

CNNニュース

No.99

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

■ 巻頭言 ■

待ったなし！！ 生体認証監視技術の法規制

—— 市民監視技術の利用拡大に危機感のない政治家は要らない！！ ——

東京オリンピック・パラリンピックでは、セキュリティ対策として、顔認証技術を積極的に活用するという。凶悪な犯罪が起きると、マスメディアが、その道の専門家と称する人たちと一体となって、監視カメラや顔認証技術の有用性を煽る。市民の中にも、あきらめの空気が蔓延している。だが、生体認証情報は、唯一無二の生物的特徴で、個人の最もセンシティブな情報である。漏れても変えられない。軽率に取り扱うことは、深刻な人権問題になりかねない。特別の法規制が要る。

米マイクロソフト社は、iPhoneに顔認証技術を使う。その一方で、この技術の法規制を求めている。昨年(2018年)12月6日、同社のブラッド・スミス(Brad Smith)社長は、首都ワシントンD.C.にあるシンクタンク、ブルッキングス研究所で講演した。そこで、監視国家の誕生を防ぐため、顔認証技術への法規制を呼び掛けた。

2019年5月14日、米カリフォルニア州サンフランシスコ市議会は、顔認証技術を行政機関や警察が利用するのを禁止する条例「秘密監視規制条例」案を可決した。この条例は、2016年9月に米自由人権協会(ACLU)が打ち出した「警察監視をコミュニティが監視する(CCOPS)プロジェクトを実現に導いたもの。こうした地方団体、さらには州レベルでの顔認証技術利用に法

規制をかける動きは全米に広がりを見せている。

イギリスは、監視カメラ(CCTV)大国として名を馳せた。だが、現在、転換期にある。プライバシーを保護し自由や人権を護る活動している市民団体「ビッグブラザーウォッチ(Big Brother Watch)」などが、顔認証のような生体情報の警察利用に法規制をかける運動を展開。今年5月1日には、英議会下院で「顔認証と生体認証戦略」と題し、ダレン・ジョーンズ議員(労働党)が発案し、法規制に向けた討議(debate)が始まった。労働党は、かつて生体認証式国民IDカードや国家DNAデータベースの導入に途を拓いた前科もある。市民団体は、この政党の平等優先・自由権軽視の制度のせん滅に苦勞した(「イギリス、国民IDカード制を廃止へ」CNNニュース64号)。しかし、市民団体も労働党も、イギリスを、中国の「天網」のような顔認証システムで国中を覆いつくすデータ国家主義には反対である。

AIを応用した顔認証式のライブ監視カメラで街中を埋め尽くすことで、犯罪の後追いは容易になる。だが、根絶は難しい。単純に先端技術だけで犯罪根絶はできない。先端技術の利用自体が社会の信頼関係を壊していないのか精査が要る。

わが国の自由とか民主とかを看板にする政党が、国民の背番号管理を推進し、市民監視技術の法規制の声を上げないのは異様だ。この国の政治家の人権感覚が問われている。

◆ 主な記事 ◆

- ・ 巻頭言～待ったなし！生体認証監視技術の法規制
- ・ 米イリノイ州生体認証情報プライバシー法を読む
- ・ マイクロソフト社スミス社長の講演のポイント紹介
- ・ 顔認証技術の市民的コントロールを考える
- ・ アメリカ自治体の顔認証技術規制条例

2019年10月10日

PIJ代表 石村 耕治

石村耕治 PIJ 代表に聞く

米イリノイ州生体認証情報プライバシー法（BIPA）を読む

—— 日米の生体認証情報規制の法的枠組み比較 ——

解説 石村 耕治（PIJ代表）

聞き手 中村 克己（CNN ニュース編集局長）

テーマパークを経営する大阪のユニバーサル・スタジオ・ジャパン（USJ）は、早くから年間パスを購入した消費者の入場ゲート管理に顔認証技術を活用している。

マイクロソフト社のOSである「Windows 10」では、PC アクセス権限者によるログインを、パスワード認証から顔・虹彩・指紋のような生体認証に変更するオプション（Windows Hello）が示されている。

富士通は2018年1月に、国内約8万人の社員を対象に、仮想デスクトップへのログインを、これまでのパスワード認証から手のひら静脈認証に切り替えていくと発表した。さらに、2拠点の事業所に（社員約5,200人）において入退場ゲートの認証に手のひら静脈を使う実証実験を開始するとした。わが国の「社畜」を育成する企業風土では、プライバシー意識の高い従業員が勤務先に生体認証情報の提供を拒否し続けることは雇用からの排除につながるのではないかと懸念されている。生体認証情報の提供を求めるにあたっては、事前に情報主体に利用目的を通知し、生体認証情報を収集する本人の同意を得ていること（オプト・イン）を義務化し、かつ同意しないことを理由に差別することを法で禁止し、人権を護る必要がある。

個人情報保護法では、第2条「個人情報」の定義において、個人情報の1つとして、第2項で「個人識別符号」をあげている。そのうえで個人識別符号の1つとして第1号で特定個人を識別することができる「身体の一部の特徴」をあげている。したがって、生体認証情報（または個人情報識別子）を取り扱う事業者は、個人情報保護法の規制を受ける。ただ、わが国の法制では、生体認証情報とこれ以外の個人識別符号とを同列で取り扱い、差別化して前者を厳しく規制していないことである。

生体認証情報である指紋はもちろんのこと、目の虹彩や顔面などは、人の唯一無二の生物的特徴で、個人の最もセンシティブな情報である。運転免許番号や身分証明書番号、個人番号（マイナンバー）、その他各種パスワードなどは、紛失したり、悪用されたとしても、変更することができる。ところが、生体認証情報は、漏れても変更ができない。双方を同列に扱うのは危険である。生体認証情報を軽率に取り扱うことは、きわめて深刻な人権問題につながりかねない。

アメリカでも、多くのIT企業が、生体認証の開発・販売にしのぎを削っている。その一方で、米フェイスブック社（Facebook）や米グーグル社（Google）のような生体認証技術を開発・利用・販売するIT企業、その技術を活用する民間企業は、次々とプライバシー侵害を理由に訴訟に巻き込まれるケースが増えてきている。

現在、連邦レベルでは、顔面、指紋、手の甲の静脈のような生体認証情報（識別子／符号）の取扱いについては、13歳以下の子どもの情報を除き、法的規制措置は講じられていない。一方、州レベルでもわずか3州が規制法を制定・施行しているだけである。そのなかでも、イリノイ州だけが、同州の生体認証情報プライバシー法（BIPA= Biometric Information Privacy Act）に民間企業が違反して生体認証情報の取扱いをした場合に、被害者は直接その企業を訴え、損害賠償を求めることができるとする法制を維持している。一方、イリノイ州法（BIPA）以外の他の州法（テキサス州法やワシントン州法）では、法を遵守しなかったことを理由に権利を侵害された情報主体（消費者や従業員など）が、直接民間企業を相手に訴訟を起こすことを認めていない。これらの州では、州司法長官（state attorney general）が住民を代理して訴訟する方式を採用している。

からである。このため、生体情報あるいは生体情報識別子、とくに顔面データの違法な取扱いをめぐるフェイスブック社（Facebook）、グーグル社（Google）、シャッターフライ社（Shutterfly）、スナップチャット社（SnapChat）など、英語では「テック・ジャイアント（tech giants）」と呼ばれる「ネット巨人」に対する消費者（ユーザー）による訴訟は、イリノイ州生体認証情報プライバシー法（BIPA）に準拠して、全米各所の連邦裁判所またはイリノイ州裁判所に起こされている。イリノイ州のBIPAを苦々しく思っているIT業界は、BIPAを骨抜きにするための法改正のためのロビーイング（政治的働きかけ）を州議会に強めている。とりわけ、フェイスブック社は、顔認証技術（FRT）の規制に反対するために、連邦議会や規制法を制定しているあるいは制定しようとしている州議会へ巨額の資金を使って法案成立

阻止に向けてロビー活動を展開している。

フェイスブック社とは異なり、マイクロソフト社のスミス社長（CEO）は、顔認証技術（FRT）の濫用や不適正な利用による偏見や差別を禁止し、プライバシーを含む自由権を護るためには、一定の法規制が必要であるというスタンスにある。まさに、マイクロソフト社は、フェイスブック社とは、対照的な経営姿勢である。

今回は、石村耕治 PIJ 代表に、CNN ニュース編集局中村克己が質問をする形で、わが国の生体認証データの法規制の仕組み、それからアメリカにおける顔認証技術（FRT）の取扱いをめぐる訴訟の動きを含め生体認証データ保護のための法規制の仕組みについて紹介していただいた。

（CNNニュース編集局）

■なぜ生体認証の利用は慎重にしないといけないのか

—— オンライン決済、PC のログイン、消費者の入場ゲート管理、労務管理などに生体認証技術の利用が広がっています。その一方で、プライバシーなど人権を護るために、生体認証を安易に利用することには慎重な対応が必要だとする意見もありますが。

（石村）運転免許番号や身分証明書番号、個人番号（マイナンバー）、金融取引や電子取引に使う各種パスワードなどは、紛失したり、悪用されたとしても、変更することができます。ところが各個人の生体認証情報である指紋、目の虹彩や顔面などは、生涯変更することができません。唯一無二の生物的特徴だからです。また、個人の最もセンシティブな情報です。それに、双方を同列に扱うのは危ないわけです。

【図表 1】可変&不変の個人識別符号（識別子）の違い



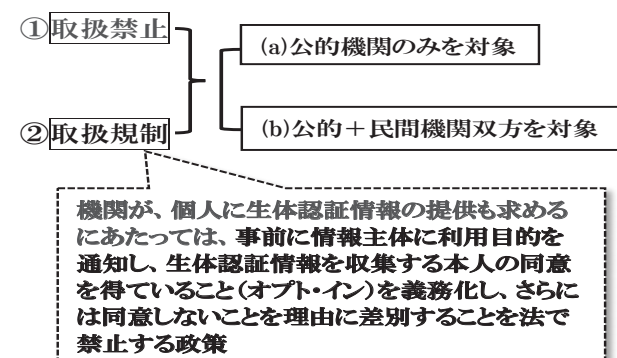
ですから、精度や利便性が高く、安価であるからといって、生体認証情報を軽率に取り扱ってはいけないわけです。きわめて深刻な人権問題につながる危険性が高いわけです。にもかかわらず、生体認証技術が、消費者の入場ゲート管理や顧客の入退店、PC のログイン、タイムカードや入退室

を含む幅広い労務管理などに広がっています。生体認証技術の利用の禁止を含む、抜本的な政策の見直しが必要です。

—— 生体認証情報の規制をめぐるのは、どのような政策的な選択が考えられますか？

（石村）いくつかの選択が考えられます。1つは、公的機関や民間機関での本人確認目的での生体認証情報の取扱いを禁止する政策です。この場合、公的機関での取扱いを禁止するやり方と、民間機関を含めて禁止するやり方が考えられます。もう1つは、公的機関や民間機関での本人確認目的での生体認証情報の取扱いを法認するけれども、個人に生体認証情報の提供も求めるにあたっては、事前に情報主体に利用目的を通知し、生体認証情報を収集する本人の同意を得ていること（オプト・イン）を義務化し、さらには同意しないことを理由に差別することを法で禁止する政策です。

【図表 2】生体認証情報の規制をめぐる政策の選択



■わが国の生体認証データの法規制の仕組み —— わが国では、生体認証データに法規制をかけているのですか？

(石村) わが国では、個人情報保護法で民間の個人情報取扱生体認証情報について、一応規制をかけています。まず、生体認証情報に特化する形で、わが国の個人情報保護法上の取扱いについて説明をします。

個人情報保護法は、第2条「個人情報」の定義において、個人情報の1つとして、第2項で「個人識別符号」をあげています。そのうえで個人識別符号の1つとして第1号で特定個人を識別することができる「身体の一部の特徴」をあげています。したがって、生体認証情報（または個人情報識別子）を取り扱う事業者は、個人情報保護法の規制を受けます。ただ、わが国の法制では、生体認証情報とこれ以外の個人識別符号とを同列で取り扱い、差別化して規制していないことです。

【図表3】わが法での生体認証情報の所在

わが国の個人情報保護法（日本法）
(定義) 第2条 第1項 この法律において「個人情報」とは、生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。 第1号 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の人の知覚によっては認識することができない方式をいう。次項第2号において同じ。）で作られる記録をいう。第18条第2項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。） 第2号 個人識別符号が含まれるもの 第2項 この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。 第1号 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であつて、当該特定の個人を識別することができるもの 第2号 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記

載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であつて、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

*は圏点は編集局

—— もう少し、やさしく説明してください。

(石村) わかりました。【図表3】をみてください。わが国の個人情報保護法（日本法）では、法第1項に定める「個人情報」として、氏名や生年月日のような①「特定の個人を識別することができるもの」（1項1号タイプ個人情報）と②「個人識別符号」（1項2号タイプ個人情報）とをあげています。2017年5月の法改正で、個人情報の定義が見直され、このようになりました。

この改正によって、①1項1号タイプの個人情報、実質的に、②1項2号タイプの「個人識別符号以外の個人情報」を指すことになったわけです。このことから、②「個人識別符号」とは何かが重要になってきます。

個人情報保護法第2条では、「個人識別符号」とは、生存する個人に関する情報であつて、2つのカテゴリーの「文字、番号、記号その他の符号」で、具体的には、政令で定める、としています（法2条2項1号・2号）。そこで、政令（法施行令）や省令（法施行規則）も見て、平たくいえば、②「個人識別符号」は、次の【図表4】のとおりです。

【図表4】日本法での「個人情報」、「個人識別符号」の定義

個人情報	①1項1号タイプ個人情報 ②2号タイプ以外の個人情報。つまり、氏名や生年月日など。改正法で、さらに、文書、画像などを追加
	《個人識別符号》 ②1項2号タイプ個人情報(個人識別符号)の類型 (i) 「特定の個人の身体の一部」、つまり、生体認証情報(データ)のような個人の身体的な特徴を電子処理するために変換した文字、番号、記号その他の符号。実例としては、DNA配列、顔認識データ、虹彩データ、音声データ、歩行データ、静脈データ、指紋や掌紋データ、その他これらの生体認証データを組み合わせたデータなど (ii) 個人番号(マイナンバー)、運転免許証番号、パスポート番号、基礎年金番号、保険証番号、在留カード番号など

—— 【図表4】からもわかるように、わが国の場合、「特定の個人の身体の一部」、つまり、生体認証情報を「個人情報」、「個人識別符号」として法

認していますが、法規制においても運転免許証番号やパスポート番号などと同列に取り扱っていません。アメリカの場合はどうなのでしょう？

(石村) 近年、アメリカにおける生体認証情報に関する法政策、とりわけ州や地方団体レベルでは、わが国とは異なる方向に動いてきています。つまり、生涯不変の「生体認証情報（データ）」を、変更可能な運転免許証番号やパスポート番号などと区別（差別化）して、センシティブ（要配慮）情報と同列あるいはそれ以上の情報（データ）として取り扱う法政策の実現を目指しています。

■アメリカにおける生体認証データの法規制の仕組み

—— アメリカの生体認証情報の法規制をめぐる政策の動きはわかりました。最初に、かなり初歩的なことを質問します。顔認証技術（FRT）は、指紋や目の虹彩などと同じく生体認証情報（biometric information）あるいは生体認証識別子（biometric identifier）の1つですが、アメリカには、現在、民間機関や公的機関が生体認証情報あるいは生体認証識別子の適正な取扱い、つまり、収集や利用、保存、廃棄などを規制する法律はないのでしょうか？

(石村) ないわけではありません。アメリカの法制は、大きく①連邦、②州、そして③地方団体にわけることができます。②州や③地方団体のプライバシー保護法制あるいは住民のプライバシーを保護するための先端的な生体認証情報（識別子）の利用規制は千差万別です。アバウトをいうと、次のとおりです。

【図表5】アメリカの生体認証情報（識別子）に関するプライバシー保護法制

①連邦 連邦には、EU（欧州連合）の一般データ保護法（GDPR=General Data Protection Regulation）のような公民双方の分野に共通する包括的な個人情報保護法（データ保護法）はない。アメリカのプライバシー保護法制は、わが国の個人情報保護法制のように、分野別の法制になっている。

【公的分野】

・プライバシー法（Privacy Act）（1974）【政府機関による個人情報の取扱いをおおまかに規制。ただし政府機関での生体認証情報の取扱いについては規制していない。】

【民間分野】

・子どものオンラインプライバシー保護法（COPPA=Children's Online Privacy Protection Act）（1998年）【この法律（COPPA）で、子供向け有害サイト規制が主な狙いであるが、民間ネット事業者が13歳以下

の子ども（以下、単に「子ども」という。）の生体認証情報を収集する場合には、親権者の同意を義務付けるものである。事業者は、子どもの画像、音声を含む子どもの写真を撮影する、ビデオ撮りする、音声録音をする前に親権者の明示の同意を得る必要がある。民間機関が子どもに顔認証技術（FRT）を利用する場合にも、COPPAが適用になり、親権者の同意が必要と示達されている（連邦取引委員会（FTC）の2015年11月15日通達）。

・生体認証情報（識別子）プライバシー保護法制定の動き 連邦議会には、顔認証技術、指紋、声紋などの生体認証情報を含む消費者のプライバシーを保護しようという議員立法が提出されてきている。しかし、IT業界やその支援を受けた議員などの抵抗も強く、成立にはいたっていない。主な議員立法をあげると、④2012年消費者プライバシー権利章典法案（Consumer Privacy Bill of Rights Act）、⑤2014年データ安全および漏洩通知法案（Data Security and Breach Notification Act of 2014）、⑥2014年個人データプライバシーおよび安全法案（Personal Data Privacy and Security Act of 2014）、⑦2014年個人データ保護および漏洩責任法案（Personal Data Protection and Breach Accountability Act of 2014）、⑧2015年個人データ通知および保護法案（Personal Data Notification and Protection Act of 2015）、⑨2018年のプライバシー権利章典法案（Privacy Bill of Rights Act of 2018）など

②州 アメリカ諸州の住民プライバシーの保護法制は、州により大きく異なり、千差万別である。

【民間分野】

・カルフォルニア消費者プライバシー法

（CCPA=California Consumer Privacy Act）（2018年。ただし、2020年施行）【この法律（CCPA）は、民間事業者による個人消費者の顔認証などの生体認証情報を個人情報と定義し、その取扱いを規制している。】

・イリノイ州生体認証情報プライバシー法

（BIPA=Biometric Information Privacy Act）（2008年）【この州法（BIPA）は、州レベルではじめて、民間機関の生体認証情報を取り扱う場合のルールを定めた法律である。内容的には、(i) 民間機関（私的事業体）が個人の生体認証識別子（biometric identifier／虹彩、目の網膜、指紋、顔面、手相、静脈パターンなど）を収集または第三者に提供する場合には、本人の同意を得ること（オプト・イン）を原則とすること、(ii) 生体認証情報を収集した民間機関は、安全措置を講じたうえで厳重に保存すること、(iii) 生体認証情報を収集・保存する民間機関は、法定期間または目的を達成した時は、それを廃棄することなどを骨子とする。(iv) 民間機関が、過失で違法な取扱いをした場合に、被害者は、各違反について最低で1,000ドル、故意の場合には最低で5,000ドルの損害賠償を民事訴訟で求償できる。】

・テキサス州生体認証識別子の収集または利用法

（CUBI =Texas Capture or Use of Biometric Identifier statute）（2009年）

・ワシントン州生体認証プライバシー法

（WBPA=Washington Biometric Privacy Law）（2017年）

・アラスカ州、ニューハンプシャー州、コネチカット州など他の州でも、この種の規制法の制定を検討中。

③**地方団体** カリフォルニア州サンフランシスコ市「秘密監視規制条例 (Stop Secret Surveillance Ordinance)」(2019年5月)【人工知能 (AI) を使った顔認証技術 (FRT) を地方団体内の行政機関や警察など公的分野で利用することを禁じる条例】

・全米の他の地方団体、さらには州でも、地方団体やその傘下にある自治体の公的機関が顔認証技術 (FRT) を利用することを禁止または制限する条例制定を検討中。

—— **アメリカの生体認証情報 (biometric information) あるいは生体認証識別子 (biometric identifier) に関するプライバシー保護法制について、もう少しわかりやすく説明してください。**

(石村) わかりました。【図表5】を参照しながら説明をします。連邦レベルでは、顔面、指紋、手の甲の静脈のような生体認証情報あるいは生体認証識別子の取扱いについては、13歳以下の子どもの生体認証情報を除いて、法的規制措置は講じられていません。一方、州レベルでは、イリノイ州などいくつかの州で生体認証情報に対して法規制を実施している状況です。地方団体レベルでは、CNNニュース本号 (99号・35頁) でも紹介しているように、カリフォルニア州サンフランシスコ市のように、顔認証技術 (FRT) を地方団体内の行政機関や警察が利用することを禁じる条例を制定したところもあります。また、全米で、公的機関がFRTの利用を禁止または制限する条例の制定を検討中の地方団体が増えてきています。

—— **「訴訟大国」と呼ばれるアメリカですから、当然、生体認証情報の不法な利用を問う訴訟が起こされていると思いますが？**

(石村) 生体認証情報の不法な利用について、伝統的に、被害者は不法行為 (tort) を問う民事訴訟を起こすことが可能です。ただ、生体認証情報の不法な取扱いを規制する制定法があれば、それを根拠の訴訟を起こすことができるわけです。現在、連邦レベルでは、13歳以下の子どもの生体認証情報の収集手続を除き、生体認証情報の取扱いを規制する制定法はありません。州レベルでもわずか3州が制定しているだけです。イリノイ州法 (BIPA) は、民間機関がBIPAに違反した生体認証情報の取扱いをした場合、被害者は直接違反者を訴えることができます。一方、イリノイ州法 (BIPA) を除き、他の州法 (テキサス州法 (CUBI) やワシントン州法 (WBPA)) では、法を遵守しなかったことを理由に権利を侵害された情報主体 (消費者や従業員な

ど) が、直接民間機関を相手に訴訟を起こすことを認めていません。つまり、これらの州では、州司法長官 (state attorney general) が住民を代理して訴訟する方式を採用しています。

—— **アメリカの生体認証情報の法規制では、イリノイ州法 (BIPA) が一番進んでいるとのことですが。石村代表は、イリノイ大学ロースクールを修了されていますから、イリノイの法環境には詳しいのではないかと思います。なぜ、イリノイ州が連邦や他の州に先駆けて、生体認証情報の法規制をしたのですか？**

(石村) 母校のイリノイ大学は、シカゴから100マイルほど南、イリノイ州のど真ん中にシャンペーンアバーナ (Champaign-Urbana) というツインシティ (双子の市内) にあります。大学が主な産業といった小都市です。巨大なキャンパスのある州立大学です。大学空港まであり、シカゴまで直行便が飛んでいます。入学が決まった後、当時住んでいた連邦の首都ワシントンD.C. の空港から、シカゴ経由で、戸惑いながらイリノイ大学空港に降り立ったのを今でも憶えています。その当時は、まだインターネットやパソコン (PC) が普及しておりませんでした。ロースクールの授業も黒板を使い、判例集とかもすべて紙媒体の時代でした。当時、IBM社製の電動タイプライターが、最先端の事務機のような感じでした。こうした時代でしたから、この州が、こんな先進的な立法をするとは、夢にも思っておりませんでした。

前置きはこの程度にして、イリノイ州の州都スプリングフィールド市にある州議会 (Illinois General Assembly) は、2008年に生体認証情報プライバシー法 (BIPA=Illinois Biometric Information Privacy Act) を制定しました。BIPAは、2008年10月3日に公布、直ちに施行されました。この背景には、イリノイ州で最大の指紋認証決済システム「ペイ・バイ・タッチ (Pay By Touch)」を運用していた民間企業が破産したことがあります。その破産した企業は、数多くの雑貨店、給油所、学校食堂などで指紋認証決済のパイロットプログラムを実施し、何千もの消費者の指紋、指紋認証データの行き先が危惧されました。指紋はもちろんのこと、目の虹彩や顔面などは、人の唯一無二の生物的特徴で、個人の最もセンシティブな情報です。運転免許番号や身分証明書番号、社会保障番号 (SSN)、その他各種パスワードなどは、紛失したり、悪用されたとしても、変更することができます。しかし、生体認証情報の場合には、変

更することができません。生体認証情報を軽率に取り扱うことは、きわめて深刻な人権問題につながる危険性が高いわけです。

そこで、イリノイ州議会は、生体認証情報の取扱事業者に対する生体認証情報や生体認証識別子の収集、利用、安全対策、保存、破棄についてプライバシーポリシーの公表を義務づけるなどして、制裁付き〔法律違反で損害をうけた被害者に対して賠償請求訴訟権を認める形〕で、法的規制を加えることにしたわけです。

—— 生体認証情報の法規制に特化したイリノイ州法(BIPA)について、やさしく説明してください。(石村) BIPAの概要は、次のとおりです。なお、BIPAの邦訳(仮訳)の最後も添付していますので、参考にしてください。

【図表 6】イリノイ州生体認証情報プライバシー法(BIPA)の概要

- ①法規制の対象となる「生体認証 (biometrics)」とは何か
- ・ (i) 「生体認証子 (biometric identifier)」とは、目の網膜 (retina) または虹彩 (iris) の映像、指紋 (fingerprint)、声紋 (voiceprint)、電子の手掌読取 (scan of hand)、顔認証 (face geometry など。ただし、筆跡、筆記署名、写真、人口統計データ (demographic data)、物理的記述 (physical description)、医学または学術目的で利用される生体認証資料 (biometric materials used for medical and scientific purposes) は含まない。
 - ・ (ii) 「生体認証情報 (biometric information)」とは、生体識別子に基づく情報をいう (詳しくは、BIPA 邦訳〔仮訳〕第 10 条参照)。
- ②私的事業体 (民間機関) が州居住者から生体認証を合法的収集するための要件
- ・ 私的事業体は、生体認証情報を取り扱うにあたり、保存計画、永久廃棄までの保存期間〔当初の目的が達成されたときかまたは当該個人と当該私的事業体とが最後の相互交流から 3 年以内か、いずれか早い方のときまで〕などを定めたガイドラインを明確にした成文のプライバシーポリシーを作成し公表すること (BIPA 第 15 条 a 項)。
 - ・ 生体認証情報を収集するにあたり、事前に情報主体に利用目的、収集と保存の期間を通知し、同意を得ていること (オプト・イン方式) (BIPA 第 15 条 b 項)。
 - ・ 生体認証情報は、本人が文書で同意するまたは法令等による場合を除き、原則開示できない。このことから、生体認証情報は第三者に販売することはできない (BIPA 第 15 条 c 項)。逆に、私的事業体は、生体認証情報を、少なくとも秘密の要配慮情報に対する水準またはそれ以上の注意義務をもって、保存、伝達、保護するように義務付けられる (BIPA 第 15 条 e 項 2 号)。

③訴訟権 (right of action)

- ・ この法律(BIPA)の違反により権利を侵害された者は、権利を侵害した者を相手に、イリノイ州巡回裁判所 (State circuit court) に訴訟を提起する権利または連邦地方裁判所 (federal district court) に補充的請求 (supplemental claim) をする権利がある。
- ・ 勝訴当事者は、各違反について、次の各号に掲げる者に対して権利回復ができる。
 - (1) この法律の過失により違反した私的事業体に対して、1,000 ドルの定額損害賠償かまたは実額賠償額か、いずれか大きい方の額
 - (2) この法律に故意に違反した私的事業者に対して、5,000 ドルの定額損害賠償かまたは実額賠償額か、いずれか大きい方の額
 - (3) 専門家の証言費用その他訴訟上の諸経費を含む、合理的な弁護士費用、および、
 - (4) その他、差止請求を含む州裁判所または連邦裁判所が適切とみなす救済

—— 生体認証情報をめぐる訴訟のタイプやその数などについて、簡潔に説明してください。

(石村) わかりました。この種の訴訟を類型別にやさしく説明すると、次のとおりです。

【図表 7】生体認証情報にかかわる主な訴訟タイプ

- ①ネット巨人 (tech giants) のユーザーによる訴訟
- 訴訟の多くは、グーグル社やフェイスブック社のようなネット巨人が、ユーザーがネットに掲載した静止写真などを、本人の同意なしに顔認証技術 (FRT) を使って顔認証データを収集し保存していることが、イリノイ州法 (BIPA) に違反していることを理由に、ユーザーが起こしたもの。
- ②企業の従業員や顧客などによる訴訟
- 民間企業が、従業員や顧客の同意なしに、指紋や顔面、目の虹彩などを労務管理、ゲート管理などに利用していることが、イリノイ州法 (BIPA) に違反していることを理由に従業員が起こしたもの。

—— 生体認証情報あるいは生体認証識別子の違法な取扱いをめぐる訴訟は、大きく①データ巨人によるユーザーの顔面データの違法な収集・保存のケースと、②民間企業による従業員の指紋や顔面などの生体情報の違法な利用のケースに分けられるとのことですが、もう少し詳しく説明してください。

(石村) わかりました。まず①のタイプの訴訟ですが、生体認証情報あるいは生体認証識別子、とくに顔面データ、の違法な取扱いをめぐるフェイスブック社 (Facebook)、グーグル社 (Google)、シャッターフライ社 (Shutterfly)、スナップチャット社 (SnapChat) などのネット巨人 (tech giants) な

どに対する消費者（ユーザー）による訴訟は、全米各所で、イリノイ州生体認証情報プライバシー法（BIPA）に準拠して起こされています。

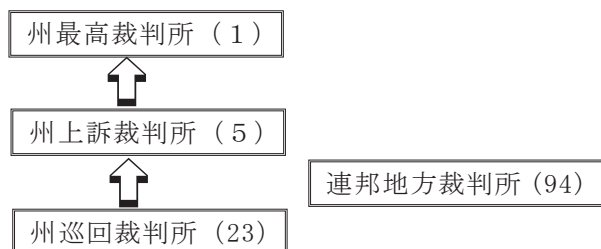
これらデータ巨人に対する訴訟は、これらの企業がユーザー本人の同意を得ないで、顔認証技術（FRT）を利用して静止写真から顔認証データを収集し保存したことが問われました。

それから、②のタイプの訴訟ですが、食品小売業のマリアノス（Marianos）、ヘルスクラブのライフタイムフィットネス（Life Time Fitness）、フォーシーズンホテル、ユナイテッド航空などが従業員の労働時間を管理する目的での本人の同意なしの指紋の収集が争われました。また、スーパーロッサ・レストラン・グループ（Superrossa Restaurant Group）による現金レジ担当した者を追跡するための指紋スキャナーの利用が裁判で問われました。

—— アメリカの場合、裁判所は、連邦と、各州にあります。この種の訴訟は、どの裁判所に起こされているのですか？

（石村）的をついた質問ですね。本来、各州法は州の居住者（個人／法人など）や州内に拠点（店舗や住宅など）を持つ非居住者など（以下、単に「居住者」といいます。）を適用対象としています。ですから、イリノイ州生体認証情報プライバシー法（BIPA）は、本来イリノイ州の居住者がイリノイ州の裁判所【同州の司法制度は3審制：①イリノイ州最高裁判所（Supreme Court）、②上訴裁判所（Appellate Court）〔5の裁判区〕、③巡回裁判所（Circuit Court）〔23の巡回区／事実審裁判所〕】に訴えを起こすことになります。

【図表 8】イリノイ州の三審制の裁判所制度



ところが、実際には、イリノイ居住者以外の人たちが、BIPAに準拠して、全米にある連邦地方裁判所（U.S. District Court）に訴訟を起こします。法律の専門用語では、これを「州法の域外適用（extra application of the state law）」といいます。

一般に、連邦法で規制されていない事項、例え

ば州内通商、について、各州が州法でその州内で合理的な範囲で規制ができるとされます。しかし、州法の域外適用について、最高法規である連邦憲法は、全米に統一的な規制が必要である事項については、連邦に州際通商規制権限を黙示的に付与しているとの法理（dormant Commerce Clause）に基づき違憲であるとの反論がなされます。つまり、この種の問題に関する一連の訴訟において、被告であるネット巨人の側は、自社の顔認証サービスは、イリノイ州だけでなく全米規模で提供されており、1州法で他州にも及ぶサービスを規制することは、連邦憲法が保障する連邦の黙示的州際通商規制権限を侵害し、違憲であると反論するわけです。もっとも、ネット巨人は、そもそも国境（州境）のないネット・オンライン・デジタル空間に拠点を置いてビジネスを展開しているわけです。こうした企業のサービスに、黙示的州際通商規制権限の法理を持ち出して州法の適用を制限する考え方（または反対の考え方）には大きな疑問符がついているのも事実です。

—— どのくらいの件数の生体認証情報の不法利用を追求した訴訟が起こされているのですか？

（石村）イリノイ州生体認証情報プライバシー法（BIPA）は、2008年に制定されました。その頃からどれくらいの訴訟が起こされたのか、和解を含め全体の訴訟件数はつかめません。最近の件数をたどってみると、イリノイ州生体認証情報プライバシー法（BIPA）に準拠して、ネット巨人を相手に、2015年には7件の訴訟が起こされています。2016年には、さらに7件の集団訴訟（class action）が提起されています。加えて、2016年には、企業の従業員や顧客などによる訴訟が提起されています。2017年までに、BIPAを典拠に、30件あまりの訴訟が提起されているといわれています。近年の傾向としては、経営側が従業員の同意を得ずに労務管理に指紋や顔面などの生体認証情報を利用している実務を争うケースが増えてきています。

2015年～2016年期では、BIPAに準拠した大多数の訴訟は、連邦裁判所に起こされていました。しかし、2017年以降は、BIPAに準拠したほぼすべての集団訴訟（Class action）は、イリノイ州裁判所に提訴されています。

—— ほとんどの生体認証情報の不法利用を糾した訴訟が、連邦裁判所からイリノイ州裁判所へ提訴されるようになったのは、どうしてなのでしょう？

（石村）集団訴訟が、連邦裁判所から州裁判所へ提起されるようになった理由は、はっきりしません。

ただ、連邦裁判所が、州法に準拠して複数の州の州民が集団訴訟を起こすことに対して、原告適格（訴訟資格）を認めることに消極的姿勢を強めていることが一因とする見方もあります。また、この背景には、2005年に制定された連邦のクラスアクション公正法（Class Action Fairness Act）の影響もあるとの見方もあります。この法律は、表向きは、集団訴訟を起こし和解に持ち込むことで多額な報酬を得ようとする弁護士を抑制することが狙いとされます。しかし、本当の目的は、集団訴訟の管轄をできるだけ州裁判所から連邦裁判所に移すことにより、「集団（クラス）認定」を難しくすることを狙ったものとされます。この結果、州法である BIPA に準拠して起こされる集団訴訟は、逆に集団（クラス）認定が難しい連邦裁判所を避けて、州裁判所に集中することになったとの見方もあります。この辺は、見解のわかれるところです。

—— 生体認証情報の不法利用を糾した訴訟内容について、もう少し詳しく紹介してください。

（石村）ネット巨人が本人の同意を得ないでウェブサイトに搭載された静止写真から顔認証データを収集・保存した取扱いの違法性を問う訴訟の概要は、次のとおりです。

【図表 9】イリノイ州法（BIPA）を根拠にした訴訟の概要

①フェイスブック社生体認証情報プライバシー訴訟

フェイスブック（Facebook）サイトの写真タグ付け機能がユーザープライバシーの侵害にあたり、イリノイ州シカゴに住む3人の原告がカリフォルニア北部地区連邦地方裁判所に起こした集団訴訟である。この訴えでは、フェイスブックがユーザーの投稿した写真に写った顔を認識するための「faceprint」を作成し、タグ付けのサジェストなどに利用していることが問われた。原告側は、ユーザーに対して明白な説明なしに「faceprint」が作成されていることが、個人の生体情報を本人の同意なしに収集することを禁じるイリノイ州の生体認証情報プライバシー保護法（BIPA）に違反していると主張した。それに対して、フェイスブック側は「ユーザーはフェイスブックの利用規約がカリフォルニア州法に基づくことに合意している」として、この訴えの棄却を裁判所に求めた。カリフォルニア北部地区連邦地方裁判所の判事は被告フェイスブック側の求めを却下した。この件に関してイリノイ州法の適用を認めた〔In re Facebook Biometric Info. Privacy Litig., (185 F. Supp. 3d 1155 (N.D. Cal. 2016))〕

②シャッターフライ社生体認証情報プライバシー訴訟

シャッターフライ社のユーザーが、ネットのアップしたデジタル写真を同社が本人の同意もなしに顔

認証技術（FRT）ソフトを利用してデータを取集・保存したのは、イリノイ州の生体認証情報プライバシー保護法（IBIPA）に違反しているとして、イリノイ北部地区連邦地方裁判所に訴えた事件である。地裁は、被告側の訴えの棄却の求めを却下した（Monroy v. Shutterfly, Inc., No. 16 C 10984 (N.D. Ill. Sep. 15, 2017)）

③グーグル社生体認証情報プライバシー訴訟

グーグルのユーザーが、同社がユーザーの静止写真を本人の同意を得ないでスキャンし保存したことは、イリノイ州生体認証情報プライバシー保護法（BIPA）に違反するとして同社を相手に、イリノイ北部地区連邦地方裁判所に訴えたもの。連邦地裁は、被告グーグル社側の訴えの棄却を求める申立てを一端退けた（Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017)）。しかし、後に、原告適格を欠くとの利用で原告の訴えを棄却した（Rivera v. Google, LLC., (N.D. Ill. 2018)）

—— 以上は、①グーグル社やフェイスブック社のようなネット巨人（tech giants）のユーザーによるIT企業の生体認証情報の違法な取扱いを理由とする連邦裁判所での訴訟ですが、②企業の従業員や顧客による生体認証情報の違法取扱いを理由とする訴訟についても、少し紹介してください。

（石村）民間企業が、従業員の同意なしに、指紋や顔面、目の虹彩などを労務管理などに利用している、あるいは、顧客の同意なしに顔認証技術（FRT）を利用して顔面データを収集・保存していたことが、イリノイ州法（BIPA）に違反していることを理由に従業員ないし顧客が、イリノイ州生体情報プライバシー法（BIPA）に準拠して、イリノイ州裁判所起こした訴訟は、次のとおりです。

【図表 10】民間企業の FRT 違法利用を問う従業員や顧客による訴訟

①雇用主による顔認証技術（FRT）の労務管理への違法利用をめぐる訴訟

シカゴ郊外にある病院が、同病院の接近が制限された放射線医学区域に入る従業員に対して、本人の同意を得ることなしに、指掌紋と目の網膜の生体情報を期間制限なしに求めたことが、イリノイ州生体情報プライバシー法（BIPA）に違反するとして、2018年3月末に、イリノイ州クックカウンティ巡回裁判所に、病院を相手に集団訴訟を起こしたもの（Case: NorthShore University HealthSystem March, 2018）。

②テーマパーク企業による入場者の生体認証情報の違法利用をめぐる訴訟

テーマパークを運営する「シックス・フラッグ社（Six Flags）」は、入場客のゲート管理に明示の同意なしに、親指の指紋の提出を求めたことが、イリノイ州生体認

証情報プライバシー法 (BIPA) に違反するとして、顧客がイリノイ州裁判所で争ったもの。本件において、イリノイ州上訴裁判所は、原告は法が求める具体的な権利侵害を受けたとは言い難く、単に軽微な BIPA 違反であるとして、訴訟を維持するに値しないと判示し、棄却した。原告 (控訴人) は、州最高裁に上告した。同最高裁は、なりすまし犯罪に悪用されたとか具体的な被害があったことを立証する必要がなく、単に法違反があったことを立証できれば、損害賠償を請求できるとし、本件を下級審に差し戻した (Rosenbach v. Six Flags Entertainment Corp., (2017 IL App (2d) (May Term 2018); Electronic Frontier Foundation,

なお、ここで上げたケースには、裁判上の和解に至ったケースは含まれていません。

—— 裁判上の和解に至ったケースについても、紹介ください。

(石村) 裁判上の和解 (settlement) は、裁判所が関与する和解のことをいいます。訴え提起前の和解と訴訟上の和解があります。裁判上の和解に至ったケースとして有名なものは、フランチャイズ方式で日焼けサロン (tanning salon) を展開している企業を相手に、BIPA に準拠した顧客による集団訴訟での裁判上の和解があります (Sakura v. L.A. Tan)。このケースでは、フランチャイズ日焼けサロンが、会員の本人確認に顧客の指紋認証走査 (fingerprint scanning) 方式を利用していました。フランチャイズ店が、①顧客から指紋認証データを収集するときに本人から明示の同意を文書で取っておらず、②データの管理もプライバシーポリシーに従っていませんでした。加えて、③閉店した場合に顧客データの破棄もずさんでした。

このケースでは、被告企業が、顧客の生体認証データを漏らしたとか、他の企業へ横流ししたとかの事実はありませんでした。原告の顧客は、被告の日焼けサロン企業が、イリノイ州の BIPA に違反して生体認証データを取り扱っていることを理由に損害賠償を求めてシカゴ市クックカウンティにあるイリノイ州上訴裁判所に民事訴訟を提起したものです。原告と被告企業とは、150 万ドル (\$ 1 = 100 円換算で、1 億 5 千万円) の支払で、2016 年 12 月 5 日に、訴訟上の和解に合意しました。

—— フェイスブック社は、顔認証技術 (FRT) の規制に反対するために、連邦議会や規制法を制定しているあるいは制定しようとしている州議会へ巨額の資金を使ってロビー活動を展開しているとのことでしたが？

(石村) マイクロソフト社の経営トップと、フェイスブック社の経営トップとは、カラーが違うように感じています。後ほど CNN 本号 (99 号・18 頁) で紹介しますが、マイクロソフト社のスミス社長 (CEO) は、顔認証技術 (FRT) の濫用や不適正な利用による偏見や差別を禁止し、プライバシーを含む自由権を護るためには、一定の法規制が必要であるというスタンスにあります。一方、フェイスブック社は、2018 年 3 月には、5,000 万人分ものフェイスブック社ユーザー情報が、イギリスの政治・選挙関連データ分析企業のケンブリッジ・アナリティカ (CA=Cambridge Analytica) (その後 2018 年 5 月に廃業) が流出し、本人の同意もなく先の米大統領選挙でクリントン候補つぶしのターゲティング広告に政治利用されたことが問題となりました。また、アメリカ国内では、同社の約 8,700 万人に及ぶユーザー情報が流出し、個人データ、プライバシーの取扱いに対する経営姿勢が問題になりました。フェイスブック社は、市民のプライバシー、人権を商品にして、儲けだけに執着しがちで、しかも社会的責任に対する意識が希薄であるとの批判を浴びています。同社のマーク・ザッカーバーグ社長 (CEO) は、2018 年 4 月 10 日に連邦議会上院司法委員会の公聴会に、翌 11 日には米連邦政府下院エネルギーおよび商業対策委員会の公聴会に召喚されました。それぞれの公聴会では、質問にたった数多くの議員から同社の企業倫理を含む経営姿勢に対して数時間にも及ぶ厳しい言葉が浴びせられました。こうした点からも明らかのように、フェイスブック社は、少し企業の社会的責任とか企業倫理に疎いようにみえます。

フェイスブック社は、業界団体であるインターネット協会 (Internet Association) やコンプ TIA (Comp TIA) などを通じてイリノイ州議会 (Illinois General Assembly) の議員と接触しています。この背景には、2015 年にフェイスブック社を相手に、同社のユーザーが、フェイスブックがユーザーの投稿した写真に写った顔を認識するための「faceprint」を作成し、タグ付けのサジェストなどに利用していることが、個人の生体情報を本人の同意なしに収集することを禁じるイリノイ州の生体情報プライバシー保護法 (BIPA) に違反していると主張し、損害賠償を求めた訴訟に悩まされたことがあるのではないのでしょうか。

—— IT 業界は、イリノイ州の生体認証情報プライバシー保護法 (BIPA) の骨抜きを画策しているということですが、どのように改悪しようとして

いるのでしょうか？

(石村) イリノイ州の BIPA は、生体認証情報を取り扱う企業にとっては、受忍義務が重いわけです。日焼けサロン企業が顧客の生体認証情報の違法な取扱いが原因で多額の和解金の支払いを命じられたケースを含む、産業界に厳しい判決が続きました。法曹界の賞金稼ぎの動きにも、産業界から批判がでてきました。産業界は、BIPA を改正し骨抜きにしたいわけです。改悪を目指して、2018 年 5 月 14 日にイリノイ州議会上院に提出された上院法案 3053 号 (SB 3053) は、次のとおりです。

【図表 11】イリノイ州の BIPA 改悪法案 (SB3053) のポイント

次の 3 つのいずれかにあてはまる場合には、BIPA は適用除外とする。

- ①企業が、生体認証情報をもっぱら雇用、求職、不正防止または安全対策目的で利用する場合
- ②企業が、生体認証情報を譲渡せず、貸与せず、取引せずその他利益の対象としていない場合、または、
- ③企業が、生体認証情報を他の要配慮個人情報と同等に厳格に保護している場合

こうした法 (BIPA) の改悪が行われると、生体認証情報の取扱いがルーズな企業にとっては都合がよいのはわかります。しかし、唯一無二で、変更が不可能な生体認証情報は、いったん漏れたら取り返しのつかないことになります。消費者や従業員の究極なプライバシーは風前の灯と化する怖れがあります。まさに人権問題だといえます。電子フロンティア基金 (EFF=Electronic Frontier Foundation) などアメリカのメジャーな市民団体は、イリノイ州議会議員に手紙を送るなど、強い警鐘を鳴らしています (EFF, `New Attack on the Illinois Biometric Privacy Act,` April 10, 2018)。

—— 連邦議会には、さまざまな議員立法が提出されていると聞きますが、その概要を教えてください。

(石村) 現在、連邦には、個人情報保護の面では、政府機関 (公的部門) による個人情報の取扱いをおおまかに規制する「プライバシー法 (Privacy Act)」(1974)【ただし、政府機関での生体認証情報の取扱いについては規制していません。】しかありません。民間機関の個人情報取扱いを幅広く規制する法律はありません。しかし、EU (欧州連合) の GDPR (一般データ保護規則) やカリフォルニア州の CCPA (消費者プライバシー法) などの制定は、連邦議会にも大きなプレッシャーとなっています。

議会民主党は、民間企業の個人情報取扱いに規制を加え消費者のプライバシーを護る立法の成立に立ち上がっています。一方、議会共和党にも、そうした動きがでてきています。「消費者の利益に奉仕しない企業は生き残れないはずだ」という市場主義に任せる形では消費者のプライバシーは護り切れないという認識が高まってきたからです。

最近、連邦議会に提出された議員立法案を簡潔にまとめてみると、次のとおりです。

【図表 12】連邦議会での民間機関個人情報取扱規制法案提出の動き

- ①アメリカ人のデータ頒布規制法 (American Data Dissemination (ADD) Act) 案〔上院法案 142 号／共和党ルビオ上院議員 (Sen. Rubio／フロリダ州選出) が、2019 年 1 月に委員会提出〕【インターネットプロバイダー企業を対象に、現行の公的機関を対象としたプライバシー法と同じ水準の規制を加える内容。規制主体としては連邦取引委員会 (FTC=Fair Trade Commission) を提案】
- ②ソーシャルメディア・プライバシーおよび消費者権利法 (Social Media Privacy and Consumer Rights Act) 案〔上院法案 189 号／民主党クロバチャー上院議員 (Sen. Klobuchar／メイン州選出) と共和党ケネディ上院議員 (Sen. Kennedy／ルイジアナ州選出) が、2019 年 1 月委員会に共同提出。2018 年 4 月に提出した上院法案 2728 号を再提出したもの〕【オンライン・プラットフォーム企業 (GAFA など) は、消費者データの収集にあたり説明に基づくデータ主体の同意を義務化。また第三者提供には「オプトアウト (opt-out)」が条件。規制主体としては、連邦取引委員会 (FTC)、州法務長官、州消費者保護担当官を提案】
- ③データ保護法 (Data Care Act) 案〔上院法案 3744 号／民主党シャッツ上院議員 (Sen. Schatz)／ハワイ州選出〕が、2018 年 12 月に委員会提出〕【オンライン・サービス・プロバイダーによるユーザー (消費者) 情報取扱いを規制。規制主体としては、連邦取引委員会 (FTC)、州法務長官、州消費者保護担当官を提案】
- ④消費者データ保護法 (Consumer Data Protection Act) 案〔民主党ワイデン上院議員 (Sen. Wyden／オレゴン州選出) が 2018 年 11 月に提案。法案は委員会未提出〕【過去 3 年間の年間平均売上高 5,000 億ドル超の個人情報取扱事業者、100 万人以上の消費者および消費者デバイスの個人情報を取り扱う事業者、および個人情報の収集、加工、保存、第三者への販売などを実質的な事業とするデータブローカーその他の事業者は、FTC の規制の対象となる。FTC は、個人情報取扱規則で、合理的なサイバーセキュリティやプライバシー保護、消費者の自己データへのアクセス権や訂正権などの取扱いにつ

いて定める。また、100万人以上の消費者および消費者デバイスにかかる個人情報取扱事業者は、FTCに年次データ保護報告書(annual data protection reports)の提出が義務。FTCは、法施行から2年以内に、消費者がウェブ上で「追跡させない(Do Not Track)権利」、つまり「忘れられる権利」を認められるように対応すること。事業者は、消費者と契約し、サービスの提供と引き換えにその消費者のデータを利用できる。FTCは、法律違反には各違反につき5万ドルまでまたは年間売上高の4%のいずれか大きい方の額までの過料を課す権限を有する。

⑤エッジプロバイダーによるネットワーク犯罪の消費者オンライン通知法(Consumer Online Notification for Stopping Edge-provider Network Transgression(CONSENT) Act)案〔上院法案2639号/下院法案5815号/民主党マーキー上院議員(Sen. Markey/メリーランド州選出)と民主党ブルーメンタール上院議員(Sen. Blumenthal/コネチカット州選出)が2018年4月に委員会に共同提案〕【オンライン(エッジ)プロバイダー(オンライン事業者)の「顧客のセンシティブな財産的な情報(sensitive customer proprietary information)」(センシティブ情報)に関するプライバシー保護を目的とした法律。主務機関はFTC。また、ここでの「センシティブ情報」とは、「金融情報、健康情報、子供関係情報、社会保障番号、正確な位置情報、通信内容、通話情報、ウェブ利用歴・アプリ利用歴・これらに相当する情報、その他本人確認情報でFTCがセンシティブと決定した情報」をいう。【したがって、生体認証情報を含むのかどうかは不明】オンライン事業者は、顧客のセンシティブ情報を収集するにあたっては、その利用・保管・利用・提供などの取扱いについて顧客から事前の説明に基づく同意(CONSENT)を得ること(opt-in)を義務化。オンライン事業者が、顧客がビジネス利用などへの提供に同意しないことを理由に差別的な取扱いをすることを禁止。オンライン事業者は、「合理的なデータ安全実務(reasonable data security practice)」を公表し、かつデータ漏れがあり相当の被害が予想される場合にはその顧客に通知義務を負う。

⑥情報透明化および個人データ規制法(Information Transparency and Personal Data Control Act)案〔下院法案6864号/民主党デルベーン下院議員(Rep. DelBene/ワシントン州選出)が、2018年9月に委員会に提案〕【概要紹介省略】

⑦アプリプライバシー、保護および安全(APPS)法(Application Privacy, Protection, and Security Act)案〔下院法案6547号/民主党ジョンソン下院議員(Rep. Johnson/ジョージア州選出)が、2018年7月に委員会に提出〕【概要紹介省略】

ちなみに、近年連邦議会に提出されたこれら一連の民間機関の個人情報取扱規制法案は、生体認

証情報に特化して取扱事業者に規制をかけることを目的としているわけではありません。

また、2020年1月1日に施行されるカルフォルニア消費者プライバシー法(CCPA=California Consumer Privacy Act)も、イリノイの生体認証情報プライバシー法(BIPA)とは異なり、生体認証情報に特化した形で法規制をかけた法律ではありません。しかし、CCPAに規定された「個人情報(personal information)」には、各種の生体認証情報を含みます(詳しくは、「カリフォルニア消費者プライバシー法(CCPA)を読み解く」CNNニュース98号21~22頁参照)。

—— わが国の個人情報保護法では、一応、「特定の個人の身体の一部」、つまり、生体認証情報(データ)のような個人の身体的な特徴を電子処理するための変換した文字、番号、記号その他の符号、具体的には、DNA配列、顔認識データ、虹彩データ、音声データ、歩行データ、静脈データ、指紋や掌紋データ、その他これらの生体認証データを組み合わせたデータなども、法規制の対象としています。わが国の法制は、イリノイ州の生体認証情報プライバシー法(BIPA)と比べた場合、どのような問題があるのでしょうか?

(石村) 指紋や目の虹彩や顔面などは、人の唯一無二の生物学的な特徴で、個人の最もセンシティブな情報です。紛失したり、悪用されたとしても、変更することができません。運転免許番号や身分証明書番号、個人番号(マイナンバー)、その他各種パスワードなどは、変更することができます。ところが、個人情報保護法では、双方のカテゴリーを「個人識別符号」として同列に取り扱っています。

これでは、プライバシーを人権と考える認識や倫理にかけられる企業が、消費者の入場ゲート管理やPCのログイン、労務管理などに生体認証を使うことを野放しにすることにもなりかねません。わが国のマスメディアには市民の生体認証情報をビジネスにするIT企業の広告があふれています。しかし、市民の「生体認証情報は究極のプライバシーである」とするトーンは極めて低いのが現実です。個人情報取扱事業者の特定個人情報(個人番号(マイナンバー)付き個人情報)の取扱いですら、適正に行われているのか、一般の市民にはますますわかりにくくなっているのが現状です。

この点、イリノイ州の生体認証情報プライバシー法(BIPA)では、生体認証情報取扱事業者(私的事業者)に対して、生体認証情報(生体認証識別子)をセンシティブ(要配慮情報)と同列あるいはそ

れ以上の厳しい基準に取り扱うように求めています。

わが国でも、生体認証情報を他の個人識別符号と差別化して法規制をする必要があります。生体認証情報を軽々に取り扱うことは、きわめて深刻な人権問題につながる危険性が高いからです。事業者や公的機関が、生体認証情報の提供を求めるにあたっては、事前に情報主体に利用目的を通知し、生体認証情報を収集する本人の同意を得ていること（オプト・イン）を義務化し、さらには同意しないことを理由に差別することを法で禁止し、市民の人権を護る必要があります。生体認証情報の不適切な取扱いは情報主体に取り返しのつかない損害につながることを周知し、かつ、コンプライアンスを徹底するためには、生体認証情報取扱事業者の受忍義務違反に対しては、刑事制裁を科すことも検討する必要があります。

加えて、アメリカの州や地方団体のように、法律や条例で、人工知能（AI）を応用した顔認証技術（FRT=facial recognition technology）を自治体の行政機関や警察が利用することを禁じる必要があります。AIを使った顔認証式のライブ監視カメラで街中を埋め尽くしても、犯罪の後追いは容易になるが、根絶は難しいわけです。社会が抱える課題によっては、単純に先端技術だけで解決できません。先端技術を使った市民の生体認証情報の取扱自体が職場や社会の信頼関係を壊していないのか慎重な検討が必要です。

—— わが国においては警察など公的機関や民間企業による生体認証情報の取扱いは極めて野放図です。また、議員も概して情報に対する人権意識が低く、生体認証情報や生体認証情報技術に対する法律や条例による規制もないに等しい法環境にあります。こうしたなか、倫理や社会的責任の希薄なIT企業がバコシ、利益のために私たち市民の生体認証技術をビジネスにし、こうした技術を使って収集された生体認証情報の取扱いも極めて不透明なのが実情です。私たち市民は、どのような手段で自分の生体認証情報を護ったらよいのでしょうか？

（石村） プライバシー保護をベースとした市民のデータを適正に活用した住みよい社会を実現できるかどうかは、公的機関や企業が生体認証情報を含む市民のデータをいかに透明に取り扱っているかにかかっています。ところが、わが国の生体認証情報をめぐるプライバシー保護政策はお寒い限りです。私たち市民が、倫理観や人権意識の希薄

なIT企業とかれらの権益の付度に終始する役人や議員にお任せにしていた付けが回ってきたということでしょう。

しかし、私たち市民は、現状を放置し、未来の世代への責任を放棄してはなりません。なぜならば、このままでは、市民の生体認証情報を国家が管理し、市民を「国畜」にする国家ができあがってしまいます。中国の「天網」のような顔認証システムで国中を包囲するデータ国家主義を批判できない人権レベルの国になりきってしまう怖れがあるからです。ですから、警察や東京五輪・パラリンピック競技大会組織委員会のような公的機関や民間企業が、顔認証情報など本人の同意もなく市民のデータを収集・利用・保管などの面で不当に取り扱っていると合理的に信じる理由がある場合には、市民は、それを問い質す権利（個人データの自己コントロール権）、正当な保障を求める権利が保障されていなければなりません。

—— アメリカは訴訟大国です。制定認証情報取扱事業者による違法な取扱いについては、イリノイ州のBIPAに準拠して裁判が起こされています。わが国でも、事業者による生体認証情報の違法な取扱いにストップをかけるためには裁判に訴えることも大事だと思いますが？

（石村） わが国に個人情報保護法は、生体認証情報も個人情報にあたるとしています。しかし、イリノイ州のBIPAとは異なり、個人情報取扱事業者が違法な取扱いで被害を受けた個人がその事業者を訴えて損害賠償請求をする規定を置いていません。しかし、民法の709条〔【不法行為による損害賠償】故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う。〕に基づき、民事訴訟で損害賠償を求めることができます。

顧客情報の流出をめぐる、民事訴訟で損害賠償を求めて争われたよく知られているケースとしては、ベネッセコーポレーション（岡山市）に関する司法判断があります。このケースは、生体認証情報の流出に関するものではありません。2019年6月28日に、控訴審の東京高裁（萩原秀紀裁判長）は、ベネッセ本体に対して、2件の訴訟の顧客ら計5人に、1人あたり2,000円を支払うよう同社側に命じる判決を言い渡しました。確かに受けた精神的苦痛に対する補償としては金額的にはわずかです。しかし、個人情報を粗末に取扱うと企業イメージを損ねることを教え、お灸をすえるには、司法を活用するのも一案です。

2014年5月27日に、福岡県弁護士会三浦邦俊会長は、「法律によらず顔認証装置を使用しないように求める声明」を出しています（【資料1】参照）。この声明では、福岡県警は、2013年12月に顔認証技術を導入していることを紹介しています。県警は「組織犯罪対策運営規程（平成18年福岡県警察本部訓令第10号）」を制定しています。しかし、この規程では、「顔認証装置の使用について、使用できる場合として対象犯罪や、検索・照合の対象となるデータベースに登録される者の属性を限定する明文規定も存在しない。」ことを指摘しています。そのうえで、「ひとたびある市民が福岡県警の対象とされた場合には、その行動が丸裸となり、そのプライバシー権を侵害するばかりか、街頭での署名活動、集会やデモ行進など、民主主義社会の基礎となる市民の表現の自由を萎縮させる危険が大きい。どのような条件の下に収集、利用、保存が許されるのか、またどのようにして目的外利用を防ぐのかをまずもって厳格に定めるべきである。さらに、対象者の同意がなくとも顔認証装置の使用を認める法律が存在しない。このような現状においては、福岡県警は顔認証データを収集、利用、保存すべきではなく、顔認証装置を使用すべきではない。」と正鵠を射た見解を表明しています。

生体認証技術の不法な収集につながる技術を開発・販売するIT企業、IT企業が開発した生体認証技術を利用して市民・消費者の生体認証情報を適正に取り扱っていない公的機関や企業を相手に、市民・消費者・従業者が、民法の不法行為を問う形で、各地で行政訴訟や民事訴訟を集団で起こして、その姿勢を糾すのも一案です。アメリカのBIPA関連訴訟ケースなどを参考にして、弁護士会や弁護士法人などが、この問題に真摯に取り組んで欲しいところです。

【主要参考文献】

- ・Charles N. Insler, “Understanding the Biometric Information Privacy Act Litigation Explosion,” 106 Ill. B. J. 34 (2018)
- ・R. Krishan & R. Mostafavi, “Biometric Technology: Security and Privacy Concerns,” 22 J. Internet L. 19 (2018)
- ・Rachel Nevarez, “The Biometric Information Privacy Act: Important Regulatory Safeguard or Class Action Boon?,” 30 DCBA Brief 8 (2018)
- ・Stephen Embry, “Illinois Biometric Information Privacy Act: Legitimate Privacy Protection or

Pandora’s Box,” (Nov. 13, 2017)

- ・See, Gabe Friedman, “First Settlement Reached Under Illinois Biometric Law” (Dec. 6, 2016)
- ・EFF, “Victory! Illinois Supreme Court Protects Biometric Privacy,” (Jan. 25, 2019)

【資料1】

福岡県弁護士会三浦邦俊会長声明（2014年5月27日）

(https://www.fbenn.jp/suggest/archives/cat7/index_5.html)

法律によらず顔認証装置を使用しないよう求める声明

当会の調査によれば、2013年（平成25年）12月に福岡県警察（以下「福岡県警」という。）に顔認証装置が導入され、すでに使用例も存在する。

顔認証装置とは、撮影された画像から人の顔の部分を抽出し、目・耳・鼻などの位置関係等を瞬時に数値化し（この数値化されたデータを「顔認証データ」と呼ぶ）、あらかじめデータベースに登録されている特定人物の顔認証データとの同一性を自動的に照合するものである。

福岡県警は、具体的な組織犯罪が生じた場合に、県警が自ら設置する防犯カメラの画像の他、民間のカメラの画像もその捜査のために収集する予定であると説明している。また、顔認証装置で検索・照合する対象となるデータベースに登録される人物については、組織犯罪を対象とすることからの限定があるという。

しかし、組織犯罪対策運営規程には、顔認証装置の使用について、使用できる場合としての対象犯罪や、検索・照合の対象となるデータベースに登録される者の属性を限定する明文規定も存在しない。

そもそも、警察は、捜査目的であっても、罪のない市民の行動に関する情報を無制限に収集したり、検索・照合の対象とする権限があるわけではない。

顔認証データは、おびただしい数の顔画像の中から瞬時に人物の同一性判定が可能であり、指紋よりもいっそう簡便に収集が可能な、高度な生体認証データである。したがって、本来、対象者の同意なしに取得することが許されないセンシティブ情報と捉えるべきである。

対象者の同意なく使用する以上、あらかじめど

のような条件の下に収集、利用、保存が許されるのか、またどのようにして目的外利用を防ぐのかを厳格に定める法律なくして顔認証データを収集・利用・保存するべきではない。

画像を収集する場面で、以下の問題がある。

①福岡県警が自ら設置している中洲・博多地区、天神地区など県内132台の監視カメラで収集される画像については、当会が再三にわたり意見を表明しているところであるが、警察が犯罪多発地帯でないのに直接公共の場所に監視カメラを設置して罪のない市民を無差別録画することは本来許されない。

②コンビニエンスストアなどから限定なく任意捜査で画像を収集すると、撮影される画像の対象は市街地中心部から郊外に至るまでの極めて広範に及ぶ。

また、顔認証装置を使用し、検索・照合する場面で、以下の問題がある。

③検索・照合する対象となるデータベースの登録者について、限定する内部規定すら存在しないというのでは、目的外利用がなされないための歯止めは期待できない。むしろ、8,000万人を超える運転免許証データがデータベースとして用いられる可能性もある。

④目的外利用がなされないための独自の物理的、技術的対策、内部及び第三者によるチェック体制も存在しない。

以上によれば、ひとたびある市民が福岡県警の対象とされた場合には、その行動が丸裸となり、そのプライバシー権を侵害するばかりか、街頭での署名活動、集会やデモ行進など、民主主義社会の基礎となる市民の表現の自由を萎縮させる危険が大きい。

どのような条件の下に収集、利用、保存が許されるのか、またどのようにして目的外利用を防ぐのかをまずもって厳格に定めるべきである。さらに、対象者の同意がなくとも顔認証装置の使用を認める法律が存在しない。このような現状においては、福岡県警は顔認証データを収集、利用、保存すべきではなく、顔認証装置を使用すべきではない。

2014年（平成26年）年5月27日
福岡県弁護士会会長 三浦邦俊

【資料 2】

《邦訳 / 仮訳》

イリノイ州生体認証情報プライバシー法 (BIPA=Illinois Biometric Information Privacy Act)

イリノイ州編纂制定法集

(ILCT=Illinois Compiled Statutes)

第740章〔民事責任（Civil Liabilities）〕第14節
(2008年、2015年3月28日までの改正を含む)

邦訳責任者 石村耕治

(略式名称)

第1条 この法律は、「生体認証情報プライバシー法 (Biometric Information Privacy Act)」として引用できる。

(立法理由、立法意思)

第5条 議会は、次の各号に記載した理由で本法を制定する。

第a項 生体認証の利用は、事業および安全検査部門において増大しており、かつ、金融取引および安全検査の合理化につながるように見える。

第b項 多くの国内の会社は、雑貨店、給油所および学校食堂における電子的指紋読取技術 (finger scan technology) を含む生体認証を利用した新たな金融取引への応用のために、この州のシカゴ市その他の地域を選定している。

第c項 生体認証は、金融にアクセスするために利用される他の唯一無二の識別子その他の要配慮情報 (sensitive information) とは異なる。例えば、社会保障番号は、紛失した場合、変更することができる。一方、生体認証は、その個人にとり生物的に唯一無二なものである。このため、紛失した場合、その個人は対応策がなく、なりすましにあう危険性も高いため、生体認証を利用した取引から退くことになるように見える。

第d項 大多数の一般の人たちは、生体認証の利用が金融その他の個人情報と結びつく場合には精神的な負担を覚える。

第e項 州法で生体認証の収集、利用、安全対策および保存を規制しても、一般の人たちは、生体認証識別子を利用した取引に関係することに躊躇する。

第f号 生体認証技術に派生する総体的な効果

については十分に知られていない。

第g項 生体認証識別子および生体認証情報の収集、利用、安全措置、取扱い、保管、保存および破棄について規制することは、一般の人たちの福祉、安全および安心に役立つ。

(定義)

第10条 この法律において、次に掲げる用語の定義は、次に定めるところによる。

「生体認証識別子 (biometric identifier)」とは、目の網膜 (retina) または虹彩 (iris) の映像、指紋 (fingerprint)、声紋 (voiceprint) 電子の手掌読取 (scan of hand) または顔認証 (face geometry) をいう。ただし、生体認証識別子には、筆跡 (writing samples)、筆記署名 (written signatures)、写真 (photographs)、正当な学術的検査もしくは調査に利用される人間の生物学的標本 (human biological samples used for valid scientific testing or screening)、人口統計データ (demographic data)、入墨の描写 (tattoo description)、または身長、体重、髪の色もしくは目の色のような身体的特徴 (physical descriptions) を含まない。生体認証識別子には、生体もしくは遺体からの移植の受け手または潜在的な受け手に代わって保存し、かつ連邦が指定した臓器調達機関が取得または保存するイリノイ献体法 (Illinois Anatomical Gift Act) に定義される提供された臓器 (donated organs)、組織 (tissues) もしくは内蔵 (parts) または血液もしくは血清 (serum) を含まない。生体認証識別子には、遺伝子情報プライバシー法 (Genetic Information Privacy Act) に基づいて規制される生物学的な資料を含まない。生体認証識別子には、医療現場で患者から入手した情報、または連邦の健康保険の持運びおよび説明責任法 (Health Insurance Portability and Accountability Act of 1996) に基づく医療行為、支払もしくは業務で収集、利用または保存した情報を含まない。生体認証識別子には、X線、レントゲン、電子断層写真 (computed tomography)、MRI、PET スキャン、マンモグラフィ、その他病気その他健康状態を診断 (diagnose)、予知 (prognose) もしくは治療 (treat) するため、または科学的検査もしくは調査の検証を推進するために使用される人体構造 (human anatomy) の電子画像 (image) または映像を含まない。

「生体認証情報 (biometric information)」とは、個人の生体認証識別子に基づき、個人の身元確認

をするために利用される情報をいう。どのように収集され、譲渡され、保存されまたは供用されたかを問わない。生体認証情報には、生体認証識別子の定義から除外された項目または手続から生じた情報を含まない。

「秘密の要配慮情報 (confidential and sensitive information)」とは、個人または個人の口座もしくは資産を一意に確認するために利用することができる個人情報という。秘密の要配慮情報には、遺伝子マーカー、遺伝子検査情報、口座または資産の所在を確認するための唯一無二の識別番号 (unique identifier number)、口座番号、PIN 番号、パスコード、運転免許番号または社会保障番号 (SSN)、これらに限定されない、を含む。

「私的事業体 (private entity)」とは、組織された、個人、パートナーシップ、法人、合同会社 (LLC)、社団 (association) その他の集団をいう。私的事業体には、州または地方団体の政府機関を含まない。私的事業体には、イリノイの裁判所、裁判所の書記官または裁判官は含まない。

「権利放棄書 (written lease)」とは、告知に基づく同意文書、または、雇用の一環として、雇用の条件として被用者が約した権利放棄をいう。

(保存、収集、開示、破棄)

第15条

第a項 私的事業体は、生体認証識別子または生体認証情報を保有する場合には、保存計画および当該生体認証識別子または生体認証情報を収集しかつ入手する当初の目的が達成されたときまたは当該個人と当該私的事業体とが最後の相互交流から3年以内か、いずれか早い方のときまでにその生体認証識別子または生体認証情報を永久に廃棄するためのガイドラインを明確にした成文のポリシーを作成し、一般に公開しなければならない。私的事業体は、生体認証識別子または生体認証情報を保有する場合には、明確にした保存計画および破棄ガイドラインに従わなければならない。ただし、権限ある管轄の裁判所が発行した有効な令状または召喚状がある場合には別である。

第b項 いかなる私的事業体も、人もしくは顧客の生体認証識別子または生体認証情報を収集、入手、購入するその他の方法で取得することはできない。ただし、次の各号に該当する場合は除く。

第1号 収集または保存する生体認証識別子または生体認証情報についてその主体またはその法的代理人に文書で通知している。

第2号 収集、保存および利用する生体認証識別子または生体認証情報についてその主体またはその法的代理人に文書で通知している。および、

第3号 生体認証識別子または生体認証情報の主体またはその法的代理人が約した権利放棄書を受領している。

第c項 私的事業体も、保有する人もしくは顧客の生体認証識別子または生体認証情報を開示、再開示または頒布することはできない。ただし、次の各号に該当する場合は除く

第1号 開示または再開示する生体認証識別子または生体認証情報についてその主体またはその法定代理人に文書で通知している。

第2号 開示または再開示が、金融取引を完結するために、その生体認証識別子または生体認証情報の主体またはその法定代理人の求めまたは承認によっている。

第3号 開示または再開示が、州もしくは連邦の法律または自治体条例によって求められている。

第4号 開示または再開示が、権限ある管轄の裁判所が発行した有効な令状または召喚状によって求められている。

第e項 私的事業体は、生体認証識別子または生体認証情報を保有する場合には、次のようにするものとする。

第1号 あらゆる生体認証識別子および生体認証情報を、当該私的事業体界で利用される相当な注意義務基準 (reasonable standard of care) をもって保存、伝達、開示から保護すること。

第2号 あらゆる生体認証識別子および生体認証情報を、私的事業体が秘密の要配慮情報を保存、伝達、および保護する方法と同様またはそれ以上の強い保護方法によること。

(訴訟権)

第20条 この法律の違反により権利を侵害された者は、権利を侵害した者を相手に、この州の巡回裁判所 (State circuit court) に訴訟を提起する権利または連邦地方裁判所 (federal district court) に補充的請求 (supplemental claim) をする権利を有する。勝訴当事者は、各違反について、次の各号に掲げる者に対して権利回復ができる。

第1号 この法律の過失により違反した私的事業体に対して、1,000ドルの定額損害賠償かまたは実額賠償額か、いずれか大きい方の額

第2号 この法律に故意に違反した私的事業者に対して、5,000ドルの定額損害賠償かまたは実額

賠償額か、いずれか大きい方の額

第3号 専門家の証言費用その他訴訟上の諸経費を含む、合理的な弁護士費用、および、

第4号 その他、差止請求を含む州裁判所または連邦裁判所が適切とみなす救済

(解釈)

第25条

第a項 この法律は、いかなる裁判所のいかなる種類の訴訟、または審判所、委員会、機関もしくは人に、生体認証識別子および生体認証情報の証拠採用 (admission) または証拠開示 (discovery) に影響を及ぼすものと解してはならない。

第b項 この法律は、X線保存法 (X-Ray Retention Act)、1996年健康保険の持運びおよび説明責任法 (Health Insurance Portability and Accountability Act of 1996) ならびにそれらいずれかの法律に基づき発出されたルールと抵触するものと解してはならない。

第c項 この法律は、いかなる形でも1999年グラム・リーチ・ブライリー法 (GLBA=Gramm-Leach-Bliley Act of 1999) 【訳注：金融サービス近代化法】タイトルVおよび当該法律に基づき発出されたルールの対象となる金融機関または金融機関の関連企業 (affiliate) に対して適用になるものと解してはならない。

第d項 この法律は、イリノイの2004年私立探偵、民間警報、民間警備、指紋認証サービス提供企業および鍵解除サービス法 (Private Detective, Private Alarm, Private Security, Fingerprint Vender, and Locksmith Act of 2004) ならびに当該法律に基づき発出されたルールと抵触するものと解してはならない。

第e項 この法律は、この州の政府機関または地方団体政府の請負者、下請負者もしくは代理人が、当該州政府または当該地方団体のために業務を行う場合に適用になるものと解してはならない。

(廃止)

第30条 (2008年10月3日に公布、2009年1月1日に施行)

(施行期日)

第99条 この法律は、公布の日から施行する。(2008年10月3日公布)

石村耕治 PIJ 代表に聞く

顔認証技術に法規制を！ 今こそ行動の時

— 米マイクロソフト社ブラッド・スミス社長の講演のポイント紹介 —

解説 石村 耕 治 (PIJ代表)

聞き手 中村 克 己 (CNN ニュース編集局長)

本 人確認方法（認証方式）として、顔面や指紋をはじめとした唯一無二の生体情報が使われる割合が高くなっている。パスワードやPKI（公開鍵）その他の方法（方式）よりも、セキュリティ（安全）対策で信頼性が高く、しかも安価（経済的）であるからである。アメリカでは、多くのIT企業が、生体認証の開発・販売にしのぎを削っている。その一方で、米フェイスブック社（Facebook）や米グーグル社（Google）のような生体認証技術を開発・利用・販売するIT企業、その技術を活用する民間企業は、次々とプライバシー侵害を理由に訴訟に巻き込まれるケースが増えてきている。

米マイクロソフト社は、「iPhone（アイフォーン）」に顔認証技術（FRT=facial recognition technology）を使う一方で、この技術の法規制を訴えている。昨年（2018年）12月6日、同社のブラッド・スミス（Brad Smith）社長兼最高法務責任者は、首都ワシントンD.C.にあるシンクタンク、ブルッキングス研究所（Brookings Institution）で講演し、監視国家の誕生を防ぐため、「顔認証：今こそ行動の時である（Facial recognition: It's time for action）」と題して、顔認証技術への法規制を呼び掛けた（<https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/>）。

スミス社長の考え方の基本は、顔認証技術

（FRT）に関する問題も、できるだけ市場原理（market forces）のルールのもとで解決すべきであるとする一方、この技術の濫用や不適正な利用による偏見や差別を禁止し、プライバシーを含む自由権を護るためには、一定の法規制が必要であるとするものである。スミス社長は、有能な企業経営者であるとともに、コロンビア大学ロースクール出身で、著名な訟務弁護士でもあることから、人権感覚も鋭い。

アメリカのIT産業界トップが、顔認証技術（FRT）に対する業界の社会的責任と法規制を求めた意見であることから注目に値する。わが国の顔認証技術（FRT）でビジネスを展開するIT産業界は、市民のプライバシー、人権を商品にして、儲けだけに執着しがちで、しかも社会的責任に対する意識が希薄である。生体認証情報は、唯一無二の生物的特徴で、個人の最もセンシティブな情報である。漏れても変えられない。軽率に取り扱うことは、きわめて深刻な人権問題につながりかねない。スミス氏の真摯な訴えに耳を傾け、業界としての社会的責任を果たすべく、利益だけを追い求める姿勢を猛省し、学ぶべき点も多いのではないか。そこで、石村耕治PIJ代表に、CNNニュース編集局中村克己が質問をする形で、スミス社長の講演の概要を紹介していただいた。

(CNNニュース編集局)

■米マイクロソフト社の顔認証技術の法規制必要性の呼びかけ

— 米マイクロソフト社は、同社のスマートフォン「iPhone（アイフォーン）」に顔認証技術（FRT）を使う一方で、この技術の法規制を訴えているということですが。一見、矛盾するような感じを受けますが？

(石村) スミス（Brad Smith）社長兼最高法務責任

者の講演によると、同社は、2018年6月に、進化する顔認証技術（FRT）に対処するための政府規制を求めると同時に、産業界の社会的責任について同社のスタンスを明確にする方針に転じたということです。スミス社長は、顔認証技術（FRT）は、社会に有用であると評価する一方で、潜在的に濫用の危険があると指摘しています。同社は、この技術の問題点について、世界中の技術者、会社、

市民団体、学者、公職者と議論を続けてきているとのことです。

—— スミス社長は、アメリカにおける顔認証や指紋などの生体情報の法規制の状況や、裁判の状況などを理解したうえで、講演で、規制の必要性を呼び掛けたのだと思います。それで、議論の結果、米マイクロソフト社は、一応の結論のようなものは得られたのでしょうか？

(石村) スミス社長の講演によると、同社は、政府が、できるだけ早く顔認証技術 (FRT) を規制するに必要な法整備の検討を開始すべきであると指摘



スミス・ブラッド社長 (public use)

しています。この技術は、丁度、底から浮かび上がってきた悪霊 (genie) のようなもので、何もしないで放置しておくと、5年

もすれば、いたるところでこの技術が使われ、社会に対する危険性が拡大すると警鐘を鳴らしています。その頃には、この技術の危険性を封じ込めることは極めて難しくなるとしています。とりわけ、市場競争 (market forces) のルールのもとで、IT 企業に対して市場での成功と社会的責任の両立を求めるには、この技術を開発する企業とその技術を利用する機関が、法の支配 (the rule of law) により統治される必要がある旨指摘しています。

—— スミス社長のいう「法の支配」は、どのような仕組みなのでしょう？

(石村) マイクロソフト社は、顔認証技術に関するすべての潜在的な問題に対して回答を用意することは難しいとしています。技術の進歩を止めることはできないけれども、同時の公益 (public interest) を保護できる立法を検討することで満足な回答が得られるのではないかと指摘しています。また、政府は、立法にあたり、この技術の発展に沿ったペースを保つことが重要なことを指摘しています。

—— 政府は、規制をかけるにしろ、顔認証技術の発展に追い付いて行かないとダメだということですね。

(石村) そうです。マイクロソフト社を含む IT 企業は、遅々として進まない政府が行動するのを待たなければならないとしています。そこで、IT 企業として独自の立場からこの技術に対する安全対策を模

索しているとのこと。

—— IT 産業界は、どのような安全対策を模索しているのでしょうか？

(石村) マイクロソフト社を含む IT 企業は、顔認証技術に対して否定的な意見を持っているわけではありません。スミス社長は、他の先端技術と同様に、顔認証技術の進化は止められないとする一方で、この技術を注意深く利用する必要があると指摘しています。マイクロソフト社は、社内での慎重な検討後、6つの基本原則を定立し、2019年初頭までに実施する計画であることを明かしています。加えて、顧客が、顔認証技術を責任ある方法で利用するに必要な情報提供と研修プログラムを公表するとしています。

—— マイクロソフト社は、他の先端技術とは差別化した形で、顔認証技術の利用に特化した責任体制を構築する方向なのですね？

(石村) そうですね。顔認証技術は、監視カメラなどと連動するかたちで、政府セクターに加え、民間セクターでも利用が進んでいます。同時に、こ



顔認証 (public use)

の技術は若い技術で、利用方法が定まっていないところがあります。そこで、スミス社長は、双方のセクター

において、社会的な利益を図る一方で、技術の濫用を防止する方向でこの技術に特化した形で安全対策を練るとアナウンスしています。

■顔認証の利点

—— マイクロソフト社は、顔認証技術のビジネスで利益をあげていますから、スミス社長は、この技術には肯定的なわけですね。

(石村) そうですね。スミス社長の講演では、顔認証技術の利点をあげています。例えば、インドのニューデリーでは、顔認証技術を使って4日で3,000人もの失踪した子どもが発見されたことをあげています。このように、講演では、ほかにもATMで顔認証技術を使うことでなりすましを防止できる例などを示して、顔認証技術の、利点、プラス面をあげています。

■顔認証の課題

—— スミス社長は、この技術の問題点、課題も

あげているのですか？

(石村) スミス社長は、顔認証技術は、その濫用の危険を秘めている点を指摘しています。顔認証技術に関して政府が対処を求められる課題としては、大きく次の3つがあると指摘しています。

【図表 1】 顔面認証の課題

- ①現在の技術の発展状況では、顔認証の判断、とりわけ、バイアス（偏見）、事例によっては、差別を禁止する法律に触れる結果も出てくる。
- ②顔認証技術の利用の拡大は、新たな市民のプライバシー侵害を引き起こす可能性を増大させる。
- ③政府による大衆監視のための顔認証技術の利用は、民主的自由（democratic freedom）の侵害につながる可能性がある。

■バイアス（偏見）や差別への対応

—— スミス社長は、顔認証技術の利用により生じるバイアス（偏見）や差別にどのように対応するように求めているのですか？

(石村) スミス社長は、とりわけ、現在の技術レベルでは、顔認証技術利用の結果、その判断の誤りの危険性が高く、偏見と差別禁止法に触れる事例も出てくることを認めています。とりわけ、最近の調査では、女性の性別や肌の色の判断において高い誤認率を示したことを指摘しています。スミス社長は、この点は、顔認証技術でビジネスを展開しているマイクロソフト社その他の IT 企業にとり、市場競争が不良なサービス改善の重い圧力になっており、IT 企業側も重要な技術面での改善点であることを認識するようになってきていると指摘しています。スミス社長は、リスクを最大限に少なくするために、IT 企業とその顧客との間で、この技術の適切な使い方について真摯に検討することも重要であることを確認しています。そのためには、市場の力が必要不可欠であるとしています。

—— スミス社長は、顔認証技術の法規制については、どのような主張をしているのでしょうか？

(石村) スミス社長は、顔認証技術に対する法規制の必要性を説いています。その理由として、次の2つあげています。

【図表 2】 顔認証技術への法規制が必要な理由

- ①市場競争による規制がより効果的に働くようにするためには、顔認証技術を利用する顧客に対して、この技術の的確性および利用の仕方や状況により生じる偏見を含む不公正な偏見のリスクについて十分に説明するとともに、検証（テスト）できるようにすることにする必要がある。現状では、こうした偏見

を減らすための各 IT 企業による努力には差がある。このため、市民団体や研究者による顔認証技術に対する評価を不透明なものにしている。この点を改善するには、新たな法律が必要である。

この視点から、新たな法律には、次の2つの項目が含まれるべきである。

- ・透明性の確保 顔認証サービスを提供する IT 企業に対して、その顧客や消費者が理解できるように、顔認証技術の性能や限界を説明する情報を提供するように義務付けること。
- ・第三者による検証および比較の制度化 商業的な顔認証サービスプロバイダーに対して、独立した第三者に自己の提供するサービスの的確性および不公正な偏見の有無について合理的な検証の実施を依頼し、かつ公表するように義務付けること。インターネットを使って遠隔アクセスする形で顔認証サービスを提供する IT 会社に対しては、より繊細な検証が求められること。

②市場競争により、顔認証サービスの利用による偏見や差別の解消は可能であるとする考え方もあるが、このサービスが消費者や市民に対する悪影響を及ぼす使い方でリスクが増大しているという証拠がある。この点を改善するには、新たな法律が必要である。

この視点から、新たな法律には、次の2つの項目が含まれるべきである。

- ・人による慎重な審査 人間は、間違いや偏見から無縁ではないのはもちろんのことであるが、一定の状況下では、顔認証判断の審査を、単純にコンピュータに任せるのではなく、適格者に委ねるのも重要である。したがって、新たな法律では、この技術を利用する機関は、消費者に影響がある「重大な利用事例（consequential use cases）」とみなす場合には、その最終判断をする前に人による慎重な審査をするように義務付けるべきである。こうした事例には、その判断が消費者の身体もしくは精神に侵害を及ぼす危険を伴う場合、人権もしくは基本権が関係してくる場合、または消費者の個人の自由もしくはプライバシーとぶつかる場合などがあてはまる。
- ・不法な差別目的での利用の回避 顔認証サービスを利用する機関は、個人消費者や消費者グループに対する差別を禁止する法律を遵守する義務を免除されないということを認識することは重要である。この法遵守義務は、顔認識の利用に基づく決定のため法のもとでの説明責任を考え合わせると、人による慎重な審査を必要とする理由になる。

■市民のプライバシー保護のための対応

—— スミス社長は、顔認証技術の利用による市民のプライバシー侵害にどのように対応するように求めているのですか？

(石村) スミス社長は、講演で、顔認証技術の幅広い利用は、新たに、市民のプライバシー侵害につ

ながる可能性を指摘しています。最たる例として、公的機関が、リアルタイムの顔認証技術の利用に基づくクラウドにつながった監視カメラを設置するケースをあげています。

そのうえで、スミス社長は、ロースクール出身でありながら先端技術に強い弁護士らしく、アメリカのプライバシーの概念の展開などについて法律論を展開しています。

—— 巨大IT企業の経営者であるスミス社長は、プライバシーの歴史などについてどのようなレクチャーをしたのですか？

(石村) スミス社長は、アメリカにおけるプライバシーは、カメラ技術の進歩からはじまったことを指摘しています。つまり、1890年に、後に連邦最高裁判事を務めることになるルイズ・ブランダイス (Louis Brandeis) とサミュエル・ウォーレン (Samuel Warren) が、共著で、ハーバード法学論集 (Harvard Law Review) に「一人にしておいてもらう権利 (the right to be let alone)」の論文を発表したのが、アメリカでのプライバシー権のはじまりであることを確認しています。その際に、2人が取り上げたのが、「早撮写真 (instantaneous photographs)」とその写真を掲載した営利の新聞の頒布について、あらたなプライバシー権 (right to privacy) を法認して市民を保護しようという考え方の芽生えであったことを指摘しています。

スミス社長は、今日、技術は、ブランダイスやウォーレンが問題にした早撮写真の技術の時代では想像できなかったほど進化しており、市民がショッピングモール (商店街) にひとたび足を踏み入れれば、あらゆる角度から撮像されるのみならず、コンピュータによりどこへ向かおうとしているのかまで認識されるようになっていくことを指摘しています。1つのカメラが撮像した情報は、蓄積され、異なる位置に設置された複数のカメラが撮像した情報とリンクされ、モール内の店舗間で共用される状態にあり、顧客が何を買おうとしているかまで予測が可能であると指摘しています。

—— ライブの顔認証式監視カメラによる人物の追行に加え、基地局・Wi-Fi・GPSなどを使ったスマートフォンからの位置情報の収集も歯止めが利かないわけです。こうした状態にあって、スミス社長は、顧客のプライバシーをどのように護ろうというのでしょうか？

(石村) 消費者である市民が古典的な意味での「一人にしておいてもらう権利」を享受できる時代で

ないことは周知の事実です。スミス社長は、マイクロソフト社の考えは、法律で商業施設が顔認証技術の利用ができないようにすることではなく、各店舗がこの技術やその他のデジタル技術の責任ある利用ができるように支援することにあると言明しています。つまり、顧客サービスの一環として、ルールある顔認証技術の商業利用を打ち出しているわけです。

—— スミス社長は、市民が顔認証式監視カメラに囲まれた常態を解消する方策は示していないわけですが、顔認証技術のルールある民間利用として、どのようなことを考えているのでしょうか？

(石村) スミス社長は、まず、市民はこの種の技術がどのように使われているのか知る権利があるとしています。つまり、この技術の透明性の確保が必要だと指摘しています。その手段として、次のような内容の新たな法律が必要だとしています。

【図表3】顔認証技術利用の透明化のための法制

- | |
|--|
| <p>①消費者への告知 消費者の身元確認をするために顔認証サービスを利用する事業者は、このサービスを利用していることを明確に伝えるために、目立つ告知をするように法律で義務付けること。</p> <p>②明確な同意 消費者が店舗に入ったときに顔認証サービスの利用に同意できるようにまたはオンラインサービスの利用を開始するときにこの種の明確な通知を受けられるように法律で義務付けること。</p> |
|--|

—— スミス社長の提案は、業界益を代弁するだけで、消費者の個人データ保護の理念からは程遠いようにもみえますが？

(石村) スミス社長も、GDPR (一般データ保護指令) を施行したEUでは、収集した個人データの目的外利用の禁止、データ主体のアクセス権、内容訂正権などを法認しており、アメリカでのプライバシー保護は遅れていることを認めています。EUの経験などを参考に、今後、進化した顔認証データの透明化法制の確立に努力していかないといいています。スミス社長の講演は、この面では、やはり業界益の代弁者のような内容だと思えます。法律家よりも、経営者の顔が大きく反映されていると感じます。

■政府機関による顔認証技術の利用のコントロール

—— 顔認証技術の利用は、民間企業に加え、警察その他の政府機関でも幅広く利用されています。CNNニュース本号でも紹介されているように、カ

リフォルニア州サンフランシスコ市のように、地方団体によっては、公的機関での顔認証技術の利用を禁止する条例を定めるところも出てきています。スミス社長は、政府機関（公的機関）でのこの技術の利用についてはどのような考えなのでしょうか？

（石村）スミス社長も、顔認証技術の政府機関による大衆監視のための利用は、民主的自由（democratic freedom）や人権（human rights）の侵害につながる可能性が高いことを率直に認めています。

スミス社長は、市場主義、民主主義、自由と人権を尊重する経営者だと思います。スミス社長は、この講演で、民主主義は、市民が、私的にも公的にも、政府から常時監視を受けることなくどの程度まで自由に集会を持ち、会合し話し合いをすることができるかどうかにより測ることができることを説いています。各種政府機関は、顔認証技術を各所で多数利用しており、一般市民の安全を確保し、かつ質の高い公共サービスにつなげていることを指摘しています。その一方で、顔認証技術は、潜在的に市民の基本的な自由を危険に陥れる目的で利用することも可能なことを認めています。政府は、顔認証技術を利用し、至る所に設置された監視カメラ網や大規模なコンピュータの力、データのクラウド保存などを結合させることで、特定の個人を常時監視することが可能であると認めています。顔認証技術は、利用の仕方では、前例のないような大規模監視に途を開くことも可能だと指摘しています。

スミス社長は、ジョージ・オーウェルが小説「1984年」で描いたような双方向通信による大衆監視国家の誕生について触れ、オーウェルは、約70年前に描いた姿は、今日の技術をもってすれば可能であると認めています。しかし、私たちは、2024年が小説「1984年」のページのようにならないようにしないとけないと警鐘を鳴らしています。このためには、常に、いかなる政府も法を超越して存在してはならないという考え方が欠くことのできない民主主義の原理でなければならないとしています。これは、今日的にいうと、政府の顔認証技術の利用は、法の支配に服さなければならないということ意味すると指摘しています。顔認証技術を規制する法律も当然こうした考えに基づいて制定されるべきであるとしています。

■政府による顔認証を使った特定個人の監視容認の要件

—— スミス社長は、政府、多くは警察など行政機関による顔認証技術の利用、とりわけ特定個人の監視のための利用について、どのような意見をもっているのでしょうか？

（石村）スミス社長は、民主的自由の侵害につながる顔認証の利用を防ぐために、法規制は、法執行機関が公共空間で特定個人の監視のために顔認証の利用ができるのは、次の要件を充たす場合に限られるべきだとしています。

【図表4】政府による顔認証を使った特定個人の監視を容認する要件

- | |
|--|
| ①裁判所の決定 この種の監視のために顔認証サービスを利用するにあたっては、その利用を認める裁判所の決定（court order）によること。または、
②緊急の場合 人の死亡その他身体への甚大な侵害につながる重大な危険またはリスクが伴う緊急性がある場合 |
|--|

—— スミス社長があげた顔認証技術利用要件は、特定個人の逮捕の要件に似ていると思いますが？

（石村）スミス社長は、警察のような法執行機関が特定個人の監視にこの技術を利用する場合には、伝統的な相当の理由（probable cause）基準による捜査令状の発行要件に準じて、裁判所は、決定すべきであるとしています。加えて、失踪者の発見などへのこの技術の利用を、適切な利用をして認めるべきであるとしています。

2018年6月に連邦最高裁判所は、政府は、人が通行した位置を確認する目的で携帯電話記録を、捜査令状なしには入手することはできない、と判断しました（Carpenter v. United States, 585 U.S. ____《2018》）（以下「カーペンター判決」ともいいます）。スミス社長は、この判断の多数意見を書いたジョン・ロバーツ最高裁長官（Chief Justice John Roberts）が、個人は、「自己の物理的移動の記録に対する正当なプライバシー権を期待できる（an individual has a legitimate expectation of Privacy in the record of his physical movements）」と述べた点に注目しています。

スミス社長は、私どもは、公共空間を自分の携帯電話を持って移動しており、しかも実際には携帯電話サービス会社と自分の位置情報を共有しているとしても、連邦最高裁は、自分の位置情報記録は、連邦憲法修正第4条〔令状主義・不合理な捜索・押収・抑留の禁止〕の保護の対象となると

判示した点を高く評価しています。つまり、スミス社長は、最高裁の判断に従うと、政府は、罪を犯したと信じるに足るだけの相当な理由があると独立した裁判官が判断し、発行した捜査令状がなければ、携帯電話やその通話位置記録を通じて私たち市民の移動を追跡することはできないという判断を尊重しなければならないと指摘しています。

—— スミス社長は、顔認証技術の公的利用に対して、この2018年のカーペンター判決をどのように生かそうとしているのでしょうか？

(石村) スミス社長は、連邦最高裁のカーペンター判決を、顔認証技術の課題に置き換えて、議論の展開を試みています。スミス社長は、顔認証については新たな憲法問題が生じていると認めたうえで、「顔面は、通話と同じ保護をする価値があるのか」と問うたうえで、「はっきりとYesだ」と答えています。

スミス社長は、マイクロソフト社は、顔認証技術により大衆監視が可能な時代に入ったことを受けて、2013年以来、市民のプライバシー権を護るために、会社が原告になって合衆国（連邦）政府を相手に4件の訴訟を起こしているとのこと。マイクロソフト社は、繰り返し、連邦憲法修正第1条〔信教・言論・出版・集会の自由・請願権〕や修正第4条〔令状主義・不合理な捜索・押収・抑留の禁止〕に具体化された永劫の価値をしっかりと保護するように求めているとのこと。スミス社長は、自由を危険にするほど顔認証技術の利用が広がりを見せる前に行動を起こすことが重要だと指摘しています。この問題は、最終的には連邦最高裁で司法的に決着がはかれることになるとしても、有権者から選ばれた人たちが、各州の州都やワシントンD.C.において、市民の権利を護るための立法に向けて行動をスタートさせるべきではないかと説いています。

アメリカにおいては、カリフォルニア州サンフランシスコ市のように、地方団体によっては、議会が、公的機関での顔認証技術の利用を禁止する条例を定めるところも出てきています。スミス社長は、公的機関での公的機関での顔認証技術の利用を禁止に賛成しているわけではありませんが、こうした立法府の取組みを支持しているものと解されます。

■法令の先を見据えたマイクロソフト社の顔認証に関する6原則

—— スミス社長は、法令による顔認証技術の規

制を上回るIT企業による自主規制の必要性を訴えているようですが、どのような内容のものなのでしょうか？

(石村) スミス社長は、この講演で、顔認証技術の新たな法令による規制は必要不可欠とする一方で、IT企業が負うべき社会的責任を法令で代替することはできないとの認識を示しています。マイクロソフト社は、2018年6月に、顔認証業務を統治するため、評価および開発に関する原則をアナウンスし、コメントを求めたことを紹介しています。同社は、6か月間にわたり、国内外の従業者、顧客、公職者、学者市民団体などからコメントやアドバイスを求め、慎重な検討をしたうえで、6つの原則にまとめ、公表しました。

—— マイクロソフト社が先を見据えて採択した顔認証に関する6原則を紹介してください。

(石村) スミス社長が講演のなかであげたマイクロソフト社の顔認証に関する6原則は、図説すると、次のとおりです。

- ①公正 (Fairness) マイクロソフト社は、すべての人々を公正に取り扱うように努める方法において顔認証技術の開発および利用するための業務を展開します。
- ②透明性 (Transparency) マイクロソフト社は、顔認証技術の性能と制限について資料を作成し、かつ伝達します。
- ③説明責任 (Accountability) マイクロソフト社は、顧客が顔認証技術を、人に重大な影響が及ぶ可能性のある利用に供する場合には、人による適切な水準のコントロールを確保できるように奨励し、かつ支援します。
- ④差別禁止 (Non-discrimination) マイクロソフト社は、サービス契約の条件として、不法な差別を行うねらいで顔認証技術を利用することを禁止します。
- ⑤告知と同意 (Notice and consent) マイクロソフト社は、民間セクターの顧客に対して、顔認証技術を利用する場合には、消費者への技術利用の告知と消費者からの同意を得るように奨励します。
- ⑥合法的な監視 (Lawful surveillance) マイクロソフト社は、法執行目的での監視が行われる場合、市民の民主的自由の保護のための主張をし、かつ、こうした自由が危険になると信じるときには顔認証技術を利用しません。

—— 世界的な優良IT企業であるマイクロソフト社は、顔認証技術に対する法令規制とは別途に、こうした6原則を梃に、企業倫理あるいは企業の社会的責任のあるIT企業のフロントランナーとしての行動をとろうとしているようにも見えますが？

(石村) スミス社長は、この講演で、顔認証は比較的历史が浅い技術であり、今後どのような問題が出てくるのか検討がつかないことを認めています。したがって、顔認証技術に関する6原則を、さらに実のあるものにするために、社内や社外からの多様な意見を聴くとアナウンスしています。

確かに、新たな技術を生み出し巨大な利益を上げているIT企業にとり、利益の確保が最大の命題であることは否定できません。マイクロソフトが、こうした6原則を梃に、企業倫理あるいは企業の社会的責任のあるIT企業のフロントランナーとしての行動をとろうとしているのには、わが国IT企業も学ばないといけないと思います。

—— 2019年4月に、ニューヨーク市に住む18歳の学生が、アップル社の店舗で同社の顔認証ソフトの誤検知が原因で盗難を働いた容疑で誤認逮捕された事件で、その学生が、深刻な精神的ダメージを受けたとして、マンハッタンにある連邦地裁に10億ドル(約1,100億円)の損害賠償の支払いを求めて訴えを起こしたと報道されていますが？

(石村) 直接マイクロソフト社のスミス社長の講演とは関係はないのですが、顔認証技術に関連するケースなので、触れます。

「USA Today」(2019年4月23日)によると、この事件では、米アップル社の顔認証ソフトによる誤検知が原因で、同社の店舗での窃盗への関与が疑われた18歳の学生に、捜査当局が自宅で逮捕令状が提示されました。しかし、提示された逮捕令状の自分とは違う人物の写真が添付されていたことから、誤認逮捕であるとして、アップル社を訴えたわけです。訴えを起こした学生によると、過去に写真付きでない仮免許証を失くしたことがあり、それを盗んだか拾った者がアップル店舗で身分証明に利用した可能性があるとのこと。その結果、アップルが店舗で窃盗犯追跡に使っている顔認証システムが検知した犯人の顔に自分の名前が誤ってリンクされたとみられるのではないかと主張しました。「深刻なストレスと苦痛」を被ったとして10億ドルの損害賠償を求めて訴えたわけです。

■むすびにかえて～待ったなしのわが国での顔認証技術の法規制

—— わが国でも、顔認証技術の法規制、IT企業によるこの技術に対する社会的責任が問われていると思います。最後に一言お願いします。

わが国では、2017年に、パナソニックが参加して、空港での出入国審査に顔認証ゲートが導入されました。また、東京オリンピック・パラリンピックでは、競技大会組織委員会が、セキュリティ対策として、顔認証技術を積極的に活用するとアナウンスしています。このように、はっきりした利用ルールも、法令や条例による規制もないなかで、監視カメラなどと連動した形で顔認証技術の利用がIT企業主導で一方向的にすすめられています。顔認証の利用は、技術の便利さが先行して、いまや行政機関や警察、公的機関、民間企業に広がっています。この技術が、私たち市民が気づかないところで、生活の見守りだけでなく、防犯、治安対策などに幅広く利用されてきています。近年登場してきている無人店舗のシステムも、民間企業による顔認証技術の塊のような設計になっています。

私たち市民は、認証された顔のデータはどこにいつてしまうのか？誤認証ないし誤検知によるトラブルが生じた場合誰が責任を取るのかも不透明です。はっきりしたルールもなく、顔認証技術を提供するIT企業側も、この技術を利用する側も、市民の疑問に答えられないのが実情です。加えて、撮像された主体への認証データのアクセス権も不透明なままです。

マスメディアやこの分野で専門家を名乗る人たちも、お隣の中国の「天網」という顔認証式の全国的な監視カメラ網を活用した国民監視制度、データ国家主義については、「人権侵害ではないか？」などと批判的な論調を展開したりしています。しかし、このままいけば、わが国内におけるIT企業主導の顔認証式の監視カメラシステムも、中国以上になることは容易に想定されます。にもかかわらず、顔認証技術の公正な利用を目指したルールづくり、法規制を提言する識者や企業は皆無に近いわけです。生体認証情報は、唯一無二の生物的特徴で、個人の最もセンシティブな情報です。漏れても変えられないわけです。軽率に取り扱うことは、きわめて深刻な人権問題につながりかねないわけです。パナソニックとか、NECとか、顔認証技術で利益を上げているわが国のIT企業に、この技術の開発・利用に対する社会的責任を感じてもらい、マイクロソフトのような姿勢を見習って欲しいとのことです。政治も、顔認証技術を野放しにするのではなく、市民のプライバシー、人権を護るための法規制を積極的にすすめないといけません。

清水晴生教授に石村耕治 PIJ 代表が聞いた

顔認証技術の市民的 コントロールを考える

対論

話し手 清水晴生（白鷗大学教授）

聞き手 石村耕治（PIJ代表）

顔 認証技術（FRT=facial recognition technology）が、幅広く使われてきている。この技術は、マイクロソフト社の iPhone（アイフォーン）、パソコン（PC）ロックの解除や、〇〇ペイといった決済サービスなどにも登場してきている。一方、警察は、AI（人工知能）やライブ監視カメラと連動させ、顔認証のアルゴリズム（情報処理手順）で、群衆のなかから指名手配犯を探し出すのに使っている。また、拘束した犯罪者のデータベースと顔写真を照合するために使っている。

2018年8月7日に、東京オリンピック・パラリンピック競技大会組織委員会は、2020年の東京五輪で顔認証技術をセキュリティ対策として利用すると発表した。委員会の方針に従い、NECなど民間IT企業が、顔認証技術の活用プログラムを進めている。

このように、顔認証技術の官民にわたる利用は、飛躍的な広がりを見せている。市民は、一般に、顔認証という生体情報による検知には、利点が多いと考えている。しかし、その一方で、「ビッグ・ブラザー（独裁者）」によるデータ監視社会化への懸念が強まっているのも現実である。

中国が適例である。同国では、個人データは国家がトータルに管理・監視するとするデータ国家主義をとる。同国では、「天網」という、顔認証システムを国中に張り巡らせている。これにより、国家が国民データを集約管理し、AI（人工知能）を活用し、国民の移動の自由を逐次把握し、トータルな国家監視のもとに置く計画を積極的に進めている。

アメリカでも、成人2人に1人にあたる2億人に近い顔面情報が官民の各種顔認証データベースに登録されている実情にあるという。しかも、収

集時の本人の同意もなく顔認証情報が収集され、顔認証データベースへの本人のアクセス権をはじめとした透明化法制がほとんど整備されていないという。この現実を、人権感覚の鋭い学者や電子フロンティア基金（Electronic Frontier Foundation）のような市民団体は、極めて憂慮している。運転免許証番号やパスポート番号は、紛失し悪用が危惧される場合は変更ができる。ところが、顔認証情報のような生体認証情報は、紛失したからといっても、変更ができないからである。

また、法規制が皆無の状態では、顔認証技術による住民監視は、自治体をあたかも「バーチャルプリズン（仮想監獄）」に仕立てるのに等しい。「無罪推定」のルールが反故にされたり、有色人種やマイノリティ、低所得者などの自由や人権を侵害したり、差別を助長しかねないからだ。

中国は、社会主義国で、人権や自由が制約されており、アメリカや日本などとは異なるはずだ。ところが、現状では、アメリカも中国並みの人権状況ではないかとの批判が巻き起こっている。わが国も、東京五輪・パラリンピックでの顔認証技術の利用についての法規制、透明化手続は後回しで、ブラックボックス化したままである。これでは、顔認証技術の利用について、中国の人権状況をとやかくいうことはできまい。

アメリカでは、トランプ政権の誕生後、国境警備などへの顔認証技術の拡大利用が懸念された。これを機に、顔認証技術利用の法規制問題が炎上した。2016年9月21日に、アメリカ自由人権協会（ACLU=American Civil Liberties Union）は、「警察の監視をコミュニティが監視する（CCOPS=Community Control Over Police Surveillance）」プロジェクトを開始した。具体的には、各州、とりわけ州内にある自治体に対して、「秘

密の監視にストップをかける条例（Stop Secret Surveillance Ordinance）」の制定を呼び掛けた。この呼びかけに応じ、州レベルでは、メイン州議会が、2017－8年会期に、上院に法案「監視技術に関する透明化を推進する法律（An Act to Promote Transparency with Respect to Surveillance Technology）」を提出している。諸州の法案の中身は千差万別である。メイン州の法案は、州が一定の活動について監視技術を取得または利用する場合には、それに先立ち、公聴会を開催しかつ州議会の承認を得ることを義務付けるものである。カリフォルニア州議会でも、2019－20会期に、規制法案が提出されている（CNN ニュース本号《99号・35頁》記事参照）。

一方、地方団体レベルでは、カリフォルニア州（加州）の地方団体で条例制定に向けた活発な動きが見られる。例えば、サンフランシスコ市は、2019年5月14日に、人工知能（AI）を使った顔認証技術（FRT=facial recognition technology）を自治体の行政機関や警察が利用することを禁じる条例案「秘密監視規制条例（Stop Secret Surveillance Ordinance）」案を、委員会（Board of Supervisors）で、8対1の賛成多数で可決した。その後、21日に市議会で可決した。1カ月以内に施行する。アメリカの主要な地方団体で、この種の禁止条例を制定したのは同市が初となった。（CNN ニュース本号《99号・35頁》記事参照）。また、加州バークレー市も条例案市議会で検討中である。同市の条例案（バークレー市自治体コードに、第2.99条「監視技術の習得および利用」を加える改正）では、①目的、②定義、③市議会承認要件、④監視装置の暫定的な取得および利用、⑤現行の監視技術へのコンプライアンス、⑥市議会による費用と効果を評定、⑦市議会承認後の監視、⑧監視技術契約への開示請求、⑨執行、⑩内部告発者の保護、⑪可分性条項からなる。オークランド市など加州の他の地方団体の議会も、同様の条例制定に向けて走り出している。

この種の地方団体条例の内容もことごとく異なる。しかし、一般には、地方団体が、監視カメラや顔認証技術のような監視技術をどのように使うのか、議会に規制権限を付与し、住民の意思に委ねることを目的とするものである。また、年次報告書の作成など、監視技術の利用に関する透明性を確保する制度の構築を目指すものである。

注目すべきは、米マイクロソフト社のブラッド・

スミス社長も、顔認証技術の濫用や不適切な利用による偏見や差別を禁止し、プライバシー権を含む自由権を護るために、この技術のホワイトボックスを含め法規制の必要性を訴えていることである。また、同社は、この技術の人権侵害につながるような不適切な利用や違法利用を防ぐために、IT産業界がこの技術に関する透明性を高め、市民に対する説明責任、社会的責任を果たすように求めている。

わが国では、東京都杉並区が「防犯カメラの設置及び利用に関する条例」を制定（平成16年7月1日施行）、監視カメラの法規制のさきがけとなった。同条例3条では、「防犯カメラを設置し、又は利用するものは、区民等がその容ぼう・姿態をみだりに撮影されない自由を有することにかんがみ、防犯カメラの設置及び利用並びに画像の取扱い（以下「防犯カメラの設置等」という。）に関し、適正な措置を講ずるように努めるものとする。」とし、規制目的が、最高裁判例に盛られたプライバシー概念を引用し、区民の個人情報保護にある旨を明確にした点は大きく評価できる。ちなみに、この条例制定にあたっては、石村耕治PIJ代表も、杉並区監視カメラに関する専門家会議に委員として参加し、積極的な役割を果たされた。

“単なる監視（防犯）カメラ”の規制と、“顔認証技術（FRT）を利用した監視（防犯）カメラ”の規制とは、分けて考える必要がある。FRTを使った紛失・悪用されても変更できない生体認証情報の収集については、本人の明示の同意が必要であると同時に、厳正な取扱い〔収集・保存・安全管理・開示・破棄など〕が求められるからである。アメリカの地方団体が、監視カメラの設置は「OK」であるが、設置される監視カメラに顔認証技術（FRT）の利用を「NO」とする条例を制定した理由である。

アメリカにおける顔認証技術（FRT）の法規制の動きを参考にし、わが国でも、自治体レベルで、顔認証技術（FRT）の法規制／ホワイトボックス化の検討を急がないといけないのではないかと。東京五輪・パラリンピックを契機に、官民共同で集約された顔認証データについては、情報主体である本人には、所有権があるはずだ。NECとか開発に携わったIT企業やデータ保存機関が、そのデータの取扱いを透明化せず、不適切に取り扱うとすれば人権問題である。顔面データの消去・管理、本人のアクセス権を含め、法的手続を定め、市民の閲覧に供する必要がある。市民の明示の同意

(opt-in) もないまま顔認証情報を収集するという透明でない顔認証技術 (FRT) の取扱いは極めて危険である。

今回は、顔認証技術の人権侵害につながるような不公正あるいは違法な利用への法規制やこの技術のホワイトボックス化、さらには、この技術で

ビジネスをする IT 企業の社会的責任を含め、顔認証技術の市民的コントロールの必要性、そのための法理論の展開や法解釈について、清水晴生 白鷗大学法学部教授と石村耕治 PIJ 代表に議論いただいた。

(CNNニュース編集部)

◆問われる東京五輪・パラリンピックでの野放図な顔認証技術の利用

(石村) 2020 年の東京五輪・パラリンピックでは、セキュリティ対策として顔認証技術 (FRT) を利用します。オリンピック史上初めてのことです。顔認証技術の利用については、安全対策のために市民にプライバシーを犠牲にすることを強いることと、人権の保護とのバランスを取ることの難しさを感じます。今回は、特に司法の介入もなく、不特定多数者を相手に監視することの法的課題について、一緒に考えていきたいと思います。

(清水) 何のルールもなく、野放し状態で、顔認証技術の利用が広がるのはダメですね。オリンピックを機会に、生体認証技術 (FRT) を使った個人データ (情報) 取扱規制の検討を急ぐ必要がありますね。

(石村) 東京五輪での顔認証は、観客ではなく、30 万人以上におよぶ出場選手や大会スタッフ、ボランティア、報道関係者に対して使われる予定です。40 か所以上の会場への出入りには電子チップを内蔵した ID カードが必要となります。東京オリンピック・パラリンピック競技大会組織委員会 (組織委員会) の警備局長によると、対象者は五輪施設に入るたびにセキュリティチェックを受けることになります。組織委員会は IT 企業の NEC と提携してシステムを開発しています。NEC の執行役員によると、メイン・スタジアムや国際放送センター、オリンピック村など 40 以上の施設に顔認証システムを導入するとのこと。しかし、顔認証システムの運用ルールとか、認証データの取扱いとかについての情報がまったく不透明です。まさに、ブラックボックスそのものです。顔認証技術 (FRT)、顔認証データ取扱主体はどこなのか (組織委員会 or 警視庁)、データ主体からの明示の同意はどう取るのか、顔認証データの刑事目的での利用や芸部提供と令状主義等々、問題だらけです。

(清水) こうした顔認証技術利用にクレームを言っている市民団体などはないのですか？

(石村) 生体認証技術などを使ったテロ対策などに

「盗聴法に反対する市民連絡会」などが反対しています。〔【声明】2020 東京オリンピック・パラリンピック (以下、たんに「東京五輪」ともいいます。) を理由としたプライバシー権と市民的自由を侵害するテロ対策に反対します。http://www.anti-tochoho.org/ss20180906.html〕ただ、こうした市民団体は、法規制といった視点から具体的な政策提言をしていない感じがします。

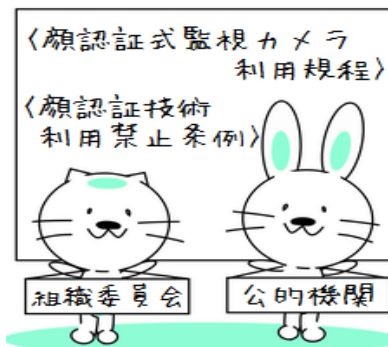
(清水) 東京都に対して、顔認証技術やそうした技術を利用したシステムの規制のための条例制定を求める動きはないのですか？あるいは、組織委員会に対して顔認証システムを透明化する運用規程の制定を求める動きはないのですか？

(石村) こうした市民団体は、オリンピックやテロ対策を理由として監視国家づくりに反対しています。しかし、顔認証技術に関する規制条例案を準備して都議会での議員条例制定を働きかける運動をするといった団体ではありません。そうした力量も欠いています。一方、わが国の自由人権協会 (JCLU) のような団体は、体制化してしまって、期待薄です。残念ながら、手本となったアメリカ自由人権協会 (ACLU) のようなエネルギーはもはやありません。

(清水) そうですか。東京都の場合、杉並区が、全国の監視 (防犯) カメラ規制条例づくりのさきがけとなった実績はありますからね。

(石村) そうですね。東京都杉並区が「防犯カメラの設置及び利用に関する条例」を制定 (平成 16

【図表 1】オリンピック悪用からルール化へ



年 7 月 1 日施行)、監視カメラの法規制のさきがけとなり、全国の自治体に波及していきました。同条例 3 条では、「防犯カメラを設置し、又は利

用するものは、区民等がその容ぼう・姿態をみだりに撮影されない自由を有することにかんがみ、防犯カメラの設置及び利用並びに画像の取扱い（以下「防犯カメラの設置等」という。）に関し、適正な措置を講ずるように努めるものとする。」とし、規制目的が、京都府学連最高裁判決（1969年12月24日大法廷判決・刑集23巻12号1625頁）に盛られたプライバシー概念（肖像権）を引用し、区民の個人情報保護にある旨を明確にした点は大きく評価できます。ただ、単なる監視（防犯）カメラの規制と、顔認証技術（FRT）を利用した監視（防犯）カメラの規制とは、分けて考える必要があります。FRTのような紛失・悪用されても変更できない生体認証情報の収集については、本人の明示同意（opt-in）が必要であると同時に、厳正な取扱い〔収集・保存・安全管理・開示・破棄など〕が求められるからです。アメリカの地方団体が、監視カメラには「OK」を出していますが、監視カメラに顔認証技術（FRT）の利用を「NO」とする条例を制定した理由です。

（清水） 顔認証技術は、スマートフォン（スマホ）その他さまざまな利用がされています。しかし、最も人権に及ぼす顔認証技術の利用は、監視カメラへの応用ではないでしょうか？

（石村） そうですね。

（清水） となると、既存の監視カメラ利用規制条例を参考に自治体条例で顔認証を含む生体認証データの取扱いを規制するというのも一案ですね。一般に、監視カメラ利用規制条例は、オムニバス（公的機関＋民間機関の双方を一括規制）方式ですよ。

（石村） そうです。ただ、顔認証情報のような生涯変更不可能な生体認証情報を本人の明示の同意なしに収集するのを認めてよいのか、そもそも論から考える必要があります。すでにふれたところですが、アメリカのサンフランシスコ市のように、「NO」としたところもあります。ところが、東京五輪では、AIを使って群衆からテロリストを自動検知するシステムの導入、映像は警視庁本部で瞬時確認をするとか・・・。

（清水） 市民から意見聴取もしない。まさに「問答無用」ですね。

（石村） ですから、顔認証技術や顔認証データの取扱主体、この場合だと、組織委員会になるのでしょうか？あるいは警視庁でしょうか？いずれにしろ、取扱主体が顔認証式監視カメラ利用規程をつくり、それを公開し、パブリックコメントを求め、市民

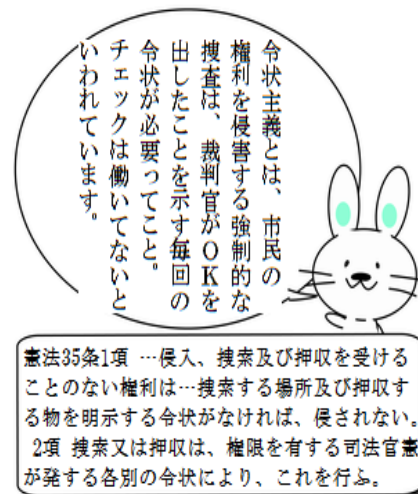
の意見を反映したうえで適正な利用をはかるのも一案です。もちろん、カリフォルニア州のサンフランシスコ市のように、公的機関が顔認証技術を利用することを禁止する条例を制定するという方向もあります。

◆顔認証技術を特定個人の検知に利用する場合の手続

（石村） 顔認証技術は、大きく①公的機関が利用するケースと②民間機関が利用するケースに分けて、検討することができます。清水先生にお伺いします。①公的機関が、顔認証技術を特定個人の検知に使う場合には、令状主義の適用との関係では、どのように解釈したらよいのでしょうか？

（清水） すでに発生した具体的な犯罪を捜査するために、捜査の相手に有無をいわず重大な権利の制約を強いる場合には「強制捜査」となります（最高裁1976年3月16日決定）。ですから、裁判官の発する個別の令状が必要となります。しかし、すでに警察が持っているデータベースと、官民の監視カメラから取り寄せた映像とを照合させるだけだとして。この場合だと、対象となった個人に対して権利の制約を強いているとはいえないともいえます。旧来の理解に従う限りであれば、の話ですが。

【図表2】令状主義とは



（石村） IT技術の発達などを考えると、旧来の理解では人権を護れないとすれば、どのような解釈、あるいは立法が求められるのでしょうか？

（清水） ビッグデータの

網羅性と情報端末の常時接続とによって、いまや個人のプライバシーが監視されるのは当然のようになっています。むしろ、監視されないのが稀になっています。ですから、これまでのようにパブリック（公的）な空間とプライベート（私的）な空間とを分けて、公開・公共空間であればプラ

イバシーは保護する必要がないという発想では追いつけなくなっています。

(石村) GPS 捜査の最高裁大法廷判決も、捜査における情報取得の「網羅性・継続性」を違法性の根拠としてはっきり指摘していましたね。

(清水) そうですね。警察を含む公的機関が映像（または画像）データ（情報）を取得したとします。この場合、これまで、データ（情報）は、自分らの所有物で、無期限・無制約にこれを自由に保管・利用し続けられるという発想・運用でした。しかし、こうした発想・運用自体が通用しなくなっていると思います。【編集部注：一般に、「画像」は静止画と音声のない動画をさすといわれます。一方、「映像」は動画をさし、音声のあるなしを問わないようです。ここでは、「映像」の言葉を使います。】

(石村) 清水先生のいわれるとおりです。各個人には、自分のデータ（情報）は自分でコントロールする権利が保障されています。ですから、映像データを（情報）を保有する警察などが、個人からの自己の映像データの開示や削除要求に応じないのでは、自己コントロールが及ばないということになります。ですから、プライバシーの権利が侵害されているといえます。

(清水) これまで、公的機関による個人市民の映像データ（情報）の取扱いについて、自己コントロール権などの問題は、隅に迫りやられてきました。しかし、官民双方の機関による個人市民の映像データ（情報）の取扱いについて、しっかり法的歯止

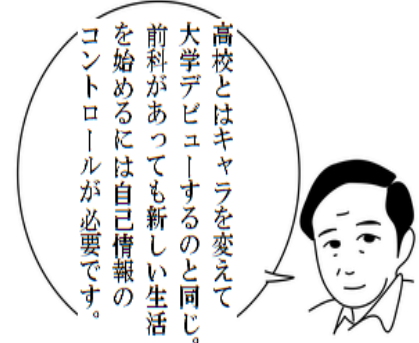
め策を考えないといけない時期に入っていますね。

(石村) 待ったなしです。わが国では、監視カメラによる映像データ（情報）に加え、顔認証技術（FRT）を使った顔認証データなど生体情報の収集も、極めて野放図に行われています。これも、もはや野放しにはできません。いずれにせよ、犯歴情報（前科など）と同様に映像データ（情報）の取扱いがいい加減で、再出発の妨げになったりする社会は好ましいとはいえません。ですから、警察などが期間の制限もなくいつまでも映像データを保有できるとするのは問題です。同時に、ネットに過去の犯歴データや画像がいつまでも搭載されるのも問題です。EU（欧州連合）では、自己情報のコントロール権として、「忘れてもらう権利（right to be forgotten）あるいは「削除権（right of deletion）」を法認しています。ですから、内容が真実（事実）であっても、忘れてもらう権利を行使して削除請求ができるわけです。

(清水) 話

【図表 3】自己情報コントロール権

を先ほどの GPS 捜査は違法とする最高裁大法廷決定に戻します。この最高裁決定では、警察が令状な



コラム

GPS 捜査と令状主義

GPS（Global Positioning System）とは地球の周りを回っている GPS 通信衛星から発信される電波を受信機が受け取り、位置を確認という仕組みです。大阪府警が、被疑者やその友人の車両に密かに GPS を装着し、位置情報を収集していることが、裁判で問われました。警察庁は 2006 年に GPS 捜査に関するルールを作成し、都道府県警察に通達していました。この内部通達では、GPS 捜査を「任意処分として実施する」、すなわち令状のいらない捜査と位置づけました。そして「犯罪を構成するような行為を伴うことなく」被疑者の使用車両などに GPS 端末を取り付けることができるとしたのです。

犯罪の捜査は令状主義に基づいて行われることが基本となっています。令状主義とは、警察や検察が行う捜査のうち、人権侵害のおそれの高い捜査については裁判所が発する令状がないとできないとするものです。よく知られているのは、逮捕

状や家宅捜索をする際の搜索差押令状などです。

2015 年 6 月、大阪地裁は令状のない GPS 捜査は違法だとする判決を下しました。続いて、2016 年 3 月、大阪高裁は、控訴を棄却しました。2017 年 3 月、最高裁判所大法廷は、上告を棄却し、GPS 捜査を令状の必要な強制処分にあたるとし、令状なしの GPS 捜査を違法としました（刑集 71 巻 3 号 13 頁）。さらに「GPS 捜査が今後も広く用いられる有力な捜査手法であるとすれば、その特質に着目して憲法、刑訴法の諸原則に適合する立法的な措置が講じられることが望ましい」という判断を示しました。

ちなみに、2012 年に、アメリカの連邦最高裁判所も、「令状をとらずに GPS 捜査するのは違憲である」という判決を出しています〔United States v. Jones, 565 U.S. 400 (2012)〕。

(CNNニュース編集部)

しに疑わしい人の車両に無断でGPSを装着して行動（位置情報）を把握するのは違法であるとしてしました。その理由は、GPS捜査は、今の刑事訴訟法に定めがあって令状があれば許される「検証」（対象の状態を五感の作用で知覚する捜査の方法）に似てはいてもそれでは捉えきれず（検察サイドは任意捜査でないとしても検証令状で可能だと主張していました。）、今の刑事訴訟法に定めがないために許されない「検索」とでも呼ぶべき、別の新たな捜査の方法だとしてしました。

（石村）「検索令状」というのがそもそも法的に存在していないわけですね。

（清水）「検索」という捜査手法は刑事訴訟法に定められていません。`法定されていないと強制捜査を行うことはできないこと、を「強制処分法定主義」といいます。

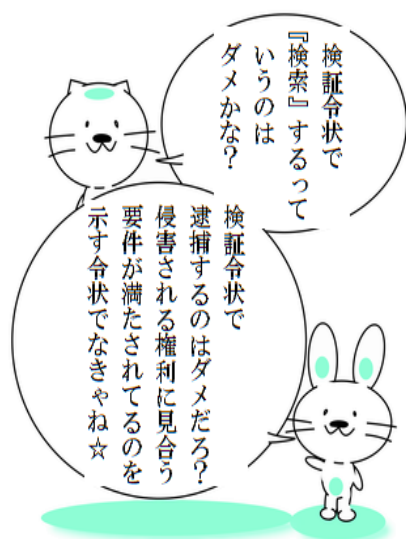
（石村）なんか、難しいですね。

（清水）それでは、イラストで説明します。次のとおりです。

（石村）顔認

証技術による捜査が強制処分であるとしてします。そうすると、この種の捜査は、法定されていないと許されないということになるわけですね。強制処分かどうかはどのように判断するのですか？

【図表4】強制処分法定主義



（清水）判例が示している基準は、先ほど挙げた「相手に有無をいわさず重大な権利の制約を強いる」かどうかです。

（石村）警察が蓄積した個人情報（プライバシーデータ）と監視カメラで収集した映像データとの照合は、データや映像にある個人の同意を得ることなしに収集されるわけです。ですから、強制捜査のひとつにあたりますね。とくに、顔認証データのような生体認証情報の収集が伴う場合には、強制捜査といえますね。

（清水）データ同士の照合はまさに「検索」そのもの

のです。ですから、強制処分法定主義違反、令状主義違反の違法捜査というべきことは、先の最高裁大法廷決定の趣旨からも明らかでしょう。

【図表5】強制捜査には専用の令状が必要



（石村）GPS捜査の最高裁判断がすでに出ているわけです。ですから、裁判で違法と認定されるまでは自由に生体認証（顔認証）情報を使って捜査ができるとする考え

はゆるされないと思います。

◆顔認証の誤検知により、誤認逮捕された場合の救済

（石村）顔認証の誤検知により誤認逮捕された場合、裁判例などに従うと、どのような救済を求めることができるのでしょうか？

（清水）逮捕自体に対しては、法律上、その拘束時間が短い（48時間）ことから救済を求めることができないとされ、運用されています。

（石村）48時間は短くないように思いますが。

（清水）私もそう思います。そして逮捕の後、釈放されずに引き続き勾留されたとします。この場合には、裁判官の勾留決定に対して勾留する理由が始めからないことを主張して準抗告という不服申立てをすることになります（刑訴法429条1項2号）。

（石村）勾留する理由がないというのは、ここでは「罪を犯したことを疑うに足る相当な理由」がないということですね（刑訴法60条1項）。

（清水）そうです。準抗告が棄却されても、今度は勾留する理由のないことがすでに明らかになったことを主張して勾留取消請求を行うこともできます（刑訴法87条1項）。この請求の却下に対しても準抗告ができるようです。また、救済措置といえるのかどうか少々疑問ですが、勾留請求や起訴の根拠となる容疑に理由がないことを担当する検察官や裁判官に対して直接説明するといった働き

かけをする方法もあると聞いています。

(石村) 保釈請求はできないのでしょうか。

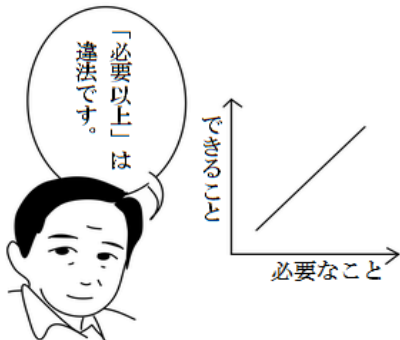
(清水) 起訴されるまではできないようです（刑訴法 207 条 1 項但書）。

◆公道などで公的機関が顔認証技術を装備した監視カメラで不特定多数者を撮像する場合の問題点は？

(石村) 一般市民が、公道、公園など伝統的な公共空間（public forum）で、表現行為や表現活動を、公的機関が顔認証技術を装備したカメラなどで常時監視することは、憲法が保障する集会の自由や言論の自由を侵害することになると思います。顔認証技術で、特定個人を監視するケースと、不特定多数者を監視するケースとでは、手続的にどう考えたらよいのでしょうか？

(清水) 具体的に犯罪が起こる前に、特定のグループに所属している人たちや、ある種の会合に参加した人たちを無差別に監視するケースですね。これは、刑事訴訟法で規制される犯罪捜査ではありません。公安警察による治安行政上のいわば広い意味でのスパイ活動ということになるかと思います。もちろん犯罪捜査ではありませんから、強制処分はできません。

【図表 6】警察比例の原則



任意捜査と同様に警察比例の原則の範囲を超えれば、つまり必要性を超えることをすれば、違法になります。

になります。

(石村) 公共空間で顔認証技術を装備したカメラなどで常時監視することは「必要以上」にあたるのでしょうか？

(清水) この点については、釜ヶ崎監視カメラ事件（大阪地裁 1994 年 4 月 27 日判決・判例時報 1515 号 116 頁）が参考になると思います。このケースで、裁判所は、肖像権、すなわち「何人も、その承諾なしに、みだりにその容ぼう・姿態を写真撮影・ビデオ録画されない自由」の侵害については、「犯罪予防の段階は、一般に公共の安全を害するおそれも比較的小さく、録画する必要性も少ない

のであって、このような場合に無限定に録画を許したのでは、右自由を保障した趣旨を没却するものであって、特段の事情のない限り、犯罪予防目的での録画は許されないというべきである」と判示しています。さらには「公道においても、通常は、偶然かつ一過性の視線にさらされるだけであり、特別の事情もないのに、継続的に監視されたり、尾行されることを予測して行動しているものではないのであって、その意味で、人は一歩外に出るとすべてのプライバシーを放棄したと考えるのは相当でない」と判示しています。

(石村) なるほど。公道上であっても継続的・網羅的な監視は別論だとするのは GPS 捜査最高裁決定とも通じる理解ですね。

(清水) 公安警察官による集会監視事件（東京高裁 2013 年 9 月 13 日判決・LEX / DB25502099）も参考

になります。このケースでは、訴えた方が負けました。裁判所は、「本件集会参加者のプライバシー等が広範囲に侵害された」とはいえないとしました。その理由は、「本件集会参加者全員を対象として一人一人網羅的にその住所、氏名等の個人情報を聴取したり、顔写真を撮ったりしたわけではな

(石村) これは、裏を返せば、参加者全員を一人一人網羅的に顔写真を撮ったりすれば「プライバシー等が広範囲に侵害」されたことになりますね。

(清水) そういうことになります。

【図表 7】公道上のプライバシー



◆顔認証によるコミュニティの「バーチャルプリズン（仮想監獄）化

(石村) 生体認証技術に対する法規制が皆無の状態では、顔認証技術による住民監視は、コミュニティをあたかも「バーチャルプリズン（仮想監獄）」に仕立てるのに等しいとの批判があります。この点について、どう考えたらよいのでしょうか？

(清水) 監獄での行刑というのは、まさに直接顔を見られるところで相手の動静を常時監視するやり方です。顔認証技術による住民監視は、監視されている側が監視されていることを意識しにくい点

が一層恐ろしいですね。

(石村) 他方で、監視されていることを意識する人たちからすると、その萎縮効果も大きいですね。

(清水) 例えば、警察は、政府に批判的な市民活動を行っている人、内部告発者の話を取材しようとする記者、デモに参加しようとする市民といった人々の動きを察知した場合、どう動くでしょうか。あえて大勢の警察官の姿を威圧的に晒したり、ビデオや写真撮影したりして、萎縮効果を狙うような行動をします。これは、先ほどの集会監視事件やモスクに出入りする人たちを監視するムスリム監視事件などでも起きています。

(石村) この国のデータ監視国家体制はますます強化されてきています。本人の同意なしでの生体認証データの集積、マイナンバーカードの強制利用の拡大による個人データの紐づけ、街中いたるところに設置された無数の監視カメラ網を使った映像データの集積、NTTやソフトバンクといった民間通信（サービス提供）事業者が設置した基地局、Wi-Fi、通信衛星などを使った携帯電話やスマートフォン（スマホ）からの位置情報データの収集、全国に張り巡らされたNシステム、さらには警察署内で行うことができるようになった通信傍受行為等々。まさに、先端技術を使った監視体制の強化は驚異的です。国家がここまでやるのでは、もはや市民は体内にGPSを埋め込まれて生活しているのと同じ変わりません。監視されていれば、安全！安心！という政府のプロパガンダに惑わされるひ弱い小市民で何が悪い、と反発する人も少なくないかも知れませんが？

(清水) 司法は、具体的事件を対象とした犯罪捜査でのGPS利用でさえ、その網羅性を理由に違法と判断しました。このことから、警察など行政が、顔認証技術を使い、網羅的・継続的かつ無差別に、しかも本人の明示の同意も得ずに生涯不変の生体認証情報による市民監視を行える仕組みは、憲法が保障した個人の自

由権の重大な侵害につながり、違法・違憲といえます。これは、現在の警察などの公的機関による顔認証技術を応用した監視カメラを使った市民監視システムでは、生体認証情報が次のような形で野放

図に収集されていることから明らかです。

①具体的事件とは無関係に、②犯罪発生以前に、③無差別に、④全国にわたって、⑤対象となる範囲が無制限のまま、⑥無期限で、⑦事後の検証も義務づけられることなしに、⑧常時、⑨網羅的に、⑩秘密裡に、⑪罪種を問わず、⑫被害の重大性・態様の悪質性といった事案の軽重も問題にすることなく、⑬より権利侵害の程度の低い方法によるべきことの手続的保障もなしに・・・

こうした現状を改善するには、警察などの公的機関が、制約なしに顔認証技術を使って住民監視を行なえないように法規制を急ぐ必要があります。

(石村) 警察が犯罪摘発を看板に顔認証技術を活用することについては、GPS利用以上に、令状主義の適用による空間的・時間的な規律が必要不可欠ですね。

(清水) 自衛隊情報保全隊事件（仙台高裁2016年2月2日判決・判例時報2293号18頁）では、自衛隊イラク派遣に反対する活動に参加していた人たちに対して行われた当局の監視活動が問われました。裁判所は、プライバシー侵害していないと判断しました。訴えた側は負けました。しかし、このケースで、裁判所は「収集された情報については、一定期間経過後は廃棄するものとされ、その管理体制も構築されており、その体制が不備であるとまで認めるに足る証拠はない」ことを、訴えを退けた理由にあげました。この裁判所の判断を、顔認証技術を使った生体認証情報（データ）の網羅的取得のケースに応用するとします。そうすると、収集した生体認証情報（データ）の利用・分析の限定、保管・廃棄のルールや保存期限の設定、情報開示を含む生体認証情報の適正な取扱体制の構築が不可欠だということになります。こうした取扱体制が不適切だと、違憲、違法になると解されます。まさに、GPS捜査大法廷判決の趣旨が及ぶものと解しなければなりません。

【図表 8】安全？安心？



◆顔認証と刑事法の「推定無罪」原則

(石村) 顔認証は、「推定無罪」のルールを反故にしたり、低所得者などの自由や少数者の人権を侵害したり、人種偏見や差別を助長しかねないという現実もありますか？

(清水) 先ほど紹介したムスリム監視事件（東京高裁2015年4月14日判決・LEX／DB25506287）では、モスクに出入りする人たちの監視庁公安部による監視の違憲性が問われました。裁判所は、情報の

継続的な収集のみならずその「保管、分析、利用」までを含めて合憲性を判断しないといけなかったとしました。しかし、裁判所は、監視活動の理由としてはテロの一般的・抽象的な脅威といった程度のもので無差別・広汎な監視の理由として足りるとしました。また、監視による個人の私生活上の自由への影響としては「不快感、嫌悪感を抱くといった事実上のものにとどまるというべき」と判示しました。

(石村) 裁判所は、宗教を理由とした捜査については無制限に許されるわけではないとしながらも、テロ防止の有効性などを検討する必要性を認めたわけです。イスラム教徒はテロを起こすかもしれないからモスクの前に立って監視してもよい、と裁判所が述べたわけです。この国の現実としてはいささか信じがたいものがあります。

(清水) 裁判所が加担しての、警察によるガバメント・ヘイト・スピーチとでもいうほかありませんね。

(石村) 外国人指紋押なつ拒否事件の最高裁判決(1995年12月15日・刑集49巻10号842頁)も、人権保障の視点からみると生体認証情報の保護には後ろ向きの判決ですよね。最高裁は、指紋は「性質上万人不同性、終生不変性をもつので、採取された指紋の利用方法次第では個人の私生活あるいはプライバシーが侵害される危険性がある。このような意味で、指紋の押なつ制度は、国民の私生活上の自由と密接な関連をもつものと考えられる。憲法13条は、国民の私生活上の自由が国家権力の行使に対して保護されるべきことを規定していると解されるので、個人の私生活上の自由の一つとして、何人もみだりに指紋の押なつを強制されない自由を有するものというべきであり、国家機関が正当な理由もなく指紋の押なつを強制することは、同条の趣旨に反して許されず、また、右の自由の保障は我が国に在留する外国人にも等しく及ぶと解される」としながら、なお当時の制度内容が「押なつ義務が三年に一度で、押なつ対象指紋も一指のみ」であるなどの理由から、「方法としても、一般的に許容される限度を超えない相当なもの」として押なつを義務づける規定が憲法13条に違反するものではないとしました。

(清水) 三年に一度、指一本と比べると、常時、オプト・インによる規制、すなわち明確な同意もなしに、顔面、虹彩・網膜、指紋・掌紋、静脈、声紋といった生体認証情報が取り放題の現状は、人権に与えるインパクトは計り知れないわけです。それがたとえ官のみならず民によるものであつて

も、憲法13条が保障する私生活上の自由・プライバシー侵害の方法・程度において明らかに相当性を逸脱した違憲な状態である、といわざるを得ませんね。

◆米連邦最高裁は、令状なしでの政府による通行した位置確認の目的で携帯電話記録の入手は違法と判示

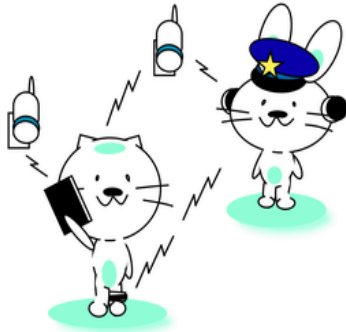
(石村) 2018年6月、米連邦最高裁判所は、政府は、人が通行した位置を確認する目的で通信事業者の基地局を利用した携帯電話／スマホ記録(位置情報データ)を、捜査令状なしには入手することはできない、と判断しました(Carpenter v. United States, 585 U.S. ____《2018》)(以下「カーペンター事件」または「カーペンター判決」ともいいます。)。カーペンター判決に照らして、アメリカでは、捜査機関が、令状なしに、他の機関が蓄積する顔認証データを入手することは違法とみる見解もありますが？

(清水) カーペンター事件の下級審、第6巡回区連邦控訴裁判所判決[819 F.3d 880 (6th Cir. 2016)]では、基地局を設置している携帯電話会社(通信事業者)とシェアしている情報だから情報主体である個人はプライバシー保護を期待できないと判断されました。この下級審判決では、本人以外の他の機関の側の同意を得ることによって個人データの入手を正当化しました。こうした理屈は、これまで日本でも使われてきました。しかし、カーペンター事件最高裁判決では、こうした入手を違憲としました。この点、基地局に関係するものではなく、通信衛星を使ったGPS捜査に関するわが国の最高裁判決でも「網羅的」な「検索」であるから令状なしでは違法、さらにはこの種の捜査を認めるには特別の令状が新たに法定されることが望ましいとされました。カーペンター事件最高裁判決も、いくら公道上でもその全容を把握するような莫大な量のセンシティブな情報の入手に令状がないのはもはや十分な合理性がないと判断しました。加えて、技術革新による新しい捜査手法と生活の私事性についての一般人の感覚・合理的な期待との間に放置できない格差が生じてしまうと判示しました。

(石村) つまり、わが国のGPS捜査最高裁判決の「網羅性」や検証を超える新たな「検索」という新手法に対するのと同様の態度が、カーペンター判決でも「莫大な量」を入手できる「技術革新」に対して示されたということになりますね。

(清水) 車に取り付ける GPS 端末が捜査機関による「装着型」であるのに対して、携帯電話／スマホは「非装着型」で体から離れることはありません。

【図表 9】ケータイ／スマホ＝警察待機？



その情報を警察が自由に入手できるということは、私たちが店頭で携帯電話の契約をするときに、合わせてもれなく捜査機関の監視端末も足首に取り付けられているのと同じだとまでカー

ペンター判決は述べています。

(石村) 2012 年 1 月 23 日、米連邦最高裁は「令状なしでの GPS 捜査は連邦憲法修正 4 条が禁止する不合理な捜索に該当し違憲」という判決を下しています (United States v. Jones, 565 U.S. 400 《2012》)。すでにふれましたが、わが国でも似たような判決〔最高裁 2017 年 3 月 16 日判決 (刑集 71 卷 3 号 13 頁)〕があります。こうした裁判例からみて、捜査機関が、令状なしに、官民を問わず、他の機関などが蓄積する顔認証データを入手することは違法だと思いますが？

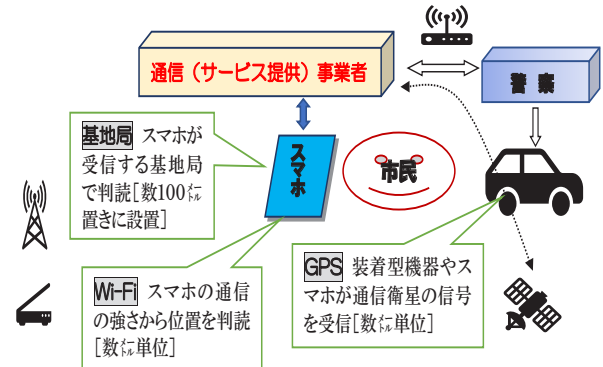
(清水) 先ほど石村先生に比較していただいたように、日本での GPS 捜査に関する 2017 年の最高裁大法廷判決とカーペンター判決は同様の視座に立つものです。それに、日本の方がアメリカよりもプライバシーの期待が低いなどということはないわけです。ですから、いったん携帯電話会社に集積された位置情報だとしても、それをスマホなど移動端末の利用者の同意なく捜査機関に差し出すとします。これでは、結局 GPS 捜査のわが国最高裁判決が新たに法定された令状を必要とした「網羅的」な「検索」を、携帯電話会社を通して行ったのと同じになるわけです。ですから、令状主義、強制処分法定主義違反の違法があり、その意味で憲法 35 条に反して違憲でもあるといわざるを得ません。

(石村) 刑事訴訟法 197 条 2 項に基づく「捜査関係事項照会」もこの限りでは制限を受けるわけですね。

(清水) 位置情報の収集をねらいとした GPS 捜査に関するわが国最高裁判決は、警察側の任意捜査だという主張をはっきりと退けました。位置情報の

収集が、基地局を持つ携帯電話会社（通信事業者）を間に挟んで非装着型になったからといって、「網羅性」や「検索」といったプライバシー侵害の本質は何ら変わらないのです。ですから、強制捜査が任意捜査に変化するなどということがあり得ないのです。これは、カーペンター判決が示したところでは。

【図表 10】スマホ／携帯電話（非装着型）や装着型機器で位置情報を収集する主な仕組み



(石村) 刑事訴訟法 197 条 1 項【任意捜査】に基づき、捜査機関が、令状なしに、官民を問わず他の機関が蓄積する顔認証データを入手することは違法といえるのではないのでしょうか？

(清水) 捜査機関が、一定期間内の監視カメラ映像データ（情報）の提供を受けるというのは、「一過性」の情報にとどまるのではないわけです。「網羅的」「継続的」に「集積」された情報を「分析」し、他の情報と「照合」「統合」するケースは、もともと捜査対象が個別具体的に特定されていなければならないという従来の捜査概念の埒外にあるわけです。ですから、GPS 捜査の最高裁判決が示しており、新たに制定された法律上のルールに従って使用期限や保管の条件を付したそれ専用の令状の発付の下でのみ行うことができるとすべきです。

(石村) 同じ刑事訴訟法 197 条の 2 項による「捜査関係事項照会」(詳しくは、CNN ニュース 97 号「対論：ポイントカード情報で太る企業とつるむ捜査当局」参照) の場合と同様に扱われなければならないということになりますね。

(清水) そういことです。

(石村) 生体認証情報は、高度なセンシティブ情報の一種です。しかも、生涯変更はできません。漏れて、悪用されたら、取り返しがつかないわけです。生体認証情報をもっと厳正に保護するためには個人情報保護法の改正も必要です。また、個人情報保護委員会も、IT 業界利益を忖度する志向が強

く市民ファーストになっていません。市民団体から「個人情報反故委員会」と揶揄されている始末です。したがって、この名ばかり個人情報保護委員会も、市民に寄り添える組織に衣替えするための抜本的な改革も必要です。いずれにしろ、顔認証技術などを使った生体認証情報取扱いの市民的コントロールをもっと確実にする法制が必要です。この点では、CNN ニュース本号（99 号）で紹介したイリノイ州生体認証情報プライバシー法（BIPA）に学ぶ必要があります。

（清水）民間機関による生体認証情報の規制を急がなければならないですね。加えて、警察など公的機関が犯罪摘発に顔認証技術を活用することについては、もっと慎重になる必要があります。顔認証技術の刑事活用については、GPS 利用のケース以

上に令状主義の適用を厳格に義務付ける法制が必要ですね。

（石村）「単なる監視カメラの設置と、センシティブ情報の収集につながる顔認証技術を応用した監視カメラとは、次元が違うのだ」、という認識を市民の間で共有する必要がありますね。

（清水）まさに、その点がポイントですね。こうした認識が共有されないと、「笛吹けども踊らず」になりますから……。

（石村）清水先生、今回は、ご多用なところ、専門的な観点から有益なご意見をありがとうございます。

（清水）こちらこそ、いろいろと勉強させていただき、感謝しております。

【最新のプライバシーニュース】

アメリカ自治体の 顔認証技術規制条例

アメリカ加州サンフランシスコ市、 行政機関や市警でのAIを使った顔認証禁止条例制定

石村 耕治（PIJ代表）

アメリカでは、公的機関が、監視カメラや身体装着カメラ（body-worn camera）などに顔認証技術（FRT=facial recognition technology）を取付け、市民の明示の同意なしに究極のプライバシーである生体認証情報（生体認証データともいう。）を取り扱うことを人権侵害とする見方が強まっている。地方団体や州の議会が、生体認証情報の収集、保管することを禁止するための法的規制条例や法律をつくる動きが積極化している。人の顔や指紋、目

の虹彩のような生体認証情報は、変更が不可能で、いったん洩れたら取り返しがつかなくなるからである。生体認証で儲けようとするIT企業に社会的責任のある行動を求めるには、わが国でも、生体認証技術の利用禁止条例や法律の制定は必要不可欠である。石村耕治 PIJ 代表に、アメリカの地方団体や州議会での禁止立法づくりの状況を紹介いただいた。

（CNNニュース編集局）

■サンフランシスコ市の公的機関での顔認証利用禁止条例

アメリカ、カリフォルニア州（加州）サンフランシスコ市は2019年5月14日に、人工知能（AI）を使った顔認証技術（FRT）を自治体の行政機関や警察が利用することを禁じる条例案「秘密監視規

制条例（Stop Secret Surveillance Ordinance）」案を、市議会（Board of Supervisors）で、8対1の賛成多数で可決された。その後、21日に市議会で可決し、施行した。アメリカの主要な自治体で、この種の規制条例を制定したのは同市が全米初となった。

この条例は、2016年9月21日に、アメリカ

自由人権協会 (ACLU=American Civil Liberties Union) が企画した「警察監視をコミュニティが監視する (CCOPS=Community Control Over Police Surveillance) プロジェクト」に応じ、同市の民主党議員が発案し条例にしたもの。この種の自治体条例は、自治体が、監視カメラや顔認証技術のような監視技術をどのように使うのか、議会に権限を付与し、住民の意思に委ねようとするものである。

【図表 1】 CCAPS プログラムとは



【図表2】顔認証技術による秘密監視禁止条例の目的は、大きく2つある

- サンフランシスコ市内にある市の施設において、顔認証技術の利用を禁止すること。（なお、同市警では、現在、顔認証技術を利用していない。このことから、現実には将来的な利用を禁止することになる。）
- あらゆる一般監視技術の利用に関する透明性と監視する制度を構築すること。

顔認証技術・AI による住民監視は、自分らの住む地域をあたかも「バーチャルプリズン（仮想監獄）」に仕立てるのに等しいとの批判がある。有色人種やマイノリティ、低所得者などの自由や人権の侵害につながり、差別を助長しかねない。顔認証技術・AI による住民監視に対しては、慎重な意見が広がっている。サンフランシスコ市条例は、監視カメラがとらえた人の顔の画像を AI で分析する顔認証ソフトウェアについて、警察など市の 53 の機関での利用を禁止する内容だ。連邦政府の管轄下にある空港や港湾での利用は認められる。つまり、この条例の適用は、市の行政機関や警察に限定される。言いかえると、州や連邦機関、民間機関には適用にならない。



サンフランシスコ市でこの条例づくりを主導した民主党所



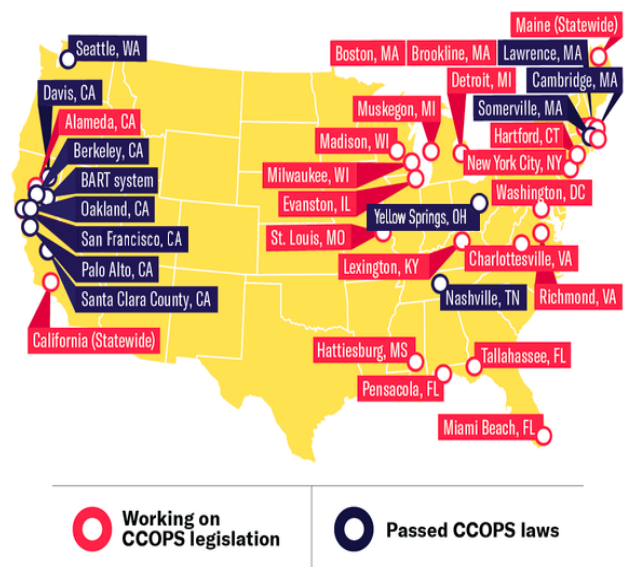
SF 市議会で条例案の説明をするア
ロン・ペスキ市議 (public use)

属のアロン・ペスキン (Aaron Peskin) 市議は、「顔認証技術は唯一無二の危険な技術 (uniquely dangerous technology) である」と述べている。

■全米での公的機関での顔認証利用禁止条例 制定の動き

生涯変更不可能な生体認証情報は、いったん洩れたら、取り返しがつかないことになる。アメリカの連邦や諸州の憲法は、政府が、本人の明示の同意なしに市民の生体認証情報を収集することを認めているとは解されない。このことから、顔認証技術（FRT）を使用したカメラなどで市民の生体認証情報を無差別に収集することは、憲法が保障するプライバシー権をはじめとして市民の人権を侵害することは明らかである。

全米では、自治体の行政機関や警察が利用することを規制する条例案「秘密監視規制条例を制定または検討する動きが広がっている。ACLU（アメリカ自由人権協会）が公表している資料によると、2019年5月現在の立法状況は、次のとおりである。（出典 Available at: <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance>）



■カリフォルニア州議会での FRT 禁止法制定の動き

カリフォルニア州では、州議会下院（2019-2020 定例会）に、2019 年 2 月 21 日に、顔認証技術（FRT=facial recognition technology）を警察官など法執行職員の身体装着カメラ（body-worn

camera) などに利用することを禁じる州刑事法 (Penal Code) 改正法案: 州下院法案 1215 号 (AB-1215) 「法執行: 顔認証その他生体認証監視 (Law enforcement: facial recognition and other biometric surveillance)」が提出されている (提出者は州議会ティン (Ting) 下院議員)。州議会下院法案 1215 号 (AB-1215) は、2 月 21 日に下院に上程後、4 月 8 日、4 月 25 日に、調整のための改正が行われた。

いまだ州議会では、法案審査がはじまっていないが、進歩的なギャビン・ニューサム (Gavin Newsom) 州知事 (民主党) のもと、成立する可能性が高い法案の 1 つである。

この法案は、警察など州内の法執行機関が、身体装着カメラを利用することを禁じるものではない。身体装着カメラに、顔認証技術 (FRT) を取付け、生体認証データの収集・保管を禁止するものである。本人の明示の同意なしに無差別に住民の顔認証などの究極のプライバシーである生体認証データを収集・保管することは、プライバシー権の侵害、憲法違反であるとの考え方に基づく。

以下に、読者の便宜も考えて、加州議会下院法案 1215 号 (AB-1215) を邦訳 (仮訳) する。

■加州議会下院法案 1215 号 (AB-1215)

【2019 年 2 月 21 日ティン (Ting) 下院議員提出、2019 年 2 月 4 日改正、2019 年 4 月 25 日改正】

「法執行: 顔認証その他生体認証監視 (Law enforcement: facial recognition and other biometric surveillance)」(邦訳・仮訳)

この法律は、州刑事法 (Penal Code) の第 832.19 条「法執行関係」に追加される。

●州議会法制局の法案概要説明 (Legislative Counsels Digest)

現行法は、治安担当官 (peace office) の身体装着カメラ (body-worn camera) により記録されたデータのダウンロードおよび保管に関する課題を処理するための政策と手続は、議会の意思で確立すると定めており、かつ、これらの政策や手続はベストプラクティスに基づくことを求めている。現行法は、とりわけ、身体装着カメラ・システムの運営や実施の政策や手続を確立する場合には身体装着カメラ・データのダウンロードや保管に関

してはベストプラクティスを考慮するように法執行機関、部局または事業体に求めている。

この法案は、法執行機関または法執行職員に対して職員カメラまたは職員カメラで収集されたデータに関していかなる生体認証監視システムの取付、起動、利用を禁止するものである。この法案は、禁止に違反した法執行機関または職員に対して衡平法上の救済または差止救済を認めるものである。

●要点のポイント

投票は多数決 予算委員会審議 (Appropriation) は不要 財政委員会 (Fiscal Committee) 審議は不要、地方団体関連プログラム (Local Program) ではない。

【法案テキスト】

カルフォルニア州の住民は、次のように制定する。

第 1 条

議会は、次のことを見出しかつそのすべてを宣言する。

第 a 項

カリフォルニア住民 (Californians) は、プライバシーは個人の自由の必要不可欠な要素の 1 つと評価し、かつ、カリフォルニア州憲法第 1 条第 1 項においてプライバシー権 (right to privacy) を保障されている。

第 b 項

顔認証その他の生体認証監視技術は、住民や訪問者の市民的権利や市民的自由に対して他に類を見ないほどの重大な脅威を与える。

第 c 項

顔認証その他生体認証監視の利用は、機能的には、憲法が保障する権利を侵害して、個人の写真付き身分証明カードの常時提示を求めるに等しい。この技術は、住民を本人の同意なしに追跡することを認めることになる。この技術は、法を遵守するカリフォルニア住民に関する巨大なデータベースを出現させ、かつ、公的な場所における自由な表現の行使の足かせになる。

第 d 項

顔認証その他生体認証監視技術は、繰り返し女性、若者や人の肌の色を誤って認識し、かつ、有害な「誤判定 (false positive)」の危険の増大を招いてきている。

第 e 項

顔認証その他生体認証監視は、職員の身体装着カメラの本来の目的が、これらの装置が透明かつ説明責任を負える道具から移動式監視システムに変質することにより損なわれている。

第f項

顔認証その他生体認証監視は、高度に警察監視下にあるコミュニティに住む住民の市民的権利や自由に対して過度に影響を及ぼしている。また、顔認証その他生体認証監視は、犯罪の被害者、必要書類不備滞在者 (undocumented persons)、罰金や課金不払者および警察から支援が必要または警察を支援する前科者を落胆させることで、効率的な警察活動や公共の安全を損ねることにつながる。

第2条

第 832.19 条は、次のとおりで、刑事法第 832.18 条の後に追加される。

第a項

本条において、次に掲げる用語の定義は、次の各号に定めるところによる。

第1号

「生体認証データ (biometric data)」とは、個人を確認するために、単独にまたは相互にもしくは他の情報と結合して利用することができる生理学的 (physiological)、生物学的 (biological) または行動的 (behavioral) 特性をいう。

第2号

「生体認証監視システム (biometric surveillance system)」とは、顔面認証その他の生体認証を実施するコンピュータソフト (computer software) またはアプリ (application) をいう。

第3号

「顔面認証その他の生体認証 (facial recognition or other biometric surveillance)」とは、次の (A) もしくは (B) 単独、または結合のいずれかをいう。

(A) 個人の生体認証データを捕捉する自動または半自動プロセス

(B) 生体認証データに基づき個人を識別するまたは個人を監視する情報を生成する自動または半自動プロセス

第4号

「法執行機関 (law enforcement agency)」とは、警察署、保安官部、州検察 (district attorney)、公共旅客運送機関警察署 (transit agency police department)、学区警察署、ハ

イウエイパトロール、カリフォルニア大学、カリフォルニア州立大学、コミュニティカレッジのキャンパス警察、カリフォルニアハイウェイパトロール部および司法省をいう。

第5号

「法執行職員 (law enforcement official)」とは、法執行機関の職員 (officer)、代理職員 (deputy)、従業者 (employee) または調査官 (agent) をいう。

第6号

「職員カメラ (officer camera)」とは、画像または音声を記録または送信するための身体装着カメラまたは同様の装置で、法執行職員が身体もしくは衣服に装着するまたは携行するものをいう。

第7号

「監視情報 (surveillance information)」とは、次の (A) もしくは (A) 単独、または結合のいずれかをいう。

(A) 個人が知っているかまたは知っていない情報で、その者の氏名、生年月日、性別または犯歴等、ただしこれらに限定されない、を含む。

(B) 生体認証データから得られた情報で、個人の情緒、精神状態または危険度の評価等、ただしこれらに限定されない、を含む。

第8号

「利用 (use)」とは、次の (A) もしくは (B) 単独、または結合のいずれかをいう。

(A) 法執行職員または法執行機関による生体認証監視システムの直接利用

(B) 法執行職員の要請に基づく法執行機関その他第三者による生体認証監視システムの利用

第b項

法執行職員または法執行機関は、職員のカメラまたは職員のカメラにより収集されるデータに関して生体認証監視システムを取付、起動または利用してはならない。

第c項

個人 (person) は、法定の制裁、罰則または救済に加え、本条に違反した法執行機関または職員を相手に権限ある管轄権を有する裁判所に衡平法上の救済または差止救済を求めて訴訟を提起することができる。

ACLU 作成の監視技術透明化モデル法

【邦訳責任者】 石村 耕 治 (PIJ代表)

【仮訳】

監視技術にかかる透明性を推進しかつ市民的権利および市民的自由を保護する法律 (An Act to Promote Transparency and Protect Civil Rights and Civil Liberties With Respect to Surveillance Technology)

(目的)

市議会¹は、監視技術に関するできるだけ早い決定を行うために、公開討論を行うことが必要不可欠である。市議会は、監視技術が、合衆国憲法修正第1条、第4条および第14条に保障された市民的権利および市民的自由に影響を及ぼすかどうかを慎重に検討することなしに、当該監視技術に関するいかなる決定も行われてはならないことを認める。市議会は、歴史的にみても、監視技術はあらゆる市民のプライバシーの侵害を引き起こす一方で、人種、民族、宗教、出身国、所得水準、性的指向または政治的信条のような要因を尺度とする監視行為はよって特定のコミュニティ（地域共同体）および集団を威圧しかつ抑圧するために使われてきたことを認める。市議会は、いかなる監視技術の利用に先立っても、市民的権利および市民的自由を保護するために、高い透明性、監視および説明責任を果たす措置を含む法的に執行可能な安全対策が講じられなければならないと認める。市議会は、ある監視技術が承認された場合、市議会と住民が市民的権利や市民的自由を保護する措置が厳格に護られているのかを検証する権限を付与するためのデータ報告措置が採択されなければならないと認める。市議会は、監視技術にかかる総コストが点検され、かつ、そのコストを上回る財政上の利益があるかどうか、また、当該技術にかかる支出が市の最良の利益にかなうかどうかの分析結果を一般住民に提供する必要がある旨認める。

以下、市議会は、次のような条項を採択して、解決をはかるものとする。

(定義)

第1条

- (A)「差別 (Discriminatory)」とは、(1) 合衆国の憲法もしくは法律、マサチューセッツ州の憲法もしくは法律、または●●市の憲章または法律のもとで差別にあたるとして禁止されている個人の特性、性格または身分、またはそうした個人の結社を理由に差別的な取扱いをすること、または、(2) 第1号に規定する特性、性格もしくは身分を有する個人に差別的の影響を及ぼすことをいう。
- (B)「差別的効果／間接差別 (Disparate impact)」とは、合衆国憲法もしくは法律、マサチューセッツ州の憲法もしくは法律、または●●市憲章または法律のもとで差別にあたるとして禁止されている実際もしくは知覚できる特性、性格または身分を有する個人が、同じような状況にありながらも、そのような特性、性格または身分にない個人に比べ、不相応に体験した有害な効果をいう。
- (C)「自治体 (Municipal entity)」とは、この市のなかに所在するあらゆる自治体政府機関、部門、局、部または課をいう。
- (D)「監視データ」とは、監視技術を使って収集、捕獲、記録、保存、処理、傍受、分析または供用されるあらゆる電子データをいう。
- (E)「監視技術 (Surveillance technology)」とは、電子監視装置、ハードウェアもしくはソフトウェアを装備した特定の者もしくは集団その他のシステム、装置または手段を使って、音声、視覚、デジタル、位置、熱、生体その他の情報または通信を収集、捕獲、記録、保存、処理、傍受、分析または共有することを可能とするあらゆる電子監視

¹ ここでは、市議会 (city council) の言葉を使っているが、それぞれの地方団体で使用されている言葉に置き換えるものとする。

装置、ハードウェアまたはソフトウェアをいう。

- (1)「監視技術 (Surveillance technology)」とは、監視対象の追跡および予測的警察活動ソフトウェアを含む、(a) 国際モバイル加入者識別番号 (IMSI= international mobile subscriber identity) キャッチャー【訳注：偽装基地局】および他のセルサイトシミュレータ (other cell site simulators)【訳注：携帯電話基地局のアンテナをエミュレート (模倣) しモバイル電話のデータを収集する装置】、(b) ナンバープレート自動認識装置 (automatic license plate readers)、(c) 電子通行料金読取機 (electronic toll readers)、(d) 監視カメラ (closed-circuit television cameras)、(e) 顔、音声、虹彩、ならびに歩行認識ソフトウェアおよびデータベースなどの生体監視技術、(f) モバイル DNA 捕獲技術、(g) 発砲音から相手の位置を測定するハードウェアおよびサービス (gunshot detection and location hardware and services)、(h) X線搭載車 (x-ray vans)、(i) 監視カメラや装着できるボディカメラなどのビデオ・音声監視および／または録画・録音技術、(j) 白熱電球や照明装置で可能な監視、(k) ソフトウェアやハードウェアを含む、コンピュータ、コンピュータサービスまたはコンピュータネットワークへ許可なくアクセスするに使用される装置、(l) ソーシャルメディア監視ソフトウェア、(m) 壁貫通レーダーまたは同様の画像技術 (through-the-wall radar or similar imaging technology)、(n) 静的スキャン位置通信ネットワーク (passive scanners of radio networks)、(o) 長距離無線通信その他無線スキャン装置 (long-range Bluetooth and other wireless-scanning devices)、(p) 近距離無線通信自動認識スキャナー (radio-frequency I.D. (RFID) scanners)、および (q) 監視技術でデータを集約するまたは分析するソフトウェア (software designed to integrate or analyze data from Surveillance Technology) をいう。本号に記載された監視技術はあくまでも例示であり、いかなる自治体も、その利用にあたり支持または承認の対象は記載されているものに限り解してはならない。
- (2)「監視技術 (Surveillance technology)」には、第1条第E項に定義された監視技術を装備、または改修もしくは一部に含む場合を除き、次の

ような装置 (devices) またはハードウェアは含まれない。(a) テレビ、コンピュータ、プリンターのような日常の事務機器、すなわち、一般住民が広く利用し、かつ、いかなる監視または監視関連業務に利用されていないもの。(b) 駐車券装置 (PTDs)、(c) 手動の非装着型、携帯デジタルカメラ、音声録音機、ビデオ録画機で、内密を利用するように設計されておらず、かつ、その機能がビデオおよび／または音声記録が人の手でとらえられかつダウンロードする仕様になっているもの、(d) 監視装置で、画像安定双眼鏡 (image stabilizing binoculars)、暗視ゴーグル (night vision goggles) のような、音声もしくはビデオを記録できないまたは送信できない、または遠隔アクセスできないもの、(e) 自治体機関のデータベースで、監視技術により収集、捕獲、記録、保存、処理、傍受または分析できるデータその他の情報を含まず、かつ含む予定がないもの、ならびに、(f) 手動の技術装置で、本来的に自治体内部での通信に利用され、かつ、無線通信や電子メールシステムのようなデータを内密に監視目的で収集できるように設計されていないもの。

- (F)「見解ベース (Viewpoint-based)」とは、合衆国憲法修正第1条で保障された権利行使を理由に、コミュニティもしくは集団またはその構成員を標的とすることをいう。

第2条

- (A) 自治体は、次に掲げることをするに先立ち、一般住民にオンライン (ネット)、文書または口頭で証言する公正かつ十分な機会を与えることを法的に義務づけられ、適正な公示を行い市議会で適切な公聴会を開催したうえで、市議会の承認を得なければならない。
- (1) 新たな監視技術のための財源を求める場合。助成金の申請、州もしくは連邦の資金の申請、または現物提供その他寄附金の募集を含む。
- (2) 新たな監視技術の取得または貸与を求める場合。その取得が、金銭その他の対価を伴うかどうかを問わない。
- (3) この法律に従い市議会が以前承認していない目的または方法において、新たなまたは既存の監視技術を利用する場合。または、
- (4) 監視技術または監視データを他の者もしくは団体と取得、共用その他利用する協定を締結するまたはその計画をする場合

(B) 自治体は、監視技術の財源確保、取得もしくは利用、または財源確保、取得もしくは利用に関する協定を締結する際の市議会の承認を求める手続の一環として、第2条第A項の規定に基づいて、市議会に対し問題の技術に関する監視影響報告書 (Surveillance Impact Report) および監視利用ポリシー (Surveillance Use Policy) を提出するものとする。

(1) 自治体の機関は、第2条第B項の規定に基づき市議会に提出された監視影響報告書および監視利用ポリシーに関し、一般住民が双方の資料を閲覧できるように、ウェブサイト (HP) に公表するものとする。

(2) 市議会は、第2条第B項の規定に基づく監視技術の承認申請が受け取ってから10日以内にそれに関する監視影響報告書および監視利用ポリシーを、文書およびウェブサイト (HP) に公表し、一般住民の閲覧に供するものとする。

(3) 自治体の当該機関は、第2条第B項の規定に基づく監視影響報告書および監視利用ポリシーの提出があつてから21日以内に、よく知られ交通の便がよい場所に一般住民を招き、その自治体が市議会に提出した監視技術承認申請に関する審議および質問応答をするために一回以上の住民集会を開催するものとする。

(4) 第2条第A項の規定により求められる市議会公聴会は、第2条第B項の規定に基づく監視影響報告書および監視利用ポリシーが提出されてから、45日間は開催されないものとする。

(5) 市議会、または市議会が指名した者は、自治体が第2条第A項の規定に基づき監視技術承認申請を行いその監視技術を引き続き利用する期間にわたり、一般住民がオンライン (ネット) で読めるように、当該監視影響報告書および監視利用ポリシーを継続して作成し、かつ、改定版を作成するものとする。

(C) 自治体は、当該自治体が第2条第B項に基づき監視影響報告書および監視利用ポリシーを提出し、第2条第A項の規定に基づく市議会から明示の承認を得ることなく、いかなる監視技術を利用してはならないものとする。

(D) 市議会は、監視影響報告書もしくは監視利用ポリシーの承認または拒否するに先立ち、提出する自治体に対して変更を求めることができる。変更は、監視利用ポリシーもしくは監視影響報告書に不適切な内容が存在すると思われる場合に、とりわけ市民的権利や市民的自由の保護、差別的かつ

見解ベース利用、差別的配置および差別的効果を避ける目的で、求めることができる。

(1) 市議会は、市議会の議員、職員または委員会から求められた監視影響報告書もしくは監視利用ポリシーに対する変更要請およびそれに対する応答については、第2条第A項の規定に基づき自治体に行われた申請を承認または拒否するための市議会での投票に先立つ少なくとも30日前に、これを、文書およびウェブサイト (HP) を使って一般住民に開示するものとする。

(2) 市議会は、当初提出された監視影響報告書または監視利用ポリシーに対する変更を行う場合には、変更された監視影響報告書または監視利用ポリシーを承認または拒否するための市議会での投票を行うに先立ち、一般住民が変更された監視影響報告書または監視利用ポリシーに対して、文書または口頭で証言する公正かつ十分な機会を与えるために、適正に公示したうえで、市議会で適切な公聴会をもう一度開催しなければならない。市議会は、公聴会実施に先立つ少なくとも30日前に、変更された監視影響報告書または監視利用ポリシーを、文書およびウェブサイト (HP) を使って一般住民に開示するものとする。

(E) 第2条第B項の規定に基づき提出された監視影響報告書は、少なくとも次のような事項を記載した法的に執行可能な成文の報告書として公開するものとする。

(1) その監視技術がどのように作動するのかなど製造者による製品の説明を含むその監視技術に関する情報

(2) その監視技術が想定する目的に関する情報

(3) その監視技術が市中において統一的に利用されずかつ標的化されていない場合には、

(a) その技術を利用しかつ標的を決定するときにどのような要因が使われるのか

(b) 第2条第E項第3号(a)の規定に基づき列挙された要因によるときには、どのような地理的場所を不相応に高い水準の利用または標的として予定しているのか

(4) 次のようなその監視技術の財政への影響

(a) 当初の取得費用

(b) その後に発生する人件費、法順遵守費、利用監査、データ保存および安全対策などの運用費

(c) その技術の利用により得られる費用の削減額

- (d) 現在または潜在的な財政源、および、
- (5) 特に確認できた評価
 - (a) その監視技術が、利用された場合、次のような市民的自由や市民的権利の及ぼす潜在的な影響
 - (i) その監視技術が、恣意的または不注意に、差別的方法で利用または配置された場合に、どのようなコミュニティまたは集団に潜在的な差別的効果もしくは悪影響を及ぼすのか。
 - (ii) その監視技術が、恣意的または不注意に、観点ベースの方法で利用または配置された場合に、どのようなコミュニティまたは集団に潜在的な差別的効果もしくは悪影響を及ぼすのか。
 - (iii) その監視技術が、恣意的または不注意に、偏頗的な (biased) アルゴリズム (自動情報処理手順) で利用または配置された場合に、どのようなコミュニティまたは集団に潜在的な差別的効果もしくは悪影響を及ぼすのか。
 - (iv) プライバシー権や匿名で行動する権利に対する潜在的な悪影響
 - (v) その他合衆国憲法修正 1 条、第 4 条および第 14 条で保障された市民的自由に対する潜在的な悪影響
- (6) 監視影響報告書は、修正されるか修正されないかを問わず、市議会の投票により承認されるまで、提案であり、免責文書 (disclaimer) とみなされる。
- (F) 第 2 条第 B 号の規定により提出された監視影響報告書は、公開され、少なくとも次のような事項を明確にした自治体による監視技術の利用に関する法的に執行可能な成文のポリシーである。
 - (1) 目的：すなわち、当該監視技術が得ようとしている特定の目的
 - (2) 承認された利用：すなわち、承認を求められている特定の監視技術の利用、および、
 - (a) その監視技術が継続的に運用されるのかどうか、または特定の状況にのみ利用されるのかどうか
 - (b) その監視技術が継続的に運用されるのかどうか、または特定の状況にのみ利用されるのかどうか
 - (c) その監視技術が、その市内に統一的に配置または標的化されるのかどうか、または、仮にそうでないとすれば、その技術が配置また

は標的を設定する場合には、どのような要因が利用されるのか

- (d) 監視技術の個々の利用に先立ち、どのようなルールが適用になるのか、そしてどのような手続が義務付けられるのか。
 - (i) 第 2 条第 F 項第 2 号の規定に基づき掲げられた個々の承認利用について、
 - a. その技術が利用される場合には、どのような現行の法的基準に適合しなければならないのか、そのような基準は現在存在するのか、またはどのような従うべき基準を提案するつもりなのか。
 - b. 裁判所の令状 (judicial warrants) が義務付けられるのかどうか。
 - c. 特定の装置利用を許可する令状または許可状には、どのような情報が記載されなければならないのか。
 - (e) 一般住民の催事や集会に対する令状なしの監視の例のように、どのようなその監視技術の潜在的な能力および利用が禁止されるのか。
 - (f) その監視技術は、即時に人を監視する場合に、データを収集する目的で、どのように、かつどの程度まで利用されるのか、
 - (g) その監視技術は、(i) 暴力的な犯罪、(ii) 非暴力的な犯罪、(iii) 重罪、(iv) 軽罪、(v) その他法令違反、重罪もしくは軽罪として分類されない犯罪行為、不法な行為、または潜在的な将来の犯罪、暴力団その他の集団への実際もしくは予見される参加にかかわる指標となる行動もしくはパターンを調査するために利用されているかどうか。および、
 - (h) その監視技術により収集、捕獲、記録、傍受された監視データの保存の範囲、状況、方法の分析および審査
- (3) データ収集
 - (a) その監視技術はどのような監視データを収集、捕獲、記録、傍受または保存する能力があるのか。
 - (b) その監視技術の利用が承認された場合に、どのような監視データが不注意に収集される可能性があるのか、およびそうした不注意なデータ収集を最小化するためのどのような対策が取られているのか。
 - (c) 第 2 条第 F 項第 3 号 (b) の規定に従い不注意に収集されたデータと確認された場合には、第 2 条第 F 項第 7 号 (f) の規定に基づき、

どのように迅速に確認しかつ削除するのか。

- (4) データベースの信頼性：適用がある場合、対象者を確認するための技術の適用におけるデータベースの信頼性
- (5) データへのアクセス
 - (a) 個人は、どのような条件に基づき監視データのアクセスを求めることができるのか、当該誰が監視データのアクセスする権限を有するのか、当該監視データにアクセスまたは関与するに先立ちどのような規則や手続に従わなければならないのか、ならびに、
 - (b) 監視データを視聴・追跡にはどのようなタイプの視聴者ログその他の方法が使われるのかおよび追跡されるのはどのような情報なのか。
 - (c) どのような部門の職員が監視データの写しを入手できる権限を有するのかの記載
 - (d) どのような手続が、監視データの写しの許可なしでの配付を防止するために規定されているのか。
- (6) データ保護：許可なしでのアクセスから監視データを保護するために講じられた、暗号およびアクセスコントロールの仕組みを含む安全対策
- (7) データ保存：監視データ保存に関する、ガバナンスを含む規則と手続
 - (a) 監視データの保存期間。この情報には、監視利用ポリシーの記載された趣旨に従った指定保存期間に関する理由の記載を含む。
 - (b) 第2条第F項第7号(a)に規定された保存期間を超えて監視データを保存する場合に遵守しなければならない特定の条件
 - (c) 第2条第F項第7号(a)に規定された保存期間が経過した後どのような手続に従って監視データを定期的に削除するのか、およびどのような監査手続に従ってデータが当該保存期間を超えて不当に保存されないようにするのか。
 - (d) 監視データのラベル貼りや索引の仕方を含む監視データを保存する方法
 - (e) 監視データが不適切に収集および／または保存されていることを確認するに使われる方法、ならびに確認された場合にそのデータ、およびその写しを含む、をどのように早急に破棄するのか。
 - (f) 個人は、自己に関して保存されている監視データが不適切に収集および／または保存さ

れていると訴えたうえでその訴えを審査するように請求し、かつ、どのようにして監視データ、およびその写しを含む、が不適切の収集または保存されたのかの説明を求め、さらには確認された不適切なデータを即時に破棄するように求めることができるように、どのような手続が規定されているのか。

- (g) 監視データを保存するに利用される技術的なシステム、ならびに誰がそのシステムおよび監視データを維持しかつ管理するのか。
 - (h) 第2条第F項第7号を遵守する責任を負う部署または個人、ならびに、いつおよびどのように遵守状況を監査するのか。
- (8) 一般住民のアクセス：監視データに一般住民はどのようにアクセスできるのか、自治体は監視データに関し●●公文書法をどのように適用しかつ遵守するつもりなのか、および、個人のプライバシーを保護するためにどのような手順を取るのか。
- (9) 対象者／被告発者のアクセス：法律に基づき、刑事または民事の調査の対象者、刑事または民事の被告発者およびその弁護人は、監視データにどのようにして、どの程度まで、どの時点で、アクセスできるのか。
- (10) 監視データの共用：自治体が、他の政府機関、部門、局、部または課と監視技術または監視データを共用する目的でアクセスする場合の要件は、次のとおりである。
- (a) 監視データの収集、集約および保存については、監視プログラムを実施する政府機関は「ある個人が犯罪行為または犯罪活動に関係しており、かつその情報が当該犯罪行為または犯罪活動に関係する場合に限り当該個人に関する犯罪課報情報を収集しかつ保存するものとする」と規定した連邦規則集（CFR）28巻パート23.20(a)を含む、連邦規則集（CFR=Code of Federal Regulation）28巻パート23に規定された原則に準拠すること。
 - (b) どの政府機関、部署、局、部もしくは係が、
 - (i) 監視技術の共用、および
 - (ii) 監視データの共用について承認を与えるのか。
 - (c) その監視技術の指定された目的および利用についてはどの程度の共用が必要なのか。
 - (d) 団体は、適用ある監視利用ポリシーを遵守し、かつ、その監視データ共用の承認を受けていない者や団体に開示することなく、その監視技術または監視データを共用するために

どのようにアクセスするのか。および、

(e) その自治体や市議会から、監視技術または監視データ共用協定について、さらに承認を受ける場合には、どのような手続をするのか。

(11) 監視データへのアクセス要求：政府機関もしくは第三者が、監視データにアクセスを求めるまたは命じる場合には、どのような法的要件を充足しなければならないのか。

(12) 研修：監視技術の利用または監視データへのアクセスを認められた個人は、どのような研修、研修資料を含む、を受けるように求められるのか。

(13) メンテナンス：監視技術の安全性および清廉性はどのように維持管理されるのか、ならびに、自治体またはその代理人がその監視技術機能に実質的変更がなされる場合の市議会での承認においてどのように説明したらよいのか。

(14) 監査および監視：監視利用ポリシーが実効性あるものであるためには、ポリシーを遵守するために内部の人員にどのような任務が付与されているのか、どのような独立当事者もしくは機関に対して監視権限が与えられているのか、ならびにこのポリシーへの違反がある場合にはどのような法的な執行できる制裁があるのかを含む、どのような仕組みが準備されているのか。

(15) 苦情の申出：特定の監視技術の設置または利用について一般住民が苦情もしくは関心事を申し出るまたは質問を提出するにはどのような手続をとる必要があるのか、どのような内部の人員がこうした伝達を受け、記録、追跡および対応する任務を担うのか。

(16) 監視利用ポリシーの素案は、修正のあるなしにかかわらず、市議会の投票により、承認を受けるときまでは、免責文書 (disclaimer) とみなされる。

第3条

本法の施行日前から利用している監視技術を継続して利用したい自治体は、この法律の施行日から120日以内に、第2条第A項第3号の規定に基づき市議会による承認手続を開始しなければならない。市議会は、その提出から180日以内に、第2項条第B項の規定に基づく監視影響報告書や監視利用ポリシーを含む当該監視技術の継続利用を承認しない場合、当該自治体は、本法の規定に従って市議会がそ

の承認をするまで当該監視技術の利用を停止するものとする。

第4条

1つ以上の自治体がその監視技術または監視データにアクセスを望む場合には、主導する自治体を指定するものとする。当該主導自治体は、その監視技術の維持管理に責任を持ち、かつすべての関連法、規則および議定書を遵守する責任を負うものとする。当該主導自治体は、その責任を他の政府機関、部門、局、部もしくは課または人員に委任しようとする場合には、それらの責任ならびに関係機関等および／または人員を明確に指定するものとする。

第5条

市議会は、その監視技術の利益がその費用を上回ると判断し、その提案が市民的自由および市民的権利を保護し、かつ、当該監視技術の利用および設置が差別的もしくは観点別要因に基づいておらず、いかなるコミュニティまたは集団に対する差別的効果を持たない場合に限り、当該監視技術の財源、取得または利用を承認するものとする。一般住民がこうした問題の検討に参加できるように支援するために、当該監視技術が利用に供される期間にわたり、あらゆる承認された監視影響報告書および監視利用ポリシーは、関連する自治体のウェブサイトの指定箇所 (HP) で一般住民に提供されるものとする。市議会は、監視技術の財源確保、取得および／または利用の承認にあたり、第2条第D項第5号 (a) の規定に基づき監視影響報告書に市民的権利または市民的自由に対する潜在的な差別的効果が生じるとの危険を確認した場合には、そうした不本意な効果があっても同意できると解してはならない。このことから、そうした効果の危険性が存在するときには、積極的に回避すべきものと認識すべきである。

第6条

(A) 自治体は、監視技術を利用する場合には、市議会から承認を得なければならない。そして、一般住民が、その自治体が利用する個々の監視技術に関する年次監視報告書 (Annual Surveillance Report) を、市議会の承認を受けてから12か月以内に、かつ、その後は毎年3月15日までに、自治体ウェブサイトから閲覧できるようにするものとする。年次監視報告書は、少なくとも前暦年の次の情報を含むものとする。

(1) その監視技術がどのように使われたのかの概要

(2) 収集された監視データが外部の者または団体との共用に提供されたかどうかおよび共用は何

度行われたか。監視データを受領した者または団体の名称、開示されたデータの類型、どのような法的基準に従ってその情報は開示されたのか、その開示を正当とする理由

- (3) 該当する場合には、監視技術が、合衆国国勢調査局により当該年に定義された個人国勢統計区（census tract）に即して地理的に配置された場所の詳細。各国勢統計区に関し、その自治体は、延べで何日間その監視技術が配置され、かつ各日ごとに報告される配置の何パーセントが（A）令状によるものであるか、そして（B）何パーセントが裁判所の許可のない令状なしのものであるか報告するものとする。
- (4) 該当する場合には、その監視技術は、どれくらいの回数にわたり、潜在的もしくは現実の（A）暴力的な犯罪、（B）非暴力歴な犯罪、（C）重罪、（D）軽罪（E）その他法令違反、重罪もしくは軽罪には分類されない違反、不法な行為、または潜在的な将来の犯罪、暴力団その他の集団への実際もしくは予見される参加にかかわる指標となる行動もしくはパターンを調査するために利用されているかどうか。
- (5) 該当する場合には、実務的可能な限り最大限の正確性をもって、その監視技術が、どれくらいの数のソーシャルメディアアカウントや住民を対象としたのかなどを含むインターネットの監視活動に利用されたのか、および報告される監視活動（monitoring）の何パーセントが（A）令状によるものであるか、そして（B）何パーセントが裁判所の許可のない令状なしのものであるか報告するものとする。
- (6) 該当する場合には、その監視技術は、どのような自動車や建物に設置されたかなど、設置の詳細
- (7) 該当する場合には、どのようなハードウェア監視技術のソフトウェアが設置されたのかの詳細
- (8) 該当する場合には、監視技術が適用される、その回数を含む、データベースの詳細
- (9) その監視技術に関して受け取った苦情または問題点の概要
- (10) 最初の監査の結果としての監視利用ポリシー違反の情報およびそれに対して取られた行為
- (11) その技術の利用が合衆国憲法修正第1条、第4条および第14条などに保障された一般住民の市民的権利および市民的自由に及ぼした

差別的、差別的効果その他の影響の分析

- (12) 公文書法の請求、対応状況を含む、に関する統計および情報、ならびに、
 - (13) その監視技術にかかった、人件費そのた運営費用を含む年間の総費用、および次年度にその技術に充当する財政源
- (B) 第6条第B項の規定に基づく年次監視報告書を提出してから30日以内に、自治体の機関は、よく知られた交通の便がよい場所に一般住民を招き、その年次監視報告書およびその自治体の機関の監視技術の利用に関する審議および質問応答をするために一回以上の住民集会を開催するものとする。
 - (C) 年次監視報告書に記載された情報に基づき、市議会はその監視技術の利益がその費用を上回るかどうか、一般住民の市民的自由や市民的権利が十分に保護されかつ安全であるかどうかを精査するものとする。利益が費用を上回らない場合、または市民的自由や市民的権利が十分に保護されかつ安全でない場合には、市議会は、その監視技術の利用を停止するように命じる、または、観測された問題点を解消するために監視利用ポリシーの修正を求めるものとする。

第7条

市議会または指名された代理人は、遅くとも各年の4月15日までに、次のような情報を含む前暦年の報告書を、文書およびウェブサイトを使って、一般住民に開示するものとする。

- (A) 監視技術の財源、取得または新規の利用に関して、本法の規定に基づき市議会へ提出された承認申請の数
- (B) 監視技術の財源、取得または新規の利用に関して、本法の規定に基づき市議会へ提出された申請の承認件数
- (C) 監視技術の財源、取得または新規の利用に関して、本法の規定に基づき市議会へ提出された申請の拒否件数
- (D) 監視技術の財源、取得または新規の利用の承認に先立ち、市議会が監視影響報告書および監視利用ポリシーの修正を求めた件数
- (E) 第6条の規定に基づき提出されたすべての年次監視報告書。公的報告書の印刷される文書は、報告書全文を印刷する形に代え、その年次監視報告書の必要箇所を検索でき、印刷できるようにする。

第8条

- (A) この法律に基づく承認を受けないで監視技術の

財源確保、取得もしくは利用等、またはこの法律が承認していない方法もしくは目的で監視技術を利用したことにより、この法律の違反した場合には、権利侵害となり、いかなる者も、この法律を執行する管轄権限のある裁判所において、差止請求、宣言的救済、職務執行令状、証拠隠滅を理由に手続を開始することができる。

(B) 裁判所は、この法律を執行するために提起された訴訟において原告が勝訴した場合、訴訟費用と合理的な弁護士費用を与えるものとする。

(C) 自治体職員またはその代理人は、自治体、州もしくは連邦が宣言した緊急事態に應える場合を除き、この法律の規定に基づき承認されたポリシーを遵守する方法による以外、いかなる監視技術も利用してはならない。また、いかなる状況においても、監視技術を、差別的、観点別または市の憲章、州の憲法もしくは合衆国憲法に違反する方法において利用してはならない。いかなる自治体の職員も、この法律または施行ルールもしくは規則の規定に違反する場合には、懲戒手続および処罰の対象となる。労働協約の規定に従い代表者となる自治体職員にとり、この法律が、当該労働協約、その労働協約に基づき署名した覚書または申合せもしくは協約対象者の間で確認しかつ確立した慣行と抵触する場合を除き、優先する。

(D) 内部通報者保護

(1) いかなる自治体または自治体を代表する者は、職員または職員応募者に対し、報酬、就労期間、条件、情報開示、適正手続権の制限、雇用上の特権または民事もしくは刑事責任などの面で、個人的行為を取るもしくは取らない、または取るもしくは取らないと脅してはならない。なぜならば、

(a) 職員またはその応募者は、この法律への違反の証拠を開示する善意の信念に基づき、いかなる関連自治体機関、自治体の法執行機関、告発もしくは捜査機関または市議会議員に対して監視技術または監視データの財源確保、取得もしくは利用に関するいかなる合法的な開示を支援するまたは支援するつもりであったと認められるからである。または、

(b) 職員またはその応募者は、この法律の目的を遂行する手続または行為を支援するもしくは参加するまたはそうするつもりであったと認められるからである。

(2) 自治体業務をする自治体職員またはその他の者は、この法律を遵守しないとす善意の苦情

申出を行った個人に対する報復を行った場合には、懲戒処分理由となる。

(3) 職員またはその応募者は、第8条第D項第1号違反により損害を受けた場合には、管轄権限のある裁判所に対して金銭的賠償および差止請求のための手続を開始することができる。

(E) 加えて、次の者は、罰則の対象となる。

(1) この法律に故意に違反した場合には、軽罪とみなされ、各違反については2,500ドル以下の罰金もしくは6月以下の懲役に処し、またはこれを併科する。

(2) この法律に過失で違反した場合には、軽罪とみなされ、各違反については1,000ドル以下の罰金に処す。

第9条

この市またはいかなる自治体も、この法律の規定に反する契約その他の協定を締結すること、および、当該契約または協定に秘密保持協定などを含むこの法律に反する条項を挿入することは違法である。この法律の制定以前に締結された契約または協定のなかにある違反規定は、法律が許容する範囲で無効であり、かつ、法的に執行できないものとみなす。本項は、この法律施行前に成立した労働協約およびその協約に基づき署名した覚書または申合せには適用されない。

第10条

この市またはいかなる自治体も、その源泉を問わず、追加的な負担金の賦課、未払いの罰金もしくは債務を含む、金銭その他の対価との交換において、いかなる非政府団体に対しても、監視データの受領または監視データの提供を促進するいかなる契約その他の協定を締結することは違法である。この法律の制定以前に締結された契約または協定は、本項に違反し、法的に可能な限り速やかに停止されるものとする。

第11条

この法律の規定は、無効とされた部分について分離可能である。この法律の規定のいかなる部分、またはいかなる者または状況に対するこの法律の適用が無効と判断された場合でも、この法律の残りの部分は、他の者または他の状況に対する適用を含め、そうした判断の影響は受けず、引き続き執行可能かつ有効である。

第12条

この法律は●●年●●月●日【交付の日】から施行する。

メイン州：監視技術の透明化を推進する法律【仮訳】

An Act to Promote Transparency with Respect to Surveillance Technology

【邦訳責任者】 石村 耕 治（PIJ代表）

この法律は、次のとおり、メイン州の住民により制定された。

第1.5章 第59条 州による監視技術の取得および利用（定義）

第1項

本条において、別段の定めがある場合を除き、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

第A号 「州の施設(State entity)」とは、事務所、省、機関、公団、組織体その他州の機関をいう。

第B号 「監視データ(Surveillance data)」とは、監視技術を使って収集、捕獲、記録、保存、処理、傍受、分析または共有されたあらゆる電子データをいう。

第C号 「監視技術(Surveillance technology)」とは、電子監視装置、ハードウェアもしくはソフトウェアを装備した特定の者もしくは集団その他のシステム、装置または手段を使って、音声、視覚、デジタル、位置、熱、生体その他の情報または通信を収集、捕獲、記録、保存、処理、傍受、分析または共有することを可能とするあらゆる電子監視装置、ハードウェアもしくはソフトウェアをいう。

（監視技術 取得および利用の要件）

第2項

州の施設は、本項に基づいて州議会で事前に承認されていない目的および方法において、監視技術を取得する、監視技術を取得、共有もしくは貸与する、監視技術を利用する、または監視技術もしくは監視データを他の施設と一緒に取得、共用その他の利用契約を締結するもしくはその提案をするために資金提供または現物支援を求めている。ただし、次の場合は別である。

第A号 州の施設が、取得または利用を予定している監視技術の機能性、監視技術に関する予定された活動、利用を予定している技

術が市民的権利および市民的自由に対する有害な影響があるかどうか、有害な影響を回避するために取られるべき措置、州の他の施設が任意に監視データの共用が認められるべきかに関する公聴会を開催する場合。この場合において、州のその施設は、公聴会に先立ち、少なくとも14日前に州内に広く頒布されている新聞に当該公聴会に関する公告をするものとする。州のその施設は、一般の人たちに対して、公聴会で文書もしくは口頭で証言を行い、かつ公聴会の閉会から10日以内に文書で証言する機会を与えるものとする。

第B号 州議会が、監視技術にかかわる予定された活動を承認する場合。本号にいう「議会の承認(legislative approval)」とは、次のような法律の制定を意味する。

- (1) 特定の活動のための監視技術を明示的に承認すること。
- (2) 前(1)にいう活動を明示的に承認するための監視技術の利用を制限すること。
- (3) 監視データを任意に共用する州の施設がある場合には、それら他の施設を列挙すること。
- (4) 立法府が監視技術の利用を承認することは、立法府が、市民的権利や市民的自由に対する有害な影響を回避するために必要と考えるいかなる措置をも取るのを条件とすること。

（無人飛行機の取得）

第3項

第95条において課される要件として、法執行機関が、無人飛行機(unmanned aerial vehicles)を取得する場合には、当該取得を求めている法執行機関を監督する統治団体の統治機関、または、州の機関の場合には当該機関の長、による承認を受けなければならない。

（無人飛行機を操作する法的執行機関）

第4項

無人飛行機を操作する法的執行機関は、連邦航空局(Federal Aviation Administration)からの

認可証の取得または免責および本 59 条の要件の充足を含む、連邦航空局が課した要件やガイドラインに完全に従わなければならない。加えて、法的執行機関による無人飛行機の利用には、次の規定が適用される。

第 A 号 法執行機関は、少なくとも第 5 項に規定された基準を満たすことなしに無人飛行機を利用してはならない。

第 B 号 メイン州憲法または合衆国憲法で保障された要件の例外にあたると認められる場合を除き、法執行機関は、令状なしに、刑事捜査目的で無人飛行機を使用してはならない。

第 C 号 第 A 号にもかかわらず、法執行機関は、無人飛行機を捜索および救助活動目的で利用することができる。ただし、当該法執行機関が、無人飛行機の利用が人に対する差し迫った危険を緩和に必要である

か、またはその利用にかかる訓練に必要である場合に限る。

第 D 号 第 A 号にもかかわらず、法執行機関は、事故の現場検証のための航空写真、森林火災そのた火災現場、洪水の現況および風害などについて、犯罪の捜査以外の目的でも無人飛行機を利用することができる。

第 E 号 いかなる場合においても、メイン州においては、州または自治体の法執行機関は、武装した無人飛行機を利用してはならない。

第 F 号 法執行機関は、言論の自由や集会の自由といった憲法上の権利の平穏な行使に対して無人飛行機を利用してはならない。

第 G 号 第 A 号にもかかわらず、法執行機関は、当該機関の行政官の長または州知事が承認した緊急事態に対して無人飛行機を利用することができる。

プライバシー
ニュース

日印連携で、アフリカでの生体認証式監視システム普及は危ない！！

わ

が国の NEC は、インドで、生体認証式国民 ID 番号カード制（アドハー・ナンバー・カード制 / Aadhaar number card system）導入に途を拓いた。この問題は、PIJ の CNN ニュース 91 号「インド、個人 ID 番号や生体認証式カードは違憲か？」で紹介した。このインドでの実績をもとに、日本の NEC とインド政府が連携し、生体認証式監視システムのアフリカ諸国での普及をわが国の経済産業省が支援するという。8 月 28 日から横浜で始まった T I CAD（アフリカ開発会議）で、日本政府は目玉策としてアナウンスした。

今後、わが国の官民関係者がアフリカ諸国を訪れ、本格的な調査に乗り出すという。しかし、

「ちょっと待った！」である。紛失・悪用されても変更できない指紋や顔、目の虹彩などの生体認証情報の汎用は危険である。とくに、法の支配、プライバシー保護法制の確立されていない途上国では、大規模な人権侵害を引き起こしかねない。独裁政権に悪用されたら、民主政体を破壊する強力なツールになる。

立憲民主とかは、こうした産官連携の危ない政策にしっかり物申したらどうか？れいわ新選組とか N 国党が伸びるのは、選挙民が給与泥棒集団に失望しているからではないか？

（CNNニュース編集部）

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 Eメール : wagatsuma@pij-web.net

編集・発行人 中村克己

Published by

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

<http://www.pij-web.net>
2019.10.10 発行 CNN ニュース No.99

入会のご案内

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

・顔認証技術を使った監視社会化、監視国家化が止まらない。99 号では、アメリカでストップをかける動きを紹介した。わが国の憲法やプライバシー専門の識者は沈黙するか、推進の旗振りが多勢だ。御用集団に頼らず、生体認証技術の市民的コントロールに向けて議論を進めよう。(N)