航空旅客情報のプロファイリングとプライバシー

代表研究者　　工　藤　聡　一　　日本大学大学院　法学研究科　教授

1 はじめに

本研究は､航空機上でテロに直接関与する可能性のある人物を搭乗前に特定するためのスクリーニングが、プロファイリング、データ・マイニングの手法を伴いつつ実施されている現状における、米合衆国憲法修正第 4 条（プライバシー保護）の問題を検討するものである。

同時多発テロ後、米国では空港における旅客身体・手荷物検査がすぐさま強化されたが、全米 20 余の主要空港における実験（2006 年）の結果、その全てにおいてダミー爆発物の持込が見逃されたと報道されているとおり､そしてその後の数々のテロ未遂事件の発生をみるとおりに､航空セキュリティを確保するには種々の手段を複合的に講ずるしかない。その意味で、活動資金源を途絶することはもちろん、通信傍受等の諜報を駆使するような事前措置、また空港における保安検査を強化し、併せて旅客情報のスクリーニング／プロファイリングによって既知又は未知のテロ実行犯を水際で確保する、予防措置も求められる。それが突破された場合の事後措置、すなわちコックピットドアの強化、スカイ・マーシャルの配置も必要とされる。

中でも、旅客情報のスクリーニング／プロファイリングは、いわゆるバックグラウンド・プログラムとして旅客一般を対象に実施されており、影響が大きい。すなわち、国土安全保障省（DHS）は、米国就航航空会社から、旅客の氏名、住所、性別の他、座席番号、決済記録、特別食リクエスト履歴（宗教上、医学上の含意あり）等、電子予約システム上の全旅客個人情報の継続的提供を受けており（19 C.F.R. 122.49d)、これをテロリスト・データベースと照合するほか、テロリストの行動パターンをプロファイルし、それと似た行動が認められる旅客を抽出し、これらを搭乗拒否、又は重点的スクリーニングの対象としている。その結果、旅行そのもののキャンセル、旅程の変更、リスケジュール等の重大な支障を来たす例が現れている。以下では、航空セキュリティの中心である空港セキュリティの現状を概観した後、そのうち、テロの脅威の前にこれまで必ずしも十分な法的検証がなされないまま運用が先行してきた、航空旅客情報のプロファイリングについて、主としてプライバシーの観点から光を当てることにする。

2 空港セキュリティの現状

2-1 航空テロの変質と空港セキュリティの対応

（1）航空テロの変質

国際テロ組織アルカイダ（al-Qaeda）の分子が一度に複数の民間機を強取するにとどまらず、それらを大量破壊兵器に転用して大規模構造物に衝突させるという酸鼻をきわめる事件の発生は、思いがけないところに潜むテロ脆弱性を白日の下にさらした。ハイジャック機を操縦するための長期にわたる訓練は彼らの際立った計画性と組織性とを示す反面、凶器として用いられたのは、高度な銃火器でも精巧な爆弾でもなく、安全基準をクリアする刃渡りの短いカッターナイフであったと推定されており、盲点を突かれたに等しい。この新奇のハイジャック類型に対応するため、米国政府は一方でテロ組織・活動に対するインテリジェンスを一層戦略的に行い、他方で空港における保安検査体制を強化し、かつコックピットドアの補強、連邦航空保安官（Federal Air Marshall, FAMs）の増員等、機上における危険の顕在化にも備えた。しかしその後も、航空テロの再発は「いまそこにある危機（clear and present danger)」であり続けている。次のような数々の未遂事件の発生、実行計画の露見は、テロの禁圧が薄氷の上にあることを物語っている。

（Shoe Bomber テロ未遂事件）　2001 年 12 月 22 日、パリ発マイアミ行のアメリカン航空 63 便に、28 歳（当時）のアラブ系イギリス人 Richard Reid が搭乗した。同人は、着用していたトレッキング・シューズの靴底に約 280 グラムのプラスティック爆弾を仕込んでおり、飛行中に導火線点火を企てたが、異臭に気

づいた乗員乗客に取り押さえられ失敗に終わったものである。その手口から Shoe Bomber（靴爆弾犯）の異名をとる。所持していたのは、強い爆発力をもついずれも結晶性粉末であるペンスリット（Pentaerythritol Tetranitrate, PETN）及び過酸化アセトン（Triacetone Triperoxide, TAPN）である。本件はアルカイダの関与がいわれており、イギリス発の計 7 便の大西洋路線便において、同様の爆破テロの計画があったことも後に明らかとなっている 。

（Liquid Bombers テロ計画事件） 2006 年 8 月 9 日、テロ計画の容疑で、主犯格の Abdulla Ahmed Ali（当時 28 歳）、Asad Ali Sarwar（当時 29 歳）、Tanvir Hussain（当時 28 歳）を含む 24 人のアラブ系イギリス人がロンドン周辺で一斉に逮捕された。アルカイダ指導者からの指示を受け航空機中の自爆テロを準備していたが、内偵を続けていた英米の捜査機関により実行を阻止されたものであ 。彼らは、飲料に擬したペットボトルを持ち込み、機内で混合して水素系の爆発物を生成するという手口で、少なくとも 7 機を飛行中爆発させ、乗客乗員の殺害のほか、地上構造物の二次被害をも狙っていたとされる。Liquid Bombers（液体爆弾犯）と称される所以である。

（Underwear Bomber テロ未遂事件） 2009 年 12 月 25 日、アムステルダム発デトロイト行のノースウエスト航空（当時）253 便の機上で、23 歳（当時）のナイジェリア人 Umar Farouk Abdulmutallab が、下着に縫い付けてあった PETN 及び TAPN のパッケージを着陸直前に爆発させようとしたが、不発に終わったものである。その手口から Underwear Bomber（下着爆弾犯）とも呼ばれる彼は、この犯行が「アラビア半島のアルカイダ（Al-Qaeda in the Arabian Peninsula, AQAP）」の指示に従うものであったことを自白している 。

航空テロに現れた「ある変化」について、多くは説明を要しないであろう。これらの謀略は、航空機の強取ではなくその破壊を狙ったものである。同時多発テロで最高潮に達したハイジャックの脅威であるが、同一手口を許すようなセキュリティ・レベルになくなったため、テロリストは航空機をターゲットとし続けながら、ハイジャックを封じられた捌け口として即席爆発装置（Improvised Explosive Device, IED）の使用にシフトしたと考えられる。巧妙に隠匿した爆発物は、金属探知機による保安検査（チェックポイント・スクリーニング）では発見し得ない弱点を突いたものである。

また、実行犯の自己狂信化（self-radicalize）の片鱗も窺える。アルカイダの工作員として長期にわたり訓練を受けたものだけでなく、アルカイダの分派の影響下でごく短期間のうちに急激に狂信化した者もいる。一般に、テロリストの自立化、拡散化というその活動を捕捉することが困難な状況が進行しつつあるといわれ、一匹狼（lone-wolf）やホームグローン（home-grown）、ホワイト・アルカイダ（white al-Qaida）といった実行犯の一層の拡散の傾向に鑑みれば、航空テロはもはや如何なる属性の如何なる者によって行われるか予断を許さないといえる。深刻化する脅威の前に、空港セキュリティは、従来認識されていたリスク要因に加えて、新たなリスク要因にも即応するという、全方位的な防御を要求されていることになる。

（２）空港セキュリティの構成

先ずもって、テロは、その意図を持つ者と（ヒト）、その実現を可能にする凶器（モノ）、さらに凶器の使用を許す環境という三つの因子が揃ったときに発生する。空港はこれらが合わさる場所であり、とくに前二者は決定的な要素であるから、従前よりこの二因子の変化に即応した空港セキュリティ対策の強化がなされてきている。すなわち、Shoe Bomber 事件をきっかけとして、手荷物検査場における保安検査対象に靴が含められるようになり、Liquid Bombers 事件以降、液体物の持ち込みは制限され、液体爆発物検査器（Bottle and Liquid Explosives scanner, BLE）によるチェックも付加されている。テロリストの搭乗を阻むために米欧間で行われている旅客予約情報（PNR）の情報共有は、同事件を教訓としたものに他ならない。Underwear Bomber 事件後は、ボディ・スキャナーが配備され、爆発物痕跡検知器（Explosives Trace Detection Portal, ETDP）の導入も進んでいる。

しかしながら、これらはいずれも対処療法であって、テロリストの狡知に対する後追いでしかない。姿のみえない彼らとの緊張関係が一層高まるこれからの時代にあっては、個々のスクリーニングの精度を向上させつつ、それらを重層化しないしは複合化して隙を作らないことが、些細な綻びから重大な被害を引き起こさないために必要になる。当初から自覚的に観念され設計されていたとはいい難いが、テロとの攻防を通じて米国が辿り着いたのが、①異物検出型スクリーニング（Contamination Detective Screening）、②個人識別型スクリーニング（Identity Verification Screening）及び③行動観察型スクリーニング（Behavior Observation Screening）というべき空港セキュリティ範疇の確立である。

①は、電磁波の照射により旅客の身体全体の輪郭を透写し、又は携行物の組成をスペクトル解析する高度

画像解析技術（Advanced Imaging Technology, AIT）を使用して、テロリストによる凶器、爆発物等の機内持ち込みを阻止しようとするものである。②は、「セキュア・フライト・プログラム（Secure-Flight Program）」において、航空旅客情報（Passenger Name Record, PNR）とテロリストデータベースとを照合して既知のテロリストの搭乗を食い止め、またテロリストの行動パターンをプロファイルしたうえで、PNR にアルゴリズムを適用して、未知のテロリストと疑われる旅客を重点的にスクリーニングしようとするものである。③は、旅客の行動、心拍、発汗等の異常から「害意（Mal-intent）」を検知する将来兆候検査技術（Future Attributes Screening Technology, FAST）を施用し、未知のテロリストの侵入を阻もうとするものである。これらは、既知と未知の実行犯双方に対応し、既知と未知の凶器双方に対応し、かつ既知と未知の環境双方に対応するために、相互に補完関係を有しているが、ここでは②の個人識別型スクリーニングを中心に考察を加える。

3 個人識別型スクリーニングの展開

3-1 個人識別型スクリーニングの生成

（１）CAPPS I から CAPPS へ

個人識別型スクリーニングにかかる実務上、及び立法上の展開は次のような経緯をたどる。1996 年の TWA800 便の空中爆発事件（当初テロが疑われた事件）後、今日的なレベルでの航空テロ防止システムの開発と運用が本格化する。クリントン民主党政権下で設置された連邦委員会での議論を踏まえ、1998 年にコンピュータ支援型旅客事前スクリーニング・システム（Computer Assisted Passenger Pre-Screening System: CAPPS I）の運用が開始される（Act of July, 1994, Pub. L. No. 103-272, sec. 44912, 108 Stat. 745, 1212-13）。ここでは三段階で旅客チェックがなされた。すなわち、第一に、住所、同行者、旅行歴、航空券購入方法等の約４０項目の特徴に照らし、疑わしき旅客を特定する。第二に、脅威として既知の個人と照合する。第三に、前二者に該当しない旅客をランダムに抽出し安全確認を行う、というものである。しかしこの CAPPS I は、①航空会社毎の個別システムとして行われ情報の共有がなされない、②氏名等の旅客情報が真正であることを前提とした表面的なものである、といった保安水準点で種々の問題を含んでいた。そして、2001 年の 9.11 同時多発テロが発生したのである。

コンピュータ支援型旅客事前スクリーニング・システムは、2004 年、こうした点に対処すべく第二世代として再構築されることとなる（CAPPS II; Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).）。CAPPS II は、新たに設置された運輸保安局（Transportation Security Administration: TSA）の下に集約された単一の政府システムとなり、航空会社から吸い上げられた旅客情報に加え、各種の政府データベース（国内及び国際指名手配者リストを含む）からの膨大な情報をも加味し、これに一定のアルゴリズムを適用し、CAPPS I に比べて脅威の抽出精度を上げる工夫がなされた。また、ここでは単に旅客とテロリストの氏名の突き合わせを行うに止まらず（No-Fly List）、要監視者の抽出を行って重点チェックを適用し遺漏なきを期すこととなった（Selectee List）。ところが、CAPPS II は結局正式に運用されることはなかった。というのは、保安水準を上げるために諜報的要素が非常に強くなったため、合衆国憲法修正第４条（不合理な捜索押収の禁止）、同修正第５条（デュー・プロセスの保障）、交通権の侵害（基本権としての市民の自由な移動の制約）、そして 1974 年連邦プライバシー法（国家機関による個人情報の利用範囲及び手続的セーフガード）等の関連で鋭い社会的批判にさられることとなり、こうした状況を重くみた TSA は施行停止を判断したのである。

（２）セキュア・フライトへ

もっともその後も航空テロの脅威が消え去ったわけではなく、TSA は拡張型 CAPPS I（Enhanced Computer-Assisted Passenger Pre-Screening: CAPPS IE）を手当することとなった。要監視者リスト（Selectee List）の利用、連邦政府による搭乗拒否者リストの統一的運用といった点で、CAPPS II の進化を摂取するとともに、人権侵害可能性の可及的排除にも配慮した、いわゆるセキュア・フライト・プログラム（Secure Flight Program）を採用したのである（Pub. L. No. 108-458, sec. 4012(a)(1), 118 Stat. 3638, 3714-15 (2004).）。情報管理の徹底に関しては、たとえば、TSA による監督の明文化がなされ、離陸後 72 時間での旅客データの廃棄がなされるなどのフローが明確となっている。セキュア・フライトは、現行制度として実施運用中である。なお現在は、素性の明らかな一部旅客を対象に、TSA Pre-Check と呼ばれるスクリーニングの簡素化プログラムも平行して運用されている。いわゆるリスク・ベースド・スクリーニングの

考え方に基づき、危険性の高い者に十分な保安資源を投下するための措置である。

3-2 個人識別型スクリーニングの確立

（1）セキュア・フライト・プログラムにおける 2 つのリスト

今日、個人識別型スクリーニングは、主として PNR から得られた旅客情報を基に、①連邦政府の法執行機関及びインテリジェンス機関が共用するテロリスト・データベースと照合された旅客について、既知のテロリスト、及びその可能性が疑われる個人として「搭乗拒否者リスト」に登載する部分と、②過去の犯行等から抽出したテロ実行犯のプロファイルと符号する属性・行動パターン等を有する旅客について、未知のテロリストの可能性が疑われる個人として「要監視者リスト」に登載する部分とを含んでいる。続いて、それぞれのリストの運用についてみておく。

（2）搭乗拒否者リスト

「搭乗拒否者名簿（No-Fly List）」は、連邦捜査局（FBI）及び国家中央情報局（CIA）等のインテリジェンス機関によって収集された特定の人物の氏名等を集積したものであり、連邦航空法に授権により、DHS 管轄下の TSA によって管理されている（49 USC § 114）。すなわち TSA は、「連邦航空局（FAA）の管理者、適当な連邦及び州の法執行官、並びに空港及び航空会社のセキュリティ担当者に対して、航空機の乗っ取りもしくはテロリスク、又は航空会社若しくは旅客の安全に対するリスクを有することが知られ、または与えること疑われる個人についての身元情報を通知する手続を設定する」権限において、このリストを運用している。2010 年 10 月以前、同様の名簿は、航空会社単位で保有され、かつ同名簿と搭乗予定者との照合も航空会社ごとになされていた。しかし同年 11 月にセキュア・フライト・プログラムが DHS によって開始されて以降、航空会社は、旅客情報をセキュア・フライトに送信し、国家的なシステムで一元的に管理されるに至っている。これは、バックグラウンドで機能するスクリーニングプログラムであり、米国国内線、及び米国発着の国際線の全旅客を対象として、連邦政府のテロリスト監視リストとの突合せを行うものである。これはまた、米国就航路線以外であっても、米系航空会社によって運航される国際線、さらには米国本土上空を通過する航空便の乗客に対しても適用される。テロリスト監視リスト（Terrorist Screening Database, TSDB）は、国土安全保障大統領令第 6 号（Homeland Security Presidential Directive 6）に基づき、TSDB に収録される以前において、テロを構成する行為に携わり、それを準備し、幇助し、又は関与していたことが知られ、又は合理的に疑われる者を収載したリストであり、法執行機関と接続する複数の政府機関の共同運営組織である、テロリスト・スクリーニング・センター（Terrorist Screening Center, TSC）が運用している。

ひとたび旅客情報が政府の監視リストと照合されると、照合結果が旅客の搭乗券の発券処理のために航空会社に戻される。航空会社は、同リストをチェックインカウンタの端末等で管理し、該当旅客に対して搭乗拒否の措置をとる。搭乗拒否者リスト上の特定の氏名又はそれに搭載された根拠は非公開である。一部メディアが報道したところでは、同リストに収載された個人名は 2011 年に 1 万人、2012 年に 2 万人であったとのことである。旅客自身が、搭乗拒否者リストに登載されているかどうかを知るのは、搭乗券の発券を受けようとするとき、または航空機に搭乗しようとするときである。すなわち、リストとの照合結果が判明するタイミングによって、当初から航空券を交付されず、又はその印刷が不可能となり、あるいは、航空機への搭乗を差し止めされるといったことがあり得る。しばしば、航空会社窓口係員は、そのような状況で旅客が搭乗拒否者リスト上にあり、DHS にコンタクトをとるよう説明するが、単に、DHS へのコンタクトを促すのみで、理由を明かさない場合もある。

（3）要監視者リスト

「要監視者リスト（Selectee List）」は、TSC によって分析されたテロリストのプロフィール及び行動パターンをアルゴリズム化し、PNR に適用したものである。同時多発テロの後、いわゆる 9/11 調査委員会報告書において、個人識別型スクリーニングの精度向上の必要性が指摘され、航空会社ではなく TSA が一元的に管理しテロリスト・データベースとの照合を行うべきとの勧告がなされた。Intelligence Reform and Terrorism Prevention Act of 2004 はこの勧告を法制化したものである。2010 年に開始されたセキュア・フライト・プログラムも、その一環である。伝統的に、政府機関は、それぞれの機関の目的に基づき、監視者情報を収集し管理するためのさまざまな方法を用いてきた。そうした各機関が個々に運用してきた以前の個別的監視者リストを一本化し、現在では、連邦政府の統合監視者リスト TSDB が運用されていることは先に指摘したとおりである。要監視者リストは機関横断的な組織である TSC によって運用されている。TSDB に搭載される個人についての根拠及び手続は非公開とされており、TSDB に搭載されている氏名等も同様で

ある。リストが開示されると、テロ組織は捕捉されていない分子を使おうとすると考えられ、より困難な対応を強いられることになるからである。

要監視者リストは、「飛行の都度、拡張されたスクリーニングを受けるよう、自動的又は意図的に選択された人物のリスト」である。ある人物がこのように選択された場合、その搭乗券に「SSSS」の文字列が表記される場合が多いとされる。

（4）是正請求制度

搭乗拒否者リスト又は要監視者リストに登載されたことについて異議をとなえる個人に対しては、TSC が主体となり、DHS その他の政府機関と連携して、登載に伴うたび重なる遅延その他の TSDB の運用にかかる問題を克服するための措置として、是正請求する制度が設けられている。すなわち、DHS TRIPS（Department of Homeland Security Traveler Redress Inquiry Program）は、理由なく名簿に登載されたことをもって、合衆国行きの便等で、搭乗拒否、追加的安全検査による遅延その他の困難を経験した旅客が、WEB からの申請により、是正措置管理番号（redress control number）を付与され、以後同様の措置を回避することができるというものである。DHS TRIP は、DHS を構成する諸機関によってレビューされるため、一定の時間を要する。審査が正常に終了した場合、DHS TRIP は決定通知を発する。この通知は、申請者が TSDB 又は搭乗拒否者リストに登載されているか否かの確認を意味せず、そのような情報の提供も含まない。ただし時に通知書は、不服の場合申請者が連邦航空法に従い（49 U.S.C. § 46110、連邦控訴裁判所に TSA の司法審査の管轄を与える根拠規定）、司法審査を求めることができる旨の文面を含むことがある。決定通知は、申請者の以後の旅行について何らかの保証を与えるものではない。また、判断の基となった記録を争い、又は修正を求める機会は与えられない。

4 個人識別型スクリーニングにおけるプライバシーの問題

4-1 個人識別型スクリーニングとプライバシーの衝突

（1）個人識別型スクリーニングにおけるプライバシーの問題

同時多発テロの発生前から、プロファイリングを含む個人識別型スクリーニングが航空保安水準に与える積極的効果と、他方でのそのプライバシー侵害可能性は議論となっていた。しかし、過誤（false positive）を恐れて脅威を見過ごし（false negative）重大な結果の発生を許すならば、同時多発テロを経験したいま、大きな禍根を残すことになろう。そのため今日では、公益と私益とのバランス確保のための理論構成を模索しようというのが判例・学説上支配的となっている。

特定の個人が搭乗拒否者リストに搭載される前に、彼又は彼女は通常、テロリスト監視リストにまず収録される。この収載は FBI その他のインテリジェンス機関の指示に基づく。リストへの登載によって搭乗を拒否されたことに抵抗しようとしても、当該個人は極めて限られた情報しか与えられない。あるいは、自らがテロリスト監視リストに載っているのかどうかさえ、返答を受けられない。連邦政府は、このような手続き上の問題を認識しているものの、国家安全保障上の理由により手続が予防的なものとなっていると説明している。しかし、修正第 4 条及び連邦プライバシー法に抵触する可能性については考慮されなければならない。

（2）合衆国憲法修正第 4 条と私人間のコミュニケーション

合衆国憲法修正第 4 条は、「不合理な捜索及び逮捕・押収から、その身体・家屋・書類及び所有物の安全を保障される人民の権利は、これを侵してはならない。宣誓または確約によって証拠づけられた相当の理由に基づくものであって、捜索すべき場所及び逮捕すべき人または押収すべき物件を特定して記載するものでなければ、いかなる令状も発してはならない。」としている。本条は、「市民の生活は政府の介入から自由であるべきである」との憲法起草者の認識を体現したものであるが、裁判所によって「独りにしておかれる権利（right to be let alone）」とも称されて、今日のプライバシーに関する包括規定としての役目を負わされてきた。その具体的保護対象は、個人の住居、又は個人的所有物という伝統的な保護を超えて拡大され、通信を含む私人間のコミュニケーションも、現代的な意味での「書類及び所有物（papers and effects）」にあたると考えられている。

この点についての先例、Katz 対 United States 事件（389 U.S. 347 (1967).）は、修正第四条に基づく救済を受けるためには、以下の 2 つの要件を満たす必要があるとする。第一に、プライバシー保護に対する主観的な期待が存すること、そして第二に、当該期待を社会が一般的に合理的であると認識していること、である。本事件において、家宅侵入のような物理的な侵害行為がなくとも、「合理的な期待」を害する行為とし

て、公衆電話ブースに盗聴器を取り付ける行為は修正第 4 条違反にあたるものとされた。

もっとも、搭乗拒否者リストに関して発生するプライバシー問題は、個人の電子的なデータのコミュニケーションの結果に関するものである。そのようなデータは、インターネット・プロバイダー（internet service provider）によって運ばれるが、これにより、修正第四条に基づくプライバシーの保護は放棄される結果、合理的な期待は認められない、というのが一般的な理解である。

（3）連邦プライバシー法による救済

Katz 事件判決から半世紀近くを経過し、行政機関によって大量の個人情報が収集され、私的なデータが脅威にさらされているとの認識から、連邦議会は連邦プライバシー法（Privacy Act of 1974）を制定した。 同法は、政府が個人情報を収集分析する秘密のデータベースを持つことを禁止するほか、その処理についても制限を加えている。すなわち、「いかなる政府機関も、いずれかの人との何らかの方法によるコミュニケーションによる記録の組織を含むいずれかの記録を開示してはならない。当該記録を有する個人に対する書面による請求、又はこれに対する事前の書面による合意のない限り、他の行政機関に対する開示も禁じられるものとする」としている。

同法をテロリスト監視リストの文脈で用いる際の課題は、明文により、それが適用除外とされていることである。理論上、当事者適格を有し原因を主張立証できれば、行政手続法（Administrative Procedure Act, 5 USC §702.）に基づき、自身の監視リスト上の地位を確認する司法手続を請求できるはずである。この点、APA は、「他の法令が、明示的又は黙示的に救済を禁じている場合」の救済を排除していることが指摘されなければならない。仮に、監視リストがプライバシー法の適用除外により同法に基づく救済を排除しているとすれば、APA に基づく救済も得られないことになる。

プライバシーの保護をめぐる議論が、搭乗拒否者リストないしその基となるテロリスト・データベースの創設と運用の文脈で一般的に行われているが、以上のとおり、修正第四条は非常に限定的な救済しか認めていない。アメリカン航空会社 CEO であった Robert Crandall が、「商業航空のシステムを使って旅行したいと思うなら、自分のプライバシーはあきらめることだ。もしもプライバシーの放棄を望まないのなら、飛ばないでおけ。君のプライバシーは、我々以外の人々の安全には換えられないのだ。（If you want to travel on the airline system? You give up your privacy. You don't want to give up your privacy? Don't fly. Your privacy isn't equal to the safety of the rest of us.）」 と表現したのは、こういうことである。

4-2 個人識別型スクリーニングの正当化事由

（1）行政的捜索に関する修正第 4 条の解釈

合衆国憲法修正第 4 条に関し、近時の Riley 対 California 事件（573 U.S. ___ (2014).）は、携帯電話の内容のプライバシーについて通話者は合理的な期待を有するとして、警察官による個人の携帯電話の令状なき捜索を違憲とした。本件で連邦最高裁は、携帯電話がもつ極めて大量の個人情報という点を重視した。携帯電話はビデオ動画、処方箋、銀行口座といったセンシティブ情報、以前であれば家宅捜索によって得られたような情報を含んでいるのである。この理論構成からは、住所や生年月日はもちろん、クレジットカード情報、疾患や宗教信条を推し量るべきミール・リクエストその他の情報を含む旅客情報は、特別の扱いを受けてよいように思われるが、この点でもプライバシーの配慮はその他の利益に劣後することになる。

すなわち、令状のない捜索は合理的でないと推定されるが、裁判所は、令状を要しない重要な例外として、「行政的捜索（administrative search）」を定義している。これは、高度に規制される産業において規則に従ってなされる探索であって、人々のプライバシー権の侵害に対して行政取締的な実質的価値が上回る場合に許容される、令状なき捜索をいう。ここに高度規制産業とは、伝統的には武器製造者、鉱業、採石業、廃物処理業、質屋などであり、その後「特別な必要性」を有する産業に拡大して解釈されている。政府の規制目的を促進するために、捜索の告知、捜索担当官の裁量の制限など、捜索は令状に代替する措置を伴うものとされ、規制目的を達するために必要最小限に仕立てられている（narrowly tailored）ことが必要となる。この行政的捜索の例外こそが、旅客情報のプロファイリングを正当化するために一般的に援用される理論的根拠である。

（2）行政的捜索としての合理性

令状なき行政的捜索の例外に該当するためには、それが合理的である必要がある。下級審は、このような合理性の存否を判断するための理論枠組を考案している。政府の「必要性」と個人のプライバシーの「期待度」とを比較考量するアプローチである（United States v. Skipwith, 482 F.2d 1272 (5th Cir. 1973).）。

前者に関しては、既知の凶器について完全な排除が約束されておらず、かつ未知の凶器が用いられる可能性を排除できないことからすると、モノの因子への対応のみでテロ対策は完結せず、ヒトの因子への対応を欠くことは許されない。そして、既知のテロリストによる成りすまし、未知のテロリストの侵入の可能性を排除できないことからすると、モノの因子についての対処もまた不可欠である。この相互補完の関係において、旅客情報のプロファイリングは、未知のテロリストへの水際対策の手段として、今日重要な一角を占めていることは間違いない。例えば、空港における行政的捜索は、銃火器、爆発物、空港の安全を害すべきその他の危険装置を探索する目的に限定される場合に一般に合憲であるとされるが、捜索がこれらの装置をそもそも不法に用いようとしているテロリストに向けられた場合に、行政行為を否定する論理は成り立たないというべきであろう。

後者に関しては、監視カメラや職務質問、身体検査や手荷物保安検査など、プライバシーが一定程度制限されるのがむしろ当たり前となっている、航空ないし航空の利用という特別な環境下では、個人情報の保護に対する期待度も、制約を受け得ると考えるのが自然である。そして旅客は、符合契約たる運送約款において、その個人情報の行政機関への提供に同意しているのである。

【参考文献】

Abeyratne, Ruwantissa, Aviation Security: Legal and Regulatory Aspects, Ashgate Publishing, 1998.

Abeyratne, Ruwantissa, Law and Regulation of Aerodromes, Springer, 2014.

Bartol, Curt R. & Bartol, Anne M., Criminal & Behavioral Profiling, SAGE Publishing, 2013.

Biles, Clay W., The United States Federal Air Marshal Service, Wendy Books, 2013.

Born, Hans, et al, International Intelligence Cooperation and Accountability, Routledge, 2011.

Bouchard, Andre E., ed., Airport Baggage and Passenger Screening, Technology Elements and Considerations, Nova Science Publishers, 2013.

Brown, David H., Airline Passenger Screening Has Become a FEMA-TYPE SNAFU, AuthorHouse, 2006.

Committee on Commercial Aviation Security, National Research Council, Airline Passenger Security Screening, Nat'l Academy Press, 1996.

Custers, Bart, et al. eds., Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases, Springer, 2013.

Edward, Halle, The Role of International Law in The Fight Against Aerial Terrorism: Penal Aspects of Aviation Law, Lambert Academic Publishing, 2012.

Elias, Bartholomew, Airport and Aviation Security, CRC Press, 2010.

Fiske, Ian D., Failing to Secure the Skies: Why America Has Struggle to Protect Itself and How It Can Change, 15 Va. J.L. & Tech. 173 (2010).

Florence, Justin & Friedman, Robert, Profiles in Terror: A Legal Framework for the Behavioral Profiling Paradigm, 17 Geo. Mason L. Rev. 423 (2010).

Haerens, Margaret & Zott, Lynn M. eds., US Airport Security, Greenheaven Press, 2013.

Israelsen, R. Gregory, Applying the Fourth Amendment's National-Security Exception to Airport Security and the TSA, 78 J. Air L. & Com. 501 (2013).

Kawakami, Sayaka & McCarty, Sarah C., Government Information Collection: Privacy Year in Review: Privacy Impact Assessments, Airline Passenger Pre-Screening, and Government Data Mining, 1 ISJLP 219 (2005).

Klitou, Demetrius, Privacy-Invading Technology and Privacy by Design, Springer, 2014.

Lowe, Dan, Note, The Flap with No Fly－Does the No-Fly List Violate Privacy and Due Process Constitutional Protection?, 92 U. Det. Marcy L. Rev. 157 (2015).

Masferrer, Aniceto & Walker, Clive, Counter-Terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State, Edward Elgar Publishing, 2013.
Meyer, Deborah L., The Spot Program: Hello Racial Profiling, Goodbye Fourth Amendment?, 10 RRGC 289 (2010).
Phythian, Mark ed., Understanding the Intelligence Cycle, Routledge, 2013.
Ravich, Timothy M., Is Airline Passenger Profiling Necessary?, 62 U. Miami L. Rev. 1 (2007).
Solove, Daniel J., Surveillance: Data Mining and the Security-Liberty Debate, 75 U. Chi. L. Rev. 343 (2008).
Smith, Donna, Passenger Profiling: A Greater Terror Than Terrorism Itself?, 32 J. Marshall L. Rev., 1998.
Sweet, Kathleen M., Aviation and Airport Security, Terrorism and Safety Concerns, 2nd ed., CRC Press, 2009.
Voegele, Amelia K. ed., Airport and Aviation Security, Nova Science Publishers, 2010.

以上、主要なもののみ。

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
次世代空港ｾｷｭﾘﾃｨの展望と課題	月刊治安ﾌｫｰﾗﾑ（立花書房）23 巻 1 号	2017.1 掲載予定
空港ﾃﾛﾘｽﾞﾑに対する三つの抑止ｱﾌﾟﾛｰﾁ	危機管理学研究創刊号（日本大学危機管理学研究所）	2016.10 投稿予定