

令和3年度補正予算Trusted Web共同開発支援事業費
「Trusted Webの実現に向けたユースケース実証事業」
最終報告書概要版

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

株式会社DataSign

2023年3月20日

目次

1. 背景・目的
2. 事業の概要
 - 2.1 事業概要及び実証の範囲
 - 2.2 社会・経済に与える価値・影響
 - 2.3 コンソーシアムの体制
 - 2.4 実証全体のスケジュール
3. 実証内容
 - 3.1 実証の実施事項、論点及び判断
 - 3.2 検証できる領域を拡大する仕組み
 - 3.3 6構成要素との対応
 - 3.4 本実証で企画・開発したシステムの概要
 - 3.5 実証を通じて得られた主な効果
 - 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）
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
 - 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
 - 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
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
 - 5.2 その他Trusted Webの課題と提言

01

背景·目的

1. 背景・目的

1.1 背景・目的

背景

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企業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企業に収集・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結果に影響を与え、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企業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企業にとっても、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。

目的

背景を踏まえ、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企業の正当性の検証や、データそのものの正当性の検証を可能にし、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、企業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。

1.2 課題と解決する内容

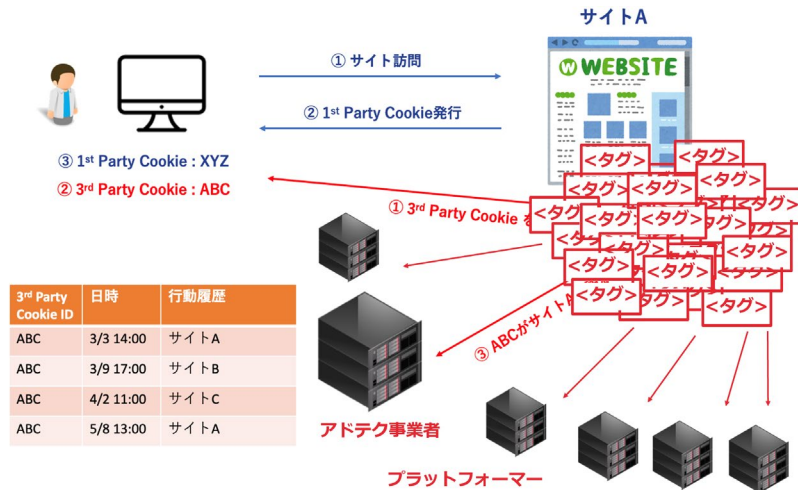
現在の課題（ペインポイント）

- ① 生活者は知らないうちに、自分のパーソナルデータが不正な第三者によって取得・利用されている。
- ② サイト運営者は、サイト訪問者の情報が、第三者によって窃取されており、適切な制御ができていない。
- ③ アドテック事業者は、広告効果があるように見せかけるボット等の存在によって、広告詐欺などの被害が出ている。

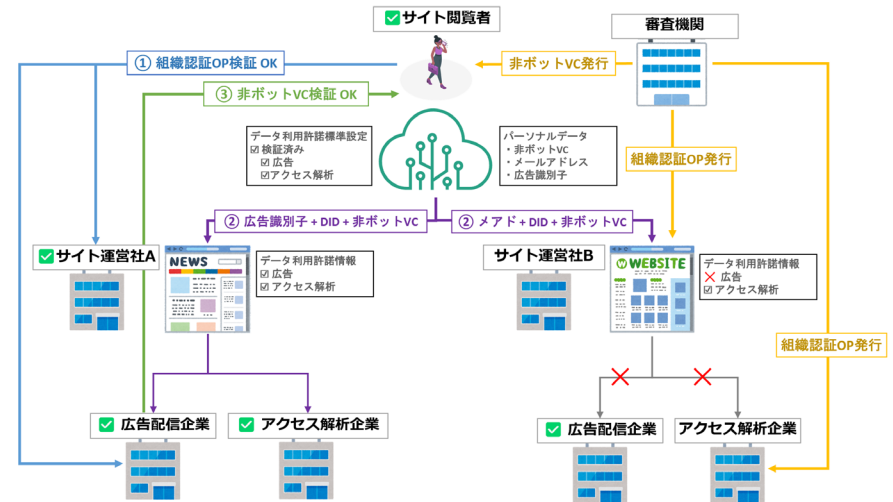
TrustedWebの実現により解決する内容

- ① 生活者個人がオンラインマーケティングで利用される識別子と提供先を管理
- ② それぞれが第三者からの証明書を持ち、お互いに確認・検証しあう
- ③ 相手方の正当性を確認、検証できない場合は、都度合意を行う

課題解決前のスキーム図（As-Is）



本実証ユースケースのスキーム図（To-Be）



02

実証の概要

2. 事業の概要

2.1 実証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」、ウェブサイトへ広告を配信する「広告配信企業」、ウェブサイトのアクセス解析を行う「アクセス解析企業」（「広告配信企業」「アクセス解析企業」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分からない、分かったとしてもそれが正当な事業者なのかわからない、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。

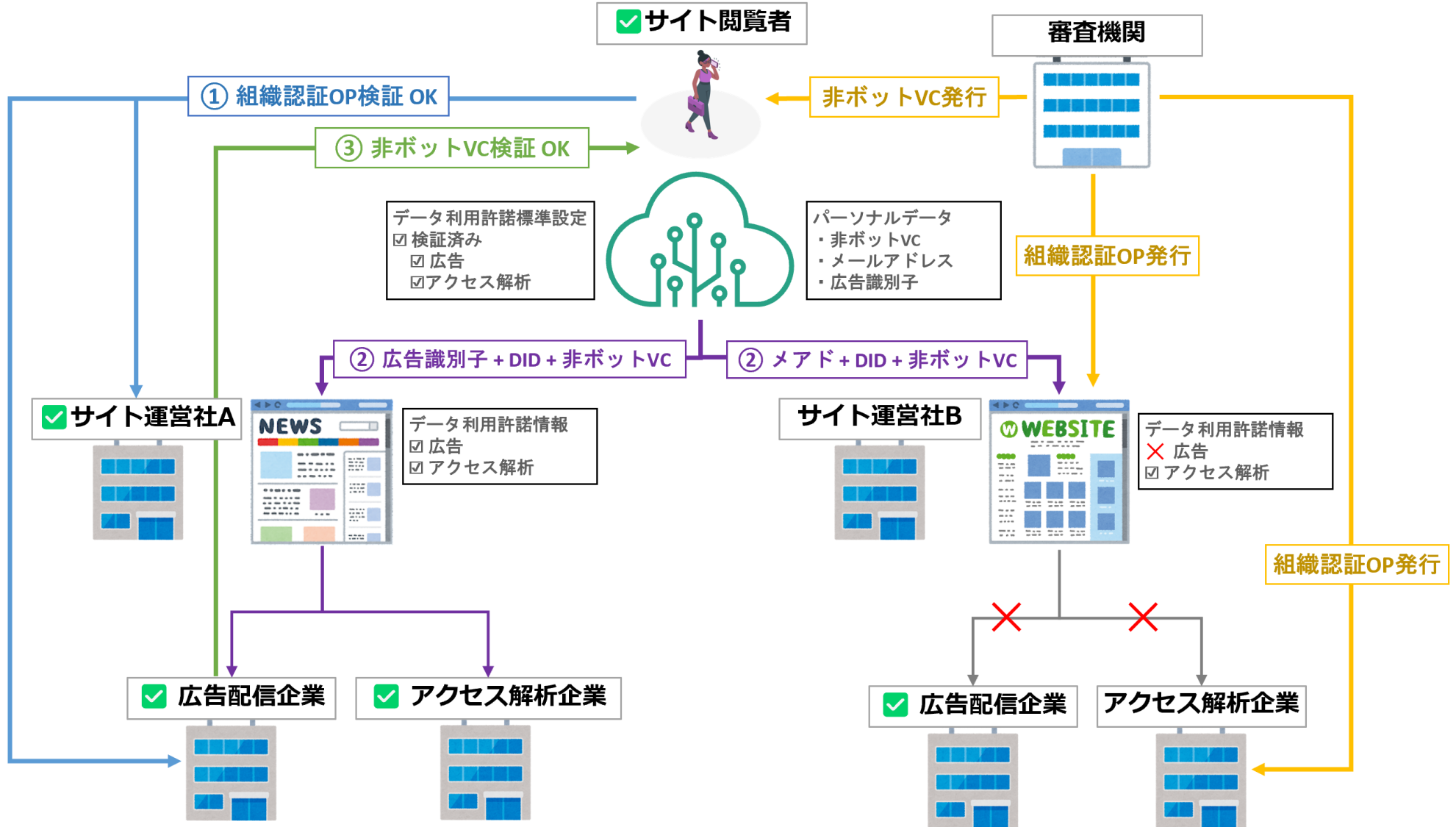
この課題を解決するために、審査機関が正当性を証明するVerifiable Credentialを各エンティティに発行し、各エンティティ間で確認・検証しあうことにより、上記の課題を解決していきたい。

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範囲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。

2. 事業の概要

2.1 実証概要及び実証の範囲



2. 事業の概要

2.1 実証概要及び実証の範囲

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">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。どこに提供して良いか判断ができない。	自らのパーソナルデータの開示範囲や利用範囲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、企業）において取り扱われているかを追跡（もしくはデータ自体を無効化）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">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「ボットじゃない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">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VC」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">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。

2. 事業の概要

2.2 社会・経済に与える価値・影響

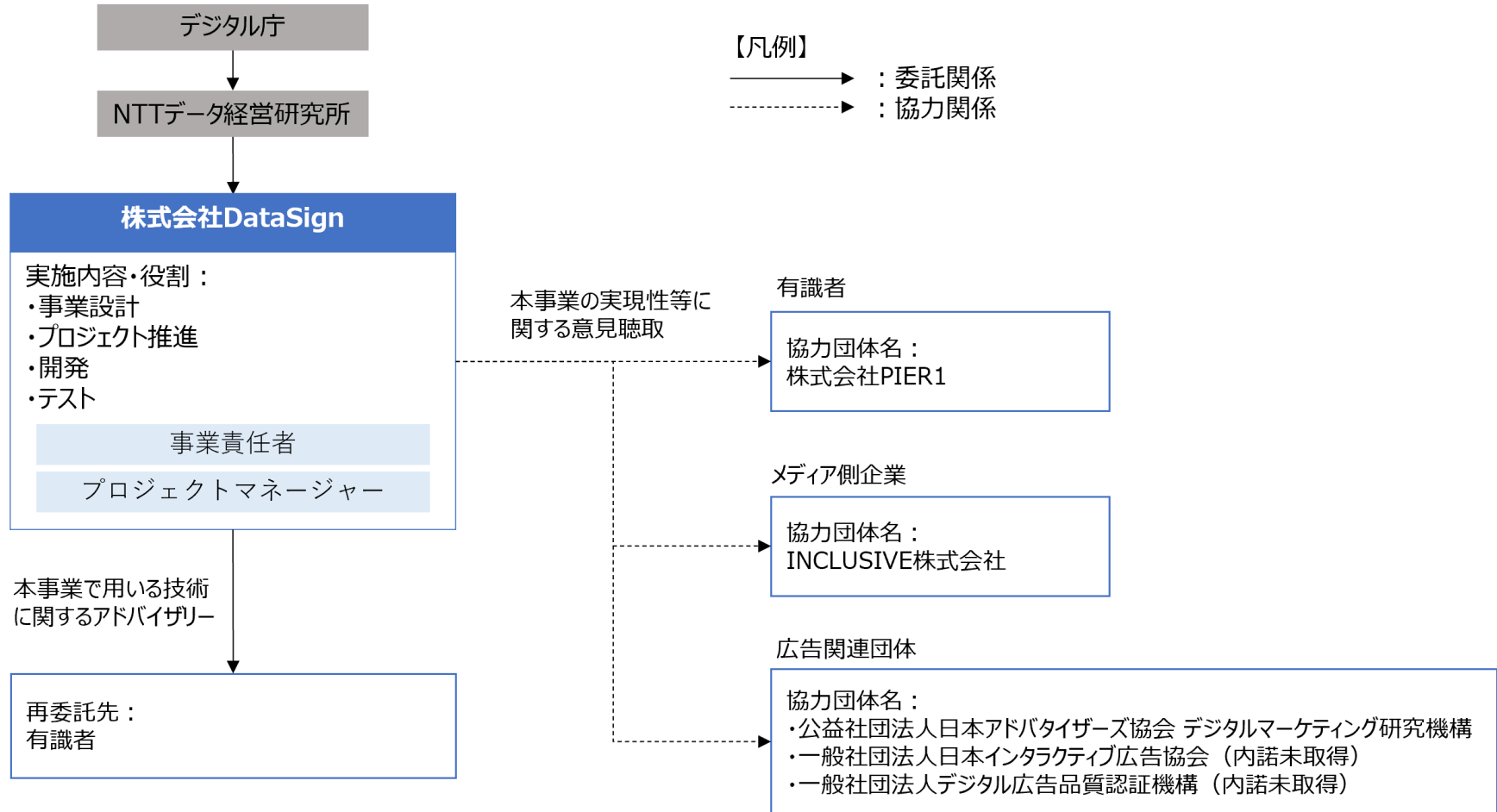
国内のインターネット広告の市場規模は、電通の発表する日本の広告費によれば2兆7,052億円とされ年20%以上の成長をしている。ただし、パーソナルデータの利活用に関して、どのように生活者の関与を実現するかが大きな課題となり、プラットフォームの独断的な判断により、広告識別子が利用できなくなるなど、公平公正なビジネス環境とは言い難い状況になっている。

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。

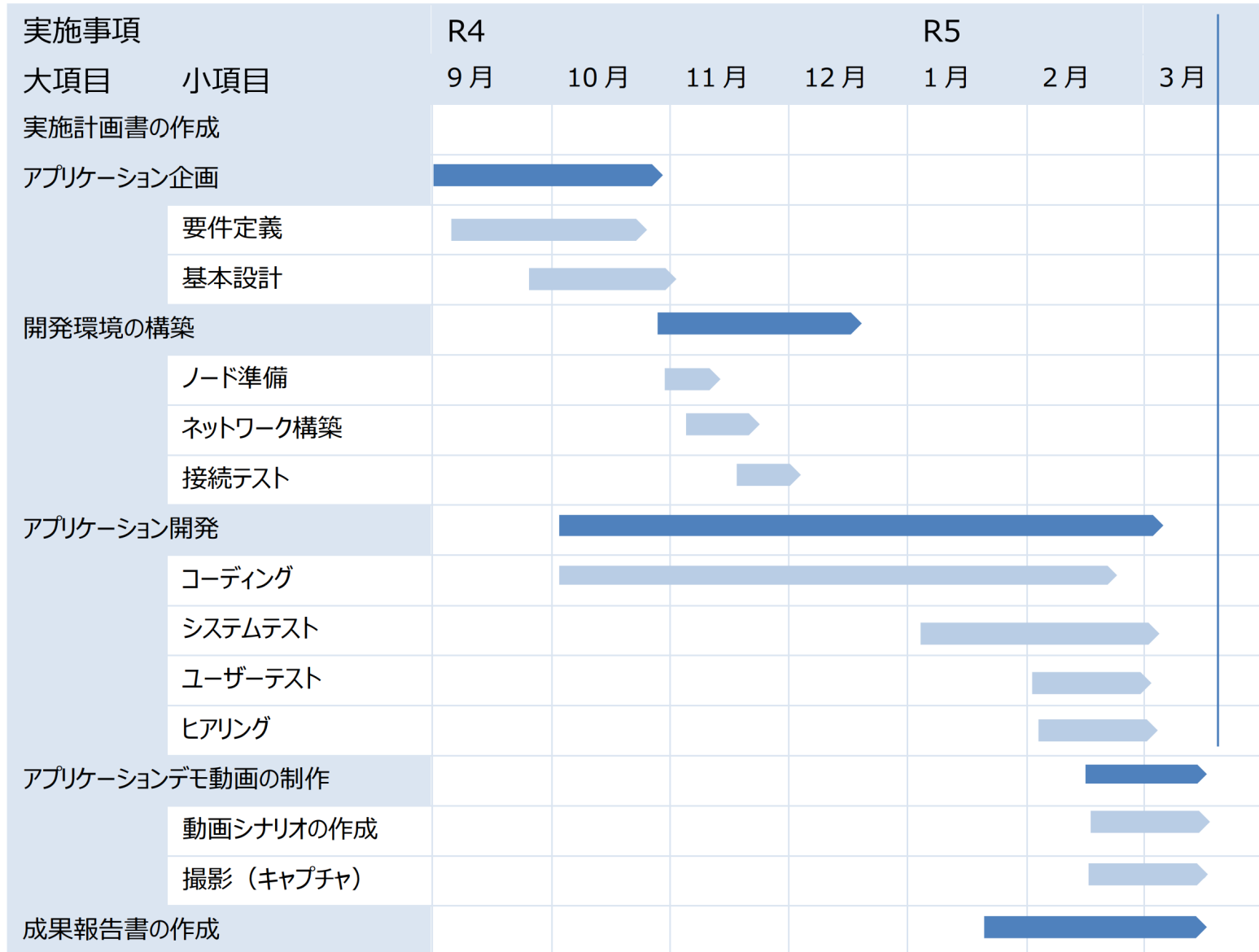
このような状況の中で、Trusted Webとして、パーソナルデータの利活用に対し生活者の関与を強め、検証できる領域を広めて、オンラインマーケティング全体のTrustを向上させ、生活者にとっても、サイト運営者にとっても、アドテック事業者にとっても公平公正なビジネス環境を構築することで、より多くの信頼性の高いパーソナルデータが活用できるようになり、利用者にとって真に価値のあるサービスが開発されていくことが期待される。

2. 事業の概要

2.3 コンソーシアムの体制



2.4 実証全体のスケジュール



03

実証内容

3. 実証内容

3.1 実証の実施事項、論点及び判断 (1/3)

プロトタイプシステムの企画・開発

実施事項	論点	判断
DIDについて	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。 B : サイト閲覧者のアクセスしているサイト (1st Party Domain) 毎にDIDを発行する。	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、広告識別子として少なくとも、1st 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、Bのデメリットは無くなり、Aのデメリットのみが残ってしまうため、Bで実装することとした。
広告識別子について	A : 1st 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、必ずしも利用者がその事実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をしてもらうこととした。
DWNについて	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のではなく、データ取得の履歴を残すトレース機能なども考えるとDWN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。

3. 実証内容

3.1 実証の実施事項、論点及び判断 (1/3)

プロトタイプシステムの企画・開発

実施事項	論点	判断
組織認証証明書について	VCを用いるか OPを用いるか	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を利用したほうが今後のインターオペラビリティを鑑みてもメリット大きいと判断し、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	ペアワイズDIDに対する非ボットVCの発行方法	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、前述の通り、DIDはアクセスしているサイト（1st 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う、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。

3. 実証内容

3.1 実証の実施事項、論点及び判断 (3/3)

記載例)

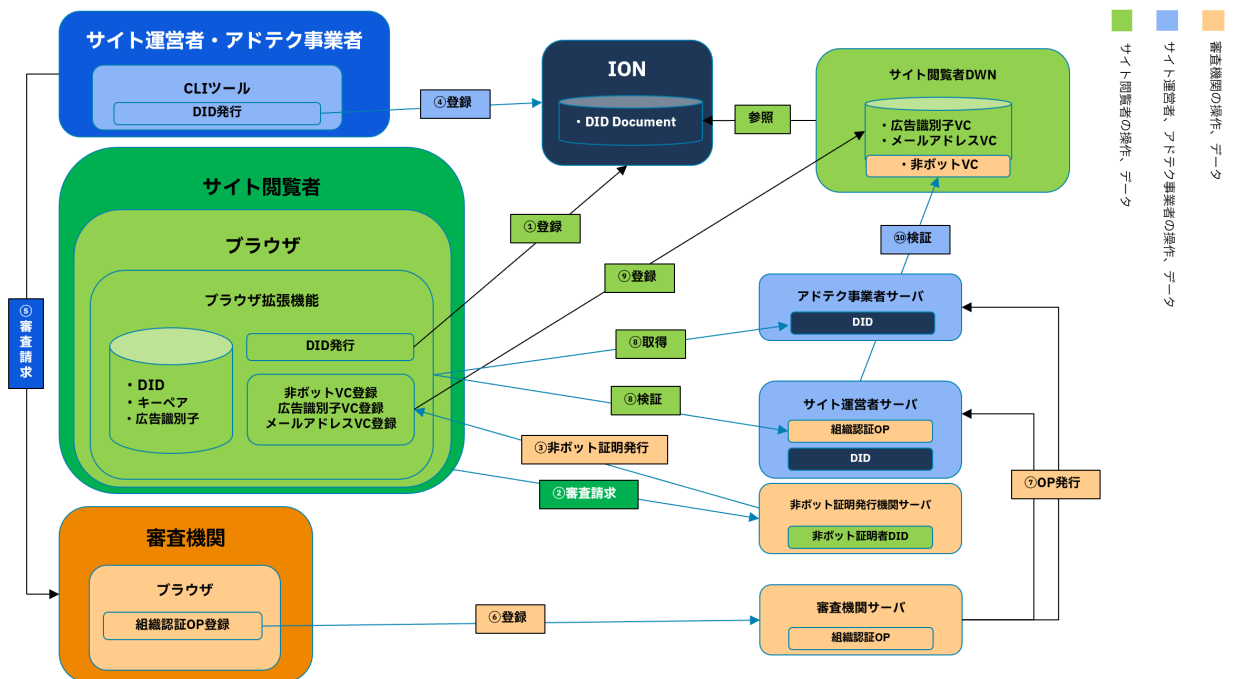
国際標準規格の調査

調査事項	調査対象機関	調査結果
DIDについての調査	W3C	別紙、DID_VC調査資料.pdf 参照
VCについての調査	W3C	
DWNについての調査	DIF	

3. 実証内容

3.2 検証できる領域を拡大する仕組み（1/3）

データスキーム図



データへのアクセス

- 審査機関が、サイト運営者およびアドテク事業者の審査を行い、OPを発行し、ドメイン配下で公開することで、そのドメインが審査機関による審査に合格した組織によって運営されていることを検証でき、非ボット証明発行機関が、サイト閲覧者の審査を行い、非ボットVCを発行し、サイト閲覧者がDWNを介してサイト運営者およびアドテク事業者に提供し、非ボットであることを検証できるようにすることで、双方向に検証できる領域を拡大している。フローは以下を参照。

登場する主体とその概要

主体	役割・設定
サイト閲覧者	各種ウェブサイトを開覧する生活者、ボットではないことを証明したうえでウェブサイトを開覧し、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）の利用範囲をサイト運営者およびアドテク事業者に伝える。
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企業を想定している。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。
アドテク事業者	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。
審査機関	組織認証証明書および非ボット証明書を発行する、単一又は複数の組織。

3. 実証内容

3.2 検証できる領域を拡大する仕組み（2/3）

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

要検証の課題	検証対象	検証方法	検証者	保有者	発行者	データの置き場	アクセスコントロールの手法	成果・留意点
サイト閲覧者データの不正取得	サイト運営者およびアドテク事業者	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OPを検証する。	サイト閲覧者が検証を行う。	OPはサイト運営者のウェブサーバに設置される。	審査機関がOPを発行する。	サイト運営者のウェブサーバで公開する。	OPは公開情報のためアクセスコントロールは行わない。	実装・標準化が進められているOP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OPのスキーム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。
ボットによるアドクラウド	サイト閲覧者	非ボット証明発行機関により発行された非ボットVCを検証する。	サイト運営者およびアドテク事業者。	サイト閲覧者がデータの保有者となる。	審査機関が非ボットVCを発行する。	非ボットVCはDWNに保存される。	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VC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。	DIF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. 実証内容

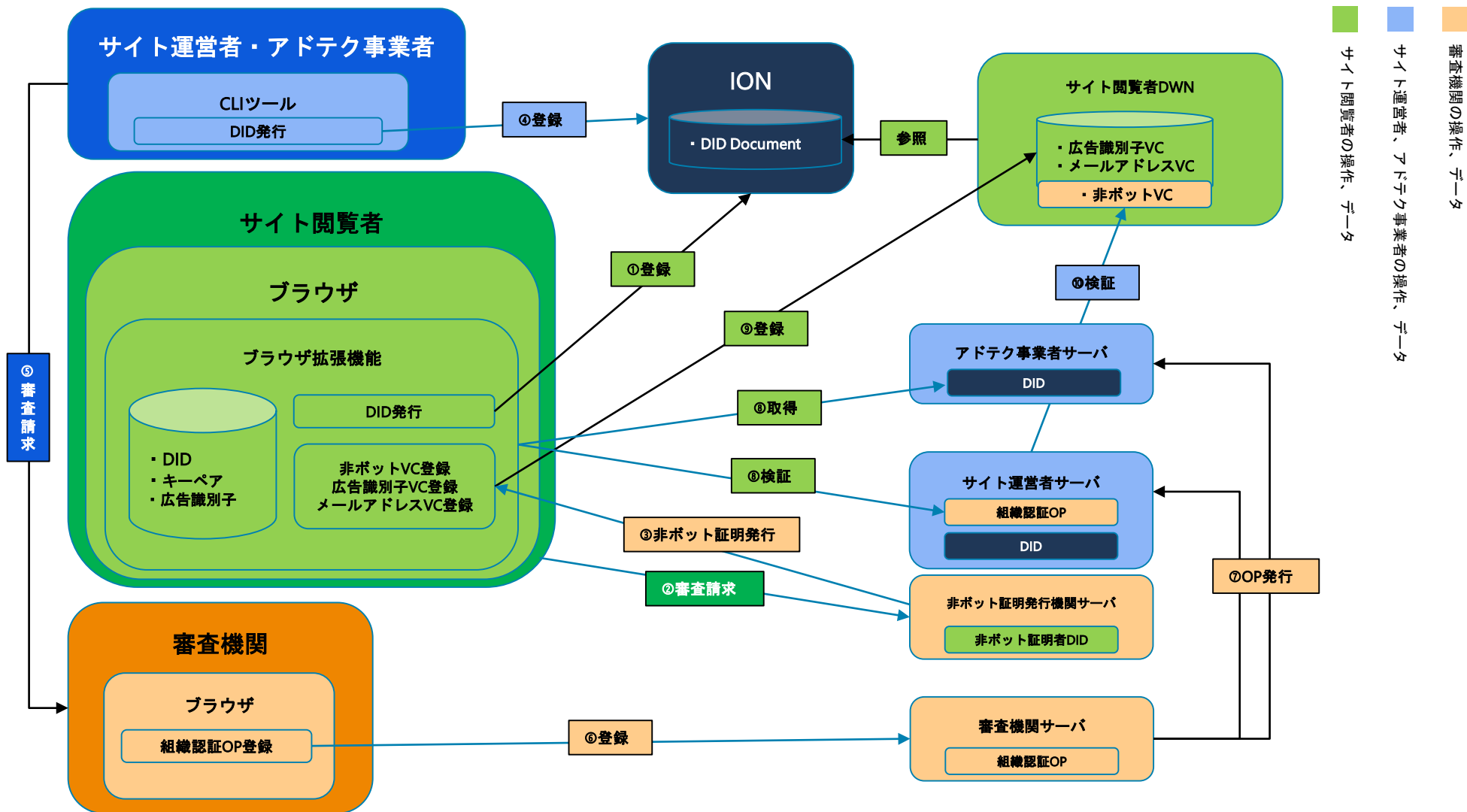
3.2 検証できる領域を拡大する仕組み（3/3）

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

合意の主体	合意の対象	合意の条件	トレースの対象	トレースの主体	トレースの手法	合意取り消しの可否・方法
サイト閲覧者とサイト運営者、アドテク事業者	広告識別子の利用範囲について合意する。	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範囲（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範囲の確認を行うことにより、合意を行う。	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。	サイト閲覧者	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。	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。
サイト閲覧者とサイト運営者	メールアドレスの利用範囲について合意する。	都度ポップアップにより利用範囲の確認を行うことにより、合意を行う。	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。	サイト閲覧者	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、提供先毎に異なる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。	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。

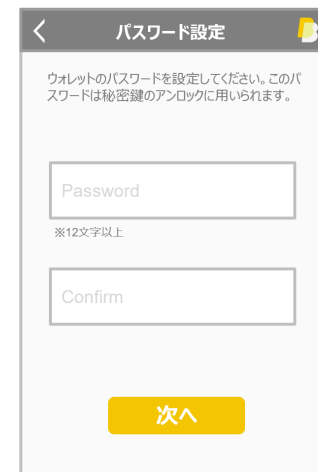
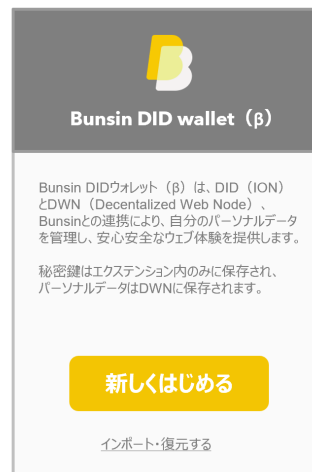
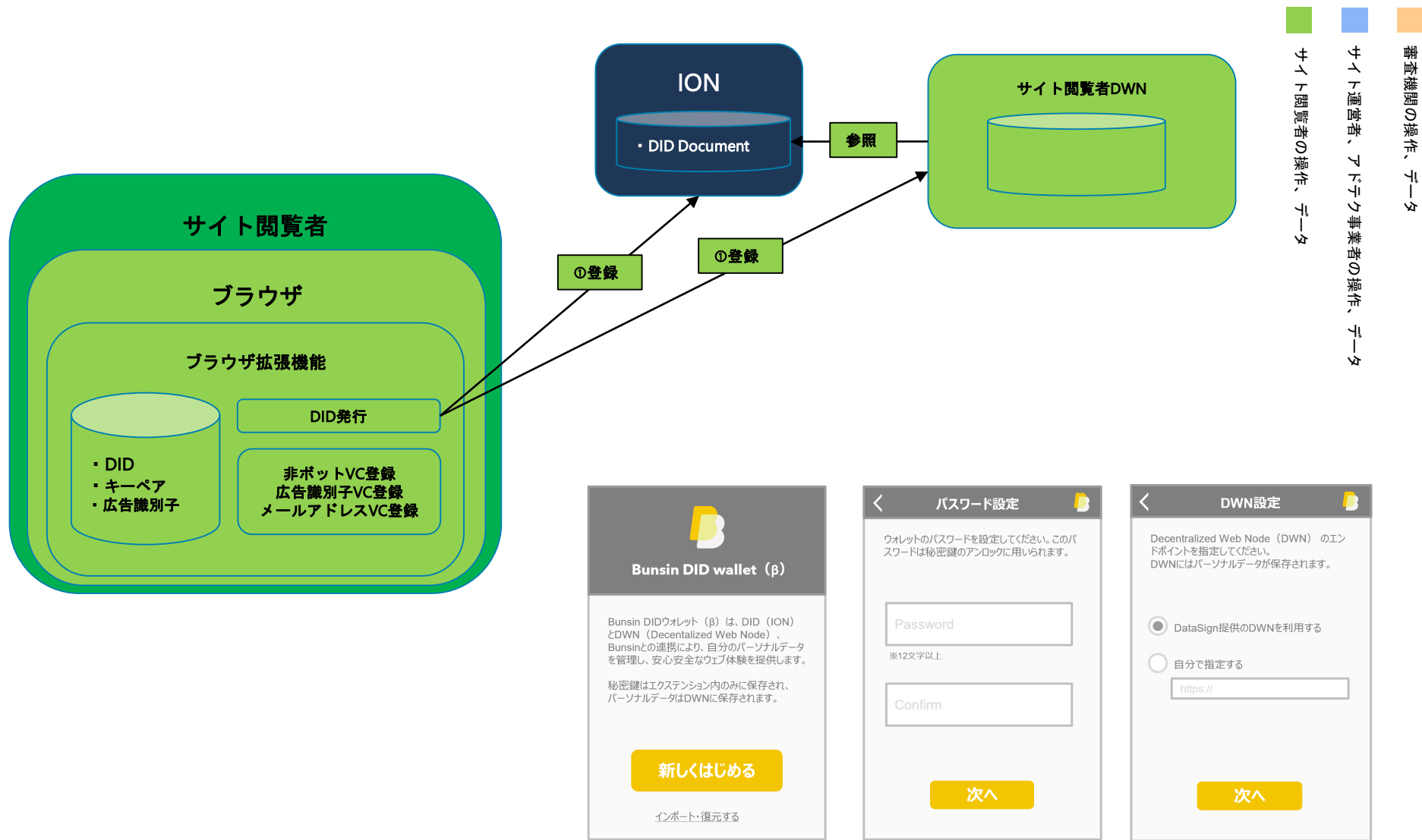
3. 実証内容

3.2.1 スキーム・フロー

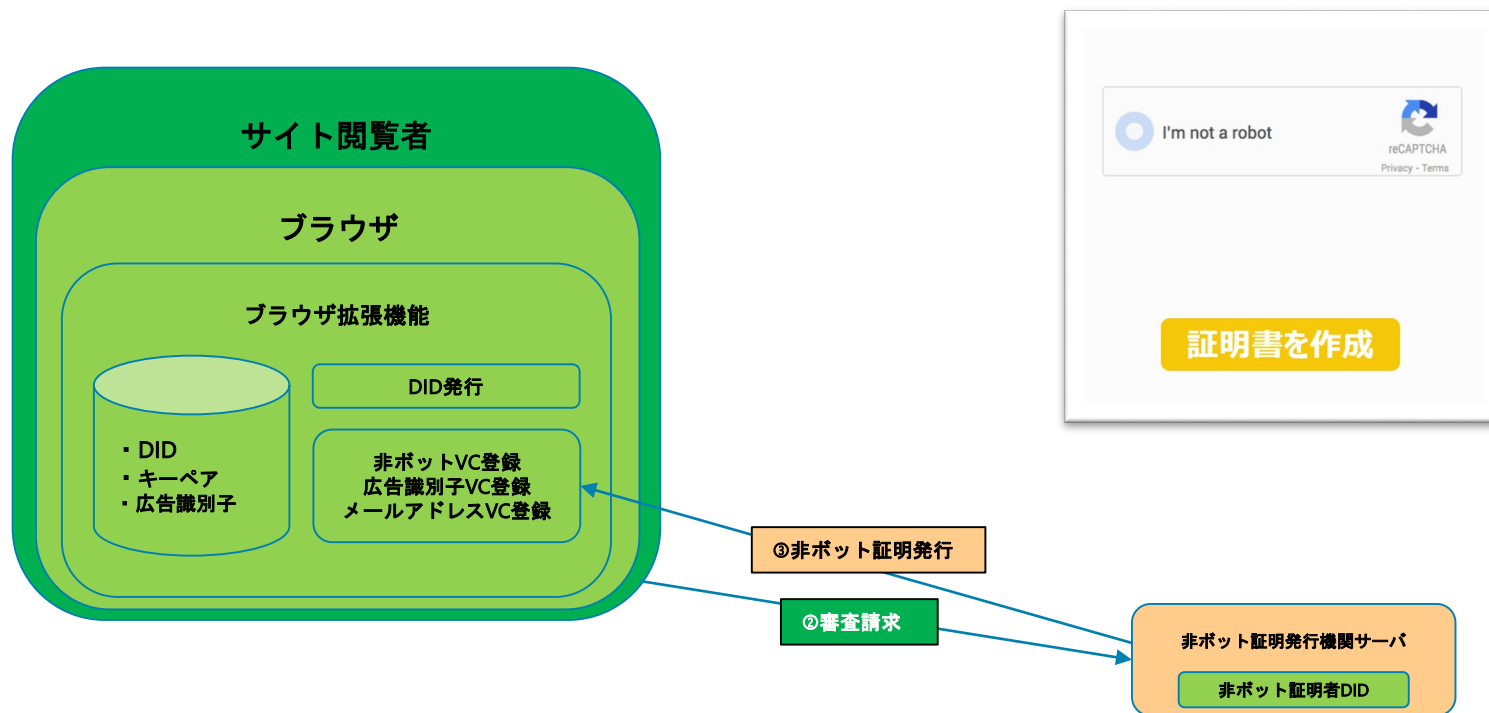


3. 実証内容

3.2.2 サイト閲覧者の準備

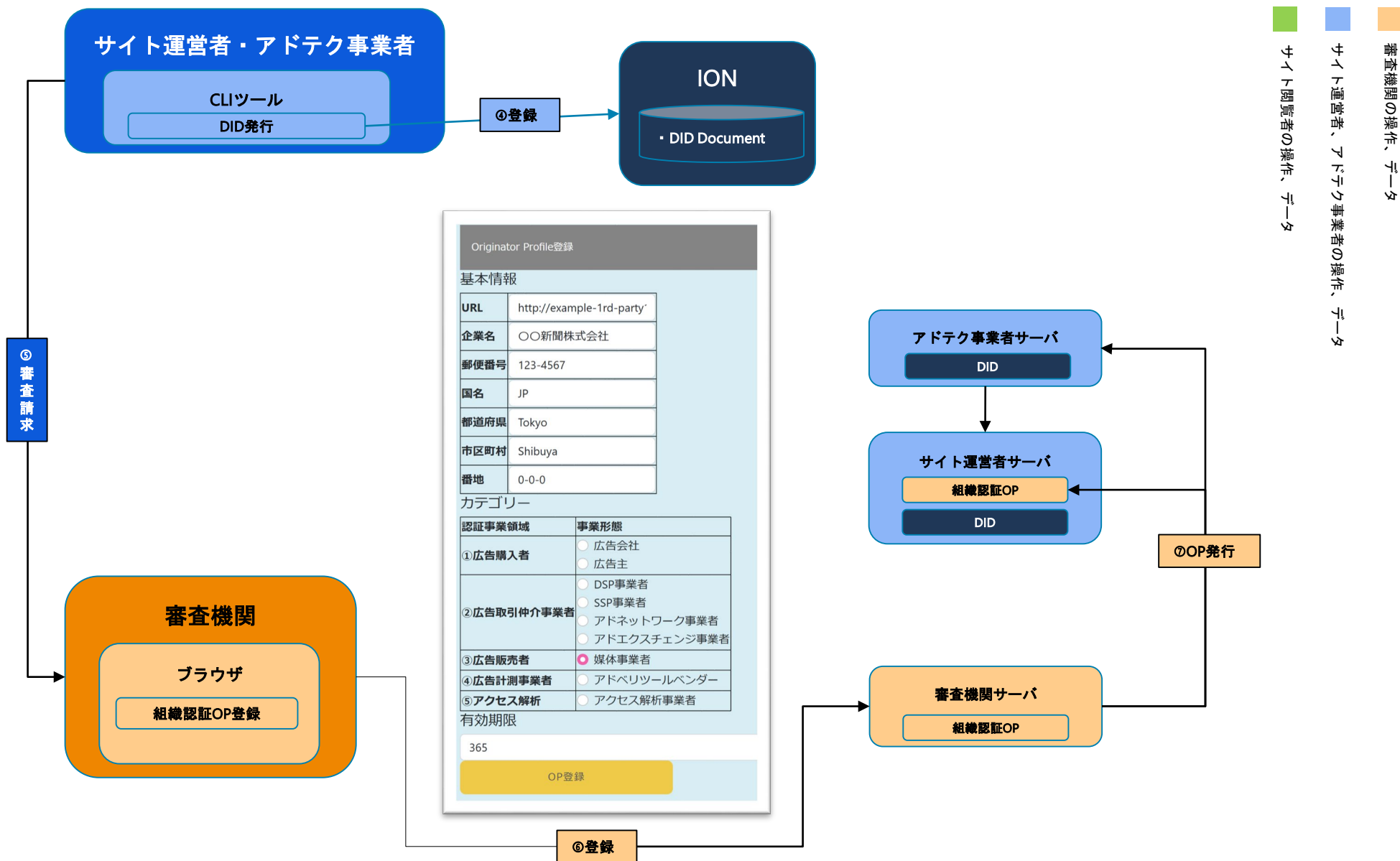


3.2.3 非ロボット証明の発行



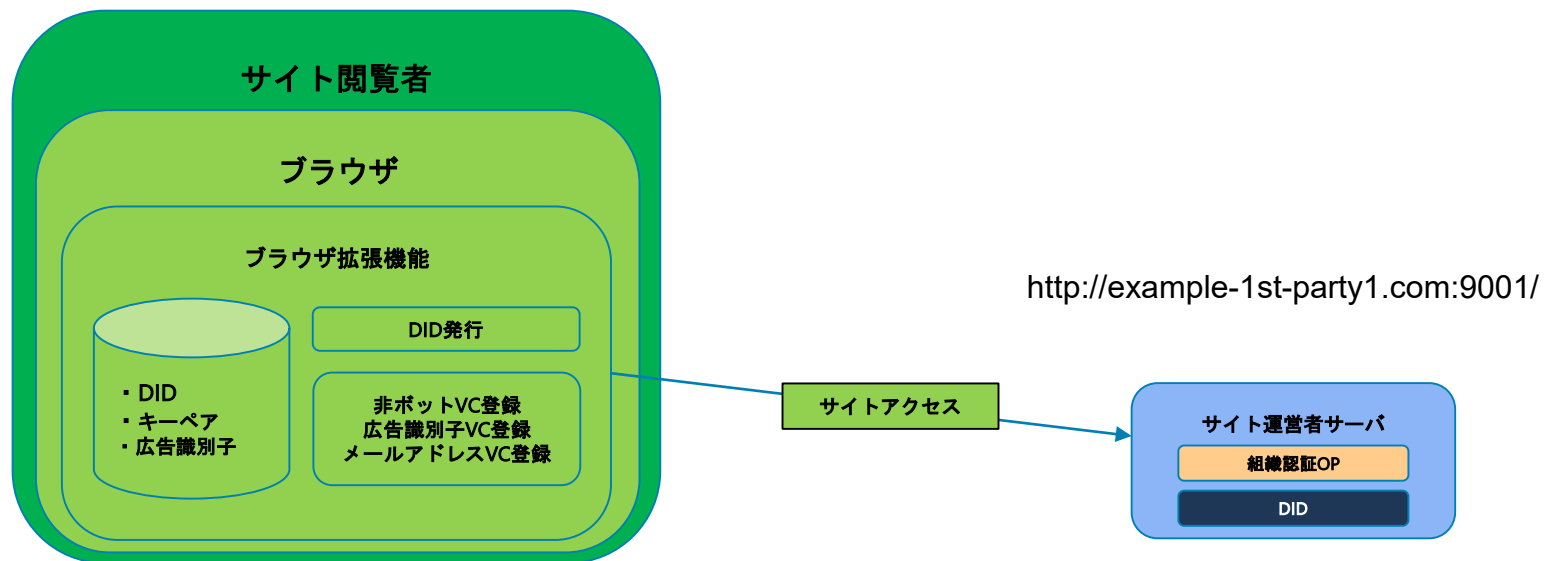
3. 実証内容

3.2.4 サイト運営者・アドテク事業者の準備



3. 実証内容

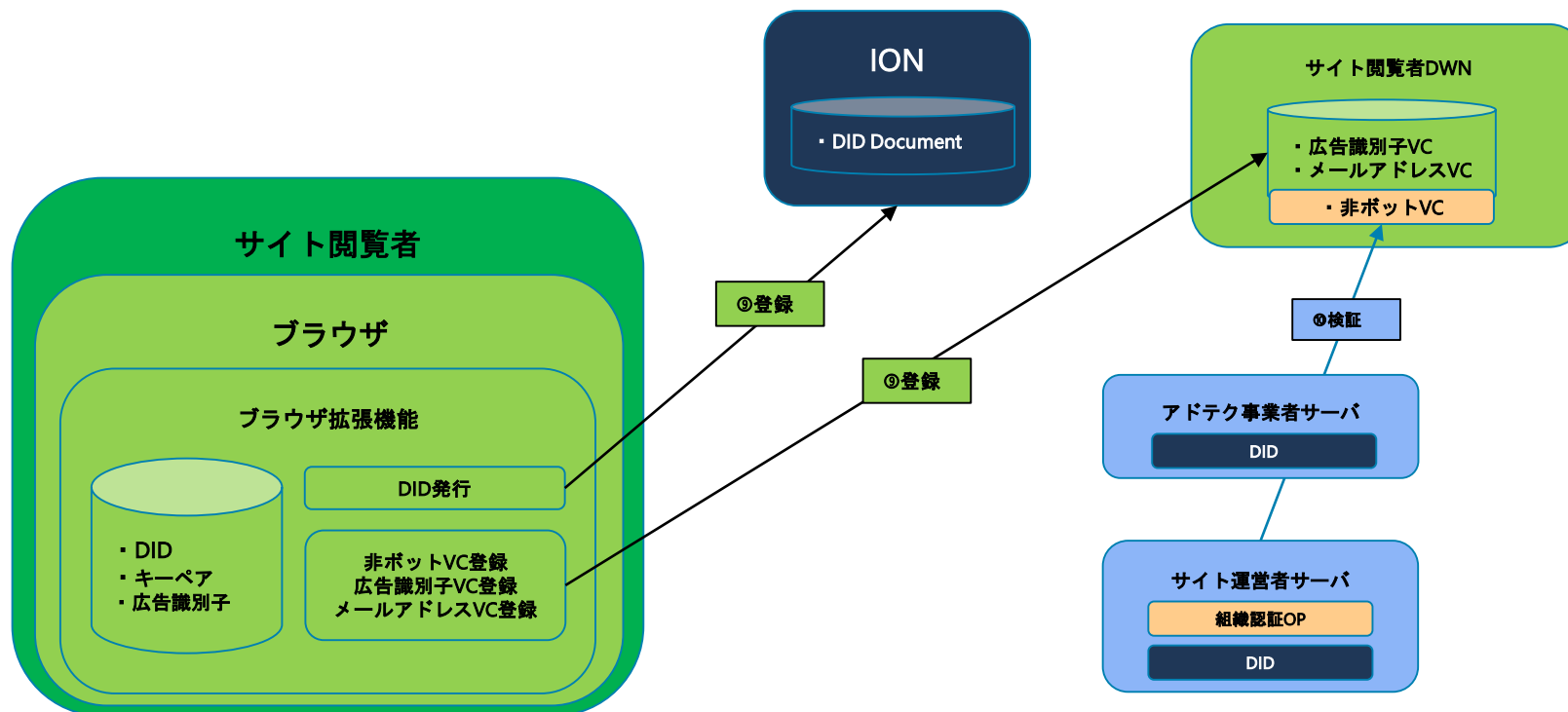
3.2.5 サイトアクセス



- 審査機関の操作、データ
- サイト運営者、アフィリエイト事業者の操作、データ
- サイト閲覧者の操作、データ

3. 実証内容

3.2.8 DWNへの配置とアクセス権設定



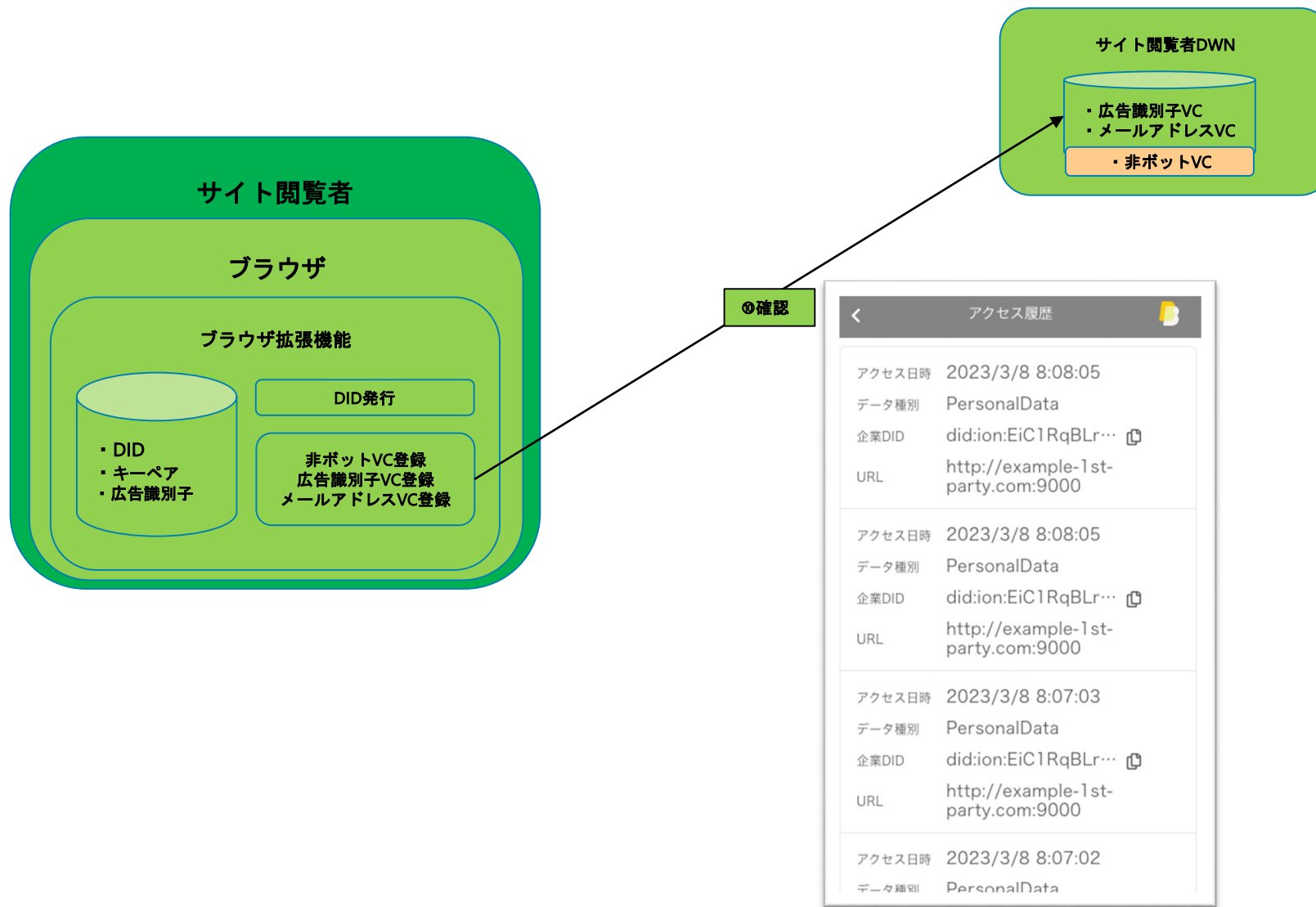
■ サイト閲覧者の操作、データ

■ サイト運営者、アドテク事業者の操作、データ

■ 審査機関の操作、データ

3. 実証内容

3.2.9 アクセス履歴確認



サイト閲覧者の操作、データ

サイト運営者、アドテック事業者の操作、データ

審査機関の操作、データ

3. 実証内容

3.3 6構成要素との対応

6構成要素	6構成要素との当てはめ	
検証可能なデータ	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(広告配信企業、アクセス解析企業等)Originator Profile[3rd party OP]
	署名者	①非ボット審査機関 ②サイト閲覧者 ③サイト閲覧者 ④審査機関 ⑤審査機関
アイデンティティ	アイデンティティとして想定されるものが何か	DID、VC、OP
	アイデンティティ管理システム（外部）は何を利用しているか。(例：OIDC for VC, DID)	DID - ION VC - DWN OP - サイト運営者webサーバー(.well-known)
	アイデンティティグラフとして想定されるのはなにか	<ul style="list-style-type: none"> - 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企業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・アドテク企業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」 - (サイト訪問者) - 「非ボットVC」 - (非ボットVC発行者)

3. 実証内容

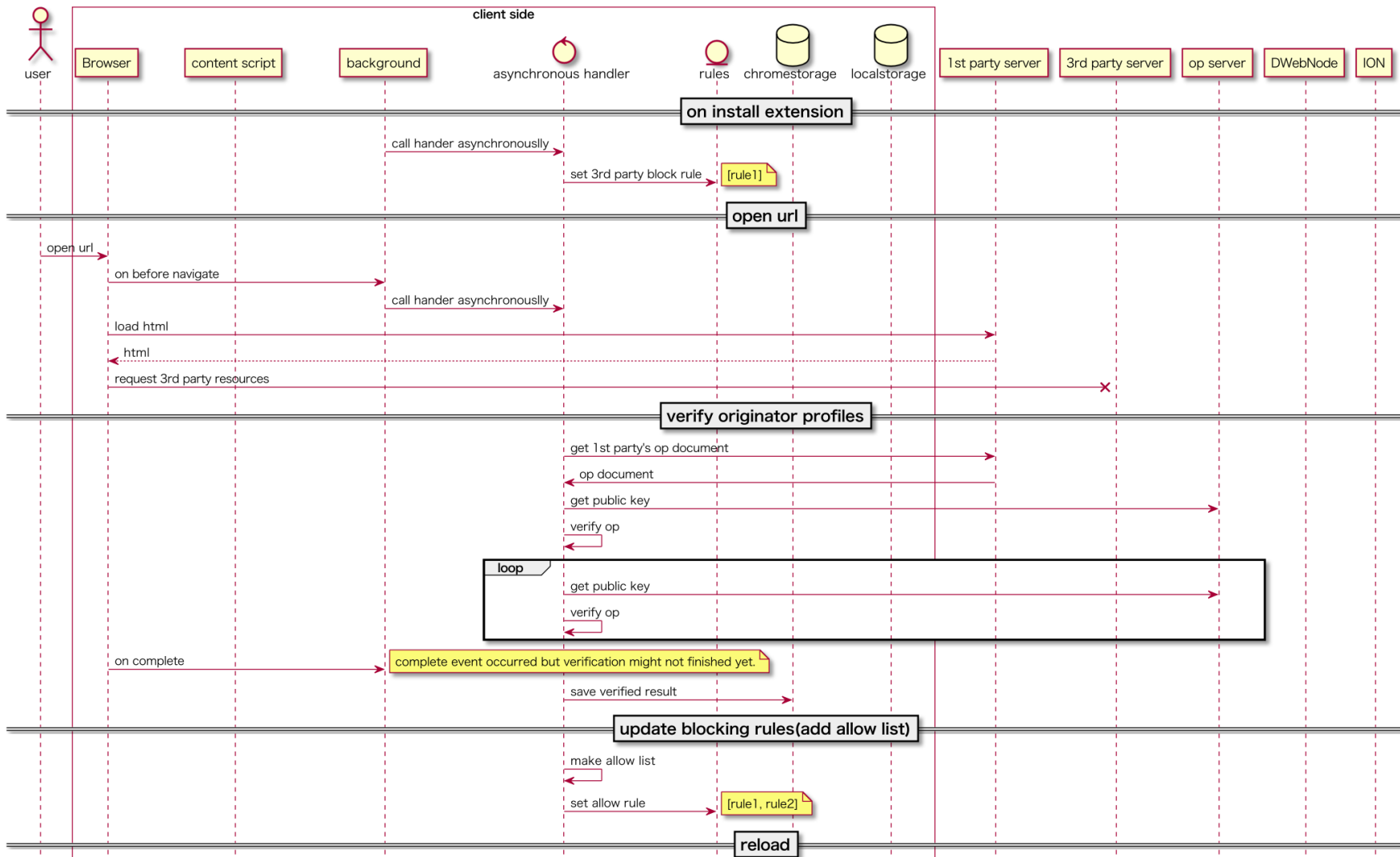
3.3 6構成要素との対応

6構成要素	6構成要素との当てはめ	
ノード	Walletか否か	クロームエクステンションmetamask/eth-hd-keyringを使用しDIDの管理を行っている
	合意形成がされているか、されているならその手段	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
	データのやりとりをどこに記録するか	<ul style="list-style-type: none"> ・Chromeエクステンションストレージ内 ・DWN
メッセージ	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	コネクションオリエンテッド <ul style="list-style-type: none"> ・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]
トランザクション	データのやり取りを記録するか	<ul style="list-style-type: none"> ・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。
	データのやり取りの検証はできるか	発行者に都度直接参照することなく検証できる
トランスポート	トランスポートのプロトコルは何か	<ul style="list-style-type: none"> ・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。

3.4 本実証で企画・開発したシステムの概要 (1/6)

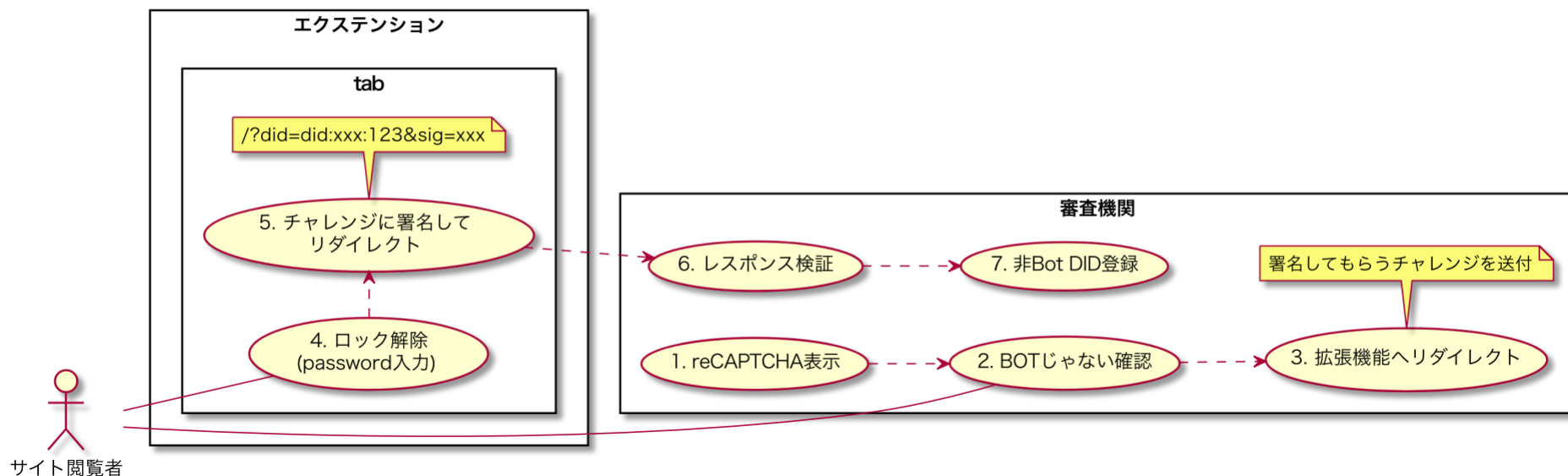
業務フロー

詳細別紙



ユースケース図

4. 非 Bot 証明



3.4 本実証で企画・開発したシステムの概要 (3/6)

操作画面 (UI)



3.4 本実証で企画・開発したシステムの概要 (3/6)

操作画面 (UI)

< DWN設定 

Decentralized Web Node (DWN) のエンドポイントを指定してください。
DWNにはパーソナルデータが保存されます。

DataSign提供のDWNを利用する

自分で指定する

次へ


< マスターDID 

このウォレットのマスターDIDです。このDIDが提供されることはありません。

did:ion:hogehogehoge
hogehogehogehogeho
gehogehogehogehoge
hogehoge


[DID Documentを確認する](#)

次へ

< 非ロボット証明 

ロボットによる不正を防ぐため、あなたが人間であることの証明書 (Verifiable Credential) を作成します。

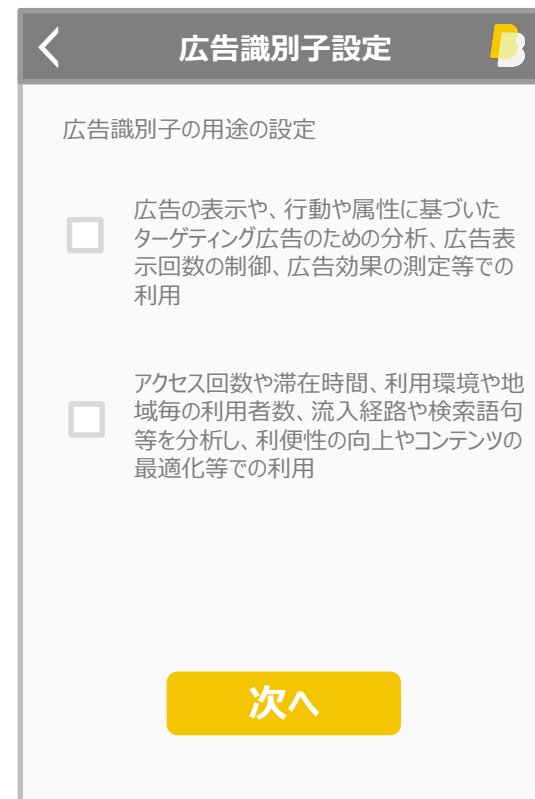
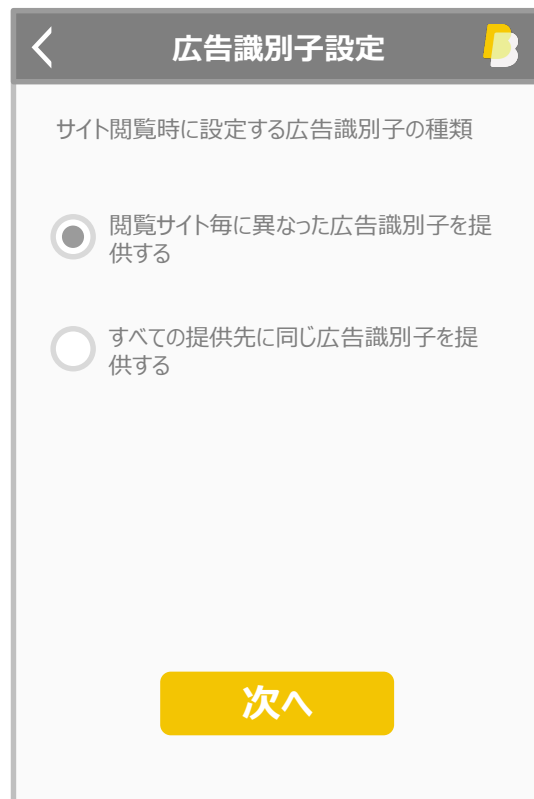
この証明書を提示することで、あなたがロボットではないことを証明できます。

I'm not a robot 
reCAPTCHA
Privacy - Terms

証明書を作成

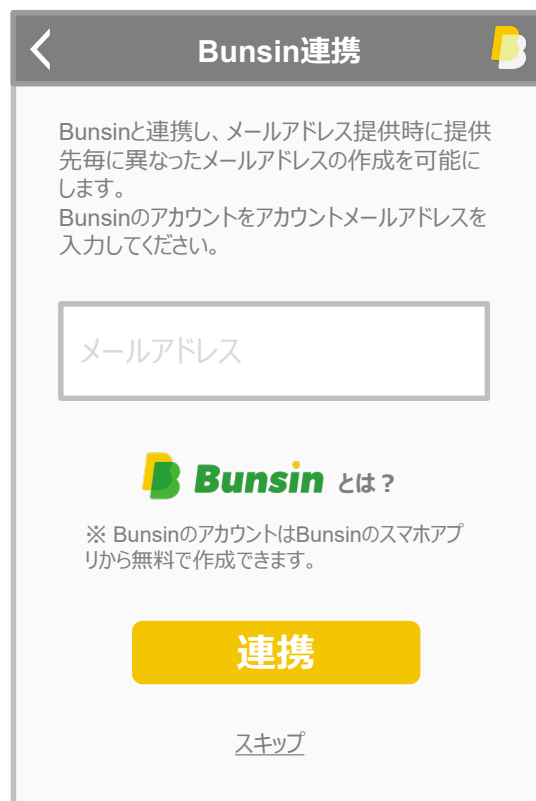
3.4 本実証で企画・開発したシステムの概要 (3/6)

操作画面 (UI)



3.4 本実証で企画・開発したシステムの概要 (3/6)

操作画面 (UI)



3.4 本実証で企画・開発したシステムの概要（3/6）

操作画面（UI）

メールアドレス提供

このサイトからメールアドレスの提供を求められています。

提供先：株式会社日本経済新聞社 ✓
利用目的：提供先のプライバシーポリシー
([リンク](#)) をご確認ください。

メールアドレス

拒否 提供する

同意確認

このサイトでは認証情報が確認できませんでした。以下の用途での広告識別子の利用を許可しますか？

広告の表示や、行動や属性に基づいたターゲティング広告のための分析、広告表示回数の制御、広告効果の測定等での利用

アクセス回数や滞在時間、利用環境や地域毎の利用者数、流入経路や検索語句等を分析し、利便性の向上やコンテンツの最適化等での利用

チェックした用途を許可

すべて拒否

3.4 本実証で企画・開発したシステムの概要（4/6）

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)	サイト閲覧者が拡張機能セットアップ時にRootDIDを発行する
機能	非Bot証明発行	サイト閲覧者が非Bot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のDIDに対して事前に非Bot証明を受けている前提で、そのDIDをissureとするJWTにVCのsubjectとなるペアワイズ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	企業DID発行	企業がDIDを発行してIONに登録する
機能	企業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. 実証内容

3.4 本実証で企画・開発したシステムの概要 (5/6)

データモデル定義

VCを採用している場合は、属性およびその取得元、属性値について下表にならうご記載ください

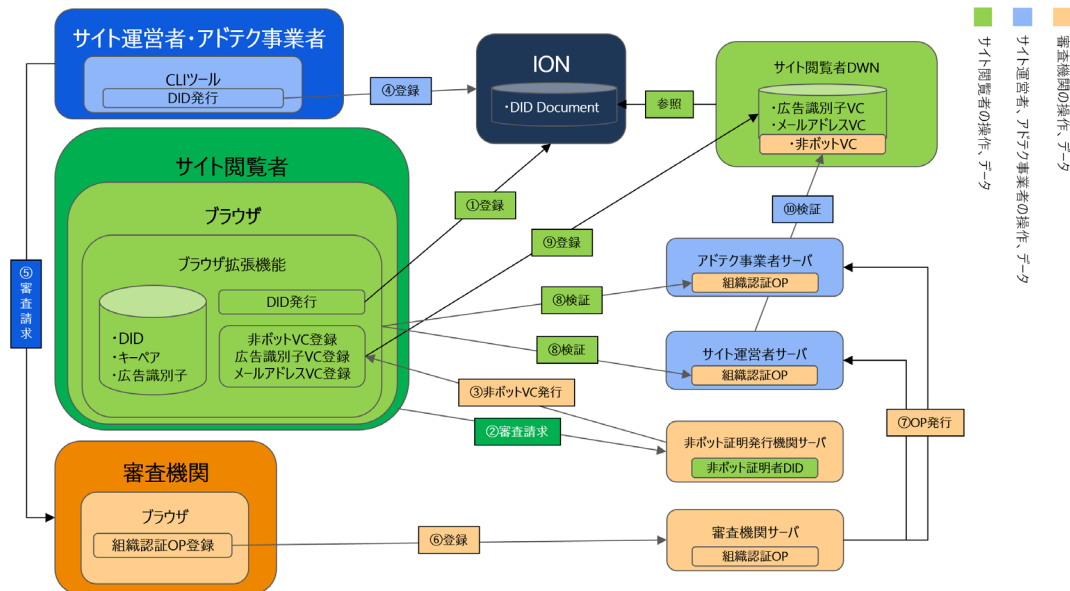
記載例)

属性値	属性取得元	属性値 (vc内)
非Bot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

3. 実証内容

3.4 本実証で企画・開発したシステムの概要 (6/6)

実験環境



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

3. 実証内容

3.5 実証を通じて得られた主な成果

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。	審査機関や審査方法の信頼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「ボットじゃない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。	ボットを完全に排除できるわけではない。（ボットじゃない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信頼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。	審査機関や審査方法の信頼をどのように担保するかについては課題が残る。

3.5 実証を通じて得られた主な成果

システムの企画・開発に関する成果

- 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。

ビジネスモデルに関する成果

- 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と。

3. 実証内容

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

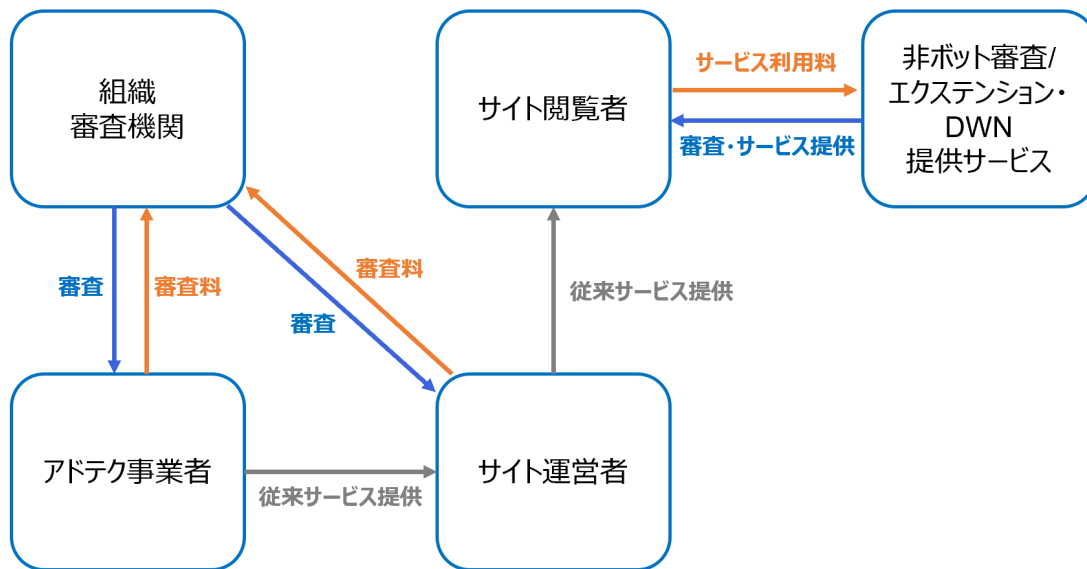
- 本実証事業で企画・開発したコードは、全てオープンソースとしてGithub上に公開することで、第三者が再構築することによって再現可能である。また、DID walletやDWNのシステムは本ニュースケースに限らず、様々な分野で活用がなされることが想定されるため、DID walletやDWNはモジュールとして切り出し、それぞれオープンソースで公開することを予定している

04

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

ビジネスモデル



ユーザーのベネフィット

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 / アドテク事業者	アドフラインドへの対応を簡略化し、アドフラインド対策コストを低減させ、かつアドフライン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なくなる。	審査料（年10～20万円程度）
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. 実証終了後の社会実装に向けた見通し

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。	広告業界の営利企業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。
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「ボットじゃない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。	ボットを完全に排除できるわけではない。（ボットじゃない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においても不慣れ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。	広告業界の営利企業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род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。	広告業界の営利企業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。

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

- 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D I D等、巨大プラットフォーマー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ないと、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. 実証終了後の社会実装に向けた見通し

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	今年度事業	課題②③への対応		
実現性の検証・社会実装に向けた実証		実証		
実サービスでの運用開始（一部社会実装）		課題①への対応	試験運用	本運用
すべてのステークホルダーを巻き込んだ社会実装				社会実装

05

Trusted Webに関する考察

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」すると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、本ユースケースでは、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と。
- 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と。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。