

卒業論文 2025 年度 (令和 7 年)

コネクティッドカーにおける運転歴データの管理・提示システムの構築

慶應義塾大学 環境情報学部
仁戸田晃

卒業論文要旨 - 2025 年度 (令和 7 年度)

コネクティッドカーにおける運転歴データの管理・提示システムの構築

要旨

キーワード:

1. 卒業論文, 2. 村井純研究室, 3. RG, 4. LaTeX

慶應義塾大学大学 環境情報学部
仁戸田晃

Abstract of Bachelor's Thesis - Academic Year 2025

Building a System for Managing and Presenting Driving History Data in Connected Cars

I WILL WRITE ENGLISH.

Keywords :

1. Thesis, 2. RG, 3. Jun Murai Lab., 4. L^AT_EX

Keio University Faculty of Environment and Information Studies
Akira Nieda

目次

第1章 序論	1
1.1 はじめに	1
1.2 本論文の構成	1
第2章 背景	2
2.1 自動車の情報化	2
2.2 コネクティッドカーとテレマティクス	2
2.2.1 コネクティッドカーとテレマティクスの概要	2
2.2.2 テレマティクスの活用事例	3
2.2.3 コネクティッドカーの発展と展望	3
2.3 コネクティッドカーとデータ	3
2.4 運転歴データを用いるサービス	3
2.4.1 利用ベース保険 (UBI)	3
2.4.2 カーシェアリングサービス	4
2.5 本章のまとめ	4
第3章 基盤技術	5
3.1 デジタル証明書と構成技術	5
3.1.1 デジタル証明書	5
3.1.2 暗号学的ハッシュ関数	5
3.1.3 公開鍵暗号	6
3.1.4 デジタル署名	6
3.2 Verifiable Credentials と Decentralized Identifiers	7
3.2.1 Verifiable Credentials	7
3.2.2 Decentralized Identifiers	8
3.2.3 選択的開示	9
3.2.4 ウォレットアプリケーション	9
3.3 本章のまとめ	10
第4章 本研究における問題定義	11
4.1 既存システムにおけるデータの流れ	11
4.2 既存システムの問題点	11
4.2.1 データのサイロ化	11

4.2.2	データのコントロール権の欠如	12
4.2.3	データの真正性の担保	12
4.2.4	各事業者のポリシーの相違	12
4.3	本章のまとめ	12
第5章	提案手法	13
5.1	提案手法の概要	13
5.2	全体アーキテクチャ	13
5.2.1	自動車アプリケーション	13
5.2.2	モバイルアプリケーション	14
5.2.3	検証者アプリケーション	14
5.3	データ辞書	14
5.3.1	基本設計	14
5.3.2	データセット構造	14
5.3.3	データ辞書の論理構成	15
5.3.4	データ辞書の物理構成	15
5.4	システムの満たすべき要件	15
5.4.1	データのコントロール可能性	15
5.4.2	データの真正性の担保	16
5.5	前提条件	16
5.5.1	自動車は純正であること	16
5.5.2	自動車メーカーは信頼に足ること	16
5.5.3	自動車はコネクティッドカーであること	16
5.6	本章のまとめ	16
第6章	実装	17
6.1	実装の概要	17
6.1.1	機能要件	17
6.1.2	システム構成	17
6.1.3	全体の開発環境	18
6.2	データモデル	18
6.3	自動車アプリ	18
6.4	モバイルアプリ	18
6.5	検証者アプリ	18
6.6	VC生成・署名の方式	18
6.7	本章のまとめ	18
第7章	評価	19
7.1	評価内容	19
7.2	本章のまとめ	19

第 8 章	結論	20
8.1	本研究のまとめ	20
8.2	本研究の課題	20
8.3	本研究の限界	20
謝辞		21

目 次

3.1	VCs における IHV モデルと仕組み	8
3.2	DIDs の例	8
3.3	DIDs のエコシステム	9

表 目 次

第1章 序論

本章では本研究の背景，課題及び手法を提示し，本研究の概要を示す．

1.1 はじめに

インターネット技術の発展に伴い、あらゆるモノがネットワークに接続される Internet of Things の概念が急速に広がっている。自動車もその例外ではなく、車両に通信機能を搭載することで、外部ネットワークと常時接続されたコネクティッドカーへと進化してきた。とりわけ、テレマティクス技術の発展は、自動車の運転や利用状況に関する詳細なデータ収集を可能にしてきた。利用ベース保険やカーシェアリングサービスにおける運転データの活用はその代表であり、車両データに基づく多様な価値提供が進んでいる。しかし一方で、現在普及しているコネクティッドカーを基盤としたサービスは、データが自動車メーカーや特定のサービス事業者のクラウド内に閉じたサイロ構造を形成している。そのため、利用者が自身の運転データを他の事業者へ持ち出したり、サービスを乗り換える際に運転履歴を引き継いだりすることは困難である。また、利用者自身が自らのデータへアクセスできない、あるいは事業者は利用者が提示してきたデータの真正性が検証できないといった課題も存在する。本研究では、このような課題に対し、Decentralized Identifier および Verifiable Credentials を活用した新たな運転歴データの管理・提示モデルを検討する。これにより、利用者自身がデータに対するコントロールを保持しつつ、データの真正性を担保し、複数の事業者間で安全かつ信頼可能な運転歴データの再利用が可能となる仕組みの構築を目的とする。

1.2 本論文の構成

本論文における以降の構成は次の通りである．

2章では、背景を述べる．4章では、本研究における問題の定義と、解決するための要件の整理を行う．5章では、本研究の提案手法を述べる．6章では、5章で述べたシステムの実装について述べる．7章では、4章で求められた課題に対しての評価を行い、考察する．8章では、本研究のまとめと今後の課題についてまとめる．

[1]

第2章 背景

本章では本研究の背景について述べる。

2.1 自動車の情報化

インターネットの発展に伴い、いまやパソコンだけではなく、あらゆるものがインターネットと接続することが当たり前になった。このような技術は“Internet of Things”の略称であるIoTと呼ばれ、社会のデジタル化に欠かせない技術となっている。自動車も例外ではなく、インターネットと自動車を接続することで自動車自体を情報化し、道路交通情報をシステム化することができる。道路交通に関する総合的な情報通信システムは高度道路交通システムと称され、“Intelligent Transport Systems”の略称であるITSと呼ばれる。自動車の情報化は社会全体の利益に繋がり、その必要性は高い。同時に、自動車と情報通信に関連する分野で、情報通信社会を支援する役割も期待されている。

2.2 コネクティッドカーとテレマティクス

本節では、コネクティッドカーとそれを支える技術であるテレマティクスについて概説し、その活用事例及び発展と展望を紹介する。

2.2.1 コネクティッドカーとテレマティクスの概要

コネクティッドカーとは、外部ネットワークと接続している自動車のことである。自動車に通信システムを搭載することで、リアルタイムに外部とデータのやり取りを行うことができ、これをテレマティクスと呼ぶ。なお、テレマティクスはIoTの一種であり、「テレマティクス (telematics)」という語は「テレコミュニケーション (telecommunication)」と「インフォマティクス (informatics)」を組み合わせた造語である。コネクティッドカーは、テレマティクスによって外部ネットワークに接続している自動車そのものである。テレマティクスに対応したコネクティッドカーにはTCU（テレマティクス制御ユニット）と呼ばれる部品が搭載され、TCUは自動車のECU（電子制御ユニット）と接続し、自動車のデータを用いて外部ネットワークとの通信を行う。また、コネクティッドカーでは「Over The Air (OTA)」という技術を用いることで車載ソフトウェアの更新を無線ネットワーク経由で行うことができる。

2.2.2 テレマティクスの活用事例

テレマティクスを用いることで、様々なシステムが実現している。例えば、自動車の事故や事件などの非常事態が発生した際に、警察や救急、メーカーや保険会社などに緊急で通報する緊急通報システムや車両が盗難された時に位置情報を元に追跡できる車両盗難追跡システムなどである。また、テレマティクスを用いるサービスも多く存在し、代表的なものとして利用ベース保険が挙げられる。利用ベース保険の詳細については後述する。

2.2.3 コネクティッドカーの発展と展望

コネクティッドカーは車両の通信機能によりリアルタイムで外部ネットワークとのデータのやり取りを行い、安全性と利便性、そしてシステム・サービス間の連携を大きく向上させてきた。テレマティクスを用いるシステム・サービスの拡大に伴い、自動車が「移動するデジタル端末」として機能しており、今後は自動運転やEV、そしてMaaS（Mobility as a Service）との統合が進み、車両データを基盤とした新たなエコシステムの中心的役割を担うことも期待される。コネクティッドカーはテレマティクスを用いるシステムの発展とともに新車に占める台数が年々増加しており、2030年には新規に出荷される乗用車のうち95%以上を占めると予想されている。

2.3 コネクティッドカーとデータ

2.4 運転歴データを用いるサービス

実際にコネクティッドカーから抽出したデータを利活用するサービスは多く存在するが、本節ではその中でも特に運転歴データを用いるサービスについて紹介する。なお、自動車からデータを抽出する方法としてはOBD-IIコネクタやスマートフォン、EDR（Event Data Recorder。車載ブラックボックスとも呼ばれる）などが存在する。

2.4.1 利用ベース保険（UBI）

利用ベース保険（UBI）はテレマティクス保険とも呼ばれ、自動車から収集した運転データを基に保険料を算出する保険である。従来の自動車保険は大数の法則に基づき、過去の膨大な統計データを元に保険料を算出していたが、利用ベース保険ではより詳細な、運転手ごとにカスタマイズされた保険料を算出することができる。例えば、責任感を持ち、安全な運転志向を持つドライバーは大きな割引を受けることができる一方、危険な運転志向を持つドライバーに対しては保険料を高く設定することができ、これにより保険会社のリスクを低減することができる。なお、保険料の算出方法として主流なものはPAYD（Pay As You Drive）とPHYD（Pay How You Drive）であり、前者は走行距離に連動し、後者は運転の仕方に連動するものである。運転の仕方には、平均速度、加速や減速の度合

い、運転する場所、運転する時間などが含まれる。利用ベース保険は特に北米市場で高い需要があり、2030 年までには世界市場で 11.34%の年平均成長率で拡大すると予測されている。

2.4.2 カーシェアリングサービス

カーシェアリングサービスは、登録された自動車を会員が共同で使用するサービスである。登録される自動車の所有者が個人であるか法人であるかや、登録される自動車の種類によって異なる様々なサービスが存在する。組織的なカーシェアリングサービス自体は 1980 年代後半にヨーロッパで始まり、日本では 2002 年に初の民間会社が発足したように決して新しいものではないが、近年のシェアリングエコノミー及びコネクティッドカーの普及により事業者数・利用者数ともに急激に規模を拡大しているサービスでもある。現在のカーシェアリングサービスでは、利用者が利用開始時に自身のスマートフォン内のモバイルアプリケーションを用いて自動車を解錠したり、利用者の運転歴データを事業者が収集したりすることが一般的である。例えば、パーク 24 グループが運営するカーシェアリングサービスであるタイムズカーにおいては、急加速・急減速などをリアルタイムで観測し、これらのデータを元に安全な運転を判定したうえで利用者にポイントを付与している。無事故走行距離とポイントに応じて利用者は 4 段階に分かれたステージに振り分けられ、ステージに応じて割引などの恩恵を受けられる。

2.5 本章のまとめ

第3章 基盤技術

本章では、提案するシステムで用いる基盤技術について紹介する。

3.1 デジタル証明書と構成技術

本節では、本研究におけるデジタル証明書の定義と、その構成技術について解説する。

3.1.1 デジタル証明書

通常、デジタル証明書は公開鍵と公開鍵の所有者を紐づけ、公開鍵の真正性を示す証明書を指すことが一般的だが、本研究では、ある主体に対する証明書発行者の主張を表現したデジタルデータと定義する。これらの主張には身分証明に関する個人情報から資格情報、ひいては大学の成績など多様な情報が含むことができ、デジタル証明書はこれらの情報を電子的に表現した上で第三者に対する提示・検証を可能とするための手段である。一般的に、デジタル証明書は以下のような要素を持つ。

- 発行者情報：デジタル証明書の発行者を識別するための情報
- 証明書の主体：証明書の主張の対象となる主体を識別するための情報
- 主張内容：発行者が証明書の主体について主張するなんらかの情報
- 有効期限：証明書の有効期限に関する情報
- 改ざんされていないことの証明：証明書が改ざんされていないことを示すための情報

これらの要素はデジタル証明書のデータモデルに従い表現され、様々な標準化団体が多様なデータモデルを提案している。その一例である、W3C による Verifiable Credentials Data Model については後述する。また、デジタル証明書はシリアライズされてデジタルデータに変換されるが、代表的なシリアライズ形式としては JSON, CBOR などがある。

3.1.2 暗号学的ハッシュ関数

ハッシュ関数とは、任意の長さのデータから要約された値（ハッシュ値）を得る関数であり、特に暗号や情報セキュリティの用途に適した性質を持つものを暗号学的ハッシュ関

数と呼ぶ。同じ入力値からは常に同じハッシュ値を得られ、またハッシュ値から入力値を計算することは困難であるという性質がある。後述する公開鍵暗号やデジタル署名でも用いられている技術であり、以下の特性を持つ。

- 原像計算困難性：ハッシュ値から元の入力値を計算することが困難である
- 弱衝突耐性：ある入力値とハッシュ値のペアがあったとき、同じハッシュ値を持つ異なる入力値を計算することが困難である
- 強衝突耐性：同じハッシュ値を持つ 2 つの異なる入力値のペアを計算することが困難である

なお代表的な暗号学的ハッシュ関数としては、SHA-256 などが挙げられる。

3.1.3 公開鍵暗号

公開鍵暗号は、暗号化と復号で異なる 2 つの鍵を使用する暗号方式である。2 つの鍵はそれぞれ秘密鍵と公開鍵と呼ばれ、秘密鍵はその所有者によって秘密を保って管理される鍵であり、秘密鍵と対になる公開鍵は広く公開され、他人が利用可能な鍵である。公開鍵暗号は広く用いられており、例えばインターネット上の通信を保護するためのプロトコルである SSL/TLS で利用されている。公開鍵暗号の代表的なアルゴリズムとしては、RSA(Rivest-Shamir-Adleman)、DSA(Digital Signature Algorithm)、ECDSA(Elliptic Curve Digital Signature Algorithm) などが挙げられる。

3.1.4 デジタル署名

デジタル署名は、あるデジタルデータが特定の主体により作成されたこと、かつ作成されたのちに改ざんされていないことを検証可能にするための技術である。デジタル署名は、以下のプロセスで作成・検証される。

- 作成プロセス
 1. ハッシュ値の計算：署名者は、署名したいデータからハッシュ値を計算する
 2. 秘密鍵による署名：計算されたハッシュ値に対して、署名者の秘密鍵を使用して署名を生成する。この生成された値がデジタル署名となる
- 検証プロセス
 1. 公開鍵の入手：まず、検証者は署名者の公開鍵を入手する。通常、公開鍵は、公開鍵と公開鍵の所有者を紐づける証明書で配布されている
 2. ハッシュ値の再計算：受け取ったデータをハッシュ関数に通し、ハッシュ値を再計算する
 3. 署名の検証：署名者の公開鍵を用いて複合したハッシュ値と再計算したハッシュ値を比較し、同じであれば検証が成功したと言える

3.2 Verifiable Credentials と Decentralized Identifiers

本節では、デジタル証明書の一形態である Verifiable Credentials と、それを支える識別子である Decentralized Identifiers について解説した後、デジタル証明書の文脈で重要な機能である選択的開示と、アプリケーションとして欠かせないウォレットアプリケーションについても解説する。

3.2.1 Verifiable Credentials

前節で解説したデジタル証明書の一つの形態として、Verifiable Credentials がある。Verifiable Credentials は W3C が標準化を進めており、一般的に Verifiable Credentials といえば W3C による “W3C VC” を指す。Verifiable Credentials はデジタル証明書そのものであり、Verifiable Credentials のためのデータモデルとして Verifiable Credentials Data Model が存在する。広義の Verifiable Credentials として、ISO/IEC 18013-5 で定義された mdoc/mDL や、IETF が標準化を進める SD-JWT VC などにも存在するが本稿では詳しくは触れない。なお、Verifiable Credentials は “VCs”、Verifiable Credentials Data Model は “VCDM” と呼ばれることが一般的なため、本稿でもこれ以降この呼称を用いる。

VCs とは、検証可能な証明書のことであり、暗号学的な手法で改ざん検知、および正当に発行されたものであるかの検証を可能にしたクレデンシャルのことである。クレデンシャルとは、発行者によって発行された、対象となる主体に対する何らかの主張（クレームと呼ばれる）の組と定義される。例えば、髪が黒く、眼鏡をかけた男性がいた場合、クレームは「髪が黒い」「眼鏡をかけている」「男性である」の 3 つとなり、これをまとめたものがクレデンシャルとなる。さらにこのクレデンシャルを暗号学的に改ざん検知、正当に発行されたものであるか検証できるようにしたものが VCs、といったイメージである。

VCs の基本的な構造は、発行者 (Issuer)、保持者 (Holder)、検証者 (Verifier) という三者の役割分担を前提としている。なお、この三者が登場するモデルは IHV モデルと呼ばれる。VCs の発行から検証までの一連の流れは下記の通りである。

1. 発行：発行者が特定の主体 (Subject と呼ばれる) に関するクレデンシャルを用意し、暗号学的な署名を施す。完成したら、Holder に送信する。多くの場合 Subject と Holder は一致するが、異なっても構わない
2. 保持・提示：Issuer から送信された VCs を受け取り、後述するウォレットアプリケーションなどに保持する。任意のタイミングで Verifier に VCs を提示する
3. 検証：Verifier は Holder から送信された VCs から検証に必要な公開鍵情報を取り出し、公開鍵を用意した上で VCs を検証する

また、各主体はデータを Verifiable Data Registry と呼ばれるデータ保管場所とやり取りする。一連の役割分担を示したのが下図である。

また、Holder が複数の VCs を保持し、場合によってはまとめて Verifier に提示するユースケースがあることは容易に考えられる。そのため、VCs には複数の VCs を合わせて提

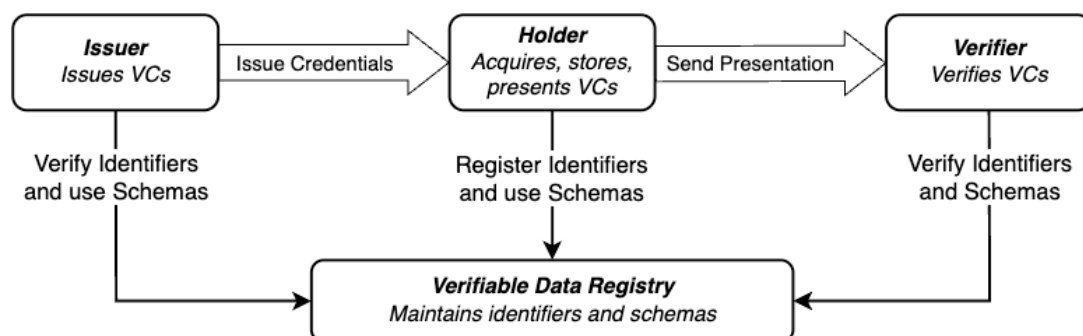


図 3.1: VCs における IHV モデルと仕組み

示する Verifiable Presentations という形式も存在する。Verifiable Presentations には、その Verifiable Presentations が正しく構成されていることを示す証明と、提示者が Holder であることを示す証明が含まれる。なお、Verifiable Presentations も “VP” と一般的に呼ばれるため、本稿でもこれ以降この呼称を用いる。

3.2.2 Decentralized Identifiers

Decentralized Identifiers は識別子の一種であり、ブロックチェーンなどの分散型台帳技術と紐づけられる。従来のアイデンティティ管理システムで用いられるような ID とは異なり、中央集権的な構造を持たないため異なるシステム間で相互運用性を持たせられたり、ID を自己管理できたりするというメリットがある。先述した VCs でも各主体の識別子としては Decentralized Identifiers が用いられることがほとんどである。なお、Decentralized Identifiers は一般的には “DIDs” と呼ばれるため、本稿でもこれ以降この呼称を用いる。

DIDs 自体は下図のような構造を持つ。“Scheme” はこの識別子が DIDs であることを示す。“DID Method” はこの DIDs がどのタイプの DIDs であることを示すもので、主に DID document（後述）の置き場所により多くの種類が存在し、代表的なものでは did:web, did:key, did:ion などが挙げられる。“DID Method-Specific Identifier” は DID メソッドの名前空間内での一意な識別子である。



図 3.2: DIDs の例

また、DIDs は下図のようなエコシステムを持つ。DIDs は単体では識別子に過ぎない

ため、DIDs に関するより詳細な情報を記載したデータとして “DID document” が存在し、さらに DID document を補助する役割を果たす “DID controller” と “DID URL” が存在する。“Verifiable Data Registry” は DIDs, DID document の置き場所として利用され、ブロックチェーンなどの分散型台帳技術が用いられることが多い。なお、DIDs から DID document を引くことを “resolve” といい、本稿ではこれ以降「解決する」と呼称する。

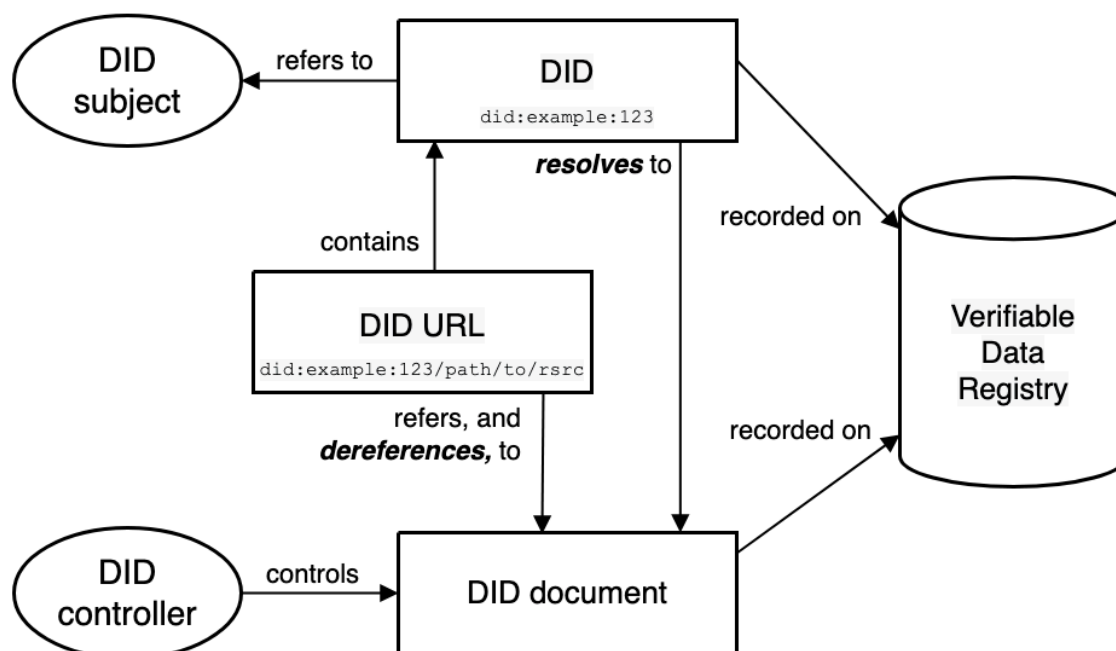


図 3.3: DIDs のエコシステム

3.2.3 選択的開示

VCs や DIDs の文脈で重要な機能の一つが、選択的開示である。選択的開示とは、Holder が Verifier に証明書を提示する際、開示する内容をコントロールできる機能である。例えば、20 歳以上であることを示しアルコール飲料を購入するユースケースでは、従来ならば運転免許証などを全て開示していたが、選択的開示を用いることで顔写真と年齢の欄のみを開示すればよくなる。選択的開示を用いることで、Holder は Verifier に対して必要以上の情報を開示することがなくなり、Holder のプライバシーを保護することにつながる。選択的開示の具体的なアルゴリズムとしては、Selective Disclosure for JWTs(SD-JWT) や、ゼロ知識証明を用いたものなどが提案されている。

3.2.4 ウォレットアプリケーション

IHV モデルにおいて、Holder が VCs などのデジタル証明書を保持するには、何らかの器が必要である。そこで登場するのがウォレットアプリケーションであり、Holder が複数

の Issuer から発行された多様なデジタル証明書を格納し、自在に組み合わせて Verifier に提示するのに用いられる。

3.3 本章のまとめ

本章では、基盤技術としてデジタル証明書とその構成技術について紹介した上で、デジタル証明書の一形態である VCs とそれに関連した一連の技術についても紹介した。次章では、既存システムにおける問題点について議論する。

第4章 本研究における問題定義

本章では、既存システムにおいて本研究が着目する問題について述べる。

4.1 既存システムにおけるデータの流れ

2.2 節及び 2.3 節で紹介した既存サービスにおいて、基本的にコネクティッドカーから収集されたデータは自動車からサービスの事業者が接続しているクラウドへと流れ、クラウドで処理をされた後に事業者へと提供される。トヨタの提供する T-Connect のように、モバイルアプリケーションへの配信などを通じて利用者にデータを提供するサービスも一部存在するが、基本的にデータは自動車とサービス事業者間を繋ぐネットワーク内にのみ存在していると言える。

4.2 既存システムの問題点

前節で述べたデータの流れは、既存サービスのような利用者と事業者の間のみで完結するユースケースにおいては十分である。しかし、特定の事業者とのみデータを共有する既存サービスは、ベンダーロックインを招きやすく、利用者にサービスの乗り換えという選択肢を与えない。例えば、利用者が保険会社を乗り換えても利用ベース保険の実績を引き継ぐことができるかや、カーシェアリングサービスをまたいでも安全運転の履歴により割引を受けられるかはひとえに保険会社やカーシェアリングサービスの判断に委ねられている。言い換えるならば、複数の事業者にまたがってデータを共有する際、既存サービスでは事業者やメーカー間の連携が不可欠であるという問題点が存在する。また、このようなシステムでは、複数の事業者が結託して利用者に断りなくデータを共有する事態が発生する可能性も否定できない。

次項からは、この問題を構成している要因についてそれぞれ述べる。

4.2.1 データのサイロ化

前述したように、既存サービスにおいてはコネクティッドカーから収集されたデータは自動車と事業者が接続しているクラウドへと流れ、クラウドで処理をされた後に事業者へと提供される。このようなシステムにおいては、利用者と事業者の間にデータが閉じ、サイロ化とでも言うべき状態が生まれる。利用者が複数事業者を利用する場合、互いに独

立したサイロが事業者の数だけ複数存在していることになり、これが複数の事業者間の連携を難しくしている要因の一つである。

4.2.2 データのコントロール権の欠如

また、サイロが構成されていると言っても、データはコネクティッドカーから抽出された後に事業者と接続したクラウドにて処理・蓄積されるため、利用者がデータにアクセスしたり、データをコントロールしたりすることは不可能に近い。仮に利用者が自分の自動車から抽出したデータにアクセスし、それをコントロールすることが可能であれば、そのデータを事業者をまたいで提示する可能性が出てくるが、そのようなシステムは現在存在しない。

4.2.3 データの真正性の担保

仮に利用者がデータを提示してきたとしても、それを事業者が信頼できるとは限らない。例えば、利用者がデータを偽造・改ざんしたり、他人の自動車から抽出したデータを提示してきたりする可能性を否定できないからである。そのため、既存サービスではデータの真正性を担保するために信頼できる自動車メーカーが製造したコネクティッドカーから信頼できる通信経路を経由してクラウドにデータを送信している。

4.2.4 各事業者のポリシーの相違

さらに、これまでに述べた要因が取り除かれたとしても、各事業者のポリシーの相違によってデータを共有することができない場合がある。各事業者はそれぞれ異なるポリシーを持っており、判断に用いられるデータは同じでも、例えば保険会社では総合した安全運転の実績を重視する一方、カーシェアリングサービスでは急な加減速の有無を重視するなど、ポリシーによってデータの評価基準が異なる。そのため、ポリシーによって処理される前の状態のデータを共有する必要がある可能性がある。

4.3 本章のまとめ

第5章 提案手法

本章では、第3章で提示した問題を解決するために、4.5節で提示する前提条件のもとで利用者のデータへのコントロール可能性とデータの真正性の担保を両立するシステムを提案する。

5.1 提案手法の概要

/* (図を載せます) */

本節では、提案するシステムの概要を述べる。システムのアーキテクチャは自動車側、モバイル側、検証者側の3つのコンポーネントから構成され、またシステムの共通言語としてのデータモデルである「データ辞書」も定義する。

5.2 全体アーキテクチャ

/* (図を載せます) */

本システムは示すように、自動車側、モバイル側、検証者側の3つのコンポーネントから構成される。

まず、自動車とモバイルアプリケーションを接続し、信頼できる通信路を確立する。自動車では、各センサから取得された情報をデータ辞書に格納し、VCに加工した上でモバイルアプリケーションへ送信する。モバイルでは取得したVCをウォレットアプリケーションに蓄積し、適宜検証者に提示する。以上が、システムの一連の流れである。

5.2.1 自動車アプリケーション

自動車アプリケーションは、モバイルアプリケーションとの間の信頼できる通信経路の確立と自動車内の各センサから取得した情報をVCに加工し送信するという2つの機能を持つ。通信経路の確立は、公開鍵基盤に基づいて行われ、自動車とモバイルアプリケーションそれぞれが持つ鍵ペアを用いて行われる。また、自動車はメーカーから割り振られた一意の自動車DIDと、VCに添付するための複数のデータDIDを持つ。自動車が発行するVCに、自動車DIDとデータDIDが紐づくことを示すVCを添付することにより、データDIDの出所を担保する。なお、データをVCに加工するときに用いる鍵ペアは、モバイルアプリケーションとの間の信頼できる通信経路を確立するときに用いたものと同じものを用いることを想定している。

5.2.2 モバイルアプリケーション

モバイルアプリケーションは、自動車との間の信頼できる通信経路の確立と自動車から送信された VC をウォレットアプリケーションに蓄積し、検証者に提示するという 2 つの機能を持つ。なお、通信経路の確立については、前項で述べたとおりである。また、受け取った VC をウォレットアプリケーションに送信する役割を持ち、ウォレットアプリケーションはそれを VP に加工し、必要なときに検証者に提示する役割を持つ。

5.2.3 検証者アプリケーション

検証者アプリケーションは、実際の事業者により多様に異なる形をとると想定されるが、基本的な役割としては、送信された VP を確認してその有効性及び真正性を検証することである。すなわち、必要な機能としては受け取った VP をパースし、記載される DID を解決した上で、含まれるデータを取り出すことである。

5.3 データ辞書

データ辞書は、システムの共通言語としてのデータモデルであり、自動車側、モバイル側、検証者側の 3 つのコンポーネントが共通のデータモデルを用いて通信を行うことを目的としている。

5.3.1 基本設計

基本設計として、データ辞書は抽象された自動車情報を JSON 形式で含み、一定時間の間の状態を記述する。自動車から取得される情報は、車両やセンサごとに種類や精度にばらつきがあり、それら全てを網羅したデータ構成を用意することは非常に難しい。また、車両の性質による特殊な情報や事業者のポリシーに依存した情報もあり、これらも全て含むことは非常に困難であるばかりかデータ量を増大させシステムの肥大化をも招く。そのため、検証に必要であると想定できるデータセットを定義することで事業者ごとのポリシーの差を吸収し、システムの基盤として利用していく必要がある。なお、データは正規化されていることを想定している。例えば、センサのパルス数ではなく速度として算出する、電圧ではなく on/off の状態として算出するなどである。

5.3.2 データセット構造

データセットとして、以下がデータ辞書に含まれる。各データは全て自動車の状態である。

- 速度

- 加速度
- 角速度
- 回転数
- 位置情報
- ライト状態
- ブレーキ状態
- 車両イベント
- スロットル開度
- ステアリング角度

5.3.3 データ辞書の論理構成

/* (図を載せます) */

データ辞書の論理構成は以下である。データの収集、加工、提供、検証を考慮したアーキテクチャを検討し、この一連の処理の構成をモデル化した。

5.3.4 データ辞書の物理構成

/* (図を載せます) */

データ辞書の物理構成は以下である。

5.4 システムの満たすべき要件

システムは満たすべき要件として以下が挙げられる。

5.4.1 データのコントロール可能性

利用者が自身の自動車から抽出したデータにアクセスし、コントロールできることである。ここでのコントロールとは、データがどこに所在してどのような内容が含まれるか利用者が把握しており、自由に任意の事業者に提示することができることであり、利用者が自由にデータを改変したり移転したりすることができることではない。

5.4.2 データの真正性の担保

データを検証した者は誰でも、そのデータが偽造・改ざんされていないことを確認できることである。具体的には、事業者が利用者から提示された VP を検証したとき、記載された DID を解決することで含まれるデータが当該自動車から取得されたものであり、利用者によって偽造されたり改ざんされたりしていないことを検証できることを指す。

5.5 前提条件

本提案手法は以下の条件を前提としている。

5.5.1 自動車は純正であること

自動車はメーカーが製造したままの状態であり、改造などを施されていない状態（純正）であることを想定している。例えば、自動車愛好家の間で行われるようなカスタム・チューニングを施された自動車などであれば、この条件を満たさない。センサーなどが改変されることは利用者がデータを改ざんしたことと同義であり、要件を満たせなくなるため、このような自動車は本提案手法の対象外とした。

5.5.2 自動車メーカーは信頼に足ること

自動車メーカーが自動車の製造時に不正な行為を行わないことを想定している。例えば、自動車メーカーがセンサーを改造し実速度よりも表示速度を大幅に下げている場合、この条件を満たさない。事業者が自動車から抽出したデータを信頼しているのは自動車メーカーを信頼しているためであることは前述のとおりであるが、自動車メーカー自体が不正な行為を行うとその信頼が損なわれるため、この条件を満たさない。

5.5.3 自動車はコネクティッドカーであること

本提案手法が対象とするのはコネクティッドカーである。ECU や TCU を持たない自動車はそもそもモバイルアプリケーションとの間に通信経路を確立したり、データを抽出したりすることができないため、そのような自動車は本提案手法の対象外とした。

5.6 本章のまとめ

第6章 実装

本章では、第4章で提案したシステムの実装について述べる。

6.1 実装の概要

前章で提案した手法を実装し、実際に動作するシステムを構築する。実装するのは自動車アプリケーション、モバイルアプリケーション、検証者アプリケーションの3つであるが、自動車アプリケーションに関しては実際の自動車で動作するアプリケーションを開発することは労力が大きいため、Raspberry Pi を用いたエミュレータを実装した。

6.1.1 機能要件

それぞれのアプリケーションの機能要件については、以下とする。

1. 自動車アプリケーション
 - ・ 基盤内の鍵ペアを用い、モバイルアプリケーションとの間の信頼できる通信経路の確立
 - ・ 自動車内の各センサから取得した情報をデータ辞書に基づいて VC に加工し、モバイルアプリケーションへ送信
2. モバイルアプリケーション
 - ・ 自動車との間の信頼できる通信経路の確立
 - ・ 自動車から送信された VC をウォレットアプリケーションに蓄積し、VP に加工
 - ・ VP を検証者に提示
3. 検証者アプリケーション
 - ・ 受信した VP を確認してその有効性及び真正性を検証し、データを取り出す

6.1.2 システム構成

/* (図を載せます) */
全体のシステム構成は以下である。

6.1.3 全体の開発環境

実装にあたり、開発環境は以下を用いた。

6.2 データモデル

データモデルは第 4 章で述べたとおり、JSON 形式で表現されたデータ辞書を用いる。

6.3 自動車アプリ

実装にあたり、自動車アプリケーションは Raspberry Pi を用いたエミュレータとして実装した。

6.4 モバイルアプリ

実装にあたり、モバイルアプリケーションは Flutter を用いて実装した。

6.5 検証者アプリ

実装にあたり、検証者アプリケーションは Typescript を用いて実装した。

6.6 VC 生成・署名の方式

/* (図を載せます) */

6.7 本章のまとめ

第7章 評価

本章では，提案システムの評価について述べる．

7.1 評価内容

（評価としては、以下を想定しています）

- 要件を満たしていること：第4章で述べた要件を満たしていること。
- システムの動作確認：サンプルデータを基にVCを発行し、モバイルに送信できること。モバイル内でウォレットアプリに送信できること。ウォレットではVPを構成し、提示できること。
- 脅威分析：DFD、STRIDEを用いる。

7.2 本章のまとめ

第8章 結論

本章では，本研究のまとめと今後の課題を示す．

8.1 本研究のまとめ

まとめます。

8.2 本研究の課題

8.3 本研究の限界

データ辞書の限界・事業者のポリシーに全て対応することはできないことを書きます。

謝辞

がああ

参考文献

- [1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. <http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20original.pdf>, 2008.