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

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

ヤンマーホールディングス株式会社

2023年3月24日

目次

01

背景・目的

1.1 背景･目的

背景

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。

目的

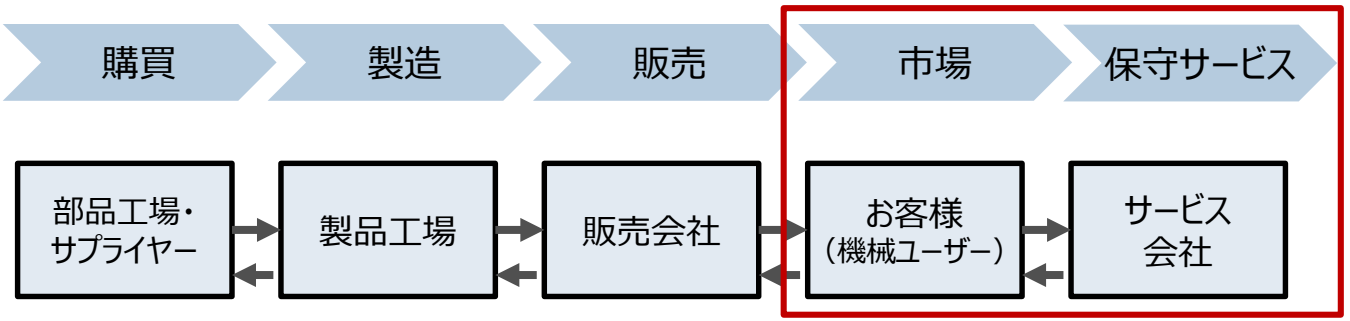
以上を背景に本ユースケース実証では、機械製品など工業製品のサプライチェーン上で発生するデータを対象として、安全にデータのやり取りが行える仕組みを検討することを目的として実施した。

02

実証の概要

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。

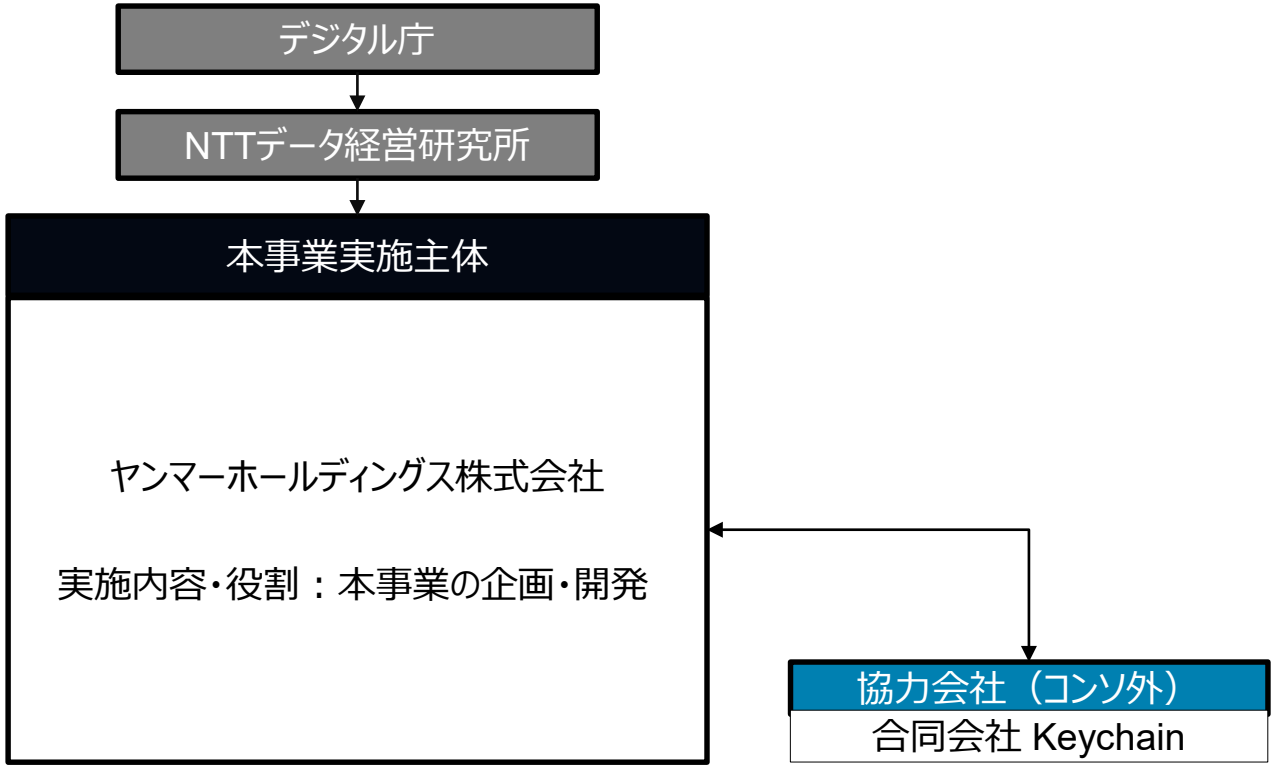


(注)サービス会社とは、機械製品の修理（リペア）やメンテナンスを行う会社や事業所を指し、以降はリペアショップと呼ぶ。

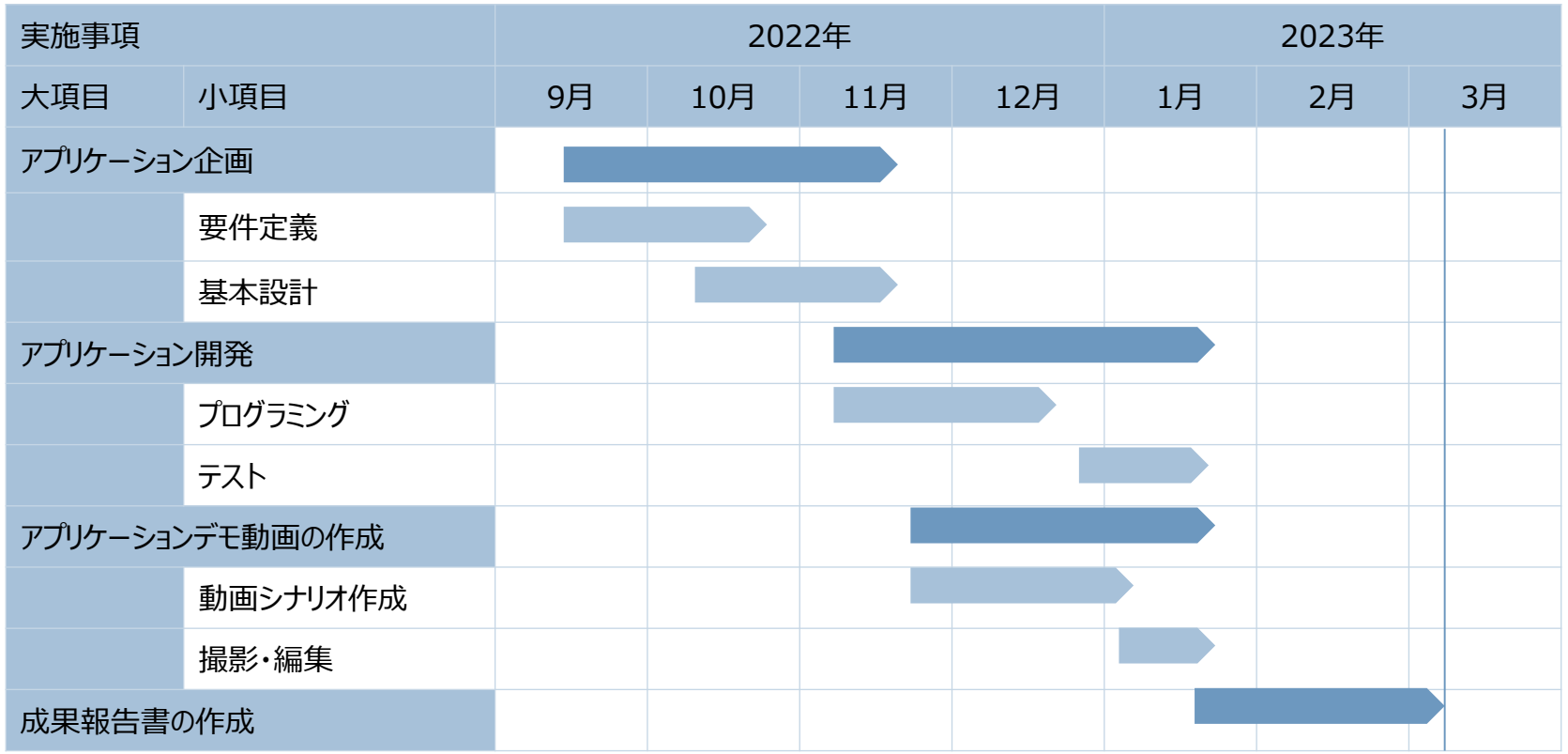
2.2 社会・経済に与える価値・影響

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



2.4 実証全体のスケジュール



03

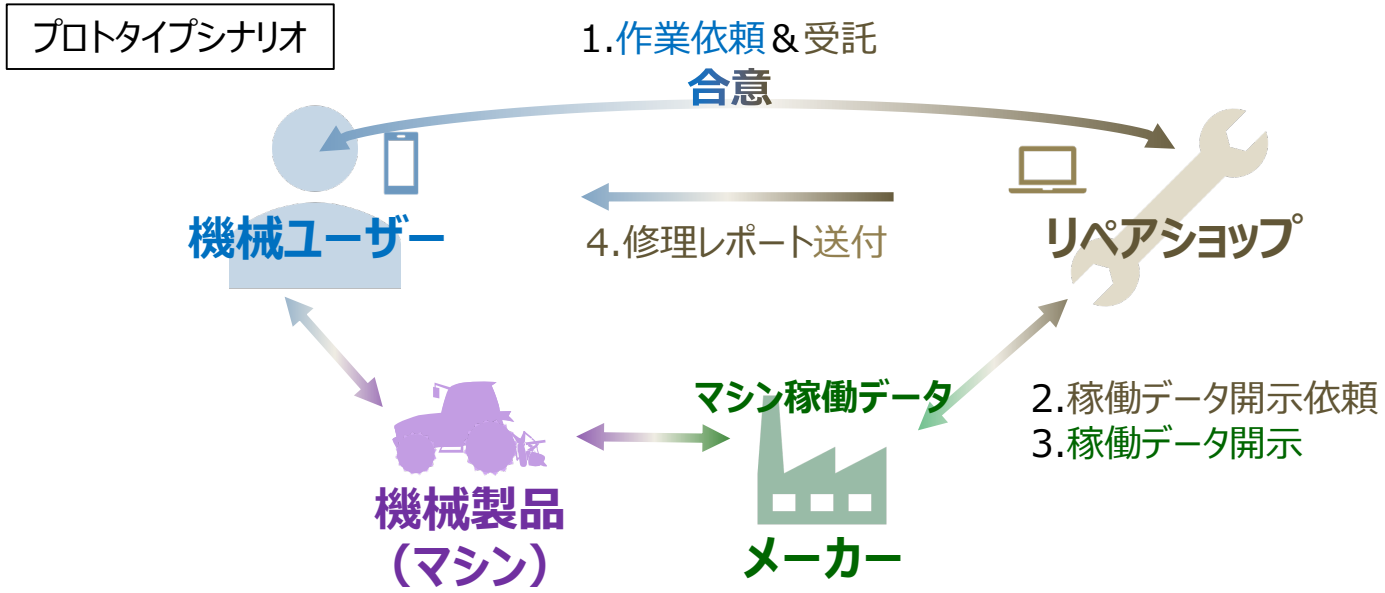
実証内容

3.1 実証の実施事項、論点及び判断

実施事項（プロトタイプシナリオ）

本ユースケースでは、機械（マシン）の保守サービスの修理依頼シーンにおけるデータ共有の仕組みの検討並びにプロトタイピングを行った。

1. 機械ユーザーが専用アプリでリペアショップを選択し修理を依頼する。リペアショップは修理依頼を受託すると、修理依頼に関する合意が成立する
2. リペアショップは稼働データを保有者するメーカーへ対象マシンの稼働データの開示を依頼する
3. メーカーは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し、対象マシンの稼働データをリペアショップへ開示する
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



3.1 実証の実施事項、論点及び判断

プロトタイプシステムの企画・開発 1

実施事項	論点	判断
要件定義	対象とするシーン	製品ライフサイクルの中でUCを一部に限定する必要があり、今回は修理シーンを取り上げた
	データコントロール （相手先の選択） （開示データのダウンロード）	データの提供者はデータの開示先をUI上で選択できるようにした。また鍵ペア方式の採択により選択した相手のみがデータを閲覧できる 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	各エンティティのデータは各エンティティが保管し必要な場合に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署名をメーカーにて検証することとした
	モノのアイデンティティ	モノのアイデンティティは、意思をもつ主体（機械ユーザー）と紐づけることとした
	データモデル	修理依頼合意書データは、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、機械ユーザーとリペアショップの両者の共有とした
	アイデンティティの発見	業務フローの中で発見プロセスを実現する。マシンとメーカーについては出荷時にペアリングする。機械ユーザーとマシンはマシン販売時にペアリングする。ショップとユーザーは、ショップDIDは機械ユーザーがアプリ上でショップ選択時に通知し、ユーザーDIDは修理依頼時に依頼先ショップへ通知する。メーカーとリペアショップは、メーカーDIDはショップアプリに初期登録し、リペアショップDIDはデータ開示依頼時にメーカーへ通知する
	検証可能性の担保	署名自身の検証を行う。署名者自身の検証はマシンと機械ユーザーについては可能と判断。
	合意形成の方法	機械ユーザーとリペアショップの修理委託に関する合意については、合意条件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とした
	合意形成に伴うやりとり記録	今回のUCにおいて合意形成過程でのやり取りの重要性は低く、またメッセージのやり取りを事後に検証する必要性も薄いと考え、やりとりの記録は行わないこととした

3.1 実証の実施事項、論点及び判断

プロトタイプシステムの企画・開発 2

実施事項	論点	判断
	合意の履行のトレース	合意の履行状況を各アプリのUI上に表示することでトレースを実現した
	合意の取り消し	取り消しの合意をもって代用できると判断した
	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、機械ユーザーのマシンの所有事実を示すことであると理解されうると判断した。ユーザインターフェース上では特に署名を意識させる必要はなく、一般的な表記とした（「機械を登録」）。
	スキームの拡張性 （機械ユーザーの変更等）	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、機械ユーザーの変更、盗品等不正対象品の修理依頼防止、リペアショップによるデータ不正要求の防止　などにも対応可能と判断した
基本設計	鍵の管理	鍵の管理はブロックチェーンで行い、ライブラリとしてKeychainを用いた。
	DIDの発行	マシンもエンティティとしてDIDを発行することで、データ公開先の制御が可能となる。また所有者（機械ユーザー）変更時にも同一マシンとして履歴のトレースを実現した。
	データの保管場所	各アプリのデータの保管場所は一元管理ではなく各アプリサーバーとし、さらにデータの保有者ごとに管理されるようにした。

3.1 実証の実施事項、論点及び判断

ヒアリングの実施

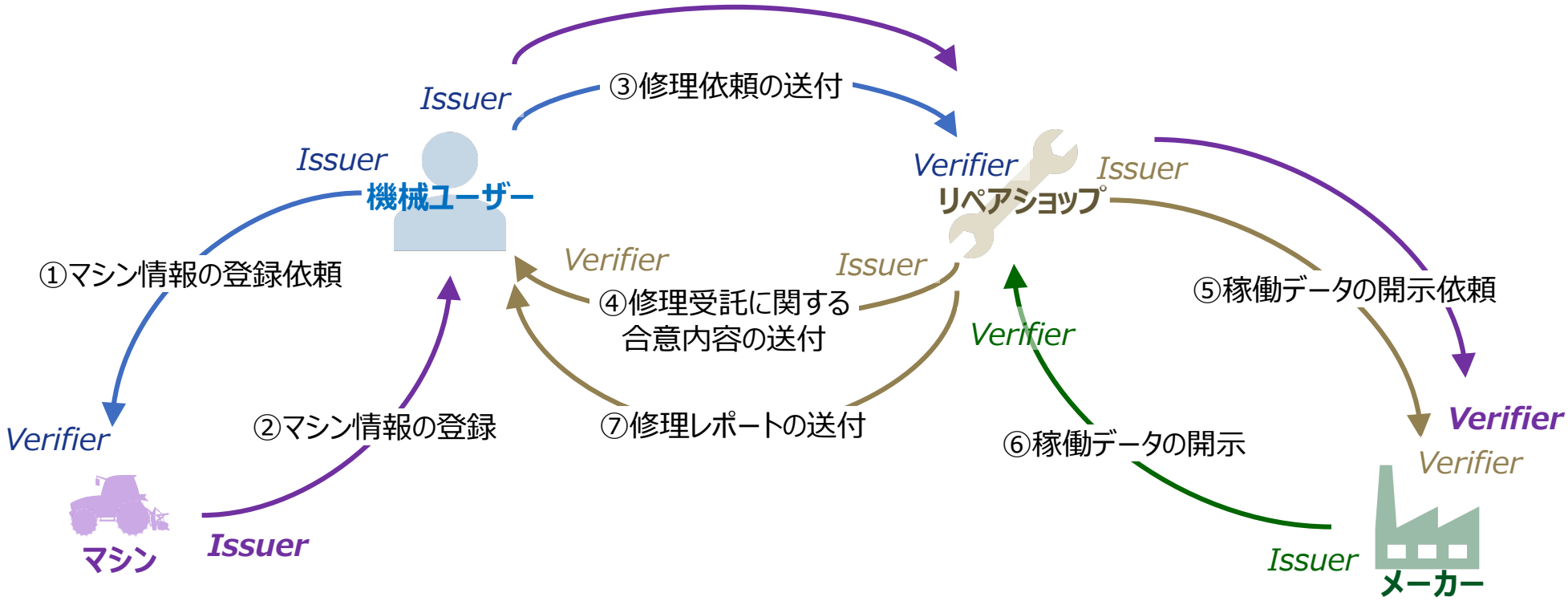
本ユースケースに関するヒアリングを実施していない

国際標準規格の調査

国際標準規格の調査を実施していない

3.2 検証できる領域を拡大する仕組み

データスキーム



※各エンティティ間のデータの授受には、それぞれ暗号化と署名検証を行う
※エンティティ間のデータのやりとりにおいて発行者（Issuer）はデータの送付側、検証者（Verifier）はデータの受領側となる
※マシンによる署名はメーカーが検証する

3.2 検証できる領域を拡大する仕組み

登場する主体とその概要

主体	役割・設定
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、自身が望む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領し、受託する場合は受領し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利用する。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	マシンを製造した法人である。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Verifierの役割を果たす。

データへのアクセス

- データのアクセスコントロールはそのデータの保有者のみが可能である
- データは各端末内のストレージもしくは各アプリサーバーに保管される。保管されたデータはデータ保有者のみがアクセス可能である
- データは暗号化してやり取りされる（開示相手の公開鍵で暗号化され送付される。開示された相手のみが閲覧できる）
- 提供される各データには閲覧期限が設定される。またデータのダウンロードは禁止される

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
依頼の正当性（機械の保有）	機械が署名した事実	署名検証 (マシン署名/メーカー検証)	メーカー	ショップ ユーザー	マシン	ショップサーバー ユーザーデバイス	アクセス可能：ショップ、ユーザー アクセス制御：暗号化
修理依頼内容の正当性	ユーザーの最終依頼内容	署名検証 (ユーザー署名/ショップ検証)	ショップ	ユーザー	ユーザー	ユーザーデバイス	アクセス可能：ユーザー アクセス制御：暗号化
受託内容の正当性（合意内容の確定）	ショップの受託内容	署名検証 (ショップ署名/ユーザー検証)	ユーザー	ショップ ユーザー	ショップ	ショップサーバー ユーザーデバイス	アクセス可能：ショップ、ユーザー アクセス制御：暗号化
稼働データ開示依頼内容の正当性	メーカーへの依頼内容	署名検証 (ショップ署名/メーカー検証)	メーカー	ショップ	ショップ	ショップサーバー	アクセス可能：ショップ アクセス制御：暗号化
提供データの正当性	メーカーが提供する稼働データ	署名検証 (メーカー署名/ショップ検証)	ショップ	メーカー	メーカー	メーカーサーバー	アクセス可能：メーカー アクセス制御：暗号化
修理レポートの正当性	ショップが提供する修理レポート	署名検証 (ショップ署名/ユーザー検証)	ユーザー	ショップ	ショップ	ショップサーバー	アクセス可能：ショップ アクセス制御：暗号化

注：ユーザーは機械ユーザー、ショップはリペアショップの略

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
ユーザーとショップ	修理箇所 金額 納期	一方が条件を提示し、もう一方がその条件を承諾することを以て合意とする（双方の合意意思の提示）	履行された左記の合意に基づく修理の状況	ユーザー	ユーザーアプリのUIに履行履歴を表示しユーザーが確認できる	合意の取り消しの合意を行うことにより可能（プロト実装外）
ショップとメーカー	稼働データの開示	ショップが送付した稼働データ提供依頼に対して、メーカーが正しい依頼であることを確認（マシン署名を検証）した上で合意する	左記の合意に基づく提供履歴	メーカー	メーカーアプリのUIに履行履歴を表示し、メーカーが確認できる	合意の取り消しの合意を行うことにより可能（プロト実装外）

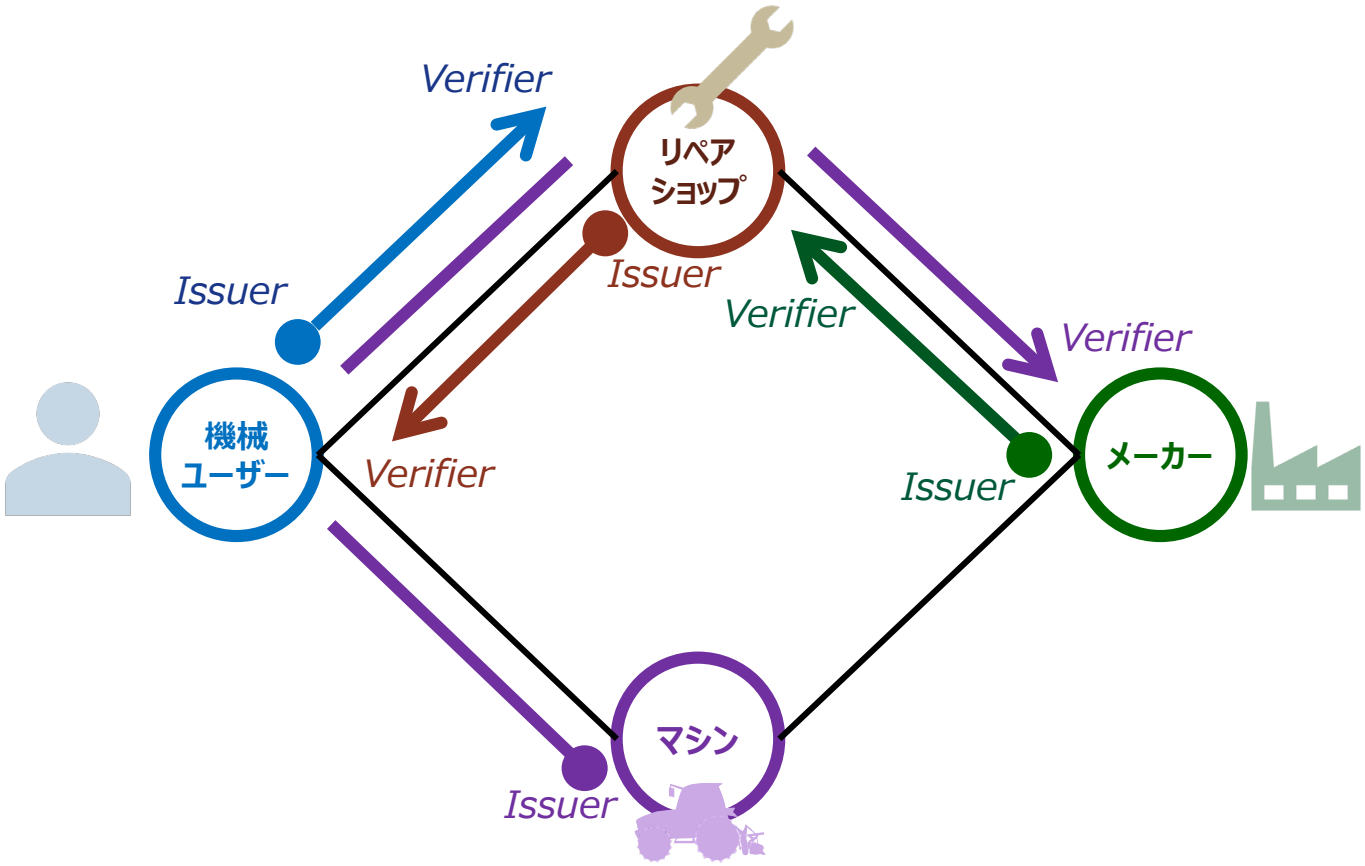
注：ユーザーは機械ユーザー、ショップはリペアショップの略

3.3 6構成要素との対応

構成要素	各構成要素との当てはめ	
検証可能なデータ	検証対象	①マシンが署名した事実 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
	署名者	①マシン ②ユーザー ③ショップ ④ショップ ⑤メーカー ⑥ショップ
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	ユーザー、ショップ、メーカー、マシン
	アイデンティティ管理システム（外部）は何か。 (例：OIDC for VC, DID)	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
	アイデンティティグラフとして想定されるのはなにか	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。
ノード	Walletか否か	Wallet（各エンティティのDIDに紐づいた鍵ペアと情報を管理する）
	合意形成がされているか、およびその手段	URI情報の交換によるペアリングによってペアリングした相手（DID）のみが復号できる
	データのやりとりをどこに記録するか	記録しない
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	どちらも可能であるが、基本はメッセージオリエンテッドである
トランザクション	データのやり取りを記録するか	記録しない
	データのやり取りの検証はできるか	合意の履行状況については、アプリ上で確認可能とする 合意前のやりとりは本UCではシナリオ上必要性がないため実装していない
トランスポート	トランスポートのプロトコルは何か	機械ユーザーデバイスとマシン間は近接無線通信、 その他はインターネットを想定する

注：ユーザーは機械ユーザー、ショップはリペアショップの略

3.3 6構成要素との対応 アイデンティティグラフとデータのやり取り

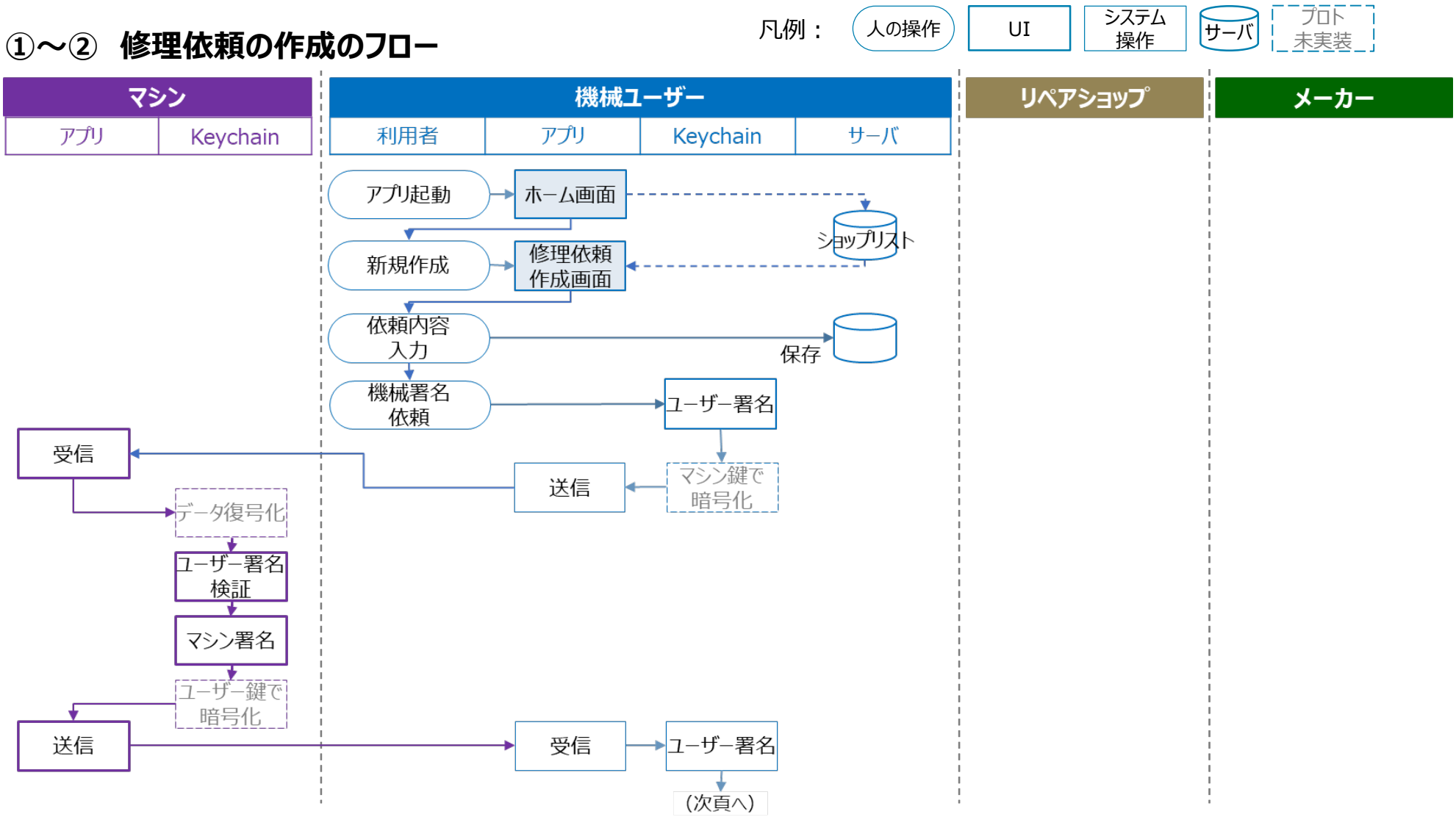


→ マシン署名検証に関するデータのやり取り
→ 機械ユーザーとリペアショップのデータのやり取り（修理依頼書）
→ メーカーとリペアショップのデータやり取り（稼働データ）
→ リペアショップと機械ユーザーのデータやり取り（合意書/修理レポート）

※メーカーと機械ユーザー、リペアショップとマシンは互いに不可視である

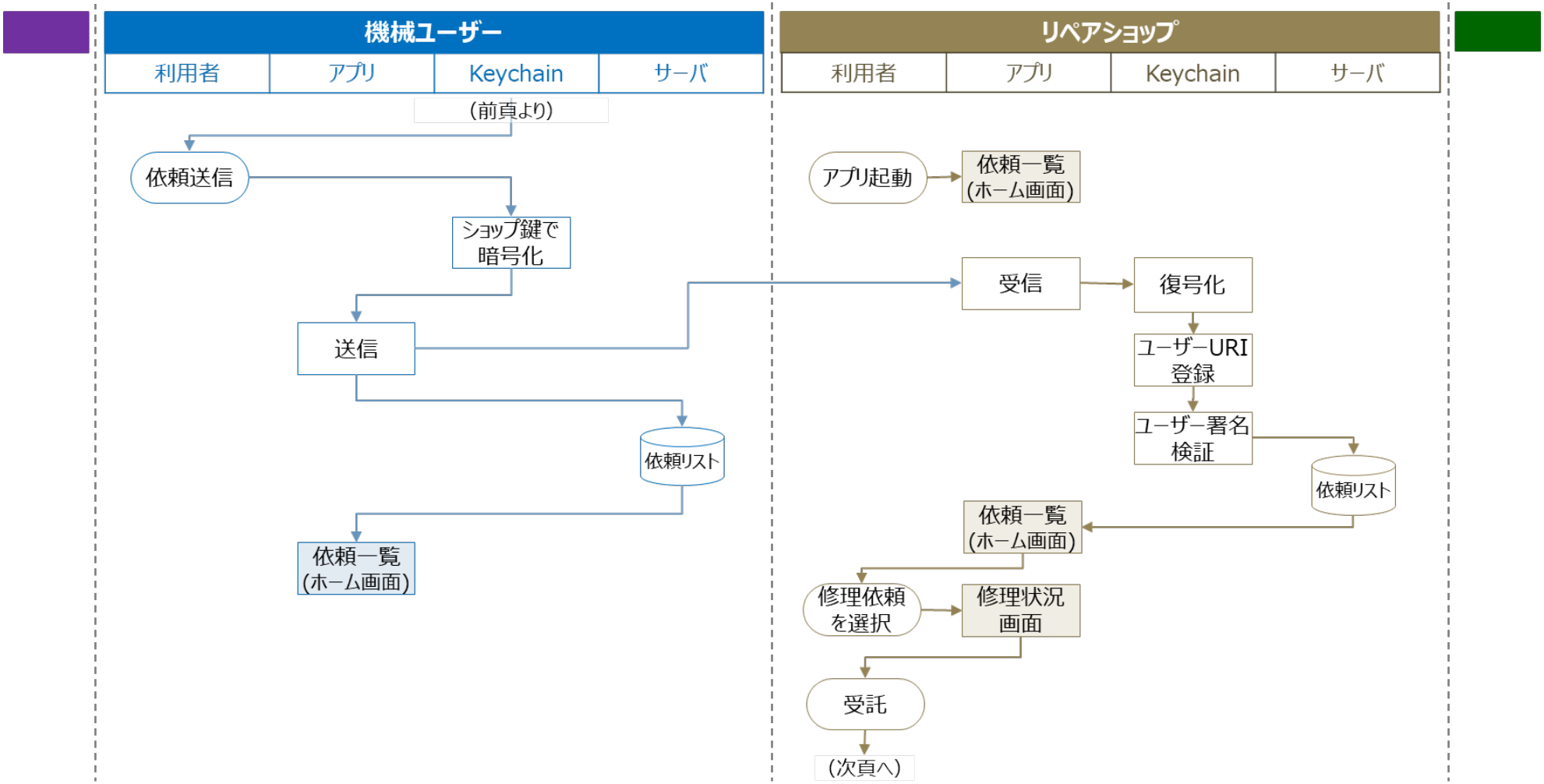
3.4 本実証で企画・開発したシステムの概要 業務フロー①②

①～② 修理依頼の作成のフロー



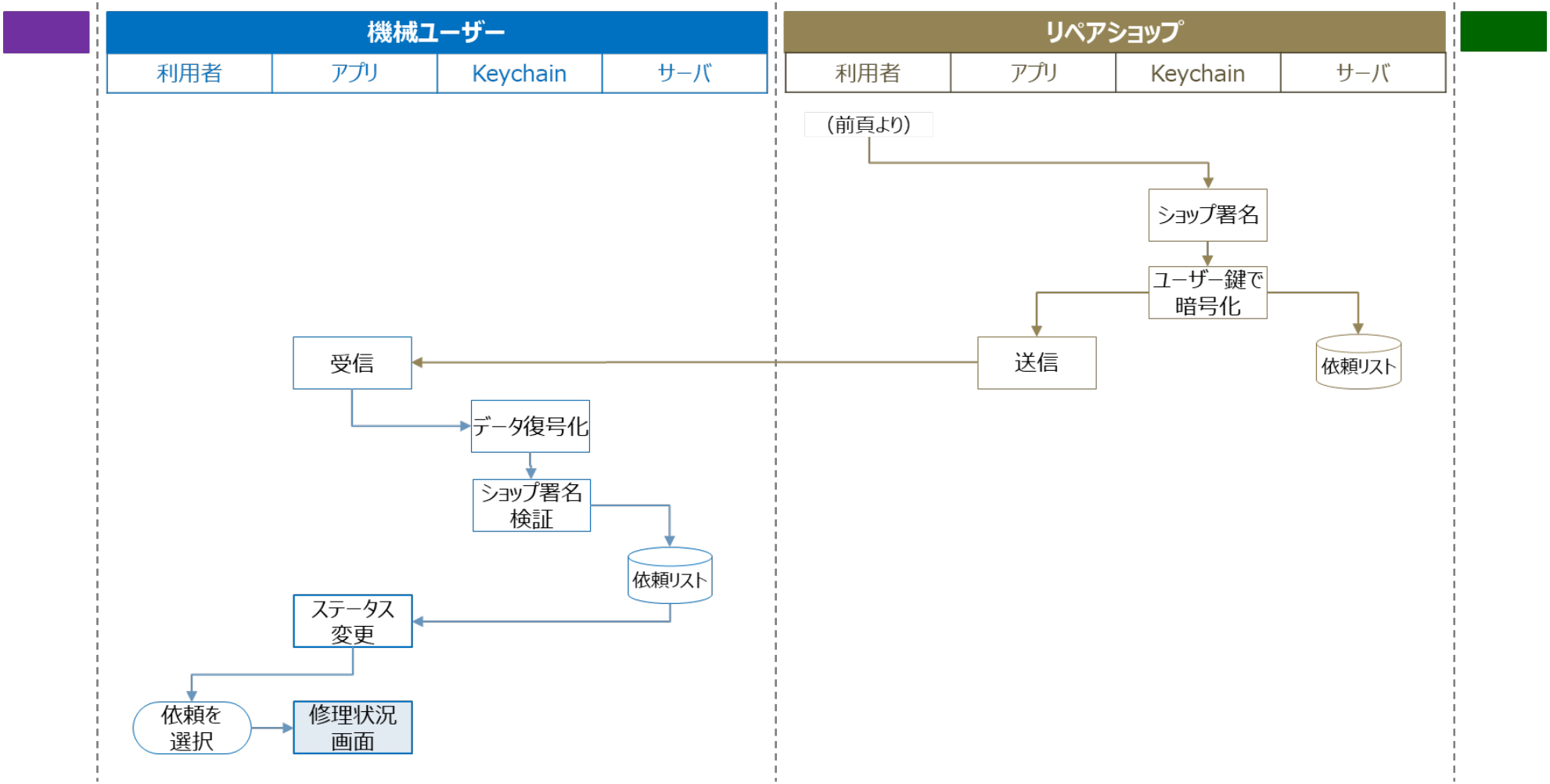
3.4 本実証で企画・開発したシステムの概要 業務フロー③

③ 修理の依頼から受託までのフロー



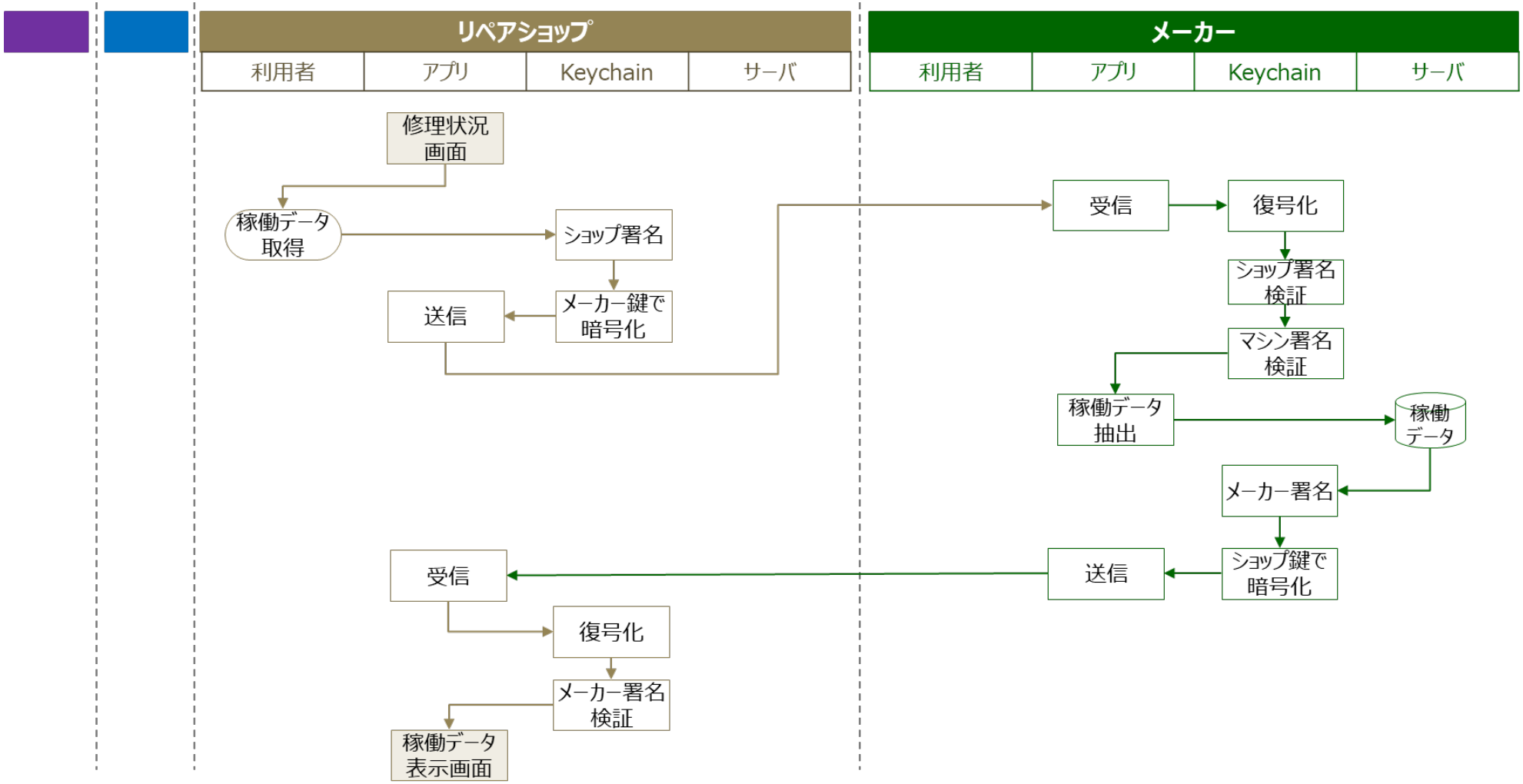
3.4 本実証で企画・開発したシステムの概要 業務フロー④

④ 修理の合意のフロー



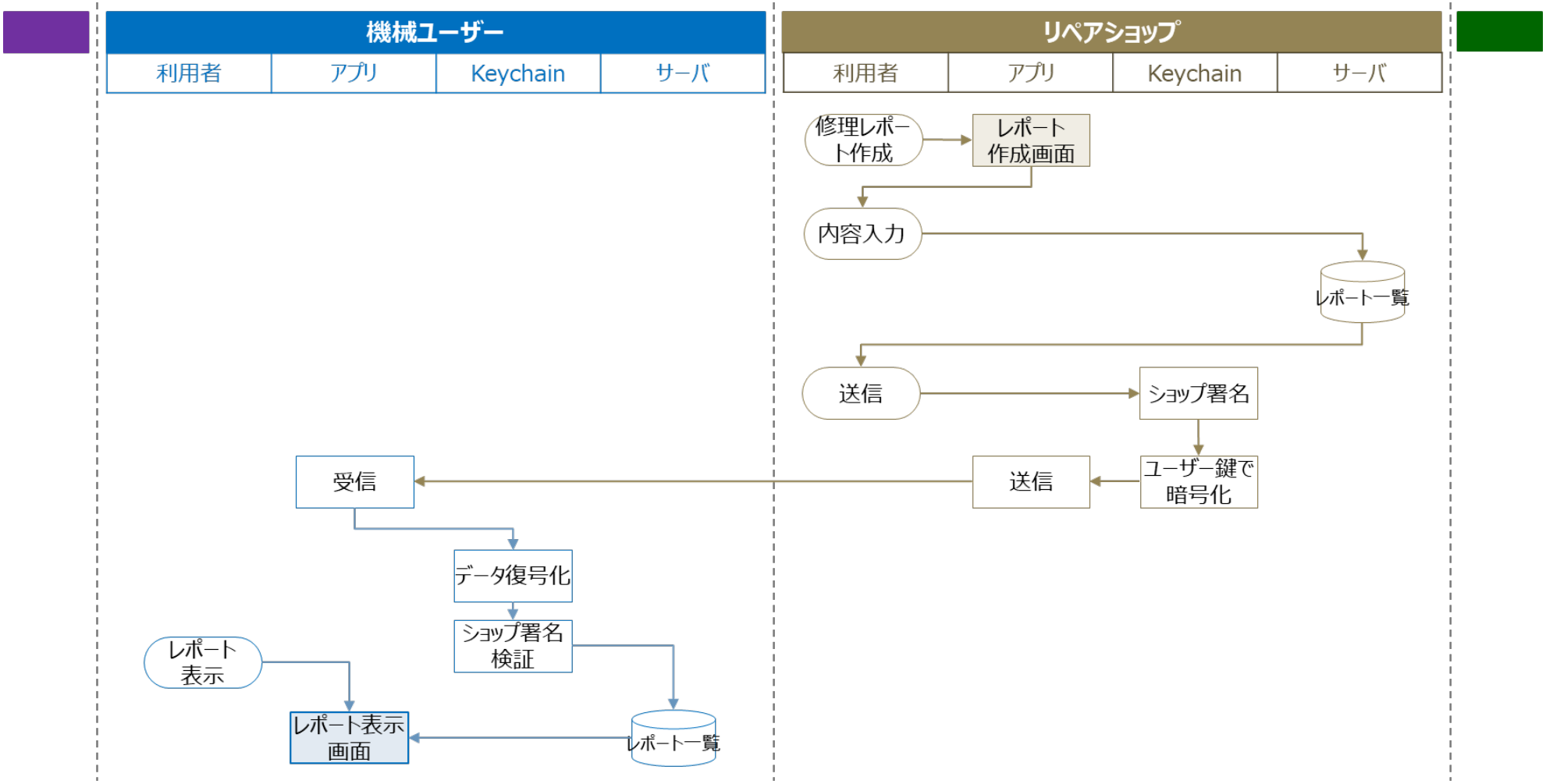
3.4 本実証で企画・開発したシステムの概要 業務フロー⑤⑥

⑤～⑥ 稼働データの依頼から提供までのフロー



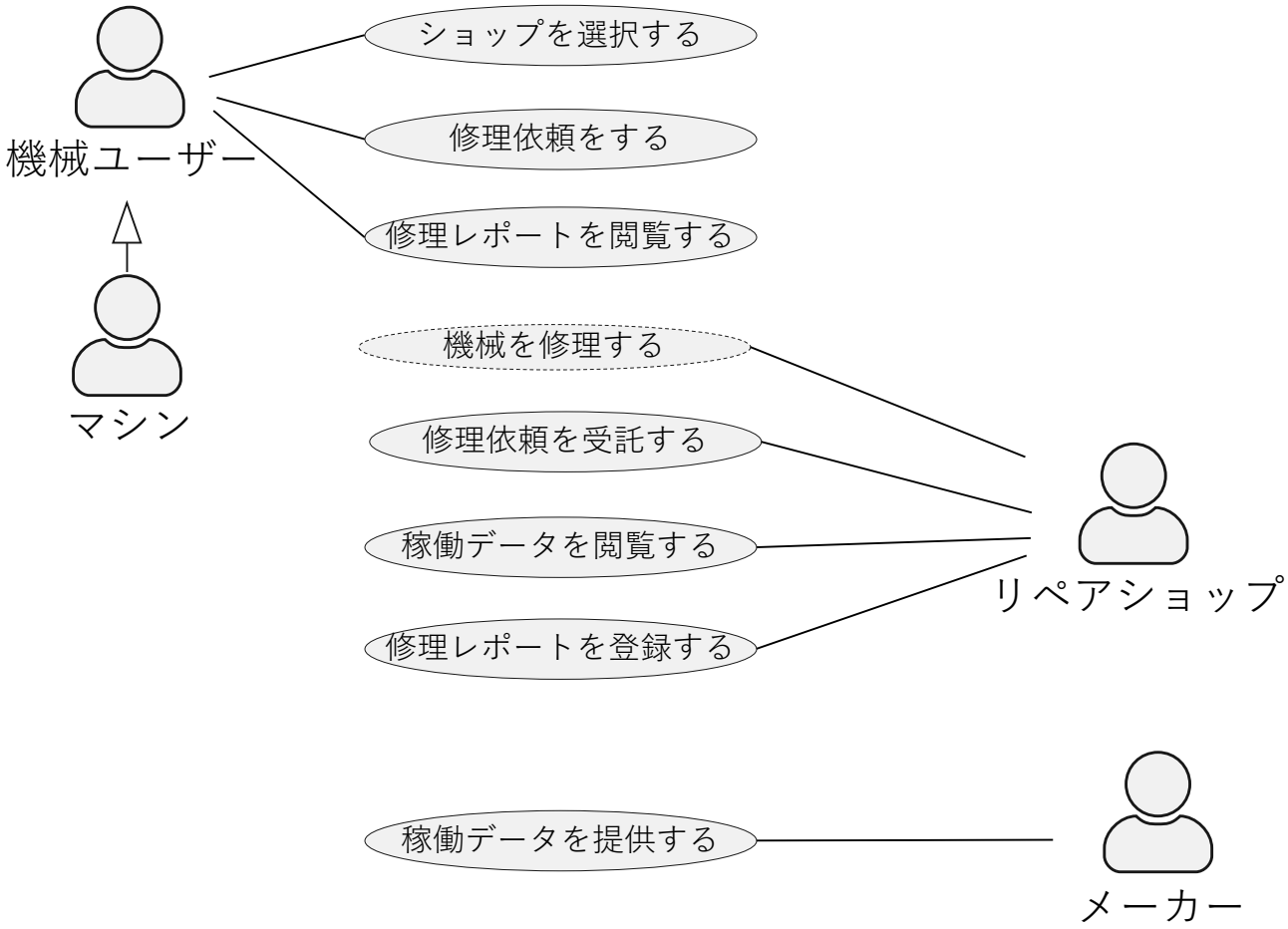
3.4 本実証で企画・開発したシステムの概要 業務フロー⑦

⑦ 修理レポート送付のフロー



3.4 本実証で企画・開発したシステムの概要 ユースケース図

ユースケース図



3.4 本実証で企画・開発したシステムの概要 ユーザインターフェース

ユーザインターフェース（操作画面）

機械ユーザアプリ

修理依頼

リペアショップアプリ

修理受付状況

メーカアプリ

稼働データの提供状況

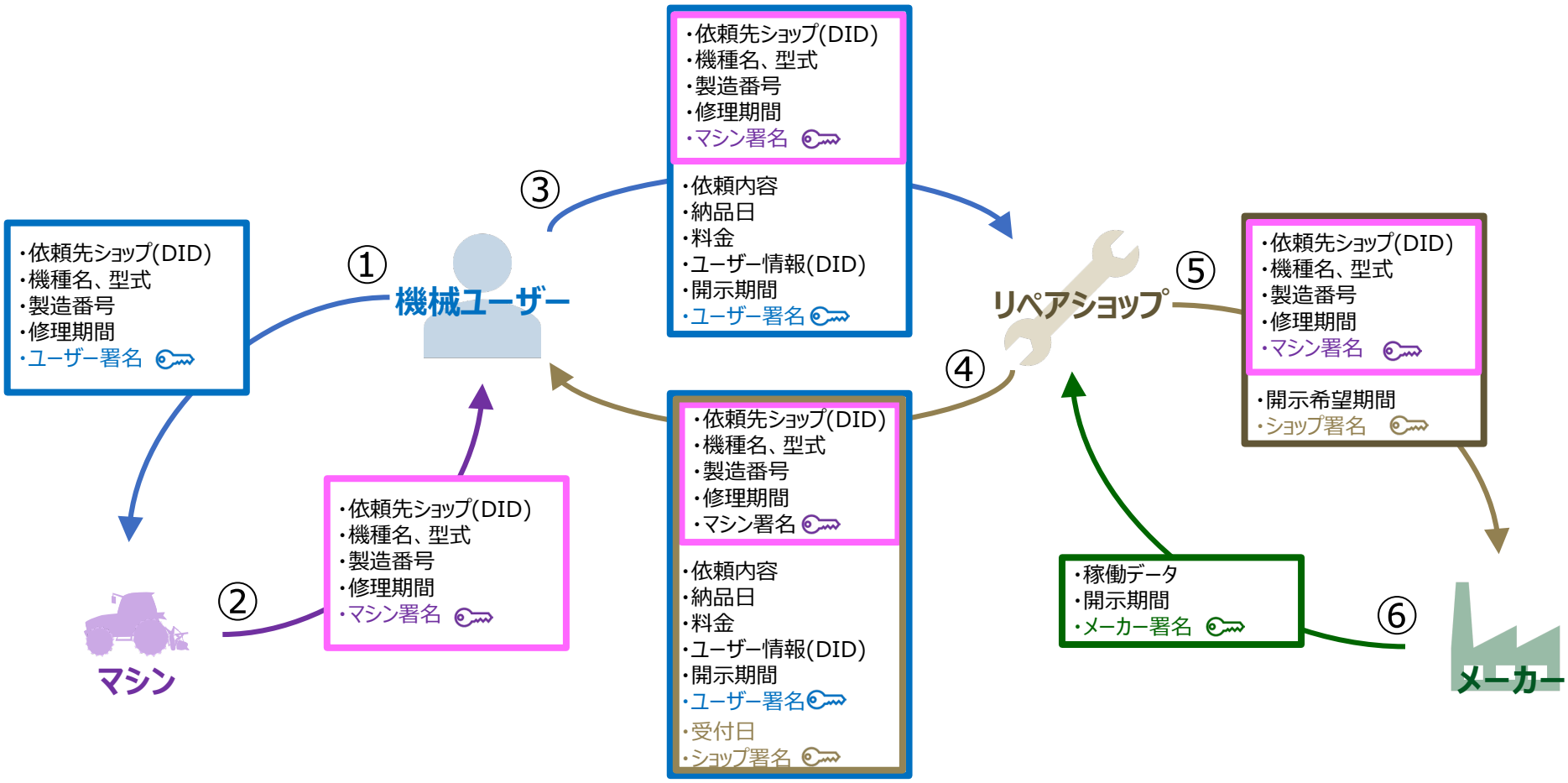
3.4 本実証で企画・開発したシステムの概要 機能一覧

機能／非機能 一覧

機能／非機能	機能名	機能概要
機能	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レポート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レポートを閲覧できる
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	データの秘匿性確保、データ保有者によるデータ開示範囲の設定

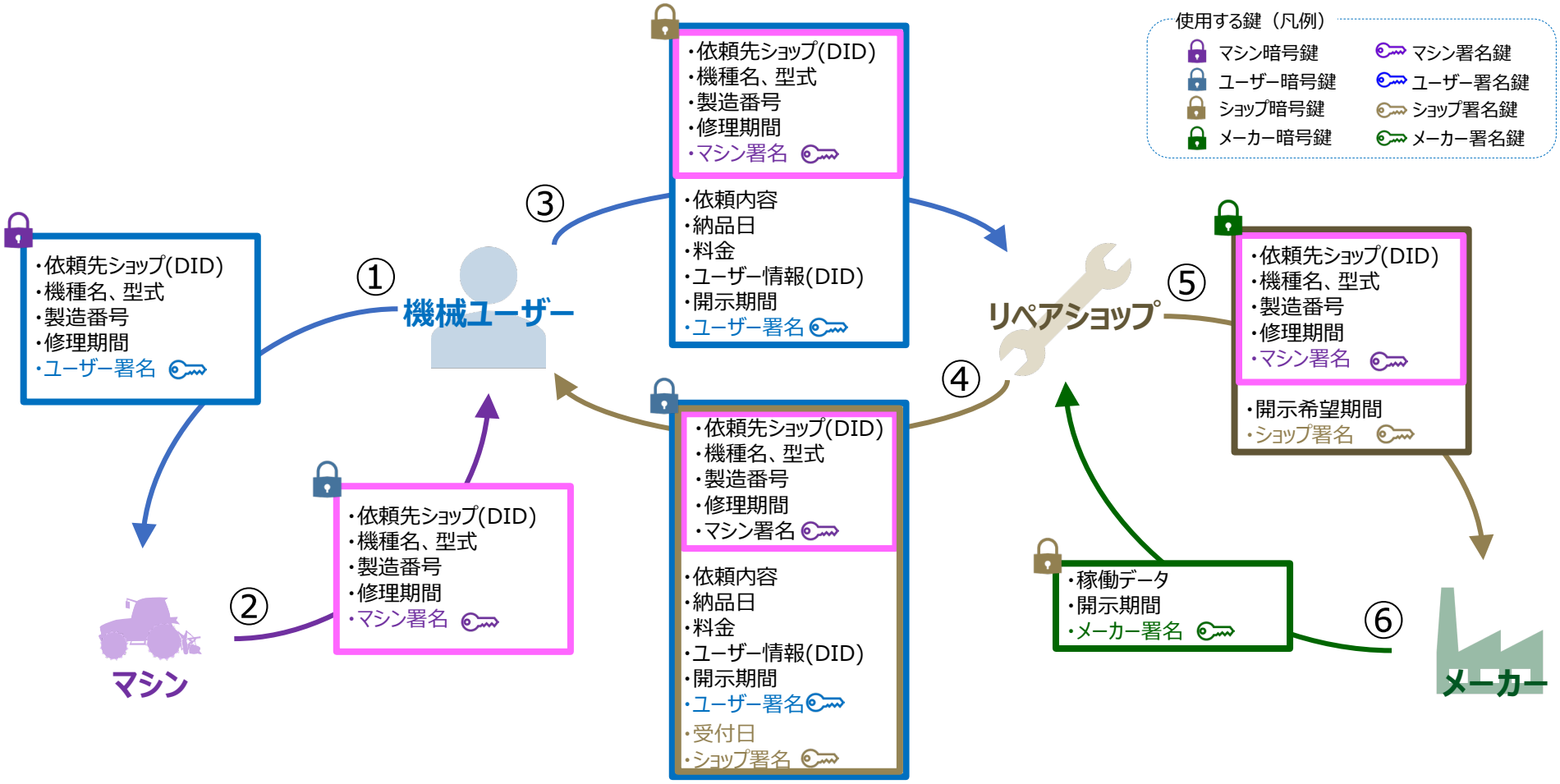
3.4 本実証で企画・開発したシステムの概要 データモデル

データモデル



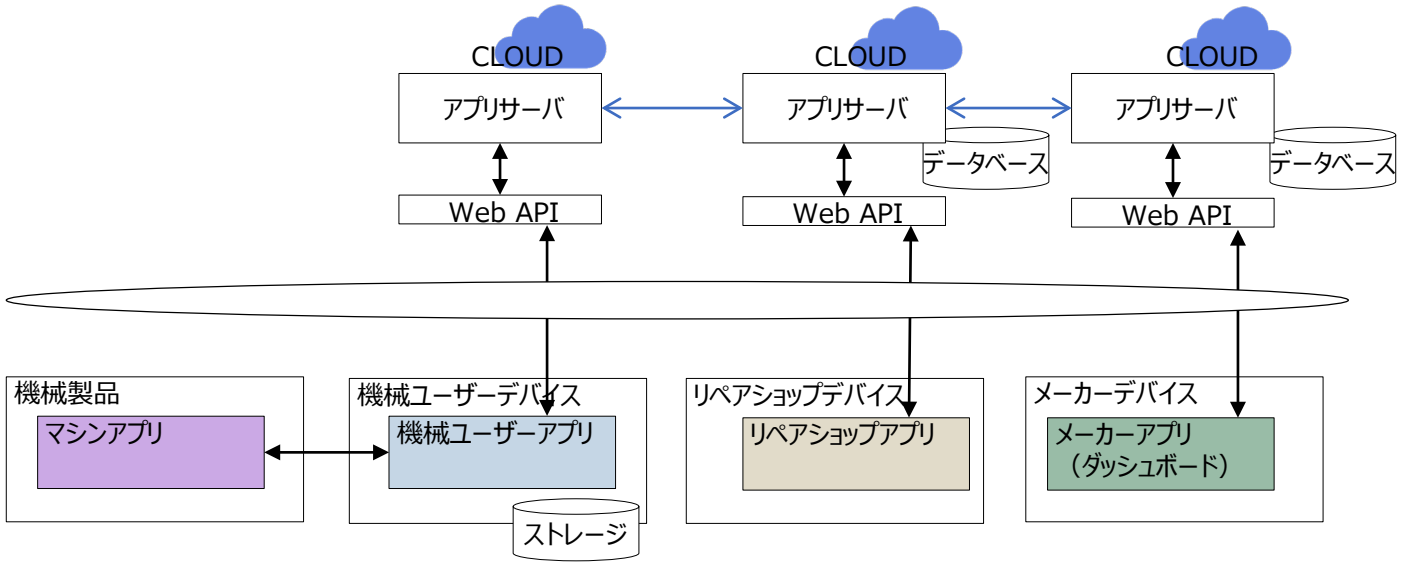
3.4 本実証で企画・開発したシステムの概要 やりとりされるデータ

データモデル（やり取りされるデータ）



3.4 本実証で企画・開発したシステムの概要 実験環境

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
Keychain	–	Keychain社の権利	有償
Amazon Web Services (AWS)	–	Amazon Web Services 社のサービス	有償（クラウドサービス利用に基づく従量課金）
VcXsrv	–	OSS	無償（GPLv3）

3.5 実証を通じて得られた主な成果

システムの企画・開発に関する成果

- 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企画し、プロトタイピングを行った。
  - ✓ 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
  - ✓ モノ（マシン）へのアイデンティティ付与
  - ✓ モノ（マシン）と法人・自然人とのペアリング：モノと責任主体との紐づけ
  - ✓ モノ（マシン）のトレーサビリティの確保：モノのDIDはライフサイクル上で同一
  - ✓ エビデンス検証に基づくデータ開示コントロール：データの開示先と開示根拠の検証
  - ✓ アイデンティティの可視範囲の局所化

ビジネスモデルに関する成果

- 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に関する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抽出された。
  - ✓ アプリケーションの提供主体
    アプリケーションを誰が開発、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、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の構築を求めることは難しい。またシステム構築の投資負担に耐えられるような中心的なエンティティを設定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。
  - ✓ 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と、システムが過大にならないよう、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毎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

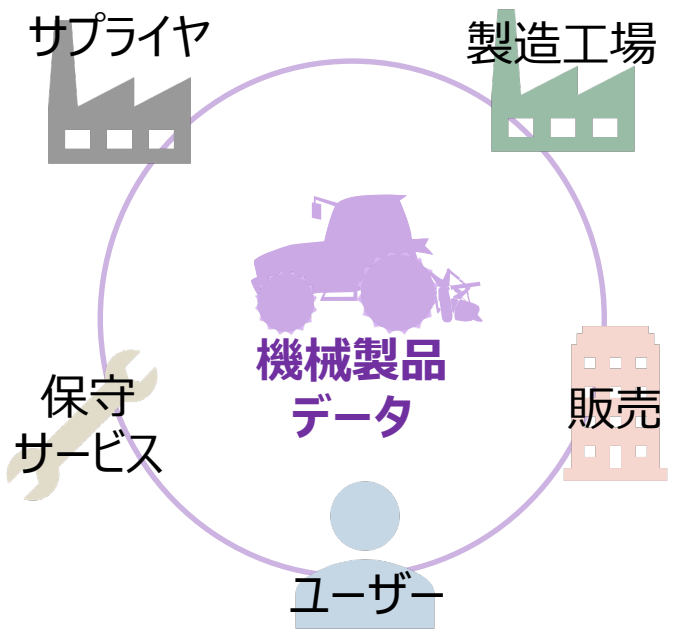
- 本実証事業で開発したシステムは、手順書（README）に沿って環境構築を行うことにより再現が可能である。ただし、本システムの一部はKeychain SDKを使って動作するため、同社のSDKライセンスを入手する必要がある。

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

理想の姿



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
サプライヤ	• 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

- 課題１　ユースケース
  - 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。農作物など非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
  - データ自体の検証は可能である。また署名者自身の検証についても、マシンやユーザー（本人確認、存在証明）の検証は可能である。ただし、ショップやメーカなどの法人・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）。
- 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
  - *Trust*向上と引き換えにシステム規模が増大する可能性がある。ユースケースや事業者によって必要となる*Trust*のレベルや負担できるコストは異なるため、アーキテクチャの指針としては、*Trust*のレベルとそのために開発すべきシステムの規模をそれぞれの事業者が判断できるようになっている必要がある。
- 課題６　ビジネスモデル
  - 各エンティティで使用するアプリケーションを誰が開発し、配布、維持、運営するのか、という課題が残った。

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

今年度のユースケース検討結果を基に、次年度以降グループ内外との連携や実証を模索する
次年度も継続して検討を行っていくが、本格展開には中期的な取り組みが必要である

- 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）
- 展開判断と展開

05

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に対する考え方
  - 自然人・法人とは異なりモノには意思がなく責任の主体とはなりえない。*IoT*デバイスなどモノ自体が生成するデータの信頼性や、署名行為などのアクションの正当性を確保するには、例えば他の責任の主体との関連付けが必要となる

- メッセージのやりとりの記録のコストベネフィット（トランザクションおよびノード）
  - 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。合意形成過程においても合意に至るまで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されなければならない。

- 合意履行のトレースの範囲とトレースの主体の明確化
  - 何をどこまでトレースすべきか（トレースの範囲）
    - ✓ 合意の事実、合意の内容、合意の形成過程　等
    - ✓ 合意が履行されなかった場合
    - ✓ 履行内容の適切さ、履行事実の確認
  - 誰がトレースを行うことを想定するか（トレースの主体）
    - ✓ 合意の当事者以外のトレースを認めるか否か．またそれを決めるのは誰か（トレース主体のコントロール）

- 合意の取り消しの連鎖の扱い
  - 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。例えば、ある合意*A*を前提とした合意者の異なる別の合意*B*について、合意*A*が取り消されたときに合意*B*も速やかに取り消せうるか

5.2 その他Trusted Webの課題と提言

Trusted 実現までのコストと推進力の確保が課題である

- 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運営・維持コストが必要となる中で、中心的なエンティティを設定せずに推進力をどこまで確保できるのかは明確ではない。

- 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。
  - 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。