

# トラストに関するワーキングチーム -中間報告-



令和3年4月26日  
内閣官房 情報通信技術(IT)総合戦略室

# データ戦略タスクフォース第一次とりまとめの概要

データ戦略の  
アーキテクチャ

ビジョン

現実空間とサイバー空間が高度に融合したシステム（デジタルツイン）により、新たな価値を創出する人間中心の社会

戦略・政策

組織

行政  
民間

ルール

データ  
ガバナンス  
連携  
ルール

連携基盤  
(ツール)

データ

利活用環境

インフラ

○ 理念：信頼（トラスト）と公益性の確保を通じて、データを安心して効率的に使える仕組みを構築する

○ データ活用の原則 自分で決められる、勝手に使われない つながる いつでもどこでもすぐに使える 安心して使える みんなで創る

○ 社会実装・業務改革

組織・ビジネス  
での取組

いかなる価値を誰に対して生み出すか、国民・行政・産業界のユーザー視点から  
ニーズ分析を行い、デジタルツインの視点でビジネスプロセスをゼロベースで見直す

データがつながることで「新たな価値を創出」

行政

重点的に

民間

ワンストップ、ワンズオンリー 取組むべき分野 データ流通、官民データ活用

○ 喫緊に取組むこと

トラストの  
枠組みの  
整備

IDの認証やトラストサービスの評価などトラストアンカーの機能整備の他、誰が(主体・意思)、何を(事実・情報)、いつ(時刻)というトラストの要素について、これらが主張されたとおりのものであること(真正性)、改ざんされていないこと(完全性)の確保・証明が必要である。以下のように整理し、各々の論点を整理  
(論点例:本人確認レベル、発行した自然人、組織、機器の確認方法)

- 主体・意思: 意思表示の証明 (意思表示が本人によってなされたものであること等の証明)
- 事実・情報: 発行元証明 (発行した自然人、組織、機器が信頼できるか等の証明)
- 存在・時刻: 存在証明 (何らかの情報が、ある時点において存在し、それ以降は改ざんされていないことの証明)

→ 整理した論点について、関係省庁で  
解決の方向性を検討開始

プラットフォーム

分野横断で検討すべき共通項目

- 共通アーキテクチャの整備 (スマートシティリファレンスアーキテクチャ)
- データ連携の共通ルールの整備<sup>\*1</sup>
- 主要データ標準、データ品質管理フレームワークの策定
- 分野間データ連携基盤でのツール開発 (データカタログ検索、データ交換、データ連携契約機能) (分野間連携のための民間促進団体DATA-EXによるポータルサイト運営)

<sup>\*1</sup> データ提供主体/データの真正性、データの取扱いに係る契約ひな形、パーソナルデータの取扱い、データ交換のための標準化、データの品質の考え方

分野ごとに検討すべき項目

- 重点的に取組むべき分野の関係省庁を中心に、官民共同での検討の場を設け、プラットフォームの在り方についてデジタル庁(仮称)発足までに整理 (健康・医療、教育、防災、農業、インフラ、スマートシティ等)
- 関係者のニーズ分析: データを中核とした新たな価値創出のための分析
- アーキテクチャの策定: スマートシティリファレンスアーキテクチャを参照
- ルールの具体化、ツール開発 (データカタログ、メタデータ、APIの整備等)

データ整備

ベース・レジストリ整備の推進 (ベース・レジストリ・ロードマップの策定)

- ベース・レジストリ<sup>\*1</sup>の選定
  - 選定基準<sup>\*2</sup>
  - 重点整備対象候補<sup>\*3</sup>
- ベース・レジストリの推進方法
  - 優先順位に従い段階的に導入
  - 成功事例をつくり効果や課題を明確化
- アクション
  - ベース・レジストリの指定 (内閣官房IT室: 2021年3月末)
  - データ整備: 先行プロジェクトの実施 (住所や法人情報等)
  - 主要データ標準の整備、データ品質管理フレームワークによる評価 (内閣官房IT室: 2021年3月末)

→ 重点整備対象候補のデータホルダーの関係省庁にて、  
2021年6月末までに課題整理と解決の方向性を検討

<sup>\*1</sup> 公的機関等で登録 公開され、様々な場面で参照される、人、法人、土地、建物、資格等の社会の基本データ

<sup>\*2</sup> 多くの手続きで使われるデータ、災害時に重要なデータ、社会的 経済的な効果が大きいデータ

<sup>\*3</sup> 個人 (マイナンバー含む)、法人、文字、不動産、住所、法律、制度、資格、公共施設、インフラ等を想定

その他基盤データの整備の推進

- 特定分野などで社会の基盤として扱われるデータの整備を促進

オープンデータの推進

- オープンデータ基本指針の改定による機械判読性の強化

包括的なデータマネジメントの推進

- 主要データ標準、データ品質管理フレームワーク等の活用

○ 引き続き検討すべき事項

<国際連携><人材><デジタル庁(仮称)の役割>

データ利活用の環境整備(データ流通市場の活性化等)

デジタルインフラの整備・拡充

国際連携

人材

データ整備方針等へのデータ戦略の反映

# データのトラストの枠組み検討の方向性と主な論点

## 検討の方向性（包括的なトラスト制度の創設）

### 【全体像】

#### ①包括的なトラスト基盤の創設

※データ戦略第一次とりまとめにて定義したトラスト（意思の証明、発行元証明、存在証明）について、包括的な制度化を目指す。

### 主な論点

- ・制度の形式をどうするか。

### 【包括的なトラスト制度の概要】

#### ①国（又は、民間機関）による認定制度の創設

#### ②各種トラストサービスのクオリファイドサービス認定基準、特定サービス基準の策定

※クオリファイドサービスの認定を受けたサービスは国のお墨付きを得る。

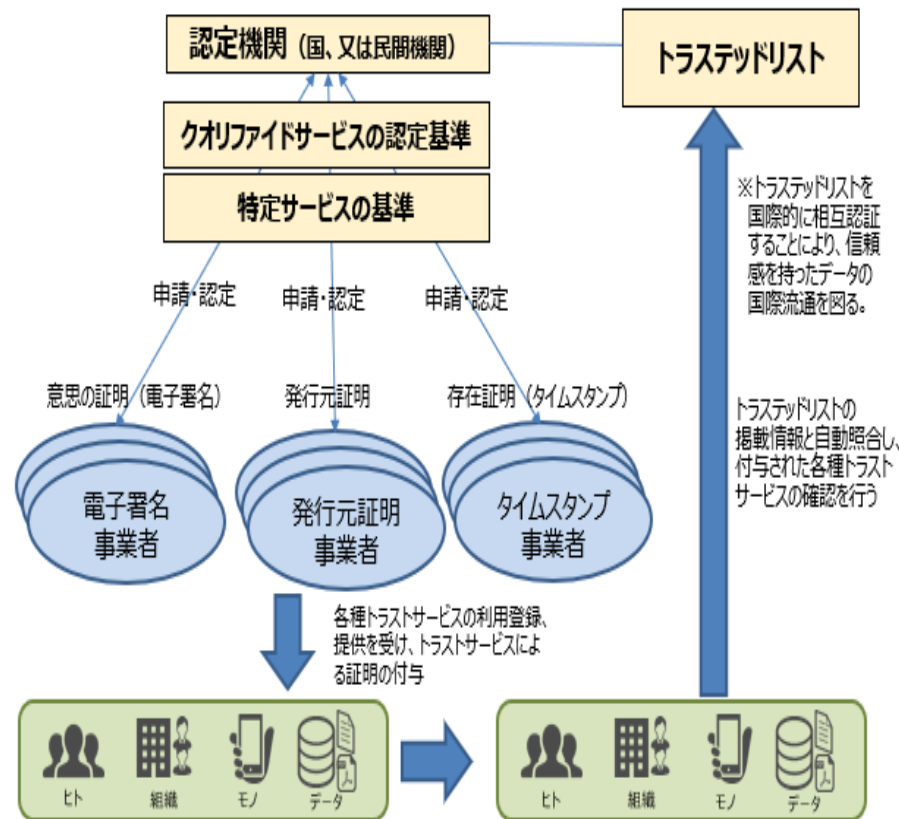
※特定サービスは、基準適合の自己宣言を経て、一定の認知を得る。

#### ③クオリファイドサービスをトラステッドリストとして公表

### 主な論点

- ・認定主体は国、民間機関のどちらであるべきか。民間機関となる場合、認定主体を認定する基準はどうあるべきか。
- ・クオリファイドサービスの認定基準、特定サービスの基準はどうあるべきか。（トラストサービス定義、技術安全基準、真偽確認方法、設備要件、業務運営要件等）
- ・国内、国際的な相互認証をうるためには、どうあるべきか。

### 【認定制度の想定イメージ】



## 今後の進め方

データ戦略タスクフォースの配下に検討WGを設置、有識者を含めた検討を進める。なおWG運営は、デジタルトラスト協議会（代表：慶應大 手塚教授）の支援を受け、推進していくことを想定。

※データ流通のトラスト確保（データが到達したか等）については、並行して検討を開始

# トラストに関するワーキングチームの開催状況

1. 第1回開催 令和3年4月8日（木） 13：00～15：00
  - (1) データ戦略タスクフォース第一次とりまとめ概要の説明及びデータのトラストの枠組み検討の方向性について
  - (2) 構成員、有識者、関係省庁からのプレゼンテーション
    - ・ 電子署名及び認証業務に関する法律の概要（山内構成員）
    - ・ タイムスタンプ認定制度に関する検討会取りまとめ（総務省 サイバーセキュリティ統括官室 高村参事官）
    - ・ 組織が発行するデータの信頼性を確保する制度に関する検討会取りまとめ（案）（総務省 サイバーセキュリティ統括官室 高村参事官）
    - ・ eIDASの概要と関連技術体系（濱口構成員）
    - ・ UNCITRALにおけるIdentityManagement及びTrustServicesに関する検討（学習院大学法学部 小出教授）
  - (3) 自由討議
  - (4) トラストの枠組み検討に向けた論点整理
  - (5) 自由討議
2. 第2回開催 令和3年4月21日（水） 10：00～12：00
  - (1) トラストサービス認定の現状について
    - ・ 電子認証局について（電子認証局会議 小田嶋様）
    - ・ 認定タイムスタンプ局について（柴田構成員）
  - (2) 発行元証明の必要性について
    - ・ 発行元証明の必要性について（株式会社三菱UFJ銀行 中武様）
  - (3) データのトラストの枠組み検討の各論点に対する検討の方向性について
  - (4) 自由討議

# トラストに関するワーキングチームによる中間報告のポイント

## 基盤となるトラスト制度の創設に関する検討状況

### 【本ワーキングチームの検討範囲について】

1. ヒト・組織・モノを特定するIdentity(属性情報)を、電子証明書に記録する仕組みの信頼性を確保する制度について、本ワーキングチームにて取り扱う。
2. Identityの附番体系や、トラストアプリケーションに必要な各種データに掲載される属性情報の正確性については、本ワーキングチームでは取り扱わない。
3. 様々な分野でのサービス提供の基盤となるトラスト制度の検討を行う。

### 【全体像】

#### 1. 基盤となるトラスト制度の創設

- (1) 電子署名法や公的個人認証法など個別の制度構築がされているが、データ社会全体を支える基盤となる制度が必要である。
- (2) 国連機関のUNCITRALやEUのeIDAS規則はトラストサービスを包括した制度となっており、我が国として電子署名法や公的個人認証法などを包括したトラスト基盤に関する制度を創設すべきである。
- (3) 意思表示証明、発行元証明、存在証明等のトラストサービスに共通する水平横断的な一般原則と共通要件を整理し、基盤となる制度を定めることが必要である。
- (4) 上記の一般原則は基盤となる制度において整理し、共通要件はトラストサービスの認定基準として整理すべきである。



# トラストに関するワーキングチームによる中間報告のポイント

## 【基盤となるトラスト制度の検討の方向性】

### 1. 国による基盤となるトラストサービス認定制度の創設

- (1) 基準策定、監督、適合性評価、認定主体の4つの軸について国が一定程度関与した制度設計が必要である。
- (2) 電子文書の法的位置づけや、トラストサービスの認定の法的・手続的な効果を明示する必要がある。
- (3) 海外との相互承認を推進するためには、法的効果について諸外国と同等の規定を置く必要がある。

### 2. 各種トラストサービスのクオリファイドサービス認定基準、特定サービス基準の策定

- (1) トラストサービスに関する技術標準は共通要件と個別要件、適格要件を体系化したものを作成すべきである。
- (2) 適合性評価機関の要件を定める国際的な整合性を持った基準を定めるべきである。

### 3. クオリファイドサービスをトラステッドリストとして公表

- (1) 認定を受けたクオリファイドサービスであることを、利用者が、必要なときに確認できる仕組みが必要である。
- (2) クオリファイドサービスを利用する者の間では、相互に相手が利用するサービスの適格性が確認できる仕組みを検討すべきである。
- (3) 利用者の利便性の観点からは認定を受けたクオリファイドサービスは、機械可読の形態で開示する、又は相互接続することを検討すべきである。
- (4) 認証局以外のトラストサービスや廃業したトラストサービスを扱うことを検討すべきである。
- (5) クオリファイドサービスを確認する仕組みは、上記よりトラステッドリストで公開する方法を検討すべきである。

### 4. トラストサービスの国際的な相互承認の実現

- (1) 国際的な相互承認をうるために、4つの項目 ①法制度、②監督・適合性評価、③技術標準、④トラストアンカー間の接続の仕組みにおいて、国際間での同等性を確保する必要がある。

令和3年4月21日開催 データ戦略タスクフォース トラストに関するワーキングチーム(第2回)

資料4 : データのトラストの枠組み検討の各論点に対する検討の方向性について

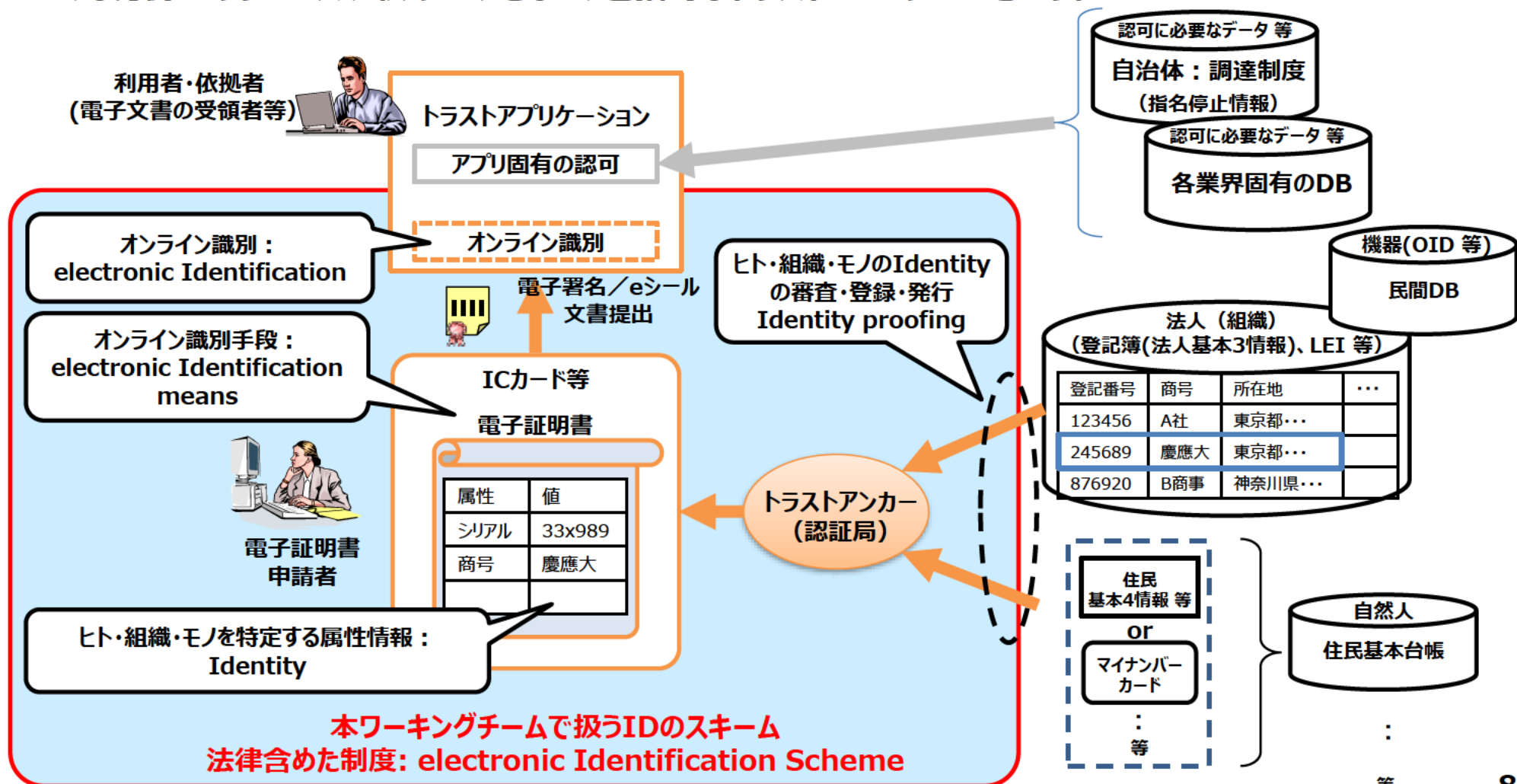
# 各論点に対する検討の方向性 -第2回-



令和3年4月21日  
内閣官房 情報通信技術(IT)総合戦略室

# 本ワーキングチームの検討範囲について

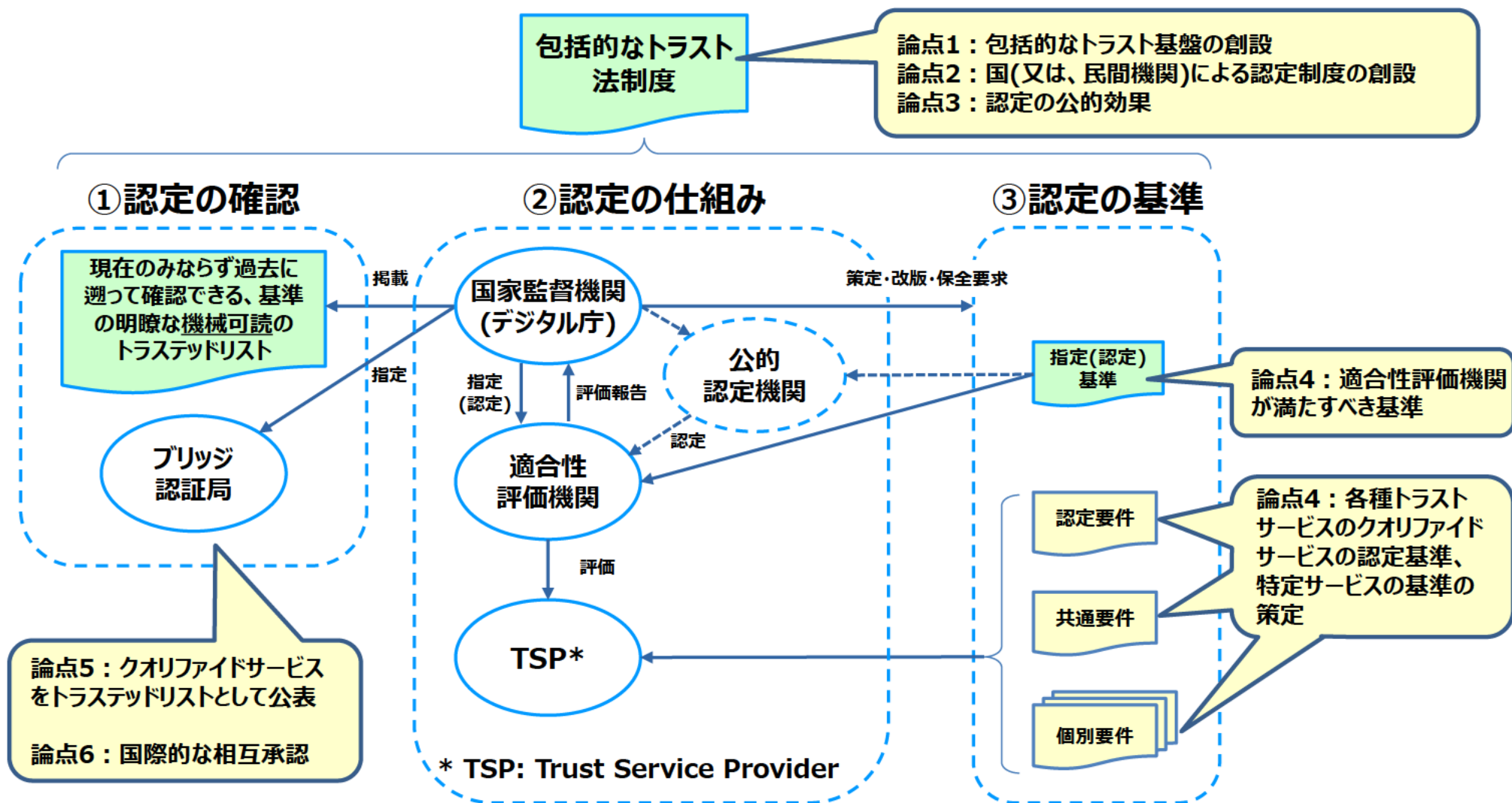
- ヒト・組織・モノを特定するIdentity(属性情報)を、電子証明書に記録する仕組みの信頼性を確保する制度について、本ワーキングチームにて取り扱う。
- Identityの附番体系や、トラストアプリケーションに必要な各種データに掲載される属性情報の正確性については、本ワーキングチームでは取り扱わない。
- 様々な分野でのサービス提供の基礎となる、包括的なトラスト基盤の検討を行う。





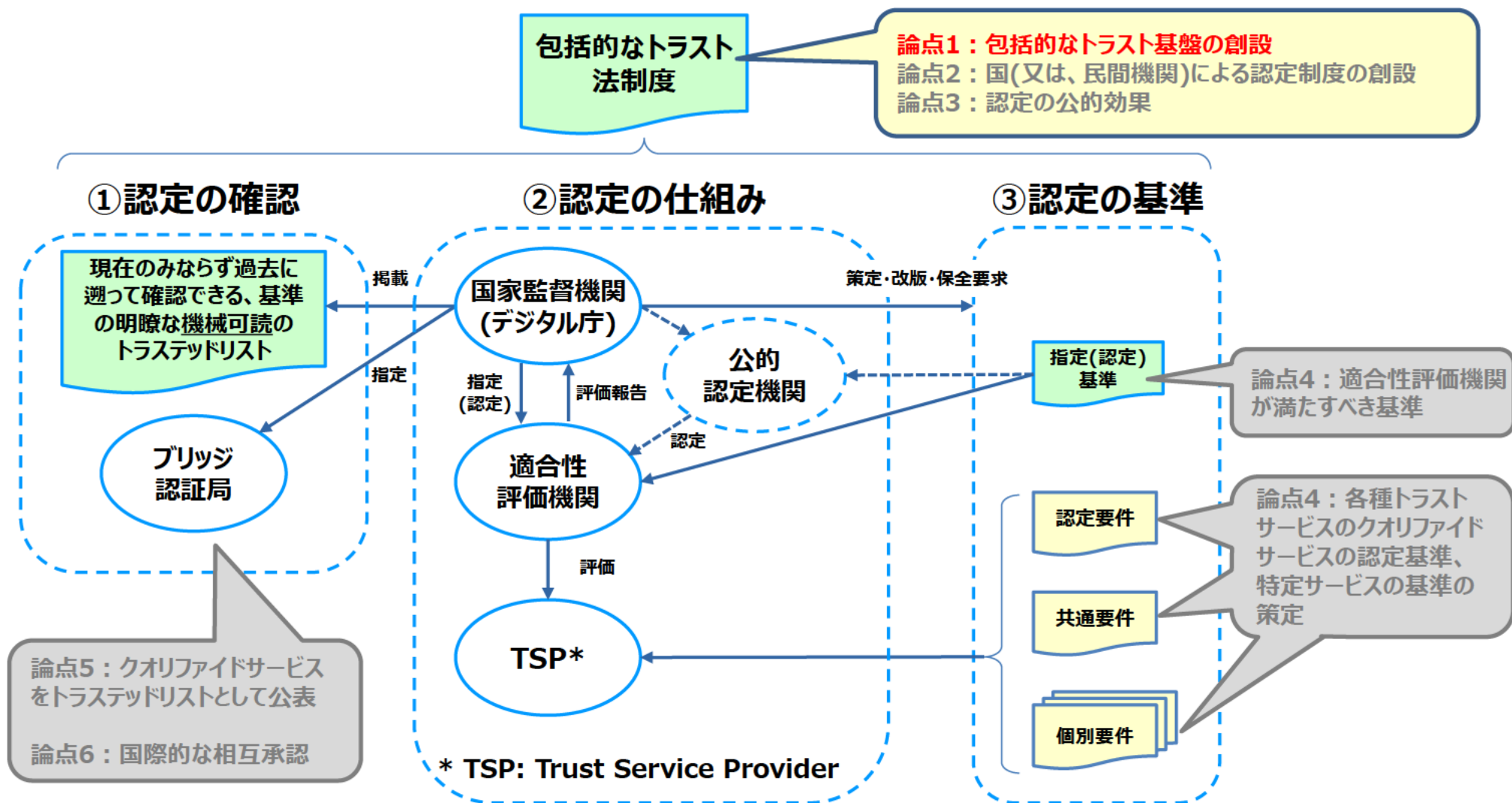
# 主な論点の全体像

## 第1回 主な論点の全体像の再掲



# 論点1：包括的なトラスト基盤の創設

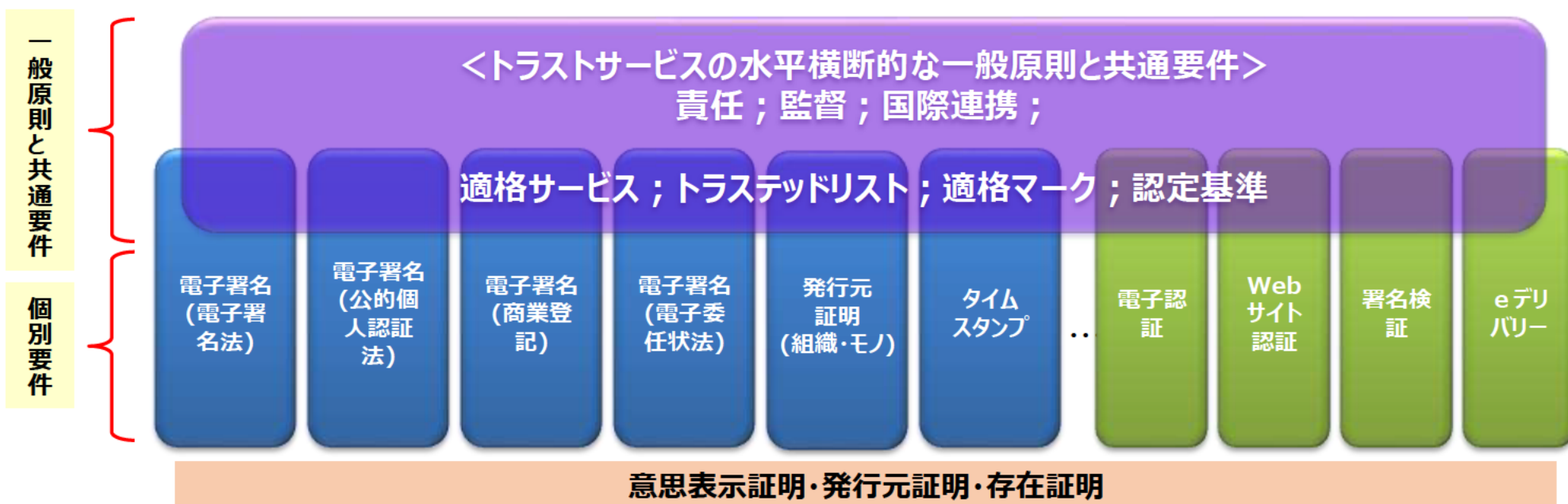
## 第1回 主な論点の全体像の再掲



# 論点1：包括的なトラスト基盤の創設

電子署名法や公的個人認証法など個別の制度構築がされているが、データ社会全体を支える包括的な制度が必要ではないか

1. 国連機関のUNCITRALやEUのeIDAS規則はトラストサービスを包括した制度となっており、我が国として電子署名法や公的個人認証法などを包括したトラスト基盤に関する制度を創設すべき。
2. 電子署名、タイムスタンプ、発行元証明などの各々のトラストサービスに共通する水平横断的な一般原則と共通要件を整理し、包括的な制度を定めることが必要である。
3. 上記の一般原則は包括的な法制度において整理し、共通要件および各トラストサービスの個別要件はトラストサービスの認定基準として整理すべき。



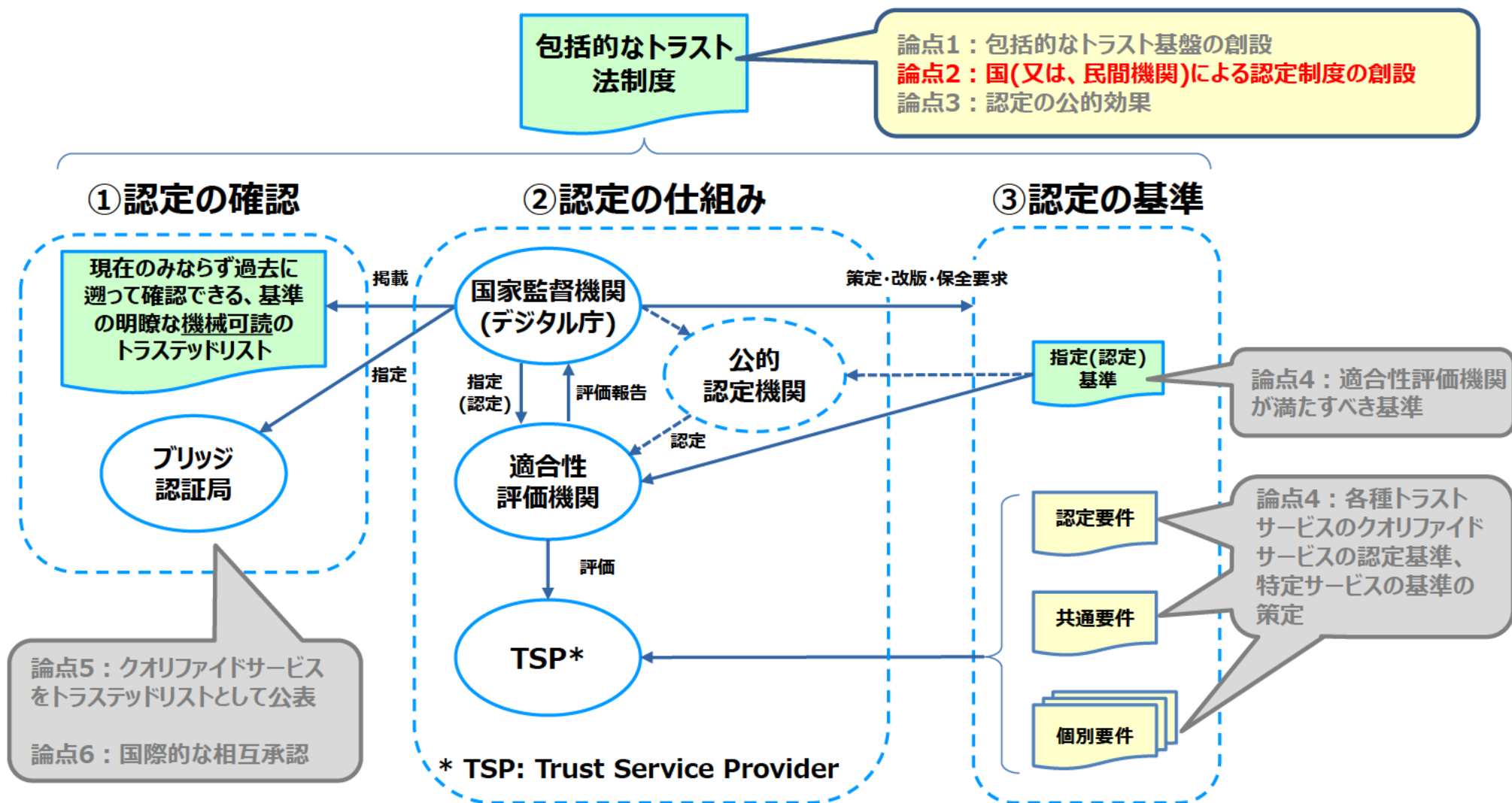
# 【参考】論点1：一般原則と共通要件

- トラストサービスの水平横断的な一般原則と共通要件のUNCITRAL、eIDAS規則との対応は以下のとおりであり、構造は一致し妥当である。今後、我が国の要件の詳細化を行う必要がある。

		第1回の論点1 P4より	UNCITRAL(WP.167)/EU(eIDAS)
一般原則	責任	・制度のフレームワーク/各プレーヤ(国、国や地方公共団体が関与する電子証明書発行機関(JPKI等)、適合性評価機関、トラストサービス事業者、利用者等)の責任範囲、等	・TSPなどの責任について、義務違反時の損害責任を負うことが明確に規定
	監査	・国による制度の統括、/安定性維持/認定基準の策定/トラストサービス事業者への監督権限	・国家監督機関はTSPとその役務に適格資格を付与することが明確に規定
	国際連携	・同一レベルの認定機関/認証機関/ベストプラクティスの交換/システム相互運用性	・法域内のトラストサービスと、同等レベルの信頼性を持つ場合、法域外で提供されるトラストサービス同様に法的効果を持つ
共通要件	トラストアンカー間の接続	・維持・公開/運用/トラストサービスの国内外の総合運用/機械可読で確認	・最低2年に一度、適合性評価機関の評価を受けなければならないなど、トラストサービスの業務責任を規定
	適格サービス	・業務責任、説明責任、業務の継続性	・自動処理に適した形式でかつ安全な方式で接続を証明する資料の制定・管理・公示を規定
	適格マーク	・簡単で、認識可能なマーク/機械可読で確認	・利用者にわかりやすいように、シンプルで認識しやすい、明確な方法で信頼マークを使用できるように規定
	認定基準	・技術/設備/運用/セキュリティの各要件/組織の安全管理、等	・業務規程・ポリシー/業界標準/財務的・人的資源、等の認定基準を規定

# 論点2：国(又は、民間機関)による認定制度の創設

## 第1回 主な論点の全体像の再掲





# 論点2：国(又は、民間機関)による認定制度の創設

認定主体は国、民間機関のどちらであるべきか。

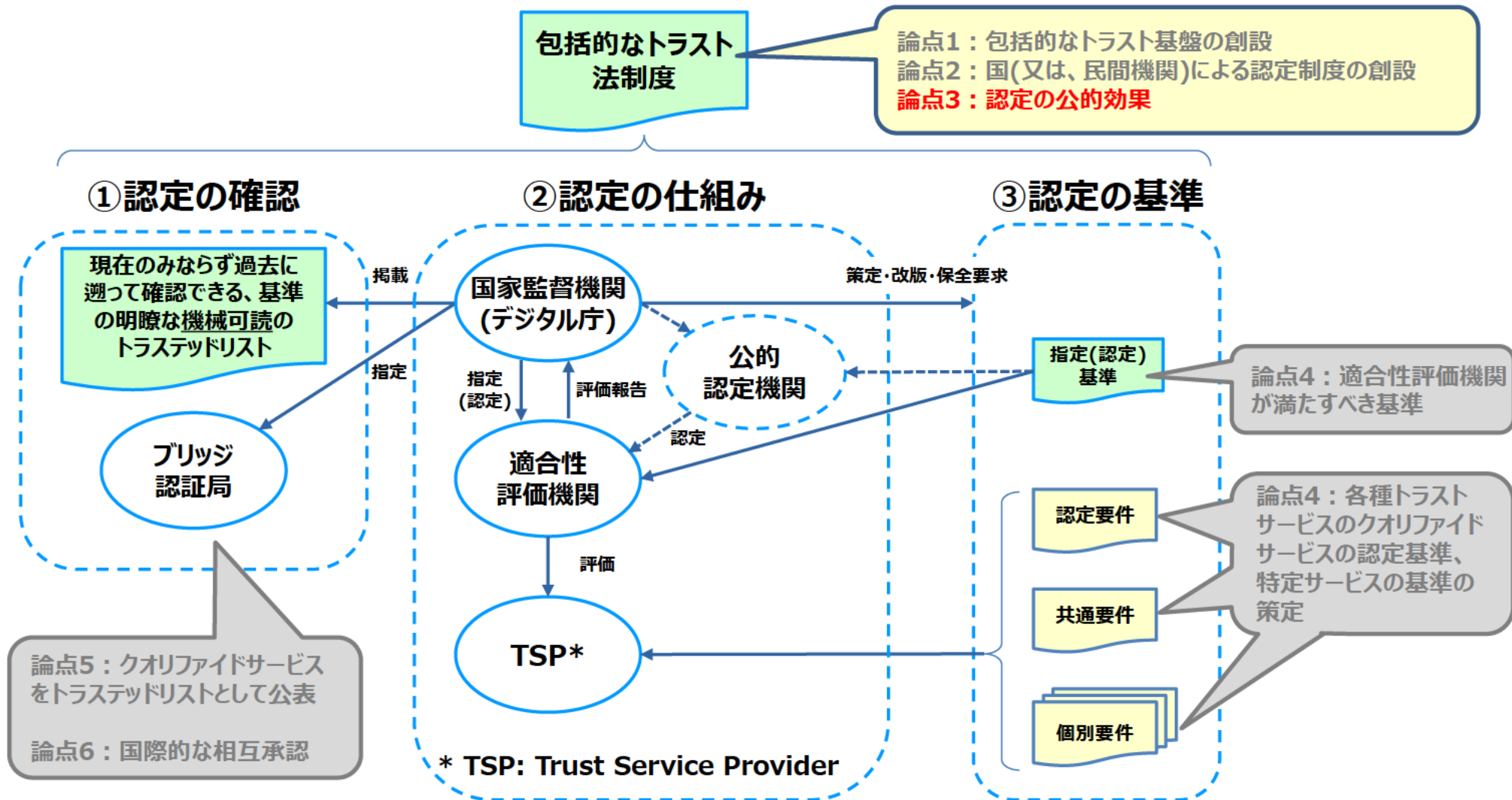
民間機関となる場合、認定主体を認定する基準はどうあるべきか。

1. 信頼のおけるトラストサービスの提供にかかるプレーヤは、①国（制度統括、認定基準策定、事業者の監督）、②適合性評価機関を認定する公的組織、③適合性評価機関（トラストサービスの準拠性監査を実施）、④トラストサービス事業者などが考えられる。
2. 認定の法的な効果を説明可能とすることが重要であり、そのためには国による適切な関与が必須である。
3. 信頼の置けるトラストサービス及びそれを提供する事業者を、利用者が容易に判別できるよう、サービス及び事業者に求められる客観的な基準が策定・公表されるとともに、サービス及び事業者の当該基準への適合性を第三者が評価・認定する制度を構築するべきである。
4. 基準策定、監督、適合性評価、認定主体の4つの軸について国が一定程度関与した制度設計が必要であり、以下の赤枠の範囲について検討することが適切である。

	適格 (日本、EU)	特定1 (EU)	特定2 (日本)	その他	
基準策定	国または 標準化機関	国または 標準化機関	国	民間機関	民間機関
監督	国	国	—	民間機関	—
適合性評価	国又は国が 指定・認定する機関	・適合性評価機関 ・自己宣言 (適合性評価報告 書を作成)	自己宣言	適合性評価機関	自己宣言
認定主体	国	—	—	—	—

# 論点3：認定の公的効果

## 第1回 主な論点の全体像の再掲



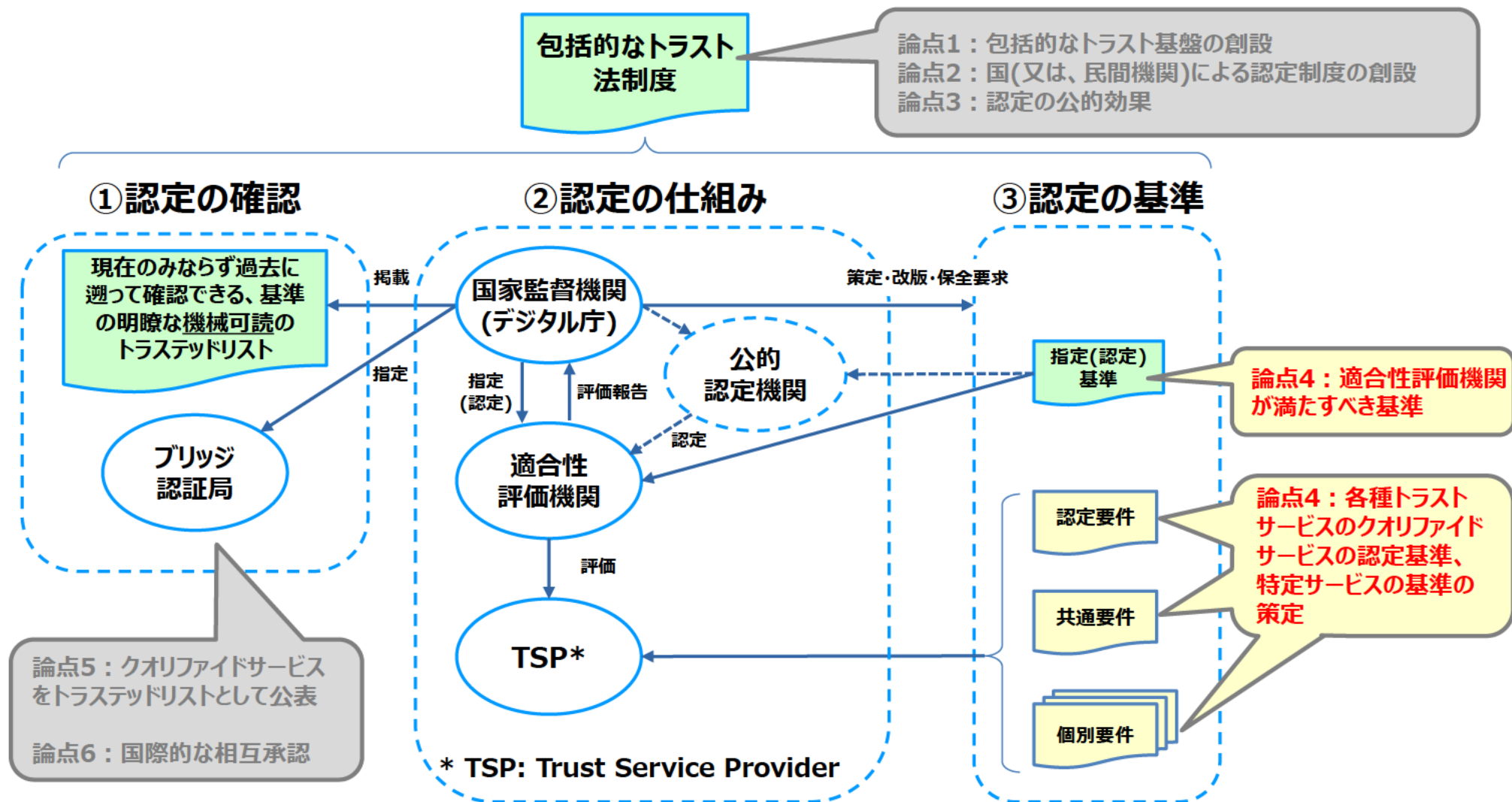
# 論点3：認定の公的効果

電子文書の法的位置づけや、トラストサービスの認定の法的・手続的な効果を明示する必要があるのではないか。

1. 電子情報・データの効力について、包括的な規定を置くことが必要である。
2. 認定等を得たトラストサービスに基づく情報の、通用性を明示する必要がある。国が制度に基づいて交付・保存・提出を求めているすべての書類について、電子化に際し、どのレベルのトラストサービスを求めるか明示すべきである。
3. 上記2の一覧を国などがまとめるべきである。
4. 海外との相互承認を推進するためには、法的効果について諸外国と同等の規定を置く必要がある。
  - (1) 海外のトラストサービスについて、我が国における法的効果を認める規定をおくことにより、我が国と相互承認する意義が高まる。
  - (2) トラストサービスの法的効果をeIDAS規則と同等程度に規定するべきである。
  - (3) 適合性評価機関やトラストサービスの責任を明記し、海外に対する法的信頼性を高めるべきである。
5. 我が国の既存制度の整理が必要である。(国が行うトラストサービスの位置づけ等)

# 論点4：各種トラストサービスのクオリファイドサービス認定基準、特定サービス基準の策定

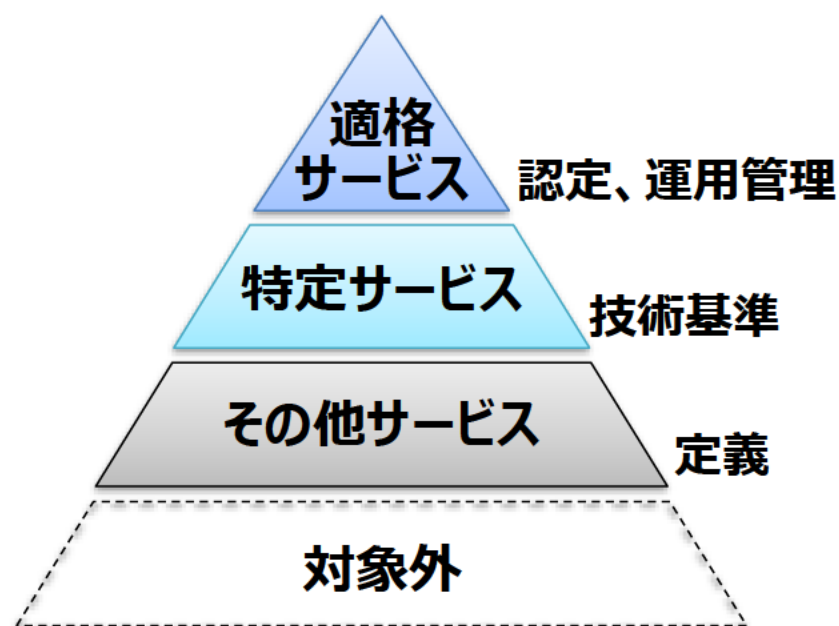
## 第1回 主な論点の全体像の再掲



## 論点4：各種トラストサービスのクオリファイドサービス認定基準、特定サービス基準の策定

クオリファイド(適格)サービスの認定基準、特定サービスの基準はどうあるべきか。  
(トラストサービス定義、技術安全基準、真偽確認方法、設備要件、業務運営要件等)

1. 国際的な評価制度と協調した統一的な制度を構築すべき。
2. 評価制度を整備するための法的枠組みを構築すべき。
3. 認定に係る技術基準、標準規格を諸外国との整合性や最新技術動向を踏まえて国の関与のもとに作成すべき。

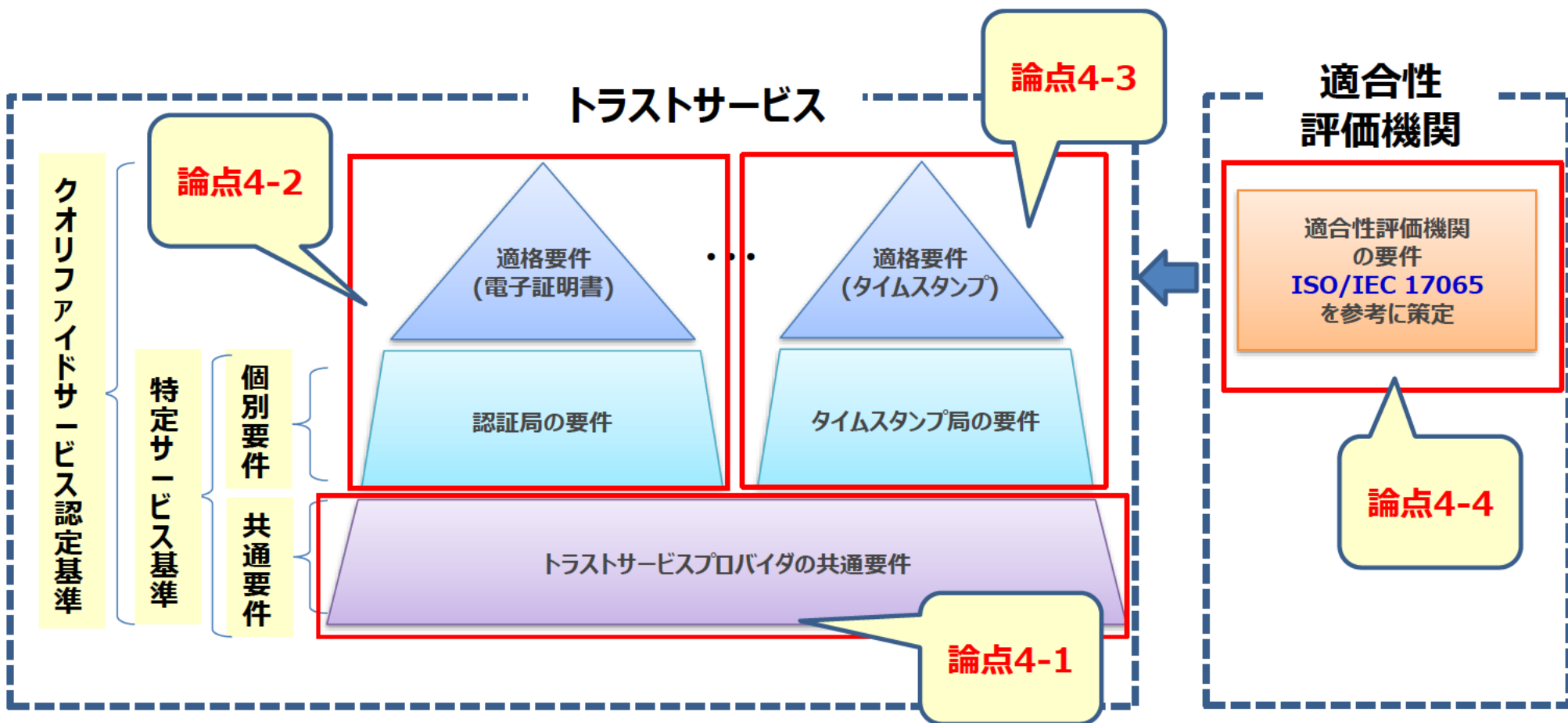


これらのサービスの評価基準として、国内外のニーズに対応した公的標準を作成



## 論点4：各種トラストサービスのクオリファイドサービス認定基準、特定サービス基準の策定

1. トラストサービスに関する技術標準は共通要件と個別要件、適格要件を体系化したものを作成すべき。
2. 適合性評価機関の要件を定める国際的な整合性を持った基準を定めるべき。



# 論点4-1：トラストサービスプロバイダの共通要件

すべてのトラストサービス事業者に対する共通的な要件として、トラストサービス事業者の共通要件を示す文書を作成してはどうか

1. UNCITRALでは、トラストサービス提供者の義務等も記述されている。また、ETSI EN319 401では、ISO/IEC 27001等の引用により、リスクマネジメント等の具体的な要件が規定されている。
2. 電子署名法や公的個人認証法等それぞれにおいて、同様の視点で要件を記載している。ただし、第1回資料2-1で示されたとおり情報セキュリティに関するリスクマネジメントの概念が含まれていない等アップデートが必要である。
3. 現行の法令が定める要件は、下記の通りさまざまな点で差異が存在している。なお、法律のみならず、施行規則、告示等の関連規定を含んだ比較をしている。

## 電子署名法

## 公的個人認証法

## タイムスタンプ

## EU (ETSI EN 319 401)

組織	電子署名法	公的個人認証法	タイムスタンプ	EU (ETSI EN 319 401)
	・欠格条項	・J-LIS	・欠格条項と財政的要件	・公平性と財政的要件
設備	・物理的アクセス ・災害被害防止措置 等	・物理的アクセス ・災害被害防止措置 等	・物理的アクセス ・災害被害防止措置 等	・物理的アクセス ・災害被害防止措置 等
技術	・アクセス制御 ・暗号制御 ・不正アクセス防止 等	・アクセス制御 ・暗号制御 ・不正アクセス防止 等	・アクセス制御 ・暗号制御 ・ネットワークセキュリティ 等	・アクセス制御 ・暗号制御 ・ネットワークセキュリティ 等
運用	・利用者へのポリシー提供 ・権利・利益侵害時における利用者への開示 等	・利用者へのポリシー提供 ・権利・利益侵害時における利用者への開示 等	・利用者へのポリシー提供 ・安全性の侵害など利用者への開示 等	・利用者へのポリシー提供 ・安全性の侵害など利用者への開示 等
	・危機管理 ・人的資源 ・組織運営のセキュリティ 等	・危機管理 ・人的資源 ・組織運営のセキュリティ 等	・リスク、インシデント管理 ・人的資源 ・組織運営のセキュリティ ・廃業計画 等	・リスク、インシデント管理 ・人的資源 ・組織運営のセキュリティ ・廃業計画 等

# 論点4-2：認証局の要件及び適格要件

- ・ヒト、組織、モノに対して電子証明書を発行する認証局の規格類として、EUなど諸外国の標準を参考にしつつ、今後、以下の文書を作成する必要がある。

## 【認証局の要件】

### ①設備基準

認証局の災害被害防止措置、設備の物理的アクセス管理、入退室管理 等

### ②技術基準

利用者鍵管理、暗号装置、ネットワーク管理、認証・権限確認基準 等

### ③運用基準

証明書ポリシー(CP)、認証業務規程(CPS)、運用体制、リスクマネジメント、事業継続計画、本人確認、証明書ライフサイクル管理 等

## 【認証局の適格要件】

上記要件に加え、

### ①適格電子証明書の発行及び管理のサポートに関する基準

(より厳格な本人確認、利用者秘密鍵の生成及び保管の装置 等)

### ②電子証明書が適格であることを示す記載に関する基準

# 論点4-3：タイムスタンプ局の要件と適格要件

- ・タイムスタンプを発行するトラストサービス事業者の規格類として、時刻認証業務の認定に関する規程等を基に、EUなど諸外国の標準を参考にしつつ、今後、以下の文書を整備する必要がある。

## 【タイムスタンプ局の要件】

### ①設備基準

TSA局の災害被害防止措置、設備の物理的アクセス、入退室管理 等

### ②技術基準

時刻源、時刻の品質管理及び証明、通信経路の安全性、タイムスタンプトークンのプロフィール、暗号技術、TSA公開鍵証明書、暗号装置 等

### ③運用基準

運用規程（TPS）、運用体制、暗号デバイス管理、事業継続計画、災害復旧計画、終了計画、秘密鍵危殆化時の対応、コンプライアンス 等

## 【タイムスタンプ局の適格要件】

上記要件に加え、

### ①TSA公開鍵証明書の条件

②同一のタイムスタンプ発行装置（TSU）で非適格タイムスタンプを発行しないこと

③タイムスタンプが適格であることを示す記載に関する基準

# 論点4-4：適合性評価機関の満たすべき要件

1. 国際的な相互承認を実現するために、トラストサービスの適合性評価機関（CAB：Conformity Assessment Body）の満たすべき要件として、国際標準等に準拠した国内標準を策定する必要がある。
2. トラストサービスの適合性評価機関を評価する仕組み（Accreditation）を、国内でどのように構築するかを早期に検討すべきである。

【我が国】  
法令等に基づく**指定調査機関による適合性調査**

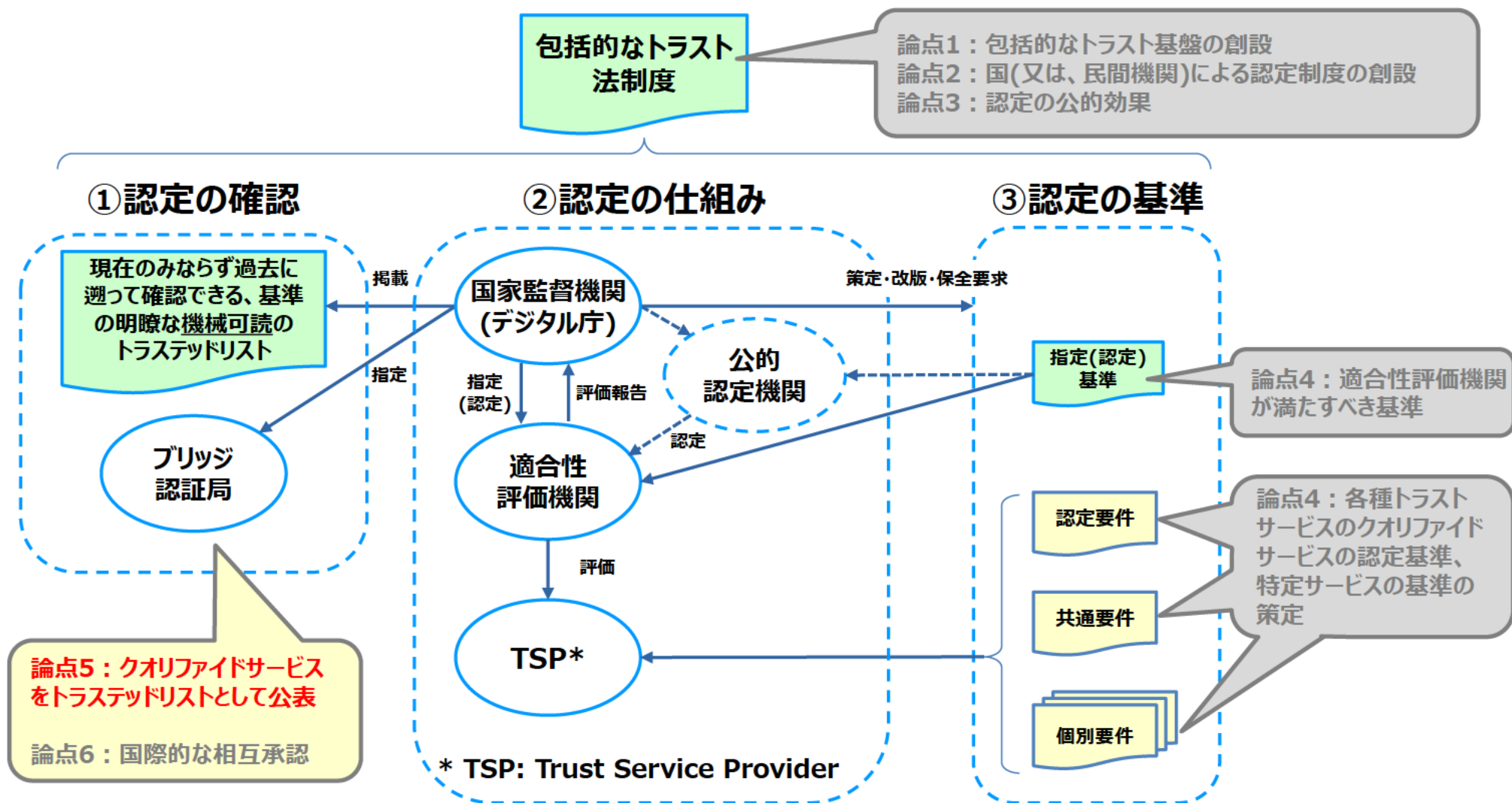
【諸外国】  
国際標準に基づき認定された**適合性評価機関による適合性評価**

電子署名法	ISO/IEC 17065 （製品、プロセス及びサービスの認証を行う機関に対する要求事項）	ETSI EN 319 403 （トラストサービス評価特有の追加基準）
第四章 指定調査機関等 第一節 指定調査機関 （指定調査機関による調査） （指定） （欠格条項） （指定の基準） （指定の公示等） （指定の更新） （秘密保持義務等） （調査の義務） （調査業務規程） （帳簿の記載） （適合命令） （業務の休廃止） （指定の取消し等） （主務大臣による調査の業務の実施）	1.適用範囲、2.引用規格、3.用語と定義	適宜追加
	4.一般要求事項	4.2.1 公平性に抵触しない活動
	5.組織構成に関する要求事項	追加無し
	6.資源に関する要求事項	6.1 認証機関の要員
	7.プロセス要求事項	7.1 一般 7.3 申請のレビュー 7.4 評価 7.6 認証の決定 7.7 認証文書 7.8 認証されたサービスの登録簿 7.9 サーベイランス 7.10 認証に影響を与える変更
第二節 承認調査機関 （承認調査機関の承認等） （承認の取消し）	8.マネジメントシステム要求事項	追加無し



# 論点5：クオリファイドサービスをトラステッドリストとして公表

## 第1回 主な論点の全体像の再掲



# 論点5：クオリファイドサービスをトラステッドリストとして公表

認定を受けたクオリファイドサービスであることを、利用者が、必要なときに確認できる仕組みはどうあるべきか。

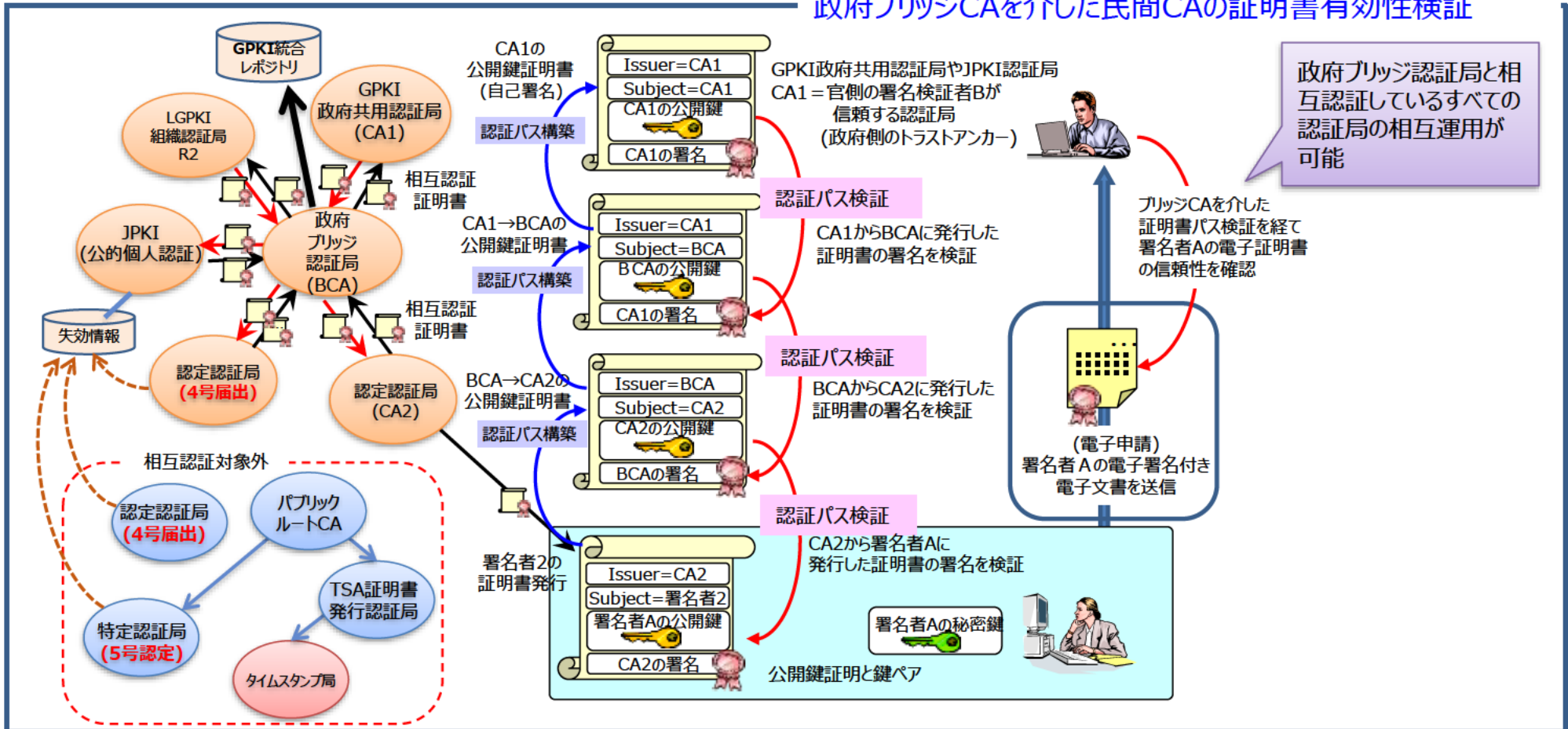
- 国内の利用者が相互に適格性を確認できるように、認定を受けたクオリファイドサービスを公表することが必要である。そのためには以下の点に留意が必要である。
  1. クオリファイドサービスを利用する者の間では、相互に相手が利用するサービスの適格性が確認できる仕組みを検討すべきである。
  2. 利用者の利便性の観点からは認定を受けたクオリファイドサービスは、機械可読の形態で開示する、又は相互接続することを検討すべきである。
  3. 認証局以外のトラストサービスや廃業したトラストサービスを扱うことを検討すべきである。
  4. クオリファイドサービスを確認する仕組みは以下が考えられるが、上記2、3よりトラステッドリストで公開する方法を検討すべきである。

方式	対象となる認証局等	一意に特定	可読性		廃業TSPの検証	日本での制度運用	課題	
			人	機械				
ブリッジ	ブリッジ認証局と相互認証	GPKI、認定認証局 (署名法認定)	○	×	○	×	○	官側の検証は問題ないが、検証に必要な情報が民間開放されていない。
リスト	官報にCA認証局のハッシュ値を公開	認定認証局 (署名法認定)	○	△	×	×	○	実際の確認が困難
	ホームページでサービス名を公開	認定認証局 (署名法認定) タイムスタンプ (デ協認定)	×	○	×	×	○	実際を検証時に本物の証明書が不明
	ブラウザーにルート証明書を登録 (Common CA Data Base:CCADB)	Webサーバー証明書を発行する パブリック認証局 (WebTrust監査、ETSI監査)	○	○	○	×	○	民間団体 (CAブラウザーフォーラム) による運用であり制度安定性が課題
	アドビ製品に登録 (AATL)	ドキュメント署名用の パブリック認証局 (WebTrust監査、ETSI監査)	○	△	○	×	○	民間企業による自社製品での運用。 PDF署名に限定
	トラステッドリストで公開 (EU Trusted List)	EUのトラストサービス事業者 (CABの適合性監査)	○	○	○	○	×	認証局だけでなくタイムスタンプ局等も取り扱える。EU域内で相互運用されているが国際的な相互運用はトライアル中

# 【参考1】論点5：クオリファイドサービスをトラステッドリストとして公表

1. 政府ブリッジ認証局を介したルート認証局の相互認証により、各クオリファイドサービスを利用する者の中で、相互に相手が利用するサービスの適格性が確認できるしくみは以下となる(米国連邦政府PKI(FPKI)と同じブリッジモデルを採用)。
2. 電子署名法の認定外の認証局やタイムスタンプ局は相互認証対象外になっている。

## 政府ブリッジCAを介した民間CAの証明書有効性検証

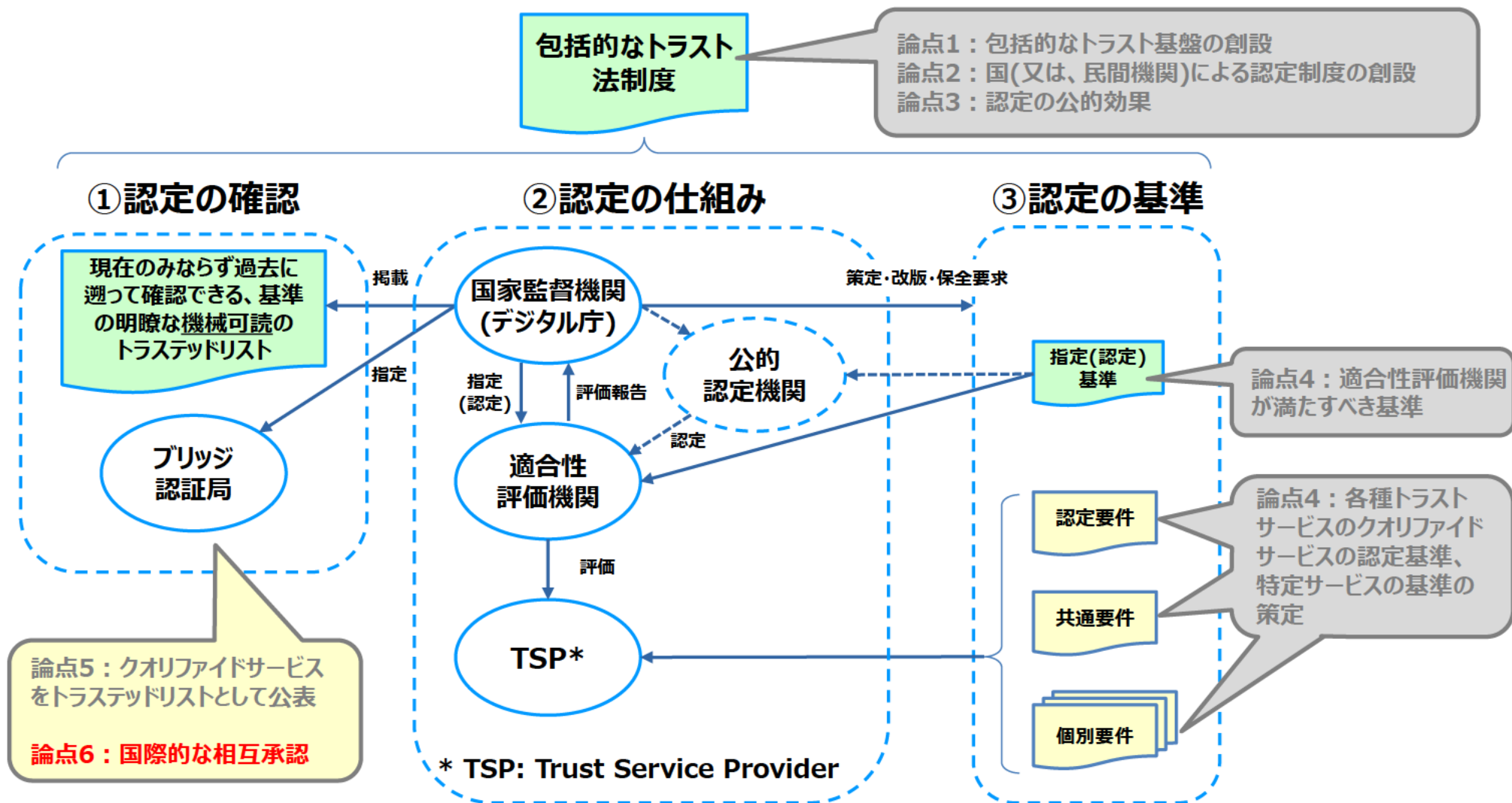






# 論点6：国際的な相互承認

## 第1回 主な論点の全体像の再掲





# 論点6：国際的な相互承認

国際的な相互承認をうるためには、どうあるべきか。

●以下の4つの項目において、論点1～5を踏まえ、国際間での同等性を確保する必要がある。

	項目	論点	国際相互承認のために必要な施策
1	法制度	論点1：包括的なトラスト基盤の創設 論点2：国(又は、民間機関)による認定制度の創設 論点3：認定の公的効果	・トラストサービスの認定に係るフレームワークの同等性 ・国による認定制度の確立 ・法的効果の同等性
2	監督・適合性評価	論点4-4：適合性評価機関の適合性	・適合性評価機関の要件の同等性 ・指導・監督の仕組みの確立
3	技術標準	論点4-1：トラストサービスプロバイダの共通要件 論点4-2：認証局の要件 論点4-3：タイムスタンプ局の要件	・技術標準の作成・維持の体制の整備 ・技術標準の同等性に関する検討
4	トラストアンカー間の接続の仕組み	論点5：クオリファイドサービスをトラステッドリストとして公表	・トラステッドリスト方式とブリッジ方式の併用