個人情報保護意識の向上を目的とした対戦型シリアスゲームの開発：人対人、人対 ChatGPT による学習効果の比較

小久保凜[†1]　大和田光紀[†1]　浜田敦[†1]　飯尾淳[†1]

概要：本研究では，個人情報保護意識の向上を目的としたシリアスゲームの開発に取り組んでいる．このゲームは対戦形式のオンラインカードゲームであり，二つの形式が存在する：一つは人対人，もう一つは人対 ChatGPT である．本論文では，ゲームの設計と概要，実施した実験の詳細，そして得られた実験データの分析結果をまとめ，ChatGPT との対戦を組み込んだシリアスゲームが個人情報保護意識向上にどのような効果をもたらすのか考察した．

1. はじめに

近年, LLM をはじめとした人工知能の進化と普及に伴い, ChatGPT のようなデジタルアシスタントが日常生活や業務の中で頻繁に利用されるようになってきた．これらの技術は情報検索からエンターテインメントまで幅広い用途で活用されており，社会に広く浸透しつつある．しかしその一方で，デジタル空間における個人情報の取り扱いやプライバシーに関する課題も増加している．特に，デジタル技術の日常化に伴い，個人情報を適切に保護するリテラシーが求められるようになってきた．個人情報保護やデータセキュリティに関する意識やリテラシーの向上は，現代の情報社会において極めて重要なテーマとなっている．しかし，従来の教育方法では，特に若年層を中心にこれらの意識を持続的に育成することが難しく，新しい教育手法が求められている．

こうした背景を踏まえ，本研究では，個人情報保護意識の向上を目的としたシリアスゲームの開発に取り組んだ．このゲームは対戦形式のオンラインカードゲームとして設計され，プレイヤー同士の対戦だけでなく，プレイヤーと ChatGPT の対戦を可能とすることで，個人情報保護に関する意識や知識の獲得を促すことを目指している．本論文では，そのゲームの開発過程，実施した実験，および実験結果の分析を通して，新たな教育手法の可能性と，ChatGPT がもたらす教育効果について考察する．

2. 研究の目的

本研究の主要な目的は，シリアスゲームを用いたリテラシー教育の，教育手法としての有効性を評価することにある. 特に, ゲーム内での対戦形式「人対人」と「人対 ChatGPT」の２つに関して，それぞれが個人情報保護意識の育成や学習への意欲にどのように影響するかに焦点を置いて分析を行った．この二つの対戦形式を比較することで，人と AI とのインタラクションが教育面でどのような効果や受容性を持つのか，そしてその特性をどのように活用すればよいのかについての新しい視点を提供する．

また，本研究は実際の実験データを基に，これらの対戦形式がプレイヤーの意識や行動に与える影響を考察している．特に，プレイヤーがゲーム内の ChatGPT との対話において，個人情報保護に関してどのようなトピックを話し合っているのかという分析は，今後のシリアスゲームの設計や教育プログラムの開発にも活用できると考える．

3. 関連研究

シリアスゲームを用いてネット上でのリテラシー教育を行なった研究として，Calvo-Morata らの取り組み[1]が挙げられる．この研究では，デジタル空間でのいじめに対するリテラシー教育を行うため，クラスルーム用のシリアスゲーム「Conectado」を導入し，没入感のあるゲームプレイを通じて被害者に対する共感を促進した．また，Hart [2]は，サイバーセキュリティ意識を高めるためのテーブルトップゲーム「Riskio」を提案している．このゲームでもロールプレイイング形式を導入しており，プレイヤーが攻撃者と防御者の両方の役割を果たすことで，サイバーセキュリティ攻撃と防御に関する知識を身につけることができるとしている．さらに Krath ら[3]は，シリアスゲームなどゲームベースの学習に関する研究を調査し, 共通点をまとめている．それによると，シリアスゲームは学習ガイドとしてユーザを誘導する，ユーザに即時のフィードバックを提供する，ユーザ同士をつなげて互いにサポートさせ合うといった機能を持っている．

また，個人のプライバシー意識については，大磯一らの研究[4]で報告されている．この研究では，デジタルサービスの採用に関して，リスク感覚，利便性，主観的な利用率などを重要な要因として挙げており，消費者の信頼を高めるためにトラブルの事例とその対応に関する情報を提供することを提案している．さらに，SNS 上での他人の個人情報の公開について，太幡直也ら[5]は，SNS 利用者の情報リ

†1 中央大学 国際情報学部 国際情報学科

テラシー教育の重要性を強調しており， SNS 上での他者のプライバシー侵害への懸念を高めることが不適切な他者情報公開を抑止する方策として効果的であると提案している．

これらの関連研究から，シリアスゲームを用いたリテラシー教育の有効性や，SNS をはじめとしたデジタルサービスの利用率が高まる現代において，個人情報保護に関するリテラシー教育の重要性が伺える．

4. ゲームの概要

4.1 開発の趣旨

本研究で開発されたシリアスゲームは，ロールプレイイング形式を採用している．この形式を通じて，プレイヤーは個人情報に関する問題をより直接的に，自分ごととして体験することができる．また，ゲーム内での他者との対話を通じて，プレイヤーは自らがどのような情報をプライベートと感じているのか，あるいはどのような情報を他人と共有しても問題ないと感じているのかを自覚する機会を得る．さらに，ゲームの進行を通じて，人々の個人情報に対する認識や価値観は異なることを学ぶ．この結果，プレイヤーは自らの個人情報だけでなく，他者の情報に対する取り扱いにもより注意深くなることが期待される．

4.2 ゲーム上の役割

本研究で開発されたゲームでは,「個人情報悪用側」と「個人情報提供側」という二つの主要な役割が設定されている．これらの役割に分かれ，1 対 1 の対戦形式で進行する．

個人情報悪用側は攻撃的な立場をとり，悪用カード（例: 空き巣，スパムメール，結婚詐欺）の内容に基づいて相手の個人情報を悪用しようとする役割となる．悪用カードの内容は，実際に個人情報が悪用された犯罪例などを元に設定した．悪用カードは全部で 19 種類である。

一方，個人情報提供側は守備的な立場をとり，所持する個人情報カード（例: 位置情報，電話番号，交友関係）を選択して，悪用側からの攻撃を防ごうとする．個人情報カードの内容は，内閣が実施した世論調査[6]の他人に知られたくない個人情報という設問で，個人情報として設定されている項目を参照した．個人情報カードは全部で 16 種類である．

また，人対人の対戦の場合，どちらの役割もプレイヤーが担当するが，人対 ChatGPT の対戦形式では，ChatGPT が個人情報悪用側の役割を担当する．このゲーム設計の狙いは,個人情報を守る側だけでなく,攻撃側の体験を通じて，個人情報を悪用する側の思考や戦略に対する理解を深めることにある．これにより，プレイヤーの個人情報に対する保護意識の向上が期待される．

4.3 ゲームの進行

ゲームは図 1 のフローチャートに沿って進行する．ゲーム上で各番号に対応する画面を表示し，ユーザの操作によって遷移する．

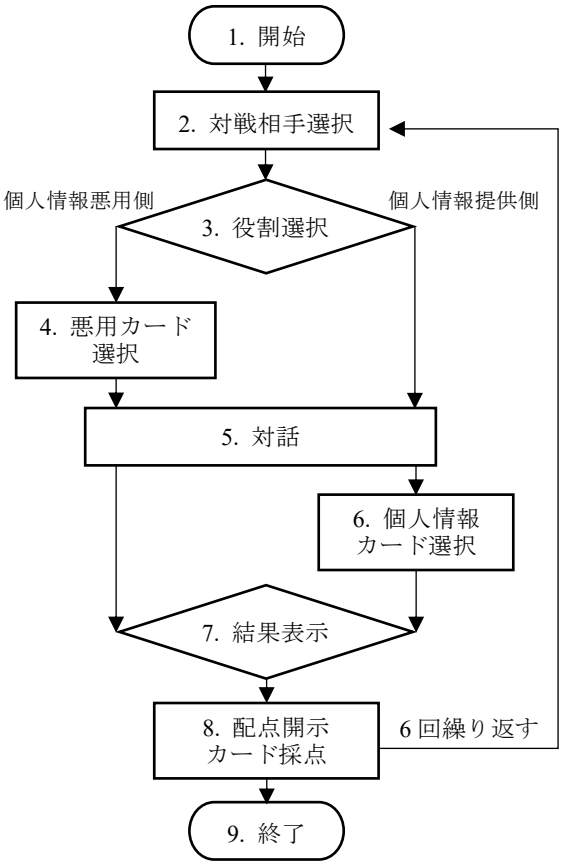

図 1　フローチャート

フローチャート内の各項目の詳細については，下記の通りである．

(1) 開始

ユーザ登録もしくはログインを行い, ゲームを開始する．実験時には，あらかじめ用意しておいた実験用アカウントでログインしてもらう．

(2) 対戦相手選択

対戦相手の選択を行う．実験時，人対人の場合は，あらかじめ指定した対戦相手を選択してもらう．ChatGPT 対戦の場合は対戦相手選択画面を表示させず，自動的に対戦相手を登録する．

(3) 役割選択

個人情報悪用側と個人情報提供側のどちらかの役割を選択する．ChatGPT 対戦の場合はこの画面をスキップし，ユーザを個人情報提供側として登録する．

(4) 悪用カード選択

個人情報悪用側に 3 枚の悪用カードを提示し，その中からゲーム内で実行する悪用カードを 1 枚選択してもらう．このとき，悪用側が選択したカードの内容は提供側には提示せず，どのような悪用方法を実行しようとしているのか提供側に推測させるようデザインしている．また，悪用側が選択したカードの内容に紐づいて，表 1 のようにカードの配点が決定する．カードの得点は，合計 100 点になるよう研究チームで話し合い，配点を決めた．その初期設定に

対して，ユーザからゲーム内で自分の考える最適な得点配分を 100 点満点で回答してもらい，そのフィードバックを集計して，その後のゲームに反映させている．カードの内容と配点の一覧は付録に掲載している．

表 1　カードの配点例

個人情報カード	ストーカー	空き巣	結婚詐欺
性別	20	0	30
位置情報	35	20	0
住所	30	40	5
年収	5	40	50
顔写真	10	0	15

(5)　対話

悪用側・提供側両方に個人情報カードを 5 枚表示し，5 枚の中で他人に知られても良いカードを 3 枚選択するため，対話を行う．選択した 3 枚は悪用側に渡され，カードの合計が悪用側の得点となる．渡さなかった 2 枚のカードの合計が提供側の得点となる．各カードの点数は表示されないため，どちらの役割も予想しながらゲームを進める．

悪用側は，どの個人情報カードを受け取れば自分が選択した悪用カードの内容を実行できるか考えながら対話を行う．提供側は，悪用側が個人情報カードをどのように悪用しようとしているか推測しながら対話を行う．人対人の場合は直接的なコミュニケーションで対話を行い，人対 ChatGPT の場合はチャット形式で対話を行う．対話の目安として，5 分間の制限時間を設けている．

また，ChatGPT は個人情報を保持せず，プライバシー意識を持たないこと，プレイヤーの個人情報保護意識の向上がゲームの目的であることを踏まえ，ChatGPT 対戦の際はプレイヤーの役割を提供側に固定している．

(6)　個人情報カード選択

悪用側との対話の内容を参考に，5 枚の中で他人に知られても良いと感じるカードを 3 枚選択する．

(7)　結果表示

悪用側・提供側が選択したカードの内容を元に得点を計算し，勝敗結果を表示する．また，実際に発生している個人情報を悪用した犯罪や，個人情報保護の対策例などを紹介し，ゲームの結果とともに，現実の事例への興味を促す．

(8)　配点開示・カード採点

悪用側が選択したカードの内容と，各個人情報カードの配点を開示する．また，自身であれば各カードにどのような点数をつけるか採点してもらい，その結果を収集する．

(9)　終了

実験時にはこの行程を 6 回繰り返し，全ての結果が得られたらゲームを終了する．

5.　システム・UI について

ゲームのシステム構成は，図 2 の通りである．

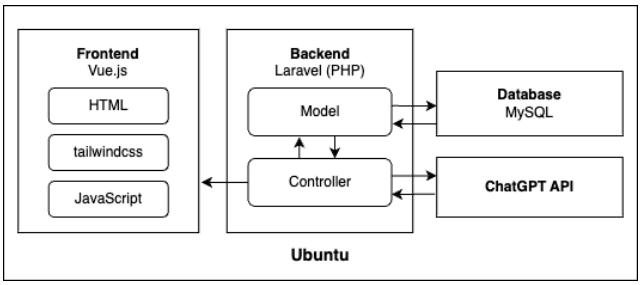

図 2　システム構成図

バックエンドは，PHP のフレームワークである Laravel を使用してシステムを管理している．フロントエンドはモダンなデザインにするため，Vue.js のフレームワークを使用している．また， ChatGPT API のモデルは gpt-3.5-turbo である．ChatGPT のチャットの制御はプロンプトベースで行い，ゲームのルールや所持しているカードの情報，どのような方向性で対話を行うかなどの指示を与えている．

ゲームの UI はシンプルにすることを心がけた．また，役割ごとにイメージカラーを設定し，自分がどちらの役割を担っているか可視化した．図 3 は ChatGPT 対戦の場合の，対話画面のスクリーンショットである．

図 3　ChatGPT との対話画面

また，悪用カード・個人情報カードそれぞれにイラストを設定するなど，内容を理解しやすいデザインを心がけた．さらに，ユーザの操作性を向上させるため，スマートフォン版・P C 版それぞれのデザインを作成し，レスポンシブデザインとなるよう実装した．

6.　実験の詳細

開発したゲームシステムを用いて，中央大学・中央大学大学院の学生を対象に，表 2 のとおり実験を実施した．

表 2　実験概要

日付	参加人数	有効データ数	対戦形式
2022/07/04	12	24	対人(直接対話)
2022/12/12	24	69	対人(直接対話)
2023/07/10	30	180	対 ChatGPT
2023/12/06	30	179	対人(直接対話/チャット)・対 ChatGPT

ゲーム内では被験者の個人情報は収集せず，匿名でプレイデータおよび ChatGPT とのチャット内容を収集した．また，実験を開始する前に実験の概要と目的の説明を行い，実験同意書への署名を求めた．さらに，実験の前には個人情報保護に対する関心度やゲームリテラシーを測るアンケートを，実験後には個人情報に対する意識の変化やゲームに対するフィードバックを求めるアンケートを実施した．三度目の実験では ChatGPT との対戦を実装したことにより，データ収集効率が大幅に向上した．

また，過去の実験結果を踏まえ，より具体的な教育効果の比較を目的として，四度目の実験では人同士の直接対話，チャットでの対話，および ChatGPT との対話の 3 パターンでの実験をランダムに 2 回ずつ，全被験者に対して実施した．本論文では，四度目の実験のうち対人（チャット対話）データのみを「7.5 人対人のチャット分析」で分析対象として取り上げ，「7.4 ChatGPT とのチャット分析」で述べる分析結果と比較した．

7. 実験結果の分析

7.1 勝敗

人対人，人対 ChatGPT それぞれの勝敗結果は表 3 のとおりである．

表 3 対戦形式・役割別の勝敗結果

	人対人		人対 ChatGPT	
役割	悪用側	提供側	悪用側	提供側
勝数	67	21	104	65
引き分け数	5		11	
勝率	72.0%	22.6%	57.8%	36.1%

表 3 から，対戦形式によらず，悪用側の方が勝ちやすいということがわかる．この勝敗の傾向は，ゲームデザインにおけるカードの選択メカニズムとも関係していると考えられる．合計得点が 100 点となるよう設計されたカードの中から 3 枚選択するというゲームのデザイン上，悪用側の得点の期待値 E[X]は 60 点となる．ChatGPT によるカード選択はランダムに行われるため，人対 ChatGPT の場合の悪用側の勝率（57.8%）は，期待値に近い結果であることがわかる．

また，対戦形式によって勝敗の分布に統計的な差が存在するかをカイ 2 乗検定によって検証した結果，カイ 2 乗統計量は 5.61，p 値は 0.0604 と計算され，自由度は 2 であった．得られた p 値が 0.05 を超えているため，人対人と人対 ChatGPT において，悪用側の勝率に統計的に有意な差があるとは言えない．

7.2 カードの選択

実験で使用した計 16 種類の各個人情報カードに対し，被験者がカードを相手に渡さなかった割合，すなわち，他人に知られたくないと感じた割合を個人情報重要度とし，図 4 のようにグラフで表した．

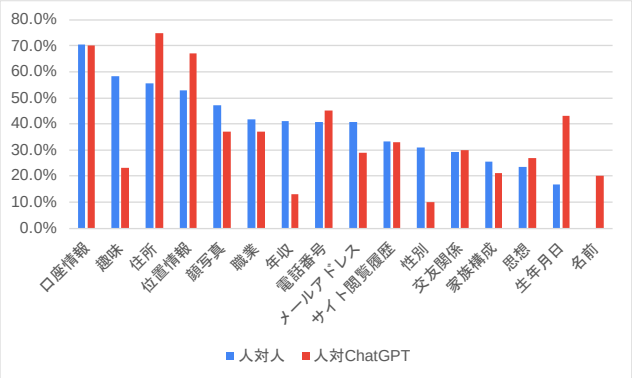

図 4 対戦形式別 個人情報重要度

この結果から，被験者が口座情報や住所などの情報を重視していること，逆に名前や家族構成などの情報を軽視していることが読み取れる．人対人と人対 ChatGPT で大きな変化はないように思われる．一番評価が分かれている個人情報は趣味であり，相手が人の場合には趣味は知られたくないと感じても，相手が ChatGPT≒機械であれば趣味を知られても問題ないと感じる人が多いのではないだろうか．

7.3 実験後アンケート

実験後にゲームの面白さと教育効果を測るため，アンケートを実施した．設問は，Q.1 またこのゲームを対戦したいか，Q.2 個人情報の漏洩について今後気を付けようと思ったか，Q.3 個人情報について以前より興味・関心をもったか，Q.4 個人情報と身近で起きる悪用について理解が深まったか，Q.5 今回のゲームが楽しかったかの 5 つで，それぞれの問いに対して 4 件法で回答を求めた．

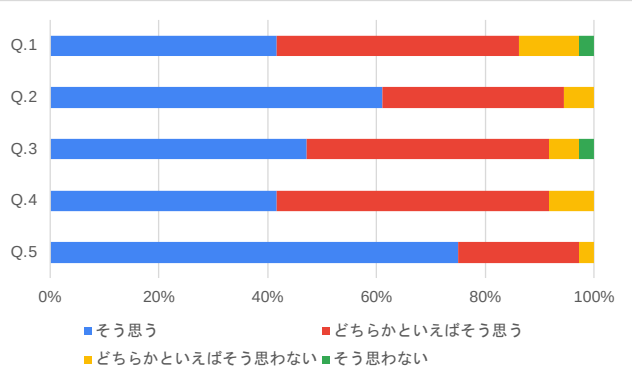

図 5 事後アンケート（人対人）

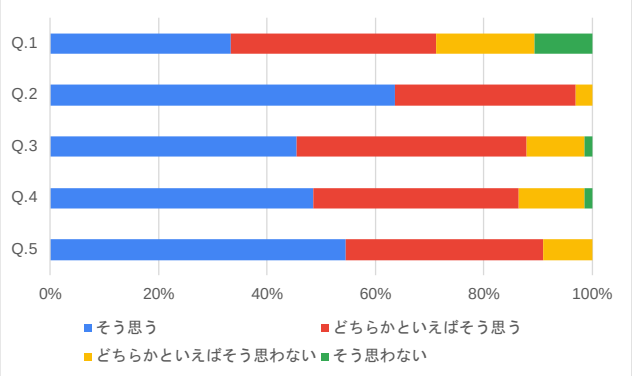

図 6 事後アンケート（人対 ChatGPT）

アンケート全体からわかる結果として，どの質問にも「そう思う・どちらかといえばそう思う」と回答した人の割合が高いことから，本ゲームのプレイ体験が被験者にとって興味深いものであり，ゲームの面白さやエンゲージメントが高いこと，個人情報保護意識を向上させるものであることが伺える．

また，図 5 と図 6 のアンケート結果に統計的な差異があるかどうかをフィッシャーの正確検定を用いて検証した．検証の際に，回答を「そう思う」「どちらかといえばそう思う」の肯定と，「どちらかといえばそう思わない」「そう思わない」の否定に分けて集計した．検定の結果，5 つの質問項目の中で「またこのゲームを対戦したい」と回答した項目のみが有意水準 0.05 で統計的に有意な差を示し（$p = 0.0057$），人同士の対戦が ChatGPT との対戦よりも好まれることが明らかになった．一方で，他の 4 つの質問項目については統計的に有意な差は見られなかった（$p > 0.05$）．

7.4 ChatGPT とのチャット分析

人対 ChatGPT の実験において，人と ChatGPT とのチャットデータを 2,399 件取得した．本節では，同データに対するテキスト分析の結果について説明する．また，2023 年 12 月 6 日の実験で，人同士のチャット対戦を実施し，チャットデータを 302 件取得した．そのデータに対してテキスト分析を行い，対戦相手の違いによるチャット内容の違いについて比較した結果は後述する．なお，ChatGPT 対戦時のチャットの開始は「あなたが 5 枚の個人情報カードの中で 1 番他人に知られたくないと感じるものはどれですか？」という ChatGPT 側からの定型質問で開始するため，開始時のチャットはデータに含めていない．これらのチャットデータに対して，キーワード・トピック・応答時間という異なる視点で分析を行った．

(1) キーワード分析

チャット内の単語の出現回数を表 4 にまとめた．

表 4　対 ChatGPT 頻出単語

単語	出現回数	単語	出現回数
情報	3,066	リスク	562
個人	1,696	アドレス	536
他人	1,547	意識	526
プライバシー	1,310	考え	515
カード	953	家族	497
電話	860	構成	399
性	814	あなた	358
住所	755	セキュリティ	338
重要	731	性別	337
番号	716	保護	335
メール	709	必要	310
抵抗	704	対し	309
他	665	対する	297
可能	643	公開	295
感じ	590	特定	285

個人情報やプライバシーに関する単語が頻出していることが表 4 から読み取れるため，こちらが期待していたような内容のやり取りが行われており，ChatGPT との対話の精度はかなり高いものであると言える．また，アドレスや電話番号，性別など，具体的な個人情報についても話し合われていることがわかる．

さらに，チャットの内容に対して単語の重要度を評価するための統計的手法である Tf-Idf 分析[7]を行い，単語の重要度を図 7 のとおり評価した．形態素解析ツールである MeCab [8]を使用して各メッセージをトークンに分割し，正規表現を用いて有効なトークンのみを選択した後，各単語の Tf-Idf スコアの平均を計算し、データセット内で最も重要度が高い単語を特定した．

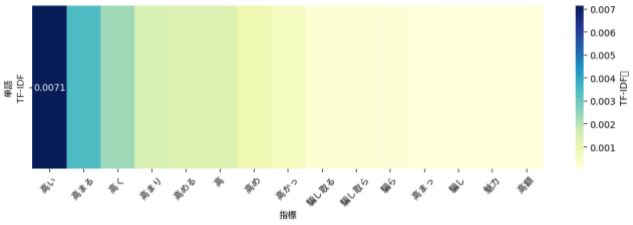

図 7　対 ChatGPT Tf-Idf 分析

Tf-Idf 分析の結果，「高い」「高まる」など，高さにまつわる単語と，「騙し取る」「騙し」などの騙すことにまつわる単語，「魅力」「高額」などが重要単語として特定された．この結果から，「高まる」「騙し取る」「魅力」など，自身が持つ個人情報のリスクや重要度，悪用手法などについて話し合われていることが推測できる．特に個人情報を悪用される際には「騙される」という意識が強いことがわかる．

(2) トピックモデリング

チャット内容のトピックモデリングを行い，対話の話題についてより深く分析した．Janome [9]の Tokenizer を使用して形態素解析を行い，その結果に対して独自に設定したストップワードを適用し，不要な単語や記号を除去した．前処理を行った後のデータから辞書とコーパスを作成し，Gensim というライブラリを利用して LDA (Latent Dirichlet Allocation）モデル[10]を構築した．トピックの数は 5 と設定し，モデルの学習を 15 回繰り返した．学習された LDA モデルから，表 5 のように各トピックの代表的なキーワードとその重要度を取得した．

表 5　対 ChatGPT トピックモデリング

Topic1	Topic2	Topic3	Topic4	Topic5
情報 (0.046)	他人 (0.059)	情報 (0.059)	情報 (0.077)	思想 (0.053)
性 (0.033)	電話 (0.049)	位置 (0.026)	個人 (0.043)	趣味 (0.017)
個人 (0.032)	カード (0.045)	犯罪 (0.025)	プライバシー (0.031)	関係 (0.017)
可能 (0.027)	情報 (0.041)	詐欺 (0.022)	重要 (0.025)	信念 (0.015)
性別 (0.024)	番号 (0.039)	職業 (0.021)	性 (0.017)	意見 (0.012)

リスク (0.022)	抵抗 (0.037)	口座 (0.020)	意識 (0.015)	個人 (0.011)
特定 (0.018)	感 (0.031)	行為 (0.018)	セキュリティ (0.015)	性 (0.010)
プライバシー (0.014)	住所 (0.030)	住所 (0.011)	保護 (0.014)	単体 (0.010)
名前 (0.014)	メールアドレス (0.023)	生年月日 (0.011)	他人 (0.013)	価値 (0.010)
公開 (0.014)	個人 (0.022)	あなた (0.009)	必要 (0.012)	可能 (0.009)
考え (0.014)	プライバシー (0.021)	趣味 (0.007)	対策 (0.012)	社会 (0.009)
家族 (0.012)	他 (0.018)	関連 (0.007)	他 (0.012)	公開 (0.009)
位置 (0.011)	家族 (0.016)	ゲーム (0.006)	慎重 (0.011)	友人 (0.008)
一般 (0.011)	構成 (0.014)	必要 (0.007)	可能 (0.010)	人々 (0.008)

Topic1 は，個人情報に関連したキーワードが含まれており，特に「リスク」や「特定」,「公開」などのキーワードから，個人情報の公開やそれに伴うリスクに関連する話題である可能性が高い．また，Topic2 はコミュニケーションや個人情報の交換，それに関連するセキュリティの問題を示唆している．特に「番号」や「メールアドレス」などの具体的な情報交換の手段に関する言及がある．Topic3 は「情報」「位置」「犯罪」などのキーワードが見られ，特に「詐欺」「口座」などの言葉から，犯罪や情報の取引・不正利用に関するトピックであることが考えられる．Topic4 は，セキュリティ」や「対策」などのキーワードが目立ち，プライバシーの保護やセキュリティに関する話題であることが示唆される．そして Topic5 は，「思想」「趣味」「関係」などのキーワードが含まれており，個人の信念や価値観，趣味や関心，人との関係性に関するトピックであると解釈される．このように，個人情報に関する話題の中でも，様々な切り口で対話が行われていることがわかる．

(3) 応答時間の比較

対話のテンポ感を測定するため，図 8 のとおり ChatGPT とユーザそれぞれのチャット受信後の応答時間を比較した．

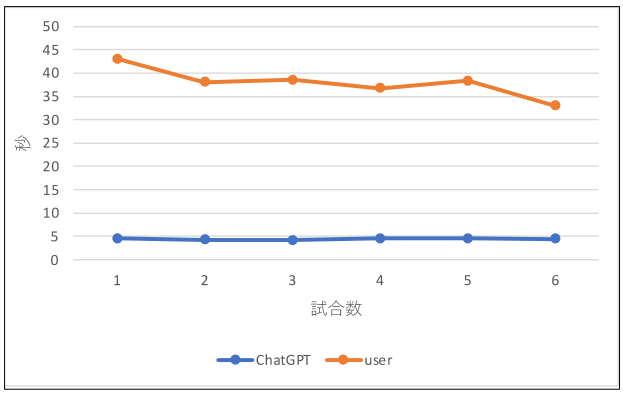

図 8　応答時間の比較

ユーザ全体の応答時間の平均は 33.6 秒、ChatGPT の平均は 4.4 秒であった．また，制限時間 5 分間の間でのチャット数の平均は 13.3 回であった．この結果から，ChatGPT のチャット出力は安定しているが，ユーザは応答するのに少し手間取っていたことがわかる．しかし，ユーザも試合回数を重ねるにつれ，少しずつ応答時間が短くなっていることが図 8 のグラフより読み取れる．この結果は，ChatGPT の応答文が長く読みづらかったため，回数を重ねるにつれて文章を読み飛ばしていたことが要因である可能性も考えられる．今後はユーザの応答時間をより短縮するため，チャット画面の UI を改善する予定である．

7.5 人対人のチャット分析

2023 年 12 月 6 日の実験で取得した人同士のチャットデータを 302 件に対して，ChatGPT とのチャットと同様の分析を実施した．しかし，データ数が少ないため，単純比較できるものではなく, あくまで補足として位置付けている．

(1) キーワード分析

チャット内の単語の出現回数を表 6 にまとめた．

表 6　対人 頻出単語

単語	出現回数	単語	出現回数
思い	47	生	14
情報	39	年	14
電話	26	月	14
職業	26	気	13
確か	23	抵抗	13
趣味	22	詐欺	12
住所	21	年収	12
アドレス	20	大丈夫	12
番号	20	重要	11
メール	18	何	11
個人	17	問題	11
思う	17	関係	11
公開	16	願い	11
番	16	性	11
日	15	たしか	11

人対人のチャットの場合は「思い」が最も出現頻度の高い単語であり，そのほかにも「思う」「大丈夫」「願い」など，ChatGPT とのチャットではあまり見られなかったような，感情に関わる単語が頻出していることがわかった．

さらに， Tf-Idf 分析を行い，単語の重要度を図 9 のとおり評価した．

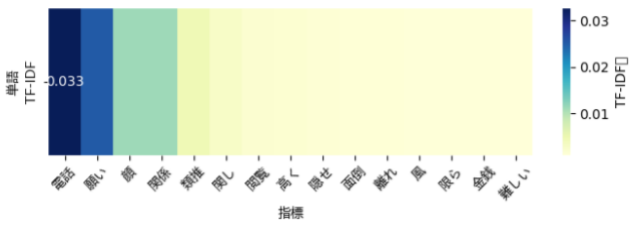

図 9　対人 Tf-Idf 分析

こちらの結果も，「願い」「面倒」「難しい」など，感情に関わる単語が出現しており，プレイヤーが自身の感じたことについて対戦相手にチャットしていることが推測できる．

(2) **トピックモデリング**

続いて，対 ChatGPT と同じ手法を用いてトピックモデリングを実施し，結果を表 7 にまとめた．

各トピックから，「電話」「住所」など，具体的な個人情報について話し合っていることが読み取れる点は，ChatGPT 対戦の際の結果と同じであることがわかる．

しかし，「笑」など，人同士のチャット特有の項目があることから，人同士のチャットの方がフランクにやり取りできるのではないかと思われる．また，「垢」（SNS などのアカウントのこと）や「バレ」など，口語や SNS 特有のワードなども項目に含まれており，同じようなトピックでもチャットの温度感などは異なることが読み取れる．

表 7　対人トピックモデリング

Topic1	Topic2	Topic3	Topic4	Topic5
職業 (0.080)	思い (0.116)	メールアドレス (0.066)	確か (0.032)	個人 (0.051)
住所 (0.045)	情報 (0.050)	お願い (0.041)	電話 (0.031)	性 (0.029)
電話 (0.042)	趣味 (0.047)	情報 (0.033)	公開 (0.030)	情報 (0.027)
番号 (0.036)	番 (0.026)	抵抗 (0.027)	番号 (0.023)	生年月日 (0.026)
気 (0.027)	年収 (0.024)	詐欺 (0.023)	一番 (0.023)	特定 (0.026)
大丈夫 (0.026)	私 (0.021)	公開 (0.020)	抵抗 (0.023)	人 (0.024)
笑 (0.022)	位置 (0.015)	問題 (0.019)	情報 (0.022)	関係 (0.024)
重要 (0.020)	大丈夫 (0.015)	位置 (0.019)	顔 (0.021)	交友 (0.024)
確か (0.020)	重要 (0.013)	確か (0.015)	趣味 (0.020)	危険 (0.023)
垢 (0.018)	同じ (0.012)	カード (0.010)	性別 (0.020)	思い (0.022)
バレ (0.017)	性別 (0.012)	番 (0.009)	人 (0.016)	電話 (0.021)
低い (0.014)	提供 (0.012)	低い (0.008)	関係 (0.012)	可能 (0.021)
年収 (0.011)	生年月日 (0.012)	悪用 (0.008)	悪用 (0.012)	確か (0.019)
怖い (0.011)	カード (0.011)	結婚 (0.008)	バレ (0.012)	自分 (0.018)

8. 実験結果の考察

実験結果から，本ゲームはプレイヤーの個人情報に対する理解を深める効果があり，エンターテインメントの要素も保持していることが確認された．シリアスゲームとしての役割を果たしつつ，参加者が楽しむことができるという二重の効果が本研究から明らかとなった．

特に注目すべきは，対戦形式の違いによってもたらされる体験の質の違いである．人対人形式においては，相手の戦略や思考を予測し，駆け引きを行うというプレイヤー同士の心理戦がゲームの魅力につながっている．これに対して，人対 ChatGPT 形式では，教育的要素が前面に出ることが特徴的である．頻出単語やトピックモデリングからもわかるように，様々な角度から個人情報保護に関して対話を行なっている．さらにチャットを通して，プレイヤーは自らの意識や個人情報に対するスタンスを言語化する機会を得る．この言語化は，個人情報に対する抽象的な意識を具体的な言葉にすることで，プレイヤー自身の理解を深化させる要因となっていると考えられる．また，言語化することで自らの意識や考えを明確にし，それに基づいてゲーム内の選択や戦略を練ることができるようになる．

これらの点から，ChatGPT のようなデジタルアシスタントをシリアスゲームに組み込むことで，プレイヤーの意識をテキストデータとして収集するとともに，言語化によって学習効果を高めることができると考えられる．この手法は，シリアスゲームの効果を最大化するための有益な情報を提供するものとして評価できるだろう．

また，人同士のチャットでの対話も，新たな手法として活用できる可能性を第 4 回実験の結果から見出すことができた．人同士のチャットでの対話は，筆者の主観ではあるが，実験を通して，直接的なコミュニケーションと比較して相手の表情が見えない分，チャット上で「笑」などの感情にまつわるキーワードが散見され，自分の感情にも相手の感情にも慎重になっているのではないかと感じた．

9. おわりに

本研究を通じて，シリアスゲームというアプローチが個人情報保護のリテラシー教育に効果的であることが示された．特に，ChatGPT を用いた対戦形式は，対話によってシリアスゲームの教育的な要素を強化し，プレイヤーの意識や行動に対して影響をもたらすことが確認された．

本研究の結果は，ゲームのデザインや実装の際の参考として，また将来的なシリアスゲームの研究や開発の方向性を示すものとして価値がある．しかしながら，本研究には限定的な実験環境や参加者の数などの制約が存在するため，更なる研究や実験が求められる．今後は，より多様な参加者や環境下での実験を通じて，本研究の結果をさらに拡張し，検証していく必要がある．

本研究を通じて得られた知見は，情報社会における個人情報保護の重要性を再認識する機会となった．シリアスゲームを用いた新しい教育手法の可能性が示された今，この分野のさらなる研究と発展が期待される．

謝辞　実験に協力頂いた皆様に，謹んで感謝の意を表する．

参考文献

[1] Calvo-Morata, Antonio, et al. "Validation of a cyberbullying serious game using game analytics." IEEE Transactions on Learning Technologies 13.1 (2018): 186-197.
[2] Hart, Stephen, et al. "Riskio: A serious game for cyber security awareness and education." Computers & Security 95 (2020): 101827.
[3] Krath, Jeanine, Linda Schürmann, and Harald FO Von Korflesch. "Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning." Computers in Human Behavior 125 (2021): 106963.
[4] 大磯一, 依田高典, and 黒田敏史. "個人のプライバシー意識等とデジタルサービス 利用に関する実証分析." 情報通信学会誌 39.3 (2021): 37-47.
[5] 太幡直也, and 佐藤広英. "他者のプライバシー意識と Twitter 上での他者情報公開との関連." 心理学研究 92.3 (2021): 211-216.
[6] 内閣府 (2006): 個人情報保護に関する世論調査（平成 18 年 9 月調査），集計表 15（Q４）他人に知られたくない個人情報.
[7] Manning, C. D., Raghavan, P., & Schütze, H. (2008). Introduction to Information Retrieval. Cambridge University Press.
[8] Kudo, T., Yamamoto, K., & Matsumoto, Y. (2004). Applying Conditional Random Fields to Japanese Morphological Analysis. In Proceedings of the 2004 Conference on Empirical Methods in Natural Language Processing (EMNLP 2004), pages 230–237.
[9] [Osada, T. (2022). Janome: Japanese morphological analysis engine. GitHub. https://github.com/mocobeta/janome
[10] Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). Latent dirichlet allocation. Journal of Machine Learning Research, 3(Jan), 993-1022.

付録

付録 A.1 悪用カード一覧

	セットA	セットB	セットC
第１試合	オレオレ詐欺	代引き詐欺	スパムメール
第２試合	SNS なりすまし	フィッシング詐欺	結婚詐欺
第３試合	ストーカー	空き巣	結婚詐欺
第４試合	宗教勧誘	いたずら電話	金銭的略取
第５試合	年金詐欺	EC サイトアカウント乗っ取り	勧誘電話
第６試合	国際ロマンス詐欺	預貯金詐欺	スパムメール

付録 A.2 個人情報カード一覧

	カードⅠ	カードⅡ	カードⅢ	カードⅣ	カードⅤ
第１試合	家族構成	電話番号	メールアドレス	住所	サイト閲覧履歴
第２試合	家族構成	交友関係	住所	メールアドレス	電話番号
第３試合	性別	位置情報	住所	年収	顔写真
第４試合	思想	住所	名前	口座情報	電話番号
第５試合	生年月日	メールアドレス	職業	趣味	電話番号
第６試合	電話番号	住所	性別	メールアドレス	家族構成

付録 A.3 カードの配点

付録 A.1 の悪用カードのセット A~C と，付録 A.2 の個人情報カードのⅠ～Ⅴに対応している．

セットA

試合＼カード	Ⅰ［点］	Ⅱ［点］	Ⅲ［点］	Ⅳ［点］	Ⅳ［点］
1	35	35	10	15	5
2	10	40	5	25	20
3	15	40	30	5	10
4	45	20	10	5	20
5	40	5	20	0	35
6	15	10	30	10	35

セットB

試合＼カード	Ⅰ［点］	Ⅱ［点］	Ⅲ［点］	Ⅳ［点］	Ⅳ［点］
1	10	15	10	50	15
2	5	5	15	40	35
3	0	25	40	35	0
4	5	5	5	5	80
5	30	30	5	10	25
6	30	30	5	10	25

セットC

試合＼カード	Ⅰ［点］	Ⅱ［点］	Ⅲ［点］	Ⅳ［点］	Ⅳ［点］
1	0	40	40	5	15
2	40	30	10	10	10
3	30	0	5	50	15
4	5	25	10	40	20
5	10	0	20	20	50
6	40	5	10	40	5