

デジタル行財政会議

データ連携基盤への「トラスト」に 関する課題

2025年4月24日

一般社団法人デジタルトラスト協議会

- データスペース・分野間連携の取組みが進む中で、デジタルトラスト、デジタルトラスト・フレームワークを改めて定義し、同フレームワークの基礎基盤となるトラストサービス群も同様に整備されるべき。
- データスペース・分野間連携は海外との連携も当然視野に入っており、国際相互運用・認証が必要不可欠。
- 国際相互運用・認証には「技術的同等性」と共に「制度的同等性」も必要。
- 「技術」は民間で検討を進めている。「制度」は国でしか実施できない。未整備なままなので、国で強力に進めていただく必要がある。
- デジタルトラストは、既に後塵を拝している状況。着実に前に進めるべき状況にある（失敗を恐れて進めることができない状況の打破）。
- デジタルトラストは全体最適が必要（例、トラストサービス群に関する不統一な制度体系）。全体最適のためにも、定義されたデジタルトラストのもと関係者でOne Teamで対応すべき。
- OECDの下に設立されたInstitutional Arrangement for Partnership（IAP）への提言を行うべき。
- 紙からデジタルへの脱却で何を狙うのか戦略が見えづらい（効率化・更なるデータの活用、など）。紙からデータ化しただけでは効果は薄い。
海外の動向を見据えたうえで日本としてのデジタルトラスト戦略が必要。

- 各国データ連携に向けてルール作りを進めている。
データ連携はデータローカライゼーションに留まらないので、
我が国としては各国ルールと相互接続性の担保が必要となる。
- データの送信者・受信者の確からしさの確保の点では取り組みが進むが、データ中身（内容・コンテンツ）の利用権も併せ設定すべき、という点を我が国DFFTとして主張していくべきではないか。

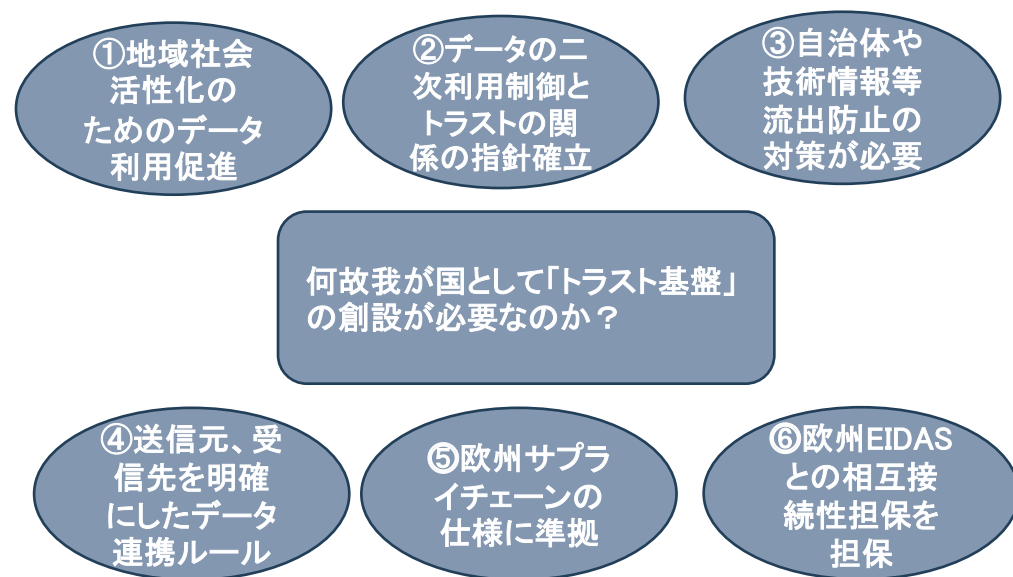
そのためには、送受の確からしさをアンカーにした仕掛け・仕組み作りが必要となる。

①地域社会活性化のためのデータ利用促進

地域社会活性化推進に対する課題として少子化や高齢化による担い手不足を克服するために自治体単独での解決から産業界をデジタルで連携し、データ利用により施策を進める。そのためには自治体と産業界とでデータ利用を安心・安全に連携可能な「地域トラスト基盤」の構築が必要

②データの二次利用制御とトラストの関係の指針確立

自治体と産業界とでデータ利用を相互に進めていくためには、極めての秘匿性の高いデータの連携を不正な二次ができないようにデータに鍵を掛けるなどの統一的な仕掛けが必要



③自治体や技術情報等流出防止の対策が必要

データのクライテリア（データの重要度区分）や知的財産権の観点から利用区分を定め、重要データの保全やデータ連携の自由度を促進するデータそのものへデータ保証をなすため、データへの信頼情報付与（トラスト付与）するルールが必要

④送信元、受信先を明確にしたデータ連携ルール

トラストアンカーを定めデータとの紐付けルールがデータ連携には必要。電子署名・タイムスタンプ・eシール・eデリバリなどデータの関係性（用途）やデータへトラスト付与の包括的（統一的）な根拠性を確立

⑤欧州DSA/英国OSAなどやeIDASとの相互接続性担保

欧州DSA（Digital Services Act）や英国OSA（**Online Safety Act**）などを参照し、データ活用のルールを我が国でも定める。その上で、データ信頼性を確保のため、欧州トラストルールの一つであるeIDASとも我が国のトラスト基盤で連携して諸外国とも相互接続性を担保

⑥欧州サプライチェーンの仕様を考慮

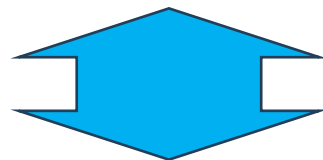
欧州で産業データ連携基盤のルール化を進めているGAIA-X・CATENA-X等ともデータ連携が必要となることが想定される。どの領域で欧州仕様を考慮するのか検討要。その上で、我が国のトラスト基盤連携の形式の決定が必要

1. データ連携システムにて検討されている越境データやCross Sectorでのデータ利用が

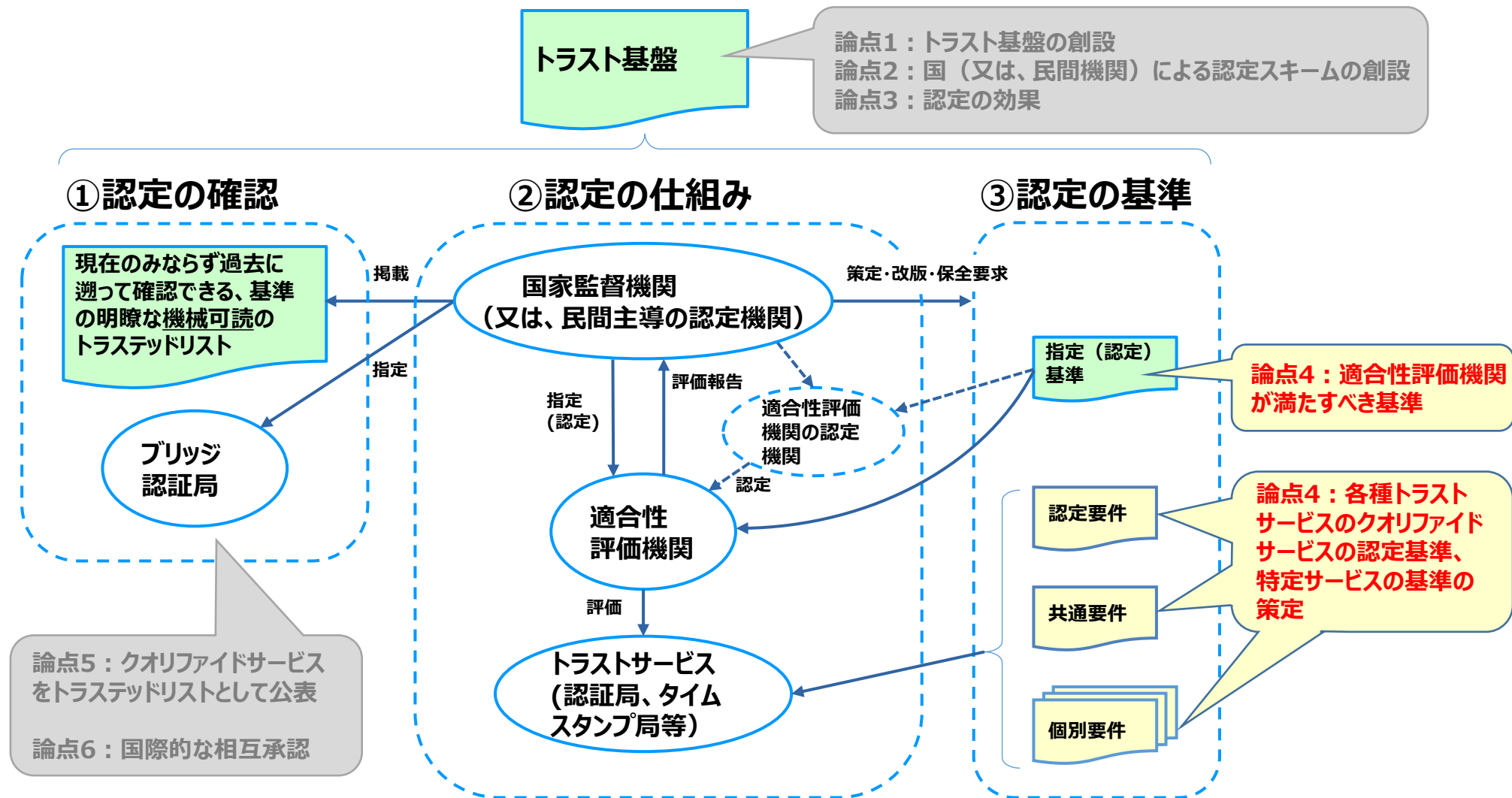
廻っていくのか各々Sectorでのデータの位置づけ: クライテリアを整備する

2. データ連携システムにおいてデータ整備をもとに、各Sectorで最重要・重要となるデータへのトラストアンカーの紐付け方を検討

3. 上記方針をもとにデータ連携基盤とトラスト基盤の連携実装推進



トラストフレームワーク整備より注出される課題に対し
「制度・ガイドライン」、「認定制度」を検討



- トラストフレームワークについては、欧州（eIDAS2.0 eIDAS2.0）のように、データ連携基盤の各コンポーネントに対応したフレームワークが検討/整備されている国もあれば、いない国もある。
 - シンガポールはガイドラインという形での推進であり、現時点でトラストフレームワークの制度化が検討されているように見えない
 - UKではWallet やVC の枠組みが新たにトラストフレームワークに追加されようとしている
 - カナダはWallet もVC もPCTF に入っているが、未だトラステッドリストに登録されていない
- 制度の運営についても、政府による運営、官民NPOによる運営等ある。
- UKのDIAFは制度の検討から、リリース、見直し、改定のサイクルが非常に速い。
- 技術標準としては、EUの標準が直接参照されていない。
- 一方でデータ連携に係るプロジェクトには、各国が参加している。

	シンガポール	カナダ	UK	米国
法人のID	• CorpPass (GovTech)	• PCTF (Verified Organization) (DIACC)	• Digital Identity and Attribute Framework(DCMS)	• Login.gov(GSA)
Wallet	• SingPass(予定) (GovTech)	• PCTF (Digital Wallet) (DIACC)	• Digital Identity and Attribute Framework(DCMS)	• NIST SP 800-63-4 2ndPD (NIST) • mDL(TSA, AAMVA, DMV)
VC	• SingPass(予定) (GovTech)	• PCTF(Credentials) (DIACC)	• Digital Identity and Attribute Framework(DCMS)	• NIST SP 800-63-4 2ndPD • mDL(TSA, AAMVA, DMV)
eSeal	–	• PCTF (Credential) (DIACC)	• UK eIDAS(DCMS/ICO)	–
Trusted List	• Accredited CA (IMDA)	• Trusted List (HTML)(DIACC)	• UK DIATF Certified Service (CSV) (DCMS)	• Trust Status List (Kantara) • FBCA (GSA)
Cloud	• サイバーセキュリティ法改正案 (Ministry of Communications and Information) • 基盤のデジタルインフラストラクチャーサービス	• Bill26 (重要サイバースystem保護法案) (Public Safety Canada) • データレジデンシー (Revenue Agency) • アプリケーションホスティング戦略(Treasury)	• Cyber Security and Resilience Bill(DSIT)	• Data Clean Room(AWS, Azure, Google Cloud) • Cloud Act(DoJ)
Data	• Free Trade Zone (Data Sharing) 規則(税関)	• データ戦略2023-2026(Treasury)	• Data Usage and Access Bill(DSIT) • Smart Data Scheme(DSIT) • National Data Strategy(DSIT)	• EO14117(DoJ) • 州レベルでの取り組み
AI	• 国家AI戦略(National AI Office) • モデルAIガバナンスフレームワーク(IMDA)	• 人口知能・データ法(ISED)	• National Data Library and AI Action Plan(DSIT)	• 州レベルでの取り組み
データ連携基盤に関連するプロジェクト、活動	• SGTRaDex • DCP (Data Collaboration Platform) • TradeTrust	• 国家データガバナンスフレームワーク • ODX (オープンデータエクスチェンジ) • LODÉ	• DSI (Data Sharing Infrastructure) • DINI • IB1(Perseus)	• DirecTrust • Li-Bridge
	• Global Battery Alliance等			

データスペース・分野間連携の取組みが進む中で、デジタルトラストは必要不可欠とされる。

現在の日本においてデジタルトラストは未定義であり、文脈で異なることも少なくない。

以下を定義して、関係者間において共通認識とする必要がある。

- ・ デジタルトラスト
- ・ デジタルトラスト・フレームワーク

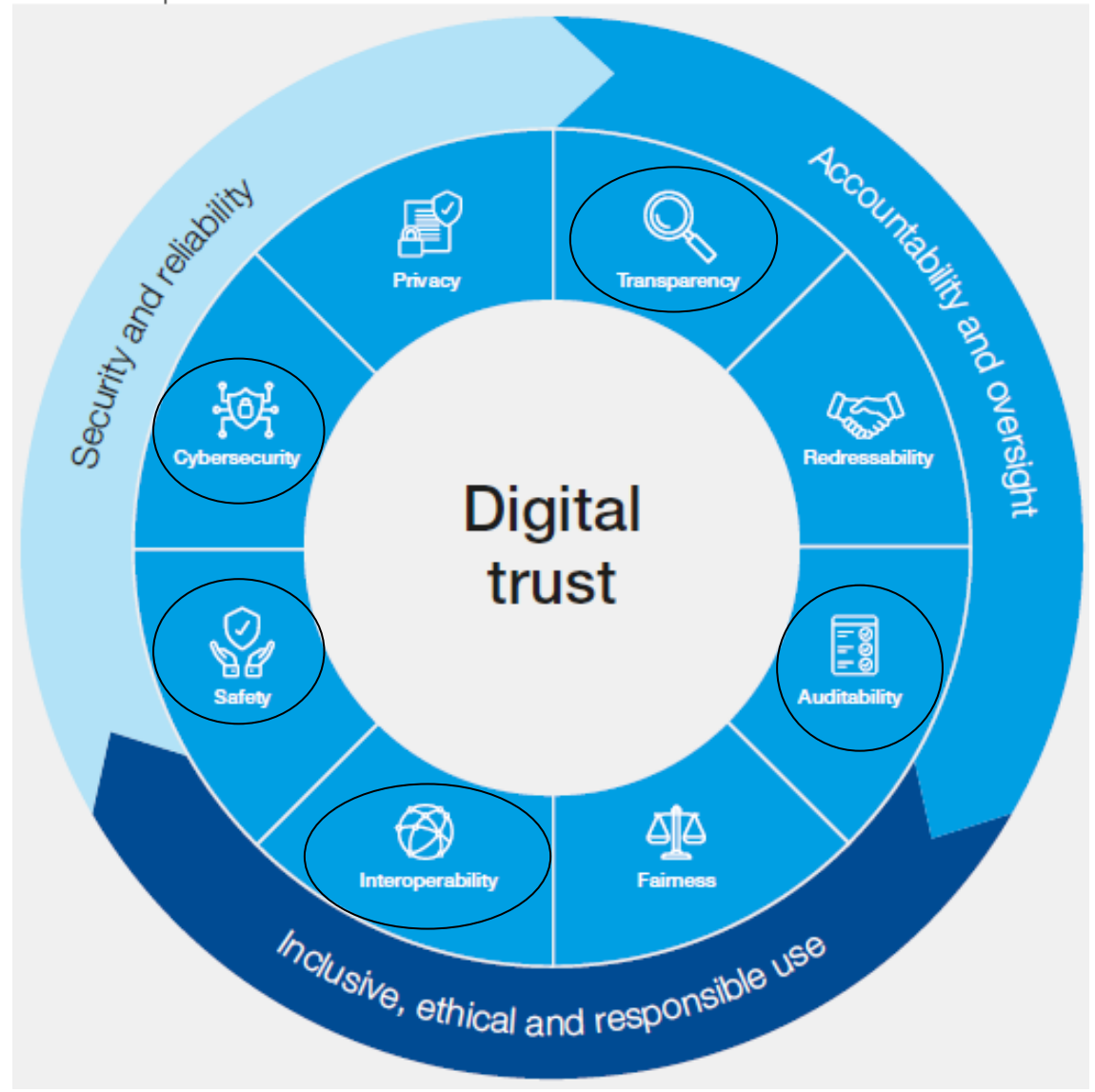
参考情報として以下が挙げられる。

- ・ [世界経済フォーラム 2022 World Economic Forum Earning Digital Trust: Decision-Making for Trustworthy Technologies](#)
→ [Earning Digital Trust : Decision-Making for Trustworthy Technologies](#)
- ・ 右図は上記資料から引用（丸囲みは本作成者にて実施）

以下から引用

[World Economic Forum 「Earning Digital Trust: Decision-Making for Trustworthy Technologies」](#)
→ [Earning Digital Trust: Decision-Making for Trustworthy Technologies](#)

FIGURE 1 | Digital trust framework



定義：デジタルトラスト

Digital trust is individuals' expectation that digital technologies and services - and the organizations providing them - will protect all stakeholders' interests and uphold societal expectations and values.

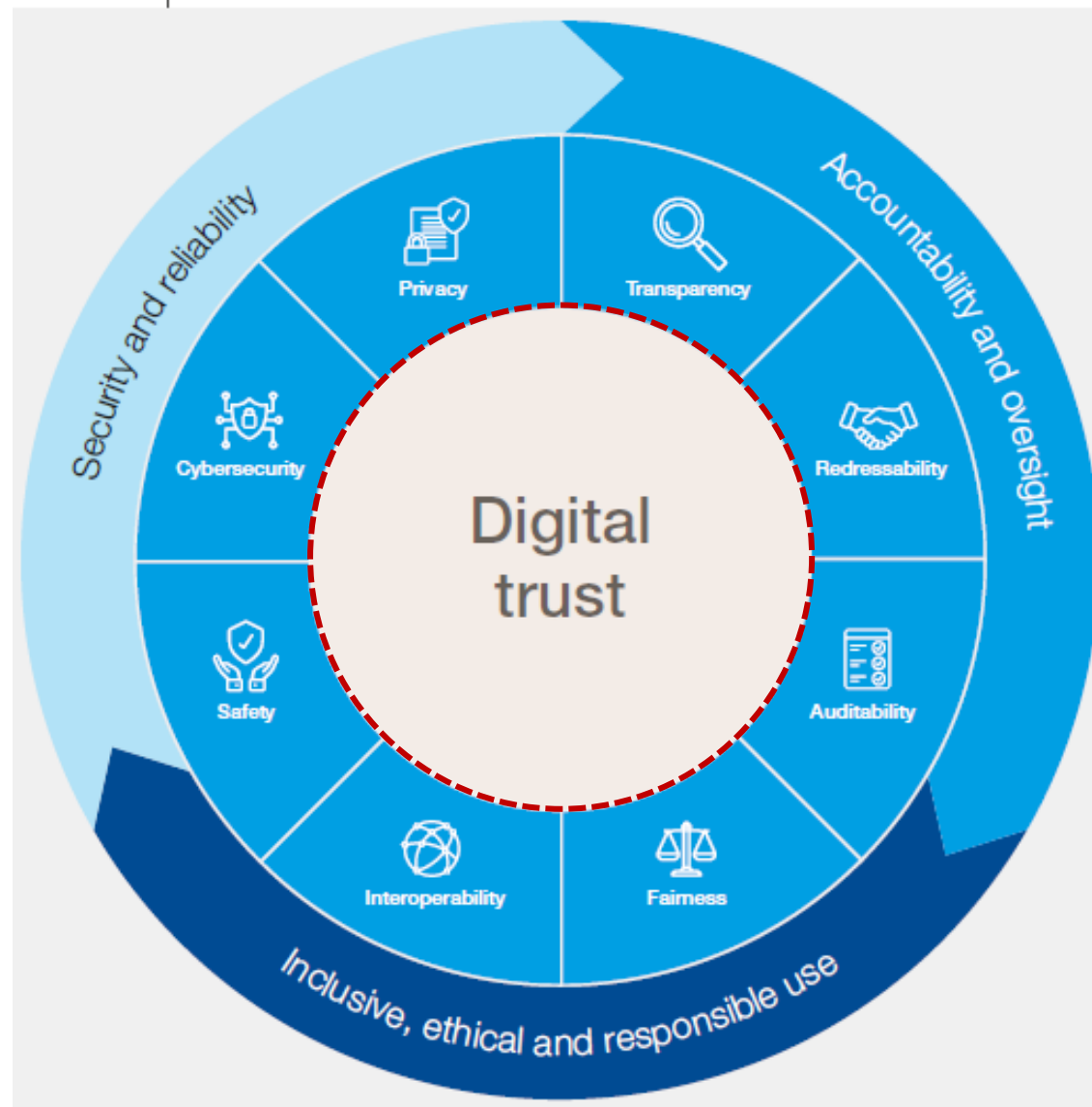
デジタルトラストとは、デジタルテクノロジーやサービスを提供する組織が、すべてのステークホルダーの利益を守り、社会の期待や価値を守るであろうという個人（組織）の期待である。（仮訳）

以下から引用

[World Economic Forum「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#)

→[Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

FIGURE 1 | Digital trust framework



Goals: Considerations that motivate or can be achieved by actions or decisions (i.e. dimensions).

ゴール： 行動や決定を動機づける、または行動や決定により達成できる考慮事項

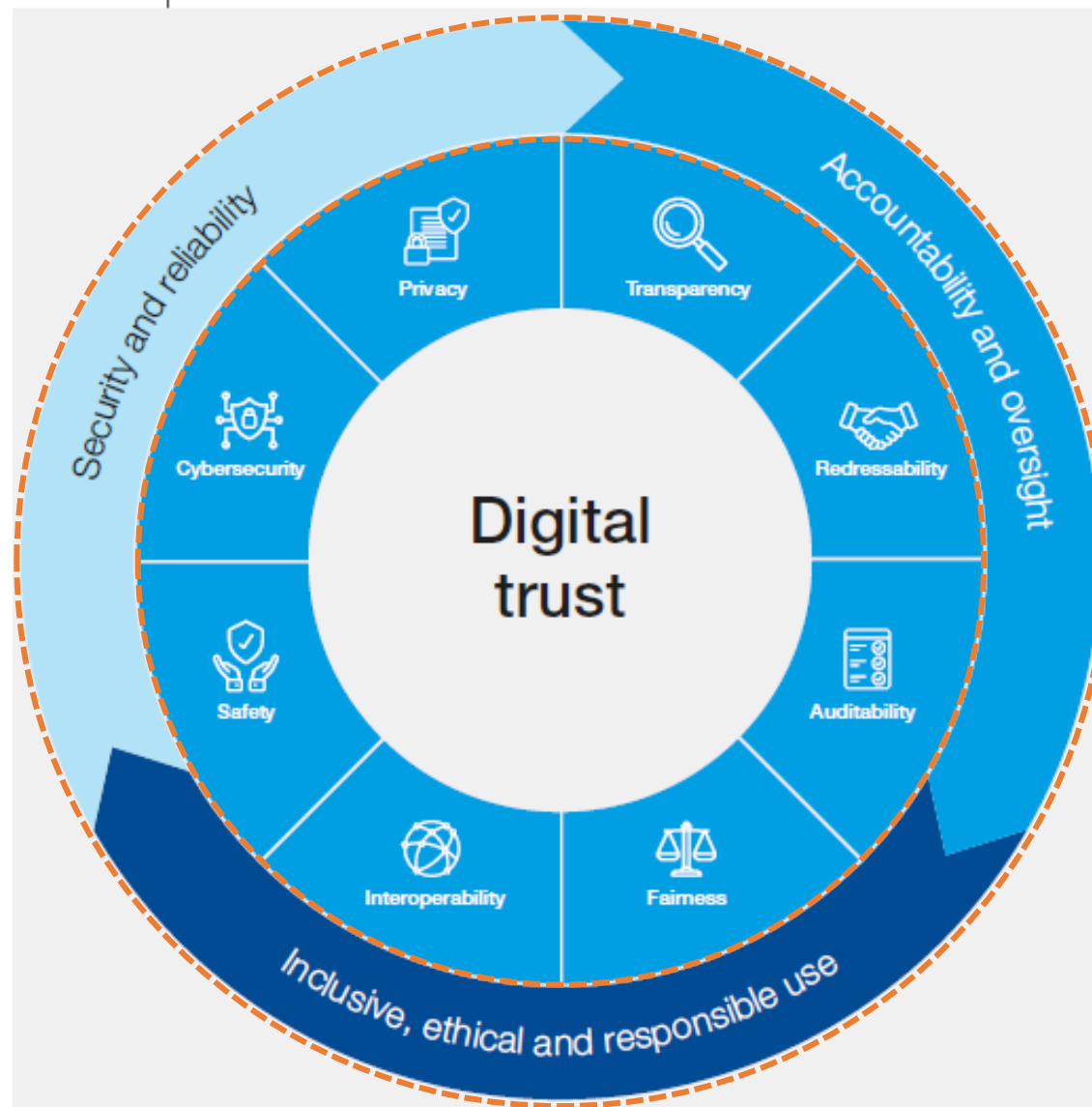
- Security and reliability (セキュリティと信頼性)
- Accountability and oversight (説明責任と監督)
- Inclusive, ethical and responsible use (包括的、倫理的かつ責任ある利用)

(以上、仮訳)

以下から引用

[World Economic Forum「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#)
→[Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

FIGURE 1 | Digital trust framework



Dimension : the framework identifies eight crucial dimensions of decisionmaking :

領域：8つの重要な領域を特定

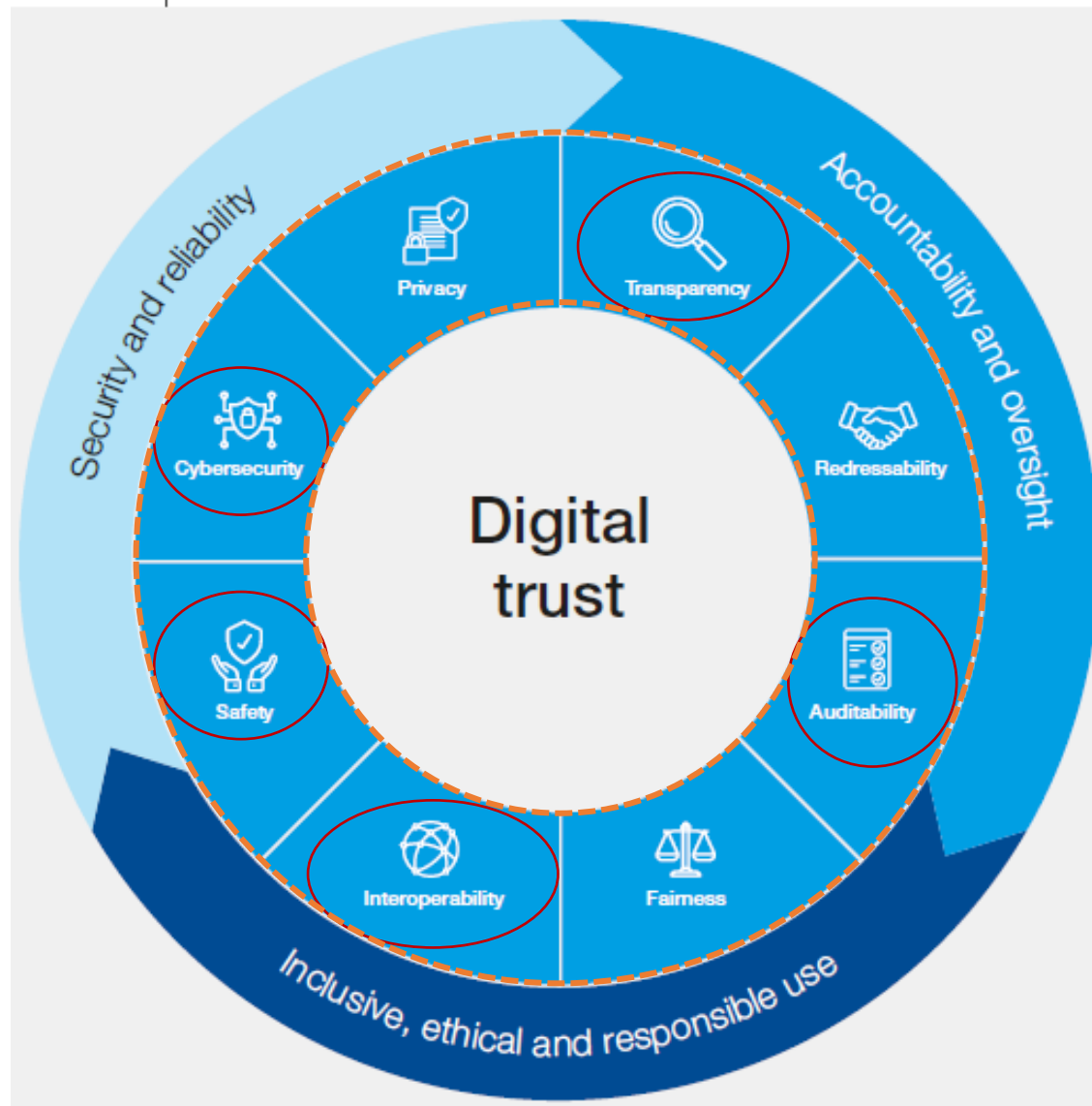
- Cybersecurity (サイバーセキュリティ)
- Safety (安全性)
- Transparency (透明性)
- Interoperability (相互運用性)
- Auditability (監査可能性)
- Redressability (救済可能性)
- Fairness (公平性)
- Privacy (プライバシー)

特に5つの領域について後段で説明。

以下から引用

[World Economic Forum「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#) → [Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

FIGURE 1 | Digital trust framework



効果的なサイバーセキュリティは、デジタルプロセスとシステムへの不正アクセスや損害のリスクを軽減し回復力を確保する。

データには陥穽が存在することから、重要な情報の改ざんや消失、物理的な破損を防ぎ、安全に情報を取り扱うために意識すべき要素。テクノロジーの意図しない使用（悪用）のリスクをも軽減する。

安全・安心・快速なデータ流通・活用のために、セキュリティ7要素の確保が必要不可欠。

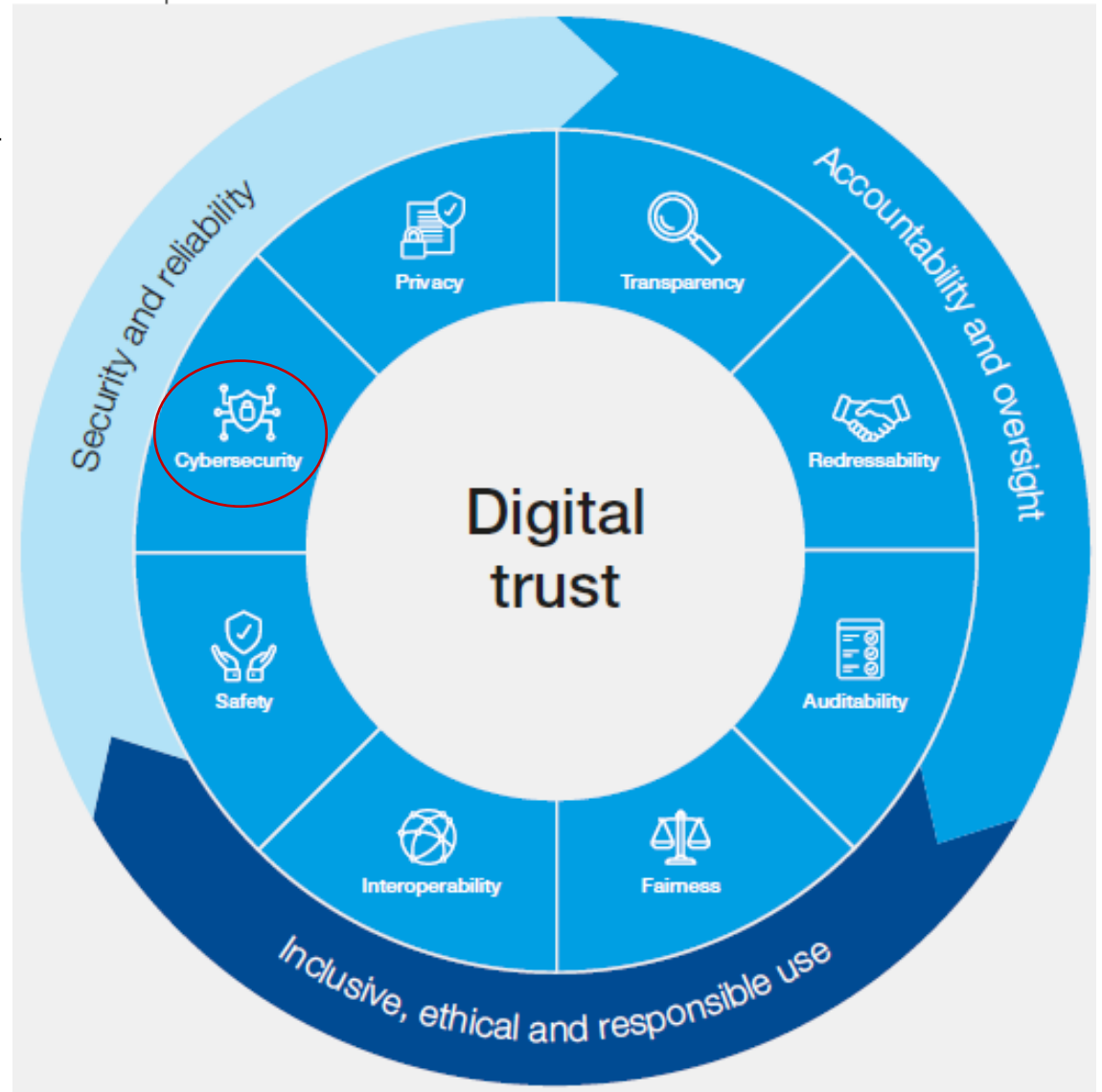
- 機密性 (confidentiality)
- 完全性 (integrity)
- 可用性 (availability)
- 真正性 (authenticity)
- 信頼性 (reliability)
- 責任追跡性 (Accountability)
- 否認防止 (non-repudiation)

トラストサービス群により、上記要素の確保が可能。

以下から引用

[World Economic Forum 「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#)
→[Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

FIGURE 1 | Digital trust framework



安全性とは、テクノロジーの使用やデータ処理によって、人々や社会に危害（精神的、身体的、心理的など）が加えられるのを防ぐ努力を意味する。

安全・安心・快速なデータ流通・活用のために、安全性確保からもデジタルトラストが必要不可欠

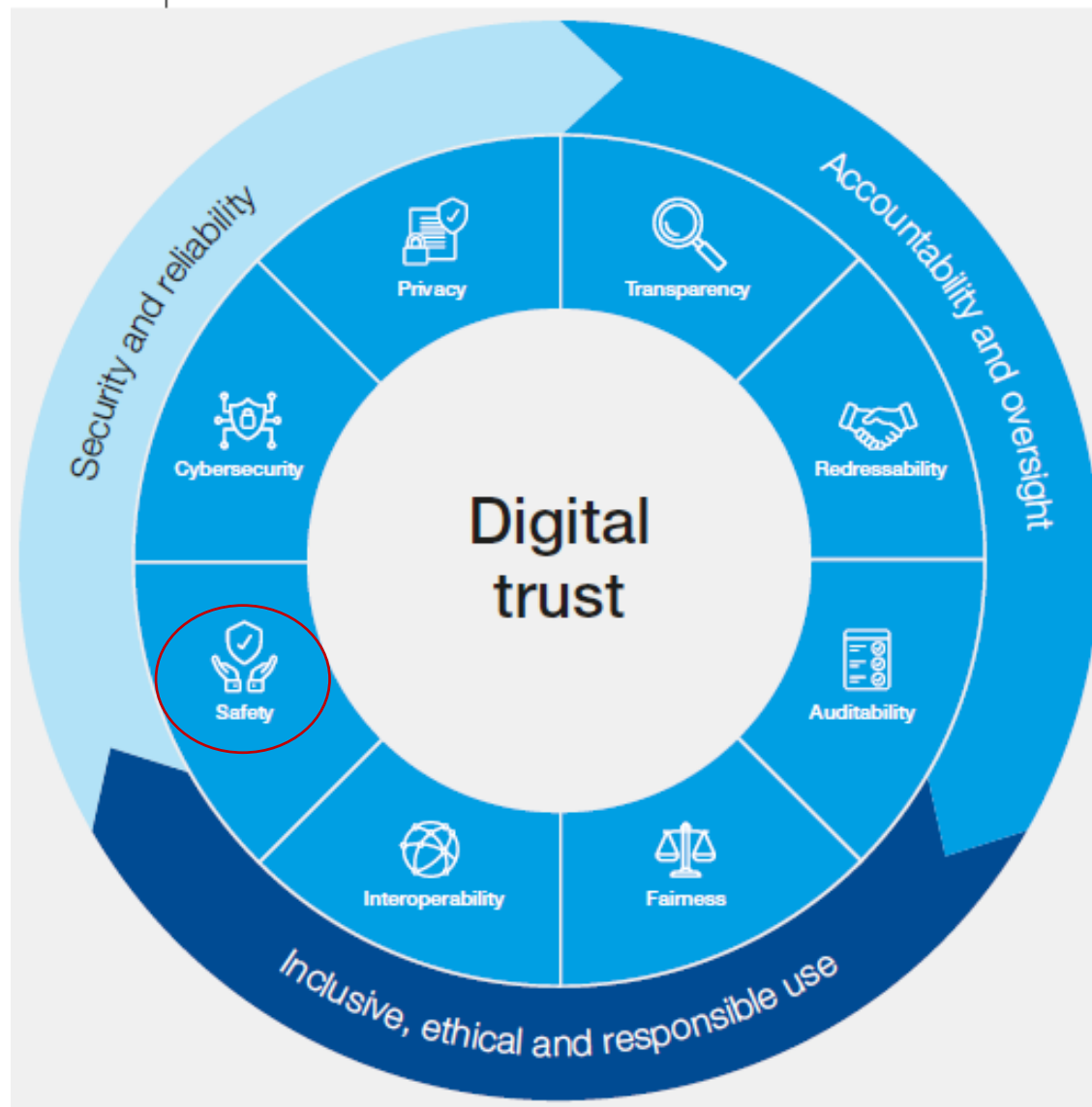
トラストサービス群により、上記要素の確保が可能

- 認証の安全性
（身元確認レベル：IAL、当人認証レベル：AAL、など）
- 経路の安全性
（Webサーバ証明書、etc）
- 授受の安全性
（eデリバリー、etc）

以下から引用

[World Economic Forum「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#)
→[Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

FIGURE 1 | Digital trust framework

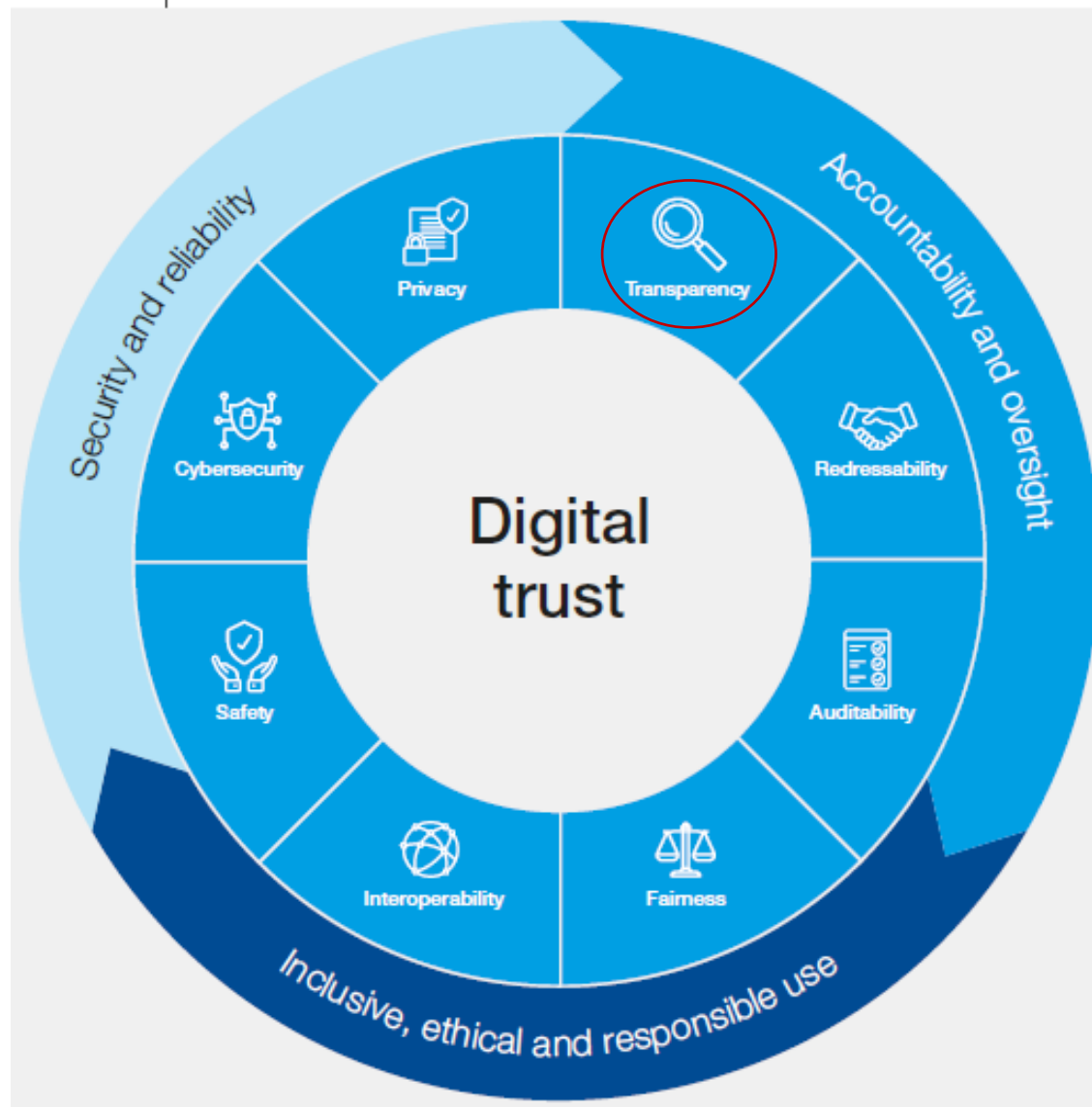


透明性を確保するためには、デジタルの運用と利用について、正直かつ明確にする必要がある。組織のデジタル・プロセスを可視化することで、組織とその利害関係者との間の情報の非対称性を低減し、同時に、組織が個人の利益のために行動するだけでなく、その行動を組織内外の人々に知らせ、理解させる意図があることを個人に示すことが可能となる。

安全・安心・快速なデータ流通・活用における透明性確保の観点から、「運用・利用・過程の可視化」が必要。

トラストサービスも利用することで「運用・利用・過程の可視化」を促進可能。

FIGURE 1 | Digital trust framework

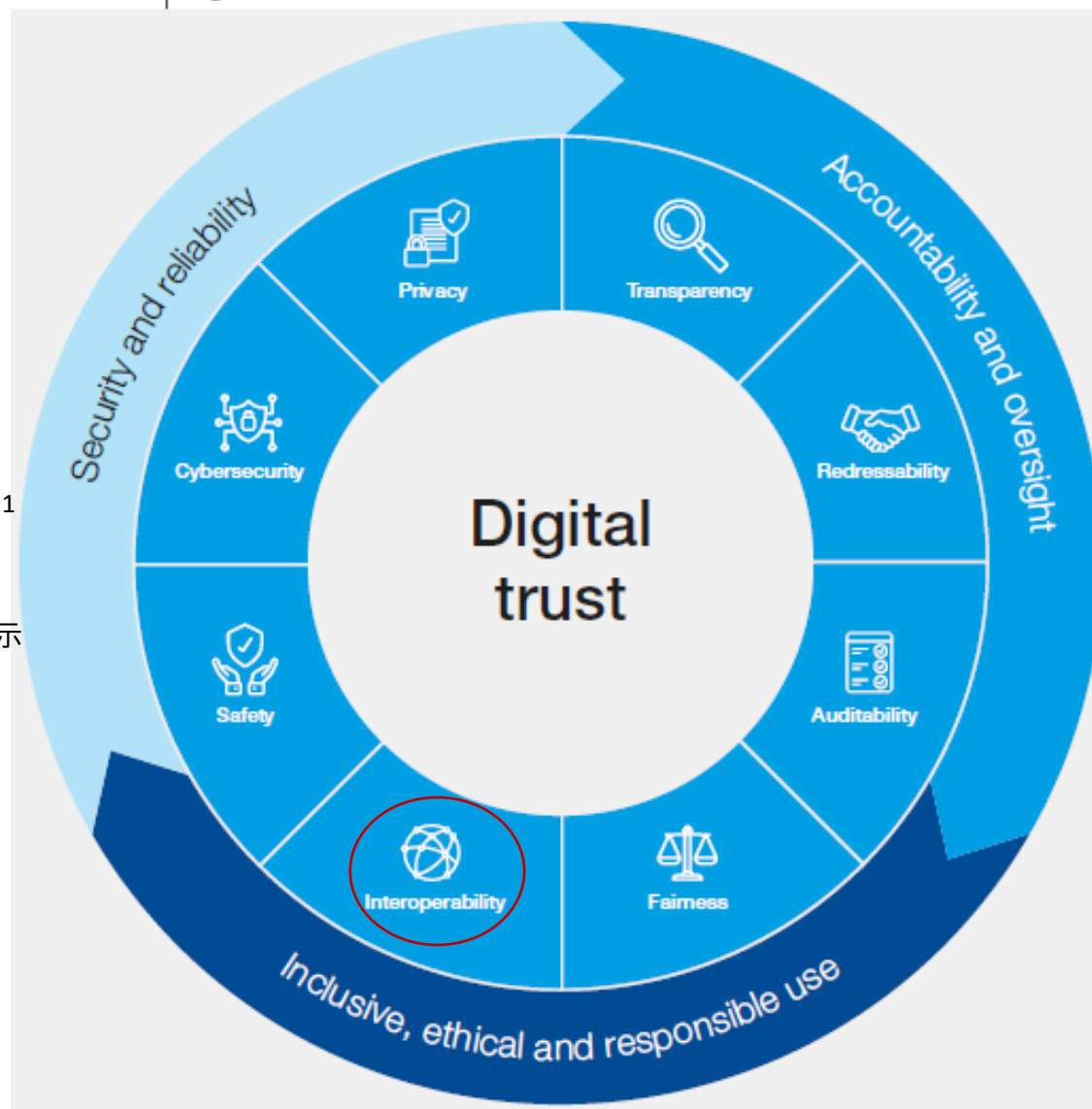


以下から引用

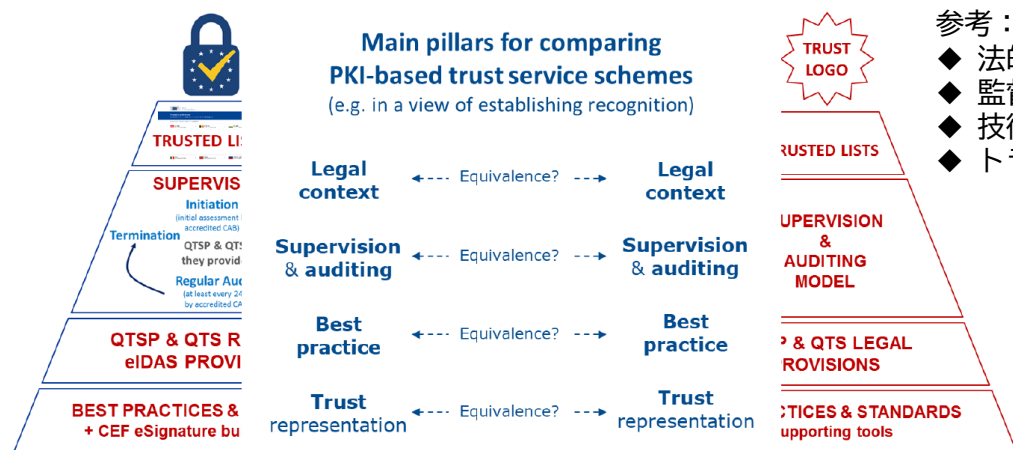
[World Economic Forum 「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#)
→[Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

相互運用性とは、情報システムが過度の負担や制限を受けることなく相互利用のために接続し、情報を交換する能力のこと。統一された技術への期待と基準がカギとなる。業界固有の技術標準は、幅広い経済成長と社会的利益をもたらすことが可能となる。デジタルトラストを支えるトラストサービスは、国内はもとより、ワールドワイドでDFFTを実現するためにも「技術的観点」だけでなく「制度的観点」で同等性が必要。また、トラストサービスは適合性評価、トラストアンカーを機械的に検証可能とする仕組みも必要。

FIGURE 1 | Digital trust framework



Methodology



参考：ETSI TR 103 684 V1.1.1

- ◆ 法的同等性
- ◆ 監督・監査制度
- ◆ 技術基準
- ◆ トラストアンカーの開示

以下から引用

[World Economic Forum 「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#)
→[Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

監査可能性とは、組織と第三者の両方が、テクノロジー、データ処理、ガバナンスプロセスの活動と結果をレビューし、確認できる能力のことである。監査可能性は、組織のコミットメントをチェックする役割を果たし、コミットメントに従うという組織の意思を示す。

ログデータだけでは、改ざんなどデジタル陥穽が存在する。

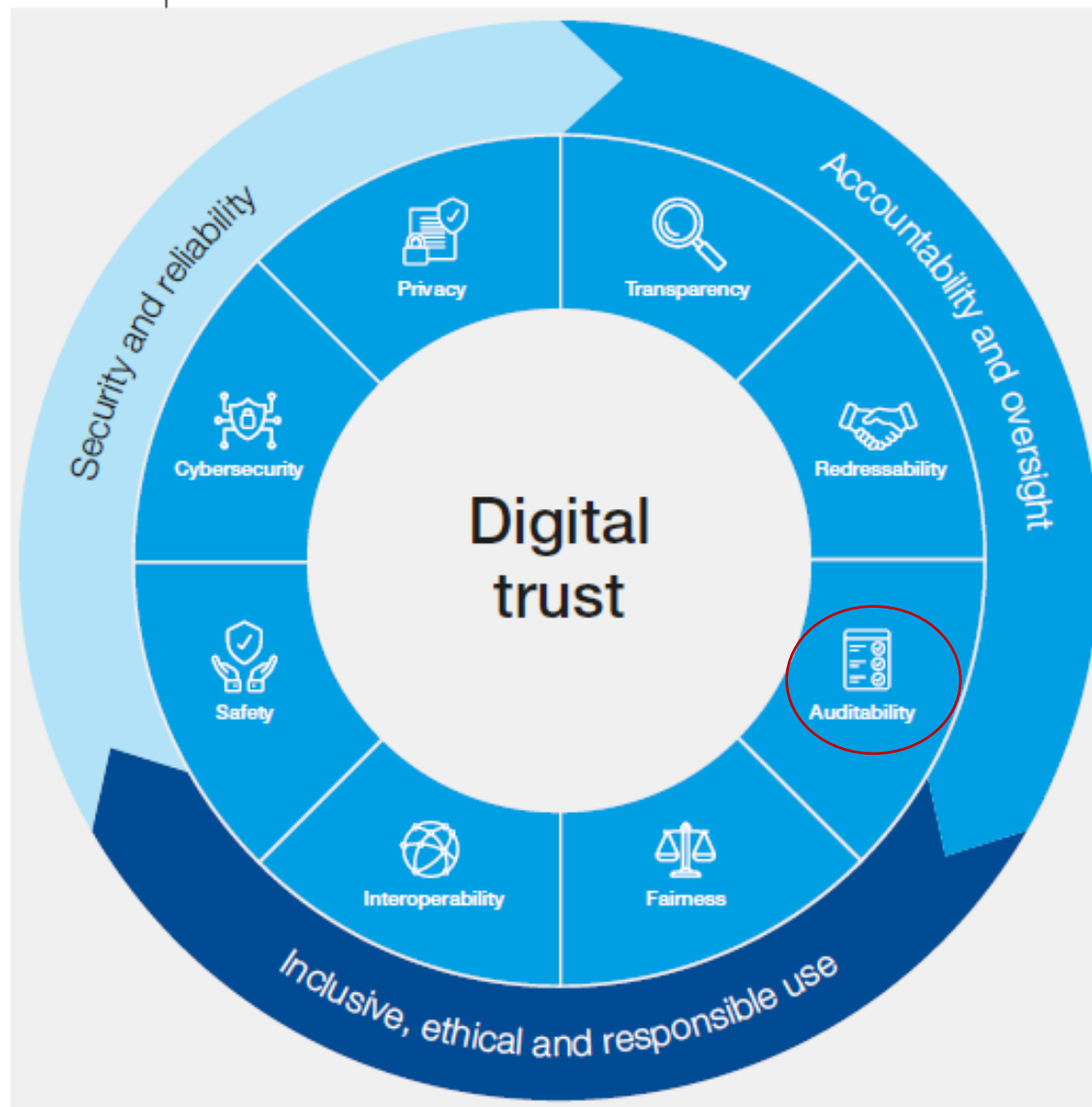
トラストサービスが最大限活用される場面であり、改ざん検知を含め必要不可欠と想定。

- 電子署名：本人の意思確認
- eシール：発出元証明
- タイムスタンプ：時刻存在証明
- etc

以下から引用

[World Economic Forum「Earning Digital Trust:Decision-Making for Trustworthy Technologies」](#)
→[Earning Digital Trust:Decision-Making for Trustworthy Technologies](#)

FIGURE 1 | Digital trust framework





JDTF
JAPAN DIGITAL TRUST FORUM