

## 「国民ID制」は、「共通番号」とともに、憲法違反の人権侵害ツール

— 「国民ID制」について、もっと学習しよう

**民**主政権は、現在、共通番号 国民背番号 と 国民ID 国民登録証〔カード〕制の2つのツールを使ったデータ監視国家 国民情報の公有化の仕組みの構築を急いでいる。

各界へ出前レクチャーに行くと、共通番号については、何がしかの知識がある聴衆が多い。だが、国民ID制については、住基ネットに反対した人たちや弁護士などを含め、はじめて聞くという人たちが多くいる。いわば、この道のプロを含め、「国民ID制とは何か」が、わかっていない。大問題である。

「国民ID」とは何か？役人は「電子政府サービスを受ける際の電子認証カード」という。だが、すでに住基カードがあり、新たな電子認証カードなど要らない。「国民ID」とは、外国人登録証と同類、実質、国内パスポート（現代版通行手形＝内国人登録証）だ。つまり、住基ネットをベースに、国民全員に新たな背番号（共通番号）のついたIC仕様の「身分証明書（IDカード）」を持たせようというわけだ。

民主政権は、共通番号と国民IDという2つの監視ツールによって、社会保障・納税・医療など幅広く「全国民の個人情報を政府が一元管

理する体制」の確立をめざしている。この体制ができあがると、国家は、共通番号というマスターキーを使い、官民の多様なデータベースに蓄積された国民のプライバシーを、串刺しにして監視できる。「役人が主役、国民はわき役」になる。「脱官僚政治」、「国民が主役」は完全に「笑い話」である。

このように、「国家が広範な個人情報を公有化し、行政情報として管理」する。私たちは共通番号付国民IDカードを提示して、役所に自分の情報をみせてもらう立場になる。これが「電子政府」だという。だが、私たちは「国民IDカードを常時携帯・提示しないと市民生活ができないような社会」を望んでいない。

イギリスで去る5月に誕生した新連立政権は、「国家が必要以上に国民の個人情報を収集しない方針」を打ち出した。そして今前労働党政権下で導入した国民IDカード制を、「恒常的な人権侵害装置」であるとして、廃止を決定した。現在、「IDカード制廃止関連法案（政府立法案）」を議会で審議中である。

民主党がめざす共通番号（マスターキー）付国民IDカード構想は、国民の個人情報の自己コントロール権や移動の自由を侵害する憲法違反のツールといえる。憲法違反の共通番号や国民IDカードは絶対に要らない。「住基」で疲弊した市民運動家や人権活動家の人たちも、負けないで、もっと学習しよう。

- ・巻頭言～国民ID制は憲法違反の人権侵害ツール
- ・共通番号、国民ID制は要らない
- ・政府、国民ID制度導入の行程表を発表
- ・監視カメラとプライバシー
- ・イギリスの監視カメラ運用基準

# 憲法違反の危険な 「共通番号、国民ID制」は要らない

— 民主政権の個人情報データを公有化するデータ監視社会構想を斬る —

石村 耕治 (PIJ代表)

## はじめに

民主党政権は、新たな背番号（共通番号）と国民ID【国民登録証】カードの二つのツールを使った新たな「国民情報の公有化」【データ監視社会】の仕組みを構築しようとしている。

民主政権は、これら2つの監視ツールによって、「政府による全国民の個人情報の一元的管理」を目指している。言い換えると、個人の自由を尊重する政府システムとは、相容れない政策を実行しようとしている。

## 民主党政権の「データ監視国家」構想の検討組織

民主党政権は、新たな背番号（共通番号）については、平成22年2月8日に、内閣官房国家戦略室内に「社会保障・税に関わる番号制度に関する検討会（以下「戦略室共通番号制度検討会」）」を設け、着々と準備をすすめている。

一方、国民ID【国民登録証】カードについては、平成13年1月に内閣に置かれ、現在まで継続している「高度情報通信ネットワーク社会推進戦略本部（通称「IT戦略本部」）」で、仕組みづくりを進めている。国民IDカード導入構想については、あまり表面に出てきていないが、I

T戦略本部では、共通番号が導入されることを前提に検討をすすめている。

さらに、税制調査会 専門家委員会納税環境整備小委員会・三木義一小委員会座長）が、「共通番号付IDカード制導入」の翼賛役を演じている。

## 民主政権の「個人情報の公有化構想」は憲法違反

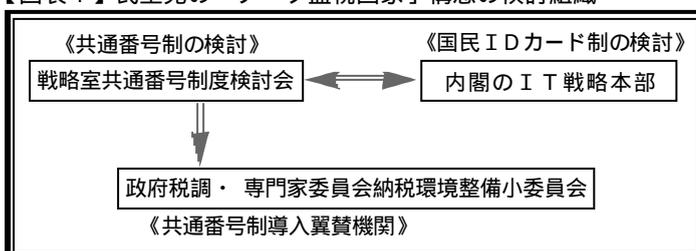
戦略室共通番号制度検討会がイメージしているのは、住基ネットを基盤にしながらも、住民票コード外の「官民にまたがり、かつ、多分野で共用する」共通番号（マスターキー）の導入である。

行政機関は、各人のマスターキーを使ってデータベース（DB）を構築し、広範な国民情報を収集・保存することになる。また、このマスターキーを、納税や社会保障などの分野で使うことになれば、民間機関も、共通番号を使ってDBを構築することになる。この結果、政府は、公権力行使の一環としてマスターキーを使えば、さまざまな行政分野のデータベース（DB）、さらには民間機関のDBに格納された広範な国民情報に容易にアクセスすることになる。

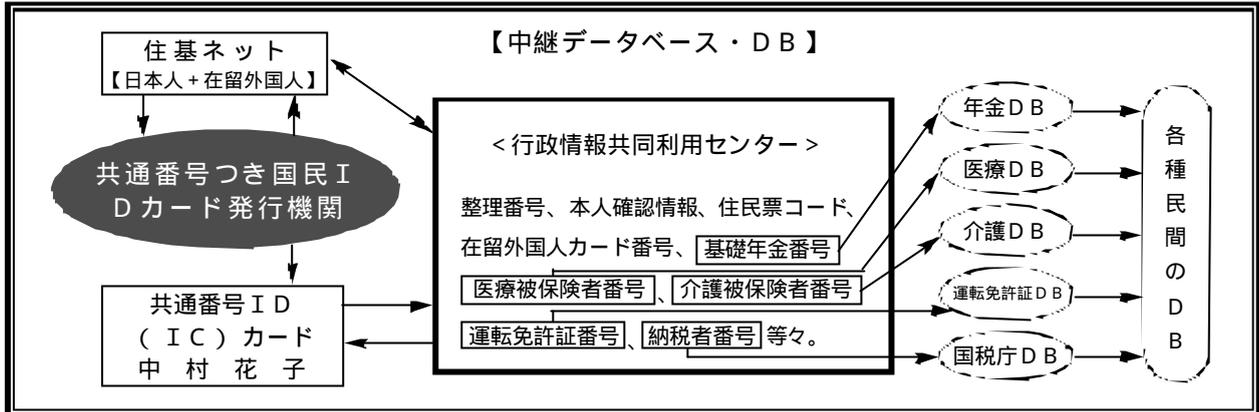
民主政権は、共通番号を使って、税、社会保障、医療、介護など多様な分野の国民の幅広い個人情報（プライバシー）を、行政や民間の多様なデータベースで分散集約管理するナショナルデータベースの構築を狙っている。つまり、共通番号は、各種データベースに入るマスターキーの役割を果たす。

この構想では、国家は、全国民の個人情報を、各人の共通番号で串刺しして、

【図表1】民主党の「データ監視国家」構想の検討組織



【図表2】共通番号つきIDカード構想のイメージ



行政情報として分散集約管理することになる。一方、国民は、行政が管理する自分の個人情報については、自分に発行された共通番号付国民ID〔カード〕を提示して見せてもらうことになる。つまり、共通番号付国民ID〔カード〕を携行しないと、行政サービスが受けづらくなるばかりか、保険診療も受けられない仕組みである。

そして、いずれは、警察官がIDカード読取機を持って巡回し、IDカードなしにはお使いにも出られない日常生活が待っている。

元財務省役人でこの構想の立役者である古川元久議員は、これを「電子政府構想」だという（日経2010年5月20日朝刊参照）。だが、わが国において、「個人情報」は個人の財産である。古川構想は、「国民のプライバシーの公有化構想」、「スーパー電子監視国家構想」そのものである。IT産業向けの新たな公共事業（公共工事）である。

また、民主政権が唱えた「国民が主役」や「地域主権」の公約にぶつかるばかりか、明らかに憲法13条〔個人の尊重〕に違反する。

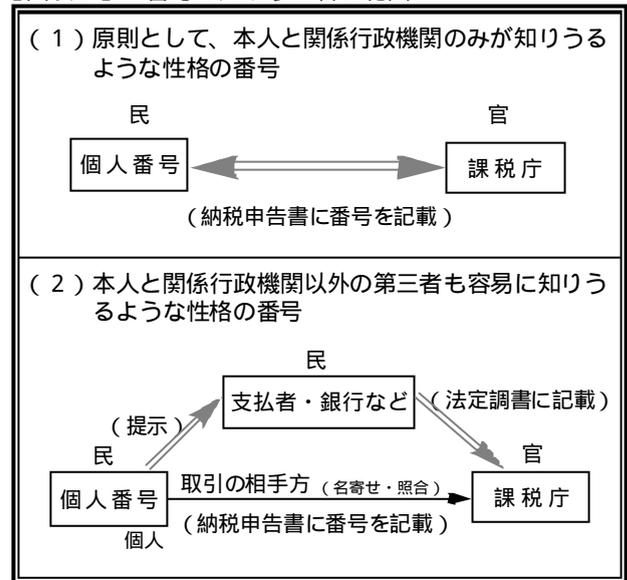
### 共通番号を「納税者番号」に使うことの意味

住基ネットで使われている住民票コードは、原則として「住民本人と行政機関のみが知りうるような性格の番号」として運用されてきている。

納税者番号（納番）制度は、納税者に重複しないかたちで番号を付け、「税の捕捉」が関係する雇用や金融取引、納税申告書や課税資料に番号をつけて課税庁に提出を求め、コンピュータで（名寄せし）集約管理する仕組みをさす。個人や事業者などすべての納税者に課税庁が付番する方式（オーストラリアなど）がある「納税者番号」に

ついて、多くの国々で採用する方式は、原則として、「納税者本人と課税庁のみが知りうるような性格の番号」である。つまり、わが国の現行の「納税者整理番号」的な性格のものである。

【図表3】番号を知りうる者の範囲



これに対して、戦略室共通番号制度検討会が導入を検討する個人用の「納税者番号（納番）」は、「納税者整理番号」をイメージしていない。「官民にまたがり、かつ、多分野で共用する」汎用の「共通番号」の導入である。給与の支払や銀行口座の開設をはじめとしたさまざまな民間取引にも使える汎用の納番の導入である。端的にいうと、「所得把握」をねらいとした納番＝共通番号である。また、課税庁などは、税務調査や名寄せ・データ照合に、各人の納番＝共通番号を頻繁に使うことを想定している。

「平成22年度税制改正大綱」が指摘するように、「一般の消費者を顧客としている小売業等に

係る売上げ（事業所得）や、グローバル化が進展する中で海外資産や取引に関する情報の把握などには一定の限界があり、番号制度も万能薬ではない」。つまり、政府自身が認めるように、納番で所得把握には限界があることは自明のところだ。むしろ、コンプライアンスコスト（納税協力費用）がかさむ懸念がある。

納番 = 共通番号の導入は、その使い方次第では、個人情報や番号情報漏えいのリスクと隣り合わせの社会をつくることになる。とりわけ、共通番号を納番（所得把握）に使うことは、共通番号を「目に見える番号（可視的な番号）」として使わざるを得ず、納番付情報が各所に垂れ流しになることは避けられない。また、ネット取引全盛の今日、ネット空間にマスターキー（納番 = 共通番号）付情報が垂れ流しになるのも必至である。

民主政権から誰一人、この危険な構想に対し異を唱えないのも異様である。かつて、民主党は、野党時代、4度も住基ネット廃止法案を出した。この政党への国民の信頼が揺らぐのも当たり前である。

### 納番なしでは「給付つき税額控除」が導入できないは「口実」

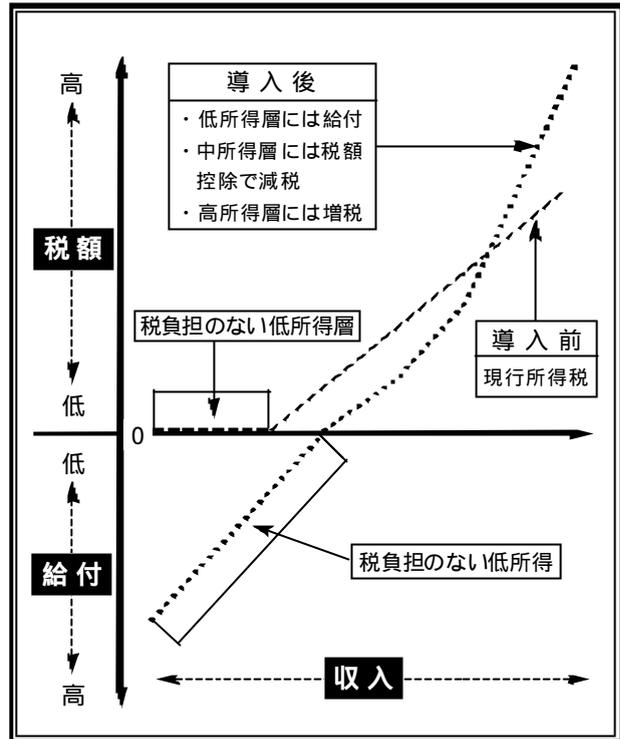
所得格差の広がりが社会問題になるなか、「税制」にこれまで社会保障で手当してきた「給付」を組み合わせ、所得の再配分機能を強める「給付（還付）つき税額控除」（refundable tax credit）を導入しようという動きが与野党に強まっている。

わが国の現行の福祉制度の下での重い課題は、生活保護などの公的扶助はおおむね働けない貧しい人を対象としていることである。言い換えると、働いても貧しい人（working poor）を支援する仕組みがうまく機能していないことである。働くよりも公的扶助を受けた方がより多くの公的生活資金（扶助）が得られ、少しでも働くと公的扶助が打ち切られてしまうことが働こうとする意欲をそいでいるとの指摘がある。

本来、「所得控除」の仕組みに比べ、「税額控除」の仕組みでは、所得の多い少ないには関係なく税額から一定額を差し引くため、低所得者に税負担軽減効果が出やすい。この税額控除の特質を活用し、社会保障（福祉）と組み合わせることで、政策を実施しようという構想である。

生活保護などの社会保障（福祉）では、働くとも給付が打ち切られてしまう。これに対して「給付（還付）つき税額控除」では、職に就き納税して

【表4】給付（還付）つき税額控除のイメージ



いながら、所得が低いために税額が一定の控除額を下回る人には控除しきれない差額分を現金で給付する仕組み。「社会保障（福祉）漬け」で生きるのではなく、「働くインセンティブ」をもって生きてもらおうという意味をもつ。

与野党ともに、「働いても貧しい人たち（ワーキング・プア）」を支援する仕組みとして、「給付（還付）つき税額控除」導入に積極的である。

給付（還付）つき税額控除は、1975年に、アメリカで、連邦所得税に勤労所得税額控除（EITC = Earned Income Tax Credit）」の名称で導入したのが最初である。その後、カナダ、アイルランド、イギリス、オランダなど他のOECD諸国などに広がった。

#### （1）「福祉」と「税制」は分離していた方がセーフティネットになる

ただ、わが国の場合、導入は多難。まず、財源の捻出に加え、既存の各種控除との調整は重い課題である。また、全員確定申告するアメリカなどと違い、職を転々とし、年末調整の適用もなく働いても貧しい500万を超える人たちに対する申告支援制度整備の課題は重い。

申告支援が十分でない、逆に、この人たちを、実質的に「切捨て、福祉ゼロ状態」に導く。過誤還付ないし不正還付があれば、この措置の適

用が認められないからである。アメリカの場合、その期間は、最長で10年にも及ぶ。

一方、課税庁の機構・サービス内容も、これら「働いても貧しい人たち」向けに大改革が必要である。まさに納税者権利憲章が必要とされるところである。

給付つき税額控除を入れても、所得のない人たち向けの生活保護は依然として必要である。結局、二重に行政サービスが必要になるわけで、給付つき税額控除をバラ色とみるのは近視眼的である。

### (2) 過誤申告、不正申告の氾濫

給付つき税額控除を実施している国では、制度の複雑さからくる過誤還付、目に余る不正還付が横行している。例えば、アメリカでは、全EITC申告の30%弱にも及ぶ(石村耕治「給付(還付)つき税額控除と納税者サービス：アメリカの「働いても貧しい納税者」の自発的納税協力問題を検証する(1)～(6)」税務弘報56巻9号～57巻5号参照)。政府税制調査会現地調査報告(2009年6月)でも、アメリカでのEITCにかかる税務執行の困難さを指摘している(<http://www.cao.go.jp/zeicho/siryuu/pdf/sg2kai2-1.pdf>)。納税と福祉を一体化し「納番で所得把握を厳正にし、不正監視する政策」は稚拙な空論といえる。

### (3) 納番なしで給付つき税額控除導入は可能

民主政権や財務省は、給付つき税額控除導入には納番が必要不可欠のようなPRをしている。しかし、給付つき税額控除を導入している諸国では、納番を導入していない国もあるし、納番があっても納税者整理番号として利用している程度の諸国(イギリス、ドイツなど)も多い(森信茂樹編『給付つき税額控除』〔中央経済社、2008年〕39頁参照)。アメリカ型の納番がないと給付つき税額控除を導入できないようなPRは不適切。納番導入誘導のための「口実」、「呼び水」である。

また、納番のない現行制度下でも、地方税法が原則として市町村内に住所を有する者のすべてに市町村税の課税ベース申告の義務を課していることから、所得額が非課税限度額以下の者も含め、すべての住民の所得把握ができる仕組みの下にある。したがって、仮に給付つき税額控除を導入するということで、所得制限のチェックが必要というのであれば、現在でも市町村がやればできる。「初めに納番ありき」の議論はいただけない。

## アメリカでは共通番号で「成りすまし犯罪者天国」に

アメリカにおいては、可視的な社会保障番号(SSN)=共通番号が、官民にまたがり、かつ、多分野で汎用されてきた結果、濫用され、「成りすまし犯罪」で手がつけられなくなっている。議会や省庁が対策をねっているが、抜本策を見出すにはいたっていない。

わが国においても、可視的な共通番号を導入すれば、成りすまし犯罪者が闊歩する社会になる怖れが強い。戦略室共通番号制度検討会では、抽象的に個人情報保護には触れるものの、番号濫用の実態にはまったく触れていない。意図的に回避している。きわめて不誠実である(サイバー税務研究No.9「アメリカにみる社会保障番号の危険性」[http://www.pij-web.net/user/pij\\_index.php](http://www.pij-web.net/user/pij_index.php))。

### 「外部不経済」につながる共通番号制

経済学の分野には「外部不経済」という考え方がある。例えば、生産過程を効率化して家庭用洗剤の価格を下げ、消費者が大量に使うとする。洗剤市場内部では製品が売れ、合理的のようにみえる。しかし、市場外では「家庭から排出された汚水処理」に莫大なカネがかかることになる。こうした現象を「外部不経済」という。

政府にとり、共通番号を使って国民情報(プライバシー)を分散集約管理するのは、確かに効率的・合理的である。しかし、一方で、国民の広範なプライバシーは、いやおうなしに、共通番号で仕分けされた官民さまざまなデータベース(DB)に分散管理されるかたちで公的支配のもとに置かれることになる。

また、不心得者は、何としてでも他人の共通番号を入手して、官民さまざまなDBに分散管理されたその人の多様なプライバシー個人情報を芋づる式に手に入れよう、あるいは、その人に成りすまして不法行為をしようとするに違いない。こうした不心得者が急増し、結果として、不心得者の追跡やその後始末に、国民サイドでのプライバシーを守る(個人情報保護)コストは途方もない額に達しよう。共通番号である社会保障番号(SSN)が濫用され、「なりすまし犯罪者天国」化したアメリカ社会が、このことを教えてくれる「反面教師」である。「対岸の火事」とばかりいってはいられない。

こうした国民サイドに発生する個人情報保護コストを内部化しないで、民主党政権が、共通番号制は、「効率的」、「合理的」で「すぐれもの」とするのは、「木を見て森を見ない」考え方の典型である。

環境破壊には目もくれず、「天然林に道路をつくって、便利になった」と叫んでいる近視眼的な人たちと同類である。破壊された自然環境修復には、とてつもない時間と費用がかかる。同じように、共通番号導入で破壊されたプライバシー環境の修復には、とてつもない時間と費用が要るはずだ。

### 共通番号を「本人確認」に使うことの危うさ

犯罪収益移転防止法という法律がある。「マネー・ロンダリング、テロ資金供与防止のため」という謳い文句で、一定の取引をする事業者などに取引相手の本人確認を義務付けた法律である。

現在は、本人確認のためには、運転免許証、健康保険証、国民年金手帳、住基カードなどが使われている。「本人確認が必要な事業者」は、金融機関等、ファイナンスリース事業者、クレジットカード事業者、宅地建物取引業者、宝石・貴金属等取扱事業者、郵便物受取サービス業者、電話受付代行業者、司法書士、行政書士、公認会計士、税理士、弁護士などである。

もし共通番号が導入されれば、金融機関に貸金庫をつくるとき、金融機関に口座を開くとき、ファイナンシャルリースでお金を借りるとき、クレジットカードをつくるとき、建物をリースするとき等々、本人確認の際には共通番号の提示が求められることになる。

官民の機関がこれらの共通番号（マスターキー）付本人確認情報をデータベースに入れて、公権力の求めに応じて開示する仕組みにエスカレートするのも時間の問題といえる。

一方で、どこかの政党の元幹事長のように、タンスやカメに現金を入れておく人たちは、この法律の枠外に置かれる。また、不法収益に群がる人たちが、この法律を遵守する可能性も極めて低い。

まさに、共通番号を導入するということは、こうしたいびつな私たちのデータ監視社会をつくることにもつながりかねない。

### イギリス新連立政権は、人権を蝕む「国民IDカード制」廃止に

イギリスで去る5月に誕生した新連立政権（保守党・自民党連立；Lib-Con Coalition Government）は、「国家が必要以上に国民の個人情報を収集しない方針」を打ち出した。そして、前労働党政権下で導入した「国民IDカード制」を、「恒常的な人権侵害装置」として、廃止を決定した。新連立政権のメイ内務相は、5月27日に「ID制廃止100日プラン」を公表した。

イギリスは、議会主権の国である。司法は、違憲立法審査権を有していない。したがって、国民は、司法ではなく、政権交代に「国民IDカード」という国民監視ツールの廃止を期待したといえる。

「リバティ（Liberty）」のような人権NGOは、当初から国民IDカード制に反対し、制度実施後は、「国民IDカード」廃止を野党（当時）に働きかけていた。政権交代が実現し、新連立政権は、政権公約にしたがい「ID制廃止法案（Identity Documents Bill 2010-11）」を用意した。

イギリスでは、内閣が提出する法案は、議会上院における議会開会式で行なわれる「女王の演説（Queen's Speech）」のなかで明らかにされる。一般国民は、この演説を通じて政府がどのような法案を準備しているか知ることができる。

イギリスの新政権誕生後の5月25日に開催された議会の女王の演説では、内務省が、「ID制廃止関連法案（政府立法案）」を準備していることを明らかにした。それらは、つぎのとおり。

【表5】IDカード制廃止関連法案の骨子

- |   |
|---|
| <p>(1) ID制廃止法案（Identity Documents Bill）<br/>【この法案は、IDカードの廃止を目的とするもの。この法案通過後は、現在カードを保有する市民について国家身分登録台帳（NIR = National Identification Register）に保管されているあらゆる個人情報が廃棄される。】</p> <p>(2) 警察改革・社会責任法案（Police Reform and Social Responsibility Bill）【この法案は、警察の職務内容を一般市民へ開示することをねらいとしたもの。】</p> <p>(3) 自由（抜本廃止）法案（Freedom Great Repeal）Bill【この法案は、市民に対する警察の影響力を制限することをねらいとしたもの。具体的には、DNAデータベースに情報入力されている人たちへの保護措置の強化、非暴力にかたちでの抗議活動をする権利の回復、および監視カメラ（CCTV）利用規制の強化など】</p> |
|---|

ちなみに、連立政権は、「移民の流入規制とIDカード制廃止」をパッケージとしている。このことから、2006年IDカード法 (ID Cards Act 2006) に基づくIDカードに代えて、外国人には、2007年国境法に基づいて居住許可証 (Residents Permits) を発給することになる。

ニック・クレグ (Nick Clegg) 副首相は、IDカード制廃止に関して、マスコミのインタビューに応じて、次のように述べている。

「このムダで、官僚発想的で、人権侵害的なIDカード制は、前政権の害悪のすべてを象徴するような存在である。早急にこのIDカード制度を廃止することにより、新政権は、閣僚になった者の身勝手な思い付きによって市民の自由を犠牲にするようなことはしない旨を約束するものである。」

「IDカード制を廃止し、国家身分登録台帳 (NIR) を廃棄することは、監視国家体制 (surveillance state) を解体するための重要な一歩である。IDカードは氷山の一角である。イギリス人の勝ち取ってきた自由を回復するための一連の急進的な改革のスタートである。」

新政権は、「IDカード制廃止100日プラン」をベースに、IDカード制廃止関連法案の早期議会通過をめざしている。2010年6月9日から、下院の第二読会で、廃止関連法案の審議がはじまった。

わが国の中央の役人、さらにマスコミなども、こうしたイギリスの動きには「どこ吹く風」である。

廃止が決まったイギリスの内務省が発行するIDカードサンプル



### ドイツでは、共通番号制は憲法違反

ドイツは、共通番号制 (unified PIN) を採用していない。複数の分野別限定番号を採用している。これには、つぎのような背景がある (CNN ニュース 6 2 号 <http://www.pij-web.net/pdf/cnn/CN->

N-62.pdf参照)。

【表6】ドイツで複数の分野別番号を採用する理由

<p>連邦憲法裁判所 (Bundesverfassungsgericht) が、1984年の国勢調査に汎用の共通番号を利用することは違憲となる可能性がある旨の示唆を含んだ判決 (Volkszählungsurteil)、および、この判決に基づいた汎用の共通番号の導入は基本法 (憲法) 上ゆるされないとする連邦議会 (Deutscher Bundestag) の解釈</p>
<p>旧東ドイツでは、中央民事登録台帳と個人識別番号制を採用していた。しかし、東西ドイツの統合条約において、国民監視システムの象徴とも見られていた東ドイツの双方の制度は廃止された事実。</p>

ちなみに、ドイツの場合、イギリスと違い、憲法裁判所が設置され、国民は、共通番号制などについて、司法に違憲判断を求めることができる体制にある。

### 政府がつくる第三者機関の限界と問題点

役所依存症の強い日本では、EU諸国などと同じように、「政府第三者機関」に有用性を見出そうとする傾向が強い。言い換えると、アメリカ型のように、政府第三者委員会に依存しない、いわゆる「民規制」を指向しようとする方向につながらない。

自由権の種類によっては、政府がつくる第三者機関 (以下「政府第三者機関」) が有害な場合もある。例えば、「報道の自由」、「信仰の自由」などについては、「政府第三者機関」では、言論統制、国定 (公定) 宗教の方向へつながらおそれが出てくる。この分野については、規制が必要としても、いわゆる「民規制」によるべきであろう。

この点、「共通番号、国民ID制」についても、「政府第三者機関」の設置、つまり情報セキュリティ論 (プライバシー保護措置を講じれば、共通番号も国民ID制もゆるされるとする主張) が唱えられ、共通番号や国民ID制度導入への「呼び水」となっているきらいがある。

しかし、共通番号+国民ID制度の導入構想に、「政府第三者機関」があれば大丈夫というスタンスは危険である。また、こうした主張は、人格権や移動の自由など人権を保障した憲法を「ないがしろにする」大きな要因となっている。した

がって、情報セキュリティ論、つまり、「政府第三者機関」を設置すれば、共通番号+国民ID制度の導入もゆるされるとする、矮小化された導入積極論に惑わされてはならない。

## むすび

~「共通番号」と「国民ID制」は一体、断固反対しよう

民主党がめざす共通番号(マスターキー)付国民IDカード構想が、このまま現実のものになるとすれば、広範な個人情報に公有化される。各人の共通番号を検索キーに使い、各種データベースに蓄積された特定個人情報に対する当局からの照会も頻繁に行われることになる。

照会の結果、「ヒット(当たり)」と出た場合には、有無を言わずに違法行為を問われる事態も出てこよう。微罪で罪を問うのにデータ照会が濫用される危険性も高い。

国民は誰しも、「IDカードを携行・提示(告知)しないと市民生活ができない社会」の実現を望んでいない。「『共通番号と国民IDカード制の導入でデータ監視社会になっても、悪いことをしていなければ怖がることはない』では済まされない。

私たち国民は、「『共通番号付国民IDカード』で『安心・安全』のトリック」を見抜く眼力が問われている。将来に「負の遺産」を残してはならない。共通番号や国民IDカードは要らない。

共通番号やID(カード)制導入について、役所や役所寄りの学者などからは、情報セキュリティ論(プライバシー保護措置を講じれば、共通番号や国民ID(カード)などを「是」とする考え方が主張される。しかし、この問題は、憲法論、人権論の視点から検討されなければならない。

民主政権は、来春の通常国会に共通番号導入法案を提出するとしている。「共通番号」と「ID(カード)制」は一体でとらえなければならない。将来に「負の遺産」を残さないためにも、スーパー電子監視国家につながる「共通番号付ID(カード)制」の導入を絶対にゆるしてはならない。

住基ネットに反対する名古屋市の河村たかし市長は、8月20日に「共通番号及び国民IDカード制度問題検討名古屋委員会」(委員長・平松毅関西学院大学名誉教授)を発足させ、国へ「もの申す」ための意見書の提出を諮問した。各地の弁護士会も検討を開始した。市民団体、人権を大事にする団体をはじめとして各界の積極的な対応が急がれる。

## 政府のIT戦略本部、「国民ID制」導入の行程表を発表 国民監視ツールの国民ID(国民登録証)カード導入の動き

(PIJ国民総背番号IDカード問題対策チーム)

**2** 010年6月22日に、政府の「高度情報通信ネットワーク社会推進戦略本部(IT戦略本部)」は、国民による行政監視のための国民ID制度」導入をはじめとした電子政府構想に関する2020年までの「新たな情報通信技術戦略」の行程表をまとめ、公表した。

新戦略では、2013年度までに「国民ID(登録証)(カード)」制の導入をうたっている。いうまでもなく、国民ID(カード)制度、内実は、「現代版電子通行手形」、「国内版パスポート」だ。IT戦略本部は、「電子政府構想」

実現のための電子証明書を格納するツールと位置付けているようだ。だが、これは「口実」。現在でも、住基カードという、電子証明書を入れたICカードはある。国民ID制とは、「国民の移動の自由」を制限する監視ツールの導入だ。

IT戦略本部は、このIDカードにより、「国民による行政監視の仕組みの整備」を行うのだという??だが、この役人がまとめた国民ID(カード)制度、発想が「あべこべ」ではないか?本当は、「行政による国民監視のために国民ID制度」だろうに。

この政権や背後で操る役人は、「国民の個人情報

報は国家が行政情報として管理する。だから、国家が、どういった自分の情報を管理しているかは、各人のIDカードを提示してみせてもらうかたちにする・・・、といった考えなのだろう。だが、わが国は広範な個人情報に公有化して国家が管理する体制をとっていないはずだ。個人情報（プライバシー）は、あくまでも各個人の財産のはずだ。本末転倒である。こうした基本が護られない国民監視ツールを導入するのが、「国民が主役」を唱えた政権の「裏の顔」なのであろうか？

「個人のプライバシーはその個人の財産である」という原則は、護らなければならない。民主政権が役人と一緒になって、このIDカードに、住基ネットをベースにあらたに創設される「共通番号・国民背番号」を入れて、国民総監視体制を築き上げる・・・。さらには、役人のささやきに乗じて消費税10%の大衆増税など出してくる。こうした状態で、「国民の生活が第一」、「脱官僚政治」などと言っても、誰も信じない・・・！（単なる役人の言いなり政権ではないのか？？何のために政権交代だったのだろうか？？）

民主政権のIDカード構想は、今年5月に発足したイギリスの新政権が「国民IDカード制度は人権侵害装置である」として、廃止を決定したものと同一類のものだ。ところが、パクられた本家・イギリスが、恒常的人権侵害装置であるととして廃止した。この事実は重い。

このままでは、国民IDカードを持ち歩かない人たちを、「非国民」とパージするデータ監視社会が待ち受けている。警察官が、「あなたのIDカードを見せて、Show me your ID！！」と職務質問してくる監視社会へまっしぐらだ。

元市民運動家を首相に輩出するなどした民主党には、共通番号付国民IDカードの導入、国民総監視体制構築は似合わない。頭を冷やして欲しい。

国民ID〔カード〕、こんな国民監視ツールは絶対に要らない！！

.....

## 《国民ID制度の導入と国民による行政監視の仕組みの整備》行程表

### 短期（2010年、2011年）

国民ID制度の検討体制を構築し、サービス

の利用目的、利用者の範囲、接続対象範囲、情報の内容、利用手段等を明確化する。  
民間ID利活用を実現する官と民との間のインターフェース実証実験を踏まえた行政情報システムとの連携可能性を検討する。  
国民ID制度における付番方法等の実現条件を整理するとともに、国民ID制度の在り方を検討する機関を明確化する。  
個人情報保護に関して自己情報を確認できる仕組み等を検討するとともに、監視等を行う第三者機関の在り方を明確化する。

厚生労働省：実証事業を踏まえ、公的ICカードの要件等の課題を整理

総務省：行政業務システムと民間事業者との連携に係る実証実験、制度的課題等の整理

経済産業省：官民連携した行政サービスモデルシステムの構築、運用

文部科学省：研究者の業績や略歴等を繰り返し審査に活用できるよう、次期e-Radの設計・開発を実施

内閣官房、関係府省：タスクフォースを立ち上げ、国民ID制度に関するサービス要件、実現条件の整理

### 中期（2012年、2013年）

国民ID制度や第三者機関の設置等に関する制度設計、関連法令の整備を行う。

公的ICカードの整理・合理化を検討する。

国民ID制度に関するシステム要件の整理を行うとともに、システム設計、構築に着手し、第三者機関の設立準備を開始する。

内閣官房、関係府省：国民ID制度の制度設計やシステム設計に着手、第三者機関の設立準備を開始、公的ICカードの整理・合理化に向けての検討を実施

文部科学省：次期e-Rad運用開始

### 長期（2014年～2020年）

国民ID制度のサービス提供を開始する。

2020年までに、50%以上の自治体において、条例改正を実施し、公平で利便性が高い電子行政を実現する。

内閣官房、関係府省：国民ID制度運用開始

## 名古屋市長、共通番号、国民ID制で、外部委員会から意見聴取 「共通番号及び国民IDカード制度問題検討名古屋市委員会」を開催

(CNNニュース編集部)

**河**村たかし名古屋市長は、かねてから住基ネットに反対の意思を表明してきた。河村市長は、住基ネットの導入に4度も廃止法案を出した民主党が、政権につくや否やあらたに国民監視のツールである「共通番号」と「国民ID」制度の導入、を打ち出してきたことに懸念を表明してきた。こうした中央集権的な仕組みの導入は、「地方主権」を唱える政権の公約と明らかに抵触する。「市民が主役」はどこへ消えた、と批判してきている。

河村市長は、8月9日の定例記者会見で、専門家から意見を聴取するために、名古屋市独自で「共通番号及び国民IDカード制度問題検討名古屋市委員会」(「市問題検討委員会」)を立ち上げることをアナウンスした。市問題検討委員会は、地方主権、住民の人権などに与える影響、導入の是非などを自治体レベルで検証し、市長へ意見を報告するのが主な任務。これまで2回開催された。

編集部は傍聴者などからヒアリングを行った。この市問題検討委員会の設置は「河村市長の英断」、との声があった。その一方で、委員自体にとっても新たなテーマであるためか、「的確な内容で審議が行われているとはいえない」、との意見もあった。現時点では、どのような報告になるのかは不透明である。

### 《市問題検討委員会の概要》

#### 1 設置目的

国が検討している共通番号及び国民ID制度が、市民生活等に与える影響について議論・検討等するため、共通番号及び国民IDカード制度問題検討名古屋市委員会を設置するもの。

#### 2 所掌事務

(1) 国が検討している社会保障・税の共通番号制度に関する課題等を整理すること。

(2) 市民の自由権の確保と地域主権に関する課

題等を整理すること。

(3) その他委員長が必要と認めること。

3 委員(敬称略・五十音順)【氏名・職名等】

- ・浅野洋(税理士・名古屋税理士会)
- ・石村耕治(白鷗大学法学部教授)
- ・稲垣隆一(弁護士・第二東京弁護士会)
- ・園田寿(甲南大学法科大学院教授)
- ・平松毅(姫路獨協大学法科大学院特別教授)

〔任期は平成22年7月29日から平成23年3月31日まで〕

委員は、個人情報、人権、税務問題などを専門とする学者や弁護士、税理士ら5人。3回の会合をもち、意見を報告にまとめ市長へ提出する。

第1回会議(8月20日午後2時:名古屋市役所)

8月20日に初めて開催された第1回検討委員会には、市民傍聴人、市職員、マスコミ関係者など多数が参集した。河村市長は「百年後の日本、この国のかたちを左右する大問題である。勇気をもって国に意見をすべきときである。力強い提言をいただきたい」とあいさつをした。

共通番号及び国民IDカード制度問題検討名古屋市委員会の委員長には、平松毅教授が選ばれた。平松委員長は、「政府は、メリットだけを強調している。しかも、地方主権どころか、個人情報の中央集権強化に走っている。こうした国の動きに警鐘をならし、住民のプライバシー権を護る行動ができるのは、市民生活に密着した自治体よりない」と議論の口火を切った。

つづいて、石村耕治・白舒大学法学部教授が基調報告を行った。基調報告の概要は、つぎのとおりである。

はじめに 政府の「共通番号付国民IDカード制度」構想の検討組織(1)共通番号【国民背番号】制導入の検討(2)国民ID【国民登録証】カード制導入の検討、(3)共通番号付国民IDカード制導入のサポーター「共通番号」で国民の個人情報の公有化  
共通番号を「納税者番号」に使うことの意味  
アメリカでは共通番号で「成りすまし犯罪者天国」に 「外部不経済」につながる共通番号制  
共通番号を「本人確認」に使うことの危うさ  
共通番号付国民IDカードは「国内版パスポート」 「共通番号付国民IDカード」を使った国民情報の公有化で「安心・安全」なのか  
イギリス新連立政権は、人権を蝕む「国民IDカード制」廃止に  
問われる共通番号導入を前提とした「意見公募」 むすび

第2回会議(9月6日午後3時:名古屋市役所)

第2回委員会は、9月6日(月)午後3時から「名古屋市公館」(名古屋市中区三の丸三丁目2番5号)で公開開催された。報告は、次のとおりであった。

- 1、平松委員 共通番号及びIDカードに関する憲法問題
- 2、園田委員 個人情報をデジタル化する意味
- 3、稲垣委員 報告

各委員の基調報告の後、若干の討論が行われた。

第3回会議(11月5日午後3時〔予定〕:名古屋市役所)

石村耕治委員の基調報告につづいて、活発な討論が行われた。

【傍聴受付連絡先】名古屋市市民経済局地域振興部区政課  
担当:成田・鈴木 電話:052-972-3114

## 日弁連「税と社会保障制度共通の番号」制度創設に関する意見書を公表 (PIJ国民総背番号IDカード問題対策チーム)

日本弁護士連合会(日弁連)は、2010年8月19日に「税と社会保障制度共通の番号」制度創設に関する意見書をとりまとめ公表した。また、8月25日づけで、内閣府、国家戦略室、財務省、総務省、厚生労働省に提出した(<http://www.nichibenren.or.jp/ja/opinion/report/data/100819.pdf>)。

### 【日弁連意見書の趣旨】

信頼できる税制と社会保障制度の構築が急務であり、また、「国民ID」や「番号」を活用した電子政府化の推進が各国で進められていることは事実であるが、それらの国と日本とは、国情や国民性などに大きな違いがあるから、拙速に「番号制」の創設のみを進めるべきではない。特に、情報公開制度の充実、EU諸国やカナダなどに存在する独立の第三者機関の設立などを前提とした、プライバシー保護を踏まえた、国民・在留外国人に信頼される制度とすることが必要であり、慎重かつ根本的な検討が必要である(<http://www.nichibenren.or.jp/ja/opinion/report/100819.html>)。

### 【日弁連意見書に対するPIJの見解】

PIJは、基本的人権を擁護し、社会的正義を実現することを使命とする専門家集団である日弁連がこの問題について、詳細に分析し、早急に意見書を取りまとめたことに対して、敬意を表し、積極的に評価したい。

しかし、「国民ID制」の本質についての分析などについては異論がある。とりわけ、情報セキュリティ論(政府第三者機関の設置など、プライバシー保護措置があれば、導入もゆるされるのでは)といった意見書のトーンには異論がある。「共通番号付国民ID制」については、正面から、すなわち「人権論」「憲法論」の視点から取り組んで欲しかった。

PIJは、「共通番号付国民ID制」は国家が国民の人格権をトータルに支配することにつながり、憲法13条などに違反する仕組みであると考え。また、政権党が唱える地域主権の確立にも逆行する仕組みであると考え。したがって、PIJは、住基ネットを基盤にした共通番号や国民ID制の導入自体がゆるされないと考え。

# 監視カメラとプライバシー

## — 求められる「監視カメラに頼らない社会」

石村 耕治 (PIJ代表)

### 《レクチャー骨子》

はじめに

～政策不在で、一番迷惑するのは市民

#### 1 職場に広がる監視カメラ

- (1) 私的空間にも広がる監視カメラ
- (2) 職場に広がる監視カメラ
- (3) なぜ、郵便局の労働現場の監視カメラだけが撤去されるのか
- (4) 監視カメラの“設置”でも、“撤去”でも潤うIT企業
- (5) どうする、監視カメラを使った行き過ぎの労務監視
- (6) 厚労省の「労働者の個人情報保護に関する行動指針」
- (7) 労務監視と自動データ処理のみでは処分を受けない権利など
- (8) イギリスにおける監視カメラによる従業員監視の基準

#### 2 人権尊重が求められる国交省のフルボディスキャナー実証実験

- (1) 国交省主導でフルボディスキャナー検査の実証実験開始

- (2) 各国で問われるフルボディスキャナー検査

- (3) 全身への電磁波照射は危険ではないのか？

- (4) 問われる検査方法の妥当性

- (5) 被検者の同意が前提

- (6) 求められる検査システムの“見える化”

#### 3 イギリスでは、新政権が政治主導で「監視カメラ濫設規制策」を実施

- (1) 監視カメラ大国、イギリスにおける従来からに監視カメラ規制策

- (2) 前政権が導入した「国民ID〔身分登録証明〕カード制」を廃止

- (3) データ監視社会へ逆走するわが国の民主政権

- (4) イギリス、政権交代で「監視カメラ濫設規制」に政策転換

- (5) 新政権の人権回復3法案に盛り込まれた監視カメラ規制策

- (6) 問題の本質を矮小化する「情報セキュリティ論」

むすびにかえて

～求められる「監視カメラに頼らない社会」

はじめに

～政策不在で、一番迷惑するのは市民

監視カメラ〔諸外国では、「CCTV = Closed-circuit Television (閉鎖回路テレビ)」あるいは「ビデオ監視装置 (Video Surveillance Device)」とも呼ばれる。〕は、国や地方の各種機関やその施設、公道・公園などの公共の場所(公的空間)に常設されている。

また、監視カメラは、金融機関から、コンビニ、マンションのエレベーター内や玄関ホール、学校の教室や介護施設など、民間施設や敷地内(私的空間)にも広がりを見せている。

企業の職場では、監視カメラを使った行き過ぎの“労務管理”が猛威をふるっている。「就労場所の監視カメラ(CCTV in the Workplace)」については、街頭の監視カメラなどとは異なる規制の必要性を説く意見も強い。

このように、監視カメラを設置・利用する目的も多様化している。また、その性能も、顔面認識技術を使い生体認証ができる監視カメラや360度魚眼レンズを搭載した監視カメラなど、高度化の一途をたどっている。

こうした現象を、「監視カメラ社会化」と呼ぶ人もいる。監視カメラ社会化の動きは、わが国のみならず、テロに怯えるアメリカや犯罪急増に悩む欧州などでも、加速している。近年、空港で「全身に電磁波を照射して危険物の機内への持込みをチェックするための新たな「フルボディスキャナー（全身透視画像検査装置）」の導入は、その最たる例の一つといえる。

最高裁は、「何人も、その承諾なしに、みだりにその容ぼう・姿態を撮影されない自由を有する」（1965〔昭和44〕年12月24日判決・判例時報577号18頁）という判断を示している。個人が、自分の承諾（同意）なしに写真を撮られない権利、あるいは撮られた写真を公表されない権利は「肖像権」と呼ばれている。

肖像権は、プライバシーなど「個人の尊厳」を護る憲法13条で保障されている。肖像権は、もともとプライバシー権とは別に発展してきたものである。しかし、プライバシー権を「自己に関する情報をコントロールする権利」ととらえる今日においては、肖像権はプライバシー権の一つと考えられている。本人の同意もなく、自分のコントロールの及ばないところで監視カメラの被写体とされ、無差別に記録されることは、まさに個人の肖像権の侵害にあたるといえる。

しかし、一方で、犯罪が多発し、手口が巧妙になるにつれて、「監視カメラは絶対ダメ！」と叫び、「プライバシー原理主義」を主張するだけでは立ち行かなくなっているのも事実である。監視カメラ社会化は、犯罪の抑止、犯人の割出・検挙などに役立つ（有用であり）、やもう得ない現象だという見方がある。

そうは言っても、明確なルールのないまま、監視カメラを一人歩きさせることでは、カメラの被写体となる個人の自由と尊厳にとり大きな脅威となるとの指摘も無視できない。イギリスのように、政権交代を機に「監視カメラ濫設規制」を打ち出し、「監視カメラ社会化」にブレーキをかける動きも出てきている。

わが国でも、真摯な対応が求められている。座視し「監視カメラ社会化」を黙認してはならな

い。監視カメラに「鈴をつけ」、その設置・利用を国民（住民）が常時「監視」できる透明化のルール・法的システムづくりばかりではなく、「濫設」対策が急がれている。

## 1 社会の隅々まで広がる監視カメラ

生活安全条例などを典拠に、マンション管理組合や自治会のような自治組織に補助金を交付して、監視カメラの設置を義務付けるあるいはしようよう（強く指導）する自治体も急増している。しかし、監視カメラの運用ルールやプライバシー影響評価などが不確かな場合も少なくない。

監視カメラはあらゆる空間に設置され、その数は増える一方である。濫設を心配する声もあるが、規制しようという市民の声は必ずしも盛りあがっていない。政治も、「安心・安全」を説くだけで、監視カメラの濫設規制に動こうともしない。市民のプライバシーを護ることに消極的あるいはまったく関心が薄い。いずれにしろ、監視カメラの濫設、自由な利用を放置しておいてよいわけではない。

### （1）私的空間にも広がる監視カメラ

私立学校、介護施設、民間企業などが「私的空間」に設置した監視カメラも問われている。とりわけ、教育現場や職場での監視カメラを使った過剰な管理は、学ぶ者、教える者、働く者の権利侵害にあたる。市民団体や労働団体などには真摯な対応が求められている。

また、私たちが「政治」を必要とするには、企業の「営業の自由」が一方的にまかり通り、人権



が風前のともしびと化するのを傍観せずに積極的に歯止め策を施し、虐げられた人々に支援の手を差し伸べて欲しいからである。誰のために政治が存在しているのか、今まさに、その姿勢が厳しく問われている。

## (2) 職場に広がる監視カメラ

企業の現場で、「監視カメラ」を使った行き過ぎの「労務管理」が猛威をふるっている。コンサルタント会社が、クライアントの職場に設置された音声収録・マイク付き監視カメラを遠隔操作、社員に逐次「雑談を止めなさい」、「しっかり働きなさい」、「姿勢が悪い」等々とアドバイスする。「IT技術の進歩はすご〜い」と、驚嘆してはられない問題もある。

### 監視カメラで労務管理するブラック会社勤務、社畜21番のつぶやき

一生懸命仕事をしているのに、監視カメラで四六時中見張られるなんて異常だ！

この職場はどうなっているんだ！これで「給料ドロボーが減る」なんて思い違いだ！

・・・でも、イヤなことは考えないようにしよう。

カメラがあったら、カメラ映りがいいように仕事をすればいいんだ。

遠くにある見張塔のゲシュタポから「社畜21番さん、お客様に対する今の電話の話し方はまずいです。マニュアルをもう一度読んで工夫してください」と天の声があったら、「社畜21番です。ご指摘ありがとうございます。努力します」って・・・。

ゲシュタポも、「嫌なら辞める！！」とおどされながら、社畜いじめなのかなあ〜??

## (3) なぜ、郵便局の労働現場の監視カメラだけが撤去されるのか

郵便局もこうした労務監視の例外ではなかった。2007年の郵政民営化の頃に、全国2万4千局のうち、特定郵便局を中心に約1万8千局に「監視カメラ」が設置された。

こうした「労務監視」に「待った！」をかけた政治家がいる。昨年9月の民主政権誕生後、全国郵政局長会（全特）の要望を受けた国民新党やみんなの党に所属する政治家である。

「郵政」の監視カメラ問題に積極的に取り組んでいるのは、みんなの党の柿沢未途衆議院議員である。柿沢議員は、『郵便局の「間仕切り」及び

監視カメラの撤去に関する質問主意書』（2010年4月1日）を総理大臣あてに提出した。

4月9日に総理大臣が回答した「答弁書」では、「一部に不適切な配置があったことにより労働の過剰監視につながり職員の士気を失わせるなどの弊害が結果としてあった」と、監視カメラなどの設置について問題があったことを認めている。（<http://www.310kakizawa.jp/rinentoseisaku.html>）

自公政権下ですすめられた郵政改革、その一環として設置された監視カメラは、特定局長や職員にはきわめて「不評」であった。

雇用主側の日本郵政グループは、政権交代など「政治の動き」に過敏だ。国民新党などからの撤去要求が出ると、「政治の暴風」を避けるために、監視カメラの撤去をすすめた。

国民新党やみんなの党の姿勢はプラス評価に値する。だが、問題は、政治が問うた監視カメラが、なぜ「郵便局だけ」なのかである。「結果が良ければ、原因を問う必要がない」といって、近視眼的に見ているわけにはいくまい。

偏頗的な「政治力」の行使は、それにより救われる選挙民の歓迎を受ける一方で、救われない選挙民の不信を増長する。

## (4) 監視カメラの「設置」でも、「撤去」でも潤うIT企業

日本郵政は、すでにふれたように、「防犯+職員の働きぶりの監視」をねらいに、特定郵便局を中心に約1万8千局に「監視カメラ」を設置した。設置費用は約700億円かかったという。

政権交代後、「政治の暴風」を避けるために、監視カメラの撤去をすすめた。撤去費用は、何と総額で32億円にも上るといふ。

この郵政向けの「公共工事」に投じられた巨額な資金の「ムダ遣い」にはおとがめなし。一方、IT企業にとっては、設置しても、撤去しても、棚ぼた利益につながる。彼らには「ムダ遣い」自体が「おいしい話」なわけである。

まさに、日本郵政における監視カメラの設置・撤去のドタバタ劇は、「ハイテク時代の公共工事」そのものといえる。その負担は、回り回って消費者に転嫁されることになる。ここでも、新たな公共事業である「国民電子監視ツール」導入の「特需」に沸くIT企業が高笑いしている。

## (5) どうする、監視カメラを使った行き過ぎの労務監視

監視カメラを使った行き過ぎの労務監視は、一般企業にジワリジワリと広がってきている。防犯と従業員の勤怠管理を徹底するねらいで監視カメラを使い、労務監視を実施することは、雇用主である企業の“営業の自由”としてゆるされるようにもみえる。しかし、防犯はかたちばかりで、過剰に労務監視を実施することは、確実に“働く者の精神を蝕む”。労働者保護諸法や人権保護上、禁止されて当然である。

例えば、労務管理・監視をねらいとし、会話音声拾う機能やスピーカー機能を持っている、遠隔操作・管理ができる、さらには360度魚眼レンズを搭載するなど超高性能な監視カメラも登場している。

のちにふれるように、監視カメラ設置の適否に関する基準の一つに「つり合いの原則」がある。必要性を超える性能を搭載する監視カメラについては、働く者の精神衛生などを加味したうえで、この基準にしたがって今一度その設置の適否が問われなければならない。

政治が、集票力のある、あるいは力の強い労働者だけを護るのではバランスを欠く。これが「政治主導??」の“実際”だとしたら、庶民の政治離れはますます加速するに違いない。今まさに、政治には、監視カメラを使った過剰な労務監視に苦しむ人たちの人権を護る行動が求められている。

市民派を標榜しながら、事実上「市民派」の看板をはずした民主政権は、中央の役人の手足となって共通番号【国民背番号】の導入や国民ID【国民登録証】カードの導入で“国民監視ツール”導入に血眼になり、他方では大衆増税を叫ぶだけである。これでは、自民などと同じで、“存在根拠なし”。国民の厳しい裁断が下るのは当たり前である。

#### (6) 厚労省の「労働者の個人情報保護に関する行動指針」

2008年に、野村証券の企業情報部門に在籍していた社員が、M&A(企業の合併・買収)の情報などをもとに4千万円を不正に取得したとして東京地検特捜部にインサイダー取引で逮捕(逮捕当日に同社員は解雇処分)、起訴された。

この事件を受けて、2008年6月に、野村証券は、情報管理、インサイダー取引再発の防止策を公表した。このなかで、企業情報部のレイアウト

を見直し、課単位で仕切りを設け、課毎にプリンターを設置。会議室を増設するなど設備の拡充を行うとともに、モニターカメラによる業務監視も行うことを決め、実施した。

労務監視をねらいに職場に設置される監視カメラは、働く者の側からは、就労者を「社畜」化し、あるいは「奴隷工場」を地で行くような労務監視のツールに見える。一方、使用者から見ると、不正の防止、職場倫理の確立などのためのツールにもなる。監視カメラの「有用性」の視点も無視できないわけで、まさに「存在が意識を決定する」関係にあるともいえる。

ちなみに、厚生労働省が、OECDのガイドラインなどを参考に作成し、2000年に出した「労働者の個人情報保護に関する行動指針」では、次のように、記している。

#### 労働者の個人情報保護に関する行動指針(抜粋)

- (4) 使用者は、職場において、労働者に関しビデオカメラ、コンピュータ等によりモニタリング(以下「ビデオ等によるモニタリング」という。)を行う場合には、労働者に対し、実施理由、実施時間帯、収集される情報内容等を事前に通知するとともに、個人情報の保護に関する権利を侵害しないよう配慮するものとする。ただし、次に掲げる場合にはこの限りでない。
- (イ) 法令に定めがある場合
- (ロ) 犯罪その他の重要な不正行為があるとするに足りる相当の理由があると認められる場合
- (5) 職場において、労働者に対して常時ビデオ等によるモニタリングを行うことは、労働者の健康及び安全の確保又は業務上の財産の保全に必要な場合に限り認められるものとする。

#### (7) 労務監視と自動処理データのみでは処分を受けない権利など

コンピュータの判断を過信することは危険である。プログラム入力や撮像したデータが不正確な場合には、思わない人権侵害につながるおそれもある。

こうしたことに配慮して、EUデータ保護指令15条は、「自動処理データのみでは処分を受けない権利」を各加盟国の国内法に盛り込むように求めている。

#### EUデータ保護指令15条

EUデータ保護指令15条〔自動処理データのみでは処分を受けない権利〕は次のように規定する。

EUデータ保護指令15条〔自動処理データのみでは処分を受けない権利〕

EU加盟国は、いかなる者に対しても、データ主体に対し法的効果または重大な影響を及ぼし、かつ、もっぱら当該データ主体の仕事ぶり、信用度、信頼性、行動のような個人の一定の側面を評価することを目的に自動処理データのみに基づいては処分の対象とされない権利を認めなければならない。

加盟国は、このデータ保護指令の他の規定に基づいて次のような場合には、自動処理データに基づく処分の対象とする旨を規定できる。

- ・その処分が、契約の締結または遂行の過程において行われており、データ主体の要求が満たされているか、または、データ主体の法律上の利益を保護する適切な措置が講じられている場合

- ・その処分が、データ主体の法律上の利益を保護する措置を規定している法律に基づいてできることになっている場合

データ保護指令を注解した「解説メモランダム (Explanatory Memorandum)」では、次のような事例をあげてコメントする。

例えば、雇用主は、コンピュータを用いた審理判断の結果のみに基づいて求職者の不採用を決めてはならない等々。・・・ちなみに、指令12条は、「データ主体の開示請求権」を保障している、この条項のもと、自動処理データで何らかの処分・決定を受けた者は、因果関係について開示をもとめることができる。

ちなみに、わが国の個人情報保護法は、「自動処理データのみでは処分を受けない権利」について、まったくふれていない。大きな課題である。

#### イギリスのデータ保護法

EUのデータ保護指令を受けて、2008年にデータ保護法(DPA)が制定された。同法は、第 7 章の「データ主体の権利その他」(7条~15条)の一環として、「損害または苦痛を与えるおそれのある取扱を停止させる権利」(10条)や「自動判定にかかる権利 (Rights in relation to automated decision-taking)」(12条)を制度的に保障する規定を置いた。

したがって、就労場所に設置された監視カメラで、従業員が精神的損害または苦痛を感じた場合、データ管理者に、文書で通知し、データ処理(撮像)の停止を求めることができる。

一方、12条1項は、「個人は、いつでも、データ管理者に対して文書で通知して、本人に重大な影響を及ぼす事項の評価を、もっぱら自動処理

手段に基づいて行わないように求める権利を有する」と定めている。そして、本人に重大な影響を及ぼす事項の例として、「仕事の遂行度(performance at work)」を掲げている。

したがって、従業員は、もっぱら監視カメラ画像を使って従業員本人に重大な影響を及ぼす事項の評価が行われていると信じられる事例においては、その停止を求めることができる。

さらに、7条は、データ主体(本人)にデータ開示請求権を認めている。したがって、就労場所に雇用主が設置した監視カメラで、従業員が精神的損害または苦痛を感じたその他不当労働行為があると信じられた場合には、本人がデータ管理者に対して問題の映像のコピー(副本)を請求することができる。そのコピーをもって争訟を開始することもできる。

#### (8) イギリスにおける監視カメラによる従業員監視の基準

イギリスでは、1998年のデータ保護法【国の行政機関、地方公共団体などの公的部門と民間部門の双方に適用されるオムニバス方式】の制定、2000年3月1日の施行以前、就労場所(workplace)への監視カメラの設置については、まったく法規制がなかった。

しかし、1988年法の施行を契機に、情報コミッショナー事務局(ICO)は、監視カメラで撮像される個人の「画像(images)」を個人の「データ」として取扱い、1988年法の適用対象とし、保護をはかることにした。

イギリスの情報コミッショナー事務局(ICO)は、監視カメラ設置・運用に一定の規制を加えることをねらいに、『監視カメラ運用基準(CCTV code of practice)』(原語は、「CCTV=Closed-circuit Television」で「閉鎖回路テレビ」の意味。しかし、以下「ICO監視カメラ運用基準」という。)を作成・公表している。2000年に初版、2008年に改定版を出している。

【以下、レクチャーは改訂版による。】

([http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/ico\\_cctv\\_final\\_2301.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctv_final_2301.pdf)) ICO監視カメラ運用基準の附録第3「従業員の監視」では、監視カメラを使った行き過ぎの労務監視に一定の歯止めをかけることをねらいにルールを明らかにしている。

イギリスにおいては、1998年データ保護法（DPA = Data Protection Act 1988）の下、監視カメラを設置し収録した画像を含む個人データ処理を行う組織体はデータ管理者（data controller）を置かなければならない。データ管理者は、個人データを取り扱うにあたって、届出事項（氏名、住所、代表者、個人データのカテゴリ、取扱目的、データの提供先、および情報を欧州経済地域外へ移転させる場合の国名）ならびに、第7データ保護原則（情報の安全保護）遵守のための措置を、「情報コミッショナー事務局（ICO = Information Commissioner's Office）」に届出をしなければならない。

ICOは、届出を行った者の登録簿を保持しなければならない。データ管理者は、ICOの登録簿に搭載されなければならない。ちなみに、「情報コミッショナー事務局（ICO）」は、イギリス政府のプライバシーおよび情報公開に関する第三者機関である。【市民団体などからは、ICOは、政府の政策追認機関で存在意義や使命が不明との指摘もある。】

ICOは、1998年データ保護法（DPA）に準拠して、『監視カメラ運用基準（CCTV code of Practice）』を作成・公表した。ICOは、2000年に、第1版を作成・公表した。その後、2008年に『監視カメラ運用基準』改訂版（以下、「ICO監視カメラ運用基準」という。）を作成・公表した。2008年改訂版は、ECデータ保護作業部会が2004年に作成・公表した『ビデオ監視方法にかかる個人データ処理に関する見解（2004年4号）（Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance）』などを織り込み、改定を加えたうえで、公表したものである。

ICO監視カメラ運用基準の附録第3「従業員の監視（Monitoring your workforce）」では、就労場所（workplace）に監視カメラを設置したうえで監視する場合に、設置者や管理者に推奨する最低限の基準を定め、この基準に相当する自主基準がある場合を除き、この基準を遵守するように求めている。わが国における監視カメラによる職場監視の規制を考える場合にも参考になるとと思われる。そこで、以下に、ICO監視カメラ運用基準の附録3邦訳（仮訳）して、紹介する。

イギリス情報コミッショナー事務局（ICO）  
『監視カメラ運用基準』附録第3「従業員の監視」〔邦訳（仮訳）石村耕治〕  
ICO監視カメラ運用基準（CCTV code of practice）〔改定版、2008年〕より抜粋

店舗のような就労場所（workplace）に監視カメラ（CCTV）を設置するとします。この場合で、就労者（workers）の監視が主たる対象ではないが、就労者の画像をとらえる可能性もあるとします。カメラ監視の目的がもっぱら犯罪を防止および発見にある場合には、仕事量ないし会社の規程の遵守状況を測定

するためにそれを利用すべきではありません。

- ・カメラを設置する場合には、カメラがとくに就労者の画像をとらえる方角に向いていませんか。

- ・収録画像は、被疑者の犯罪行為がある場合に限り見ることになっており、就労者を常時監視するかたちになっていませんか。カメラが、犯罪の防止および発見を目的に設置されているにもかかわらず、犯罪目的以外に利用されていませんか。

- ・就労者の画像は、犯罪行為、明白な不正行為ないし他者に危険を及ぼす行為のような、放置できないことを見る場合に限り利用されていますか。

- ・就労者の画像が懲戒手続に使用される場合、当該就労者が撮影されたすべての画像を見たとうえで、質問に答えられるように、画像が保存されていますか。静止画像では十分でないのですか。

事案によっては、就労場所の監視を目的にとくに監視カメラを設置するのが適切であることがあり得ます。本監視カメラ運用基準の第4条に定める意思決定手続を踏んだうえで、その設置が正当であると認められるかどうか検討すべきです。とりわけ、より多くの研修またはより厳しい監督が、より適切な問題対処方法ではないかを検討すべきです。

事例：就労者が収納庫から物品を盗んでいる疑いがあるとします。この場合には、そこに監視カメラを設置するのは適切といえます。ただし、監視は継続的あるいは権利侵害的であってはならず、かつ、その問題に対処するに必要な程度でなければなりません。

事例：就労者が、会社の方針に反して、就労時間内に携帯電話を掛けている疑いがあるとします。そこで、終日就労者を監視するためにこれらの機の角度に向けて監視カメラを設置したいと考えているとします。これは、権利侵害的かつ必要性を超えた例にあたります。継続的監視は、きわめて例外的な状況においてのみ許されるべきです。例えば、毒性物質が使用され、かつ、手続を護らない場合には生命に重大な危険を及ぼす場合です。

- ・監視カメラの設置は、就労者が私用（private）となるべきと期待している領域以外に限定されるべきです。監視カメラは、便所あるいは私室に対しては利用されるべきではありません。

・就労者が、監視カメラが従業員の監視（staff monitoring）がねらいであり、かつ、どのような目的に使われるのか認識していますか。来訪者に対して監視カメラが作動中であることをどのように周知していますか？

・監視カメラが、内部方針を執行するために利用されている場合には、就労者はその方針を十分に理解し、かつ、十分な研修を受けていますか。

・被写体となった就労者からの画像開示申請に適切に対処するための手順を定めていますか。

就労者は、原則として、監視されていることを知らされるべきです。ただし、例外的に、秘密の監視が、特殊な捜査の一環として行われている場合は除きます。秘密の監視とは、ビデオまたは音声録音装置が利用され、かつ、監視対象者に監視が行われていることを知らされていない場合を指します。雇用主は、秘密の監視を認めるに先立ち、次の点を確認しなければなりません。

・これはあくまでも例外的なのですか、そして、犯罪行為があったと疑う根拠ないしそれに匹敵する非行があるのですか。

・特殊の捜査に対してのみカメラが利用されるのですか、そして、その捜査が終了したときにカメラは撤去されるのですか。

・カメラが利用されていることを就労者に教えることは、その捜査に不利益になりますか。

・事実を知らない就労者の権利侵害を考慮していますか。

・意思決定は、上級経営陣によってなされていますか。

監視カメラは、トイレや私室のような私用となる領域には、設置すべきではありません。ただし、きわめて例外的ですが、重大な犯罪の疑いがある場合には、その限りではありません。こうした例外は、唯一、警察が関与する意思のある場合に起こり得ます。しかし、純粋に内部的な懲戒事案ではあり得ません。

事案によっては、ある捜査に必要ということで設置された秘密のカメラが、他の犯罪行為ないし懲戒につながる犯罪の証拠を偶然に見つけ出すかも知れません。雇用主は、こうした証拠を、明白な不正行為ないし他人を危険に陥れる不正行為のような、重大な犯罪があると思われる場合に限り利用することができます。

す。こうした証拠を、軽微な懲戒事案に大げさに利用することは、不当です。

事案によっては、秘密の監視には、2000年捜査権限法（Investigatory Powers Act 2000）に基づいて定められた規則（RIPA）および2000年捜査権限法（スコットランド）（Investigatory Powers 《Scotland》 Act 2000）に基づいて定められた規則（RIPSA）が適用されます。必要に応じてアドバイスを求めることができます。

就労者の監視に関しては、ICO発行の雇用実務規程（Employment practices code）を参照できます。

## 2 人権尊重が求められる国交省のフルボディスキャナー実証実験

2009年12月末に起きた米機爆破未遂事件では、テロ容疑者が、爆発物を下着に縫い込んで、空港の金属探知機をすり抜けた。

この事件が大きな契機となり、これまでの「金属探知」や「ボディチェック（pat-down）」では不十分ということで、世界各地の空港で、乗客や搭乗員の人体全体へ電磁波を照射し、「全身透視画像を撮って検査する機器（フルボディ・イメージング・マシン・全身透視画像検査装置）」が導入されてきている。この機器は、英語では「フルボディスキャナー（full body 【whole body】 scanners）」と呼ばれる。

### （1）国交省主導でフルボディスキャナー検査の実証実験開始

国交省は、7月5日から9月10日まで、成田国際空港で、フルボディスキャナー検査の実証実験を開始した。実証実験計画を読むと、「有用性」を強調しつつも、実施に先立ち、被検者である個人、乗客のプライバシーについては、かなり慎重な検討がなされていると見てとれる。しかし、この透視検査では、人体全体へ電磁波を照射し、「個人の全身（あるいは全裸）の3次元画像」を取り扱うことにつながる。乗客には、嫌悪感が極めて強い検査方法である。

### （2）各国で問われるフルボディスキャナー検査

今回は実証実験だが、それでも、この検査方法に対する乗客の感情などを勘案したうえで、かなり慎重な運用が求められる。事実、アメリカなどでは、女性乗客がフルボディスキャナー検査で「侮辱を受けた」という苦情が、空港当局へかなりの数で寄せられている。

また、アメリカ、カナダなど各国のプライバシーを守る市民団体は、「この検査方法はプライバシーの侵害にあたる」あるいは「人種差別につながる」などの理由で、フルボディスキャナーの利用を止めるように訴えている。

イギリス政府の平等・人権委員会（Equality and Human Rights Commission）も、空港でのフルボディスキャナー検査に慎重な姿勢を明らかにしている。この検査方法が、プライバシー侵害に加え、特定国出身者などへの人種偏見を助長したり、信教の自由を侵害することにつながる恐れも強いというのが主な理由である。

### （３）全身への電磁波照射は危険ではないのか？

フルボディスキャナー検査では、電磁波を人体全体へ照射することになる。ここで照射する電磁波は、ミリ波（テラ波）で、人体にはほとんど影響がないとされる（安全性についての科学的根拠を確認できていない、という意見もある）。X線とは異なり、安全性は高いとされる。

危険なX線の照射ではないとはいうものの、透視をねらいに電磁波を「人体全体へ照射する」ということで、健康への不安感は強い。とりわけ、妊娠している女性などへ不安を与えるものであってはならない。

女性乗客へ妊娠しているかどうかを問うことも一案であるが、そもそも妊娠しているかどうかは本人の高度のプライバシー【センシティブ情報】である。ある意味では、医療情報などと同類とみてもよい。したがって、フルボディスキャナー被

スキャナー使用「全身透視画像」



検者の選択において、女性乗客に妊娠の有無を申告させること自体、慎重でなければならない。

### （４）問われる検査方法の妥当性

これまでの検査方法とは異なり、フルボディスキャナーによる透視検査では、「個人の全身（あるいは全裸）の3次元画像（three-dimensional images of individual's naked bodies）」を取り扱うことにつながる。乗客の嫌悪感、恥辱感、プライバシー流出などへの不安感はすこぶる強い。

事実、アメリカにおけるフルボディスキャナー検査に対するクレームの大半は、女性乗客からのものである。透視のためにミリ波などを全身に照射し、全裸にして検査することに対する被検者の嫌悪感、羞恥心への配慮不足に起因している。

フルボディスキャナーによる透視検査で検知される画像情報は、見方によっては、医療情報と同じような本人の高度のプライバシー【センシティブ情報】である。「テロ防止・安全対策」という「利益（法益）」と、「乗客個人のプライバシー権」の保護とのバランスのとれた対応が求められている。

「性悪説」、つまり、乗客全員がテロリストと仮定してのフルボディスキャナー検査の広範な利用には異論がある。とりわけ、テロの可能性がほとんどない状況で、恒常的にフルボディスキャナー検査を実施し、乗客に対して一方的に受忍義務を課するのは、問題が大きい。「テロ防止・安全対策」上の「必要益」を著しく越え、「乗客個人のプライバシー権」上の「保護法益」を不当に侵害するものといえる。こうした運用はゆるされないものと解される。

最高裁は、判決で「みだりに撮影されない権利」、つまり「肖像権」を認めている。一般に、肖像権は広い意味でのプライバシー権の一部と解されている。フルボディスキャナー検査では、原則として「記録映像」は残さない、消去するとしている。また、女性の検査は女性の検査者が担当するとしている。

しかし、電磁波を全身の照射し、被検者の高度の全裸画像を撮像し、検査することは、実施の仕方次第では、本人の肖像権、プライバシー権の侵害につながるおそれもある。

### （５）被検者の同意が前提

公的機関や民間機関が市民に個人情報の提供を求める場合には、事前に「本人の同意」を得るこ

とがプライバシー法上の鉄則である。したがって、仮に正式にフルボディスキャナー検査を導入するとした場合には、被検者の事前の同意を得る仕組みをどのように構築するかは重い課題となる。

レギュラーに航空機を利用している乗客などは、爆発物を機内に持ち込む可能性はほとんどないことは、搭乗履歴などから容易にチェックできるはずだ。こうした乗客については、従来の金属探知・ボディチェックで十分であろう。また、フルボディスキャナー検査を本人が望まないならば、当然、従来の検査方法の選択が許されてよい。「いやな奴は乗るな」といった荒っぽい理屈で済まされることではない。

#### (6) 求められる検査システムの「見える化」

フルボディスキャナー検査システムの「見える化」をさらにすすめ、この「システムの運用を常時「乗客・市民が検査」できる体制」をどう確保するかが最大の課題である。法制上の根拠もなく、市民に不透明なかたちで安易にこうした検査方法を正式に導入し、まじめな乗客・市民のプライバシー権を危殆に陥れることは許されない。

憲法13条【個人の尊重】は、「すべての国民は、個人として尊重される。」と定める。また、憲法31条【法的手続の保障】は、「何人も、法律の定める手続によらなければ、その生命若しくは自由を奪われ、又はその他の刑罰を科されない。」と定める。フルボディスキャナー検査システムの運用の仕方次第では、違憲となる疑いも出てくる。

### 3 イギリスでは、新政権が政治主導で「監視カメラ濫設規制策」を実施

イギリスでは2006年5月の総選挙で政権交代が実現した。新連立政権は、前労働党政権下で実施されたさまざまな国民の自由を制限する政策を転換する方針を明らかにした。

#### (1) 監視カメラ大国、イギリスにおける従来から監視カメラ規制策

イギリスは、世界でも名だたる監視カメラ大国として知られている。しかし、監視カメラの設置に、まったく規制がなかったわけではない。

すでにふれたように、英政府の第三者委員会・情報コミッショナー事務局(ICO=Information Commissioner's Office)は、1988年データ保護

法(Data Protection Act 1998)に準拠して「ICO監視カメラ運用基準」(ガイダンス、「ガイドライン」に相当)【CCTV code of practice 1008】を公表し規制を加えてきた。

イギリスの場合、データ保護法は、原則として私人の生活や家族に関する事項には適用がない。したがって、私人の家屋や敷地などに設置する監視カメラには、監視カメラ運用基準は適用にならない。

イギリスにおいては、伝統的に「パブ」が庶民の社交場所として重い役割を担ってきた。しかし、ICOは、アルコールや食事を提供するパブに設置された監視カメラについて、数多くの苦情を受けていた。このため、別途に、「パブに設置された監視カメラに関する運用基準」(ICO view of CCTV in pubs in England)(以下「パブカメラ運用基準」という。)を作成・公表している。

イギリスの場合、アルコール飲料を提供するパブは、酒類の小売免許が必要である。この小売免許の発行・更新にあたり、申請者は、パブカメラ運用基準にしたがって適正に監視カメラを設置・運用するように求められる。

監視カメラ規制においては、その目的(必要性)を超える「性能」や「数量」のカメラの設置に対して一定の歯止め策が必要である。これを監視カメラ規制における「つり合いの原則」あるいは「比例原則」という。

しかし、ICO監視カメラ運用基準では、「数量」規制をかけていなかった。このため、監視カメラの「濫設」に歯止めをかけるのは難しい実情にあった。このことが、新政権の「監視カメラ政策の見直し」にもつながった。

#### (2) 前政権が導入した「国民ID〔身分登録証明〕カード制」を廃止

2006年に前労働党政権は、ID【身分登録証明】カード法(Identity Card Act 2006)を制定し、国民・居住外国人全員に順次、生体認証式の身分登録証カードを発給する政策を実施した。

いわゆる「国内版パスポート(inner passport)」、「現代版通行手形」の常時持ち歩かせる制度を導入したわけである(PIJ発行のCNNニュース55号では、イギリス労働党政権の「ID【身分登録証明】カード制導入」案を紹介した。参照願いたい。)

だが、市民団体に加え、当時野党であった保守党、さらに自由民主党(LDP)は、労働党政権

の「国民IDカード制」導入に反対した。政権を奪取した後は、人権侵害のおそれの強いIDカード制を廃止する旨を政権公約（マニフェスト）にうたっていた（CNNニュース55号、25頁参照）。

2010年5月に下院総選挙が行われた。この総選挙で勝利した後、LDPと連立した保守党政権（キャメロン党首・首相）は、5月14日に、DNAデータベースの見直しなどを含む、「IDカード制の廃止」を声明した。

### （3）データ監視社会へ逆走するわが国の民主政権

翻って、わが国の民主政権は、2013年までに国民IDカード【登録証】制の導入をもくろんでいる。真似した本家のイギリスが制度廃止したのにもかかわらずである。

民主党は、政権を奪取する以前に4度も住基ネット廃止法案を出したはずだが。政権奪取後は、豹変し、いまや“共通番号制（国民総背番号制）万歳”、現代版通行手形である“国民ID（カード）制万歳”の始末である。

民主政権の唱える「国民が主役」はどこかに吹っ飛んでしまい、役所のいいなりである。国民監視ツールである「共通番号付国民IDカード制」で、データ監視収容所列島化をめざしている。

私たち市民は、“共通番号付国民IDカードを携行・提示しないと市民生活ができない社会”の実現を望んではいない。将来に“負の遺産”を残してはならない。共通番号や国民IDカードは絶対に要らない。共通番号付国民IDカード制導入に加え、役人のいいなりになって消費税率10%の大衆増税を持ち出し普天間問題を煙に巻こうとした「菅」政権の「脱官僚政治」の看板ははげ落ちてしまった。「官」のお抱え運転手のようになって、これでは自民政権と同じ（いや、もっと悪い）わけで、「存在根拠なし」と見る人も多い。

### （4）イギリス、政権交代で「監視カメラ濫設規制」に政策転換

話をイギリスの新政権の監視カメラ規制策にもどそう。イギリスは、「監視カメラは有用」という見方が独り歩きし、“監視カメラ大国”と揶揄されるほど、国中に監視カメラが設置され、重症の“監視カメラ中毒症”にかかっていた。

新政権は、監視カメラ（CCTV）の無制限設置に規制をかける方針も打ち出した。政策転換の

理由は、監視カメラがテロリストや組織暴力の縮小にあまり効果がない。むしろ、人権面でのマイナス効果に配慮する必要があるとの認識に基づく。こうした政策は、LDPの政権公約を大幅に取り入れた結果でもある。

今回のイギリスの政権交代、“自由”、“人権”を大事にする政策を打ち出した保守党&自由民主党との新連立政権は、監視国家体制をすすめた労働党政権下で蹂躪された「国民の人権回復のための関連3法案」を議会で審議中である。

人権回復3法案は、連立政権のパートナーである自由民主党（LDP）【保守勢力である日本の自民党とは異なり、イギリスのLDPは超革新政党】の政権公約（マニフェスト）に基づいて議会上に上程されたものである。

### （5）新政権の人権回復3法案に盛り込まれた監視カメラ規制策

人権回復3法案のうちの一つ「自由（抜本廃止）法案（Freedom《Great Repeal》Bill）」には、「監視カメラの規制（Regulation of CCTV）」が盛り込まれている。それでは、新政権は、どういった監視カメラ規制を目指しているのでしょうか？

イギリスの自由民主党（LDP）は、2009年11月に（1）自由法案の全文および（2）自由法案逐条解説を公表している。（2）自由法案逐条解説（第7）で、監視カメラ規制の方向性を示しており、参考となる。以下に、仮訳して紹介する。

#### 《第7. 監視カメラ規制》

イギリスは、世界で最も監視された社会になっている。イギリスは、世界の総人口の1%以下を占めるだけなのに、地球上の監視カメラ総数の5分の1がこの国に設置されている。労働党が構築した全体主義国家（Big Brother State）においては、監視カメラはあらゆる場所に行き渡っている。イギリスには、400万台を超える監視カメラが設置されている。これは、人口あたり14人に1台、また、各人は、毎日、300台を超える監視カメラに撮影されている勘定になる。1990年代に、内務省は、犯罪対策費の78%を監視カメラの設置に費やし、過去10年間で5億ポンドを超える公金を監視インフラの構築へ投資してきた。

私どもは、監視カメラは万能薬でないと考えている。監視カメラは、スピード違反のドライバーを捕まえるためなどにも使われている。また、駐車場において、窃盗犯罪を防止するために使われている。にもか

かわらず、犯罪防止のため、あるいは、被疑者を法廷で裁くための、監視カメラが確実に役立っているとの証拠はほとんどない。内務省の研究では、次のように結論づけている。「監視カメラ・スキームは、一般的に見て犯罪抑止という面ではほとんど効果がない」と。また、監視カメラで収集した多くの証拠が、裁判所では不採用となっている。にもかかわらず、監視カメラはこの国のいたる所に広く普及してきており、その技術は日ごとの進歩してきている。カメラはいたる所に数を増やしてきており、例えば、自動ナンバープレート認識（ANPR = Automatic Number Plate Recognition）ソフトウェアを組み込んだ監視カメラ【いわゆる、我が国のNシステム】が出現している。監視カメラが本質的に規制を受けていないことに対して、次第に疑いの目が強くなっている。

自民党は、人々のあらゆる動きが記録される監視社会へ向かって夢中遊行させられるようになる前に、監視カメラの利用、その全面的な規制に向けて公に議論されるべきである、と考える。最近、議会上院が出した報告書は、次のように結論づけている。イギリスは、監視カメラの利用において「世界をリードしている」。しかし、その利用について、「ほとんど制限がない」。つまり、その利用について、明確な法的規制がない、と。法的規制に必要性について注目されているのは、唯一、自動ナンバープレート認識（ANPR）についてだけである。まさに、今、行動する時である。自民党は、プライバシー保護のために、監視カメラの利用と規制について【内閣の求めで女王が任命する】王立調査委員会（Royal Commission）に緊急に諮問して答申を求めたいと考える。ケンブリッジ市議会のように、多くの地方議会は、監視カメラの利用に関する運用基準の作成において優れた実績をあげている。このことは、王立調査委員会が、調査を開始し、法的な強制力のある運用基準の検討をする適切な場所といえる。

#### （6）ドイツでは、監視カメラ設置を認める法律に違憲判断も

イギリスは、議会主権の国であり、裁判所は違憲立法審査権を有しない。したがって、人権侵害、憲法違反を理由に不法な監視カメラについて裁判所へ救済を求めることは難しい。勢い、政治解決が求められてくる。

これに対して、ドイツは憲法裁判所を置いている。したがって、不法な監視カメラを認めることにつながる法律があれば、人格権（プライバシー）侵害を理由に憲法判断を求めることができる仕組みになっている。

2007年2月23日ドイツ連邦憲法裁判所は、バイエルン州データ保護法を違憲とした。バ

イエレン州データ保護法16条は「個人情報の収集は、収集している機関の管轄に属する任務を遂行するために必要である場合に許される」、また、同17条1項2号では「個人情報は、蓄積された目的のためにのみ、変更され、利用されることができる。」とアバウトに定めていた。しかし、この規定ぶりでは、監視カメラ（ビデオ録画）をする場合、その目的、動機、範囲などについて明確に限定するようには求められないことになる。これでは、市民は、自分の個人情報がどのように収集・管理・利用されるのかわからない。

連邦憲法裁判所は、公共空間での監視カメラ設置を無造作に認めることにつながる州データ保護法は、個人の自己情報コントロール権を侵害する」として憲法違反としたわけである。仮に個人情報を収集・利用するとしても、その詳細がデータ主体に明確になっており、あらかじめ法定されていないと人格権の侵害、憲法違反となるという論理である。（ある意味では、わが国憲法84条の租税法律主義・課税要件明確主義につうじるところがある。）

また、2008年3月11日、自動車登録番号読取装置（わが国のNシステムに相当）についても、ドイツ連邦憲法裁判所は、違憲と判断している。いわく、自動車登録番号読取装置という運転者など（本人）の人格権侵害を授權（許容）する法律では、法治国家である以上、その目的、動機、範囲などについて明確に限定するようになっていなければならない。とりわけ、この法律は、その装置で収集された情報は、犯罪記録とデータ照合（結合）できると規定している。しかし、こうした結合の結果、本人は、他者がどのような自己情報をもっているのかコントロールすることができなくなる。つまり、この法律は、番号を読み取られた本人の自己決定権（自己コントロール権）を奪うものであり違憲であるとしただけである。（ちなみに、わが国の最高裁は、自動速度監視装置による運転者および同乗者の容貌の撮影を合憲としている（昭和61年2月14日判決・最判集40巻1号48頁）。【平松毅『個人情報保護』（有信堂、2010年）などを参照】

#### むすびにかえて

～求められる“監視カメラを市民が監視”できる仕組み

ひとくちに監視カメラといっても、その利用目

的はさまざまである。ここでは、主に公共空間に設置された監視カメラを中心に据えて、その規制のあり方について点検してみた。

現在までのところ、法（条例）形式かガイドラインかを問わず、民間団体が制定したものなどを除けば、イギリスの「監視カメラ運用基準（CCTV code of practice）」（2008年）のような、監視カメラに関する全国共通の運用基準（モデル）の制定には到っていない。2003年の通常国会に提出された民主党法案「行政機関等による監視カメラの設置等の適正化に関する法律案」がある程度ではないかと思う。

民主党がつくったこの法案では、すでにふれたように、国の行政機関だけが法の適用対象である。地方や民間機関は法の適用対象としていない。私人・民間の分野はできるだけ私的自治に委ねるべきとの考えに基づいた立法案である。一つの尊重すべき見識ではある。

東京都杉並区の監視カメラ専門家会議でも、民間機関が設置・利用する防犯カメラについては、できるだけ自主規制（ガイドライン等）に委ねるべきとの意見もあった。しかし、市民サイドからの自主規制づくりが遅々として進まないなか、民間機関が設置する一定の防犯カメラも条例による規制の対象にすることにした。

もちろん、防犯カメラが要らない社会の構築が常に理想であることは言うに待たない。防犯カメラを設置しても、犯罪は設置されていない地域に移動するだけ。こうした規制法は、逆に監視カメ

ラ設置の“呼び水”になり、しまいには“監視カメラ列島化”、しかねないと危惧する声もある。しかし、この種の規制に一定の役割を期待しながら、防犯目的とプライバシーの保護とを両立させざるを得ないのも現実である。

商店会や自治会などの組織、民間のホテルやマンションの建設主などに、防犯設備の一部として、監視（防犯）カメラの設置を義務づける条例を定める自治体が相次いでいる。政治は、確実に“監視カメラ濫設”の方向を目指している。

これらの条例には、市民の自由と個人の尊厳を守り、監視（防犯）カメラの設置利用手続を適正化・透明化しようといった定めは見当たらない。“監視カメラを市民が監視”できる運用基準や法制づくりが急がれる。

また、イギリスのように、第三者機関である情報コミッショナー事務局（ICO）が作成・公表した「ICO監視カメラ運用基準（CCTV code of practice）」はあるが、基準に合格すれば、いくらでも設置できる環境にあったことから、あらたに誕生した政権が、“監視カメラの濫設規制”を打ち出した国もある。

イギリスの事例は、わが国にも教訓になる。いくら立派な監視カメラの運用基準や規制のための法制づくりに精を出しても、「街頭」などはもちろんのこと、「職場」に忍び寄る監視カメラなどの“濫設規制”ができれば、実効性のある“監視カメラを市民が監視できる体制”は確立できないからである。

## 偽造免許で住基カード詐取、振り込めサギに悪用 ～公的カードやコード番号は「おいしい犯罪ツール」？

CNNニュース編集部

**振**り込め詐欺グループの指示で、偽造した他人名義の運転免許証を使って、東京都練馬区役所から住基カードをだまし取ったとして、警視庁は9月13日、容疑者を逮捕した。容疑者は、詐取した住基カードで、携帯電話や口座を不正入手していた。東京都内では今年5月以降、同様の手口の事件が約20件確認されている。

住民票コードは、原則として“第三者には見せない番号”としてつくられている。このため、コ

ードの濫用はない。だが、住基カードは公的なIDカード（身分証明カード）。成りすまし犯罪者にとっては、“おいしい犯罪ツール”と映る。

民主政権がすすめる共通番号や国民IDカード制では、共通番号を“第三者にも見せる番号”として使うとしている。となると、成りすまし犯罪者にとっては、カードだけでなく、番号も“おいしい犯罪ツール”となるのは必至。わが国を「なりすまし犯罪者天国」へ導く共通番号や国民IDカード制は絶対にご免だ。

情報コミッショナー事務局 (ICO=Information Commissioner's Office)

# イギリスの監視カメラ運用基準

仮  
訳

邦訳 石村 耕治 (白鷗大学教授)

ICO監視カメラ運用基準 (CCTV code of Practice) [改定版、2008年]

(http://www.ICO.gov.uk/upload/documents/library/data\_protection/detailed\_specialist\_guides/ICO\_cctvfinal\_2301.pdf)

イギリスは、プライバシー保護や情報公開などの問題に対処するために、政府から独立した第三者機関として「情報コミッショナー事務局 (ICO = Information Commissioner's Office)」を設けている。

ICOは、1998年データ保護法 (Data Protection Act 1988) に準拠して、『監視カメラ運用基準 (CCTV code of Practice)』を作成・公表している。(“CCTV=Closed-circuit Television,”で“閉鎖回路テレビ,”の意味。しかし、以下「ICO監視カメラ運用基準」という。)

『ICO監視カメラ運用基準』は、2000年に、第1版が出された。その後、2008年に改訂版を作成・公表した。2008年改訂版は、ECデータ保護作業部会が2004年に作成・公表した『ビデオ監視方法にかかる個人データ処理に関する見解 [2004年4号] (Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance)』などを織り込み、改定を加えたものである。

イギリスにおいて、企業や機関などの「組織体 (body)」が、監視カメラを設置して画像 (images) を含む個人データ処理とするこの場合、ICOに届出 (notification) しなければならない。また、監視カメラを設置したうえで監視を行う場合には、設置者は、このICO監視カメラ運用基準 (ただし、ICO監視カメラ運用基準に相当する自主基準がある場合はそれによることも可能。) を遵守し、データ管理者 (Data Controller) を置いて、適正な管理をするように求められる。

ICO監視カメラ運用基準は、わが国の監視カメラ規制のあり方を考えるうえでも、参考になるとと思われる。そこで、以下に、ICO監視カメラ運用基準を抄訳 [仮訳] して、紹介する。

\*この邦訳は、イギリスの監視カメラ問題を学習研究する際の便宜をはかる目的で仮訳したものを公表するものである。したがって、正式に引用する場合には、原文を参照するように推奨したい。また、記者の許可なしにこの邦訳を二次利用・配布することは遠慮願いたい。

## 【コラム】 イギリスの「1998年データ保護法」とは

イギリスにおける個人情報保護の“基本法”は、「1998年データ保護法 (DPA = Data Protection Act 1998)」である。画像 (images) を含む個人データを取扱う企業や機関など「組織体 (body)」は、DPAにしたがってデータ処理を行うように求められる。個人データはデータ主体【わが国の個人情報保護法にいう「本人」の相当】の同意なく収集・処理することはできない。また、本人には開示請求権・訂正請求権を保障している。個人データを取扱う組織体は、データ管理者 (Data Controller) を置くことになっている。データ管理者については、情報コミッショナー事務局 (ICO = Information Commissioner Office) に届出なければならない。届出およびその更新はオンラインでもできる (online notification process)。

データ保護法は、別表で、次のような「データ保護に関する8原則」を規定している。

- 第1 個人データは、公正・適法に処理されること
- 第2 個人データは、特定の適法な目的がある場合に限って収集されること
- 第3 必要以上の個人データ処理の禁止
- 第4 個人データは、正確・最新であること
- 第5 個人データを、必要以上の期間を超えて保存しないこと
- 第6 個人データ主体の権利の保障
- 第7 無権限・違法な個人データ処理、偶発的な個人データ棄損・消失等への対策を講じること
- 第8 欧州経済地域（E E A）外への個人データ移動の原則禁止

\*ちなみに、情報コミッショナー事務局（ICO）は、データ保護法のほかに、情報公開法（Freedom Information Act 2000）環境情報規則（Environmental Information Regulations 2004）など、いくつもの法令を所管する独立委員会である。

## ICO監視カメラ運用基準 (CCTV code of Practice)

### 《目次》

- 第1．まえがき
  - 第2．この運用基準について
  - 第3．この運用基準の適用範囲
  - 第4．監視カメラを利用するまたは継続して利用するかどうかの判断
  - 第5．効率的な管理
  - 第6．カメラの選定および設置
  - 第7．装置の利用
  - 第8．収録物の管理および画像の利用
  - 第9．責任
  - 第10．管制
- 附録第1．1988年データ保護法：データ保護原則
- 附録第2．限定監視カメラ装置の利用者用のチェックリスト
- 附録第3．従業者の監視

### 第1．まえがき

監視カメラによる監視は、私たちの毎day生活の一部になっています。私たちは、数えきれないくらいの監視カメラでとらえられています。街頭を動き回るとき、店舗や事務所を行き来するとき、さらには道路や公共交通網を使って旅行するときといったように。監視カメラの利用については従来から一般市民の支持は得られてきてはいるものの、毎日仕事に出かける普通の個人の生活に介入

することにもなることは避けられません。情報コミッショナー事務局（ICO）の調査によりますと、一般市民は、監視カメラが、効率的で安全措置が施されたかたちで責任をもって利用されることを期待していることがわかりました。監視カメラの利用について一般市民の信用と信頼を維持するために、その利用に有用性があり、かつ、その利用が監視社会の一端を担っているとの疑念が増加しないようにすることは、必要不可欠です。

この運用基準は、2000年の初版の改定版です。2000年以降、監視カメラの利用方法や活用技術が進化し、かつ、監視カメラに適用する法的環境が広がったことで発行されました。また、監視カメラをもっとプライバシー・フレンドリーな方法で利用することを支援できるような動きがありました。この改定運用基準は、こうした状況の変化や現場で監視カメラがどのように使われているかを学んだ結果を初版のガイダンスに織り込んだものです。この運用基準の作成にあたり、監視カメラを利用している機関との話し合いが行われ、かつ、多くの重要な意見を徴収するために意見公募（公開諮問）が実施されました。

しかしながら、この運用基準の目的は、初版と同じです。すなわち、監視カメラを適正な運用基準にしたがって運用することを支援することにあります。監視カメラを運用する人たちがこの基準の定めを遵守することは、法律にしたがっていることにつながるだけでなく、その職責を真摯にまっとうしていると示すことによって一般市民の信頼を勝ち得ることもつながります。

リチャード・トーマス  
情報コミッショナー

## 第2 . この運用基準について

この運用基準は、監視カメラその他個人の画像を観察・収録する装置の運用関係者に対して運用上の適正なアドバイスをするものです。また、この運用基準は、(例えば、車両登録番号のような)個人に関連する画像のような情報にも適用されます。この運用基準では、参考事例において「監視カメラ」および「画像」の言葉を使っています。諸機関が保有する個人に関する情報には1998年データ保護法(DPA=データ保護法)が適用され、この運用基準に盛り込まれたガイダンスは、操作者がデータ保護法の規定にしたがって運用者の負う法的義務を遵守できるように支援するものです。

データ保護法は、諸機関に対して法的義務を負わせるとともに、個人に権利を付与する法律です。例えば、自己情報の開示を求め入手する権利や個人が損害を被った場合に賠償を求める権利です。

基本的な法的義務とは、データ保護法自体を遵守することにあります。この運用基準は、データ保護法に定める法的要件をどのように充足するのかについて情報コミッショナーの見解を記したものです。諸機関は、これらの要件を充足できる代替手段を選ぶこともできます。ただし、法律違反の危険がない場合に限られます。

この運用基準に記された見解は、法的拘束力を有するデータ保護原則(附録1として収録)に基づいています。データ保護原則は、データ保護法の要点をまとめたもので、監視カメラの存置および実際の操作にあたり遵守すべきことを定めたものです。この運用基準の各規定には、情報コミッショナーの見解に沿って適正運用が達成できるように積極的に取り組まれるべき問題を掲げています。

この運用基準に記された情報コミッショナーの見解は、次のようなことを目的としています。

データ保護法を遵守したうえで個人の画像を収録するのを支援すること

収録された画像が利用可能なこと、および、

画像が収録された人たちを再確認すること

この運用基準は、2000年(2001年に再

版)に情報コミッショナー事務局が発行した初版の運用基準および〔小規模利用者向けの〕補遺ガイダンスに取って代わるものです。初版が出されて以降に生じた技術的变化、操作上の変動および法改正を反映させたものです。

この運用基準は、その作成にあたり監視カメラの運用者や専門職がかかわっており、初版の運用基準を活用した人たちの経験を織り込んだものです。また、この運用基準は、ICOが行った監視技術に対する一般市民の反応に関する調査およびより一般的な「監視社会」問題に関する調査の結果を反映させたものです。

## 第3 . この運用基準の適用範囲

この運用基準は、次に掲げたうちのいずれかの目的で、識別できる個人の画像または個人に関する情報を収録する監視カメラその他の装置の利用に適用されます。

個人が何をしているかを観察すること。例えば、店舗にいる個人や街頭を歩いている個人を監視すること。

個人に関して何か処置をしようとする場合。例えば、犯罪を捜査している警察に画像を提供する場合

個人の画像をその個人のプライバシーに影響を及ぼす方法で利用する場合、例えば、画像をテレビ会社へ提供する場合

ほとんどの監視カメラは、個人の行動の観察、収録を目的としています。このことは、監視カメラを利用するほとんどの機関ないし企業に対しては、データ保護法およびこの運用基準の定めが適用になるということです。装置の規模は考慮されません。したがって、監視カメラ装置に対するデータ保護法の適用に関する小規模利用者向けの旧ガイダンスは、本運用基準に取って代わられました。

カメラの利用が家庭内目的に限定されている場合には、データ保護法は適用除外となります。この適用除外は、個人が押入り強盗から自分の家庭を護るために監視カメラを利用する場合に適用になります。この場合には、カメラが道路その他そ

の個人の家屋の近隣の領域を監視することになっても構いません。また、携帯電話、デジタルカメラ、家庭用ビデオカメラを使って、レクリエーション目的で撮影された画像も、データ保護法は適用除外となります。

事例：自分の家族内で利用する目的で自分の子どもの出生行為をビデオに撮る場合には、データ保護法は適用除外になります。

この運用基準は、本来的に、企業や諸機関が自らの監視カメラ装置を使って個人の画像を日常的に収録する場合を適用対象としています。特殊な画像収録装置については、この運用基準の適用対象になりません。もっとも、こうした特殊の装置であっても、データ保護法に定められた要件は適用になります。

法執行機関の秘密の監視活動には、この運用基準は適用になりません。なぜならば、こうした活動は、2000年捜査権限法（Investigatory Powers Act 2000）に基づいて定められた規則（RIPA）および2000年捜査権限法（スコットランド）（Investigatory Powers (Scotland) Act 2000）に基づいて定められた規則（RIPSA）が適用になるからです。

ニュースメディアまたは映画製作のような芸術目的での従来型のカメラの利用には、この運用基準は適用になりません。なぜならば、こうした利用は、データ保護法において特例の対象となっているからです。この運用基準は、メディアに対して監視カメラで収録画像を提供することには適用されません。

この運用基準のすべての定めが監視カメラ装置に完全に適用になるというわけではありません。画像の利用の規模によります。小規模利用者（例えば、零細小売業者）にも、データ保護法は適用になりますが、性能が高い装置ではないと思われる場合には、運用基準の多くの定めは不適用となります。本運用基準附録2では、監視カメラの利用が非常に限定的で、プライバシー侵害の危険は少なく、人手も限られている場合の特例的なガイドランスを定めています。もちろん、この場合でも、本則適用を選択することができます。小規模

利用者であっても、本運用基準附録2のあるチェックリストに掲載されていない目的で監視カメラ装置の利用を望む場合には、運用基準全体（本則）を読む必要があります。雇用主が自らの従業員の監視に監視カメラを利用する場合には、本運用基準の附録3が適用になります。

注：監視カメラで収録された画像にはデータ保護法が適用されます。この運用基準は、ダミーカメラまたは非操作型のカメラには適用がありません。

#### 第4．監視カメラを利用するまたは継続して利用するかどうかの判断

監視カメラの利用は、プライバシー侵害につながることもあります。なぜならば、法を遵守している多くの人たちを監視下に置き、毎日の行動の動きを収録することができるからです。監視カメラを利用するかどうかについては細心の注意が必要です。監視カメラの設置が可能である、それを維持できる、あるいは一般市民の支持があるということが、設置の一番の動機であってはなりません。有用かどうか、適切な対処方法であるかどうか、そして、個人に対してどのような影響を及ぼすかを、慎重に検討すべきです。

事例：夜間に、駐車場で、しばしば車がいたずらされ、ドアを押し破られるとします。この場合、監視カメラの設置よりも、照明の改善が、問題の解決にもっと効果的でないかどうかを熟慮すべきです。

こうした問題については、その評価の一部として、監視カメラ装置が人々のプライバシーの及ぼす影響を客観的に検討すべきです。これは、難しいあるいは時間のかかる手続になると思われるかもしれません。もちろん、評価の事務量は、設置を検討している装置の大きさや人々のプライバシー<sup>1)</sup>に及ぼす影響の度合によって異なると思います。

監視カメラの設置が、すべての条件を充足しているかどうかを判定する際には、影響評価の結果を用いなければなりません。そして、条件を充足していると判断した場合には、実際にどのように運用するかを決めなければなりません。

影響評価を行う場合には、次の事項を確認してください。

監視カメラ画像はどの機関が利用しているの

ですか。データ保護法<sup>2)</sup>に基づいて誰が法的責任を負うのですか。

その機関は、どのような目的で監視カメラを利用しているのですか。対処しようとしている問題は何なのですか。

監視カメラの利用によってどのような効果が得られますか。

監視カメラの技術が現実的にそうした効果を生むことができるのですか。もっとプライバシー侵害的でない解決策、例えば照明の改善、で同様の目的を達成できませんか。

特定できる個人の画像を必要としているのかどうか。あるいは、その装置は、個人を特定することができないような画像を利用することができますか。

設置を検討している特定の装備・装置は、現在望んでいる効果を生み、かつ、将来にわたっても適切であり続けますか。

将来の需要はどれくらいで、それがどれくらい広範な画像の利用につながるのですか。また、そうした需要にどのように対処するつもりですか。

監視下に置かれる人たちの意見はどうですか。

監視下に置かれることになる人たちの権利侵害を最小化するために、とりわけ、特別の懸念が示された場合には、どのように対応をしますか。

監視カメラ装置が、公共機関自体、あるいは公共機関に代わって運用されているとします。この場合、その機関は、幅広い人権問題、とりわけ、欧州人権条約第8条〔私的および家庭生活を尊重される権利〕の適用について検討する必要があります。このことから、次のような点を含めて検討することになります。

設置を計画している監視カメラ装置は、適切な法律に準拠しており、かつ、法律を遵守し

ていますか。

設置は、公共の安全、犯罪の防止または国家安全保障のような、緊急の要請に対処するための必要性によるものですか。

設置を適切と認める状況がありますか。

設置は、対処する問題とつり合いが取れていますか。

こうした事項にあてはまらない場合、監視カメラの利用は適切でないこととなります。

## 第5．効率的な管理

個人情報取扱について明確な基準を定めることは重要です。個人に関する画像の取扱についても同様です。画像の管理、すなわち、何を録画すべきか、画像はどのように利用されるべきか、画像は誰に対して開示できるのかなどについて、責任者を置くことも重要です。こうした判断をする組織体（body）は、データ管理者（data controller）と呼ばれ、法的にデータ保護法を遵守する義務を負います。

複数の機関が関係する場合、各機関がそれぞれ責務を負うことになっていることを忘れてはなりません。複数の機関が監視カメラ装置の目的や運用について判断を下した場合、データ保護法にしたがうと、複数の機関が責任を負うこととなります。警察が、地方団体の所有するカメラから「生の情報（live feed）」の提供を受けるのが一例です。

誰が画像の管理をし、かつ、画像をどのように利用できるのかを誰が決めますか。関係する複数の組織体が責任を共有することに同意していることおよび各組織体はその責任を自覚していますか。

自らがデータ管理者であることを情報コミッション事務局に届出をした一つ（あるいは複数の）組織体は、責任を負担していますか。届出は、画像を利用する目的、開示請求に応じることその他細目をカバーしていますか<sup>3)</sup>。

機関が、画像編集のような処理事務を、外部

の者に委託している場合、責任の所在について文書契約のなかにはっきりと記してください。契約において、画像は、機関の指示に基づいてのみ処理ができる旨を確認すべきです。また、契約においては、保存や適切な研修を受けたスタッフに担当させるなどの安全性の保障についても記してください。

さらに、監視カメラ装置を実際どのように利用するかを決定する明確な手続を定める必要があります。

画像の利用について、明確に定義されかつ特定された目的に合っていることを確認していますか。また、この点について、装置を運用している人たちと連絡を取り合っていますか。

実際に画像がどう取り扱われるべきかについて、この運用基準に基づいて、手続が明確に文書化されていますか。その手続には、開示についてのガイダンスおよび収録画像をどのように保存すべきかを含みます。こうした手続は、担当する人たちに周知されていますか。

従うべき手続を確認する責任は、指定された担当者に配賦されていますか。指定担当者は、基準が設定され、手続が基準に適合するかたちでとられるかどうかを確認しなければなりません。また、指定担当者は、監視カメラ装置がこの運用基準を遵守し、かつ、〔被写体となった〕本人からアクセス権行使がある場合にそれに応じる法的義務があることを確認しなければなりません。

手続が法令を遵守しているかを確認するために、定期的に積極的な検査または監査が実施されていますか。これは、装置の運用者自身または第三者が実施することができます。

監視カメラの利用について現在も正当な理由があるかどうかについては、定期的に検討されるべきです。情報コミッショナーへの届出は毎年更新しなければなりません。このことから、監視カメラを継続して利用すべきかについて考える時間は十分にあります。

## 第6．カメラの選定および設置

いかなる監視カメラ画像も、収録目的に合致するものでなければなりません。監視カメラの利用目的にかなうカメラ装置や設置場所を選ぶことは重要です。定置型カメラや移動式カメラはともに、その現場に設置されなければなりません。また、画像の収録にあたっては、関係のない領域を視野に入れてはならず、また、個人の私的財産のような、監視の対象とすることを予定していないものを収録しないように限定される必要があります。カメラは現場に設置されなければならず、また、装置に対しては、画像を鮮明に保つために必要な技術的な調整をしなければなりません。

事例：冬季に設置された定置型カメラは、春や夏の草木の成長によって見えにくくならないように点検をしてください。

監視カメラを利用する目的とは無関係な空間を視野に入れることを最小限にするためにカメラの位置は注意深く選ばれなければなりません。

監視カメラが特定の問題に対処するために設置されている場合、通常その問題が起きる時間帯にのみ収録されるように装置の設定を検討すべきではないでしょうか。あるいは、他のプライバシー・フレンドリーな画像処理方法の採用を検討すべきではないでしょうか。例えば、装置によっては、あらかじめ設定された領域の動きをとらえるかたちで、懸念すべき事件が起きようとするときに限って収録しはじめます。こうした装置は、長時間録画を可能にします。

カメラは、その技術的機能および設置される状況を考慮して、鮮明な画像を映し出すことができるように設置されていますか。

明るさや各カメラが観察する領域の幅を考慮して、カメラは適切に設置されていますか。

安全に破壊行為からカメラを保護するに適切なかたちでカメラが設置されていますか。

装置は、秒ごとに十分なサイズの画像、解像

および枠で映し出していますか。

更衣室やトイレのような、高度のプライバシー保護が期待されている領域において、カメラは、極端に重大事件に対処する必要があるなど、極めて例外的な状況がある場合に限り、利用されるべきです。この場合、監視対象となっている人たちがそのことを知ることができるように最大の努力が尽くされなければなりません<sup>4)</sup>。

どの程度鮮明な画像が適切といえるのか判断にあたっては、監視カメラの利用目的およびその目的達成に必要とされる鮮明度合を考慮する必要があります。内務省科学発展部（Home Office Scientific Development Branch）<sup>5)</sup>は、次の4つの分野のいずれに使用するかによって判断するように推奨しています。

監視（Monitoring）：通行の流れまたは、個人の容姿を撮像する必要がない場合において人々の動きを観察することです。

探知（Detecting）：顔面を観察する必要なしに、人の存在を画像で探知することです。

認証（Recognising）：知っている人物かを確認する、あるいは、知らない人物かを判断することです。

本人確認（Identifying）：裁判所においても合理的疑いを超えてその人物が本人であると確認するに利用できるような高鮮度の顔面画像を収録することです。

内務省マニュアルに盛られたガイダンスでは、それぞれの目的にしたがって必要とされる画像の鮮明度について詳しく記しています。

## 第7．装置の利用

監視カメラ装置が、その装置が設置された目的にあった鮮明度の画像を映し出せることは重要です。本人確認が目的であるにもかかわらず、本人確認に役立たないような鮮明度の悪い画像では、その装置を設置した目的を達成できません。

録画された画像および印刷物、さらにはライ

ブスクリーン映像が、適正かつ鮮明ですか。この点は、収録過程において詳細な画像を不用意に失うことがないようにするためにも重要です。

録画資料について圧縮装置の利用を考えていますか。デジタル装置では、高度の圧縮をすると、録画再生をしたときに鮮明度の悪い画像につながります。

画像の原形が不用意に損なわれないかたちで記録媒体を設定できますか。

画像が正確であるかどうかについて、日時を記録したスタンプを押すようなかたちで、定期的な検査を実施していますか。

自動顔面認証技術が利用されている場合、顔面画像が鮮明に録画される場所にカメラが設置されていますか。対応策を講じるのに先立ち、照合結果について人の手による点検が行われていますか。

装置が高鮮度の画像を映し出せるように、定期的なメンテナンスが実施されていますか。

無線式の装置が使用されている場合には、他に傍受されないように十分な安全措置が施されていますか。

監視カメラは、一般市民の会話を録音するために使用されてはなりません。なぜならば、これは、高度な権利侵害にあたり、正当とされないからです。したがって、音声録音の機能を有しない装置を選ぶべきです。装置が音声録音機能を備えている場合には、それを切るかその他望ましい対策を施してください。

十分な安全措置を講じたうえであれば、例外的に音声録音が認められる場合があります。それは、次のような場合です。

音声警告装置（例えば、急激な警告音のような騒音パターンを段階的に変更する装置）。会話は録音されてはならないし、運用者はそれを聞いてはなりません。

監視カメラの包囲網にある「救助ポイント（help points）」から救助を求める人が発する双方向音声情報。

警察の留置所の拘束領域のように、担当者と特定個人との間の会話において何を言ったのか信頼できる記録が必要となる場合<sup>6)</sup>。

タクシの「パニック・ボタン（panic button）」のように、特別の脅威に応じて記録が始まるもの。

例外的に音声録音認められる場合において、音声録音をするあるいはするかも知れないということは、はっきり表示しなければなりません。監視下に置かれている人たちに対して注意を促す放送をするための音声の利用は、監視カメラが設置された目的に直接関係する内容に限定されるべきです。

音声付の監視あるいは音声機能がある場合、それは利用できなくなっていますか。

警報装置に基づいて音声利用される場合、会話が観察されるあるいは記録されるのを防止する措置がとられていますか。

救助ポイントで音声会話をする場合、会話は救助を求める人がはじめられるようになっていますか。

注意を促す放送機能が利用される場合、その内容は、監視カメラ装置が設置された本来の目的にあたるものに限定されるようになっていますか。

## 第8．収録物の管理および画像の利用

### 8．1 画像の保存および観察

収録物は、画像の清廉性が維持される方法で保存されなければなりません。これは、監視カメラ装置に収録された個人に対して権利を保障し、かつ、収録物を法廷で証拠として利用することができるようにするためです。このためには、画像を保存し、〔不正な〕アクセスを制限できる媒体を

注意深く選ぶ必要があります。画像が法廷で証拠として利用される場合には、その画像をどのように取り扱うべきかを考えに入れて保存する必要があるかも知れません。さらに、収録された画像は、保存しておく理由がない場合には、破棄されるべきです。いつこの判断をすべきかは、まさに監視カメラの利用目的によります。

現代の監視カメラ装置の多くは、デジタル録画技術を採用しています。そして、これら新技術は独特の問題を抱えています。ビデオテープの場合は、テープを外すのはいとも簡単でしたから、警察のような法執行機関が捜査の一部として利用したいというときには、テープを提出することになります。権限のある法執行機関は画像を利用することができることになっている、ということ想定しておくことは重要です。画像が利用できないとなると、カメラ監視の目的を損なうことにもなりかねません。

法執行機関から要請があった場合、装置から容易に収録画像のコピーをつくれますか。コピーを作成するとすると、装置を稼働させておくことに問題が生じませんか。

収録画像を、法執行機関が直接利用できるようになっていますか。

収録画像をさらに詳しく検証するために領置したい旨の申出があった場合、どのようにしますか。

原則として、モニターでライブ画像を観察できるのは、運用者に限られます。ただし、モニター室の平面に現場を映し出すかたちでモニターできる場合は別です。

また、収録画像は、指定された安全室のような、限定された領域で観察されなければなりません。個人のプライバシー保護が求められる領域から得られる画像のモニターあるいは観察は、その権限のある者に制限されなければなりません。

モニターは、映し出される画像を考慮に入れて、正しく設置されていますか。

モニターが観察する領域は適切かつ権利侵害を起こすおそれがないですか。

モニターを観察できるのは、権限ある人に限定されていますか。

事例：銀行の顧客がモニタースクリーンで自分自身を観察することができるようになっており、これは問題がありません。なぜならば、顧客は、自分が見渡せないシーンはモニターで見ることができないようになっているからです。モニターを見ることができる顧客だけがモニターに映るかたちになっているからです。

事例：ホテルのレセプション領域にあるモニターが、レセプション領域外の視角にある廊下やエレベーターにいる顧客を映し出しているとします。この場合、モニターではホテルスタッフのみがそれらの領域を観察できるようにしなければなりません。したがって、一般の人はそれらの領域を観察できないように、モニターの向きを変えなければなりません。

知れません。

事例：一般市民の多くが、自分の車が被害にあっている監視カメラの映像場面を欲しがっているとします。被害者の加入している保険会社が裁判を起こすのに必要であるというのが理由です。この場合、その要望が、誠実なものかどうか、さらには、他の関係者の身辺に対する危険があるかどうかを考慮すべきです。

画像の開示を制限するための取決め方法は、監視カメラ設置の目的に合っていますか。

開示請求事務担当者が、開示に応じることが適切かどうか、また、どのような場合に不適切となるのか、状況を判断するに必要な分かりやすいガイダンスを用意していますか。

画像を誰（請求した者の氏名および機関の名称）に提供したのか、さらにはその請求理由の詳細とともに、開示の日付を記録していますか。

## 8.2 開示

監視カメラ装置から得られた画像の開示（disclosure）は、その装置が設置された目的にそって実施されなければなりません。例えば、装置が犯罪の防止や発見を支援する目的で設置されている場合、法執行機関が犯罪捜査の必要があるというときには、その機関に画像を開示することは適切といえます。しかし、本人確認のできていない個人の画像をメディアへ開示すること、あるいは、画像をインターネットで流すことは、適切ではありません。本人探しがねらいであれば、メディアへ画像を開示することができます。しかし、原則として、法執行機関以外にはこうした開示をしてはならないことになっています。

注：監視カメラ装置が犯罪の防止や発見を目的に設置されていないとしても、法執行機関が画像の開示を求めており、それに応じないとすれば犯罪防止や発見を妨害することにつながるとみられる場合には、開示は適切といえます。

画像の開示請求に対しては、慎重に対処すべきです。例えば、大量の収録画像の開示請求に応じることが、関係する個人には不当とみられる可能性があります。ある程度限られた状況においては、第三者に収録画像を開示する必要性が被写体となった個人の利益にまさり、妥当といえるかも

開示するかどうかは、監視カメラを設置している機関の決定によらなければなりません。情報開示するかどうかは、機関の裁量に任されています。ただし、裁判所の命令ないし情報開示の権利行使<sup>7)</sup>があり、それにとまう受忍義務を負う場合は別です。画像を警察のような他の機関に提供したとします。この場合、提供を受けた機関が、画像のコピー（副本）についてのデータ管理者になります。その機関は、副本の再提供に関しデータ保護法を遵守する義務を負います。

画像の開示方法に関し、請求した画像の受領者だけが観察するかたちになることを確認すべきです。

## 8.3 保存

データ保護法は、いかなる装置または収録物に対しても適用ある最長もしくは最短の保存期間について、何ら規定をしていません。したがって、収録画像の保存期間については、各機関におけるそれぞれの収録目的によるべきです。

各機関は、画像収録目的を達成するのに厳格に必要な期間を超えて画像を保存すべきではありません。しかし、法執行機関が犯罪捜査をしている

場合で、現場検証の一環として画像を観察する機会を与える場合など、長期間に渡り、画像を保存する必要が出てきます。

事例：自動現金預け払い機（ATM）の場所に詐欺防止目的で監視カメラ装置を設置しているとします。この場合、数週間に渡って画像を保存する必要があります。なぜならば、疑わしい取引は、被害者が銀行から明細書を受け取るまでは発覚しないからです。

事例：タウンセンターの監視カメラ装置が収録した画像は、犯罪があったことが明らかになるまでの期間保存される必要があります。例えば、1ヵ月間。正確に必要な期間は、経験に基づいて、できるだけ短くされるべきです。

事例：パブに設置された小規模な監視カメラ装置は、事件が極めて短期間に明らかになるとみられるということであれば、短期間だけ画像を保存することで足りるともいえる。しかし、警察に犯罪の届出をしてから、警察が画像を収集するまでの間、その画像を保存すべきです。

画像保存期間を短期間に設定していますが、これは、自身の画像収録目的に基づいて決定しましたか。

画像保存ポリシー〔方針〕は、監視カメラ装置を運用している人たちの理解を得て、作成しました。

保存期間終了時に、安全な方法で、確実に画像を永久に削除するための措置がとられていますか。

画像の保存期間の設定がこの運用基準にそっているかどうかについて、体系的なチェックをしていますか。

## 第9．責任

### 9．1 周知

カメラ監視を行っている場合、その旨を周知しなければなりません。

最も効率的に周知をする方法は、監視カメラの射程領域の入口に人目につきやすい表示をしたう

えで、さらにその領域の内部にも補強的に同じような警告表示をすることです。また、駅のように、すでに音声による広報が利用されている場合には、この警告は、音声で補強することもできます。

分かりやすく目立つ表示は、とりわけ、カメラ自体が非常に目立ちにくい場合、あるいは、監視下に置かれる必要がないと思われる人たちのいる場所に設置される場合に重要です。一般に、監視カメラで撮られているかどうか分かりにくい場合ほど、警告表示は、分かりやすく目立つことが重要です。

特別の事情がある場合には、監視カメラ装置を使って音声録音をすることもあります。このことについては、はっきりと目立つかたちで表示されなければなりません。

警告表示にあたっては、次の点に留意すべきです。

はっきりと見やすく、読みやすいこと、

その装置を運用している機関、監視カメラの利用目的および（これらの事項について監視下にある人たちが分からない場合）の連絡先に関する詳細を記すこと、ならびに、

歩行者あるいは車の運転者が見るのかなど、状況を勘案して、表示の大きさは適切であること。

監視カメラ装置を誰が運用しているのかがはっきりしている場合には、運用者について表示する必要がありません。例えば、店舗に設置された装置については、その店舗が責任を負うことは明らかです。一般市民から監視カメラ装置について質問があった場合に、誰が対応し、どう対処するのかをすべての従業者が理解している必要があります。公共空間（public spaces）やショッピングセンターに設置された装置については、それに責任を負っている会社、機関または当局の名称および連絡先の詳細を表示しなければなりません。

監視カメラが稼働中の旨を周知する表示をしていますか。

警告表示には十分な情報が記されていますか。

表示事例：「画像は防犯および公共の安全の目的で収録され、モニターされています。この監視カメラ装置は、ブリーントウン区評議会が管理しています。詳細は、電話01234567890」

## 9.2 情報主体の開示請求

個人は、自分の画像が収録されている場合、別段の約束をしている場合を除き、収録画像のコピー（副本）を提供してもらって、自分の画像の開示を求める権利があります。副本は、請求を受取った日から40暦日以内に提供しなければなりません。10ポンドまでの料金の支払を求められます（これは、現在議会が法定した最高額です）。開示請求人は、自分が画像主体であり、監視カメラ装置のなかに自分の画像があるかどうか確認ができるように詳しい情報を提供しなければなりません。開示請求があった場合、次の点を点検しなければなりません。

監視カメラ装置の運用関係者は、どのようにして画像主体からの開示請求の適否を確認するのですか。

画像主体からの開示請求を取扱う内部手続を定めていますか。この手続には、裁判になるときに備えて、請求が受理されたことやその取扱経緯などの記録が保存されているかどうかも含みます。

また、はっきりと文書化された手続があれば、開示請求があったときに、請求人である個人に説明して支援することができます。開示請求があった場合、次の点について判断をしなければなりません。

画像を探し出すのにどの程度の詳しい情報が必要ですか。本人確認に役立つように、請求人は自分自身の写真または監視カメラ装置で収録されたと信じる時にどのような服装をしていたかの記述書を提出する必要があるかどうかをはっきりさせることができますか。

請求のあった日付、時間および場所についての細目をはっきりさせることができますか。

請求された画像の提供にどれくらいに料金を課しますか（ただし、最高10ポンドまで）。その支払方法はどうしますか。このことを開示請求人に説明してください。

請求人に画像のコピー（副本）をどのように提供しますか。

開示請求人の画像とともに第三者の画像が映っている場合、第三者の画像をぼかす必要があるかどうかを検討しなければなりません。そのまま画像を提供することは第三者のプライバシーを、不当に侵害する、または正当な理由もなく侵害するもしくは危険に陥れることにつながるかもしれません。したがって、第三者の画像には、ぼかしを入れるべきです。多くの場合、権利侵害をしないかたちで画像の開示が可能です。

第三者の本人確認ができないようにすべきであると判断するとします。この場合、問題の画像に修正ないしぼかしを加える作業が必要となります。この作業を外注するために他の機関と契約をする必要が出てくるかも知れません。この場合、処理業者との間で、情報をどのように的確に利用し、かつ、確かな安全保護措置を講じる旨を記した契約を文書で結ぶ必要があります。

事例：公共空間に据え付けられた監視カメラは、街頭を歩く人たちや勤務先に通勤する人々を収録しています。何も不穏な事件も起きていない場合には、その画像を、第三者の画像に修正を加えることなく開示することができます。

事例：画像は、開示請求をした個人が、友人グループと一緒にタウンセンターの監視カメラに向かって手を振りながら映っています。この場合には、請求人は友人と一緒にいることをすでに承知していることから、プライバシーに対する期待益はほとんどないといえます。請求人に対して、友人の顔に修正を加えることなしに画像を開示したとしても問題がないように見えます。

事例：画像は、医師の手術室の待合所の様子を映し出しています。個人はプライバシーと秘密を漏らさないという高度の期待益を有しています。第三者の画像は、公開するに先立ち、修正（ぼかすあるいは削除）をすべきです。

## 9.3 情報公開 (Freedom of Information)

公共機関の場合、開示請求は、2000年情報公開法（FOIA = Freedom of Information Act 2000）【訳注：“Freedom”の原義は「自由」ですが、わが法との対比するにあたり分かりやすさを確保するために、ここでは「公開」という訳語を使います。】または2002年情報公開（スコットランド）法（FOISA = Freedom of Information Act 2002）に基づいて受理することになります。公共機関は、情報公開請求に責任をもって担当する数多くの職員がいます。これら職員は、その事務に精通しています。請求を受理してから20仕事日以内も対応しなければならないことになっています。

FOIA第40条およびFOISA第38条は、個人情報について2種類の適用除外を定めています。公共機関が、監視カメラ映像について請求を受けた場合に検討すべきことは、次のとおりです。

開示を求められた画像は、請求人のものですか。もし、そうであれば、その情報は、FOIA/FOISAが適用除外になります。したがって、この請求は、さきにふれたデータ保護法に基づく情報主体からの開示請求の問題として取り扱わなければなりません。

開示を求められた画像は、請求人以外のものですか。これらの画像は、その情報の開示がデータ保護原則と抵触しないのであれば、開示することができます。

現実的には、個人が、問題の監視カメラ画像から本人であることが確認できるとすると、その個人に関する個人情報にあたります。これは、請求者が、情報公開請求によって開示を求めた情報は、潜在的にいかなる目的に対しても利用できる画像となり、おかしくなります。関係する個人はこうした事態を想定していないものと思われず。したがって、こうした取扱は、データ保護法と抵触する不適切な処理といえます<sup>8)</sup>。

この運用基準は、情報公開請求の取扱に関する包括的なガイドではありません。

注：映像がFOIA/FOISAの適用除外となる場合、データ保護法に抵触することなく事例によっては、その理由を斟酌して、合法的に画像提供を受けることができます。開示請求に関するアドバイスとし

て、本運用基準第8〔画像の利用〕を参照ください。

#### 9.4 その他の責務

監視カメラ装置の管理者は、さらに、データ保護法の下で個人が有する2つの権利に注目する必要があります。一つは、実質的かつ不当な権利侵害もしくは危険を引き起こす可能性のある処理の停止を求める個人からの請求です（データ保護法10条）。そして、もう一つは、個人に対して自動処理されたデータを基に処分を下すことの停止を求めるための当該個人からの請求です（データ保護法12条）。

これまでの経験からすると、監視カメラ装置の管理者がこの種の請求を受ける可能性は極めて低いといえます。もし請求があった場合には、情報コミッショナー事務局が発行したこれらの請求権に関するガイダンスを利用することができます<sup>9)</sup>。また、処分を下す場合に、自動顔面認証技術を利用するとすれば、人権侵害が関係してきます。ただ、この場合は、データ保護法の枠内でいうもっぱら自動ベースで処理されたデータを使って行われる処分にはあたらないといえます。

監視カメラ装置が公共空間に設置される場合、監視カメラ装置を運用する機関は、安全産業局（SIA = Security Industry Authority）が設けている免許制度に注意を払うべきです。公共空間監視カメラ（CCTV）免許は、監視カメラ装置の管理サービスを、役務提供契約に基づいて運用専門職（operatives）が提供する場合に必要になります。イングランド、ウェールズおよびスコットランドにおいては、2001年民間安全産業法（Private Security Industry Act 2001）の下、SIA免許を得せずに公共空間監視カメラ管理者の委託契約を結ぶ場合、その運用者は刑事罰の対象となります<sup>10)</sup>。

#### 第10. 管制

この運用基準に盛り込まれたガイダンスにしたがい監視カメラ装置を設置したとします。その後の実務においては、継続的にデータ保護法および運用基準を遵守するように求められます。開示請求があった場合には、次のことをしなければなりません。

請求者に対して、画像主体としてどのようにして開示請求をしたらよいのか、請求を誰に

宛ててしたらよいのか、請求にあたってはどのような情報を提供すればよいのかを教示すること。

請求者に対して、この運用基準のコピーまたは情報コミッショナー事務局（ICO）のホームページの詳細を提供すること。

装置の管理または運用基準違反があった場合、どのように苦情申立てをしたらよいのかを教示すること。

監視カメラ装置または画像を利用するスタッフは、この運用基準を遵守するための研修を受けなければなりません。とりわけ、スタッフは、次のことを知っておいてください。

画像の収録および保存についての機関のポリシー（方針）

画像を安全に取扱う方法。

画像の提供要請、例えば警察からの要請、を受けた場合の対処方法。

画像主体からの開示請求への対応方法および請求を受けた場合の対処方法。

あらゆる画像は、犯罪者の手に落ちないように十分な安全措置を講じたうえで保護しなければなりません。安全措置には、次のような、技術的、組織的および物理的な措置を含みます。

無線の伝達装置に対して傍受を防ぐために十分な安全措置を講じること。

画像のコピー（副本）を作成する業務を適切なスタッフに限定すること。

画像のコピー（副本）が開示されたときに、受領者に安全に送達すること。

管制室および画像を保存する場所の安全を確保すること。

スタッフは安全手続についての研修を受け、

かつ、監視カメラ画像が不正に利用された場合にはスタッフには制裁が科されること。

スタッフに対して、監視カメラ画像が不正に利用された場合には、犯罪となる旨の注意を喚起すること。

この運用基準にしたがって文書化された手続は、機関内から選抜された個人または第三者によって定期的に審査されなければなりません。これは、その監視カメラ装置が継続して設置されている間について一定のスタンダードを確保するためです。

同時に、その装置が当初意図していた目的を果たしていることを確認するとともに、その有用性について定期的審査（少なくとも年一回）をすべきです。その目的を達成していない場合には、停止するか、あるいは、修正されるべきです。

監視カメラ装置の運用および個人の開示請求の仕方に関する質問に答える場合に利用できる情報がありますか。

その情報には、この運用基準の勧告に対する自身の見解およびデータ保護コンプライアンス（法令遵守）に関心をもつ個人に対する情報コミッショナー事務局の利用情報を含んでいますか。

コンプライアンスにかかる定期的評価（レビュー）を実施していますか。そのレビューには、この運用基準の定めに沿ったコンプライアンス（法令遵守）、継続的な運用上の有用性、および装置が継続的にその設置目的に適合しており存続に合理的理由があるかどうかの判断を含んでいますか。

レビューの結果についての記録が保存されていますか。また、その結果を取り入れて運用を行っていますか。

#### 注記

<sup>1)</sup>大規模な監視カメラ装置を設置する、あるいは、その利用を検討しており、それに対して重大なプライバシー

一侵害の懸念が占められたとします。この場合には、ICOのプライバシー影響評価ハンドブックの利用を検討することが望ましいといえます。

2) 監視カメラを企業ないし機関が使用するとします。この場合、データ保護法に基づいて法的責任を負う者（「データ管理者 (data controller)」）は、その企業ないし機関の構成員たる個人ではなく、組織体 (body) です。

3) コミッショナーへの届出は、それ自体で、監視カメラ装置が法令遵守していることを証するものではないことに注意してください。データ保護原則（附録1参照）を遵守する必要があります。あらゆる機関が届出を求められるわけではありません。現行の届出要件については、次のHPにアクセスすることで、資料を入手できます。[www.ICO.gov.uk/what\\_we\\_cover/data\\_protection/notification.aspx](http://www.ICO.gov.uk/what_we_cover/data_protection/notification.aspx)

4) 表示の利用については、第9「責任」を参照してください。

5) 監視カメラ操作要件マニュアル (v0.4 55/06)  
<http://scienceandresearch.homeoffice.gov.uk/hosdb>

6) 警察が使用する身体装着式ビデオ装置 (headcams) に対しては、ICOとの協議を経て制定された、内務省ガイドライン『身体装着式ビデオ装置 (Guidance for the police use of body-worn video devices)』が適用になります。the Home Office police publications page, <http://police.homeoffice.gov.uk/news-and-publications/> 参照。

7) データ主体のアクセスおよび情報公開請求についての詳しい情報は本運用基準第9を参照ください。

8) 情報公開法に関するもっと詳しい資料はICOのHPからも入手できる。第40条に関する特別ガイダンス (FOI Awareness Guidance No 1) [www.ioc.gov.uk](http://www.ioc.gov.uk)

9) 「どのように自分の情報を処理するのをストップさせるか」および「個人情報の自動処理に基づく処分の差止め」の資料は、ICOのHPから入手してください。[www.ICO.gov.uk](http://www.ICO.gov.uk)

10) この要件は、北アイルランドでは適用がない。詳しくは、[www.the-sia.org.uk](http://www.the-sia.org.uk)から入手ください。

(b) センシティブな個人データ処理については、法別表第3に掲げる要件の一つでも満たさないとき

2. 個人データは一つ以上の明確かつ適法な目的がある場合に限り収集されるものとする。また、個人データは、その目的に適合しない方法において再処理してはならないものとする。
3. 個人データは、それらを処理する目的との関係において、適切かつ妥当であり、かつ、過大であってはならないものとする。
4. 個人データは、正確でなければならず、かつ、必要な場合には最新に保たれなければならないものとする。
5. いかなる目的で処理される個人データも、その目的に必要なとする期間を超えて保有されてはならないものとする。
6. 個人データは、本法に定めるデータ主体の権利にしたがって処理するものとする。
7. 権限のないまたは違法な個人データの処理および個人データに対する過失による損失、棄損、または損害に関しては、適切な技術的および組織的な対策を講じるものとする。
8. 個人データは、ヨーロッパ経済圏 (EEA = European Economic Area) 外の国や領域に対して移転してはならないものとする。ただし、個人データ処理に関してデータ主体の権利と自由に関する十分な水準の保護を保障している国や領域については、その限りではない。

この附録は、データ保護原則を完全に説明したものではありません。詳細は、ICOの『法律ガイダンス (Legal Guidance)』参照ください\*。

\*The ICO's "Data Protection Act 1998 Legal Guidance"は、次のHPへアクセスしてください。[www.jco.gov.uk](http://www.jco.gov.uk)

## 附録第1 (Appendix 1)

### 1988年データ保護法：データ保護原則

1. 個人データは、公正かつ適法に処理されるものとする。ただし、次に該当する場合にはデータ処理を行ってはならない。
  - (a) 法別表第2に掲げる要件の一つでも満たさないとき

## 附録第2 (Appendix 2)

### 限定監視カメラ装置の利用者用のチェックリスト 小規模な小売店舗および事業所での監視の実施

監視カメラ装置およびそれを使って収録された画像は、装置を利用する目的ならびに監視カメラ装置およびその目的についての情報コミッショナーへの届出（1988年データ保護法に定める法定要件）についての責任者である\_\_\_\_\_によって管理されます。

私たち\_\_\_\_\_は、監視カメラ利用の必要性を検討し、犯罪の防止および発見ならびに顧客の安全保護に必要であると判断しました。監視カメラは、その他の目的には利用しません。私たちは、監視カメラの利用について年次評価を実施します。

	チェック日	担当	次回評価日
情報コミッショナーへの届出がなされ、次の更新日が記録された。			
装置の運用について責任を負う指定された個人がいる。			
装置は、法執行機関（通例、警察）が犯罪の捜査に利用できる鮮明な画像を映像でき、かつ、要請があった場合に装置から取出しが容易であることから、選定された。			
カメラは、鮮明な画像を映し出すことのできるように設置されている。			
カメラは店舗を訪問していない人の画像収録を回避できる位置に設置されている。			
監視カメラが作動中であることを示す見やすい表示がある。その表示には、その装置の責任者が明確でない場合の連絡先についての詳細が記載されている。			
監視カメラから収録された画像は安全に保存されており、限られた人数の権限ある者だけがアクセスできるようになっている。			
収録画像は、事件が明るみに出るに必要な期間（例えば、盗難の届出までの間）およびその事件を捜査するに必要な期間に限り、保存される。			
法執行機関に対する場合を除き、画像は第三者へ提供しない。			
ある個人が自分自身の画像のコピー（副本）を請求してきた場合にはどのように対応すべきかについて知っている。よく分からない場合には、申請があったときに、管理者が、情報コミッショナーに助言を求めることができることを知っている。			
装置が正常に稼働し、かつ、高鮮度の画像を映し出すことができるかを確認するために、定期的なチェックが実施されている。			

このチェックリストは、次回の評価の日まで安全な場所へ保管してください。

## 附録第3 (Appendix 3)

### 従業員の監視 (Monitoring your workforce)

店舗のような就労場所 (workplace) に監視カメラ (CCTV) を設置するとします。この場合で、就労者 (workers) の監視が主たる対象ではないが、就労者の画像をとらえる可能性もあります。カメラ監視の目的がもっぱら犯罪の防止および発見にある場合には、仕事量ないし会社の規程の遵守状況を測定するためにそれを使用すべきではありません。

カメラを設置する場合には、カメラがとくに就労者の画像をとらえる方角に向けていませんか。

収録画像は、被疑者の犯罪行為がある場合に限り見るようになっており、就労者を常時監視するかたちになっていませんか。カメラが、犯罪の防止および発見を目的に設置されてのにもかかわらず、犯罪目的以外に利用されていませんか。

就労者の画像は、犯罪行為、明白な不正行為ないし他人に危険を及ぼす行為のような、放置できないことを見る場合に限り利用されていますか。

就労者の画像が懲戒手続に利用される場合、当該就労者が撮影されたすべての画像を見たとうえで、質問に答えられるように、画像が保存されていますか。静止画像では十分でないですか。

事案によっては、就労場所

の監視を目的にとくに監視カメラを設置するのが適切なことがあります。本監視カメラ運用基準の第4条に定める意思決定手続を踏んだうえで、その設置が正当であると認められるかどうか検討すべきです。とりわけ、より多くの研修またはより厳しい監督が、より適切な問題対処方法ではないかを検討すべきです。

事例：就労者が収納庫から物品を盗んでいる疑いがあるとします。この場合には、そこへ監視カメラを設置するのは適切といえます。ただし、監視は継続的あるいは権利侵害的であってはならず、かつ、その問題に対処するに必要な程度でなければなりません。

事例：就労者が、会社の方針に反して、就労時間内に携帯電話を掛けている疑いがあるとします。そこで、終日就労者を監視するためにカメラの角度に向けて監視カメラを設置したいと考えているとします。これは、権利侵害的かつ必要性を超えた例にあたります。継続的監視は、きわめて例外的な状況においてのみ許されるべきです。例えば、毒性物質が使用され、かつ、手続を護らない場合には生命に重大な危険を及ぼす場合です。

監視カメラの設置は、就労者が私用（private）となるべきこと期待している領域以外に限定されるべきです。監視カメラは、トイレあるいは私室に対しては利用されるべきではありません。

就労者は、監視カメラが従業員の監視（staff monitoring）がねらいであり、かつ、どのような目的に使われるのか認識していますか。来訪者に対して監視カメラが作動中であることをどのように周知していますか。

監視カメラが、内部方針を執行するために利用されている場合には、就労者はその方針を十分に理解し、かつ、十分な研修を受けていますか。

被写体となった就労者からの画像開示請求に適切に対処するための手続を定めていますか。

就労者は、原則として、監視されていることを知らされるべきです。ただし、例外的に、秘密の

監視が、特殊な捜査の一環として行われている場合は除きます。秘密の監視とは、ビデオまたは音声録音装置が使用され、かつ、監視対象者に監視が行われていることを知らされていない場合を指します。雇用主は、秘密の監視を認めるに先立ち、次の点を確認しなければなりません。

これはあくまでも例外的なものですか、そして、犯罪行為があったと疑う根拠ないしそれに匹敵する非行があるのですか。

特殊の捜査に対してのみカメラは利用されるのですか、そして、その捜査が終了したときにカメラは撤去されるのですか。

カメラが利用されていることを就労者に教えることは、その捜査に不利益になるのですか。

事実を知らない就労者の権利侵害を考慮していますか。

意思決定は、上級経営陣によってなされていますか。

監視カメラは、便所や私室のような私用となる領域には、設置されるべきではありません。ただし、きわめて例外的ですが、重大な犯罪の疑いがある場合には、その限りではありません。こうした例外は、唯一、警察が関与する意思のある場合に起こり得ます。しかし、純粋に内部的な懲戒事案ではあり得ません。

事案によっては、ある捜査に必要ということで設置された秘密のカメラが、他の犯罪行為ないし懲戒につながる犯罪の証拠を偶然に見つけ出すかも知れません。雇用主は、こうした証拠を、明白な不正行為ないし他人を危険に陥れる不正行為のような、重大な犯罪があると思われる場合に限り利用することができます。こうした証拠を、軽微な懲戒事案に大げさに利用することは、不当です。

事案によっては、秘密の監視には、2000年捜査権限法（Investigatory Powers Act 2000）に基づいて定められた規則（RIP A）および2000年捜査権限法（スコットランド）（Investigatory Powers 《Scotland》 Act 2000）に基づいて定められた規則（RIP S A）が適用されます。必要

に応じてアドバイスを求めることができます。  
就労者の監視に関しては、ICO発行の雇用実

務規程 (Employment practices code) を参照できます。

## 共通番号導入前提の国家戦略室の 「意見公募」に異議あり (PIJ国民総背番号IDカード問題対策チーム)

**政**府は、7月16日に、新たな「税と社会保障共通番号」(国民総背番号)の導入について、利用範囲やどのタイプの番号が望ましいかを、同日から8月16日まで意見募集した (<http://www.npu.go.jp/policy/policy03/archive07.html>)。今回の意見公募【アンケート調査】は、国家戦略室共通番号制度検討会が、参院選の直前の6月29日に公表された『中間取りまとめ』が土台。

この意見公募は、導入を前提とした“誘導型”、回答書式で実施。民主政権の背番号導入に賛成の人のみが、利用する範囲は、「税のみ」「税と社会保障」「幅広い行政分野」などの中から選ぶかたち。また、使う番号は「基礎年金番号」「住民票コード」「新たな番号」の3案から選ぶやり方。

そもそも新たな国民総背番号制導入に反対な人たちの意見はいらぬ、として排除される翼賛的な意見公募方式自体、社会調査方法としてまったく不適切。

アンケート調査の基となった『中間取りまとめ』では、共通番号が可視化して汎用されることで成りすまし犯罪社会化し苦悩しているアメリカ

などの実情についてはふれずじまい。また共通番号の汎用が国民の人権侵害につながる可能性、さらには、共通番号とそれを格納する国民ID【国民登録証・現代版電子通行手形】制度で、この国のかたちがどうなるのかについても、国民に説明責任を尽くしていない。

アンケートの説明では、共通番号制は「社会インフラとして整備する必要がある」と強調。つまり、「背番号を使って国民の幅広い個人情報を国家が管理するのは当たり前」というトーン。だが、わが国は、国民のトータルなプライバシーを国家管理する体制の国ではない。“個人情報”は国民各人の財産、が基本とする憲法秩序の国だ。

国家戦略室は、「反対意見があれば、選択肢を選んだ後にその理由を書く、記述欄に書いてほしい」としている、と報道された。だが、こうした社会調査手法自体が大問題で、これを平然とすすめる民主政権に大きな疑問符が付いている。

国民は、「ビッグブラザー」(Big Brother: ジョージ・オーウェルの小説『1984年』)に登場する国民を常時監視する監視国家体制をつくった独裁者の登場を望んでいない。

編集及び発行人

プライバシー・インターナショナル・ジャパン  
(PIJ)

東京都豊島区西池袋3-25-15 IBビル10F 〒171-0021  
Tel/Fax 03-3985-4590

編集・発行人 中村克己

Published by

Privacy International Japan (PIJ)  
IB Bldg. 10F, 3-25-15 Nishi-ikebukuro  
Toshima-ku, Tokyo, 171-0021, Japan  
President Koji ISHIMURA  
Tel/Fax +81-3-3985-4590

<http://www.pij-web.net>

2010.10.8発行 CNNニュースNo.63

### 入会のご案内

季刊・CNNニュースは、PIJの会員(年間費1万円)の方だけに送りしています。入会はPIJの口座にお振込み下さい。

郵便振込口座番号

00140-4-169829

ピ・アイ・ジェ - (PIJ)

### NetWorkのつぶやき

・河村たかし名古屋市長が、8月9日に定例記者会見で、共通番号と国民ID(カード)制問題検討のための外部委員会について発表。朝日新聞の記者も参加・質問。ところが、翌日の記事掲載なし。この外部委員会についても記事にしない。この新聞の最近の「偏向」体質が気になる。(N)