

**Trusted Web の実現に向けたユースケース実証事業  
成果報告書**

オンラインマーケティングにおけるパーソナルデータの流通

2023年3月20日

代表機関：株式会社 DataSign

## 目次

1	背景と目的	1
2	事業の概要	1
2.1	事業概要及び実証の範囲	1
2.2	社会・経済に与える価値・影響	3
2.3	コンソーシアムの体制	3
2.4	実証全体のスケジュール	4
3	実証内容	5
	用語集	5
3.1	実証の実施事項、論点及び判断	5
3.1.1	プロトタイプ of 企画・開発	5
3.1.2	国際標準規格の調査	10
3.2	検証できる領域を拡大する仕組み	10
3.2.1	データフロー	10
3.2.2	データフローに登場する主体とその概要	11
3.2.3	検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容	13
3.2.4	本システムで形成を目指す合意とその履行のトレースの内容	15
3.3	6 構成要素との対応	17
3.3.1	検証可能なデータ	17
3.3.2	アイデンティティ	17
3.3.3	ノード	18
3.3.4	メッセージ	18
3.3.5	トランザクション	18
3.3.6	トランスポート	18
3.3.7	その他	19
3.4	本実証で企画・開発したシステムの概要	19
3.4.1	業務フロー	19
3.4.2	ユースケース図	19
3.4.3	操作画面 (UI)	19
3.4.4	機能一覧/非機能一覧	19
3.4.5	データモデル定義 (VC および OP)	20
3.4.6	実験環境	20
3.4.7	システムの構成要素	20
3.5	実証を通じて得られた主な成果	20

3.5.1	システムの企画・開発に関する実証内容・得られた主な成果 .....	20
3.5.2	ビジネスモデルに関する実証内容・得られた成果 .....	22
3.3	本実証で開発したシステムの第三者による再現可能性（A 類型のみ） .....	22
4	実証終了後の社会実装に向けた見通し .....	24
4.1	社会実装時に想定しているビジネスモデル・ユーザーのメリット .....	24
4.2	実証を通じて判明したユースケースの課題とその解決方針 .....	25
4.3	本ユースケースの社会実装に向けたマイルストーン .....	27
5	Trusted Web に関する考察 .....	29
5.1	Trusted Web のアーキテクチャに関する課題と提言 .....	29
5.2	その他 Trusted Web の課題と提言 .....	29

## 1 背景と目的

オンラインマーケティングにおいて、生活者のメールアドレスや電話番号、Cookie やそれに紐づく行動履歴、位置情報などのパーソナルデータが本人の意思に関わらずさまざまな事業者によって収集されている。パーソナルデータがいつの間にか知らない事業者に収集・利用され「気持ちが悪い」といった印象論だけでなく、リクナビ内定辞退率問題では、就職活動における採用判断に影響を与え、ケンブリッジ・アナリティカ事件では、Facebook のデータが第三者に不正に利用され、選挙の結果に影響を与えるなど、オンラインマーケティング事業者により収集されたパーソナルデータが本人の意図しない利用をされることにより、本人の権利利益を害する事案が起きている。

これらの問題を解決するために、主に法的な対応を含めたガバナンスによって、個人の権利利益を保護するような動きは世界で活発化しているが、技術的な解決の方法は未だ社会実装されていない。

また、パーソナルデータを利用するオンラインマーケティング事業者にとっても、広告識別子が利用できなくなっていくなどの社会情勢もあり、加えて、収集するデータがすべて正しいとは限らないため、アド Fraud やボットにより生成される不正なデータをフィルタリングする等の対策を行っているが、堂々巡りの状態が続いている。

これらの課題を解決するために、生活者が自らのパーソナルデータをコントロールできるようにし、パーソナルデータを活用する事業者の正当性の検証や、データそのものの正当性の検証を可能にすることを通じて、パーソナルデータの利用についての合意形成と履行の確認ができるような仕組みを構築することで、事業者はより有用なパーソナルデータを生活者の意図に沿って活用ができるようになり、生活者も安心してオンラインメディアやオンラインサービスを利用することができるようになる。

## 2 事業の概要

### 2.1 事業概要及び実証の範囲

本ユースケースでは、ウェブサイトを開覧する「サイト閲覧者」、ウェブサイトを運営する「サイト運営者」、ウェブサイトに広告を配信する「広告配信事業者」、ウェブサイトのアクセス解析を行う「アクセス解析事業者」（「広告配信事業者」「アクセス解析事業者」を総称して「アドテク事業者」と記載する場合もある）を対象とした課題の解決を目指す。

誰がパーソナルデータを収集しているかわからない、分かったとしてもそれが正当な事業者なのかかわからない、また収集する側も、収集したパーソナルデータが正当かわからない等、オンラインマーケティングにおけるパーソナルデータに関する課題は多い。

この課題を解決するために、審査機関が正当性を証明する証明書を各エンティティに発行し、各エンティティ間で確認・検証しあうことにより、上記の課題を解決していきたい。

正当性を確認できた場合には、一定のパーソナルデータの利用やウェブサイトへのアクセスについてはあらかじめ利用目的を設定しておくことで、アクセスするたびにパーソナルデータ利用やウェブサイトアクセスに関する確認や同意を都度行うことの無いような UX・UI を実現し、ユーザビリティを向上させ、各エンティティ

のオンラインマーケティングにおける負担を減らすことも検討する。

また、「サイト閲覧者」に対しては、パーソナルデータの提供履歴を確認し、必要に応じて無効化できるようにすることで、透明性を確保し、一定のトレースも可能とする機能の実装も行う。

なお、事業者の正当性の意味するところは審査機関による審査内容によって異なってくると考えられるが、本実証では審査の内容については検討対象外としているため、第三者によって何らかの審査を受け、審査基準を満たした事業者を正当な事業者としている。

本ユースケースでは、以下の表 1 に記載した課題の解決を目指す。

表 1：本ユースケースで解決を目指す課題

課題の対象	解決すべき課題	Trusted Web システムによって解決できること
サイト閲覧者	<ul style="list-style-type: none"><li>自分のどんなパーソナルデータがどこに提供されているのかわからない。</li><li>パーソナルデータをどこに提供して良いか判断ができない。</li></ul>	自らのパーソナルデータの開示範囲や利用目的をコントロールすることで課題解決に資する。また、提供したパーソナルデータが合意した範囲（期間、事業者）において取り扱われているかを追跡できるようになり、審査されていないサイト運営者やアドテク事業者にパーソナルデータが渡ることを防ぐことができる。
サイト運営者	<ul style="list-style-type: none"><li>不正なサイト閲覧かどうか確認ができない</li></ul>	サイト閲覧者から「非ボット VC」を受領し検証することで不正なアクセスによるデータのノイズを除去することができ、正確なデータの活用が可能となる。
	<ul style="list-style-type: none"><li>正当なアドテク事業者か判断できない</li></ul>	アドテク事業者から「正当なアドテク事業者である OP」を受領し、検証することで、不正なアドテク事業者にデータが渡ることを防ぐことができる。
アドテク事業者	<ul style="list-style-type: none"><li>不正なサイト閲覧かどうか確認ができない</li></ul>	サイト運営者によるサイト閲覧者を装うボットを使ったアドフランドや不正なアクセスによるデータのノイズを除去することができ、正確なデータの活用が可能となる。

## 2.2 社会・経済に与える価値・影響

国内のインターネット広告の市場規模は、電通の発表する日本の広告費によれば 2 兆 7,052 億円とされ年 20%以上の成長をしている。ただし、パーソナルデータの利活用に関して、どのように生活者の関与を実現するかが大きな課題となり、プラットフォームの独断的な判断により、広告識別子が利用できなくなるなど、公平公正なビジネス環境とは言い難い状況になっている。

また、アド Fraud による被害額も Spider Labs の調査によると 1,000 億円以上に上ると推定されており、対策が急務となっている。

( <https://prt-times.jp/main/html/rd/p/000000098.000031981.html> )

このような状況の中で、Trusted Web として、パーソナルデータの利活用に対し生活者の関与を強め、検証できる領域を広めて、オンラインマーケティング全体の Trust を向上させ、生活者にとっても、サイト運営者にとっても、アドテック事業者にとっても公平公正なビジネス環境を構築することで、より多くの信頼性の高いパーソナルデータが活用できるようになり、利用者にとって真に価値のあるサービスが開発されていくことが期待される。

## 2.3 コンソーシアムの体制

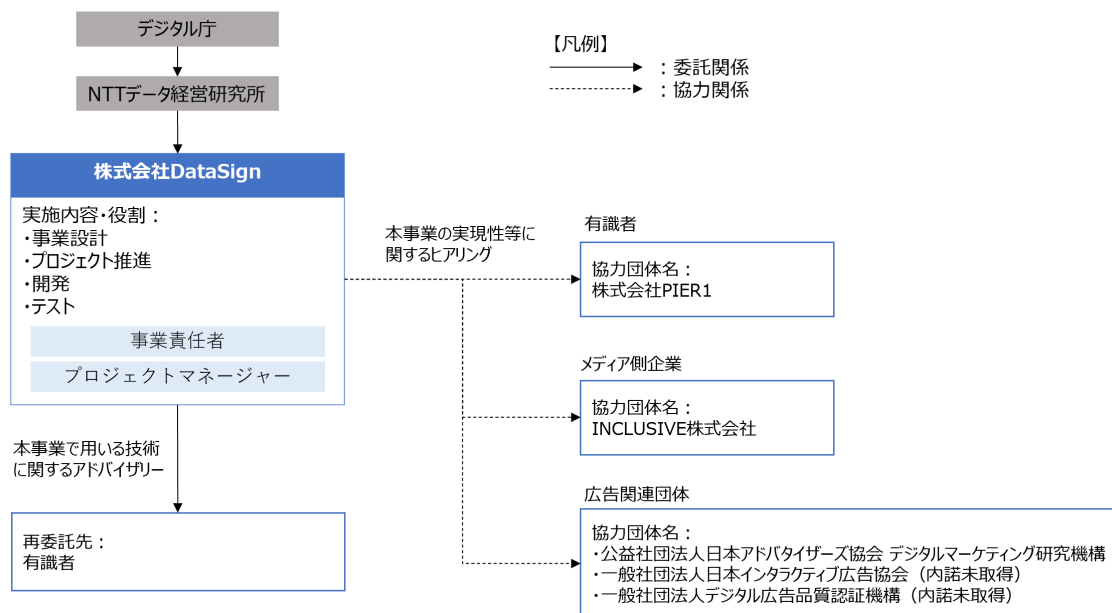


図 2.3 実施体制図

## 2.4 実証全体のスケジュール

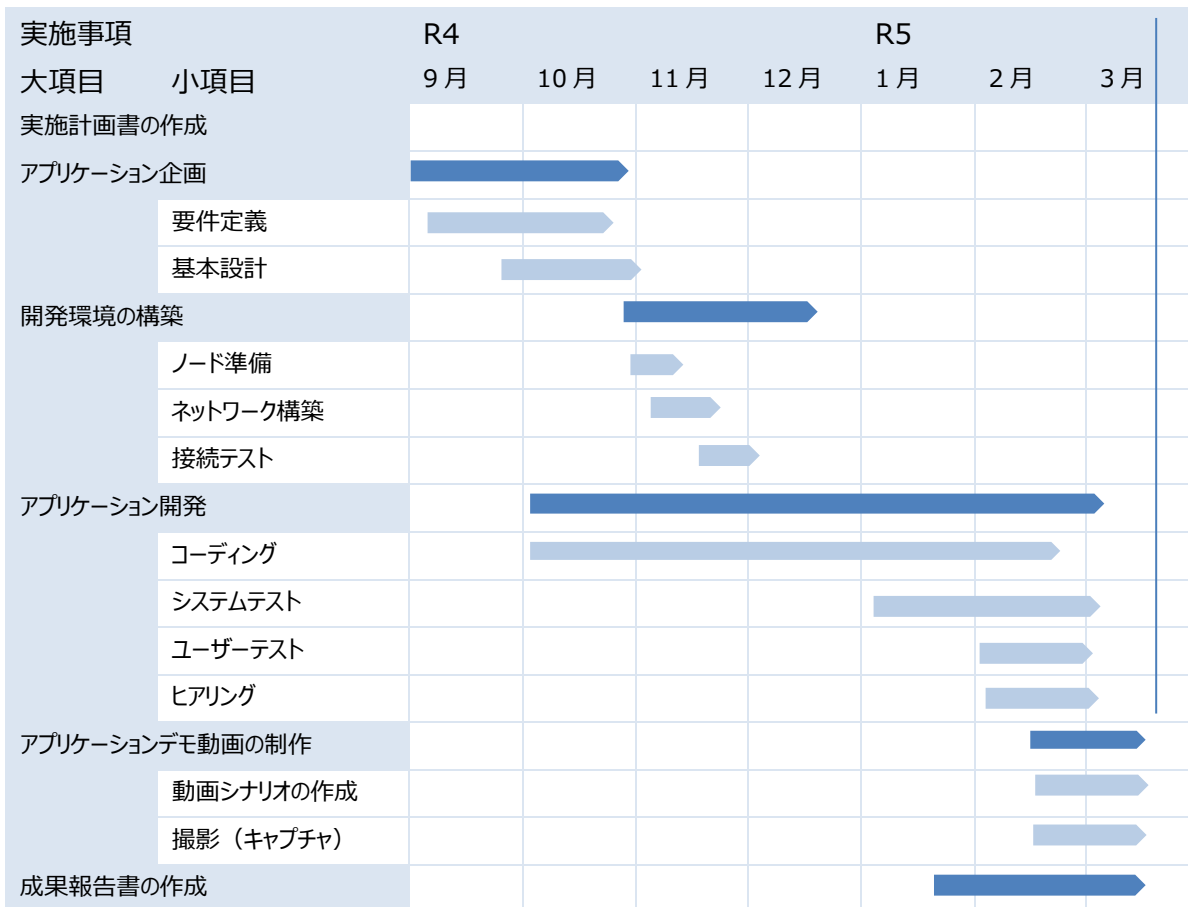


図 2.4 実証全体スケジュール

### 3 実証内容

#### 用語集

- DID : Decentralized Identifiers。W3C によって標準化されている分散型識別子。  
( <https://www.w3.org/TR/did-core/> ) 本実証では ION を利用しており、本文書内においては基本的に ION ( <https://identity.foundation/ion/> ) のことを指す。
- Root DID : 本ユースケースではペアワイズ DID として提供先毎に DID を発行しているが、その元となる DID のことを指す。Root DID の秘密鍵があればそこから派生したペアワイズ DID を復元することも可能。
- VC : Verifiable Credentials。W3C によって標準化されている検証可能な証明書。  
( <https://www.w3.org/TR/vc-data-model/> )
- OP : Originator Profile。Originator Profile 技術研究組合によって仕様策定が行われている情報の発行者や流通経路を検証可能にする技術、およびその証明書のことを指す。本文書内においては基本的に証明書のことを指す。( <https://originator-profile.pages.dev/ja-JP/> )
- DWN : Decentralized Web Node。DIF によって標準化が進められている分散型ノード ( <https://identity.foundation/decentralizeDWN/spec/> ) 。
- サイト閲覧者 : ウェブサイトを閲覧する生活者。
- サイト運営者 : ウェブサイトを運営する主体。
- アドテク事業者 : 「広告」や「アクセス解析」のための機能をサイト運営者に提供する主体。
- 広告識別子 : サイト運営者やアドテク事業者が「広告」や「アクセス解析」のためにサイト閲覧者を識別するための識別子。
- Bunsin : DataSign が提供する、メールアドレス発行サービス。提供先毎に異なったメールアドレスを発行することで、自分の意思でメールアドレスの提供を行っていない事業者からメールが送付されてきた際に、どこに提供したメールアドレスかを特定し、漏洩元を特定しメールの受信をブロックすることができる。

#### 3.1 実証の実施事項、論点及び判断

##### 3.1.1 プロトタイプの企画・開発

###### (1) 企画・開発時の論点

###### ➤ DID について

DID は昨年度 Trusted Web のプロトタイプとして実装したものと同様、ION を利用することとした。サイト閲覧者の DID の発行方法について、当初提供先毎にすべて DID の値が異なるペアワイズ DID を想定していたが以下の論点により、アクセスしているサイト (1<sup>st</sup> Party Domain) 毎に DID を発行することとした。

A : ペアワイズ DID として、すべての提供者に対してサイト閲覧者は異なる DID を発行する。



#### メリット

- ・ サイト閲覧者はすべての提供先に違う DID を付与するため、名寄せを行われるリスクが最小となる。

#### デメリット

- ・ 1 回のサイトアクセスについて、複数の DID を発行するため、オーバーヘッドが多くなりサイト表示の遅延リスクがある。
- ・ 大量の DID が発行されるため、管理が煩雑になる。

B：サイト閲覧者のアクセスしているサイト（1<sup>st</sup> Party Domain）毎に DID を発行する。

#### メリット

- ・ 1 回のサイトアクセスに 1 個の DID を発行するため、サイトアクセス時のオーバーヘッドが少ない。
- ・ サイト毎 に DID を発行するので管理がしやすい。

#### デメリット

- ・ 名寄せを行われるリスクがある。

当初 A のペアワイズ DID の方式で実装することを予定していたが、今回のユースケースにおいては、現時点では 1<sup>st</sup> Party Cookie で同等が利用できることを踏まえ、広告識別子として少なくとも、1<sup>st</sup> Party Domain 毎に識別子を発行することとしたため、A のメリットは無くなり、B のデメリットは 1<sup>st</sup> Party Cookie のデメリットと同等のため、B で実装することとした。

#### ➤ 広告識別子について

広告識別子についての論点は以下。

A：1<sup>st</sup> Party Domain 毎に異なる識別子を発行する。

B：グローバルに共通の広告識別子を発行する。

広告識別子は検証が行われたサイト運営者およびアドテク事業者への提供、もしくは、検証ができない場合は、ポップアップによる個別確認を行うこととしていたため、B を採用する方向で検討していたが、必ずしもサイト閲覧者がグローバルに共通の広告識別子を発行することを認識できているとは限らないと考え、サイト閲覧者がエクステンションを利用する際の初期設定で、どちらのタイプ広告識別子を発行するか、サイト閲覧者自身に選択してもらうこととした。

#### ➤ DWN を利用するか、しないか

当初、サイト閲覧者もサイト運営者もアドテク事業者も DWN にデータを保存し、DWN を介してデータのやりとりを行うことを想定していたが、そもそも DWN を用いない方法によって実現可能であるとの指摘を受けた。しかしその場合、サイト閲覧者のデータはローカルに保存され、ローカルのデータが失われてしまった場合に、復元することができない。今回は広告識別子やメールアドレスなどの情報であるためそこまで復元に対する必要性がないのでは、との指摘も受けたが、必ずしもリアルタイムですべての情報をやりとりするわけではなく、データ取得の履歴を残すトレース機能なども考えると DW

Nを利用するメリットは大きく、実際にはオンラインマーケティングに利用されるデータは多岐に渡るため、今後多様なデータが用いられることを鑑みるとローカルに保存する際の容量や仕組みの確保、復元に対する必要性が課題となることは明白なため、サイト閲覧者のDWNは利用することとした。サイト運営者、アドテク事業者については、DWNの必要性が乏しいため、利用しないこととした。留意事項として、DWNは Decentralized な仕組みであるがゆえに、サイト閲覧者が自分自身でサーバーを用意し、自分専用のDWNを構築することも可能であるため、自分専用のDWNのエンドポイントが当該サイト閲覧者の識別子として利用されてしまうリスクが残る。

➤ 組織認証VCについて

当初、サイト運営者、アドテク事業者に対し、審査機関が VC を発行することを想定していたが、Originator Profile の仕様の検討状況やユースケースを調査した結果、今回のユースケース独自のVCを発行するのではなく、業界標準として検討が進められているOPを利用したほうが、本ユースケースだけのVCのスキーマを定義し、サイト運営者やアドテク事業者、審査機関との認識合わせ、それぞれ個別で実装をしていくよりも、今後のインターオペラビリティを鑑みるとメリットが大きいと判断し、開発に大幅な変更が必要となったが、メリットを優先し、審査機関はVCではなく、OPを発行し、サイト運営者、アドテク事業者はOPの仕様に沿って、“.well-known” 配下にOPを配置することとした。

➤ 非ボットVCについて

当初、非ボット審査機関が、非ボットVCをサイト閲覧者に発行し、サイト閲覧者は、サイト運営者、アドテク事業者に対する非ボット証明として提供することを想定していたが、前述（3.1.1（1）のDIDについて）の通り、DIDはアクセスしているサイト（1<sup>st</sup> Party Domain）毎に都度発行されるため、非ボットVCが発行されたDIDと、サイト運営者、アドテク事業者に提供するDIDが異なることとなってしまい、非ボットの検証が行えないことがわかった。そのため、実装においては、非ボット審査機関が審査を行い、証明書は発行するが、その時点ではDIDに紐づいたVCの状態にはせず、都度発行されるDIDが発行された時点で、エクステンションが当該DIDに紐づいたVCの発行を非ボット審査機関にリアルタイムに要求し、発行されたVCをDWNに保存することとした。プロセスは以下ようになる。

1. サイト閲覧者がウェブサイトアクセス
2. サイト閲覧がサイト運営者、アドテク事業者のOPを検証
3. 検証がOKであれば、エクステンションがDIDを発行
4. エクステンションがRoot DIDの秘密鍵で、「発行されたDID」を署名し、非ボット審査機関に非ボットVCを要求
5. 非ボット審査機関が対象のDIDをsubjectとする非ボットVCを発行

(2) ユーザーテスト（DataSignにより実施）

- 審査機関（OPの発行）  
審査機関がOPを発行する手順、動作についてテストを行い、問題なく動作することを確認した。
  
- サイト運営者  
サイト運営者が審査機関から受領した自社およびアドテク事業者のOP、スクリプトによって発行したサイト運営者自身のDIDをウェブサーバに設置し、取得するテストを行い、問題なく動作することを確認した。  
また、提供を受けたパーソナルデータに対し、DWNから取得できることを確認し、問題なく動作することを確認した。
  
- アドテク事業者  
アドテク事業者がスクリプトによって発行したアドテク事業者自身のDIDをウェブサーバに設置し、取得するテストを行い、問題なく動作することを確認した。  
また、提供を受けたパーソナルデータに対し、DWNから取得できることを確認し、問題なく動作することを確認した。
  
- サイト閲覧者  
サイト閲覧者がブラウザエクステンション（Bunsin DID Wallet）をブラウザにインストールしたうえで、サイト運営者のウェブサイトアクセスし、アクセスしたウェブサイトにてOPが設置されていた場合にOPの検証が正しく行えること、指定したパーソナルデータの提供が行われていること、提供したデータに対するアクセス履歴がエクステンションで確認できることを確認した。また、アクセスしたウェブサイトにてOPが設置されていない場合に、パーソナルデータの提供が行われていないことの確認を行い、問題なく動作することを確認した。また、OPが設置されていない一般のウェブサイトにおいては、OPを検証できないとして第三者の提供するスクリプトをブロックできたことが確認された。  
また、サイトアクセス時に事前の処理（OPの検証等）が発生することから、オーバーヘッドが発生しアクセス速度に影響が出るという懸念があったが、サンプルサイトにおいては、数百ms程度であり、体感上の影響はなかった。しかし、これはサンプルサイトをlocalhostで疑似的に再現しているテストであり、実際に運用されているウェブサイトでのテストが行えていないため、ウェブサーバの性能やネットワーク遅延等の影響は評価できていない。

### 3.1.2 ヒアリングの実施

#### (1) ヒアリング概要

本ユースケースにおける課題および課題の解決方法、検証するデータの種類、検証内容、合意内容、データのフロー、ユーザーインターフェースについて説明を行い、懸念事項や社会実装において障壁になる点、社会実装におけるファーストステップになると考えられる事項について、以下にヒアリングを行った。

- 公益社団法人日本アドバイザーズ協会 デジタルマーケティング研究機構
- 一般社団法人日本インタラクティブ広告協会（JIAA）プロジェクト・フェロー
- INCLUSIVE 株式会社（メディア側事業者）

## （２）ヒアリング結果

### ➤ ユースケース全体について

- 取り組みとしてはすばらしいが、すべてをすぐに社会実装することは難しい。社会実装のステップを分けて、できることから社会実装を行っていくことが考えられる。このユースケースでは、OPを提示していないと第三者へのデータの送信が行われない仕様となっているが、そのまま社会実装してしまうと、現状においてはほとんどのウェブサイトが正常に動作しなくなってしまう。最初のステップとしては、認証されている事業者かどうかの可視化を行う部分から始めていくのが良いのではないか。
- 一社が独占してこれらの機能を提供するのではなく、標準技術を用いて誰でもエコシステムに参加できるように実現を試みていることは、評価できる。
- 現状、JICDAQ の認証や JIAA への加入については、それぞれのウェブサイト会社名が表示されるだけであるが、これらの情報をOPとしてオンライン取引の中で利用できるインフラストラクチャとして期待できる。

### ➤ 審査機関によるサイト運営者、アドテク事業者の審査について

- 審査機関が審査するにあたり、どのような審査を行うかが課題となる。現状の JICDAQ の認証ではマネジメントシステムの認証をベースとしているが、このユースケースにおいて適切なものは検討が必要。
- DSP なのか SSP なのか等、事業形態によって審査項目も変わってくると考えられ、データの取り扱いについて審査するとなると、サービス約款なども審査する必要がある。JIAA のインフォメーションアイコンの審査では約款等の審査も行っている。
- 業界団体への加入時や更新時の審査がそのまま審査結果として用いることもできると考えられるため、業界団体加盟事業者であることの証明として利用することもできるのではないか。

### ➤ サイト閲覧者の UX/UI について

- エクステンションの初期設定時に DID や DWN 等の言葉が表示されるが一般には理解されない。社会実装においては、それらがどのようなものか説明するか、もしくはそれらを意識させないような UX にする必要がある。
- パーソナルデータの提供条件の事前設定においても、一般の利用者には意味がわからないと思われる。細かい設定を自分でするよりも、利用者の性格や属性に合わせて、自動で設定が行われるというような機能が考えられる。
- OP を設置したサイト運営者やアドテク事業者には、事前の設定に基づいてデータが提供され、都度確認が行われないため、クッキーバナー等による都度合意による UX の問題点にも対処しようとする趣旨は理解できるが、OP を設置してはいるが、自分としてはデータを提供



登録される。

- ② サイト閲覧者は非ボット証明発行機関に非ボット審査を請求する。
- ③ 非ボット証明が完了したら非ボット証明発行機関は非ボット証明をサイト閲覧者に発行する。  
この際、非ボット証明情報はブラウザエクステンション内に保存される。
- ④ サイト運営者およびアドテク事業者は CLI ツールを用いて自身の DID を発行し、ION に DID Document が登録される。(この DID をサイト運営者およびアドテク事業者のウェブサーバで公開する)
- ⑤ サイト運営者およびアドテク事業者は審査機関に審査を請求する。
- ⑥ 審査機関が審査を行い、審査機関サーバーで OP を発行し、サイト運営者およびアドテク事業者に渡す。(渡す手段は問わない)
- ⑦ サイト運営者は自身のウェブサーバに OP を .well-known 配下に公開する。
- ⑧ サイト閲覧者は、サイト訪問時に、サイト運営者ウェブサーバからサイト運営者およびアドテク事業者の OP を取得し検証する。
- ⑨ 検証が OK であれば、サイト閲覧者は、ブラウザエクステンションを通じてアクセスしているサイト (1<sup>st</sup> Party Domain) に提供する DID を発行し、その DID に紐づいた非ボット VC (※1)、広告識別子 VC、(ある場合は、メールアドレス VC) (※2) を DWN に登録し、当該サイト運営者およびアドテク事業者しかアクセスできないようにアクセス制御 (※3) を実施する。
- ⑩ サイト運営者およびアドテク事業者は、各 VC を取得し、検証を行う。

※1 非ボット VC の詳細な発行プロセスについては、3.1.1 (1) 企画・開発時の論点を参照

※2 広告識別子 VC、メールアドレス VC はサイト閲覧者によりブラウザエクステンションから発行される。

※3 アクセス制御の方法は、④で公開されているサイト運営者およびアドテク事業者の DID の秘密鍵を保有している者のみが当該情報にアクセスが可能となるように、DWN 上でアクセス制御を実施する。

### 3.2.2 データフローに登場する主体とその概要

- サイト閲覧者
  - 各種ウェブサイト閲覧する生活者、ボットではないことを証明したうえでウェブサイト閲覧し、パーソナルデータ (本ユースケースではメールアドレスと広告識別子を想定) の利用目的をサイト運営者およびアドテク事業者に伝える。
  - 役割: ボットではないことの証明書を保有し、パーソナルデータの利用目的を事前に設定する。閲覧するウェブサイトが正当なウェブサイトであることが検証できた場合には、事前設定された利用目的内のパーソナルデータをウェブサイト運営者に提供する。正当なウェブサイトであること

が検証できなかった場合には、都度パーソナルデータの利用目的をウェブサイト毎に設定する。

- サイト運営者

- ウェブサイトを運営する組織。いわゆるオンラインメディア事業者を想定している。公開するウェブサイトが正当な組織によって運営されているものであることを審査機関に審査してもらい、OPを発行してもらう。

- 役割：運営するウェブサイトサイトにサイト閲覧者が訪問した際に、サイト閲覧者が正当な閲覧者であることを検証し、パーソナルデータとその利用目的を受け取り利用する。サイト閲覧者のパーソナルデータの利用目的に従って、広告配信事業者やアクセス解析事業者に、ウェブサイトの情報とともに必要なデータを送信する。

- アドテック事業者（広告配信事業者・アクセス解析事業者）

- サイト運営者のウェブサイトを経由して取得したパーソナルデータを利用する組織。正当な組織であることを審査機関に審査してもらい、OPを発行してもらう。

- 役割：パーソナルデータを利用する正当な組織であることを証明し、サイト閲覧者が設定した利用目的（本実証の場合、広告とアクセス解析）でサイト運営者からの依頼に基づき、パーソナルデータを利用する。サイト閲覧者がボットでないことを検証できない場合は、そのデータは利用しない。正当な組織であることを証明できない場合は、基本的にサイト閲覧者のパーソナルデータを取得できない。

- 審査機関（非ボット証明発行機関含む）

- 以下の証明書を発行する、単一または複数の組織

- ① サイト運営者や広告配信事業者・アクセス解析事業者が正当であることを審査し、その証明書を発行する。本事業では、一般社団法人日本インタラクティブ広告協会や一般社団法人デジタル広告品質認証機構等の団体が審査機関としての役割を果たすものとして検討を行う。

- ② サイト閲覧者がボットではないことを審査し、その証明書を発行する。

- 役割：サイト運営者や広告配信事業者・アクセス解析事業者、サイト閲覧者から審査依頼を受け（依頼を受けず外形的に審査する場合もあると考えられる）、一定の基準に従って審査を行い証明書（OP）の発行、更新、停止を行う。

### 3.2.3 検証できる領域を拡大し、Trust を向上するために本システムで検証を行うデータ及びデータのやり取りの内容

- サイト閲覧者データの不正取得

以下のやり取りにより、表 1 で示した、サイト閲覧者の「どこに提供して良いか判断できない」という課題および、サイト運営者の「正当なアドテク事業者か判断できない」という課題を解決できる。

- ① 検証できる領域を拡大し、Trust を向上するために、検証が必要な課題  
正当性を検証できないウェブサイトやアドテク事業者による、サイト閲覧者データの不正取得。
- ② 検証対象（データ/データのやり取り）  
サイト運営者およびアドテク事業者。
- ③ 検証方法  
審査機関により発行されたサイト運営者およびアドテク事業者の O P を検証する。
- ④ 検証者  
サイト閲覧者が検証を行う。
- ⑤ データの保有者  
O P は審査機関が発行し、サイト運営者のウェブサーバに設置される。
- ⑥ 発行者  
審査機関が O P を発行する。
- ⑦ データの置き場所  
サイト運営者のウェブサーバ（対象ドメインの .well-known 配下）で公開する。
- ⑧ アクセスコントロールの手法  
O P は公開情報のためアクセスコントロールは行わない。
- ⑨ 成果・留意点  
実装・標準化が進められている O P を本実証に取り込むことができたことが成果。留意点としては、現在の O P のスキーマでは本実証のユースケースに完全に合致させることができなかったため、追加フィールドで対応した。



- ボットによるアドフroud（表 1：サイト運営者およびアドテク事業者の課題）

以下のやり取りにより、表 1 で示した、サイト閲覧者の「自分のどんなパーソナルデータがどこに提供されているのかわからない」という課題および、サイト運営者、アドテク事業者の「不正なサイト閲覧かどうか確認ができない」という課題を解決できる。

- ① 検証できる領域を拡大し、Trust を向上するために、検証が必要な課題  
サイト運営者やアドテク事業者が取得したデータの主体が人間であることを検証できないことにより、ボットによる閲覧数等の水増しなどの広告詐欺が起きている。
- ② 検証対象（データ/データのやり取り）  
サイト閲覧者。
- ③ 検証方法  
審査機関（非ボット証明発行機関）により発行された非ボット V C を検証する。
- ④ 検証者  
サイト運営者およびアドテク事業者。
- ⑤ データの保有者  
サイト閲覧者がデータの保有者となる。
- ⑥ 発行者  
審査機関が非ボット V C を発行する。
- ⑦ データの置き場所  
非ボット V C は DWN に保存される。
- ⑧ アクセスコントロールの手法  
DWN に対してアクセスコントロールを実施する。サイト閲覧者は非ボット V C の取得可能者の DID に対して閲覧権限を付与し、その DID を保有するサイト運営者やアドテク事業者だけがサイト閲覧者の DWN から取得することができる。
- ⑨ 成果・留意点  
D I F によって標準化が進められている DWN を実装できたことが成果。留意点としては DWN

のエンドポイント情報自体がサイト閲覧者の識別子として使われてしまう可能性があること。

#### 3.2.4 本システムで形成を目指す合意とその履行のトレースの内容

- サイト閲覧者の広告識別子の利用目的における合意

以下の合意により、表 1 で示した、サイト閲覧者の「自分のどんなパーソナルデータがどこに提供されているのかわからない」という課題を解決できる。

① 合意の主体

サイト閲覧者とサイト運営者、アドテク事業者

② 合意の対象

広告識別子の利用目的について合意する。

③ 合意の条件

OPによって検証できたサイト運営者およびアドテク事業者に対しては、事前に設定したパーソナルデータの利用目的（本事象では「広告」または「アクセス解析」）で利用されることに合意する。

検証できなかったサイト運営者およびアドテク事業者に対しては、都度ポップアップにより利用目的の確認を行うことにより、合意を行う。

④ トレースの対象

広告識別子の取得をトレースする。利用についてはトレースが困難。

⑤ トレースの主体

サイト閲覧者がサイト運営者およびアドテク事業者による広告識別子の取得をトレースする。

⑥ トレースの手法

サイト閲覧者が、DWNへのサイト運営者およびアドテク事業者からのアクセス（データ取得）を記録する。

⑦ 合意の取り消しの可否および方法

合意の取り消しは、サイト閲覧者がDWNに保存された広告識別子を削除することによって行う。また、削除された広告識別子は再利用されない。削除以前のデータについてダウンロードが

行われていた場合は、提供先にそのデータが残ってしまうが、削除後、広告識別子は収集されない（もしくは別の値になっている）ので、過去のデータに基づいた広告の配信やアクセス解析はできなくなる。

- サイト閲覧者のメールアドレスの利用目的における合意

以下の合意により、表 1 で示した、サイト閲覧者の「自分のどんなパーソナルデータがどこに提供されているのかわからない」という課題に加え、メールアドレスについてはその利用についてもトレースすることで、誰がパーソナルデータを利用しているかわからないという部分も解決できる。

- ① 合意の主体

サイト閲覧者とサイト運営者

- ② 合意の対象

メールアドレスの提供時はポップアップが表示され、提供先および利用目的（例えば、当社から新商品のお知らせを送信します等）について提示を行うため、メールアドレスの提供先および利用目的について合意する。

- ③ 合意の条件

都度ポップアップにより提供先および利用目的の確認を行うことにより、合意を行う。

- ④ トレースの対象

メールアドレスの取得および、メールアドレスへのメールの送信をトレースする。

- ⑤ トレースの主体

サイト閲覧者がサイト運営者によるメールアドレスの取得をトレースする。

Bunsin のサービスを利用している場合は、Bunsin のサービスにより、送信されてきたメールのトレースが可能

- ⑥ トレースの手法

サイト閲覧者が、DWN へのサイト運営者からのアクセス（データ取得）を記録する。

Bunsin のサービスを利用している場合は、Bunsin のサービスにより、提供先毎に異なったメールアドレスを生成し、提供先以外から当該メールアドレスにたいしてメールが送信されてきた場合に、不正を検知。

- ⑦ 合意の取り消しの可否および方法

合意の取り消しは、サイト閲覧者がDWNに保存されたメールアドレスを削除することによって行う。Bunsin を利用している場合、当該メールアドレス自体も無効化される。

### 3.3 6 構成要素との対応

#### 3.3.1 検証可能なデータ

##### (1) 検証対象

- ① サイト閲覧者非ボット証明[非ボット VC]
- ② サイト閲覧者広告識別子[広告識別子 VC]
- ③ サイト閲覧者メールアドレス[メールアドレス VC]
- ④ サイト運営者 Originator Profile[1st party OP]
- ⑤ アドテク事業者(広告配信事業者、アクセス解析事業者等)Originator Profile[3rd party OP]

##### (2) 検証者

- ① サイト閲覧者
- ② サイト運営者
- ③ アドテク事業者

#### 3.3.2 アイデンティティ

##### (1) アイデンティティとして想定されるもの

DID、VC、OP

##### (2) アイデンティティ管理システム

DID - ION

VC - DWN

OP - サイト運営者 web サーバー(.well-known)

##### (3) アイデンティティグラフとして想定されるものは何か

- サイト閲覧者からサイトをみたアイデンティティグラフ
  - (サイト閲覧者) -「ドメイン名」- (サイト) -「OP」- (OP 発行者)
- サイト閲覧者からアドテク事業者をみたアイデンティティグラフ
  - (サイト閲覧者) -「ドメイン名」- (アドテク業者) -「OP」- (OP 発行者)
- サイト・アドテク事業者からみたアイデンティティグラフ
  - (サイト・アドテク業者) -「ペアワイズ DID」- (サイト閲覧者) -「非ボット VC」- (非ボット VC 発行者)

### 3.3.3 ノード

#### (1) Wallet の使用有無

- ・ DWN 上では Wallet は使用してないが、サイト閲覧者については、metamask/eth-hd-keyring (「システムの構成要素」参照) を鍵管理に用いたクロームエクステンションにより DID の管理を行っている。
- ・ サイト運営者、アドテク事業者側では今回 Wallet の UI は提供しておらず、DID 発行スクリプトによって DID の発行を行っており、秘密鍵管理については実装していません。

#### (2) 合意形成がされているか、されている場合その手段

- ・ DWN には合意形成の結果、サイト閲覧者が誰に対し何の情報を取得可能にさせるかのアクセスコントロールを行っている。データ提供の合意は OP 検証成功による自動提供 or 提供の意志を確認する UI を用いてサイト閲覧者が DWN へのアクセスを許可する。詳細は 3.2.4

#### (3) データのやり取りの記録場所

- ・ Chrome エクステンションストレージ内
  - ② DWN にどのパーソナルデータを配置したか、という情報
- ・ DWN
  - ② DWN に対して誰がアクセスし、どのパーソナルデータを取得したか、という情報

### 3.3.4 メッセージ

#### (1) コネクションオリエンテッドかメッセージオリエンテッドか

- ・ OP の取得[リクエスト+レスポンス]
- ・ 非ボット VC の取得[リクエスト+レスポンス]
- ・ パーソナルデータの取得[リクエスト+レスポンス]
- ・ 非ボット VC の発行 [リクエスト+レスポンス]

### 3.3.5 トランザクション

#### (1) データのやり取りの記録・検証はできるか

- ・ サイト閲覧者がどの利用許諾に基づいて取得したかの履歴を閲覧可能
- ・ 一次アクセスについては履歴の閲覧が可能だがその後のノードを介さず第三者移転したトランザクションについては、Bunsin メールアドレスへの送信のみになる。

### 3.3.6 トランスポート

#### (1) トランスポートのプロトコル

- ・ HTTPS(REST API)
- ・ サイト閲覧者のデータについては DWN を介して https によってデータの Transport を行う。

OPについては、ドメイン配下の.well-known ディレクトリに op-document を配置し、https によってデータの Transport を行う。

### 3.3.7 その他

## 3.4 本実証で企画・開発したシステムの概要

### 3.4.1 業務フロー

- 添付 業務フロー.pdf 参照

### 3.4.2 ユースケース図

- 添付 ユースケース図.pdf 参照

### 3.4.3 操作画面 (UI)

操作画面については成果報告書概要版にて記載する。

### 3.4.4 機能一覧/非機能一覧

表 3.4.4 機能/非機能一覧

機能/非機能	機能名	機能概要
機能	DID 発行(サイト閲覧者)	サイト閲覧者がブラウザエクステンションセットアップ時に Root DID を発行する
機能	非ボット確認	サイト閲覧者が非ボット証明を受けた DID を審査機関内のシステムに保持する
機能	VC 発行	サイト閲覧者が Root DID に対して事前に非ボット証明を受けている前提で、その Root DID の秘密鍵で署名した JWT にペアワイズ DID を含めて VC 発行を審査機関に要求
機能	広告識別子提供	サイト閲覧者がメディア運営事業者やアドテク事業者に対して広告識別子を提供する
機能	メールアドレス提供	サイト閲覧者がメディア運営事業者やアドテク事業者に対してメールアドレスを提供する
機能	OP 発行	審査期間がサイト運営者、アドテク事業者の Originator Profile を発行する
機能	事業者 DID 発行	事業者が DID を発行して ION に登録する
機能	事業者のパーソナルデータ取得	サイト閲覧者から許可を得た、サイト運営者、アドテク事業者がパーソナルデータを DWN から取得する
非機能	サイト表示速度	各検証をサイトアクセス前に行うため、サイト表示速度について、問題がないか確認をする

### 3.4.5 データモデル定義(VC および OP)

表 3.4.5 データモデル定義

属性値	属性取得元	属性値 (VC または OP 内)
非ロボット証明	VC	notBot
広告識別子	VC	adId
メールアドレス	VC	mailAddress
URL	Originator Profile	url
サービス名	Originator Profile	name
郵便番号	Originator Profile	postalCode
住所(国)	Originator Profile	addressCountry
住所(都道府県)	Originator Profile	addressRegion
住所(市区町村)	Originator Profile	addressLocality
住所(番地号)	Originator Profile	streetAddress
事業領域	Originator Profile	businessCategory

### 3.4.6 実験環境

- 添付【DataSign】実験環境図\_別紙.pptx 参照

### 3.4.7 システムの構成要素

コンポーネント名称	型式 (製品の場合)	OSS か否か	ライセンス
ion-tools	@decentralized-identity/ion-tools	OSS	Apache-2.0
eth-hd-keyring	@metamask/eth-hd-keyring	OSS	ISC
dwn-sdk-js	@tbd54566975/dwn-sdk-js	OSS	Apache-2.0
did-jwt	did-jwt	OSS	Apache-2.0
did-jwt-vc	did-jwt-vc	OSS	Apache-2.0

## 3.5 実証を通じて得られた主な成果

### 3.5.1 システムの企画・開発に関する実証内容・得られた主な成果

対象	ペインポイント	成果	残された課題
----	---------	----	--------

サイト閲覧者	自分のどんなパーソナルデータがどこに提供されているのかわからない。	パーソナルデータはDWNに格納され、サイト閲覧者やアドテク事業者からのアクセスはアクセス履歴に記録される。	一次アクセスのみを記録するため、サイト運営者やアドテク事業者が取得したデータを第三者に渡すケースなどはトレースできない。
	どこに提供して良いか判断ができない。	審査機関から証明書（OP）の発行を受けたサイト運営者やアドテク事業者は一定の信頼が担保されるため、サイト閲覧者は自分で判断しなくてもよい。（公開鍵は審査機関ウェブサイト配下に公開されている）	審査機関や審査方法のトラストをどのように担保するかについては課題が残る。 また、審査を受けていないサイト運営者やアドテク事業者については自分で判断する必要がある。
サイト運営者	不正なサイト閲覧かどうか確認ができない	サイト閲覧者から非ボット VC を受け取ることで、検証に成功した非ボット VC に記載されている DID と広告識別子 VC に記載されている DID の突合せを行い、その他の広告識別子については集計対象外とすることで、不正なアクセスによるデータのノイズを除去することができ、正確なデータの活用が可能となる。	ボットを完全に排除できるわけではない。（非ボット VC を受領したブラウザ環境をそのままボット化する等）
	正当なアドテク事業者か判断できない	アドテク事業者から「正当なアドテク事業者である OP」を受領し、検証することで、不正なアドテク事業者にデータが渡ることを防ぐことができる。	審査機関や審査方法のトラストをどのように担保するかについては課題が残る。
アドテク事業者	不正なサイト閲覧かどうか確認ができない	サイト閲覧者から非ボット VC を受け取ることで、検証に成功した非ボット VC に記載されている	審査機関や審査方法のトラストをどのように担保するかについては課題が残る。



		DID と広告識別子 VC に記載されている DID の突合せを行い、その他の広告識別子については集計対象外とすることで、サイト運営者によるアドフraudや不正なアクセスによるデータのノイズを除去することができ、正確なデータの活用が可能となる。	
--	--	--	--

以下その他の成果

- DID/VC/DWN/OP を用いて、オンラインマーケティングにおけるパーソナルデータの流通に対し、現在の課題を解決し得ることを実際にシステムを構築することを通じて実証することができたこと。
- サイト閲覧者の提供情報(非ボット証明、広告識別子、メールアドレス)を VC で管理することにより DWN で、アクセス制御や提供履歴管理ができたことで、DWN+VC という現在注目されている標準技術を用いたユースケースを提案でき、Trusted Web における DWN の活用に限らず Web5 等も含めた、今後の技術の発展に寄与ができること。
- Originator Profile を使用して組織の認証を行うことで、今後汎用的となりうる仕組みの上で管理できる可能性があり、また、現状の OP に対して不足している部分等をフィードバックすることで、より多くのユースケースで OP が利用されるような貢献ができることが成果として考えられる。
- DID、VC、や DWN のライブラリは開発途上のものが多く実装されていない機能や、定まっていないルールが散在しており現時点での開発は困難なものが多かったが、これらを利用した機能を実現できたことで、標準化された仕様を具体的なコードとして実装することで、現在公開されているオープンソースのコードに不足している部分や補う必要がある部分に気づいた。また、これらの補う必要がある部分を補完したコードを公開することで、コミュニティに貢献ができることが分かった。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

- 組織認証(OP の profile set)については、Originator Profile 技術研究組合と連携し、今後のビジネスモデルの基礎となる組織認証について足並みを揃えることができたこと。  
具体的には、Originator Profile の技術仕様を開示いただき、技術仕様に沿って、OP を生成、配置するように、開発を行った。必ずしも本ユースケースが Originator Profile 技術研究組合が主眼を置くユースケースでは無いため、その点においても、OP の汎用性を示すことができるのではないか。

### 3.6 本実証で開発したシステムの第三者による再現可能性（A 類型のみ）

- 本実証事業で企画・開発したコードは、全てオープンソースとして Github 上に公開することで、第三者が再構築することによって再現可能である。また、DID wallet や DWN のシステムは本ケースに限らず、様々な分野で活用がなされることが想定されるため、DID wallet や DWN はモジュールとして切り出し、それぞれオープンソースで公開することを予定している。

## 4 実証終了後の社会実装に向けた見通し

### 4.1 社会実装時に想定しているビジネスモデル・ユーザーのメリット

想定しているビジネスモデルは、サイト閲覧者がエンドユーザーとなり、本ユースケースで必要となるエクステンションや DWN、非ボットの審査を行う、サービス提供者が当該サービスを提供し、エンドユーザーがサービス利用料を支払うことを想定している。ただし、これらの機能自体がビジネスモデルを構築するというよりは、これらの機能を生かした別のビジネスモデルを、各サービス提供者がそれぞれ構築する競争領域になる。

また、組織審査機関（OP の Issuer）に対し、サイト運営者やアドテク事業者が、審査費用を支払うことを想定している。現状でも広告関連団体への加盟料を支払っているため、その一部または追加料金が審査費用として利用されることが考えられる。

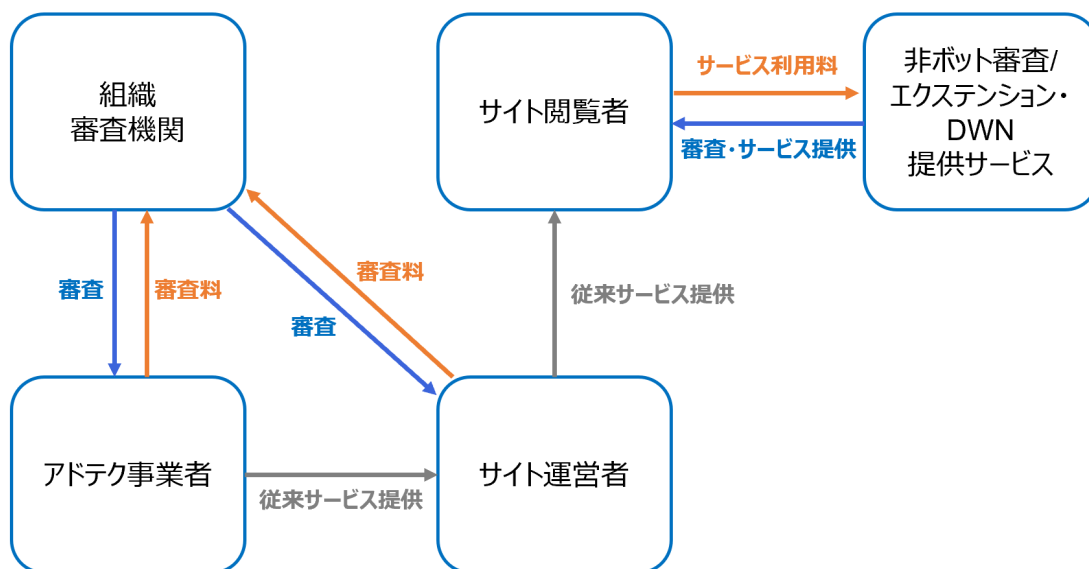


図 4.1.X ビジネスモデル

表 4.1.X 各ステークホルダのベネフィット及び想定している利用料

ステークホルダ	ベネフィット	負担するコスト
組織審査機関（OP の Issuer）	業界団体が審査機関になることが考えられるため、その業界（今回のユースケースの場合アドテク業界）のエコシステムの改善につながることをベネフィットと考えられる。	OP 発行サーバ運用コスト（月 10 万円程度）
サイト運営者 / アドテ	アド Fraud への対応を簡略化し、アド	審査料（年 10～20 万円程）

ク事業者	フラウド対策コストを低減させ、かつアドフラウド自体を減らすことができ、広告主にとっても間接的に余分な広告費を支払う必要が無くなる。	度)
サイト閲覧者	知らぬ間に、自分のデータが横断的に収集されることがすくなくなり、本人の権利利益の侵害が起きにくくなる。	各サービス提供者のビジネスモデル次第（無料～月 5000 円程度）
エクステンションや DWN、非ボットの審査を行う、サービス提供者	新たな仕組みが構築されることによるビジネス機会	ビジネスモデル次第

#### 4.2 実証を通じて判明したユースケースの課題とその解決方針

対象	ペインポイント	成果	残された課題	解決方針
サイト閲覧者	自分のどんなパーソナルデータがどこに提供されているのかわからない。	パーソナルデータは DWN に格納され、サイト閲覧者やアドテク事業者からのアクセスはアクセス履歴に記録される。	一次アクセスのみを記録するため、サイト運営者やアドテク事業者が取得したデータを第三者に渡すケースなどはトレースできない。	第三者に渡されたことを完全にトレースすることはほぼ不可能だが、一部 Bunsin メールアドレスで実現しているように、利用されたときに検知できる仕組みをその他のパーソナルデータでも実装していくことが考えられる。
	どこに提供して良いか判断ができない。	審査機関から証明書（OP）の発行を受けたサイト運営者やアドテク事業者は一定の信頼が担保されるため、サイト閲覧者は自分で判断しなくてもよい。	審査機関や審査方法のトラストをどのように担保するかについては課題が残る。 また、審査を受けていないサイト運営者やアドテク事業者については自分で判断する必要がある。	広告業界の営利事業者のみで構成される業界団体による審査ではなく、マルチステークホルダーにより構成される審査機関を設置することが望ましい。

対象	ペインポイント	成果	残された課題	解決方針
サイト 運営者	不正なサイト 閲覧かどうか 確認ができな い	サイト閲覧者から「非ボ ット VC」を受領し検証す ることによって不正なアクセスに よるデータのノイズを除去 することができ、正確なデ ータの活用が可能とな る。	ボットを完全に排除でき るわけではない。(非ボ ット VC を受領したブラ ウザ環境をそのままボッ ト化する等)	都度生体認証を行う などの方法が考えられ るが、アクセスするた びに生体認証を求めら れることは、本ユース ケースにおいては、UX においても不便なもの となってしまったため、現 状の方法が現時点に おいては最適であると 考えられる。
	正当なアドテ ク事業者か判 断できない	アドテク事業者から「正 当なアドテク事業者であ るOP」を受領し、検証 することで、不正なアドテ ク事業者にデータが渡る ことを防ぐことができる。	審査機関や審査方法 のトラストをどのように担 保するかについては課 題が残る。	広告業界の営利事 業者のみで構成され る業界団体による審 査ではなく、マルチス テークホルダーにより構 成される審査機関を 設置することが望まし い。
アドテク 事業者	不正なサイト 閲覧かどうか 確認ができな い	サイト運営者によるアドフ ラウドや不正なアクセスに よるデータのノイズを除去 することができ、正確なデ ータの活用が可能とな る。	審査機関や審査方法 のトラストをどのように担 保するかについては課 題が残る。	広告業界の営利事 業者のみで構成され る業界団体による審 査ではなく、マルチス テークホルダーにより構 成される審査機関を 設置することが望まし い。

- その他課題①：エンドユーザー（もしくは巨大プラットフォーマー）に対するメリットの訴求。  
本ユースケースにおいて課題と設定している事項が、エンドユーザー（サイト閲覧者）に認識されておらず、この課題が解決されることに対するメリットの訴求が難しい。巨大プラットフォーマーがこれらの仕組みをブラウザ等に組み込むことで、エンドユーザーに普及することが最も近道であるため、国際標準化等の取り組みが重要であり、OP はそれに向けた検討を行っているため、サポートするために無

理をして採用した。

ただし、OP による検証はまだしも、DWN や DID 等、巨大プラットフォームが分散型のデータ流通についてメリットを見出すことは考えにくい（見出すとしたら分散化したものの再集約）ため、本質的な課題の解決を行うためにはチャレンジを続けるしかなく、多くのチャレンジの中から、これらの仕組みをベースとしたキラーアプリが世の中に現れ、普及する道筋しか見えないため、チャレンジを続ける。

- その他課題②：組織が審査を受けるメリット

本ユースケースの仕組みが普及しないと、審査を受けるメリットが弱く、審査を受ける事業者が多くなると、この仕組みを採用するメリットが弱い。そのため、新たな認証制度を設けるのではなく、現在行われている認証制度を OP 化する（例えば広く普及している ISMS や P マークなど）等の進め方を考える必要がある。

- その他課題③：審査を受けないサイト運営者 / アドテク事業者の扱い

本ユースケースにおいて、審査を受けないサイト運営者、アドテク事業者については、都度ポップアップにて合意を行うことになるが、OP が普及していない現時点においては、ほとんどのサイトでポップアップによる合意が必要になってしまうため、サイト閲覧者が煩わしいと感じ、仕組み自体を利用しなくなってしまう可能性が高い。

そのため社会実装時においては、ポップアップによる合意が必要となるケースを少なくするなど、工夫が必要となる。

#### 4.3 本ユースケースの社会実装に向けたマイルストーン

- 本ビジネスモデルの社会実装については、令和 6 年度まで継続的な実証を行い、令和 7 年度以降の商用化を想定している。前述の課題②③については、令和 6 年度上半期まで対応を行い、広告関連団体や Originator Profile 技術研究組合との調整を行い、方針を決定することを予定している。令和 7 年度のサービス開始当初は、広告エコシステムを対象としてサービスを提供するが、令和 8 年度以降は、対象領域を広げていく。課題①への対応は継続的に行っていく必要がある。


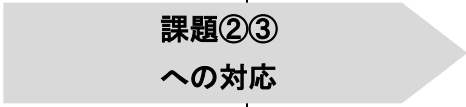
	(今年度) R4 年度	R5 年度	R6 年度	R7 年度
プロトタイプシステムの企画・開発				



図 4.3 .X 社会実装に向けたマイルストーン

## 5 Trusted Web に関する考察

### 5.1 Trusted Web のアーキテクチャに関する課題と提言

- ・ 課題・提言：6 構成要素のうち、現在のインターネット/Web にあるものは何か、無いものは何かを示してほしい。  
詳細：例えばホワイトペーパー内のアイデンティティの項において「その管理を自らの制御下に置くことができる技術を活用できる」と記載されているが、Facebook や Google から提供されるアイデンティティも自ら制御はできないわけでは無いともとれる。プラットフォーム中心のウェブでは 6 構成要素のうちどれがどのような観点で足りていないのかもしくは、Passkey 等の実装によってどの部分が足りてきたのか、等の論点が欲しい。
- ・ 課題・提言：単純に 6 構成要素で使われている言葉の理解は難しい。  
詳細：例えば検証可能なデータの説明において「Trusted Web での操作の対象となるデータを、検証可能性の視点での特性を手がかりにして整理したもの、および、それについての操作を含む。」という文章の中でも「検証可能性の視点での特性」とは何なのか、それを「手がかりに」とするのはどういうことなのか、単に「デジタル署名によって検証できるデータ」が検証可能なデータではないのかよくわからない。
- ・ 課題・提言：勉強会での「「検証可能性を担保できる」のであれば技術の組み合わせに制約は無い」という部分に関して、ホワイトペーパーからはそれを読み取れない。  
詳細：例えば、ホワイトペーパー内の「それぞれのエンティティ（人、法人等）は、複数のアイデンティティを持ち、使い分けられる」という点は、検証可能性とは別の議論ではないか。
- ・ 課題・提言：European Digital Identity Wallet との比較  
詳細：European Digital Identity Architecture and Reference Framework で公開されているアーキテクチャに対する Trusted Web への当てはめ、比較を行ってほしい。
- ・ 課題・提言：Trusted Web のオープンソースプロジェクト  
詳細：Trusted Web のアーキテクチャを実現するオープンソースプロジェクトを開始し、Trusted Web 参加希望者がだれでも利用できるよう SDK を提供してはどうか。

### 5.2 その他 Trusted Web の課題と提言

- ・ 課題・提言：ユーザーによるコントロールとリテラシー  
詳細：ユーザー自身によるデータのコントロールについて、しっかりコントロールできるほど、操作が



煩雑になり、また、ユーザーのリテラシーを求めるものになってしまう。この課題に対し、本ユーザーズでは、OP によって検証できた組織に対しては、事前の合意設定に応じて自動的にデータが提供される設計とした。

- ・ 課題・提言：ユーザーのプライバシー  
詳細：ユーザーのプライバシーを Trusted Web としてどのように担保すべきか、という議論をすべきである。今後の課題として、「セキュリティ」の中でプライバシーバイデザインについて触れられているものの、セキュリティの中のプライバシーという位置づけでは無く、プライバシーについても主題として検討されるべき。特に公開されることが前提となるような公開鍵についてのプライバシーリスク等については各国の法制度との関連を含め、整理し、Trusted Web としての方向性を示してほしい。
- ・ 課題・提言：法制度の整備  
詳細：Trusted Web に関連する法制度を洗い出し、必要な改正等について提言を行うべきである。今後の課題として「仕組みの普及について」の中で「法令等で利用を義務付けることは難易度が高い」との記載があるが、Trusted Web を普及させるにあたって、大規模プラットフォームには一定の義務を設けるなどの検討を行っても良いのではないか。
- ・ 課題・提言：インセンティブ  
詳細：インセンティブについて、現在のインターネット・ウェブがどのようなインセンティブによって成り立っているのか、を整理し、Trusted Web で考えられるインセンティブを考察する等を行ってほしい。（例えば、DNSSEC の普及にはどのようなインセンティブ設計がなされているか、等）
- ・ 課題・提言：パーソナルデータに関わる部分とそうでない部分の分離  
詳細：ホワイトペーパー内においてパーソナルデータに関わる部分と、関わらない部分で分けたほうが良いのではないか。アーキテクチャにおいても特に分かれていないため、分かりにくくなっている部分もあると感じた。