2005/7/1 発行

プライバシー
インターナショナル
ジャパン（PIJ）
国民背番号問題検討
市民ネットワーク
Citizens Network Against
National ID Numbers（CNN）

季刊発行
年４回刊

CNNニュース No.42

■巻頭言■

「住基ネットへの参加強制は憲法違反」との画期的な判決下る

――住基ネット訴訟で、金沢地裁、「住基ネットからの離脱は、憲法上の権利」、個人情報の住基ネットからの削除を命令！！

住基ネットはプライバシーの権利などを侵害し憲法に違反するとして、石川県の市民が国や県などを相手に、個人情報の削除や損害賠償を求めて訴えていた。この裁判の判決が、５月３０日に、金沢地裁であった。井戸裁判長は「ネットからの離脱を求めている原告に限れば、住基ネットに関する住民基本台帳法の条文は憲法１３条に違反する」と判示。また、「住基ネットは原告らのプライバシーを犠牲にしてまで達成すべきものとは評価できない」として、訴えていた市民の個人情報の国への提供禁止と削除を県に命じた。損害賠償については棄却したが、個人情報削除を命じたのは全国で初めて。画期的な判決だ。

井戸裁判長は「個人情報に住民票コードが付けられれば、多面的な情報が瞬時に集められ、住民が行政の前で丸裸にされる」と指摘。住基ネットの目的は「住民の便益」と「行政事務の効率化」とし、「プライバシー権と住民の便益のどちらを優先させて選択するかは、各個人が自らの意思で決定すべきで、行政が便益の方が価値が高いと押し付けることはできない」と述べた。また、同裁判長は、住基ネットのセキュリティについては、一定の情報保護措置が講じられているが、全国の市町村で確実に実施されるか疑問とした。

これまで、住基カードの発行差し止め訴訟でカード発行を合憲とする判決などは出ているが、住基ネットからの離脱をめぐる判決では初めてのもの。東京をはじめ全国１３地裁でも同様の訴訟が係争中だが、与える影響は大きい。

同じく住基ネットの違法性が争われ、金沢地裁判決の翌日（５月３１日）に下された名古屋地裁判決では、市民の訴えを一笑に付し、これを認めなかった。同地裁での裁判では、審理が突然打ち切られるなど、西尾裁判長の高慢な訴訟指揮が目立ち、摩擦が多かった。

住基ネットは、２００２（平成１４）年８月に一次稼働した。だが、現在でも、福島県矢祭町、東京都杉並区、国立市の３市区町は参加を見合わせている。

今回の金沢地裁の判決は、「住基ネットからの離脱は、各個人の憲法上の権利」と宣言したものであり、その意義はきわめて大きい。裁判官のサラリーマン化、司法消極主義の病が蔓延している中、司法権の優位、司法権の独立といった面でも高く評価できる判決である。現在、選択的離脱を認めている横浜市方式の公認、さらには住基ネット自体を違憲の創造物であるとの判断、に導く重要な〝典拠〟にもなりうる名判決である。

２００５年７月１日

PIJ代表 石 村 耕 治

◆主な記事◆

PIJ石村代表に聞く

無線ＩＣタグ・ＲＦＩＤとプライバシー

― ＲＦＩＤ関係個人情報保護に関する公共政策はどうあるべきか

《話し手》石村耕治（白鴎大学教授・PIJ代表）
《聞き手》中村克己（CNNニューズ副編集長）

今日、わが国を含め世界のＩＴ業界が、成長株の一つとして最も注目しているＩＴ技術の一つが「ＲＦＩＤ（＝Radio Frequency IDentification）」、「アール・エフ・アイ・ディ」である。この〝ＲＦＩＤ〟の邦訳はさまざま。「無線ＩＣタグ」、「ＩＣタグ」、「電子荷札」、「電子タグ」、「非接触型ＩＣタグ」あるいは「次世代バーコード」等々。一般に欧米では、「ＲＦＩＤ」、直訳すれば、「無線周波数識別」。わが国では「無線ＩＣタグ」あるいは、単に「ＩＣタグ」、と呼ばれている。ここでは、一応、「無線ＩＣタグ」の言葉を使っておく。

一般に、無線ＩＣタグは、いろいろな商品情報やその流通経路をつかむために使われる本当に小さい電子機器だ。専用の読取書込み装置（リーダーライター）を使って、ＩＣタグに入っているデータをチェックしたり、情報を入力することも可能だ。ＩＣチップはごま粒大（０．４ミリ角～１ミリ角）の大きさ。ＩＣチップには、無線用アンテナもついており、電波でやり取りができる。従来のバーコードとは違って、タグが数メートル離れていても情報を読み取ることができる。

現在は、スーパーのレジでは、商品に付けられたバーコードに赤い光線を照射するだけで、買い物の清算はすばやくできる。もう一歩進めて、マーケットにある全商品に無線ＩＣタグを装着しておく。今度は、レジそのものが不要になる。レジゲートに内臓された受信機で、買った商品に付けられた無線ＩＣタグに盛られた情報を瞬時に読み取り、顧客カードないしはポケットにある電子財布の機能を持つ携帯電話で自動的に清算を終えることも夢でなくなる。これが、無線ＩＣタグが「次世代バーコード」とも呼ばれる理由でもある。

このように、無線ＩＣタグを商品に装着すれば、万引やニセブランドの把握、生鮮品の産地証明などが簡単にできるというのがＲＦＩＤのセールス・ポイントだ。また、無線ＩＣタグから入手できる追跡情報を使って、製造や在庫管理を効率化できる。さらに、消費者の嗜好やトレンドを読み取ることもできることから、企業の経営者には〝朗報〟ともいえるが、消費者にとっては不気味だ。一方、雇用主が従業員の制服に無線ＩＣタグが組み込まれた名札（バッジ）をつけさせれば、働きぶりを追跡・監視することも可能になる。また、無線ＩＣタグが組み込まれた顧客（ポイント）カードで、その顧客の店内での行動を追跡・監視することも可能。さらに、例えば、書店でこうした仕組みが使われれば、タグが装着された書物を、現金で買わない限り、その購入者の思想・嗜好・宗教などのセンシティブ情報を読み取られる危険もある。

商品購入後のＩＣチップを無効にできる仕組み、消費者への遮断チップの提供など、働く者や消費者のプライバシーを守る仕組みの構築が立ち遅れている。

今回は、こうした無線ＩＣタグをめぐる多岐にわたるプライバシー問題について、石村耕治PIJ代表に、ＣＮＮニューズ編集部の中村克己が聞いた。

（CNNニューズ編集部）

■　ＲＦＩＤ（無線ＩＣタグ）とは何か

（中村）「無線ＩＣタグ」については、一般の消費者の関心がそれほど高いとはいえない現状にあると思います。そこで、まず、「無線ＩＣタグ」とは何かについて、お話ください。

（石村）わが国では、一般に「無線ＩＣタグ」は、単に「ＩＣタグ」、あるいは「電子タグ」と呼ばれています。これに対し、欧米では、「ＲＦＩＤ（＝Radio Frequency IDentification）」、「アール・エフ・アイ・ディ」と呼ばれています。

（中村）〝ＲＦＩＤ〟の邦訳がさまざまあるということですね。

（石村）そうです。直訳では、「無線周波数識別」システム。一般には、「無線ＩＣタグ」、「ＩＣタグ」、「電子荷札」、「電子タグ」、「非接触型ＩＣタグ」あるいは「次世代バーコード」等々と。

（中村）一応、最初に、最適な言い回しを選んでください。

（石村）ここでは、一応、「無線ＩＣタグ」、「ＲＦＩＤ」の言葉を使います。

（中村）それでは、話をすすめて行きたいと思います。

（石村）ＩＣチップは、ごま粒大（０．４ミリ角～１ミリ角）の大きさの電子機器です。カードに装着されますと大きくなりますが、タグに装着しますと、本当に小さなものになります。ですから、ＩＣタグは、いろいろな商品情報やその流通経路をつかむために使うことができるわけです。専用の読取書込み機装置（リーダーライター）を使って、ＩＣタグに入っている情報をチェックしたり、別の情報を入力することも可能です。無線タイプのＩＣタグには、無線用アンテナもついており、電波でやり取りができます。

（中村）ＩＣチップは、カードに装着されると「ＩＣカード」になりますが、いま取り上げているのは、商品とか、着衣などに装着されるケースですよね。

（石村）そうです。それも無線が可能なタイプのＩＣチップ・ＲＦＩＤ あるいは無線ＩＣタグについてです。

（中村）ＲＦＩＤ ・無線ＩＣタグの用途は広いですよね。例えば、現在、商品管理に使われているバーコードに替わる利用方法などは、その典型ですよね。

（石村）そうです。現在、商品管理に使われているバーコードでは、製造国・製造者・商品名程度の情報しか操作することができません。このため、品目単位での商品管理が限界でした。

（中村）それが、ＲＦＩＤ・無線ＩＣタグを使えば、どれくらい在庫管理などの方法を改善できるのですか？

（石村）そうですね。ＲＦＩＤ ・無線ＩＣタグでは、大容量、書換え可能といった特性を生かして、商品一点一点に個別のコードを割り振ることができ、より多くの情報を製品に搭載することができます。それに、個々のＩＣタグ自体が無線で情報をやり取りできるため、大量の商品タグ情報を一度に調べることができます。

（中村）従来のバーコードとは違って、無線ＩＣタグの場合は、情報取扱容量も大きく、書換えも可能、しかも数メートル離れていても情報を読み取ることができる〝優れもの〟ということですね。

（石村）そういうことです。

〔図表１〕ＲＦＩＤ技術の特徴とシステムの構図

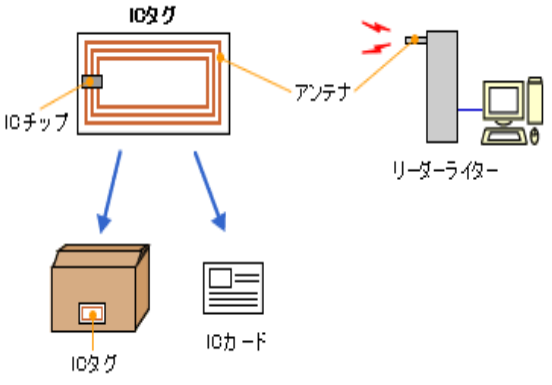
ＲＦＩＤ技術は、①物ないしは人の個体ＩＤやデータを管理する「ＲＦＩＤタグ」と、②そのＩＤを認識・制御する「リーダーライター」と③「アンテナ」装置で構成され、大きく次の二つのタイプに分けることができる。

（ａ）　アクティブ型タグ

～電池を内蔵し、自力で電波を発するタイプのＩＣタグ（例えば　野生動物に装着、行動監視用のタグ）

（ｂ）　パッシブ型タグ

～電池を内蔵せず、リーダーライターのアンテナから出力する電波や磁界を受けて交流することで、ＩＣチップにデータを登録（エンコード）、またデータを返送する仕組みで作動



■　ＲＦＩＤ・無線ＩＣタグの実用化

（中村）これまでは、ＩＣチップは、商品などに付着させる形よりは、ＩＣカードの中に入れる形が一般的だったわけですよね。

（石村）そうです。ＩＣチップは、極めて小さいものですから、タグにして商品に装着させるか、ＩＣカードに入れる必要があります。無線で情報をやり取りできるタイプのＲＦＩＤ・無線ＩＣタグを商品に装着し追跡管理する、ＲＦＩＤの商用およびその普及は、これからの課題とされています。

（中村）現在は、まだ普及していない、ということでしょうか？

（石村）ＩＣチップを商業目的でＩＣカードに入れて普及している例としては、ＪＲの改札口で定期券をタッチまたはかざすだけで通過できるＪＲ東日本の「Ｓｕｉｃａ」やＪＲ西日本の「ＩＣＯＣＡ」をあげることができます。これらのＩＣカード化された乗車券の中にはＩＣチップと無線用アンテナが埋め込まれていて、自動改札機に据え付けられているリーダーライターとの間で（１３．５６ＭＨｚ帯の周波数を使用して）近距離通信を行い金額データの読み取りや、所定の運賃を差し引いた情報のカードへの書き込みを行なう仕組みになっています。

（中村）ＪＲ東日本のスイカ（Ｓｕｉｃａ）カードは、非接触型のＩＣカードですね。

（石村）そうですね。また、ＮＴＴドコモが「おサイフケータイ」として売り出している「ｉモードＦｅｌｉｃａ」にもＲＦＩＤ技術が使われています。ＩＣタグが内蔵されているｉモードＦｅｌｉｃａ対応の携帯電話をリーダーライターにかざすだけでショッピングや搭乗手続きができるというものです。さらに、ＪＲ東日本では、Ｓｕｉｃａ機能を搭載した携帯電話「モバイルＳｕｉｃａ」を利用したサービスを２００５年度後半に開始する計画のようです。

（中村）そうなると、例えば携帯電話で新幹線も利用できるようになるわけですか。便利ですね。

（石村）便利かどうかは、見る角度によって違ってくると思いますが。

（中村）それから、ここでいう「ＲＦＩＤ・無線ＩＣタグが入ったＩＣカード」と、ＣＮＮニューズ前号（４１号）で特集した「生体認証型ＩＣカード」とは、基本的には別物と考えてよいわけですね。

（石村）そうですね。将来的には、「ＲＦＩＤ機能を搭載した生体認証型ＩＣカード」も当然でてくるかもしれませんが・・・。ただ、ＲＦＩＤ機能でドアが自動的に開くのでは、バイオメトリクス（生体認証）を使った意味がなくなる場面も想定されます。ですから、ケース・バイ・ケースでしょう。

■　ＲＦＩＤ・無線ＩＣタグはユビキタス社会の落とし子

（中村）ＩＣタグのそもそもの始まりは、どういったところにあったのでしょうか。

（石村）ＩＣタグの研究を始めたのは、第二次大戦時のアメリカ軍だといわれています。直接の契機は、戦時物資の管理・調達（ロジスティクス）への活用が狙いだったようです。戦後は、核物質の管理に活用されました。１９７０年代に、それまでもっぱら軍事目的に使われていた技術が民間に開放され、世界に広まったわけです。わが国でも、ＩＣタグは１９８５年から工場の生産管理などに使われてきています。

（中村）その後、何でもコンピュータ、つまり、ユビキタス（ラテン語の〝偏在〟の意味）の時代に入り、あらゆる物にＩＣチップを組み込めば便利な社会になるという考えが広まってきましたね。こうしたトレンドに乗り、「無線ＩＣタグ」も汎用されていったわけですね。

（石村）そうです。バイオメトリクス（生体認証）、音声認識、ナノテクなど、他の先端技術とともに、ユビキタス社会実現のツールとしてさまざまな分野で利用が期待されているのがＲＦＩＤ・無線ＩＣタグ技術です。

（中村）とくにＲＦＩＤは、監視カメラなどと同様に、個体識別、トレーサビリティ（追跡能力）といった面で威力を発揮する技術ですよね。

（石村）〝トレーサビリティ（追跡管理、履歴管理）〟とか、英語でいえば格好がいいのですが、言い方を換えれば、〝監視のための技術〟です（笑い）。

（中村）ユビキタス（なんでもコンピュータ）社会とは、一歩間違えれば、監視社会の構築を意味することになるのですね。

（石村）まさに、この点が、今回の検討課題なわけです。

ＲＦＩＤ・無線ＩＣタグを使う場合、無線局の申請は要らないの？

原則として無線局の申請が要らないように、２００２（平成１４）年9月に、１３．５６MHz帯のＲＦＩＤ・無線ＩＣタグに関する法規制のやり方が変更されました。

改正前まで、ＲＦＩＤ・無線ＩＣタグは「無線設備」として規制されていました。このため、空中線電力が１０mWを超える機器を利用する場合には、構内無線局あるいは簡易無線局の免許が必要でした。（ただし、１０mW以下の機器の場合には、混信防止機能を備え、技術基準適合証明を受けたものは無線局の免許は必要ありませんでした。）

２００２年の法改正以降、ＲＦＩＤは「高周波利用設備」として規制されることになりました。高周波利用設備も総務大臣の許可が必要ですが、つぎの①か②に当てはまるＲＦＩＤ・無線ＩＣタグの場合には許可は要りません。ですから、いずれかの条件を満たす場合には、ＲＦＩＤ・無線ＩＣタグを購入・利用する側は、自由に設備を設置することができます。

① 設備から3mの距離における電界強度が毎メートル５００マイクロボルト以下のもの

② 一定の技術的要件を満たし総務大臣による型式の指定を受けたもの

通例、ＩＴ企業が販売するＲＦＩＤ・無線ＩＣタグは、上に述べた条件にマッチし、総務大臣による型式指定を受けています。ですから、購入・利用する側は、ほとんどの場合、無線局の申請は要らないということになります。２００２年の法改正は、実質的にＩＴ企業によるＲＦＩＤ・無線ＩＣタグの開発・販売を奨励するための政府規制緩和にあったといえます。

■　ＲＦＩＤ・無線ＩＣタグの光と影

（中村）確かに、繊維の洗い方の情報の入った無線ＩＣタグを衣服に付けて、最適な洗い方を自動選択する洗濯機でジャブジャブするのも夢ではなくなる・・・。こんな話を聞けば、ＩＣタグって便利、素敵と、主婦などは飛びついてくるかもしれませんね。

（石村）そうでしょうね。環境保全を狙いとした家電製品や車輌などの廃品管理にＩＣタグを装着しておけば、違法廃棄した者の追跡管理にも活用できます。

（中村）ＩＣタグ市場は、２０１０年には年間１０億個を越す需要が見込まれているとも聞きます。相当、期待されている先端技術なのでは？

（石村）ＩＴ業界にとってはそうでしょう。けれども、無線ＩＣタグには、いい話ばかりではありません。

（中村）〝影〟の部分があるということですか。

（石村）そうです。無線ＩＣタグが悪用されれば、情報を読み取ることのできる側の人や企業に消費者性向や嗜好などが容易に見透かされてしまう危険性があります。ほとんどの商品に無線ＩＣタグが付けられれば、「この人がつけている時計はＡ社製品、コートはＢ社製品、下着はＣ社製品」といったように。また、誰かが読取書込み機（リーダーライター）を持って街を歩けば、「この家のテレビはＤ社製、電子レンジはＦ社製、読んでいる本は、御用学者著『住基ネットは愛国者の味方』・・・」といったことも現実になりかねないわけです。

（中村）無線ＩＣタグで、〝電子のぞき社会〟の悪夢も現実のものになりかねないわけですね。

（石村）そうです。それに、リーダーライターを持った外部者が、勝手に情報の書換えを行う可能性も出てきます。

（中村）これでは、逆に、いまの家電とかの方が安全、ということにもなりかねませんね。

（石村）そうともいえます。それから、企業が従業員の制服に無線ＩＣタグが組み込まれた名札をつけさせれば、働きぶりを追跡・監視することが可能になります。また、スーパーマーケットでは、無線ＩＣタグが組み込まれた顧客カード、ポイントカードで、その顧客の店内での行動を追跡・監視することも可能になります。

●　米・加州では生徒の監視にＲＦＩＤ名札着装が社会問題に

（中村）要するに、ＲＦＩＤ・無線ＩＣタグが自由に闊歩するとすれば、容易に監視社会にツールに化けてしまうということですね。

（石村）そうです。事実、カリフォルニア州では、あるＩＴ企業が、今年1月１８日に、突然、地方のある小中学校で、生徒に、氏名・顔写真・学年などが書かれたＩＤカードとそのＩＤカードを入れるＲＦＩＤ・無線ＩＣタグがついたビニー

ルケースを首からぶらさげさせ、教室などのドアに設置されたリーダーで電波を受ける手法で生徒の行動を追跡、学内のコンピュータで監視するパイロットプログラムを実施したことが問題になりました。全米から集中的な批判を浴びましたが。

（中村）父母が求めたのではないのですか。

（石村）そうではないです。生徒管理の徹底を望む校区委員会とＲＦＩＤ技術の売込みに躍起なＩＴ企業がタイアップして実施したようです。同校の勇気ある父母の行動と主要な人権団体による中止を呼びかける運動で、やっとのことで、２月７日にやめさせました。〔この問題については、本号別稿（１３頁以降）を参照してください～編集部〕

（中村）わが国の場合、人権についてバランス感覚の希薄な学校管理者が多いのが現状です。ＩＴ企業が学校にこうした提案を持ち込めば、〝防犯第一〟とかいって進んで協力するのではないかと一抹の不安を感じますが。監視カメラで学校を囲んで「わが校はこれで安全」とか・・・そんな学校環境が普遍化してきていますから。

（石村）確かに、父母はもちろんのこと、教職員にも、漠然とした「プライバシー」感覚はあるのでしょう。しかし、具体的なケースに即して「プライバシー」をどう守るのかとなると、何もできないのが現実でしょうね。大学で労働法を教えている教員が、自分のところで労働組合をつくろうと教職員が言い出すと、一番先に逃げ出す・・・。本当は、そんな人物が労働法など教えてはいけないのでしょうけど、現実はこんなものです。

（中村）とは言っても、学校教育の現場で、明確なプライバシー保護政策がないまま、なし崩し的にこんな監視システムが導入されてしまっては、子どもの人格形成に与える影響が大きいと思いますが。

（石村）こうしたアメリカの動きを、わが国のＩＴ業界が黙って見過ごしているわけはありません。

（中村）当然、わが国のＩＴハイエナ企業は、鼻をくんくんさせている。

（石村）そうですね。実は、「見守りタグ」とのネーミングで、無線ＩＣタグを活用した新たな防犯対策システムの試行が、横浜市青葉区内の小学校で４月５日から始まりました。実験台とされたのは、横浜市立みたけ台小学校（同市青葉区）の児童約３００人。ＮＴＴデータが主体となり、青葉区の地域住民など官民一体でつくる「安心安全情報に関する協議会」が協力するというものです。

（中村）こうした児童監視システムは、児童の移動の自由とか、児童情報の外部提供など個人情報の保護の面など、〝人権〟論的に大きな問題をはらんでいるように見えますが・・・。

（石村）仰せのとおりです。このシステムがはらむプライバシー侵害的な側面についての評価がまったく行われないまま事が進展していることは大きな問題だと思います。〔この問題については、本号別稿（１３頁以降）を参照してください～編集部〕

（中村）この実験が成功すると、自宅の子ども部屋の監視にも最適とか、とんでもない父母も出てきかねません。そして、回りまわって、いずれは、これら児童の父母が働く職場にも「働きぶり見守りタグ」とか称して、労務管理の手段として跳ね返ってくるのは必至でしょう。

（石村）仰せのとおりです。監視カメラによる職場の労務管理に続く、無線ＩＣタグによる職場の労務管理と、・・・職場の電子監視が進む一方です。

（中村）連合とか、民主党とか、こうした問題に対するアクション・プランを考える必要があるのでしょうけど。

（石村）ほとんどの連中は、組合サラリーマン、国会サラリーマン集団です。でも、組合費の天引き徴収（チェックオフ）で持続可能、パーティ券を売り付けだけは躍起。ふつうの市民が選挙に行きたくなくなるのも分かります。

（中村）名札ＩＣタグによる児童の監視問題に対する市民運動団体による早急な取り組みが求められていますね。

● 国連の生体認証式＋ＲＦＩＤパスポート計画

（石村）話は変わりますが、国連（ＵＮ）の国際民間航空機関（ＩＣＡＯ）が、すべてのパスポートに、指紋とか目の虹彩といった生体認証情報（バイオメトリクス）とＲＦＩＤ・無線ＩＣタグの装着をする計画を進めています。

（中村）国際テロ対策ですか？

（石村）主眼はそうでしょうけども。欧米の主な人権団体は、ＩＣＡＯの計画は、センシティブな個人情報の超国家的な共有にもつながり問題だ、と計画の中止を求めています。

（中村）それに、パスポートに組み込まれたＲＦＩＤ・無線ＩＣタグで、外国人の移動の自由を制限・監視するのも狙いなのでしょうけど。

（石村）今年はじめにアメリカに行きましたが、出入国管理がすさまじい。入国時に両手の人差し指の指紋と顔写真を、無差別にとるわけです。

（中村）ノーというと、入国させないわけですか。
（石村）そうです。それに、荷物検査もひどいのです。機内に持ち込めず預けるカバンのカギはかけるな。かけていて不審と思われる場合には、検査官にはカギを壊す権限があるというのです。
（中村）実際に壊しているのですか。
（石村）ケースによっては、そうでしょう。ただ、ホテルでＴＶをみていたら、荷物検査現場での問題が多く、盗難が多発、預ける旅行カバンには貴重品を入れないように、との広報が流れているのです。
（中村）驚きますね。
（石村）それ以上に、機内持込荷物の検査や身体検査のやり方がひどいんです。靴を脱げ、金属製の装着品をはずせ、はまだ分かります。問題は身体検査や手荷物検査です。適当に現場の検査官がターゲットを選んでやっているんです。
（中村）ターゲットにされたら大変（笑い）。
（石村）そうなんです。徹底的にチェックします。隣で検査を受けていた日本女性の場合、金属探知機で下着かなんかの留め金が引っかかったようで、女の係官が、手を入れて確認しているといった具合です。その女性は今にも泣き出しそうでしたが・・・。
（中村）黙ってみていたのですか？
（石村）どうやって助けるのですか。まあ、余りにも自分の荷物をひっくりかえすものだから、「どうやってターゲットを選んでいるんだ？搭乗まで時間があるときか、法的根拠はあるのか・・・」と質問してみましたが。
（中村）答えはあったのですか？
（石村）「おまえはロイヤー（法律家）か？誰をチェックするかは我々のデスクレション（自由裁量）だ・・・」とか言っていましたが。
（中村）要するに、どこの国でも、とくに外国人には人権が制限されるのでしょうけど。今でも、こうした実情ですからね。国連機関（ＩＣＯＡ）が提案した生体認証情報（バイオメトリクス）＋ＲＦＩＤ・無線ＩＣタグを装着したパスポート計画は問題ですね。
（石村）〝次世代バーコード〟とも言われるのがＲＦＩＤ・無線ＩＣタグです。この計画が現実のものになるとすれば、それこそ、外国人は〝人間バーコード〟を付けて出歩く時代になりかねません。
（中村）〝外国人を見たら犯罪者と疑え！〟といった社会でいいのかが問われていますね。

●　米・運輸保安局がＲＦＩＤ搭乗券導入を提案

（石村）アメリカでは、連邦運輸保安局（ＴＳＡ）は、ＲＦＩＤ・無線ＩＣタグを組み込んだ搭乗券の導入を検討しています。
（中村）何が狙いなのでしょうか？
（石村）当局は、乗客は「登録渡航者」プログラムに適格者として認定され、ＲＦＩＤ・無線ＩＣタグ入りの搭乗券を持っていれば、「特別レーン」ですばやく搭乗手続きができる仕組みだと説明していますが・・・。
（中村）頻繁にフライトを利用する人には便利なような気もしますが。「登録渡航者」になるには、詳細な個人情報を当局に提供し、認定を受ける必要があるのでしょうけど・・・。
（石村）現在のところ、詳細は分かりません。ただ、アメリカ連邦航空局（ＦＡＡ）は、「アフリカの安全な空港計画（Safe Skies for Africa Initiative）」と名づけて、はじめにアンゴラ、タンザニア、ジンバヴエなどアフリカ諸国をターゲットにこのプログラムを開始する腹積もりのようです。
（中村）ということは、赤信号の他国の空港からの搭乗客が対象なのですか。
（石村）ですから、このプログラムの本当の狙いは、空港内での搭乗客の居場所の追跡・監視が狙いなのでしょう。欧米の主要な人権団体は、搭乗券に組み込んだＲＦＩＤ・無線ＩＣタグを使った、乗客の選別・追跡・監視プログラムは、人権侵害であると厳しく批判していますが。
（中村）今の時点では、このプログラムは、ＶＩＰを選抜する仕組みなのか、あるいはＰＯＷ（戦犯）を監視する仕組みなのか定かではないということですね。
（石村）あるいは、双方を包括するプログラムなのかも知れません。

■　問われるＲＦＩＤ技術を売る側と買う側の社会的責任

（中村）ＲＦＩＤ・無線ＩＣタグは、本当にいろいろな用途があるのですね。
（石村）これは、裏返せば、ＩＴ企業にとってはＲＦＩＤ・無線ＩＣタグの販路が極めて広いということでもあります。
（中村）企業の存亡をかけて売り込みに必死になるのも分かります。

（石村）ＩＴ企業が、無線ＩＣタグを商品の在庫管理や盗難防止に活用したり、生徒の行動監視に売り込むのは、それこそ〝営業の自由〟でしょう。ですが、消費者が買った後もその商品にタグがついていてはプライバシー保護の観点から大きな問題です。また、小学生を商品のように取り扱い、無線電子タグをくくりつけ電子的に追っかけたり、個別に本人や保護者のインフォームドコンセント（十分に説明をした上で同意）を得ることなしに一律に監視対象にすることも問題です。

（中村）まさにＩＴ企業による営業の自由の〝乱用〟と見ていいですね。

（石村）商品を売るためには手段を選ばずでは、企業倫理が問われてきます。ＲＦＩＤ・無線ＩＣタグを売るＩＴ企業は、プライバシーなど人権を尊重した上でビジネスを展開する社会的責任（ＣＳＲ）を負っているといえます。

（中村）それから、こうした技術を買って、利用する側の倫理も問われてきますね。

（石村）見方によっては、ＲＦＩＤ・無線ＩＣタグを購入し、これを利用して個人情報を取扱う側（事業者や学校関係者など）の社会的責任の方が重いといえます。システムやプログラムの影響評価もろくにせず、「人権」がすっぽり抜けてしまっているのですから・・・。

（中村）この４月から、個人情報保護法も全面実施になりました。こうした法環境では、とりわけ個人取扱事業者にあてはまるものは、プライバシーないしは個人情報をないがしろにする形で、ＲＦＩＤ・無線ＩＣタグを使ってはいけないでしょう。しっかりしたルールがないといけませんね。

■　わが国は、ＲＦＩＤ関連プライバシーをガイドラインで保護する政策を選択

（石村）わが国政府は、無線ＩＣタグの利用規制について、法律ではなく、ガイドラインで対応する公共政策を選択しました。総務省と経済産業省と共同で策定し、２００４年6月８日に公表した「電子タグに関するプライバシー保護ガイドライン」〔本稿末尾の別表（１１頁以降）を参照してください～編集部〕がそれです。

（中村）役所は、早々とガイドラインをつくっているのですね。

（石村）欧米におけるＲＦＩＤ・無線ＩＣタグをめぐるプライバシー論議を察知して早めの対応をしたのでしょう。このガイドラインがつくられるよりも先の２００３年４月に、産業経済省は「商品トレーサビリティの向上に関する研究会中間報告」と出しています。

（中村）この報告の内容は？

（石村）ＲＦＩＤ・無線ＩＣタグの有用性を認め、これを安い価格で供給できるようにし、個人情報を活用して、商品のトレーサビリティ（追跡管理、履歴管理）や効率的な在庫管理を推進しようといった骨子のものです。

（中村）イケイケドンドンが、今度は、ガイドラインで、一転、プライバシーが大事というわけですか。

（石村）個人情報保護法も全面施行されましたし、無線ＩＣをやりたい放題にしておけませんからね。

（中村）ということは、ガイドラインは、企業などがＲＦＩＤ・無線ＩＣタグを利用して商品や個人情報を管理する際に、消費者のプライバシーが侵害されないようにするのが目的で策定したものですね。

（石村）そうです。個人情報保護法をベースに、ＲＦＩＤ・無線ＩＣタグ技術を使う事業者のルールを定めたものです。とくに、このガイドラインは「消費者に物品が手交された後も当該物品に電子タグを装着しておく場合に、当該電子タグ及び当該電子タグが装着された物品を取り扱う事業者が対応することが望ましい規則について定めたもの」です。

（中村）ということは、先ほど触れた横浜市の小学校での「見守りタグ」といいましたか？ともかく、児童の行動監視にＩＣタグを使うケースに、このガイドラインは、うまく当てはまらないような気がしますね。

（石村）「見守りタグ」は、基本的に、ガイドラインにいう「消費者に物品が手交された後も当該物品に電子タグを装着しておく場合に」該当すると思います。

（中村）ただ、児童の行動監視目的での無線ＩＣタグの利用については、これを社会的に認知するということでコンセンサスが得られたとしても、最低でも、こうした目的での利用規制をするためのガイドラインが必要だと思います。

●　ガイドラインの骨子

（石村）両省（総務省と経済産業省）がまとめたガイドラインの内容は、つぎの１０項目です。

① 電子タグ（無線ＩＣタグ）の有用性と消費者のプライバシーとのバランスの確保
② このガイドラインの適用範囲～事業者がＩＣタグがついたまま商品を消費者に渡した場合に事業者に求められる対応
③ 電子タグが装着されていることの表示など
④ 電子タグの読み取りに関する消費者の最終的な選択権の留保
⑤ 電子タグの社会的利益などに関する情報提供
⑥ 電子計算機に保存した個人情報データベースと電子タグの情報を連係して使う場合の取扱
⑦ 電子タグ内に個人情報を記録する場合における情報収集および利用の制限
⑧ 電子タグ内に個人情報を記録する場合における情報の正確性の確保
⑨ 情報管理者の設置
⑩ 消費者に対する説明および情報提供

● ガイドラインの解説

（中村）このガイドラインの対象となるのは、電子タグ（無線ＩＣタグ）事業者および商品を扱う事業者ですね。しかも、電子タグ付きの商品が消費者に手渡された後も、電子タグを外さないケースに限定したものですよね。

（石村）そうです。これは、無線ＩＣ（電子）タグは、将来的にリサイクル等の目的で、購入後も商品に付けておくことが想定されています。しかし、電子タグの情報は遠隔から読み取れる性質を持つため、消費者が望まない形で、所持する商品の属性などの情報が読み取られるおそれがあることを考慮したものです。

（中村）少し、このガイドラインについて、教えてください。まず、③「電子タグが装着されていることの表示など」では、具体的にどういったルールを定めているのですか？

（石村）事業者はまず、消費者に対して電子タグが装着されていること、装着場所、性質、記録されている情報の内容を表示しなければならない、とのルールを定めています。

（中村）④「電子タグの読み取りに関する消費者の最終的な選択権の留保」とは、具体的にはどういったことをさしているのですか。

（石村）そうですね。消費者が電子タグの読み取りをできないようにしたいと望むとします。その場合には、電子タグの読み取りができないようにする方法を消費者に提示する必要があるとしていますね。

（中村）具体的な方法を挙げているのですか？

（石村）挙げています。（ａ）「アルミ箔で覆って読み取り機との通信を遮断する」方法、（ｂ）「電子タグ内の情報を電磁的に消去する」方法、そして、（ｃ）「電子タグ自体を取り外す」方法を挙げています。

（中村）⑤「電子タグの社会的利益などに関する情報提供」とは、どういった状況を想定しているのですか。

（石村）事業者が④に従い消費者の求めに応じて無線ＩＣタグを読み取れなくしたとします。この場合であっても、もし消費者利益や社会的利益が損なわれることがあるなら、その情報を提供するように事業者に義務付けています。自動車の修理履歴とか、環境保全目的でのリサイクル履歴などを想定しています。

（中村）⑥「電子計算機に保存した個人情報データベースと電子タグの情報を連係して使う場合の取扱」とは、どういったケースを想定しているのでしょうか。

（石村）電子タグを扱う事業者が、電子タグ本体には個人情報を記録していない場合でも、コンピュータの個人情報データベース等と電子タグ情報を連係して用いている場合には、その情報は個人情報保護法の適用を受けることを確認したものです。

（中村）⑦「電子タグ内に個人情報を記録する場合における情報収集および利用の制限」では、どういったことを事業者に求めているのでしょうか。

（石村）事業者がＩＣタグ内に個人情報を記録しているとします。この場合、その事業者は、取り扱う個人情報の件数にかかわらず、その情報の利用に際して、利用目的を本人に通知あるいは公表するようにすべきだとしています。本来の目的以外にその個人情報を使う場合にも、本人の同意を得るようにすべきだとしています。

（中村）⑧や⑨は、タイトルを読んでのとおりだと思いますが。

（石村）⑧や⑨では、仰せのとおりです。事業者は、ガイドラインの基本的考え方に沿った上で、さらに事業実態に応じた消費者との関係を踏まえ、電子タグの取扱について適切な対応を取ることが望まれています。また電子タグのプライバシー保護に関する責任者を定め、連絡先を教える必要があります。

（中村）⑩「消費者に対する説明および情報提供」では、消費者保護のために、どういったことに努めるべきだとしているのでしょうか？
（石村）⑩では、事業者、事業者団体や政府機関などは、電子タグの利用目的、性質、メリット・デメリット等に関して、消費者の理解に務める必要があるとしています。

●　〝害〟ドラインではないのか？

（中村）このガイドラインでは、すべて「努める」との表現です。努力規定だけで、「しなければならない」といった義務規定はありませんね。
（石村）そうです。しかも、このガイドラインの①目的では、「電子タグの有用性を利活用しつつ、消費者の利益を確保し、電子タグが円滑に社会に受け入れられるようにするために、電子タグに関する消費者のプライバシー保護について業種間で共通する基本的な事項を明らかにすること」を挙げています。
（中村）余りにも、ＩＴ業界寄りのガイドラインではないかと思いますが。
（石村）仰せのとおりです。個人情報保護法が全面実施されたから、無線ＩＣタグで監視の対象とされることになる消費者（被監視者）のプライバシーも考えておこう、といった姿勢がありありですね。
（中村）それこそ、消費者にとっては、〝害〟ドラインにも見えてきますね（笑い）。
（石村）まあ、この害ドラインの〝まえがき〟では、このガイドラインは、諸環境の変化にともない見直しをはかる。また、関係者の間で新たなコンセンサスが得られた場合は修正する、旨の公約をしています。
（中村）ということは、実害が出れば、それに応じて、見直されるということですね。アメリカの諸州でのＲＦＩＤ・無線ＩＣタグ規制立法のように、ＩＣタグを使った個人情報の取り扱いの「原則禁止」をはっきりと打ち出した上で、「例外的・限定的」にその利用を認めるという立法政策は、わが国では難しいのでしょうか。
（石村）アメリカでも、ＩＴ業界の強い抵抗で、いまだ法案成立のメドがたっていない状況です。なかなか、企業献金など政治とカネの兼ね合い、すんなり「消費者が主役」になれないのが現実のようです。
（中村）わが国の場合、これに、役人の天下りなど行政と企業との悪しき関係も「消費者が主役」の法律ないしはガイドラインができない重い要因になっているのでしょうけど・・・。
（石村）視点をかえてみれば、どう「営業の自由」と「人権」のバランスをとるべきかの問題でしょうけど。
（中村）こうした対応は、政治主導か、役所主導かにかかわらず、〝哲学〟がしっかりしていないとダメだということでしょう。

●　ガイドラインのポイント

（石村）もう一度、わが国のガイドラインを個人情報保護の視点から整理して、ポイントを挙げてみると、つぎのとおりです。

〔図２〕「電子タグに関するプライバシー保護ガイドライン」のポイント

・無線ＩＣタグ・ＲＦＩＤに個人情報が記録されている場合、その件数にかかわらず、個人情報保護法が適用になる。事業者は情報の利用目的を特定した上で情報を最新の状態に保ち、漏えい、改ざんの防止に努めなければならない。

・タグ自体に個人情報が保存されていない場合でも、タグの情報とデータベースの情報を照合することで個人が特定できるときには、個人情報保護法が適用される。

・商品が消費者の手に渡った後もタグをつけたままにしておく場合、タグの装着場所や、タグ内の情報について表示するか、あらかじめ説明をするようにしなければならない。

・消費者が個々の判断でタグを読み取りを不能にできるよう、その方法も説明するか、表示しなければならない。タグの読み取りを不能にすることによって、商品の修理の履歴が分からなくなるとか、リサイクルしにくくなるなどといった不利益が出る可能性がある場合は、表示などでその情報を提供するように努めなければならない。

・また、各事業者は、タグに関するプライバシー保護の責任を持つ情報管理者を設置し、連絡先を公表しなければならない。

（中村）ガイドラインによるこの程度のルールで、ＲＦＩＤ・無線ＩＣタグ技術のターゲットとされる個人のプライバシーないしは個人情報を十分に保護できるのでしょうか。

（石村）「無いよりは益し」なのか、そうではなくて、特別法を制定してもっと厳格にプライバシーを保障すべきなのかは、諸外国の対応などを点検した上で考える必要があろうかと思います。

■　米・諸州では、ＲＦＩＤ関連プライバシーを法律で保護する方向

（石村）すでに触れたように、アメリカ諸州では、法律による規制に向かっています。カリフォルニア、バージニア、マサチュセッツ、メリーランド、ニューメキシコ、ユタなどでは、消費者のプライバシーを守るための立法の実現に向けた動きを加速しています。〔ＣＮＮニューズ本号では、カリフォルニア州の法案の紹介を含め、同州での立法の現状を紹介しています（２２頁以降）～編集部〕

（中村）アメリカとわが国との違いを挙げるとすれば、どういった点なのでしょうか？

（石村）アメリカの場合には、ＲＦＩＤ関連プライバシー問題については、政治（議会）と市民団体が中心になって検討をしています。一方、わが国の場合には、行政と企業、それに御用学者・識者が中心になって検討しています。

（中村）つまり、消費者や政治は、舞台には上がっていないという状況なわけですね。

（石村）そうです。それに、政策提言（アドボカシー）専門のＮＧＯのだらしなさも目立ちます。

（中村）PIJも含めて、ということですね（笑い）。

（石村）そうですが、ある意味では、中村副編集長の手腕にもかかっていることです（笑い）。

（中村）石村代表、今回は、わが国でのＲＦＩＤ・無線ＩＣタグをめぐるプライバシー保護の課題について、分かりやすく説明してくださり、ありがとうございました。

〔別表〕総務省・経済産業省「電子タグに関するプライバシー保護ガイドライン」

第１（ガイドラインの目的）

本ガイドラインは、電子タグの有用性を利活用しつつ、消費者の利益を確保し、電子タグが円滑に社会に受け入れられるようにするため、電子タグに関する消費者のプライバシー保護について業種間に共通する基本的事項を明らかにすることを目的とする。

第２（ガイドラインの対象範囲）

本ガイドラインは、消費者に物品が手交された後も当該物品に電子タグを装着しておく場合に、当該電子タグ及び当該電子タグが装着された物品を取り扱う事業者が対応することが望ましい規制について定めるものである。

第３（電子タグが装着されていることの表示等）

消費者に物品が手交された後も当該物品に電子タグを装着しておく場合には、事業者は、消費者に対して、当該物品に電子タグが装着されている事実、装着箇所、その性質及び当該電子タグに記録されている情報（以下「電子タグ情報」という。）についてあらかじめ説明し、若しくは提示し、又はその包装上に表示を行う必要がある。当該説明又は掲示は、店舗において行うなど消費者が認識できるように努める必要がある。

第４（電子タグの読み取りに関する消費者の最終的な選択権の留保）

事業者は、消費者に物品が手交された後も当該物品に電子タグを装着しておく場合において、消費者が、当該電子タグの性質を理解した上で、当該電子タグの読み取りをできないようにすることを望むときは、消費者の選択により当該電子タグの読み取りができないようにすることを可能にするため、その方法についてあらかじめ説明し、若しくは提示し、又は当該物品若しくはその包装の上に当該方法について表示を行う必要がある。

【電子タグの読み取りができないようにする方法の例】

１．アルミ箔で覆って遮断できる場合はアルミ箔で覆うなど電子タグと読取機との通信を遮断する。

２．電子タグ内の固有番号を含む全部若しくは消費者が選択する一部の情報を電磁的に消去し、又は当該情報を読み取ることを不可能にする。

３．電子タグ自体を取り外す。

第５（電子タグの社会的利益等に関する情報提供）
　事業者は、第４に基づき消費者が電子タグの読み取りをできないようにした場合であって、物品のリサイクルに必要な情報が失われることにより環境保全上の問題が生じ、又は自動車の修理履歴の情報が失われることにより安全への影響が生じる等、消費者利益又は社会的利益が損なわれる場合には、これらの利益が損なわれることについて表示その他の方法により消費者に対して情報を提供するように努める必要がある。
第６（電子計算機に保存された個人情報データベース等と電子タグの情報を連係して用いる場合における取扱い）
　事業者が、電子タグに記録された情報のみでは特定の個人を識別できない場合においても、電子計算機に保存された個人情報データベース等と電子タグに記録された情報を容易に連係して用いることができるときであって、特定個人を識別できるときにあっては、当該電子タグに記録された情報は個人情報保護法上の個人情報としての取扱いを受けることとなる。

　※個人情報保護法上個人情報取扱事業者に係る義務（例示）
（１）個人情報の利用目的関係
　・　利用目的をできる限り特定
　・　利用目的以外の利用は本人の同意が必要
（２）個人情報の取得関係
　・　個人情報の不正な取得の禁止
　・　個人情報を取得した場合は、速やかに利用目的を本人に通知または公表
（３）個人データの管理関係
　・　個人データを正確かつ最新の内容に保つように努める
　・　個人データの漏えい、滅失、き損等の防止のため安全管理措置が必要
　・　個人データを第三者へ提供する場合は、本人の同意が必要

第７（電子タグ内に個人情報を記録する場合における情報収集及び利用の制限）
　電子タグ内に個人情報を記録して取り扱う事業者は、当該事業者が取り扱う個人情報の件数にかかわらず、個人情報を収集又は利用する場合は、当該電子タグ内に記録された個人情報に関して、利用目的を本人に通知し、又は公表するように努める必要がある。また、当該情報を利用目的以外に利用する場合には、消費者本人の同意を得るように努める必要がある。
第８（電子タグ内に個人情報を記録する場合における情報の正確性の確保）
　電子タグ内に個人情報を記録して取り扱う事業者は、当該事業者が取り扱う個人情報の件数にかかわらず、個人情報を記録する場合は、当該電子タグ内に記録された個人情報に関して、次の事項を満たすよう努める必要がある。
１　電子タグ内に記録された個人情報を使用する目的と内容に照らし合わせて、正確かつ最新の内容に保つこと。
２　消費者の求めに応じて、当該消費者に関係する電子タグ内に記録された情報及び電子タグの識別情報からひも付けされる当該消費者の個人情報を開示し、また当該消費者の求めに応じてこれらの情報の間違いを訂正すること。
３　電子タグ内に記録された情報の滅失、き損、改ざん及び漏えいを防止すること。
第９（情報管理者の設置）
　事業者は、電子タグに関するプライバシー保護に係る情報の適正な管理及び苦情の適切かつ迅速な処理を保護するため、これらに責任を有する情報管理者を設置し、連絡先を公表する必要がある。
第１０（消費者に対する説明及び情報提供）
　当事者、事業団体及び政府機関等の関係機関は、電子タグの利用目的、性質、そのメリット・デメリット等に関して、消費者が正しい知識を持ち、自ら電子タグの取扱いについて意思決定ができるよう、情報提供を行う等、消費者の電子タグに対する理解を助けるよう努める必要がある。

住基ネット、監視カメラに次ぐ、危険な「ＩＣタグ」監視に反対しよう

横浜市の小学校で、４月から、ＮＴＴデータが、ＩＣタグで児童の登下校監視システム実験を開始

― アメリカ・カリフォルニア州では、児童へのＩＣタグ監視システム実験に父母が抗議、中止に

《対論》

石村耕治（白鴎大学教授・PIJ代表）
辻村祥造（税理士・PIJ副代表）

横浜市立みたけ台小学校（同市青葉区）の児童約３００人を実験台に使い、この４月から、ＮＴＴデータが、青葉区の地域住民など官民一体でつくる「安心安全情報に関する協議会」が協力を得て、ＩＣタグを使った児童の登下校の安全管理システムの実験が始まった。児童約３００人が「見守りタグ」を携帯し、通学区内（約１平方キロメートル）の３０ヵ所に受信機アンテナ「見守りスポット」を設置。児童がアンテナ近辺を歩くと、タグから自動的に電波が発信され、これを「見守りスポット」が受信。この情報が父母らの携帯電話やパソコンに電子メールで瞬時に送られ、児童の居場所や登下校状況などが確認できるというもの。

タグには通報ボタンが付いていて、児童が通学路で、犯罪や、事件などに巻き込まれた場合、ボタンを押せば、父母や警備会社だけではなく、近隣に住む協力者にも異常が知らされる仕組み。被害児童の名前や連絡先、発生時刻、場所などの情報が即時にパソコンや携帯電話などにメールが届き、地域住民がいち早く現場に駆けつけて児童を確認、警備員や警察の到着を待つという仕組み。

こうした児童監視システムは、児童の移動の自由、児童情報の外部提供や個人情報の保護の面など、〝人権〟論的に大きな問題をはらんでいる。このシステムがはらむプライバシー侵害的な側面についての評価がまったく行われないまま事が進展していることは大きな問題だ。

一方、アメリカ・カリフォルニア州では、ＩＴ企業が、今年１月に、ある小中学校で、７年生・８年生をサンプルに、自動出席確認プログラムを実施したことが問題になった。このプログラムは、生徒に、個人番号・氏名・顔写真・学校名・学年などの情報の詰まったＩＤカードを、ＲＦＩＤ（無線ＩＣタグ）がついたビニール製のケースに入れ、首から吊り紐でぶらさげさせ、タグから発信される電波を基に中央のコンピュータで行動を監視するもの。生徒管理の徹底を望む教育委員会とＲＦＩＤ技術の売込みに躍起なＩＴ企業がタイアップして実施した。主要な人権団体が中止を呼びかける運動を展開し、2月７日に実験を中止させた。

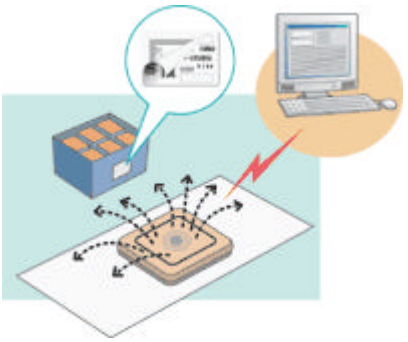
横浜市の実験をこのまま放置しておいてよいのであろうか。アメリカ・カルフォルニア州での反対運動の実情を紹介しながら、わが国での問題の所在を探りたい。石村耕治PIJ代表に、辻村祥造PIJ副代表が聞いた。

（CNNニューズ編集部）

● 横浜市では、すでにＩＣタグで登下校児童の安全管理システム実験を開始

（辻村）「見守りタグ」とのネーミングで、無線ＩＣタグを活用した新たな防犯対策システムの試行が、横浜市青葉区内の小学校で４月５日から始まりました。この実験には、「安全管理」をモットーにしてはいるものの、いろいろな問題が隠されていると思います。カリフォルニア州でも同じような実験が開始されたものの、プライバシー保護団体による反対運動で、中止に追い込まれたとのことでした。で、今回は、初めに横浜市の小学校での実験についてお話いただき、その後で、この実験がはらんでいる問題点を浮かび上がらせるためにも、カリフォルニア州でのＩＣタグ名札（バッジ）実験の頓挫の経緯を紹介していただき

たいと思います。
（石村）了解しました。まず、横浜市でのＩＣタグ実験を活用した児童監視システム実験についてですが、これは、まったく無風の中で開始されています。父母や市民団体などからは、ほとんど異論がなかったようです。
（辻村）政策提言団体である私どもPIJが、今、無線ＩＣタグの問題に取り組み出したところです。ちまたの市民運動団体は、まだ、住基ネット廃絶や監視カメラ反対などで精一杯、ＩＣタグについての事の重大さに気づいていないと思います。
（辻村）横浜市の実験では、監視システムはどういった仕組みになっているのでしょうか。
（石村）やさしくいえば、通学区内にアンテナ（リーダーライター）を設置して、ＩＣタグをつけた児童がそこを通過すると、アンテナから出る電波で位置を確認し、父母らの携帯電話やパソコンにメールで連絡して瞬時に居場所が把握できる仕組みです。また不測の事態には「通報ボタン」を押すと、近くの住民が駆けつける仕組みになっているようです。ＩＴ（情報技術）を活用した〝次世代のお守り〟で、安全で安心できる街づくりに必須のアイテムとのふれこみも。
（辻村）でも、よく考えると、児童が電波の届かない通学区外に連れ去られるかも知れないではないですか。日本国中にアンテナを設置するつもりなのですかね。余り役立たないシステムのような感じもしますが・・・。もう少し、「見守りタグ」システムについて、詳しく話してください。
（石村）電子名札といえる「見守りタグ」はＮＴＴデータ（東京都江東区）が開発したものです。手のひらサイズの小型装置（縦６センチ、横３．１センチ、重さ２０グラム）に、この無線ＩＣタグが埋め込まれています。
（辻村）それから、システム試行についても、もう少し詳しく・・・。
（石村）実験台とされたのは、横浜市立みたけ台小学校（同市青葉区）の児童約３００人。ＮＴＴデータが主体となり、青葉区の地域住民など官民一体でつくる「安心安全情報に関する協議会」が協力するというものです。
　児童３００人が「見守りタグ」を携帯し、通学区内（約１平方キロメートル）の３０ヵ所に受信機アンテナ「見守りスポット」を設置。児童がアンテナ近辺を歩くと、タグから自動的に電波が発信され、これを「見守りスポット」が受信。この情報が父母らの携帯電話やパソコンに電子メールで瞬時に送られ、児童の居場所や登下校状況などが確認できるというものです。
　タグには通報ボタンが付いていて、児童が通学路で、犯罪とか、事件に巻き込まれた場合、ボタンを押せば、父母や警備会社だけではなく、近隣に住む協力者にも異常が知らされる仕組みになっています。被害児童の名前や連絡先、発生時刻、場所などの情報が即時にパソコンや携帯電話などにメールで届き、地域住民がいち早く現場に駆けつけて児童を確認、警備員や警察の到着を待つという仕組みです。



●　児童監視システムで問われる人権感覚

（辻村）こうした児童監視システムは、児童の移動の自由とか、児童情報の外部提供など個人情報の保護の面など、〝人権〟論的に大きな問題をはらんでいるように見えますが・・・。
（石村）仰せのとおりです。このシステムがはらむプライバシー侵害的な側面についての評価がまったく行われないまま人体実験が行われていることは大きな問題だと思います。この問題は、〝人格権〟の視点が議論されないまま、追跡管理の視点だけが先行し、児童を家畜並みに取り扱うことにつながりかねないわけですから。
（辻村）それに、この実験が成功すると、回りまわって、いずれは、これら児童の父母が働く職場にも「働きぶり見守りタグ」とかのネーミングで、労務管理の手段としてＩＴハイエナは企業に売り込みをはかるに決まっていますからね。
（石村）「働きぶり見守りタグ」とか名づけても、システムの内実は、「社畜監視システム」ですよね。
（辻村）ですから、教師は勇気を持ってもっと発言しないといけませんね。児童のプライバシーをもてあそぶのは危険です。
（石村）それに自分自身を窮地に追い込みかねません。これら学校の教職員の行動監視にも「見守りタグ」を使えと、父母が言い出しかねないわけです。
（辻村）教職員の「倫理面での電子監視」も兼ねてですか。

（石村）そうですね。ＩＣ（ＲＦＩＤ）タグ監視国家にまっしぐらの感じがします。
（辻村）１９９９〔平成１１〕年に1,０４２件だった学校不法侵入や登下校時の事件件数は、２００２年には2,１６８件と、３年で２倍近くに急増しています。地域住民が、児童の安全を守るために役立つといわれれば、余り深く考えないでＩＴハイエナの甘い言葉を鵜呑みにするのも分からないわけでもないですが・・・。
（石村）それが今のわが国での〝地域社会の常識〟といったことなのでしょうけど・・・。文部科学省学校健康教育課の大金伸光専門官は「児童をめぐる事件が多発するなか、地域の実態に応じた取り組みは重要」という認識を示したと報道されています。ＮＴＴデータでは、７月までの３ヵ月の試行後、問題点を検討した上で、商品化を目指す方針とのことです（同社公共事業ビジネス事業本部営業統括部）。
（辻村）でも、文科省のような役所がお墨付きを与えるのは、ちょっと待った！ですね。
（石村）仰せのとおりです。それに、現在ある総務省・経済産業省の「電子タグに関するプライバシー保護ガイドライン」（２００５年６月）は、〝商品〟のトレーサビリティ（追跡管理・履歴管理）に関するものです。〝人間〟のトレーサビリティに関するルールを定めたものではありません。ＩＣタグ名札による児童監視問題に対する市民運動団体による早急な対応が求められています。

● 山口でつくられるハイテク刑務所は「ＩＣタグ監獄」

（辻村）新聞で紹介されていましたが、今度、山口県美祢市に建設されることになっている塀や鉄格子のないハイテク刑務所は、強化ガラスや赤外線センサーに加え、ＩＣタグで受刑者の監視をすることになっているようです。
（石村）無線ＩＣタグで、常時、受刑者や職員の所在確認をするという発想です。
（辻村）現在、犬の場合、一部で、ＩＣタグの入った小さなカプセルを体内に埋め込むことで、トレーサビリティを高めるやり方がとられています。受刑者の場合は、ＩＣタグのついた腕輪とか、足輪をはめさせるのでしょうか？
（石村）そのうち、裁判所の許可があれば、ＩＣタグの体内埋め込みも強制できる時代に入るかもしれませんね。
（辻村）特に受刑者や性犯罪の犯歴がある者は、〝人権〟が制限されても仕方がない、という風潮にありますから。それこそ〝人体実験〟に適材と見られる可能性がありますね。
（石村）ともかく、横浜市の小学校で実験に入った「見守りタグ」の発想と山口の「ＩＣタグ監獄」の発想とは、本質的には同じですよね。
（辻村）〝商品〟の追跡監視ではなく、〝人間〟の追跡監視である点、こうしたシステムの実験については、もっと慎重に点検する必要があろうかと思います。
（石村）法律の専門家ですら、押し寄せる先端技術の波に飲み込まれ、人権感覚を麻痺させられています。しかし、まさに、〝ＩＴ（先端技術）〟優先ではなく、〝人格権〟優先の発想が求められています。
（辻村）ＮＴＴデータが仕掛けた「見守りタグ」システムも、新たな公共事業として、日本国中にアンテナを張り巡らして「ＩＣタグ収容所列島」化しようという発想が基になっているでしょう。
（石村）実際、そうしない限り、「見守りタグ」システムなど、欠陥商品と名指しされるのは目に見えています。決められた小さな地域でこのシステムを採用しても、カネ喰い虫、役立たず、です。

● 米・加州では仮想「電子監獄学校」実験が問題に

（辻村）ところで、カリフォルニア州での児童へのＲＦＩＤ（無線ＩＣタグ）名札の着装実験は始めたものの、すぐに頓挫したとのことですが。こうした経緯に至ったのも、無線ＩＣタグを使った〝人間〟の追跡監視が、人格権（プライバシー）侵害ではないかと問題になったからですね。
（石村）仰せのとおりです。それに、父母サイドからの「電子監獄学校」に対する嫌悪もありました。
（辻村）問題の経緯を話してください。
（石村）実験校となったのは、カリフォルニアの州都サクラメントの北東にあるシャター（Ｓｕｔｔｅｒ）という小さな町にある公立のブリタン小中学校（Brittan Elementary School）です。この学校で、今年の１月１８日から、インコム社（ＩｎＣｏｍ）というＩＴ企業が、ＲＦＩＤ（無線ＩＣタグ）を使った「インクラス（ＩｎＣｌａｓｓ）」と名づけられた自動出席確認システムの導入実験を始めました。
（辻村）それで、この「インクラス」システムは、どういった仕組みになっているのですか？
（石村）この仕組みでは、各生徒に、まず１５桁

の番号・氏名・顔写真・学校名、学年などの詰まったＩＤカード（名札）をビニールケースに入れ、吊り紐で首にぶらさげさせます。このビニール製のケースにはＲＦＩＤ（無線ＩＣタグ）が装着されていますから、各教室入口に設置されたアンテナ（リーダーライター）から出ている電波で無線ＩＣタグと交信し、学内にあるコンピュータに送られたデータで所在確認ができます。また、本人の出入り履歴を管理すれば、電子出席簿にできるわけです。

インクラス・システムで、児童が教室に出入りする際に、戸口に設置されたＲＦＩＤリーダーで本人確認、学内のコンピュータで情報管理

●　インクラス・プログラムへ父母が反発

（辻村）なるほど。原理は単純なのですね。で、このインクラス・プログラムへの批判があったというのですが、どういった理由からですか？

（石村）批判の出所は、大きく二つに分けられます。一つは、父母からの批判。そして、もう一つは、プライバシー保護団体からの批判です。

（辻村）父母からはどういった批判がでたのでしょうか。

（石村）この学校では、在校中は、全校生徒に番号・名前・写真などの入ったＩＤカードをビニールケースに入れて紐（ストライプ）で首からぶらさげるように強制しています。このうち、インクラス・プログラムでは、７年生と８年生１６０人のビニールケースにだけＲＦＩＤ（無線ＩＣタグ）が装着されたわけです。生徒は、ＩＤカードをぶらさげていなくとも、とがめられることはないようですが、積極的にイヤだといえる雰囲気ではなかったようです。

（辻村）で、生徒はともかく、父母は、どういった反応だったのでしょうか？

（石村）父母の多くは、インクラス・プログラムに反対ではなく、実験を開始した校長や教育委員長の判断を支持していたようです。しかし、インコム社には、一部の父母から正式な抗議文が寄せられました。ただ、これらの抗議は、ＲＦＩＤ（無線ＩＣタグ）の装着を問題にしたものではなかったようです。むしろ、氏名や写真が入ったＩＤカードは、生徒が学外に出てもそのまま装着してしまう可能性があり、不審者のターゲットとされることが危惧されるとの批判でした。それから、生徒は学外でも、ＲＦＩＤ（無線ＩＣタグ）で追跡管理されるのではないかとの指摘もあったようです。

（辻村）このインクラス・プログラムは、横浜市の「見守りタグ」とは違い、学外で機能する仕組みではなかったはずでしたよね。

（石村）仰せのとおりです。その父母の誤解です。それから、父母からは、１５桁のＩＤ番号での管理も、生徒に与える心理的な影響が大きいので止めるべきであるとの意見もありました。

（辻村）当初、田舎の一公立小中学校での、パイロット・プログラムで、余り厳しい批判もなかったのに、全米から集中砲火を浴びることになったのはなぜなのでしょうか？

（石村）実験開始から少したった１月３０日に、二人の生徒の父母が、アメリカ自由人権協会（ＵＣＬＡ）に対して、問題提起を行ったことが、直接の契機になりました。まあ、インコム社も、保守的な片田舎での実験だから、それほど強い批判は起きないだろう、と見ていたきらいがあります。

（辻村）ところが、ＵＣＬＡの呼びかけに呼応して、全米の主だったプライバシー保護団体が一斉に「ＩＣタグを使った子どもの電子監視」を問題にしだしたわけですね。

（石村）そうです。ＩＣタグを使って、子どもを「在庫商品」を管理するような扱いをしたり、子どもの行動を家畜やペットを管理すると同じ手法で監視するパイロット・プログラムを実施したことが大問題になりました。全米から集中的な批判を浴びました。

（辻村）これを契機に、無線ＩＣタグは、容易に監視社会にツールに化けてしまうということが分かってしまったことが大きな原因でしょうか？

（石村）それもあると思います。でも、やはり、実験校の父母の勇気が、このプログラムを中止に追い込む直接の契機になったといえます。

（辻村）その父母は、どういった批判をしたのですか？

（石村）その父母は、「子どもに無線ＩＣタグを

持つことを事実上強制し、学校に子どもを追跡する権限を認めることは、インフォームドコンセント（理由をよく説明し、本人の同意）を得た上での個人情報の収集が許されるとするプライバシー保護の基本原則に反する行為である」といった主旨の抗議を学校区委員会および校長あてに申し立てました。抗議文を仮訳すると、次のとおりです。

身分証明書カードおよび無線ＩＣタグ（ＲＦＩＤ）による生徒の追跡管理実験に対する抗議文〔仮訳〕

ブリタン・スクール２３４０　ペッパー通りサッター、カリフォルニア　９５９８２

２００５年1月３０日

この正式な抗議文は、ブリタン小中学校の校区委員会および教育長兼校長のアニー・グラハム氏あてのものです。校区委員会は、小中学の高学年生を対象に、その父母に説明をすることもなく、かつ、親権者の同意を得ることもなく、身分証明書（ＩＤ）カードおよび無線ＩＣタグ（ＲＦＩＤ）を使った追跡管理を強制的に実施しました。私たちは、次の点についての校区委員会の決定に対する抗議を行うために文書を提出します。

２００５年1月１３日に、私ども子どものいる家庭に、週刊広報誌が送付され、ブリタン小中学校の全生徒の安全確保を進めるために新規のＩＤ名札を導入する旨が通知されました。

２００５年1月１８日に、私どもの学年の子どもは、写真・氏名・学年を表示したＩＤカードをさげて帰宅しました。このＩＤカードは、横5．5インチ、縦４インチの大きさのビニールケースに入っており、首からつりさげられるようになっていました。カードの裏面には、約４インチ四方のなじみのない物体を密封した筒がありました。週刊広報誌には、その筒には何が入っているのか、それがどんな目的に使われるのか、何の説明もありませんでした。なじみのない物体が入った筒が本来の不安の原因ではあるものの、最もはっきりしている関心事は、生徒の氏名や学年などがよく見える名札を常時衣服の表面に装着するように義務付けていることです。

２００５年1月１９日に、私の妻と私は、ブリタン小中学校校長のアニー・グラハム氏に対しより詳しい説明を求め、私たちの関心事を伝えるために、集会を開くように求めました。開催された集会で、私たちは、こうした名札やその裏面にある筒に入れられたＩＣチップは、学校に所属しない人たちと見分けるのを容易にするためのものであるとの説明を受けました。私たちは、生徒の名前が表示されている事の重大さについて話しました。ブリタン小中学校の校内は一般に開放されています。これは、ほとんどの公立学校で一般的なことです。そこでは、生徒を送り迎えするために毎日、朝と午後にたくさんの人たちがおります。また、小学生の児童の多くは、自分の名札をつけたまま歩いて通学しています。児童は通学の途中でどこかに立ち寄ったりもしますから、児童に誰かが近寄ってくる可能性があります。この場合、その者は直ちにその児童の氏名や学年を知ることができますから、明らかに児童のプライバシー権を侵すことになります。不審者が特定の子どもないし家族を標的にしている場合、あるいは、子どもに危害を加える狙いで名札の情報を使おうとする場合、このＩＤカードはその企てを容易にするといえます。

また、私たちは、ＩＤカードの裏面の筒に入っている物体について質問をしました。それで、その筒には無線ＩＣチップが入っており、校内にいる生徒を追跡するパイロット・プログラムの一部として実験が行われている旨の説明を受けました。トイレを含む学校のドアというドアにはリーダー（読取機）が設置されており、それでもって生徒が出入りする度に記録をしている、との説明でした。ここで再び、私たちは、プライバシー問題、とくにトイレに入る子どもたちを追跡していること、に関心を持ちました。私たちは、グラハム氏に対し、その時の会合が校区で初めてであったことから、新しいプログラムの開始に際して父母会が開催されていないことについて、その理由を質しました。グラハム氏は、この新しいプログラムについては父母会が持たれなかったこと、そのわけは校区委員会の賛成があり、それが必要な手続のすべてであったためと回答しました。

２００５年１月２６日に、私たちの求めに応じて、ブリタン校区委員会の委員長のドン・ハグランド氏は、グラハム校長、ガルファロ副校長、フローリー・ターナー副校長およびバーミー・ディダリオ副校長、インコム社社長と共に集会に参加しました。ディダリオ氏は、私たちにＲＦＩＤ送信機の仕組みや、それがどのように出欠をとる際に教師を支援するのに使われるのか、さらには、新たに開発されたソフトを用いて学校がどのように出欠報告を作成できるのかについて、詳しく説明を求めました。私は、私の子どもの安全、プライバシーの侵害、さらには、子どもの部外秘情報へのアクセスについて関心を持っていることを訴えました。私は、グラハム氏に対し、今回はパイロット・プログラムであるものの、親権者のいかなる同意も得ないで実施されたこと、さらには、私たちの子どもにはこのプログラムに参加して欲しくないことを話しました。グラハム氏は、このプログラムへの参加は強制的なものであり、親権者の同意は要しないこと、したがって、私たちの子どもが参加しないとすれば「重大な問題を抱えることになります」と言われました。

私たちは、親権者として、自分らの道徳的信念と信仰に基いて、私たちの未成年の子どもにとり何が最良であるのかを決定する法的な権利を有しているとの確信を持っています。

ＩＤカードを装着するのは、民間の職場では一般的な慣行となっている一方で、カリフォルニアの公立学校制度の中で、生徒にＩＤカードの装着を義務付ける方針を採用している学校は他に例がないと見ています。雇用主が雇用の条件として従業員に名札の装着を義務付けることと、公立学校で小学生や中学生にこうしたことを義務付けることとは、まったく異なることです。この種のＩＤカードは、プライバシーの侵害であり、装着は厄介であり、しかも子どもにとっては危険です。校内では、ＩＤカードをひったくろうとしたり、他の子どもの首からＩＤカードを剥ぎ取る「タグ」と呼ばれるゲームが流行していることが、校区委員会で報告されました。また、生徒からの報告によると、吊り紐が切れて、コードでつないでいる例もあるようです。多くの親たちは、子どもがケガをするのではないかと心配をしています。私がグラハム氏の尋ねたところ、「些細な」ケガは想定の範囲内であり、新しい吊り紐も用意している、との回答でした。

それから、最後に、管理職の方々は、ＩＤカードを首からさげてドッジボールをされてみてはいかがでしょうか。

ＲＦＩＤ（無線ＩＣタグ）は、もはや新しい技術ではないものの、小売や製造業における優れた在庫管理の方法として急速に広まってきています。この技術で、即時の商品在庫管理が可能になり、かつ、小売業者は消費者の購買嗜好や出費癖の追跡ができると報告されています。今回の実験においても、プライバシー保護団体から、この技術がプライバシー侵害的である旨の注意が喚起されています。まさに、私は、カリフォルニアの公立学校で小学生ないし中学生の追跡をするのにＲＦＩＤを利用している前例を見つけることができませんでした。私たちの子どもは「在庫商品」ではありません。

教育とは、お互いを尊敬しあい、かつ、許しあうことを教えることです。教育とは、あらゆる動向を監視する「ビッグ・ブラザー（全体主義国家の独裁者）」体制を志向するものではありませんし、あるいは、子どもは重罪を犯した犯罪者よりも小さな権利を持っている存在に過ぎないと感じさせることにあるのでもありません。
〔邦訳中略〕私たち親権者はいかなる権利も有しておらず、したがって、子どもにとり何がベストなのかは学校が決める、と言うのでしょうか。私たちの道徳的信念や信仰は保障されないのでしょうか。私たちの子どもは、復讐の恐れから開放された良い教育を受ける権利を有していないのでしょうか。

敬具
差出人の氏名・住所　〔個人情報保護のため黒塗り〕
同時送付先：

・ドン・ハグランド、ブリタン校区委員会の委員長
・ジェフ・ホーランド、シャター郡視学官
・ラス・グリーン、カリフォルニア州教育委員会
・マーシャ・ベッドウエル、州教育委員会法務官
・サム・アネスタッド、州上院議員
・ダッグ・ラマルファ、州下院議員
・電子プライバシー情報センター（ＥＰＩＣ）
・アメリカ自由人権協会（ＡＣＬＵ）

● 実験校の父母の抗議活動をプライバシー保護団体が支援

（辻村）実験校の勇気ある父母のこうした抗議活動は、その輪を広げていったのですね。
（石村）そうです。実験校の父母は、主だった人権団体にも働きかけをしました。電子プライバシー情報センター（ＥＰＩＣ）、アメリカ自由人権協会（ＡＣＬＵ）、電子フロンティア基金（ＥＦＦ）など主要なプライバシー保護団体が、無線電子タグ（ＲＦＩＤ）を使った児童・生徒監視システムの人権に与える危険性に警鐘を鳴らしました。この問題は全米に報道されるようになり、世間の注目を浴びるようになりました。
（辻村）実験校の父母の間では、安全対策として支持する意見が多かったのか、それとも、教育現場にはふさわしくないとして反対する意見が多かったのでしょうか。
（石村）田舎の学校での出来事でしたから、大方の父母は、学校がやることだから仕方がないといった雰囲気だったようです。
（辻村）まあ、最初に問題を告発した生徒の父母は異端視されたでしょう。でも、こうした勇気ある人たちの行動と、この行動をしっかりと受け止める運動団体がないと、抗議の輪は容易に広がりませんからね。で、運動はどう広がっていったのでしょうか？
（石村）主だったプライバシー保護団体が、共同で、ブリタン小中学校の理事会に対して、実験を中止するように意見書を送付しました。送付された意見書を仮訳すると、次のとおりです。

生徒のＩＤ名札に無線ＩＣタグ（ＲＦＩＤ）を装着することの安全性と市民的自由に関する意見書

ブリタン小中学校理事会　ドン・ハグランド　様
２３４０　ペッパー通りサッター、カルフォルニア９５９８２　　Ｆａｘ（５３０）８２２－５１４３
２００５年2月7日

用件：生徒のＩＤ名札に無線ＩＤ（ＲＦＩＤ）を装着することの安全性と市民的自由に関して

ハグランド　様
私どもは、この文書で、最近、貴殿の校区において生徒に無線ＩＣ（ＲＦＩＤ）タグがついた名札を装着するように義務付ける決定をしたことについて、強い関心を持っていることをお伝えします。この新規の名札は、その利用から得られるとされる効率性よりも、権利侵害的な新技術の利用に伴う危険性の方が勝っております。ブリタン校をより安全にするというよりは、むしろ子どもたちを危険にさらします。私どもは、このプログラムの安全性の重大さと市民的自由を考え、直ちにこの軽率な実験を中止するように勧告します。

校区が無線ＩＣ（ＲＦＩＤ）タグつき名札の着装を義務付ける本来の目的は、安全と管理の効率化にあるのは明らかですが、この種の名札には問題があり検討を要するといえます。私どもが校区の父母とともに調査したところによると、ブリタン校ではこれまで安全面や出席面でいかなる問題も生じていないことがはっきりしています。これら双方の点に関する限り、子どもを追跡する装置を使うことなしにすでに対応ができています。

しかし、より重要なことは、ＲＦＩＤ名札の装着は、何者かがＩＣチップ読取機を持っている場合にその者に生徒の本人情報や位置情報を流すことになり、かえって生徒の身の安全と防護策を危険にさらすことになることです。ＲＦＩＤ名札の装着は、学校関係者ではない、何者かがブリタン校の生徒を標的にし、かつ見つけ出すことを極めて容易にします。ＲＦＩＤ読取機は格安になっており、しかも広くどこででも入手できることから、生徒への脅威は増します。校区と会社は、どのようにして生徒の個人情報や位置情報への不正なアクセス、利用および開示から生徒を保護するつもりなのか、十分な保障を示していません。
重大な安全問題があることに加え、生徒にＲＦＩＤ名札の装着を義務付けることは、学校を刑務所のよ

うな環境にすることを意味します。ＲＦＩＤ名札の利用は、生徒を尊重せず、信頼もしないような環境をつくりあげることにつながり、年齢にかかわらず全ての子どもの尊厳を傷つけるでしょう。合衆国も批准している世界人権宣言では、人としての尊厳を、人間として存在する本質的な要素として、かつ、自由と平等の一要件として、保障するとうたっています。ブリタン校区は、感受性の強い生徒に対して、これら生徒を監視する際に、現在おなじような技術が家畜や配送台、ハイテク刑務所の受刑者にも使われている、と極めて不穏当な発言をしています。ある父母が私どもに言いました。子どもが学校から帰宅するやいなや、名札をテーブルに投げつけ、「僕は、食料品、肉切れ、オレンジだ」と。

この新たなプログラムの実施によって生じた問題の重大性を考えると、生徒の父母に相談することなく進められた校区の決定は、まったく驚きであります。私どもが知る限りでは、どの父母も、この技術の導入についてまったく相談を受けていないばかりか、子どもたちがＲＦＩＤ名札の装着を義務付けられる以前にこのシステムの評価あるいは導入を正当化する根拠について質問をする機会すら与えられていませんでした。私どもが知る限りでは、校区は、父母の疑義に応えるのではなく、むしろ子どもに対するけん責処分をほのめかしたようです。これは、正しいことではありません。いかなる子どもやその父母も、生徒の身の安全、防護策、さらにはプライバシー権の保護を求めたとしても、このことでもって処分の脅しを受けることがあってはなりません。生徒とその父母の権利は、校門でストップできません。ティンカー　対　デス・モイネス・インディペンデント・スクール・ディストリクト事件連邦最高裁判決〔３９３ Ｕ．Ｓ．５０３（１９６９）〕を参照してください。私どもは、校区委員会がブリトン校の生徒やその家族が唱えたプライバシーと市民的自由に関する意見を尊重し、委員会が行った決定を見直すように勧告します。

敬具

・ニコル・オザー
技術と市民的自由政策担当部長
アメリカ自由人権協会（ＡＣＬＵ）

・リー・ティエン
上席団体内弁護士
電子フロンティア基金

・レドリック・ローラント
政策担当部門
電子プライバシー情報センター（ＥＰＩＣ）

●　実験は中止に

（辻村）ブリタン小中学校の生徒の父母やプライバシー保護団体の抗議を受け、学校側はどういった対応をとったのですか？

（石村）システムを納入する手はずになっていたインコム社は、プライバシー保護団体連合から意見書を受け取った同日の２月７日に、急きょプロジェクトを中止しました。１６０人の生徒は、名札とＩＣタグについたビニールケースをインコム社に返却しました。

（辻村）それで丸く収まったのですか？

（石村）グラハム校長は、このプロがラムは、「出欠確認の自動化」が本来のねらいであり、生徒の行動監視がねらいではなかった、と弁解していたようです。また、同校が最先端を行く学校の見本になるいいチャンスだったのに、残念だと言っていたようです。

（辻村）しかし、現実には、各生徒の居場所が四六時中追跡・監視できるわけですから、校長の弁解には納得がいかないですね。

（石村）インコム社のＨＰ（ホームページ）には、生徒の学内での位置確認も含め、常時追跡・監視可能が売り物になっていたようです。それに、後でわかったことですが、インコム社は、実験に協力する学校側には、システム設置やメンテナンス費用を請求しないばかりか、実験の結果がよく他校でもシステム導入が決まれば売上げの一部を同校に寄付する協約を学校側と交わしていました。また、ベンチャー企業のインコム社の創業者の一人が、同校のネットワーク管理を請け負っていた関係から、今回の実験校にブリタン小中学校が選ばれた理由のようです。

（辻村）問題のある取引のような気がしますね。

（石村）まあ、アメリカの高校では、ソフトドリンクの企業とタイアップして、校内にソフトドリンク・バーを設置しているところが多いのです。生徒がドリンクを飲めば飲むほど、その企業から、学校にバックマネーが落ちるという仕組みです。

（辻村）学校は、そのお金を学校の運営資金とし

て使っているわけでしょうけど。「営業の自由」という視点では問題ないのでしょうけど・・・。
（石村）ソフトドリンクの飲みすぎで、肥満児が増える一因になっているようで、問題にはなっています。

● 「安全」優先で、問われる「監視されない権利」の保障

（辻村）ともかく、わが国の場合、管理教育が大好きで、人権意識の希薄な学校管理者が多いのが現状です。ＩＴ企業が、こうした「出欠自動確認・校内安全監視システム」を学校に売り込めば、進んで導入するのではないかと思います。
（石村）受刑者のみならず看守にもＩＣタグを着装させ監視するハイテク監獄と同じ発想で、児童・生徒だけでなく教職員もＩＣタグで追尾・監視しようという学校管理者が出てくるのが懸念されます。
（辻村）確かに、刑務所のように監視カメラで学校を囲んで「わが校はこれで安全」とか・・・そんな学校環境が普遍化してきていますからね。
（石村）外部から不審者の侵入、それから危険物を持って校内で暴れる生徒の増加等々・・・、「校内全方位監視でプライバシーゼロになっても、安全な学校環境の方がいい」という風潮がますます強くなってきていますから、無線ＩＣタグを開発・製造販売するＩＴ企業も、「特需」におおはしゃぎでしょう。
（辻村）ＩＴハイエナ企業にとって「大きなビジネス・チャンス」であるとは言っても、学校教育の現場で、明確なプライバシー保護政策がないまま、なし崩しにこんな電子監視システムがドンドン導入されてしまっては、子どもの人格形成に与える影響が大きいと思います。
（石村）同感です。プライバシー影響評価がないに等しいですからね。ともかく、「安全」という公益と「人権」という保護法益があります。もう一度、原点に立ち返って見てみる必要があります。いま、まさに、教育現場における児童・生徒・学生の〝人権〟、とりわけ〝監視されない権利〟を、どう保障するかが問われています。
（辻村）ここでいう「監視されない権利」とは、どういった法概念なのでしょうか。
（石村）「個人として尊重される権利」をベースに、「移動の自由」、「表現の自由」などの「自由権」を集成した権利として構築できると思います。受刑者などのように、こうした自由権を一定限度まで制限される人を除いて、「監視されない権利」は当然に保障される、と考えていいのではないでしょうか。
（辻村）考え方によっては、プライバシー権の一部としても構成できますよね。
（石村）むしろ、「日照権」とかと同じように、新たな現代的な人権として「監視されない権利」を育てていく方がベターだと思います。
（辻村）そうですね。この種の権利が確立できれば、学校現場で、教職員や父母などが、子どもたちには「監視されない権利」があるんだ、それを保障するには、どういった「安全」対策までは許されるのか、といった基準もつくれるし、評価もできるようになりますね。それに、一般の職場などでも使える。
（石村）現在は、「安全」がすべてで、監視のオリの中で教育をやろうという感覚です。やはり、まず、「監視されない権利」をカサにして、子どもたちに降り注いでくる「安全」という名の〝監視の雨〟を考えていくべきですね。
（辻村）でないと、わが国の教育現場は、監視カメラ、生体認証型ＩＣカード、無線ＩＣタグ（ＲＦＩＤ）等々、「電子監視収容所列島」化してしまいますからね。
（石村）それに、教育の現場で、子どもたちに対しても「監視されない権利」について、しっかり教えないといけません。子どもたちに、「監視されない権利」がちゃんと根付けば、新たな電子監視機器が出てくれば、それを〝評価〟〝見る目〟ができてきますからね。
（辻村）息の長い活動が要りますね。学校関係者や父母はもちろんのこと、自治体の首長や議員、さらには普通の市民が、「監視されない権利」をしっかりと考えられるようにならないといけませんからね。理論の構築、それから分かりやすい市民向けテキストをつくる必要がありますね。
（石村）プライバシー運動を引っ張っている市民団体や労働組合、政党などには、是非とも「監視されない権利」を確立するためのソフトな市民運動を積極的に展開して欲しいと思います。あらゆるところで、〝私たち国民には「監視されない権利」があります〟と、スローガンを繰り返すのが、単純ですが、最も効果があると思います。
（辻村）同感です。政党のマニフェストなどにも、この「監視されない権利」をうたわせる必要がありますね。PIJのこれからの政策提言の目玉にもしないといけませんね。この辺で終わりにしたいと思います。ありがとうございました。

アメリカ・加州のプライバシー保護のための ＲＦＩＤ規制法案

― 諸州で加速するＲＦＩＤ（無線ＩＣタグ）への法規制の動き

PIJ・ＲＦＩＤに関するプライバシー問題検討プロジェクトチーム（ＰＴ）

ＲＦＩＤ（＝Radio Frequency Identification）、あるいは「アール・エフ・アイ・ディ」は注目を集めているＩＴ（情報技術）である。〝ＲＦＩＤ〟は、「無線ＩＣタグ」、「ＩＣタグ」、「電子荷札」、「電子タグ」、あるいは「非接触型ＩＣタグ」等々、さまざまに邦訳されている。欧米では、「ＲＦＩＤ」が一般的な呼び名である。直訳では、「無線周波数識別」。ここでは、わが国で一般的な呼び名である「無線ＩＣタグ」の言葉を使っておく。

ユビキタス（何でもコンピュータ）の時代に入り、あらゆる物に無線ＩＣタグを組み込めば便利な社会になるという考えが広まってきている。商品に装着すれば、万引やニセブランドの把握、生鮮品の産地証明などが簡単にできる。あたかも万能薬のような扱いである。

だが、無線ＩＣタグには、いい話ばかりではない。悪用されれば、情報の読取ができる側の人や企業に消費者性向や嗜好などが容易に見透かされてしまう。無線ＩＣタグで、〝電子のぞき社会〟出現の悪夢も。従業員や生徒のユニフォームに着装させると、行動の監視もできる。

この結果、市民は、いつも、どこかで監視されているという、鉄条網のないＲＦＩＤの〝オリ〟の中でくらすことを余儀なくされかねない。これを「安心の代償」と考えるのか、それとも「自由の侵害」と考えるのか、人によって違うのは当然である。ただ、企業や雇用主が、一方的に、ＲＦＩＤは消費者・市民・従業員・生徒の便益のなるのだといった考え方を押し付けるのではダメである。各個人が自らの意思で選択・自己決定できる仕組みが用意されていなければならない。

企業が、無線ＩＣタグを商品の在庫管理や盗難防止に活用したり、従業員や生徒の行動監視に売り込むのは、それこそ〝営業の自由〟というかも知れない。だが、消費者が買った後もその商品にタグがついていてはプライバシー保護の観点から大きな問題だ。また、子供の行動追跡が本人や保護者のインフォームドコンセント（十分に説明をした上で同意）を得ることなしに一律に実施されることも問題だ。まさにＩＴ企業による営業の自由の〝乱用〟にあたる。

わが国政府は、無線ＩＣタグの乱用規制について、法規制ではなく、ガイドラインで対応する選択をし、総務省と経済産業省は共同で、「電子タグに関するプライバシー保護ガイドライン」を策定、２００４年6月8日に公表した〔本号１１頁に掲載〕。企業などがＲＦＩＤ・無線ＩＣタグを利用して商品や個人情報を取扱う際に、消費者のプライバシーが侵害されないようにするのが目的。

これに対して、アメリカ諸州では、法律による規制に向かっている。カリフォルニア、バージニア、マサチューセッツ、メリーランド、ニューメキシコなどは、消費者のプライバシーを守るための立法の実現に向けた動きが加速している。

そこで、今号では、カリフォルニア州の法案および関連資料を、石村耕治（PIJ・ＲＦＩＤに関するプライバシー問題検討プロジェクトチーム座長）に邦訳（仮訳）してもらい、掲載することにした。今後、この問題に関する公共政策策定の一助となればと願っている。

（CNNニューズ編集部）

カリフォルニア州議会２００４年上院第１８３４号法案〔仮訳〕「ＲＦＩＤ（無線周波数識別）規制法案」

── ブラウン上院議員提出（共同提案代表者～マチャード上院議員）

２００４年2月２０日

事業に関して、事業及び専門職法典第８部に第２２．７章を追加する法律

法制局要旨

上院第１８３４号法案は、ブラウンによる提案で、ＲＦＩＤシステム（Radio frequency identification system・無線周波数識別）に関する修正を目的としたもの。

現行法は、さまざまな事業の特別の事業規制を課している。

本法案は、民間事業者が、一定の要件を充たす場合を除き、個人の識別に使うことのできる情報を収集、保存、利用若しくは頒布する目的で、ＲＦＩＤタグを消費者向け商品に着装した電子商品コードシステムを利用する又はＲＦＩＤ読取機を利用することを禁止するものである。この法案は、図書館が、特定の要件を充たす場合を除き、貸出者を識別するに使うことのできる情報を収集する目的で貸出物にＲＦＩＤタグを装着して利用することを禁止するものである。

・表決～過半数を要す。　・歳出割当承認～必要なし。　・財務委員会～関係なし。　・州が強制する地方団体のプログラム～なし。

カリフォルニア州民は、次のように法律を制定する。

第１条　事業及び専門職法典第８編に、次のように、第２２．７章（第２２６５０以下）を追加する。

第２２．７章　ＲＦＩＤ（無線周波数識別）

第２２６５０条　　民間事業者は、個人の識別に使うことのできる情報を収集、保存、利用若しくは頒布する目的で、ＲＦＩＤタグを消費者向け商品に着装した電子商品コードシステム又はＲＦＩＤ読取機を利用してはならない。ただし、次のすべての要件を充足する場合には、その限りではない。

第（ａ）項　その情報が法律で許容される範囲内で収集されている。

第（ｂ）項　その情報が、小売店舗でＲＦＩＤタグが付けられた品目を購入若しくは賃借する取引を遂行する目的で顧客によって提供されている。

第（ｃ）項　いかなる場合においても、その情報が、顧客が品目を購入若しくは賃借する取引を開始する以前又はその取引を終了した時には収集されていない。

第（ｄ）項　その情報は、もっぱら購入若しくは賃貸する品目に現実に関わった顧客に係るものであり、かつ、もっぱら当該品目に係るものである。

第２２６５１条　図書館は、貸出者の識別に使うことのできる情報を収集、保存、利用若しくは頒布する目的で、ＲＦＩＤタグを貸出物に装着した電子商品コードシステム又はＲＦＩＤ読取機を利用してはならない。ただし、次のすべての要件を充足する場合には、その限りではない。

第（ａ）項　その情報が法律で許容される範囲内で収集されている。

第（ｂ）項　その情報が、その図書館の収集物及びサービスを利用する目的又は、ＲＦＩＤタグが付けられた貸出物を含む、図書館から貸出物を借り出す目的で、貸出者によって自発的に提供されている。

第（ｃ）項　いかなる場合においても、その情報が、貸借者が当該貸借物を実際に貸借しようとする以前又はＲＦＩＤタグが付けられた当該貸出物の貸借取引が終了した時には収集されていない。

第（ｄ）項　その情報は、もっぱら貸借する貸借物に現実に関わった貸出者に係るものであり、かつ、もっぱら当該貸出物に係るものである。

加州議会下院：２００４年上院第１８３４号法案の公聴会

ＲＦＩＤシステムに関する２００４年6月２２日の公聴会

加州議会下院事業及び専門職委員会（ロー・コレア委員長）

上院第１８３４号法案（ブラウン上院議員提出）：２００４年6月１４日修正
州議会上院での表決：２２対９で通過

・議題：ＲＦＩＤシステム（Radio frequency identification system・無線周波数識別システム）

・法案要約：会社や図書館が、特定の要件を充足しない限り、顧客を個人として識別できる情報を収集、保存、利用若しくは頒布する目的で、ＲＦＩＤシステムを商品に付けることを禁止するものである。〔以下、邦訳省略〕

・現行法は：金融機関に対し、顧客の同意を得ることなしに関係のない第三者に対して公の支配にない個人と識別できる情報を頒布又は売却することを禁止している。金融機関は、顧客の個人情報を市場調査企業及び提携企業に頒布する場合には、該当者に対し「拒否できる選択（opt-out）」の機会を与えるように求められる。
・現行法は、「会員カード」プログラムを有する店舗に対し、会員カード申請に際して運転免許証番号及び社会保障番号を収集することを禁じ、かつ、顧客の個人情報を売却又は頒布することを禁じている。
・現行の連邦法は、ビデオ貸出店及び図書館に対し、当初、顧客から明示の同意を得ることなしにその顧客の記録を頒布又は売却することを禁じている。

・財政への影響：不明。本法案は本質的に財政とは無関係である。

・解説：

・《本法案の目的》この法案は、個人を識別できる情報の追跡及び収集を防ぐために、ＲＦＩＤ並びに電子商品コード（ＥＰＣ）システムの利用に規制をかけることが目的である。
・現実には、この法案は、民間事業者及び図書館が消費者向け商品及び図書館の蔵書にＲＦＩＤタグを装着しかつ追跡することを規制することになる。情報の収集は、その取引時に制限され、当該取引に関連するものであり、かつ、当該取引に関する特定の品目及び個人に限定されることになる。
・法案提案者は、本法案が将来のプライバシーの濫用又は侵害を事前に封じるに必要であると主張する。一方、法案に反対する者は、未完成なものであり、かつ、技術の発展に不当な制限を課すものであると主張する。プライバシー擁護者によっては、この法案を支持するのではなく、一般的な論題について自らの考え方を説き、かつ、この問題に対する代替的な手法を提案している。

・ＲＦＩＤ技術（Radio frequency identification technology・無線周波数識別技術）：ＲＦＩＤは、技術者にとっては、離れたところにある品目を自動的に識別するために電波を使いかつ情報を保存することをさす一般的な呼び名である。概念的には、ＲＦＩＤ技術は、特定の情報を保存し、追跡し、付加し、かつ変更することを可能とし、クレジットカードや身分証明証カードで使われているバーコードや磁気帯とかなり似た機能を有している。しかし、ＲＦＩＤは、２５から３０フィート離れたところから、商品を読み取る手動の読取機を持つ人の任務を解いて、まっすぐでない角度から読取もできるゴマ粒大のコンピュータ・チップを使用している。
・例えば、工場で梱包された商品を積んだ台にＲＦＩＤタグを装着しておき、一方で、倉庫にＲＦＩＤ読取機（アンテナともいう）を設置しておけばその扉を開かなくとも、荷送り人に対し、数量、型式、製造日及び目的地を容易に伝達することができる。アンテナは、壁、棚、及び戸口に設置でき、かつ、それによって通り抜けたタグのデータの読取及び記入ができる。
・法案提案者は次のようにいう。「ＲＦＩＤタグは、来る１０年以内に図書館の蔵書から食料雑貨に至るまであらゆる物に、バーコードに代わって

装着されることが予測される。これにより、企業は出荷や在庫管理を自動化でき、数百億ドルの経費を節減できる。１タグあたり約２０から５０セント、読取機１台あたり1,０００ドル程度かかることから、ＲＦＩＤシステムが普及するにはいまだ高すぎる。しかし、専門家の調査によると、需要が伸びれば、製造コストは下がり、次の１０年以内に、ＲＦＩＤ技術の利用はもっと容易になるとみられている。」

・法案提案者は、すでにＲＦＩＤ技術が利用されている数多くの例をあげている。カリフォルニア・ファストラック（FasTrack）自動橋梁通行料金システム、ペット動物に移植されたＩＤチップ、消費者商品相互作用追跡のためのパイロット計画、ウォルマート（WalMart）のような大規模小売業によるショッピング・システム（商品の一部にＲＦＩＤ開示タグをすでに付けている）。また、提案者は、重大なプライバシー問題を引き起こすＲＦＩＤ利用の実例及び予測例をあげている。小売店舗におけるＲＦＩＤを使った消費者行動の監視、病院における患者の追跡、ＥＵ通貨へのＲＦＩＤタグ挿入の動き、さらには、図書館蔵書の追跡及び図書館利用者のプロファイリング（人物像の描写）。

・法案賛成論：　法案提案者は次のようにいう。「上院法案第１８３４号は、事業者が商品を購入した人々に関しどのような情報を収集できるのかを変更を加えるものではない。代わりに、その収集方法、この場合にはＲＦＩＤ、に焦点を絞っており、かつ、この収集方法が標準的な賃貸・購入取引の範囲外で顧客に関する情報を収集する目的で利用することができるかどうかである。」

・プライバシー擁護者は、ＲＦＩＤは監視カメラと同様に普遍化し、かつ、市場調査人に対し人々の動向や買手の行動を追跡するもう一つの方法を与えることになる、ということに関心を払っている。例えば、理論的には、事業者はあらゆる物にＲＦＩＤタグをつけることが可能である。すなわち、このことは、ＲＦＩＤのアンテナによって、どこでも、人々の衣類、宝石、さらには着ているものの製造者を識別することはもちろんのこと、人々の財布、カバン、買物袋の中身を追跡することを可能にする。こうした情報を収集し、集約しかつ操作する能力を、店舗やレストランに出入りし商店街を歩き回る人々が顧客になるかどうか想定しかつ識別することに利用できるとすれば、事業者に対し強力な市場調査のための武器を与えることになる。」

・「上院法案第１８３４号は、店舗や図書館が、この新たな技術を使ってすでに現在バーコードを使って収集していると同様の情報を収集することができるようになることから生じる特別のプライバシー問題を提起しようというものである。その一方で、同時に、人々が買物をしたとき又は店舗を出た後にその人々を追跡するためにこの技術を使うのを禁止しようというものである。」

・法案反対論：反対連合は、ＲＦＩＤが近年活用されだした新技術であり、かつ、規制をかけることはこの技術の発展を意図的にねじ曲げることにつながる、と主張する。反対連合は、次のことを指摘する。「いくつかの主要な小売業者は、製造業者から、２００５年1月1日までに、状況に即応できる集荷台基準を採用するためにＥＰＣとＲＦＩＤを設置するように求められている。私どもは、ＲＦＩＤの設置が、陳列棚への商品の素早い補充、盗難の防止及び模造商品の識別を可能にし、消費者の利益につながっている、と信じる。さらに、商品のリコール（不良商品回収）を、より効率的かつ実効性のあがる方法で行うことが可能になる」と。

・また、反対論者は、次のように主張する。「１９９９年に実地テストと試行のためのＭＩＴ自動ＩＤセンターを創設し、かつ、通知、選択、教育、記録の利用、記録の保存及び安全に関する業界ガイドラインの採択により、ＲＦＩＤ技術がプライバシーに与える潜在的な影響についてすでに検討を行っている」と。

・反対論者は、次のように主張する。「上院法案第１８３４号は、ＥＰＣとＲＦＩＤの利用に対してその技術が幼い段階で数多くの規制をかけることになる。私どもは、こうした規制により、この技術から消費者が得られる潜在的な利益を少なくしてしまうという予想されていない数多くの結果をもたらすものと信じる。」と。カリフォルニア食料雑貨商協会は、次のように強調する。「ＲＦＩＤ技術は約２０年前のインターネットと同様な段階にある。インターネットは、その利用から数多くの余り好ましくない副産物がでている一方で、ほとんどのカリフォルニア州民は、否定的な面よりも利益の方がまさっていると見ている。私どもは、ＲＦＩＤに関して現在よりも１０年あるいは２０年後を考えて欲しいわけです。」と。

・上院法案第１８３４号に中立的なプライバシー擁護者：ＲＦＩＤに対する一般的な関心　プライバシー擁護者連合（アメリカ自由人権協会《ＡＣＬＵ》、エレクトロニック・フロンティア基金《ＥＦＦ》、プライバシー権クリアリングハウス《ＰＲＣ》）は、この法案に賛成はしていないものの、「ＲＦＩＤは、不適切に利用された場合には、消費者のプライバシーを危険に陥れ、匿名での買物を難しくし、したがって、市民の自由に脅威を与える」と考えている。
・一般に、プライバシー擁護者は、ＲＦＩＤ技術が「プロファイリング」の可能性につながることから、重大なプライバシー問題を引き起こすと主張する。ＲＦＩＤは、極めて小さくかつ目立たないので、普段の物品や衣類につけることができる。このため、人々は自分が追跡されていることを知らない。さらに、ＲＦＩＤが広く普及することは、タグ情報からなる「巨大なデータベース」の創設及び当該データベースへの個人識別データの接続を許すことにもつながる。個人情報とＲＦＩＤデータが接続された場合、「個人は、自分の知らないところであるいは同意なしに、プロファイリングが行われかつ追跡されることになる。」
・「こうした接続が行われないとしても、ＲＦＩＤタグは、各々に唯一無二の識別子を内蔵しているので、それ自体で個人を追跡することを可能にする。追跡者は、唯一無二の識別子を使えば、当初追い回している人の名前を知らなくとも、移動する個人を追跡することができる。」
・本法案の代替案として、連合は、ＲＦＩＤシステムが引き起こす問題をまとめた次のような三部構成の提言をしている。
・第一に、ＲＦＩＤは「正式な技術評価を受ける必要があり、かつ、ＲＦＩＤタグは、この評価が実施されるまで消費者向け商品に装着されるべきではない。」
・第二に、「ＲＦＩＤの利用は、公正な情報慣行（ＦＩＰ＝Fair Information Practice）の諸原則に従って運用されなければならない。」　ＦＩＰは、３０ヵ国を超える加盟国からなる世界機関であるＯＥＣＤが、公共サービス及び法人企業活動における善良なガバナンスの育成に重要な役割を果たすねらいで採択したプライバシー・ガイドラインである。」
・第三に、「次のようなＲＦＩＤの利用の仕方は、即禁止されるべきである。」例えば、消費者にタグのついた商品を強制すること。消費者にタグを探知しかつ不能にすることを認めないこと。同意なしに個人を追跡すること。さらには、通貨にタグを装着すること。
・さらに、プライバシー擁護者は、本法案に対して、とりわけ、次のような修正を行うように提言している。ＲＦＩＤは運転免許証やＩＤカードへ装着することが認められるべきではない。公的セクターの事業者は、民間セクターからデータを収集することが禁止されるべきである。図書館でのＲＦＩＤの利用禁止規定は、地方団体がもっと厳しい規制を望む場合の足かせにならないようにするために、削除されるべきである。商品にＲＦＩＤ装着の表示が義務付けられるべきである。消費者には、ＲＦＩＤを読取、かつ不能にする権利が与えられるべきである。その他の透明化策が講じられるべきである。

《法案への記名の賛成／反対》

・賛成　提出なし
・反対

・アメリカ自由人権協会
(America Civil Liberties Union)
・アメリカ電子協会
(American Electronics Association)
・カリフォルニア商工会議所
(California Chamber of Commerce)
・カリフォルニア食料雑貨商協会
(California Grocers association)
・カリフォルニア小売業協会
(California Retailers Association)
・消費者専門商品協会
(Consumer Specialty Products Association)
・エレクトロニック・フロンティア基金
(Electronic Frontier Foundation)
・ジェネラルモーターズ会社
(General Motors Corporation)
・全米食料雑貨製造者団体
(Grocery Manufacturers of America)
・プライバシー権クリアリングハウス
(Privacy Rights Clearinghouse)

EU（ヨーロッパ連合）
RFID技術にかかるデータ保護の課題に関する作業部会報告書（2005年1月19日）

EU個人データ保護作業部会

Article 29 Date Protection Working Party
Working document on data protection issues related to RFID technology
(January 19, 2005)

《邦訳責任者》　PIJ代表　石　村　耕　治

EU（ヨーロッパ連合）加盟諸国においては、さまざまな分野でRFID技術（Radio Frequency Identification technology＝無線周波数識別技術）の使用が進んできている。この技術を基にしたRFIDシステムは、①無線ICタグ、②リーダーライター（読取・書入れ機）、③RFIDアプリケーション（応用ソフト）などからなる。この地域におけるRFID技術の使用が広がるにつれて、RFIDシステムに関する個人情報（データ）保護、あるいはプライバシー保護が、次第に重い課題となってきている。

EUは、データ保護作業部会で、RFID技術にかかるデータ保護の課題について検討を行ってきた。そして、2005年1月19日に、「RFID技術にかかるデータ保護の課題に関する作業部会報告書」を公表した。

この作業部会は、EC95／46EC指令（EU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〕の下で設けられたものである。同作業部会における検討は、EC95／46EC指令30条および2002／58／EC指令15条に準拠して行われたものである。

CNNニューズ編集部では、今号で、特集《RFID・無線ICタグとプライバシー》を組んでおり、今年1月に出された「RFID技術に係るデータ保護の課題に関する作業部会報告書」の紹介は、必要不可欠との認識を持っていた。そこで、PIJの「RFIDに関するプライバシー問題検討プロジェクトチーム」の座長である石村耕治代表に、急きょ、この報告書の邦訳（抄訳）をお願いした。石村代表には、拙速な依頼にもかかわらず、邦訳作業を開始くださり、お礼を申し上げたい。

ちなみに、EU個人データ保護指令の概要は、すでにCNNニューズ7号および8号に掲載されているので、参照されたい。

（CNNニューズ編集部）

EU・RFID技術にかかるデータ保護の課題に関する作業部会報告書（2005年1月19日）〔抄訳〕

EU個人データ保護作業部会

1．　はじめに

無線周波数識別（RFID＝Radio Frequency Identification）技術は、一般にRFID・無線ICタグとして知られており、さまざまな目的で使われている。また、企業、個人および（政府を含む）公共サービスは、この技術の使用から恩恵を

受けている。後にこの報告書で詳しく触れるように、ＲＦＩＤ・無線ＩＣタグは、小売業者の在庫管理、消費者の購買意欲の増進、薬物の安全度の改善、さらには制限された地域への人の立入りを効率的に規制するためにも活用することができる。

ＲＦＩＤ技術の使用から受けられる恩恵ははっきりしているものの、この技術の幅広い活用は、この技術が持つ予期しなかった欠点を浮き彫りにする。データ保護の現場において、ＥＣデータ保護法２９条に基く作業部会（以下「２９条作業部会」）は、人間の尊厳やデータ保護を求める権利を侵害するようなＲＦＩＤ技術の使用に注意を払っている。とくに、企業や政府が、個人のプライバシー領域を詮索するためにこの技術を使おうとする可能性に関心を持っている。同一人物に関するあらゆる種類のデータを密かに収集すること、公共空間（空港、列車の駅、店舗）を移動する個人の追跡、店舗における消費者行動の監視を通じてプロファイル（人物像の描写）を可能にすること、消費者が持ち歩く薬剤、身に着けている衣服やアクセサリーの詳細を読み取ること等々。これらは、まさに、プライバシーが問題になるＲＦＩＤ技術の使用例といえる。ＲＦＩＤは比較的コストが安いということもあって、この技術を、信頼の置ける関係者のみならず零細な業者や個人である市民までが入手できることにつながり、事態を悪化させている。

こうした新たな問題の出現が、２９条作業部会に対し、ＲＦＩＤ技術について、プライバシーその他の基本権の保障の面からの検討を強く求めることになった。とりわけ、この目的を達成するために、２９条作業部会は、この技術の製造業者や使用者、さらにはプライバシー保護団体などの利害関係人から意見を聴取した。２９条作業部会が行った分析結果は、この作業報告書に集約されたわけであるが、そのねらいは、次の二つである。第一に、ＲＦＩＤ使用者に対し、ＥＣ指令、とりわけデータ（個人情報）保護指令およびプライバシーと電子通信に関する指令に定められた基本原則を適用するためのガイドラインを示すことである。そして、第二に、この作業報告書に基いて、２９条作業部会が、技術（ＲＦＩＤタグ、ＲＦＩＤリーダー、ＲＦＩＤアプリケーション〔応用ソフト〕）の製造業者やこの技術の使用者が、データ保護指令の下での義務を遂行できるようにするため、ＲＦＩＤ規格の標準化団体に対しプライバシー評価手法を確立する責任を負わせることにある。

２９条作業部会は、ＲＦＩＤ技術の使用についての歴史が比較的浅いことを考慮して、この報告書は初期段階の現状分析を集成したものであると考えている。本作業部会は、引き続き現状を分析し、さらに経験が積み上げられた段階で、次の報告書を出す考えである。こう考えることは、ＲＦＩＤ技術が、未来志向的な知的環境における重要な「信頼感あるもの」の一つになるためにとりわけ必要である。したがって、今回は初期の報告書であり、２９条作業部会は、この問題についてさらに検討を続けていく所存である。

２．　ＲＦＩＤ技術～技術とその使用

〔本章は項目目次のみ邦訳、他は省略〕

２．１　　ＲＦＩＤ技術の基本

２．２　　各部門での多様な使用例

- 輸送／流通
- 空港
- 健康医療
- 安全およびアクセス規制
- 小売利用

３．データ保護とプライバシー面からの検討

ＲＦＩＤのアプリケーション（応用）に際しては、多くの場合、データ（個人情報）保護問題を考えに入れているが、後に触れるように、それを考えに入れていない場合も見受けられる。本章においては、ＲＦＩＤ技術のさまざまな使用から出てくるデータ保護面での主要な論点を整理してみる。

３．１　ＲＦＩＤが個人データと結合する情報を収集するために使われる場合

最初のデータ保護問題は、ＲＦＩＤ技術が個人データと直接または間接に関係する情報を収集するために使われる場合に生じる。まず、製品に付けられた固有のＲＦＩＤタグ番号が、それを購入した顧客の記録と結合する事例を考えてみよう。例えば電化製品販売店が、販売する製品に、クレジットカードでの支払の際に顧客の名前とシステム的に結合でき、かつ、その販売店の顧客データベースに接続できる固有の製品コードをふったタ

グを付けたとする。とりわけ、この場合、その目的は、製品の保証にあったとする。次に、消費者がスーパーマーケットの店舗にいる間、その者の嗜好、どのセクションでどの程度の時間を費やしたか、さらには、買物をする目的もなく何回その店舗を訪れたかなどを読取りかつ記録する目的をもって、個人の名前で本人を識別できるタグ付きのスーパーマーケットの顧客カードあるいは同様の仕掛けの事例を考えてみよう。

これらの事例では、ＲＦＩＤ技術を使って集められた情報が個人データと結び付いている以上、プライバシーが問題になることは明らかである。ＲＦＩＤ技術は、こうした顧客カードを使った消費者の嗜好を学び取る能力や個人の人物像を描写する能力を伸ばすとともに、商品ごとにタグを付けることで消費者の入店の確認や店内におけるその者の嗜好をモニターするのを可能にすることから、潜在的にダイレクト・マーケッティングを増加させる。さらに、この技術の使用が広がるにつれて、データ管理者が処理するデータ（の種類や量）を増加させる原因となり、問題を増やす結果を招く。

３．２　タグに個人データを蓄積するために使われるＲＦＩＤ

第二のタイプのプライバシー問題は、ＲＦＩＤタグに個人データが蓄積される場合に生じる。こうした利用例は、乗車切符に見られる。ある機関が、乗車証の所有者の名前や連絡先などをタグに搭載した定期券に対応できるＲＦＩＤ技術を使った非接触型の改札システムを導入するケースを考えてみる。このケースにおいて、その機関は、識別される個人がどこに移動しているのかを常時知ることができることになる。これは、明らかに個人のプライバシーに影響を及ぼす。システムを導入した機関が情報を入手できることに加え、標準的なリーダー（読取機）を持っている者はだれでもＲＦＩＤタグの存在を探知できることから、第三者も密かに同じ情報を入手することが可能になる。ＲＦＩＤシステムは、非常に攻撃されやすいことに注目すべきである。このシステムは、無線式、非接触で作動することから、攻撃をかける者は、他人に気づかれることなく、リモコンで受動的にデータの読取が可能である。

３．３　「伝統的な」識別子を使うことなしに追跡をする場合のＲＦＩＤの利用

第三のタイプのデータ（個人情報）保護問題は、ＲＦＩＤ技術を、個人を追跡しかつ個人データにアクセスし入手するために使う場合に生じる。ＲＦＩＤ技術がいかに個人のプライバシーに影響を及ぼすかについて、いくつかの事例をあげることができる。

例えば、日用雑貨チェーン店が、ショッピングカート（買物車）の動きを見るために、顧客に対して、来店の度に使える無線ＩＣタグの付いた仕掛け（例えば、割引券）を配布することが考えられる。この場合、その店舗は、個人が購入した製品をモニターするために、（割引券で識別できる）タグの付いた仕掛けに搭載されている識別番号を使い、その製品がどれくらい消費されたか、さらにはどのチェーン店でその製品を消費者が購入したかについてのファイルをつくることができる。そのチェーン店は、個人の所得、健康、生活様式、購買嗜好などを推測することができる。こうした情報は、マーケッティング、目標値設定、あるいは思い切った価格設定など、さまざまな意思決定に利用することができる。こうした仕掛けを使えば、個人が店舗に入ってくる度に本人識別ができることになることから、記録されたその消費者の嗜好にそって売り込みをすることも可能になる。店舗がこうした情報を収集できるようになることに加え、リーダー（読取機）を持つ第三者もそうした情報を入手する可能性も出てくる。このようにして、識別された個人について、本人からの同意を得ることなしに、さまざまな決定ができることになる。ＲＦＩＤの使用は、オンライン空間におけるクッキーの利用と同様であり、たとえその情報項目だけでは直ちにその個人を識別することはできないとしても、情報の連結によってその個人を識別することは可能といえる。なぜならば、その個人について蓄積されたあるいはその個人を取り巻く大量の情報を通じてそれほど困難もなく本人確認ができる可能性があるからである。さらに、収集された個人データは、その個人の扱い方ないしランク付けを考える際に利用できる。こうしたＲＦＩＤの使用は、重大な個人情報保護問題を引き起こす。

他の事例としては、ＲＦＩＤタグを使用すれば、そのＲＦＩＤ技術の使用の際に他にはっきり

した識別子を用いていなくとも、個人データの処理を進めることができることがあげられる。個人Ｚが、店舗Ａおよび店舗ＢからＲＦＩＤタグ付きの製品を持って店舗Ｃに入ってきたと仮定しよう。店舗Ｃは、リーダー（読取機）で、Ｚのバックを探索し、その中にある製品（番号はまぜこぜ状態にあると思うが）を読み取れる。店舗Ｃは、その番号を記録する。そして、翌日、Ｚが店舗Ｃにやってきたときに、ＣはＺを探索する。昨日読み取られた製品Ｙが、今日も読み取れたとすると、その番号はＺが常にはめている時計に付けられたものと見て取れる。店舗Ｃは、製品Ｙの番号を「キー」として使うファイルを作成する。このようにすれば、Ｚが店舗に入ってきた時に、彼の時計に付いたＲＦＩＤ番号を照会番号として使うことにより、Ｚを追尾することができることになる。これにより、店舗Ｃは、個人Ｚ（氏名は不詳）の人物像の描写（プロファイル）をすることができ、かつ、Ｚが次に店舗Ｃを訪れたときに彼の買物袋に何が入っているのかを追跡することができる。この場合、店舗Ｃは、個人データを取り扱っており、データ保護法令の適用を受けることになる。

最後に、ある物品の性質を明らかにする情報が搭載されたタグを使用する事例を考えてみよう。ある人の持ち物が非常に個人的なものであり、かつ、その持ち物に第三者が知ることはその人のプライバシーを侵害することになる情報が入っていると仮定する。このような仮定にあたるのは、次のようなケースである。読取機を持つ者が目の前を通過する人の小切手、本、薬品ないし貴重品を探知できる場合である。こうした情報を第三者が知り得ることはその物品を所有する人のプライバシーを侵害することになる。テロリストが群集の中にいる特定の国籍を持つ人を探知できるとすれば、同様の問題が生じる。パスポートに関する情報あるいは極めてセンシティブな情報のように、重要な個人情報が仕掛け（無線ＩＣタグ）自体に搭載されている場合があてはまる。こうした場合には、より大きな人権侵害が生じるように思われる。

こうした事例から分かるように、ＲＦＩＤ技術の使用に関するいくつかの重大なデータ保護やプライバシー問題は、タグが出す情報ないしメモリーコンテントに対する不正なアクセスにより、個人をその者の意思に反し密かに追跡することが原因となっている。

次の章においてより詳しく述べるように、上記のようなＲＦＩＤ技術を使ったデータ処理作業に対し、ＥＣ指令、とりわけデータ保護指令に定められた基本原則を適用するためのガイドラインを定めることが重要である。

４．ＲＦＩＤ技術を使って収集された情報に対するＥＵデータ保護法の適用

４．１　ＲＦＩＤ技術を使って収集およびその後処理されたデータに対するデータ保護指令の適用に関するガイドライン

データ保護指令は、その適用範囲という要件から見ると、あらゆる個人データ処理に対して適用される。指令において、「個人データ」は極めて広く定義されており、「識別されたまたは識別されうる自然人に関するあらゆる情報」を含むとしている。そこで、問題となるのは、このデータ保護指令は必然的にＲＦＩＤ技術を使って収集されるデータに適用になるのかどうかである。答は、原則として、ＲＦＩＤ技術の具体的なアプリケーション（応用）次第、ということである。とりわけ、ＲＦＩＤのアプリケーションが一般的なデータ保護指令に定義される個人データの処理を伴っているかどうかによる。

あるＲＦＩＤのアプリケーションによる個人データの収集方法に対してデータ保護指令が適用になるのかどうかを検討する場合に、私たちは、（ａ）ある個人に関して（relates）処理されたデータの範囲を決定し、その上で、（ｂ）当該データが識別された（identified）または識別されうる（identifiable）個人に関するものであるかどうかを判断しなければならない。データが個人の識別、性格もしくは行動に関するものである場合、または、そうした情報がその個人の扱い方ないしランク付けを考える際にもしくは決める際に使用される場合には、当該データは個人に関するものといえる。情報が識別されうる者に関するものであるかどうかを検討する場合、データ保護指令の注解第２６「人を識別するために管理者その他の者が合理的に使うことのできるあらゆる手段を考慮すべきである」とした規定を適用しなければならない。

このように見ると、データの収集をねらいとしたいかなるＲＦＩＤ技術のアプリケーションの場合にも必ずデータ保護指令が適用になるというわけではないのは明らかである。また、ＲＦＩＤ技

術を使った個人情報の収集、収集された個人情報の処理に対しデータ保護指令が適用になるケースはさまざまであることも明白である。

ＲＦＩＤ技術を使って収集された情報の利用を考える場合には、それをする前に、その情報がデータ保護指令にいう「個人データ」にあたるかどうかを判定するための評価を実施しなければならない。ＲＦＩＤ情報が上記のように定義された個人情報を含んでいないまたは個人情報に関係していない場合には、データ保護指令の規定は適用されない。したがって、タグ情報が、他の識別されうる資料、例えばその人の写真もしくは氏名および住所、または照会番号などと結合されていない場合には、データ保護指令は適用にならない。前記第３章において記述した３つの事例に対しては、データ保護指令の規定が適用される。第一の事例においては、ＲＦＩＤ技術を使って収集された情報内容が直接にクレジットカードないし顧客カードと連動しているので、指令の適用がある。第二の事例においては、ＲＦＩＤタグに氏名のような個人情報が搭載されているので、直ちにデータ保護指令が効力を持つ。最後の事例では、個人の行動を追跡する目的でＲＦＩＤ技術を使っており、大量のデータ集積ならびにコンピュータ・メモリーや処理能力があるとすると、たとえ識別されていないまたは識別されえないとしても、データ保護指令は適用になる。

４．２　データ保護要件の遵守に関するガイドライン

ＲＦＩＤ技術を使いデータを収集するデータ管理者（本報告書では「技術の使用者」ともいう）は、データ保護指令を遵守する義務を負う。さまざまなＲＦＩＤの使用状況の各々に対し、どのようにデータ保護要件が適用になるのかを定めるのは難しい。しかし、データ管理者が、取り巻くデータ処理状況に照らして利用できる一般的なガイドラインを定めることはできる。後記第５章で詳しく触れるように、製造業者は、データ管理者がデータ保護指令の下での自己の義務を遂行できるように支援し、かつ、個人が自己の権利を容易に行使できるようにするために、プライバシー苦情処理方式を確立する直接の義務を負っている。

《原則》

本作業部会は、ＲＦＩＤ技術、および他の技術、を使用する際に適用ある要件の骨子は、データ保護指令の注釈第２に、次のように定められていることを強調しておきたい。「データ処理システムは人に奉仕するために設計されている。〔中略〕このようなシステムは、自然人の国籍もしくは居住地いかんにかかわらず、自然人の基本権および自由、とりわけプライバシー権、を尊重し、かつ、経済的および社会的な発展、取引の拡大ならびに個人の福祉に貢献するものでなければならない。」

・データの質に関する原則～データ管理者は、ＲＦＩＤを使ってデータを収集する場合には、次のような複数のデータ保護原則を遵守しなければならない。

利用制限原則（目的原則）～この原則は、とりわけ、データ保護指令第６条１項ｂ号に具体化されており、収集目的に合わない処理を禁止する。

データの質の原則～指令にあるこの原則は、個人データは、収集する目的に照らして、適切であり、かつ、過剰にわたるものでないことを求めている。したがって、いかなる不適切なデータも収集してはならないし、また、不適切に収集したときには、消去されなければならない（第６条１項ｃ号）。また、データは正確、かつ、最新なものに保つように求められる。

保存原則～この原則は、個人データが収集された目的に必要とされる期間よりも長く保存されたり、または、収集目的を越えて処理されないように求める。

・データ処理の法的根拠～データ保護指令第７条によると、個人データは、データ処理を適法とする複数の根拠のうちのいずれか一つを満たした場合に限り、処理することができる*。

〔注記～指令第７条は、次のようなデータ処理を適法とする法的根拠をあげている。①データ主体がその処理に対し明示の同意を与えた場合、②データ主体が一方の当事者である契約の履行のためにその処理が必要である場合、③管理者に課された義務を遂行するために処理が必要である場合、④データ主体の生命にかかわる利益を保護するためにその処理が必要である場合、⑤公益上の任務を遂行するためにその処理が必要である場合、⑥責任ある当事者の適法な利益のためにその

処理が必要である場合。ただし、データ主体の基本権および自由、とりわけ個人のプライバシー権を保護が当該当事者の適法な利益に勝っているときは、その限りではない。〕

ほとんどのＲＦＩＤ技術が使われている状況において、データ管理者がこの技術による情報の収集を適法とする場合に使える法的根拠としては、本人からの同意が唯一であろう。例えば、スーパーマーケットは、顧客カードにＲＦＩＤ技術を用いた情報収集機能を持つタグを付ける場合には、その顧客カードの入手の際に、取得された個人情報が結合されることについて、契約に明確な条項を置くかあるいは本人の同意を得ることが必要であろう。もっとも、ＲＦＩＤシステムを用いて収集された個人データの処理において、本人からの同意を得たことが常にその処理を適法とするための唯一の適切な法的根拠であるとは限らない。例えば、病院が、手術器具にＲＦＩＤを装着し、手術の終了時に患者の体内に器具を置き忘れる危険の防止に努めたとする。この場合のデータ処理については、他の法的根拠、すなわちデータ保護指令第７条に予定されるデータ主体の生命にかかわる利益において適法とすることができることから、その患者の同意が必要というわけではない。

法的根拠として、同意が用いられたと仮定する。この場合、指令第２条および第７条ａ号によると、次の要件を満たさなければならない。①同意は自由意思で行われなければならない。したがって、同意は「詐欺または脅迫」から解放された上で得られなければならない。②同意は個別的なものでなければならない。言い換えると、同意は、目的を絞った特定されたものに関するものでなければならない。③同意は、特定個人の有効な意思表示でなければならない。④同意は、説明の上で得られなければならない。最後に、同意は「不明瞭ではなく」得られなければならないということについてであるが、これは、一つを越える目的を有する場合には同意があったものとみなされないということである。

・情報提供要件～データ保護指令第１０条によると、データ管理者は、ＲＦＩＤ技術を使って情報処理をしている場合には、データ主体に対し、次のような情報を提供しなければならない。管理者の身元、処理の目的、さらには、とりわけ、データの受領者およびアクセス権があることに関する情報。この要件の遵守について、第４章で述べた状況に照らしてみると、小売店舗は、データ主体に対し、最低でも次のような点についての明確な通知をしなければならない。

①製品もしくはその包装にＲＦＩＤタグが付いていることおよびリーダー（読取機）があること
②これにより収集される情報の詳細～とりわけ、データ管理者は、個人に対し、こうした仕掛けがあることにより、その個人の積極的な行為がなくともタグと情報をやり取りできる旨をきわめてはっきりと知らせなければならない。
③その情報を利用する目的～（ａ）ＲＦＩＤ情報と結び付くデータの種類、（ｂ）その情報が第三者に提供されるのかどうかなど
④管理者の身元

さらに、ＲＦＩＤに使用方法によっては、データ管理者は、次の事項を個人に知らせなければならない。⑤さらに情報が読み取られるのを防ぐために、どのようにタグを遮断できるのか、その製品に付いているタグをどのように読取不能にできあるいは取り外しができるのか、また、⑥どのように情報開示権を行使できるのか。こうした通知は、前記３．１の例においても必要である。消費者向け製品用のタグ管理システム（EPC Global）において、その通知は、前記①の程度の説明でもよいといえるが、さらに説明をし、資料で補完するべきである。

データ保護指令第６条ａ号にいう公正な処理原則においては、データ主体に対し、明確かつ包括的な方法で説明を行うように求めている。

最後に、本作業部会は、このような説明をする際には、データ主体がＲＦＩＤのアプリケーション（応用）の影響を容易に理解できるようにするための簡潔な手引をつけることが大事であると考える。

・データ主体のアクセス権～データ保護指令第１２条は、データ主体に対しデータの正確性およびそのデータが最新のものになっているかどうかをチェックできる機会を与えている。こうした権利は、ＲＦＩＤ技術を使って個人データを収集している場合にも認められる。さきに触れたタグ付きの顧客カードを発行しているスーパーマーケットのケースでは、アクセス権の付与は、その人と結合する、入店の回数、購入した商品など、あらゆる情報の開示につながるであろう。

前記３．２で触れた個人情報の入ったＲＦＩＤタグの場合において、個人は、タグに蓄積された情報を知る権利および容易にアクセスできる手段を用いた修正を求める権利を行使できる。

・安全に関する義務～データ保護指令第１７条は、データ管理者に対し、過失もしくは不法な侵入または違法な開示から個人データを保護するために、適切な技術的かつ組織的な措置を講じる義務を課している。この措置は、組織的または技術的なものでも足りる。この要件は、ＲＦＩＤとプライバシーを促進する技術の必然的な利用のタイトルで、次の第５章において展開する。

５．データ保護原則の適切な実施を確保するための技術的・組織的な要件

ＲＦＩＤアプリケーション（応用ソフト）の使用者は、さきに触れた諸原則およびデータ保護指令第６条１項に定められている収集データ最小化の原則を必ず遵守すべきである。

２９条作業部会は、ＲＦＩＤ技術を使って収集した個人データを処理するにあたり、データ保護原則を遵守するには、技術的な対応が重要な役割を演じるものと考えている。例えば、ＲＦＩＤタグやＲＦＩＤ読取機（リーダー）のデザイン、さらにはＲＦＩＤの利用が統一規格に従っているとする。この場合には、個人データの収集および利用の最小化、ならびに許可されていない者が個人データにアクセスするのを技術的に不可能にでき、不法な処理方法を防止するに大きな効果をあげることができる。

この点に関し、２９条作業部会は、次のことを強調したい。すなわち、ＲＦＩＤアプリケーションの使用者は、ＲＦＩＤを使って収集した個人データについて最終的な責任を持っていること。しかし、その一方で、ＲＦＩＤ技術の製造業者や規格の標準化団体は、ＲＦＩＤ技術を使う者が活用できるデータ保護・プライバシー遵守のＲＦＩＤ技術を確保する責任を負っていること。このような基準が、実際にＲＦＩＤ技術を使用する際に、広く適用されるように、制度を整備する必要がある。とくに、データ管理者が、ＲＦＩＤ技術を使って個人データの処理を行っている場合に、データ保護指令に定められた要件を充足するに必要な手段を持てるように、ＲＦＩＤプライバシー遵守基準が用意されていなければならない。したがって、本作業部会は、ＲＦＩＤタグ、リーダーおよびＲＦＩＤアプリケーション（応用ソフト）の製造業者、さらには規格の標準化団体は、次のような勧告を受け入れるように提言する。

５．１　規格の統一と互換性がデータ保護原則の適用に及ぼす影響

技術がどうのような状況にあれ、通例、新しい技術が問題なく採用されかつ応用されるためには、互換性を確保するための中核となる運転者を選ぶ規格の統一のプロセスは重要である。また、規格の統一は、データ保護やプライバシー要件の遵守にもつながる。

ＲＦＩＤシステムの構成部分、すなわち、タグやリーダー（読取機）のデザイン、タグに装填するデータ、リーダーとタグの間を交信する通信プロトコル（手続）、リーダーが集めたデータの管理など、全てが規格統一の対象となるまたは対象になりうる。すでに標準化団体その他の団体は、ＲＦＩＤの分野においてある程度の作業を行っている。ＲＦＩＤ規格の統一は、特定の物品の取引が行われている数多くの市場に影響を及ぼすであろう。

当初は狂牛病危機に応える形であったが、国際標準化機構（ＩＳＯ）は、分野別（荷物輸送用コンテナ、輸送ユニット、動物など）の特別の標準（規格）を整備してきている。ＲＦＩＤタグおよび無線接触領域（エア・インターフェイス）向けのＩＳＯ１８０００シリーズや物品の管理用ＩＳＯ／ＩＥＣ１５９６３・２００４）などがある。〔以下、邦訳中略〕

ほとんどのＲＦＩＤ統一規格においては、技術面での仕様の中にデータ保護機能を採り入れることが可能である。例えば、最近、ＩＳＯが整備したリーダー・タグ・プロトコルの規格は、ＯＥＣＤ（経済協力開発機構）が整備した公正な情報慣行（Fair Information Practices）を採り入れるために改正が予定されている。

最近、ヨーロッパ電気通信標準化協会（ＥＴＳＩ）は、ＵＨＢ無線周波帯で利用できる周波数およびリーダーの出力を増加することにより、小売部門における物品の識別においては最も精巧なものであるＲＦＩＤシステム使用に関する新たな欧州規格を承認した。この革新は、とくにリーダーによるタグの読取範囲を広げるものである。

ＲＦＩＤシステム（ハードウエア、ソフトウエ

アおよび作られたデータ）の互換性は、一連の規格統一の成果である。企業サイドからは、ＲＦＩＤシステムの互換性は評価されている。まさに、持続性あるビジネスモデルであるために、小売業者は、タグを読み取るリーダーがそれをつくった製造業者により違っているようなことは避けられなければならない。データ保護の視点からは、互換性は、技術的にデータの質を高め、それによって、データ保護指令第６条１項の遵守にもつなげることができる。ところが、その一方で、ＲＦＩＤの互換性は、適切な措置が講じられなければ、データ保護にマイナスの副作用が伴う可能性がある。例えば、指令に謳われた目的限定の原則を適用し、規制をかけることは難しくするかも知れない。また、プライバシー面から求められるアクセス権の管理も、数多くのデータを操作できる要因が増すことから、きわめて重い課題となってくるかも知れない。

５．２　ＲＦＩＤの所在通知、可視性および作動状態に関する技術的・組織的な措置

第４章で触れたように、ＲＦＩＤ技術の使用者は、データ主体に対し、データ処理の目的やＲＦＩＤ装置の所在に加え、次のようなことを通知するように求められる。

第一に、個人はＲＦＩＤまたはそれに反応するＲＦＩＤリーダー（読取機）の所在を知らされなければならない。世界標準になる方向にある絵文字標識その他この目的達成のための通知手段が必要なことは明らかである。こうしたタイプの通知手段は、ＲＦＩＤ技術を用いた違法かつ秘密の個人情報の収集を防ぐためにも必要である。例えば、店舗ないし病院がリーダーを作動させていたとする。この場合には、個人にその旨を通知しなければならない。

第二に、前記と同様な理由から、（個人データの秘密収集を防ぐために）個人を取り巻くところ（例えば、衣類や物品）にあるＲＦＩＤの所在の表示が、もう一つの要件となる。これは、ＲＦＩＤの大きさから、ほとんど目に付かないようにできるからである。この要件を充足するための方法は、さまざま考えられる。標準的な通知によることもできるし、また、技術的な対応も可能である。

第三に、現実には、ＲＦＩＤの所在の通知だけでは不十分であろう。したがって、ＲＦＩＤの機能または同時始動についても、データ保護指令の下で個人になされるべき通知の一部である。したがって、機能または稼動状態について見やすい表示をする手段も必要である。また、置かれた環境に応じて、ＰＥＴ技術（例えば、暫定的停止、タグ除去機能など）を用いることや組織的な措置を講じることは、ある程度この通知を簡素化できる。

２９条作業部会は、あらゆる当事者がこれら三つの通知に関する課題について、引き続き、さらに研究・開発をする必要があることを強調しておきたい。

５．３　アクセス権、修正権および削除権の行使のための技術的・組織的措置

あとで述べるように、ＲＦＩＤ技術の構築の仕方によっては、データ保護指令第１２条で付与されているアクセス権、修正権および削除権の行使を大きく実効あるものにすることができる。

ａ）タグ内容へのアクセス（データ保護指令第１２条ａ号）

技術的には本質的なことであるが、ＲＦＩＤタグ・コンテント〔内容〕にアクセスするには、その人の方向に反応するタグプロトコルとディスプレイの付いたリーダー（読取機）が必要となる。複雑なアプリケーション（応用ソフト）でない場合、完ぺきなＩＴの応用環境においては、タグに挿入された記号の識別子だけでもってアクセスが可能である。思うに、ごく限られた記号情報（客体、データ管理者の身元、データ収集目的などの記述など）を搭載したＲＦＩＤタグであったとしても、個人によるコンテントへのアクセスに関する問題を引き起こす。

こうした情報へのアクセスを可能にする一つの方法は、ＸＭＬに使われている記号の規格を定義することである。どのような型式をとっていようとも、こうした記号の記述は、第三者による違法なアクセス問題を引き起こす。（第３章参照）

ｂ）内容の修正（データ保護指令第１２条ｂ号）

コンテント（内容）へのアクセスの場合とは異なり、修正の場合には、その人にコンテントの読取と修正をモニターできるタグプロトコルと互換性のあるＩＴシステムに反応するリーダー（読取機）が必要になる。

考えられる一つの可能性は、タグの中に連番を消去もしくはスクランブル（信号の暗号化）をか

ける機能および限られた種類・型式項目の記載の全部もしくは一部のみを利用できる機能を埋め込むことである。（違ったプライバシー問題への対応においては、逆のやり方も可能である。）

ｃ）内容の削除（データ保護指令第１２条ｂ項）

タグに遮断機能を付け、そのタグがリーダー（読取機）の射程内に入ったときに、個人データ処理の適法性を根拠に、個人に対し、その個人のデータの処理を停止することを認めるべきなのであろうか。こうした機能は、パスポートに埋め込まれたＲＦＩＤタグのケースでは合理的といえないように見える。一方、消費者向け製品に装着されたＲＦＩＤタグの場合には、データ保護の観点から見ると、必要といえる。この問題は、ＲＦＩＤに関するシドニー宣言に表されたように、データ保護とプライバシーコミッショナーに関するシドニー会議において検討された。

ここ数年において、さまざまな解決策が発表された。一つは、「殺人」命令（「キル」コマンド）と呼ばれる手法の導入である。これは、「殺人」命令を発すれば、タグを永久にあるいは一時的に反応を停止することができるものである。永久停止は、ヒューズの作用、タグのメモリーにスクランブル（暗号化）をかけるまたはタグを取り外すことで行うことができる。一時停止は、技術的にまたはソフトウェアロックをかけることにより行うことができる。この方法に関する問題は、店舗の外部でＲＦＩＤ機能を再利用することの利点を失うことである。したがって、他の方法が提案されている。

これは誇張であり、ＲＦＩＤタグの蓄積されたデータはゼロになることはない、という違った見方がある。タグはそれでも反応するが、ただ、照会した場合に、番号の代わりにゼロの連番を応答してくる。これは、本当にＲＦＩＤの機能を遮断するわけではない。タグは、それでもなお反応しかつタグの付いた物品を持っている人の情報を、次のような形で伝達してくる。第一に、ゼロの連番だけで応答してくるＲＦＩＤタグばかりではない。タグが存在しているというだけでも重要な情報である。その人は、店からタグの付いた物品を何か買ったということ示している。名の知れた会社ならば、知性のある推測が可能である。第二に、まず、ＲＦＩＤタグは高価な物品に利用することができる。数年にわたり、単なるＲＦＩＤタグの存在は、（例えゼロの連番あるいは価値のないデータの応答をしてくるだけであっても）、窃盗犯にとっては、クロークないし駐車場に盗む価値のある物品を探し出すのに助けになるであろう。最後に、ＲＦＩＤタグは次第に増えてきているので、店舗は、リーダー（読取機）の照会に応答してくるが、ごみのようなデータを送信してくるタグはいらないと思うかも知れない。

他にタグに物理的な覆いをかけてしまう方法がある。この方法は、買物客が故意に行うことができる。例えば、財布に覆いをかけて使えば、タグが装着された銀行小切手は探知されることはない。また、アルミ箔で覆われたＲＦＩＤパスポート用カバーがあれば、パスポートを開かない限り、パスポートの内容を保護するに十分である。もっとも、覆いは、すべての場合のＲＦＩＤアプリケーションに適しているわけではない。例えば、タグのたくさん付いた衣服は、それを着ている時に覆いになる資材で覆うことはできない。また、この方法は、個人に不当に重い負担を課すようにみえる。なぜならば、タグの情報漏れを防ぐことについて最終的に個人が責任を負わされることになるからである。

これらのことに加え、タグの機能遮断の仕組みがどのようになるべきかについて検討するにあたり、ＲＦＩＤ技術の標準化団体、製造業者および使用者は、個人がタグの取り外しを選択したとしても、いかなる意味においても処罰されることのないように配慮すべきである。

なお、ここで、２９条作業部会は、あらゆる当事者がこれらの課題について、引き続き、さらに研究・開発を重ねる必要があることを強調しておきたい。

５．４　処理する場合の法的根拠

・タグ機能遮断機～５．３で触れたタグ機能遮断機の必要性に加え、データ保護指令の他の規定は、この機能（タグの遮断機能）があることを求めている。データ保護指令の下においては、本人の同意のあることがＲＦＩＤ技術を用いた個人データの収集を認める唯一の法的根拠である（本稿４．２参照）。このため、個人は、いつでも個人データ処理にかかる同意を撤回することができる（第７条ａ号）。個人は、タグに機能を遮断できる装置が付いていない場合には、自分の情報を引き続いて提供したくないとしても、同意を撤回する自己の権利を行使することができない。ＲＦＩＤタグに搭載された個人情報が、同意以外の法的

根拠に基いて提供・収集されている場合であっても、必ずしもＲＦＩＤタグに機能遮断機のような装置が必要というわけでなない。例えば、雇用関係において、働きぶりをモニターするために使われているタグ搭載個人情報は、データ処理がその雇用関係の範囲内で行われている限りにおいてタグ機能遮断機を搭載する必要はないように思われる。

ＲＦＩＤアプリケーションの種類にもよるが、例えば個人がデータ処理に関する同意を撤回するもしくはそれに反対する権利およびタグ機能を遮断する権利を有しているとする。この場合には、ＲＦＩＤ技術の製造業者および使用者は、タグの機能の遮断を容易に操作できるようにすべきである。言い換えると、データ主体が簡単にタグの機能を遮断できるようにすべきである。

５．５　データの安全性

・<u>タグおよびＲＦＩＤアプリケーションへの暗号利用</u>～ＲＦＩＤタグに個人データを搭載しているとする。この場合、データ保護指令第１７条によると、そのタグには、データの違法な開示を防ぐための技術的な措置を搭載していなければならない。こうした措置が付いていないときには、リーダー（読取機）を持った者は、タグを「起こして」、そのタグに搭載されている情報を入手することができる。こうした措置は、データ保護指令第６条１項ｄ号の下において、データの清廉性を補償し、それによって、違法な書換えを防ぐためにも必要とされる。

どのタイプの技術的な措置がいいのかは、データの性質にもよる。後にさらに検討するように、ほとんどのタグにおいては、リーダー（読取機）を持った第三者による情報の読取を防ぐために、データの暗号処理やリーダー認証を求めることができる。ＲＦＩＤのラベルに患者の身元、担当の医師および病院スタッフが世話をする手順が入っている状況を想定するとします。この場合、こうした情報がリーダーを持った第三者に読み取られないようにするために、それを防止する暗号のような技術的な措置を講じるのは、病院の義務であることは容易に理解できる。

最も一般的かつ安全な方法は、標準的な認証プロトコル（手続）を使うことである（例えば、ＩＳＯ／ＩＥＣ９７９８）。これらは、すでに、各種ネットワークやＩＣカードで広く使われている。これら標準的なプロトコルにおいては、サイプトグラフィック・プリミティブ（暗号要素）が使われる。共通鍵暗号方式、つまり送り手（暗号化）と受け手が（解読に）同じ鍵を使う方式、においては、メッセージ認証コード（ＭＡＣｓ＝Message Authentication Methods）、共通暗号アルゴリズム（例えば、データ暗号規格《ＤＥＳ＝Data Encryption Standard》、先端暗号化規格《ＡＥＳ＝Advanced Encryption Standard》）が使われる。また、非対称鍵暗号方式、つまり各当事者がそれぞれ公開鍵、秘密鍵を持つ方式、においては、非対称暗号アルゴリズム（例えば、ＲＳＡ、ＥＣＣ）または署名スキームが使われる。

いくつかの暗号認証方式は、すでに車輌の起動停止装置あるいはアクセス制御システムで実用化されている。これらには、しばしば専売のアルゴリズムが使われている。これは、標準的なアルゴリズムよりも操作が容易でありかつそれほど高価でないためである。ただ、センシティブなデータを保護するに必要な安全性を確保するためには標準的なアルゴリズムを使うべきである。こうしたプロトコルやアルゴリズムを使うことの利点は、これらがすでに幅広く使われていること、したがって、多くの当事者によりテストされかつ活用されてきていることである。このため、現在、幅広くその安全性が証明されている。

すでに、共通アルゴリズム（例えばＡＥＳ）はＲＦＩＤタグに適している記事を載せた出版物がある。共通暗号アルゴリズムを使うことの問題点は、鍵（キー）の設定と鍵の管理が複雑なことである。非対称暗号アルゴリズム方式では、この問題を避けることができる。ただ、問題は、非対称方式は共通方式に比べ高価なことである。

６．むすび

ＲＦＩＤ技術は、多様な目的での利用やさまざまなアプリケーションに使われてきている。その一部では厳正なデータ保護措置が講じられてきている。本作業部会は、現時点において、この作業部会報告書を刊行することは重要であり、これによりＲＦＩＤ問題についての継続的な検討に資することができると考えた。本作業部会は、この報告書の内容はＲＦＩＤに関する議論に貢献し、また、利害関係者に対してはこの報告書に挙げられた諸原則に従うように望みたい。

この作業部会報告書は、入手可能な情報を基

に、ＲＦＩＤ技術の発展状態、とりわけさまざまな部門でのこの技術の応用の現状を精査した上で、整理したものである。本作業部会は、引き続き発展しているＲＦＩＤの使用に注目している。この分野は絶え間なく発展しており、したがって、より多くの経験が得られれば、検討中の課題についてもより多くの英知がえられる。このことから、本作業部会は、利害関係を有する当事者と協力して、引き続きこの分野における技術的な発展をモニターしたい。この作業部会報告書に関しては問題が出てくるであろうことから、得られる経験を基に必要に応じて改訂をして行きたい。さらに、ＲＦＩＤ技術とそのアプリケーションの進展しだいでは、今後、本作業部会は、その特別な分野・アプリケーション向けの補完的な手引書を提供することにより、特定の分野・アプリケーションに絞ってより詳細な検討を行うことも考えている。

付録～ＲＦＩＤ技術　〔邦訳は省略〕

２００５年1月１９日、ブルッセルの夕暮れ時に
作業部会　会長　ピーター・シャール

No. 1

最新のプライバシーニュースを点検する

≪ひ弱なわが国のプライバシー保護環境の実態≫

個人情報保護法に便乗、企業が従業員に責任転嫁する傾向強まる

── 自民党のどさくさ便乗立法を注意深く監視しよう！

CNNニューズ編集部

個人情報保護法が、この４月から全面実施され、企業が、顧客情報などの取り扱いにかなり神経質になってきている傾向がうかがえる。この新法は、個人情報を扱う〝事業者〟を規制するのが主な目的であり、情報を漏らした個人への罰則規定は置かれていない。こうした法制ではゆるすぎる。民間独自の視点から補強が必要と称して、企業が、個人情報を取り扱っていない従業員からも情報漏えいをしない旨の誓約書ないし同意書を取り、責任転嫁する傾向が強まり、問題となっている。ちなみに、この新法の実施に便乗し、従業員に無理やり制約ないし同意を求めた項目には、個人情報と関係がない企業の財務情報などが含まれているほか、漏えいした場合、個々の従業員に損害賠償を求めるものもあるという。しかし、これは、「あらかじめ損害賠償を決めた契約は無効とする」労働基準法に違反するのは明らかだ。

こうした企業サイドのデマンドに呼応するかのように、自民党の「情報漏えい罪検討プロジェクトチーム」（事務局長・平井卓也衆議院議員）は、企業で取り扱う情報を漏えいした従業員などを処罰できるようにする提案をまとめた。その骨子は、従業員や退職者、データ処理委託先の従業員らを対象に「不当利用防止の義務規定」を新設。本人や第三者の不正な利益を図る目的で情報を漏らした場合には、１年以下の懲役または５０万円以下の罰金を科すというもの。内実は、〝社畜〟への企業情報漏えい責任転嫁立法、内部通報者お仕置き立法としても機能しそうな危ない提案。この提案を、個人情報保護法に盛り込むつもりなのか、刑事法の改正として実現するつもりなのか、今ひとつ定かではない。

すでに触れたように、個人情報保護法では、過去６ヶ月間に５，０００件を超える個人情報をデータベース化している事業者を規制対象にし、情報の利用目的や第三者への提供の制限などを義務付けている。しかし、従業員などが自分のパソコンなどに顧客データなどを入力した後に漏らした場合は処罰の対象にならない。現行法はあくまで事業者が従業員や委託先を監督するよう求めているに過ぎないからだ。これでは、生ぬるいという声もあるかもしれない。

ただ、自民党が新設を狙っている「不当利用防止の義務規定」の処罰のターゲットに、個人情報と関係がない企業の財務情報なども含まれているとすれば、これを、個人情報保護法の改正に盛り込むのは完全筋違い、悪乗り。従業員の人権弾圧立法であることはもちろんのこと、法律の便乗改悪そのものだ。自民党の立法活動を私たち市民が注意深く監視する必要がある。

No. 2

最新のプライバシーニュースを点検する

≪ひ弱なイギリスのプライバシー保護環境の実態≫

英労働党勝利で、どうなる「生体認証国民総ＩＣカード制」導入の〝悪夢〟の行方

CNNニューズ編集部

労働党は、先（２００５年5月5日投票）の総選挙で議席を大幅に減らしたものの、勝利した。5月１７日に、エリザベス女王は、貴族院で国会の開会を宣言、３期目のブレア政権の当面の施政方針を示した。イギリスでは、女王が国会の会期冒頭で演説をし、政権の施政方針を代読するのが伝統。女王の演説では、焦点になっている生体認証型国民総ＩＣカード制（ＩＤカード法案）を含む治安対策法案、熟練移民を優遇する移民対策法案など、ブレア政権が２００６年１１月までの会期中に審議を予定している５０法案のリストを提示した。

テロリスト裁判には伝統的な対審手続や証拠原則を使わないとする提案などは取り下げられ、今国会での審議法案リストからは外された。しかし、昨年提案され、与党労働党内からも異論がでて審議が一時棚上げされていたＩＤカード法案は、再び今国会に提出された（ＩＤカード法案について詳しくはＣＮＮニューズ４１号参照）。

野党保守党の影の内閣デイビス内相は、ＩＤカード法案賛否に優柔不断な態度を取り続けている党首に見切りをつけて、下院では同法案に反対することを決めた。今回の総選挙で議席を減らした与党労働党は、党内に同法案に異論を唱える造反議員を抱えており、法案通過は余り楽観視できない状況にある。

一方、反ＩＤカード法案運動の連合体「ＮＯ２ＩＤ」傘下の各団体は、体勢を整え、同法案の廃止に向けた運動の拡大・強化に入った。

ブレア政権の生体認証情報を含め幅広い国民の個人情報を国家管理する「絶望国家」づくりは絶対にストップさせなければならない。いったんこんな仕組みの導入を許したら、なりすまし、偽造カード、カード盗難等々、警察にとっても〝カード犯罪対策〟が重荷になるのは必至だ。ともかく、こんな「メイド・イン・イングランド」の監視システムが輸出されたら、他国の国民はたまらない。

それにしても、ブレア政権が出した生体認証式ＩＤカード制のような人権感覚を疑う政策は、ドイツやフランスなど大陸諸国からは出てこない。

ところが、島国のイギリスでは、監視カメラ、生体認証ＩＣカード等々、〝電子監視収容所列島化〟政策が目白押しの状況だ。悲しいかな、この東洋の島国にも、こんな「メイド・イン・イングランド」の監視システムを真似ようとする御用学者や、この連中を笑みを浮かべながら操っている役人がわんさいる。当然、わが国でも、住基ＩＣカードを生体認証型に移行するから、全国民に、指紋を出せ、人相を撮らせろ、目の虹彩を撮らせろ、と役人が騒ぎ出す〝悪夢〟が危惧される。対岸の火事といって座視してはいられない。

第１０回ＰＩＪ定時総会のご報告

プライバシー・インターナショナル・ジャパン事務局

PIJの第１０回定時総会が、さる２００５年5月7日（土）、東京・池袋の豊島勤労福祉会館において、第一部定時総会、第二部　講演のかたちで、次のとおり開催されました。定時総会では、すべての案件が承認されました。

PIJ　第１０回定時総会

２００５年5月7日（土）

於　豊島区立勤労福祉会館

第一部　定時総会

一、開会宣言　司会者

一、議長選任

一、議事

第１号議案　２００４年度活動報告承認の件

第２号議案　２００４年度収支報告並びに財産目録承認の件

第３号議案　２００５年度活動計画承認の件

第４号議案　２００５年度収支予算案承認の件

一、報告

役員に関する報告（今回は改選なし）

《代　表》

石村耕治（白鴎大学教授）

《副代表》

辻村祥造（税理士）

加藤政也（司法書士）

《常任運営委員》

我妻憲利（税理士《事務局長》）

高橋正美（税理士《編集長》）

益子良一（税理士）

平野信吾（税理士）

白石　孝（自治体職員）

勝又和彦（税理士）

加藤　弘（税理士）

中村克己（会社役員《副編集長》）

《相談役》

河村たかし（衆議院議員）

一、閉会宣言　司会者

第二部　記念講演

生体認証型ＩＣカード普及に潜むワナ

講　師　石村耕治（PIJ代表・白鴎大学教授）

PIJ活動状況報告書（２００４年４月～２００５年３月）　PIJ事務局作成

年　月　日	活　動　報　告　内　容	場所・掲載紙（誌）等	参加担当
０４．４．３	朝日新聞「ＮＰＯ課税取消請求棄却」判決へのコメント	朝日新聞朝刊	石村代表
０４．４．６	住基ネットについて国立市長との打ち合わせ	国立市役所	石村代表
０４．４．２７	公益法人制度改革についての公法協との打ち合わせ	公法協	石村代表
０４．４．２８	朝日新聞「公益法人改革」へのコメント	朝日新聞朝刊	石村代表
０４．４．３０	新宗連・勉強会～公益法人制度改革と宗教法人への影響	東京・新宗連会館	石村代表
０４．５．１４	東京税理士会税制審議部講演～公益法人制度改革	東京税理士会	石村代表
０４．５．１５	PIJ・２００４年定時総会	東京・豊島勤労福祉会館	PIJ役員
０４．６．４	宗教法人法制と税制に関する研究会（宗法税研）出席	東京・新宗連会館	石村代表
０４．６．１０	朝日新聞〔関西版〕「堺市、住基ネット、契約切れ後も運用」へのコメント	朝日新聞朝刊	石村代表
０４．７．９	宗法税研、研究例会出席	東京・新宗連会館	石村代表
０４．７．１０	コラム～住民が監視できる監視カメラの仕組みを	月刊誌ｅ－ｇｏｖ７月号	石村代表
０４．７．２３	都宗連、打ち合わせ	東京・上野	石村代表
０４．７．２８	International Herald Tribune=ＩＨＴ〔英字紙〕～Time to talk about political-religious ties	ＩＨＴ	石村代表
０４．７．３０	岐阜税研～住基ネットを使わない電子申告・電子申請	岐阜・グランヴェールク岐山	石村代表
０４．７．３１	河村たかし後援会出席・講演～住基ネットを使わない電子申告	名古屋・逓信会館	石村代表
０４．８．６	宗法税研、研究例会出席	東京・新宗連会館	石村代表
０４．８．１８	PIJ運営委員会	PIJ事務局	PIJ役員
０４．９．１３	宗法税研、研究例会出席	名古屋・グランドホテル	石村代表
０４．１０．１４	全互職講演～公益法人制度改革	東京・フロラシオン青山	石村代表

PIJ活動状況報告書（２００４年４月～２００５年３月）～続き～　PIJ事務局作成

年　月　日	活　動　報　告　内　容	場所・掲載紙（誌）等	参加担当
０４．１０．２１	公法協・公益法人制度改革に関する会議出席	東京・銀行倶楽部	石村代表
０４．１０．２９	九州弁護士会シンポ・基調講演 ～監視カメラとプライバシー	北九州市・ リーガロイヤル・ホテル	石村代表
０４．１１．５	都宗連・宗教法人管理者研修講演 ～公益法人制度改革	東京・関口会館	石村代表
０４．１１．６	小山市市民講座～納税者番号制とは何か	栃木・小山市	石村代表
０４．１１．１１	宗法税研、研究例会出席	東京・新宗連会館	石村代表
０４．１１．１５	公益法人制度改革に関するインタビュー・週刊誌	白鴎大学	石村代表
０４．１１．１９	岐阜税研～金融一体化課税と選択的納番制	岐阜・グランヴェールク岐山	石村代表
０４．１２．９	中国新聞１２月９日インタビュー記事～監視カメラ	中国新聞朝刊	石村代表
０４．１２．１７	立正佼成会幹部学習会～公益法人制度改革	東京・立正佼成会	石村代表
０５．１．２０	宗法税研・最終報告書発行・記念講演	東京・新宗連会館	石村代表
０５．２．６	全仏顧問弁護士連絡会例会講演～公益法人制度改革	京都・西本願寺	石村代表
０５．２．７	立命館大学生団体勉強会講演～監視カメラ規制	京都・立命館大	石村代表
０５．２．８	新宗連総会講演 ～公益法人制度改革の宗教法人への影響	東京・妙智会教団	石村代表
０５．３．１０	日宗連：宗教法人と税制シンポ講演	東京・立正佼成会	石村代表
０５．３．２５	岐阜税研～個人情報保護法と税理士事務所の対応	岐阜・グランヴェールｸ 岐山	石村代表
０５．３．２９	民主党ＮＰＯ・公益法人改革ＰＴでの意見陳述	東京・第２議員会館	石村代表
０５．３．３０	名古屋税研～個人情報保護法と税理士事務所の対応	名古屋・グランドホテル	石村代表
０５．３．３１	PIJ運営委員会	PIJ事務局	PIJ役員

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・髙橋正美
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
2005.7.1発行 CNNニューズNo.42

入会のご案内

季刊・CNNニューズは、PIJの会員（年間費1万円）の方にだけお送りしています。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
ピー・アイ・ジェー（PIJ）

NetWorkのつぶやき

・政府税調が「長者番付」の公表を、廃止を含めて見直すことにしたという。当り前である。この国が資本主義の道を歩んでいるというなら、金持ちのプライバシーを護らないような政策はやめて当然だ。問題は、政治家、高級官僚など「公人」の資産公開制度の〝精度アップ〟をどうするかである。（N）