# 職場における監視にまつわる倫理的な課題

長門裕介
社会技術共創研究センター実践研究部門・特任助教（常勤）

# 職場監視とホワイトカラー労働の変化

- **生産性向上のため、AIや顔認証などを利用した職場監視技術に多くの期待が寄せられている**
  - 特にコロナ禍以降、ホワイトカラーに対しても大規模に導入されている
  - キー入力や作業画面のスクリーンショットなどを送信し、自動で判定する
- **ほとんどの管理職はハイブリッドワークで生産性が向上すると信じていない***
  - 労働時間、ミーティングの数、メールのやり取りといったアクティビティ指標が増加していても生産性に不安がある
  - ホワイトワーカーが初めて体験する強度の職場監視

(*Microsoft’s 2022 Work Trend Index)

# 法的な議論：職場監視と正当な目的

- 施設管理や勤務状況を把握する目的でカメラを設置することやGPSでのモニタリングは正当であると考えられることが多い*
- 組合活動を委縮させる目的での監視やたんなる好奇心で従業員のメールを閲覧することは逸脱・濫用とみなされる可能性もある**
- キーロガーやスクリーンキャプチャー、内蔵カメラの遠隔操作といった新しいモニタリング手法については議論が継続中
  - 英国ICOのガイドラインはさしあたり参考になる（付録）

(*大谷 2018, **尾崎 2023)

# 実証研究：どれくらいの効果があるのか？*

- **監視でのパフォーマンス向上はさほど期待できないかもしれない**
  - 生産性向上という一般的な期待に反し、パフォーマンスへの有意な効果なし (r = -0.01)*
  - 向上したケースでは業績評価と組み合わせているケースが大きい
- **負の影響が（若干）発生しているかもしれない**
  - 仕事満足度の低下(r = -0.10)は、監視が従業員の自律性と職務コントロール感を損なうことを示唆
  - ストレスの増加(r = 0.11)は、常時監視される心理的プレッシャーと関連
  - 反生産的な職場行動の増加(r = 0.09)は、監視への反発として解釈可能

(*Siegel 2022)

# 議論：メタアナリシスの結果をどう見るか

- 勤務状況を把握するという目的があり、満足度の低下やストレスの発生もさほどではないなら、導入するメリットはともかく差し控えるほどの問題もないのでは？
- 昇進昇給と結びつけるとパフォーマンスは向上するが、勤怠管理や防犯といった目的から逸脱するというジレンマがあるのでは？
- 有色人種やトランスジェンダー、非組合員といった従来疎外されてきた労働者には負の影響が大きいのでは？

# 議論：プライバシーに絞りすぎない方がいい？

- **自動化されたシステムによる大規模監視は、プライバシーの侵害にはあたらない*（？）**
  - プライバシーを「アクセス説」の立場から捉える（情報へのアクセスがあって初めてプライバシー侵害となる）と自動システムはプライバシー侵害の主体とはなり得ない
- **プライバシー侵害の有無に注目するのではなく、委縮効果や自律性の低下、社会的信頼の低下などに注目すべき**

(*Macnish 2020)

# 提案：職場文化への影響を考えよう

- **監視が組織文化に与える影響は個人の行動変容にとどまらない***
  - 相互信頼に基づく関係から、監視と確認に基づく関係へと変化
  - 水平的監視（peer surveillance）によるチーム内の緊張関係の増加
  - 監視によって、非公式なコミュニケーションが減少
- **労働者間の連携を破壊することそのものの倫理的問題**
  - 古典的な職場監視が組合監視でもあったことを考えるべき
  - 職場民主主義といった労働についての新しい議論からもアプローチできる
  - 「自分たちのやり方」からの疎外：そもそもブルーワーカーの間ではこうした問題は早くから知られていたのでは？

(*Kayes 2023)

# 文献表




- Kayas, O. G. (2023). Workplace surveillance: A systematic review, integrative framework, and research agenda. *Journal of Business Research*, 168, 114212.
- Macnish, K. (2020). Mass surveillance: A private affair?. *Moral Philosophy and Politics*, 7(1), 9-27.
- Microsoft. (2022). 2022 Work Trend Index: Annual Report. Microsoft.
- Siegel, R., König, C. J., & Lazar, V. (2022). The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis. *Computers in Human Behavior Reports*, 8, 100227.
- 大谷卓史. (2017). 「ICTによる人事・労務管理とその規制―日本及び海外における現状―」.『人工知能・ロボットと労働・雇用をめぐる視点（平成29年度　科学技術に関する調査プロジェクト）』国立国会図書館, 105-108.
- 尾崎愛美. (2023). 「モニタリングとHRテクノロジー」山本龍彦、大島義則編『人事データ保護法入門』勁草書房, 56-69.

# 非従来型のケースに関するICOの取り組み

- Non-traditional in this case means - analysing the text of emails and social-media messages, scrutinising who’s meeting with whom, gathering biometric data and understanding how employees are utilising their workspace

# Can we use biometric data for time and attendance control and monitoring？

- 生体データの処理（例えば、労働者の指紋を使用して職場にアクセスできるようにする）は、労働者に職場へのアクセスを与える便利な方法であるが、データ保護の権利と自由および労働者と雇用者の間の信頼 関係にリスクをもたらす可能性がある。従って、従業員のバイオメトリクス情報の処理には慎重な検討が必要である。また、バイオメトリックデータの処理には、パスワードとは異なり、侵害された場合にリセットできないため、より高い被害のリスクが伴うため、バイオメトリックデータを保存する際に特別なセキュリティ対策が必要かどうかを検討する必要がある。

# Can we use biometric data for time and attendance control and monitoring？

- ワークスペースへのアクセスを顔認証に依存する場合、同意していない労働者のために別のアクセスなど、生体データの処理を伴わない代替手段が必要である。これは労働者に不利にならないようにしなければならない。例えば、生体データオプションを使用しないことを選択した人が、さらに歩く必要がある場合である
- バイオメトリクス情報処理の同意が提供されたかどうかに関係なく、システムがすべての労働者をスキャンする場合、これは同意していない労働者のバイオメトリクス情報の処理を含むことになる。これは、同意していない人のデータを処理するための合法的な根拠がないため、違法となる

# Can we use biometric data for time and attendance control and monitoring？

- 顔認証は、一部の人口層に対しては精度が低く機能することが、数多くの研究で示されている。英国のGDPRの公平性の原則を遵守するためには、システムの偏りを評価し、軽減する必要がある。システムの提供を別の組織に依頼している場合は、そのシステムが使用予定のグループや個人に適していることを確認する必要がある。使用するシステムが偏見や差別を引き起こす処理につながる場合、英国GDPRの公平性の原則に違反することになる。

# Can workers object to the use of biometric data for access control?

- **労働者は、雇用主が依拠する法的根拠が以下のものである場合、勤怠関連の目的のために生体データを使用することに異議を唱えることができる。**
  - 公共的な業務（公共の利益のために行われる業務の遂行）。
  - 公的な業務（雇用主に与えられた公的な権限の行使のため）
  - 正当な利益
- **同意に頼る場合、労働者は拒否することができ、労働者に不利益を与えない代替案を提供されるべきである。**

# （付録）ICO Employment practices guidance draft (2023)



- ☐ 私たちは、より侵入性の低い手段を用いない理由についての考察を含め、バイオメトリクス情報に依存する根拠を文書化した。
- ☐ 私たちは、必要に応じて、合法的な根拠と特別なカテゴリー条件を特定している。
- ☐ DPIAを実施した。
- ☐ DPIAでは、労働者と協議をした。
- ☐ 同意に依拠する場合、個人データの処理に同意していない労働者に対しては、認証または本人確認のための代替方法を導入している。
- ☐ 正確性と公平性を考慮し、特定されたリスクは軽減している。
- ☐ 自動化された意思決定に関連する権利について検討した。
- ☐ バイオメトリクス情報を入退室管理に利用することについて、労働者に周知している。
- ☐ アクセスコントロールのための生体データの使用に異議を唱える労働者の権利について検討した。
- ☐ 私たちは、私たちが処理するあらゆるバイオメトリックデータのセキュリティを保護するために、適切な組織的および技術的措置があることを保証している。

☐ We have documented our evidence base for relying on biometric data, including our consideration of why we are not using less intrusive means.

☐ We have identified a lawful basis and a special category condition where necessary.

☐ We have carried out a DPIA.

☐ We have discussed the proposed monitoring with workers during our DPIA.

☐ Where consent is relied on, we have put in place alternative methods for authentication or identification for workers who have not given their consent to the processing of their personal information.

☐ We have made manual reviews available for any workers having issues with access denial due to

October 2023 - 1.0.0

automatic errors.

☐ We have considered whether further security measures are required when processing biometric data.

☐ We have considered accuracy and fairness. We have mitigated any identified risks.

☐ We have considered the rights of individuals relating to automated decision-making.

☐ We have informed workers about the use of their biometric data for access control.

☐ We have considered workers' rights to object to the use of biometric data for access control.

☐ We have ensured there are appropriate organisational and technological measures to protect the security of any biometric data we process.

# ICO Employment practices guidance: Monitoring at work Impact scoping document

## Impact scoping

The table below outlines some of the potential impacts (benefits and costs) we have considered on each of the affected groups. This is not an exhaustive list, and it does not imply any hierarchy of impacts considered. We have not yet considered the likelihood or magnitude of any of these impacts. Many of them may not materialise or may only impact small subsets of the affected groups.

**Table two: Potential impacts**

| Employers | Workers | ICO | Wider society |
|---|---|---|---|
| **Benefits** | | | |
| • Greater degree of regulatory certainty.<br>• Reduced potential to face regulatory action from the ICO if the guidance is followed.<br>• Higher workplace morale resulting in higher employee retention with associated productivity benefits.<br>• Improved DP compliance could lead to increased trust from consumers. | • Reduced risk of data protection harm to workers.<br>• Higher morale amongst workers. | • Gives a better position to assess compliance and take appropriate regulatory action where required.<br>• Providing guidance may help mitigate the burden of regulatory action later.<br>• Less likelihood of complaints from members of the public. | • Reduction in harms could improve overall societal welfare.<br>• Benefits to business could lead to knock-on benefits to wider society. |
| **Costs** | | | |
| • Costs of familiarisation with the guidance.<br>• Compliance costs could increase for employers that are not already compliant.<br>• Sunk costs for organisations which have invested in monitoring software that they now realise is non-compliant. | • Reduced workplace monitoring using personal data could lead to increases in other forms of monitoring (eg micromanagement). | • Reputational risk if ICO is perceived to have overreached. | • Disbenefits to business could lead to knock-on disbenefits to wider society (eg suppliers of monitoring software). |