

White paper

Trustable Internet

～ 人々が安心して利用できる信頼できるインターネットの実現に向けて ～

V1.0

2022 年 10 月 13 日

TIAL : Trusted Internet Architecture Lab.

目次

概要（Executive Summary）	3
前提としている対象読者層と前提知識.....	4
1 背景.....	4
1.1 データ社会の進展とその信頼性	4
1.2 ユースケースと課題	5
1.3 要件分析.....	5
2 Trustable Internet とは	7
2.1 Trustable Internet アーキテクチャ	7
2.2 Endorsement Layer	7
3 Trustable Internet の実現アプローチ	8
3.1 信頼できるデータ社会を目指すグローバルな動き	8
3.2 データに確からしさの根拠を付与するエンドースメントの仕組み	9
3.3 フィジカル空間を反映する エンドースメントグラフ.....	11
3.4 閲覧者の確からしさの判断支援	13
3.5 全体動作.....	14
4 実現にむけた今後の取り組み.....	16
5 参考文献.....	17

概要 (EXECUTIVE SUMMARY)

インターネットは社会・経済活動において欠かせないものになっている。それを活用するスマートフォンや SNS の普及により、個人や組織などが、いつでもどこでも世界にデータを発信し、閲覧できるようになった。これらのデータの中には、誤った内容を含む、いわゆる偽情報である場合もあり、これらによる社会問題も実際に起きている。インターネット上のデータにそのような疑いがあったとしても、データの確からしさ（正しさの程度）を確認できないことが多い。そのような中で、その確からしさの判断を閲覧者自身で下さざるを得ないのが現状であり、これらのデータに基づいて行われる意思決定が的確でなくなる可能性がある。

従来、データの確からしさを確保する手法としては、文書の承認管理システムや配送荷物の追跡システムのように個別システム毎に証跡を記録する機能を組み込む方法や、インターネット以外の方法で事前にデータ送受信者の間で信頼を構築する方法が取られてきた。しかし、膨大なデータが存在するインターネット上でその確からしさを確認できる汎用的な方法は存在せず、該当データが本当に正しいかどうかの判別は非常に困難となっている。

そこで我々は、データの確からしさを確認するための仕組みをインターネットにオーバーレイしたレイヤとすることで、既存のインターネットには影響を与えず、インターネット利用者は従来と同様に Web/アプリケーションを利用することが可能なアーキテクチャを「Trustable Internet」として提唱する。

Trustable Internet は、データを生成、修正、確認などのデータに関与した人やモノの情報を付加情報として格納、共有するためのインターフェースを提供するエンドースメントレイヤ(Endorsement Layer)を持つ。そして、データを起点としてデータに対して紐づけられた付加情報がどのようなつながりを持っているかを表現したデータ構造を持つエンドースメントグラフ(Endorsement Graph)を有している。

付加情報はインターネット上から、および人やモノが付与するフィジカル空間からの情報を蓄積し、データの生成時あるいは生成後に人や機器等により付与される。閲覧者がインターネット上のデータを閲覧する際は、必要に応じて、データの確からしさの根拠となる付加情報を複数の視点から確認できるようにし、また、個人の主観も考慮してブラウザに重畳するなどして提示する。さらに、エンドースメントグラフにおいて確からしさを判断するための情報が不足していることを指摘し、新たな情報を付与できるようにすることで、インターネット上のデータがより信頼できるものになる。

Trustable Internet により、インターネットにオーバーレイした構成をとることで、従来のシステムに影響を与ることなくデータの確からしさを確認するための汎用的なアプローチが実現可能となる。これにより、インターネット上の様々なデータに確認可能な情報を付加することが可能となる。また閲覧者がデータとデータに関連する付加情報からデータの確からしさや矛盾がないかどうかを確認できるようにし、それを根拠に主観的な判断を支援できるようになる。

従来、インターネット上のデータの確からしさの判断は個人に委ねざるを得なかったが、多角的な視点から確からしさを判断でき、それに基づく意思決定をよりの確にできるようになる。これにより、データの確からしさが不明なまま利用することや、偽情報やフェイクニュースを信じたまま再拡散することなどを未然に防ぐことが可能になると期待される。さらに、判断可能な範囲が拡大することにより経済活動・社会活動も範囲が拡大し、社会全体での最適な方法が選べるようになると考えられる。たとえば、災害などの迅速な判断が必要な時に情報が迅速に提供可能にできると考えられる。

前提としている対象読者層と前提知識

本ホワイトペーパーは、読者層として、IT ビジネスに取り組む関係者、および IT エンジニアにとどまらず、政策立案に関わる関係者を想定している。

想定する対象読者層：1 章、2 章は、技術バックグラウンドを必ずしも有しないビジネスサイドの関係者や政策立案者にもご理解いただけるように記載した。3 章については、内容が技術面に踏み込んでおり、IT エンジニアを読者層として想定している。

前提知識：3 章は、W3C をはじめとする Web 技術についての知識があることを前提としている。

なお、本ホワイトペーパーでは、文中で使用している 4 つの用語について下記の意味で用いている点に注意いただきたい。

- エンドースメント：データに対して、人やモノによって裏付け／関連付けること
- 情報：裏付け／関連付けされたデータ
- データ：インターネットから、あるいはフィジカル空間から取得され、かつエンドースされていない/エンドース対象となるデータ
- データの確からしさ：データの正しさの程度

1 背景

1.1 データ社会の進展とその信頼性

インターネットは現代において社会・経済活動において欠かせないものになっている。スマートフォンや SNS の普及により、個人や組織などが、いつでもどこでも世界にデータを発信し、閲覧できるようになった。また、センサなどのシステムから取得したデータは、企業や行政などがさまざまなサービスのために活用するようになってきた。これに伴い、インターネットでやりとりされるデータの信頼性が以前にもまして重要になってきた。

これらのデータの中には、誤った内容を含みいわゆる偽情報である場合もあり、これらによる社会問題も実際に起きている。インターネット上のデータにそのような疑いがあっても、データの確からしさ（正しさの程度）を確認できないことが多い。そのような中で、その確からしさの判断を閲覧者自身で下さざるを得ないのが現状であり、これらのデータに基づいて行われる意思決定が的確でなくなる可能性がある。

データの信頼性を高めるために、インターネット上で発信されるデータの発信者、個人や法人を識別する規格や法制度を整備する動きがある[1]。また、個人や法人の識別に加え、個人の資格や能力、法人の登記や信用情報をも確認できる仕組みが整備されつつある[3][4]。また、インターネット上のデータの発信者だけでなく、その人がその分野の専門家であるかどうかなどの、データの確からしさの判断に必要な情報を確認できるような仕組みも検討されているが、まだ実用化までは至っていない状況である。

1.2 ユースケースと課題

確からしさが不明なデータが発生し、拡散するユースケースとして、図 1 に示す災害時の情報伝達を挙げる。

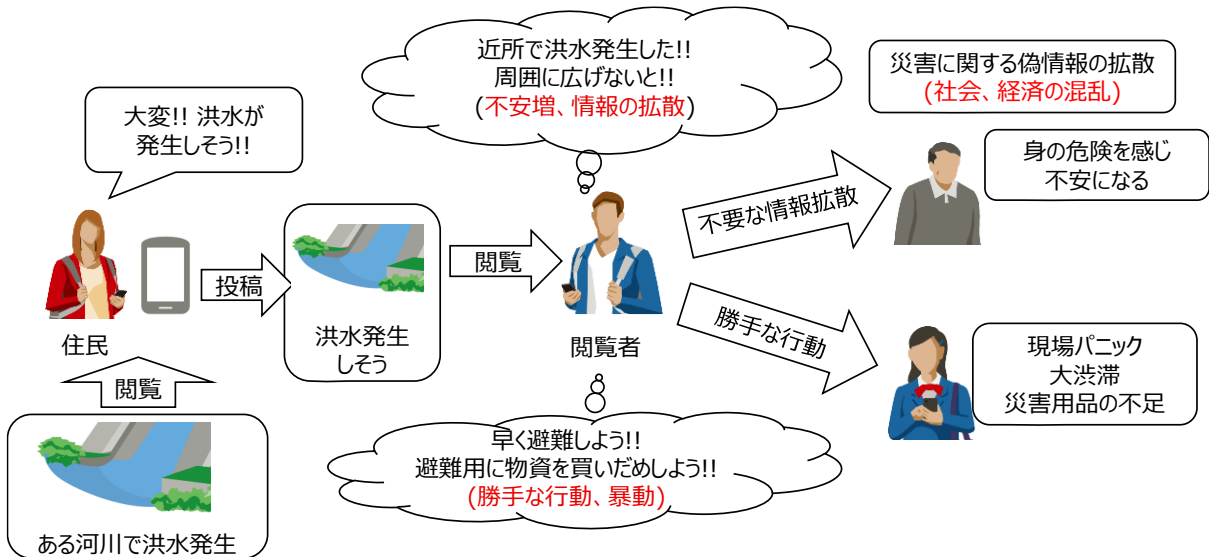


図 1. 災害時の情報伝達のケース

ある河川で発生した洪水のニュースに対して、ある住民がニュースを切り取って SNS に「洪水が発生しそう」というメッセージと共に投稿した。本人は善意から洪水の発生を伝えただけだった。しかし、直接確認できずに不安になっている閲覧者は投稿された情報を見て、閲覧者自身の近所で洪水が発生したのかもと誤ってしまい、近所で洪水が発生した可能性を周囲に伝えていく。その途中で、「洪水が発生しそう」という可能性のメッセージに様々な憶測の情報が追加され、ついには「洪水が発生にちがいない」と確信する住民が現れ始め、メッセージの内容も「洪水が発生した」という事実のメッセージに変化し、拡散してしまう可能性がある。その結果、さらに多くの住民の不安を煽り、住民の勝手な行動、例えば、不安に煽られて物資の買占め、暴動などを誘発し、社会・経済の混乱を引き起こしてしまう。

災害時のように、正確な情報が不足するときには、こうしたわずかな情報に憶測の情報が追加され、瞬間に真偽不明な情報が拡散してしまう。また、どの情報が正確で、どの情報が憶測なのかもわからないまま広がり、途中で内容も変化することが多い。インターネットは、様々な人が自由に発信できる場であるが、発信されたデータの中には、その確からしさを判断できないものが多く、真偽不明なままデータを利用せざるを得ない。その判断がデータの閲覧者に委ねられることにより、誤解やヒューマンエラーといったミスを生じさせることになる。

1.3 要件分析

このユースケースでは 2 種類のデータが存在している。最初に生成されるデータと、この最初に生成されたデータを修正して二次的に配信されるデータである。

最初に生成されるデータは、人が見聞きしたことをテキストに書き起こしたり、写真を撮影するなどして最初に生成したデータである。装置やシステムが生成する場合もある。これらのデータは、フィジカル空間での

状況の一部を表現したものであり、全てではない。また、人が生成するデータは、想像や憶測で補いながら生成したり、言葉で表現しにくい内容であるなど、その状況を受け手が同じように理解できないことがある。

二次的に発信されるデータは、最初に生成されたデータを人が一度受信して再発信されるデータである。人が受信する場合、メッセージをそのまま再発信することもあるが、メッセージの一部を切り出したり、解釈して表現し直すなどして再配信することがある。その際、受信者の想像や憶測が入り込む可能性がある。また二次的に発信されたデータが、さらに再発信されることもある。

このように、元のデータ生成時や再発信時に、人の憶測が入ったり、解釈により内容の変化が生じること、事実と異なるデータがサイバー空間の中で生み出されると考えられる。

このような事実と異なるデータが生成されるプロセスにデータの閲覧者が意図せず加担することを防ぐためには、手元にあるデータが確かなものでないことが閲覧者に分かれば、そのデータを拡散することや、それに基づいて誤った行動を起こすことが減ると考えられる。そのようなデータの確からしさが分かるように閲覧者を支援する仕組みがあれば、その真偽をそのまま鵜呑みにすることがなくなり、ミスが軽減されと考えられる。

本ホワイトペーパーでは、情報の側面に着眼し、有用な情報の蓄積と、情報間の関係性の充実によって、サイバー空間において、よりの確な判断をくだせるということを志向するものである。以下の要件で示すように、生成されたデータに対して、第三者視点の情報や実世界からの情報、さらには閲覧者の視点を考慮することで、その達成に近づくと考えている。

【要件(i)】サイバー空間上のデータの確からしさの根拠となる情報を取得できること

SNSの投稿のようなデータだけから、そのデータの確からしさを判断することは難しい。しかし、例えばデータに関連する情報として、データの発信者や発信地、情報の出し手の専門性が閲覧者から確認できるようになれば、そのデータの確からしさ（信ぴょう性）を見極めるための根拠として、確からしさの判断支援に利用できるようになると考えられる。加えて、情報間の関連性を強化し、根拠となる多面的・多数の情報間に矛盾点はないかなどの傾向を見出すことを可能にする。さらには、データ生成後に、そのデータに関して後から判明した事実や、専門家による生成データに対する判断等、生成されたデータの確からしさを確認した第三者が持つ情報を、関連情報として後からデータに紐づけて閲覧者から確認できれば、これらの情報もまたデータの確からしさの根拠として、確からしさの判断支援利用できると考えられる。

【要件(ii)】データとフィジカル空間の状態が一致／乖離している根拠となる情報を示すことができること

図 1 では、実際には閲覧者の周辺で洪水が発生していないにも関わらず、テキストデータに洪水という言葉が記載されており、現実の状態とデータの内容に乖離があった。これに対し、例えば水位情報や発信者の位置情報など、フィジカル空間で取得可能な、より信頼できる情報を根拠として利用することで、サイバー空間で生み出された「洪水」という言葉と事実（水位や位置）が乖離しているかどうか分かるようになる。

【要件(iii)】積極的に根拠となる情報を提供するための仕組みがあること

これらの仕組みが実社会で持続的に運用されるようなエコシステムの構築も必要となる。例えばデータの発信者や第三者から得られた根拠情報だけでは、データの確からしさを判断するための材料が不足していると閲覧者が感じる場合もあると考えられる。この場合に、閲覧者がさらなる根拠となる情報の提供を依頼し、依頼に応じて根拠となる情報を提供できるようにすることで、閲覧者のデータの確からしさに対する疑問を解消することにつながると考えられる。また、閲覧者にとって価値のある情報を提供した提供者を信頼性が高い情報提供者と評価するなど、提供者が根拠を提供するインセンティブを与えることができると考えられる。

2 TRUSTABLE INTERNET

2.1 Trustable Internet アーキテクチャ

従来のデータの確からしさを確認する手法としては、文書の承認管理システムや配送荷物の追跡システムのように、個別システム毎に証跡を記録する機能を組み込む方法や、インターネット以外の方法で事前にデータ送受信者の間で信頼を構築する方法が取られてきた。しかし、膨大なデータが存在するインターネット上でその確からしさを確認できる汎用的な方法は存在せず、該当データが本当に正しいかどうかの判別は非常に困難となっている。

我々は、データの確からしさを高めるための仕組みを持つレイヤをインターネットにオーバーレイした構成により、既存のインターネットには影響を与えず、インターネット利用者は従来と同様に Web/アプリケーションを利用することができ、必要に応じてデータの確からしさの根拠となる情報を取得することができるアーキテクチャを提案する。このアーキテクチャを「Trustable Internet」と呼ぶ（図 2）。

Trustable Internet において、確からしさの判断対象となるデータに付加され、人やモノによりそのデータに対する「裏付けが取られた」情報をエンドースメントデータ(Endorsement Data)と呼ぶ。また、それらを格納、共有する仕組みを持つレイヤをエンドースメントレイヤ(Endorsement Layer)と呼ぶ。

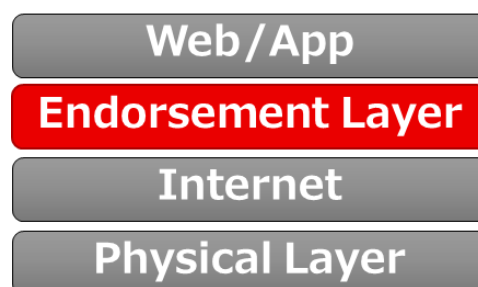


図 2. Trustable Internet アーキテクチャ

2.2 Endorsement Layer

エンドースメントレイヤは、確からしさの判断対象となるデータに付加されたエンドースメントデータを管理する機能を持つ。また、エンドースメントレイヤは、判断対象データを起点として、判断対象データに紐づけられたエンドースメントデータのつながりを表現する仕組みを有している。このようなつながりを表現したデータ

構造をエンドースメントグラフ（Endorsement Graph）と呼ぶ（図 3）。エンドースメントデータの詳細やエンドースメントグラフの実現方法に関しては次章で述べる。

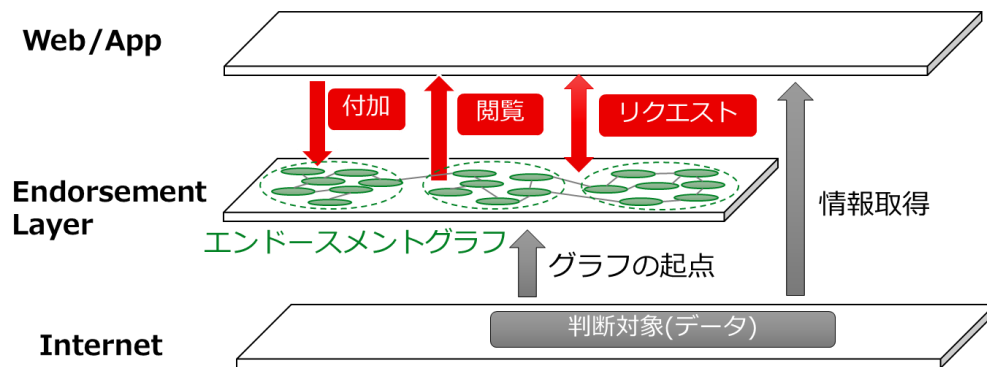


図 3. エンドースメントグラフ

エンドースメントレイヤは、人が所有する端末やモノ(機器)のアプリからエンドースメントグラフにアクセスするために以下のインターフェースを備える。

1. **付加**: データの発信者やデータの閲覧者、あるいはデータ管理システムは、インターネット上のデータに対し、その確からしさの根拠となる情報を任意のタイミングで付加することでエンドースメントデータを生成することができる。付加する際、改ざん防止処理策が適用される。
2. **閲覧**: データ閲覧者は、確からしさの判断対象データに対して、エンドースメントグラフを介してデータの確からしさの根拠となるエンドースメントデータの繋がりを閲覧することができる。
3. **リクエスト**: データ閲覧者は、閲覧しているエンドースメントデータからはデータの確からしさを判断できない場合、判断対象データに対して不足している根拠情報を新たに付加することをリクエストすることができる。また、根拠情報の提供者がリクエストに応じて根拠情報を付加できるように、判断対象データに対するリクエスト状況を確認することができる。

3 TRUSTABLE INTERNET の実現アプローチ

3.1 信頼できるデータ社会を目指すグローバルな動き

近年活発に、信頼できるデータ社会を目指すグローバルな動きがみられる。

人・組織などの実体と対となるサイバー空間におけるデジタルアイデンティティ実現を目指し、欧州では、欧州委員会において EU 市民ならびに企業間の電子取引におけるアイデンティティならびにその属性証明の仕様を統一し、デジタル ID ウォレットの積極的な導入を図るなど、トラストサービスの実現を図る EU の規則である eIDAS の適用・改正が進んでいる [1]。

また日本では、内閣官房配下の Trusted Web 推進協議会により、人、組織、機器のデジタルアイデンティティを使って、データのやりとりにおける信頼性を実現するビジョンならびにアーキテクチャを表す Trusted Web の策定が進んでいる。

国際標準化の動向としては、W3C(World Wide Web Consortium)において分散型アイデンティティのための標準規格 Decentralized Identifiers (DIDs) [2]ならびに個人の取得資格などのデジタルアイデンティティへの第三者検証可能なデジタル証明書 Verifiable Credentials (VC) Data Model [3]の策定が進んでいる。また、これらの規格を元に分散型アイデンティティを提供する様々なシステムが開発されており [4] [5] [6]、デジタル化された様々な資格情報を、個々人の意志で、インターネット上で自由に開示できる世の中が近づいている。

データの信頼性を確保するためのこれらの取り組みは総じて、これまで発展を遂げてきた Web 技術ならびに公開鍵暗号技術をベースにデジタルアイデンティティを使ってデータの出元の真正性を担保することを通して、データの信頼性を確保するための策定ならびに普及が進められている。それに対して、Trustable Internet は標準的な Web 技術ならびに公開鍵暗号技術に加え、これら新たな規格・基準も踏まえつつ、データの検証領域をフィジカル空間にまで拡大し、偽情報の悪影響を排除可能な信頼できるインターネットに基づく社会の実現を目指すものである。

以下の各章では、エンドースメントレイヤとエンドースメントグラフを実現するためのアプローチについて述べる。これらのアプローチと 1.3 章で述べた要件は以下のような関係である。

- 3.2 データに確からしさの根拠を付与するエンドースメントの仕組み：要件(i)
- 3.3 フィジカル空間を反映するエンドースメントグラフ：要件(ii)
- 3.4 確からしさを高めるための閲覧者の真偽判定支援：要件(iii)

3.2 データに確からしさの根拠を付与するエンドースメントの仕組み

ここでは、【要件(i)】「サイバー空間上のデータの確からしさの根拠となる情報を取得できること」を満たすために、エンドースメントレイヤ上で管理され、閲覧者によって利用される、エンドースメントデータとエンドースメントグラフについて述べる。

[エンドースメントデータ]

「エンドースメントデータ(Endorsement Data)」は、インターネット上のデータに関する情報、あるいは個人・法人・デバイスなどに関する情報をデジタル署名によって改竄不可能な形で記録したデータである。インターネット上のデータにエンドースメントデータを付与することで、閲覧者が、そのデータの生成者や生成場所、第三者がデータの内容をどのように評価しているかなどを確認できるようにし、エンドースメントデータからインターネット上のデータの確からしさを判断できるようにする。また、エンドースメントデータを付与した個人・法人・デバイスなどの身元や機能もエンドースメントデータによって表現し、閲覧者に利用可能にする。

先に挙げたユースケースの分析では、「洪水発生」というデータそのものの発信者が誰であるか、添付された画像がどこで撮影されたものであるか、などの確からしさの根拠となる情報を、閲覧者が確認可能なが要件となっていた。また 発信者が、例えば洪水が発生した河川の近隣住民であるなども確からしさの根拠となる情報としてわかる必要があった。

エンドースメントデータでは、これらの確からしさの根拠となる情報を「プロパティ(Property)」として扱う。プロパティはインターネット上のデータや個人・法人・デバイス等の属性や機能を表現するものとする。例えば、「洪水発生」というインターネット上の文字データに対しては発信者、生成日時などがプロパティに該当する。個人・法人であれば氏名・商号や住所、保有資格など、デバイスであれば製造メーカなどがプロパティであ

る。これらプロパティは閲覧者にとってデータの確からしさの根拠となりうる。これに対して、プロパティが付与される、「洪水発生」というデータや、そこに添付された画像など、閲覧者が確からしさの判断の対象とするインターネット上のデータそのものを「判断対象(Target Data)」と呼ぶ。判断対象に対して、プロパティを生成しエンドースメントデータを発行した個人・法人・デバイス等を「エンドーサー(Endorser)」と呼ぶ。先のユースケースにおいて「洪水発生」というデータの発信者というプロパティを生成したエンドーサーは発信者自身であり、発信者の住所というプロパティを生成したエンドーサーは発信者の属する自治体である。判断対象、エンドーサーを総称して「オブジェクト(Object)」と呼ぶ。オブジェクトはエンドースメントデータを付与される対象である。

Trusted Internet では、エンドースメントデータをオブジェクトに紐づいた以下の 4 つから構成されるデータと定義し、インターネット上のデータの確からしさの根拠を管理する。

1. プロパティ
2. エンドースメントデータを発行したエンドーサー
3. エンドーサーのエンドースメントデータ
4. エンドーサーが、オブジェクトプロパティを事実であると認めることを示すために、オブジェクトのプロパティに対して作成されたデジタル署名

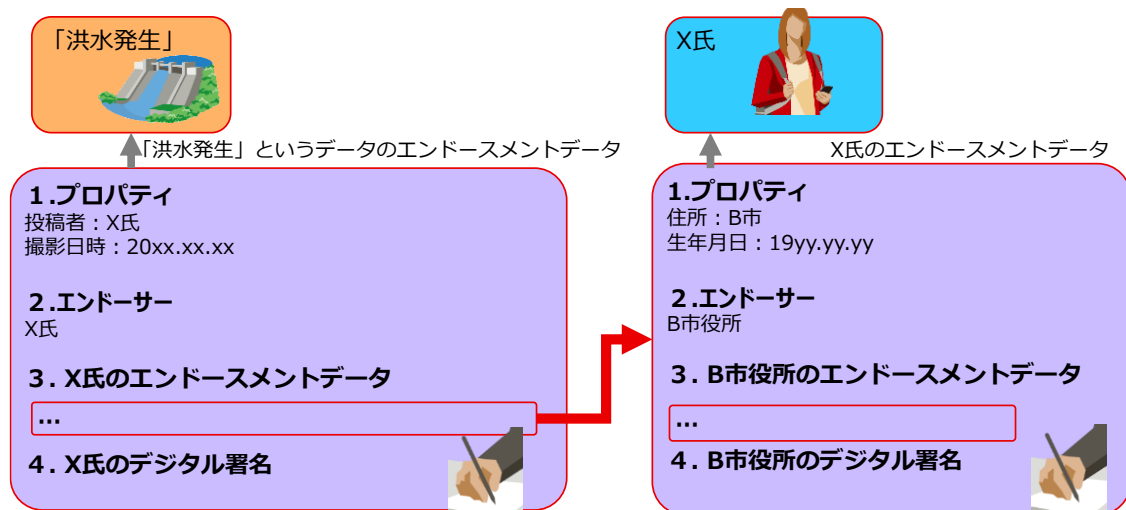


図 4. エンドースメントデータの例

このうち、個人であるエンドーサーのエンドースメントデータ、例えば X 氏が B 市の住民であることの根拠となるデータなどは、信頼できるデータ社会を目指すグローバルな動き 3.1 節で述べた、第三者検証可能なデジタル証明書を利用することができる。Trustable Internet では様々なシステムから発行されたデジタル証明書をエンドースメントデータとして取り込むことで、実社会における信頼情報をインターネット上で利用可能にすることを目指している。

[エンドースメントグラフ]

エンドースメントグラフは、エンドースメントデータと判断対象との関係と、エンドースメントデータの発行関係をグラフとして表現したものである。グラフとして表現することで閲覧者は、確からしさを判断したい判断対象のエンドースメントデータから、判断対象のプロパティ、そのプロパティを生成・確認したエンドーサー、そのエンドーサーのプロパティ、のように連鎖的に確からしさの根拠を辿ることができるようになる。以下にエンドースメントグラフを具体的な例を挙げて、内容を説明する。

図 5 は河川が氾濫したという一般市民からの投稿（＝判断対象）に対して作成されるエンドースメントグラフの例である。投稿の閲覧者は、このエンドースメントグラフより、投稿された画像が投稿者の居住地と異なる場所で撮影されたものであることや、行政機関からの投稿内容とは反するデータが提供されていることが分かる。これらにより、閲覧者はこの投稿が信ずるに値しないものと判断できる。

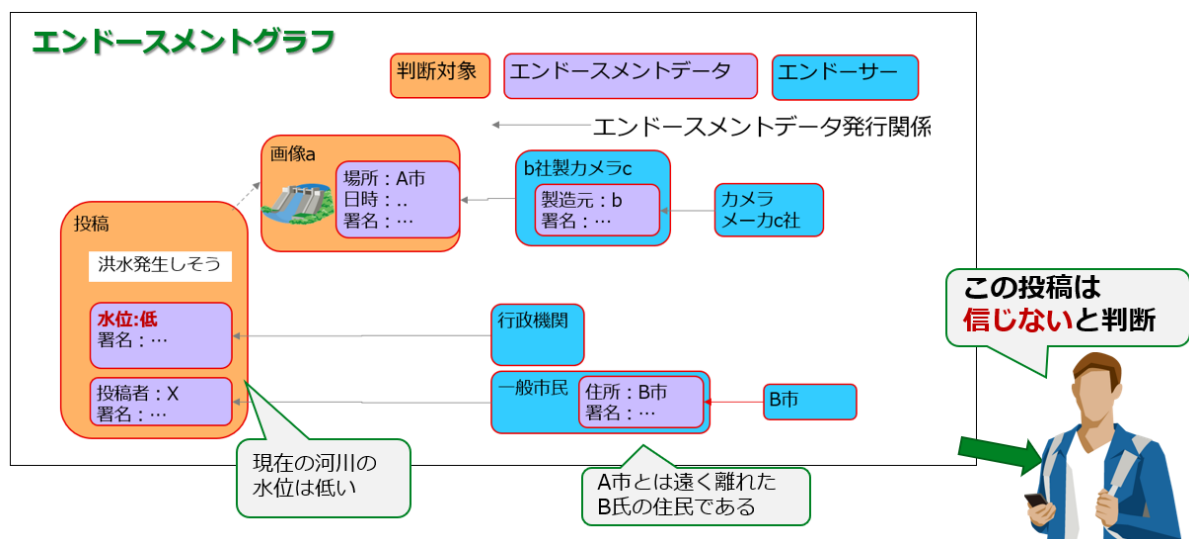


図 5. 一般市民の投稿に関するエンドースメントグラフの例

このように、エンドースメントレイヤにおいて、エンドースメントデータとエンドースメントグラフを管理し、閲覧者が取得可能にすることで、閲覧者にデータの確からしさの根拠を提供できるようにする。

3.3 フィジカル空間を反映するエンドースメントグラフ

ここでは、フィジカル空間で取得した事実情報に基づいて、サイバー空間のデータと事実が一致していることが確認できるようにするための、確からしさの根拠の付与と活用の過程を、ユースケースに基づいて、フィジカル空間の状況の感知、エンドースメントグラフへの追加、サイバー空間のデータとの一致の順に説明する。

[フィジカル空間の状況の感知]

フィジカル空間の状態や状況は、水位情報や位置情報など、フィジカル空間における様々な事実情報を、インターネットを介して取得することで感知または認知することが可能である。

フィジカル空間の事実情報を取得するセンサはIoT(Internet of Things)としての機能を備え、エッジ(例えば、IoT Gateway)を通じてインターネットに接続される。事実情報はエッジにおいてインターネットで利用可能なデータモデルに従って取得される。

一方、機器は製造者が正しい手順に従い製造し、設置者や保守者が決められた手順で設置、保守されている。それら機器の製造者情報やメンテナンス情報は、取得時にエッジ等でエンドースメントデータとして付与することにより、閲覧者はエンドースメントデータを閲覧することで、これらのプロセスを経たことを確認できるようになる。

このように、センサ機器の製造や設置、保守などが正しく行われていることが確認できることで、センサ機器から取得した情報が、判断対象となるサイバー空間のデータの確からしさの根拠として利用することができる。

さらに、位置情報を活用することで、フィジカル空間から取得した情報がどこで生成されたものなのか、どのような経路辿ってきたのかなどのエンドースメントデータを得ることができ、その確からしさを高めることができる。そのような位置情報は、例えばインターネットを構成するシステム（ネットワーク機器等）から取得することが考えられる。このようなエンドースメントデータを活用することで、フィジカル空間からの情報が実際の場所に関するものかどうかを確認出来るようになる。

[エンドースメントグラフへの追加]

前述のとおり、センサを介してフィジカル空間から得られた情報は、エンドースメントデータとして活用できる。フィジカル空間の情報は、判断対象のデータの生成時の他、事後検証という形など、いつでもエンドースメントグラフに追加できる。例えば、センサが川に設置される水位センサであれば、取得した情報を川の状態を示す根拠として追加することができる。この場合、エンドースメントレイヤにおいて、判断対象であるデータ(この例では洪水に関する SNS データ)に対して、センサからの情報(水位センサーによる水位の値)をエンドースメントデータとして追加する。

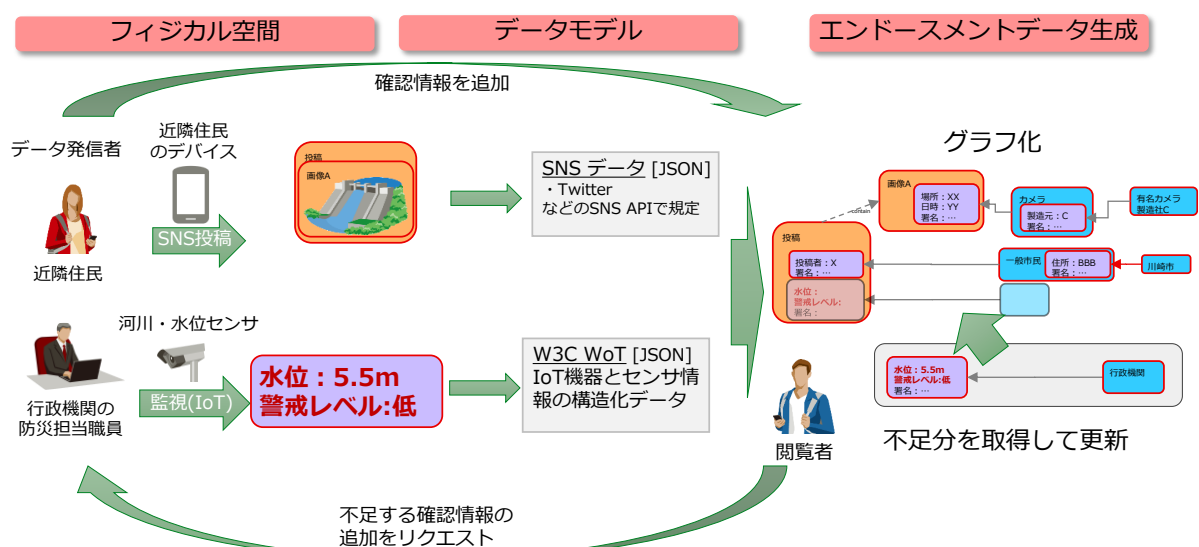


図 6 . フィジカル空間を反映するエンドースメントグラフ

[サイバー空間のデータとの一致]

一般的に、データの確からしさの確認を行うために、ビッグデータ解析を用いる手法が用いられる場合が多い。これは、元のデータを分析したうえで、そこに含まれる要素とそれらに関連する多くのデータをビッグデータとして解析するものである。たとえば、元のデータと似た投稿がないか、同じ場所や似た地形を持つ場所の過去の災害事例があるか、など、様々な関連データをインターネット等から収集し、機械学習により元のデータの確からしさを推定する。

しかし、ビッグデータ解析では、判断対象となる「洪水発生」というデータや、そこに添付された画像など、データそのものの確からしが高まる訳ではないことから、現実との不一致が生じる場合がある。これに対して、サイバー空間に加え、フィジカル空間から得られるエンドースメントデータを活用することで、データが発信された場所と、水位が取得された場所がことなること、など事実と乖離している状況が分かるようになる。

さらに、インターネット上の様々なデータにエンドースメントデータが付与されていくことで、エンドースメントレイヤに様々なエンドースメントグラフが蓄積される。これらのエンドースメントグラフを多角的に評価することで情報の一致／不一致や矛盾を検知できるようになり、エンドースメントデータが付与されていないデータについても、確からしさを判断することも可能になると考えられる。これにより、エンドースメントレイヤの重要性、必要性がさらに高まっていくことが期待できる。

3.4 閲覧者の確からしさの判断支援

エンドースメントグラフが取得可能な世界では、閲覧者がインターネットから「ある河川の状態」というフィジカル空間の情報を検索すると、インターネットとエンドースメントグラフの両方から情報を取得することができる。つまり、河川の水位情報や避難情報だけではなく、それら情報の根拠となるエンドースメント発行主体の情報も同時に閲覧することができる。

また、閲覧者はエンドースメントグラフより得られるエンドースメントデータを手掛かりに、データの確からしさを自ら判断することができる。ここで取得できたエンドースメントデータが少ない場合、閲覧者は判断対象に追加情報、すなわち追加のエンドースメントデータをリクエストすることができる。エンドーサーである情報提供者やデータ管理システムが、リクエストが多く発生しているデータに対してさらなる情報を付与することができれば、閲覧者はそれら発行主体が価値の高い情報を提供する提供者と考えることで、エンドーサーはより積極的にデータに対して情報付与を行うようになると考えられる（図7）。

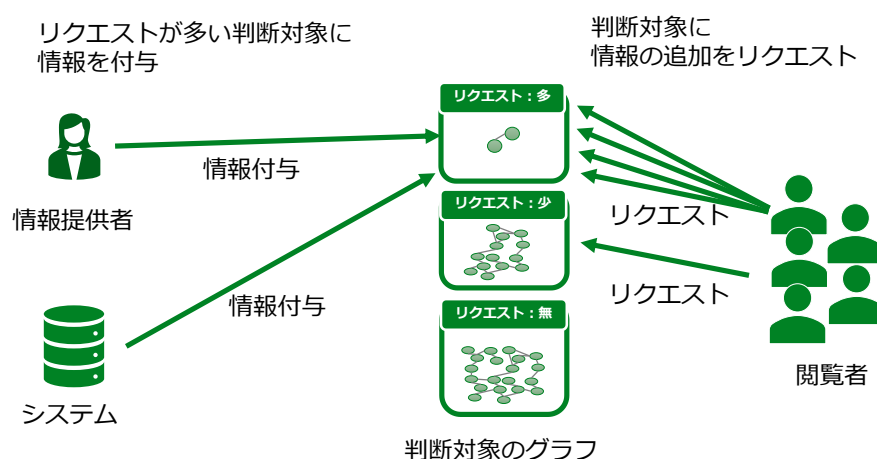


図7. 情報のリクエストと情報付与

一方、閲覧するエンドースメントデータが多く、その関係が複雑になる場合は、閲覧者に対して判断を支援するための仕組みをアプリやブラウザ拡張機能で提供する方法が考えられる。例えば、判定基準を事前定義し、その判定基準にそったデータのみを閲覧者に提示するアプリやブラウザ拡張が考えられる(図 8)。判定基準としては、例えば SNS の投稿ルールやガイドライン、データ管理企業のデータ利用ポリシーなどを適用することが考えられる。

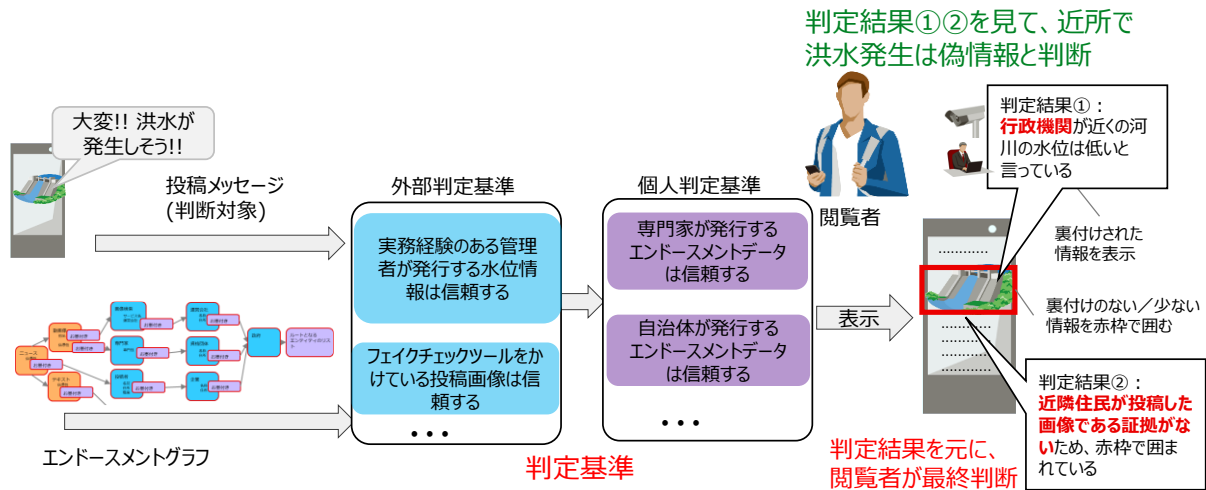


図 8. 外部判定基準／個人判定基準によるデータの確からしさの判断支援

図 8 の例では、サービスや団体のルールやポリシーを表す外部判定基準と、閲覧者のホワイトリスト／ブラックリストを定めた個人判定基準を用いて、エンドースメントグラフを解析する例を示している。外部判定基準は、情報の生成プロセスに関連した判定条件を定義している。一方、個人判定基準は、閲覧者の主義や趣向により信頼する人、モノを条件としている。これらの判定基準を利用して、閲覧者に対してデータに対する補助情報を表示したり、警告を表示したりすることにより、確からしさの判断支援を行う。

このような判断支援により、閲覧者の利便性が向上することで、さらなるエンドースメントデータのリクエストや、リクエストに対する根拠情報の付与を促すことが期待される。

3.5 全体動作

ここではユースケースにおける確からしさが不明な情報が拡散されてしまうという課題が、Web アプリからのデータとフィジカル空間からの情報から生成されるエンドースメントグラフを利用して解決する一連の流れを説明する(図 9)。

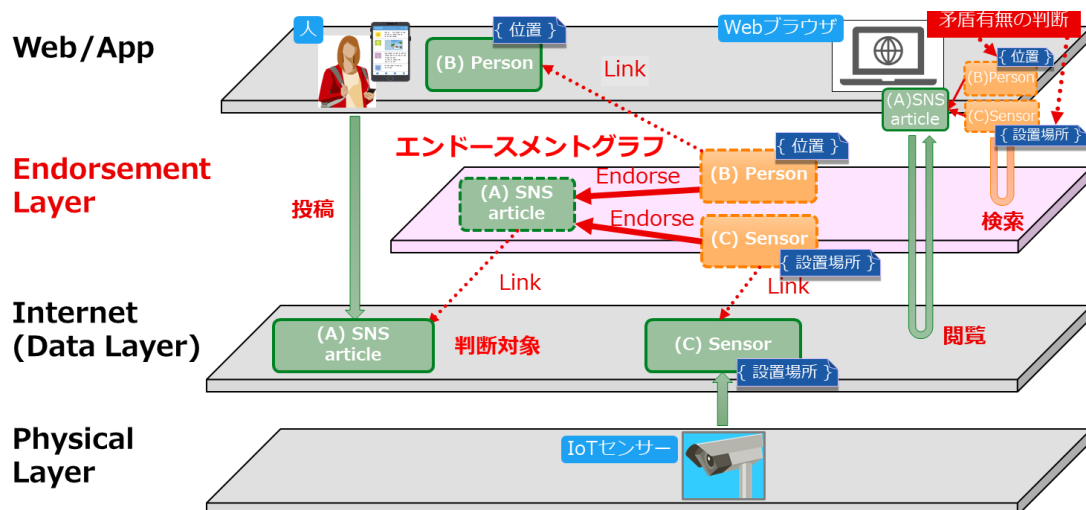


図 9. 全体動作

- (1) ある住民が、スマートフォンを使い、SNS に「洪水が発生しそう」というメッセージを投稿する。その投稿メッセージはデータ化されインターネットで閲覧可能となる。そのデータの発信者の ID を、投稿記事の確からしさの根拠としてエンドースメントグラフを生成する。先に述べたように、洪水など災害が発生しているかどうかの根拠は、専門知識を持つ人、あるいは現場にいる人(例えば、気象予報士、土木分野や災害対策の専門家、近隣住民など)による情報発信であるかどうか判断材料となり得る。この情報は(B)でデータ化される人の属性で表される。
- (2) データとフィジカル空間の状態が一致／乖離していることを示すために、川に設置された水位センサから常時取得されているデータに対し、例えば SNS のメッセージを閲覧した行政機関の担当者が、エンドースメントデータとして追加するプロセスを経ることで、元の SNS 投稿記事の確からしさの根拠として利用できる。エンドースメントデータは、元の SNS 投稿時だけでなく、事後に追加することもできる。
- (3) 閲覧者がインターネットから川の状態を検索するときには、インターネットとエンドースメントグラフの両方から情報を取得し、この川に関する情報だけでなく、その状態に関する根拠となるエンドースメントデータを同時に閲覧できる。例えば、判断対象に対して人やセンサなど複数のエンドースメントデータが付与される際、複数のエンドースメントデータの間には矛盾がある場合、判断対象の信ぴょう性に欠けると判断することが可能となる。このユースケースの場合、閲覧者は、SNS 投稿の発信者の位置とセンサの設置場所が異なっていることが分かることで、閲覧者の近くで洪水が発生しそうだったことが勘違いであることを認識し、その投稿をさらに拡散することを思いとどまることができる。
このようにして「洪水が発生しそう」というデータの確からしさは、そのデータの根拠となるエンドースメントデータに基づき閲覧者が判断する。

以上で説明したように、インターネット上のデータに対して、フィジカル空間との紐づけが可能となり、データの閲覧者は客観的な根拠を確認しながら、データの確からしさを判断できるようになる。

4 実現に向けた今後の取り組み

今後、Trustable Internet の実現にむけて、Trusted Internet Architecture Lab.では技術開発とエコシステム構築に双方に関してブラッシュアップを進めていく予定である。現時点では以下のような取り組みを考えている。

(1) エンドースメントグラフを扱うためのプロトコル開発のための取り組み

エンドースメントデータおよびエンドースメントグラフを扱うためのインターネットおよび Web プロトコルを確立していく必要がある。

- エンドースメントデータが分散している環境においてエンドースメントグラフの閲覧などの処理を実現していくためのプロトコルの確立
- 閲覧者の複数の視点に応じた、多次元化したエンドースメントグラフの構築手法

(2) エコシステムを構築するための取り組み

エコシステムまでをセットにしたアーキテクチャ、仕組みを検討していく必要があり、以下のような観点について取り組む予定である。

- データを閲覧する人は、エンドースメントグラフを元にデータの確からしさを判断できるようになるため、一定のメリットを享受できるようになる。一方で、データに対してエンドースメントデータを付与する人（エンドーサー）のモチベーション、メリットについても考慮していく必要がある。この解決のためには、例えば、レピュテーションの仕組みを導入することで、元のデータの確からしさを高めるような情報を付与する人に対して高い評価を与えるなどのインセンティブ付与が考えられる。あるいは、トークンや NFTなどを付与するなど、直接的なリワードを与えることも考えられる。
- Disinformation（偽情報）やフェイクニュースを判別するための AI 技術に基づく取り組みなども進められており、これらの技術と組み合わせによる精度向上が考えられる。
- 複雑な社会状況などの様々な状況を表現した情報をエンドースメントデータとして取り込んでいくためには、例えば、否定のプロパティや確率的なプロパティなど、効果的なエンドースメントデータの表現形式を検討する必要がある。
- また、エンドースメントデータに関して、エンドーサーの想定外の利用・拡散が行われないようなプライバシー対策、安全対策の検討も必要である。
- さらに、エンドーサー／データ閲覧者双方が簡単に利用できるように、UX を高めるための仕組みが必要になる。

(3) ユースケースの拡充

今後、データの扱いが本コンセプトに基づいて進化した場合を想定した、実用感のあるユースケースの拡充に向けた検討も必要である。例えば以下のようなユースケースの検討を考えている。

- Disinformation（偽情報）やフェイクニュースに対するエンドースメントグラフの活用
- 既存のコミュニケーション／情報収集手段と組み合わせによる、エンドースメントグラフの活用
- 国を超えた域外流通におけるデータの信頼性の向上

5. 引用文献

- [1] European Commision, “European Digital Identity Architecture and Reference Framework – Outline | Shaping Europe ’ s digital future,” [オンライン]. Available: <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>.
- [2] The World Wide Web Consortium (W3C), “Decentralized Identifiers (DIDs) v1.0,” [オンライン]. Available: <https://www.w3.org/TR/did-core/>.
- [3] World Wide Web Consortium (W3C), “Verifiable Credentials Data Model v1.1,” [オンライン]. Available: <https://www.w3.org/TR/2022/REC-vc-data-model-20220303/>.
- [4] The Linux Foundation, “Hyperledger Indy – Hyperledger Foundation,” [オンライン]. Available: <https://www.hyperledger.org/use/hyperledger-indy>.
- [5] Microsoft Corporation, “分散型 ID (アイデンティティ) ソリューション | Microsoft Security,” [オンライン]. Available: <https://www.microsoft.com/ja-jp/security/business/identity-access-management/decentralized-identity-solution>.
- [6] TBD, “Web5 | TBD,” [オンライン]. Available: <https://developer.tbd.website/projects/web5/>.