社会安全とプライバシー
Japanese Journal of Social Safety and Privacy

解説

AI システムの検証可能な出力監視

藤井 雄作

群馬大学 大学院理工学府

〈fujii@gunma-u.ac.jp〉

要旨：膨大なデータを処理し，プライバシーを含む情報を取り扱う AI システムの普及は，民主主義社会におけるプライバシー保護の重要性を増大させている．著者は，プライバシーを含むデータを取り扱う AI システムの出力を対象とした「AI 出力の検証可能記録」(Verifiable Record of AI Output) を提案している．この手法は，出力データに対して事前に定義されたルール適合性を確認し，その過程を透明かつ改ざん防止の形で記録・公開するものである．これにより，AI 利用の透明性と信頼性を確保しながら，悪用や乱用のリスクを抑止することが可能となる．本提案は，プライバシーを含む膨大なデータを取り扱う他の AI システムへの適用可能性も
有しており，民主主義社会における AI の責任ある利用のためのテンプレートとして機能することが期待される．

キーワード: 人工知能，プライバシー，社会基盤，民主主義，社会安全，国家安全保障，公共政策，規制，ブロックチェーン，ファイアウォール

１．はじめに

近年，膨大なデータを扱う AI システムが普及し，公共の利益や国家安全保障など多様な目的での活用が期待される一方，プライバシー保護が民主主義国家における重要な課題となっている[1-6]．プライバシー保護が確保され，社会からの信頼を得ることが，AI の持続可能な導入に不可欠である．著者は，出力データのルール適合性を透明かつ改ざん防止の形で記録・公開する「AI 出力の検証可能記録」を提案し，これによりプライバシー保護と AI 利用の透明性・信頼性を両立しつつ，民主主義社会における責任ある AI 利用のテンプレートとしての可能性を示している[5]．

この著者による研究[7] では，プライバシー侵害リスクが比較的高いユースケースとして「あらゆる地点が AI に接続された街路カメラで監視される広範な公共空間」(Public space watched by AI-connected cameras) を対象とする[8,9]．中国の一部都市では，これに近いシステムが構築されつつあると推測される[10,11]．このシステムにおける社会的に許容される利用目的として，(1) 行方不明者の追跡，(2) 子供の見守り，(3) 公共空間の異常検知，(4) 犯罪・テロ行動の分析を想定する．

既存のプライバシー保護策には，入力データの匿名化，出力データの匿名化，AI プロセスの可視化，データの最小化，保持期間の制限，ユーザー同意の取得などがある[12-19]．しかし，AI システムに対する信頼を高めるには，悪用を確実に防ぐ監査体制が必要であり，その仕組みはシンプルでわかりやすいことが望ましい．著者は，AI 出力に焦点を当てた「AI 出力の検証可能記録」を提案している[7]．これは，AI 出力が事前定義されたルールに適合するかを確認し，その記録を改ざん不可能な形で公開することで，AI の透明性と信頼性を向上させる．また，この仕組みをテンプレートとして，プライバシー保護が必要な他の AI システムへの適用可能性も議論する．本解説では，著者の論文[7]の内容，AI 出力に焦点を当てた「AI 出力の検証可能記録」について解説する．

２．「AI 接続カメラでモニタされた公共空間」の特徴

図１に示す「AI 接続カメラでモニタされた公共空間」は，AI に接続された街路カメラで広範な公共エリアをモニタリングするシステムであり，既存街路灯をカメラ内蔵型に置換することで低コストでの実現を目指している[7-9]．夜間には街路灯が全ての地点を照明し，複数のカメラが視野をカバーし，画像を保存しつつ AI サーバと連携する．

このシステムで実装が想定される 4 つの利用機能は以下の通りである：

[Function-A] ヒト・車両の追跡[20,21]：誘拐された子供や容疑者などを画像処理で追跡し，現在位置や画像を出力.
[Function-B] 子供の見守り：家から帰宅までを追尾し，異常時には保護者への通報や声掛けを行う.
[Function-C] 異常な状況の検知[22,23]：犯罪行為や事故などを検知し，通報や音声での警告を実施.
[Function-D] 行動パターンの分析と通報[24]：犯罪者やテロリストと類似する行動パターンを検出し，警察に通報. これらの機能は社会安全を向上させるが，同時にプライバシー侵害のリスクも存在する. そのため，以下のプライバシー保護策が必要とされる：

- 社会的議論に基づき，AI 利用目的を法制化・ルール化[25,26].
- 「Government Regulatory Agency for AI」がルールを AI 運営会社やユーザーに通達. 例として，米国の NIST や European AI Office が挙げられる[27-30].
- AI 運営会社やユーザーによる自己対策だけでは，誤魔化しや利益相反を防ぐのは難しいため，ルール遵守を監査する仕組みが不可欠である[31,32].

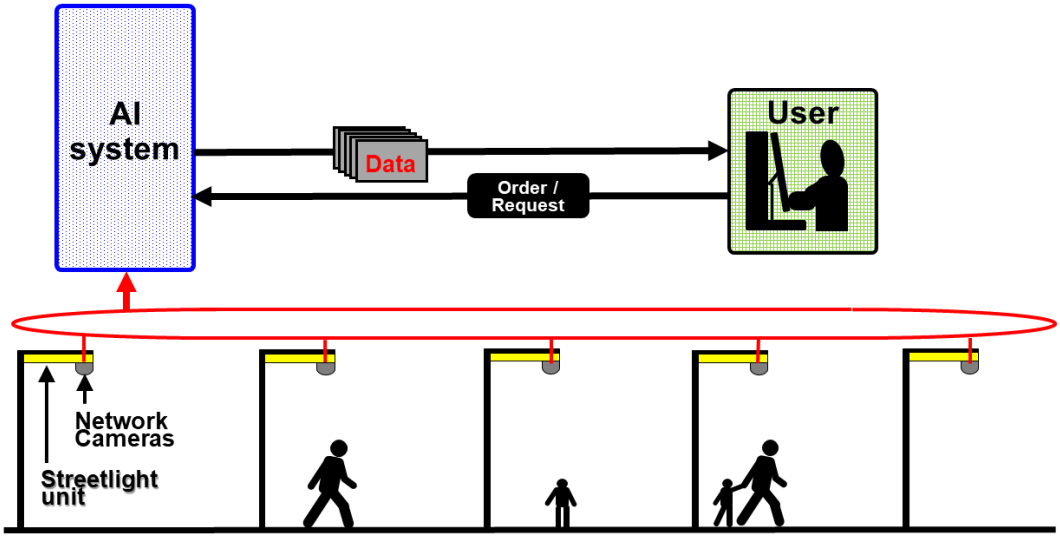

図1.「AI 接続カメラでモニタされた公共空間」の模式図 [7]

3. 「AI 出力の検証可能記録」の提案

3.1. コンセプト of 「AI 出力の検証可能記録」 for 「AI 接続カメラでモニタされた公共空間」図２に示す「AI 出力の検証可能記録」は，AI 運営会社や AI User（警察，警備会社など）のルール遵守を監査するためのシステムであり，以下の特徴を持つ：

1. 政府による統括：「Government Regulatory Agency for AI」が全体を管理.
2. 利用目的の明確化：AI 機能は事前の社会的議論を基に法令「Rules」で利用範囲を規定. しかし，故意や過失による悪用，乱用などのリスクが依然存在.
3. AI User 規制：警察や警備会社は利用時に申請が必要. 申請内容と判断結果を記録し，規制可能に. ただし，
   AI システム自体の監査は不十分.
4. AI system 規制：独立機関 Recorder が出力を Firewall[33]で管理し，「Rules」適合性を判定. 記録は保持されるが，信頼性の証明が課題.
5. 改ざん防止記録：Recorder と政府機関により，判断過程と出力内容を匿名化し，Blockchain で記録[34,35] .
6. 監査可能性：記録は公開され，市民や監査機関による監査が可能. 不正が明らかになることで，プライバシー保護への信頼感が向上.

改ざん防止には Blockchain が有効だが，経済性を優先した改良版や電子署名の活用も選択肢となる. 方法の選定は，改ざん困難性と運用負担のバランスを考慮して行われる.

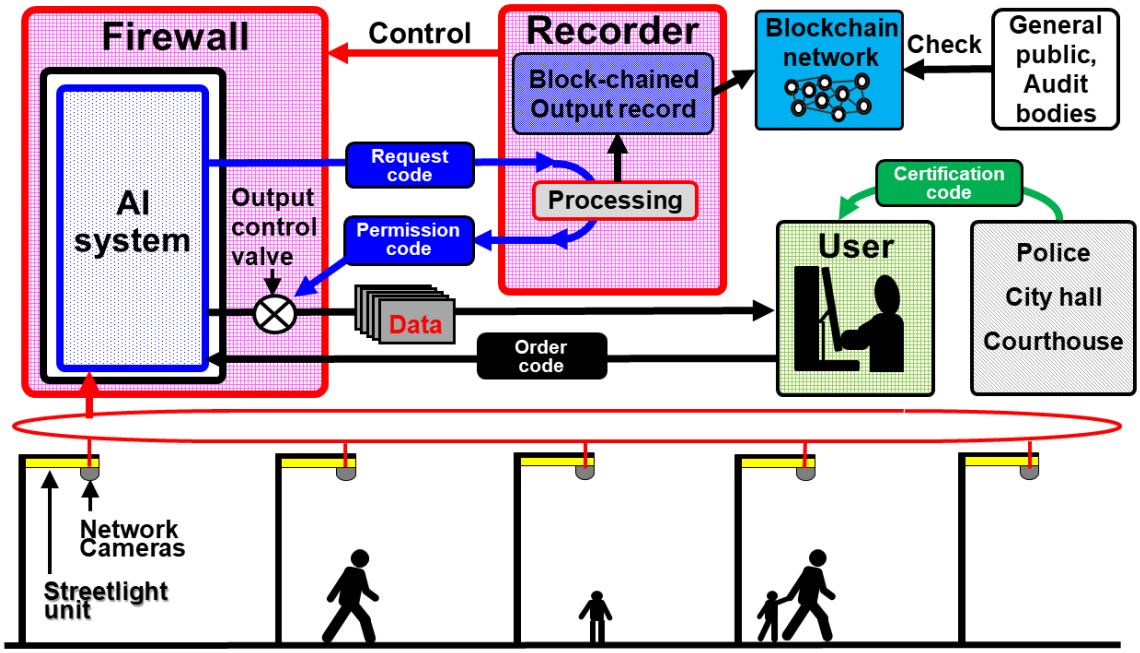

図2.「AI 出力の検証可能記録」を適用した
「AI 接続カメラでモニタされた公共空間」の模式図 [7]

3.2. Procedure of 「AI 出力の検証可能記録」 for 「AI 接続カメラでモニタされた公共空間」
図２に示す「AI 出力の検証可能記録」を実装した「AI 接続カメラでモニタされた公共空間」の動作手順は以下の通り：

1. ルールの策定：「AI system の動作」や「出力要求」は，事前に社会的議論を経た「Rules」に基づき，「AI system 運営会社」と「AI User」が遵守する．ルールは「Government Regulatory Agency for AI」が策定・伝達する．
2. 利用許可申請：AI User は「Rules」に基づき使用申請を行い，政府機関が判定して許可を発行する．
3. 許可プロセスの記録：申請から許可発行までのプロセスは匿名化され，Blockchain に保存．検証可能かつ改ざん不可能な形で記録される．
4. Firewall 設置：Recorder が AI system を Firewall で保護し，出力を管理．
5. 出力許可判定：AI system は出力前に Recorder からの許可を取得し，Firewall を通じて制御される．
6. 出力管理：Recorder は出力要求を「Rules」に基づき承認・非承認し，Firewall の開閉を制御する．
7. プロセス記録：すべてのプロセスは匿名化され，Blockchain に保存．市民や監査機関が確認可能．
8. 監査：市民や監査機関が記録を監査し，「Rules」に適合しているか確認する．

メッセージ内容の概要
[Rules]：AI 利用法を規定する法令．Blockchain で変更履歴を保存．
[Request for AI usage]：AI User が利用許可を申請するメッセージ．
[Permission of AI usage]：「Rules」に基づいて許可された利用範囲を記載したメッセージ．
[Order for AI output]：AI User が解析・出力を依頼するメッセージ．
[AI output permit application]：AI system が Recorder に送る出力許可申請メッセージ．
[AI output permit conditions]：Recorder が Firewall に送る許可条件．
[AI output]：Firewall を通じて送信されるデータ．
[Anonymized record]：Blockchain に保存される匿名化された記録．

以上により，AI 利用における透明性と信頼性が確保される．

3.3. ４つの機能例 for「AI 接続カメラでモニタされた公共空間」with 「AI 出力の検証可能記録」
図２に示す「AI 接続カメラでモニタされた公共空間」の AI system には以下の 4 つの機能が実装され，AI output の許可手続きが行われる．AI User（警察署，警備会社など）は「Government Regulatory Agency for AI」から許可を得て，AI system に送信．AI system が出力結果を Recorder に申請し，許可内容が一致していれば
Firewall が開放される．

機能例
[Function-A] ヒト・車両の追跡
- 許可内容：誘拐被害者や容疑者，迷子の現在位置と関連する画像・ビデオ．
- 条件：一回の許可で 1 ターゲットの追跡が可能．

[Function-B] 子供の見守り
- 許可内容：子供の外出中に異常が検知された場合の保護者・警備会社・警察への通報．スマートフォンやカメラを通じた声掛けも含む．
- 条件：一回の許可で 1 年間の監視が可能．

[Function-C] 異常な状況の検知
- 許可内容：異常が検知された際，警備会社や警察への通報．
- 条件：一回の許可で 1 年間の監視が可能．

[Function-D] 行動パターンの分析と通報
- 許可内容：犯罪者やテロリストと類似する行動パターンを持つ歩行者の検出と通報．
- 条件：一回の許可で 1 年間の分析が可能．

これらの手続きにより，AI system の透明性と適切な利用が担保される．

4. 考察
AI system のプライバシー保護法は，公共の利益（SDGs [36]，国家安全保障，経済発展など）とのバランスを考慮し，AI output に単純な出力規制を掛けるアプローチが現実的と考えた．本研究では，「AI 接続カメラでモニタされた公共空間」を例に，以下の必要条件を示した：
- ルールの制定：利用目的や範囲が社会的議論を経て法律で明確化される．
- ルール適合性の記録：AI の動作に必要な情報を確実に記録．
- 監査の実施：記録に基づき客観的かつ確実な監査が可能であること．
- 仕組みの簡便性：管理・監査が分かりやすく実行可能であること．

出力制限を重視する理由として，以下が挙げられる．
- 入力データは Big Data で制限が困難．
- AI の内部プロセスはブラックボックスで制御が難しい．
- 出力制限は対象が特定でき，個別に検証可能．

関与する主なプレイヤーとして，以下が挙げられる[37]．
- Government Regulatory Agency for AI：AI の管理・監督を行う．
- Recorder：Firewall の運用や出力記録の匿名化・保存を担当．競争原理による低コスト化が望ましい．
- AI system 運営会社：システム開発・運用を担い，適正な料金を徴収．

AI output が有効な 5 つのカテゴリとして，以下が挙げられる．
- 監視システム[38]：安全と効率向上のためのリアルタイム監視．
- 個人情報管理システム[39]：PII の管理と保護．
- マーケティングシステム[40]：行動パターン分析による広告や販売促進．
- 研究・開発システム[41]：Big Data の分析による製品開発・基礎研究．
- 公共政策システム[42,43]：政策決定や公共サービス改善への活用．

ルール適合性のプロセスとして，以下が挙げられる．

- 各 Function の用途と出力が厳密に定義される．
- 出力はルール適合性を判定し，改ざん不可能な形で記録・公開．
- 記録に基づき監査を実施し，不正や乱用を防止．

今後の展望として，社会実験を通じて「AI 接続カメラでモニタされた公共空間」および「AI 出力の検証可能記録」の実現可能性を検証．これを基に，Big Data を扱う他の AI system への適用を目指すべきである．

５．結言

膨大な情報を扱う AI system が出現し，民主主義国家においてプライバシー保護が重要課題となっている．本解説では，著者の最近の研究[7]に基づき，プライバシー保護コンセプト「AI 出力の規制」について説明した．

まず，街路カメラがすべての地点をモニタする「AI 接続カメラでモニタされた公共空間」を例にとり，以下の
4 つの機能を取り上げた：

1. 人や車両の追跡
2. 子供の通学路の見守り
3. 公共エリアの異常検知
4. 犯罪やテロ行動パターンの分析

これらの機能は社会安全に効果的である一方，プライバシー保護が課題である．その対策として，著者が提案[7]している「AI 出力の検証可能記録」について説明した．このコンセプトは以下を特徴とする：1. 事前定義されたルール内での出力制限：AI output はルール適合性が確認された場合のみ許可．
2. 改ざん不可能な記録：出力判定プロセスを匿名化し，検証可能な形でブロックチェーンに記録・公開．
3. 市民と監査機関による検証：悪用・乱用を防ぎ，信頼性を確保．

適切な管理には正確な計測が必須であり，民主主義においては客観的な監査が重要である．本研究の提案は，AI output の計測・記録・公開に基づく監査を実現する．このテンプレートを他の Big Data を扱う AI system に
も適用する可能性を検討し，社会実験を通じた実現可能性の検証が必要である．

謝辞

研究の実施にあたり，2021 年度科学研究費助成事業　国際共同研究加速基金（国際共同研究強化（B），課題番号：21KK0080）の助成を受けました．また，群馬大学の太田直哉教授，Nanyang Technological University（シンガポール）の Xie Ming 准教授とは，有意義な議論をさせていただきました．ここに深い謝意を表します．

参考文献

[1] Saharnaz Dilmaghani, Matthias R. Brust, Grégoire Danoy, Natalia Cassagnes, Johnatan Pecero, Pascal Bouvry, "Privacy and Security of Big Data in AI Systems: A Research and Standards Perspective", Proceedings of 2019 IEEE International Conference on Big Data (Big Data), December 2019, Los Angeles, CA, USA.
https://doi.org/10.1109/BigData47090.2019.9006283

[2] Bernd Carsten Stahl, Laurence Brooks, Tally Hatzakis, Nicole Santiago, David Wright, "Exploring ethics and human rights in artificial intelligence – A Delphi study", Technological Forecasting and Social Change, Vol.191, 122502, 2023. https://doi.org/10.1016/j.techfore.2023.122502

[3] A. Luusua, J. Ylipulli, M. Foth, et al., "Urban AI: understanding the emerging role of artificial intelligence in smart cities", AI & Soc, Vol.38, pp.1039–1044, 2023. https://doi.org/10.1007/s00146-022-01537-5
[4] S. Sherman, "The Polyopticon: a diagram for urban artificial intelligences", AI & Soc, Vol.38, pp.1209–1222, 2023. https://doi.org/10.1007/s00146-022-01501-3
[5] G. Paltieli, "The political imaginary of National AI Strategies", AI & Soc, Vol.37, pp.1613–1624, 2022. https://doi.org/10.1007/s00146-021-01258-1
[6] R. Eglash, M. Nayebare, K. Robinson, et al., "AI governance through fractal scaling: integrating universal human rights with emergent self-governance for democratized technosocial systems", AI & Soc, 2024. https://doi.org/10.1007/s00146-024-02029-4
[7] Y. Fujii, "Verifiable record of AI output for privacy protection: public space watched by AI-connected cameras as a target example", AI & Society, 2024.
https://doi.org/10.1007/s00146-024-02122-8
[8] Y. Fujii, N. Yoshiura, N. Ohta, A. Takita, H. Ueda and K. Maru, "Abuse Prevention of Street Camera Network by Browsing-History Disclosure", Journal of Community Informatics, Vol.12, No.1, pp.152-156, 2016. https://openjournals.uwaterloo.ca/index.php/JoCI/article/view/3216
[9] Y. Fujii and N. Yoshiura, "Will every streetlight have network cameras in the near future?", SCIENCE, eLetters (21 October 2016). http://science.sciencemag.org/content/347/6221/504/tab-e-letters
[10] Paul Bischoff, "Surveillance camera statistics: which cities have the most CCTV cameras?", Comparitech (last viewed on 2nd Sep. 2024). https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/
[11] Dave Gershgorn, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space", Medium (last viewed on 2nd Sep. 2024). https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-spaceddc22d63e015
[12] Abdul Majeed, Seong Oun Hwang, "Differential Privacy and k-Anonymity-Based Privacy Preserving Data Publishing Scheme With Minimal Loss of Statistical Information", IEEE Transactions on Computational Social Systems, Vol.11, No.3, pp.3753-3765, 2024. https://ieeexplore.ieee.org/document/10275805
[13] Mohammed Khader, Marcel Karam, "Assessing the Effectiveness of Masking and Encryption in Safeguarding the Identity of Social Media Publishers from Advanced Metadata Analysis", Data, Vol.8, No.6, 105, 2023. https://doi.org/10.3390/data8060105
[14] Saranya A., Subhashini R., "A systematic review of Explainable Artificial Intelligence models and applications: Recent developments and future trends", Decision Analytics Journal, Vol.7, 100230, 2023. https://doi.org/10.1016/j.dajour.2023.100230
[15] Tobias Eichinger, Axel Küpper, "On data minimization and anonymity in pervasive mobile-to-mobile recommender systems", Pervasive and Mobile Computing, Vol.103, 101951, 2024.
https://doi.org/10.1016/j.pmcj.2024.101951
[16] Roger Clarke, "Data retention as mass surveillance: the need for an evaluative framework", International Data Privacy Law, Vol.5, No.2, pp.121–132, 2015. https://doi.org/10.1093/idpl/ipu036
[17] Dimitris Potoglou, Fay Dunkerley, Sunil Patil, Neil Robinson, "Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study", Computers in Human Behavior, Vol.75, pp.811-825, 2017. https://doi.org/10.1016/j.chb.2017.06.007
[18] Hannah Carnegy-Arbuthnott, "Privacy, Publicity, and the Right to Be Forgotten", Journal of Political Philosophy, Vol.31, No.4, pp.494-516, 2023. https://doi.org/10.1111/jopp.12308
[19] Ben Saunders, "Opt-out, mandated choice and informed consent", Bioethics, Vol.37, No.9, pp.862868, 2023. https://doi.org/10.1111/bioe.13228
[20] Haifei Ma, Canlong Zhang, Yifeng Zhang, Zhixin Li, Zhiwen Wang, Chunrong Wei, "A review on video person re-identification based on deep learning", Neurocomputing, Vol.609, 128479, 2024. https://doi.org/10.1016/j.neucom.2024.128479
[21] Sani Abba, Ali Mohammed Bizi, Jeong-A Lee, Souley Bakouri, Maria Liz Crespo, "Real-time object detection, tracking, and monitoring framework for security surveillance systems", Heliyon, Vol.10, No.15, e34922, 2024.
https://doi.org/10.1016/j.heliyon.2024.e34922
[22] Md. Muktadir Mukto, Mahamudul Hasan, Md. Maiyaz Al Mahmud, Ikramul Haque, Md. Ahsan Ahmed, Taskeed Jabid, Md. Sawkat Ali, Mohammad Rifat Ahmmad Rashid, Mohammad Manzurul Islam,

Maheen Islam, "Design of a real-time crime monitoring system using deep learning techniques", Intelligent Systems with Applications, Vol.21, 200311, 2024. https://doi.org/10.1016/j.iswa.2023.200311
[23] Dan Xu, Yan Yan, Elisa Ricci, Nicu Sebe, "Detecting anomalous events in videos by learning deep representations of appearance and motion", Computer Vision and Image Understanding, Vol.156, pp.117127, 2017. https://doi.org/10.1016/j.cviu.2016.10.010
[24] G. Sreenu, M. A. Saleem Durai, "Intelligent video surveillance: a review through deep learning techniques for crowd analysis", Journal of Big Data, Vol.6, 48, 2019. https://doi.org/10.1186/s40537-019-0212-5
[25] Seokki Cha, "Towards an international regulatory framework for AI safety: lessons from the IAEA's nuclear safety regulations", Humanities and Social Sciences Communications, Vol.11, 506, 2024. https://doi.org/10.1057/s41599-024-03017-1
[26] Olivia J. Erdélyi, Judy Goldsmith, "Regulating artificial intelligence: Proposal for a global solution", Government Information Quarterly, Vol.39, No.4, 10174, 2022.
https://doi.org/10.1016/j.giq.2022.101748
[27] NIST-Artificial intelligence (last viewed on 2nd Sep. 2024). https://www.nist.gov/artificial-intelligence
[28] N. Emery-Xu, R. Jordan, R. Trager, "International governance of advancing artificial intelligence", AI & Soc, 2024. https://doi.org/10.1007/s00146-024-02050-7
[29] European AI Office (last viewed on 2nd Sep. 2024). https://digital-strategy.ec.europa.eu/en/policies/ai-office
[30] J. Laux, "Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act", AI & Soc, 2023. https://doi.org/10.1007/s00146-023-01777-z
[31] Carolyn Cordery, Bimal Arora, Melina Manochin, "Public sector audit and the state's responsibility to 'leave no-one behind': The role of integrated democratic accountability", Financial Accountability & Management, Vol.39, No.2, pp.304-326, 2022. https://doi.org/10.1111/faam.12354
[32] Huishui Su, Yu Lu, Oleksii Lyulyov, Tetyana Pimonenko, "Good Governance within Public Participation and National Audit for Reducing Corruption", Sustainability, Vol.15, No.9, 7030, 2023. https://doi.org/10.3390/su15097030
[33] NIST, "Guidelines on firewalls and firewall policy", NIST SP 800-41 (last viewed on 2nd Sep. 2024).
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-41r1.pdf
[34] Iqra Sadia Rao, M. L. Mat Kiah, M. Muzaffar Hameed, Zain Anwer Memon, "Scalability of blockchain: a comprehensive review and future research direction", Cluster Computing, Vol.27, pp.5547-5570, 2024. https://doi.org/10.1007/s10586-023-04257-7
[35] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, Shahbaz Khan, "A review of Blockchain Technology applications for financial services", BenchCouncil Transactions on Benchmarks, Standards and Evaluations, Vol.2, No.2, 100073, 2022. https://doi.org/10.1016/j.tbench.2022.100073
[36] Francesco Fuso Nerini, Mariana Mazzucato, Johan Rockström, Harro van Asselt, Jim W. Hall, Stelvia Matos, Åsa Persson, Benjamin Sovacool, Ricardo Vinuesa, Jeffrey Sachs, "Extending the Sustainable Development Goals to 2050 — a road map", Nature, Vol.630, pp.555-559, 2024. https://www.nature.com/articles/d41586-024-01754-6
[37] B. Arogyaswamy, "Big tech and societal sustainability: an ethical framework", AI & Soc, Vol.35, pp.829–840, 2020. https://doi.org/10.1007/s00146-020-00956-6
[38] Liesbet van Zoonen, "Privacy concerns in smart cities", Government Information Quarterly, Vol.33, No.3, pp.472-480, 2016.
https://doi.org/10.1016/j.giq.2016.06.004
[39] Huan Liu, Kai Li, Yan Chen, Xin (Robert) Luo, "Is personally identifiable information really more valuable? Evidence from consumers' willingness-to-accept valuation of their privacy information", Decision Support Systems, Vol.173, 114010, 2023. https://doi.org/10.1016/j.dss.2023.114010
[40] Hitmi Khalifa Alhitmi, Alin Mardiah, Khalid Ibrahim Al-Sulaiti, Jaffar Abbas, "Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions", Cogent Business & Management, Vol.11, No.1, 2393743, 2024. https://doi.org/10.1080/23311975.2024.2393743

[41] Justin Delfino, "AI-driven Research and Development: A paradigm shift in innovation", R&D World (last viewed on 2nd Sep. 2024). https://www.rdworldonline.com/ai-driven-research-and-development-a-paradigm-shift-in-innovation/ [42] Tanja Sophie Gesk, Michael Leyer, "Artificial intelligence in public services: When and why citizens accept its usage", Government Information Quarterly, Vol.39, No.3, 101704, 2022. https://doi.org/10.1016/j.giq.2022.101704
[43] Hartwig Pautz, "Policy making and artificial intelligence in Scotland", Contemporary Social Science, Vol.18, No.5, pp.618–636, 2023.
https://doi.org/10.1080/21582041.2023.2293822

藤井雄作 FUJII, Yusaku
群馬大学大学院理工学府

1989 年 3 月東京大学工学部船舶工学科卒業，1991 年 3 月東京大学大学院工学系研究科修士課程修了．2001 年東京大学より博士（工学）の学位修得．1991 年 4 月川崎製鉄株式会社入社，工業技術院計量研究所，産業技術総合研究所 を経て，現在，群馬大学大学院理工学府教授．2004 年より NPO 法人 e 自警ネットワーク研究会理事長．社会安全工学，知能計測工学，空気感染症対策（ロックダウン代　替手段としての電動ファン付き呼吸保護具「自由外出マスク」），防犯カメラシステム（プライバシー保護機能付き公共空間街路カメラシステム「e 自警ネットワーク」），精密計測，光波干渉計などが専門．