資料２

トラストを確保したDX推進SWG
トラストサービスのアシュアランスレベルの考え方

2022年2月8日

慶應義塾大学
手塚　悟

トラストを確保したDX推進SWGスケジュール（案）

2021年12月末

- トラストスコープで集中的にニーズやユースケースを検討する範囲特定
- 電子化できる手続・取引の主要事例

2022年3月末

- トラスト実態調査分析結果に基づく対応検討
- IDのアシュアランスレベル整理
- トラストサービスのアシュアランスレベル整理

2022年6月末

- トラストポリシー基本方針
- ユースケース選定
- 報告書とりまとめ（日・英）

出典：第1回トラストを確保したDX推進SWG資料1

トラストサービスのアシュアランスレベルにおける主な論点案

1 アシュアランスレベルの基準

- トラストサービスのアシュアランスレベルに関して、どのような基準が考えられるか
- 考慮すべき要素（トラストレベルの担保、国際的な通用性、ユーザーへのわかりやすさ等）
- 具体的なユースケースにおける検討

2 機動性の確保

- 技術進化に対応した柔軟な見直しが求められる中、機動性の確保するための考え方
- トラストアシュアランスレベルの策定/運営の在り方

出典：第4回トラストを確保したDX推進SWG資料1

トラストサービスの定義（１）

別紙

プラットフォームサービスに関する研究会
トラストサービス検討ワーキンググループ
最終取りまとめ

プラットフォームサービスに関する研究会

トラストサービス検討ワーキンググループ

はじめに

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）、Society5.0。

このような Society5.0 として実現される社会においては、ICT 機器の爆発的な普及や、AI の能力の飛躍的な増大とその活用に伴うビッグデータの分析・利活用の進展、すべての人とモノが繋る IoT（Internet of Things）等の社会実装が進み、社会のあらゆる場面でデジタル革命が浸透することで、今までにない、新たな価値が生み出されることが期待される。

Society5.0 の中核となるデータ駆動型社会（Data-driven society）では、良質、最新、正確かつ豊富なリアルデータが価値の源泉となり、経済社会活動を支える最も重要な糧となることが見込まれる。これは、とりもなおさず、経済社会を支える中核的な要素としてのデータの重要性が飛躍的に増大することを意味する。

このような様々な可能性を秘めるデータ駆動型社会においては、そのバックボーンとなるデータの真正性やデータ流通基盤の信頼性を確保することが極めて大切となる。そのためには、インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み（トラストサービス）の実現に向けて、包括的な検討を加えることが必要となってくる。

また、海外に目を転じてみれば
に、その基盤を支えるために包括
うな国際的な動向も見据えなが
とが必要である。

このような状況を背景に、本ワーキンググループが「プラットフォームサービスに関する研究会」の下に設置された。本ワーキンググループは、我が国におけるトラストサービスの現状と課題を整理し、課題を解決するための方策について検討を行い、今般、これまでの事業者ヒアリングや構成員の意見等を踏まえ、取り組むべき事項の全体像を最終取りまとめとして整理した。

インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み（トラストサービス）

出典：総務省　プラットフォームサービスに関する研究会　最終報告書（2020年2月）別紙
https://www.soumu.go.jp/main_content/000668595.pdf

トラストサービスの定義（２）

- 各種トラストサービスのイメージ

（ア）電子データを作成した本人として、ヒトの正当性を確認できる仕組み
→電子署名（個人名の電子証明書）

（イ）電子データがある時刻に存在し、その時刻以降に当該データが改ざんされていないことを証明する仕組み
→タイムスタンプ

（ウ）電子データを発行した組織として、組織の正当性を確認できる仕組み
→eシール（組織名の電子証明書）

（エ）ウェブサイトが正当な企業等により開設されたものであるか確認する仕組み
→ウェブサイト認証

（オ） IoT 時代における各種センサーから送信されるデータのなりすまし防止等のため、モノの正当性を確認できる仕組み
→モノの正当性の認証

（カ）送信・受信の正当性や送受信されるデータの完全性の確保を実現する仕組み
→eデリバリー

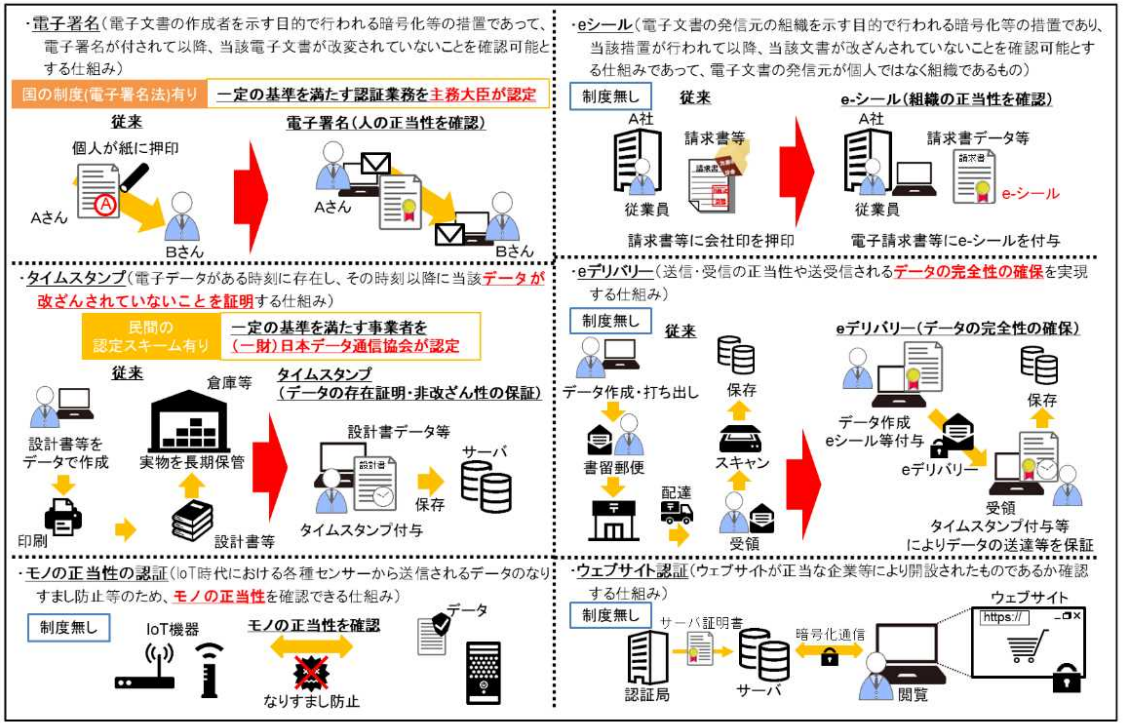
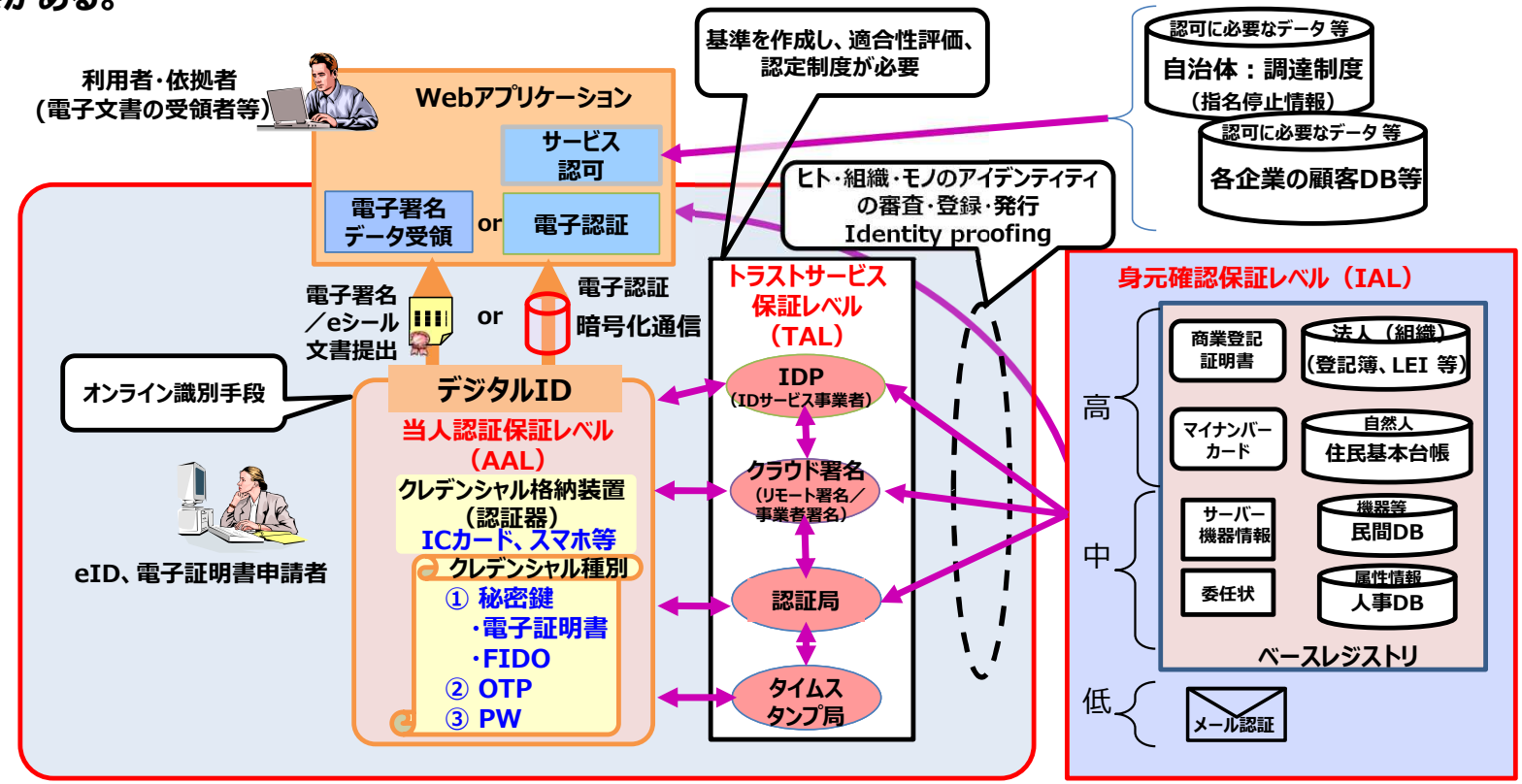


図 1 各種トラストサービスのイメージ

出典：総務省 プラットフォームサービスに関する研究会 最終報告書（2020年2月）別紙
https://www.soumu.go.jp/main_content/000668595.pdf

トラストの全体像（１）

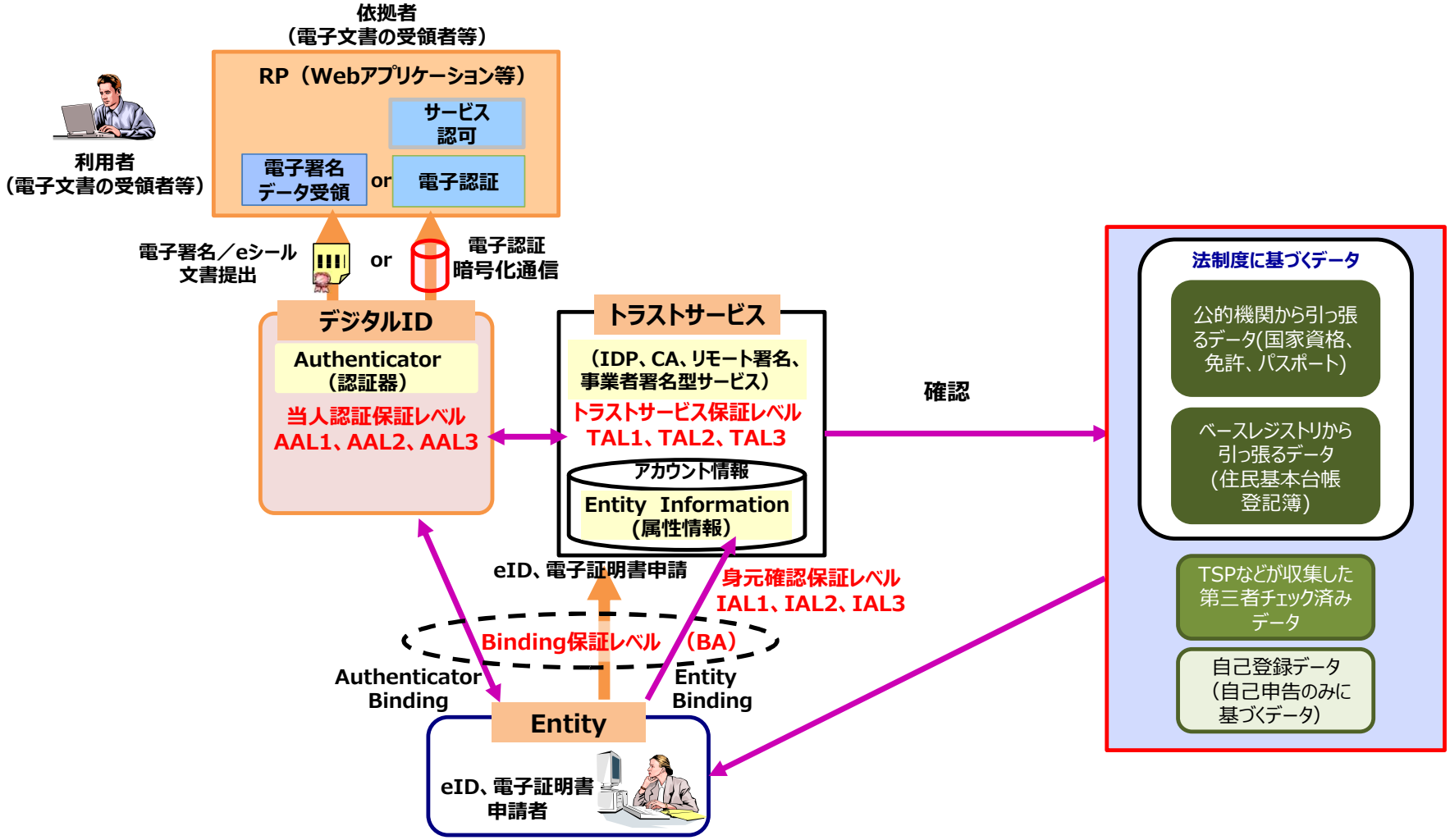
- トラストのレベルは、身元確認（IAL）、当人認証（クレデンシャル）の強度（AAL）、トラストサービスの信頼度（TAL）で決定され、手続き記録の真正性（証拠力）が求められる程度で電子署名もしくは電子認証が選択されうる。
- 従来は業務アプリケーション毎の判断で本人を確認しクレデンシャル（パスワード等）を発行し利用者を特定していたが、社会的混乱を防ぐためベースレジストリと紐づけたデジタルIDをトラストサービスから発行するスキームの創設が重要となる。
- そのためにはデジタルIDの保証レベルや、デジタルIDを発行するトラストサービスに求められる保証レベルを検討し認定制度を創設する必要がある。



出典：第1回トラストを確保したDX推進SWG資料5

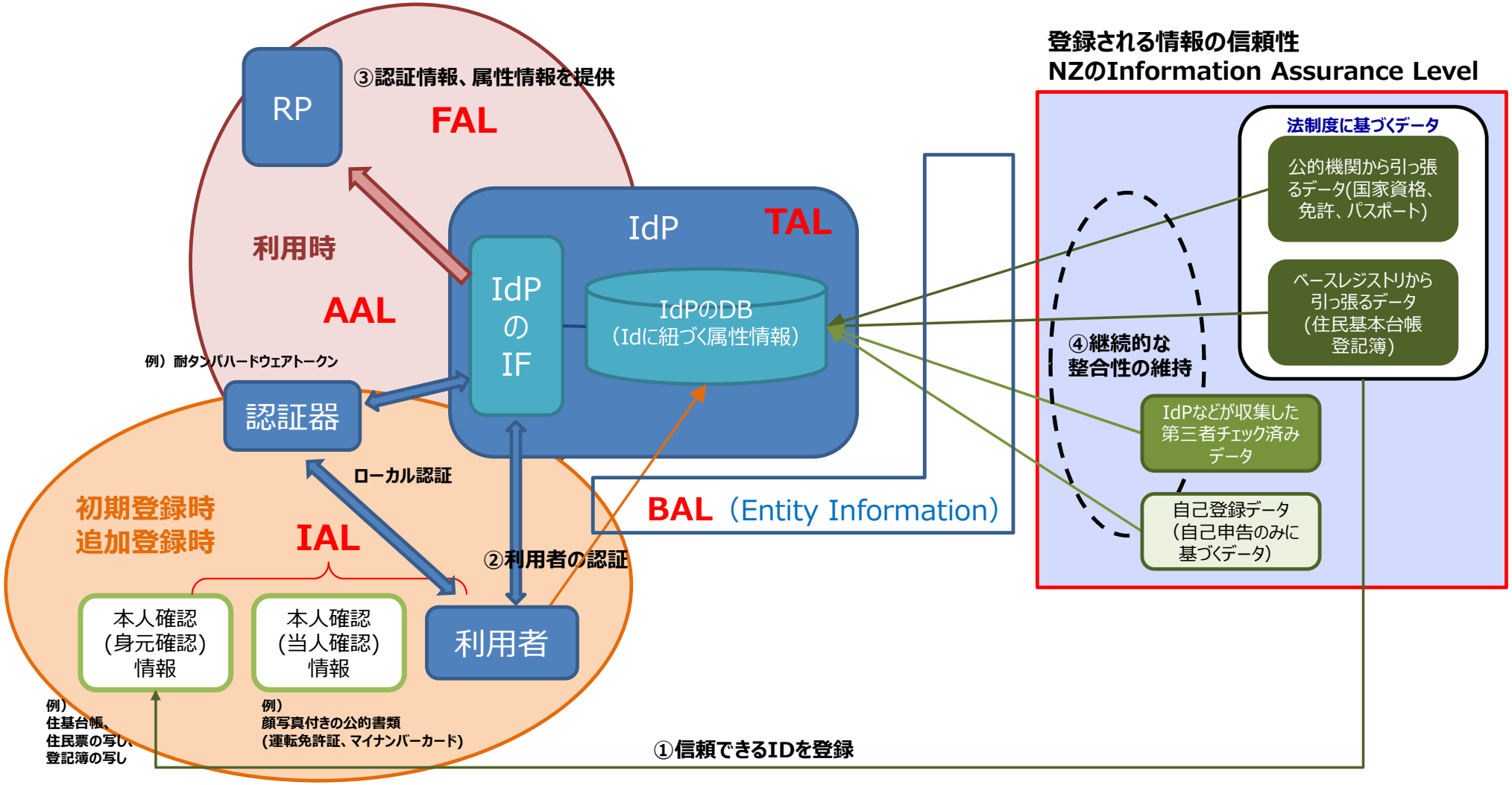
トラストの全体像（２）

●トラストサービスのアシュアランスレベルの全体像におけるBinding 保証レベルの位置づけ



IDPにおける各アシュアランスレベルの考え方

●Entity Informationの正確性のライフサイクルを通じた維持（属性情報変更の反映等）が重要



論点1：アシュアランスレベルの基準

- トラストサービスのアシュアランスレベルに関して、どのような基準が考えられるか

● トラストサービス事業者（IDプロバイダー、クラウド署名サービス※、認証局、タイムスタンプ局等）の運営ポリシーをトラストサービスアシュアランスレベル（TAL：Trust service Assurance Level）として整理すべきである。
  - 組織要件（組織の責任）
  - 設備要件（ファシリテイ要件）
  - 技術要件（暗号技術等）
  - 鍵管理要件（適格署名生成装置等）
  - 運用要件（複数人による相互牽制）
  - 監査要件（内部監査、外部監査、適合性監査、認定）
  - その他

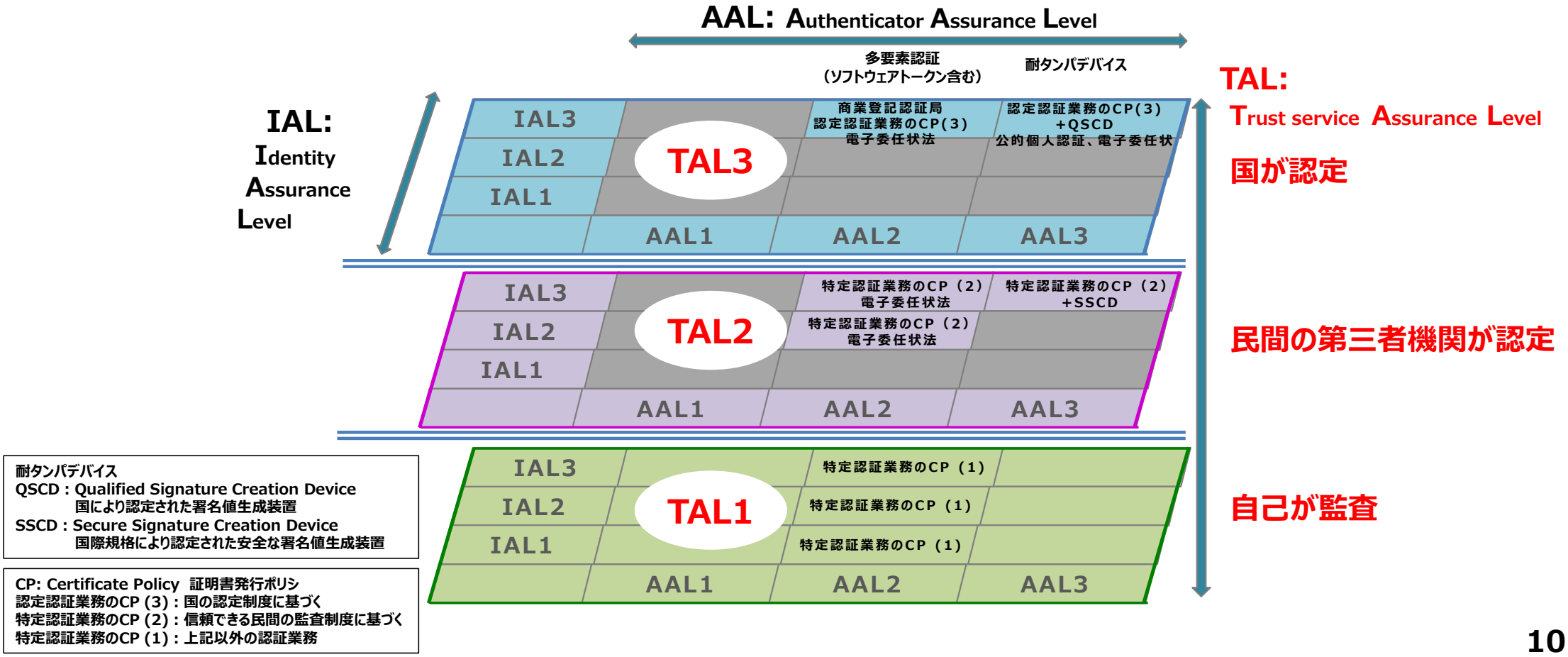
● これらをトラストサービスに共通する基準、個別の基準として整理し、TAL1、TAL2、TAL3のアシュアランスレベルを定義する。それぞれの認定主体としては以下を想定する。

  TAL3：国が認定
  TAL2：民間の第三者機関が認定
  TAL1：自己が監査

※　当事者の署名鍵によるリモート署名サービスおよび利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービス（令和2年7月17日　主務三省Q&Aより）

論点1：アシュアランスレベルの基準

- アシュアランスレベルの基準はIAL、AAL、TALの組み合わせから構成される。（下図は認証局を例にしたイメージ）
- IDプロバイダー、クラウド署名サービス、認証局、タイムスタンプ局等に対してユースケースに応じた基準を作成すべき。



耐タンパデバイス
QSCD：Qualified Signature Creation Device
国により認定された署名値生成装置
SSCD：Secure Signature Creation Device
国際規格により認定された安全な署名値生成装置

CP: Certificate Policy 証明書発行ポリシ
認定認証業務のCP (3)：国の認定制度に基づく
特定認証業務のCP (2)：信頼できる民間の監査制度に基づく
特定認証業務のCP (1)：上記以外の認証業務

論点1：アシュアランスレベルの基準

- 考慮すべき要素（トラストレベルの担保、国際的な通用性、ユーザーへのわかりやすさ等）

● トラストレベルの担保
  - ニーズと基準や制度との整合性を担保する必要がある。
  - 各トラストサービス固有の脆弱性に対する「脅威耐性」ベースでの検討が必要である。
    （例:同じ設備要件でもトラストサービスにより対象やレベルが異なる）

● 国際的な通用性
  - 国際的な基準との整合性や関連基準の参照をする。
    （ISO/IEC 27000シリーズ、CAB/F baseline requirement、ETSIやCEN規格、Webtrust監査基準、等）
  - 適合性評価機関の国際的な整合性確保
    各トラストサービスに対し上記基準への適合性評価を行う機関の要件を国際標準（ISO/IEC 17065、ETSI EN 319 403など）を参考に規定する。

● ユーザーへの分かりやすさ
  クオリファイド(TAL3)、アドバンスド(TAL2)等、どのレベルを満たしたトラストサービスであるか、利用者にとってわかりやすい仕組みの検討が必要である。
    （認定トラストサービスの機械可読な形での公開や、署名検証など当該トラストサービスに基づく情報（署名値やタイムスタンプトークンなど）の検証などの利用時にどのレベルのトラストサービスであるかユーザーが分かる形の基準策定）

論点２：機動性の確保

- 技術進化に対応した柔軟な見直しが求められる中、機動性の確保するための考え方

● 各基準は法令から参照される独立した技術規格として策定されるべきであり、変化する技術進化や国際標準に対応したメンテナンス性が確保される必要がある。

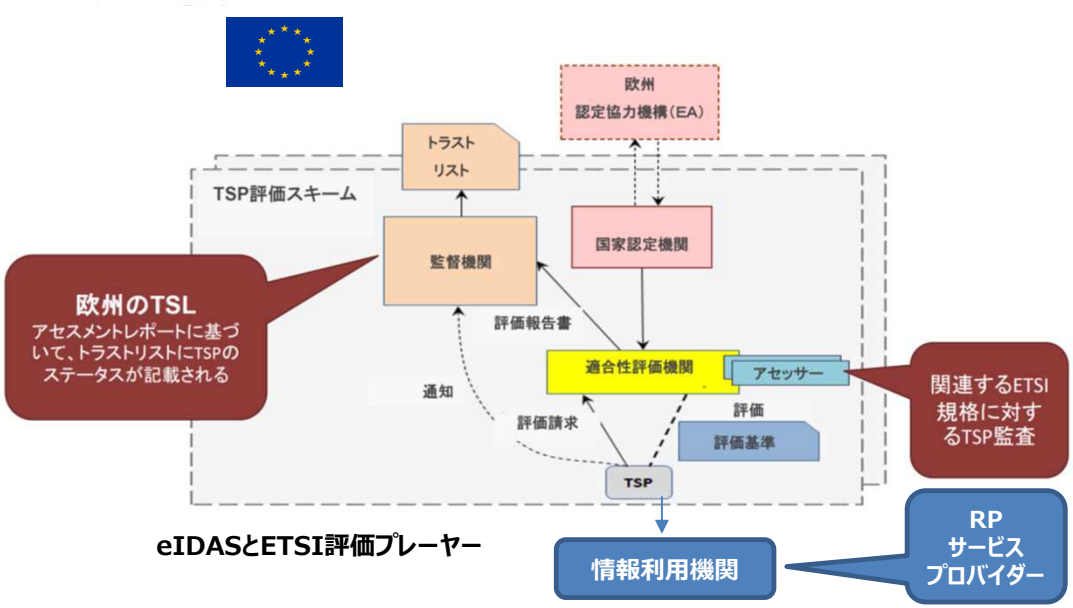
- トラストアシュアランスレベルの策定/運営の在り方

● 各基準は諸外国の標準などを参考に国の関与の下に、トラストサービスフレームワークに対応してクオリファイドレベル(TAL3)とアドバンスドレベル(TAL2)等に応じて作成することが必要である。

● 変化する技術進化や国際標準をウオッチし適時、適切に基準のバージョンアップを行う体制、運営の在り方の検討が必要である。

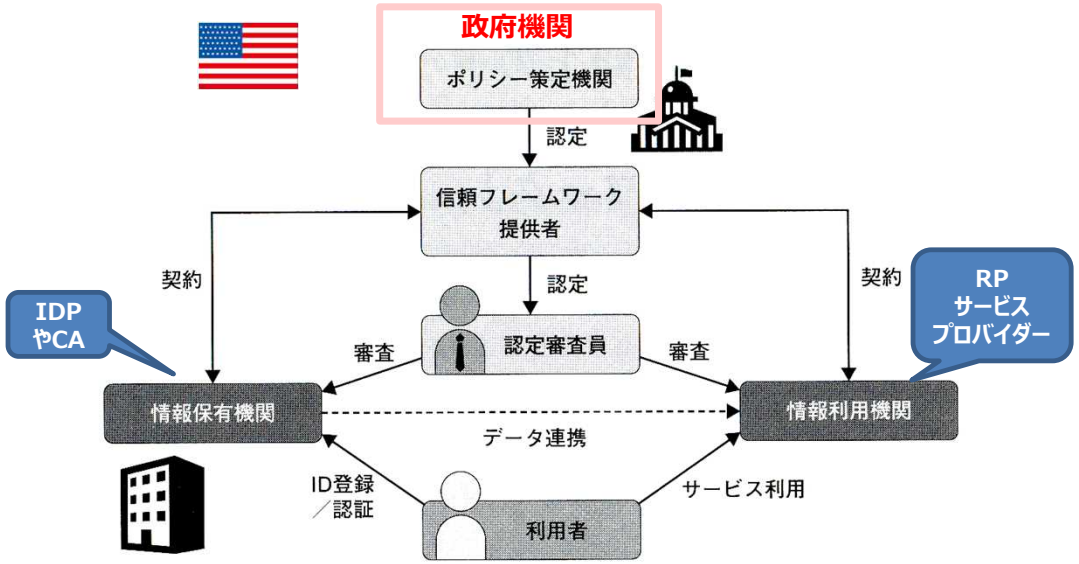
海外のトラストフレームワーク

●欧州、米国のトラストフレームワークを比較すると、そのポリシーは両者とも国(政府）主導により策定されている。



eIDASとETSI評価プレーヤー

TUViT Clemens Wanko
Audits based on ETSI CP for qualified TSP and global recognition
Japan-Europe Internet Trust Symposium
July 4 th , 2017 を参考に追記

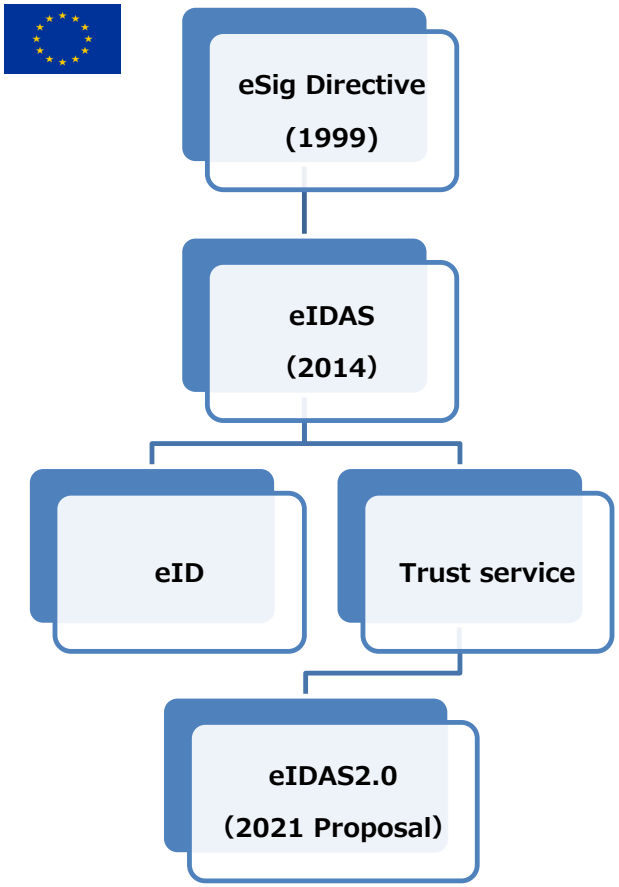


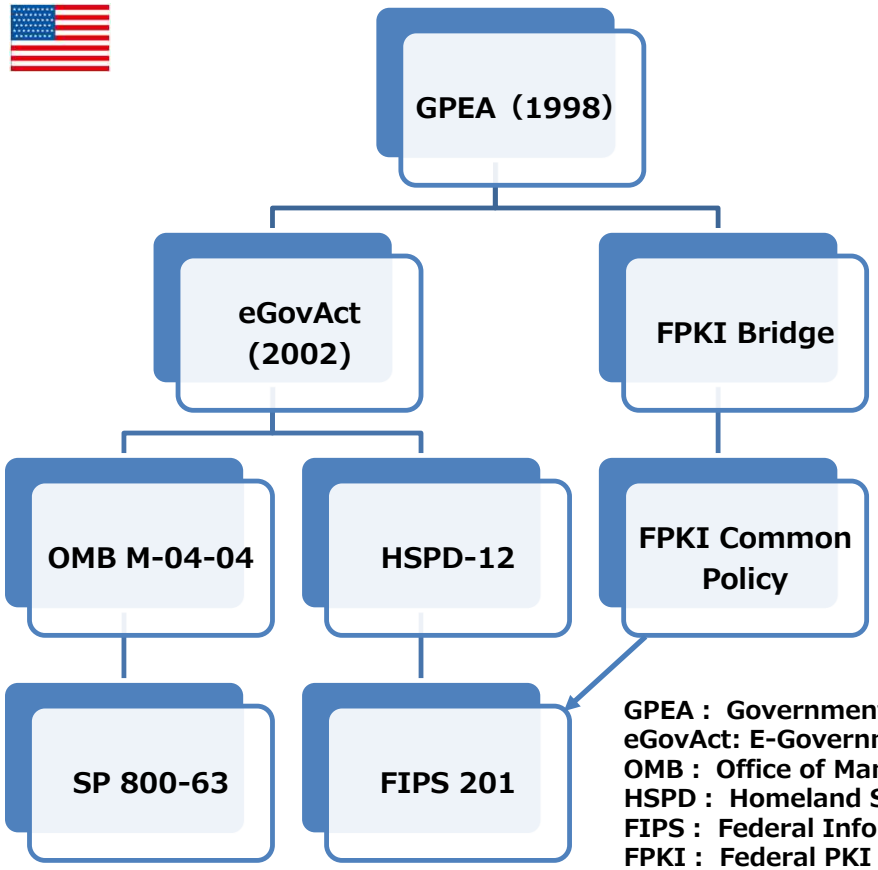
図表 9-1 アイデンティティー・トラストフレームワークの構成
出所：山中進吾『信頼フレームワーク最新動向』（2011）を基に筆者

崎村夏彦,「デジタルアイデンティティー」,日経BP,2021年7月20日 を参考に追記

海外の制度化プロセスの事例

●欧州、米国の制度化プロセスを構成する法制度やポリシー、技術基準の概要は、以下となっている。





GPEA： Government Paperwork Elimination Act
eGovAct: E-Government Act
OMB： Office of Management and Budget
HSPD： Homeland Security Presidential Directive
FIPS： Federal Information Processing Standards
FPKI： Federal PKI

主な国際的なトラストフレームワークの比較表

Table 4: Comparison between the trust frameworks (based on (Hamaguchi, 2016))

	ETSI	WEBTRUST	eIDAS	FPKI	ISO 27000
Law	Supports eIDAS Regulation	N/A	eIDAS Regulation	e-Government Act of 2002	N/A
Objective	Technical interoperability and trusted third party assessment	Technical interoperability and trusted third party assessment	Legal recognition of electronic trust services	Identity management and trust across organizational, operational, physical and network boundaries	Information security
Governor	ETSI Board	N/A	EU Committee	CIO Council	
Harmonization Body	ETSI ESI	PKI Assurance Task Force	FESA	N/A	
Accreditation Body	National Accreditation Bodies	CPA Canada	NAB	FPKI Policy Authority	National Accreditation Bodies
Conformity Assessment Body	CAB accredited to EN 319 403	Same as above	Conformity Assessment Body	FPKI Certificate Policy Working Group	Conformity Assessment Body
Supporting Technical Standards	ETSI Standards, CA/B Forum: BRG, EVCG + NetSec	WebTrust Criteria	ETSI Standards, CEN Standards	NIST SPs, FIPS 201, FPKIPA Documents	
Assurance to be achieved	Best Practices and Legal Compliance	Best Practices	Legal Compliance	Technical Compliance, Interoperability with FPKI system	Technical Compliance to Management Requirements

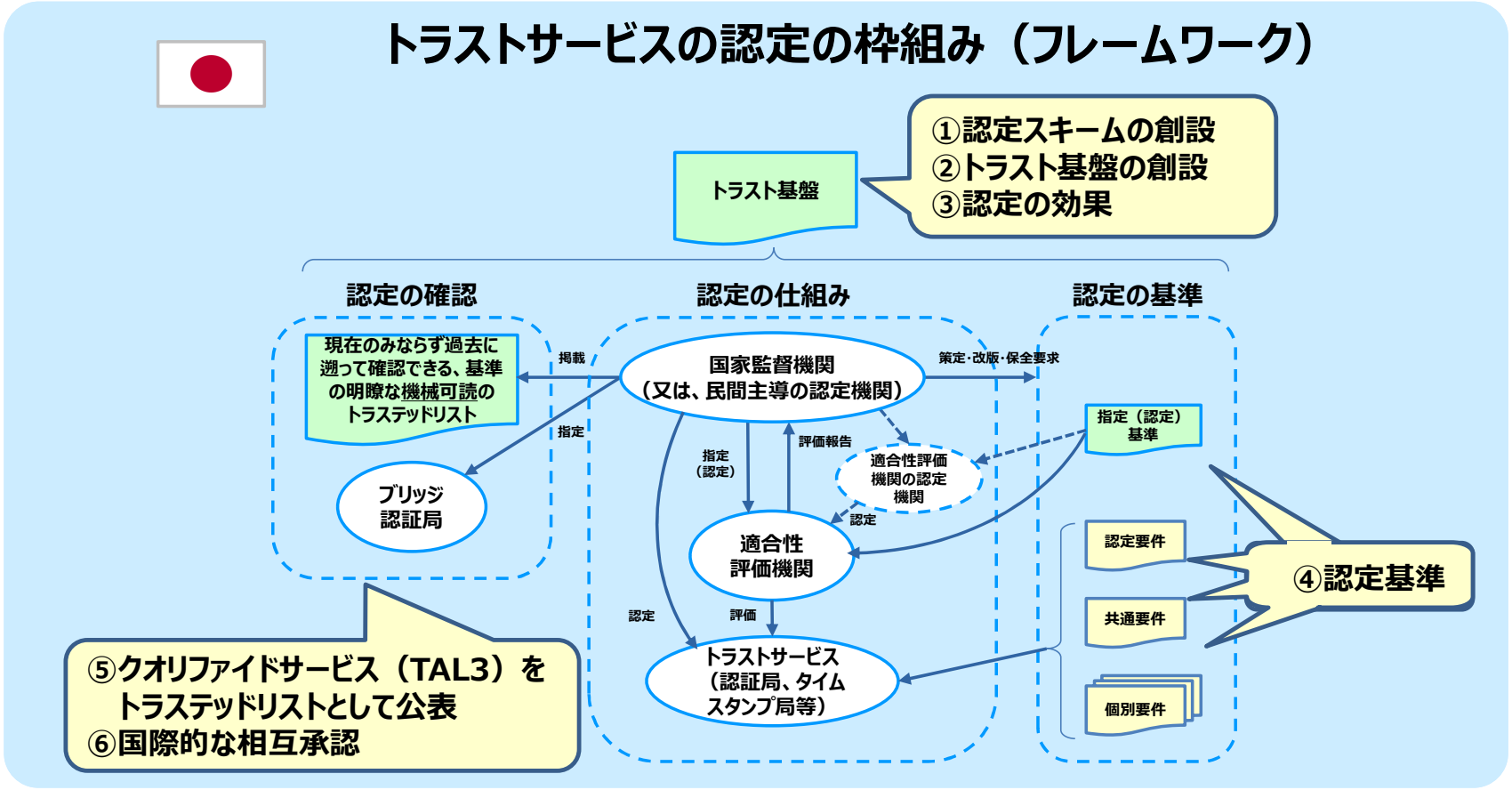
https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

日・EU・米国のトラストフレームワークの比較表

	EU	米国		日本（案）	備考
当局	欧州委員会	米国国土安全保障局	Federal CIO Council	デジタル庁	欧州も米国も政府機関
レギュレーション	eIDAS	FISMA NIST SP800-63	e-government Act Common Policy root CA	トラストポリシー	欧州は法で規定、米国は国立機関で規定
トラストフレームワークプロバイダ	EU 各加盟国	Kantara Initiative（KI）	Certipath Bridge CA	民間TFP（TAL3は国に限る）	欧州は各加盟国、米国は政府機関または民間団体
審査基準	ETSI,CEN 規格群 ・ETSI EN 319 401（一般ポリシ） ・ETSI EN 319 411-1（証明書発行者のポリシ） ・ETSI EN 319 421（タイムスタンプ局のポリシ） 等	KI Identity Assurance Framework（IAF）およびService Assessment Criteria（SAC）	CBCA CP	官民共同スキームによる策定（国が一定関与）	欧州は欧州委員会の指示の下、標準化団体で策定 米国は政府機関または民間団体で策定
認定審査機関	適合性評価機関（CAB）のAssessor	KI Accredited Assessors	Assessor	適合性評価機関等	欧州は認定機関から適合性評価機関としての認定を取得、米国はフレームワークによって異なるが自己宣言型も認められている
公表	トラステッドリスト	トラストレジストリ	FBCA	トラステッドリストおよびBCAのハイブリッド	欧州はトラステッドリスト、米国はFBCA及びリスト方式

トラストサービスの認定の枠組み

- TAL3に関するトラストサービスの国による認定の枠組みを検討すべきである。

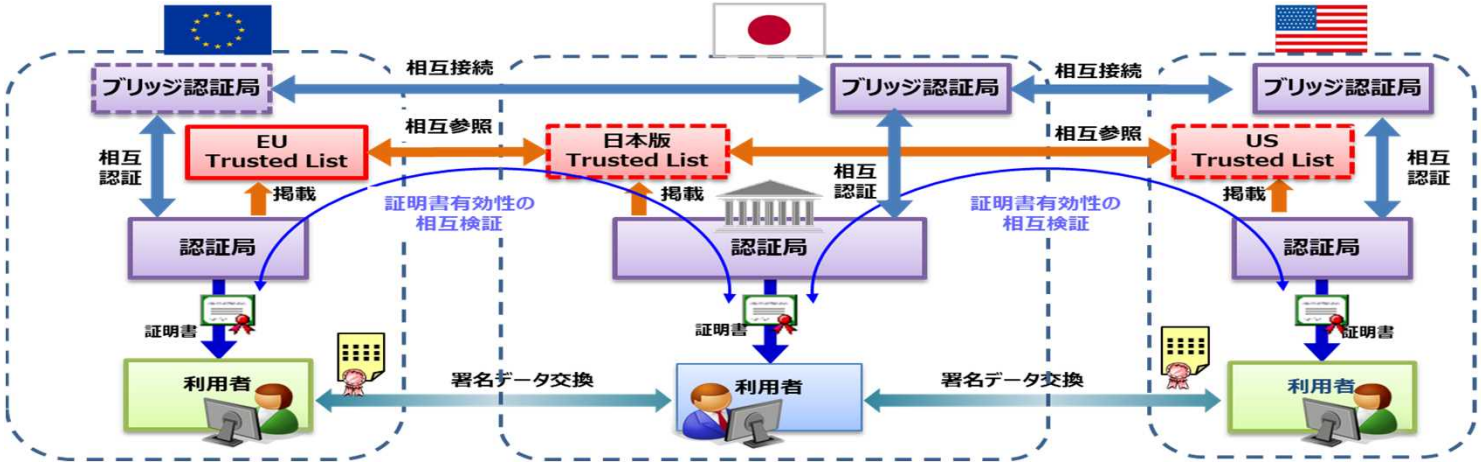


出典：第7回データ戦略タスクフォース資料1を参考に追記

トラストに関する国際的な相互承認

●国際間の利用者が相互に適格性を確認できるように、以下の項目の同等性などを検討し、相違点を補完することが必要である。

	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 トラスト基盤の創設 論点② 国（又は、民間機関）による認定フレームワークの創設 論点③ 認定の効果	・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（又は、民間機関）による認定フレームワークの確立 ・トラストサービスの効果の同等性
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



出典：第7回データ戦略タスクフォース資料1