

巻頭言

機能不全の電子政府戦略、 "どうでも e-Japan、"

1 999年に、当時の小淵内閣は、「すべての行政手続を2003年度までに電子化」する構想をぶちあげた。同時に、当時の自治省（現総務省）は、住民票コード（背番号コード）と住基カード（国民登録証）を核とした住基ネットを強引に導入した。その後、2001年には、「電子政府（e-Japan - イ・ジャパン）」戦略も練り上げられた。

役人が当初「作文」したのとは裏腹に、行政手続の電子化は遅々として進んでいない。ようやく、e-Japanの目玉として、今年（2004年）2月から、住基カードなどが使える国税の電子納税申告（e-Tax）が東海4県で始まった。だが、このインタ-ネットを使ったe-Taxの利用者数は、去る5月末までで3,500件程度。この地域での申告総数の1%にも満たない。

国税庁は、今後、e-Taxの全国展開を目指し、2006年度までに全申告の5%を電子化するのが目標。だが、前途は多難だ。いちいち電子認証（電子証明書）などが要るインタ-ネット申告は、煩雑すぎる。誰も使いたがらない。納税者本人が電子申告する場合でも小難しい。ましてや、税理士など代理人が納税者本人に代わってインタ-ネット申告する場合はなおさらだ。

早くから電子出願制度を整備したのが特許庁。

ここでは、当初から、特許庁と弁理士との間での電子代理人出願（電子申請）には、インタ-ネットではなく、専用回線を使っている。特許庁は、2005年度中に、専用回線に加え、インタ-ネットからでも電子出願ができるインフラ整備をする予定という。だが、煩雑な電子認証が要らない専用回線を使った電子出願の方が、明らかに使い勝手がよい。インタ-ネット方式への早急な転換など止めた方が賢い。

一方、総務省のe-Japan戦略や国税庁のワナにはまってしまったのが、税理士会だ。

米国や豪州では、代理人電子申告には専用回線を使っている現実に目を向けようもしない。鳴り物入りでスタートしたものの、このままでは機能不全に陥るのは目に見えている。だが、役所社会主義の護送船団方式に物申す勇気もない。

インタ-ネット申告用の電子証明書の発行サービスを始めた民間会社も苦しんでいる。ミロク情報サービスは、これまでの発行数は200件程度とのことだ。当たり前である。格安の住基カードで電子認証ができるとなれば、個人納税者は民間の認証サービス業者など使わない。まさに、住基カードなど「民業圧迫」の典型だ。その住基カードの発行枚数も、昨年8月に始まって以来全国で25万枚程度とか、当初の計画の1割にも満たない。住基ネットは、その構築に約400億円、年間維持費に約200億円という巨大プロジェクト。

いまや、巨額のムダを生む「箱モノ」化しつつある。それでも、誰も責任を取らない、まるで他人の「どうでもe-Japan、」。

増税の足音だけが高くこだましてくる。

2004年10月12日

PIJ代表 石村 耕治

主な記事

- ・巻頭言～機能不全の電子政府戦略、「どうでもe-Japan、」
- ・《対論》求められる年金と課税データ照合プログラムの透明化
- ・杉並区、住基ネットで国と都を提訴へ
- ・金融所得一体化課税と選択納番制
- ・電子認証に関する質問の件
- ・ドイツにおける「監視カメラ規制」の現状
- ・監視カメラとプライバシー保護に関するECの見解
- ・プライバシーコラム・書評

求められる 年金と課税データ照合プログラムの透明化

—— 問われる密室での「年金保険料未納者の所得把握のための
納税者情報との照合」と「納税者データの不正閲覧」

対
論

河村たかし（衆議院議員・PIJ相談役）

石村 耕 治（白鷗大学教授・PIJ代表）

行政の効率化の進展とともに、行政手続の情報化・電子化がかなりのスピードで進んできている。税務の分野における電子申告や電子納税等の導入はその一つである。さらに行政の効率化を旗印に、税務分野と他の分野との間の情報交換の進み方も顕著である。最近の、年金保険料未納者の所得把握などをねらいとした、国と地方との間での納税者情報などの大掛かりな相互利用（データ照合）プログラムの稼働も、こうした動きの一つととれる。

国や自治体の税務行政は、さまざまな情報を大量にもっている。これら税務行政が保有する情報は、便宜的に、大きく「税務行政情報（又は税務執行情報）」と「納税者情報（又は税務個別情報）」に分けることができる。これらのうち、納税者情報は、とりわけ深くプライバシーに係わってくる。このため、職員に守秘義務を課すなどして目的外利用などを厳しく制限している。

しかし、一方で、納税者情報のデータ化・集約化で、行政の職員が個人情報をも幅広く拾い読み・不正に閲覧するのはますます容易な環境になりつつある。また、インターネットなどの通信手段を使えば、入手情報の外部提供も瞬時にできる。

こうした環境において、今後一層、情報主体である国民・納税者のプライバシー権、とりわけ「自己情報のコントロール権」をいかに的確に保護できるかは重要な政策課題となる。

今回の対論では、「自己情報のコントロール権」確立の課題について、論点を「年金保険料未納者の所得把握のための納税者情報との照合プログラムの透明化」と「納税者データの不正閲覧の法的統制」に絞って、石村耕治PIJ代表と河村たかし衆議院議員に議論を願った。

（CNNニュース編集部）

年金保険料未納者の所得把握のための 納税者情報との照合プログラムの透明化

（石村）国民年民保険料未納問題が大きくクローズアップされました。河村代議士は、この問題の火付け役だったようですが。

（河村）あっちこっちに飛び火して、どえらい問題になりました。まあ、しかし、いままで、役人が「密室」で、好き勝手にやってきたわけです。ここに、「国民のメス」が入ったことは、大きな成果ですね。

（石村）私も同感です。それで、今回は、未納問題の続きと言っては何ですが。最近、社会保険庁は国税庁（税務署）、総務省（市町村）と連携し国民年金の未納対策に本格的に取り組むことを決め、三省庁は年金保険料と税金の徴収情報の一部を2004

年分から相互に交換する方針を固めました。そこで、この問題について、「国民・納税者は主役」の視点から点検してみたいと思います。

（河村）分かりました。統計によりますと、国民年金の定額保険料を4割弱の人が払っていないとのこと。大変な数字です。この中には、国民年金保険料を納めなければならない程度の所得があるのに未納の人も多数いますからね。

（石村）それで、社会保険庁によると、これを発見しにくくしているのは未納者の正確な所得を把握できない制度的な欠陥も一因と言っています。

（河村）今回の三省庁の計画は、こうした欠陥を補うために、役所間でデータを融通し合おうというわけですね。

（石村）仰せの通りです。この計画がうまく運べば、社会保険庁は税務当局からの情報を生かし、

国民年金保険料の納付義務を果たさず未納を続ける人からの強制徴収を拡大することになります。一方で、税務署や市町村は保険料を納めたと虚偽申告して所得税・住民税上の社会保険料控除を受けるほ脱行為を防止できるとのことです。三省庁は、これらの情報を照合するためのネットワークシステム（データ照合プログラム）を、今秋から順次稼働させるとのことです。

（河村）それで、プログラムの内容はどうなっていますか。

三省庁による
データ照合プログラムの骨子

（石村）三省庁によるデータ照合プログラムの骨子は、次のとおりです。

(1)
まず年内に、社会保険庁と国税庁・税務署に照合システム導入し、2005年度初めをめぐり地方税事務の窓口となる全国約3,000の市町村に広げる方針である。社会保険庁や市町村の既存パソコンに専用ソフトを組み込み、それぞれが持つ個人情報の一部をインターネットや磁気テープで共有できるようにする。
(2)
社会保険庁は、明年（2005年）当初に、今年一年間の国民保険料リストか未納者リストのどちらかを国税庁と市町村に提供する。リストの管理番号には年金事務の管理に使っている基礎年金番号を添付し、この番号をマスターキーを使って、データ照合プログラムを実施する。
(3)
税務署は、そのリストをもとに保険料を納めた人にだけ社会保険料控除を認める。データ照合は明年、2004年分の確定申告から開始する。
(4)
一方、市町村は、社会保険庁のリストに基づいて保険料未納者の所得額リストを作成し、社会保険庁に提供する。国税庁と市町村は税額計算などに必要な個人データを共有しており、この一部を社会保険庁に提供することになる。

（河村）こうしたデータ照合プログラムは、未納保険料の強制徴収の強化や不正な税逃れの防止がねらいであることはもちろんのこと、保険料の未納を牽制する意味合いもあるわけです。

データ照合プログラムとは

（石村）わが国では、国土交通省の自動車登録ファイルと都道府県の自動車税ファイルとの照合プ

ログラムのように、これまでも、データ照合（データマッチング、コンピュータ照合）を実施してきました。

（河村）データ照合は、行政の効率化に不可欠と見るのはよいとしても、本質的には“情報の外部提供、目的外利用”にあたりますからね。

（石村）仰せの通りです。ちなみに、理論的には、照合実施機関内部での本来の目的を超える個人情報の利用を「目的外利用」と見て、外部機関へ個人情報を提供する「外部提供」と峻別してとらえることもできます。例えば、川崎市個人情報保護条例（10条）はこうした考え方をとっています。

（河村）こうした考え方に従うと、とりわけ三省庁間でのデータ照合プログラムにおけるデータ提供は“外部提供”にあたりますよね。

（石村）そうです。この場合の提供とは、一つのデータシステムないしはデータベースから他のものへのデータの移転行為を指します。

（河村）ここで言うデータ移転は、電話回線ないしはインターネットを利用するなど、システムないしはデータベース相互間での直接的な伝達だけを指すわけではないわけですね。

（石村）仰せの通りです。磁気テープなど実物を移転する場合やプリントアウト（印字）された情報を再入力する場合なども含まれます。

(1) データ照合プログラム実施の根拠規定

（河村）役所は、データ照合プログラムを実施するには法的根拠が必要ですよ。その辺はどうなっていますか。

（石村）現在の法環境を前提とすれば、一応、各税法における「官公署等への協力要請」（例えば、所得税法235条2項、地方税法20条の11）の規定とか、国民年金法上の「資料の提供等」（108条）の規定とかを根拠規定とみることになると思います。

（河村）ただ、この協力要請制度では、そのルールや法的限界はまったく明確にされていませんよね。となると、例えば、税務行政庁が、いかなる官公署に対し、いつ、どのような納税者情報の提供に応じたのかなどについて、情報主体である国民・納税者はこれを問題視するのは難しいですね。

（石村）ですから、手続を整備しないまま、現行の協力要請規定などを根拠に、各種のデータ照合プログラムをエスカレートさせていくことでよいのか、早急な検討を要する政策課題であるわけです。

（河村）問題点は分かりました。

(2) データ照合プログラムの実施と守秘義務

(石村) 前に触れたように、現在も社会保険庁は、保険料の徴収などに必要な場合には、未納者の所得情報などを市町村に求めることは可能なわけですが、しかし、守秘義務違反となる恐れがあるとのことで、協力に消極的な自治体も多い。したがって、現実には、照会ないしは照合は進んでいないわけですね。

(河村) この問題に対処する意味で、第159国会で成立した国民年金法の一部を改正する法律(平成16年6月11日、法律104号)では、加入者本人にも「資産又は収入に関する書類その他の物件の提出を命じることができる」(国民年金法106条)旨の規定を設けたわけですね。

(石村) 良し悪しは別として、これによって、市町村が、該当する情報を提供しても守秘義務との抵触を大分、回避しうる形となったと思います。

データ照合プログラムをめぐる諸問題

(河村) わが国では、これまでもデータ照合が実施されてきているけれども、国民、納税者にその運用の実態について、役所から説明がなされていないわけですね。

(石村) 役所には、データ照合に関し、国民、納税者の「自己情報のコントロール権」をどのように保障すべきかといった認識はほとんどないようにも見えますから。

(河村) わが国は、伝統的に「密室行政」でしたから、役人に認識がないとしても、事情は分かるような気もします。ただ、国民・納税者の側からすれば、自分の個人情報を役人が好き勝手に利用できるのでは怖いのでからね。

(石村) データ照合は、課税もれの防止とか、社会保障プログラムにおけるさまざまな不正のチェックなどを効率的に行うことを可能にします。このことから、「公共利益の保護」を理由に、その必要性が説かれています。

(河村) そうは言っても、一方では、プライバシー権の保護を理由に、無制約なデータ照合を認めてはいけませんし、厳正な法的コントロールの下に置かなければならないとの意見も強いわけですからね。

(石村) 仰せの通りです。こうした意見の根底には、次のような負の評価があります。

a	データ照合は、ある特定の目的のために提供、収集された情報を他の目的に利用することになる。しかも、データ照合は、プログラム内容が公開されないとすると、本人からの明示の同意を得ることなしにデータ移転を実施することにつながる。本人の情報上のプライバシー権、すなわち「自己情報のコントロール権」への保護を欠いたプログラムといわざるを得ない。
b	行政の効率化を旗印に、データ照合プログラムが際限なく拡大していくとすれば、住基コードや基礎年金番号などのマスターキー(共通番号)化はますますエスカレートし、「データ監視国家」化を推進することになる。とくに、住基コードと違い、基礎年金番号のように法的安全措置が十分でない番号のマスターキー化は、プライバシー権の保護面で由々しい問題をはらんでいる。
c	通例、税務調査などの行政調査の実施には、その調査の「合理的な必要性」が求められる。これに対し、データ照合は、実質的に、無作為抽出もしくは合理的な必要性の有無の確認がないままの恣意的な行政調査を認めるに等しい効果を持つ。
d	データ照合の結果、「当たり(hit)」と出た場合、その人を「不正あり」と推定しかつ当該個人に無条件に過重な挙証責任を転嫁する結果ともなりかねない。
e	一般に、データ照合は、「バルク・ベース(bulk base)」、すなわち、大量かつ一斉に実施される。このため、プログラムに誤ったデータなどが利用されると、「再調査の必要あり」と選出された人の感情、社会的な地位ないしは与信などに与える被害が甚大なものになる恐れがある。データの清廉性の確保、誤謬データの効率的な抽出、削除の制度化など、システム設計が入念になされないと、人権侵害を招きかねない。
f	データ照合により、個人の人物像をイメージすることが可能となる。時効のような仕組みもないことから、マスターキー(共通番号)を使い、複数の行政庁から得た個人情報に継続的に蓄積していくことにより、その個人の「全体像」をプロファイルすることも可能になる。つまり、利用済みデータの廃棄、その監視などについての統一的なルールがないと、国家(国・自治体)が各個人の「人物ファイル」を保有することを可能にする。

g	<p>一般に、他の行政庁から提供を受けた情報については、必ずしも安全管理がよくないことが指摘される。また、データ照合に係わる統一的なデータ管理基準（法律、ガイドライン等）がないと、データ照合の拡大に伴い、情報の不正開示や不正閲覧の危険性は格段に高まる。</p>
---	--

**データ照合プログラムの
透明化策をグローバルに点検する**

（河村）ここで指摘したことは、立法府としても、まじめに考えなければならない問題だと思います。

（石村）一般に役所は、データ照合プログラムは、行政機関個人情報保護法や各自治体の個人情報保護条例などの枠内で実施されなければならないのは当然であり、その枠内で実施されている限りでは、特別の法的規制は必要ないとする考え方をとっています。

（河村）ただ、今回の三省庁による年金・税金データ照合プログラムは、国と自治体にまたがるものですよ。

（石村）国の行政機関個人情報保護法でカバーできるかどうかの問題があります。しかも、規模的にも、わが国史上最大なものになります。

（河村）まさに、負の評価を避けるためにも、先進各国の立法例などを参考に、データ照合プログラムに対する法的ルールづくりをする好機といえますね。諸外国では、こういった法的ルールを置いているのでしょうか。

**（１）主要三カ国での
データ照合プログラム透明化法制**

（石村）先進各国でのデータ照合プログラム透明化の仕組みは多様です。一般法であるプライバシー保護法の枠内で対応する国。別途、個別法を制定して対応する国。個別のガイドラインで対応する国など、さまざまです。

（河村）まあ、分かり易くいくつか例をあげてください。

（石村）それでは、カナダ、オーストラリア、アメリカ合衆国（以下「アメリカ」）の三カ国に絞って、その実情を点検して見ましょう。

（ a ）カナダにおける透明化法制の特質

（石村）カナダは、連邦プライバシー法の運用監督にあっている連邦内閣予算局（TBC=Treasury Board of Canada）が、「データ照合政策実施ガイ

ドライン（Guidelines on the Implication of the Policy on Data Matching）」を公表しています。また、連邦のデータ照合プログラムについてはすべて、連邦プライバシーコミッショナーによる監査・評価などの対象となっており、事前通知が求められます。

（カナダ連邦内閣予算局（TBC）のHP参照
www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP2_5-1_e.asp）

（ b ）オーストラリアにおける透明化法制の特質

（河村）なるほど。他の国ではどうですか。

（石村）それから、オーストラリアは、個別法として、1990年に、連邦データ照合プログラム（給付及び租税）法（Data-matching Program《Assistance and Tax》Act1990《C t h》）を制定し、その後、1991年、1994年に、「データ照合プログラム実施に関するガイドライン（Guideline for the conduct of the data-matching program 1991,1994）」を公表しています。また、連邦のデータ照合プログラムについてはすべて、連邦プライバシーコミッショナーによる監査・評価などの対象となっており、「連邦行政庁におけるデータ照合実施に関するガイドライン（Guidelines for the Use of Data-matching in Commonwealth Administration）」を公表しています。

（オーストラリア連邦プライバシーコミッショナーのHP参照
www.privacy.gov.au/act/datamatching）

（河村）プライバシーコミッショナーとは、政府から独立した連邦議会直属のオンブズマンでしたよね。

（石村）そうです。プライバシー問題を専門に扱う特別オンブズマンです。

（ c ）アメリカにおける透明化法制の特質

（石村）最後に、アメリカは、一般法であるプライバシー保護法の枠内に、特段の規定を設ける形で透明化策を実施しています。1988年に「コンピュータ照合・プライバシー保護法（Computer Matching and Privacy Protection Act）」を制定し、それを一般法である「連邦プライバシー法（Privacy Act of 1974）」に編入しました。また、行政運営の総合調整任務をこなす大統領府にある行政管理予算局（OMB）が、連邦プライバシー法の運用監督にあたっています。同局は、各

種「照合プログラム実施に関するガイドライン (Guidelines on the Conduct of Matching Programs)」を公表しています。

(アメリカ行政管理予算局《OMB》のHP www.whitehouse.gov/omb/privacy/matching.html)

(2) アメリカ法制の下での透明化策の分析

(河村) アメリカは、オーストラリアやカナダとは異なり、議会直属の独立したプライバシーコミッショナー(プライバシー特殊オンブズマン)のような制度を置いていないですね。

(石村) 仰せの通りです。わが国と似た制度にあるとみてよいです。

(河村) と言うことは、アメリカのデータ照合プログラム透明化の仕組みは、わが国での透明化策を検討する場合の良いサンプルとなるわけですね。

(a) 照合プログラム実施の際の事前手続

(石村) そうですね。アメリカ連邦プライバシー法は、二つ以上の記録システムにある個人データをコンピュータを使って比較するプログラム(照合プログラム)の透明化についての規定を置いています(3条《o》項)。この規定によると、照合プログラムに参加するすべての行政機関内に、データ保護委員会を設けるように求めています。

(河村) データ保護委員会は、各役所の中でどういった役割を演じるのですか。

(石村) 照合プログラムに関する一切の監督・調整業務を行っています。その範囲は、プログラムの評価、費用対効果分析、年次報告書の作成・当該機関の長及び行政管理予算局への提出、コンプライアンス状況の検査などに及びます。

(河村) データ照合を実施する役所は、いろんな手続を踏むように義務付けられているんでしょうけど。

(石村) そうです。照合プログラムの実施にあたり、実施機関は、事前に、次のような手続を取るよう求められます。

その実施を連邦官報に、次の項目を公示すること
参加機関の名称、照合の目的、照合プログラムに実施する法的根拠、利用に供する記録と個人の種別、実施期間、パブリックコメント及び質問の提出先
提供機関と受領機関との間で、次の項目について書面による取決めをすること
照合の目的及び法的根拠、照合を正当とする理由及び予想される成果、利用に供する記

録と個人の種別、連邦からの給付・助成の受領等や連邦官職への応募に際し、提出された情報が照合プログラムの対象となる旨を、その申請時等に申請者に告知する手続、照合記録の保存及び廃棄に手続、照合される記録とプログラム実施結果への安全確保措置、照合に使用された情報のコピーや再提供の禁止、提供された情報の管理・返却・廃棄手続、照合に使われる情報の清廉性の評価、取決めの遵守状況を会計検査院長が監査できる旨など

その取決めを連邦議会の委員会に報告し、国民の閲覧に供すること

(河村) きちんとした手続を定めているんですね。

(石村) むしろ、わが国がひどすぎると見た方がいいのでしょうけど(笑い)。

(河村) これらに加え、他はどんな手続があるのですか。

(b) 照合プログラム実施後の手続

(石村) 照合結果に基づいてその後の手続を進めるにあたり、照合プログラムに参加した連邦行政機関は、情報主体である本人を保護するために、その本人の不利益処分の基礎として使われる情報について、独立して調査し、清廉性を確認するように求められます。

(河村) この調査・確認なしには、当該本人に対し不利益処分をすることができないわけですね。

(石村) そうです。それから、当該本人に対しては、調査結果を争う機会があることを告知しなければなりません。

(河村) この告知をしないで不利益処分をすることはできない。

(石村) そうです。ちなみに、調査結果に関する争いは、それぞれの申請に係る不服申立手続によることができます。

一方、情報の提供機関は、データ照合の取決めが護られないと信じる理由があるときには、受領機関に対し照合プログラムのために、いかなる情報も提供してはなりません。また、照合プログラムに関する取決めの更新を行ってはならないことになっています。

(河村) やはり、アメリカでは、個人情報を使役所が利用する場合には、本人の権利を尊重する考え方が、浸透していますね。わが国でも、議員立法も含め、真剣な検討が必要ですね。

納税者データの不正閲覧の法的統制

(石村) 話は変わりますが、わが国では、つい最

近、年金加入歴の漏えいが取りざたされました。

(河村) 社会保険庁職員が業務用カードを使い国民の年金情報が登録されている社会保険オンラインシステムにアクセスした場合には、一応記録が残るようですね。まあ、カードの管理とか、かなりずさんなようでしたけど。ともかく、アクセス記録などを参考に、厚生労働省が調査したところでは、東京の社会保険業務センターや全国312箇所ある各地の社会保険事務所などの職員328人が、「興味本位」で専用端末から個人データを閲覧したことを認めたとか。

(石村) 他にも、今年6月には、宇都宮市の主税課の職員が、自分の業務用IDカードを使って、トラブルになっていた隣家の人の個人情報を閲覧し、その内容をもとにその人を中傷していた事件が発覚しています。

(河村) この種の事件は、探せば、かなりの数あるのではないかと思います。

アメリカの 「不正閲覧からの納税者保護法」に学ぶ

(石村) かつて、アメリカでも、連邦税務行政庁である内国歳入庁 (IRS=Internal Revenue Service) において、職員による興味本位での不正閲覧が大きな問題になりました。

(河村) 課税庁の職員が、納税者データをのぞき見していたわけですか。

(石村) そうです。政治家とか芸能人とかの。そこで、1997年に、連邦議会は、「不正閲覧からの納税者保護法 (Taxpayer Browsing Protection Act)」を制定し、職員が興味本位で納税者データを拾い読みするのを禁止し、処罰の対象とすることで対処しました。その後、この法律は、連邦税法典である内国歳入法典 (Internal Revenue Code) に編入されました。

(河村) どんな規定を盛ったのですか。

(石村) 同法典によると、連邦職員 (IRSと契約関係にある一定の者を含む) または州職員は、法律で認められる場合を除き、連邦納税者の申告書もしくは申告書情報に故意にアクセス (閲覧) することは違法とされます。

(河村) 罰則は、どの程度厳しさなのですか。

(石村) 違法な閲覧をした者は、5,000ドル以下の罰金若しくは5年以下の懲役又は併科、プラス訴訟費用の負担を求められます。また、有罪の宣告を受けたときには、免職又は解雇されます (7213条)。

データ照合プログラムの導入と 不正閲覧からの国民・納税者保護策

(河村) わが国社会保険庁のケースでは、情報が漏えいした事実が確認できなかったということで「役所センス」の決着を見ました。年金個人情報の閲覧だけでは、国家公務員法や行政機関個人情報保護法などには抵触しないわけです。そのため、職務上の不適切な行為の責任を問い、反省を求めるということで、処分 (訓告や給与返納) は内規に基づくしかなかったというわけです。

(石村) 今後、稼動が本格化する三省庁による年金・税金データ照合プログラムでは、年金データと納税データがリンケージされることになりすからね。不正閲覧が行われれば、国民・納税者のプライバシー侵害の被害も甚大のものになりかねないわけです。

(河村) 内部牽制の強化はもちろんのことですが、ここであげたアメリカの立法例などを参考に、罰則をもって不正閲覧を防止する法的対応が必要な段階に入っていますね。

求められる 「開かれたデータ照合プログラム」

(石村) 課税漏れや社会保障プログラムにおけるさまざまな不正が多発し、手口が巧妙になってきています。「データ照合は絶対ダメ」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す。しかし、データ照合プログラムは、こうした不正摘発などの効率化に有用であると見るのはよいとしても、密室行政の延長線上で実施されてはならないわけです。また、その濫設、自由な運用を放置してよいわけはありませんから。

(河村) データ照合は、その運用次第では、個人の情報プライバシー権、「自己情報のコントロール権」を侵害するプログラムにもなりますからね。

(石村) ところが、今回の三省庁による年金・税金データ照合プログラムでは、今のところ「自己情報のコントロール権」を保護するための透明化策が、国民・納税者にはまったく見えてこないわけです。

(河村) アメリカなど諸外国でのデータ照合プログラムの透明化策を参考に、情報主体の「自己情報のコントロール権」を保障する統一的な手続、法的システムづくりが必要ですね。

(石村) この場合、プログラムの存在の公開・周知をはかることはもちろんのこと、国民・納税者が、その適正な運用に常時参加し監視できる仕組

みをしっかりと確立することが肝要です。また、プライバシー侵害的な照合プログラムについては、実施機関に対する自治体の住民情報提出拒否権なども制度化される必要があります。

(河村)仰せの通りだと思います。自治体が中央の役所の御用聞きのような感じでは、住民のプライバシー権は護れませんからね。

(石村)今回は、ご多用な折、対論に参加くださり、ありがとうございました。一つ、議員立法を含めて、この問題に真摯に対処くだされば幸いです。

(河村)重々承知しております。こちらこそ、今回は大変勉強になりました。石村代表のご活躍を期待しております。

8月24日、 東京都杉並区が 住基ネットで「区民選択制」を認めない 国と都を提訴へ！

CNNニュース編集部

東京都杉並区は8月24日、国および東京都を被告として、住基ネット受信義務確認等を請求する訴え(「住基ネット受信義務確認等請求事件」)を東京地方裁判所に提起した。

住基ネット稼動以降、不参加の姿勢を貫いている自治体はいくつかある。杉並区もそうした自治体の一つだ。国民の人格権を国が一元管理しようという住基ネット構想に対し、首長として抵抗してきた山田宏区長には敬意を表したい。当選するやいなや住基ネット見直し公約を反故にした、上田清司埼玉県知事や松沢成文神奈川県知事に比べると、山田区長はきわめて「誠実」である。

住基ネット不参加を貫く杉並区では、2003年(昨年)12月現在で、区民の約8割、42万7000人余りが住基ネットに参加を希望。一方、不参加希望は、残り8万6500人程度である。こうした住民意思を尊重する必要もあり、山田区長は「現実的な対応」を迫られていた。

そこで、山田区長は、昨年6月4日に、横浜市になって、住基ネットへの「区民選択制」での参加を求める方向に舵を切った。つまり、横浜市と同様に、将来の全員参加を前提にして段階的参加をする政策に転換する方針を打ち出した。

だが、国と都はこうした形での参加を認めようとしない。交渉にも応じようとしない。そこで、山田区長は、国と都を相手に訴訟を起こすことに決めた。

訴訟の骨子は、次のとおり。全員のデータをいったん都に送信し、不参加希望者分を削除するため、都がデータを受信する義務がある。

国と都に、区民の対し参加・不参加の意向を調査するためにかかった費用など4,476万円余りと訴訟費用の損害賠償を請求する。

区は、この訴訟に同意を求める議案を、2004年(今年)2月の区議会に提案した。しかし、提訴に反対ムードの自民・公明などの動きから、区議会は、国や都との交渉を見極めようという方向にシフトし、3月に、同議案は全会一致で継続審議となった。

ところが、その後、交渉は、一向に進まない状況にあった。そして、提訴議案は、再び今年6月の区議会に提出された。

どこの地方議会でも、国政レベル以上に、議員の動きは複雑怪奇である。この点では、杉並区議会自体も他と余り変わりがない。

6月15日、杉並区議会の午後の総務財政委員会では、午前中欠席していた「杉並自民議員連盟」に1人が欠席し、9人に委員で、国と都

を提訴する議案を審議した。委員からの質問に、区側は「交渉には進展が見られず、提訴するよりない」と回答。また、山田区長も、「地方と国とは対等な立場である」と主張した。

質問が終わってから、公明が「提訴は最終手段。区民の理解を得ることにもっと時間をかけるべき」として、提訴議案の継続審議を求める動議を提出した。委員長を除く委員8人のうち、公明2人、共産2人の4人が継続審議に賛成したため可否同数となった。その後、委員長が「議会の良心に従い道義を否決する」と、動議を委員長権限で否決した。すると、公明2人は「採決には加わらない」と退席した。その後、杉並自民議員連盟や民主などが「公平な判断を仰ぐべき時期にきている。こう着状態が続けば区民の利益が守れなくなる」として、提訴議案に賛成を表明した。最終的には、住基ネット不参加の継続を求める共産を除く、提訴議案を賛成多数で委員会可決した。

6月18日には、杉並区議会本会議で、提訴議案を賛成多数で可決した。

石原都知事は、「区民の意思に関して法律違反をしているのは杉並区の方だ。むしろ住基ネットを使えない杉並区民は区を訴えたらいい」といった姿勢。麻生総務大臣も、「区民選択制には応じられない。訴えを受けてたつしかない」との姿勢である。

国は、いわゆる「横浜方式」、つまり、住基ネットへの「全員参加を前提とした段階的参加方式」を、杉並区には認めようとしぬ。その理由は、裁判を通じて明らかにされよう。ただ、これまでのところ、国は、個人情報保護関連5法が成立し、住基ネットの本格稼働が実施されるなど、横浜市に認めたときは状況が異なっている、と説明。また、横浜市も、全員のデータが送信されないうちは、違法状態にある、との認識だ。

(訴状、訴訟提起に至った経過などについて詳しくは、杉並区HP参照

《www.city.suginami.tokyo.jp》)

《プライバシーコラム》

税理士事務所の所長をしています。従業員が勤務中に私用でEメールを使わないようにモニターしても問題はないのでしょうか

事務所の個々の従業員の氏名やEメールアドレスと結びついた形で送信したり受信したメールは個人情報にあたります。

個人情報保護法上は、モニタリングをする旨をあらかじめ従業員の知らせておけば問題ないとされます。ただ、厚生労働省は、2000年12月に「労働者の個人情報の保護に関する行動指針」を公表しています。

この中で、「電子メールのモニタリングでは原則として送受信記録、あるいはこれにメールの件名を加えた範囲について行うものとし、必要やむを得ない場合を除いてはメールの内容にまで立ち入らないようにするなど、あくまでも目的の達成に必要な不可欠な範囲内で行い、労働者

等の権利利益を侵害しないように十分配慮することが望ましい」としています。

一方、会社が従業員のEメールを無断でモニターしたことが問われた裁判では、「社会通念上相当な範囲を逸脱した監視がなされた場合に限り、プライバシー権の侵害となると解するのが相当である」と判示しています。

したがって、事務所内の私用メールに対するプライバシーの保護は極めて限られているといえます。問題を未然に防ぐためには、あらかじめ事務所の「Eメールポリシー」を定めておくのがよいでしょう。この場合、労使協調の観点から、所長のEメールについても従業員がモニターできるくらいの開かれた事務所づくりの姿勢が必要です。

関与先でEメールが税務調査対象となる時代ですから、事務所では私用メールを原則として送受信しないようにすることが肝要です。

(PIJ個人情報保護プロジェクトチーム)

不公平税制を助長し、 プライバシー公有化を招く

「金融一体化課税」も「選択的納番制」もいない

—— “選択的納番制” は一律納番制の「裏口導入」への “呼び水” ——

PIJ代表 石村耕治

納税者番号制度とは何か

納税者番号制度（「納番制」）では、納税者1人ひとりが、異なる番号（「納番」）を持つことになる。番号を付けるのは課税庁などで、納税者は勤め先や取引先などに出す資料や課税庁に出す申告書には、自分の納番を必ず書くことになる。また、給与を支払う勤め先、納税者と取引する金融機関、不動産会社なども、従業員、取引相手から聞いた納番を課税庁に出す資料には、必ず書くことになる。一方、課税庁は、各人の納番をマスターキーにして、納税者から出された申告書などの情報とその納税者の勤務先や取引先から出された資料の情報とをコンピュータで突合せ（名寄せ）し、申告内容が正しいかどうかをチェックする。

納番制は、脱税や課税漏れなどを防ぎ、所得の把握格差をただすのに役立つという見方がある。一方で、役所が各納税者のふところ具合や家計を含め幅広い金融プライバシー（人格権）を管理、公有化することになることから、導入への反対は根強い。だが、政府は、「金融所得一体化課税」という税金が安くなる新しい課税方式を希望する人にだけ納番をとってもらおう。嫌な人はとらなくともよいといった、いわゆる「選択的納番制」の形で、反対論を巧みにかわし、わが国への納番制の“裏口導入”を図る構えだ。

どのような付番の方式が 考えられるのか

わが国での納番制導入の本格的な論議は、1988年に政府税制調査会（「政府税調」）が導入を進めるべきだとする報告書を公表したことに始まる。

納税者は、大きく「個人」と、法人や法人格のない社団（任意団体）など「法人等」に分けられる。納番制の導入となると、この区分を基に納税者に番号を付ける（「付番」）ことになる。個

人や法人等のすべての納税者に対し課税庁が付番する（オーストラリア）方式と、法人等には課税庁が付番し、個人には住民票コード（北欧諸国）ないしは基礎年金番号（アメリカ、カナダ）など既存の番号を転用する方式がある。最近の議論から見て、わが国では、の方式となるのではないか。

「総合課税に納番制が似合う」 といていた政府税調

わが国の所得課税においては、従来から、公平な課税を実現するために、所得の種類により税金負担能力（担税力）に差異があることなどを考え、各所得ごとに金額を計算し、それらを集約し、総合課税する考え方を理念としてきた。

また、伝統的に、額に汗して得た給与のような「勤労所得」に軽く、一方で資産所得あるいはその一部である金融所得など、いわゆる「不労所得」に重く課税すべきであるという考え方を基調としてきた。こうした課税の原則や基調は、特定の階層の納税者に富・所得が過度に集中しないように、分かち合い・再配分する政策をとるのに有用であるからである。

かねてから、政府税調は、10種類に分かれている個人の所得のうち、利子や配当など、いわゆる“金融商品”から生じる「金融所得」が分離課税になっている現状は好ましくない。すべての所得を集約し、累進税率で総合課税にするのが公平である。そのためには納番制が必要だと説いてきた。

税制は「公平・中立・簡素」であることが基本とされる。2000年7月の政府税調『わが国税制の現状と課題』では、税制全体がこれらの基本原則にマッチしていること、その中でもそれぞれの担税力に応じて分かち合う「公平」が最も大切であると謳っている。また、とりわけ、個人に対する所得課税では、金融資産からの所得を含め、

総合課税を原則とすべきであるとしている。

政府税調、「金融所得一体化課税」、 選択的納番制」導入に豹変！

ところが、近年、政府税調は、この主張をやめた。そして今度は、「金融所得」に軽く課税するのに納番制が必要だといひ出したのである。まさに豹変。

2004年6月15日、政府税調は「金融所得課税の一体化についての基本的な考え方」を公表した。その骨子は、これまでの総合課税は事実上棚上げにして、各種の金融所得への課税は「20%の申告分離課税方式」に統一する。その上で当面、上場株式等の売却損益に限り他の金融所得とできるだけ幅広く相殺・損益通算を認める。

ただし、この課税を受けるには納番の取得を条件とする（「選択的納番制」の導入）というもの。

これで、「株の投資で損をしても、配当や利子などでも穴埋めできるようになる」という。現行は、株式取引で売却損を出した場合、同じ株式売却益の範囲では穴埋め相殺し、納税額を減らせる。だが、預貯金の利子など異なる金融商品から得た利益との間では相殺できない。政府税調は、これが、株式投資をためらわせ、個人の金融資産を現金・預貯金に一極集中（現在55%）させる原因と判断。そこで、納番制を入れて管理し、預貯金の利子など幅広い金融商品からの利益でも通算できるようにするというわけだ。

内実は、「株取引」でリスクを負った人だけへの優遇策。いわば「貯蓄（間接投資）しないで、株を買え（直接投資をしる）」という政策。これで、「貯蓄は美德」とずっと政府にマインドコントロールされてきた国民が、貯蓄から株取引に一拳にシフトするとは到底思えない。逆に、税収減を招いて、富裕層だけの優遇に終わりがかねないのだが。

上場株式等の売買損益については、現実には、今でも納税者が証券会社に開設した特定口座を通じれば、損益通算できる。また、損益通算の対象を預貯金の利子にまで広げるから納番制が必要といっても、超低金利が続く中、どだい意味のない話である。どうやって実質無金利の利子と通算しろ、というのであろうか。むしろ、全国に13億超ある預貯金口座の納番管理がターゲットなのではないのか。損益通算の拡大に納番が必要というなら、なぜペイオフ損失にまで対象を拡大しないのかなど、疑問だらけである。やはり、「選択的納番制」は要らない。

「二元的所得税」、「金融所得一体化課税」はわが国には似合わない

こうした「金融所得一体化課税」のような政策税制の実施で、総合課税の原則は見る見る瓦解して行っている。その一方で、特別配偶者控除の原則廃止、老年者控除の廃止、公的年金等の控除の縮小など、弱い者いじめの税制改悪、弱者への増税プランが目白押しの状況である。

「金融所得一体化課税」は、いわゆる「二元的所得税」理論を「和風」に味付けしたものだ。「二元的所得税」理論とは、「勤労所得」は累進税率で重課する一方で、「資産（不労）所得」あるいはその一部である「金融所得」は一律の税率でフラット課税（軽課）するというもの。社会主義経済から脱却し、市場経済への移行、「投資」を呼び込むのに役立つということで、北欧諸国で流行っている。

こうした税理論は、「役所社会主義」に慣れ親しんだわが国にも似合うはずだ、と政府税調やその背後にいる財務省などは考えているのかも知れない。だが、北欧諸国では、社会保障制度がしっかりしているから、勤労所得に重く課税しても、コンセンサスが得られている。これに対し、年金制度一つとて見てもお先真っ暗なのがわが国の現実。この国には、総合課税の原則を捨ててまでも、こうした政策税制を導入する社会的基盤があるとは思えない。したがって、「金融所得一体化課税」も「選択的納番制」も要らない。

納番制でクロヨン問題の解決はムリ

クロヨン（9・6・4）という言葉を目にしたことがあると思う。これは、各納税者間の所得格差を表わした言葉だ。サラリードワーカー（給与所得者）の場合、税金は給料などから天引徴収される。一方、雇い主である企業の方は、従業員に支払った額を課税庁に報告する。収入あるいは所得は、ガラス張りの状態にある。このため、自営業者などに比べ、所得の把握度は格段に高い。納番制の導入は、こうした所得把握の格差をなくそうということで、声高に主張されてきた。「サラリードワーカーは元もと裸、納番制なんか恐くない」と叫ぶ、森を見て木を見ない「労働貴族」が闊歩する労組などが端的な例だ。

この点に関し、政府税調は、「事業所得を完全に把握するには、売上げ又は仕入れに関する取引のすべてを納税者番号制度による資料収集の対象とする必要があるが、それは現実に不可能である

う」(88年報告)という。当たり前の話である。確かに、居酒屋や八百屋での支払の際に、事業者と消費者が納番を提示・交換し合い、書類をつくりすべて課税庁に報告する仕組みを導入すれば、現金取引の完全な捕捉も夢ではない。だが、これは非現実的で、日常の取引をストップさせる要因にしかない。課税庁もパンクしてしまう。

こう見ると、納番制を入れても、捕捉のターゲットは、個人の「資産所得」と、サラリドワーカーやその配偶者などのちょっとした副収入程度になる。

このうち、「資産所得」については、資産家に傾斜的に税金を安くする政策税制の相次ぐ導入で、フラット課税化が止まらない。あえて巨額なコストをかけて納番管理をしても、それに見合う税収が上がるかどうかは定かでない。そもそも相続時精算課税制度などは、課税庁に納税者情報の長期保有を許し、時効の仕組みを反故にする。また、税制は「簡素」でなければならないという理念にも反する。

いずれにしろ、このように見ると、納番制の重要なターゲットは、サラリドワーカーに絞られる。つまり、「我われは元もと裸」などと叫んでいる階層の納税者が課税庁による徹底した監視のターゲットになる。

体を張って生活者を守る税制を主張しない、「歌を忘れたカナリヤ」のような労組。「納番制で、役所にサイフを管理してもらえば、もっと楽チン」とでもいいかげんな感じの労組。雇用主と一緒にあって、「社畜」をマインドコントロールし、役所にエールを送る労働貴族のタコツボ化したような機能不全の労組。衰退するのは当たり前だ。もちろん、すべてがまるで他人事、役所の言いなり、自分を守るためのタコツボにこもっている議員も同じである。

選択的納番制は必ずエスカレートする

そもそも納番制の導入は、総合課税の実現をプロパガンダに主張されたもの。だが、完全な総合課税の実現は、大半の個人が確定申告をするという事態を招く。政府税調やその背後にいる財務省は、大量の納税者が税務署に押し寄せることになる総合課税など望んでいなかったと見てよい。当初から、真の狙いは、総合課税に名を借りた「納番制を使った国民監視システムの導入」にあったのではないか。

まさに、最近になって総合課税のルールから脱

線し、「金融所得の一体化課税を選択する人には納番制が似合う」と言い出したのは、その証だ。だから、選択的納番制は「呼び水」で、いったんこれを認めれば、一律導入にエスカレートしていくのは必至である。

納番の垂れ流しで、 成りすまし犯罪の多発は必至

11ケタの住民票コードとIC仕様の住基カードを使い、全国民のプライバシーを全国一元管理する国民総背番号制の仕組みが住基ネット(住民基本台帳ネットワークシステム)だ。国民の猛反対に背を向けて導入された。また、2004年秋からは、社会保険庁、国税庁(税務署)、総務省(市区町村)の三省庁が連携し、基礎年金番号を使って、年金未納者の所得把握のために年金情報と納税情報とを照合するプログラムが動き出した。

今度は、「納番制」の導入だという。納番制は、選択導入か、一律導入かを問わず、いったん認めてしまえば、プライバシー保護は重い課題になる。納番の利用は、徐々にエスカレートし、課税が関係してくるあらゆる民間の取引に使われることになる。番号コードの利用を罰則付きに限定しないと、あちこちに垂れ流しになってしまう。結果として、アメリカのように、他人の社会保障番号(SSN)を盗用しその人になりすまし、不正に消費者ローンを利用したりする「なりすまし・身元盗用(identity theft)」犯罪が多発し、手がつけれなくなる恐れがある(CNNニュース26号以下参照)。

民力を削ぐ番号を使った超監視国家を排す

国民監視システムが、役所によって続々と構築されてきている。だが、政治は、国民のプライバシー(人格権)を一元管理する仕組みづくりに迎合的ですからある。年金制度改革論議の中で、自営業者の所得把握を強められるという「幻想」などから、民主党が提唱した国民全員を対象とした納番制導入案は最たる例の一つ。

だが、同党も、この国のかたちが、わずかの隙間もない超監視国家で、国民が役所の情報奴隷となることを望んではまい。今こそ、政治は、徹底した人格権重視の政策を打ち出すべきである。

一方、私たち国民も、超監視国家を排すためにも、役所依存から脱皮し、自らで考え責任をとる民力を培うことが肝要だ。納番制はいらない。

問われる電子政府（e-Japan）構想

—— 外国人に差別的な公的個人認証制度を再考する

—— 河村たかし議員（PIJ相談役）が、総務省に問う

住基ネットを使った公的個人認証は、在日外国人が利用できないなど、差別的な仕組みになっています。電子政府・電子自治体構想の実現にあたっては、日本人と外国人とが平等に参加できる体制を整える必要があります。このためには、住基ネットを廃止し、日本人・外国人がともに民間の認証制度を利用する仕組みを構築する必要があります。

河村たかし衆議院議員が、住基ネット構築した総務省に対し、「電子認証に関する質問」を行い、回答を得ましたので、その内容の評価はせずに、今号に掲載しました。（CNNニュース編集部）

<p>《電子認証に関する質問》 衆議院議員河村たかし事務所</p> <p>2004年8月18日</p>	<p>総務省自治行政局自治政策課（山崎氏）からの回答</p> <p>2004年8月20日</p>
<p>1</p> <p>政府の住基ネット等を基盤とした電子政府構想では、個人の電子申請・申告等の際には、個人認証ツールとして、住基カードを使うように奨励している。しかし、在日外国人は、住民基本台帳に載っておらず、電子申請・申告等を行う場合には、高価な民間認証サービスしか利用できない。こうした制度的な欠陥を総務省はどう考えているのか。また、どのような対応措置を考えているのか、見解を聞きたい。</p>	<p>ご質問の中にもあるとおり、公的個人認証サービスは住民基本台帳を基礎としており、住民基本台帳に記録されていない外国人住民はサービスの対象となっていません。電子政府・電子自治体の推進に当たっては、できる限り日本人住民だけでなく外国人住民にも同様のサービスを利用できるようにすることが重要だと考えています。このため、平成14年5月より、外国人登録事務を所管している法務省と共同で「外国人登録を活用した公的個人認証サービスについての有識者研究会」を開催しています。その検討過程において外国人登録事務のオンライン化に関する課題が提起されました。これらの課題について、一定の方向性が示された段階で結論に向けた検討を行う考えです。</p>
<p>2</p> <p>総務省は、同じく納税しているにもかかわらず、電子政府構想の下で、電子納税申告など行政手続の面で、在日外国人と住基ネットサービスを使える者とを、不当に差別することにつながる仕組みは、憲法あるいは国際人権法上、問題はないと考えているか。</p>	<p>電子政府・電子自治体の推進に当たっては、できる限り日本人住民だけでなく外国人住民も同様のサービスを利用できるようにすることが重要と考えています。</p>
<p>3</p> <p>総務省は、こうした差別を自治体が解消使用とする場合に、どのような支援措置を想定しているのか。あるいは、総務省は、こうした自治体に対する支援措置をまったくしなくともよいと考えるか。自治体が特定の民間認証局と提携して、これら外国人に対する廉価での電子証明書の発行をするなどの対応を奨励することは考えられるか？</p>	<p>現時点では地方公共団体から具体的な要望を受けていませんので、お答えすることができません。</p> <p>（以上）</p>

ドイツにおける監視カメラ規制の現状

— ドイツ連邦共和国ノルト・ヴェストファーレン（NRW）州
データ保護監察官発行『データ保護報告（2001年、2003年）』
所収「ビデオ監視（監視カメラ）」項目を抜粋・翻訳紹介する

石村善治（福岡大学名誉教授）

ドイツにおいても、監視カメラ（ビデオ監視）のあり方がプライバシーの保護の面からさまざま議論されてきている。CNNニュースでは、これまでも、英米を始めとして各国の問題状況を紹介してきた。

今回は、石村善治福岡大学名誉教授（憲法・言論法）に、ドイツ連邦共和国ノルト・ヴェストファーレン（NRW）州データ保護監察官発行『データ保護報告（2001年、2003年）』に所収された「ビデオ監視（監視カメラ）」項目を抜粋・翻訳し、「ドイツにおける監視カメラ規制の現状」を紹介いただいた。

ドイツは、連邦制度を敷き、16の州がそれぞれ立法権を有している（ドイツ基本法70条）。1970年に、同国（当時は西ドイツ）のヘッセン州が、世界で最初の個人情報保護法（データ保護法）をつくったことで知られている。同法は、ドイツの内外を問わず、プライバシー保護についてその後の世界に動きに対し先駆的な役割を果たした。

現在、ドイツでは、連邦に加え、各州が、官民双方を規制対象とするオムニバス方式の州データ保護法を制定している。また、同法のもと、既存の行政機関から独立して、法運用の監督業務を行うデータ保護監察官を置いている。同監察官は、年次の「データ保護報告」を作

成・公表している。

今回、翻訳・紹介いただいたノルト・ヴェストファーレン（NRW）州データ保護監察官発行『データ保護報告（2001年、2003年）』に所収された「ビデオ監視（監視カメラ）」項目では、ビデオ監視（監視カメラ）問題についての論点を整理し、規制のあり方やルールについて、データ保護監察官の見解などが掲載されている。ドイツにおける「監視カメラとプライバシー保護」の現状を知るには、重要な資料といえる。わが国における、問題状況や規制のあり方を探る上での典拠の一つになるといえる。

石村善治名誉教授は、住基ネット差し止め裁判を進める会・九州の共同代表をされ、住基ネット違憲訴訟をリードされている。ちなみに、石村善治名誉教授と石村耕治 PIJ代表とは一字違い、「よく親子では？」と問われるとのこと。しかし、善治教授は九州男児、耕治代表は津軽男児で、出はまったく異なる。「リベラル」という意味では、親子同様の“同志”とのこと。善治名誉教授には、ご多用な折、邦訳のお骨折りをいただき、心からお礼申し上げます次第である。

（CNNニュース編集部）

ノルトライン・ヴェストファ - レン州データ保護監察官

「2001年 データ保護報告」

[Datenschutzbericht 2001

Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen]

（石村善治 訳 2004.6.1）

3 ビデオ監視（P. 60～P. 71）

3.1 公的場所でのビデオ監視

公的場所でのビデオ監視は、すべて情報の自己決定権の侵害であり、したがって常に比例原則にかなった法律の根拠を必要とする。

3.1.1 論争的討論

すでに、1999年第14回デ-タ保護報告は、3.8.1でビデオ監視をテ-マとして掲げた。最近でも、ますます意識的にこのテ-マが議論され、それに対する賛成と反対は、ほぼ同じであった。ビデオ監視のための二つの法律的原則の枠の中で、州議会のすべての会派のメンバーは、デ-タ保護に有利な見解、すなわち“イギリス的状况”（britische Verhältnisse）例えば、街路全体に隙間なく全面に及ぶような監視に、反対する見解を示した。

ビデオカメラの設置は、公的な討論の中では、しばしば安全の改善のための手段であると云われる。そのさい通常提案されるのは、麻薬患者又は浮浪者が頻繁に留まる場所、あるいは、建築構造上市民（男性・女性）の不安感の原因となる場所への設置である。その地域が、他の場所よりも犯罪性が客観的に高いかどうかという問題と、不安感に対する手段としてビデオ監視機が設置されるべきかどうかという問題とは、しばしば区別されずに判断されている。

市民（男性・女性）の基本権を著しく侵害する可能性のある手段は、主観的に脅威を感じるにすぎないような状態を除去するためには設置されるべきではない。ビデオ監視は、危険な状況の場合には、撮影によって画像を得ることによって、秩序違反又は犯罪行為の処罰又は民事上の請求権の実行のための助けとなるかもしれない。しかし、もし人や物への危害を与える事件に関与し得るような人物がその「現場に」いないならば、ビデオカメラによって監視された場所の安全性が増すことにはならないだろう。ビデオカメラの設置は、もしある人物が画像上に認識され得る場合、又は特殊の技術によって認識され得る場合、常にデ-タ保護法上の問題が生じる。その場合、ビデオカメラによる監視（Beobachtung）と記録（Aufzeichnung）とは区別されなければならない。ビデオカメラによる人物の監視は、すでにデ-タの収集でもある。この技術は、複数の場所を同時に監視することを一人の人に許すことになり、そのことによって、監視されるべき場所に実際に人を投入するのとは異なった性質の監視がなされることになる。とくに、カメラの監視領域に入った個人は、本人が現に監視されていることを知らない。このような背景を考慮すると、デ-タ保護法の観点から、ビデオ監視に対して最低限、次のことが要請される。

	ビデオカメラの設置には、規範として明確な法律上の原則（Grundlage）を必要とし、通常要請される一般条項（Generalklausel）は根拠とはならない。その際画像（Bild）の記録（Aufzeichnung）を認める規定は、単なる監視を認める規定より厳格でなければならない。
	ビデオ監視の実施以前に、実施の目的を明確に定め、適切性（Geeignetheit）と必要性（Erforderlichkeit）とが審査されなければならない。ビデオ監視は、監視される人物を比例原則に反して（unverhältnismässig）侵害してはならない。
	何人も、ビデオで監視されている地域（Zone）を横断しないで、望む場所を訪問できる可能性が、常に存しなければならない。
	具体的な危険がある場合には、個人の保障のための措置（Eingreifen）を可能にする組織的な対策（Vorkehrungen）が講じられねばならない。
	具体的な危険がある場合には、個人の保障のための措置（Eingreifen）を可能にする組織的な対策（Vorkehrungen）が講じられねばならない。
	画像の記録が許されるかどうか、又どのような目的で許されるか、明確に定められなければならない。その場合、基本的に目的拘束原則が適用される。すなわち、画像は、記録された際の目的のためにのみ利用することが許される。
	事前に定められた目的のためにもはや必要でなくなった画像は、遅滞なく消去されなければならない。
	特定の場所がビデオ監視されているという事実は、当該関係者に常に認識できるようにされなければならない。このことは、例えば、国際的絵文字（ピクトグラム）及び監視地点の指示を含む適切な掲示板を設置することによって可能である。

	さらに、記録された画像で識別される個人は、当人に対する基本権侵害の適法性を審査させる機会を持つために、通知を受け（benachrichtigt）ことを保障されなければならない。
	適切な期間において、ビデオ監視が依然として必要かどうか、及びどの程度必要かどうかについて、あらためて判断されなければならない。

3.1.2 デ - タ保護法によるビデオ監視

（連邦）デ - タ保護法は改正により、公共の場所を特定するという前提のもとで、ビデオ監視を認める条項を挿入した。その際、監視（Beobachtung）と記録（Aufzeichnung）を区分し、記録に関する通知の義務（Benachrichtigungspflicht）を明示した。さらに、建物（Gebäude）がビデオによって監視されていると云う事実について、その建物に関係のある者の認識が可能でなければならないとした。

ノルトライン・ヴェストファ - レン州デ - タ保護法（DSG NW）第29b条（光学・電子工学的監視 = Optisch-elektronische Überwachung）によれば、ビデオカメラによる監視は、それが家屋権（Hausrecht）の保障に役立ち、当該関係者の有する保護に値する利益を優先させる根拠がない限りにおいて認められる。同条項は、ビデオカメラの設置は、常に公共の場所と当該関係者との間の衡量を前提としている。したがって、すべての官庁において直ちにビデオ監視を設置することにはならない。

この規定によれば、とくに家屋の人及び車の出入口のビデオによる監視は可能である。この規定は、その土地を、その土地の状況により、直接に個人によって監視することができない場合に意味がある。しかし、この規定は、原則的には公共の道路および広場のビデオ監視を認めるものではない。画像の貯蔵（Speicherung）は、目的達成のために不可避である場合であって、具体的な危険がある場合に限り（nur bei einer konkreten Gefahr）、証拠目的（Beweiszwck）のために認められる。すなわち、記録は、その事件に関連する場合にのみ許される（anlassbezogen erfolgen kann）。具体的にいえば、それは、秩序違反又は犯罪行為が行われるか又は直接なされていることが認識される場合である。その他、記録は、それがもはや必要でなくなれば、遅滞なく消去されな

なければならない。記録がなされた（erfolgt）場合には、原則として、当該関係者に通知されるべきである。

3.1.3 水泳場でのビデオによる監視

監視されることなく自由時間をエンジョイできないのか？ビデオカメラは、本来今まで誰も予想もしなかった領域にまで進入してきている。ビデオカメラにより、女性レジ係の意向により、男女の来客が、脱衣・着衣のさいに監視されている。

自由時間を楽しもうと思ひ、市営水泳場にてかけたある男性市民は、こんな経験をしなければならなかった。そこには、全部で11のビデオカメラがあり、その内の一つは男女共同脱衣室の中にあつた。

ビデオ監視は、“画像で個人の人物がはっきりわかるので、当該関係者の自己情報決定権への侵害となる。男女共同脱衣室での自己情報決定権の侵害は、男女の来場者の着衣・脱衣のさいに監視される可能性のありうる肉体の一部（Intimbereich）に著しくかかわるものであるだけに、とくに重大である。すべてのカメラは家屋権の保障のためのものである。しかし、共同脱衣室では、家屋権は、そこに来ている人物の保護されるべき利益の背後に退く。したがって、脱衣室でのビデオ監視は、許されない。

市は共同脱衣室でのビデオカメラを除去する勧告にしたがった。

3.1.4 警察法によるビデオによる監視

（連邦）デ - タ保護法の改正と関連して、ノルトライン・ヴェストファ - レン州警察法（§ 15 a PolG NRW）は、個々の公的に自由に進入し得る場所でのビデオによる監視を、厳格な制限の下で、警察に許す規定を定めた。この規定によれば、個々の公的な場所でのビデオ監視は、著しく重大な犯罪行為がその場所で繰り返し行われた場合に限り、及びさらにその場所で著しく重大な犯罪行為が繰り返されるであろうという予測が正当である限りにおいてのみ許される。ビデオによる監視はオ - プンに行われなければならない。監視が一般に公にされていない場合には、適切な措置によってそれを知らされなければならない。

記録は、その事例に関連するもののみ（anlass-

bezogen) なすことができる。犯罪行為が開始されたか、又は現に犯罪行為が行われているという疑いが監視によって明らかになった場合に、始めて記録することができる。とくに、厳格な目的拘束 (Zweckbindung) が定められており、いかなる例外も許されていない。

記録されたデータは、その記録がもはや必要でない場合には、遅滞なく消去しなければならない。さらに、当該関係者に通知する義務がある。

法律改正後、若干の警察長官は、ビデオ監視の利用につき、公式に懐疑的 (skeptisch) 意見を表明した。また、ある (大都市の) 警察本部 (Polizeipräsidium) は、ビデオ監視のパイロット調査をなすことを計画している。

3.1.5 ビレフェルトパイロット調査計画

ビデオ監視が予定される領域の犯罪事実に関する警察のリストからは、ラベンス・ベルク (Ravensberg) とロツホダル公園 (Rochdale Park) を、犯罪重点地と位置づけるべきか否かについては、明確ではない。1999年に21件、2000年の最初の7カ月間、5件につき、重大な犯罪行為を理由として、捜査手続きが行われた。ビレフェルト公園 (Bielefelder Park) の事件を些細なものとして無視するわけではないが、そこでの犯罪の重要性が高いとは断定し得ないであろう。また、その地域が犯罪重点地であるとする推定を正当とするようなその他の事実にも欠けている。したがって、ビデオ監視のための法律上の前提は存在しない。

私は、このような法律解釈を支持し、すくなくとも、時間的・空間的領域として、監視から自由な地域 (Zone) を維持するよう、積極的に付言した。このことは、少なくとも、当該関係者に対する負担 (Belastung) を軽減しうることになるであろう。

3.2 企業又は私人によるビデオ監視

3.2.1 連邦データ保護法 (BDSG) の規定。必要性。

今まで、個人が、デパート (大型商店) (Warenhäuser) の中や給油所又は近隣の人々によるビデオ監視に対して自己防衛を望んだとしても、連邦データ法は、なんら法的援助を与えるこ

とができなかった。このようなことに対して、民事法上の差止め請求による個人の自衛にまかせたままにしないためには、連邦データ保護法の明確な規範を定め、ビデオ監視が許される場合の要件を確定し、それによってこの領域での“なりゆき任せ” (Wildwuchs) に限界を置くことが要請される。残念ながら、これに関する連邦データ保護改正法案の規定は適当ではあるまい。改正法案によれば、家屋権の保障又は自己の営業目的を果たすために必要であり、当該関係者の保護に値する利益を優越させる根拠が存しない場合には、ビデオ監視は許されることになる。なぜなら、一般的人格権の侵害も、3.1.1で述べた情報の自己決定権に対するデータ保護法の要請が尊重される場合に限り、受忍され得るからであり、その要請は、本質的には、私人によって公的に自由に近づき得る領域においても満たされなければならないからである。(参照: 第59回連邦・州データ保護監察官会議決定 [14./15.3.2000] - 資料 Nr.14)。

以下の諸点が強調される。

公的に自由に近づきうる領域のビデオカメラによる監視は、安全保障に役立ち、その目的を達成するために必要とされる場合 (erforderlich) に限り許される。さらに、監視は、当該関係者の保護に値する利益の方が、監視者の個人的利益よりも勝る場合には、比例原則に反することになる。監視が、当該関係者の保護に値する利益の侵害と結びつく場合には、それに対抗して、他の方法では保護が期待しえないような重大な私的権利についての保護がなされねばならない。とくに、監視は地面全体を覆うものであってはならない (nicht flächendeckend)。通常、ビデオ (カメラ) の設置は、人が自分の住所又は仕事場へ、ビデオ監視ゾーンを横切らずに行ける可能性が無くなってしまふようなものであってはならない。

画像の記録が完成される前に、画像の貯蔵がビデオ監視の目的を達成するために不可 (unerlässlich) であるかどうかにつき、さらに吟味されなければならない。単なる監視とは違って、記録は、当該関係者の一般的人格権に対する、より強度の侵害を意味する。なぜなら、記録は私的監視者に、画像データ処理の可能性を高めるからである。非公共の場所での貯蔵の場合、貯蔵された画像の目的外利用の危険性もある。したがって、特別の予防措置 (例えば、目的の特定化、データ

へのアクセス (Zugriff)、貯蔵目的期間の拘束力をもった決定) がなされなければならない。

私人によるビデオの記録に関しては、記録画像が特定人物を示す場合、つまり、人物が特定される場合には、上に述べた通知義務が、さらに不可避となる。このようにして、はじめて、当該関係者は記録の消去を請求することによって、自らを守ることが保障される。

非公共部門における監督官庁によるコントロールを確実に行うという点からすれば、私人や私的機関によるビデオ監視についての通知義務 (Anzeigepflicht) は、ビデオの設置が心配のないものであるかどうかを事前に審査することができるために必要であるというだけでなく、それによって、監視装置についての内容全体を把握し得るし、議会および公衆の情報伝達もより容易になり得る。

これに対して、公的に進入しえない領域 (nicht öffentlich zugänglichen Raum) におけるビデオ監視が、その領域の所有者によって行われ、かつ、それが家屋権に基づくものである限りにおいては、ビデオカメラの設置は広く (weitgehend) 許されることになる。たしかに、第三者 (例えば賃借人) の権利に対する許されない侵害、例えばとくに守られている領域 (3.2.2 参照) への隠しカメラによる撮影又は監視もあり得るであろう。そのような侵害に対する保護は一般的人格権によって保障されることになる。

3.2.2 業務用及び住居用建築物 (Geschäfts- und Wohngebäude) の確保のためのビデオ監視

監視は、ほとんどの場合、家屋の入口の外で、家屋権の保障に基づいて行われるが、しかし、場合によっては公共の道路 (Verkehrsraum) において過度に行われたり、場合によっては種々の生活状況の中で当該関係者が侵害されることがある。

ビデオ監視による銀行 (Sparkasse) の安全確保によって、銀行襲撃のさいの警察の犯罪捜査を容易にしたり、犯罪者がどのような車で犯行現場にたかについての情報や、襲撃後の逃走路の情報が与えられたりしている。また、そのために、交通の激しい市街中心街からの放射道路 (Ausfallstrasse) の対抗路の電柱頭にビデオカメラが設置され、全道路面 (Strassensektor) や、銀行によって設けられた駐車場も監視されているこ

とがある。また、常時撮影し、15分後にはその上に新しく撮影し以前のものを消去するいわゆるリンク貯蔵 (Ringspeicherung) も企画されており、緊急時 (Alarmfall) にはすべてが貯蔵されているようである。

たとえ、監視装置のあることが認知 (verständlich) されており、あとになってそれを確かめる (nachvollziehbar) ことができたとしても、法的には許されるものではない。町並み (Strassenzuge) や駐車場は公的な路面 (Verkehrsfläche) であり、基本的には家屋権を根拠に監視することは許されない。場所柄あるいは状況からみて、公的根拠に基づき、監視がどうしても (bedingt) 避けられない場合にのみ、例外的に監視が可能である。

しかし、その場合も、やむを得ない限度に止どまるべきである。その審査判断にあたっては、監視される当該関係者の保護に値する利益がまず重要な意味をもつ。人物をはっきり解るように撮影することは、通りや駐車場を移動する多くの人物をコントロールし、記録することとなり、その人たちの権利を不当に侵害することになる。このような法律の見解に基づいて、銀行は前の計画を改めた。

ある保険会社の施設 (Gebäude einer Versicherung) でのビデオカメラの設置については他とは異なった評価がなされる。ここでは、建物の外面玄関に設置された6個の監視カメラが、地下駐車場の入口のコントロールや表玄関の侵入や汚損防止に役立っている。これらのカメラは、建物の正面玄関の外の歩道 (Bürgersteig) の狭い道も写している。撮影された画像は、画像モニターに写される。

しかし、連結されている記録装置により技術的には記録が可能であっても、それらは記録されていない。カメラによる撮影は、公的に誰でも通れるところでは、小さな区域内だけ、しかもそれは監視するに止どまり、往来の人たちには、モニターしていることがはっきりしているカメラのあることの認識が可能であり、また、それを避けることが可能である限りにおいて、保護されるべき利益が比例原則に反して (unverhältnismässig) 侵害されたことにはならない。

私は、不適切な使用を避けるために、安全を考慮して、記録装置を分離するよう勧告した。

たしかに、例えば、住居施設の所有者が、地下駐車場や、一部は私用だが公的にも利用、され、一部は公的でもある路面を、家屋権を根拠に監視

するようなビデオ監視装置には疑問がある。また、ある設置カメラは、画像を、約1時間、経過監視し得るモニタ - 付きの場所に移送している。画像は記録されていないが。

地下駐車場は、原則的には、特定の固定場所を賃借した個人によって利用される。監視のために、ガレ - ジの安全な利用を確保するという目的のためにのみビデオ監視が行われ、また、さらに賃借契約で合意されているならば、原則的には、その監視に対しては、なんらデ - タ保護法上の疑念は存在しない。同乗者、男女の訪問者がビデオ監視に関して明瞭に知りうるような掲示がなされなければならない。

一般的に公的に自由に通れる屋外領域 (Aussenbereich) においては、状況はまた別である。上に述べたように、公的な路面は、基本的には、家屋権を根拠にして監視されてはならない。特に個別的な状況では、監視が例外的に正当化される場合はありうる。

その例として、屋外領域に2個の固定カメラが設置され、その一つは曲がり角 (Wendehammer) に向けられ、他の一つはトラック車の駐車場所に向けられている。その他、電柱に設置されているズ - ムつきの巡回可能な監視カメラがある。(私有地の) 駐車場に設置されているカメラは、トラック車の保護に役立っている。相対的に狭い監視地域を通る人は、きわめて短時間カメラでとらえられる。

このような相対的に狭い範囲で監視されている人の人格権侵害は、まだ受忍しうるであろう。それに対して、曲がり角に向けられたカメラは、基本的にかなり広範囲の監視地域をとらえており、とくに公的なこどもの遊び場や道路への入口だけではなく、対面している家屋の入口にも向けられている。

このような監視措置の目的は、住居施設や地下駐車場の自由な通行を確保することにある。公的な路面の監視をこのような範囲に例外なく認めるような異常な状況は存在していない。したがって、監視は許されない。

結局、回転式カメラによる包括的に監視できるカメラもデ - タ保護法上疑念がある。カメラの回転によって、モンタ - ジュマストから359度の広範囲にわたって監視することは技術的に可能である。ズ - ム交換レンズによって、200メートル離れた車両の標識と人物の顔さえ、認識できる。監視の活動半径 (Radius) や細部の正確度

は、所期の目的 “ 施設の安全の保障 ” にとっては必要なことではない。当該関係者にとっては、カメラで監視されている領域を通行せざるを得ないのであるから、このような包括的な監視の可能性は当該関係者の人格権の比例原則に反した (unverhältnismässig) 侵害である。

したがって、適切な予防措置を講じることによって、必要な限度に縮小されるような唯一の適切な措置が実施されるよう、保障されなければならない。例えば、カメラの巡回範囲を技術的に変更することによってその範囲を制限したり、ズ - ムレンズを他の近くだけしかとらえないレンズに変えたりすることである。

住居施設の所有者が自分以外の人に監視を委託する場合には、どのような前提のもとに監視を行うことが許されるかを、事前に義務として明確にしなければならない。

基本的には、公的な路面 (Verkehrsfläche) の個人によるいかなるビデオ監視も許されない。そのような路面の一部でもとらえるようなビデオカメラによる監視が例外的に受忍されうるかどうかは、それぞれの個別的事例において慎重に吟味されなければならない。

3.2.3 公共交通手段でのビデオ監視

ビデオ監視は、地下鉄やバスの前で止まっていない。そのような監視器具の取り付けは公共交通手段によって促進され、一般的には乗客の安全確保のための特別サ - ビスとしてみんなの前であらわれている。たしかに、監視と記録は乗客の軽微な侵害とはいえない。

ビデオ技術の設置と監視の実施は、次の原則にしたがって計画され、そして一部はすでに実現されている。

車両ごとに4個のミニカメラが設置され、運転主 (男女) の側におかれている一つのモニタ - に、立像 (Standbilder) が短期の取り替えて移送される。それとならんで、24時間の貯蔵能力のあるデジタル記録装置の上に、常時記録されている。その間、直接車内で気づかれたり、または後になって乗客から障害事件として確認される事件が生じていなければ、新しい画像がその上に重ねられ、したがって、古い画像が消去される。事件がおこれば、乗客の通告により、保安指導機関、またはとくに交通事業の中の特定の人によって、デ - タ記録体 (例えばフロッピ - 《Festplatte》や

ディスク)またはビデオカセットが独立した記録装置から取り出され、使用される。必要とされる画像は、再現され、証拠物件として用いられ、一方その他の記録は消去される。

ドイツ交通事業団体のイニシアチブで、はじめに共同懇談会において、公共交通機関のビデオ設定のための一般規則を作る試みがなされた。この規則は交通事業社の注目を引くよう勧められるはずである。そのさい、目的は、個々の交通事業体が決定する前に、いわば予防的デ・タ保護の中に、ビデオ技術の設定のための基準を見出せるようにすることである。

バスや列車の中でのビデオ設置は、乗客の安全な運送と盗難の阻止のためにのみ役立ち、この目的のために必要なものでなければならず、乗客の人格権を比例原則に反して侵害してはならない。

監視は、交通機関の中に、カメラによってとらえられていない領域があること、乗客は、監視されない乗り物を使うことができるように、カメラでとらえられていないゾ・ンが残されていることによって、原則として比例原則に一致することとなる。

監視によって具体的な危険状態に対する予防がなされ、監視によって、乗客の安全のために介入することができる。

記録は、記録をなす誘因、例えば安全の確保を侵害するような事件が確認されるといった理由がある場合に行われる。

記録画像の利用は、目的に適合した利用のみ、また、利用の権限のある者によってのみ行わ

れる。不必要となった画像は遅滞なく消去される。

監視していること、記録していること、および責任者(電話番号を付して)については明瞭に分かるように知らされる。個人に関することの利用の際には、当該関係者に知らされる。

必要な安全措置は、営業指示書に明示される。ビデオ設置がまだ必要であるか否か、あるいは、デ・タ保護対策を新しく評価しなおすかどうかについて、一定の期間をおいて審査する。

3.3 Web - C o m s 広告の別種にすぎないのか?

公共施設(美術館、市役所、大学)及び私的施設(商店パッサージ、インタ・ネット・カフェ)も世界的メディアに登場し、広告に注目させようとしている。この目的のためにWeb - C a m sを設定している。このさい、まず第一に、多くの者が、Web - C o m sの領域の中に留められている人物の権利を侵害するものであることを看過している。すでに、特定人の写像(Abbildung)は、その者の人格権を侵害している。それとは別に、いずれの場合も、インタ・ネットによる画像の頒布(Verbreitung)は、当該人の同意が事前になされていない限り、当該人の権利を侵害する。さらに、権限のない画像の頒布は芸術著作権法により処罰される。

ノルトライン・ヴェストファ - レン州デ - タ保護監察官 「2004年 デ - タ保護報告」

[Datenschutzb ericht 2003

Die Landesbeauftragte für den Datenschutz und Beauftragte für
das Recht auf Information Nordrhein-Westfalen]

5 ビデオ監視 (P . 5 5 ~ 5 9)

ビデオ技術の急速な発達(例えば顔貌認識システム)は、日常生活の多くの分野での利用の恒常的な増加と同時に、不安(Besorgnis)をひき起

している。このような技術の進出(Einsatz)と、当該関係者の自己情報決定権及び一般的人格権に対する侵害とは結びついている。この侵害については、非公的領域における監視機関の手段による望ましい事後審査がなされていない。

先のデ - タ保護報告 (15 . デ - タ保護報告 2001 3 . 以下。60頁)以後、法状況は変わった。公的領域においては、警察の権限が拡大された。非公的領域においては現在、ビデオ監視の許容性に関して連邦デ - タ保護法第6 b 条によって審査される。この非公的領域では、とくに、公共交通手段内、停留所及び駅のビデオ監視の設置が増大した。その他私有地所有者の近隣監視カメラが喜ばれ、私人が画像をインタ - ネットに記録する Web - C a m s が、残念ながらますます好まれてきている。

ノルトライン・ヴェストファ - レン警察法 (PolG NRW) の改正計画によって、公共道路及び広場におけるビデオ設置のための厳格な条件が緩和され、それによって、個々の公的に進入しうる場所に対するビデオ監視を、容易にできるようにしようとする目論がなされている。

たとえば、街通り又は市街地区までを、ほとんど全面的に監視する、いわゆる “イギリス的状况” (britische Verhältnisse) にまでは、まだ至っていないにしても、新しい計画によって登場するビデオ監視に対する設置の敷居は、低下し、監視の方向へさらに踏み出したとみなされねばならない。

“極めて重大な” 犯罪行為は、将来もはや、監視を実行しうるために必要なこととはなくなるだろう。記録の可能性も非常に拡大されている。法案に対するデ - タ保護法上の疑念も今のところ残念ながら見られない。その他、前と同じように、ビデオ監視が言われているように犯罪行為の減少に至るのか、それは単なる押し退け (Verdrängung) にすぎないのか、まだ実証されていない。

非公共領域におけるビデオ監視 (私人又は企業による) の設置は、現在では、連邦デ - タ保護法第6 b 条 (§ 6 b B D S G) の中の特別法的規定を前提にして審査されるべきである。たしかに、この規定は公的に進入しうる領域の監視のみを対象にしている。

したがって、労働現場や住宅のようなセンシティブ (sensibl) な領域の監視の場合に対する特別の保護規定を欠いている。また、同法第6 b 条第1項3号の規定も問題である。なぜなら、ここでは、正当な利益の保障のためのビデオ監視の許可は、デ - タ保護の原則によれば、つねに極端な例外事例の場合に問題となりうる一般的な緩和規定 (Auffang - regelung) と理解されているものであるからである。今まで、ビデオ監視が、具体的な

目的のための正当な利益を保障するために要請された事例は知らない。

この間、公共交通手段でのビデオ監視の設置のために (15 . Datenschutzbericht 2001 3 . 2 . 3 S . 69)、交通企業の駅、市電、及びバスでの監視の許可の要請に関して、連邦全体で議論され、投票され、議決された。基準の作成にはドイツ交通事業団体 (Verband Deutscher Verkehrsunternehmen in Köln) 及び当總會、非公共領域デ - タ監視最高機関 (Dusseldorf Kreis)、連邦・各州デ - タ保護受託官会議が参加した。それによって、確定された基準が、原則として連邦全体に広がるデ - タ保護法による許可のための基準となる。この要請は、付録 Nr . 6 に掲載されている。

ノルトライン・ヴェストファ - レン州では、安全施設のための促進策 (それはビデオ監視設備のためのものでもあるが) が交通手段の中に備えられている。デ - タ保護法上なら許されない監視施設が計画されたり、それに補助金が出されたりすることを避けるために、交通大臣には、促進カタログを承認機関に渡すよう要請され、また、同大臣には、補助金受領者に、承認申請書といっしょに提出する安全コンセプトとの中にデ - タ保護法の要求についても配慮するよう要請している。

私的領域では、しばしば、土地所有者から、近隣者のビデオカメラによる土地の監視が行われているという苦情の申立てがなされる。そのような監視は、それがもはや家屋権の保障のためのものではないがゆえに、すなわち、家屋で生活している者の安全又はその所有権のための危険の排除のためのものではないがゆえに、通常許されるものではない。多くの場合に、ビデオカメラは、それが自分の土地を越え、単に隣人の土地のみならず、公的な交通領域にまで監視できるように設置されている。監視が許されるのは、自分の土地の境界までであって、家屋権はもはやそれ以上にまでは及ばないからである。

さらに、私的な住居家屋 (アパ - ト) の中でも、エレベ - タ - 又は郵便受けの被害を避けるためにビデオカメラが設置される。そのようなビデオ監視の許可は、連邦デ - タ保護法第6条bでは判断できない。なぜなら、これは公的に進入し得ない領域でのことであるからである。それにもかかわらず、ここでも、設置されたカメラは他の賃借人並びに来訪者の一般的人格権を侵害する。

一般的人格権は、国家によってだけでなく、そ

の放射効果に基づいて私法関係においても尊重されなければならない。

賃借人は建物の中で原理的に監視されることなく移動することができるという権利を有する。賃借関係においては原則的には賃貸借法上の根拠から要求される賃貸借当事者間のデータのみが取り扱うことが許される (§ 28 Abs. 1 Nr. 1 BDSG)。他のデータは正当な利益の保障のためにだけに取り扱われる。そして、このことは、賃借人の保護に値する利益が、ビデオ監視の排除に優越すると考えられる根拠が存在しない場合にのみ認めてよい (§ 28 Abs. 1 Nr. 2 BDSG)。

このことは、ビデオ監視が家屋権の保障のために必要でなく、また、賃借人の保護に値する利益が侵害される場合には、とくに吟味されるべきである。したがって、これらの諸条件は、連邦データ保護法第6b条の条件にかなっている。

例えば、住居施設の住居管理者が家屋の入口部分に二つのビデオカメラを設置し、郵便箱とラウンジの隅に向けられていた。郵便箱の監視のためのビデオカメラは許されるが、入口部分のラウンジの隅 (Aufenthaltsecke) に向けられたカメラは許されなかった。過去、何度も何度も、個別の郵便箱がこわされ、郵便物が盗まれた。とくに、この場合、ビデオ監視によって迷惑を受けた人物の保護に値する利益は所有権保護の利益を越えるものではない。むしろ、保護に値する利益は、正常に郵便配達を受ける賃借人の利益の方にもあてはまる。

ここでは、監視は、まさに家屋住居者の保護のためにもなされる。それ以上に、郵便箱の領域はいきなり問題になったにすぎず、抜き出された郵便物の監視は不可能である。たしかに、ビデオ監視を指示するはっきり認識できる国際標識 (Piktogramm) が郵便箱に直接近接して示されていなければならない。それに対して、ラウンジの隅に向けられた他のカメラは家屋権の保障のためには必要ではない。というのは、事件 (かみ屑籠の燃焼やガラス窓の破損) はすでに2年以上も前のことであったから。

ビデオ監視と顔貌認識システムの結合が技術的に可能であることは、再びデータ保護に新しい要請をなげかけている。この新しい技術は、データ保護法の基本原則と合致するかいなかの吟味なしに設定されている。公的領域においても私的領域においても、データ保護の個人情報に係わるデータの、自動化された操作を新規に導入する前に、

計画されている操作が、当該関係者の権利や自由に特別のリスクを示すものであるかどうか (§ 4 d Abs. 5 BDSG)、あるいは自動化された操作の設定によって、情報の自己コントロール権に対する危険が生じるかどうか (§ 10 Abs. 3 Satz 1 DSG NRW) を審査しなければならない。

自動化された操作をインストールされた顔貌認識システム (Gesichtserkennungssystem) の設定は、基本的に、“単なる”ビデオ監視に対する当該関係者の権利への新たに付加された侵害を意味している。

顔貌認識システムの機能として、しばしば、画像データベース (Bilddatenbank) の構築や育成があり、また新規に得られた画像とデータベースに貯蔵されている画像との比較や新規画像の自動的貯蔵とが挙げられる。ビデオ監視と結びつくそのような操作が、§ 6b BDSG、あるいは §§ 15 a PolG NRW, 29b DSG NRWの法的条件を満たすかどうか、はなはだ疑問とせざるを得ない。むしろ、特定の領域での許される設定に必要な要請を定める特別法規 (spezielle gesetzliche Regelung) が必要である。そのような法律規定が欠けている限り、これらの導入は一般的データ保護規定によって支持されるべきではない。

最後に、やたらに手を振り回すインタ - ネット狂 (Internetfreaks) の “悪習” (Unsitte) にも付言しなければならない。かれらは Webcam を用いてかれらの仲間 (Umgebung) を、人物をも認識できる (Personen erkennbar) ようなかたちで、自分のウェブサイト、コピーしている。

ほとんどすべての場合に、これは自己宣伝 (Eigenwerbung) か又は自己表示 (selbstdarstellung) である。これには § 6b BDSG による正当な利益が存しないことは別に、それ以上に人物のシャ - プな画像 (したがって、人物が特定しうる) をインタ - ネットで世界中 (weltweit) に公開する必要はない。遠景の撮影は完全に認められる。 (5 ビデオ監視。55頁 ~ 59頁)

(以上)

〔仮訳〕

監視カメラとプライバシー保護に関する E C の見解 (2004年2月11日採択)

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)

E C データ保護作業部会

Opinion 4 / 2004 on the Processing of Personal Data
by means of Video Surveillance

《邦訳》 PIJ代表 石村耕治

E U加盟各国においても、監視カメラの利用(あちらでは「ビデオ監視」という)が広がり、個人のプライバシー保護との調和が、E Uのプライバシー政策上の重要な課題の一つとなってきた。例えば、「極端に監視カメラ社会化」が進んでいるイギリスの現状については、すでにCNNニュース32号で紹介したところである。

E Uは、2004年2月11日に、「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)をまとめて公表した。

この見解は、E C 95 / 46 指令(E U個人データ保護指令)29条〔個人データ処理にかかる個人の保護に関する作業部会〕の下で設けられた作業部会(データ保護指令29条データ保護作業部会)が、まとめたものである。加盟各国のビデオ監視規制の現状を分析するとともに、プライバシー保護の観点から、E U共通のルールを明確にする方向で、ビデオ監視を「監視」しようというのが狙いである。

ビデオ監視(監視カメラの利用)には、画像などの個人データ(個人情報)の処理が伴う。E Uにおいては、この点に着眼して、ビデオ監視を規制し、一定のルールに乗せようというものである。言い換えると、監視カメラを設置し

た機関が、市民の本人識別のために、画像さらには音声などを個人情報(個人データ)として利用する場合には、広く個人データの処理一般に適用される「E U個人データ保護指令」の法原則に従うように求めるものである。これによって、市民の人権や自由を保護しようというわけである。

わが国でも「監視カメラとプライバシー」問題がようやく記論されるようになってきた。しかし、とかく「悪いことをしなければ、監視カメラなど怖くない」といった考えが主流だ。いまだ、プライバシー保護のための法的インフラ整備の議論は未熟である。

こうした現状を踏まえ、E Uおよび加盟各国の現状紹介をかねて、PIJ監視カメラ立法対策プロジェクトチーム(PT)の座長 石村耕治(PIJ代表)が、データ作業部会の見解の全文を仮訳した。わが国での成熟した議論に向けての一助となればと願っている。なお、この見解にある、注記の翻訳は省略した。(一般に、「見解(Opinion)」は、特定のテーマについてE Uの考えを表明するものであり、法的拘束力はない。)

ちなみに、E U個人データ保護指令の概要は、すでにCNNニュース7号および8号に紹介されているので、参照されたい。

(CNNニュース編集部)

1. はじめに

ここ数年、欧州においては、公共機関や民間機関による画像収集装置の設置が目立って増加して

きている。こうした状況から、ビデオ監視装置を設置する際に適用されるべき要件や条件、さらにはデータ主体に対する必要な安全確保措置について、欧州共同体レベルおよび各加盟国の双方にお

いて、活発な議論が展開されてきている。

また、EC 95 / 46 指令（EU 個人データ保護指令。以下「データ保護指令」または単に「指令」）が各加盟国内で適用されて以降ごく最近まで、多様な分野において使用される閉鎖回路 TV、カメラその他より複雑なツールなどは、数量的にも大幅に増加傾向にある。

さらに、利用できる技術、デジタル化および小型化の進展、イントラネットやインターネットの発展、さらには画像および音声記録装置の利用により、データ提供の機会は格段に広がってきている。

雇用環境における情報処理作業に加え、この件については、すでにデータ保護作業部会が詳細な報告書にして公表済みのところであるが（「雇用環境における個人データ処理に関する見解（2001年8号）」）～ビデオ監視技術の蓄積・発展は、安易にすべての市民に受け入れられがちである。また、ビデオ監視装置と相互に関連する形で拡大する傾向にある。

断片的な分析からではあるが、ビデオ監視は極めて多様な目的に利用されている。ただ、その利用は、次のようないくつかの分野にグループ分けができる。

- 1) 個人の保護
- 2) 財産の保護
- 3) 公益
- 4) 犯罪の防止、捜査および取締
- 5) 証拠としての活用
- 6) その他の法益

また、ビデオカメラおよび同類の装置の設置に対しては異なる要件が適用される。

場合により、現実には、ビデオ記録装置の設置は、特定の加盟国においては法律で義務化されている。例えば、カジノへの設置があげられる。あるいは、他に、例えば失踪した子どもや成年の追跡調査の場合のように、データ主体の関係者が特別の重要性を指摘した目的を達成するための設置がある。一方、ビデオ記録装置の法外な利用の実態があることも指摘できる。その多くは発展途上国で起きているが、例えば顔面認識装置が重婚を防止する目的で使われている。あるいは、現地の警察当局が、自白しない犯罪者は刑務所で過酷な生活を強いられることになることを知らせるために画像を公開するやり方をとっている。

このように、ビデオ監視は、一定の状況下ではある程度正当化されうる。一方で、適切な要件や取決めを十分に検討することなしにビデオカメラ

が利用されることに對し保護が必要なケースもある。ときには、ビデオ監視装置の利用が、公共機関が与える大掛かりな補助金や保険約款の優遇条件に起因していることもある。

同様に、ビデオ監視については心理的な効果もある。つまり、一般的には、ビデオ監視は、その良し悪しは別として、しばしば、犯罪の防止には有用との視点から、「重要な道具」と見られていることである。

このように、ビデオ監視は、いくつかの技術がすでに利用でき、これからも拡大し、進化していく分野である。

今回の作業報告書は、各加盟国の法律の詳しい規定および一部異なる規則の現状分析から入り、より統一かつ調和のとれた手法が求められていることを明らかにするのを目的としている。

今回の作業報告書は、事件、事態および状況を遠隔モニターするための監視のあり方に関するものである。したがって、例えば、各加盟国当局の活動や議会の透明性の関し、特定の事案を、事案ないしは傾向基準を用いて直接に点検するといったものではない。

各作業者は、関係する分野および本作業部会が調査を予定している技術的発展の双方について、自己の分担の中に、特記することができる。

さらに、ここで検討された原則は、画像の収集、これに伴う音声や指紋データのような生体データにも適用することができるものである。

これらの原則は、さらに、具体的な適用において、ビデオ装置によるのではなく、むしろ遠隔操作、例えば人工衛星をベースのGPSのようなシステムを使った個人データの処理に関しても、応用することができる。

本作業報告書は、第一に、個々のビデオ監視装置を設置する際の適法性および妥当性を評価する場合においては、広範な基準があることを周知すること目的としている。

ただし、次のようなことに力点が置かれている。

- a) 加盟国の権限ある機関は、ビデオ監視の評価にあたり、一般的な視点から、そして、この件に関しグローバルに通用する選択的かつ体系的視点を持って、それを実施することが求められる。公共および民間の領域における画像収集装置の急激な増加が、市民の権利や基本的な自由に対する不当な制限を課すことにつながってはならない。そうでないと、市民は、現実に、数多くの公

共空間や民間の空間において重苦しい身元確認を求められるという、不相应なデータ収集手続を強いられることにつながりかねないからである。

- b) ビデオ監視技術の発展を受け入れる傾向を具体的に評価すること。これは、顔面認識、さらには、特定の事件やその張本人を描き出す目的を持った無差別かつ積極的な予防的監視、～伝統的な静的な監視とは対照をなすもの～、から想像される人間の行動の研究やそれを予測するソフトの応用の広がりを防ぐことにねらいがある。この新たな監視技術は、個人の顔面の特徴を自動的に収集するとともに、その「異常な」行動について自動的に警告や暗示をすること、～こうしたことには多分に差別の危険を伴うものであるが～、を基礎としている。

2. 国際的な法文書

a) 人権と基本的自由条約

プライバシーの保護は、人権条約第 8 条により保障されている。

b) 1981年108号個人データの自動処理の関する個人の保護のための欧州議会条約

この条約の適用は、EC95/46指令（EU個人データ保護指令）と同様に、核となる活動（後記参照）に限定されない。個人データの処理を要するビデオ監視活動も、この条約の適用対象となる。この条約に基づいて組織された諮問委員会においては、音声および画像は、間接的な形を含め、本人と識別できる方法で個人情報として利用する場合には、個人データとみなすことにしている。

欧州理事会は、最近、ビデオ監視方法を使ってデータを収集しかつ処理する場合の個人の保護に関する指針的な原則をまとめた。これらの原則があることにより、データ主体に対しては、欧州理事会文書の規定に従い、より厳格な安全確保措置を適用しなければならなくなった。

c) 欧州同盟の基本権憲章

欧州同盟の基本権憲章は、第 7 条において、私人、家族生活、家庭および通信の保護を、そして第 8 条において、個人データの保護について定めている。

3. EC95/46指令

（EU個人データ保護指令）の下での監視

音声および画像データを含む個人情報処理の特徴は、いくつかの要点を示す形で、EC95/46指令（EU個人データ保護指令）の中に、はっきり示されている。

データ保護指令では、自然人の基本権および自由の観点から、プライバシーおよび私人の生活の保護ならびにより広範な個人情報の保護をうたっている（指令 1 条 1 項）。

ビデオ監視方法を使って収集される情報のかなりの部分は、公共の場所ないしは公的に立入ることが認められた場所に移動したときに撮像され、本人と識別されたいしは識別されうる者に係わるものである。こうした移動中の個人は、本人が権利や自由が完全に奪われることを望まない私的空間や私的画像が関係する場合に比べると、より程度の低いプライバシーの保護を望んでいるともいえる。また、本報告書では、加盟国の領域に合法的に所在する個人の移動の自由権、～これは人権および基本的自由の保護に関する欧州条約への追加的議定書 4 号の 2 条により保障されている～についても検討する。

移動の自由は、唯一、民主社会における特別の目的を達成するために必要な場合に限り制限することができるに過ぎない。データ主体は、自己の移動や行動について、過度に精神的な規制を受けることなく移動の自由を享受する権利を有する。同時に、自己の移動の追跡ができ、さらには、数多くの公共の場所ないしは公的に立入ることが認められた場所において複数の機関から必要以上にビデオ監視を受けることにより、いかなる人的な介入もなしに、その個人の疑わしいと思われる行動を自動的に「識別」するソフトを使い「警鐘」を与えることができるような厳格な監視の対象となることなしに、移動の自由を享受する権利を有する。

自然人の音声や画像データ処理の特定情報的な性格については、データ保護指令の前文に列記されている。その適用範囲については、下記において考察されるが、データ保護指令にある該当する前文および条項は、以下のとおりである。

- a) データ保護指令は、原則として、この方法において収集された特定の種類の個人データを蓄積、操作その他の利用に供する技術の重要な発展に係わる事項に対しても適用されるものとする（指令前文第 14 参照）。

- b) データ保護指令にうたわれた保護の原則は、その者を識別する管理者またはその他の者により合理的に利用されるとされるあらゆる手段を考慮した上で、音声や画像情報を含む、識別されたもしくは識別されうる者に関するいかなる情報にも適用される（指令2条a号および前文第26参照）。

前記の例に加え、データ保護指令は、とくに、次のような個々の規定の枠内で明白にそのすべての効力を有する。

1)	データの質～画像は、公正かつ合法的に、さらには、特定、明白かつ適法な目的をもって処理されなければならない。画像は、データは妥当、適切かつ過剰ではなく、さらにはその目的に不相応な方法で処理をしてはならないという原則に従って利用されなければならない。画像は、限定された期間にわたり保存されなければならないなど（指令6条参照）。
2)	データ処理の適法性の基準～この基準に基づき、ビデオ監視方法を使った個人データの処理は、少なくとも第7条に列挙された要件の一つを根拠に、それを実施するように求められる。すなわち、明瞭な同意があること、契約上の義務からの必要性があること、法律上の義務を遵守するため、データ主体の重要な利益保護のため、公益目的での業務遂行のため、または公権力行使のため。
3)	ビデオ監視において、センシティブなデータ（特定データ）または犯罪に関するデータの利用が関係する場合には、特定の種類のデータの処理に適用される安全確保措置に対象となる（指令8条による）。
4)	データ主体に対する情報の提供（指令10条および11条参照）。
5)	データ主体の権利、とくに、開示請求権および適法な理由に基づくデータ処理拒否権（指令12条および14条a号参照）。
6)	個人の関する自動的判断に関し適用される安全確保措置（指令15条による）。
7)	処理作業の安全（指令17条）。
8)	処理作業について監視機関への通知（指令18条および19条による）。

9)	データ主体の権利および自由に対する特別の危険をもたらす恐れがある処理作業への事前の検査（指令20条の下）
10)	ならびに、 第三国へのデータ移転（指令25条以下による）。

音声および画像データの処理に関する特定情報の性格は、最終的には、データ保護指令の最後の条項で認められた。当該条項では、とくに、欧州委員会が、この件に対するデータ保護指令の適用について検討し、かつ、情報技術の発展を考慮しかつ情報社会の発展に照らして、必要と思われる適切な提案をするものとしている（指令33条参照）。

4. 各加盟国においてビデオ監視に適用される規定

すでに、いくつかの加盟国においては、憲法、特別の法律ないしは政令その他各国の権限ある当局が出した決定をベースに、ビデオ監視に関する事例研究が行われている。

少数の加盟国においては、ビデオ監視については、個人データ処理が伴うかどうかにかかわらず、特別の規定の適用がある。こうした規制の下では、閉鎖回路テレビその他類似の監視装置の設置や利用にあたっては、国のデータ保護機関が多少なりとも参加している行政機関からの事前承認を前提としている。こうした規制は、当該装置の操作に責任を持つ主体が、公的な性格のものか民間かで異なる。

それ以外の加盟国においては、現在、ビデオ監視は、特定の法律の規制対象とされていない。しかし、とりわけ意見、ガイドラインないしは運用基準を通じて、データ保護機関が一般的なデータ保護規定を援用してきている。イギリスやイタリアがそうした例である。

ベルギー

データ保護機関の見解、とくにビデオ監視装置を利用した画像処理については、1999年12月13日の見解（1999年34号）。集合住宅の玄関でのビデオ監視装置の利用に関しては、2000年1月10日の見解（2000年3号）

デンマーク

ビデオ監視の禁止に関する2000年2月1日付けの総合法律76号。本法は、原則として、民間機関が、一般の通行に使用されている公道、通路、広場その他類似する場所をビデオ監視することを原則として禁止している。ただし、次のような場合には例外が認められている。

- ・2002年6月3日のデータ保護機関の決定～大規模なスーパーマーケット・グループによるビデオ監視およびパブでのインターネットを使った実況送達
- ・2003年6月3日のデータ保護機関の決定～民間が経営する公共交通機関では、デンマーク・データ保護法に定められたルールを守ることを条件に、原則としてビデオ監視が許される。
- ・2003年11月13日のデータ保護機関の決定～公共機関が実施するビデオ監視に対する制限の追加

フィンランド

フィンランドにおいては、ビデオ監視に関する特別な法律は存在しない。ただし、多くの異なる法律において、ビデオ監視その他の技術的な監視、観察もしくはモニターについての規定がある。ビデオ監視および会話の記録に関しては、しばしば問題になっている。次のようないくつかのケースがある。

例えば、データ保護オンブズマンは、顧客サービスや職場における電話での通話の録音について見解を公表している。

「ビデオ監視におけるプライバシー（2001年4号）」と題するパンフレットが発行されている。

ギリシャ

- 1) アセンズ地下鉄における閉鎖回路テレビの設置の関する文書（2000年1月28日、文書390号）
- 2) 閉鎖回路テレビに関する指令（2000年9月26日、指令1122号）
- 3) ホテルにおける閉鎖回路テレビに関する決定（2002年84号）

アイルランド

1998年および2003年データ保護法事例研究1996年14号（閉鎖回路テレビの使用）

フランス

データ処理、データファイルおよび個人の自由に関する法律

〔CNIL〕（1978年1月6日、法律78-17号）。1994年6月21日のデータ保護機関による勧告（94-056号）。就労場所その他でのビデオ監視に関するデータ保護機関のガイダンス。

公共の場所における公共の安全のためのビデオ監視に関する特別法（安全に関する法律、1995年1月21日、法律95-73号、2000年9月11日オールドナンスによる修正）。

法律95-73号の施行に係わるデクレ（1996年10月17日、デクレ96-926号）および通達（1996年10月22日）

ドイツ

2001年改正連邦データ保護法第6条b項
国境警備法第25条

州警察法上の警察によるビデオ監視に関する規則
議会では、非公開のビデオ監視を禁止する法案を審議中

イタリア

個人データ保護法典（2003年6月30日、運用基準の採択を認める政令196号）

2002年4月10日プライバシー決定（2号、運用基準採択の推進）、2001年9月28日プライバシー決定（銀行が使用する生体および顔面認識技術）ならびに2000年11月29日プライバシー決定（いわゆる「ビデオ監視デカログ」）

1999年6月22日大統領令250号（シテイセンターおよびアクセスが制限された地域への車両の乗り入れ規制）

1992年11月14日政令433号および1993年法律4号（博物館、国立図書館および資料館への適用）

2002年2月4日法令45号（全国ルートの乗客船）

1970年5月20日法律300号4条（いわゆる労働者法）

ル ク セ ン ブ ル グ

個人データの保護に関する個人保護法(2002年8月2日)10条および11条

オ ラ ン ダ

1997年に出版された特別に公共空間における個人および財産の保護を目的としたビデオ監視のためのガイドラインを含むデータ保護当局の報告書。この1997年ガイドラインの最新版は、2004年に入手できる。2003年に、ビデオカメラ監視を使った捜査がすべてのオランダ自治体に導入された。

最近、下院において刑法改正が成立、2004年1月1日に発効した。これにより、一般人が立入れる場所の画像を同意なしに撮ることを刑事処罰の対象とするになった。

政府は、地方自治体法の改正案を提出した。この改正案は、一定の要件(例えば、ビデオ監視の効果を定期的に評価する義務を課すなど)の下、公的目的をもって公の支配において、ビデオ監視装置を利用する明確な権限を市議会および市長するものである。

ポ ル ト ガ ル

1998年7月22日法令231号(自衛のための民間警備活動および装備)

1998年8月4日法律38号(スポーツ競技に係る暴力事件で取られるべき対策)

2001年9月28日法令263号(ダンス会場)

2002年4月12日法令94号(スポーツ競技)

ス ペ イ ン

1997年法律4号(公安機関による公共空間のビデオ監視)

1997年法律4号、1999年施行規則596号

ス ウ ェ ー デ ン

ビデオ監視についての特別法がある。通常のビデオ監視については、1995年法律150号。非公開のビデオ監視(刑事捜査)については、1995年法律1506号。

通常のビデオ監視を行う場合には、原則として、県行政委員会からの承認が必要である。これに対し、郵便局、銀行、店舗などの場合には、承認は不要である。県行政委員会の決定は司法審査の対象となる。

デジタル技術を使ったビデオ記録は、個人データ処理とみなされ、通常のビデオ監視に関する法律で特に規制されていない範囲までデータ検査院の監督の対象となる。

調査員界はビデオ監視に関する報告書を公表している(SOU 2002:110)。

イ ギ リ ス

2000年閉鎖回路テレビ運用基準(情報コミッショナー)現在、改定中

さらに、重要な規制措置としては、アイスランド(2000年法律77号)、ノルウェー(2000年4月14日法律31号第7編)、スイス(連邦コミッショナーの勧告)、ハンガリー(データ保護機関による2000年12月20日勧告)がある。

5. EC95/46指令(EU個人データ保護指令)が一部または全部不適用な事例

EC95/46指令(EU個人データ保護指令)は、公共の安全、防衛、国家の安全および刑法分野での国家活動、その他EC法の適用対象外の活動目的で、音声や画像データ処理をする場合には、適用されない。もちろん、データ保護指令は、こうした活動にも一般的には適用がある。ただ、多くの加盟国では、国内法で、こうした活動に対し、この指令が適用除外になるように定めている。

(A)

いくつかの加盟国においては、前記のような目的で処理作業を行う場合にもすべて、個人データの自動処理の関する個人の保護のための欧州議会条約(1981年108号)および関連する欧州議会勧告、さらには加盟国の一定の規定に従って設けられた安全確保措置が適用になる(指令3条2項および前文第16参照)。警察や司法当局が実施する調査活動の関係するビデオ監視、さらにはその場所に関する情報提供をすることなしの「覆面」のものを含む、国の安全のためのビデオ監視は、特別の性格のものでありかつ特別の規定の存在を前提とするものである。したがって、この種の処理作業について、本報告書では詳しく触れていない。

しかし、本作業部会は、データ保護指令の枠

外にある他のいくつかの個人データ処理作業の場合と同様に、現実の公共の安全義務の遂行または刑事犯罪の防止、捜査および取締を理由に実施されるビデオ監視は、人権および基本的自由の条約 8 条の規定に定められた要件を尊重しなければならないことを強調したい。同時に、当該ビデオ監視については、一般に周知され、かつ、具体的な危険と特定の犯罪の防止に関連しかつ比例して～例えば、危険にさらされているという前提、ないしは合理的に犯罪が起きる可能性のある公的な出来事に関連して～いなければならない。ビデオ監視装置の効果～例えば、非合法の活動が他の地域もしくは部門に移動するかもしれないという事実～が考慮されなければならない。また、データ管理者は、常に、データ主体がどのように自らの権利を行使できるか明確にしておかなければならない。

ビデオ監視が、次第に警察と他の公的機関（例えば、自治体）、民間機関（銀行、競技団体、交通会社）との共同で実施されるようになってきている状況にある。この場合、履行されるべき業務に関するそれぞれの役割と責任が不明瞭になる危険がある。

(B)

第二に、データ保護指令は、純粋に個人あるいは家庭内活動の枠内にある場合には、自然人による処理作業には適用されない（指令 3 条 2 項および前文第 1 2 参照）。

これは、例えば、ビデオ監視が、窃盗の防止、ないしは、いわゆる「電子家庭」の管理に関連して、家庭内部での出来事を遠隔操作する形で実施されている状況においても該当する。ただし、たとえビデオ監視装置が、財産の保護ないしは安全の確保をねらいとしているとしても、私人の居住場所外もしくは近隣に設置されている場合には、該当しない。

この場合、第一に、ビデオ監視装置は、自分の居住場所に入るドアの所有者による利用とはいえない。むしろ、複数の入口および居住地域をモニターするための、契約、連合あるいは集合住宅ベースでの、複数の所有者による利用にあたる。したがって、データ保護指令が適用になる活動にあたる。

ビデオ監視装置が一つのドア、階段の踊り場、駐車場などをモニターねらいで、個人の家

庭の利益のために管理されているとする。この場合、個人データ処理はもっぱら個人的利用されかつデータは第三者に提供されない事実を根拠に、データ保護指令の適用を避けることはできる。しかし、この場合でも、当該装置の管理者は、隣人やその他の通行人の法律上の権利や利益を尊重する義務は免除されない。EU加盟国においては、これらの権利や利益は、現実には、データ保護原則とは無関係に、私人の権利、画像、家庭生活および私的空間を護る一般（民法）規定により保護されている。例えば、一貸室のドアの外に設置したカメラの撮影角度によっては、同じ階にある医院ないしは弁護士事務所の顧客を体系的に記録することができる。したがって、職業上の守秘義務に不当な介入となる恐れがある。

ビデオ設置の指導にあたっては、通告や情報の掲示、さらには家宅侵入ないしは犯罪がなかったと分かった場合には、定期的な（数時間内の）画像の削除など、特別の注意が払われる必要がある。

(C)

最後に、データ保護指令 9 条は、加盟国が、データ処理がもっぱらジャーナリズム、文学もしくは芸術的な表現のために行われている場合、とりわけ音声視覚分野においては、規定の適用除外または軽減措置をとることを予定している（指令前文第 1 7）。表現の自由に関するルールとプライバシー権との調和をはかるために必要な適用除外規定を置かなければならない。この点に関して、ビデオ監視にあたっては、とくにインターネットカメラないしはオンラインカメラを設置するときには、広告活動や旅行振興活動に含まれた目的への流用ないしはその目的とのギャップをなくするために、個人の保護に特別の注意を払うように求められる。

6 . ビデオ監視と個人データの処理

すでに触れたような多様な状況に照らして、本作業部会は、一部もしくは全部につき自動手段を用いた閉鎖回路テレビその他ビデオ監視装置を使って画像や音声データなどの個人データを処理する場合、ならびに記録システムの一部をなすもしくは記録システムの一部とする計画において個人

データを自動手段以外で処理する場合には、E C 95 / 4 6 指令 (E U 個人データ保護指令) の適用があるという事実に注目すべきである、と考えている。

次の場合には、認識されたまたは認識されうる自然人の画像および音声データは個人データに当たる。

- a) 画像が、人の特性を捕らえていないときであっても、閉鎖回路装置の中で使用されている場合
- b) 画像が個人の顔面を撮影していないとしても、その画像に、他の情報、例えば、自動現金預払機の監視に関して、車輛のナンバープレートないしは提示が求められた暗証番号が含まれている場合
- c) 画像の収集が、例えば、速度制限を守らないときに限り、しかも、ビデオ撮影がまったく日常的な必要性に基づいて行われ、かつ、「中央」と接続ないしは画像を遠隔の端末などに送信するために伝達手段が使われている場合。ただし、処理に使用された媒体～例えば、携帯用のビデオ機器か、カラー画像か・白黒画像か～、使用された技術～例えば、ケーブル仕様か、光ファイバー仕様か～、装置の型式～例えば、固定式か、交換式か～、携帯式か、画像収集方法の特質～例えば、継続的か、非継続的か～、は問わない

データ保護指令にいう識別性は、個人の場合、第三者が保有する情報もしくは特別な技術や装置を使い他から得た情報とのデータ照合により確保することもできる。

したがって、データ管理者が最初に注意すべきことの一つは、ビデオ監視が識別できる人の個人データの処理を伴っているのかどうかを点検することである。伴っているとすれば、データ保護指令は、加盟国の国内法が、公共の安全目的の場合には承認が要るかどうかにかかわらず、適用がある。

これは、次のような例から説明できる。銀行の入口か内部に装置が設置された場合には、その装置により顧客の識別がねらいとなる。ところが、一定の状況の下では、データ保護指令は適用除外となるかも知れない。例えば、自動車の道路の全画像を提供する装置に対すると同様に、自然人に関する情報が含まれていないあるいは抽出できないような、水源ないしは廃棄物処理地域を識別す

るために収集される空間調査画像が、そうした例にあたるといえる。

7. データ管理者の義務および必要な注意

A) 適法な処理

適法な処理の要件 (指令 6 条 a 項による) に照らして、データ管理者は、その部門に適用される～法律、規則、法律に相当する運用基準等における～一般的規定や特別の規定を遵守しているかどうかについて、事前に点検しなければならない。これらの規定には、公共の安全目的に加え、個人データ保護に関する以外のこと、例えば特定の行政機関の特別の許可を得かつ当該機関の指示に従うように求めること、が書かれているかも知れない。

ビデオ監視がデータ保護原則に準拠して行われ、かつ、プライバシーが不適切に利用されないように、あらゆる限りの措置が講じられなければならない。

また、この点に関して、監督機関が発した勧告やその他自主規制文書に定められたところに従い、最良の運用がなされるように配慮しなければならない。

さらに、他の国内法の規定、～憲法原則、民法や刑事法の規定など～が点検される必要がある。とりわけ、「肖像権」もしくはその者の生活の本拠を保護するために適用される原則を点検するにあたっては、判例をあたる必要があり、その者の世帯以外の居住場所～例えば、ホテル、事務所、トイレ、着換場所、室内の電話室等～は、私人の居住場所とみなされる。

ビデオ監視装置が、民間機関もしくは公共機関により設置されている場合で、しかも一定の公的職務については捜査当局のような特定の行政機関のみが法律に基づいて遂行できるとされているとする。この場合で、地方自治体が、設置の理由として安全ないしは犯罪の防止、捜査および取締目的をあげているときには、これらの目的を策定しかつ周知するにあたり、データ管理者が適法に遂行できる業務の範囲については、特別の注意を払わなければならない。

この点は、とくに、地方自治体が公序や公共の安全に関し直接の権限を有していないのにも拘らず、監視活動において補助的な役割を果たすような場合に問題になる。監視が犯罪の取締目的で行われ、実際に犯罪が起きたときに証拠に利用され

るようになっている場合も同様である。

B) 特定、明確かつ適法な目的

データ管理者は、データ収集の目的が不特定ないしは不明確でないようにしなければならない。これは、データの処理がその目的に相応している（指令6条b号）のかどうかを評価する場合の明確な基準を定めるためでもある。

明確性とは、データ主体に提供される情報およびその通知の中に収集の目的をあげることが必要であることを意味し、データ保護指令20条に従い処理が行われる前に検査を要することを意味する。

収集された画像は、単なる機械的な再生に供されるようなことは明確に禁じられる。例えば、コピーは原則禁止となる。

他の重要なプライバシー政策問題、例えば、画像がいつ削除されるのか、データ主体の開示請求、データに対する法律相談などの重要な問題に関し対応策を示す場合、その目的を文書しておくものとする。

C) データ処理の適法性の要件

データ管理者は、ビデオ監視をするにあたり、前記A)に述べたような特定の規定を遵守するとともに、とくに個人データ保護の観点から、少なくともデータ保護指令7条の下でのデータ処理に関する適法性の要件の一つを充足していることを確認するものとする。

極めて稀な事例であるが、カジノ運営の例のように、ビデオ監視にかかるデータ処理が、法律上の義務遂行に起因する場合、あるいは患者の蘇生チームが遠隔モニターをするような、現実の利益を保護する必要性に因る場合がある。さらに、交通事犯ないしは犯罪多発地域の公共交通機関での暴力行為の防止にある場合もある。つまり、データ管理者は、しばしばデータ保護指令第7条e号にいう公益のため、あるいは特定の規定の下での公権力行使のために、処理業務の遂行を求められることがある。こうした場合に、データ管理者は、データ主体の利益、基本権および自由を優先させながらも、これら法律上の利益を確保するものとする（指令7条f号参照）。

公益を目的とする事例と公権力の行使を目的とする事例の双方のうち、とくに後者においては、データ処理作業にセンシティブな要因が多く、デ

ータ管理者は、業務、権限および法律上の利益を比較検討する場合、注意深さが求められる。こうした検討を行う際に、理由もなしにその業務や権限の範囲を拡大することは絶対に禁止されるべきである。

とくに、相対立する利益を比較検討する際には、ビデオ監視装置の設置、一定のデータ蓄積ないしはその他処理作業に伴い、保護されるべき利益が対立しないように、事前に関係当事者から意見を聞くなど、特別の配慮がなされなければならない。

最後に、データ主体の同意を得ることに関し、公権力の行使を目的とするデータ処理の場合には、不明確であってはならず、明確な情報に基づかなければならない。同意は、個別に得られなければならないし、個人の私生活が行われている居住場所に関しては、とりわけである。

データ処理の適法性については、犯罪関連のデータに対する特別の安全確保措置を定めたデータ保護指令の規定を考慮して、評価されるべきものとする（指令8条5項参照）。

ビデオ監視が個人の権利や自由に対する特別の脅威をもたらす恐れのある場合には、事前検査の仕組みを使ったデータ処理に関する最初の評価の結果を見定めた上で、追加的な措置や対応をとるものとする。

ビデオ監視方法にかかるデータ処理作業は、公共機関が実施する場合には、常に明確な法律の根拠に基づくべきである。

D) ビデオ監視利用における比例原則

データはそれを求めた目的に合致しかつ比例したものでなければならないという原則は、第一に、閉鎖回路テレビや同類のビデオ監視装置は、補助的な存在としてのみ利用できることを意味する。

すなわち、こうした装置に依存することを正当化する目的が存在すること。

比例原則によると、ビデオ監視装置は、物理的かつ論理的にも、画像収集が伴わない他の防止手段、保護手段もしくは安全手段、すなわち破壊行為に耐え得る防護ドア、自動玄関開閉装置または合同警報システムの使用、夜間の街頭防犯灯の改善などをもってしても、依然として不十分であり、かつ、前記の適法な目的を達成できないと証明できる場合に限り、利用できることになる。

比例原則は、相応の技術の選択にあたっても適

用される。ビデオ監視装置の継続利用の要件やデータ処理方法は、開示原則や保存期間とも関連する。

例えば、行政機関は軽い犯罪に対応するということでは、ビデオ監視装置の設置を避けるべきである。例えば、学校その他の公共場所での喫煙禁止、公共の場所での吸殻の投げ捨てや散らかしの防止をねらいとする場合が、これにあたる。

言い換えると、事例ごとに、求められた目的に関し、「妥当性の原則」を適用する必要がある。これは、管理者側に、一種の「データ最小化義務」を負わせることになる。

例えば、競技場周辺で暴力事件が連続している場合、あるいはバス停やその周辺地域でバスへの襲撃が相次いだ場合、相応のビデオ監視や警報システムを設置することは適法といえる。バスの運転手に対する侮辱や車輦へのいたずら書きを防ぐのをねらいとした装置の設置には、問題がない。データ保護機関が問題としているのは、ゴミ箱の外ないしはゴミを捨ててはいけない場所にゴミ袋を放置するような、軽い行政罰の対象となるような市民を識別するためとか、水泳場で窃盗をしようとする人を探し出すためとかの場合である。

こうした場合には、公的ではない居住場所と同様と見て、ビデオ監視装置の設置に対し、比例原則をより厳しい基準で適用すべきである。

この点については、加盟各国の権限ある当局間での情報や経験の交換が有用といえる。

こうした検討結果は、とくに徐々に増加傾向にある公共建築物や役所およびその周辺における自警や財産の保護目的でのビデオ監視の利用に対しても応用できる。こうした活用の仕方による大規模なビデオ監視への依存がもたらす間接的な効果を、より一般的な視点から評価するように求められる。例えば、複数の装置の設置が本当に抑止効果を発揮しているのかどうか。犯罪者ないしは破壊者が、ただ単に他の地域に移動したり、他の活動に移って行っただけではないのかどうか。

E) ビデオ監視活動の実施における比例原則

データは適切、妥当なものでありかつ過度であってはならないという原則は、いったん公権力の行使目的が適法とされると、データ処理に適用ある「配置にかかる比例原則」に従って、注意深い評価を行うように求める。

第一に、撮影の配置にあたっては、とりわけ次の点を考慮しなければならない。

- a) 撮影角度が求められた目的に関係しているか。例えば、監視が公共の場所において実施されている場合には、その角度は、求められた目的とは無関係のものや身体的特徴がはっきりと識別できたりしないように設定されなければならない。あるいは、とくに、ズーム機能が使えるときには、その近隣にある私人の住宅の内部がはっきりと覗けないように設定されなければならない。
- b) 撮影に使う装置の型式。例えば、固定式か、移動式か
- c) 実際の配置。例えば、カメラの位地、固定した視野の利用か、移動式カメラか等々
- d) 撮影時にズームができるかどうか、ないしはそれ以降に画像を、例えば保存目的で、電磁処理できるかどうか、さらには、個々の画像を、ぼかしたり、消去できるかどうか
- e) 画像停止機能
- f) 音声、視覚できる警報の送達を受ける「センター」との接続
- g) ビデオ監視結果から取られる措置、例えば、入口の閉鎖、監視スタッフの召集等々

第二に、「画像の保存および保存期間についての決定」に関して考慮する必要がある。個々の事例における特徴を見ながら、保存期間はできるだけ短くなるようにする必要がある。

限られた事例、例えば、スーパーマーケットの現金取扱場所のようなところでは、装置は、単に画像を閉鎖回路テレビで視覚できれば十分であり、記録を残す必要はない。これに対し、他の事例、例えば、私人の居住場所のようなところでは、画像を記録する理由あり、と見てよい。ただし、保存は数時間、またその日の終わりまであるいはその週の終わりまでには自動的に消去されるものとする。例外的に、警告が発せられている場合または特に留意すべき要請がある場合には、警察ないしは司法当局が決定を下すまで、しばらくの間、消去せずに記録を維持する合理的理由がある。

例えば、シティセンターや通行が規制された地域への許可なしの車輦の乗入れ防止を目的とした装置では、違反した者のみを画像に記録すべきである。

この比例原則問題に関して、できるだけ短期の保存が望ましいとしても、1週間は過多とはいえない点に十分に留意すべきである。例えば、ビデオ監視画像は、強盗をする前に銀行の周りを往来する者の識別に利用することができるからである。

第三に、人を識別する場合には、顔面その他画像化された行動や行為が加わると、より確実なものにできるという点に注目すべきである。例えば、銀行は、顧客の画像と行為とが結合する場合、容易に本人確認ができる。

この点に関して、銀行の入口に設置された装置により得られるビデオ監視画像を一時的に保存することと、銀行がその顧客の同意を得て提供を受けた写真や指紋などより権利侵害につながりかねないデータを永続的に収集するデータバンクをつくることとの間には、はっきりとした違いがあることを認識しなければならない。

最後に、データ保護指令25条以下にある適切な保護の規定に照らして、ビデオ監視活動とは無関係の機関には適用のない「第三者へのデータの伝達」に係る原則と、全部または一部のデータを海外ないしはオンライン形式で開示することに関して、どのように考えるべきか、検討が必要である。

画像が妥当でありかつ過多ではないことを求める要件は、複数のビデオ監視装置の管理者がそれぞれ情報を保有している場合で、それらを照合（マッチング）するときにも適用があるのは明らかである。

こうした安全確保措置は、個人データ処理を、できる限り防止または少なくすることにねらいがあることから、いくつかの加盟国の国内法においては、「個人データ利用削減の原則」と言われる原則に沿ってとられている。

この原則は、あらゆる部門において実施されるべきである。なぜならば、多くの目的が、当初は個人情報に利用が必要であるように見えても、現実には個人データに依存することなくあるいは現実には匿名のデータの利用によって達成できる事実があるからである。

こうしたことは、事業での人員の合理化の必要性ないしはユーザーに提供されるサービスの改善といった正当化できる要請がある場合にも、検討を要する。

F) データ主体へ提供される情報

公開でビデオ監視装置を適切に利用することとは、データ保護指令10条および11条の従いデータ主体に対し適切な情報を提供することを意味する。

データ主体は、データ保護指令10条および11条に沿って情報提供を受けるべきである。公共の行事、催事ないしは広報活動に関しビデオ監視が行われている場合、データ主体は、それが作動中である事実に気づかされるべきである。データ主体は、監視されている場所について詳しく知らされるべきである。

監視装置の正確な場所について特記する必要はない。しかし、監視の理由については明瞭にされるべきである。

情報は、監視場所と合理的な距離内にあるところに掲示されるべきである。極めて限られたケースではあるが、撮影事情に照らして、監視場所から500メートル離れたところに情報を掲示するのも許される。

情報は、判読可能であり、しかも、分かりやすく簡略に掲示されるべきである。情報は、ビデオ監視や禁煙情報に関してすでに有用とされているシンボルを使うことも可能である。情報は、画像が記録されているかどうかにより異なるものとなるかも知れない。ビデオ監視の目的や担当の管理者が、事例に応じて決めなければならない。情報提供の様式は、個々の掲示場所に応じて調整されるものとする。

データ主体へ情報を提供する義務は、データ保護指令10条、11条および13条に定められる事例に該当する場合に限り、特定かつ正当な理由があるものとして、免除される。例えば、被告人側弁護士が適法に実施した調査の過程において収集したデータに対しては、防護権行使の一環として、当該情報の提供がその目的達成を妨げることになる場合に限り、暫定的に開示請求を制限できる。

最後に、目の不自由な人たちに対する情報の提供にあたっては、特別の配慮がなされるべきである。

G) 追加的要件

前記3・3)においても述べたように、データ保護立法に定められる追加的要件、注意点および安全確保措置に関して、さらには、データ保護指令18条、19条および28条の下で、独立した規制当局の監督の対象となり、かつ、そこへの通知の対象

となる個人データの処理に関して、本作業部会は、とくに次の点に注目して欲しいと考える。

- a) もっぱらビデオ監視方法の目的の範囲内で、ないしは、その操作が適切かどうかを調べるために当該装置を維持する目的で、記録された画像を審査する場合には、特定の、しかも限られた数の自然人のみにアクセスが認められるものとすべきである。言い換えると、これは、データ主体からの開示請求または警察もしくは司法当局が犯罪捜査目的で発行した法的な命令に基づいて認められることになる。

ビデオ監視が、犯罪の防止、捜査、取締のみを目的としているとする。この場合には、二つの開示キー～つまり、管理者が持つ一つと警察が持つもう一つ～を使用する方式は、多くの場合に、画像が、短期の画像保存期間になされるデータ主体の適法な開示請求権を侵害することなしに、しかも、許可されていないスタッフよりもむしろ警察のスタッフによって審査されることが保障されるという意味では、有用性が高い。

- b) データ保護指令 17 条にあげられたような問題が起きないように、適切な安全確保措置が講じられるべきである。例えば、不正操作、データや関連する証拠の改ざんもしくは破壊を防ぐねらいから、データ主体、第三者もしくはデータ管理者自身の権利を守るのに有用な情報の頒布など。
- c) また、記録された画像の質を保つことも重要である。とくに、同じ記録媒体を継続的に使用すること。これにより、以前に記録された画像を完全に消去することの失敗の危険を少なくすることができる。
- d) 最後に、ビデオ監視活動に常時かかわる処理者が十分な訓練を受けかつその義務を全うするために従うべき手続に注意することは重要である。また、管理者や処理者が、誤りを犯す危険や画像化された個人を正しく識別する手法の関する訓練を受けることは、有益なことと考える。

H) データ主体の権利

収集されたデータのうち特別の性格を有するものについては、データ保護指令の 13 条および 14 条に基づくデータ主体よるデータ処理拒絶権の行使を拒否してはならない。E C 95 / 46 指令 (EU 個人データ保護指令) は、確実にデータ主体が、何時でも、特別の状況において、適法な根拠に基づいて自らに関するデータの処理を拒絶することが認めている。

データ主体にはそっとしてもらい権利があり、画像は通例短期間保存される。このことは、データ主体が自らの存在確認をしてもらうための個人データの開示請求をする権利を狭めることになる。しかし、具体的に請求が行われた場合に、画像の短期保存は該当する画像の検索を容易にし、結果として、この開示請求権は保護されることになる。また、この場合、第三者の権利を暫定的に保護する措置が採られる必要がある。

画像の保存期間が短期であることから、調査、費用および労力を理由に、画像の検索に制限を付すことができる。いかなる制限も、予定された保存期間内に特別の事案が起きた場合のデータ主体の防御権に十分な配慮をした上で、すべて本法で規定されなければならない (指令 13 条 1 項参照)。

I) 特定データの処理作業に係わる追加的安全確保措置

もっぱら画像化される者の人種、宗教もしくは政治的見解、労働組合への加盟または性生活に関するビデオ監視を行うことは禁止されるべきである (指令 8 条)。

作業部会は、識別されたまたは識別されうる者の画像を収集するためのビデオ監視の多方面への適用をねらいに徹底した検討を行っているものではない。しかし、画像収集のやり方によっては、その良し悪しについて個別に評価された方がよいとの理由から、データ保護指令 20 条にいうデータ処理作業の事前検査の仕組みの活用注目する必要があることを強調したい。

これまでの経験および検討結果から、とくに、次のような事前審査を必要とする事例をあげることができる。

- a) 複数のデータ管理者が管理する永続的相互接続可能なビデオ監視装置
- b) 画像に加え指紋のような生体データが結合 (例えば、銀行の入り口)

- c) 声音識別装置の利用
- d) 比例原則の適用がありかつ特定の法律を根拠に、記録された画像、識別データを使った同時自動検索システムを応用した検索システムの設置
- e) つけひげやかつらで変装したような通行人の識別のみならず、犯罪嫌疑者に焦点を合わせた顔面認識システムの利用。手形、一定の肉体的な特徴（例えば、肌の色、眼球、ほお骨等）を用いた標準的な識別装置ないしはその他異常行動の前歴（不意の行動、一定の距離の繰り返しの往来、駐車の仕事等）を使った、特定個人を自動的に識別できるシステムを含む。この点について、下記にあげた事例に関し生じる可能性を考慮し、人為的な介入が必要
- f) 自動的に、人の行動のルートや往来、さらには復元ないしは予測を可能とするもの
- g) 必要な身元確認をしないでその場所に近く事実を知らせる標準的な警報ないしは火災報知とは異なる、人のプロファイル、諜報分析および介入システムに基づき自動決定を行うもの

8. 雇用関係にかかるビデオ監視

本作業部会は、すでに、2001年9月13日に採択された「雇用関係にかかる個人データ処理に関する見解（2001年8号）」、2002年5月29日に採択された「職場における電子通信の監視に関する作業部会報告書」において、より一般的な文言を用い、雇用関係にかかるデータ主体の権利、自由および尊厳を護るねらいで、いくつかの原則を明らかにし、注意を喚起している。

前記の報告書での検討事項に加え、ビデオ監視の現実の適用範囲について言うと、労働作業の質や量を直接にあるいは遠隔場所から管理する目的で設置されたビデオ監視装置の利用は、雇用関係にかかる個人データ処理を伴うことから、原則として許されないこととすべきである。

ただし、ビデオ監視装置が、生産や職業上の安全義務を達成する目的で、適切な完全確保措置を講じた上で、遠隔操作により間接的に使用されているような場合は別である。

さらに、これまでの設置実務から判断して、被用者が私的利用に供するために確保された場所あ

るいは雇用業務遂行用ではない場所、例えば、トイレ、シャワー室、ロッカー、休憩場所のような場所は監視の対象とされるべきではない。もっぱら財産を保護しかつ重大な犯罪を防止し、捜査し、取締るために収集された画像は、些細な規律違反で被用者を懲戒にふすために利用してはならない。被用者は、何時でも、収集された画像の内容を使って反論をすることが認められるべきである。

情報は、その場所で働いている被用者その他あらゆる者に対しても提供されなければならない。この情報には、管理者の確認、監視の目的、その他データ主体にかかる公正な処理を保障するのに必要な情報を含む。例えば、会社の経営陣が検査の対象とする記録、記録の期間および犯罪取締当局に記録を開示する要件。また、例えば、雇用関係においては、情報の提供にあたり、記号を使ったとしても十分であるとはみなされない。

9 結論

本作業部会は、ビデオ監視分野におけるEC95/46指令（EU個人データ保護指令）の下で採択された措置の各加盟国での統一適用に資する目的で、この作業部会報告書を作成した。

* * *

この報告書にあげられた原則に沿って、この枠内で、各加盟国は、生産者、サービスプロバイダーおよび、販売者ならびに技術、ソフトおよび技術の開発を行っている研究者の活動に関する指導基準をつくることは重要である。

* * *

ブルッセル・ドン
2004年2月11日
作業部会長

《プライバシーコラム》

インターネット上のHP（ホームページ）に書かれた氏名とメールアドレスに自由にメールを送ってもいいのでしょうか

一般に、HPに掲載された氏名とEメールアドレスがそのHP作成者のものである場合には、そのHPの内容に関する問い合わせや苦情をいうコンタクトポイント〔連絡窓口〕と考えられます。また、HPへ公開しているのは、本人が自発的に自分の個人情報を不特定かつ多数の人

たちに提供しているケースにあたります。したがって、原則として、直接本人あてにメールを出すのは問題ないと解されます。ただ、そのEメールアドレスへ、広告宣伝用のEメールを送ろうとする場合には、その旨を本人に通知しなければ、個人情報保護法違反となると解されず（18条1項）。また、送ったメールの内容が、掲載した人を強迫するものであったり、卑猥なものであったりするときなどには、そのEメールを送った人が刑事制裁や民事の損害賠償請求の対象となるといえます。

（PIJ個人情報保護プロジェクトチーム）

《新刊書・書評》

吉田竜太郎・西邑亨 共著
『地域住民と自治体のための
住基ネット・セキュリティ入門』
七つ森書館〔2004年9月発行〕
価格 1,575円

2003年秋、長野県は、住基ネット対応チームを組織し、いわゆる「安全確認調査」ないしは「侵入実験」～「住基ネットに係る市町村ネットワークの脆弱性調査」～を実施した。そして、2004年2月に、長野県は、同調査チームが作成した最終報告書～「住基ネットに係る市町村ネットワークの脆弱性調査最終結果について」～を公表した。この最終報告書では、市町村の情報セキュリティの基本が全くなっていないことが指摘された。

この調査チームにメンバーとして加わったのが著者の1人、吉田氏である。本書は、吉田氏が2004年3月に行った講演記録を、先端技術専門のライターである西邑（にしむら）氏が市民向けにポリッシュしたもの。

本書は、住基ネット運用現場での「セキュリティ音痴」の実情を紹介するとともに、「セキュリティとは何か」について得々と説いた書物。「個人情報を守る」ということがいかに至難の技であるかが分かる。ただ、脱住基ネット論者には、「住基ネット容認論を甘くする塩」と映る可能性も。調査チームの最終報告書も収録されているので、資料をしても有用。一般人たちや自治体職員にとっても分かり易いセキュリティの入門書。是非とも一読されたい。

（PIJ 常任運営委員 平野信吾）

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 高橋正美・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>
2004.10.12発行 CNNニュースNo.39

入会のご案内

季刊・CNNニュースは、PIJの会員（年間費1万円）の方だけに送らせています。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

・PIJの相談役の河村たかし衆議院議員が『国敗れて議員あり』（徳間書店、1,680円）を出した。「役人天国」「議員天国」、この国の「国民がわき役」の実態を斬ったもの。総理になるのはどえらい。是非一読を

(N)