Trusted Web の実現に向けたユースケース実証事業

成果報告書

機械製品サプライチェーンにおけるトレーサビリティ管理

2023 年　3 月 24 日（提出日）

ヤンマーホールディングス株式会社

目次

1　背景と目的

機械製品はライフサイクルが長く、それぞれのライフステージにおいて多くのデータが発生する。しかしながら、それらデータの多くは各社・各機能部門での局所的な利用に留まり、必要な範囲で十分に活用されているとはいえない。データが適切に共有されなければ、製造業においても製品をそのライフサイクルに亘ってトレースできないといった問題が生じ、トレーサビリティの確立が困難なものになる。

データを安全に共有するためには、データを提供する側と利用する側が、データの利用者であれば利用するデータの真正性、データの提供者であればデータの開示範囲や利用範囲を限定できるなど、互いに安心してデータをやりとりできる信頼性の確保とそのための仕組みが必要である。またサプライチェーンの各プレーヤーは互いに相対的な関係にあり、誰もがデータの提供者にも利用者にもなって、互いにデータをやり取りする必要がある。

以上を背景に本ユースケース実証では、機械製品など工業製品のサプライチェーン上で発生するデータを対象として、安全にデータのやり取りが行える仕組みを検討することを目的として実施した。

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機械製品サプライチェーン上でやりとりされるデータに対して真正性を確保し検証可能な形で、必要な範囲に共有される仕組みを検討する。例として、サプライチェーンの中から保守サービスにおける修理サービスシーンを取り上げ、お客様とサービス会社およびメーカー間でのデータ共有の仕組みをプロトタイピングし、コンセプトの検証を行った。本ユースケースでのサービス会社とは、機械製品の修理（リペア）やメンテナンスを行う会社や事業所を指し、以下リペアショップと呼ぶ。

この機械修理シーンにおいてもサプライチェーン上の他のユースケースと同様に、異なる法人や機能部門間でのデータ共有の問題が生じている。例えば機械の修理を行う際には、その機械製品の過去の稼働データを活用することにより、故障の箇所や原因の特定、パーツの適切な交換などがより効果的に行えるものと考えられるが、リペアショップはそのようなデータを保有しているわけではない。一方、メーカーは提供サービス改善のため自社製品の市場での稼働データを収集し、保有している。この稼働データは、メーカー以外の関係者にも提供され、様々に活用できると良い。しかし、メーカーには開示すべき相手や目的を客観的に検証する手段がなく、またデータの開示範囲を客観的な根拠の下に必要十分な範囲で適切に設定する方法がないという状況である。

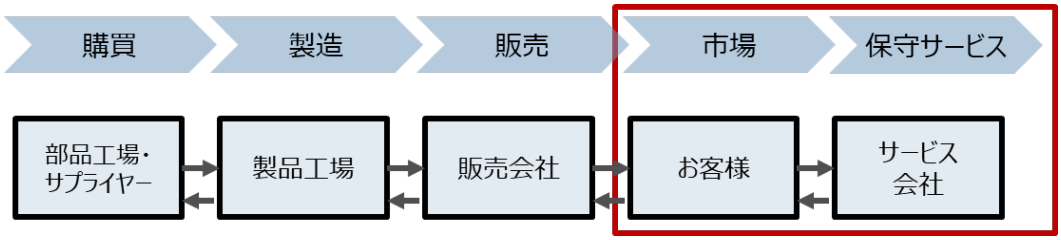

図 2.1-1　事業概要及び実証の範囲

2.2　社会・経済に与える価値・影響

機械製造業において、部品サプライヤーからの調達、工場での製造、製品の販売、保守サービスなど製品サプライチェーンおよびライフサイクル上で様々なデータが生じている。しかしながら、その利用はそれぞれの工程内に留まっている。このように各工程に散らばるデータを、必要とする関係者と安全に共有できれば、互いに自工程と他工程のデータを掛け合わせるなどの連携が可能となる。その結果たとえば、自身の携わった製品がどこから来て、その後どこへ行き、どのような状態であるかを追跡、すなわち製品トレーサビリティの実現につなげることができる。製品のトレーサビリティ強化により、不具合発生時の不具合工程の早期特定（品質・生産性の向上）、リコール対象製品の早期特定（リスク管理強化）、顧客への製品製造過程の情報の見える化（顧客からの信頼性の向上）などの効果が期待できる。

2.3　コンソーシアムの体制

本ユースケースの実施主体は、ヤンマーホールディングス株式会社であり、本実証事業の企画およびプロトタイプシステム開発を行う。プロトタイプシステムの一部に合同会社 Keychain のライブラリを利用した。

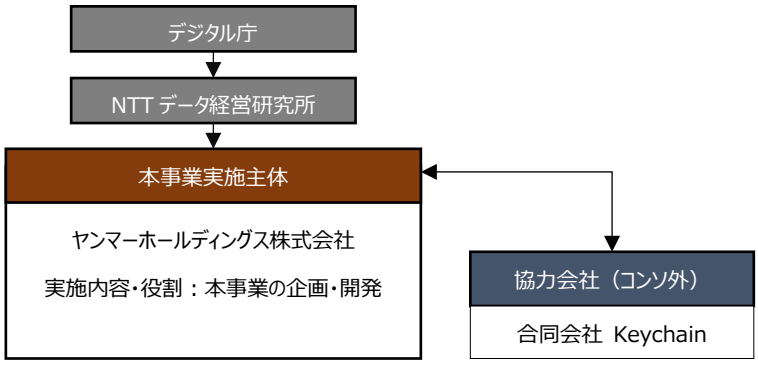

図 2.3-1 実施体制図

2.4　実証全体のスケジュール

活動開始から 11 月までの約 2 か月は企画フェーズとしてユースケースの対象範囲検討やアプリケーション要件定義、システム基本設計を行った。続いて、1 月までの約 2 か月間は開発フェーズとして、アプリケーションシステムの開発を実施した。最後にデモ動画や成果報告書等の作成を実施した。図 2.4-1 は実証全体スケジュールである。

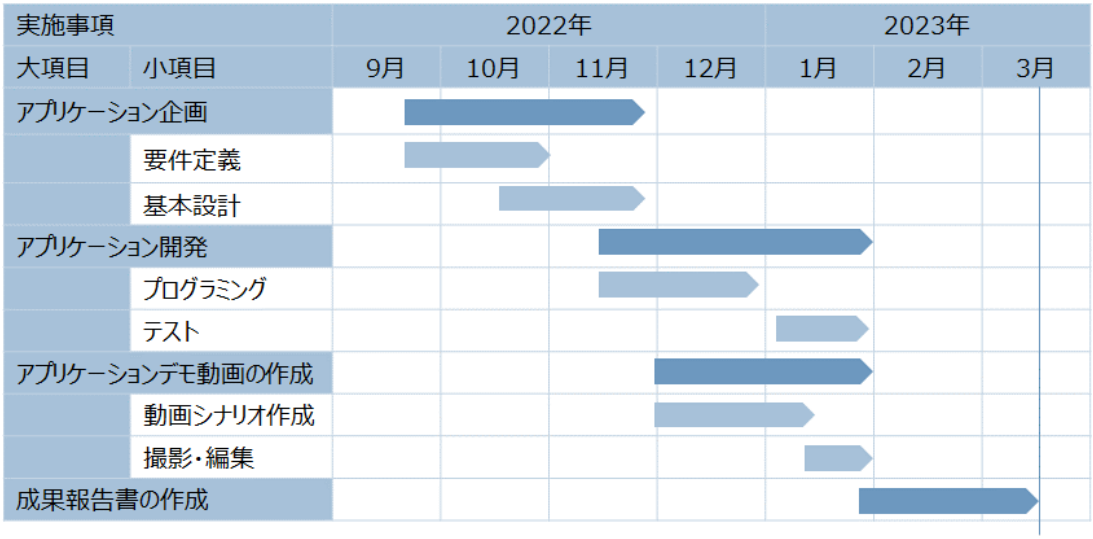

図 2.4-1 実証全体スケジュール

3　実証内容

3.1　実証の実施事項、論点及び判断

3.1.1 ユースケースシナリオ

本ユースケースでは、機械製品の保守サービスにおける修理依頼シーンでのデータ共有の仕組みをプロトタイプとして検討した。エンティティは、機械ユーザー、機械製品（以下、マシン）、リペアショップ、メーカーの４つとし、マシン修理時のデータのやり取りを対象とした。プロトタイプシナリオを以下に記し、図 3.1.1-1 へ図示する。

1. 機械ユーザーは、依頼先のリペアショップを選択しマシンの修理を依頼する。リペアショップは機械ユーザーからの依頼内容を確認し、受託することでユーザーとの修理委託に関する合意が成立する。
2. リペアショップは、マシン稼働データを保有するメーカーへ対して、対象マシンの過去の稼働データについて開示を依頼する。
3. メーカーは、リペアショップからの稼働データ開示依頼に対し、対象マシンおよび修理依頼が存在することを確認できたことを以てリペアショップへ稼働データを開示する。データの開示にあたっては適切な開示期間を設定する。
4. リペアショップは修理完了後、修理レポートを作成し機械ユーザーへ送付する。

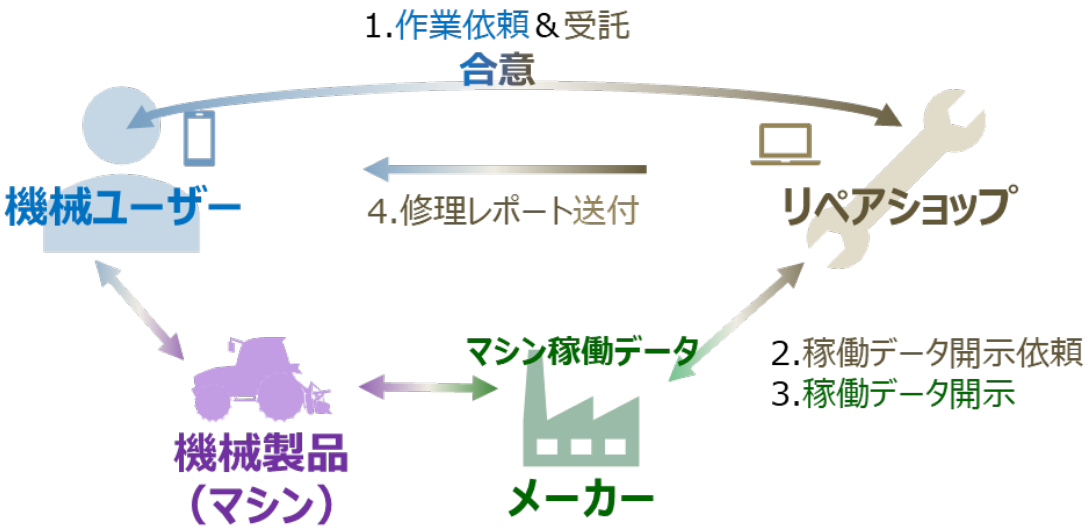

図 3.1.1-1 プロトタイプシナリオ

3.1.2プロトタイプの企画・開発における論点及び判断

本ユースケースにおける検討ポイントと各判断について、以下に要件定義フェーズと基本設計フェーズに分けて述べる。

（1） 要件定義フェーズ

- 対象とするシーン

  本ユースケースでは、製品サプライチェーン・ライフサイクル全体を想定しているものの、プロトタイプ構築にあたっては範囲が広いため、プロトタイプシナリオとして取り上げるシーンを一部に限定した。スマートフォンの他 IoT デバイスとして機械製品を取り上げることができること、及びプロトタイプシステムの実現可能性を考慮して、今回は保守サービスシーンを題材として取り上げることとした。

- データコントロール

  データ保有者が自身のデータをコントロールできる仕組みとして、下記 2 点（開示相手の選択と開示データのダウンロード）の観点から検討した。

  - 開示相手の選択

    開示相手をアプリのユーザーインターフェース上で選択できるようにした。鍵ペア方式により、選択した相手のみがデータを閲覧できるとした。

  - 開示データのダウンロード

    ダウンロード後のデータのトレースが困難となるため、データ開示先はデータをアプリ上で閲覧できるのみでダウンロードはできない仕様とした。

- データ開示の方法

  データは保有者が保管し、別のエンティティがデータを必要とする場合は、データの保有者から開示を受ける形とした。

- 依頼の根拠確認（エビデンス検証）

  修理依頼時にマシンが付したマシン署名をメーカーにて検証することとした。メーカーはこのマシン署名を検証することによりその依頼の根拠を確認できるため、リペアショップの依頼に誤りがあった場合に稼働データの提供を防ぐことができる。

- モノのアイデンティティ

  本ユースケースにおいて機械製品（マシン）は中心的プレーヤーであるため、マシンにもモノとしてアイデンティティを与える。しかし、モノには意思はなく単独で責任主体とはなりえないため、責任主体となる別のエンティティを紐づける必要があると考える。マシン（モノ）は機械ユーザーの支配下にあるため機械ユーザーと紐づける（ペアリングする）こととした。このペアリングにより、マシン署名は機械ユーザーからの依頼により実行される。また機械ユーザーの本人確認についても、当該マシンの販売時に販売会社にて行える。

- データモデル

  機械ユーザーとリペアショップは修理依頼の合意がなされると、修理依頼合意データを保有する。修理依頼合意データは、マシン署名が施されたデータを含めるとともに、合意データ全体に対し機械ユーザーとリペアショップが合意の意思表示のため双方署名を付したものであり、契約書のように両者が保有すべきデータであると考え、両者の共有とした。

- アイデンティティの発見

  業務フローの中で自然にアイデンティティの発見が実現されるように考え検討した。アイデンティティの発見はマシンとメーカー、機械ユーザーとマシン、機械ユーザーとリペアショップ、リペアショップとメーカーの４つの関係者間において必要とされ、それぞれ以下のような方法で発見が可能と判断した。

  1. マシンが他のアイデンティティを発見する方法
     - マシン出荷時にメーカーとペアリングを行うことで、メーカーの DID を知ることができる（出荷作業の一部として取り扱う）
     - マシン販売時に機械ユーザーとペアリングを行うことで知ることができる。（販売手続きの一部）

  2. 機械ユーザーが他のアイデンティティを発見する方法
     - マシン購入時にマシンとペアリングを行うことで知ることができる。（販売手続きの一部）
     - 機械ユーザーが UI 上でリペアショップを選択した際に受信する（アプリ仕様）。リペアショップの DID は、機械ユーザーのアプリサーバで管理されている。

  3. リペアショップが他のアイデンティティを発見する方法
     - 機械ユーザーから送付された修理依頼データを確認することにより、リペアショップは機械ユーザーの DID を知ることができる。修理依頼データに機械ユーザーの DID が含まれる（データモデル）。
     - メーカーの DID は、リペアショップアプリに初期登録しておく（アプリ仕様）。

  4. メーカーが他のアイデンティティを発見する方法
     - リペアショップから送付された開示依頼データを確認することにより、メーカーはリペアショップの DID を知ることができる。開示依頼データにリペアショップの DID が含まれる（データモデル）。
     - マシン出荷時にマシンとペアリングを行うことで、メーカーの DID を知ることができる（出荷作業の一部として取り扱う）

- 検証可能性の担保

  データのやり取りには署名検証を用いることにより検証可能性を確保する。また署名者本人の検証については、マシンについては出荷時にメーカーとペアリングを行い、機械ユーザーについては販売時に本人確認の上マシンとペアリングを行うということにより対応できると考える。リペアショップについては、アプリサーバに登録するときに法人確認をすることで対応できると考える。メーカーについては、産業機械等の製品場合は、そのメーカー実在性は相当程度保証されていると考えられるため、メーカーの法人確認は省略した。

- 合意形成の方法
  機械ユーザーとリペアショップの修理依頼に関する合意について、合意内容が記述されたデータに双方が確認の上署名して共有することによって合意が成立したとする。合意内容は両者で検証が可能である。

- 合意形成に伴うやりとり記録
  今回のプロトタイプシナリオにおいては、合意形成過程でのメッセージのやり取りの記録の重要性は低く、また後から検証する必要性も薄いと思われたため、やり取りの記録は行わないこととした。

- 合意の履行のトレース
  各アプリのユーザーインターフェース上に合意履行の状況を表示することにより合意履行のトレースを実現する。今回のシナリオにおいて、トレースを必要とするのは合意の当事者だけであろうと考えた。

- 合意の取り消し
  合意の取り消しは合意の一種と考えられるため、合意の時と同様に取り消しの合意をもって代用することとした。ただし今回のプロトタイプシナリオでは、合意の取り消しは優先して対応したい事項ではないためプロトタイプ実装の対象外とした。

- 署名の意図の明確化
  機械ユーザーにとってのマシン署名の意図は、機械ユーザーがマシンを所有するという事実を示すことであり、このことは機械ユーザーに理解されうると考える。ただし署名を意識させる必要はないため、ユーザーインターフェース上は修理のための機械を修理依頼書に登録する手続きの 1 つとして、一般的な表記とした（「機械を登録」）。

- スキームの拡張性
  マシンと機械ユーザーの紐づけと、メーカーによるマシン署名の検証により、機械製品のオーナー変更や盗品等不正対象品の修理依頼の防止、リペアショップによるデータ不正要求の防止などにも対応できると判断した。

（2） 基本設計フェーズ

- 鍵の管理
  鍵の管理はブロックチェーンで行う。プロトタイピングは Keychain のライブラリを用いた。Keychain のライブラリを活用することで、鍵の管理と DID の発行の両方を委ねることができる。

- DID の発行
  マシンもエンティティとして扱い、DID を発行させる。これによりマシンもデータの開示先を制御できるようになる。またマシンの所有者（機械ユーザー）が変更になった場合でも、同一マシンとしてその履歴をトレースできる。DID の発行は Keychain ライブラリを用いる。この場合、その鍵ペアが保管されるブロックチェーン

上の URI を DID として扱うことになる。

- データの保管場所
  データのコントロール権をデータの保有者に与えるため、機械ユーザーアプリ、リペアショップアプリ、メーカーアプリの各アプリのデータは、それぞれのアプリサーバに保存することとした。またアプリサーバでは、保有者ごとにデータが管理される。ブロックチェーンを利用することも検討したが、処理速度が懸念されるため、スマートデバイスや IoT デバイス上のアプリケーションを想定した場合には適さないと判断し見送った。

3.1.3ヒアリングの実施
実施なし

3.1.4国際標準規格の調査
実施なし

3.2　検証できる領域を拡大する仕組み
3.2.1 データフロー
本プロトタイプシナリオにおけるデータのやり取りの内容を、その順番に従って①から⑦の番号を付して下記に記す。また、データフロー図として図 3.2.1-1 に記す。

① マシン情報の登録依頼
  機械ユーザーは自身のマシンに対してマシン署名を要求する。機械ユーザーはマシンに署名を要求するデータに自身の署名を付し、マシンはその機械ユーザー署名を検証する。
② マシン情報の登録
  マシンは機械ユーザーから送られたデータに対して自身の署名を付して返送する。
③ 修理依頼の送付
  機械ユーザーは修理依頼をリペアショップへ送付する。修理依頼データにはマシン署名が含まれる。機械ユーザーは修理依頼データに自身の署名を付し、リペアショップはその機械ユーザー署名を検証する。
④ 修理受託に関する合意内容の送付
  リペアショップは修理を受託し、合意内容を機械ユーザーへ送付する。リペアショップは合意内容のデータに自身の署名を付し、機械ユーザーはリペアショップ署名を検証する。
⑤ 稼働データの開示依頼
  リペアショップは修理対象マシンに関する稼働データの開示をメーカーへ依頼する。開示依頼データにはマシン署名が含まれる。リペアショップは開示依頼データに自身の署名を付し、メーカーはその署名を検証する。
⑥ 稼働データの開示
  メーカーはリペアショップへ稼働データを一時的に開示する。メーカーは開示依頼データに含まれるマシン署名を検証することにより、開示依頼の妥当性を確認する。メーカーは稼働データに自身の署名を付し、リペアショップはその署名を検証する。

⑦　修理レポートの送付

リペアショップは作成した修理レポートを機械ユーザーへ送付する。リペアショップは修理レポートデータに自身の署名を付し、機械ユーザーはその署名を検証する。

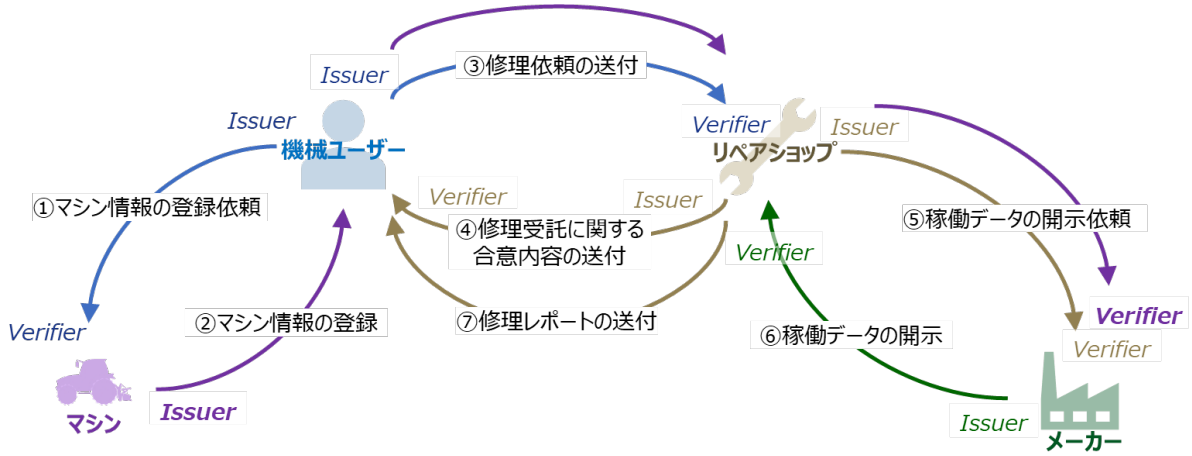

図　3.2.1-1　データフロー図

各エンティティ間でやり取りするデータには発行者(Issuer)が署名を付し、検証者(Verifier)がその署名の検証を行う。原則として、データを送付する側がデータの発行者であり、かつ保有者（Holder）となり、データ受領する側が検証者となる。ただし、マシン署名が付されたデータの発行者はマシンであるが、保有者は機械ユーザーとリペアショップの双方とし、マシン署名の検証はメーカーが行う。

データをやり取りする際は開示相手の公開鍵で暗号化して送付し、そのデータは開示された相手のみが復号化し閲覧できる。また開示されたデータは開示側が設定した条件の範囲で利用できる。

データのアクセスは、そのデータの保有者だけがコントロールできる。データをダウンロードすることは本プロトタイプシナリオでは許可しない。また、データの置き場所は各端末内のストレージもしくはアプリごとに用意されるサーバー（アプリサーバー）に保存され、データの保有者だけがアクセスできる。

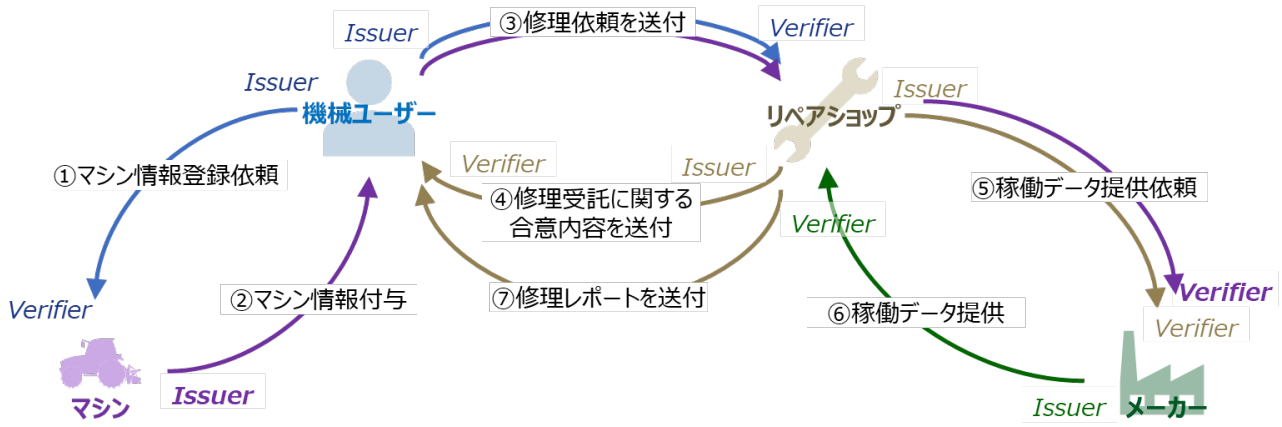

図　3.2.1-2　各エンティティ間のデータ授受における役割

3.2.2 データフローに登場する主体とその概要

データフローに登場する主体についてそれぞれの概要を記す。本プロトタイプシナリオにおける主体は、機械ユーザー、マシン、リペアショップ、メーカーの４者である。

- 機械ユーザー
  機械製品を所有する自然人である。自身が所有する機械製品の修理を、希望するリペアショップへ依頼する。依頼に際しては機械製品とやり取りをして、修理対象の機械の署名を付した上でリペアショップに必要なデータを送付する。修理後はリペアショップより修理レポートを受け取る。

- マシン（機械製品）
  本ユースケースにおいてトレーサビリティの対象となる機械製品である。機械ユーザーからの依頼を受けて、修理依頼データに機械の情報と機械の署名（マシン署名）を付加して機械ユーザーに返送する。

- リペアショップ
  機械製品の補修や修理を行う法人である。機械ユーザーからの修理依頼を受け、受託する場合は受け取った依頼データに自身の署名を付して機械ユーザーへ返送する（これにより双方の合意が成立する）。また、修理に必要となる過去の稼働データの提供をメーカーに依頼し、活用する。修理後は修理結果を記したレポートをユーザーに送付する。

- メーカー
  マシンを企画・設計・製造する法人である。出荷後の機械の稼働データを保有しており、必要な場合にリペアショップに、必要な範囲のデータを一時的に提供する。マシン署名に対しては検証者の役割を果たす。

3.2.3 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

本プロトタイプシステムにおいて検証の拡大が図れると考えられる領域は下記の通りである。
なお、下記いずれにおいても、データへのアクセスコントロールはそのデータの保有者に限られ、またやり取りする際には送付相手の公開鍵で暗号化して送られる。

- 依頼の正当性（機械の保有）
  メーカーが稼働データをリペアショップへ開示する際、対象のマシンが正当なものであることを確認するため、稼働データの提供依頼データ内のマシン署名を検証する。メーカーとマシンは事前（製品出荷時）にペアリングする想定により、メーカーはマシン署名を検証できる。なお、マシン署名は機械ユーザーの依頼により付され、リペアショップを経由してメーカーへ送付され、機械ユーザーおよびリペアショップがマシン署名含むデータを保有している。

- 修理依頼内容の正当性

リペアショップは、受け取った修理依頼が機械ユーザーにより作成されたものであることを確認するため、機械ユーザー署名を検証する。リペアショップは通知を受けた機械ユーザーとペアリングし、機械ユーザー署名を検証できる。依頼内容データは機械ユーザーが保有する。

- 受託内容の正当性（合意内容の確定）
  機械ユーザーは、受け取った合意データが依頼したリペアショップにより作成されたものであることを確認するため、リペアショップ署名を検証する。合意データはリペアショップと機械ユーザーの両者が保有する。

- 稼働データ開示依頼内容の正当性
  メーカーは、受け取った開示依頼データがリペアショップにより作成されたものであることを確認するため、通知されたリペアショップとペアリングし、リペアショップ署名を検証する。また、メーカーはその開示依頼の内容の正当性をマシン署名の検証により確認した上で、リペアショップへデータを開示できる。開示依頼データはリペアショップの保有である。

- 提供データの正当性
  リペアショップは、受け取った稼働データに付されたメーカー署名を検証する。稼働データの保有者はメーカーである。

- 修理レポートの正当性
  機械ユーザーは、受け取った修理レポートがリペアショップにより作成されたものであることを確認するため、リペアショップ署名を検証する。修理レポートの保有者はリペアショップである。

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

本プロトタイプシステムで形成する合意は、機械ユーザーとリペアショップ間での修理内容に関する合意と、リペアショップとメーカー間での稼働データの開示に関する合意　の 2 点である。

- 修理内容（修理箇所、金額、納期）に関する合意
  機械ユーザーとリペアショップがマシンの修理内容について合意する。機械ユーザーがリペアショップへ送付した修理依頼内容に対して、リペアショップが自身の署名を付して機械ユーザーへデータを返送したことを以て合意とする。合意の履行状況については、機械ユーザーがユーザーアプリ上で確認（トレース）できる。合意の取り消しについても同様の方法で、「合意の取り消し」を合意することにより可能である。ただし、合意の取り消しは今回のプロトタイプシステムでは実装していない。

- 稼働データの開示に関する合意
  リペアショップとメーカーは稼働データの開示に関して合意する。リペアショップからの稼働データ提供依頼が正しい依頼であることをメーカーが確認（マシン署名を検証）したのち、合意がなされる。合意の履行状況については、メーカーがメーカーアプリ上で、確認できる。合意の取り消しについても同様の方法で、「合

意の取り消し」を合意することにより可能である。ただし、合意の取り消しは今回のプロトタイプシステムでは実装していない。

3.3　6 構成要素との対応

Trusted Web ホワイトペーパーv2.0 （P.47）に整理される 6 構成要素（検証可能なデータ、アイデンティティ、ノード、メッセージ、トランザクション、トランスポート）について、本プロトタイプシステムでの対応について以下に記す。

3.3.1 検証可能なデータ

本プロトタイプシステムで検証可能とするデータは 6 つあり、それぞれ検証対象と検証者を記す。

3.3.1.1 検証対象

① 機械が署名した事実
② ユーザーの最終依頼内容
③ ショップの受託内容
④ メーカーへの依頼内容
⑤ メーカーが提供する稼働データ
⑥ ショップが提供する修理レポート

3.3.1.2 検証者

① メーカー
② リペアショップ
③ 機械ユーザー
④ メーカー
⑤ リペアショップ
⑥ 機械ユーザー

3.3.2 アイデンティティ

3.3.2.1 アイデンティティ

本プロトタイプシステムでは、機械ユーザー、リペアショップ、メーカー、マシンの 4 つのエンティティに対してアイデンティティを付与する。

3.3.2.2 アイデンティ管理システム

Keychain ライブラリを活用して、ブロックチェーン基盤上の鍵保管場所を示す URI を DID として使用する。

3.3.2.3 アイデンティグラフ

機械ユーザーの可視範囲はリペアショップとマシン、メーカーはリペアショップとマシンに限られる。本ユースケースで

はこのようにアイデンティティによって可視性に違いがあり、機械ユーザーとメーカーなどは互いに不可視である。図 3.3.2-1 のアイデンティティグラフ（アイデンティティ間の可視性およびデータのやり取り）において、黒線で結ばれたアイデンティティ同士は互いに可視性を持つ。

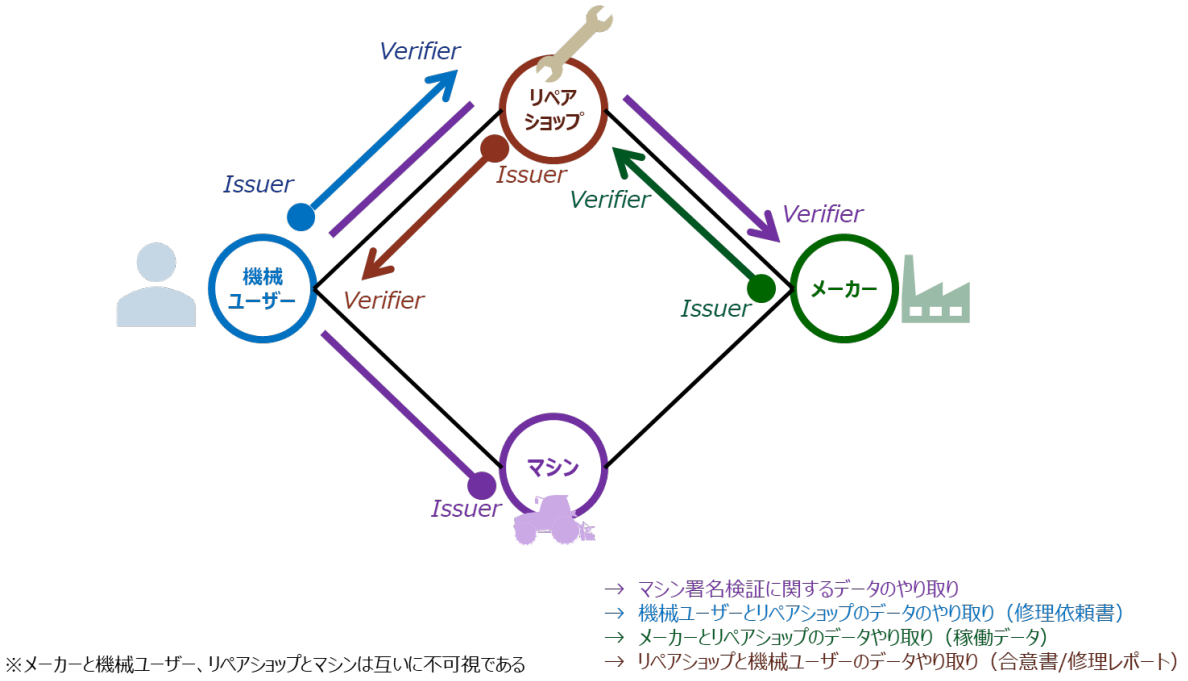

図 3.3.2-1 アイデンティグラフとデータのやり取り

3.3.3 ノード

3.3.3.1 Wallet の使用有無

本プロトタイプにおいては各エンティティのデバイスはそれぞれ DID に紐づいた鍵情報並びに情報を管理するアプリケーションを有す。鍵ペアは Keychain ライブラリを使用して生成、並びに管理を行う。

3.3.3.2 合意形成とその手段

データのやり取りをする相手とデータのやり取りを行うことについての合意については、URI 情報の交換（ペアリング）により行う。ペアリングによりこの合意が確定する。一方、契約内容に関する合意については、署名を付したデータの受け渡しにより確定する。この受け渡しはアプリケーション上において、UI と連動したアクションにより実現される。

3.3.3.3 データのやり取りの記録場所

合意形成過程でのメッセージのやり取りの記録の重要性は低く、また後から検証する必要性も薄いと思われたため、本プロトタイプシステムではデータのやり取りは記録しない。なお、ブロックチェーン上に記録されるのは各アイデンティティの DID や鍵情報のみである（Keychain Library の仕様に基づく）。

3.3.4 メッセージ

コネクションオリエンテッドもメッセージオリエンテッドも可能であるが、メッセージオリエンテッドを基本とする。

3.3.5 トランザクション

データのやり取りの記録場所（3.3.3.3）と同様に、本プロトタイプシステムではトランザクションの記録や検証は行わない。

3.3.6 トランスポート

トランスポートのプロトコルとして、機械ユーザーとマシン間は近接無線通信が考えられ、その他はインターネットを想定する。ただし、今回のプロトタイプシステムでは実装外である。

3.3.7 その他

特になし

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

本プロトタイプシステム利用時の業務フローについて、以下順に、修理依頼の作成のフロー（図 3-2 データフロー①②に該当）、修理の依頼から受託までのフロー（同③）、修理の合意のフロー（同④）、稼働データの依頼から提供までのフロー（同⑤⑥）、修理レポート送付のフロー（同⑦）について記述する。

- 修理依頼作成のフロー

  機械ユーザーはアプリを起動し修理依頼を新規作成する。アプリ上で、依頼するリペアショップの選択と依頼内容の入力を行い、続けて修理対象のマシンに署名を依頼する。署名の依頼は、機械ユーザーが機械ユーザーアプリとマシンを近接無線通信等で接続して行う（ただし、プロトタイプではマシンアプリは実装外）。接続が完了すると、マシンに内蔵されているマシンアプリがユーザー署名を検証し、データへ機械情報と自身のマシン署名を付して機械ユーザーへ送信する。これらマシン側の処理は自動で行われる。機械ユーザーはそのデータを受信し、自身の署名を付しリペアショップへの修理依頼データとする。

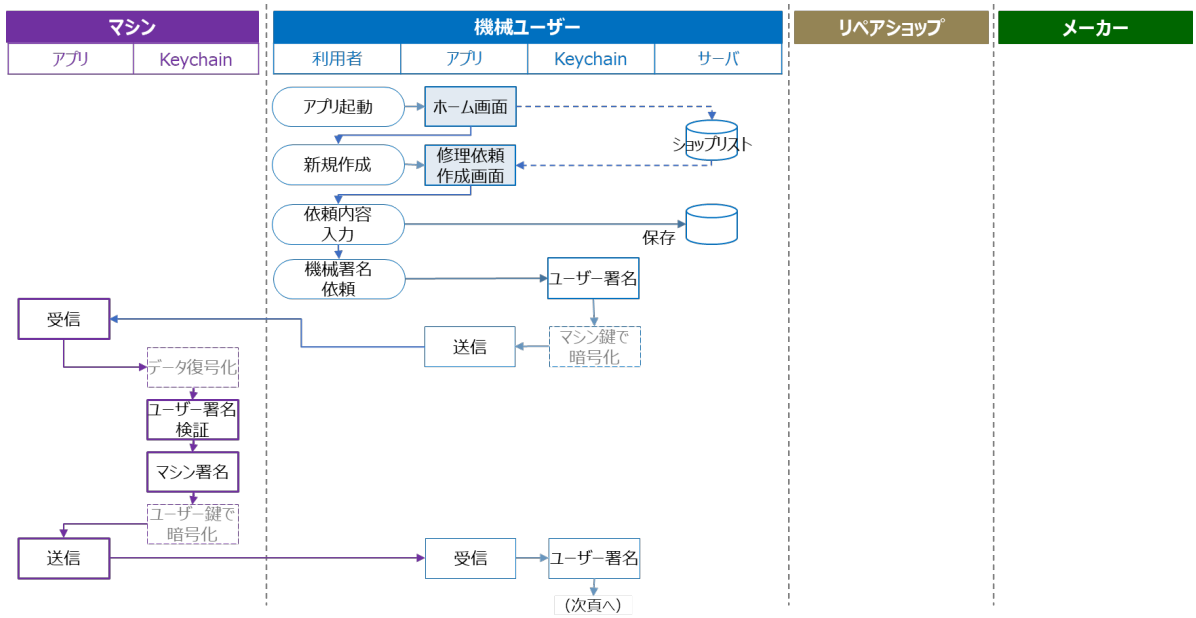

図 3.4.1-1 業務フロー（修理依頼作成のフロー）

- 修理の依頼から受託までのフロー

  機械ユーザーはアプリ上でリペアショップへ修理を依頼すると、修理依頼データがリペアショップの公開鍵で暗号化して送信される。リペアショップはアプリで受信したデータを自身の暗号鍵で復号化した後、機械ユーザーの DID（URI）の登録と署名の検証を行い、リペアショップの依頼一覧へ追加される。リペアショップは修理依頼を選択するとその詳細が表示され、修理依頼を受託する。

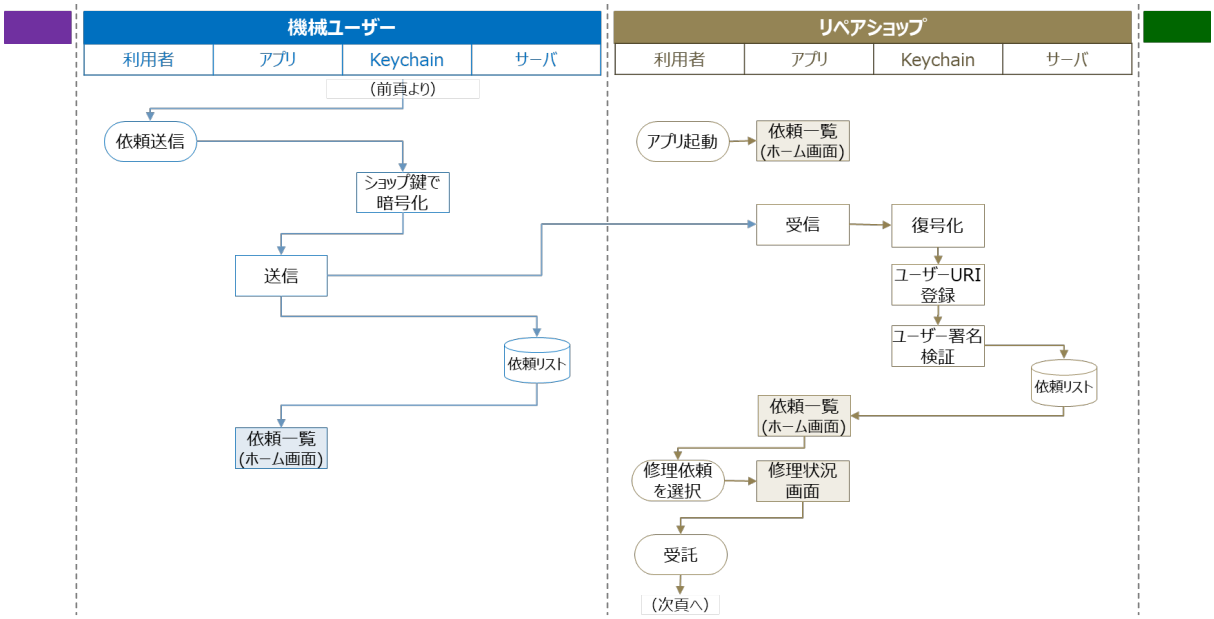

図 3.4.1-2 業務フロー（修理の依頼から受託までのフロー）

- 修理の合意のフロー

  リペアショップが修理を受託すると、リペアショップは機械ユーザーから受信したデータに自身の署名を付したものを UI 上で機械ユーザーへ送信する。機械ユーザーは、受信したデータを自身の暗号鍵で復号化した後、リペアショップ署名を検証し、依頼リストのステータスの更新を行う。

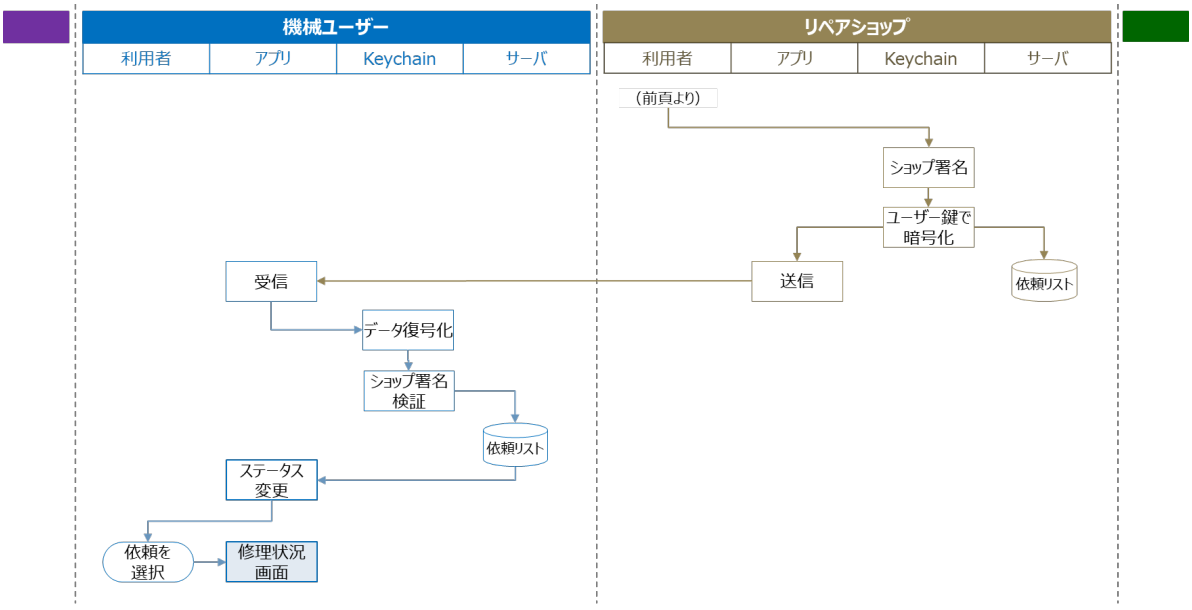

図 3.4.1-3 業務フロー（修理の合意のフロー）

- 稼働データの依頼から提供までのフロー

  リペアショップは UI 上で稼働データの取得をメーカーへ依頼する。稼働データ開示依頼データに自身の署名を付し、メーカーの公開鍵で暗号化して送信する。メーカーは受信したデータを自身の暗号鍵で復号化し、リペアショップ署名とマシン署名について検証する。その後、対象マシンの稼働データを抽出し、そのデー

タに自身の署名を付しリペアショップの公開鍵で暗号化して送信する。リペアショップは受信したデータの復号化とメーカー署名の検証を行い、UI 上に稼働データを表示する。

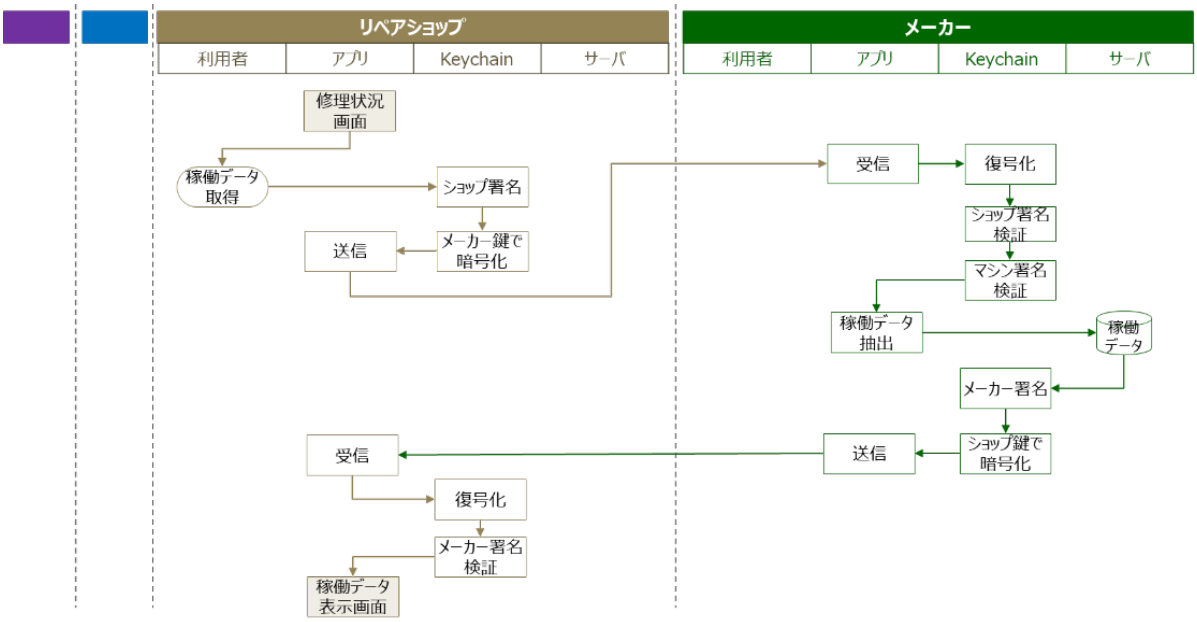

図 3.4.1-4 業務フロー（稼働データの依頼から提供までのフロー）

- 修理レポート送付のフロー

  リペアショップは UI 上で修理レポートの内容を入力し、そのデータへ自身の署名を付し機械ユーザーの公開鍵で暗号化して送信する。機械ユーザーはアプリで受信したデータの復号化とリペアショップ署名の検証を行い、UI 上で表示する。

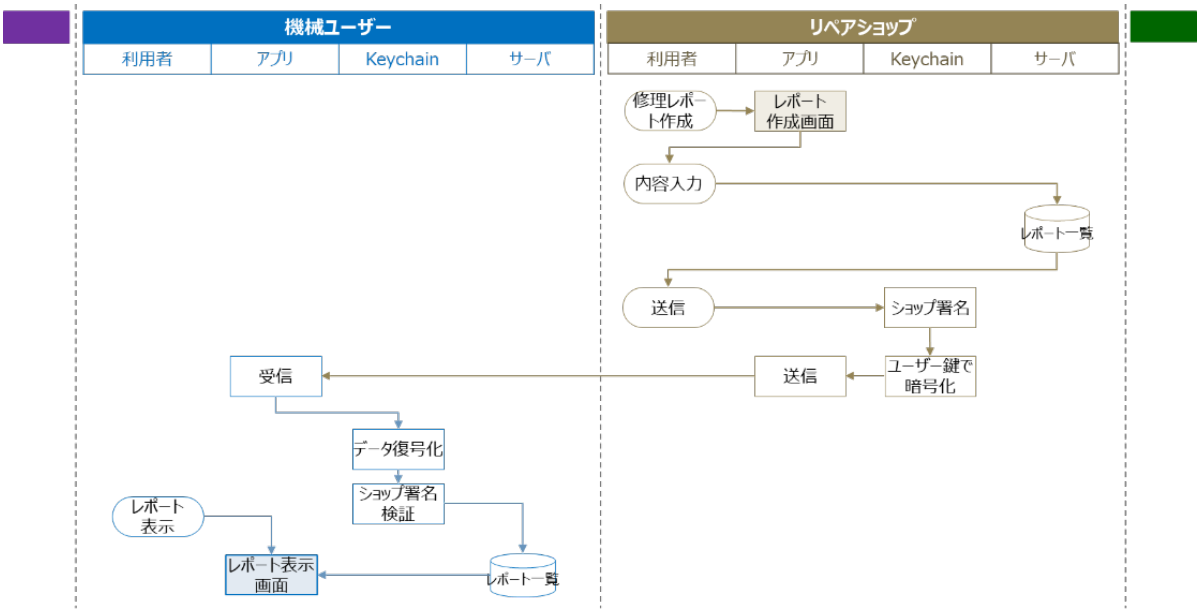

図 3.4.1-5 業務フロー（修理レポート送付のフロー）

3.4.2ユースケース図

ユースケース図を図 3.4.2-1 に示す。機械ユーザーがマシンの修理をリペアショップに依頼するシーンを想定している。リペアショップはマシンの稼働データをメーカーから取得し、故障要因の特定などの修理サービスに活用する。

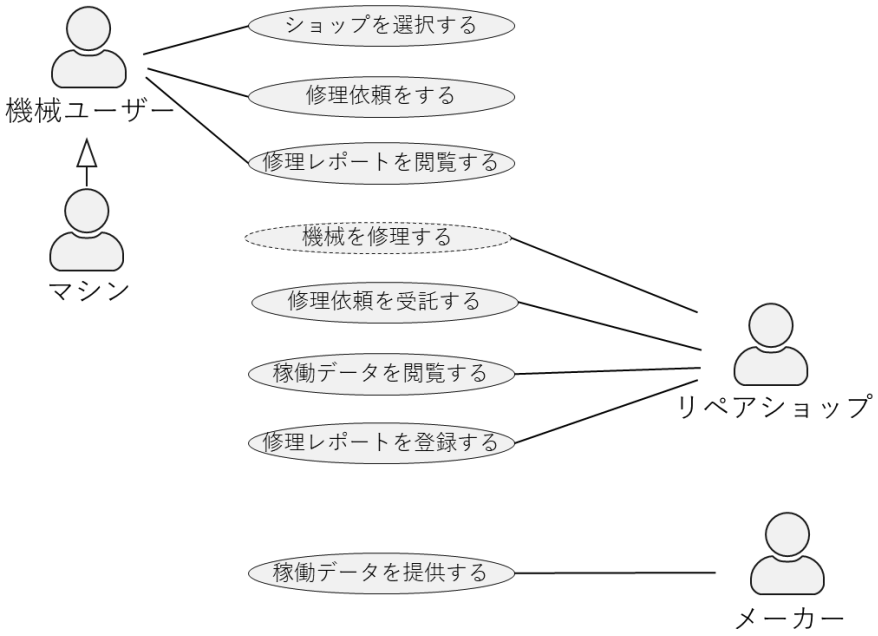

図 3.4.2-1 ユースケース図

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へ記載する。

3.4.4機能一覧/非機能一覧

本プロトタイプシステムにて機械ユーザーに必要な機能として、リペアショップの選択マシンへの署名依頼、稼働データの開示範囲の設定、修理依頼、修理レポート閲覧、履歴の閲覧を挙げた。リペアショップについては、修理依頼の受託、メーカーへの稼働データの提供依頼、修理レポートの送付を挙げた。メーカーについては、稼働データの提供機能を挙げた。

非機能面では、可用性として 365 日 24 時間の稼働を想定したシステムであること、エンティティの数にスケーリングする性能や拡張性を持つこと、移行性を持ったシステムであること、データセキュリティを担保することを挙げた。機能および非機能の一覧を表 3.4.4-1 に記す。

表 3.4.4-1 機能/非機能一覧

機 能 / 非機能	機能名	機能概要
機能	リペアショップ選択機能	機械ユーザーが修理依頼先のリペアショップを選択できる
機能	マシン署名依頼機能	機械ユーザーがマシンに修理内容についての署名を要求できる
機能	稼働データ開示範囲設定機能	機械ユーザーが稼働データの開示期限を設定できる
機能	修理正式依頼機能	機械ユーザーが所望のリペアショップに修理依頼を送信できる
機能	修理正式受託機能	リペアショップに届いた修理依頼を受託できる
機能	稼働データ提供依頼機能	リペアショップがメーカーに修理対象マシンの稼働データを開示要求できる
機能	稼働データ提供機能	メーカーがリペアショップに要求のあった稼働データを送信できる
機能	稼働データ閲覧機能	リペアショップが開示された稼働データを閲覧できる
機能	修理レポート送付機能	リペアショップが修理報告書を機械ユーザーに送信できる
機能	修理レポート閲覧機能	機械ユーザーが修理報告書を閲覧できる
機能	合意履歴トレース機能	機械ユーザーがマシン修理に関する合意の履歴を閲覧できる
非機能	可用性	365 日 24 時間稼働を想定
非機能	性能/拡張性	エンティティの増加に合わせて、システムをスケールアウトできる
非機能	移行性	コンテナ技術、クラウドオーケストレーション技術を採用
非機能	セキュリティ	データ秘匿性確保、データ保有者によるデータ開示範囲の設定

3.4.5データモデル定義(VC データモデルを採用する場合)

図 3.4.5-1 へ本プロトタイプシステムにおけるデータモデルを記す。図中の①～⑥は各エンティティ間のデータフローを示す。

機械ユーザーからマシンへ送られるデータ（①）は、依頼先ショップ（DID）、マシン機種名・型式、マシン製造番号、修理期間のデータ に機械ユーザーの署名を付したものである。マシンから機械ユーザーへ送られるデータ（②）は、依頼先ショップ（DID）、マシン機種名・型式、マシン製造番号、修理期間のデータ にマシン署名を付したものである。機械ユーザーからリペアショップへ送られるデータ（③）は、マシンから受け取ったマシン署名付きデータ（図 3-11 内桃色枠のデータ）、修理依頼内容、納品日、料金、機械ユーザー情報（DID）、開示期間 に機械ユーザー署名を付したものである。リペアショップから機械ユーザーへ送られるデータ（④）は、機械ユーザーから受け取ったデータ（図 3-11③青枠内のデータ）、受付日 にリペアショップ署名を付したものである。リペアショップからメーカーへ送られるデータ（⑤）は、マシン署名の付されたデータ、開示希望納期 にリペアショップ署名を付したものである。メーカーからリペアショップへ送られるデータ（⑥）は、稼働データ、開示期間 にメーカー署名を付したものである。

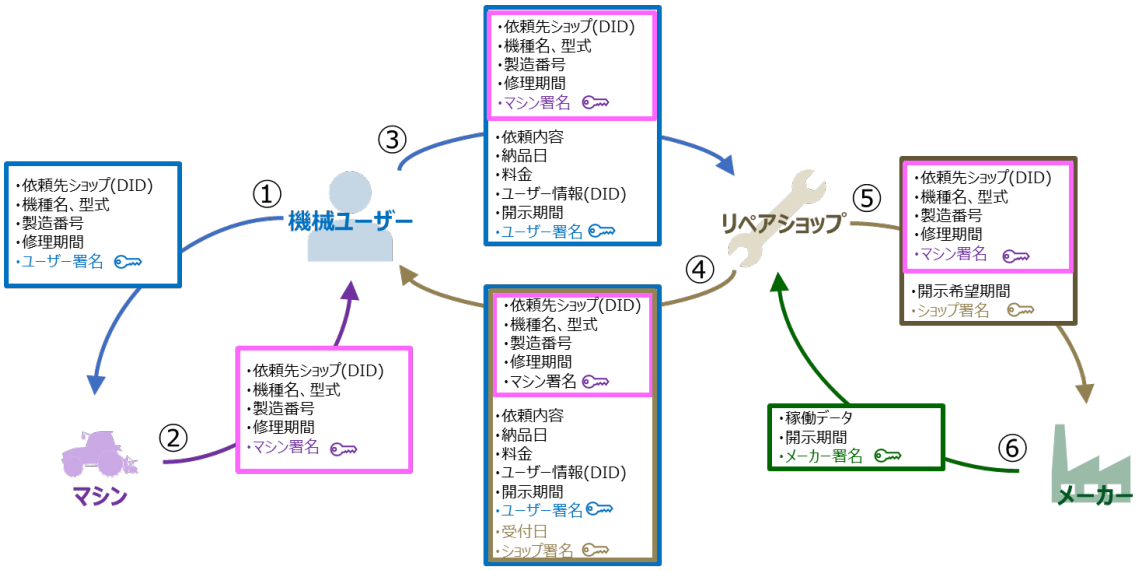

図 3.4.5-1 データモデル

3.4.6 実験環境

本システムは、各エンティティがそれぞれ保有するデバイスおよびクラウドにおけるコンピューティングリソースにより構成され、Web 通信を介して連携する。各エンティティは、スマートデバイスや PC または組み込みコンピューターが想定される。

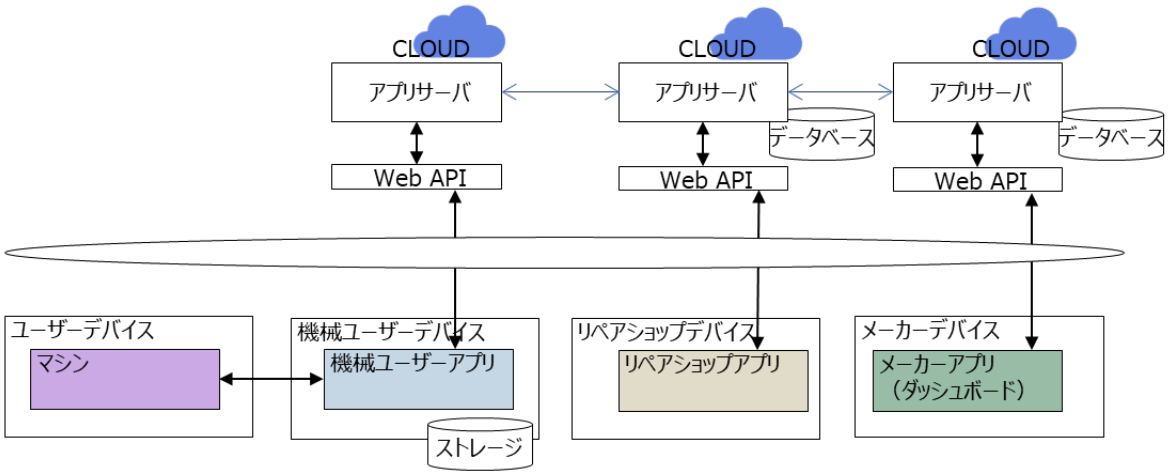

図 3.4.6-1 実験環境

3.4.7システムの構成要素

本プロトタイプシステムは、各アプリにおいて暗号化および署名の鍵管理に有償の Keychain ライブラリを使用している。また、アプリサーバーおよび WebAPI は Amazon Web Service、X サーバーとしてフリーソフトウェアの VcXsrv を利用している。

表 3.4.7-1 主要な製品・ライブラリー覧

コンポーネント名称	型式	OSS か否か	ライセンス
Keychain	―	Keychain 社の権利	有償
Amazon Web Services	―	Amazon Web Services 社のサービス	有償（従量課金）
VcXsrv	―	OSS	無償（GPLv3）

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

機械製品のサプライチェーン上で発生するデータを対象として、機械製品の修理依頼シーンを取り上げ、関係するプレーヤー間でデータを安全にやり取りし共有するためのスキームを定義し、プロトタイピングを行った。機械製品に与えたデジタルアイデンティティは、製品ごとにその来歴を追跡する製品トレーサビリティのための仕掛けになる。

- 機械製品の修理シーンにおけるスキームの企画とプロトタイピング
  - 機械ユーザー、保守サービス、メーカー間のデータのやり取りスキームを定義
- モノ（マシン）へのアイデンティティの付与
  - 機械製品に DID を発行する
- モノ（マシン）と法人・自然人とのペアリング
  - 非責任主体である「モノ」を他の責任主体と紐づけて扱う
- モノ（マシン）のトレーサビリティの確保
  - モノ（マシン）の DID はそのモノのライフサイクルに亘って使い続け、その時々のオーナーはモノの DID に紐づけられた情報の一部と捉える。これにより、その時々のモノの正当な所有者の確認や検証が可能となり、例えば盗品など、正当な所有者以外からの修理依頼防止に役立つ
- エビデンス検証に基づくデータ開示コントロール
  - データの開示先自身の検証だけでなく、開示の根拠（対象となるマシンの署名）も検証できるようにした。データ開示先の正当性だけでなく、開示依頼の正当性も検証でき、その上でデータの開示条件を設定し、開示できる（メーカーからリペアショップへの開示）
- アイデンティティの可視範囲の局所化
  - アイデンティティの可視範囲を必要な範囲に限定することで、とりわけ慎重な扱いが求められるユーザー情報などを過度に広範囲のエンティティに知らせないようにした。本プロトタイプシナリオにおいては、ユーザー情報の開示はリペアショップへの開示だけで足りることを示した。

3.5.2 ビジネスモデルに関する実証内容・得られた成果

本ユースケースは製品サプライチェーン上のデータ共有を題材としているためビジネスモデルそのものについての検討ではなかったが、社会実装に向けてはいくつかの課題が明らかになった。

- アプリケーションの提供主体

  アプリケーションを誰が提供し、維持、運営していくのかという課題に関して検討が必要である。システムの構築には相応レベルの開発力が必要となる中で、サプライチェーンのような多種多様な参加者で構成されるユースケースにおいては、全参加者にそのような一定レベルのシステムの構築を求めることは難しい。投資負担に耐えられる中心的なエンティティの存在なしに、全体の推進力をどこまで確保できるのかは明確ではない。
- 必要なシステム規模の見極め

  参加者間でのコスト負担の考え方の整理が必要である。開発コストに加え、維持コスト、データ保存コストを誰が負担すべきか、どのように配賦すべきか、という点について全参加者で合意できる基準を設けられるかどうかがまだ不明である。また、必要とする Trust のレベルと、それぞれが開発すべきシステム規模について、サプライチェーンの参加者ごとに見極めが必要である。

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）

本実証事業で開発したシステムは、手順書（README）に沿って環境構築を行うことにより、再現が可能である。ただし、本システムの一部は Keychain SDK を使って動作するため、同社の SDK ライセンスを入手する必要がある。

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

本ユースケースの目指す姿は、機械製品のサプライチェーンと製品ライフサイクル上で発生する様々なデータの信頼性を向上させるとともに、それらを製品に関わる多数のステークホルダーの間で安全に共有できる状態である。データのやり取りに関するこのような環境が整備されることにより、各々が所有するデータの活用や、異組織間でのデータ連携が一層進み、例えば製品毎にその来歴をトレースできるようになるなど、製品トレーサビリティの向上につながるものと考える。

一方、このようなシステムの構築および維持にかかるコストの負担については、データによる利益を享受するステークホルダーにて負担されることが望ましい。そのためには負担の配賦方法について参加者で合意できる形で決めることができなければならないが、現時点では明確な見通しを持つまでには至っていない。

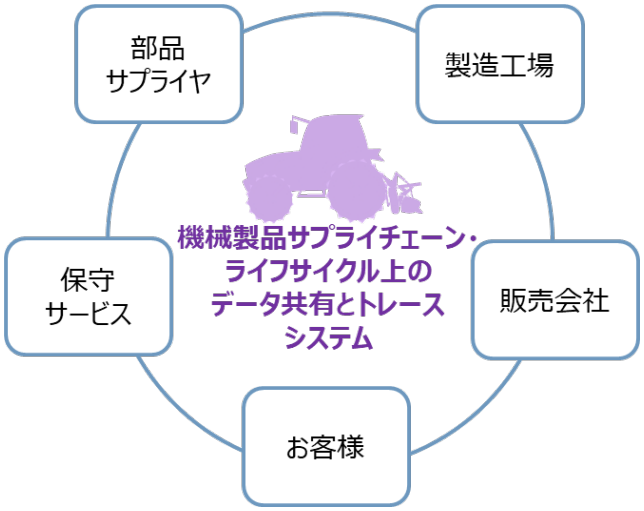

図 4.1-1 理想の姿

表 4.1-1 ユーザーのベネフィット

ステークホルダー	ベネフィット	負担するコスト
サプライヤー	• 調達部品の情報の信頼性を確認できる • 自社の部品情報の信頼性が向上する • 納品した部品を追跡できる	システム利用料等
製品工場	• 調達部品の情報の信頼性を確認できる • 自社の部品情報の信頼性が向上する • 納品した部品を追跡できる	
販売会社	• 販売する製品の信頼性を確認できる	
保守サービス	• 製品や部品情報の信頼性を確認できる • 過去の保守履歴の信頼性を確認できる • 自社の保守情報の信頼性が向上する	
お客様	• 製品に関する情報の信頼性を確認できる	負担なし

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

本実証を通じて判明した 6 つの課題について、以下に述べる。

課題１ ユースケースの拡大

今回のユースケースはサプライチェーンの一部に過ぎないためさらに対象を拡げて検討する必要がある。また、机上検討に留まっているため、実際の利用者のニーズと擦り合わせながら、全体フロー、システム、ユーザビリティを確認し、改善していく必要がある。

課題２ モノのアイデンティティ

今回の“モノ”はIoTデバイスを対象としたもので演算処理（署名）ができるという前提に立っている。非 IoT デバイスのトレーサビリティ管理に本 UC を援用する場合は注意が必要になる。

課題３ 検証可能性

今回のプロトタイプシナリオでは、やり取りされるデータ自体と署名者自身については検証可能である。ただし、リペアショップやメーカーなどの法人あるいは組織内の担当者の正当性までは検証できていない（未検討である）。

課題４ 合意の履行のトレース、合意取り消しのトレース

合意の履行のトレースは合意主体間でのみ可能であり、第３者によるトレースはできないことになっている。合意の取り消しについても同様であり、特に合意の取り消しの事実を、当事者からの連絡以外に第３者が知る手段は提供できていない。合意の履歴をブロックチェーン上に記録するなどの対応が必要と考えられる。

課題５ システム実装

ブロックチェーンの利用を鍵管理に限定することによりシステム全体のレスポンスの向上を図ったが、その反面、鍵管理以外の機能をすべてアプリケーション側で実現させることになった。これは開発コストの増大につながる。また、サプライチェーンの参加者によって負担できるコストは異なるため、中心的な推

進プレーヤーを設けない場合には、必要とする *Trust* のレベルと、そのために開発すべきシステムの規模を参加者それぞれが判断する（判断できる）必要がある。

課題６　ビジネスモデル

ビジネスモデルについては、各エンティティで使用するアプリケーションやシステムを誰が開発し、配布、運営するのかが課題となった。参加者間でのコスト負担の考え方について整理が必要である。

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

今回の検討結果を基に、サプライチェーン全体がカバーされるよう他のユースケースについても検討を行う。また机上検討から実地検討への移行も必要であり、今後協力先を探しつつ、複数の参加者による連携や実証を模索する。ただし、本格展開についてはシステム的な課題も合わせて解決する必要があるため、中期的な取り組みになると見込まれる。

- ✓ サプライチェーン上の他のユースケースの検討
- ✓ 適切なシステム実装の規模の見積もり
- ✓ 試験導入（一部トライアル）
- ✓ 展開・展開判断

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

- モノへのアイデンティティ
  - 自然人・法人とは異なり、モノには意思がなく単独では責任主体になりえないため、本ユースケースではモノのアイデンティティに対し、意思主体である機械ユーザーを関連付ける必要があると考えた。責任主体との関連付けがなければ、そのモノ自体のアクションの正当性が問われるケースなどが想定されうる。モノのアイデンティティの取り扱い方について考え方の整理が必要である。
  - モノはさらに、特に演算機能の有無により、IoT デバイスと非 IoT デバイスは分けて考える必要があると思われる。署名や検証、暗号処理を行えないデバイスは単独では Trust を保証する形でのデータのやり取りができないため、例えば製品のトレーサビリティにおいても、トレースできるモノの単位が製品の種別によって異なるものとなる。ほぼ同一のユースケースであっても、実際の実装面ではモノの種別によって大きな違いが出る可能性がある。

- トランザクション・ノード
  - トランザクションやノードにおけるデータのやり取りの記録や検証には大きなコストがかかるため、実装にあたってはそのベネフィットとの比較が必要である。また合意形成過程についても、仮にもし合意に至るまでのすべてのやり取りを記録するとするならば、同様にその必要性や効果およびそのためのコストを考慮して、実装の可否が判断できるようになっている必要がある。
  - またデータのやり取りの記録は、トランザクションとノードのそれぞれで定義されているため違いが分かりにくい。両者の記録の役割と、それぞれがそれぞれの目的に沿って記録すべきものが何かについて、違いを明確にする必要がある。

- 合意履行のトレースの明確化
  - 合意の履行については、何をどこまでトレースするのかというトレースの範囲と、誰がトレースすることを想定するのかというトレースの主体について明確さが必要と思われる。たとえば次のような論点が挙げられる。
  - トレースの範囲について
    - トレースすべきものとしては、日時や合意者などの合意事実だけとするケース、合意の内容までトレースするケース（変更履歴をトレースしたいというニーズがある場合に想定される）、合意の形成過程までトレースするケース（どのような交渉経緯や事情により合意がなされたかその過程を検証したいというニーズがある場合に想定される）などが考えられる。
    - 「合意履行のトレース」という概念に合意を履行しなかったことについてのトレースを含めるのかどうかを明確にしたい。仮に含めるとする場合にはそのトレースはいつ実施されること想定するかが実装上の課題になる。一般に合意がなされなかったという状況は、「合意の履行」の観点からは重要な事象であり、適時のトレースとさらには通知までなされることが実装要件になると考えられる。
    - 合意履行のトレースにはどこまでの確からしさを求めるかが課題になるが、なかでも、正しく履行されたのかどうか、また履行されたという債務者側の主張が本当に真実かどうかを正確に判断することは難しい。ついては「合意履行のトレース」という場合、それはどこまでの真実性や確実性が確認できたことをもって「トレースができている」ということにするのか、なんらかの共通の認識があった方が良い。
  - トレースの主体について
    - 合意履行のトレースについては誰がそのトレースを行うのか、そのトレースの主体についても考える必要があるのではないか。主体としては、合意を行った当事者間でのみトレースできれば良いケース（本ユースケースはこちらに相当）、合意に関わらなかった第 3 者によってもトレースを必要とするケース、などが考えられる。
    - さらに後者すなわち、第 3 者によるトレースを想定もしくは許容する場合には、そのトレースを行って良いとするかどうかを合意当事者がコントロールしたいケースも想定されうる（合意のトレースの主体のコントロール）。

- 合意の取り消しの連鎖の取り扱い
  - 合意の取り消しについてはその取り消しが第 3 者に影響するケースが存在する。その場合どのようにその第 3 者がその取り消しを知りうるかという問題が出てくるたとえば、ある合意 A を前提としてなされた合意 A とは合意者の異なる別の合意 B について、合意 A が取り消された時に速やかに合意 B も取り消せるような仕組みをどのように実現するか、言い換えれば、ある合意の取り消しを、他のステークホルダーが、どのようにかつ速やかに認識できるかという問題について検討が必要と思われる。（本ユースケースの場合では、ショップがメーカーからデータの開示を受けた後で、ユーザーとの修理契約が取り消されていたといったケースが想定できる。また、本ユースケースでは合意の取り消しの合意を行うことで足りると考えたが、取り消しの合意を第 3 者が直ちに知りうる手段にまでは踏み込むことはできていない。）

5.2　その他 Trusted Web の課題と提言

- 実現のための推進力

　システムの構築には相応レベルの開発力が必要となる中、多種多様なプレーヤーが参加するサプライチェーンのようなユースケースにおいては、全参加者に一定レベルのシステム構築を求めるのは難しいと思われる。また、システムの構築には一定の投資や維持コストが発生する中で、Trust 実現までの間、中心的なエンティティを前提とせずに全体の推進力をどこまで確保できるのかは明確ではない。（今回の本ユースケースにおいてはアプリケーションを誰が開発・配布・維持・保守するのかが課題として残った。）

- システム開発コストの抑制

　システム構築コストの低減のためには、考え方や要求仕様の提示だけでなく、リファレンスソフトウェアや共通ライブラリあるいは何らかのソフトウェアプラットフォームなど、実装レベルで共有できるソフトウェア資産の提供が望まれる。

　また、システム規模については、ユースケースや事業ごとに、それぞれのコストベネフィットに応じた見極めが必要になると思われるため、Trusted Web の各構成要素に対して実装のレベルや可否を事業者が判断できるように、それぞれの実装の必要性がその効果と合わせて明確になっていることが求められる。

以上