位置情報を活用したライフスタイル認証のゲームプレースタイルへの適用

小林 良輔[1,a)]　Mhd Irvan[1]　Franziska Zimmer[1]　Roberta Tamponi[1]
Maharage Nisansala Sevwandi Perera[1]　山口 利恵[1]

概要：近年 e スポーツが普及し，e スポーツ大会も開催されるようになった，大会の参加人数を増やすためにオンライン開催が一般的だが，運営者は登録したプレーヤーが実際に操作しているかを検証する必要がある．しかしながら従来の個人認証手法では，正当プレーヤーと不正操作プレーヤーが結託している場合に検知することができない．そこで我々は，ゲームのプレースタイルから本人かどうかを検証できないかを考えた．物理空間では位置情報を活用した認証手法が存在するが，その手法をゲーム内にも適用することでプレーヤーを認証することを試みた．しかし実験の結果，ゲーム内の位置情報のみではプレーヤーの特性を見出すことは難しいことがわかった．ゲームデータ特有の特徴量の選択含め，適切な認証手法の設計が必要である．

キーワード：e スポーツ，プレイヤー認証，協力的なりすまし，プレースタイル認証

Application of Location-based Lifestyle Authentication to Game Play Style

Ryosuke Kobayashi[1,a)]　Mhd Irvan[1]　Franziska Zimmer[1]　Roberta Tamponi[1]
Maharage Nisansala Sevwandi Perera[1]　Rie Shigetomi Yamaguchi[1]

Abstract: In recent years, eSport games have gained popularity, and eSport tournaments have started to be held. To increase the number of participants, it is common to hold these tournaments online. However, organizers of the tournaments need to verify that the registered players are the ones actually playing the game. Traditional authentication methods of user authentication fail to detect cases where legitimate players collaborate with unregistered players. Therefore, we considered whether it might be possible to verify the identity of a player based on their gameplay style. While there are authentication methods in the physical world that utilize location data, we attempted to apply this approach within the game to authenticate players. Our experiments revealed that it is difficult to identify player characteristics only applying in-game location data to phisical location-based authentication methods. We can find the necesitty to design appropriate methods for authentication using game data including various features.

Keywords: eSport, player authentication, collaborative impersonation, playstyle authentication

1. はじめに

近年，コンピュータゲームやビデオゲームを使って行われる対戦競技の e スポーツ (エレクトロニック・スポーツ) の普及が拡大してきており，2025 年の日本における市場規模は 200 億円を超えると予測されている [1]．この分野では参加プレイヤー同士が競う大会が開催されており，参加者が集まって実施されるオンサイト形式と，オンラインで実施される形式とがある．運営者は大人数の参加を可能と

[1] 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo
[a)] kobayashi@yamagula.ic.i.u-tokyo.ac.jp

して大会の規模を大きくするため，オンライン形式での実施が一般的である．このような大会において成績優秀者は賞金を獲得することができるが，健全な大会運営のために運営者は賞金を不正に獲得されないよう保証しなければならない．特にオンライン形式の大会においては注意が必要である．

不正な賞金獲得方法として，正規に参加登録したプレイヤーでなく，不正プレイヤーが大会に参加して賞金を獲得することが考えられる．例えば，ゲームの熟練度を表す指標であるランキングといった参加条件を満たさないプレイヤーが不正に大会に参加することである．このような不正プレイヤーは参加条件を満たす正当プレイヤーになりすまして大会に参加しようとするが，賞金を獲得したいと考えている正当プレイヤーは不正プレイヤーと協力する恐れがある．このようなケースで被害を受けるのは，不正プレイヤーがなりすました正当プレーヤーではなく，大会運営者や他の参加者となる．なお本紙では，不正プレイヤーが正当プレイヤーと協力してなりすますことを協力的なりすましと呼ぶこととする．

プレイヤーが正当かどうかを検証するために個人認証という技術がある．しかしながら協力的なりすましにおいては，従来の認証手法で不正プレイヤーを検知することは難しい．従来の認証手法では，パスワードのように正当ユーザーのみが保持する情報を利用して認証を行うが，上述のような正当プレイヤーと不正プレイヤーが協力するケースにおいては，不正プレーヤーが容易に認証情報を入手できるからである．そこで我々は，協力的なりすましにおける不正プレイヤーを検知するために，ゲームログデータを活用した新たな認証手法を提案する．ゲームプレイに関係のないデータを認証情報とするのではなく，実際にプレイしている内容が正当プレイヤーによるものがどうかを検証することで，不正プレイヤーを検知するのである．

本紙で提案する手法は，ゲームログデータとしてゲーム内におけるプライヤーが操作するキャラクターの位置情報を活用したものである．ゲーム内という仮想空間ではなく，現実空間における人の位置情報を活用した個人認証手法に関する研究 [2] は存在する．この既存手法では人の移動履歴情報からその人のライフスタイルにおける特徴を抽出し，その特徴から個人性を見出し認証に活用している．この手法をゲームログデータの位置情報に適用することで，プレイヤーのプレイスタイルを見出し認証に活用することを目的とする．なお本手法の検証のために，“Counter-Strike: Global Offensive” (CS:GO) [3] のデータを利用した．

1.1 本紙の構成

本紙の構成は以下の通りである．2 章では，本研究の関連研究について述べる．3 章では，本研究のデータセットの対象とした CS:GO について概要を記述する．4 章では，人の位置情報を活用した既存認証手法について説明し，その後本研究で採用した手法について説明する．5 章では，本研究で実施した実験について説明する．まず実験に使用したデータセットについて述べ，その後に実施した実験シナリオとその結果について説明する．そして実験結果から得られる考察について述べる．最後に 6 章で，本紙の結論を述べてまとめとする．

2. 関連研究

ゲームログデータを活用した認証手法に関する既存の研究については十分ではな．Nair et al. [4] は「Beat Saber」というゲームのプレイ情報から個人が特定されるという研究結果を発表している．しかしながらこの研究では，キャラクターのログデータが活用されているのではなく，プレーヤーの両手と頭部に搭載されたモーションセンサーでプレーヤーの行動データを取得し，そのデータを活用したものである．すなわち従来の腕の振り等の行動を活用した認証手法の類似であり，ゲームログデータを使用したものではない．

3. CS:GO

本章では本研究で採用した “Counter-Strike: Global Offensive” (CS:GO) についての概要を説明する．CS:GO は *Valve Corporation* と *Hidden Path Entertainment* によって開発されたマルチプレーヤーによるファーストパーソン・シューティングゲーム (FPS) である．5 人対 5 人のチームで構成され，一方が「テロリスト (T)」チーム，もう一方が「対テロリスト (CT)」チームとなって対戦する．テロリストチームは爆弾を設置したり人質を捕らえることを目的とし，対テロリストチームは爆弾を解除したり人質を救出することを目的とする．また両チームとも相手チームを全滅させることで目的達成とすることも可能である．

対戦の舞台となるマップは複数用意されており，それぞれのマップによって異なる戦術や戦略が必要となる．また対戦はラウンド制となっており，最大 30 ラウンドが行われる．その中で先に 16 ラウンド勝利したチームが勝利となる．各ラウンドでは約 2 分の制限時間があり，ラウンド内で倒されたプレーヤーは次のラウンドが開始するまで復活することはできない．ラウンドごとにチームは交代し，テロリストチームは対テロリストチームに切り替わり，またその逆も行われる．

CS:GO は e スポーツとしても人気が高く，多くの国際大会が開催されている．これらの大会にはプロチームが参加し，賞金をかけて競い合っている．メジャーな大会では *Valve Corporation* のサポートや共同スポンサーシップがあり，賞金額も大きくなっている．過去には賞金総額が 1,000,000 ドルにもなる ELEAGUE Major: Boston 2018 が開催された [5]．このように CS:GO は e スポーツとして

人気があり，賞金額が大きな大会が開催されていることから協力的なりすましの被害を受ける恐れがあるタイトルである．そのため本研究の目的として適切なタイトルであると考えらえ，手法の検証とためにそのデータを活用した．

4. 提案手法

本研究は位置情報を活用した認証手法 [2] を，CS:GO 内におけるプレイヤーが操作するキャラクターの位置情報に適用することで，プレイヤーを認証できるかを検証するものである．この章では，既存認証手法について概要を説明し，CS:GO 内における位置情報に適用するために変更した処理について記述する．

4.1 既存手法の概要

図 1 は位置情報を活用した認証手法の概要を表したものである．この手法は大きく登録フェーズ (Enrollment Phase) と検証フェーズ (Verification Phase) の 2 つのフェーズからなっている．登録フェーズでは，個人の特性を表した情報であるテンプレート (Template) が作成され登録される．検証フェーズでは，事前に登録されたテンプレートと認証情報 (Authentication Information) を比較することで類似性スコア (Similarity Score) が算出される．算出された類似性スコアの値によって認証結果が決定される．すなわち，類似性スコアが与えられた閾値よりも大きい場合は認証結果が受容となり，そうでない場合は拒否となる．

ここで使用されるテンプレートや認証情報は，GPS 等のセンサーによって収集された位置情報から作成される．ただし収集された位置情報 (collect data) がそのまま使われるのではなく，事前に前処理を施されることによってフォーマットされた情報 (format data) を元にして作成される．[2] によれば，位置情報を活用した認証手法は人の生活における行動パターンの習慣性を利用した認証手法であり，その行動習慣にはゆらぎが存在する．生活習慣は 1 日単位の周期性を持っており [6]，毎日反復される行動パターンを認証に利用するが，この行動パターンは毎日同じ時間に同じ行動をとるというわけではない．人はパターン化された行動をとっていたとしても，時間のずれなどが生じるのである．このずれを行動習慣のゆらぎと呼び，位置情報を活用した認証手法では前処理を施すことで，ゆらぎを吸収できるようなデータ形式に変換しているのである．

行動習慣のゆらぎは，時間のゆらぎと位置のゆらぎに分けることができる．毎日同じ電車に乗るなど行動パターンが決まっていたとしても，電車の遅延等で必ず同じ時間に電車に乗るとは限らず，時間がずれることもある．これが時間のゆらぎの例である．また，日によっては同じ電車でも違う車両に乗ることも想定される．これが位置のゆらぎの例である．これらのゆらぎを吸収するための処理として，それぞれの情報を丸めている．すなわち時間情報に対

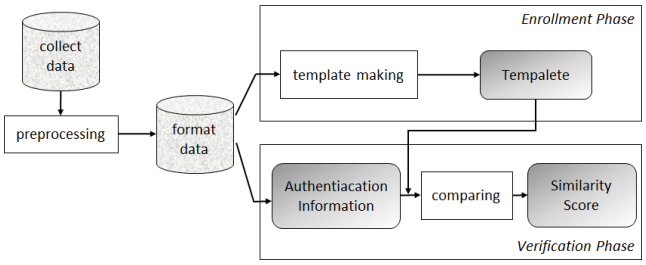

図 1 位置情報を活用した認証手法概要 [2]

しては，分秒の情報を削除して 1 時間単位に丸めており，また位置情報に対しては，緯度経度情報を約 1km 四方のメッシュコードに変換している．

4.2 本手法における前処理

前節で，位置情報を活用した認証手法の概要について説明したが，本研究では CS:GO 内におけるプレイヤーが操作するキャラクターの位置情報に対してその認証手法を適用する．そのためにはデータ形式，すなわち図 1 の “format data” の形式を合わせる必要があり，前処理部分は本研究独自の処理を行う必要がある．本節ではその前処理について説明を行う．

4.2.1 データ形式

まず，CS:GO 内におけるキャラクターの位置情報がどのように表されるかについて説明する．3 章で記述した通り，CS:GO は 2 チームによる対戦ゲームである．この 1 つの対戦のことをデモと呼ぶ．デモごとにマップは設定され，そのマップ上で対戦が行われる．1 回のデモは最大で 30 のラウンドからなり，プレイヤーはラウンドことにテロリストチームと対テロリストチームのサイドを切り替えながら対戦する．1 ラウンドは最大で約 2 分からなり，このラウンドごとに 2fps(フレームレート) でキャラクターの位置情報を取得している．キャラクターの位置情報は，マップごとの (x, y, z) 座標からなる．以上のデータ形式を表すと，表 1 となる．

表 1 CS:GO におけるキャラクター位置情報のデータ形式

項目	説明
デモ	1 回の対戦
マップ	
ラウンド	最大 30 回の繰り返し
サイド	‘T’ or ‘CT’
フレーム	2fps ごとに繰り返し
時間	ラウンド開始からの時間
位置	時間での (x, y, z) 座標

この位置情報を本紙では次のとおり表すこととする．すなわち，キャラクター c のマップ m，ラウンド r における時間 t での位置 l を，

$$l = L_c(m, r, t)$$

と表す．

4.2.2 時間のゆらぎ吸収処理

既存の認証手法 [2] では，時間のゆらぎ吸収処理では 1 時間単位に丸め処理を実施しており，1 時間ごとに最も長い時間滞在した場所をその時間の位置としていた．つまり 1 日で見ると，0 ～ 23 時それぞれ 1 時間ごとに位置が設定されるように処理が行われた．本研究では同様の形式となるようにするため，1 ラウンドの行動を 1 日の行動と同等だとみなし，1 ラウンドの時間を 24 分割してそれぞれに位置を設定するようにした．これは人の行動パターンが 1 日単位の周期性を持つように，CS:GO においてのプレースタイルが 1 ラウンドの周期性を持つのではないかと推測されることによる．

この処理を式で表すと次のとおりである．ラウンド r の終了時間を T_r $(\geq t)$ とし，$\frac{nT_c}{24} \leq t < \frac{(n+1)T_c}{24}$ $(n \in \{n \in \mathbb{Z} \mid 0 \leq n \leq 23\})$ を満たす時間 t において最も長い時間滞在した位置を l_n とすると，

$$l_n = L_c(m, r, n)$$

となる．

4.2.3 位置のゆらぎ吸収処理

既存手法における位置のゆらぎ吸収処理では，緯度経度情報をメッシュコードに変換することによって，位置情報の丸めを行っている．本研究でも同様に，ピンポイントの位置を広さのあるエリアに変換することによって丸め処理を行うが，その変換には既に用意されている Awpy [7] を使用した．Awpy は python で稼働する，CS:GO のデータを対象とした分析や可視化のためのライブラリである．Awpy を利用することで，マップと (x, y, z) 座標の情報から対象となるエリアの ID を取得することができる．

4.3 その他の相違点

前節で既存の位置情報を活用した認証手法と，本研究での手法との異なる点として前処理を挙げて説明した．前処理で得られたデータをその後に処理に適用させることで，既存手法と同様に認証をすることが可能だが，注意すべき点がある．本研究でのプレーヤーを認証する手法は，プレースタイルが反復されるであろうことを活用したものだが，CS:GO のゲーム特性上，すべてのラウンドでプレースタイルが反復されることは期待できない．プレーヤーは，デモを行う舞台となるマップと，テロリストか対テロリストかといったチームサイドとでプレースタイルが変わることが推測される．そこで本研究では単純にラウンドごとに認証を実施するのではなく，設定されたマップとサイドの情報もキーとして認証することとする．すなわちキャラクタ c，マップ m，サイド s としてテンプレートは $T_{(c,m,s)}$ で表すことができる．またキャラクター c におけるマップ m_1，ラウンド r_1 の情報と比較するためのテンプレートは $T_{(x,m_1,s_1)}$ でなければならない．ただしここで x は任意のキャラクターであり，c のラウンド r_1 におけるサイドは s_1 である．

5. 実験

この章では本研究で実施した実験について記述する．

5.1 データセット

まずは本実験で使用したデータセットについて説明する．本実験で使用した CS:GO のデータセットは ESTA と呼ばれるオープンデータであり，web から誰でもダウンロードすることが可能である [7]．このデータセットには以下の特徴が含まれている．

- プレイヤーの行動 (ダメージ、キル、手榴弾の投擲、爆弾の設置/解除、フラッシュ、および武器の発砲) に関する時空間データ

- ゲーム内で 1 秒あたり 2 フレーム、すなわち 2 Hz で解析されたフレーム

また ESTA データセットは，Online と LAN のサブセットから構成されている．Online には 2021 年 1 月から 2022 年 5 月までの主要なオンライン大会からの 878 のデモが含まれており，LAN には 2021 年 7 月から 2022 年 5 月までの主要なオンサイト大会からの 680 のデモが含まれている．表 2 はそれぞれのデータ量を表したものである．なおプレーヤーについては Online と LAN のサブセットで重複しているものもあるため，合計がそれぞれの単純な和とはなっていない．

表 2 ESTA のデータサイズ

	Demo	Round	Action	Frame	Size	Player
Online	878	23,444	4.7M	4.4M	2.2G	339
LAN	680	18,338	3.9M	3.5M	1.7G	250
Total	1,558	41,782	8.6M	7.9M	3.9G	394

本研究の実験ではこのデータセットの中で，LAN のサブセットでかつ，ラウンド数が 200 以上のプレイヤー，マップ，サイドの組み合わせのデータを使用した．本研究はまったくの新しい試みであり，ファーストステップとして全データで検証するのではなく，まずは一部のデータを用いて検証するといった意図である．使用したデータはプレイヤー，マップ，サイドの組み合わせの数が 130，およびラウンドの合計が 32,539 であった．プレイヤー，マップを個別にみると，プレイヤー数が 40 であり，マップ数が 7 であった．サイドは既述の通り，T と CT の 2 通りである．

5.2 実験シナリオ

本節では本研究で実施した実験シナリオについて説明

する．

5.2.1　テンプレート作成ラウンド数の決定

4 章で既述した通り，本手法はまず登録フェーズで個人の特性を表した情報であるテンプレートを作成する．このテンプレートはフォーマットされたデータを元に作成されるが，どれだけの量のデータから作成されるかは決定されていない．既存研究ではテンプレート作成期間として 30 日間のデータを元に作成されていたが，本手法でも同様の期間，すなわち 30 ラウンドのデータがテンプレート作成に適切かは明らかではない．そこでまずは，テンプレート作成に必要なラウンド数を決定する．ラウンド数を 10 ～ 100 と 10 ラウンドごとに変化させて，テンプレート作成に最も適切なラウンド数を決定する．検証には残りのラウンドのデータを使用する．例えば 200 ラウンドのデータがあり，50 ラウンドのデータをテンプレート作成に使用するとした場合，最初の 50 ラウンドのデータでテンプレートを作成し，残りの 150 ラウンドのデータで検証を行う．既述の通りラウンドごとに認証を実施するため，この例では 150 回の認証テストが実施される．検証の評価指標については EER を採用するが，これについては後述する．

5.2.2　キーごとの特徴

4.3 節で既述した通り，本手法ではテンプレートはキャラクター，マップ，サイドをキーとして作成され，認証テストのための比較処理もマップ，サイドが同一のものを対象としている．そこで次のシナリオとして，キーごとに認証結果を整理した場合に，どのような特徴が見られるかを検証する．

5.2.3　評価指標

本実験での評価指標については FRR(False Rejection Rate) と FAR(False Acceptance Rate) を採用した．それぞれの定義については以下の通りである．ここで本人テストとはテンプレートと同じユーザーのデータを認証情報としたテストであり，他人テストとはテンプレートと異なるユーザーのデータを認証情報としたテストである．

$$FRR := \frac{\text{認証失敗回数}}{\text{本人テスト回数}}$$
$$FAR := \frac{\text{認証成功回数}}{\text{他人テスト回数}}$$

また EER(Equal Error Rate) についても評価指標として用いる．FRR と FAR はトレードオフの関係にあり，セキュリティパラメータ k を変化させることで一方を改善させるともう一方が悪化することになる．そこで $FRR = FAR$ となる k を算出し，そこでの値を EER と定義する．すなわち，

$$EER := FRR \quad where\ k = k_1$$
ただし, $FRR = FAR \quad where\ k = k_1$

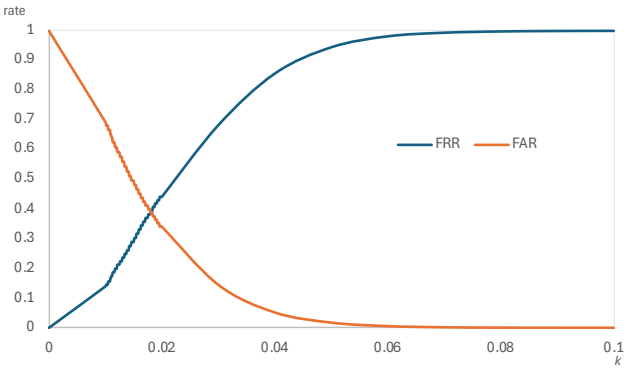

図 2　テンプレート作成ラウンド回数が 100 の時の FRR と FAR

5.3　実験結果

前節で述べた実験シナリオを実施した結果について本節にて説明する．

5.3.1　テンプレート作成ラウンド数の決定

表 3 はテンプレート作成ラウンドごとの EER を表している．ラウンド数が 20 を超えると，テンプレート作成ラウンドが増加するに従って EER は減少していることがわかる．一方でラウンド数が 60 を超えたあたりから EER は減少はしているが，それほど変化しておらず収束傾向にあることもわかる．そこで本実験ではテンプレート作成ラウンドをこれ以上増加させず，EER が最も低い値であった，ラウンド数 100 を採用することとした．

表 3　テンプレート作成ラウンドごとの EER

ラウンド数	10	20	30	40	50
EER	0.413	0.423	0.409	0.403	0.402

ラウンド数	60	70	80	90	100
EER	0.397	0.396	0.395	0.395	0.391

テンプレート作成ラウンド回数が 100 の時の，セキュリティパラメータ k を変化させた場合の FRR と FAR の挙動は図 2 である．この EER を得た時，つまり図 2 の FRR と FAR が交差している箇所のセキュリティパラメータは $k = 0.180$ であり，この後の実験についてはこの k の値も採用した．

また図 3，4 は FRR と FAR それぞれのヒストグラムである．

5.3.2　キーごとの特徴

本節ではプレイヤー，マップ，サイドごとの認証結果について見ていく．図 5 はプレイヤーごとの認証結果を FRR と FAR で表したものである．本実験で使用したデータに含まれているプレイヤー数は 40 名である．

また図 6 はマップごとの認証結果を FRR と FAR で表したものである．本実験で使用したデータに含まれているマップは 7 つであった．一部のマップについて FAR が 0 となっているが，これは認証結果が 0 ではなく，マップと

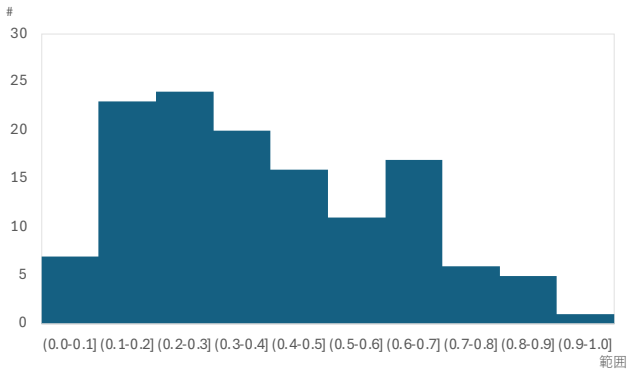

図 3　FRR のヒストグラム

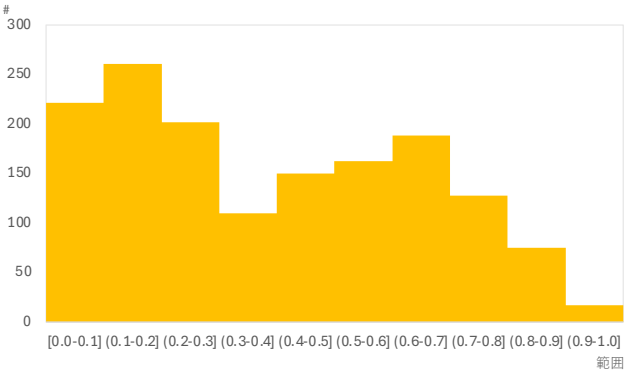

図 4　FAR のヒストグラム

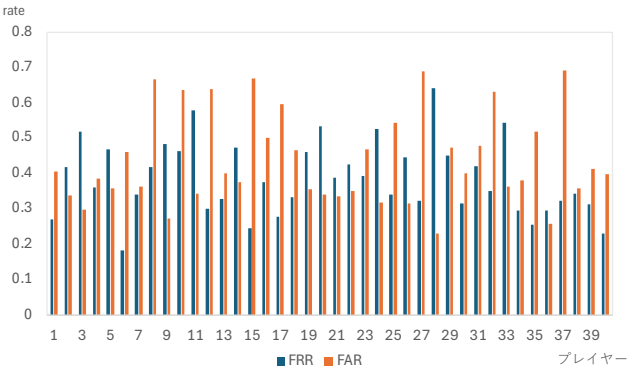

図 5　プレイヤーごとの FRR,FAR

サイドが同じで他人のデータがこのマップにおいては存在しなかったため，FAR が算出できなかったことが理由である．

また表 4 はサイドごとの認証結果を FRR と FAR で表したものである．サイドについては既述の通り，テロリストチームと対テロリストチームの 2 通りである．

表 4　サイドごとの FRR,FAR

サイド	FRR	FAR
T	0.398	0.447
CT	0.389	0.327

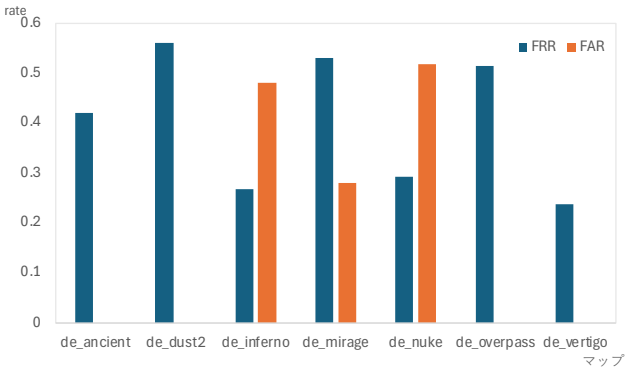

図 6　マップごとの FRR,FAR

5.4　考察

本実験では，$EER = 0.391$ と十分な結果を得ることはできなかった．物理空間における人の位置情報を活用した個人認証手法を，サイバー空間，すなわちゲーム内のキャラクターの位置情報に適用させることで，人と同様にキャラクターを認証するということは実現できたとは言えない．ただしこの結果がそのままゲームのログデータを用いてキャラクターを認証することができないと，結論づけることもまたできないと考えている．5.1 節で記述した通り，本データセットにはキャラクターの行動に関して非常に多くの特徴量が含まれている．一方で本研究で採用したのはそのうちの一部である，位置とマップ，サイドの情報のみである．特徴量を増やすことで認証精度を向上させ，ゲームログでキャラクターの認証を実施することを期待することができる．

本実験の結果を細かく見ると，図 3,4 からエラー率は一定ではないが，低い値となっているデータも存在していることがわかる．エラー率が低くなることに寄与する情報を捉えることが今後重要である．

図 6 からは，de_mirage と de_inferno, de_nuke の FRR と FAR の傾向が逆になっていることがわかる．de_mirage では FRR が大きく FAR が小さい値となっているが，de_inferno と de_nuke では逆に FRR が小さく，FAR が大きい値となっている．この結果から，de_inferno と de_nuke では誰もが似たようなプレースタイルを取るため，認証成功する確率が高くなり，一方で de_mirage では本人でも似たようなプレースタイルを取ることができず認証失敗する確率が高くなることが推測できる．

表 4 からは，サイドによって FRR はそれほど変化しないが，FAR は大きく異なっていることがわかる．この結果から，テロリストチームでのプレースタイルはプレイヤーによって差異は大きくないが，対テロリストチームでのプレースタイルは，プレイヤーによって差異が大きくなるということが推測できる．

6. おわりに

本紙で我々は，近年普及が拡大してきているｅスポーツにおいて，協力的なりすましによる被害の可能性を指摘した．従来の認証手法では協力的なりすましを検知することは難しく，被害を防ぐためには新たな認証手法が必要である．そこで我々はｅスポーツのログデータを活用した認証手法が，協力的なりすましに有効である主張した．ｅスポーツのログデータを活用した認証手法としては，人の位置情報を活用した既存認証手法を，ｅスポーツ内でのプレイヤーが操作するキャラクターの位置情報に適用する手法を提案した．実験結果としては EER=0.391 と十分はものではなかったが，今後改善の余地があることを本紙で指摘した．

本研究ではｅスポーツのログデータのうち，一部の特徴量のみを認証に使用したが，特徴量を増やすことで認証精度を改善させることが期待できる．今後の課題としては，人の位置情報を活用するといった既存手法を適用するのではなく，対象となるログデータに適切な手法を見つけることが重要である．特徴量を増やすことはその一つの課題となるであろう．

謝辞　本研究は，JST ムーンショット型研究開発事業，JPMJMS2215 の支援を受けたものです．

参考文献

[1] 一般社団法人日本ｅスポーツ連合：ｅスポーツとは，入手先 ⟨https://jesu.or.jp/contents/about_esports/⟩ (2024.08.15).

[2] 小林良輔 and 山口利恵：位置情報を活用した認証手法における認証精度と検知時間との関係，2022 年暗号と情報セキュリティシンポジウム (SCIS), 2022.

[3] M Nazhif Rizani and Hiroyuki Iida: *Analysis of Counter-Strike: Global Offensive*, 2018 international conference on electrical engineering and computer science (ICECOS), IEEE, pp.373–378, 2018.

[4] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F. O'Brien, Louis Rosenberg and Dawn Song: *Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, pp.895–910, 2023.

[5] Counter-Strike: Global Offensive ：Blog, 入手先 ⟨https://blog.counter-strike.net/⟩ (2024.08.21).

[6] 大橋久美子：看護における「生活リズム」：概念分析，聖路加看護学会誌, vol.14, pp.1–9, 2010.

[7] Peter Xenopoulos and Claudio Silva: *ESTA: An Esports Trajectory and Action Dataset*, arXiv preprint arXiv:2209.09861, 2022.