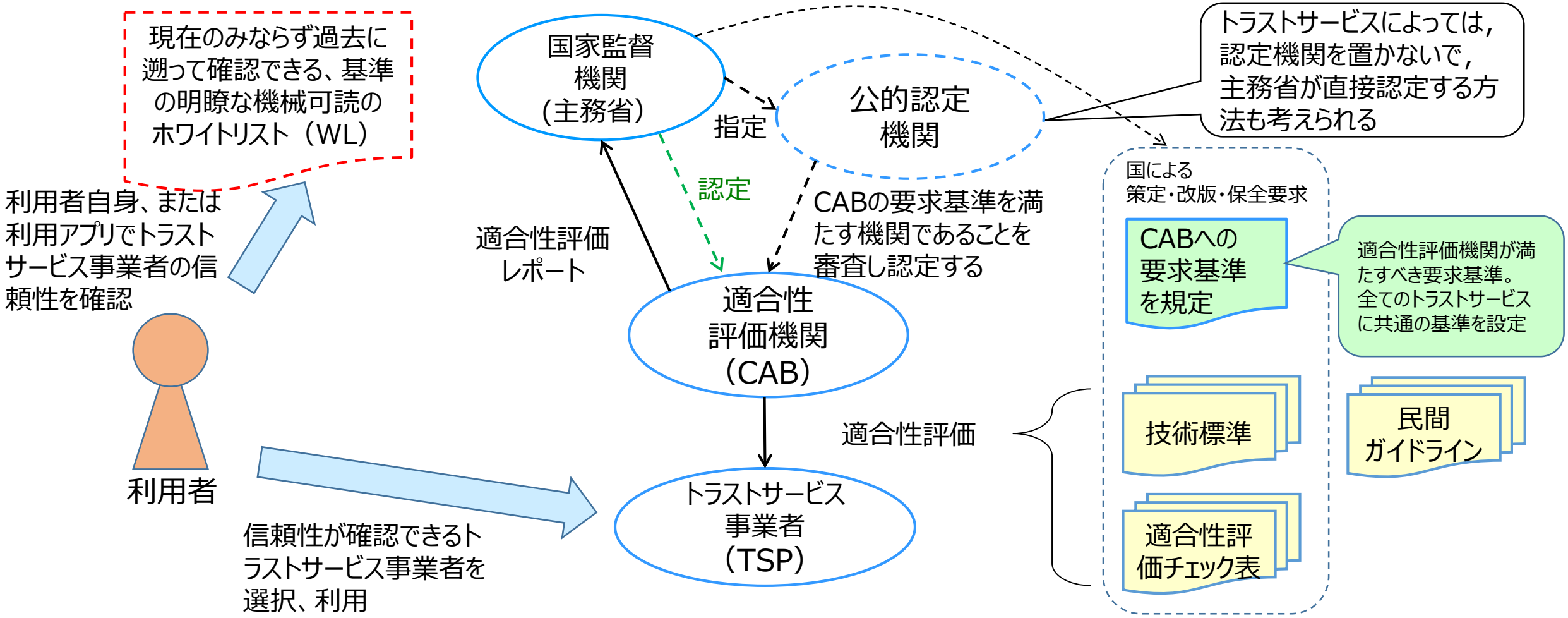
※認証局は電子署名法に基づいた適合性評価体制（指定調査機関としてのJIPDEC）があり、タイムスタンプは民間で適合性評価（日本データ通信協会による認定スキーム）がされている

- 各トラストサービスの技術要素や相互牽制（複数人による管理）などの信頼性を維持する内部運用体制には共通性があり、適合性評価の方法，手順等はトラストサービスの種類によらず共通化できる。制度の効率的な維持や適合性評価機関の経営の健全性確保のためには様々なトラストサービス事業者を横断的に監査できることが望ましいのではないか

■ 各トラストサービスに対する準拠性評価の実施体制の整備
- 各TSPに求められる技術，運用などの基準を定めた上で，基準に対する適合性評価の方法（チェックリスト）を定め、評価を実施する体制を整備する。

# TSPの適合性評価の枠組みのイメージ

・適合性評価の枠組みはトラストサービス事業者（TSP)の信頼性を担保できる仕組み。
・国または国が指定する公的認定機関が適合性評価機関を認定する。適合性評価機関が基準に基づいてTSPを監査・評価し、主務省に報告の上でTSPを公的に認定する。
・認定されたTSPを機械可読なホワイトリストで公開。



# 2. 技術的な基準とその評価体制の整備（技術標準）

**利用者からのニーズの声**：リモート署名サービスを用いた電子契約サービスの信頼性が確認できない。認定認証業務でリモート署名が使えない。法人による電子署名の根拠が、 EUでのeシールのようには示されておらず、簡易的な利用ができない。新たな技術革新に呼応した技術基準の維持・改訂・メンテナンスを、その基準を参照する法令等と整合させつつ行うことが必要。
**発生している課題**：各トラストサービスに求められる技術・運用などの基準は、関連する暗号技術や国際標準の更新、また新規格の登場などに伴いメンテナンスが必要。認証局、タイムスタンプ局の技術、運用基準はあるが、そのような変化への対応は個別になされ確実なメンテナンスが実施出来るとは言えない。また、リモート署名など新技術に対する標準を作成する体制が無いため、リモート署名サービス事業者の提供するサービスの信頼性が確立していない。民間では、社会を広範に巻込む継続的な活動は困難。
**課題解決には**：トラストサービス事業者の信頼性を評価するためには、日本としての技術標準を構築・維持していく体制が必要。

## ■ 日本としての技術標準を構築・維持していく体制創り

- トラストサービスの信頼性を確保するためには、各トラストサービスの技術基準の構築、維持が必要。
- 各トラストサービスの認定に関わる技術基準(*)を、最新の動向を踏まえて民間で策定。
- かかる技術基準の策定にあたって， 技術基準と公的制度との整合性が維持可能となる体制を、官民の協力で確立すべき

(*) 技術標準の例

- トラステッドリストのフォーマット
- 電子署名フォーマット/生成・検証処理
- TSPの要件(証明書やタイムスタンプなどのトークンのフォーマット、証明書ポリシ、運用要件など)
- リモート署名の技術・運用要件など
- 署名生成装置/ハードウェア暗号装置の要件

# 3. トラストアンカーの開示

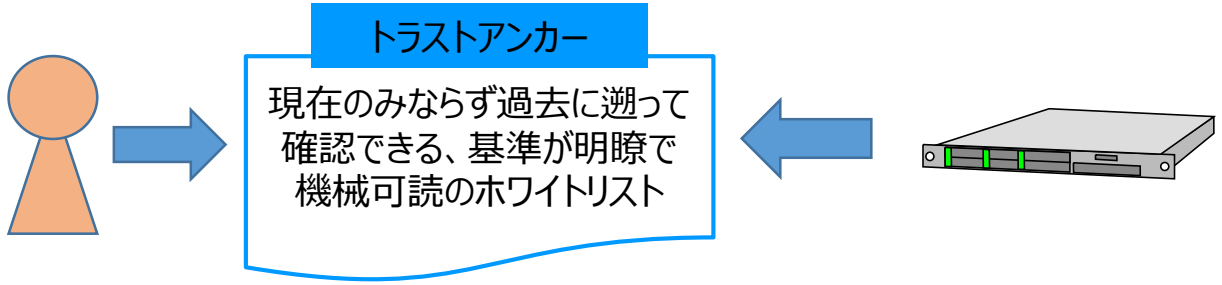
**利用者からのニーズの声**：「今利用しようとしているサービスは信頼できるのか？」、「利用するサービスが将来停止しても、正当なサービスだったことを証明したい」、「これらを利用者が手動で確認せずに機械可読とすることで自動で簡便に確認できる手段はないのか」
**課題**：ホワイトリストの信頼性確保と機械処理可能化
**課題解決には何が必要か？**：一定の基準を満たしたサービスであることを機械可読で確認できるホワイトリストが、公的な機関から完全性を担保されてトラストアンカーとして公開されていること

■ トラストアンカー

- （何らかの基準に基づき）信頼できるトラストサービスをトラストアンカーと呼ぶ。
- 権威のある者が、その者が持つ基準に照らして信頼できると判断したトラストアンカーを、ホワイトリストの形で公表し、これを一般の利用者が用いる方法があり（例えば，EUのトラステッドリスト）利便性が高い。例えば、トラストサービス毎に信頼できるトラストサービスのリストを記載したものを一つにまとめて公表。
- ホワイトリストには、発行者の電子署名をつける他、ホワイトリストのフィンガープリントを官報に載せることにより，改ざん検出が可能となる。

■ 機械可読（Society5.0）な、現在のみならず過去に遡ってトラストを確認できるホワイトリスト

- XML等の機械可読なフォーマットでホワイトリストを公開すれば、アプリケーションがこれを読み込むことにより、アプリケーションに入力された情報の信頼性が自動的に確認可能となる。
- インボイス制度の導入を背景に自動処理の推進が望まれている。機械可読なホワイトリストを公開することで，アプリケーションで正しい発信元を自動的に確認できるため，「なりすまし」や「偽造・ねつ造」といったデジタル特有の課題を解決できる。



# 4. 公的な枠組みの整備

## ■ 1. 準拠性／適合性の評価・監査

利用者の声：タイムスタンプが諸外国で認められるか不安、リモート署名事業者の安全性が利用用途に適しているか分からない
課題：認定・認証のスキームがないか非標準で独自のものである

解決策

- ETSI EN 319 403 等（適合性評価機関に対する能力、一貫性のある運営及び公平性に関する要求事項）に基づき適合性評価機関を国または国が指定する公的認定機関が認定する。これが下記のホワイトリストへのトラストアンカー掲載の根拠となる。
- 次項のスキームで定められた技術標準に基づき適合性評価機関がTSPの準拠性／適合性を評価・監査する。

## ■ 2. 技術標準の構築・維持

利用者の声：技術基準は、それを参照する法令等と整合しつつ、新たな技術革新に呼応して維持、改訂、メンテナンスすることが必要
課題：民間では社会を広範に巻込む継続的活動は困難

解決策

- 制度全体の整合性を確保するため、TSPの認定に関わる技術基準の標準としての構築・維持を国の行政機関あるいは国から委任を受けた標準化機関（日本規格協会、情報規格調査会、JIPDEC、日本データ通信協会など）が担う。

## ■ 3. トラストアンカーの開示

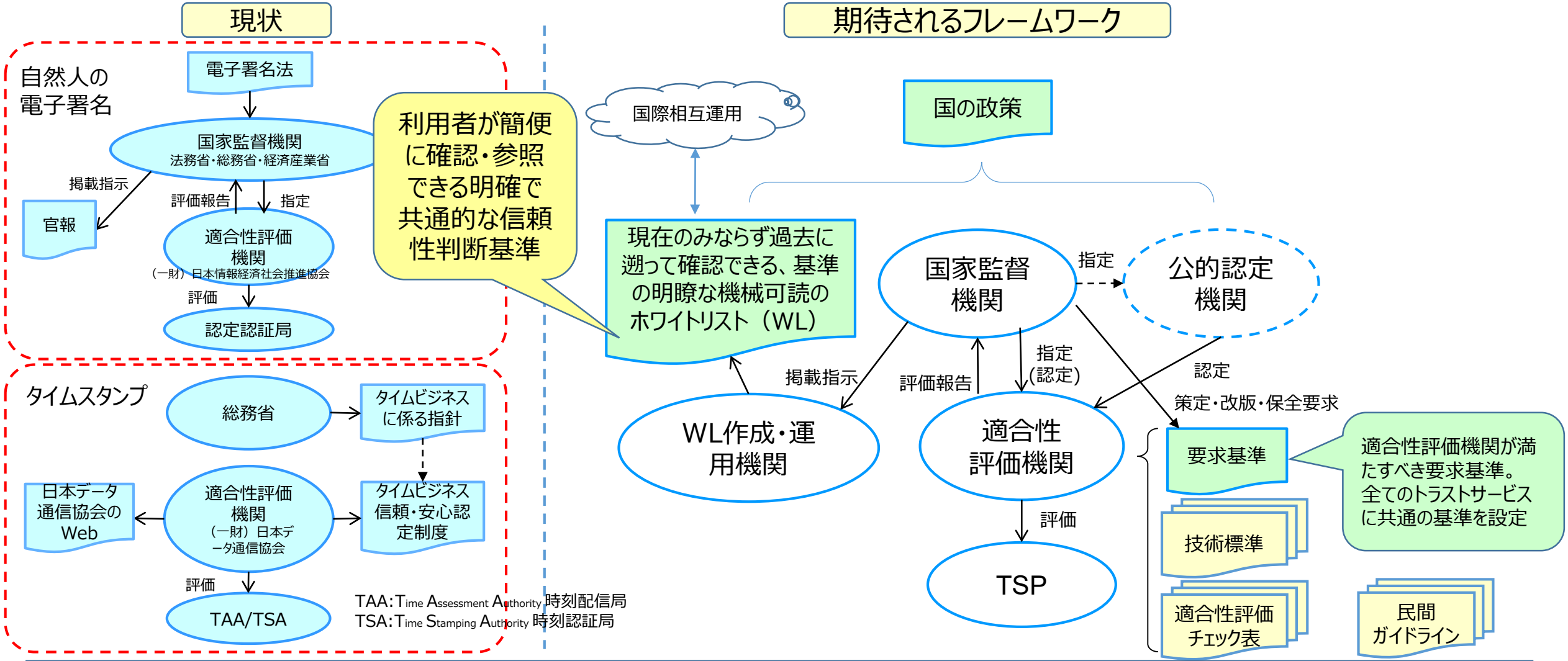
利用者の声：トラストアンカーのホワイトリストを確認できる機械可読な仕組みが必要
課題：ホワイトリストの信頼性確保と機械処理可能化

解決策

- 上記１.の準拠性／適合性の評価・監査のスキームにより得られた格付け（一定の基準を満たしているかなど）を、事業者や業務の識別のための情報、その他、エンドユーザによる確認に必要な情報とともにXML等で記述された機械可読のホワイトリストとして実現する。国際的な相互運用の実現を考えた場合、EUのトラステッドリストの形式を採用することも有力な手段である。
- ホワイトリストには信頼性確保のため国の行政機関等（独の場合、ドイツ連邦ネットワーク庁）の公的立場の電子署名を付す。
- 電子署名の付されたホワイトリストを、国の行政機関あるいは国から委任を受けた機関が、検証ツール等による機械的な取得が可能な位置および形態でインターネット上に公開する。

# まとめ：トラストサービスの信頼性を保証するフレームワーク

国際的に通用するDFFT実現のためのトラストサービス基盤の公的枠組み構築が必要

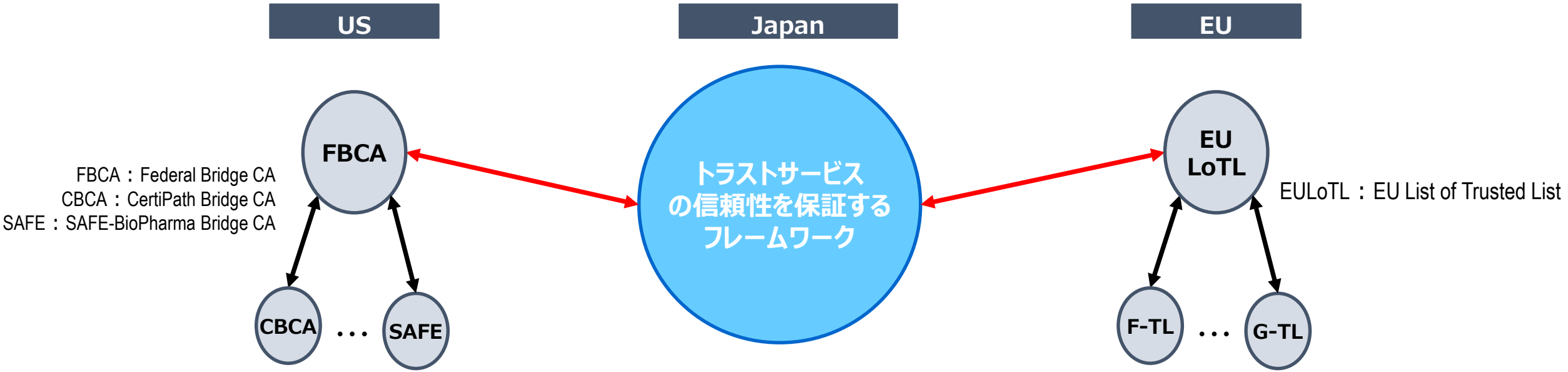



※電子帳簿保存法等にタイムスタンプが明確に位置づけられたことで、タイムスタンプの普及が進んだことを踏まえると、今後、国税、医療、建設などの各種利用シーンにおいて、所管省庁の法令・ガイドライン等にトラストサービス（タイムスタンプ、電子署名、eシール等）の利用の推奨が位置づけられることで、利用者にとってはわかりやすくなり、トラストサービスの利用が一層促進されると考える。

# 「トラストサービスの信頼性を保証するフレームワーク」と国際的な相互運用

これまでの紙中心の世界とは異なる発想で大胆な改革を行い、DFFTを実現するトラストサービス基盤を構築し枠組を明示する。
わが国の枠組みを明快な形で提示して、海外との相互運用への提案を行う

DFFT：Data Free Flow with Trust




・国際的な協調のためには、日本のトラストサービスの仕組みが明快で海外の政策担当者・利用者にとって理解が容易であることが必要
・海外での訴訟等の手続において、日本のトラストサービスが発行した情報の法的有効性を示しやすいことが重要