신항공보안 정책적용에 있어서의 프라이버시 문제점

Implementation of the New Aviation Security Policy and Privacy Protection Problem

김장환*, 강자영(한국항공대학교)

I. 서론

9/11 테러 사태 이후 미 정부는, 자국 영토를 출입하는 항공기 승객 및 승무원의 개인 정보를 미 행정부에 제출할 것을 요구하는 다양한 법규들을 채택하였는데, 특히 항공사는 미 세관 및 국경보안국(CBP)이 Passenger Name Record(PNR : 항공기 승객 기록)에 내장된 탑승객 정보에 접근할 수 있도록 허락해야 하고, 이를 위반할 경우 벌금 부과, 착륙 금지, 도착 지연 등의 불이익을 당할 수 있다고 명시 하고 있다[1].

테러에 맞선 대응은 민주 사회의 필수 불가결한 요소임에는 틀림없지만 이 과정에서 개인의 기본권 및 자유(프라이버시 및 정보 보호 권리 포함) 또한 반드시 존중되어야 한다. 상업적 용도로 수집되어 항공사 DB 및 관련 예약 시스템에 저장된 개인 정보를 공공 기관이 접근하도록 허락하는 행위는 전 세계적으로 전례가 없는 경우일 뿐만 아니라 정보 보호 기본 원칙에 어긋난다. 그러나 9/11 테러와 최근의 런던 테러 사건에서 보는 것처럼 사회적, 경제적 파장이 엄청나고 그에 따른 후유증 또한 심각한 상황임을 간과할 수 없다. 현대의 테러리즘은 무차별적이고 대량살상을 목표로 하여 자신들의 존재를 알리고 그로인해 발생하는 사회적인 불안과 정부에 대한 시민들의 불신을 갖게 하는 효과를 얻을 수 있다. 즉, 무고한 시민들의 목숨을 잃는 것만으로 끝나는 것이 아니라 그에 따른 후유증으로 결국 정부가 시민들로부터 질타와 외면을 받아 정권자체의 존립에 큰 악영향을 미치게 된다. 그렇기 때문에 이 문제는 개인적인 프라이버시 차원을 넘어 국제사회 공통의 안전과 발전을 위해서 세계가 함께 다루어야 할 문제이다.

II. 미국의 항공보안정책 분석

1. 9/11과 보안정책 강화

9/11 테러 이후, 미국의 보안정책 변화와 프라이버시에 대한 방안을 살펴보면 미국 정부는 국토보안 강화를 위해 활발한 노력을 전개하고 있음을 알 수 있다.

우선 첫번째로 애국법(Patriot Act)을 제정하여 테러 방지 및 차단을 위해 적절한 도구 제공을 위한 미국의 단결 강화 법안(USAPA)은 9/11 발생 6주 만에 법제화되어 입법 구조에 많은 변화를 가져왔으며, 미 법기관의 감청 및 수사권을 대폭 확대시켜 연방 감청법의 프라이버시 보호 규정을 현저하게 약화시켰다. 이 법은 2001년 9/11 테러가 터진 후 45일 만에 테러 예방 차원에서 만들어졌는데 올해 말로 5년의 시효가 만료될 예정이었다. 총 215개 조항의 애국법은 연방수사국(FBI)의 권한을 대폭 확대했다. FBI는 테러 용의자로 판단되면 영장 없이 가택수색, 이동도청, 계좌추적을 할 수 있다. 인터넷.e-메일 조회와 의료기록 조사도 가능하다. 그러나 시민의 자유를 제한한다는 논란도 많았다.

애국법이 논란을 빚자 콜로라도 등 7개 주와 378개 카운티 의회는 지난해 애국법 반대 결의안을 통과시켰으나 최근 런던 테러의 영향으로 이 법의 효력은 무기한 연장됐다.[2]

두번째, 미국 방문객 및 신원 표시 기술인 US VISIT을 제안하였다[3]. 2003년 10월, 미국 정부는 테러 및 범죄행위 예방을 위해 미국에 입국하는 모든 외국인의 비자를 자동으로 추적·검색하는 컴퓨터 시스템을 개발하여, 2005년까지 미국의 주요 50개 국경 및 입국심사 장소에서 가동할 계획이라고 발표했다[4]. 단, 이미 생체인식 ID 카드를 발급하고 있는 일부 국가는 대상에서 제외되도록 하였다. 이 시스템의 개발

이 완료될 경우, 외국 주재 미국 영사관 관리들이 비자 신청자의 지문과 사진을 테러리스트 및 범죄자 DB와 1차적으로 대조한 후, 미국 국경 관리자들이 외국인 입국자의 지문과 비자 서류상의 지문 일치여부를 확인하여, 테러 및 범죄용의자의 입국을 차단하게 된다. 또한 비자 기간이 만료된 외국인에 대해서는, 자동으로 여행기록과 비자 정보를 분석하고 경고 신호를 보내게 된다[5].

세번째, Student and Exchange Visitor Information System(SEVIS : 유학생 및 교환 방문자 정보 시스템)가 있는데 이는 9/11 테러 이후, 비이민자와 유학생의 감시·추적·관리를 위해 만들어진 인터넷 기반 시스템으로, 2003년 2월 15일부터 시행되고 있다[6]. 이민국, 학교, 미대사관이 하나의 시스템으로 미국비자 획득부터 미국 입·출국, 출결석 사항 등의 일련의 모든 행동을 감시할 수 있도록, 학교가 정부에게 학생의 개인신상 정보, 학업 정보(입국 심사 허가 내역, 전공과목 변경 등) 및 징계 정보 등과 같은 학생 정보를 제출토록 하고 있다.

네번째, 국토안보부(Department of Homeland Security : DHS)의 설치를 들 수 있다. 미 정부는 새롭게 나타나고 끊임없이 진화하는 위협을 해결하기 위해, 관리기술과 최신 기술의 이점을 살려 기민하게 대응할 수 있는 신설 조직으로, 22개 기관을 통합하여 약 380억불 예산규모의 국토안보부를 정식으로 설립하여 더 많은 법적 강제력과 정보 공유권을 가졌지만 그것은 매우 제한된 수준의 정보자료 공개 의무만을 가졌다[7].

다섯번째, Total Terrorism Information Awareness(TIA)와 Computer Assisted Passenger Profiling System Ⅱ(CAPPS Ⅱ) 프로그램의 도입을 추진하였다.

미국의 국민 및 항공기 이용 여행객들의 테러 및 범행 가능성을 사전에 파악하여 테러 발생을 방지하고자 하는 프로그램이지만 이러한 국가안보 계획들은 불가피하게 프라이버시 보호와 충돌하는 경우가 종종 발생하는데 그 대표적인 침해논란이 되고 있는 것이 TIA와 CAPPS Ⅱ이다. 이러한 프라이버시 침해 논란에 대한 미 정부의 대응으로는 DHS 설립 근거법에 제한적인 프라이버시 조항을 포함하여 시민권리 담당관(Civil Right Officer)과는 별도로 프라이버시 담당관(Privacy Officer)을 두도록 규정하고, 프라이버시 담당관은 프라이버시법 준수 여부, 자체 규정에 대한 프라이버시 영향평가 보고서 작성, 의회에 제출할 연간 보고서의 작성을 담당토록 하고 있다. 그리고 DHS가 범국가적 ID 시스템이나 카드를 개발하지 못하도록 금하고 있다. 또한 국토안보부에 프라이버시국(Privacy Office)을 설치하여 약 350명의 직원들이 근무하고 있어 연방기관의 개인정보 수집·사용·제공 등과 관련된 프라이버시보호법의 준수 여부를 감독하고 있다. 이에 따라 우리나라도 TIA와 CAPPS Ⅱ 프로그램의 도입배경, 이행 그리고 프라이버시 관련 논의의 분석을 통해 향후 한국정부의 정보사용 노력에 표본으로 삼을 필요가 있다.

2. 보안 프로그램과 프라이버시 문제점

Total Terrorism Information Awareness(TIA) 프로그램

TIA 프로젝트는 Defense Advanced Research Project Agency(DARPA)의 Information Awareness Office(IAO) 임무 중 하나로, 정부가 수집·축적한 시민의 개인 기록들을 분석하여 모든 사람들의 정보서명(Information Signature)을 획득하고, 이를 통해 잠재적 테러리스트와 범죄자를 추적할 수 있도록 개발된 프로그램으로 수집된 DB에는 국민의 금융기록, 의료기록, 통화 기록 그리고 여행(항공기 승객 등) 기록 등이 포함되고 있다[8]. TIA 프로젝트의 핵심 성공요인 및 프라이버시 침해에 대해 살펴보면 우선 초대형 정보 DB를 들 수 있는데 TIA 프로젝트는 분석의 정확성을 위해 방대한 양의 개인정보 수집이 불가피하고, 수집된 개인정보는 중앙 집중화된 거대한 DB에 보관하게 되어, 이러한 정보가 유출·오용될 경우 심각한 프라이버시 침해를 야기할 수 있게 된다. 그렇기 때문에 거대한 양의 정보에서 패턴이나 공통점을 찾을 수 있는 분석툴(Discovery Tool) 및 데이터마이닝의 개발이 필요하다. 여러 가지 요인에 의해 변경될 수 있는 개인의 행동을 몇 가지 변수를 이용하여 성향별로 분류하는 것은 완전할 수 없으므로, 테러리스트 및 강력 범죄를 야기할 소지가 있다고 잘못 판명된 많은 시민들이 정부로부터의 불필요한 감시·감독을 받게 될 소지가 많은 단점이 있다. 따라서 개개인의 인식과 추적을 가능하게 하는 생체 기술의 개발이 필요하다.

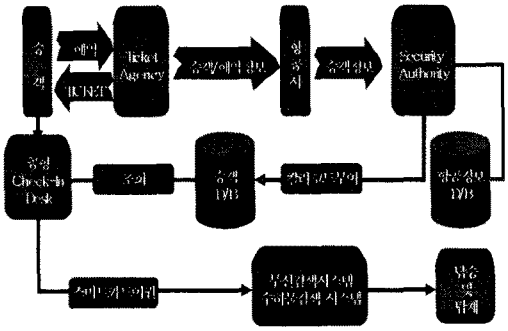
DARPA는 이미 얼굴 인식이나 걸음걸이 등과 같은 기술들을 통하여 멀리에서 사람을 인

식할 수 있도록 만들어진 'Human ID at a Distan ce' 프로그램에 예산을 조성하고 생체기술을 이용하여 개개인을 식별하고자하므로, 다양한 생체정보의 수집이 필요하고 이에 따라서도 프라이버시 침해가 야기되고 있지만 현재 ICAO와 체결중인 미국의 188개 주는 2010년 4월 1일까지 ICAO 표준 MRPs(Machine Readable Passports)를 발부받아야 된다. 현재 110개주가 그렇게 하는 반면에 40개주 이상이 2006년 말까지 e-passport나 생체인식 여권으로 교체하려는 계획을 갖고 있다[9].

TIA 프로젝트에 대한 주요 반대로 시행 보류에 대한 것을 살펴보면 우선 미 상원은 '연방 데이터베이스로부터의 시민 보호법(안)'을 제안('03. 7)하여 행정부가 TIA 프로그램의 범위와 예산에 대한 상세 보고서를 제출할 때까지 그 프로그램에 대한 예산 지급을 중단토록 하였고 정부기관의 개인정보 사용에 대한 책임을 부과하고, 단순추정(Hypothetical Scenarios)에 근거한 정보 탐색을 금하게 하였다. 그리고 상하원 양원 협의회는 TIA 프로그램과, 이의 이행을 위해 만들어졌던 정보인지사무국(Information Awareness Office: IAO)의 철수를 2004년 최종 국방비 지출안(Final defense spending bill for 2004)에 포함('03. 9)시켰었다.

CAPPS 프로그램

CAPPS I의 도입은 폭발물 감지를 위해 모든 여행객의 가방을 검사(Full screening)하기보다는, 선별적으로 검색할 수 있도록 1996년 노스웨스트 항공이 개발했고 미국은 1998년부터 시행하였다[10]. CAPPS I의 주된 골자는 승객이 항공사에 제공하는 정보(결제정보 등)에 기초하여 경험적 데이터마이닝 기법을 이용하여 여행객들에게 '위험점수'를 부여하여 모든 승객을 분류하고자 만들어진 시스템으로서, 위험 수준에 따라 초록, 노랑, 빨강으로 분류되며 빨강으로 분류된 승객의 경우에는 심각한 위험을 야기할 수 있다고 판단하여 법집행 기관의 조치가 필요(탑승거부 등)함을 의미하는 것이다[11-12]. 그리고 9/11 테러 이후 미 국회가 제안하여 추진된 CAPPS II는 국토안보부가 항공사로 하여금 CAPPS I에 승객사진이 포함된 신원확인 정보를 포함하도록 하고 동 승객정보를 TSA에 제출하도록 하고 있다[13]. TSA는 먼저 승객정보(최대 50년 보유)를 정부의 요주의 인물 명단(Terrorism watch lists)과 대조하고, 2차로 민간의 금융·의료·신용·상거래 DB 등도 점검하여, 테러리스트뿐만 아니라, 공항안전과는 무관한 경찰 수배자 및 범죄자들의 검거를 의도하고 있다.



<그림 1> 승객 사전 검색 시스템의 적용 모식도[14]

<그림 1>을 보면 승객이 처음 항공 티켓을 예약하기 위해 여행사 또는 공항의 발권소로 접촉을 하게 된다. 그러면 여행사나 각 공항의 발권소에서 항공사로 승객의 예약정보를 확인하게 되고 항공사는 신원조회 요청을 받은 고객에 대한 '칼라코드'를 부여하게 되고 그 '칼라코드'를 부여받은 승객은 공항에서 Check in을 하게 된다. 여기서 칼라코드는 각각 '레드', '옐로우', '그린' 등의 방식으로 구분되어지는데 가령, 항공기의 이용수가 빈번하고 사회적으로 안전하다고 분류된 사람들에게는 '그린코드', 그 수준이 보통인 사람들에게는 '옐로우코드', 사회적으로 위험인물에 속할 경우는 '레드코드'를 부여하게 된다. 이때 승객과 수하물은 부여받은 '칼라코드'에 따라 단계별로 무선검색시스템과 수하물검색시스템을 거치게 되는데 칼라코드별로 보안검색의 단축 또는 증가될 수 있게 된다. 그 후에 고객은 탑승수속을 완료하게 된다[14].

CAPPS II에 대한 주요 반대 이유를 살펴보면 프라이버시 옹호자들은 이 시스템이 불법적으로 사생활을 침해할 뿐 아니라, DB 착오 시 무고한 승객에게 누명을 씌울 수 있다고 주장하고 있다. 또한, 필요이상으로 많은 개인정보가 필요 이상의 기간동안(최대 50년의 보유기간) 정부에 의해 보관되는 것은 지나치며, 미래에는 CAPP S II 시스템이 정부 건물들과 공공장소 그리고 배, 기차, 버스와 같은 모든 운송수단에의 접근을 통제하기 위해 배치될 수 있을 것이라 우려를 하고 있다. 이에 대한 국토안전부의 대응으로는 다양한 이익집단 및 프라이

버시 전문가의 의견을 수렴하고, 프라이버시 책임자를 고용하여, CAPPS II 계획을 개인의 사생활을 침해하지 않으면서도 비행 중의 승객의 안전을 보장하는 방향으로 수정하였고('03. 7) 개인정보 수집의 제한을 두어 은행기록, 신용기록, 의료기록 등은 미사용하기로 하였다. 또한 수집된 개인정보의 보유 기간을 단축하여 대부분의 승객정보는 여행이 끝난 즉시 삭제되도록 하였다[15]. 다만, 몇몇 '높은 위험'을 보유한 승객들의 정보 보유 기간은 여전히 고려 중에 있다[16]. 그리고 상업적 정보제공자에 의한 CAPPS 정보의 사용 금지를 들 수 있는데 CAPPS II가 부정확한 정보를 보유하고 있다고 생각될 경우 승객들이 문의할 수 있도록 Passenger Advocate Office를 설치하였고 이들은 승객들의 잘못된 정보의 근원이 어디인지를 알아내고 이를 수정하기 위한 조치를 취하도록 하였다. 예를 들면 테러리스트와 동명이인인 경우 잘못 판명될 수 있다는 우려가 있었음에도 불구하고 그것에 대한 어떠한 대책도 없었으나, 수정안에서는 신원확인을 추가하여 이러한 문제점을 제거하였다.

그러나 CAPPS II는 여전히, 정보주체의 정보열람 및 수정과 관련한 사법적인 강제 권한, 개인 정보 유출의 기록의무, 보관 가능한 정보범위의 제한 등을 포함한 다양한 프라이버시 보호 규정으로부터 예외적용을 받고 있다[17]. 이에 대한 미 의회의 반응을 살펴보면 상하원 양원 협의회는 2004년 DHS 예산에 GAO(Government Accountability Office)가 CAPPS II 시스템의 효율성을 국회에 보증할 때까지, 교통안전국이 CAPPS II 프로그램을 시행하는 것을 금한다.' 라는 내용을 포함시켰었다('03. 9). 하지만 최근의 근황을 보면 의회의 국정조사 결과, 새로 도입된 항공기 승객검색 시스템 담당 공무원들이 연방 사생활보호법을 위반했다는 사실이 밝혀진 지 불과 몇 주 만에, 국토안보부(Depart ment of Homeland Security; DHS)가 이 프로그램에 대한 감시감독을 완화하고 승객들의 상업적 데이터베이스를 테러리스트 검색에 이용할 수 있도록 하라는 압력을 의회에 가하고 있다.

내년에 국토보안에 대한 연방자금지원안을 수정하며 논란을 빚고 있는 보안비행프로그램으로 비행기 탑승객 중 테러리스트를 가려내기 위해 현재 승객의 신원 및 개인 배경 등을 파악하는 것이 가능해 진다는 게 주요 내용이다. 의회의 국정조사 담당기구인 정부회계감사원(The Gove rnment Accountability Office)은 3월 보안비행이 요건을 갖추기 위해 필요한 열 개의 테스트 중 지금까지 9개를 통과했다고 밝혔다. 이를 통해 현재 항공사 기반의 승객검색 프로그램을 중앙 집중화하려 했던 오랜 의회의 노력은 통일되고 확대된 테러리스트 감시 대상 명단과 비교하여 승객정보를 확인하는 데에만 그치도록 제한될 것이다. 교통안전국은 내달 두 개의 항공사를 이용하여 항공보안 운영시험을 계획하고 있으며 2006년 일반승객 전체 검색으로 확대할 계획이다[18].

III. 결론

CAPPS II는 전 세계 공항의 안전을 강화시키는데 큰 기여를 할 것으로 예상된다. CAPPS II를 효과적으로 추진하기 위해 미 교통안전국은 국제간의 협력을 모색하는 한편 대내외적으로 국가차원의 대중홍보를 강화해야 할 것이다.

미 교통안전국은 CAPPS II에 대해서 국민과 입법부가 걱정하는 요지를 어떻게 감소시켜 사용가능하게 만들어질 수 있는지 설명할 필요가 있고 어떻게 그러한 결정을 하게 되었는지 어떤 정보를 분류하여 선택하게 되는지 알려줄 필요가 있다. 그리고 그들의 정책에 대해 반대 또는 지원하는 조직들 간에 규칙적인 대화를 해야 한다. 정부, 민간단체 그리고 비정부 조직, IT 전문가와 변호사들로부터 지지를 받기 위해 그들로 이루어진 위원회를 형성해야 한다. 이 위원회의 책임은 시민들에게 효과적인 지지를 얻을 수 있는 과정을 발전시키고 설계하는 것인데 이런 상호협력적인 노력은 지금의 반대 세력을 감소시킬 것이다. 시민들의 반감을 줄일 수 있는 보다 다양한 방법은 CAPPS II의 디자인 개발에서부터 대중을 활발히 끌어들이는데 있다. 그렇게 함으로써 그 시스템의 활성화에 대해서 시민들의 지지를 받을 가능성이 생기게 된다. 하지만 프라이버시와 자유에 대한 관심과 국가안전보장의 균형을 맞추는 것은 여전히 어려운 숙제이다. 테러리스트로부터의 위협을 억제하기 위해 시민들의 정보를 공급하는 것은 국가 정책에 있어서 중대한 결정이다. CAPPS II를 사용하여 일반 시민들의 어떠한 정보가 공개되어 DB가 만들어졌는지에 대해서 미 교통안전국은 밝힐 필요가 있다. 법규를 준수하는 어떠한 승객도 테러리스트 공격으로 자신이 희생자가 되는 것을 원하지 않는다. 그리고 미 교통안전국은 테러를 막기 위해서 승객들과 몇몇

의 자유를 타협하여 CAPPS II의 정책을 흔쾌히 수락하게끔 할 수 있다. 그러한 정책이 적합하게 개발된다면, CAPPS II는 생존력 있는 시스템이 될 수 있다. 미 교통안전국은 시민들의 믿음을 구축하고 의회와 일반 대중에게 지지받기 위해서는 그 시스템과 운영에 관한 사항들을 보다 투명하게 할 필요가 있다.

국민의 개인정보를 이용하여 미국 정부의 국가보안 노력의 효과성 및 효율성을 증대시키고자 했던 시도들이 여러 프라이버시 관련 단체 및 집단의 반대에 의해 보류되거나 무산되었고 한국 정부도 행정 편의성 등의 이유로 꾸준히 개인정보의 수집·축적 및 이용을 증가시키고 있으나, 최근 보호와 이용의 가치가 충돌하는 사태가 발생하고 있다.

현재 국가간 항공기 승객 정보 이전을 요청하는 국가가 점점 증가함에 따라 많은 나라들이 승객 정보사용에 대한 글로벌적 접근의 필요성을 인식하고 있으나 제3국에 대한 공정성 문제 및 다양한 환경을 고려한 기준을 만들고 난 후의 글로벌적 접근방식을 요구하고 있다. 그렇기 때문에 한국 또한 보안을 목적으로 다른 국가로부터의 항공기 승객 정보의 이전을 고려할 경우, 이러한 글로벌적 접근을 염두에 두고, 조화로운 방안을 모색할 필요가 있다.

참고문헌

[1] Aviation and Transportation Security Act, Public Law no. 107 - 71 (2001).

[2] http://edition.cnn.com/2005/LAW/07/24/gonzales.patriot/index.html

[3] 김재성, "국외 생체여권 구축현황", 2004.12, 2004년 생체인식 기술세미나 및 생체인식 포럼, pp.3-4.

[4] Statement by Adm. James M. Loy, Transportation Security Administrator Regarding the Discovery of Items Aboard Southwest Airlines Flights, TSA Public Affairs, 2003. 10.

[5] Robert O'Harrow, Jr., "TSA Modifies Screening Plan." In Christopher Smith, "[Salt Lake] Airport Watches, Waits on New Security," the estimate is higher, with 400 to 500 people red flagged annually(Salt Lake Tribune, 28 Aug. 2003, 2003 WL 3691522).

[6] http://www.sevis.net

[7] Homeland Security Act of 2002, Public Law no. 107 - 296.

[8] CAPPS II will continue to evolve, expanding the number of databases in the future (interview with Source I).

[9] http://www.icao.int/mrtd

[10] Sara Kehaulani Goo, "Airlines Hustling on Data Disclosure: Policies Being Drafted Under Pressure," Washington Post, 24 Jan. 2004.

[11] Lane County Bill of Rights Defense Committee.

[12] Ibid.

[13] Federal Register, vol. 68, no. 10, 15 Jan. 2003.

[14] 김장환, 전동구, 강자영, 송병흠, "유비쿼터스 IT 기술과 항공보안", 한국항공경영학회지, 제3권 제1호, 2005. 6. p.177.

[15] Ibid., p. 45269.

[16] Ibid. No explanation for "other data" or "superseded" has been provided, leaving significant room for discrepancy as to what type of data TSA will maintain and for how long.

[17] The Privacy Act 5 U.S.C. § 552a(e)(4)(I).

[18] http://www.wired.com/news/privacy/0,1848,68518,00.html