異なるサービス提供者間における トラストモデルとその実装に関する研究

平野 流[1] 廣井 慧[1] 米澤 拓郎[1] 河口 信夫[1,2]

概要：超スマート社会の実現例として，事業者間連携プラットフォームがあげられる．事業者間連携プラットフォームでは，事業者間での情報交換を可能にすることで多様で柔軟性のあるサービスの実現が期待される．しかし，一般的に事業者間にはトラスト (信頼関係) が存在し，トラストに基づいた情報交換が促される必要がある．本稿では，事業者間におけるトラストモデルを考案し，同時にトラストモデルを事業者間連携プラットフォームに導入する方法を提案する．具体的には，事業者の認証情報による情報交換をするためのトラストフレームワークというトラストモデルの枠組みとビット列を用いた認証方法を提案する．また，トラストモデルを導入した事業者間連携プラットフォームの処理性能を，実社会において想定されるシナリオにおける処理性能と比較し有用性を評価する．結果として，想定したシナリオにおける処理性能の約 2.5 倍の処理性能を得ることができた．

A Study of Trust Model between Different Service Providers and Its Implementation

RUI HIRANO[1] KEI HIROI[1] TAKURO YONEZAWA[1] NOBUO KAWAGUCHI[1,2]

1. はじめに

2016 年の科学技術基本計画 [1] で超スマート社会が提唱された．超スマート社会では，「必要なもの・サービスを，必要な人，必要な時に，必要なだけ提供し，社会の様々なニーズにきめ細やかに対応できる社会」を目指している．産学官や関係府省による連携のもと，サービスや事業の「システム化」，システムの高度化，複数のシステム間の連携により，多様なサービスプラットフォームを構築する取り組みが 2020 年に向けて計画されている．

超スマート社会を実現する一つの例として，事業者間連携プラットフォームがあげられる．事業者間連携プラットフォームでは複数の事業者間での情報交換を可能とすることで，多様で柔軟性のあるサービスを実現できる．

具体的な例として，図 1 のようなタクシーやバス，鉄道などの移動サービスプロバイダとユーザプロバイダ，目的地までのルートを探索するルーティングプロバイダが連携し，時間，場所にかかわらず最適な移動方法をユーザに提供するサービスが考えられる．さらに，ポイント事業者や広告事業者などの連携サービスプロバイダが連携に加わることで，ポイントによる支払いや還元，広告費用による割引などのサービスも考えられる．このように，事業者間連携プラットフォームでは様々な事業者が連携し合うことで，今までにない複雑で柔軟なサービスが実現できる．

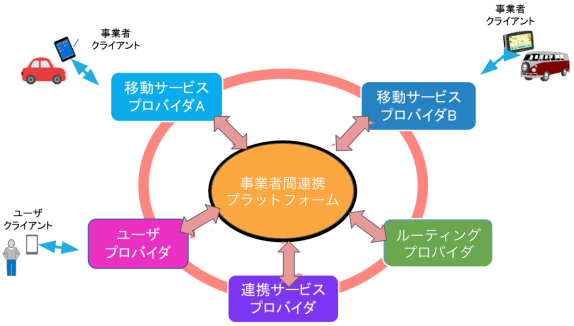

図 1 事業者間連携例

事業者間連携プラットフォームは，複数の事業者による

[1] 名古屋大学大学院工学研究科 Graduate School of Engineering, Nagoya University
[2] 名古屋大学未来社会創造機構 Institutes of Innovation for Future Society, Nagoya University

情報交換を目的としているが，一般的に事業者間にはトラスト (信頼関係) が存在しており，信頼していない事業者には情報を与えたくないというニーズがある．しかしながら，現状の事業者間連携プラットフォームでは送られた情報が全ての事業者に送られてしまい，事業者間の信頼関係に基づいた情報の制御がほとんどされていない．

本論文では事業者間のトラストを構成する要素を考察し，事業者間の信頼に基づいて事業者間連携プラットフォームにおける情報交換を行うためのトラストモデルを提案する．このトラストモデルでは事業者がトラストを委譲し，事業者の認証情報に基づいて情報交換を行う．

さらに，実際の事業者間連携プラットフォームにトラストモデルを導入し，処理性能や実世界での実用性を評価する．結果として，想定の 2.5 倍の処理性能を得られ，実世界で十分運用可能であることがわかった．

本論文の構成は次のようになっている．まず，第 2 章で事業者間連携プラットフォームにおけるトラストが必要になる理由，課題，研究目的を示す．次に，第 3 章でトラストの概念，トラストモデル，アクセス制御方式に関する既存研究について述べる．さらに，第 4 章で事業者間連携におけるトラストモデルの考案とその認証手法について論じる．そして，第 5 章でトラストモデルを導入した事業者間連携プラットフォームの処理性能実験とその評価をし，第 6 章でまとめとする．

2. ビッグデータ流通とトラスト

2.1 事業者間連携プラットフォームの必要性

近年，IoT 機器の普及により様々なデータが大量に飛び交っている．ビッグデータが流通され，活用されることによって新しい価値の提供ができるようになる一方，ビッグデータの流通量は以前では想像できないほど多くなっており，大量で多様なデータをリアルタイムで処理する必要性がある．そのため，事業者間で大量のデータをリアルタイムで共有したり交換することができる事業者間連携プラットフォームは，ビッグデータ流通に適しているといえる．

また現在，名古屋大学河口研究室では「Synergic Mobility」というプロジェクト [2] が進行している (図 2)．このプロジェクトでは自動運転車が普及した社会を想定し，車両に搭載されたセンサを用いて実世界データを収集すると同時に，人の移動や配送，移動販売，インフラ点検など，あらゆる事業者が連携できるプラットフォームの創出を目指している．河口研究室では「Synergic Exchange」[3] という事業者間連携プラットフォームを開発しており，実用化を進めている．

このように，超スマート社会の実現には事業者間連携プラットフォームが重要になっている．事業者間連携プラットフォームを活用することで，様々な事業者が多様な情報の交換を素早く行うことができ，社会の様々なニーズに柔軟に対応するサービスの提供が可能となる．

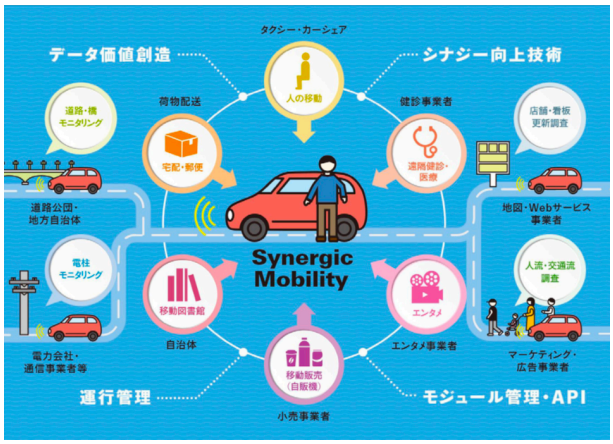

図 2 Synergic Mobility の概念図

2.2 課題

事業者間連携プラットフォームでは事業者間連携が円滑に行われるための課題がいくつかある．まず，信頼に関する課題があげられる．事業者が安心して連携を取れるには，信頼のできる事業者にのみ情報を与えればよい．しかし，事業者間連携には多くの事業者がオープンに参加できることが重要であり，信頼できない事業者が存在する可能性がある．そのため，事業者ごとに信頼できる相手を求める必要があるが，大規模な数の事業者が連携することを考えると一つ一つ確認していくのは多くのコストがかかり適切ではない．

次に，実装に関する課題があげられる．事業者間連携にはリアルタイムで大規模なメッセージが送受信されるため，高速な処理が求められる．また，事業者が増えた場合に容易にプラットフォームに参加できるような拡張性が必要となる．その他にも，システムトラブルがあった時の回復方法や複数の連携プラットフォーム間での連携といった課題があげられる．

2.3 目的

本論文の目的は大きく 2 つある．1 つ目は，事業者間連携プラットフォームにおける事業者間の信頼関係を構成する要素について考え，その要素に基づいたトラストモデルを考案することである．2 つ目に，事業者間連携プラットフォームへの導入をふまえ，事業者が増えた際にも柔軟に対応できるような拡張性をもち，信頼に基づく情報交換を高速かつ自動的に行える方法を提案することである．

3. 関連研究

3.1 信頼に関する既存研究

まず，「信頼」という概念に関する既存研究を述べる．千葉らの研究 [4] では，信頼のメカニズムは信頼する当事者

と信頼される対象と両者を含む社会の状況という 3 つの要素で成り立つという．端的にいうと，信頼するという行為を「他者の行為に本質的に不確実性がある状況で，相手が望ましい行動をするであろうと予期して，危険を伴う行為 (コミットメント) を行うこと」と表現している．

Audun らの研究 [5] では，「信頼している人の信頼している人は信頼できる」というような評判による人と人との信頼性の連鎖を代数的に表現している．評判による信頼性は人を介するほど薄まっていくこと，複数の人から信頼を得ているほど信頼性が高まることなどに着目している．

本研究における事業者間の信頼関係にも行為の不確実性や第三者による評判が要素になると考える．

3.2 トラストモデルに関する既存研究

森らの研究 [6] では，ソーシャルネットワーク上におけるトラストモデルを，二者間の間接的なつながりを評価するエッジクラスタリング係数という指標を用いて表現している．相手との信頼を密にするには，自分との間に信頼関係にある第三者を通して，相手との間になるべく多くの間接的な信頼関係を手に入れることが重要だと述べている．

第三者との信頼関係によって相手との信頼関係を測るという点で，ある程度の不確実性が伴う．信頼できる者との繋がりの数を要素として第三者からの評価を表しているが，事業者間における信頼の要素としてはまだ不十分である．しかし，事業者間の繋がりを提携しているグループとして表すのであれば，提携グループは当事者間の信頼関係となるので要素としては有用であると考える．

3.3 Access Control List に関する既存研究

Accecc Control List(以下，ACL) とは，コンピュータ上のリソースに誰のどの操作を許可するかをリストにしたものである．ACL を用いることでコンピュータ上のアクセス制御を実現できる．ACL はリソースに対して，表 1 のようにアクセスに関するオプションが与えられる [7]．Poslad らの研究 [8] によると，一般的に Foundation for Intelligent Physical Agents(以下，FIPA) と呼ばれる団体が策定するソフトウェアエージェントシステムの仕様について，認証による信頼性の確立とセキュリティの安全性を検証した．

事業者における認証による信頼性の確立は，事業者の属性を認証情報の 1 つとすることで表すことができる．そのため，ACL や FIPA のような認証情報によるアクセス制御は，事業者間連携の仕組みに適しているといえる．

3.4 センサ情報共有プラットフォーム

本研究が対象としている事業者間連携プラットフォームに関する関連研究として，スマートシティを実現するためのミドルウェア [9][10][11]，テストベット上のアプリケーション開発のためのツール群 [12][13] などが挙げられる．

表 1 ACL のオプション

設定	説明
Open	誰でも
Authenticated	許可された者のみ
WhiteList	ホワイトリストとして認証された者のみ
Roster	所有者のグループに加入している者のみ
Presence	所有者から購読した者のみ

これらのシステムには異なるユーザが連携するために，センサ情報を共有する機能は有しているが，そのアクセスモデルは既存の方式の踏襲にとどまっており，本研究が対象としているトラストに関する考慮はなされていない．また，オープンデータを公開しつつ，その公開者間でオープンなネットワークを構築する目的で CKAN[13] が構築されている．CKAN にはユーザロールに従ってデータのアクセス権限を制御可能であるが，本研究が対象している動的な情報には対応しておらず，またその指定可能な範囲も限定的である．本研究では Synergic Mobility プロジェクトに代表されるような，センサ情報だけでなくそのセンサ情報をもとにサービスの交換を行うことができ，需給交換ネットワークの実現に寄与することを目的としている．従って，その参加ユーザの多様性とそれに付随して懸念されるプライバシやセキュリティの問題を同時に解決するトラストフレームワークの構築が必要となる．

4. トラストモデルの提案

まず最初に，本研究におけるトラストを構成する要素を定義し，その詳細について述べる．次に，それらの要素を考慮し，事業者間のトラストを表す認証情報について述べる．さらに，トラストモデルの中核であるトラストフレームワークについて述べ，ステークホルダーとその役割について説明する．最後に，事業者間連携プラットフォームに導入する際の認証方法について述べる．

4.1 トラストを構成する要素

本研究では，「事業者間のトラストを構成する要素は，第三者による口コミや認証機関による認証情報と，事業者間での直接的なインタラクションによって構成される」と定義する．まず，第三者による認証を具体的に言えば，「一部上場企業であれば信用できる」「大企業であれば信用できる」などその事業者の属性で社会的信用の大きさを表したものである．事業者の属性は，ほとんど変化性に乏しく静的な情報だと言える．次に直接的なインタラクションの例として，連携した際のレスポンスの速さや契約内容の遵守性，情報保守性などがあげられる．直接的なインタラクションは，短期間で変化する可能性があるため動的な情報だと言える．

このような第三者による評価と二者間でのインタラクションによる信頼性は契約の前後で変化すると考えられ

表 2　認証情報

	種類	主な説明
静的な情報	属性	企業規模，時価総額，事業種，経営状況
	提携	提携しているグループに関する情報
動的な情報	行動	取引，安全性，情報保守性，金銭的行為

る．一般的に，契約の前では直接的なインタラクションはほとんど発生しえないので，第三者の認証や口コミによる信頼性が要素となる．そして，契約後には契約相手との直接的なインタラクションも要素として加わる．事業者間での直接的なインタラクションにより，信頼関係の大きさは絶えず変化していくことが予想される．

4.2　認証情報

事業者はトラストフレームワークと契約し連携プラットフォームに加わることで，監査機関から認証情報が発行される．認証情報は表 2 のように静的な情報と動的な情報に大別できる．

静的な情報には，主に事業者の属性と提携しているグループの情報が記される．事業者の属性は，企業規模，時価総額，事業種，経営状況などがあげられる．企業規模は，大企業や中小企業，上場企業，株式会社，合同会社などのことである．これらの属性は一種の信頼性を表しており，各事業者が信用できる企業を決める重要な要素となる．連携グループの情報は，複数の事業者間の提携しているグループのことを表す．例えば，図 3 の交通 IC カード相互利用の連携があげられる．この図は交通 IC カードの相互利用の連携グループを表しており，交通 IC カードのみ，電子マネーのみ，両方可など様々な条件でそれぞれ提携されていることがわかる．連携グループの情報を認証情報に加えることで，このような複雑な連携にも容易に対応可能となる．

次に，動的な情報には事業者の行為による変化性の高い情報が記される．例えば，取引回数や取引頻度などの取引に関する行為，システムのセキュリティが万全かなどのシステム安全性，情報を漏洩せず保護できているかといった情報保守性，支払い延滞や支払い能力の有無などの金銭的行為などがあげられる．

4.3　トラストフレームワーク

トラストモデルの概要を図 4 に示す．このトラストモデルには，トラストフレームワークと監査機関，ポリシー作成機関，そして事業者が存在し，各事業者はトラストフレームワークにトラストを委譲する．そして，各事業者の認証情報に基づいて情報交換の制御を行う．

まず，ポリシー作成機関は事業者間連携プラットフォームに参加する全ての事業者が遵守すべきポリシーを作成する．ポリシーには，最低限の事業者の属性や事業種のほかに，連携プラットフォームの種類ごとに違ったポリシー

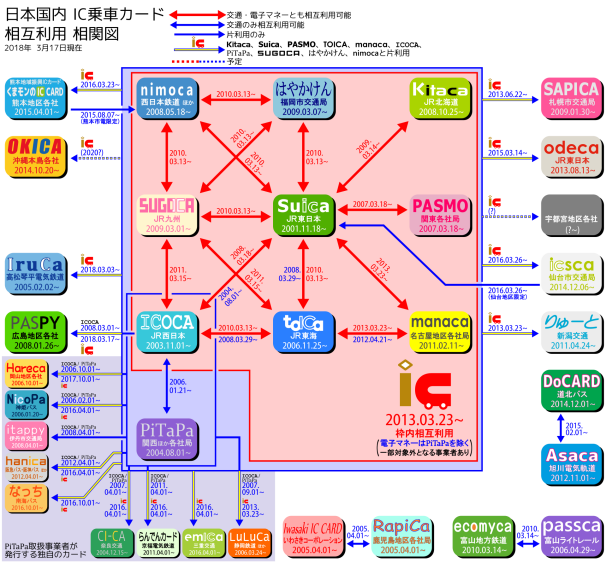

図 3　全国交通 IC カード相互利用状況 (wikipedia より引用 [15])

がある．例えば，証券会社関連の連携プラットフォームでは 1 日の取引高やストップ高になった際の取引制限などがあげられる．決済会社関連の連携プラットフォームでは，1 日の購入金額や取引回数などがあげられる．トラストフレームワークとそのポリシーに遵守できる事業者が契約を結ぶことで，事業者に対して認証情報が発行される．事業者はトラストフレームワークにトラストを委譲することになり，認証情報に基づいた情報交換に合意しているものと見なされる．

認証情報には事業者の属性や事業種などの情報が記される．各事業者は情報を交換する際に認証情報を参照し，送信先の事業者を決める．具体的には，後述の認証情報ビットと送信先ビットという二つのビット列を用いて情報ごとに送信先を決定する．

監査機関は事業者がポリシーに遵守しているかどうかを監査する役割と認証情報の発行や更新，削除等の変更をする役割をもつ．事業者がポリシーに反していると判断した場合，事業者に対して警告，罰則，契約解除などの処置をとる．また，事業者がトラストフレームワークと契約した際に事業者の認証情報を作成し発行する．さらに，事業者間の連携グループや事業者の属性が変化した場合に，事業者からの申し込みののち認証情報の変更を行う．

4.4　トラストのバリデーション手法

トラストを表現する方法として，ビット列による表現を提案する．ビット列表現の利用で高速な処理が可能となり，安定した大規模なメッセージの送受信が期待される．以下では，認証情報ビットと送信先ビットという二つのビット列を用いて，Mobility as a Service(MaaS) の一例として挙げられる移動事業者統合型ルーティングサービスを例にして説明する．このサービスでは，簡単のためタクシー，バ

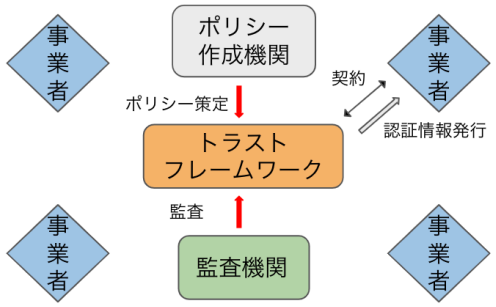

図 4　トラストモデルの概要

表 3　認証情報ビットの例

事業者	事業者 ID	大企業	中小企業	提携 1	提携 2
タクシー	1	1	0	1	0
バス	2	0	1	1	1
鉄道	3	0	1	0	1
ルーティング	4	1	0	0	1

ス，鉄道，ルーティング事業者のみが連携し，属性を企業規模 (大企業と中小企業)，提携グループをタクシーとバスのグループ，バスと鉄道とルーティングのグループの 2 グループとする．

4.4.1　認証情報ビット

認証情報ビットは各事業者ごとの認証情報をビット列にしたものである．表 3 に認証情報ビットの例を示す．各行に受信する事業者の事業者 ID と認証情報の要素が記してあり，認証情報で満たしている要素にビットを立てることでビット列を作成する．この例では，タクシーは大企業であり提携グループ 1 に属しているという認証情報を表している．鉄道は中小企業であり，提携グループ 2 に属しているという認証情報を表している．

4.4.2　送信先ビット

送信先ビットの例を表 4 に示す．送信先ビットは，送信者が送る情報毎の送信先を表すビット列である．各行に事業者の情報 ID と認証情報の要素が記してあり，送信する事業者の情報 ID と受信する事業者の属性や提携グループを選択してビットを立てる．表 4 の例では，タクシーの運賃の情報は提携グループ 1 にのみ送られることを表しており，鉄道の到着時刻は提携グループ 2 に属している大企業と認証されている事業者に送られることを表している．

4.4.3　認証方法

次に認証情報ビットと送信先ビットを用いた認証方法について図 5 と共に述べる．前提として，認証情報ビットと送信先ビットは事業者間連携プラットフォーム内のトラストデータベースに保存される．そして，送信者から受信者に情報を与える流れは以下のようになる．

表 4　送信先ビットの例

情報	情報 ID	大企業	中小企業	提携 1	提携 2
タクシー：運賃	a	0	0	1	0
バス：位置	b	0	1	1	0
鉄道： 位置	c	0	1	0	1
鉄道：到着時刻	d	1	0	0	1

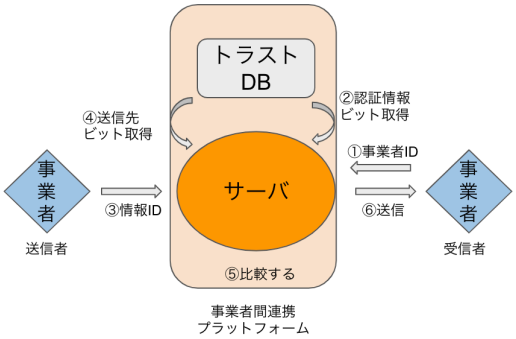

図 5　認証の流れ

表 5　認証方法の例

	大企業	中小企業	提携 1	提携 2
バス認証ビット	0	1	1	1
鉄道送信先ビット： 位置	0	1	0	1
論理積演算結果	0	1	0	1

(1) 受信者が事業者 ID をサーバに送る
(2) サーバでトラストデータベースから受信者の事業者 ID から受信者の認証情報ビットを取得する
(3) 送信者が情報を送る際に送信者の情報 ID を付与して送る
(4) サーバでトラストデータベースから送信者の情報 ID から送信者の送信先ビットを取得する
(5) 送信先ビットと認証情報ビットを比較する
(6) 送信先ビットを満たす認証情報をもつ受信者に情報を送信する

送信先ビットと認証情報ビットを用いた認証方法には論理演算を用いる．まず，認証情報と送信先ビットを論理積演算する．そして，論理積演算結果が送信先ビットと等しくなった場合に送信する．これにより，鉄道の送信先ビットを満たす事業者に情報を送ることが可能となる．表 5 にバス事業者に鉄道の位置情報を送信するか判断する計算方法を述べる．バス事業者の認証情報と鉄道事業者の位置情報の送信先ビットを論理積演算する．この場合，論理積演算結果が鉄道事業者の送信先ビットと等しいため位置情報がバス事業者へ送られる．

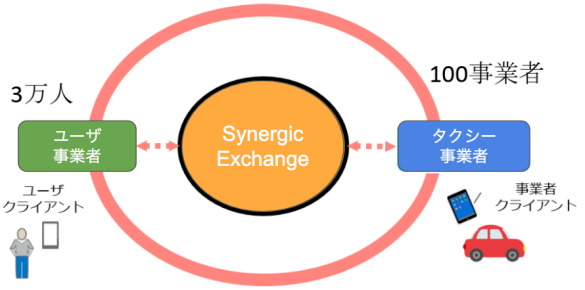

図 6　タクシー事業者とユーザ事業者による連携例

5. 実験と評価

4 章で取り上げたトラストのビット列表現を用いて，河口研究室が開発している事業者間連携プラットフォーム「Synergic Exchange」[3] に実装し処理性能を評価する．ここで実社会における事業者間連携として，図 6 のようなタクシー事業者とユーザ事業者による移動サービスを想定する．具体的な数値としてユーザ数が 3 万人，タクシー事業者を 100 社とし，一人当たり 1 日 1 回利用し一回の取引で 10 回メッセージを送受信すると想定する．その結果，想定される処理性能は毎秒約 350 メッセージとなる．以下の実験では，この値を比較値として評価する．

5.1 実験環境

表 6 に実験環境の詳細を示す．通信プロトコルは Google の開発した gRPC を利用し，サーバ側とクライアント側で二台の PC を用いた．二台の PC 間は有線ケーブルをスイッチングハブで接続した．

5.2 実験方法

ユーザプロバイダからサーバにメッセージを送信し，サーバでビット列を用いて認証を行なった後，タクシープロバイダへ送信されるまでを 1 メッセージとする．そして，合計 1000 メッセージを送信してタクシーが受信し終わるまでの時間を計測し，1 メッセージの平均を算出することを 1 ステップとする．今回の実験では，計 10 ステップ行い 1 メッセージの平均時間を測定結果とした．

そして，サーバでの認証処理手法は処理なし，if 分岐による処理，bit 演算による処理の 3 パターンに分けて行った．計算方法の詳細を以下に示す．

- 処理なし
  サーバーで処理をせず，送信されたメッセージをそのまま受信側へ送る．
- if 分岐による処理
  送信された情報を事業者に送るかどうかを if 文でひとつずつ比較していく．

表 6　実験環境

使用した機材等	機材の詳細
通信プロトコル	gRPC(Google Remote Procedure Call)
PC（サーバ）	Vaio Intel Core i7-6567U
PC（クライアント）	Surface Intel Core i7-4650U
LAN アダプタ	PLENEX GU-1000T
スイッチングハブ	NETGEAR 1000Mbps

表 7　処理性能測定結果

手法	平均通信速度 (ms)	毎秒 msg 数 (msg/s)	処理なしとの比較 (%)
処理なし	1.149	870.1	100
if 分岐	1.243	804.0	92.4
bit 演算	1.156	864.8	99.4

- bit 演算による処理
  4.4.3 項で述べた認証方法に従い，認証情報ビットと送信先ビットを論理積演算し，その結果が送信先ビットと等しければ情報を受信側へ送信する．

5.3 実験結果

手法毎の 1 メッセージの平均通信速度，毎秒メッセージ数，処理なしとの割合比の実験結果を表 7 に示す．if 分岐では平均通信速度が 1.243ms，bit 演算が 1.156ms となっている．また，毎秒メッセージ数では，if 分岐が 804.0msg/s，bit 演算が 864.8msg/s である．処理なしとの比較では，if 分岐が処理なしの 92.4%，bit 演算では 99.4%となり，bit 演算は if 分岐よりも高い処理性能を持っていると言える．

また，比較値とした処理性能の毎秒約 350msg と比較すると，約 2.5 倍の処理性能が得られていると言える．以上から，想定した規模の実社会の事業者間連携に，十分に対応できる処理性能が得られた．

6. まとめ

本研究では，事業者間連携プラットフォームにおいて，事業者間の信頼関係に基づいて情報を交換するためのトラストモデルとして，各事業者が中央機関にトラストを委譲するトラストフレームワークを提案した．さらに，トラストモデルを事業者間連携プラットフォームに実装し，実社会における実用性を測るため，実際に想定される利用例を挙げ，トラストモデルを実装した事業者間連携プラットフォームの処理性能を比較する実験を行なった．実験の結果，想定される性能の 2.5 倍の処理性能を得られた．

トラストフレームワークという外側の枠組みは固まってきたが，認証情報に何を採用するかなどの中身を精査する必要がある．そのため今後は，小規模な事業者間連携プラットフォームの具体例を考え，そのプロトタイプを開発し実際に使用することで，認証情報の内容の精査を行う．また，事業者間連携プラットフォームが増えた際に生じる

トラストフレームワーク間の情報共有などの連携にも対応する必要がある.

謝辞 本研究は JSPS 科研費 JP17KT0082 の助成を受けたものです.

参考文献

[1] 内閣府, “第 5 期科学技術基本計画”, https://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf, 2016.
[2] 河口 信夫, “自動運転社会における Synergic Mobility の創出”, 2018 年電子情報通信学会総合大会, BP-3-1(2018).
[3] Github, “Synergic Exchange”, https://github.com/synerex/synerex_alpha
[4] 千葉 隆之, “信頼の社会学的解明に向けて”, 年報社会学論集, 1996 巻, 9 号, p211-222, 1996.
[5] Audun Josang, “Trust and Reputation Systems”, LNCS, 2006 年.
[6] 森 純一郎, 武田 英明, 石塚 満, “信頼の構造 : 社会ネットワークの構造に基づく Trust モデル”, JSAI, 2007 年.
[7] ignite realtime - “All About Pubsub”, https://www.igniterealtime.org/support/articles/pubsub.jsp.
[8] Stefan Poslad, Monique Calisti, “Towards improved trust and security in FIPA agent platforms”, 2000.
[9] Raffaele Giaffreda. “iCore: A Cognitive Management Framework for the Internet of Things”, pages 350–352. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
[10] Internet of things - architecture. http://www.iot- a.eu.
[11] Preventis, Alexandros, Kostas Stravoskoufos, Stelios Sotiriadis and Euripides G. M. Petrakis. “IoT-A and FIWARE: Bridging the Barriers between the Cloud and IoT Systems Design and Implementation.” CLOSER (2016).
[12] Citysdk. http://www.citysdk.eu.
[13] D. Pfisterer, K. Romer, D. Bimschas, O. Kleine, R. Mietz, C. Truong, H. Hasemann, A. Kroller, M. Pagel, M. Hauswirth, et al. “Spitfire: toward a semantic web of things”. Communications Magazine, IEEE, 49(11):40–48, 2011.
[14] CKAN - The open source data portal software, https://ckan.org
[15] 交通系 IC カード全国相互利用サービス, https://ja.wikipedia.org/wiki/.