

* 英文: [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-558619](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-558619))

日本版 US-VISIT の実施に対する国際抗議署名

法務大臣
鳩山邦夫殿

2007年11月6日

Privacy International (発起団体)
London

日本国内連絡先
小倉利丸 (Privacy International, International Advisory Board)

日本へのすべての入国者から指紋と顔写真を収集する計画について

来日する外国人すべてへの指紋押捺と顔スキャンの計画に関して、私たち、人権と市民的自由に取り組む世界中の団体は、法務省による出入国および難民認定法の実施を目前に控えて深い憂慮の念を抱いていることを表明するためにこの書簡をしたためています。

私たちは、日本に来日する人々と日本在住の外国人に対する指紋押捺と顔スキャンの計画が、世界中の国境管理のなかでも最悪のやり方を真似ることによって、市民的自由に対してきわめて重大な侵害をまねいていると考えます。

私たちは、このシステムの実施を再考することを求めるものです。私たちはまた、法務省は世界に対して、この種のシステムのデータ処理の性格についてほとんど何の説明もしないままであり、なぜ人々が日本を訪れてこのような迷惑きわまりないことに直面しなければならないのか説明すべだと考えます。私たちはこのシステムの実施が日本の旅行業や日本に来る外国人労働者の流れに悪影響を及ぼすと考えます。

背景

日本の出入国管理計画では以下のように述べられています。

「テロリスト、過去に我が国から退去強制された外国人及び犯罪を犯した外国人を水際で確実に発見し排除するためには、従来から行っている偽変造文書対策を更に強化するとともに、バイオメトリクス(生体情報認証技術)の出入国審査への活用が有効と考えられる。

そこで、「テロの未然防止に関する行動計画」(平成16年12月10日国際組織犯罪等・国際テロ対策推進本部決定)に基づき、上陸審査時に外国人の顔画像及び指紋情報の取得を行うため、実施に当たっての諸留意点を整理した上、諸外国の動向等を踏まえつつ、法的整備を行っていくこととするなど、必要な準備を進めていく。」*1

すべての日本に入国する外国人の顔スキャンと指紋押捺を行い、この情報を長期間保有し(80年にわたって保有するともいわれている)他の個人情報と結びつけるというこのシステムをこの数週間以内に実施しようとしている時に、私たちはこの問題に関心を払うようになりました。

プライバシーの権利への侵害

日本の計画は個人の人権、とりわけプライバシーの権利に反するものです。プライバシーの権利は、多くの国際人権条約ではっきりと認められているものです。世界人権宣言はその第12条でプライバシーの権利を定めています。同様の文言は国連の市民的及び政治的権利に関する国際規約の第17条、移住労働者条約第14条、そして子どもの人権条約第16条でも採用されています。私たちは、日本の最高裁が日本国憲法第13条のプライバシーの権利を評価してきたということにも留意しています。

日本のシステムは無差別にプライバシー上重要な個人情報を全ての外国人の旅行者から集めることを目的としています。このような人間の情報を処理する大規模なプロジェクトは、日本を訪れる全ての訪問者をあたかも犯罪者であるかのように扱うものです。

私たちは取得された情報の保護措置や異議申し立ての方法に関する情報がないことに驚きを禁じ得ません。そのかわりに、私たちに示されているのは、テロリズムと闘うことの重要性についてのレトリックとこの新たな要求に応じなかった者を確実に強制的に送還するということなのです。

これは、日本のプライバシー法が国際標準にてらして不十分なものであるとみなされるが故にとりわけ危惧されるものです。私たちは、日本が OECD のプライバシーガイドラインなどの国際的な標準を最近のふたつの法律にあるていど適用していることに留意しています。民間企業に対する法律はある程度国際標準に従っていますが、政府機関によって保有されているデータの使用と共有に適用されている法律はきわめて不十分なままです。これは、日本政府が大量の個人情報を収集するのに必要な透明性の構造をもっているという私たちの信頼を損なうものです。

人権の保護は、個人が外国との国境で入国を待っている瞬間にもっとも弱いものになります。伝統的に、政府は他国からの入国者を互惠主義の名目のもつて敬意を払います。つまり、もし、日本がわが国の市民を敬意をもって扱うならば、わが国は日本の市民を同じように扱うということです。日本は、観光客や海外からの商用で来日する旅行者の詳細な個人情報を、プライバシー保護の裏付けもなければ異議申し立ての手段もないなかで、入国の条件として無差別な方法で収集することによって、彼らの尊厳に対して、著しく敬意を損なうような扱いをするということを示しています。

私たちはまた、日本政府が実施しようとしているシステムをこれまで批判してきたことにも留意します。2002年の国際民間航空機関の会合において、日本代表は「日本人は合衆国の提案を残念に思っている」とし、代表は「なぜ合衆国が日本の市民をもはや信用しなくなったのか」理解に苦しむとともに生体情報の一方的な使用は毎年米国を訪れる1700万人に悪影響をもたらすであろう」と述べました。^{*2} 私たちはこの事態の成り行きと見解に驚きを禁じ得ません。

複雑でリスクのあるシステム

個人情報を収集しそれをデータベースで集中管理することはプライバシーを危険にさらすとともに、セキュリティのリスクを招くことになるでしょう。

私たちは、日本が US-VISIT プログラムによって米国が作り出したやり方に従っていくというのは大きな間違いだと確信しています。日本のシステムが実施されるまで、世界で唯一合衆国だけが、すべての入国者の指紋と顔スキャンを行いこの情報を長期にわたって保有するということをやってきました。このプログラムが実施されて数年、私たちは皆今合衆国が国境管理の模範例ではなくむしろ悪しき教訓として銘記すべきであるということを理解しています。

US-VISIT システムは日本のシステムと同様の方法で承認されました。すなわち、ほとんど公の

場での議論や政策的な検討もなされないまま高度な政治的な判断で承認されたものです。米国では、慎重な政策的な開発と展開のかわりに、政府はテロとの闘いと犯罪というレトリックに頼りました。数年を経た現在、US-VISIT システムは結局、多くの問題点が指摘され、先進的な国境管理システムなるもの現実がはっきりしてきました。米国政府の報告から以下のことがわかります。

- 4年間で 13 億ドルを支出してシステムの半分しか達成できていない。*3
- 「効果的なプログラムへの監督や透明性の十分な基盤」を欠いたまま、「不明確な計画あるいはコスト、利益、リスクによって正当化された」プロジェクトへの支出が続いていること。
*4
- 米国政府は「関連する国境のセキュリティと移民法執行に際してのイニシアチブとのはっきりとした関係性も含めて、明確に規定された運用の状況もなしに、US-VISIT に投資しつづけている」*5
- 「コンピュータと操作上の諸問題を確認し評価するための管理運営が不十分であり一貫性を欠いた扱いがなされており」したがって「期待外れにおわる」とみられつづけてきたように、「長年にわたって USVISIT の管理は難問と将来の不確かさに直面しつづけている。」*6
- 「新たな情報の取得も財務管理もなく」、プロジェクトの責任者は「経済的に USVISIT への投資の拡大を正当化することやその運用によって得られるインパクトの査定に失敗しており」、その評価の範囲が極めて限られていることにその原因もあって「出入国に関する運用と設備の機能のインパクトの評価がなされていない。」*7
- 「契約が効果的に管理、監督されていない」*8
- そして最後に、セキュリティは「弱体化し、総体として、個人を特定しうる情報を含めて、権限をもたない個人がプライバシー上重要な情報を読み、コピーを取り、削除し、変更を加え、US-VISIT システムを妨害しうる」といったリスクが増加している。」米国上院の国土安全保障委員会の議長、ジョセフ・リーバーマンによれば、米国政府は「この国境を越える潜在的なテロリストを捜し出すプログラムに納税者の金を 17 億ドル使っているが、このプライバシー上重要な情報をハッキングし、変更したり削除するといったことを防止するもつとも根本的な予防措置をとっていない。」という。*9

したがって、米国の国境管理システムはしばしばうまくいかないのは驚くにあたりません。幾度となく米国の国境管理システムはダウンし、その結果何千人もの人々がシステムの不具合が解消されるまで待たされました。たとえば、2007年8月に、2万人の旅行者がロサンゼルス空港で立往生し、空港のロビーや、空港が満杯になったために、空港内に入ることすら禁じられて飛行機から降りられず飛行機の中で一夜を過ごす旅客もいました。*10

もっとさまざまな問題が世界中で起きています。査証データベースが保有する個人情報を第三者が利用できるために潜在的ななりすましの危険性をもたらすような劣悪なセキュリティ・プロトコル*11 や指紋のミスマッチが多くての不当な措置をもたらしています。適切な計画と配慮なしに、日本を訪れる人々は、開示を強いられる彼らの個人情報が適切に日本のシステムで保護されると信じる理由はどこにもないのです。

効果的な国境管理に向かうのか？

日本は米国の後を追うようなことをしないように注意すべきです。ここ最近、米国は出入国と入国手続きに関しては、訪問地のランクでは最悪を記録し、ついで中東が続いています。*12

ツーリストや商用旅行者をテロリストのように扱うのではなく、日本への訪問者を歓迎するもっとよい方法がある。国境での身分証明犯罪に関してプライバシーに配慮した方法があります。そして、すべての訪問者のプライバシーを侵害し日本のシステムからのデータ漏洩によって訪問者たちのアイデンティティの窃盗の危険にさらすことなく国境において犯罪者を特定する効果的な方法があります。

たとえば、出入国管理官は、インターポールによって収集された世界中の盗難や紛失パスポートを参照することができます。こうしたことを実施している国はきわめてわずかです。これはより効果的でバランスのとれた解決方法のようにおもわれるかもしれません。

しかし、このような方法すら、旅行者の流れをなおかつ妨げるかもしれない間違いがありうるので細心の注意が払われなければならないのです。たとえば、米国の出入国管理官が16日間に集めた190万件のパスポート記録のうち、273件が盗難によるものとされました。しかし実際には219件は盗難ではなく、64件は未解決なままです。どのようなウォッチリストであっても、誤ったデータに対する必要な異議申し立てを認めるような明確な監視と透明性をもった仕組みが確立されてい

ければなりません。わたしたちはすでに米国のウォッチリストが、深刻なシステムの整合性の問題からますます手に負えないものになっており、間違っ無関係の人々をテロリストとみなして多くの問題が生じてきたことを見てきました。私たちは日本が実施するいかなるシステムも同様の問題を抱えることになるであろうと考えます。*13

わたしたちの経験では、テクノロジーのシステムは適切な政策的な配慮がなければ大抵の場合失敗します。私たちはまた移民政策は、それが果たすべき必要な注意と慎重な配慮をほとんど欠いた複雑な領域であると考えています。全ての日本への訪問者の指紋押捺と顔スキャンという日本の計画は、こうしたリスクを裏付けるものです。私たちは、日本での審議が日本語でのみなされてきた結果として、私たちの見解をもっと早くに提示できなかったことを残念に思います。

日本の計画は、日本が世界に占める位置にダメージを与え、すばらしくかつ美しい国をツーリストがこれまでのようには訪れるこのないような国にしてしまうことになるでしょう。そして、いたずらに、日本のグローバル経済のリーダーとしての役割を傷つけることになるでしょう。もしあなたの計画が根本から見直されることがなければ、日本政府がグローバルな旅行者のプライバシーとセキュリティの利益を十分に保障して計画をたてたと断言することに対して私たちは、日本への旅行のボイコットが唯一の手段となるということを憂慮するものです。

是非とも計画を見直していただきたい。また、もし、日本がこのような方向に進めば他の諸国もこれに追随し、日本がやったように日本の市民の指紋を採取しはじめるでしょう。こうしたシステムは、日本にとっても複雑で、リスクが大きく、不安全なものとなるでしょう。これは日本や日本の市民にとっても、そして私たちにとっても住みたいと思うような世界ではありません。

署名団体

Privacy International (発起団体)

Action on Rights for Children (UK)

APC Africa Women (Africa)

APC.au (Australia)

ArabDev (Egypt)

Asian Coalition for Housing Rights (Japan)

Association For Progressive Communications (International)

Associazione per la Liberta nella Comunicazione Elettronica Interattiva (Italy) ATTAC Japan

(Japan)

Australian Privacy Foundation (Australia)

AZUR Developpement (Congo)

Big Brother Awards (France)

Bluelink (Bulgaria)

British Columbia Civil Liberties Association (Canada)

BytesForAll.org (South Asia)

Canadian Internet Policy and Public Interest Clinic (Canada)

Colnodo (Colombia)

Community Education Computer Society (South Africa)

Digital Rights (Denmark)

Digital Rights Ireland Electronic Frontier Finland (Finland)

Electronic Frontier Foundation (US)

Electronic Privacy Information Center (US)

European Digital Rights (EU)

Fantsuam Foundation (Nigeria)

Focus on the Global South (Asia)

Foundation for Information Policy Research (FIPR)

Foundation For Media Alternatives (Philippines)

GreenNet (UK)

Greenspider (Hungary)

Index on Censorship (International)

International Civil Liberties Monitoring Group (International)

International Movement Against All Forms of Discrimination and Racism (Japan)

International Solidarity Action of the Have-Nots (Japan)

IRIS - Imaginons un reseau Internet solidaire (France)

Iuridicum Remedium (Czech Republic)

Japan Computer Access for Empowerment (Japan)
Japan Lawyers Network for Refugees (Japan)
JCA-NET(Japan)
Jinbonet (South Korea)
Joint Labor Union of Christian Offices and Businesses (Japan)

Laneta (Mexico)

Network Against JUKINET(Japan)
Networkers against Surveillance Task-force (Japan)
Netzwerk Neue Medien (Germany)
No2ID (UK)
NODO Tau (Argentina)

OneWorld Platform South West Europe (Bosnia-Herzegovina)
Open Rights Group (UK)

Peace Boat (Japan)
Peace Not War Japan (Japan)
People's Coalition against Wiretapping Law and Organized Crime Law (Japan)
People's Plan Study Group(PPSG) (Japan)
PINCH! Against War and Surveillance (Japan)
Privacy Journal (US)

RITS - Information Network for the Third Sector (Brazil)

San'ya Welfare Center for Day-Laborers' Association (Japan)
Sex Worker and Sexual Health (Japan)
Solidarity Network with Migrants Japan (Japan)
Statewatch (UK)
StrawberryNet (Romania)
Swiss Association to Defend Fundamental Rights (Switzerland)
Swiss Internet User Group (Switzerland)

Ungana Afrika (Africa)

VOICE (Bangladesh)

Wamani (Argentina)

WiLAC (Uruguay)

WomensNet (South Africa)

<注>

- *1 : 『第3次出入国管理基本計画』III 出入国管理行政の主要な課題と今後の方針
- *2 : Notes from Meeting of ICAO New Technologies Working Group', Berlin, Germany, June 25-28, 2002, documents unclassified by the U.S. Department of State in August 2004.
- *3 : Government Accountability Office, Prospects For Biometric US-VISIT Exit Capability Remain Unclear, July 28, 2007, GAO-07-1044T.
- *4 : Government Accountability Office, 'U.S. Visitor and Immigrant Status Program's Long-standing Lack of Strategic Direction and Management Controls Needs to Be Addressed' , August 2007, GAO-07-1065.
- *5 : Government Accountability Office, 'Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified', February 2007, GAO-07-278.
- *6 : Government Accountability Office, 'US-VISIT Program Faces Operational, Technological, and Management Challenges', March 20, 2007, GAO-07-623T.
- *7 : Government Accountability Office, US-VISIT Has Not Fully Met Expectations and Longstanding Program Management Challenges Need to Be Addressed, February 16, 2007, GAO-07-499T.
- *8 : Government Accountability Office, 'Contract Management and Oversight for Visitor and Immigrant Status Program Need to Be Strengthened', June 2006, GAO-06-404.
- *9 : Lieberman Cites Vulnerability of Terrorism Tracking Data', August 3, 2007, statement available at <<http://lieberman.senate.gov/newsroom/release.cfm?id=280527&&>>.
- *10 : Mayor calls for Probe of LAX Computer Crash', CBS, August 13, 2007.
- *11 : Security concerns hit web visa applications', Joe Churcher, The Scotsman, May 18, 007.
- *12 : How to help the huddled masses through immigration', Gideon Rachman, Financial Times,

March 12, 2007.

*13 : U.S. to use Interpol Passport Database for Screening', Spencer Hsu, Washington Post, May 6, 2007.