

# 職場における監視の背景とその影響

ELSIフォーラム 2024

2025.01.24

カテライ アメリア



大阪大学 社会技術共創研究センター

Research Center on Ethical, Legal and Social Issues

# 職場における監視の 背景とその影響

# 職場における監視のルーツ

職場へのAIの「侵入」は1890年代から20世紀初頭に確立された**産業労働搾取の古い慣行への回帰**として理解されるべき

## 第一波：「コントロールの危機」への（初期的）対応

- 工場の機械化により、雇用主は工場現場のスピードに追いつく情報処理の導入を必要とし、**監視の方法も変わった**
- Frederick Winslow Taylor：労働者を「労働者」と「監視者」に分け、**効率性を高めるために、労働者の細やかな動作を分析**
- → 「監視されていない労働者は非効率的な労働者」と主張

## 第二波：コンピューターの導入により、デジタル監視の普及 → テクノストレスの一般化

## 第三波：リモートワークの普及により、収集されるデータ種目の拡大

# コントロール危機の解決策としてのテクノロジー導入

## 後期資本主義の主要な特徴：

新自由主義的な職場におけるデジタル監視措置の普及により、  
労働プロセスの質的特徴が根本的に侵食された

- 1980年代から、職場におけるデジタル技術の導入を「トロイの木馬」として問題視された

→ デジタル技術は効率性を高めたり、退屈な要求や作業から労働者を解放したりするのではなく、**労働過程における労働者の更なる搾取につながる**

→ **労働者がテクノロジーを「活用」するのではなく、テクノロジーが労働者を「活用」して、生産性と利益の向上を図る**

# 職場における監視の影響

仕事満足度の低下

プライバシー侵害

ストレスの増加

信頼の低下

組織への  
コミットメントの  
低下

離職率の増加

抵抗や非生産的な  
労働行動の増加

手続き的・分配的  
不正義

自律性の低下

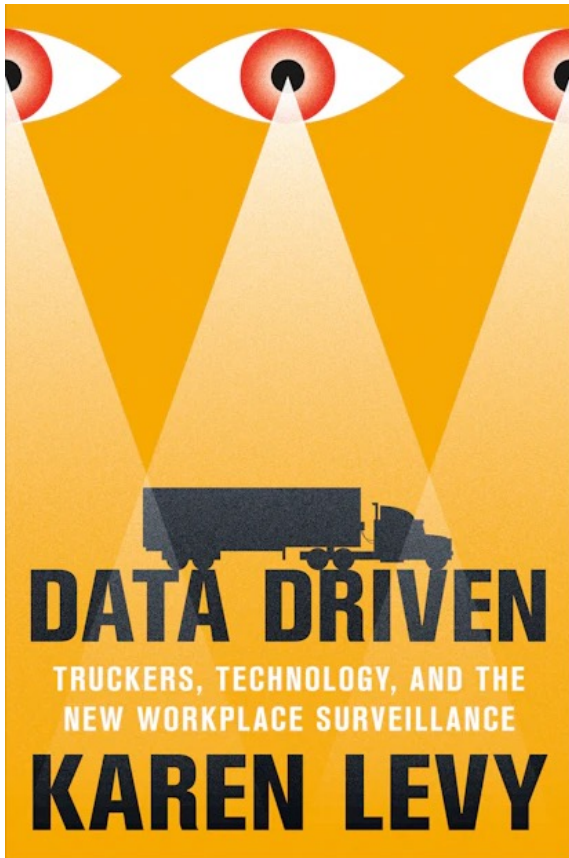
創造性の低下

労働者のパフォーマンス、価値観、社内文化への影響により、  
企業にも悪影響を及ぼす可能性も

# 心理社会的リスク要因

- **侵襲的とみなされる手法に基づいた監視**
  - 特定の個人やグループに関する情報が比較的多く収集されている場合
  - 労働者の思考・感情・生理機能を対象とするテクノロジーの場合
  - 労働者自身によるデータへのアクセスが制限されている場合
- **信頼されているという感覚を損なう監視**  
(信頼 = 能力 + 善意 + 誠実さ)
  - 監視されていることを信頼されていないことの証と捉えられる可能性がある
  - → 能力・組織に対するコミットメント (善意) ・誠実さが問われていると思われる
- **技術のデザイン** (意図されないデータも収集される場合など)
- **ファンクション・クリープ** (目的外利用)
- **職業上の自主性を侵害する監視**
- **透明性及び開放性に欠けている監視**
- **経営層からの支持の欠如**
- **差別的なアウトカム**
- **手続き上の不公平性**
- **感情労働** (感情のコントロール等が強いられる場合)
- **監視に対する怒りの反応を引き起こす性格特性**

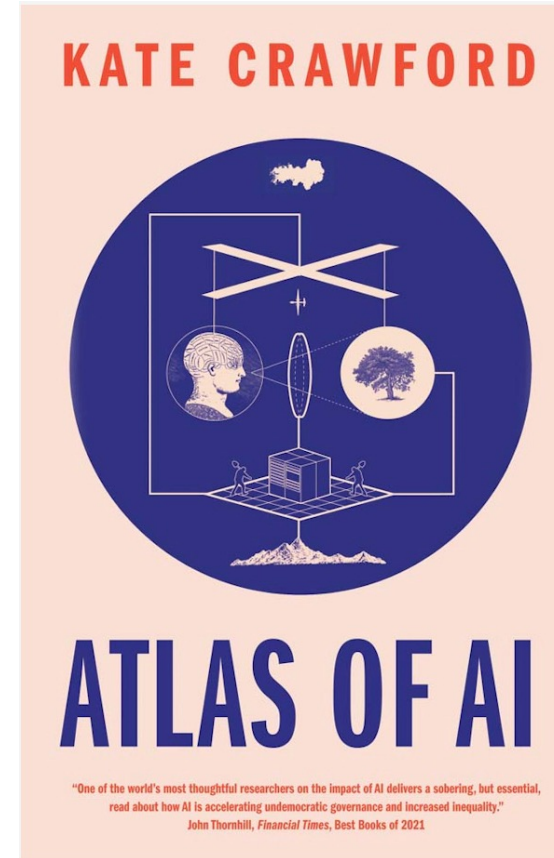
# Workplace surveillanceの事例



2022年  
Karen Levy

准教授@  
Cornell University

社会科学的研究により、米国のトラック運転手の業務に導入されている監視手法の影響を研究



2021年  
Kate Crawford

教授@USC  
Senior Principal  
Researcher @ Microsoft  
Research

AIの複数の社会的課題を包括的に議論  
→ 職場への監視の導入のインパクトについても議論

# Levy (2022) : 電子ログ装置の事例 (米国)

- **背景①**トラック運転手に危険を伴う長時間勤務が余儀なくされていた
- **背景②**紙媒体で管理されていた運転記録の改ざんが見られたことが問題視された
- **Electronic logging device (ELD、電子ログ装置)** が導入された
  - トラック運転手の勤務時間を自動的に記録し、指定の勤務時間を超過することを制限する
- **ELDの導入が安全性の向上に繋がらなかったことが明らかになった**
  - トラックの事故数が減少することもなく、小型キャリアの事故数が増加した
  - ELD導入が義務付けられた初年度は、一般車両の死亡事故が減少した年であったにもかかわらず、大型トラック事故による死亡者数は30年ぶりの高水準に達した
- → **トラック運転手の自立性が制限され、監視されていることや新たな時間的制限による精神的苦痛といった課題も浮上した**



# Crawford (2021) : Amazon社の事例

Amazon社の倉庫では、効率を向上させるために監視技術が導入されている

- **Picking rate** (割り当てられた時間内に梱包すべき品目の数) を満たさなければならないと、従業員にプレッシャーがかかる
- **身体的負傷**も → 労働者のけがが増加し、対応するためにアマゾン倉庫内の自動販売機で痛み止めが従業員に提供される

ロボットが人間にとって代わるかどうかではなく、人間がいかにしてロボットのように扱われるようになっていくのか？

- 従業員追跡技術の導入が、米国Amazon社における最大の労働組合の設立運動につながった

'Lack of respect': outcry over Amazon employee's death on warehouse floor

Work carried on as usual in the facility as workers were not informed of colleague's death even as the body lay on the floor

Michael Sainato

Mon 9 Jan 2023 08:00 GMT

Share



📷 Demonstrators hold a banner during a protest against Amazon in New York in December 2019. Photograph: Bloomberg/Getty Images

「遺体が床に横たわっていても従業員らは同僚の死亡を知らされず、倉庫内では通常通り作業が行われていた」

# 事例

顔認証技術などを用いた監視技術の課題

# 労働者の人権へのインパクト

## 顔認証技術を用いた監視技術の職場での実装

- 労働者の自己決定、自主性、選択の可能性、信頼に悪影響を及ぼす
- 最終的には組織全体の生産性にも悪影響を及ぼす
- 労働者の人権及び尊厳を脅かす
- 「テクノストレス」・「燃え尽き症候群」を増加させる
- 労働者との関係を根本的に変える → 所属組織に対するコミットメントと負の相関関係にある

**「合理的」と思われる基準を超えてしまう**

# Stark et al., 2020

- Pew Research Centerによって行われた調査の結果をもとに、職場の監視に向けた顔認識技術の活用に関する意見を分析した
- 個人の自主性、同僚・雇用主に対する信頼感を損なう
- 6つの課題を特定：

プライバシー

ファンクション・  
クリープ

予測的適合性

信頼の欠如

ストレス+仕事に  
対する不満感の  
向上

離職率の上昇

職場における監視は、既存の不平等を悪化させ、長年にわたる差別的慣行を技術的不透明さで定着させる可能性を秘めている

# Awumey et al., 2024

## 開発・実装・利用で生じる5つの 社会技術的危険

### 対人関係

- プライバシー侵害
- 自立性の欠如

### 代表性

- 多様性に未対応
- ステレオタイプ化

### 分配

- 経済的・機会的損失
- 機会の不平等

### サービス品質

- 労働の激化
- 過度の労働の要求

### 社会システム

- 情報の非対称性
- 機能不全なメンタル・モデルの形成

# リスク

- 労働者にとって、**特定の行動がシステム上どう評価されているかが不透明**であるため、危害の可能性が増す
- 既存のほとんどの活用事例では、**顔認証監視技術の限られたベネフィットは、雇用主に偏っている**  
→ 労働者のプライバシー、ウェルビーイング、雇用への公平・公正なアクセスが脅かされる
- **労働中の行為を分析しても、個人に関する機密な情報も収集されることにあたる**
  - → システム・取得データ等の目的外利用を開発段階から防ごうとしても、**ファンクション・クリープを完全に防ぐことが困難**
  - **例)** 加速度計からのデータで精神疾患や筋骨格系疾患の存在など、身体的・精神的「健康」に関する機密情報が漏洩する可能性
- 職場においては、上下関係や同調圧力の影響で、**自由に同意することは困難である**ため、従業員は「脆弱」な対象者とみなされている

# 対処の可能性？

- 課題への対処が困難な場合も多い

- 透明性の向上が求められる

法的保護のメカニズムがなく、ほとんどの労働者にはデータがどう収集され、どう活用されているかがわからない

- 当事者参画の重要性

システムのデザイン・開発・学習・実装を通して、労働者の声を反映すべきである

# 参考文献

- Awumey E, Das S and Forlizzi J (2024) A Systematic Review of Biometric Monitoring in the Workplace: Analyzing Socio-technical Harms in Development, Deployment and Use. In: *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, Rio de Janeiro Brazil, 3 June 2024, pp. 920–932. ACM. Available at: <https://dl.acm.org/doi/10.1145/3630106.3658945> (accessed 8 July 2024).
- Ball K (2021) Electronic monitoring and surveillance in the workplace. *European Commission Joint Research Centre*. Epub ahead of print 2021.
- Crawford K (2021) *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven: Yale University Press.
- Ho M-T, Mantello P, Nguyen H-KT, et al. (2021) Affective computing scholarship and the rise of China: a view from 25 years of bibliometric data. *Humanities and Social Sciences Communications* 8(1): 282.
- Ienca, M., Malsiner, G., 2022. Mental data protection and the GDPR. *J. LAW Biosci.* <https://doi.org/10.1093/jlb/lfac006>
- Levy K (2022) *Data driven: truckers, technology, and the new workplace surveillance*. Princeton University Press. Epub ahead of print 2022.
- Mantello P, Ho M-T, Nguyen M-H, et al. (2021) Bosses without a heart: socio-demographic and cross-cultural determinants of attitude toward Emotional AI in the workplace. *AI & SOCIETY*. Epub ahead of print 6 November 2021. DOI: 10.1007/s00146-021-01290-1.
- Mettler T (2023) The connected workplace: Characteristics and social consequences of work surveillance in the age of datification, sensorization, and artificial intelligence. *Journal of Information Technology*. 02683962231202535.
- Stark L, Stanhaus A and Anthony DL (2020) “I don’t want someone to watch me while I’m working”: Gendered views of facial recognition technology in workplace surveillance. *Journal of the Association for Information Science and Technology* 71(9). Wiley Online Library: 1074–1088.



# 付録

# A Systematic Review of Biometric Monitoring in the Workplace: Analyzing Socio-technical Harms in Development, Deployment and Use

Ezra Awumey

eawumey@andrew.cmu.edu  
Human-Computer Interaction  
Institute, Carnegie Mellon University  
Pittsburgh, Pennsylvania, USA

Sauvik Das

sauvik@cmu.edu  
Human-Computer Interaction  
Institute, Carnegie Mellon University  
Pittsburgh, Pennsylvania, USA

Jodi Forlizzi

forlizzi@cs.cmu.edu  
Human-Computer Interaction  
Institute, Carnegie Mellon University  
Pittsburgh, Pennsylvania, USA

*Fairness, Accountability, and Transparency (FAccT '24), June 03–06, 2024, Rio de Janeiro, Brazil.* ACM, New York, NY, USA, 13 pages. <https://doi.org/10.1145/3630106.3658945>

## 職場における生体認証モニタリングの体系的な文献レビュー： 開発・実装・活用における社会技術的危険の分析

- FAccT 2024にて発表（倫理を対象としたACMのカンファレンス）
- AI-BWM = AI-powered biometric work monitoring（AIを活用した生体認証による職場監視）
- 41,160件の文献から関連文献を選出
- 129件の論文を分析し、社会技術的危険を特定

社会技術的危険	開発	実装	利用
Socio-Technical Harms	Development	Deployment	Use
対人関係で生じる危険 Interpersonal Harms	<b>Privacy:</b> when sensors used in the development of AI-BWM systems leak private information about workers [Höller, 2018; Kröger, 2019; Mandal, 2022].	<b>Loss of Agency:</b> when AI-BWM systems collect sensitive information about workers to support patriarchal managerial practices [Grandinetti, 2019; Naous, 2022; Chowdhary, 2023].	<b>Privacy:</b> when workers fear that AI-BWM may disclose private information about them or be used to infer things beyond its intended purpose [Stark, 2020; Richter, 2020; Fugate, 2023].
代表性に関する危険 Representative Harms	<b>Reifying Essentialist Categories:</b> when datasets are unsuitable for creating deployable AI-BWM technologies used on diverse populations [Merone, 2017; Bisogni, 2022; Kang 2023].	<b>Stereotyping:</b> when AI-BWM is used to categorize workers into ideal and underperforming groups (e.g. healthy or unhealthy) [Esmonde, 2021; Mettler 2022; Roemmich, 2023a].	<b>Alienation:</b> when workers report low alignment of reported internal states, and the assessments of AI-BWM systems [Kaur, 2022].
分配で生じる危険 Allocative Harms	<b>Economic and Opportunity Loss:</b> when AI-BWM systems are designed without consideration of how they might be used to disadvantage or deny resources to certain groups [Kaur, 2022; Boyd, 2023].	<b>Economic and Opportunity Loss:</b> when managers deny workers opportunities for failing to meet requirements set by AI-BWM systems [Ajunwa, 2019; Watkins, 2020].	<b>Alienation:</b> when workers are denied opportunities given to other workers based on the evaluations and predictions of AI-BWM technology [Mantello, 2021].
サービス品質で生じる危険 Quality of Service Harms	<b>Labor Intensification:</b> when AI-BWM systems are designed to narrowly target certain worker behaviors and metrics indicative of their performance [Boyd, 2023; Howell, 2023].	<b>Alienation:</b> when managers use AI-BWM systems to demand additional labor or challenge workers' accounts of their own work [Levy, 2015; Roemmich, 2023b].	<b>Labor Intensification:</b> when workers feel compelled to modify their behavior to avoid unfavorable evaluations from AI-BWM systems [Howell, 2023; Roemmich, 2023b.]
社会システムで生じる危険 Social System Harms	<b>Information Asymmetry:</b> when AI-BWM systems are not designed to provide equal benefit (information) to both employers and workers [Vatcha, 2020].	<b>Information Asymmetry:</b> when management does not share or clearly communicate the information generated by AI-BWM systems with workers [Greene, 2023].	<b>Erroneous Information:</b> when workers develop dysfunctional mental-models regarding the purposes of AI-BWM use [Carpenter, 2016; Fugate, 2023].

社会技術的危険	開発	実装	利用
対人関係で生じる危険	<p><b>プライバシー侵害</b></p> <p>開発過程で使用されるセンサー等で労働者の<b>機密情報</b>が取得される</p>	<p><b>自立性の欠如</b></p> <p>家父長制的な管理慣行を支持するために労働者に関する<b>機密情報</b>が取得される</p>	<p><b>プライバシー侵害</b></p> <p>AI-BWMが機密情報を漏らしたり、<b>本来の目的を超えた事柄を推測するために</b>使用される</p>
代表性に関する危険	<p><b>本質主義を反映するカテゴリーの具体化</b></p> <p>多様性に対応していない<b>データセット</b>が用いられる</p>	<p><b>ステレオタイプ化</b></p> <p>AI-BWMを用いて、労働者を「理想的な」「劣っている」などの<b>カテゴリーに分類する</b></p>	<p><b>疎外 (Alienation)</b></p> <p>内心の状態とAI-BWMによる評価の<b>整合性の低さ</b></p>
分配で生じる危険	<p><b>経済的・機会的損失</b></p> <p>システムは、<b>特定のグループに不利益をもたらされる可能性</b>について考慮されずに設計される</p>	<p><b>経済的・機会的損失</b></p> <p>労働者がシステムによって設定された要件を満たさないため<b>機会の提供が拒否される</b></p>	<p><b>疎外 (Alienation)</b></p> <p>AI-BWMの評価と予測に基づいて、<b>他の労働者に与えられる機会等が与えられない</b></p>

社会技術的危険	開発	実装	利用
サービス品質で生じる危険	<p><b>労働の激化</b></p> <p>システムは、特定の行為や指標を限定的に対象とするように設計される</p>	<p><b>疎外</b></p> <p>過度の労働を要求したり労働者自身の労働に対する認識を否定するためにシステムが（経営者によって）利用される</p>	<p><b>労働の激化</b></p> <p>AI-BWMからの不利な評価を避けるために労働者に行動変容が強いられる</p>
社会システムで生じる危険	<p><b>情報の非労働者</b></p> <p>AI-BWMは、雇用主と労働者に同等の利益・情報を提供するように設計されていない</p>	<p><b>情報の非対称性</b></p> <p>経営層は、AI-BWMによって生成された情報を労働者に明確に共有したり、伝えたりしていない</p>	<p><b>誤情報</b></p> <p>労働者がAI-BWMの使用目的に関する機能不全なメンタル・モデルを持つ</p>