생체여권(전자여권)에 대한 의견

2007. 10. 22

인권단체연석회의

(거창평화인권예술제위원회/구속노동자후원회/광주인권운동센터/다산인권센터/대항지구화행동/동성애자인권연대/문화연대/민주화실천가족운동협의회/민족민주열사희생자추모(기념)단체연대회의/민주사회를위한변호사모임/민주주의법학연구회/부산인권센터/불교인권위원회/빈곤과차별에저항하는인권운동연대/사회진보연대/새사회연대/안산노동인권센터/에이즈인권모임나누리+/외국인이주노동자대책협의회/울산인권운동연대/원불교인권위원회/이주노동자인권연대/인권과평화를위한국제민주연대/인권운동사랑방/장애와인권발바닥행동/장애우권익문제연구소/전국장애인차별철폐연대/전국불안정노동철폐연대/전북평화와인권연대/전쟁없는세상/진보네트워크센터/천주교인권위원회/평화인권연대/한국교회인권센터/한국DPI(한국장애인연맹)/한국게이인권운동단체친구사이/한국성적소수자문화인권센터) + 함께하는시민행동

1. 요약

현재 논의되고 있는 생체여권(전자여권) 사업은 전면 중단되어야 한다. 외교통상부가 주장하는 도입목적을 타당하지도 않을뿐더러, 다른 역효과와 심각한 인권침해 문제만을 야기하고 있다. 본 의견은 생체여권(전자여권)을 기술/보안/인권/헌법/외교 등의 관점에서 분석한 연구의 결과이다. 구체적인 문제점들은 다음과 같다:

① 위변조 방지는 사진 전사식 여권으로도 충분하다.
② 사진전사식 여권이 위변조 가능하다면 똑같은 방법으로 생체여권(전자여권)도 위변조될 수 있다.
③ RFID를 사용하는 생체여권(전자여권)의 특성상 새로운 종류의 위변조이 가능성이 제기되고 있다.
④ 보안기술은 개인정보유출을 방지하고 있지 않고, 위변조 여권 검출에만 초점이 맞추어져 있다.
⑤ ICAO 표준에 따라 도입된 세계 각 국의 생체여권(전자여권)은 해킹되고 있다.
⑥ 보안문제로 인해 EU에서는 현 생체여권(전자여권) 표준의 폐기가 권고되고 있다.
⑦ 생체인식기술은 태생적으로 완벽해질 수 없다.
⑧ 지문정보를 보관하지 않는다는 외교통상부의 주장은 일관성이 없다.
⑨ 무인/자동심사대는 필요하지도 가능하지도 않다.
⑩ 또한 이는 테러방지라는 외교통상부의 또 다른 도입목적과 정면으로 충돌하는 것이다.
⑪ 한국엔 테러위협도 테러리스트도 존재하지 않는다. 외교통상부가 방지해야할 테러는 어디있는가?
⑫ 생체정보를 이용해 테러를 방지하는 것을 불가능하다. 미국에서도 회의론이 확산되고 있다.
⑬ 지문정보를 수록하는 생체여권(전자여권)은 세계적 추세가 아니다.
⑭ 미국비자면제는 기만이다. 사실상 비자심사가 강화된다.
⑮ 미국이 비자면제 조건으로 요구하고 있는 것들은 반인권적인 조건들이다.

여권법 개정안은 헌법상 기본권으로 보장되고 있는 개인정보 자기결정권을 제한하는 기본권 제한입법이다. 그러나 위에 나열한 것처럼 여권법 개정안은 그 목적이 타당하지 않아, 기본권 제한입법의 요건을 충족하지 못하고 있다. 생체여권(전자여권)은 개인정보를 정보주체의 인지/동의 없이 국제적으로 유통시킴으로써 개인정보 자기결정권을 침해하고 있는 것은 물론, 경우에 따라서는 양심·종교·이동의 자유를 제한할 수 있는 심각한 인권침해 제도이다. 특히 국가가 국민의 개인정보를 과도하게 수집함으로써 국가가 국민에 대해 우월적 지위를 확보하게 되고, 이는 곧 감시망으로서 기능하게 된다. 이러한 감시의 시선은 점차 국민들의 의식 속으로 내면화되어 국민 개개인의 의사결정/행동을 위축시키게 될 것이다. 이는 개인의 다양한 참여를 바탕으로 하는 민주사회의 근본을 흔드는 것이라 하겠다.

2. 들어가며

가. 프라이버시와 개인정보자기결정권

현행 헌법 제17조에서 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.'고 하여, 인간적 존재로서의 모든 국민이 소극적으로는 그 사사(私事)와 사생활(私生活)의 내용 및 명예·신용 등을 침해받지 아니하고, 적극적으로는 자신이 원하는 대로의 자유로운 활동과 생활을 영위하는 것을 침해 또는 간섭받지 않도록 규정하고 있어, 사생활

의 비밀과 자유의 불가침에 대하여 프라이버시에 관한 권리(right of privacy)라 해서 헌법상의 기본적 권리로 인정하고 있다.

전통적으로 프라이버시는 홀로 있을 권리, 간섭받지 않을 권리를 의미하여 왔으며, 정보사회에서는 자신의 정보를 통제할 수 있는 권리로까지 의미가 확장되어 왔다. 이를 정보 프라이버시 또는 개인정보 자기결정권이라고 하는데, 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.

예를 들어, 가까운 사람에게 알려준 개인 신상에 관한 정보나 연락처가 본인의 인지/동의 없이 공개되는 것, 환자의 의료기록을 병원 측에서 다른 기관으로 전송하는 것, 인터넷 사이트에서 수집된 개인정보가 거래되거나 유출되는 것, 정부 부처에 의해 수집된 개인정보가 다른 목적으로 사용되거나 다른 부처와 공유되는 것 등의 경우 피해자인 개인은 '기분 나쁨'을 느끼게 된다. 이것은 프라이버시가 침해된 것에서 생기는 감정이며, 위에서 설명한 개인정보자기결정권이 침해된 경우라고 볼 수 있다.

또한 헌법재판소는 위와 같은 개인정보유출을 방지하고 프라이버시를 수동적으로 보호하는 것뿐만 아니라, 능동적 의미로서의 개인정보자기결정권의 필요성까지 인정하고 있다. 즉, 개인정보의 수집/처리의 국가적 역량강화로 국가가 개인의 일거수일투족을 파악할 수 있게 된 현대사회에서 개인의 의사결정의 자유를 보호하기 위한 장치, 나아가 자유민주체제의 근간이 훼손될 가능성을 차단하기 위한 최소한의 헌법적 보장 장치로서 개인정보자기결정권을 승인하고 있다.[1)]

나. 생체정보의 위험성

개인정보 중에서도 생체정보는 특별히 민감하게 다루어야 한다. 헌법재판소는 NEIS 사건에 대한 판결에서 "일반적으로 볼 때 개인의 인격에 밀접히 연관된 민감한 정보일수록 규범명확성의 요청은 더 강해진다고 할 수 있다"며 개인정보 자기결정권에서 개인정보를 논할 때 민감한 정보를 더 중요하게 다루어야 한다고 판시한 바 있고, 국가인권위도 생체정보에 대해 생태성, 일신전속성, 고유성 등을 특징으로 하는 민감한 개인정보라며, 다른 개인정보보다 엄격하게 다루어야 한다고 의견을 표명한 바 있다.[2)] 꼭 이러한 근거를 들지 않더라도 생체정보는 특별히 민감하게 다루어야 한다는 것이 일반

1) "오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다. 이와 같은 사회적 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내제된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장 장치라고 할 수 있다." 2005.5.26 선고99헌마513 결정

2) "특히 지문 정보 등 생체정보는 생태성, 일신 전속성, 영속성의 특성이 있는 아주 민감한 정보이므로 그 정보의 수집 및 관리에 있어서도 다른 개인정보 보다 더 엄격한 절차와 기준에 의해 수집되는 것이 바람직하다고 본다." 2007.4.12 국가인권위 '여권법 전부 개정 법률(안)'에 대한 의견표명

적인 함의이다.

생체정보는 개인과 분리할 수 없는 정보로, 개인에 대한 절대고유의 식별자로 기능할 수 있다. 다시 말하면, 다양한 개인정보를 한데 모을 수 있는 강력한 식별기능을 할 수 있어, 이를 응용하면 개인의 위치를 정확하게 파악하고 추적할 수 있다. 뿐만 아니라 다양하게 산재되어 있는 개인정보를 상호 링크할 수 있게 됨으로써 개인이 전혀 알 수 없는 상태에서 구체적인 개인을 묘사할 수 있게 된다. 이것은 결코 거부할 수 없는 프라이버시의 침해이다. 또한 생체인식기술을 이용하게 되면 국가에 의한 개인의 이동 및 행동에 대한 감시가 증대된다. 그 결과 국가 또는 단체는 예방하고자 하는 행동을 예측할 수 있는 우월한 지위를 갖게 된다.

본 의견의 배경으로 이러한 생체정보의 위험성을 염두에 둘 필요가 있겠다.

다. 기본권 제한입법인 여권법 개정안

개인정보자기결정권의 보호대상이 되는 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.[3] 따라서 여권의 경우, 개인정보를 수집하는 것, 여권에 개인정보를 수록하는 것, 수집한 개인정보를 보관하는 것은 모두 개인정보자기결정권에 대한 제한에 해당한다. 기본권을 제한하는 것은 헌법 제37조 제2항[4]에 따라 법률로써만 가능하며(법률유보의 원칙), 입법의 목적이 정당해야 하고, 목적달성을 위한 방법이 적정하고, 피해는 최소에 그쳐야 하며, 공공의 필요가 해당 입법에 의하여 침해될 기본권보다 우월할 경우에만 정당화될 수 있다.

우선 법률유보의 원칙과 관련하여 헌법재판소는 NEIS 사건에 대한 판결[5]에서 개인정보자기결정권의 제한을 위해서는 법률에 개인정보의 수집·보관·이용 등의 주체, 목적, 대상 및 범위 등을 법률에 구체적으로 규정하는 것이 바람직함을 분명히 하였다. 예를 들어, 여권의 경우 사진의 수집이 필요하다면, 수집의 목적, 사진을 수집하는 것, 나아가 사진정보를 어떻게 보관하고, 어떤 방식으로 어디까지 유통시킬 것인가, 또 누가 이용가능한가 등이 법안에 명시되어 있어야 한다고 볼 수 있다.

그러나 9월 4일 국무회의를 통과한 여권법 개정안은 수집할 개인정보에 대해 제5조에서 "여권발급 받는 자의 신원, 여권발급기록 등 여권업무의 수행에 필요한 관련정보", 제8조에서 "지문(指紋), 그 밖에 여권의 발급에 필요한 본인의 여권정보" 라는 표현만

---

3) 2005.5.26 선고99헌마513 결정

4) 국민의 자유와 권리는 국가안정보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법류로써 제한할 수 있으며, 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다.

5) "국가권력에 의하여 개인정보자기결정권을 제한함에 있어서는 개인정보의 수집·보관·이용 등의 주체, 목적, 대상 및 범위 등을 법률에 구체적으로 규정함으로써 그 법률적 근거를 보다 명확히 하는 것이 바람직하다. 그러나, 개인정보의 종류와 성격, 정보처리의 방식과 내용 등에 따라 수권 법률의 명확성 요구의 정도는 달라진다 할 것이고, 일반적으로 볼 때 개인의 인격에 밀접히 연관된 민감한 정보일수록 규범명확성의 요청은 더 강해진다고 할 수 있다" 위 2003헌마 282 결정

을 사용하고 있어, 정보의 수집·보관·이용 등의 주체, 목적, 대상, 범위가 전혀 명시되어 있지 않고, 따라서 법률 유보의 원칙에 위반된다고 볼 수 있다.

그 전에 목적이 정당한 경우에만 입법이 될 수 있음으로 외교통상부가 제안한 여권법 개정의 입법목적에 대하여 논의해볼 필요가 있다고 하겠다. 즉 생체여권(전자여권)의 도입목적에 대하여 '정당한가?', '기능할 수 있는가?', '공익의 필요가 침해될 기본권보다 우월한가?' 등의 분석이 필요하다. 외교통상부는 생체정보를 수집하고 여권을 전자화해야 하는 이유로 ① 국제범죄 및 테러방지 ② 위변조 방지 등 보안성 강화 ③ 국민 편의 증대 ④ 미국 비자면제 프로그램(VWP) 가입 등을 들고 있다. 본 의견에서는 외교통상부가 주장하고 있는 생체여권(전자여권) 도입목적을 기술/보안/인권/헌법/외교 등 여러 각도에서 분석해보고자 한다.

3. 여권에 적용되는 기술/보안

가. 위변조 방지

2005.9.30 발급이 시작된 현재의 사진전사식 위변조방지, 여권의 국제신인도 제고, 국민 편의 증진 등의 목적으로 도입되었다.[6] 사진을 스캔하여 프린트하는 사진전사식 여권은 ICAO(국제민간항공기구)에서 표준으로 채택하고 있는 기계판독여권(Machine Readable Travel Document)을 충족하고 있으며, 초박막 필름에 한국을 상징하는 무궁화, 훈민정음, 거북선 이미지와 함께 다양한 문양을 넣고 특수렌즈로만 볼 수 있는 고스트 이미지 등의 최첨단 보안요소를 다수 적용하여 위변조가 사실상 불가능하다. 그런데 외교통상부는 2006년부터 위변조 방지, 여권의 국제신인도 제고, 국민 편의 증진 등 1년 전 사진전사식 여권의 도입목적을 다시 거론하며, 생체여권(전자여권) 도입을 추진하기 시작하였다.

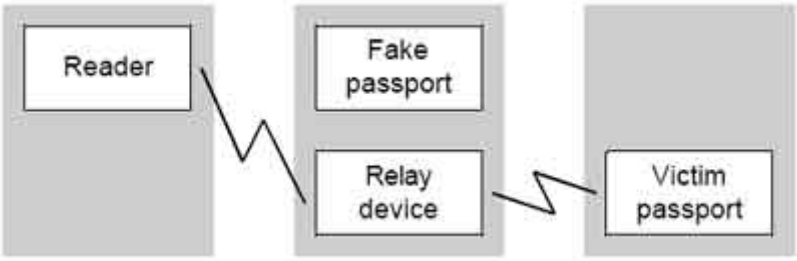
사진전사식 여권에 대한 위변조가 가능하다면, 사진전사식 여권의 어떠한 취약점 때문에 어떠한 방법으로 위변조가 가능했으며, 그것을 보완하는 방법/기술이 무엇인지를 찾는 순서로 새로운 여권의 도입이 논의되어야 한다. 그러나 위와 같은 평가와 논의가 있기는커녕, 사진전사식 여권에 대한 위변조가 실제로 있었는지조차 공개되지 않고 있다.

나아가 생체여권(전자여권)이란 사진전사식 여권에 개인정보와 생체정보가 저장된 칩(Contactless IC Chip)을 내장하는 형태로, 기존의 사진전사식 여권에 대한 위변조가 가능하다면, 내장된 칩과 무관하게 똑같은 방법으로 생체여권(전자여권)에 대한 위변조가 가능하게 된다. 왜냐하면 ①여권이란 출입국심사대 뿐만 아니라, 여행지 곳곳에서 수시로 제출해야 하는 신분증이고, ②실제로 생체여권(전자여권)을 출입국심사에 전면적으로 적용하고 있는 나라는 없으며, ③출입국심사에 사용된다 하더라도 기술의 불안

6) "여권의 위.변조 방지와 품질개선 및 여권 관리 업무의 효율화", "세계적 수준의 품질과 보안성을 갖춘 여권으로서 우리나라 여권의 국제신인도 제고와 국민들의 해외 출입국시 편의를 더욱 증진할 것으로 기대된다." 2005.9.7 외교통상부 보도자료 '사진전사식 신여권 발급 개시'

정성으로 인해 칩이 불능화된 생체여권(전자여권)도 인정해주고 있기 때문이다.

또한 비접촉식인 RFID[7] 기술을 이용하는 생체여권(전자여권)의 특성상 새로운 종류의 위변조가 가능한 것으로 보고되고 있다. 예를 들면, 출입국심사의 절차에 따라 해당 직원에게는 RFID가 불능화된 본인의 여권을 보여주고, 주머니 속에 다른 사람의 여권을 가지고 있다가, RFID 리더로 신호를 보내주는 방식의 위변조가 가능하다. 혹은 주머니 속에 다른 사람의 여권을 가지고 있을 필요 없이 중계기(Relay device)를 통해 뒷사람의 여권정보를 RFID 리더로 흘려보내 출입국심사를 통과하는 것도 가능하다.



<중계기(relay device)를 이용한 여권 위변조>

ICAO 표준 생체여권(전자여권)의 복제에 성공했던 루카스 그룬발트(Lukas Grunwald)는 생체여권(전자여권)의 조작은 위조의 위험 이외에도 여권 RFID 태그에 손상된 데이터를 넣어 검사 시스템을 망가뜨리거나 백엔드 출입국 감시 컴퓨터에 악성코드를 퍼트릴 가능성이 있다고 지적했다. 실제로 그는 생체여권(전자여권)의 결함을 이용해 칩을 복제하고 여권 사진이 들어있는 JPEG2000 이미지 파일을 수정하는 방식으로 두 업체에서 만든 판독기의 시스템을 충돌시켜 마비시키는데 성공하기도 했다.

위와 같은 사실들을 볼 때 생체여권(전자여권) 도입목적 중 하나인 위변조 방지는 가능하지도 않을뿐더러, 오히려 새로운 위변조를 가능하게 하는 효과만 있게 된다. 따라서 위변조 방지라는 목적은 달성될 수 없다 하겠다.

나. ICAO 표준 보안기술

1) PKI: Public Key Infrastructure

PKI는 공개키와 비밀키 쌍을 이용하는 암호화 시스템으로, 데이터의 무결성(integrity), 보낸 사람의 인증(authentication), 데이터의 기밀성(confidentiality) 등을 보장하는데 사용된다. 생체여권(전자여권)에는 PKI 다양한 사용방법 중 전자서명(digital signature)만이 사용되며 이는 데이터의 무결성을 보장하고 보낸 사람을 인증하는 기법으로, 데이터의 기밀성은 보장해주지 못한다. 데이터의 기밀성을 보장하기 위해서는 받는 사람의 공개키로 암호화를 해야 하는 PKI 특성상 받는 사람이 여럿인 여권유통의 구조에서는 PKI로 여권에 담기는 정보를 암호화하는

7) Radio Frequency IDentification: 라디오 주파수를 이용한 무선인식 기술, RFID 태그와 RFID 리더로 구성된다.

것은 불가능하다. 물론 PKI가 아닌 다른 암호화기법을 적용하는 것도 어렵다 하겠다.

외교통상부도 스스로 PKI를 수동적 인증(Passive Authentication), 즉 칩 데이터가 변조되지 않았음을 확인하는 기술이라고 설명하고 있다. 즉, 위변조를 방지하지만 개인정보유출이나 복제를 방지하는 것은 아니다. 따라서 9/19 통외통위 전자여권 도입에 관한 공청회에서 진술되었던 'PKI로 암호화를 한다'는 주장[8]은 거짓이라 할 수 있다.

2) BAC: Basic Access Control

외교통상부는 BAC에 대해 "칩-판독기(reader)간 보안 채널을 형성하여 칩과 판독기간 교신 과정상에서의 정보 해킹을 방지하는 기술"이라고 설명하고 있다. 즉, 위에 설명한 PKI로 칩에 저장된 데이터를 암호화할 수 없기 때문에, 여권과 리더기와의 통신자체를 암호화하려는 접근통제기법이라고 볼 수 있다. BAC의 암호화 기법에는 강력한 3DES 알고리즘[9]이 사용되는데, 문제는 그 암호의 공유방법에 있다.

암호화는 송신자와 수신자간에 미리 약속된 암호를 공유하고 있음을 전제로 한다. 암호를 안전하게 공유할 수 있는 통신채널(secure channel)이 있다면, 그 채널을 이용해 암호를 공유할 것이 아니라 전송하고자 하는 데이터를 공유하면 되지 않는가하는 질문은 암호학의 오랜 딜레마로 남아있을 정도로, 암호가 노출되지 않도록 공유하는 것이 암호학의 오랜 숙제이며 기본이라고 할 수 있다.

ICAO 표준 생체여권(전자여권)은 여권마다 고유한 암호를 부여하고, 또 그것을 공유하기 위해서 암호를 여권에 노출되어 있는 정보로 구성하는 것을 제안하고 있다. 실제로 BAC에 필요한 암호는 여권에 적혀있는 생년월일, 만료일, 여권번호 등으로 구성한 9자리 숫자로 이루어지며, 이는 모두 여권의 신상정보 페이지에 프린트되어 있는 정보이다. 출입국 심사대에서는 여권 신상정보 페이지 하단에 있는 Machine Readable Zone(MRZ)를 스캔하여 위와 같은 정보를 얻을 수가 있다.

---

8) "모든 정보가 PKI기술로 암호화되어 있다는 점이다. PKI는 임의로 암호화된 정보를 해독하려 할 경우 현존하는 수퍼컴을 이용한다 하더라도 수백 년이 걸려도 풀기 어려운 암호체계이다." 2007.9.19 전자여권 도입에 관한 공청회 中 한국정보보호산업협회 배영훈 회장 진술 '전자여권의 올바른 이해'

9) NIST에서 제안한 표준암호화기법인 Data Encryption Standard를 3번 연속해서 적용하는 암호화 알고리즘. 컴퓨터성능향상으로 인해 Key가 56bit 크기인 DES가 brute-force 공격으로부터 안전하지 않게 되자 같은 알고리즘을 다른 Key로 3번 연속 적용하여 Key Size가 168bit가 되게 하는 효과를 만들어내었다.

결론짓자면, BAC는 암호학의 가장 중요한 원칙을 어기고 있다. 즉, 공개된 정보로 암호를 만들어 공유하고 있다. 외교통상부도 BAC에 대해 '교신과정에서의 해킹을 방지하는 기술'이라고 설명하고 있는데, 이는 통신과정에서의 불법적인 정보유출(skimming)을 방지한다는 의미이다. 다시 말하면, 분실된 여권은 무방비이다.[10] 여권을 여는데 필요한 비밀번호는 여권에 적혀있고, 누구든지 접근이 가능하다. 나아가 영국에서는 여권을 열어보지도 않고 BAC를 뚫는데 성공했다. BAC 암호를 구성하기 위해 여권에서 얻어야 하는 개인정보들은 여권이 아닌 다른 곳에서도 쉽게 구할 수 있었다.

3) AA: Active Authentication

"능동적 인증, 여권에 내장된 Chip이 복제되지 않았음을 증명하는 기술"이라고 외교통상부는 설명하고 있다. 여권의 특정부분은 물리적으로 읽기가 불가능하도록 하는 방법을 이용한다. 마찬가지로 이것은 출입국심사대에서 여권의 복제여부를 판단할 수 있는 근거가 될 뿐이지, 여권의 유통과정에서 여권에 담긴 개인정보유출을 방지하는 것과는 상관이 없는 기술이다.

4) EAC: Extended Access Control

"생체정보를 별도로 보호할 목적으로 적용되는 보안 기술"이라고 외교통상부는 설명하고 있다. EAC는 그 존재 자체로 생체여권(전자여권)의 보안이 취약함을 증명하고 있는데, 생체정보에 대해서 별도의 보안이 필요했던 것 자체가 나머지 보안기법들이 안전하지 않음을 증명하고 있는 셈이다. 또한 유럽 등에서 도입된 생체여권(전자여권)이 끊임없이 복제/개인정보유출 공격을 당하자 ICAO에서 BAC가

10) 2006년 한 해 한국여권은 66,798개가 분실되었고, 2007년엔 8월까지 51,511개가 분실되었다.

취약점을 인정하고 새롭게 도입한 기술이다. 즉, ICAO 표준은 아직도 밝혀지지 않은 문제점을 가지고 있을 가능성이 높다 하겠다.

5) RFID: Radio Frequency IDentification

RFID는 라디오주파수를 이용한 무선인식기술로 교통카드에 널리 사용되는 기술이다. 여권에 사용되는 RFID는 근거리에서만 인식 가능하도록 설계되었지만, 리더에 달린 안테나의 성능에 따라 원거리인식이 가능하다. 생체여권(전자여권)에 RFID에 사용됨에 따라, 생체여권(전자여권)에 저장된 정보를 멀리서 몰래 빼내가는 것은 물론, RFID를 몰래 추적·관리하는 것도 가능해졌다. 또한 정보를 빼내는 데 실패하더라도, RFID를 통해 여권소지자의 국적을 파악하는 것이 가능해졌으며, 이에 따라 불특정다수의 대중으로부터 특정 국가의 여행자를 색출해내는 것이나, 특정 국적의 생체여권(전자여권)이 다가오면 자동으로 폭발되는 폭발물 같은 테러도 가능해졌다. 이에 따라 미국/독일 등에서는 'RFID = 기폭장치'라는 인식이 확산되고 있으며, 생체여권(전자여권)을 발급받은 사람들은 RFID 불능화를 위해, 여권을 전자레인지에 돌리거나, 해머로 두드리고 있는 실정이다.

ICAO는 위와 같은 위협이 실험/보고된 이 후에야 생체여권(전자여권)에 차폐막을 만들 것을 권고한 바 있다. 하지만 차폐막 역시 여권이 온전히 닫혀 있을 때만 기능하는 것으로 여권의 RFID를 보호하는 데 적절하다고 볼 수 없다. 또한 RFID를 사용한 이 후에 그것을 차폐막으로 보호한다면, 애초부터 비접촉식 RFID가 아닌 접촉식 인식 방법을 사용하는 것과 차이가 없어, RFID를 사용할 이유가 없다는 주장만 뒷받침하는 꼴이 되고 말았다. 또한 생체여권(전자여권)에 왜 RFID를 사용해야 하는지, 그 명확한 이유는 한 번도 설명된 적이 없다.

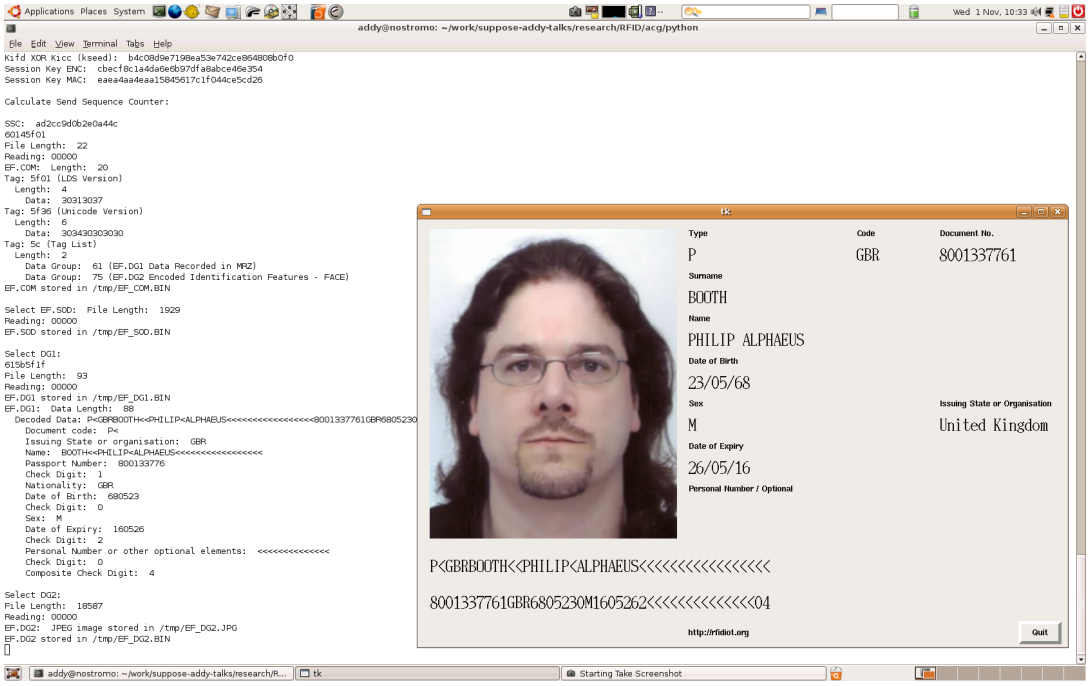
6) ICAO 표준 생체여권(전자여권) 해킹사례

2006년 8월 라스베가스 BlackHat 컨퍼런스에서 루카스 그룬발트(Lukas Grunwald)는 2주간의 연구 끝에 ICAO 표준 생체여권(전자여권)으로부터 정보를 내려 받아, 새로 구입한 RFID Chip으로 복제하는 데 성공했다.[11] 영국의 가디언에서도 2006년 11월 아담 로리(Adam Laurie)와 함께 생체여권에서 개인정보를 빼내는 데 성공했으며, 2007년에는 데일리메일에서, 여권을 열어보지 않은 상태로, 여권에서 정보를 빼내는 데 성공했다. 이 외에도, 영국, 독일, 네덜란드, 벨기에 등 ICAO 표준 생체여권(전자여권)이 도입된 국가들에서 복제/개인정보 유출 사례가 보고되고 있다. 그 중 영국의 아담 로리(Adam Laurie)가 유출하여 인터넷에 게시[12]되어 있는 여권정보와 사진은 다음과 같다.

---

11) http://biopass.jinbo.net/tech03.php 에서 실제 동영상을 확인할 수 있다. BBC에서 제작한 동영상으로 Lukas Grunwald가 생체여권(전자여권) 복제를 시연하고 있다.

12) http://www.rfidiot.org/phil.png 여기서의 개인정보와 사진은 영국의 전자주민증/생체여권 반대운동 단체인 NO2ID의 Phil Booth의 신상에 관한 것이며, 본인의 허락 하에 인터넷에 게시되어 있다.



<아담 로리(Adam Laurie)가 여권으로부터 유출해낸 개인정보와 사진>

현재, 영국에서는 생체여권(전자여권) 리콜운동이 진행 중이다.

7) 부다페스트 선언

2006년 9월, 유럽연합(EU)의 공식후원을 받는 보안전문가 네트워크 FIDIS는 부다페스트에서 ICAO 표준 생체여권(전자여권)에 대한 연구결과를 발표했다. 이들은 ICAO 표준 생체여권(전자여권)이 그 목적과는 다르게, 보안을 심각하고 후퇴시키고, 명의도용/신원위조의 가능성만 급격히 증가시키고 있다고 지적했다. 따라서 현재 유럽연합(EU)의 각 국에서 도입한 생체여권(전자여권)은 3년 안에 폐기하고, RFID와 생체정보를 사용하지 않는 방향으로 새로운 여권 표준을 제정할 것을 권고하고 있다.

8) 결론

미 국무부 여권 서비스 담당 부차관보인 프랭크 모스(Frank Moss)는 계속되는 생체여권(전자여권) 해킹에 대해 “전자여권을 고안한 사람들도 오래 전부터 칩 복제가 가능하다는 사실을 익히 알고 있었으며, (데이터 페이지에 여권 소지자의 디지털 사진을 넣는 등의) 다른 보안 장치들을 통해서 위조되거나 개조된 여권으로 미국을 포함한 다른 나라로 입국하는 것을 막을 수 있다.”고 말하고 있다. 즉, 위변조 여권을 출입국심사대에서 걸러내는 것이 중요하지, 중간에 개인정보유출은 어쩔 수 없다는 입장인 것이다.

전체적으로 보았을 때 ICAO 표준 보안기술은 출입국심사대에서 여권의 진위여부

만을 파악하는 데에만 초점이 맞추어져 있고, 여권 유통과정에서 개인정보의 유출을 방지하는 기술은 매우 미약하다. 세계 각 국에서의 복제/개인정보유출 사례를 보아도 ICAO 표준 생체여권(전자여권)은 FIDIS에서 권고하였듯이 폐기되어야 할 표준이며, 그 보안에 심각한 문제점이 있다고 할 수 있다. 따라서 보안성 강화라는 도입목적 역시 달성될 수 없다고 하겠다.

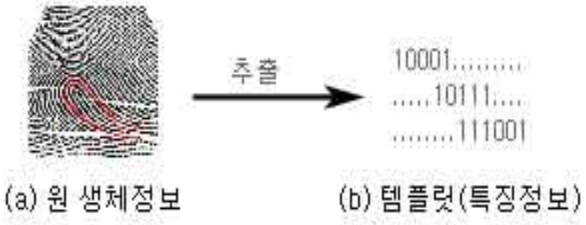
4. 생체인식 시스템과 생체정보(Biometrics)

가. 배경지식

생체인식기술이란 사람의 생체적 특징(지문, 홍채 등) 내지 행동적 특징(음성, 필체 등)을 이용하여 그 사람의 신원을 자동화된 장치를 통해 인증/식별하는 기술을 말한다. 모든 생체인식 시스템은 다음과 같은 4가지 기본원리로 구성된다.

① 원 생체정보의 조사: 지문인식 센서 등 사용
② 특징정보(템플릿) 계산: 원 생체정보로부터 특정점들을 추출하여 수치화한 정보 산출
③ 기준정보 등록: 시스템에 최초 템플릿 정보 저장(reference data)
④ 대조(인증/식별): 이용자로부터 다시 추출해낸 생체정보를 기준정보와 비교/ 일치 여부 판정

②에서 템플릿이라 함은 센서로부터 입력받은 원 생체정보(raw material)에서 몇 가지 특징점들을 가지고 계산해낸 대한 수학적 모델이다. 예를 들면, 채취된 지문에서 이른바 융선의 시점, 단점, 중심점 등의 특징점들을 추출하여 그 조합을 수치로 나타내는 것이다. 정보통신부와 한국정보보호진흥원(KISA)에서 마련한 생체정보 보호 가이드라인은 생체정보에 대한 용어정의에서 생체정보에 대해 "가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다."고 설명하고 있어, 원 생체정보와 특징정보인 템플릿 정보 모두 생체정보의 범주에 포함된다고 할 수 있다.



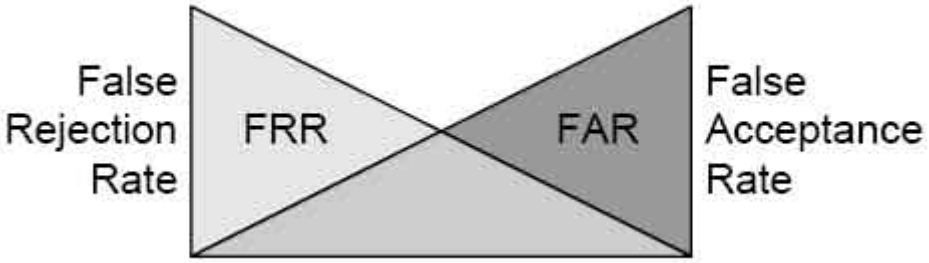
④에서 생체인식 시스템에서 본인을 확인하는 방법에는 두 가지가 있는데 첫째는 (a)인증(verification)으로, 갓 추출해낸 생체정보와 신분증(여권)에 저장되어 있는 정보를 1:1로 비교하여 일치여부를 검사하는 방법이다. 두 번째는 (b)식별(identification)로, 갓 추출해낸 생체정보가 최초 신분증(여권) 발급 시 시스템에 제출되어 데이터베이스(DB)에 저장되어 있는 기준정보들 사이에 존재하는지 1:多로 검색해보는 방법이다. 이에 대해서는 생체여권(전자여권) 표준인 ICAO Doc 9303과 위에 설명한 생체정보 보호 가이드라인에서 자세하게 설명을 하고 있다.

④에서 일치여부를 판정하는 것은 기준정보로 저장되어 있는 템플릿과 새롭게 센서로 인식하여 계산해낸 템플릿을 비교하고 양자가 일치하는 비율을 계산하여 이루어진다. 비교결과 두 템플릿이 일정 기준 값(threshold) 이상으로 일치하는 것으로 드러날 경우, 두 템플릿이 '일치한다'고 판정하게 된다.

나. 두 가지 오류율

생체인식 시스템은 확률에 기반한 시스템이다. 왜냐하면 일치여부의 판단은 몇%정도 일치하는가에 근거하기 때문이다. 예를 들어, 비교대상인 두 템플릿이 99% 이상 일치할 경우 일치하는 것으로 판정하는 시스템을 생각해볼 수 있다. 여기서 99%가 위에서 설명한 기준값(threshold)이 된다. 다시 말하면 기준값의 설정에 따라 일치여부의 가/부가 바뀔 수도 있는 시스템이다.

따라서 생체인식 시스템에는 항상 두 종류의 오류율이 상존하게 된다. 첫째는, 본인의 생체정보가 입력되었음에도 불구하고 타인으로 판정하는 비율, 즉 본인거부율(FRR: false rejection rate)이고, 둘째는, 타인의 생체정보가 입력되었음에도 등록된 사람으로 인식하는 본인오인율(FAR: false acceptance rate)이다. 두 가지 오류율은 당연히 기준값의 설정에 따라 반비례하는 관계(trade-off)이고, 이는 확률에 기반하고 있는 생체인식시스템의 태생적 한계로 지적되고 있다.



<FAR과 FRR의 반비례 관계>

우선 외교통상부에서는 생체여권에 사용되는 지문인식기술의 인증실패율이 0.004%라고만 밝히고 있어, 당연히 본인거부율과 본인오류율을 동시에 표기해야 하는 생체인식 시스템의 기본원칙을 어기고 있다. 또한 0.004%의 인증실패율은 시스템에 지문을 등록한 직 후 같은 센서로 다시 지문을 채취하여 나온 이상적인 수치로, 다른 조건, 다른 위치에서 다른 센서로 지문을 수집하여 템플릿 계산을 할 경우 인증실패율은 훨씬 더 높아질 것임이 자명하다. 외교통상부가 본인오인율은 표기하지 않고 있어, 생체여권(전자여권)의 인식에서 어느 정도의 에러가 발생할지 정확하게 가늠할 수 없지만, 이상적인 수치인 0.004%, 그것도 반쪽에 불과한 이 오류율만 적용하여도 1,300만 명의 여권 소지자가 10회 인증을 할 경우 5,200번의 에러가 발생하는 것으로 계산할 수 있다.

좀 더 명확한 이해를 돕기 위해, 런던공항의 시뮬레이션 결과를 살펴보자.[13] 런던공항에서 접근통제를 위해 지문인식기를 사용할 경우 1,600명의 직원들이 하루 90,000번의 지문스캔을 한다고 한다. 이 때 업체에서 제공한 지문인식기의 오류율은 -역시 이상적인- 본인거부율은 0.001%이며 본인오인율은 1.5%이다. 시뮬레이션 결과는 하루 1,500번의 잘못된 알람이 울리게 되는 것으로 계산되었다.

다. 얼굴인식과 지문인식

얼굴인식에 대해서는 외교통상부도 4.35%의 인증 실패율을 들어 신뢰할 수 없다는 입장을 표명하고 있다. 얼굴생체정보를 이용한 생체여권을 도입할 필요가 없다는 주장을 스스로 하고 있는 셈이다.

또한 얼굴인식과 지문인식을 동시에 사용할 경우 인증실패율이 낮아질 것이라는 일반적인 인식과는 달리 두 개 이상의 생체정보 인식을 사용할 경우 인증실패율이 높아지는 것으로 결론지을 수 있다. 왜냐하면, 한 가지의 생체정보를 사용할 경우 두 개의 오류율이 존재하지만 두 개의 생체정보를 이용할 경우, 각각의 생체정보에 대해 두 가지의 오류율이 존재하고, 이 오류율들은 각각에 대해 독립적이기 때문에 전체적으로 네 가지의 오류율이 존재한다고 볼 수 있다. 따라서 두 개의 생체정보 인증이 모두 일치를 판정할 경우, 그 신뢰성은 높아지겠지만, 일치인데도 불구하고 일치임을 판정하지

13) “Biometrics is not a Panacea" 피터 구트만(Peter Gutmann), 오클랜드 대학

못할 확률도 높아진다 하겠다.

라. 지문정보의 보관

외교통상부는 제출한 여권법 개정안에서 “여권 신청인이 제공한 지문은 여권발급에 필요한 최소한의 기간으로서 대통령령으로 정하는 기간 동안만 보관·관리하여야 한다.”라고 명시하고 있고, 국회에 제출한 자료에는 보관기간이 6개월 이내가 될 것이라고 답변한 바 있다.

하지만 9/19 전자여권 도입에 관한 공청회 진술내용에 따르면 지문정보를 보관하지 않겠다는 것은 원 생체정보로서의 지문을 보관하지 않겠다는 것이고, 원 생체정보로부터 추출해낸 템플릿은 보관하는 것으로 밝히고 있다.[14] 위의 ‘배경지식’에서 설명하였듯이 정보통신부의 용어정의에서도 원 생체정보와 템플릿을 모두 생체정보의 범주에 포함하고 있는데, 원 생체정보만을 삭제해 놓고 ‘생체정보를 보관하지 않는다’라고 주장하는 것은 사실상 거짓말이라 하겠다.

또한 생체인식 시스템에서 템플릿 추출 알고리즘은 국가/업체/기계마다 상이하고, 따라서 한국에서 추출/저장한 생체정보의 템플릿으로는 외국에서 비교/확인이 불가능하다. 이에 따라 ICAO 표준 생체여권(전자여권)은 지문 등 생체정보를 수록할 시 템플릿이 아니라 원 생체정보를 그대로 저장하여 국제적으로 호환 가능하도록 하고 있다. 이는 외교통상부가 생체정보 유출의 가능성을 원천적으로 방지하기 위해, 원 생체정보를 데이터베이스(DB)에 보관하지 않겠다고 하는 것에 비추어 볼 때 일관성도 없을뿐더러, 데이터베이스(DB)에 보관하지 않는 것의 의미도 삭감시켜 버린다고 할 수 있다.

마. 식별(identification)

외교통상부는 생체여권(전자여권)의 도입배경으로 공공연히 ‘본인인증(identification)의 신뢰도를 높여 출입국 심사의 정확성과 신속성도 확보할 수 있어’라는 표현을 사용하고 있다. 여기서 ‘identification’이란 식별, 색출의 의미로서 위에서 설명하였듯이 수집한 생체정보가 최초 여권 발급 시 데이터베이스(DB)에 저장된 기준정보들 중에 존재하는가를 찾아보는 1:多 검색이라고 할 수 있다. (가. 배경지식의 그림참조)

식별(identification)의 신뢰도를 높이려면, 당연히 지문 등 생체정보의 데이터베이스(DB)가 필요하고, 나아가 데이터베이스를 외국의 출입국심사대와 공유하는 것이 필요하다. 물론, 국가마다 템플릿 추출 알고리즘은 상이하므로, 데이터베이스에 저장되는 생체정보는 원 생체정보를 포함하고 있어야 한다고 할 수 있다. 따라서 원 생체정보를 보관하지 않는다는 외교통상부의 주장은 앞뒤가 맞지 않는다.

---

14) “따라서 원본 데이터를 굳이 따로 보관할 필요가 없으며, 초기에 전자여권 발급 시에 본인확인을 위한 최소한의 기간만 원본데이터를 보관하게 될 것이다.” 2007.9.19 전자여권 도입에 관한 공청회 中 한국정보보호산업협회 배영훈 회장 진술 ‘전자여권의 올바른 이해’

개인에게 수집한 정보를 법적인 근거도 없이 국경을 넘어 타국으로 전송하는 것은 처음에 설명한 개인정보 자기결정권을 심각하게 침해하는 것이라고 할 수 있다. OECD의 개인정보의 국제적 유통 및 프라이버시 보호에 관한 가이드라인[15], 정보통신부의 생체정보 보호 가이드라인 등을 위반하는 것이다.

바. 개인정보보호기구

ICAO는 Doc 9303에서 생체여권(전자여권) 도입의 제약조건(constraints)으로 여권에 생체정보를 저장하는 것이 각 국의 개인정보보호법, 프라이버시보호법을 준수할 것을 규정하고 있다.[16] 이와 관련하여 일본과 유럽연합(EU)의 모든 국가들은 각 국에 개인정보보호법과 개인정보보호기구를 가지고 있다. 한국정부만이 개인정보보호법이나 개인정보보호기구를 두고 있지 않다.

외교통상부 홈페이지 전자여권 소개페이지에서는 전자여권의 개인정보보호 정책으로 위에서 서술한 ICAO의 네 가지 보안기술(PA, AA, BAC, EAC)을 나열해 놓고 있어, 외교통상부가 과연 개인정보보호의 의미가 무엇인지 알고 있는지 의심스러울 정도이다. 이는 생체여권(전자여권)의 논의과정에 프라이버시 전문가나 개인정보보호 전문가가 참여하지 않은 것에 대한 당연한 귀결이다.

또한 생체여권(전자여권)의 이용에서 각 국에서 수집해가는 생체정보는 어떤 식으로, 얼마동안 보관되는지 전혀 통제의 약속이 존재하지 않는다. 예를 들어, 미국의 출입국 심사대에서 채취해가는 지문은 100년 간 보관된다. 2007.11부터 지문을 채취할 예정인 일본은 70-80년 정도 보관할 것으로 계획하고 있다. 이 정보들에 대한 정보주체, 혹은 한국정부의 통제권(열람/수정/삭제 등)은 전혀 존재하지 않는다. 이런 식으로 생체정보가 과다하게 제출된다면 현재 한국의 인터넷 환경에서 주민번호가 과다하게 수집되어 나타나는 부작용과 다를 바 없는 현상이 국제적으로 생체정보에 관해 일어나게 될 것임은 자명하다.

사. US-VISIT

US-VISIT는 생체인식 시스템에 기반한 미국 출입국 시스템의 총합이다. 미국은 US-VISIT에 따라 2004년부터 미국을 출입하는 외국인으로부터 지문을 채취하고 있다.

하지만 미국 내에서도 US-VISIT에 대한 효용성의 문제가 끊임없이 제기되고 있다. US-VISIT에 대한 연구보고서를 작성했던 GAO[17]의 랜디 하이트(Randy Hite)는 와이어드뉴스와의 인터뷰에서 US-VISIT를 목표 없이 날아가는 비행기에 비유하며, 이유도

15) OECD 프라이버시 가이드라인 요약: ① 수집 제한의 원칙 ② 정확성의 원칙 ③ 목적 명확화의 원칙 ④ 사용 제한의 원칙 ⑤ 안전 확보의 원칙 ⑥ 공개의 원칙 ⑦ 개인 참가의 원칙 ⑧ 책임의 원칙

16) ICAO Doc 9303, "9.2 The biometrics information stored on travel documents shall comply with any national data protection laws or privacy laws of the issuing State."

17) Government Accountability Office: 미 국회 내 초당적 전문연구그룹

없이 예산만 잡아먹고 있다고 혹평했다. 실제로 2006년까지 150억 달러가 넘는 예산이 투입되었지만, US-VISIT가 잡아들인 범죄자는 미 국토안보부(DHS)의 보고에 의하면 372명에 불과하다. 이들은 모두 가벼운 범죄자로, 미국이 목적하는 심각한 테러리스트는 한 명도 잡히지 않았다.

US-VISIT에 대한 많은 회의적 기사 중 하나인 워싱턴 포스트의 기사는 다음과 같다.

> "계약자와 정부는 궁극적인 가상 국경 시스템이 어떻게 작동할 것인지, 언제 쯤 완성될 것인지에 대해 명확한 상(idea)도 없이 함께 일하고 있습니다. 이런 계약은 '무한 배달-무한 수량 계약'이라고 합니다. 정부는 이 프로젝트를 언제든지 취소시킬 수 있습니다. 전체 시스템이 작동하지 않더라도, 계약자는 그 때까지의 작업에 대해 돈을 받습니다. 이 모든 이유에서, 최종 금액이 얼마나 될지는 아무도 모릅니다."[18)]

누군가를 테러리스트라고 규정하는 것은 가능하지 않다. 이라크나 아프가니스탄에서 미국의 전쟁에 분노를 느끼며 자라나고 있는 청소년들이 테러리스트와 동의어는 아닌 것이다. 미래에 테러행위를 하고 싶은 자들이 스스로 테러리스트라고 선언을 하고 테러리스트 신분증을 발급받아 테러활동을 시작하는 것이 아닌 이상 생체인식을 이용해 테러를 방지한다는 발상은 애초부터 불가능하다. 이러한 발상이 가능하려면 테러활동을 하려는 사람들이 미 국토안보부(DHS)에 지문을 등록하고 다음과 같은 신분증을 발급받아 가지고 다녀야 한다.

18) "In this case, the contractor and the government are working together without a clear idea of how the final virtual-border system will work or when it will be completed over the next decade. Such an arrangement is known as an "indefinite delivery-indefinite quantity contract." The government can cancel the project at any point. The contractor is paid for specific tasks along the way, even if the overall system ultimately does not work. For all those reasons, no one is certain of the final cost." WashingtonPost 2005.5.23 U.S. Border Security at a Crossroads

<지문으로 테러리스트를 잡으려면>

나아가 미 스탠포드 대학의 로렌스 베인(Lawrence Wein)의 연구에 따르면, US-VISIT에 등록된 테러리스트가 미국 출입국심사대에서 색출될 확률은 53%에 불과했다. 물론, 등록되지 않은 경우는 0%이다.

생체인식 시스템을 이용해 테러리스트나 심각한 범죄자가 잡힌 적은 단 한 번도 없다. 왜냐하면, 테러란 과거가 아니라 미래에 존재하기 때문이다. 따라서 생체여권(전자여권)의 도입으로 테러를 방지한다는 외교통상부의 주장은 정당하지 않다.

5. 자동 출입국 시스템과 지문

가. 지문수집의 필요성

외교통상부는 본인인증의 신뢰도를 높이고 나아가 향 후 도입될 것으로 예상되는 무인/자동화 출입국 심사대를 위해 지문정보의 수집이 필요하다고 주장하고 있다. 또 유럽연합(EU)의 각국에서도 09.6까지 여권에 지문정보를 수록할 예정인 바, 지문수집이 세계적인 추세라고 주장하고 있다. 본 의견에서는 미국의 출입국심사절차를 살펴보는 것을 통해 외교통상부의 주장을 반박하고자 한다. 미국의 출입국심사에 관해서는 미 의회의 전문연구그룹인 GAO(Government Accountability Office)가 2007.7 미 의회에 제출한 US-VISIT에 관한 보고서[19]를 참고하였다.

나. 미국의 출입국심사

19) http://www.gao.gov/new.items/d07870.pdf Homeland Security Needs to Immediately Address Significant Weakness in Systems Supporting the US-VISIT Program

GAO의 보고서에 따르면 미국의 출입국심사절차는 다음과 같다.

> “여행자가 출입국심사부스에 도착하면, 담당관이 문서리더를 이용하여 여행자의 기계판독여권(MRTD)을 읽거나, 여행자가 기계판독여권을 가지고 있지 않은 경우 여권에 기재된 정보를 시스템에 수동으로 입력한다. 시스템에서는 입력된 신상정보를 통해 여행자가 ①미국에 위협을 가할 가능성이 있는 사람인지 ② 미국에 입국할 수 있는 기간을 위반한 사람은 아닌지 ③ 미국이나 해외에서 범죄용의자로 수배 중인 사람이 아닌지 등을 판단해낸다.
>
> 첫 번째 심사부스에서 담당관에 의한 신상정보 검사가 끝나면 두 번째 생체정보 시스템에 의한 검사가 시작된다. 두 번째 부스에서의 담당관은 여행자의 지문을 채취하고 사진을 찍는다. 시스템이 지문을 채취/검사하는 동안, 담당관은 여행자에게 그/녀의 여행목적과 체류기간 등을 질의한다. 담당관이 여행자를 통과시켜줘도 된다고 판단하면, 시스템에 체류기간 등 필요한 정보를 입력한다.
>
> 두 번째 생체정보 시스템에서의 검사가 끝나면, 첫 번째 심사부스의 담당관은 출입국심사의 빨간불이나 녹색 불을 표시 받게 된다. 예를 들어, 시스템이 여행자의 신상정보와 여권의 신상정보가 일치하지 않는다고 판단하면, 담당관은 빨간불을 보게 되고 여행자의 출입국심사는 다음 조사단계로 넘어가게 된다. 다음 조사단계에서 여행자가 미국에 입국할 수 없는 것으로 결론 내려지면, 여행자는 추방당하거나 다른 조치가 취해진다. 이러한 정보는 두 번째 조사구역의 담당관에 의해 시스템에 입력되고 적절한 조치가 취해진다. 녹색불은 여행자의 생체정보가 US-VISIT의 watch list에 포함되어 있지 않고, 예전에 미국을 여행자인 경우, 예전 여행 시 수집된 생체정보와도 일치하고 있다는 것을 의미한다.”

현재 이러한 출입국심사를 운용하고 있는 미국이 무인/자동화 출입국 심사대를 설치한다는 것은 쉽게 상상하기 어렵다. 미 국무부 여권 서비스 담당 부차관보인 프랭크 모스(Frank Moss)는 이미 미국은 자동화된 검사 시스템을 사용할 계획이 없다고 말한 바 있다. 이는 비단 미국뿐만 아니라 테러방지를 큰 의미를 부여하고 있는 몇몇 국가에서도 마찬가지이다. 오히려 미국의 출입국심사를 모델로 하여 출입국심사를 강화하는 방향으로 각 국의 출입국 심사대가 진화할 것이다. 미국은 올해 말부터 개별 여행자의 열손가락 지문을 채취하는 것으로 출입국 심사를 강화할 예정이다.

과연 한 국가의 출입국심사를 무인/자동화할 필요가 있는 것인가 하는 근본적인 의문도 존재하지만, 외교통상부 스스로 밝히고 있는 테러방지라는 생체여권(전자여권)의 또 다른 도입목적과 무인/자동화 출입국심사대는 정면으로 충돌하고 있는 것으로 생각된다.

다. 결론

본인인증(verification)은 한국이 아니라 한국인이 해외여행 시 외국당국에 의해 진행되는 과정이다. 외교통상부의 본인인증의 신뢰성을 높이기 위해 지문의 수집을 주장하지만, 애석하게도 현재 세계에서 지문을 통한 본인인증을 진행하고 있는 나라는 없다. 어디에서도 지문을 통해 인증을 해주지 않는데, 지문을 통한 본인인증의 신뢰도를 높인다는 주장은 정당하지 않다. 미국에서의 지문채취조차 본인인증(verification)이 아니라, 테러리스트 데이터베이스에서의 색출/식별(identification)을 위해 사용된다. (인증과 식별의 차이는 본 의견 '4.가'의 첨부그림 참조)

미국과 일본을 비롯한 대다수의 국가들은 여권에 지문을 수록할 계획을 가지고 있지 않으며, 따라서 여권에 지문을 담는 것이 세계적인 추세라는 외교통상부의 주장은 타당하지 않다. 또 무인/자동화 심사대는 전술한대로 외교통상부의 테러방지라는 목적에도 부합하지 않으며, 미국을 비롯한 선진국들은 그와는 반대로 출입국심사를 강화하는 방향으로 정책을 정하고 있다.

또한 국가인권위도 여권법 개정안에 대한 의견에서 밝혔듯이 기존 정보만으로도 여권의 기능은 충분히 수행할 수 있다고 생각된다.[20] 따라서 여권에 지문을 수록할 이유는 전혀 없다고 하겠다.

6. 미국 비자면제 프로그램(VWP)

가. 미국 비자면제 프로그램(VWP) 가입의 전제조건

외교통상부는 2007.4.11 '전자여권 도입사업 시행 계획' 중 전자여권의 조기발급 필요성에 대해 "한·미 FTA 협상 타결로 인해 양국 간 물적 교류를 뒷받침 할 인적 교류 활성화를 위해 미국 VWP 가입의 중요성이 중대한 바, 전자여권 조기 도입긴요"라고 설명하고 있다. 일반적으로는 생체여권(전자여권) 도입만 해결되면 미국 비자면제 프로그램(VWP)에 가입할 수 있는 것으로 인식되고 있다.

하지만 미국 비자면제 프로그램 가입의 전제조건은 다음과 같다.

20) "이와 같이 개별 국가의 전자여권 도입 현황과 여권의 본래 사용 목적, 개인정보에 대한 국제적 기준 등을 고려할 때, 여권에 기재되는 정보가 여권소지자를 구분할 수 있을 정도의 개인 정보를 수록하면 충분할 것으로 판단되며," - 2007.4.12 국가인권위 '여권법 전부 개정 법률(안)'에 대한 의견표명

구분	요건	변동내역
필수적 요건	비자거부율	수정(완화)
	전자 여권	불변
	사법 협력	불변
	도난·분실 여권 통보 협정 체결	수정(강화)
	ETA 시스템 도입 협조	신규
	불체자·범법자 추방 협조	신규
	여행자 정보 공유 협정 체결	신규
재량적 요건	공항보안기준 충족	신규
	항공 보안관 제도 실시	신규
	여권 및 여행자 문서 기준 충족	신규
	대테러전 협력	신규

또한 위와 같은 한국의 준비뿐만 아니라, 미국에서도 US-VISIT 프로그램계획에 따라 전자여행허가제(ETA)가 도입되고, 미국 내 출국통제 프로그램(Exit-Control)이 97%이상 완성해야 하는 등의 준비가 필요하다.

나. 전자여행허가제(ETA)

자국으로의 여행을 허락해주는 것을 비자(VISA)라고 하는데, 미국이 입국자격여부를 심사해서 통보해주는 전자여행허가제(ETA)란 사실상 비자제도이다.

외교통상부는 전자여행허가제(ETA)의 문제점을 꼬집은 아시아경제신문의 10/8 “전자여권, 개인정보 줄줄 샌다” 제하의 기사에 대해 해명 보도자료를 배포한 바 있다. 해명 보도자료에서 외교통상부는 “현재에도 미국비자를 받을 때 전과기록이 있는지 체크하도록 되어있고 전자여행허가제(ETA)를 통해서는 기존 ‘비자인터뷰 신청서’ 나 ‘입국신고서’ 작성 시 제공되는 수준의 정보를 제공할 것이기 때문에, ETA로 인해 기존방식보다 더 많은 개인정보가 유출될 가능성은 없다고 하겠습니다.”라고 설명을 하고 있는데, 이는 전자여행허가제(ETA)가 이름만 다른 비자제도임을 스스로 인정하고 있는 셈이다. 또한 전자여행허가제(ETA)도 신청 시 비용(fee)을 납부해야 하는 것으로 미국 법안에 명시되어 있다.

또 전자여행허가제(ETA)를 위해 민감한 개인정보인 생체정보와 사법기록이 민간인 여행사 등에 노출될 가능성도 제기되고 있다. 미 9/11 위원회 법에 따르면 전자여행허가제(ETA)에 제출하는 기본정보를 “개인신상(biographical)정보와 법적인 집행과 관련해 존재하는 정보나 위험성 여부를 판단할 수 있는 정보로, 국토보안청장이 미국 여행을 허가하는데 필요한 정보라고 결정하는 정보”라고 정의해놓고 있다. 또한 CBS의 김진우 워싱턴 특파원은 7월 27일 타전한 기사를 통해 전자여행허가제(ETA)를 위해서 한

국인들의 미국 입국에 필요한 인적사항과 전과기록 등을 여행사에 제공해야하는 과정이 필요하다고 전한 바 있다.

따라서 비자면제가 되기 전에는 미 대사관에 직접 제출하던 생체정보(지문)과 개인의 사법기록을 이제 여행사를 통해 미국으로 전송하게 될 수도 있는 것이다. 이 역시, 개인정보 자기결정권에 중대한 침해를 가하는 것이라 하겠다.

한편 유럽연합(EU)은 미국이 전자여행허가제(ETA)를 실시하려는 것에 대해 '다른 이름의 비자제도'라며 강한 불쾌감을 표시하고, 미국이 이를 시행할 경우 상호주의의 원칙에 따라 유럽연합(EU)도 미국인들에게 비슷한 비자제도를 마련하겠다고 응수하고 있다.

다. 여행자 정보공유 협정

비자면제 프로그램(VWP) 가입의 전제조건 중 하나인 여행자 정보공유 협정에 대해서 외교통상부는 "해당국은 미국과 협정을 통해 가입국 국민이 미국 여행 시 미국과 미국 시민의 안보와 복지에 위협을 주는지 여부에 대한 정보를 공유"라고 설명을 하고 있다. 어떠한 정보를 제공할 것인가 하는지에 대해서는 미국 측과 협의를 하고 있다고 밝히고 있다. 하지만 위에 서술한 외교통상부의 설명은 미국의 9/11 위원회 법에 정의되어 있는 Passenger Information Exchange[21] 부분을 그대로 번역한 것이어서, 과연 진정으로 협의를 하고 있는 것인지는 의문스럽다. 위에 서술된 미국 시민에게 위협을 주는지에 대한 정보란 개인의 사법기록을 의미하는 것으로 생각된다. 여행자 정보공유 협정은 기존에 개인의 제출기록에 의존하던 비자심사를 정부 간의 정보공유로 확인/검증하는 결과를 낳게 되어 비자심사가 오히려 강화되는 것으로 볼 수 있다.

또한 미국 정부가 미 국토안보부(DHS)에 데이터베이스(DB)를 운용하고, 이를 출입국 심사에 반영하는 시스템을 구축하고 있는 것과는 달리, 한국정부는 미국 여행자들의 정보를 제공받는다 하더라도 그것을 사용할 수 있는 아무런 시스템을 가지고 있지 않은 바, 여행자 정보 공유협정은 사실상 한국이 미국에게 한국인들의 개인정보를 넘기는 일방적인 여행자 정보 상납 협정이라고 생각할 수 있다.

여행자 정보공유 협정에서의 가장 큰 문제점은 민감한 개인정보를 국가간의 협정을 통해 거래한다는 점이다. 한국 내에서도 개인의 사법기록은 검찰과 경찰만이 조회할 수 있는 민감한 개인정보이다. 또한 어떠한 개인정보도 정부 부처간 임의로 교환/공유하는 것은 금지되어 있다. 그런데 이제 미국 정부가 한국인들의 사법기록을 조회해볼 수 있게 하는 협정을 맺겠다는 것이다. 미국은 이러한 개인정보 교환/공유를 유럽연합(EU)에도 요청하고 있지만, 유럽연합(EU)은 유럽인들의 프라이버시 문제를 이유로 거절하

21) "The government of the country enters into an agreement with the United States to share information regarding whether nationals of that country traveling to the United States represent a threat to the security or welfare of the United States or its citizens." Passenger Information Exchange - Secure Visa Waiver Travel Act

고 있다.

라. 미국으로 전송되는 개인정보

현재에도 미국은 미국으로 향하는 여행자들의 항공기 예약 정보(PNR: Passenger Name Record)를 수집하고 있으며, 한국의 항공사들도 미국으로 개인의 항공기 예약 정보를 전송하고 있다. 이는 개인의 정보를 불필요하게 타인에게 전송하는 것으로 명백하게 개인정보 자기결정권을 침해하는 것으로 볼 수 있으며, 또한 전송된 정보는 미 국토안보부에 75년간 보관되면서 정보주체인 개인에게는 열람/수정/삭제의 권한이 전혀 없는 바 OECD 프라이버시 가이드라인 등을 위반하는 심각한 인권침해하고 볼 수 있다.

이에 대해 유럽연합(EU) 인권재판소는 개인의 PNR 정보를 전송하는 것이 프라이버시 보호에 관한 유럽연합의 인권선언이나 헌장에 위배하므로 무효라고 판결한 바 있다. (C-317/04, C-318/04) 한편 한국 외교통상부는 이에 대해 국제항공운송협회(IATA)의 규정에 따라 개별 항공사가 미국정부에 개인정보를 전송하고 있다고 최재천 의원의 질의에 답변한 바 있다.

또한 현재 미국 비자 심사 시 미 대사관에서 채취된 지문은 미 본토로 전송되어 75년간 저장되는 바, 역시 개인정보 자기결정권 침해라고 할 수 있다. 또한 미국 비자발급이 거부된 사람들의 지문정보도 미 국토안보부(DHS)에 75년간 저장되어 미국비자 발급이 거부된 사람의 입국을 저지하는 용도로 사용되고 있다. 이는 개인정보 자기결정권 뿐 아니라, 이동의 자유까지 제한하고 있어 상황이 심각하다 하겠다.

마. 미국의 개인정보 보호 현황

외교통상부는 미국으로 전송된 여타의 개인정보들이 미국 측에 의해 안전하게 보관되고 있다고 최재천 의원의 질의에 답변한 바 있다. 답변의 핵심적인 내용은 다음과 같다. “다양한 형태로 보관된 정보 보안을 위해 물리적(physical), 기술적(technical), 행정적(administrative), 환경적(environmental) 인 보호 전략을 수립·시행하고 있음”

하지만 2007.7 미 국회에 제출된 미 국회 전문연구그룹 GAO의 보고서에 따르면 상황이 정반대임을 알 수 있다. GAO는 해당 보고서에서 “US-VISIT 프로그램의 정보보안에 중대한 결함이 존재하고 있으며, 개인을 식별할 수 있는 민감한 정보들이 승인되지 않은 접근을 통해 유출, 수정, 오용, 파기될 가능성에 노출되어 있다”고 논술하고 있다. 구체적인 문제점으로는, ① US-VISIT에 포함된 시스템들의 사용자들에 대한 적절한 인증/식별을 하지 않았고, ② US-VISIT에 저장되어 있는 정보들에 대한 접근을 적절히 제한하지 않았고, ③ 내/외부의 네트워크 경계에 대한 통제가 적절하게 보장되지 않았고, ④ 서버가 존재하는 위치에 물리적인 보안이 구현되어 있지 않고, ⑤ 민감한 정보가 네트워크를 통해 전송될 적에 지속적으로 암호화되지 않았으며, ⑥ 서버, 단말기에 대한 사용자 기록(log)을 남기지 않고 있음을 들고 있다.

따라서 외교통상부의 주장과는 달리 미국 내에서는 미국 내에 저장되는 개인정보들이 제대로 보호되고 있지 않다는 주장이 제기되고 있는 상황이다. 한국 정부의 할 일은 미국비자면제 프로그램(VWP) 가입을 통해 더 많은 개인정보를 전송하는 협정을 체결하는 것이 아니라 이전에 전송되고 있는 개인정보들이 잘 보호되고 있는지, 또한 그렇게 정보를 전송하는 것이 정당한 것인지를 먼저 판단해야 하는 것으로 생각된다.

바. 출국통제 시스템(Exit-Control)

GAO는 또 다른 보고서[22]에서 효과적인 출국통제 시스템(Exit-Control)을 구축하는데, 5-10년의 시간이 걸릴 것으로 보고하고 있다. 이는 생체정보를 이용하는 출국통제 시스템의 구축을 위해선 기존의 출입국심사대 구조를 총체적으로 바꾸는 공사가 미국 전역에서 시행되어야 하기 때문이다. 이러한 어려움 때문에, 미국은 생체정보를 이용하는 대신 여행자에게 RFID 태그를 부여하는 방식으로 출국통제 시스템을 시험한 바 있다. 이는 실패로 돌아갔다.

한국의 미국 비자면제 프로그램(VWP) 가입요건 중 하나인 미국은 출국통제 시스템 구축이 5-10년 걸릴 것으로 예상되는 바, 한국에서 생체여권(전자여권)을 무리하게 조기 도입해야 한다는 주장은 타당하지 않다 하겠다.

사. 미국비자 면제의 효과

한편, 외교통상부는 조선일보의 '1년 앞도 못 내다본 전자여권'라는 제목의 기사에 대한 해명 보도자료(2007.9.15)에서 미국비자면제가 사실 별 효과 없음을 스스로 인정한 바 있다. 그 내용은 다음과 같다.

> "전자여권 발급 개시와 함께 미국 비자면제 혜택을 받으려는 신청자들로 인하여 여권 신청이 집중될 것인가와 관련, 첫째, 기존 여권은 여전히 유효한 만큼 새 여권으로 교체해야 하는 것은 아닙니다. 둘째, 미국과의 비자면제가 언제 이루어질지 아직 확실하지 않습니다. 셋째, 여권 소지자중 미국 비자를 이미 발급받은 사람은 전자여권으로 교체할 필요는 없습니다. 마지막으로 관광.상용 이외의 목적으로 미국에 체류하고자 하는 사람은 비자를 받아야 하므로 역시 전자여권으로 교체할 필요가 없으며, 관광.상용의 경우에도 비자를 받는 것이 유리한 경우도 있습니다."

아. 결론

미국이 비자면제를 이유로 한국의 여권법을 바꾸라 하는 것은 명백한 내정간섭이다. 현재 미국비자면제 프로그램(VWP) 가입된 국가들도 미국 비자면제에 가입된 상태에서 비자면제를 계속해주는 조건으로 생체여권 도입 등을 강요받은 바 있다. 이런 식의 계

22) 'US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry' GAO http://www.gao.gov/docsearch/abstract.php?rptno=GAO-07-248

속되는 내정간섭은 한국이 미국 비자면제 프로그램(VWP)에 가입된 이 후에도 반복될 가능성이 높다고 생각된다.

전체적으로 미국비자면제 프로그램(VWP)의 조건들에 대해 신중한 고려가 필요하다. 현재 미국의 비자면제 프로그램(VWP)에는 27개국이 가입되어 있지만, 현재 미국이 한국에 제시하고 있는 조건으로 가입되어 있는 국가는 없다. 유럽연합(EU)은 미국의 전자여행허가제(ETA), 여행자 정보 공유협정 추진에 대해서 분명하게 불쾌감을 표시하고 있다. 상호주의의 원칙, 프라이버시 원칙에 어긋나기 때문이다. 미국이 제시하고 있는 조건을 봤을 때, 미국비자면제는 사실상 기만이며 이를 위해 생체여권(전자여권)을 도입하는 것은 정당하지 않다 하겠다.

7. 양심·종교·이동의 자유

가. 여권

여권은 대한민국의 통치권이 미치지 아니하는 곳으로 여행하고자 하는 국민에 대하여 대한민국 국민으로서의 신분을 공적으로 증명할 수 있는 신분증일 뿐 아니라, 유효한 여권을 소지하는 것은 '출입국관리법'에 따라 적법하게 대한민국을 출입국하기 위한 요건이 되므로 여권은 사실상 해외여행에 대한 허가증이라고 할 수 있다. 이처럼 여권은 헌법상 국민의 기본권인 거주·이전의 자유, 특히 해외여행의 자유와 직접적인 관련이 있다.

나. 양심·종교·이동의 자유

양심적·종교적 이유로 인해 생체정보의 제공을 거부하거는 경우 이에 대한 생체여권(전자여권) 이외의 대안마련이 없다면, 헌법 제19조와 제20조의 양심, 종교의 자유에 대한 침해를 야기하거나 특정 행정절차참여를 사실상 금지하는 것과 같아 적법절차의 원칙에도 위배된다. 또한 여권발급을 원함에도 불구하고 이러한 한계 때문에 여권을 발급받을 수 없는 사람들은 헌법 제14조의 이동의 자유를 침해당할 수 있으며, 이로 인해 또 다른 차별의 문제가 발생할 수 있다.

한국은 세계에서 유일하게 전 국민지문날인 제도를 가지고 있는 국가로, 따라서 세계에서 유일하게 지문날인 거부자들이 존재하고 있다고 볼 수 있다. 지문날인반대연대의 자료에 따르면 2,000명이 넘는 지문날인 거부자들이 존재하고 있을 것으로 추산되며, 이들은 주민등록증 없이 여권 등의 대체 신분증을 이용해 살아가고 있다.

따라서 지문정보를 수록하는 생체여권(전자여권)은 개인정보자기결정권 침해 이외에도 양심·종교의 자유, 나아가 이동의 자유를 제한하는 것이라 할 수 있겠다.

8. 결론

이상 외교통상부가 주장하는 생체여권의 도입목적인 ① 국제범죄 및 테러방지 ② 위변조 방지 등 보안성 강화 ③ 국민 편의 증대 ④ 미국 비자면제 프로그램(VWP) 가입 등이 타당하지 않고, 기능할 수 없음을 살펴보았다. 오히려, 생체여권(전자여권)을 도입하지 않는 것이 외교통상부의 주장에 부합한다고 생각할 수 있을 정도이다. 따라서 기본권 제한입법의 요건인 목적의 정당성, 방법의 적정성, 피해의 최소화, 비례의 원칙 등을 충족하지 않는다 하겠다. 이번 여권법 개정안은 위헌적이며, 국민의 기본권을 심각하게 침해하는 것이다. 현재 논의되고 있는 생체여권(전자여권) 사업은 전면 중단되어야 한다.

9. 참고자료

가. 외교통상부

- 2007.2.23 전자여권 도입을 위한 공청회 자료집
- 2007.4.11 전자여권 도입사업 시행 계획 | 전자여권 도입추진단
- 2007.9.19 전자여권 도입을 위한 공청회 자료집 | 통외통위
- 2007년 국정감사를 위해 외교통상부가 국회 통외통위에 제출한 자료들
- 외교통상부 홈페이지 '유럽안전여행'
- 외교통상부 홈페이지 '미국 비자 면제 프로그램(VWP) 바로알기'
- 외교통상부 홈페이지 '전자여권, 개인정보 줄줄 샌다' 해명 보도자료

나. 국내

- 외교통상부 답변에 대한 인권시민사회단체 입장
- '개인의 사생활, 국가적 감시, 그리고 규범' | 국회 미래사회연구포험 (진영, 변재일 의원)
- 여권법 개정안에 대한 의견 | 민변 이은우 변호사
- 생체여권과 인권 | 민변 조범석 변호사
- 생체정보의 보호 | 용인송담대학 박영철 교수
- 생체정보 보호 가이드라인 | 정보통신부
- RFID 이용 가이드라인 | 정보통신부
- 통외통위 2008년도 예산검토보고서 | 통외통위
- 개인정보보호 관련 사회적 공감대 형성을 위한 공청회 | 행정자치부
- 해커들, 전자여권 복제하다 | 아이뉴스24
- 전자여권, 개인정보 줄줄 샌다 | 아시아경제
- 당신의 생체정보가 미-일을 오간다면 | 오마이뉴스

다. 해외

- ICAO Doc9303 (생체여권 표준) | ICAO(국제민간항공기구)
- 부다페스트 선언 | FIDIS

- 2006 Privacy Report | Privacy International
- Homeland Security Needs to Immediately Address Significant Weaknesses in Symtems Supporting the US-VISIT Program | U.S GAO Report
- Why Biometrics is not a Panacea | Peter Gutmann (University of Auckland)
- ‘US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry:’ | U.S GAO Report
- ePassport 'at risk' from cloning | BBC
- US-VISIT Report | EPIC
- 미 9/11 위원회법 | 미 의회
- The European Union and United States lay groundwork for a 'global security envelope' using biometric IDs. | FedTech
- 개인정보 국제적 유통 및 프라이버시 보호를 위한 가이드라인 | OECD
- Cracked it | Guardian
- 'Safest ever' passport is not fit for purpose | the Daily Mail

10. 문의/담당

진보네트워크센터 김승욱, 02)7744-551, saakan99 at jinbo.net