電子選挙における生成 AI による誘導を想定した耐強制性

上繁 義史 [1,*]　櫻井 幸一 [2]

概要：電子選挙の研究においては，秘密投票，自由投票の性質を担保するとともに，票データを安全に取り扱うために，暗号プロトコルの研究が行われている．安全性の要件として，耐強制性が知られているが，情報的な安全性を担保する視点に限定されている．SNS や生成 AI が使用されて起こる情報障害が近年の選挙における投票行動に影響を与えている現状を踏まえると，強制者が心理的，物理的に影響力を行使することを考慮しておらず，この性質の定義としては必ずしも十分ではないと考える．そこで，本稿では，投票所における監視下での投票を仮定し，この視点を含めた耐強制性について考察を行い定義する．強制者が起こす脅威に基づいて，生成 AI の支援の影響やコストへの考慮を含めたリスクについて定性的に考察し，定義の妥当性について議論する．

キーワード：電子選挙，耐強制性，生成 AI，心理学的影響

Coercion Resistance in E-Voting Systems Against Generative AI Manipulation

Yoshifumi Ueshige[1,*]　Kouichi Sakurai[2]

Abstract: In the field of electronic voting research, studies on cryptographic protocols are being conducted to ensure the nature of secret and free voting while securely handling vote data. While coercion- resistance is known as a security requirement, it is limited to the perspective of ensuring informational security. Given the current situation where information disruptions caused by the misuse of social media and generative AI are influencing voting behavior in recent elections, the definition of coercion does not adequately consider the psychological and physical influence exerted by coercive actors, making it insufficient in this context. Therefore, this paper assumes voting under surveillance at polling stations and defines coercion-resistance from this perspective. Based on the threats posed by coercive actors, we qualitatively examine risks, including the influence and costs of generative AI support, and discuss the validity of the definition.

Keywords: Electronic election, coercion-resistance, generative AI, influence of psychology

1. はじめに

近年の選挙において，生成 AI や SNS 投稿（記事，写真，動画など）の活用が，投票者の選好に大きく影響する様子が見られた．2024 年 2 月のインドネシア大統領選挙において，生成 AI を用いて，スハルト元大統領（故人）が特定候補を支持する演説を行っている動画が作成され公開された．2023 年 1 月，アメリカ大統領選挙の予備選挙において，バイデン前大統領を名乗る音声で投票に行かないように呼びかける虚偽の内容の電話がかかった事案があった．これも AI の悪用だと考えられている．他にも，世界的に，選挙期間中に真偽不明の情報の拡散されるケースが散見され，一部が偽誤情報であることが後日検証されたが，その一方，情報の内容が検証困難な投稿もあった．このような情報の作成に，生成 AI が悪用されたとの報道があった．別の方法として，選挙と無関係な地域の住民が SNS の広告収入を見込んで偽誤情報を作成，拡散させるケースも見られた[1]．インターネット上の投稿を主な情報源と考える人ほど，フィルターバブルやエコーチェンバー現象により，偽誤情報を信じこむリスクが高くなる．これにより影響を受けた投票者の選好が特定の方向に誘導されたり，他の候補者の支持者との間で過度の対立を煽られたりする状況は常に起こる可能性がある．特に，偽誤情報により誤った信念が確立されると，その後に訂正情報がもたらされても，先に認識した偽誤情報を正しいと認識する傾向が指摘されている[4]．この傾向は確証バイアスと呼ばれ，偽誤情報の影響がなければ適正に行われたであろう判断が阻害される．これによって本来の民意が歪められたならば，選挙システムが民主的手続きとしての機能を発揮できなくなると考えられる[5]．このリスクは，投票プロセスのスコープ外であり，投票者の意思や思考に作用するものであって，投票日以前から生じる．よって，投票方式が紙の投票用紙による選挙から，電子選挙に移行した後にも残留すると考えられる．

電子選挙の研究は 1980 年代から行われている．この分

1 長崎県立大学
University of Nagasaki
2 九州大学
Kyushu University
* yueshige@sun.ac.jp

野の研究としては，準同型暗号[6][7]，Mixnet[8][9]，ブロックチェーンを用いた手法[10]，否認可能暗号を用いた手法[11]，既存技術を中心とした実装[12]-[14]などが知られている．いずれの方式においても，秘密投票を実現するためのセキュリティ要件（完全性，健全性，匿名性，多重投票の防止，無証拠性，耐強制性など）を満たすよう設計されている．しかしながら，実際の選挙での電子選挙の実施例は必ずしも多くはなく，エストニア[24][25]，アメリカ，アラブ首長国連邦など[14]で部分的に利用されるにとどまる．日本においては，在外投票への適用を視野に実証実験が行われており，スマートデバイスの利用を前提とした機能要件の詳細化や二重投票の防止などのセキュリティ要件の分析について報告されている[14]. 2024 年 12 月の四条畷市長選挙では，各投票所に設置されたタブレット端末の画面表示をタップすることで投票が行われた．各投票所のタブレット端末に蓄積された票データを専用の USB メモリにより収集し，担当者が直接開票所に持参することにより，全ての投票所の票データを集めている．投票から票データの収集に至るまでインターネット上での通信を全く利用していないことが特徴と言える．

電子選挙のセキュリティは，電子投票システムの技術的なセキュリティ要件について議論されているが，投票者にもたらされる情報に起因する認知バイアスの影響が十分考慮されておらず要件が不足していると考えられる．電子投票システムの外部で生じる事象ではあるが，投票日前までに投票者が受け取った情報による本来の意思とは異なる選好を行うリスクを含めた包括的な検討がなされる必要がある．

本研究では，その端緒として投票前の投票者への作用における耐強制性について改めて議論し，強制のモデル化と耐強制性の定義を行うことを目的とする．また，強制の影響とどのような条件でこれを回避できるか（耐強制が成立するか）について知見を得ることも目的とする．本研究では主に強制者とその対象である投票者（以後「被強制者」とよぶ）を対象とし，強制者は指示に従う方向に被強制者を誘導するため，認知バイアスを確実に活用できるように生成 AI の支援を受けることを想定する．

本論文の構成は以下のとおりである．2 節で関連研究を説明し，3～6 節で強制と耐強制について述べる．これらの節で強制者のモデル化や強制の利得に基づく評価について述べ，最後 7 節でまとめとする．

2. 関連研究

Yu のプレプリント[15]で，現行の選挙を前提に，候補者が AI を活用することによる選挙への政治的影響，投票者への心理的影響，セキュリティ，倫理などへの影響について考察している．投票者のターゲティングに活用し，引き付けるメッセージの内容や公開のタイミングなどを効率化する可能性が指摘されている．その一方で電子選挙システムを想定した検討は見られない．同様に AI 利用がもたらすリスクに関する論考も見られる[5][16].

湯浅[17]は，近年のアメリカ大統領選挙に合わせて発信されたディープフェイク情報の選挙へ影響と，これに対抗する各州における法規制の状況を紹介しており，アメリカでは州ごとにディープフェイクの定義，規制の対象期間，規制の対象者，違反者への対処，救済処置などについて，差異が見られることを紹介している．

Jamroga らは，ゲーム理論に基づく考察により，投票における強制についてのモデル化を行っている[18]．強制者が投票者を強制するコストに基づいて利得を計算しているが，強制者の戦略に関する具体的な考察は見られない．ゲーム理論の応用については，情報セキュリティとは別分野であるが警備ゲームについての研究が知られていて，空港におけるテロ抑止[19]や施設の警備一般における犯罪抑止[20]を目的として，人数やコストの制約のもとで，抑止効果の高い警備員の配置計画の方法を述べている．

Yang らは，LLM による投票行動の傾向について分析しており，一部のパラメータを調整することにより人間の投票傾向に近づけることが可能であることを示している[21].

3. 本研究における仮定

本研究では，投票前に強制者が被強制者を自分の指示に従うように誘導/強制することを想定し，その効用によって影響力を評価するモデルを考える．そこで，以下の節で，エンティティなどに関する定義を行う．

3.1 エンティティ

本研究におけるエンティティとしては，以下を仮定する．

(1) 強制者

強制者は選挙において特定候補者を当選させる目的で，投票者の一部を被強制者として誘導もしくは強制し，投票者の選好を自分の指示に従わせようとする個人もしくは組織とする．特定候補者の当選を阻止したい場合は，別の候補者を当選させるように働きかければ良いので，目的としては上述のもので十分である. 誘導や強制を行うにあたり，目的を達成するために，合理的判断を行うと仮定する．また，遂行にかかるコストを負担する能力を有し，本稿ではその上限は仮定しない．計算能力については，既存の生成 AI を利用したシステムを実行できる環境・能力を有するものとする．電子投票システムの暗号プロトコル実行においては honest とし，本研究では投票の通信の観察や内容の取得等の介入は想定外とする．強制の動機については，本稿では検討の対象外とする．

(2) 被強制者

被強制者は当該選挙における一般の投票者であり，強制者によって誘導され選出された者とする．原則として，強制者の指示による特定候補者に投票する．投票所では電子

投票システムを操作して投票行動を行う．被強制者には，合理的判断を行う者と行えない者が混在しているものとする．

(3) 投票所監視者

投票所監視者は投票所において，各投票者（強制者及び被強制者も含む）の投票行動が適切に行われているかを監視する．本稿では電子投票システムの詳細には立ち入らないが，投票所監視者は，受付において投票者の認証を監視する名簿対象係相当，電子投票システムの投票端末起動トークンを貸与する投票用紙交付係相当，投票端末を正しく操作しているかプロセスを監視する投票立会人相当，投票が正しく行われたことを監視する投票管理者相当の者が含まれる．

3.2 本稿で想定する投票までのプロセス

各エンティティが行う内容を図 1 に示す．

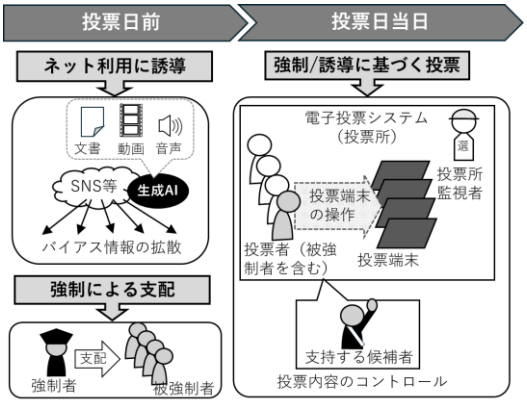

図 1　投票日までの各エンティティの行動

Figure 1 Behavior of Entities Prior to Election Day

4. 誘導もしくは強制の主な手段

この節では，強制者が当該選挙の投票者に対して行う誘導や強制の方法について概説する．

4.1 生成 AI で作成した記事や動画の SNS への自動投稿及びフィードバック情報に基づく誘導

強制者は既存の生成 AI を利用して，様々な内容の偽誤情報を生成し，SNS への投稿やフィードバック情報の管理を行うツールを運用しているものとする．このツールの利用について説明する．

ダミーのユーザ ID，認証情報，メールアドレス，プロフィール（人物の写真画像を含む）を生成する．生成された各データを，ツールを用いて自動入力して，各種ソーシャルネットワークサービスの新規アカウントを作成する．これによってダミーのアカウントを複数作成する．

投票者を対象に，当選させたい候補者，その所属組織への支持を呼び掛ける情報（記事，写真，動画）や対立候補者，対立組織の評価を低下させるような偽誤情報を生成する．生成 AI を用いるので，投票者のプロフィールに合わせて多言語に対応することも容易である．生成した情報は，上記で作成したダミーのアカウントから自動投稿する．

このツールの活用で，選挙と無関係かつ直接利害関係のない全くの第三者に記事の作成及び拡散を依頼する内容を投稿することも想定される（広告収入による経済的動機で第三者から依頼を受けるケースについては実例がある[1]）．

投票所監視者の監視の効果を減じるために，投票所監視者に対して，認知的過負荷を生じるほどの大量の偽誤情報を生成して投稿する．これにより，後述する強制者と被強制者の利得（行動のインセンティブにあたる量）にて強制者に有利にはたらくことを期待している．

上記の機能のほかに，ダミーID，認証情報，プロフィール情報の管理や投稿後の「いいね」「コメント」の情報取得，強制者へのフィードバックを行う機能を想定する．注目を集めるために，このツールで「いいね」を押すことも考えられる．

4.2 誘導から強制への移行

SNS 等におけるエコーチェンバー現象が期待できるため，強制者の発信に関心をもった者は比較的考えが近しいと考えられる．4.1 のツールから得られたフィードバック情報から，彼らを選び買収や利益供与の申し出を行って，被強制者として投票を促す．

強制する手段としては，脅迫も考えられるが，選挙の規模が大きくなると実施が困難である．投票所，選挙区，候補者についての虚偽情報の流布による扇動も考えられる．この段階では，対象人数に比例して対応や管理のコストが増大するとみなせる．

強制の効果としては，投票所に行かせて，強制者の指示する候補者に投票させるか，棄権させるかの 2 つの選択となるが，特定候補者を当選させることを目的とするので，前者の効果に限定する．

4.3 被強制者の投票行動の検証

電子投票システムにおいて暗号学的な耐強制性が成立していることを仮定すれば，強制者が検証可能な投票内容の情報を直接得ることはできない．

被強制者の直接的な投票行動を監視するために，スマートグラスなどを用いて，直接的な監視が考えられ，暗号学的な耐強制性を破ることが可能であるが[22][23]，監視のためのコスト増大（スマートグラスの購入，監視システムの導入，運用，維持管理など）を避けられない[2]．

そこで，直接の監視を行わなくても，監視に相当する心理的影響のある誘導を行うことによって，強制者の指示通りの投票行動を行わせる．一般に投票所内で投票端末の操作などを撮影することは不可能と考えられるため，被強制者が指示通りの投票を行ったかについて個別に把握するのは困難である．同一の投票所に一度に複数人で行くなど，相互に行動を牽制させることは可能であるが，本稿では具体的な方策は未検討である．誘導や強制の成否は，投票期間終了後の集計結果に基づく推測によらざるを得ない．

5. 強制のモデル化及び耐強制性の定義

本節以後では，強制に関する諸記号を定義し，強制者や被強制者の主観による利得を考え，耐強制性の定義を提案する．

5.1 強制に関する諸記号

投票者Vが取りうる選好（候補者）の集合を$X = \{X_1, X_2, \cdots, X_n\}$とし，選好$X$に対応する確率（候補者が選ばれる確率）を$P(t) = \{P_1(t), P_2(t), \cdots, P_n(t)\}$ $(\sum_{i=0}^{n} P_i(t) = 1)$とする．$P(t)$は投票者個々人によって異なると考えられ，自身の支持に基づく主観確率とみなせる．選好順序は選挙期間を通して変化することが考えられるので，それぞれのP_iは時間tの関数と考えることができる．

5.2 強制及び耐強制の定義

投票者が票を投じる候補者$X_B \in X$は投票の時点で$P_B = \max_i P_i$を満たす者と仮定する．強制者Cが望む選好を$X_C \in X$とすると，被強制者の選好が$X_B = X_C$となるようにCがVに干渉する．

強制者による被強制者の選好への干渉行為の集合を$Int = \{In_1, In_2, \cdots\}$と書く．投票日前に複数の干渉行為$Int$を行うことによって，投票者$V$が候補者$X_C$を選好するように被強制者の選好の確率$P(t)$を変化させることを企図する．$Int$の複数の要素を作用させるのは，同種の情報（候補者$X_C$への支持）に接する機会を増やすことで，単純接触効果の影響により，X_Cへの好印象を持つことを期待できるためである．

強制者の干渉を受けた結果としての選好を関数Fとして記述し，

$$X_B = F(V, X, P, X_C, Int)$$

と書く．もし

$$X_C = F(V, X, P, X_C, Int)$$

が成り立てば，強制は成功となる．これには，強制や誘導なしにX_Cを選好するケースも含まれる．逆にIntの作用にもかかわらず

$$X_C \neq F(V, X, P, X_C, Int)$$

となる場合も考えられ，これは強制の失敗を意味する．

本研究では，上記のような，強制の失敗を保証できる選挙システムが耐強制性を有するものと定義する．

この定義の特徴としては，暗号学的な定義と異なり，証拠に関する議論が含まれておらず，投票前の時点の強制者の干渉行為と被強制者の選好を含んでいる点が挙げられる．また，主観確率に基づくが，選好に関する確率を含む表現となっている．この定義を満たすには，インターネット上の選好にかかわる偽誤情報の作用を無効化する仕組みと投票システムを包含する選挙モデルが要請されていると捉えることができる．

6. 強制者と被強制者の利得の定義と考察

6.1 強制者の利得

ゲーム理論を参考に，本稿では強制者の利得を検討する．利得の最大値を$Gain$と書く．これは強制者による主観評価に基づいており，強制を行うにあたっての自己効力感ととらえることができる．AI の支援を受けることにより自己効力感が高まり$Gain$は上昇すると考えることができる．

強制コストの利得への影響を$Cost$，投票所監視者の利得への影響を$Officers$と書く．この 2 つの影響は強制者にとっては利得を下げる方向に作用するとみなせる．強制のコスト$Cost$が上昇すると，誘導や強制の状態の維持においてマイナス方向の要因になると考えられる．また，投票所監視者の影響$Officers$が増大すると，被強制者が候補者X_Cを選好する可能性が損なわれると考えられ，やはりマイナス方向の要因になる．

よって，強制者の望む選好が行われるときの強制者の利得は

$$u_c = Gain - Cost - Officers$$

と書ける．

強制者の利得u_cについて，$Cost$を変数としたグラフを書くと図 2 のようになる．グラフにおいて，利得u_cが正の区間では，強制者は投票者への干渉行動Intを行うインセンティブが働くと考えられる．強制者が生成 AI を利用することにより，自分の行動の精度（確度）の向上が見込まれるため，その分だけ利得が上昇すると考えられる．

利得u_cが負となる区間においては，強制のコスト増大の影響が無視できなくなり，強制者のインセンティブが押し下げられ，結果として耐強制性を満たすと解釈することができる．このことから，強制者の支払うコストを上昇させることで強制者の認識する利得が減少し，耐強制性を確保するのに有効であるといえる．

横軸を$Officers$に置き換えた場合も，利得u_cの直線は単調減少となると考えられる．被強制者が投票所内で不正行為を行う場合は，投票所監視者の影響$Officers$を増大させ

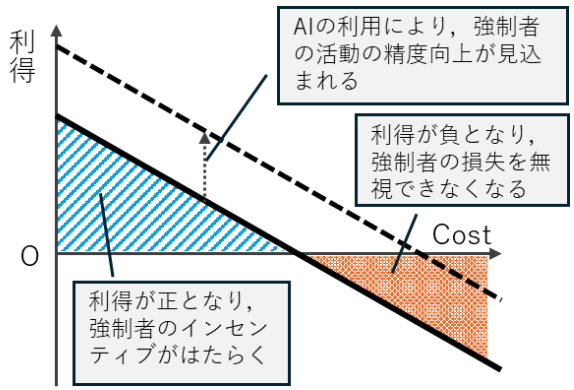

図 2　コストの変化による強制者の利得の変化

Figure 2 Variation in the Coercer's Payoff with Respect to Cost Changes

ることによって，強制者の利得を負にすることが考えられる．よって，耐強制性の視点からは$Officers$を増大は有効と考えられる．しかしながら，選挙の規模（国会議員選挙や地方自治体の首長選挙など）では，1 回の選挙当たりに開設される投票所数が膨大な数となるため，それぞれの投票所に監視を支援するシステムを導入するような，投票所の開設コストの増大につながる対策は困難と考えられる．また，4.1 で述べたように，強制者からの認知的過負荷を起こすレベルの情報に接した場合，$Officers$が減じられることも考慮する必要がある．

被強制者が投票所内で全く不正を行わずに通常の投票行動を行う場合においては，投票所監視者がどのような対応をしても（コストをかけても），耐強制という視点においては効果がないと考えられるが，本モデルでは，この点について説明できていない．

6.2 被強制者の利得

次に，被強制者の利得について考察する．強制者の場合と同様に，主観評価の影響が大きくなる．強制者の場合と異なるのは，被強制者自身が認識する自己の利得と，第三者から見た被強制者の利得を考える点にある．前者は強制者の指示に従って投票を行うことに対する利得，後者は強制を回避するなどして，自由意志で投票を行うことに対する利得である．

利得を考える上でのパラメータを以下の通りとする．インセンティブの利得への影響を$Incentive$と書く．これは「強制者の考えに沿って自分の手で投票を行う」という誘因が働いているため，被強制者の認識としてはプラスの要因となると考えられる．

投票所監視者の利得への影響を$Officers$，法律や条例などのルール遵守による利得への影響を$Compliance$とする．この 2 つの要素は被強制者の視点（すなわち強制を受け容れている立場からの視点）では自身の行動に対する阻害要因となるため，利得としてはマイナスの影響をもたらすと認識される．それぞれの被強制者において，$Compliance$と$Officers$のマイナスの影響の程度は必ずしも一定ではないと考えられる．すなわち，強制者の指示に沿った投票行動をとることに積極的な立場であれば，利得を下げる効果は限定的になると考えられる．また，逆に消極的な立場であれば，マイナスの影響が大きくなり利得を大きく低下させる可能性が見込まれる．被強制者の立場の違いによる，$Compliance$と$Officers$のマイナスの影響の程度を係数αによって表すものとする．

第三者から見た場合の利得としては，本来正のインセンティブに相当する．これは，ルールを守ることが客観的には当然のことであり，投票所監視者もルールを守る限り，自分の行動の正当性を確保してくれると考えられるため，いずれもプラスの方向に作用するとみなすことができる．

これらの考察から，被強制者の利得は以下の 2 つの式で表すことができる．

被強制者の認識する自身の利得：

$$u_{v1} = Incentive - \alpha(Compliance + Officers)$$

第三者から見た被強制者の利得：

$$u_{v2} = Compliance + Officers$$

これらの式の特徴は，被強制者から見た利得と第三者から見た利得では，一部の要素の符号が反転していることである．これは後に耐強制性の議論で扱う．

被強制者の選択肢とその利得の変化とその要因を表 1 に示す．表中の↑は利得の上昇傾向，↓は下降傾向を意味する．

表 1　被強制者の行動の選択と利得の関係

Table 1 Effect of Behavioral Decisions on the Coerced Party's Payoff

	被強制者の認識する自身の利得の高低	第三者から見た被強制者の利得の高低
強制者の指示通りに投票	↑（利益/身の保全への期待）	↓（自由投票の棄損，犯罪の可能性）
強制者に従わずに棄権	↓（強制者からの制裁への恐れ）	↓（自由選挙の棄損）
強制者に従わずに自由投票	↓（利益逸失/身の保全への恐れ）	↑（自由投票の実行）

表 1 の解釈の例として，被強制者が強制者の指示通りに投票したときのケースを説明する．被強制者の認識としては，利益が与えられるか，身の保全が図られることを期待できることから，利得が上昇傾向になることとなる．第三者から見た場合，自由投票の原則を棄損すること，投票に至る過程で犯罪の可能性が考えられることから，利得は低下すると解釈できる．

次に，被強制者の利得の変化を図示することを考える．2 つの要素$Compliance, Officers$の合計を変数として（本来は別の軸であるが，本論文での分析上差し支えないので，まとめて 1 変数として扱う），被強制者の利得のグラフを書くと，図 3 のようになると考えられる．

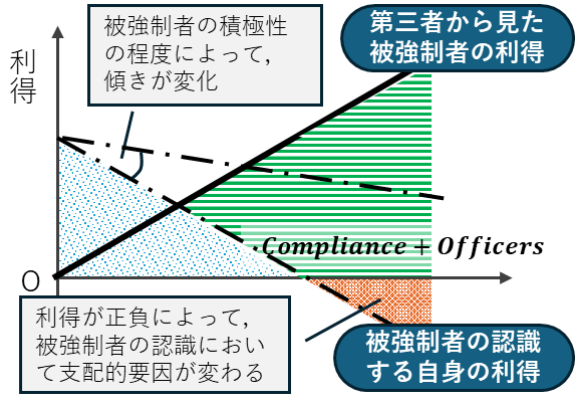

図 3　被強制者の利得

Figure 3 Coerced Party's Payoff

図 3 から，被強制者の認識する自身の利得u_{v1}において，$Compliance + Officers$が小さい間（利得が正である間）は強制者の影響が支配的であり，強制者の指示に従う方が良いと考えている状態である．逆に利得u_{v1}が負になると，ルール遵守と投票所監視者の影響が支配的となるため，強制者の指示に従うことが自身にとっても不利益であると認識すると解釈できる．

この影響はαによって変化する．$\alpha = 1$に近い値であれば，直線u_{v1}のマイナスの傾きが大きくなるので，上述の説明の通りの傾向とみなすことができる．一方，$\alpha = 0$に近づくと，直線u_{v1}は初期値$Incentive$からの減少幅が小さくなるので，その分だけ$Compliance + Officers$の影響も$\alpha = 1$の近い場合と比べて限定的となり，$Compliance + Officers$が大きくならないと，利得への影響は上記の説明の通りとならない．$\alpha = 0$のときは，直線u_{v1}は初期値$Incentive$で一定となる．このことは，被強制者が強制者に従って投票行動を行うために，$Compliance + Officers$の影響を全く認識しない（意に介さない）と考えられる．

次に，第三者から見た利得u_{v2}を考えると，単調増加となっていることが分かる．被強制者の認識による自身の利得u_{v1}との交点を境界として，u_{v2}が上回ることが分かる．交点より右側（$Compliance + Officers$が大きい側）ではu_{v2}が優勢になっていると考えられるので，被強制者が投票を行うよりも前に，第三者から見た利得を説明するなどして，自分の考えに基づく自由投票が合理的な判断であることを認識させられれば，強制者からの影響を脱する可能性があることが示唆される．

7. まとめ

本論文では，近年の選挙に様態から，投票前から誘導や強制が行われる可能性が高いことを想定し，この段階での耐強制性を検討した．まず生成 AI を利用した SNS 等への投稿により投票者を誘導・強制する状況を考え，強制者の干渉行為に基づく強制についてモデル化した．耐強制性の定義を与え，強制者の干渉行為によらずに自由投票を確保できる選挙システムの必要性を述べた．正の影響，負の影響を与える要因に基づいて強制者と被強制者の利得についてモデルを考えた．そのグラフを解釈して耐強制性確保へとつながる性質を検討した．その結果，強制者については，実行コストの影響を増大させることによって，強制を行う利得を減じる効果が期待されることを示すことができた．被強制者については，自身の認識する利得と第三者から見た利得を分けて考え，後者が前者を上回る状況において，投票前の説得などから強制の影響を脱する可能性を生むことが示唆された．

今後は，本研究の知見を拡張して，暗号学的な耐強制性を包含した定義について検討を行う．また，モデルの詳細化を進めることによって，ゲーム理論に基づく理解を進めていき，耐強制性を確保できるセキュリティ要件を詳細化する予定である．

謝辞　本研究は 2025 年度長崎県立大学学長裁量教育研究費（課題名「電子投票システムにおける AI 等を活用した人的側面に関する安全性強化」）の支援を受けて行われた．

参考文献

[1] 山口真一：ソーシャルメディア解体全書 フェイクニュース，ネット炎上，情報の偏り：勁草書房（2022）
[2] 上繁義史，櫻井幸一：電子投票における参加者の戦略選択に基づくセキュリティリスクに関する一考察，2025 年暗号と情報セキュリティシンポジウム（SCIS2025），3F3-2，（2025）．
[3] 笹原和俊：SNS の中で“つくられる真実”と“対立する正しさ”，心理学ワールド，Vol. 98，pp. 12-15，（2022）
[4] 鈴木悠：情報操作型サイバー攻撃における認知的側面，日本セキュリティ・マネジメント学会誌，Vol. 38, No. 1，pp. 13-20，(2024).
[5] Stockwell, A., et al.: AI-Enable Influence Operations: Safeguarding Future Elections, Research report of Centre dor Emergin Technology and Security, The Alan Turing Institute, (2024).
[6] Benaloh, J. and Tuinstra, D.: Receipt-free secret-ballot elections (extended abstract), Proc. of the twenty-sixth ACM symposium on Theory of Computing (STOC), pp. 544-553 (1994).
[7] 小林哲二：準同形の一方向性関数による無記名の電子投票方式の機能拡張，第 7 回情報科学技術フォーラム，pp. 89-90，（2008）．
[8] Sako, K. and Kilian, J.: Receipt-Free Mix-Type Voting Scheme-A practical solution to the implementation of a voting booth, Advances in Cryptology -EUROCRYPT '95, LNCS 921, pp. 393-403, (1995).
[9] Lee, B., et al.: Providing Receipt-Freeness in Mixnet-Based Voting Protocols. Proc. of 6th International Conference on Information Security and Cryptology - ICISC 2003, pp. 245-258, (2004).
[10] Gupta, S. P. and Tripathi, A. M.: E-Voting using Blockchain, Journal of Physics: Conference Series, 1911 (1), (2021) 入手先 <https://doi.org/10.1088/1742-6596/1911/1/012001>, (参照 2025-02-21).
[11] Howlader, J., et al.: Uncoercibility In E-Voting And E-Auctioning Mechanisms Using Deniable Encryption, International Journal of Network Security & Its Applications 3(2), pp. 97-109, (2011).
[12] Hao, F., et al.: End-to-end Verifiable E-voting Trial for Polling Station Voting, IEEE Security & Privacy, Vol. 18 (6), pp. 6-13, (2020).
[13] Agate, V., et al.: SecureBallot: A secure open source e-Voting system, Journal of Network and Computer Applications 191 (2021) 103165.
[14]（株）情報通信総合研究所：令和 6 年度 在外選挙インターネット投票システムの技術的検証及び運用等に係る調査研究事業 最終報告書（概要版），総務省，(2025)，入手先< https://www.soumu.go.jp/main_content/001022659.pdf>（参照 2025-08-19）
[15] Yu, C.: How Will AI Steal Our Elections?, OSF Preprints un7ev, Center for Open Science.(2024)，入手先 <https://doi.org/10.31219/osf.io/un7ev>（参照 2025-02-21）.
[16] Maine, I. M. and Esiefarienrhe, B. M.: The Impact of Artifical Intelligence, Ethical Implications and Technologies on the Electorical Process, E-Journal of Humanities, Arts and Social Sciences (EHASS), Vol. 5, No. 16, pp 3211 – 3219, (2024).

[17] 湯淺墾道：特別解説　米国大統領選挙とディープフェイク，情報処理 Vol.65 No.7, pp. 344-346, (2024).
[18] Jamroga, W., and Tabatabaei, M: Preventing Coercion in E-Voting: Be Open and Commit. In: Krimmer, R., et al. Electronic Voting. E-Vote-ID 2016. Lecture Notes in Computer Science, vol 10141. Springer, Cham. (2017)，入手先 <https://doi.org/10.1007/978-3-319-52240-1_1>（参照 2025-02-21）.
[19] 宝崎隆祐：警備ゲームの動向，日本オペレーションズ・リサーチ学会機関紙，Vol. 64，No. 10，pp. 614-621, (2019).
[20] 鈴木勉：警備ゲームモデルに基づいた空間的警備戦略と犯罪抑制効果に関する数理的研究，日本都市計画学会 都市計画論文集 Vol.55 No.1, pp. 79-84，(2020).
[21] Yang, J. C. ， Dailisan, D., Korecki, M., Hausladen, C. I.,Helbing, D.: LLM Voting: Human Choices and AI Collective Decision-Making, Proceedings of the 2024 AAAI/ACM Conference on AI, Ethics, and Society (AIES '24), pp. 1696-1708, (2025)
[22] 上繁義史，櫻井幸一：紙ベースの投票における不正行為防止の仕組みを電子投票に展伸させるための一考察，2024 年暗号と情報セキュリティシンポジウム（SCIS2024），1B1-4，（2024）.
[23] Ueshige, Y. and Sakurai, K.: A Study on Extending the Mechanism for Preventing Fraud in Polling Stations to Electronic Voting Schemes, Proc. of the 2024 5th International Artificial Intelligence and Blockchain Conference, pp. 62-66, (2025) 入手先 <https://dl.acm.org/doi/10.1145/3702359.3702368 >（参照 2025-02-21）.
[24] Pereira, O.: Individual Verifiability and Revoting in the Estonian Internet Voting System, Financial Cryptography and Data Security. FC 2022 International Workshops pp 315–324, (2022).
[25] 湯淺墾道：エストニアの電子投票，社会文化研究所紀要 65 号，pp. 39-71，(2009).