Journal of the Korea Academia-Industrial cooperation Society
Vol. 21, No. 5 pp. 637-647, 2020

https://doi.org/10.5762/KAIS.2020.21.5.637
ISSN 1975-4701 / eISSN 2288-4688

항공안전 향상을 위한 생체인식 기반 항공보안시스템 도입 및 국제표준화 활성화 연구

조성환[1], 윤한영[2*]
[1]바른기회 연구소, [2]한서대학교 항공융합학부

A Research on the Analyzing Biometric Aviation Security System and Proposing Global Standardization to Improve Aviation Safety

Sung-Hwan Cho[1], Han-Young Yoon[2*]
[1]Research Lab for Fair Opportunity
[2]Division of Comprehensive Aviation Studies, Hanseo University

요 약 테러리즘 양상의 변화와 과학기술의 발전으로 항공보안 분야의 선제적 대응 필요성에 따라 각 국가는 공항 및 항공관련 기관에 생체인식기술을 활용하고 있으며 적극적으로 확대하여 도입하고 있다. 항공안전을 위협하는 요소를 사전에 예방하기 위한 ICAO 항공보안계획은 글로벌 항공운송산업의 지속적인 발전을 위한 전제로써 생체인식을 기반으로 한 항공보안 시스템 구축 및 향상 방안을 강구하였다. 본 연구의 목적은 생체인식기술을 도입하여 각 국가 간 균질적인 항공보안시스템을 구현하는 데 기초자료로 활용되기 위함이다. 본 연구는 주요 선진국의 생체인식기반 보안시스템 운영 현황을 살펴보고 법적·제도적 분석을 통한 정책적 시사점을 도출하고자 하였다. ICAO 회원국들이 항공테러를 사전에 예방하고 항공보안 관련 정보를 실시간으로 공유하기 위해 항공여객의 생체인식정보 활용을 위한 ICAO 회원국 간 표준화 방향 및 구체적인 가이드라인이 필요하다. 항공안전을 향상하기 위해 항공보안시스템에서 생체정보의 활용은 이제 거의 모든 국가에서 보편적으로 이루어지고 있는 시대적 흐름이 되었다. ICAO 차원에서 국제적 표준 기준이 제시 된다면 글로벌 항공운송산업의 안전 향상 위한 생체정보 활용 시, 회원국 간 실시간적인 정보 공유 등을 통해 발생할 수 있는 항공안전 위협 요소 또는 예상되는 보안사고를 일관성 있게 대처 할 수 있을 것이다.

Abstract Airports and civil aviation authorities have recently utilized and expanded the use of biometric technologies to respond proactively against the rapid changes in aviation terrorism due to scientific development. The Global Security Plan (GASeP) developed by the International Civil Aviation Organization (ICAO) is regarded as precondition for sustainable development of the global air transport industry. Thus GASeP has sought to improve aviation security system using biometic technologies. The purpose of this paper is to realize the equivalent access of aviation security system throughout the world with biometric technologies. First, this paper reviewed the current biometric-security system operated by the EU, USA and international society. Second, legal and institutional processes regarding personal biometric information were analyzed to suggest political implications. This paper concluded that ICAO should propose a global standardization and prepare guideline materials among its 193 member states to prevent aviation security breaches and to share related information on a real-time basis because time is required to utilize biometric technology to improve aviation safety and to develop global air transport.

Keywords : ICAO, Global aviation security plan, Aviation security, Biometric technology, Aviation safety

*Corresponding Author : Han-Young Yoon(Division of Comprehensive Aviation Studies, Hanseo University)
email: zeno61@hanmail.net
Received February 4, 2020 Revised March 11, 2020
Accepted May 8, 2020 Published May 31, 2020

1. 서론

1.1 연구의 배경

개인정보로써 가장 민감한 항공여객의 생체정보는 과거의 심리적 거부감과 달리 급격한 과학기술의 발달로 인해 생체인식의 보안 안정성, 기술의 효율성 등에 대한 신뢰가 형성되었다. 이에 따라 항공보안뿐만 아니라 각 산업 분야에서 활용 저변의 폭이 확대되고 있다.

최근 들어 테러리즘 양상의 변화와 과학기술의 발전으로 항공보안 분야의 선제적 대응 필요성에 따라 각 국가는 공항(만) 및 항공관련 기관에 생체인식기술을 활용하고 있으며 적극적으로 그 범위를 확대 도입하고 있다[1].

국제민간항공기구(ICAO, International Civil Aviation Authority)는 항공기 안전과 항공보안을 담보하기 위하여 첨단기술 적용 등을 포함한 글로벌 항공보안계획(GASeP, Global Aviation Security Plan)을 수립 및 시행하고 있다. 하지만 GASeP의 세부 시행령 격인 편람(Doc.) 8973 (Aviation security manual)에서 생체정보 활용에 대하여 언급만 있고 별도의 세부지침은 Doc. 9303을 참조하라고 명시되어 있다.

1.2 연구의 목적

항공안전을 위협하는 요소를 사전에 예방하기 위한 ICAO 항공보안계획은 글로벌 항공운송산업의 지속적인 발전을 위한 전제로써 생체인식을 기반으로 한 항공보안 시스템 구축 및 향상 방안을 강구하였다. ICAO Doc. 8973은 여객의 생체정보를 활용한 항공보안과 관련하여 3 가지 카테고리 즉, 안면인식(Facial recognition), 홍채인식(Iris scan) 및 지문인식(Finger print)만을 언급하고 있을 뿐 구체적인 실행방안이나 다른 생체정보를 활용한 기술의 활용 등을 언급하고 있지 않다[2].

ICAO Doc. 9303 MRTD(Machine Readable Travel Document)에서는 항공여객의 필수정보로서 포함되어야 하는 3가지 생체정보로써 안면인식은 필수적이고 지문 또는 홍채 인식은 선택으로 지정하고 있을 뿐이다. 본 연구는 생체인식기술을 도입함에 있어 각 국가 간 균질적인 항공보안시스템 구현을 위해 국내외 공항 및 항공안전감독기관들의 생체인식기반 보안시스템 운영현황을 살펴보고 관련제도(법률) 분석을 통한 정책적 시사점을 도출하고자 하였다. 생체인식정보(개인정보)를 활용하는 각 국가 간 법률제도와 사회적 환경에 따라 그 적용범위 및 적용 대상이 상이하다. 따라서 ICAO 회원국들이 항공테러를 사전에 예방하고 항공보안 관련 정보를 실시간으로 공유하기 위해 항공여객의 생체인식정보 활용을 위한 ICAO 회원국 간 표준화 방향 및 구체적인 가이드라인을 제시하고자 한다.

2. 본론

2.1 생체인식정보의 정의

생체인식정보란 기본적으로 사람의 얼굴, 지문, 홍채, 음성, 지문, 손등 정맥, 유전자 단백질 등이 있다. 생체인식정보는 인간의 외적 특징을 포함하기도 하는데, 이러한 특징들은 걸음걸이, 말투 억양, 필체, 서명 등 쉽게 변하지 않는 개인마다 가지는 독특한 신체적·행동적 특징들을 포함한다[3].

생체정보를 생체인식보안유지 시스템 등에 입력·저장하여 개인의 동일성 여부를 판단하는데 활용함으로써 출입국 수속의 편의성을 증대하고 공항세관 및 항공기 탑승수속 등에서 보안성을 강화할 수 있기 때문에 항공운송의 거의 전 분야에 생체인식정보 활용 기술 응용되고 있다[4].

항공운송산업뿐만 아니라 일상생활에서도 개인적인 보안장치로 생체인식시스템이 보편화되기 시작하여 생체인식정보의 활용은 지속적으로 증가되었다. 개개인별 특성 인식의 정확성, 정보의 불변성, 정보수집 및 검색 편의성 등의 유리한 긍정적 측면이 있다는 장점이 있으나, 생체인식정보는 변하거나 바꾸기 어려운 특성 때문에, 일단 그 정보가 누출되는 경우 생체인식정보의 소유자가 자신의 생체정보를 바꾸는 것이 쉽지 않으므로 후속 피해가 막대할 수 있다는 단점도 있는 것이 현실이다[5].

2.2 생체인식정보 인증 시장규모

글로벌 IT 전문 시장조사기관인 트랙티카(Tractica)에 따르면 전 세계 생체인식정보 인증 시장은 2017년 20억 달러에서 시작하여 2024년 149억 달러에 이를 것으로 조사되었다. 향후 10년간 개인들의 휴대용 장비를 통한 생체정보인식 인증시장이 전체 시장에서 가장 큰 비중을 차지할 것으로 예측되었다. 또한 생체인식정보들 중에서 홍채인식, 안면인식 그리고 ECG(심전도, Electrocardiogram) 순으로 활용될 것으로 예측되었다.

Tractica는 향후 금융, 헬스 케어, 음성인식 AI, 공공서비스 분야가 생체정보인식 인증의 주요 시장으로 확대될 것이라면서, 생체정보인식 인증방식들 중에서는 지문, 홍채, 음성인식이 가장 큰 매출을 올릴 것으로 예상하였다.

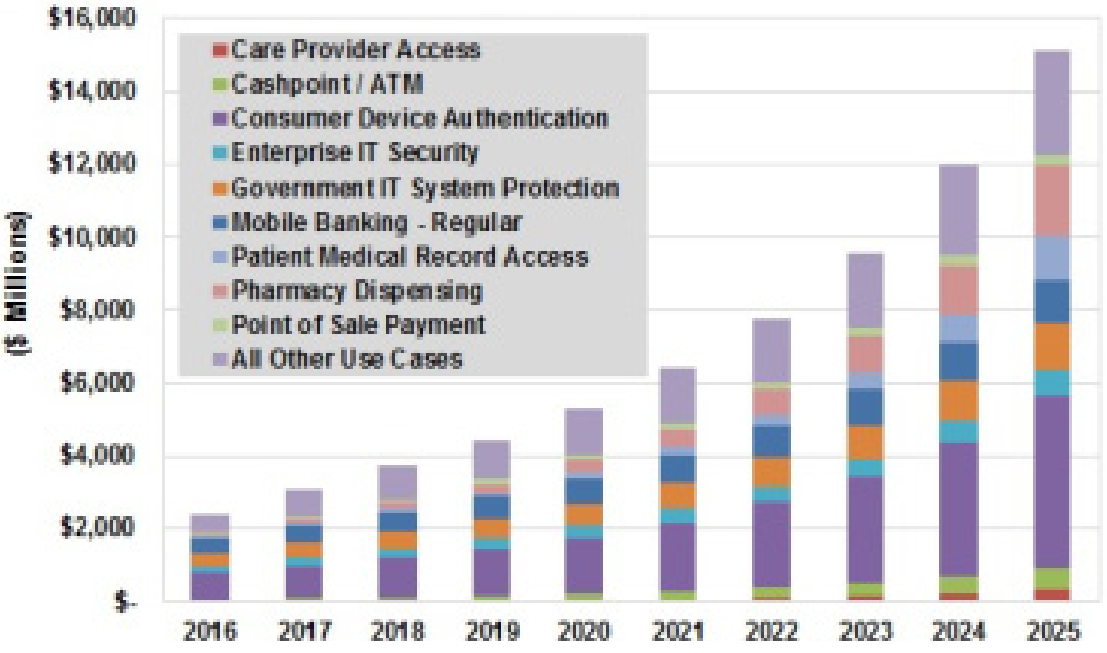

Fig. 1. Annual Biometircs Revenue, World Market 2016-2025 (Source: Tractica)

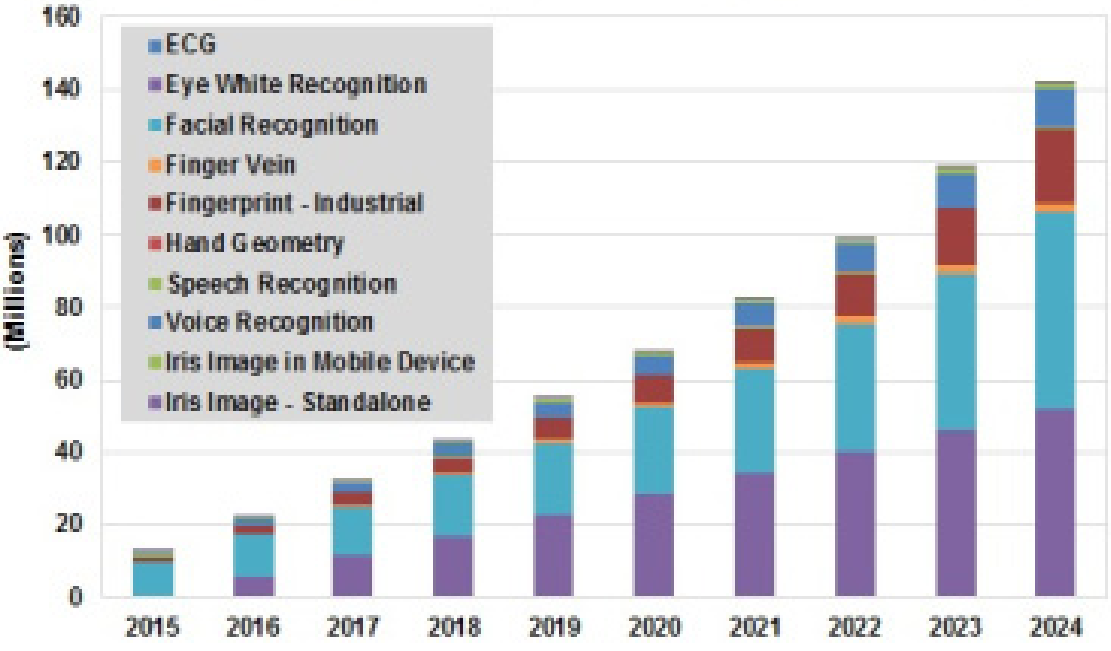

Fig. 2. Biometircs Device and License by Modality, World Market 2015-2024 (Source: Tractica)

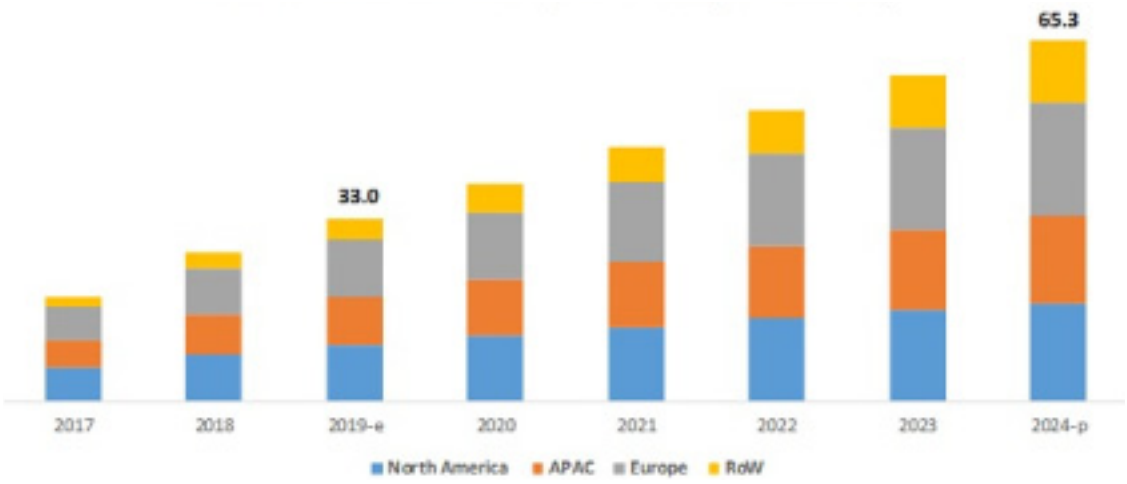

Fig. 3. Biometric System Market by Region (Unit: USD billion, RoW: Remaining countries of the World)

AIM(Acurity Market Intelligence)에 따르면 2019년 330억 USD 규모의 세계 생체인식정보 인증 시장은 2024년 약 650억 USD 규모로 확대되고 시장은 연간 14.6%씩 고성장할 것으로 전망하였다. AIM은 지문인식이 생체정보인식 인증방식들 중에서는 가장 큰 성장을 할 것으로 전망하였다.

2.3 생체인식 기술

생체인식 센서(Biometric sensor)는 생체 인식 입력 신호(지문, 음성, 정맥패턴, 홍채, 얼굴 인식 등)를 전기적 신호로 변환하는 센서를 말한다. 지문인식 센서 기술에는 광학식, 정전용량식, 초음파 방식이 있으며, 기본적으로 빛으로 지문의 밝기를 측정하는 광학식, 전압의 차이를 이용하는 정전용량식 그리고 초음파 방식 등이 있다. 초음파 방식은 광학식과 비슷하나 빛 대신 음파를 이용해서 사람 지문의'높낮이'를 측정하는 방식이다[6][7].

통상적으로 같은 지문을 가질 수 있는 확률은 수백억분의 1정도로 알려져 있어서 사실상 전 세계에 똑같은 지문을 가진 사람은 없다고 할 수 있다. 확률적으로 오류의 확률은 없다고 할 수 있으나, 센서의 상태에 따라 실제 사용 시 약 0.5%의 인식오류가 있는 것으로 알려져 있다.

홍채의 모양이 각기 다르다는 사실이 과학적으로 발견된 이후 1995년 홍채인식 시스템이 최초상용 개발되었다. 홍채인식은 생체인식정보 인증기술들 중 가장 최신 기술로 신뢰도가 높은 방식이라 생체인식기술 중 가장 정확도가 높다고 알려져 있다[8].

지문 인식기능이 특수한 센서를 사용하여 접촉된 부위를 스캔 하는 방식인 반면 홍채의 경우 직접 신체에 접촉하는 것이 아니라 카메라로 홍채를 촬영하여 모양을 분석하는 것이기 때문에 디지털 데이터 처리 알고리즘이 더 중요 하다. 홍채를 촬영할 때 해상도에 따라 보안성에 영향을 받으므로 그에 맞는 특수카메라가 필요하며 홍채인식의 오류 확률은 한쪽 눈만 사용했을 때 100만분의 1, 양쪽 눈을 사용했을 때는 무려 1조분의 1의 확률로 생체인식정보 시스템들 중 보안성이 가장 높다[9].

정맥 인식은 손바닥 정맥과 손가락 정맥을 이용하는 방식이며 몸속에 내재되어 있기 때문에 복제가 거의 불가능하여 국가보안시설 군 또는 경찰과 같이 강력한 보안출입통제가 요구되는 곳에서 주로 사용된다. 정맥인식은 특수한 센서가 필요하지 않아 핏줄 패턴을 읽을 수 있다면 활용 가능하다. 적외선을 이용해 얇은 피부 아래의 정맥 패턴을 투시 촬영, 홍채 인식과 마찬가지로 패턴을 분석하는 알고리즘을 이용해 데이터를 활용하는 방식으로 정맥인식의 오류 확률은 지문 인식과 홍채 인식의 중간인 대략 0.0001%로 알려져 있다[10].

생체인식정보가 보안 인증에 활용되기 위해서는 보편성, 유일성, 불변성 및 편의성 등의 기본요건을 만족해야 한다. 지문의 경우 나이가 들어도 변하지 않고 개인뿐만 아니라 일란성 쌍둥이도 서로 상이하다. 지문인식센서가 대부분의 스마트폰에 탑재될 만큼 소형화 및 편의성도 높아져서 지문인증 방식은 이제 일상생활에도 보편적으로 도입되었다.

Table 1. FRR and FAR for Types of Biometic system

unit : percentage(%)	Fingerprint	Retina	Finger vein	Palm vein	Face
FRR (False Rejection Rate)	0.1 ~ 0.5	0.0001 ~ 0.1	0.01 ~ 0.1	0.01 ~ 0.3	1.0 ~ 2.6
FAR (False Acceptance Rate)	0.001 ~ 0.01	0.00008 ~ 0.0001	0.00008 ~ 0.0001	0.0001 ~ 0.001	1.0 ~ 1.3

정맥인식은 생체인식 기술의 정확성에 대한 평가 지표인 FRR(본인 거부율) 및 FAR(타인 수락율)이 지문에 비해 우수하지만 인식센서 소형화의 어려움과 비교적 고가인 탓에 해외 ATM(은행 자동입출금기) 및 공항/항만의 출·입국관리소 등을 중심으로 도입되는 추세이다[11].

홍채인식은 최근 들어 스마트폰에 탑재 가능할 만큼 인식 센서의 소형화됨에 따라 지문인증에 이어 대중화되고 있다.

얼굴인식의 경우 스마트폰 등 이용자의 휴대용 단말기에 탑재된 카메라를 통해 획득 가능하여 편의성은 높은 반면 조명 등 외부 환경의 영향으로 인해 정확성이 떨어질 수 있다. 또한 노화로 인해 얼굴 특징이 변화될 수 있기 때문에 다른 생체정보에 비해 불변성이 떨어지는 것으로 평가되어 정확성이 가장 낮은 방식이다. 이를 보완하기 위해 이용자 주변 환경 및 밝기에 상관없이 얼굴인식이 가능한 기술들이 개발되고 있지만 인식센서 소형화의 어려움 및 비용문제로 제한적으로 사용되고 있는 상황이다.

3. 국내•외 법적 고찰

3.1 국내법령 현황

현행 국내법령에는 일관된 생체정보 규정이 부재한 상황이다. 개인정보 보호법과 정보통신망법은 개인정보의 처리에 있어 개인정보 보호를 위하여 정보주체의 사전 동의를 필요로 하는 엄격한 기준을 두고 있다. 그러나 개인정보 보호법과 정보통신망법에서 모두 개인정보로서 중요한 위치를 차지하고 있는 생체인식정보에 대해서 일관되게 규정하고 있지 않고 있다.

항공기의 운항 및 그와 관련된 항공시설의 방어를 포함하여 테러로부터 국민의 생명과 재산의 보호 및 공공의 안전을 확보하는 목적의 '국민보호와 공공안전을 위한 테러방지법(약칭: 테러방지법지법)'은 테러위험인물에 대하여 민감한 정보를 포함한 개인정보를 수집할 수 있도록 허용하고 있으나 생체인식정보에 관한 별도의 규정이 없는 실정이다. 테러방지법 관련 내용은 다음과 같다.

제9조(테러위험인물에 대한 정보 수집 등) ① 국가정보원장은 테러위험인물에 대하여 출입국·금융거래 및 통신이용 등 관련 정보를 수집할 수 있다. 이 경우 출입국·금융거래 및 통신이용 등 관련 정보의 수집에 있어서는 「출입국관리법」,「관세법」,「특정 금융거래정보의 보고 및 이용 등에 관한 법률」, 「통신비밀보호법」의 절차에 따른다.

② 국가정보원장은 제1항에 따른 정보 수집 및 분석의 결과 테러에 이용되었거나 이용될 가능성이 있는 금융거래에 대하여 지급정지 등의 조치를 취하도록 금융 위원회 위원장에게 요청할 수 있다.

③ 국가정보원장은 테러위험인물에 대한 개인정보(「개인정보 보호법」상 민감 정보를 포함한다)와 위치정보를 「개인정보 보호법」 제2조의 개인정보 처리자와 「위치정보의 보호 및 이용 등에 관한 법률」 제5조제7항에 따른 개인위치정보 사업자 및 같은 법 제5조의2제3항에 따른 사물위치정보사업자에게 요구할 수 있다. 〈개정 2018. 4. 17.〉

④ 국가정보원장은 대테러활동에 필요한 정보나 자료를 수집하기 위하여 대테러 조사 및 테러위험인물에 대한 추적을 할 수 있다. 이 경우 사전 또는 사후에 대책위원회 위원장에게 보고하여야 한다.

동법 시행령 제45조(고유식별정보의 처리)

관계기관의 장은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제9조에 따른 테러위험인물에 대한 정보 수집, 대테러조사 및 테러위험인물에 대한 추적 등에 관한 사무
2. 법 제12조에 따른 테러선동·선전물 긴급 삭제 등 요청에 관한 사무
3. 법 제13조에 따른 외국인테러전투원에 대한 규제 등에 관한 사무
4. 법 제14조에 따른 신고자 보호 및 포상금 지급 등에 관한 사무
5. 법 제15조에 따른 테러피해의 지원 등에 관한 사무
6. 법 제16조에 따른 특별위로금 지급 등에 관한 사무

이러한 연유로 2019년 7월 국회에서는 항공오보안법 일부개정법률안이 발의되었다. 강훈식 의원이 대표 발의하였으며 주요 개정법률안 내용은 다음과 같다.

가. 생체정보에 대한 정의규정을 신설함(안 제12조제12호 신설).
나. 항공보안 확보를 위하여 공항운영자, 항공운송사업자가 본인 일치여부 확인을 위해 신분증을 육안으로 확인으로 하던 것을 국가기관이 보유하고 있는 생체정보로 대체할 수 있도록 함(안 제14조2 제1항부터 제4항까지 신설).

항공보안법 일부개정법률(안)

제2조에 제12호를 다음과 같이 신설한다.

12. "생체정보"란 항공보안 확보를 위하여 탑승권 발권, 보호구역 진입, 항공기 탑승 등의 과정에서 사람의 얼굴·지문 등에 관한 정보를 이용하여 본인 일치여부 확인에 활용되는 개인정보를 말한다.

제14조의2를 다음과 같이 신설한다.

제14조의2(생체정보를 활용한 본인 일치여부 확인) ① 공항운영자는 보호구역으로 진입하는 사람에 대하여, 항공운송사업자(「항공사업법」 제2조제20호에 따른 항공기취급업자 포함)는 탑승권의 발권 및 항공기에 탑승할 때 공항운영자의 생체정보관리시스템을 이용하여 본인 일치여부를 확인할 수 있다.

② 제1항에 의한 생체정보 활용의 경우 행정기관이 가지고 있는 생체정보를 활용할 수 있다. 이 경우 공항운영자는 행정기관에 생체정보 제공을 요청할 수 있으며 행정기관은 정당한 이유 없이 그 요청을 거부하여서는 아니 된다.

③ 공항운영자 및 항공운송사업자는 제2항에 따른 생체정보는 「개인정보 보호법」에 따라 처리하여야 한다.

④ 제1항 및 제2항에 따른 생체정보를 활용한 본인 일치여부 확인방법 등 필요한 사항은 국토교통부령으로 정한다.

3.2 국외 주요 선진국 법률 및 제도

지문과 같은 생체정보는 일찍이 미국이나 캐나다 등과 같이 본인확인제도가 발달하지 않은 국가에서 사회보장의 부정수급을 방지하기 위한수단으로 활용되었다. 하지만 2001년 9.11 항공테러로 인하여 여권 등 각종 본인확인을 위한 문서에 생체정보를 포함시켜 출입국이나 범죄수사와 같은 공공분야로부터 다양한 인식 및 인증의 기반으로 사용되었다.

최근에는 지문·홍채·얼굴인식 등 바이오인식 기술과 공개키 암호화 기술을 융합해 비밀번호의 입력 없이 지문인식 한번만으로 결제가 가능한 온라인 간편 인증(FIDO, Fast Identity Online) 기술이 본격적으로 개발되고, FIDO 연합이 설립되어 생체정보 기술을 활용한 인증방식에 대한 기술이 표준화되었다. FIDO는 비밀번호의 문제점을 해결하기 위한 목적으로 FIDO 얼라이언스에 의해 제안된 사용자 인증 프레임워크이다. 인증 기법(authentication method)과 그 인증 정보를 주고받기 위한 인증 프로토콜(authentication protocol)을 분리하는 것을 핵심 아이디어로 한다[12]. FIDO는 비밀번호 없이 인증하기 위한 Universal Authentication Framework (UAF) 프로토콜과 비밀번호를 보완해서 인증을 위한 Universal 2nd Factor (U2F) 프로토콜로 구성된다. 지문, 홍채 등 바이오인증을 적용하기 위해 주로 사용된다.

그러나 현재까지 어떤 국가에서도 여전히 생체정보에 대한 규정이 독자적으로 구축되지 않고 기존의 개인정보 관련하여 그 전체적인 틀 속에서 이해되고 있는 것으로 판단된다. 생체정보 활용 서비스는 전 세계에 걸쳐 과학기술의 특성상 보편적인 서비스의 성격을 갖는다. 하지만 각 국가마다 처한 기술적 상황 및 제도의 차이가 있기 때문에 생체정보의 활용 현황에 비추어 생체정보의 개념과 범위 등이 명확하지 않은 우리 법제의 현실을 환기하고 개선방안을 논의하기 위해 주요 선진국들의 관련 법령 및 제도가 어떻게 구축되어 있는지 살펴보았다.

가. 유럽연합

유럽은 개인정보 보호와 같은 인권과 관련하여 오랜 역사적 사건들과 전통을 보유하고 있다.유럽 내 여러 국가들은 각각 개인정보보호법을 가지고 있으나 국가별 법적 차이로 인하여 EU 국가들 간에 정보가 자유로이 활용되기에는 제한적이므로 유럽연합 역내에서 정보의 자유로운 활용을 가능하게 할 전체적인 기준을 필요로 하게 되었다.

개인정보의 활용을 증진하고 또한 개인정보의 보호를 강화하기 위하여 1981년 EU 이사회는 개인정보 자동화 처리를 위한 개인보호의 협약을 체결하였다. 유럽연합은 일찍이 1995년에 개인정보의 처리에 있어 정보주체를 보호하고 EU회원국 간 개인정보의 자유로운 활용을 보장하기 위하여 EU 개인정보보호지침을 정한 것이다.본 지침에서 말하는 개인정보는 신원이 확인되었거나 확인 가능한 자연인에 관한 정보로서, 특히 신원을 확인할 수 있는 자는 직·간접적으로 특정 식별번호 또는 신체적, 생리적, 정신적, 경제적, 사회적, 문화적 동일성에 관하여 하나 또는 그 이상의 식별요소에 근거하여 확인될 수 있는 자를 의미한다.

여기서 개인정보의 정의는 신체적, 생리적 식별요소라는 생체정보의 징표가 포함되어 있어 생체정보는 곧 개인정보로서 자연스럽게 해석될 수 있다. 2016년 상기 규정은 GDPR(General Data Protection Regulation, 개인 정보보호일반규정)으로 변경되었다.

GDPR Article 4(1)

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(13) 'Genetic data'
(14) 'Biometric data'
(15) 'Data concerning health'

생체인식정보의 발전 및 적용 환경의 변화를 반영하여 GDPR에서 새로이 규정하고 있는 내용으로, GDPR 4조(Article 4)는 유럽연합 내에 근거를 두고 있는 기업 외에도 그 상품이 유럽연합 내의 특정 국내 시장을 목표로 하거나 개인정보의 처리가 유럽연합 내에 있는 사람의 행동에 관한 것일 경우에는 유럽연합 밖에 있는 기업도 본 규정의 규율 범위 안에 포함시킴으로써 그 적용 범위를 유럽시장 전체로 확대하였다. 생체정보와 관련하여 특별한 고려를 하고 있는 다음의 규정을 살펴보면 보호대상인 개인정보의 범위를 세분화하고 개인정보의 유형을 병렬적인 개념으로 나열하였다는 데 그 특징이 있다.

나. 미국

미국 국가과학기술위원회(NSTC, National Science and Technology Council)는 생체정보라는 개념을 두 가지, 즉 일반적인 의미의 생체정보(Unique physical characteristics)와 생체정보로부터 추출한 생체인식정보(Biometrics)로 구분하고 있다.

연방정부와 각 주(州)정부가 각 분야별로 관련법을 제정해온 미국의 이러한 방식을 영역별 혹은 분야 별 규율 방식이라고 한다. 연방정부 차원의 대표적인 개인정보 관련 법률은 연방정부 기관이 보유하고 있는 개인정보보호에 관한 개인정보법(Privace act of 1974)이다. 각 주(州)단위로도 주정부가 규정한 개인정보보호 관련 법률이 존재하기도 한다.

생체정보에 관하여 연방차원에서 별도로 제정된 개별 법률은 존재하지 않으나 9.11테러 이후 국가안보 등을 이유로 출입국 및 보안 관련된 법에서 신분 확인을 위한 목적으로 규정되었다.

샌프란시스코는 미국에서 처음으로 경찰 등 행정 당국의 안면인식 기술을 이용한 감시를 금지하는 법안 가결하였다. 샌프란시스코 시(市)가 법안을 최종 통과시키면 미국 내 첫 안면인식 기술 감시 금지 도시가 될 전망이다. 오클랜드와 버클리도 비슷한 법령을 제정했으나 제한적 수준으로서 사실상 사법·행정 기관의 전면 금지 법안은 워싱턴과 매사추세츠에 이어 샌프란시스코가 세 번째가 되는 것이다.

텍사스 상법 (Texas Business and Commercial Code) 5003.001 조항에서는 생체 정보식별자에 관하여 다음과 같이 규정하고 있다.

Clarifies that a person may not sell, lease or otherwise disclose the biometric identifier of a person captured for a commercial purpose unless: (a) the individual consents to the

disclosure for identification purposes in the event of the individual's disappearance or death; (b) the disclosure completes a financial transaction that the individual authorized; (c) the disclosure is required or permitted by a federal statute or by a state statute other Texas Gov't Code Chapter 552; or (d) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant. (Note: "biometric identifier" is defined as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.)

Clarifies that a person who possesses a biometric identifier captured for a commercial purpose shall destroy the biometric identifier according to the following rules: (a) within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires; (b) if the biometric identifier is used in connection with an instrument or document that is required by law to be maintained, within a reasonable time, but not later than the first anniversary of the date the instrument or document is not longer required to be maintained by law; or (c) if the biometric identifier has been collected for security purposes by an employer, on termination of the employment relationship.

일리노이 주는 생체정보 개인정보보호법(BIPA, Biometric Identification Privacy Act)을 2008년 통과시켰다. 생체정보식별자는 눈동자 패턴, 홍채 패턴, 지문, 음성, 손바닥 형상, 얼굴 형상을 대상으로 한다고 명시되어있다. 생체정보식별자의 정보는 다음의 경우를 제외하고는 상업적인 목적으로 사용해서 안 되며, 생체정보를 수집하기 전에 개인에게 통보해야 하고 생체정보식별자 개인의 동의를 받아야 한다. 생체정보식별자 개인의 정보공개와 관련하여 상업적인 목적으로 획득한 개인의 생체정보식별자를 보유하는 정부기관은 본인의 동의 없이 생체정보식별자를 매매, 임대 또는 제3자에게 공개해서는 안 된다. 또한 생체정보식별자가 누설되지 않도록 동등한 혹은 다른 비밀정보를 보호하는 방법보다 더욱 주의하여 보관, 전송해야 한다고 규정한다.

Article 10 "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.

이 법의 생체정보식별자에 관하여(정의) 망막 혹은 홍채, 지문, 성문, 손과 얼굴모양을 대상으로 한다고 규정하고, 생체정보식별자에는 작성샘플, 서명, 사진, 타당한 과학적 실험에 사용된 인간생물학 샘플, 인구통계, 신장, 체중, 모발 색 또는 동공의 색과 같은 신체적 묘사는 포함하지 않는다고 하여 생체정보의 각 식별자에 대한 규범적 평가를 포함하고 있다.

미국은 9.11테러 이전부터 생체인증을 이용한 개인인식기술이 개발되고 채택을 검토하고 있던 중에 9.11 테러가 발생하였고, 그 후 대통령의 제안으로 생체인증을 이용한 개인인식기술을 채택하였다. 이에 맞춰 응용에 대한 연구개발과 국가과학기술위원회(NSTC) 중심으로 정부부처 간 생체인식에 대한 정책을 실시. 생체인식정보를 활용하여 얼굴인식과 헬스 및 피트니스와 같은 웰빙산업, 소비자금융전자상거래, 기업보안, 출입국관리시스템과 생체인식형 여권, 운전면허증, 복지연금수급, 범죄수사, 귀 인식 스마트폰 등 다양한 분야에서 활용하고 있다.

미국은 부처 간에 서로 공동으로 활용할 수 있도록 다양한 생체정보활용 프로그램을 운용하는바, 미국 국가표준기술원(National Institute of Standards and Technology, NIST)은 1960년대부터 연방수사국의 법집행과 과학수사기술을 지원하기 위한 지문정보기술에 대한 연구 등 그동안 생체정보 분야에서 지문 및 얼굴인식의 일치여부와 호환, 형사사법정보 체계, 다양한 복합형태의 생체정보에 대한 측정, 평가 및 표준화에 대한 연구를 수행한 바 있다. 국토안보부(Department of Homeland Security, DHS)는 생체인식정보와 관련하여 다음의 주요기능을 운용하고 있다.

- REAL ID, 테러의 예방과 사기를 감소시킬 목적으로 연방정부가 발행한 신분증명 서류의 정확도와 신뢰성을 제고하기 위함

- 바이오인식관리사무국(Office of Biometric Identity Management, OBIM)은 2013. 3. US-VISIT99) 프로그램을 시하면서 전자여권에 사진(필수), 지문(선택) 등 바이오정보를 수록한 IC 칩을 탑재하도록 시행
- Trusted Traveler Program, 교통안전국(The Transportation Security Administration, TSA)은 항공안전의 강화와 세관 서비스의 증대를 위한 목적으로 민간 영역과 더불어 등록여행자 프로그램을 개발 중이며, 이는 교통안전국의 감시와 더불어 민간 영역에서 제공되는 자율적인 시장 주도 프로그램으로서 역할을 수행

국토안보부 외에도 美 법무부(Department of Justice, DOJ)는 주로 범죄수사와 관련된 바이오정보 인식체계를 가지고 있다. 특히 연방수사국(FBI)은 바이오인식표준으로 전자지문전송 명세서(Electronic Fingerprint Transmission Specification, EFTS)를 사용하고 있으며, 형사사법정보서비스 부서에 의해 전국적으로 운용되는 지문 및 범죄기록 시스템으로서 통합자동지문인식체계인 IAFIS (Integrated Automated Fingerprint Identification System)를 보유하고 있다. 아울러 연방수사국의 바이오인식과 신원확인 운용의 핵심조직인 바이오인식특성화센터(The Biometric Center of Excellence, BCOE)를 운용하고 있다.

美 국무부(Department of State, DOS)의 가장 큰 업무 중 하나는 미국 전자여권을 관리하는 것으로 즉 일성의 컴퓨터칩이 부가된 것이다. 이 칩은 여권의 사진부착면에 시각적으로 인식될 수 있는 사항과 동일한 데이터를 저장하고 있으며, 디지털 사진을 내장하고 있다. 디지털 사진의 내장은 국경에서 안면인식시술을 통하여 비교를 가능하게 한다. 이러한 미국의 e-passport는 새로운 모습을 갖고 있고, 추가적으로 위조방지와 보안을 위한 특성을 체화한 것이다.

다. 국제민간항공기구(ICAO)

서론에서 제시한 바와 같이 Doc. 8973 Aviation Security Manual, Registered traveller programme (11.5.17.3)에서 항공여객의 생체정보는 안면인식, 홍채스캔, 지문(visage electronic photograph, iris and/or fingerprinting) 3개 카테고리 만을 구분하고 있으며, 구체적인 실행방안과 관련하여 Doc 9303(MRTD)를 참조하라고 언급하고 있다.

Doc 9303 MRTD에서는 생체정보에 포함되어야 하는 3가지로 안면인식은 필수사항이지만, 지문(fingers)과 홍채(iris)는 선택사항으로 지정되어 있다. ICAO TRIP(Traveller Identification Programme : 여행자 신원확인 프로그램) Guide on Border Control Management에서도 얼굴, 지문 및 홍채만을 언급하고 있다.

Doc 9303 Part 9 3.1. ICAO Vision on Biometrics

Doc 9303 considers only three types of biometric identification systems. with respect to storage of these three biometric features in the contactless IC of an eMRTD, the issuing State or organization SHALL conform to the relevant international standard. The types of biometric are:

- Facial recognition - MANDATORY. MUST comply to [ISO/IEC 19794-5];
- Fingerprint recognition - OPTIONAL. if used, MUST comply to [ISO/IEC 19794-4];
- Iris recognition - OPTIONAL. if used, MUST comply to [ISO/IEC 19794-6];

4. 결론

4.1 연구의 요약

2018년부터 대한민국 국내선 모든 공항에서 승객 동의를 받아 별도로 등록한 생체정보인 손바닥 정맥과 지문을 활용한 본인확인시스템 운영 중이다. 인천국제공항의 경우 2020년 말 시범운영을 목표로 한 인천국제공항은 손바닥 정맥과 지문을 이용한 생체인식 시스템 용역 착수 예정이다.

인천국제공항은 국제선 탑승수속 간소화, 항공보안·출입국관리 강화 등을 목적으로 생체정보를 활용한 승객 신원확인시스템 도입을 위한 관계기관 협의체 구성 및 운영 중이다. 경찰청은 내국인 지문을, 법무부는 내·외국인 지문 및 얼굴 등을 관할하여 업무 협업을 추진 중이다.

생체정보와 관련한 국제적 규범 및 국가 규정들을 통해서 생체정보의 활용을 기본적인 원칙으로 하고 생체정보의 보호를 침해하는 경우에 생체정보의 활용을 제한하는 경향을 확인할 수 있었다.

EU 개인정보보호규정은 유럽연합 회원국 간의 자유

로운 활용을 지향하고 있으며 EU 역외의 적용에 있어서는 개인정보의 보호를 기본적인 원칙으로 하지만 적절한 보호가 보장된다는 전제하에 개인정보의 활용을 허용 한 것이다. EU GDPR은 EU 국가들 간에 동등한 수준으로 개인정보를 보호하고자 하며, 미국의 개인정보 보호체제는 주마다 서로 다른 보호 규정을 두고 있고 필요에 따라 보완하도록 하는 자율적인 방식으로 운영되고 있다.

유럽의 경우 포괄적이고 체계화 및 일원화된 개인정보 보호 규정을 두고 있으나 미국의 경우는 필요한 경우에 대응해서 개인정보 보호 규정을 마련하는 방식으로 운영되며 미국은 규제를 최소화하고 개인정보의 활용에 역점을 두고 있는 것이 확인 되었다.

유럽은 역사적인 특징으로 인하여 인권의 보호를 중요한 가치로 여기고 있어 포괄적인 방식의 법제로 운영되고 있으나, 미국은 자유로운 역사적, 사회적, 문화적 환경으로 인하여 규제보다는 개인정보의 활용을 중요한 가치로 여기고 있는 것으로 사료된다.

ICAO는 유럽 외 국가들이 유럽의 국가들에 생체인식 서비스를 제공할 경우와 미국에 서비스를 제공할 경우에 각각의 규정에 따른 기준의 차이를 상호주의 관점에서 감안해보면 생체인식정보의 체결국간 호환의 문제가 발생할 수 있을 것으로 판단하고 있는 것으로 사료된다. 한국과 유럽연합 간의 개인정보 활용의 상황에서, 서로 개인정보 보호수준이 유사하다면 개인정보 제공과 관련하여 크게 문제가 되지 않을 것이나 양 지역의 개인정보 보호 범위에 큰 차이가 있는 경우에는 개인정보 제공과 관련 상호인정 가능성이 희박할 것이다. 따라서 유럽연합의 개인정보보호 수준이 우리나라의 보호 수준 보다 높은 경우에는 우리나라의 보호 수준을 유럽연합의 수준으로 맞추어야 할 것이다.

반면 우리나라와 미국 간의 서비스 제공이 있는 경우에는 우리의 개인정보 보호 수준이 미국 보다 높으므로 미국과의 상호 호환을 상정하였을 경우 개인정보 보호수준을 미국의 수준으로 낮출 필요는 없으나 우리의 개인정보가 국내에서만큼 높은 수준으로 보호되지 못하거나 침해될 수 있을 우려가 있을 수 있다.

생체정보 데이터 활용 서비스가 인터넷을 통해서 여러 국가에 배포 되고 있고, 여러 국가의 이용자들이 서비스에 접근하고, 또한 여권에 생체정보가 수록되어 있으며 공항 출입국 심사에서 생체정보를 활용하므로, 그 보호 문제는 생체정보 데이터 활용 서비스와 관련하여 제기될 있는 법적 문제이기도 하다.

4.2 생체인식 기반 항공보안의 국제표준화

4장에 제시된 바와 같이 ICAO Doc 9303 MRTD에서 생체정보에 포함되어야 하는 3가지로 얼굴은 필수, 지문과 홍채는 선택으로 지정하고 있으며, ICAO TRIP에서도 얼굴, 지문 및 홍채만을 언급하고 있다.

ICAO 193개 회원국들은 개인정보보호에 관한 규정을 두고 있으나 국가별로 생체정보 활용 등의 규정의 차이를 포함하여 문화적 정서적 차이에서 나타나는 생체인식 서비스에 대한 거부감 등으로 인하여 ICAO는 항공여객 생체정보 데이터 활용 서비스에서의 관한 문제를 해결하려는 노력에도 불구하고 회원국들의 의견 합의 도출이 쉽지 않은 상황이다.

각 국가의 법률마다 생체정보에 관심을 두는 분야가 다른데 특히 EU의 경우 공적 분야에서, 미국의 경우 사적 분야에 더 비중이 높은 것으로 보인다. 하지만 아직 어느 나라도 생체정보의 개념이나 유형, 보호 등에 관하여 법, 제도 등을 완결적인 형태로 갖고 있지는 않은 것으로 판단된다.

생체정보의 개념을 생체인식정보로 인정하고 있는 미국의 경우는 주목할 만하지만, 미국 또한 연방차원에서는 생체정보를 개인정보의 체계 속에 포함시켜서 이해하고 있으며, 독자적인 규범적 지위를 가진 개념으로 인정하고 있는 것으로 보이지 않는다. 따라서 각 국가의 법제 및 기술, 문화의 차이 등으로, 공항 및 항공 관련 기관 마다 생체인식 서비스 도입에 따른 생체 정보적용이 각각 상이하여 그에 따른 항공보안에 다소 차이가 있을 수 있기에 보다 균질적인 생체인식 기반 항공보안시스템의 정립이 필요하다 할 것이다.

따라서 ICAO 회원국 공동의 목표인 항공안전을 확보할 수 있도록 회원국 간 공항신설 또는 시설개량 시 적절한 생체인식정보의 적용을 위한 생체인식 시스템 가이드라인 정립이 필요한 시점이다. 항공안전을 향상하기 위해 항공보안시스템에서 생체정보의 활용은 이제 거의 모든 국가에서 보편적으로 이루어지고 있는 시대적 흐름이 되었다. ICAO 차원에서 국제적 표준 기준이 제시 된다면 글로벌 항공운송산업의 안전 향상 위한 생체정보 활용 시, 회원국 간 실시간적인 정보 공유 등을 통해 발생할 수 있는 항공안전 위협 요소 또는 예상되는 보안사고를 일관성 있게 대처 할 수 있을 것이다.

References

[1] D. S. So, S. S. Park, "A Study on the Acceptance of Security Screeners of Airport Full Body Scanners by Applying Extended Technology Acceptance Model (TAM)", Journal of Korean Society of Hazard Mitigation, Vol. 18, No. 5, pp.73-81, 2018.
DOI: https://doi.org/10.9798/KOSHAM.2018.18.5.73

[2] D. S. So, S. S. Park, "A Study of the Relationship between Security Screeners' Job Stability and Their Public Service Motivation to Improve Aviation Security", Journal of Korean Society of Hazard Mitigation, Vol. 19, No. 1, pp.123-133, 2019.
DOI: https://doi.org/10.9798/KOSHAM.2019.19.1.123

[3] M. Faundez-Zanuy, "Biometric Security Technology", IEEE Aerospace and Electronic System Magazine, Vol. 21, No. 6, pp.15-26, 2006.
DOI: https://doi.org/10.1109/MAES.2006.1662038

[4] I. McAteer, A. Ibrahim, G. Zheng, W. Yang, C. Valli, "Integration of Biometrics and Steganography: A Comprehensive Review", Technologies, Vol. 7, No. 34, pp. 1-22, 2019.
DOI: https://doi.org/10.3390/technologies7020034

[5] K. Dharavath, F. A. Talukdar, R. H. Laskar, "Study on Biometric Authentication System, Challenges and Future Trends: A Review", IEEE International Conference on Computational Intelligence and Computing Research, December 26-28, 2013.
DOI: https://doi.org/10.1109/ICCIC.2013.6724278

[6] A. Jain, K. Nandakumar, A. Ross, "Score Normalization in Multimodal Biometric Systems", The Journal of Pattern Recognition Society, Vol. 38, pp.2270-2285, 2005.
DOI: https://doi.org/10.1016/j.patcog.2005.01.012

[7] E. P. Kukula, M. J. Sutton, S. J. Elliott, "The Human-Biometric-Sensor Interaction Evaluation Method: Biometric Performance and Usability Measurements", IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 4, pp. 784-791, March, 2010.
DOI: https://doi.org/10.1109/TIM.2009.2037878

[8] W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review", Symmetry, Vol. 11, No. 141, pp.1-19, January 2019.
DOI: https://doi.org/10.3390/sym11020141

[9] A. Ross, A. K. Jain, "Biometric Sensor Interoperability: A Case Study in Fingerprints", Biometric Authentication, ECCV International Workshop, BioAW 2004, Prague, Czech Republic, May, 2004.
DOI: https://doi.org/10.1007/978-3-540-25976-3_13

[10] H. Benaliouche, M. Touahria, "Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint", Scientific World Journal, pp.1-14, January, 2014.
DOI: https://doi.org/10.1155/2014/829369

[11] H. AlShehri, M. Hussain, H. Aboalsam, M. Alzuair, "A Large-Scale Study of Fingerprint Matching Systems for Sensor Interoperability Problem", Seonsors, Vol 18, No. 4, pp.1-18, 2018.
DOI: https://doi.org/10.3390/s18041008

[12] R. Lindemann, "The Evolution of Authentication", In: Reimer H., Pohlmann N., Schneider W. (eds) ISSE 2013 Securing Electronic Business Processes. Springer Vieweg, Wiesbaden, 2013.
DOI: https://doi.org/10.1007/978-3-658-03371-2_2

조 성 환(Sung-Hwan Cho) [정회원]

- 2009년 6월 : 한국체육대학교 대학원 (안전관리학석사)
- 2018년 2월 : 한국항공대학교 대학원 (경영학박사)
- 2000년 3월 ~ 2011년 3월 : 관세청 인천공항세관 조사과
- 2011년 3월 ~ 2013년 9월 : ㈜에어퍼플 이사
- 2013년 9월 ~ 현재 : 바른기회 연구소 소장

〈관심분야〉
항공경영, 항공안전, 출입국 및 세관

윤 한 영(Han-Young Yoon) [정회원]

- 1988년 2월 ~ 1999년 6월 : 한국공항공사 재직
- 1999년 6월 ~ 2018년 3월 : 인천국제공항공사 재직
- 2004년 2월 : 한국항공대학교 경영대학원 (항공경영학석사)
- 2012년 2월 : 한국항공대학교 대학원 (경영학박사)
- 2018년 4월 ~ 현재 : 한서대학교 항공융합학부 부교수

〈관심분야〉
항공경영, 공항운영, 공항서비스