1.検討の背景

○COVID-19を契機に社会全体のデジタルトランスフォーメーション（DX）が加速。**サイバーとフィジカルが融合**していく中で、様々な社会活動が行われる**「デジタル社会」に移行。**

○しかしながら、**様々な課題が顕在化。“一握りの巨大企業への依存”**でも、**“監視社会”**でもない**第三の道を模索**することが必要。

○こうした中、デジタル社会の基盤として発展してきた**インターネットとウェブ**では、データの受け渡しのプロトコルは決められているが、**Identity管理も含め、データ・マネジメントの多くはプラットフォーム事業者など各サービスに依存。**サイロ化され、外部からの検証可能性が低く、「信じるほかない」状況。

○2020年6月の「デジタル市場競争に係る中期展望レポート」の提言を受け、**DFFTの具現化**も視野に、2020年10月に**「Trusted Web推進協議会」を発足。**これまでの検討結果を踏まえ、今後、**内外の様々な関係者と協力・連携していくための叩き台**として本ペーパーをとりまとめ。

2.直面している課題とその原因

○**インターネットとウェブ**は、**グローバルに共通な通信基盤**として発展して、**広く情報へのアクセスを可能とし**、その上で**様々なサービスが創出**。

○しかしながら、デジタル社会における様々な**社会活動において求められる責任関係**やそれによってもたらされる**安心を体現する仕組みが不十分**な状況であり、ユーザーが**信頼の多くをプラットフォーム事業者などに依拠**する中で、**その歪みが様々なペインポイント**をもたらしている。

ペインポイントの例

○フェイクニュースや虚偽の機器制御データなど、**流れるデータへの懸念**
○生体情報も含めたデータの集約・統合による**プライバシーリスク**
○COVID-19等を契機に議論されている**プライバシーと公益のバランス**

○**サイロ化された産業データ**の未活用
○**勝者総取り**等によるエコシステムのサステナビリティへの懸念
○社会活動を行う上での社会規範による**ガバナンスの機能不全**

原因

○　やり取りされるデータが信頼できるか
○　データをやり取りする相手方を信頼できるか
○　相手方における提供したデータの取扱いを信頼できるか
について、懸念がある状況

インターネットとウェブがもたらしてきた**ベネフィットを活かしつつ**、**一定のガバナンスや運用面での仕組みとそれを可能にする機能をその上に付加**していくことが必要。
→　カギとなるのが“Trust”

3.Trusted Webが目指すべき方向性

目指すべき方向性

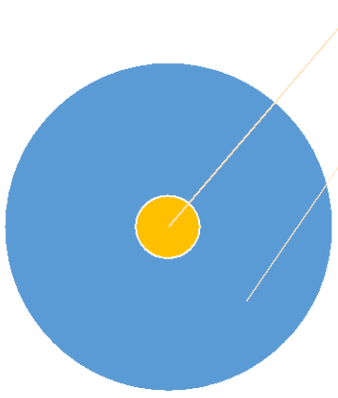
○**目的**：デジタル社会における様々な**社会活動に対応するTrustの仕組み**をつくり、**多様な主体による新しい価値の創出**を実現。

○**Trustの仕組み**：　**特定サービスに依存せず**、
- **相手に開示するデータのコントロール**を可能とし、
- データのやりとりにおける**合意形成の仕組みを取り入れつつ、**
- **検証（Verify）できる領域を拡大**し、これまで**事実を確認せずに信頼していた領域を縮小**することにより、**Trust**（相手が期待したとおりに振る舞うと信じる度合い）**を高めていく。**

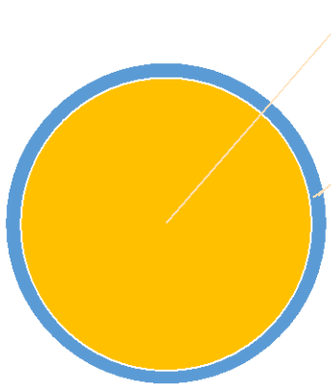
○**アプローチ**：インターネットとウェブのよさを活かし、その上に重ね合わせる**オーバーレイのアプローチ**

***Trust:　事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い**

仕組みによりVerifiable（検証可能）な部分が変わる



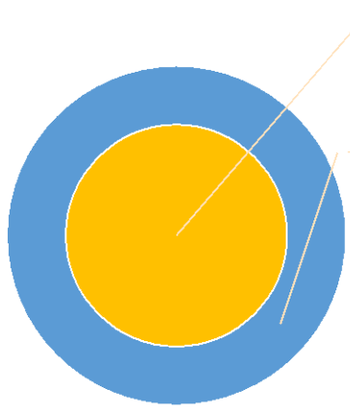
現在のインターネット：
検証できる部分が小さく、相手を大きく信頼しないと意思決定できない。



ブロックチェーンなど：
検証できる部分が大きく、相手を信頼する要素が少ない。
（暗号アルゴリズムの信頼性など、信頼するところはある）

*ただし、この方式はトレードオフが発生するため、全ての領域でできるわけではない。

Don't trust, Verify



目指すところ：
ある程度検証できる部分を担保しながら、継続性や、相互運用性、更改容易性を充足する仕組み
→「Trust」を高める

4.Trusted Webのアーキテクチャーを構成する主な4つの機能とガバナンス

デジタルアイデンティティの管理・検証

①Identifier(識別子)管理機能

✓識別子の管理

ユーザーが識別子を自ら発行し、それを**様々な属性（Identity）と紐付け**ることができる。

→ これまでは**サービス毎の識別子**でロックインされ、**自らの属性**（年齢、連絡先等）**が紐づけられて管理されていた**が、**自らが属性の開示範囲をコントロール**し、**個人の特定を回避**することが可能。

②Trustable Communication機能

✓信頼できる属性の管理・検証

第三者によるお墨付きやレビュー等を受けた自らの属性（卒業証明や検査結果、信頼度等）**を自分で管理**し、**相手に対し必要な範囲で開示**、**相手**は発行者等に**都度照会することなく、属性を検証**できる。

→ **データの出し手の確からしさで判断**することで、**メッセージの内容の正しさを推定**することができる。

デジタル上での意思の反映・検証

③Dynamic Consent機能

✓動的な合意形成

データのやりとりをするに、双方で**様々な条件設定をして合意を行うプロセスと結果を管理**することができる。

→ これにより、**データのやりとりにおける条件をコントロール**。画一的な規約ではなく、**双方の意思を反映し、齟齬があれば動的に修正**できる。

④Trace機能

✓条件履行検証

合意の際の選択により、合意形成のプロセスや合意の履行を**モニタリング**し、**適正であるか検証**することができる。

→ **データ移転後に完全にその利用がブラックボックスになることについての懸念を払拭**するもの。

ガバナンス

○**マルチステークホルダーによるガバナンス**
（Trustを裏付ける経路や連鎖を分散協業して支える、ルールや運用について合意形成）

○**政府の役割**（**トラストアンカー**の一翼を担う、**支える制度整備・運用**）

○**透明性の確保**（様々なステーホルダーが検証して牽制）

○エコシステムを**持続的にするためのインセンティブ設計**
（貢献するエンジニアやTrustを支える機関等の公共的役割に対する設計）

4

Trusted Webの今後の活動（今年度）

○3月に基本的構想であるホワイトペーパー1.0公表。
○2021年度は、構想具体化に向け、①プロトタイプ、②ユースケースベースでの検証、③潜在的な産業界ニーズの見える化を実施。その上で、④ホワイトペーパーを改定→国際標準化へ。

シンプルなユースケースを念頭にミニマムな機能の書き出し

①プロトタイプ開発 ⇔ **②ユースケースベースでの検証**

- 「個人」の属性情報のやりとり
- 「法人」の行政庁との情報のやりとり
- 「モノ」の付加価値の訴求につながる情報のやりとり

機能・課題の洗い出し
標準化・普及への布石

③潜在的な産業界ニーズの見える化

④ホワイトペーパーの改定

⑤国際標準化に向けた基礎固め（W3Cなど）

＜関連する動き＞
○EUでは、本年6月、分散型で自らの属性データを管理するDigital ID Walletを域内各国政府等において導入する法案を発表。認証のためのお墨付きのついた属性情報の利用を含め、Trusted Webと類似した発想（2030年までに広く普及を目標）。さらに大規模プラットフォーム事業者などに、Walletの受入れを義務付け。2022年9月までに技術仕様を定めたToolboxを策定予定。
○同じくEUにおいて、BtoBのデータのやりとりを中心に、GAIA-Xの中でデータのコントロールなどの仕組みの検討あり。