Computer Security Symposium 2017
23 - 25 October 2017

利用者のコンテキストを信頼する同行者検証

大神 渉[1]　五味 秀仁[1]

概要：会場への入退場を管理するなどのサービスでは，入場を許可する際に不正行為，特に各個人のなりすましを防ぐことが期待されている．サービス提供者は事前に情報を登録している利用者本人だけでなく，利用者が連れてきた同行者もなりすましていないことを検証する必要がある．これは利用者とその同行者同士が金銭などの動機づけによって結託して同行者のなりすましを成功させようとするためである．本稿では，利用者の環境情報に注目し，利用者の環境情報における同行者の存在をサービス提供者が検証可能なシステムを提案し，Android アプリケーションとして実装した．また，収集データを使って最適な手法について考察を行った．

キーワード：UWS, 同行者の検証, トラスト, コンテキスト認識

Companions Verification Using The Trusted User Context

Wataru Oogami[1]　Hidehito Gomi[1]

Abstract: Services such as managing entrance or exit is expected to prevent attack, especially spoofing. In order to prevent it, the number of cases where users pre-register their information in a Service Providers (SP) has increased. It is necessary for the SP to verify not only the person registered his information in advance and also his companions. In this paper, we focused on the user's context information and proposed a system that the SP can verify the existence of companions and implemented it as an Android application. In addition, we conducted experiments to confirm that we can respond flexibly to the circumstances of users.

Keywords: Verifing companions, Trust, Context-awareness

1. はじめに

実世界でサービス提供を受ける際に，ネットワークを介したオンラインで登録した情報により，なりすましなどの不正行為が行われていないか確認する手段が必要とされている．例えば，電子チケットの販売サービスでは，転売行為を防止する目的で購入時に登録しておいた情報を使い，当日会場でチケットを提示した人と購入者が一致していることを確認する．その際，サービス提供者 (Service Provider; 以下 SP) は身近な人間と共に参加したいとする購入者の要望を叶えるために，一度の購入につき複数の同行者分まで登録を行うことでサービスの利便性を高めている．つまり，SP はこれまで検討してきた登録者だけではなく，同行者についてもその不正の有無を検証する方法がユーザーの利便性と両立した上で提供する方法が必要とされている．

同行者の不正を検証する手法として，**登録者の自己申告を信頼する方法**と，**登録者と同行者双方を確認する方法**の 2 つが多く採用されている．これらの手法では，不正行為の防止する代わりにサービス提供時のユーザーや SP が負担を負わなくてはならない．

登録者の自己申告を信頼する方法は，SP が登録者を本人であることを確認したうえで，登録者が自己申告した同行者の確認を省略する方法である．登録者は本人が選んだ任意の同行者と一緒に参加することが可能となるメリットが有る．しかし，登録者と同行者は結託して虚偽の申告を行う可能性があり，SP が申告を適切であるか検証することはできない．SP は登録者の申告が信頼できないリスク

[1] ヤフー株式会社
Yahoo Japan Corporation, 1-3 Kioicho, Chiyoda, Tokyo 102–8282 Japan

を軽減するため，例えば同行者の人数を 1 人に制限するなどの利用制限を行う．これでは登録者は共に行きたい人数を満たせないため，サービスを受ける上で負担が大きい．

一方，**登録者と同行者双方を確認する方法**は，登録者が同行者の分の情報を合わせて SP に登録しておくことで，登録者と同行者双方をそれぞれ確認する．SP は登録者と同行者双方が登録されている情報と一致する人物であることを確保でき，不正行為を防止する効果が高い．しかし，登録者と同行者の結託を防ぐために登録者の後に登録者と同行者の情報を変更することが許可されていない．そのため，登録者は登録時までに全ての同行者を決定しておく必要があり，もし同行者や自身がいけなくなってしまった場合には心理的，金銭的負担が発生する．一方で，同行者も例えば住所や電話番号など自身を確認する情報を登録者に預けて登録してもらうため，その心理的負担が大きい．また，SP も会場での確認を行う手間が同行者分だけ増えるため，運用負担が増加する．

SP は運転免許証などのほか，生体情報を使うことでより厳密に登録者の確認方法を充実させる一方，このように登録者と同行者が結託して不正行為を行っている際に検証する方法をユーザーの利便性を確保した上で提供できていない．本稿は，SP が登録者を様々な方法で確認した上で，登録者の普段のふるまいから同行者として指定したユーザーが登録者と結託する不正行為を働いていないことを検証するシステムを提案，実装した．また，実装を通じて得たデータを通じて最適な運用についても議論を行った．

本稿では，**登録者の自己申告を信頼する方法**が実現するユーザーの利便性と**登録者と同行者双方を確認する方法**が実現する不正行為の防止効果について共有し (2 章)，それらをもとに前提となる新たなトラストモデルについて論じる (3 章)．さらに，これらを解決する方法を設計，具体的な問題を解決するシステムを実装し (4 章)，最後に提案システムに対する攻撃耐性や限界について考察した (5 章)．

2. 問題

問題設定に必要なロールをその信頼関係から整理し，具体的なユースケースを提示して，その課題分析を行う．

2.1 ロール

問題を扱う上で必要なロールとその信頼関係を整理する．

SP Service Provider．ユーザーが信頼できる第三者機関でサービスを提供する主体．サービスを提供する際に後述する登録者やその同行者が信頼できないケースが存在するため，それらを検証することで信頼可能か (提供が可能か) を判断する．

登録者 サービスを提供してもらうために事前に SP が検証に必要とする情報を登録するユーザー．例えば，興行チケット販売を行う SP に対して，その購入者を指す．サービス提供を受けるために SP を信頼してできるだけ正確なデータを預ける．また，同行者を信頼し，動機があれば結託して第三者を同行者として偽る可能性がある．

同行者 登録者が SP に申告し SP がそれを認めた場合，登録者と共に SP からサービス提供を受けるユーザー．登録者が自分自身だけを登録するなど同行者が存在しなくてもよい．本稿では，同行者が存在する場合に起こる問題について議論する．サービス提供を受けるために登録者を信頼し，できる限りそれに協力する．また，サービス提供を受けるために第三者がなりすまして，SP の検証を誤らせようとする可能性がある．

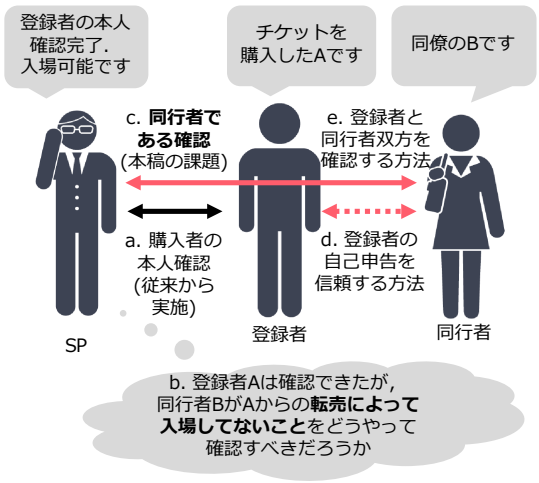

図 1 ユースケース: 転売防止のための検証と従来手法

2.2 ユースケースと従来手法の分析

図 1 に本稿が解決する問題のユースケースとして，興行チケットにおける登録者 (購入者) による同行者への転売が疑われるケースを提示する．一般的に転売行為とは，登録者が他人へ自身が購入したチケットを売りつける不正行為を指す．つまり，金銭などを受け取る代わりに，購入したチケットを第三者が持参することで登録者や同行者になりすまそうとする行為である．SP は転売を防止するため，SP はオンラインでの購入時に登録者自身の情報 (例えば，氏名や住所など) を登録させる．また，登録者がそれらの情報を確認する手段 (例えば，運転免許証) とともにチケットを提示することで，SP は登録者を検証し，それが正しい場合にのみサービス (入場の許可) を提供する．従来，購入したチケットを登録者本人が使うことを SP が検証することで防止を試みてきた [1]．しかし，多くの興行は複数人で参加することが多く，チケットは複数枚が同時に購入されることが多い．このように登録者以外に同行者が存在する場合，転売が行われていないことを確認する手法について，特に登録者自身は本人であるものの，同行者として適切な人物が入場を試みていることを SP がユーザーの利便性が

十分に確保しながら検証する手段が提供されていない．

ユースケースの問題を図 1 の記号 **a-c** を使って示す．

a. 登録者 A は本人が会場へ来場し，SP が事前に登録した情報と照合することで A であることが確認する．

b. 一方，SP は会場にて登録者が同行者と申告した B について，登録者の申告が適切であるかを検証できない．

c. これは，A がチケットの購入時に B の情報を登録していない，あるいは B を連れてくることは未定であったため，SP が直接 B を確認する情報がないことが原因である．

これらの問題に対して，従来手法では図 1 内の **d. 登録者の自己申告を信頼する方法**と **e. 登録者と同行者双方を確認する方法**の 2 つのアプローチから解決を試みている．

d. 登録者の自己申告を信頼する方法は，SP が登録者を本人であることを確認したうえで，登録者が自己申告した同行者の確認を省略する方法である．登録者は購入したチケットを同行者へ譲渡するために結託し，登録者の自己申告が嘘の可能性がある．つまり，登録者は同行者へ転売を行っている可能性があり，その場合両者は結託して入場を SP に許可させたい動機が存在する．したがって SP が同行者自身を直接確認できないこの方法は，SP による同行者が適切な人物でないかもしれないというリスクの受容であり，そのリスクを軽減するための実施例が存在する．例えば，入場時に登録者と同行者が同時に入ることが求められる [2]，購入枚数が制限されている [3]，などが存在する．これらのサービスでは，SP のリスク受容が多い (不正利用の排除数を少なくする) ほど，同時に入場する人数や入場のタイミングを柔軟に変更できるなどユーザーの利便性が高くなる．しかし，リスクを軽減しようとする (不正利用可能なチケットを減らす) ほど，逆にユーザーの利便性は低くなる．

e. 登録者と同行者双方を確認する方法は，登録者が同行者の分の情報を合わせて SP に登録しておくことで，登録者と同行者双方を確認する方法である．もし，登録時以降に追加で情報を追加・変更が可能な場合，登録者と結託することにより，転売を行った同行者であっても登録が可能であるため，この手法では禁止とされている実施例 ([4][*1] など) がある．これらのサービスでは，同行者も登録者と同様に事前に登録された本人であることを確認できる．一方，登録者は事前に同行者を予め決める必要があり，ユーザーの予定に柔軟に対応することが難しく利便性が制限されることがある．また，SP にとっても従来行ってきた登録者の確認 (**a**) に加えて同行者も同様の手間をかけるため検証の負荷が大きい．

このように，従来手法による同行者の確認では，転売行為を防ぎつつユーザーの利便性のバランスを取る必要があり，以下の 3 つの課題がある．

[*1] 「※転売防止対策のため、2 枚でお申込みの場合、お申込み時に 2 名様分までの同行候補者の登録が可能です。」

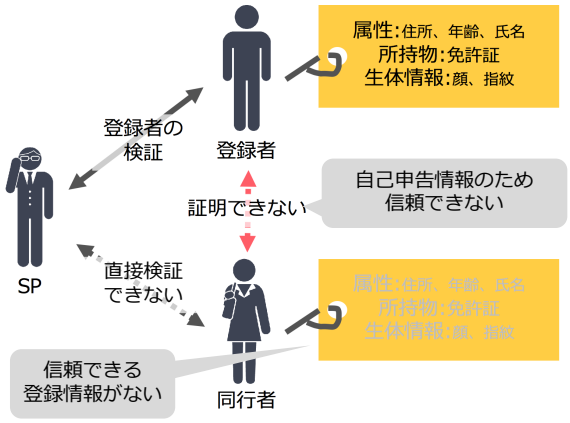

図 2　従来のトラストモデル

(1) 登録者の自己申告を信頼できないリスクが発生する (手法 **e**)

(2) 登録者が同行者を予め決定する必要がある (手法 **d**)

(3) サービス提供の際にユーザーと SP 双方の負担が大きい (手法 **d, e**)

本稿ではこれらの課題を解決するための手法を提案する．

3. システム設計のアプローチ

従来手法における利点を組み合わせることによってこれらの課題を解決する．つまり，登録者の自己申告を信頼する方法におけるユーザーの利便性を保ちつつ，登録者と同行者双方を確認する方法における不正行為の防止を期待し，SP と登録者，同行者の 3 者間でどのようなトラストモデルが検証に適するか議論する．また，そのトラストモデルにおいて SP が信頼し，検証すべき情報についても本章で整理する．

3.1 トラストモデル

本稿の課題を解決する前に，従来手法におけるトラストモデルを提示し，その問題点について整理する．図 2 に，従来手法で検証を行う際の 3 者間のトラストモデルを示す．SP は登録者に事前に登録してもらう情報を使って登録者を検証する．一方，SP から見て同行者は登録者が申告した情報であり，登録者と同行者が結託している可能性があるためこれを信頼できない．また，登録者の自己申告を信頼する方法では SP が直接同行者を検証するための情報がなく，同行者を信頼することができない．既に述べたとおり，登録者と同行者双方を確認する方法により同行者の情報を登録してもらうためには 3 者がサービスの提供を受けるまでに何らかの負担を追う必要があり，利便性が低下する．このように，従来手法では，自己申告に対して十分な信頼が得られず，直接 SP が持つ情報を元に同行者を検証するには負担が大きくなる．

これらの問題を解決するためには同行者を別の方法にて信頼できるモデル構築が必要である．そこで，従来手法の

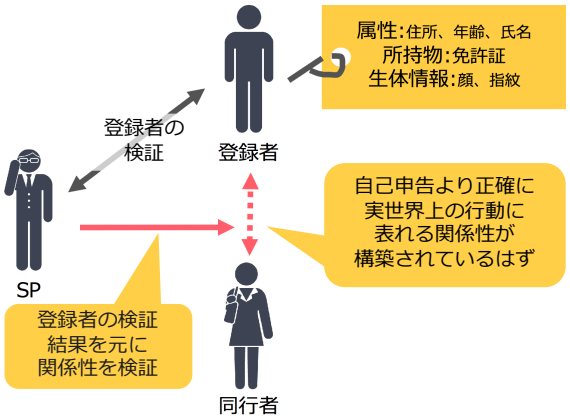

図 3　信頼する情報の変更

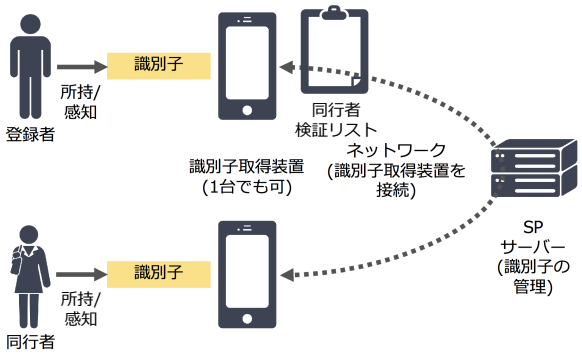

図 4　設計: システム構成

トラストモデルを元に，この問題を解決しうる信頼のポイントを整理する．図 3 のトラストモデルに示すように，従来手法と信頼する情報を変更する．従来手法では，登録者の自己申告を検証する方法を SP が持たず，検証を行おうとするとユーザーに不利益が生じ得る．そこで，この自己申告自体が正しいかどうかを登録者自身の振る舞いから SP が検証することを可能にする．SP は後述する登録者のコンテキスト情報を用いることで登録者と同行者の関係性を検証することができる．

3.2　コンテキスト情報とそれを用いた検証

ユーザーの実世界の行動に基づいた情報をコンテキスト情報と呼ぶ．コンテキスト情報は，例えば GPS (Global Positioning System) やユーザーの周囲にある Wi-Fi のアクセスポイント，スマートフォンに組み込まれた加速度センサなどユーザーの行動や状況を SP が理解することに役立つ．本稿で議論するトラストモデルは，種々のコンテキスト情報を解析することにより，登録者と同行者の関係性を SP が検証可能にすることを想定している．コンテキスト情報は数が多いため，全てを網羅することはできないが，それを活用した検証について具体例を 2 つ列挙する．

3.2.1　近接コンテキスト情報

近接コンテキスト情報とは，実世界で物理距離の近接を検知するための情報である．例えば，Bluetooth 機器は周囲に存在する機器の情報を取得することで，ユーザーの周囲にある機器の数やそれらと情報を共有するための識別子を得ることができる．また，GPS や Wi-Fi による位置情報を用いればユーザーの絶対位置を知ることができ，それらを複数のユーザーと比較することでそれらが近接しているか否かを検証することが可能である．

3.2.2　行動コンテキスト情報

行動コンテキスト情報とは，実世界でユーザーの行動に紐付いた情報である．例えば，スマートフォンの加速度センサを用いれば，ユーザーが走っている，歩いているなどその行動の状態を知ることができる．また，ストレージ内の写真を分析することにより，共に時間を過ごした家族や友人等を知ることもできる．

4.　設計と実装

これまで議論したアプローチで課題を解決するシステムを設計・提案し，その具体的な実装を示す．

4.1　設計

まず，提案手法を実現するために必要なシステム構成から抽象的な設計を提案する．図 4 に提案手法の抽象設計を示す．まず，各部の用語を以下のように整理する．

識別子　ユーザーの所有物や周囲環境を特定する記号．例えば，スマートフォンには MAC アドレス (Media Access Control Address) が機種ごとに割り振られている．提案手法では，コンテキストに応じた識別子を必ず付与するものとする．

識別子取得装置　識別子を取得するための装置．例えば識別子が NFC カードへ付与された記号であれば，それを読み取るリーダーが該当し，図 4 のようにスマートフォン (取得装置) 自身から識別子を取得する場合があってもよい．提案手法においては，必ず 1 つ以上の識別子取得装置が存在する．識別子取得装置にはその上で動作する SP が提供するアプリケーションが含まれても良い．

ネットワーク　識別子取得装置同士または後述する SP が提供するサーバーと必要に応じて接続する媒介．

サーバー　識別子取得装置からの情報を元に，何らかの処理を行った後返答する装置．例えばネットワークとしてインターネット網を用いる場合，Web サーバーとして動作する．

同行者検証リスト　SP が登録者のコンテキスト情報とポリシーから作成する同行者候補とその条件のリスト．同行者検証リストは識別子取得装置やサーバー上で SP が生成し，管理する．

提案手法は用いるコンテキストに応じて，具体的に必要な実装が異なる．図 4 に示した例を使って，このシステムが

先述したユースケースでどのように動作するかを述べる．識別子として WiFi の SSID (Service Set Identifier) を，識別子取得装置としてスマートフォンを，ネットワークとしてインターネット網を，サーバーは WebAPI を提供する Web サーバーとする．SP はスマートフォンに向けてアプリケーションを提供し，登録者と同行者はそれぞれ自身のスマートフォンにインストールする．また，その際各自ユーザー ID を使ってログインする．

(1) アプリケーションは登録者周囲の SSID を定期的にセンシングする．
(2) 手順 1 においてセンシングした SSID は都度ネットワークを通じて SP へ送信し，ユーザー ID と紐付けて管理する．
(3) 登録者は SP のサービスにてチケットを購入する．(この手順は 1, 2 と順番が前後しても良い)
(4) 登録者及び同行者はイベント当日に会場へ来場する．
(5) まず，登録者はサーバーから電子チケットを取得する．
(6) 手順 5 で入手した電子チケットとともに，登録者は例えば運転免許証と事前に登録しておいた情報を使って，本人であることを SP が検証する．
(7) 次に登録者はサーバーに対して，同行者を例えばそのユーザー ID を使って申告する．
(8) SP はサーバー上で登録者と同行者の SSID のリストを比較し，同行者検証リストを作成する．
(9) 手順 7 の申告に応じて，同行者検証リストにそのユーザー ID が含まれているか確認し，含まれている場合には同行者にも登録者と同様のチケットを提供する．

ネットワークやサーバー，識別子取得装置は用いるコンテキストにより適切に縮約して実装することができる．

4.2 近接コンテキストを用いた実装

ユースケースにおける具体的な課題を解決できることを示すため，Bluetooth 機器を用いてユーザー同士の近接コンテキストを使い転売行為による同行者のなりすましを防ぐ方法を実装した．Bluetooth 機器のセンシングでは連続的に多くの行動的特徴が得られることがわかっている [5]．図 5 に実装したシステムを示す．この実装では，ネットワークやサーバーを用いず，識別子として Bluetooth 機器の UUID を，識別子取得装置として各ユーザーが所有するスマートフォンを用いた．また，登録者は SP が配布するアプリケーションを事前にインストールし，以下の手順に従って提案手法を実現する．

(1) 登録者が SP の Web サイトにおいて，同行者の人数を指定してチケットを購入する．
(2) 登録者のアプリケーションは普段の生活圏において，周囲の Bluetooth 機器の UUID[*2] をセンシングし，記憶する．実装では 30 分毎にセンシングし，その値を計測した Unix timestamp とともに CSV として保存した．
(3) 登録者や同行者の予定に柔軟に対応するため，イベントの開催日が近くなったらチケットの受け渡し期間を設ける．受け渡し期間が始まったら，アプリケーションはそれまで蓄積したコンテキスト情報から同行者検証リストを作成する．この際，SP のポリシーを反映する．
(4) 受け渡し期間では，登録者が申告した同行者に購入したチケットを渡すことができる．この際，手順 3 で作成した**同行者検証リストの中からのみ**同行者を選択する．
(5) 会場で登録者が SP による検証によって確認した後，同行者に受け渡された情報はチケットとしてその真正性を確認することで入場することが可能である．

受け渡された情報はスマートフォン上の OS 上で SP が提供したアプリケーション以外からアクセスを受け付けず，同行者から他人への譲渡は許可しない．

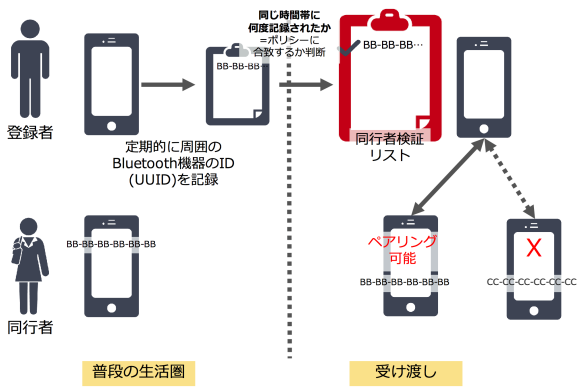

図 5 近接コンテキストを用いた実装

こうした実装により，2.2 章で述べた課題を以下のように解決している．

(1) SP が登録者の自己申告を信頼できないリスクは，登録者の日常生活圏におけるコンテキストを SP が提供するアプリケーションによって観測し，同行者を特定する事によって解決した．
(2) 登録者は SP の購入時にアプリケーションをインストールすることにより，同行者を予め購入時までに決定する必要がない．
(3) サービス提供の際にはユーザーと SP 双方の負担を軽減している．まず，ユーザーに対しては受け渡し期間で受け渡しができるため，個々の事情に合わせて来場時間を決めることができ，また購入枚数に制限をかけずに SP による同行者の検証が実現可能である．また，SP は登録者の検証を行うこと，同行者に関しては情報の真正性を確認することによって従来手法と同様の

[*2] Universally Unique IDentifier

表 1　実装環境

OS	Android 7.1.1
プラットフォーム	Android Studio 2.3.3
言語	Java

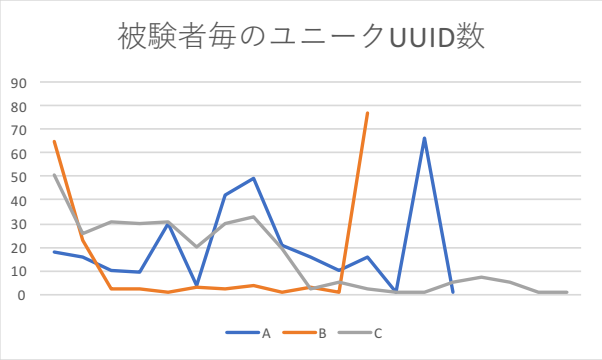

図 6　被験者のセンサデータの概要
縦軸:取得したデータ数 横軸:各被験者別の時間経過

表 2　収集データ

被験者名	A	B	C
ユニーク UUID 数 [デバイス]	209	77	163
計測期間 [日]	4	2	2
同行対象 [台]	1	2	2
同行対象検知 [回]	1	5 + 4	0 + 0
総センシング [回]	15	11	19

検証にかかる負担でサービスの提供可否を判断することが可能である．

また，今回実装した環境を表 1 に示す．

4.3　取得データ

実装によって得られたコンテキスト情報を分析し，ポリシーで本稿の課題を解決しうるかについて議論する．

4.3.1　分析

被験者として 3 人に協力してもらい，実装したアプリケーションを使って，30 分毎，2 日間以上被験者の周囲に存在する Bluetooth 機器の UUID を収集した．予め被験者には自身が同行者として許可しても良い UUID(同行対象と呼ぶ) を申告してもらい，取得データは各被験者のスマートフォン内のストレージに蓄積し，そのデータを分析する．まず，図 6 に被験者毎の時間軸におけるユニーク UUID 数を示す．それぞれで時間は異なるものの，各個人によりコンテキスト情報が対して大きく異なり，登録者の周囲の環境を把握できることが読み取れる．ヒアリングの結果，在宅とオフィスへの勤務の時間帯などにより顕著な違いがあることがわかった．また，表 2 に収集したデータの概要を示す．被験者 A, B は同行対象の持つデバイスを検知することができたが，被験者 C に関しては同行対象を一度も検知することができなかった．被験者 C の同行対象は両方別のプラットフォーム (iOS) の iPhone を使用しており，今回のアプリケーションによって明確な前準備 [*3] がない状態では自動的な検出ができなかった．

また，アプリケーションはバックグラウンドで 30 分毎に動作することを意図していたが，総センシング回数から，各スマートフォン上での電力，メモリなどのリソース不足などによりデータ収集がキャンセルされることがわかった．プラットフォーム間の違いや動作の制御などは実システムの運用において検討する今後の課題である．

表 3　同行者検証リストのポリシーによる絞り込み

被験者名	A	B	C
ポリシーなし	209	77	163
2 回以上	48	20	49
3 回以上	25	4	2
4 回以上	6	2	2
4 回以上+時間帯	0	2	0

4.4　ポリシー設定

提案システムにおいて課題を解決する際に最も重要なことは，登録者が申告したい同行者が同行者検証リストに含まれているか，そして申告する同行者が結託によりなりすましていないかである．つまり，収集したデータに対してどのようなポリシーを SP が設定すれば適切な制御ができるかという議論である．当然だが，ポリシーによって SP が受け入れ可能なレベルも異なり，一概に最適なポリシーを提供することは難しい．

もし，必要以上に厳しいポリシーを適用した場合，同行者検証リストに適切な同行者が入らず，提案手法によりユーザーの行動を制限してしまう．一方，ポリシーをゆるくすることによりユーザーに結託を許してしまう可能性がある．ここでは，簡易なポリシーと厳しいポリシーの例をあげ，それぞれの特徴について議論を行う．

簡易なポリシー一番簡易なポリシーの例として，日常生活におけるセンシング回数の頻度で設定することが可能である．このポリシーによって作成した同行者検証リストは，近接コンテキストの特性が活かされる．つまり，日常生活圏で接したことの有る多くのデバイスを対象として，同行者として申告することが可能であり，ユーザーの利便性を高める可能性がある．

厳しいポリシー厳しいポリシーの例としては，簡易なポリシーに加えて時間帯など別の情報が活用できる．例えば，ある一日で検知した UUID を別日の同一時間帯に検知することは反復性のある関係性でなければ再現が難しい．

表 3 にそれぞれのポリシーを適用した結果，今回の実装で収集したデータがどの程度の大きさの同行者検証リストを作成するかを示す．それぞれ，頻度の回数以上のカウントがあった UUID の数と，さらに同一時間帯 (1 時間内の誤

[*3] 「設定」から「Bluetooth」を選択し，周囲の対応機器を探すことが同行者のスマートフォン上で行う

差) で検知された UUID の数を示している．

前述のように様々な要因の影響を受けて今回の取得データは完全なものではない可能性もあるが，被験者 A のように長い期間データを取得しても頻度 2 回以上のユーザーだけでも 48 台 (ポリシーがない場合の約 23%) まで絞り込んでいる．また，データの取得回数 (表 2 参照) に依存して特に低い頻度のデバイスが増えることがわかるため，例えば各個人での回数における比率など動的に決定するパラメータによって調整することで制御が可能になる可能性がある．被験者 B で厳しいポリシーにおいても検知できた 2 台のうち，1 台のデバイスは被験者 B が希望する同行者であった．また，頻度 3 回以上のみのポリシーであれば被験者 B が指定する 2 つのデバイスが含まれている．ここから，登録者のコンテキスト情報にポリシーを適用することにより同行者候補を適切に選択できる可能性がある．また，被験者 C の結果から，厳しいポリシーが大きく絞り込みに寄与していることがわかる．今回の実装においては計測していないが，時間帯だけではなく接続履歴や RSSI (Received Signal Strength Indicator) など他のパラメータを使うことで更に厳しくできる可能性があり，これらは実験により明らかにできる可能性がある．

5. 考察

提案手法を用いることで，SP は登録者の検証結果が正しいことを元に，登録者の申告をその行動から同行者として適切か検証を行い，課題を解決できることについて既に述べた．ここでは，提案手法の適用や実施を考える上で，他の攻撃によるなりすましの可能性と，提案手法のユーザー利便性の限界について述べる．

5.1 他の攻撃手法

登録者と同行者の結託により，登録者の日常的な行動と全く関係のない識別子に対して同行者検証者リストがそのなりすましを防御可能である．提案した設計では，ユーザーがそれぞれ 1 つの識別子だけを持つ場合を取り上げた．ただし，現実には例えば複数のスマートフォンを所持するなど，個人が正当な理由で所有する識別子が 2 つ以上存在することは十分に考えられる．

例えば，ユースケースにおいて登録者が 2 つのスマートフォンを所有し，会場において登録者の確認を受けた後，別の端末に受け渡し，その端末を入場時に一時的に貸与する攻撃が考えられる．この攻撃が成功する理由は 2 つあり，1 つは，登録者の他のデバイスを同行者のものとしてみなしてしまう識別性である．もう一つは，持ち運び可能な状態 (ベアラートークン) でチケットを受け渡せることである．これらに対して提案手法がどのように対応可能であるか考察を行う．

まず，十分な識別性を確保するためにはポリシーの工夫とコンテキスト情報の拡充で対応する．ポリシーの工夫は，共起が強すぎる識別子を排除することで登録者自身の不正を防ぐ．登録者は 2 台のスマートフォン A, B を所有しており，本稿の実装を適用すると，A に登録者のデバイスとしてアプリケーションをインストールすると，ほぼ常時同じコンテキストを共有するデバイス B は非常に強い共起を持つ UUID として同行者検証リストに加えられる．ポリシーを工夫することによって，こうした識別子を排除することで識別性は確保できるものの，例えば休暇期間の家族なども排除してしまい，利便性を損ないかねない．そこで，他のコンテキスト情報を使うことでこれをカバーする．例えば，登録者が複数台のスマートフォンを保つ場合，本稿の実装の他，デバイスの加速度など動きも共起する可能性が高く，また，他人の利用しているデバイスは違う行動を起こしている可能性が高い．実際の動作に限らず例えば登録者が一人で複数のゲームアプリをプレイするなどは難しい．このように同行者検証リストを作る際に強すぎる識別子を排除しつつ，複数のコンテキスト情報を取得することにより更に柔軟に同行者検証リストを作成することが可能である．

一方，識別性を確保したところで，100%登録者の所有する複数識別子を同行者検証リストから省くことはできない．例えば，普段は使わない余剰デバイスなどを使う場合，それらを識別することは難しい．識別できない登録者の別識別子は，ベアラートークンとして結託した同行者に貸与される可能性が有る．そこで，同行者にはチケットを提示する際に例えばスマートフォンのロックなど，識別子に対して適切な人間で有るかを SP の目前において確認することによりこれを解決する可能性がある．スマートフォンのロック方法をとっても，パターン入力，PIN コード，指紋等様々な方法があるが，結託によって簡単に情報共有できるものではなく，生体情報などを使うことが望ましい．

5.2 提案手法の限界

これまで，課題としてユーザーの利便性の問題も取り上げてきたが，提案手法にも限界が有る．ここでは，実装及び実験を通じてわかった提案手法の限界を 3 点考察する．

1 つ目の限界は，多くのユーザーがコンテキスト情報の取得を停止していることである．これは実装に限った話ではなく，電池消費量や不要な通信を避けるために Wi-Fi の利用を避けたり，あるいはアプリケーションの一部機能の権限を許可したりしない．こうした登録者及び同行者に対しては本提案手法が提供できない可能性がある．そこで，各ユーザーが利用可能な複数のコンテキスト情報を用いると共に，機能を実施するための情報提供に対して十分な理解を得て実施することが必要である．

2 つ目の限界は，同行者検証リストを使って同行者へサービスを提供可能であることを事前に明示することが難しい．

前述の通り，同行者検証リストは受け渡し期間になるまで確定しないため，登録者および同行者が受け渡しを意図した相手に行えるのかどうかがそれまでわからず，利便性を低下させてしまう可能性がある．そのため，例えば事前に同行者が決まっている場合には従来手法を用いるなど，複数の選択肢がユーザーに与えられる必要がある．

3 つ目の限界は，例えば今回の実装において遠方の親類など，登録者のコンテキスト情報に表れない同行者の検証はできない．趣味嗜好などで共通したインターネット上の匿名でのつながりなど，他のドメインでのみつながりのある同行者は例えば電話帳など他のコンテキスト情報を使うだけでは検証ができない．今後の課題として，過去の写真や認証連携における属性交換などにより，間接的にコンテキスト情報を共有したことを検証する方法を検討する．

6. 関連研究

登録者とともに同行者が存在し，それらに対して検証が必要な状況は本稿のユースケースや来客システムなど社会に広く浸透しているシステム，ケースである．しかし，登録者と同行者の間に金銭などの具体的な動機づけが生じ，結託によってなりすましが成立するケースについて議論する研究は少ない．本人性を高い確率で検証できる生体情報を用いる [1] など，登録者本人の確認はこれまで以上に堅牢になるなか，SP が信頼できない同行者の検証やその利便性には社会的注目が集まることが予想される．ここでは，提案手法に関連するコンテキスト情報や信頼を元にしたアクセスコントロール手法としてこれまでの研究を紹介する．

コンテキスト情報を用いたアクセスコントロールを行う研究として，Khan ら [6] が医療ドメインにおけるコンテキスト情報を用いたアクセスコントロール手法を提案している．これらは各個人のロールに加えてそれぞれの状況を認識してそのアクセスコントロールを行う．コンテキスト情報をつかって柔軟に状況認識を行うことでリソースへのアクセスを管理しているという点で同行者への制御と類似する問題ではあるが，登録された個人を認証しユーザーに提供してよいかを判断する点で問題設定が異なっている．

また，信頼を元にしたアクセスコントロールとしては Banyal ら [7] がクラウドコンピューティング環境において動的な信頼を与えることでこれを制御する手法を提案した．これらは登録された各個人に対して要求された権限に必要な信頼を証拠となる情報から動的に計算することで制御する．個々人の信頼に基づいたアクセス制御を行うという点においてリスクを増減できる点で本稿のトラストモデルと類似するが，信頼関係や事前情報のない同行者の検証を行うという点において本稿の問題設定とは異なる．

7. おわりに

登録者と同行者が結託する可能性がある時に，これまで注目されていた登録者の本人性の検証だけでなく，同行者との結託を行う必要性について問題を提起した．また，この問題に対して，SP が信頼できる情報を持つことが様々な面で難しい同行者の確認を，登録者のコンテキスト情報を使うことでユーザビリティを損なうことなく検証することによって実現するシステム設計を提案・実装した．今後の研究では，より多くのユーザーに提案手法を提供するため，実際のサービスにおける提供を実施し，提案手法のメリットを検証したい．また，使用するコンテキスト情報の選択肢を様々に増やすことにより，ユーザーの利便性やポリシーの多様性を確保することで，例えば熱心なファンには多くの信頼を与えるなど，これまで吸収できなかった同行者に関する SP のポリシーを実現したい．最後に，アプリケーションの更に精緻な実現と，攻撃を再現しその実態や利便性の向上を定量的に示すことは今後の課題である．

参考文献

[1] Okumura, A., Hoshino, T., Handa, S., and Nishiyama, Y. Identity confirmation to issue tickets using face recognition. Technical report, NEC Informatec Systems Ltd., 2016.

[2] スマートフォン専用電子チケットアプリ「EMTG チケット」入場方法のご案内. `https://fan.tsite.jp/ticket/emtg_guide`. 参照 2017–08–14.

[3] サカナクション公式サイト. `http://sp.sakanaction.jp/feature/nf1r_20170218`. 参照 2017–08–14.

[4] 星野 源 | チケット情報・販売 ローチケ hmv[ローソンチケット]. `http://l-tike.com/concert/hoshinogen/`. 参照 2017–08–21.

[5] Yiqiang Chen, Zhenyu Chen, Junfa Liu, Derek Hao Hu, and Qiang Yang. Surrounding context and episode awareness using dynamic bluetooth data. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pp. 629–630, NY, 2012. ACM.

[6] M. Fahim Ferdous Khan and Ken Sakamura. Context-awareness: Exploring the imperative shared context of security and ubiquitous computing. In *Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services*, pp. 101–110, NY, 2012. ACM.

[7] R. K. Banyal, V. K. Jain, and Pragya Jain. Dynamic trust based access control framework for securing multi-cloud environment. In *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, pp. 29:1–29:8, NY, 2014. ACM.