Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.6, Dec. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1563

금융 보안에서 휴먼팩터를 고려한 인간과 인공지능의 역할 및 협업 모델

이 보 라,† 김 인 석‡
고려대학교 정보보호대학원

The Role and Collaboration Model of Human and Artificial Intelligence Considering Human Factor in Financial Security

Bo-Ra Lee,† In-Seok Kim‡
Korea University, Graduate School of Information Security

요 약

전자금융 규제 완화와 함께 핀테크가 활성화되었다. 인공지능에 대한 논의가 금융업에서도 활발하다. 하지만 신기술의 이면에는 보안 위협의 증가라는 문제가 있다. 과거보다 연결이 되고, 금융업의 채널과 주체가 다양해지면서 보안 취약점이 증가했다. 보안에 대한 기술적, 정책적 논의가 있지만 결국 모든 논의의 본질은 인간이다. 금융의 기본은 신뢰와 보안이고, 이를 위해 인간적 요소에 대한 관심은 중요하다. 본 연구는 금융 보안을 위한 인간과 인공지능의 역할을 각각 제시한다. 나아가 인간과 인공지능이 서로의 한계를 보완한 협업 모델을 도출한다. 이를 뒷받침하기 위해 금융과 IT의 발전, 인공지능, 휴먼팩터, 그리고 금융 보안 위협에 대해 우선 논한다. 본 연구는 신기술의 시대에 보안 위협이 심화되지만 반대로 기계, 기술을 활용하여 이를 극복할 수 있다는 방향성을 제안한다.

ABSTRACT

With the deregulation of electronic finance, FinTech has been revitalized. The discussion on artificial intelligence is active in the financial industry. However, there is a problem of increasing security threats behind new technologies. Security vulnerabilities have increased because we are more connected than before, and the channels and entities of the financial industry have diversified. Although there are technical and policy discussions on security, the essence of all discussions is human. Fundamentals of finance are trust and security, and attention to human factors is important. This study presents the role of human and artificial intelligence for financial security, respectively. Furthermore, this derives a collaborative model in which human and artificial intelligence complement each other's limitations. To support this, it first discusses the development of finance and IT, AI, human factors, and financial security threats. This study suggests that the security threats will intensify in the era of new technology, but it can overcome them by using machinery and technology.

Keywords: Human Factor, Artificial Intelligence, Finance, Security, Collaboration

I. 서 론

1.1 연구 배경

금융업을 포함한 각 산업 분야에서 사물인터넷, 클라우드, 블록체인, 인공지능의 IT 신기술을 적용하려는 움직임이 활발하다. 2015년 3월에는 전자금융거래 시 공인인증서 사용 의무가 폐지되었다[1]. 2015년 6월에는 금융감독원 보안성심의 의무가 폐지되었다[2]. 금융위원회는 이와 같은 전자금융감독

Received(09. 27. 2018), Modified(11. 13. 2018), Accepted(11. 13. 2018)

† 주저자, jrohns1@naver.com
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

규정의 개정을 고시하였고, 민간 중심의 자율적 보안과 사후 규제로 패러다임이 전환되었다. 금융업은 핀테크 활성화와 전자금융 규제 완화 정책으로 변화를 겪고 있었다. 때마침 각 분야에서 블록체인과 인공지능에 대한 논의가 활발해지면서 금융업의 변화의 흐름은 더욱 탄력을 받았다.

인공지능이라는 용어는 John McCarthy가 1956년에 개최한 다트머스 회의를 통해 처음 사용되었다[3]. 인공지능의 3차 붐은 양질의 빅데이터와 오픈 소스로 공개된 학습 알고리즘에 기인한다. 또한 GPU (Graphics Processing Unit) 기반의 컴퓨팅 파워 향상도 AI의 발전에 영향을 미쳤다. 이를 통해 딥러닝의 여건이 나아졌다. 2012년의 구글 브레인 프로젝트에서 1,000만 개의 이미지를 학습시키는 데 3일 간 16,000대의 컴퓨터를 사용했다. 바이두 인공지능 연구소에서는 GPU를 이용하여 1년 뒤 이와 동일한 성능을 3대의 컴퓨터로 구현했다[4].

과거에 비해 은행, 보험, 여신전문, 증권 등 금융업의 비대면 채널이 활성화되었다. 가령 국내 은행의 인터넷뱅킹 이용 건수 및 금액은 증가해왔고, 인터넷뱅킹 중 모바일뱅킹이 차지하는 비율도 늘었다[5]. 디지털 기기와 정보 기술의 발전으로 금융업의 서비스 환경에 변화가 일어나고 있다. 은행의 경우 결제 및 자산관리 앱 출시, 인터넷전문은행의 출현[1], 포털 업체의 금융 서비스 제공 등 변화를 겪고 있다.

금융 서비스를 비대면 채널을 통해 고객이 직접 접하게 되면서 보안 위협도 증가했다. 즉, 고객 접점이 다양해져 금융회사의 정보 보호 노력만으로는 보안을 유지하기 어렵게 되었다. 금융업 관련 주체와 서비스가 많아지면서 보안에서 휴먼팩터가 더욱 중요해졌고, 이에 대한 연구가 필요하다. 금융, 인공지능, 보안 등 이 모든 논의는 인간을 위한 것이고, 결국 본질은 인간이기 때문이다.

1.2 연구 목적

정보 보호 분야에는 "100% 완벽한 보안은 없다."라는 말이 있다. 보안에서 가장 약한 링크는 인간이고[6], 보안은 이 약한 연결만큼의 보안성을 제공한다[7]. 따라서 금융회사에서 보안 프로그램을 도입하고, 인증을 강화해도 위협은 사라지지 않는다. 사회가 연결되고, 산업이 온라인화되면서 보안 위험도 증가했다. 다양한 기술이 모바일에 적용되어 새로운 위협이 나타났다[8]. 금융권에 클라우드, 인공지능의 도입이 확대되면 예측이 어려운 보안 문제는 증가할 것이다. 하지만 국가 산업의 부흥을 위한 투자와 기술 발전 지원, 초연결사회로의 진입은 피할 수 없는 흐름이다. 본 연구를 통해 기술 발전의 흐름은 받아들이고, 위협을 식별하며 대안을 제시하고자 한다.

본 연구의 목적은 크게 두 가지이다. 첫 번째는 금융 보안에서 휴먼팩터의 중요성을 강조하기 위함이다. 두 번째는 인공지능으로 대변되는 기술 패러다임의 변화를 받아들이고, 이로써 증가할 금융업의 보안 위협을 완화시키기 위한 인간과 인공지능의 협업 모델을 제시하기 위함이다. 즉, 기술의 도입으로 위험 요소가 증가했지만 해당 기술을 수용하고, 이를 활용해 보안 위협을 줄이자는 인식의 전환을 위한 것이다. 금융 분야의 현실적인 보안 문제에 대해 AI와 인간이 서로의 한계를 보완하고, 상생하는 모습을 제안할 것이다.

1.3 연구 방법 및 구성

본 연구에서는 휴먼팩터, 금융, 인공지능 관련 이론과 역사에 대해 다루기 위해 문헌 분석의 방법을 사용하였다. 문헌 조사를 통해 수집한 자료는 정량적 방법과 정성적 방법으로 분석하였다. 또한 사례 분석과 비교 연구의 방법을 통하여 각 개념의 공통점, 차이점을 파악하고, 국내외 동향을 살폈다.

본 논문의 구성은 다음과 같다. 제1장에서는 연구의 배경과 목적, 연구 방법 및 구성에 대해 논한다. 제2장에서는 기존 선행 연구의 동향을 살핀다. 본 연구의 이해를 돕기 위해 제3장에서는 인공지능의 정의와 역사, 국내외 동향과 주요 기술, 제4장에서는 휴먼팩터의 정의와 관련 이론을 살펴본다. 제5장에서는 금융과 IT, 보안에 대해 논의한 후 금융 보안 위협을 채널과 주체별로 살핀다. 제6장에서는 인간과 인공지능의 역할과 협업 모델을 제시한다. 제7장은 인공지능 활용 시 고려할 사항을 다룬다. 마지막으로 제8장 결론에서는 본 논문의 연구 결과와 의의, 한계, 향후 연구 및 발전 방향에 대해 논한다.

II. 선행 연구

휴먼팩터 또는 인공지능 보안과 관련된 국내외 연구들이 있다. 관련 연구를 살펴보면 Reza Alavi[6]는 SWOT 분석과 역장분석(Force Field Analysis)의 방법을 통해 정보 보안에서의 휴먼팩터에 대한 연

구를 수행했다. 해당 연구는 휴먼팩터를 직접적인 요인, 간접적인 요인으로 나누어 진행하였다. 조사 결과 '커뮤니케이션, 인식, 관리 지원'이 상위 3위 안에 속하는 중요한 휴먼팩터임을 제시했다. 이수미[7]는 보안에서 휴먼팩터가 가장 위협적인 요소일 수 있다고 하였다. 사회공학, 인지력의 한계, 위협 불감증 등 인간에 의한 위협을 분류하고, 보안 교육, 홍보의 중요성에 대해 언급했다. Brian M. Bowen 등[9]은 사회공학 중 피싱 공격 가능성에 대한 측정 연구를 했고, 이는 조직의 보안 관련 경계 태세에 유용하게 활용 가능하다고 하였다.

Gary Hinson[10]은 보안에서 인간적 요소에 주의를 기울일 것을 강조하였다. 기술적 측면 이외에도 직원과 관련된 위험을 평가할 것을 제안했다. Kun-woo Kim 등[11]은 보안 교육이 형식적인 활동으로 간주되고 있다고 했다. 교육학과 사회 심리학을 기반으로 직원의 행동 변화를 위한 보안 교육 프레임워크를 연구하였다. 그러나 이 프레임워크에 대한 신뢰성과 타당성 검증, 구체적인 교육 방법에 대해 추가 연구의 필요성이 있다고 하였다.

Sizwe M. Dhlamini 등[12]은 보안 시스템의 관리 툴로 AI의 가치에 주목했다. 데이터의 범람으로부터 인간이 중요한 정보를 고립시키는 데 도움이 되도록 보안에서 인공지능을 활용할 것을 제안했다. Madhavi Dhingra 등[13]은 사람이 결정을 하는 것을 인공지능이 도울 수 있음을 제시했다. 또한 네트워크 보안, 모니터링, 접근 제어 등에서 인공지능의 역할을 언급했다.

국내외 휴먼팩터와 관련된 연구를 보면 휴먼팩터의 중요성을 언급하고, 관련 보안 위협을 분류했지만 이에 대한 구체적인 대안 제시가 부족하다. 기존 연구의 한계점을 보완하고 좀 더 깊이 있고, 확장된 논의를 할 필요성이 있어 본 연구를 수행하였다. 또한 선행 연구는 각 시대에 맞게 연구되었다. 이 중에는 신기술 시대에 맞게 연구를 다시 수행해야 되는 부분이 있을 것이다.

인공지능, 휴먼팩터 관련 선행 연구에서 보안, 특히 금융 보안에 초점을 맞추어 수행한 연구는 많지 않다. 인공지능 보안에 대한 논문의 경우도 이를 휴먼팩터와 연관시킨 연구는 부족했다. 본 연구는 금융 분야의 보안 영역에 초점을 맞추고, 인공지능과 휴먼팩터를 연결하여 연구를 수행할 것이다. 인간이 가장 약한 링크인 상황에서 수용 가능한 상태의 보안, 완벽에 가까운 보안을 실현하기 위해 인간적 요인에 주목하고자 한다.

III. 인공지능

1950년에 앨런 튜링은 철학 저널에서 "Can machines think?"라는 질문을 던졌다[3]. 기계가 생각할 수 있는지의 여부를 떠나 인공지능에서 튜링의 논문은 의미가 있다. 이후 이를 지지하거나 반론하는 연구들이 이어졌고, 학계와 각 산업 분야에 영향을 주었기 때문이다. 튜링이 'machine'과 'think'라는 단어에서 시작해 관련 실험을 제안한 후 인공지능에 대한 다양한 논의와 발전이 있었다.

3.1 인공지능 정의 및 분류

인공지능(Artificial Intelligence)에 대한 정의는 다양하다. 인공지능의 정의는 기술의 발전, 시간의 흐름에 따라 학문과 비즈니스 현장에서 다양한 의미로 사용되고 있다. 인공지능의 개념은 앞서 존재하기보다는 시대와 기술의 변화에 따라 형성되고 있다. 인공지능은 이를 둘러싼 학문의 발전, 각 산업 분야의 활용에 따라 그 시점에 보이는 공통의 특징을 통해 정의할 수 있다[14].

1956년에 인공지능 단어의 등장에 기여한 John McCarthy는 2007년에 인공지능의 정의에 대해 언급했다. 그는 "인공지능은 지능형 기계를 만드는 과학 및 공학이다."라고 했다[14]. 이 외에도 인공지능에 대한 여러 정의가 있다. 금융보안원에서 정리한 인공지능은 인간의 지능을 컴퓨터나 시스템으로 만든 것 또는 만들 수 있는 방법론이나 실현 가능성을 연구하는 기술 혹은 과학이다[15]. Nils J. Nilsson은 "인공지능은 컴퓨터를 지능적으로 만드는 데 전념하는 활동이고, 지능은 속한 환경에서 앞을 내다보고 이에 대응하는 능력이다."라고 정의했다[16].

Russell과 Norvig은 Fig. 1과 같이 인공지능을 목표에 따라 4가지로 분류했다[3]. 이들은 합리적 생각, 합리적 행동, 인간처럼 생각, 인간처럼 행동하는 시스템으로 인공지능을 정의했다. 이 분류는 인공지능에서 추구하는 네 가지 목표를 보여준다. Fig. 1의 상단은 사고 과정과 추론, 하단은 행동에 관한 것이다. Fig. 1의 좌측은 인간 지능, 우측은 합리성의 관점을 다룬다. 인간을 중심으로 한 접근법은 가설과 실험적인 확인을 포함한 경험 과학이어야 한다. 반면에 정확하게 생각하거나 행동을 하는 시스템이

있다면 이는 합리적이다. 합리성을 중심으로 한 접근법은 수학과 공학의 결합을 포함한다[3].

	Human Intelligence	Rationality
Thought Processes	Thinking Humanly	Thinking Rationally
Behavior	Acting Humanly	Acting Rationally

Fig. 1. Four categories of AI definitions

John Searle은 1980년 "Minds, brains, and programs"라는 논문을 통해 중국어 방 실험을 제안한다. 이는 튜링 테스트에 대한 반박 논증이었다. Searle은 해당 논문에서 인공지능을 강한 인공지능과 약한 인공지능으로 구분하였다. Searle은 약한 인공지능의 경우 마음에 관한 연구에서 컴퓨터는 단지 인간에게 강력한 도구를 제공한다고 했다. 예를 들어 컴퓨터는 인간이 더 엄격하고 엄밀하게 가설을 공식화하고 검증할 수 있게 해준다는 것이다. 반면에 그는 강한 인공지능의 경우 컴퓨터는 단순히 도구가 아니며 인간과 같이 마음을 가진다고 했다[17].

Searle의 인공지능 구분으로 보면 Fig. 1에서 좌측은 강한 인공지능에 가깝고, 우측의 정확한 생각과 행동을 강조하는 시스템은 약한 인공지능에 가깝다고 볼 수 있다. Table 1은 두 가지 유형의 인공지능의 차이점이다[17][18][19].

Table 1. The difference between Weak AI and Strong AI

Weak AI	Strong AI
· Imitate and mimic intelligence using predefined rules and algorithms · Implement a part of human intelligence · Solve problems in specific areas	· Actually thinking and doing the work with autonomous judgment · Having feelings, minds, self-consciousness like a human being · Implement human-level intelligence · Solve various problems

3.2 인공지능 역사

인공지능 분야에는 두 번의 부흥기와 두 번의 침체기가 있었다[20]. 70년대 중반부터 80년대 초반까지는 암흑기이다. 기대와 달리 연구 개발이 한계에 봉착해 각 국가에서 프로젝트가 취소되고 지원이 중단되었다. 두 번째 암흑기는 80년대 후반부터 90년대 초반까지이다. 프로젝트와 기술 개발에서 원하는 결과가 나오지 않아 막대한 연구 자금의 지원이 끊겼다. 또한 기술의 발전을 하드웨어가 따라가지 못하면서 기술 성장이 둔화되었다[3][21]. 현재 인공지능은 세 번째 부흥기를 맞고 있다[20]. 인공지능의 역사를 Table 2에 구성하였다[20][21]. 인공지능은 이를 실현할 때까지 부흥과 침체를 반복할 것이고, 이 기술의 발전과 적용을 위한 인간의 노력은 계속될 것임을 알 수 있다.

Table 2. History of Artificial Intelligence

Year	Content
1940s	· Study of function and action of neurons
1950s	· Artificial intelligence is defined through Dartmouth meetings · Game artificial intelligence and reasoning program announced
1980s	· Expert system shows practicality and AI is spotlighted
1990s	· IBM's Deep Blue won the World Chess Champion in 1997
2000s ~	· Deep learning has emerged and begin to show performance in image and speech recognition · IBM Watson wins quiz champion at Jeopardy Quiz Show in 2011 · Google's AlphaGo Beat Go player Lee Sedol in 2016

3.3 국내외 인공지능 관련 동향

현재 국내 인공지능 산업은 초기 단계에 있다. 미국, 일본 등 주요 국가와 비교할 때 국내 인공지능 관련 기술 수준, 특허 및 논문 건수, 시장 규모는 열위에 있다[22]. 가령 2016년 인공지능 분야 기술 수준은 미국을 100으로 보았을 때 한국은 73.9이며 미국과 2.2년의 기술 격차를 보였다[23]. 중국은 인공지능에 대한 공격적 투자와 육성 정책으로 크게 성장했고, 인공지능 투자 규모, 특허출원 기업 수 등에서 미국에 이어 2위인 상황이다. 인공지능 논문은 양적인 측면에서 중국이 1위, 질적인 측면에서는 미국이 1위이다[22]. 한국의 AI 시장 규모는 꾸준히 증가해 2020년에는 11조 1,000억 원에 도달한다는

전망이 있다[23].

Table 3은 인공지능 역량 확보를 위한 국가별 인공지능 관련 정책 동향이다[15]. 물론 구글, 페이스북, 바이두, 알리바바 등 기업의 관련 동향에도 주목해야 한다[21][22]. 인공지능은 컴퓨터공학, 심리학, 철학 등 여러 학문과 관련이 있다[3]. 인공지능은 학문의 연구자와 각 산업의 실무자가 함께 노력해야 그 실현 가능성을 높일 수 있다. 학계와 산업계의 협력과 한국 AI 시장의 성장을 가능하게 하는 정부의 정책적 지원이 필요하다.

Table 3. Policies related to AI by country

Country	Content
USA	Support 'Brain Initiative' for studying mechanism of dynamic understanding of brain function
China	The 'China Brain' project, proposed by Baidu President Li Yanhong, is included in the government's research plan
Republic of Korea	The 'Exobrain' task for 10 years has three steps and a step-by-step goal ('13 ~ '23)
EU	Joint research on the human brain with the 'Human Brain Project'
Japan	Selected as the core strategy of economic growth in the field of robotics, announced 'Robot New Strategy'

3.4 인공지능 주요 기술

자연어 처리, 음성 인식, 이미지 인식과 같은 인공지능 기술 분야가 있다. 인공지능의 기반 기술 영역을 '지각, 인식', '추론, 계획', '학습, 적용'으로 구분할 수 있고, 이 중 '학습, 적용'과 관련해 머신러닝과 딥러닝을 살펴볼 수 있다. 머신러닝은 데이터로부터 규칙, 패턴을 추출하여 프로그램을 생산하는 방법 또는 데이터를 활용해 자동으로 구조를 변경하는 방법을 통칭한다. 딥러닝은 머신러닝의 한 분야이고, 뉴런의 전기 화학적 신호로 인간 두뇌의 작동 방식을 컴퓨터 SW 형태로 모델링하는 인공 신경망의 다층 구조를 활용하는 방식이다[21].

머신러닝은 학습 방법에 따라 Table 4와 같이 세 가지로 분류할 수 있다[21]. 머신러닝과 딥러닝의 차이점은 머신러닝은 기계 학습을 위한 데이터의 특징 추출(feature extraction)에 인간이 개입한다. 반면에 딥러닝은 인간이 추출한 특징을 학습하는 대신 데이터를 있는 그대로 입력 받고, 기계가 스스로 주요 특징을 학습한다[18][21].

Table 4. Classification of machine learning by learning method

Division	Content
Supervised Learning	There is a leader who gives the correct answer label(output value) when learning.
Unsupervised Learning	Use learning data that does not specify the correct answer label (output value).
Reinforcement Learning	If the learner decides to act on the input, the leader compensates accordingly.

IV. 휴먼팩터

4.1 휴먼팩터 정의

본 논문에서 휴먼팩터(Human Factor)는 '기술, 인간, 기계, 정보 등의 요소가 각 기능을 가지고 상호 작용하는 조직, 체계, 시스템에서의 인간적 요소'라고 정의한다. 고도의 안전성이 요구되는 원자력 발전소의 경우 기계 시스템 측면의 안정성이 높지만 휴먼에러가 문제가 되고 있다. 체르노빌 원자력 발전소 사고 역시 인간적 요소가 원인이었다[24]. 이와 마찬가지로 정보 보안에서 기술적인 보안 수준을 높여도 인간과 관련하여 보안에 허점이 드러나고 있다. 한편 휴먼팩터는 인간과 기계와의 관계를 연구하는 인간공학(Human Engineering)과 연결된다[24].

4.2 휴먼팩터 이론

본 절에서는 연구의 기반이 되는 휴먼팩터 관련 이론을 살펴본다. Fig. 2는 Heinrich의 도미노 이론이다. 사고 발생 과정에는 사회적 환경, 개인적 결함, 불안전한 행동이나 상태, 사고, 재해의 5가지 요인이 있다. 이들은 도미노처럼 연결되어 있으며 3단계의 불안전한 행동(인적 요인), 불안전한 상태(물적 요인)가 직접적인 사고 원인이다. 사고는 어떤 원인의 결과이고, 이 원인이 식별되어 제거되면 사고의 반복을 막을 수 있다. 가령 인간의 착오, 부주의와

같은 불안전한 행동 또는 설비 결함과 같은 불안전한 상태를 제거하면 사고를 예방할 수 있다[25].

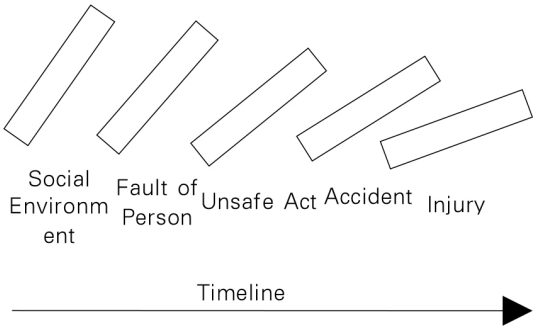

Fig. 2. Heinrich's Domino Model

Fig. 3은 Reason의 스위스 치즈 모델이다. 이에 따르면 사고는 최종적으로 인간의 불안전한 행동에 의해 발생하지만 불안전한 행동의 전제 조건, 불안전한 감독, 조직적인 영향이라는 잠재적인 실패 요인들이 있다. 각 요인들이 서로 연결되어 있는 상태에서 위험을 막지 않거나 방어에 실패하면 사고로 이어진다는 것이다[25][26].

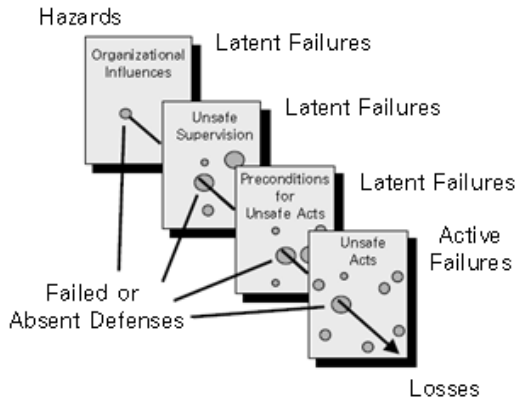

Fig. 3. Reason's Swiss Cheese Model

Rasmussen의 위험 관리와 연관된 사회 기술적 시스템 계층 모델이 있다. 이에 따르면 계층 구조를 수평적으로만 보는 것이 아니라 수직적으로도 살펴볼 필요가 있다. 어떤 사고가 단지 특정 레벨의 작업자에 의해 발생한 것만은 아닐 수 있다. 이 모델의 level 1부터 6까지 중 L5는 프로세스나 기술과 상호 작용하는 직원의 활동을 나타낸다. 이 레벨과 관련해서는 철학, 인간과 기계의 상호 작용, 휴먼팩터와 같은 분야에 대한 지식이 필요하다[25].

V. 금융 보안 위협

5.1 금융, IT, 그리고 보안

금융업과 IT는 그 발전 과정과 역사를 함께해 왔다. 금융 시스템의 발전이 금융업의 발전을 견인하기도 하고, 다양하고 복잡해지는 금융 업무를 지원하도록 금융 시스템이 발전한 측면도 있다. 손 안의 금융을 가능하게 하는 스마트폰의 확산을 넘어 금융 분야에서는 Industry 4.0 시대의 금융으로의 변화를 앞두고 있다. 메인프레임 기반 계정계, 정보계 시스템에서 지능화, 개인화된 초연결시대로 나아가고 있는 금융 분야의 과거, 현재, 미래에 대해 [1]을 재구성하여 Fig. 4에 제시했다. 현재 삼성페이, 네이버페이 등 간편결제가 활성화 되었고, 기존 금융회사가 담당하던 영역에서 비금융회사의 역할은 더욱 확대될 전망이다[1].

금융업과 IT의 발전과 함께 보안도 변화해 왔다. PC가 대중화되고 바이러스, 웜이 확산되어 보안의 중요성이 인식되고, APT(Advanced Persistent Threat) 공격 등 보안 위협이 진화해왔다[8]. 공격에 대한 방어도 모니터링, 탐지에서 위협 예측과 실시간 대응 방식으로 변화했다. 신기술 적용이 확대되고, 초연결시대로 갈수록 새로운 형태의 보안 위협이 등장할 것이다.

IT와 함께 발전해 온 금융업은 인공지능 기술이 도입되면 금융 서비스와 보안 측면에서 다시 변화를 겪을 것이다. 기존 IT와 인공지능은 차이점이 있기 때문이다. 기존의 컴퓨터는 계량화된 데이터만 처리했다. 이와 달리 인공지능은 구조화되지 않은 데이터도 인식하고 분석할 수 있어서 인간의 능력 수준에 더 근접한다[18].

인공지능과 초연결의 시대로 갈수록 보안 위협은 사이버 공간에 한정되지 않는다. 점차 공격의 대상이 사이버 공간을 넘어 인체, 물리적 자산 등 현실 세계로 확장될 가능성이 크다[27]. 인간이 컴퓨터, 인터넷을 발명한 후 현실과 사이버 세계의 경계가 모호해지고, 두 공간이 겹치는 영역은 증가했다. 가상 세계와 물리 세계가 서로 영향을 주고받으며 사람의 대화, 금융, 쇼핑 등 생활 방식을 바꾸고 있다. 이는 보안에서도 마찬가지이며 초연결시대에는 가상과 물리적 공간의 중복 영역이 더 넓어질 것이다. 신기술

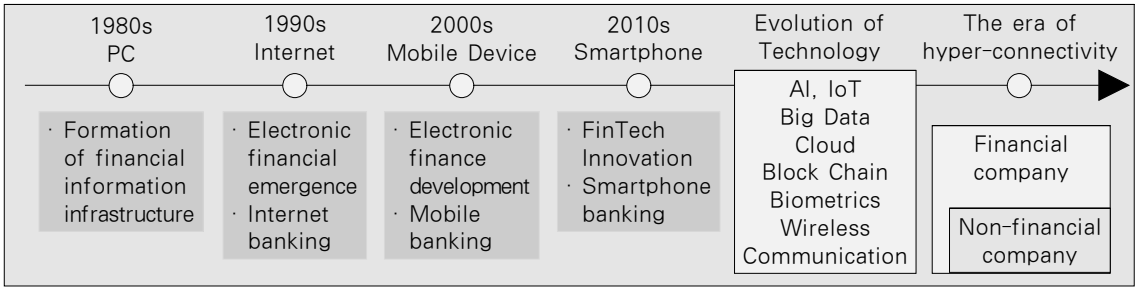

Fig. 4. Changes in technology and financial services

이 도입될수록 보안도 사이버 세계를 넘어 현실의 '공간'과 '사람' 관점으로 확장하여 살펴야 한다.

간편결제로 금융 서비스를 이용하는 등 데이터를 통한 가치의 교환이 일어나고 있다. 금융회사는 데이터를 안전하게 저장하고, 지켜야 한다. 금융업은 신뢰를 기반으로 하며 보안을 유지해야 한다. 이를 위해 지켜야 되는 대상, 보안을 위한 방법과 행동의 주체를 명확히 해야 된다. 본 연구에서는 금융 보안의 목표를 고객의 자산(데이터)과 정보(데이터)를 안전하게 지키는 것이라고 명시한다. 단, 사이버 공간뿐만 아니라 물리적 공간, 그리고 보안의 3대 요소인 비밀성, 무결성, 가용성을 함께 고려해야 한다[27].

보안을 가상 세계에서 사람, 공간 영역으로 확장하기 위해 물리적, 관리적, 기술적 보안으로 구체화하여 살펴볼 수 있다. ISO 27001은 정보 보호 관리 체계에 대한 국제적 표준이다. 이는 무결성, 기밀성, 가용성, 부인방지를 위하여 11개의 통제 영역, 133개의 세부 통제 항목으로 구성되었다[28]. 이 통제 영역처럼 금융 보안에서는 정책, 사람, 시설물, 시스템 등 물리적, 관리적, 기술적 영역 모두를 고려해야 한다. 아무리 망분리를 하고, 기술적, 물리적 보안을 유지해도 인간적 요인에 한계가 있으면 소용이 없다. 한편 Fig. 5와 같이 금융업의 보안을 채널별, 주체별로 나누어 분석하는 것도 의미가 있다.

5.2 채널별 금융 보안 위협

금융 업무가 복잡, 다양해지고 서비스 채널이 많아지면서 보안 취약점도 증가했다. 오프라인의 영업점 채널에서 온라인 채널로 금융 거래의 무게 중심이 이동하고 있다. 과거에는 금융회사를 사이에 두고 금융 서비스를 접했다[1]. 현재는 모바일 플랫폼을 통해 금융 소비자가 직접 클릭 또는 터치를 하며 상품 신규, 송금을 할 수 있다. 스마트폰의 출현과 보급의

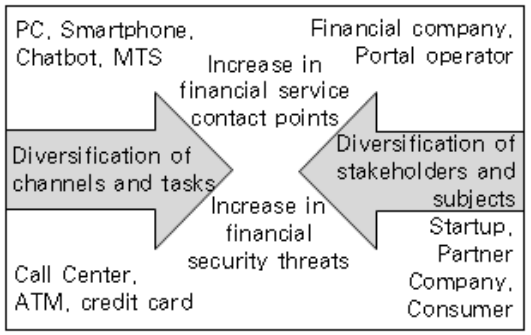

Fig. 5. Financial channels, entities and security threats

확산으로 인터넷뱅킹에서 모바일뱅킹의 등록 고객의 수가 증가했고, 2014년을 기준으로 일평균 이용 건수에서 PC 기반 인터넷뱅킹을 모바일뱅킹이 추월했다[5]. 이처럼 금융업에서 비대면 채널의 비중이 증가했다. 전자금융의 채널이 다양해질수록 전자금융사고 건수와 피해 금액도 증가하는 양상을 보였다[29]. ATM, PC, 스마트폰 채널에서 사물인터넷, 챗봇으로 채널이 다양해지면 금융 서비스의 접점 증가에 따라 공격의 접점도 증가할 것이다.

온라인 채널이 활성화되고 신기술 관련 금융 서비스가 확대된다고 해도 전통적인 금융 시스템과 영업점 채널의 보안을 간과해서는 안 된다. 창구에서도 타깃형 공격, 도청, 피싱에 이용되는 대포통장 개설, 허술한 비밀번호 관리와 복사지 파쇄, 단말기 악성코드 감염의 문제가 발생할 수 있다[8]. 이처럼 온라인뿐만 아니라 오프라인 채널에서의 보안도 물리적, 관리적, 기술적으로 고려되어야 한다.

가상 세계와 물리 세계의 경계가 더욱 허물어지고 있기 때문에 어느 한 부분만 살핀다면 보안의 연결고리가 끊길 수 있다. 은행의 경우 대외계, 계정계, 정보계 시스템이 있다. 금융기관 시스템에는 인터넷

뱅킹, 모바일뱅킹, ATM, 콜센터 등으로 구성된 서비스 채널이 있다. 이러한 온라인 채널과 함께 창구, 태블릿 브랜치 등의 채널 모두 보안의 대상이다.

디지털 기술이 도입되면서 다양한 비대면 금융 서비스가 등장했다[1]. 온라인 펀드 가입, 온라인 보험 해약, 인터넷전문은행을 통한 대출, MTS(Mobile Trading System)와 같은 서비스가 활성화되었다. 파밍, 카드 위조 등 전자금융 거래의 공격 유형도 다양해졌고[30], 이들은 물리적, 관리적, 기술적 보안 영역과 연결될 수 있다.

5.3 주체별 금융 보안 위협

금융업 관련 주체의 다양화는 보안 취약점 증가에 영향을 준다. 금융업의 보안을 좌우하는 금융 서비스를 둘러싼 이해관계자에 대해 살펴볼 필요가 있다. 서비스의 융합으로 관련 주체는 늘어나고 있다. 가령 스타트업 협업, 오픈 API 개발, 포털 사업자의 금융업 진출 등으로 이해관계자가 다양해졌다. 이에 따라 금융 서비스의 접점이 많아지고, 위협은 증가한다. 따라서 인간적 요인에 초점을 맞추고, 관련 주체를 기준으로 보안 위협을 살펴야 한다.

[29]는 2004년부터 2013년까지 국내 전자금융 관련 사고를 분석하여 위협을 25개로 분류했다. 이 위협을 4가지 측면으로 구분했다. 각 대상별로 보면 이용자 14개, 네트워크 5개, 전자금융 보조업자 1개, 금융회사와 전자금융업자 5개로 나타났고, 이용자 측면의 위협이 가장 많았다.

링크를 클릭하려는 사람의 의지까지 막을 수는 없다. 사회공학 등 인간에 의한 위협은 다양하다. 보안을 위해 기술과 솔루션뿐 아니라 과정과 사람에 주목해야 한다[7]. 기술적으로 워터링 홀, 부채널 공격 등 진화하는 공격에 대응할 방법을 찾는다고 해도 약한 링크인 인간적 요인에서 구멍이 뚫릴 수 있다. 이해관계자는 다양해지고 있지만 금융회사, 협력회사, 금융소비자, 정책 입안자로 한정하여 살펴보겠다.

5.3.1 금융회사

금융회사는 일반적으로 본사와 지사, 지점의 조직으로 구성되어 있다. 고객을 직접 대면하는 지점, 기획과 금융 서비스 출시, IT, 보안 업무 담당자 등 여러 이해관계자가 있다. 이때 금융회사의 보안에 영향을 미치는 인간적 요소에 주목해야 한다. 2011년 H카드사의 내부 직원이 이메일로 9만 7천 건의 고객 정보를 유출했다[8]. 내부자 위협의 증가는 인식 교육, 데이터 보호 전략이나 솔루션의 부족에 기인한다는 입장이 있다[31]. 내부자 공격에서 비관리자보다 관리자에 의한 사고 비율이 높고, 80%인 비기술적인 공격이 8%인 기술적인 공격보다 높은 비율을 차지했다는 SEI의 2012년 조사 결과가 있다. 또한 내부자에 의한 정보 유출 비율이 금융 분야에서 높고, 내부자와 파트너를 더하면 외부자에 의한 정보 유출 비율보다 높게 나타났다는 Verizon의 2008년 조사 결과도 있다[30].

H카드사 사례와 달리 비의도적이지만 부주의, 판단 착오에 의한 보안 사고가 있다. 또한 특정 직원이 타깃이 되어 공격을 당하는 경우도 있다. 접근 권한이 있는 내부 직원은 항상 잠재적인 위협에 있다. 사이버 보안에서 인간 행동에 관한 한 연구에서는 "사람의 행동은 일관성이 없고, 관계에 의해 강하게 영향을 받는다."라고 했다. 시간 절약과 편리함을 위해 패스워드를 공유하고, 바이러스 검사를 하지 않은 상태로 이메일 첨부 파일을 열람한다는 것이다[31]. 조직 구성원 중 시스템 운영자 측면에서 보면 시스템 운영자 또한 인간이고 실수할 가능성이 있다. 시스템 운영자의 잘못된 시스템 구현으로도 보안 문제를 야기할 수 있다.

금융기관은 다양한 로그인 방식을 제공하고, 인증 DB 암호화 등 보안 강화를 위한 대응을 했다[32]. 한편 공인인증서 폐지가 언급되고 있고, 핀테크 혁신으로 간편 인증이 확산되었다. 그러나 복잡도가 낮은 비밀번호 사용의 경우 무작위 대입 공격(Brute Force Attack)이라는 위협이 있고[32], 실제로 해당 공격이 발생한 사례가 있다. 금융 서비스 기획자는 새로운 서비스를 도입할 때 금융업의 특성과 본질을 잊지 않아야 한다. 보안은 유행이 아니라 기본이다. 이제 모든 부서와 업무가 보안과 연관되어 있다. 각 업무 담당자는 의도적인 행동과 비의도적인 실수, 부주의를 경계해야 한다.

5.3.2 협력회사

금융회사의 IT 개발과 운영에서 협력회사와의 협업은 기존부터 이루어졌다. 과거에 비해 은행, 보험, 여신전문, 증권업의 비대면 채널 서비스가 확장되었다. 모바일 금융 플랫폼의 출시 과정에서 수탁사와의 협업은 더욱 활발한 모습을 보이고 있다. 금융회사

못지않게 협력사의 인간적 요소에도 관심을 가져야 한다. 2014년 카드 3사 개인 정보 유출은 외주업체 직원이 카드사 고객 정보에 접근하여 이를 유출한 사건이다. 이 사건을 계기로 외주업체 직원 관리 등 내부 통제의 중요성이 부각되었다[8].

개정된 '금융기관 검사 및 제재에 관한 규정 시행세칙'에 따르면 외주업체의 개인신용정보 등 부당 이용 및 유출은 위탁 금융기관 소속 직원의 행위로 간주된다[8]. 즉, 수탁사 직원의 잘못으로 보안에 허점이 생기는 경우에는 금융회사의 책임과 전체 리스크로 이어진다. 금융회사는 협력회사의 휴먼팩터에도 관심을 가지고, 적합한 협력 파트너 회사를 선별할 수 있어야 한다.

5.3.3 금융소비자

일반적으로 '정보 보호 교육', '보안 정책의 준수'라고 하면 금융회사 임직원의 의무로만 여기는 경향이 있다. 그러나 현재 금융소비자는 서비스를 선택하고, 플랫폼으로 직접 금융 업무를 처리한다. 따라서 가장 약한 링크인 인간적 요인에서 금융소비자라는 주체에도 주목해야 한다. 휴먼팩터에서 고객에 대한 논의의 필요성이 커졌다. 금융회사 임직원의 보안 의식 고취, 금융 시스템 보안 강화로 인해 고객은 타깃이 될 수 있다. 금융회사, 협력회사의 노력만으로는 부족하고, 고객이라는 휴먼팩터에도 관심을 가져야 한다.

Fig. 6은 온라인뱅킹 시스템 공격이라는 최종 공격 목표에 이르기 위해 사회공학, 피싱, 악성코드 등의 공격에서 상위 공격으로 이어지는 공격트리를 보여준다[33]. 금융소비자에 대한 사회공학 공격으로 사회적, 심리적 요인을 이용해 정보를 탈취하는 공격이 있고[30], 이는 공격자의 의도적인 공격이다. 한편 금융소비자가 스스로 취약점을 보이기도 한다. 사용자는 인지력에 스트레스를 받으면 패스워드를 쉽게 구성하는 경향이 있다[7]. 보안카드 내용을 PC에 저장하였고, 이것이 유출되어 공인인증서 재발급이 된 경우도 있다[32]. 이들은 금융소비자의 직·간접적 실수 또는 부주의로 정보가 유출되는 경우이다.

금융소비자에게 금융기관 사이트로 링크된 이메일을 발송하고, 링크 클릭 시 가짜 금융기관 사이트로 유도하여 금융 정보를 유출하는 피싱의 사례를 주위에서 접할 수 있다. 특별히 비용을 들이지 않아도 사람들의 성향, 주의 부족을 이용해 공격이 가능하여 관련 보안 위협이 발생하고 있다[7].

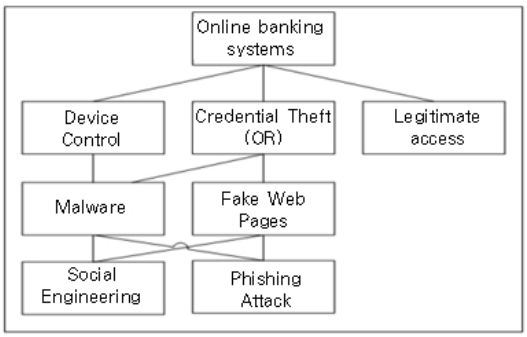

Fig. 6. Attack Tree Model

[9]는 컬럼비아 대학교에서 직원과 학생 4,000명을 대상으로 수행한 피싱 관련 연구이다. 연구자는 2009년의 한 조사 결과 사회공학 공격의 거의 4분의 1이 피싱이었음에 주목했다. 4가지 유형의 이메일을 각각 500개 보내고, 이후 2,000개를 더 보냈다. 연구자는 기업 수준의 피싱 공격 가능성에 대한 측정에 초점을 맞추었고, 사용자의 경우 잠재적인 위협을 인식하도록 훈련받을 수 있다고 했다. 이와 같은 연구를 각 조직에 맞게 활용하고, 금융소비자와 관련된 연구를 수행하여 대안을 마련할 수 있다.

기업과 공공기관의 서비스를 이용하는 과정에서 개인 정보의 주체는 자신의 정보를 의식적, 무의식적으로 제공한다[34]. 그러나 초연결시대에는 서비스를 이용하는 고객의 의무가 지금보다 커질 것이다. 금융업에 신기술이 도입되면 금융소비자에게도 보안에 대한 책임 공유가 필요하다. 신기술을 적용한 금융 서비스 이용에 있어서 고객 접점의 보안 위협이 증가할 것이고, 서비스 이용에는 금융소비자의 동의와 책임도 있다고 보아야 한다. 금융회사 임직원뿐만 아니라 고객의 보안 의식 제고도 중요하다.

5.3.4 정책 입안자

국가의 정보 보호 정책, 각 금융회사의 정보 보호 정책은 제대로 설계되어야 한다. 그런데 정책을 만들고, 운영하는 것은 결국 '사람'이다. 정책을 구현함에 있어 가장 큰 방해 요인도 인간이다. 따라서 정보 보호 정책에 있어서도 휴먼팩터는 중요하다. 보안 정책은 조직의 정보 자산 이용자에게 정보 보호의 필요성을 설명한다. 이는 조직의 비전, 미션, 목적을 지지하고 달성하는 과정에서 정보 보안의 역할을 정의하고, 통제되고 안전한 방식으로 조직을 운영하려는 경

영자의 의지를 반영한다[35].

기술과 정책, 그리고 인간의 관계를 살펴볼 수 있다. 기술은 정책을 변화시키고, 정책은 기술의 활용법과 방향성을 안내한다. 인간에 의해 기술이 발전하고, 인간은 이에 맞게 정책을 개정한다. 기술과 프로세스는 계속 변화하는데 정책이 머물러 있으면 안 된다. 반대로 인간은 정책을 통해 기술의 발전 방향성을 이끈다. 더 나아가 정책에는 미래 기술의 변화가 고려되어야 한다. 즉, 앞으로의 기술 발전과 영향력을 고려한 정책의 선제 대응도 필요하다. 이처럼 기술과 정책의 중심에는 인간이 있고, 결국 본질은 인간이다. 인간은 기술과 정책을 발전시키고, 기술과 정책은 인간의 삶에 영향을 준다.

정책 입안자가 정책을 제대로 설계하지 못하는 것은 위협 요인이다. 가령 암호화 프로토콜이 제대로 설계되지 않은 상황에서 이를 적용하는 경우를 생각해 볼 수 있다. 잘못 설계하면 실행을 해도 문제가 되며 이는 정책에 있어서도 마찬가지다. 보안 정책의 실패는 정보 보호 정책 작성을 위한 기술과 이해의 부족에 기인하기도 한다. 그리고 조직 문화를 반영하지 못하면 조직 내의 보안을 위한 효과적인 지침을 제공하는 정책이 아니다[35]. 보안 정책이 정책의 입안자에 의해 수립되어 이를 준수해야 하는 모든 구성원의 입장을 제대로 반영하지 못하기도 한다[36].

보안 정책 입안자가 주먹구구식의 일관성 없는 정책을 수립하는 것은 보안을 방해하는 요인이다. 정책 그대로만 하면 되도록 설계되지 않은 애매모호한 정책은 관련 주체에게 혼란을 준다. 각 부처의 정보 보호 관련 법률의 요구사항이 다르고, 법규 준수에 대한 혼란이 있다[30]. 구성원이 정책에 대한 공감대를 형성하고, 같은 방향으로 일관성을 가지고 업무를 수행할 수 있도록 하는 정책을 마련해야 한다.

VI. 인간과 인공지능의 역할 및 협업 모델

금융업에 인공지능이 도입되고, 연결이 증가함에 따라 보안 취약성은 증가할 것이다. 물리적, 기술적, 관리적 보안에서 휴먼팩터와 관련된 보안 위협 역시 증가할 것으로 보인다. 신기술은 금융 분야에도 적용되고 그 모습이 구체화될 것이다. 하지만 역발상을 할 수 있다. 피할 수 없는 신기술의 흐름 속에서 AI의 도입으로 보안 위협이 증가하지만 인공지능이라는 기술 자체를 이용해 보안 문제를 해결할 수도 있다. 인간과 인공지능이 각자의 역할을 수행하고, 필요한 경우 협업을 하여 서로의 한계를 보완할 수 있을 것이다. 본 장에서는 인간의 역할(H-H), 인공지능의 역할(A-A), 인간과 인공지능의 협업(H-A)이라는 역할 및 협업 모델을 제시할 것이다.

본 연구와 유사한 관점의 연구가 있다. [37]은 인공지능이 의료, 금융, 교육 분야에서 유용하지만 보안, 프라이버시, 윤리적 측면에서 잠재적인 위험이 있다며 이에 주목한 연구이다. 위험에 대한 대책으로 AI 설계에서 윤리 규칙을 포함하고, 투명하고 설명 가능하며 견고한 AI 시스템을 만들어야 된다고 했다. 연구자는 AI 개발 관련 법, 정책의 강화와 표준의 필요성을 주장했다. 반대로 AI 기술 자체를 활용하여 보안과 프라이버시를 강화할 수 있다고 전망했다. 해당 연구자는 인공지능이 도입되면 발생할 예상 위협들이 있지만 반대로 AI를 통해 보안, 프라이버시 등을 강화할 수 있다는 구조로 연구를 했다.

본 장에서는 인공지능을 약한 인공지능으로 한정할 것이다. 3.1절에 약한 인공지능에 대한 정의가 있다. 약한 AI는 정확하게 생각하거나 행동하는 시스템이고, 인간이 좀 더 엄격하고 엄밀하게 가설을 공식화하고 검증할 수 있게 해준다. 또한 사전에 정의된 규칙과 알고리즘을 이용해 지능을 흉내 내고, 인간 지능의 일부를 구현하며 특정한 조건과 한정된 영역의 문제를 해결한다.

강한 인공지능의 실현 가능성에 대해서 불가능하다는 입장이 있다. 특정 데이터 제공자에 의한 학습 데이터의 부족, 편견 개입과 관련해 AI에 대한 회의적인 시각도 있다. 본 연구는 인공지능의 실현 가능성을 떠나 본 장에서 제시하는 역할 및 협업 모델에서 이와 같은 역할을 수행하는 '기계'를 인공지능이라고 표현할 것이다. 또한 인공지능은 실현될 때까지 침체와 부흥을 반복하며 거론이 될 것이고, 본 장에서는 약한 인공지능의 실현을 가정한다.

6.1 인간의 역할(H-H)

본 절에서는 인간의 역할을 주체별로 살핀다. 신기술 시대에 금융회사, 협력회사, 금융소비자, 정책입안자의 인간적 요소는 중요할 것이다. 인간과 인간 간의 관계와 역할에 주목하여 이를 살펴보겠다.

6.1.1 금융회사

금융회사가 휴먼팩터에 초점을 맞추어 수행할 수

있는 다음과 같은 보안 관련 임무가 있다. 우선 임직원의 보안 교육과 보안 문화의 정립이 있다. [11]은 교육을 통해 인간의 행동에 영향을 주는 태도, 주관적 규범, 지각된 행동 통제라는 3가지 요인을 변화시키는 것과 관련한 연구이다. 해당 연구자는 교육과 훈련을 통해 보안에 대한 사용자의 판단과 지식을 증가시킬 수 있다고 했다.

구성원의 행동을 변화시키고 설득하기 위해 사회심리학적 방법을 활용할 수 있다. 정보 보안 인식이란 구성원이 정보 보안의 사명, 중요성, 적합한 수준, 개인별 보안 책임과 행위에 대해 이해하는 상태이다. 이러한 인식을 갖도록 하여 사용자 관련 사고를 줄일 수 있다[36]. 또한 내부 통제, 정보 파기에 대한 교육을 해야 된다. 이에 대한 성과 측정으로 문제점을 파악하고, 개선안을 마련할 수 있다[34].

금융회사 구성원 간 커뮤니케이션의 부족으로도 보안 문제를 유발할 수 있다. 임직원은 상대방이 이해할 수 있는 용어로 전달을 해야 한다. 협력업체, 고객과의 소통에서도 마찬가지이다. 애매하지 않은 지침, 매뉴얼을 작성하고, 정확하게 전달해야 한다. 각 주체에게 왜, 어떻게 그리고 어디까지 보안을 지켜달라고 할지 설득하고, 공감을 이끌어야 한다.

보안과 관련해 처벌뿐 아니라 인사고과, 상여금에서 보상을 받도록 할 수 있다. 보안도 보상을 받을 수 있는 분야라는 인식이 확산되도록 포상이 이루어져야 한다. 이를 위해 구체적 평가를 할 수 있는 방법을 마련해야 한다. 매슬로우 욕구 단계 이론에 따르면 인간은 일의 능력, 성취 등 자아실현의 욕구와 승진, 직책 등 존경의 욕구, 그리고 연금, 안전한 작업 조건 등 안전의 욕구가 있다. 허즈버그의 2요인 이론에 따르면 성취, 업무를 통한 성장, 승진이라는 동기요인이 있다[38]. 공포소구는 바라는 결과를 얻기 위해 두려움의 요소를 포함한 설득력 있는 수단이다[31]. 이 이론들을 활용하여 보안 관련 보상과 처벌에 관한 금융회사의 방침을 세울 수 있다.

보안은 보안 담당자 혼자만의 문제가 아니다. 이제 보안과 관련 없는 영역을 찾기 어렵다. 예를 들어 고객 정보를 활용하는 마케팅 부서, 법적 위험에 대응하는 법무팀도 보안과 관계가 있다. 이를 고려하여 보안의 경험이 있는 전문가를 배치하고, 인력 양성을 해야 된다. 한편 신기술의 시대에 설계자는 보안을 고려한 설계를 해야 한다. 경영진의 역할도 중요하다. 경영진의 관심은 구성원이 보안에 관심을 갖게 할 수 있다. 규정이라고 하며 충분한 설명 없이 준수를 강요하면 불만을 유발할 수 있다. 인식 교육, 훈련의 효과를 위해서는 설득, 능동적 참여와 같은 조직적 행동이 필요하다. 구성원이 보안 행위를 능동적으로 수행하는 환경을 만들어야 한다[36].

6.1.2 협력회사

협력업체 직원에 대한 교육이 필요하고, 이는 관리적 통제에 해당한다. 외주업체 사고 사례를 공유하고, 수탁회사 직원에 대한 정보 보호 인식 제고를 위한 지원을 해야 된다. 이와 같이 협력회사와 그 직원의 인간적 요소에 대한 보안 통제가 필요하다. 협력사와의 계약부터 해지까지를 관리하고, 위탁회사의 정보 부당 이용 시 위탁 계약을 해지해야 한다[8]. IT 기기 반입과 출입을 철저하게 관리하는 물리적 통제, 방화벽과 망분리와 같은 기술적 통제를 할 수도 있다. 금융회사가 정한 보안 기준에 부합하도록 협력회사의 자체적 노력이 있어야 한다.

6.1.3 금융소비자

금융소비자의 보안 의식 고취가 필요하다. 안전한 전자금융 거래를 위한 사용자 유의 사항을 숙지해야 한다. 또한 인증에서 우수한 안정성의 보안 등급을 가진 보안토큰의 사용은 불편한 것이 아니라 문제 발생 상황을 가정하면 오히려 안전하고 편리한 것이라는 인식을 가져야 된다. 금융소비자도 필요 시 교육을 받고, 보안을 위한 습관을 길러야 한다. 현행법에서는 보안 문제 발생 시 금융회사 임직원에 대한 처벌 규정이 강하다. 앞으로는 관련 주체들의 상황, 고객도 주의를 기울였는지 여부에 따라 금융회사에 대한 처벌 정도를 조절하여 금융회사 이외의 주체들의 보안 실천 의지를 높일 필요가 있다.

6.1.4 정책 입안자

정보 보안 정책은 포괄성, 명확성, 간결성이 있어야 한다. 정책은 모호하지 않고, 읽기 쉬운 용어를 포함하며 명확해야 한다. 또한 현실적이어야 한다. 현실적 요구 사항을 반영할 수 있도록 주기적으로 재검토해야 한다. 이때 정책 입안자가 모든 것을 정하는 것이 아니라 정책을 수립할 때부터 정책을 준수해야 하는 구성원들의 대표자를 참여시켜 현실적인 정책을 수립해야 된다. 정책의 효과를 위해서는 보안

정책의 품질이 보장되어야 한다[36]. 만약 임직원이 정책을 만들고, 개정하는 과정에 참여한다면 정책을 더 잘 받아들일 것이다.

보안 정책은 다양한 사람을 대상으로 한다. 그러므로 정책은 간단하고 이해할 수 있는 정의를 포함해야 한다. 보안 정책은 독립적으로 작성할 수 없고, 관련이 있는 정책, 표준, 절차, 프로세스에 의해 뒷받침된다. 정책은 실제로 구현 및 집행이 가능해야 한다. 이를 위해 정책에서 다양한 용어는 구체적인 비즈니스 환경에 맞게 작성될 필요가 있다. 그리고 정책은 조직의 정보 자산의 모든 사용자에게 전달되어 공감대를 형성해야 한다[35].

처벌 기반 접근법은 구성원의 정책 준수 여부가 처벌에 대한 공포에 의해 결정된다. 반면 훈련 및 교육 기반 접근법은 구성원을 설득하기 위한 것으로 구성원에게 보안 정책의 준수가 중요한 이유를 설명해 준다. 조직 구성원은 보안 정책을 읽을 충분한 시간이 부족하므로 보안 인식 프로그램으로 관련 메시지를 전달할 수 있다[36].

정책 입안자는 일관성 있는 정책을 제시해야 한다. 보안 정책은 구성원이 이것만 지키면 된다는 확신이 들도록 제대로 설계될 필요가 있다. 정부도 일관성 있는 정책으로 디지털 금융 혁신을 이끌어야 한다[1]. 협의의 단기적인 정책이 아닌 장기적이고 포괄적인 광의의 보안 정책이 필요하다[30]. 물론 기술의 변화에 따라 정책은 변한다. 20년 전에 작성된 보안 정책에는 지금보다 전자적인 정보 보안에 대한 언급이 적고, 물리적인 보안 정책에 대한 세부적인 언급이 있다[35]. 그리고 신기술 시대의 정책은 해당 기술을 고려해야 한다. 즉, 시대에 따라 변화하되 큰 틀의 일관성과 방향성을 유지하고, 공감대 형성을 하는 보안 정책이 필요하다.

금융회사, 협력회사, 금융소비자를 고려한 보안 정책이 필요하다. 정보통신망법 등은 금융회사의 부담을 가중시키고 있다[30]. 금융회사 이외의 각 이해당사자를 고려한 정책도 마련해야 된다. 정책의 입안자는 관련된 모든 주체들의 생각과 행동을 바람직한 방향으로 이끌 수 있는 정책을 고안해야 한다.

6.2 인공지능의 역할(A-A)

인공지능 기계와 기계 간의 관계와 역할에 초점을 맞출 수 있다. AI의 상속 및 동기화, 비동기화, AI 보안 위협 대응으로 나누어 살펴본다.

로봇의 행동과 환경을 학습하고, 대용량의 지식을 공유 및 재사용할 수 있는 객체 모델이 있다. 축적된 대용량의 지식으로 서비스를 제공하고 지식을 재사용할 수 있는 것이다[39]. 이와 마찬가지로 인공지능을 객체지향으로 설계하여 앞서 구현한 AI의 상속과 재정의가 가능하다면 효율적일 것이다. AI 간 상속 구조와 동기화의 상황을 가정하겠다.

우선 학습 데이터가 객체지향으로 상속된다면 데이터의 분류, 군집 및 관리가 용이할 것이다. 데이터가 복잡한 경우 그 효용성이 부각될 수 있다. 특정 기능을 갖는 AI를 구현하기 위해 특정 속성을 갖는 AI를 상속하도록 할 수 있다. 인공지능 간의 데이터 실시간 공유와 동기화도 가능할 것이다. 데이터를 매번 인간이 제공하기에 한계가 있기 때문에 이는 유용하다. 이와 같이 객체지향 구조는 기계와 인간에게 효율성을 제공할 것이다.

상위의 인공지능이 여러 인공지능에게 특정 시점에 어떤 역할을 수행하도록 알리거나 작업을 조정할 수 있다. 중요도와 업무의 속성에 따라 분류하여 AI 기계를 그룹화하고, 상위 AI를 중심으로 한 승인 구조를 형성한다. 이 경우 다른 기계에 대한 감시도 수행할 수 있다. 또한 인공지능은 동일한 레벨에 있는 다른 기계와 유기적으로 협업할 수 있다.

인간의 자식은 부모에 의해 습득된 기술과 지식을 상속하지 못한다. 단, 복잡하고 진화된 정서적인 적응력을 소유하게 된다. 반면 AI 복제본은 원본과 동일할 것이다. 몇 년이나 세기를 지나 자랄 필요가 없이 몇 시간, 몇 분 만에 재생산이 가능하다. 즉, 빠른 재생산이 가능하다[40]. 이를 고려하여 시간적 측면에서 보안을 위하여 기계가 수행하기에 더 나은 역할을 찾을 수 있다. 6.3절의 Table 5에 따르면 인간은 상대적으로 시간적인 한계가 있다.

인공지능 기계는 서로 간 위협 정보를 공유할 수 있을 것이다. 예를 들어 M1과 M2라는 두 인공지능은 서로 복제본이고, 같은 역할을 한다. 위험 상황이 발생했고, M1이 이를 감지하여 M2에게 전달할 수 있다. 또한 M1과 M3라는 인공지능은 부모, 자식 관계이고, 특정 분야의 보안 관제를 담당하고 있다. 하나의 인공지능이 위협 정보를 찾아 이를 다른 기계와 공유 및 동기화하여 다른 기계의 불필요한 작업을 줄일 수 있다. 위협 정보를 함께 분석하여 정확성을 높이고, 대응 방안을 마련할 수 있을 것이다.

기밀의 데이터를 다루고, 높은 보안성이 요구되는 작업을 하는 인공지능은 다른 AI와 독립적으로 작동

해야 한다. 이것은 다른 기계와 비동기화 상태이고, 연결과 호환이 되지 않을 것이다. 6.3절의 Table 5에 제시한 것처럼 AI는 데이터 폐기를 통해 메모리를 삭제할 수 있다. 현재 시점에서 인간의 기억을 완전히 제거하기는 어렵다. 기밀의 업무와 관련하여 독립적 AI를 통해 높은 보안성을 확보할 수 있다.

인공지능에는 보안 위협이 있다. 해킹과 같은 외부 공격, AI 자체의 오작동으로 인한 위협 모두 문제이다. 다음과 같은 공격 유형이 있다. 공격자가 업무용 AI의 학습 과정에 잘못된 레이블이 부착된 데이터를 삽입해 시스템이 부정확한 결과를 도출하도록 하는 데이터 중독 공격이 있다. 또한 공격자는 AI를 활용해 기존 공격 방식을 고도화하거나 새로운 공격을 수행한다. 공격에 필요한 지능, 기술에 AI를 활용하여 공격 비용을 감소시키고 대규모 공격을 수행한다. 자동화된 AI로 SW 취약점을 찾아 짧은 시간 동안 대량의 공격을 수행할 수 있다[41]. 이러한 공격에 대응하도록 인공지능은 견고하게 설계되어야 한다. AI는 학습을 통해 공격을 식별할 수 있어야 하고, 위협 상황을 동기화된 인공지능 기계와 공유하고 대응할 수 있다.

6.3 인간과 인공지능의 협업(H-A)

기술과 사람은 상호 보완적이다[10]. 금융 보안에는 휴먼팩터와 관련된 위협이 있고, 보안과 관련하여 인간은 불완전하며 한계가 있다. 이 경우 인공지능 기술을 통해 보완할 수 있는 부분이 있다. 한편 인공지능은 기계이고, 기계의 고장은 치명적인 사고를 초래할 수 있다[42]. 비행기, 우주선, 자동차와 같은 기계는 완벽하지 않다. 기계는 전력을 필요로 하고, 기계에 결함이 있을 수 있기 때문에 인간이 보완해야 될 점이 있다. 즉, 보안에서 휴먼팩터의 문제점을 AI로 보완하고, AI의 문제점을 인간이 보완하며 상호 협력을 할 수 있다.

하버드대 심리학과 교수 하워드 가드너는 인간은 8가지 다중지능을 가지고, 이 지능들은 상호 협력한다는 다중지능 이론을 주장했다. 또한 인간은 경험, 창조성, 윤리, 의지 등 고급 인지 능력이 있다고 했다. 인간의 다중지능을 넘어서는 기계 대신에 특정 영역의 지능을 특화해 인간의 의사 결정과 지식 노동을 돕는 기계의 등장에 대한 예상이 있다[43].

Table 5에서 인간과 인공지능의 특징과 한계를 비교하였다. 인공지능은 약한 AI와 강한 AI로 나누었다. 이는 3.1절의 인공지능 정의에서 Table 1을 참고하여 확장한 것이다. Table 5는 인간과 인공지능의 협업 모델에 활용하기 위한 것이다.

3.1절에 따르면 약한 AI는 특정 분야의 작업을 정확하게 수행한다. 즉, 엄밀하고 정확한 영역을 학습하여 흉내를 낸다. 3.1절에서 약한 인공지능은 'Humanly'와 거리가 먼 것으로 간주되었다. 반대로 강한 AI는 자아, 감정을 가지기 때문에 보안에서 휴먼에러와 유사한 문제를 초래할 수 있다. 강한 AI는 전력과 학습 데이터를 필요로 하고, 데이터 즉, 기억도 삭제할 수 있다는 점에서 인간과 차이가 있다. 본 절에서는 인공지능을 약한 AI로 한정한다. 또한 금융 보안이라는 공동의 목표를 위해 인간과 AI라는 요소가 서로 한계를 보완하며 상호 작용하는 시스템적 접근의 방안을 제안한다.

6.3.1 객관성과 주관성

사람의 행동은 일관성이 부족하고, 관계에 의해 영향을 받는다[31]. 약한 인공지능은 주관성을 배제하고, 객관적인 판단을 하는 기계이다. 고객이 서류를 갖춘 상태에서 금융 업무, 온라인 송부 및 검증을 할 때 기계가 인간보다 더 객관적이고, 정확할 수 있다. 동일한 상황에서 인간은 감정이나 긴급함에 따라 잘못된 결정을 내릴 수 있다. 반면 인공지능은 감정에 휘둘리지 않고 체계적이고 일관성 있는 결정을 할

Table 5. Comparison of Human, Weak AI, Strong AI

Division	Human	Weak AI	Strong AI
Charact eristic	· Emotion, Ego, Subjective, Objective · Difficulty of complete elimination of memory, experience, and knowledge	· Strict, Accurate, Objective	· Emotion, Ego, Subjective, Objective
		· Needs learning data · Possible to delete learning contents and memory through data or machine disposal	
Limit	· Careless, Mistake · Time limit	· Power Requirement, Machine Life · External attack, hacking · Machine defect, malfunction	

수 있다[20].

Table 5에 따르면 인간은 주관적, 객관적 판단을 하고, 약한 인공지능은 객관적 판단을 한다. 인간이 객관적, 이성적으로 판단하려고 해도 주관이 개입될 수 있다. 인간의 주관적 가치가 개입되어 발생하는 보안 위협을 약한 AI의 객관성을 활용해 보완할 수 있다. 객관과 주관의 차이는 각각 사실과 의견이라는 점이다. Table 6에 객관성과 주관성을 비교하였다[44]. 금융에서 객관적이고, 공정한 판단이 필요한 업무에는 약한 AI를 활용하고, 유연성과 경험이 필요한 경우 인간이 참여하여 협업할 수 있다.

Table 6. Objectivity vs. Subjectivity

Objectivity	Subjectivity
· Fact · Unbiased, balanced · Not influenced by experience · Proof through mathematical calculations or facts · Important when making rational decisions · Supported by clear data	· Opinion · Prejudice intervention possible · Affected by experience, characteristics · Difficult proof through specific facts or figures · Related to emotion · Reflect perspective and temporary

사람의 부주의와 판단 착오는 문제를 야기할 수 있다. 이와 관련하여 4.2절의 휴먼팩터 이론에서 살펴본 인간의 불완전한 행동을 고려할 필요가 있다. 의도하지 않았지만 사회공학 등 외부 공격으로 인한 휴먼에러, 감정이나 금전적 유혹으로 의도를 가지고 행한 문제 상황이 있다. 또한 인간이 정확하고, 객관성과 일관성이 있는 판단을 하는 데 실패하는 경우가 있다. 그러므로 객관적인 기계를 활용하여 인간적 요인으로 인한 문제를 보완할 수 있다.

금융업의 경우 트레이딩, 자산관리 등에서 인공지능의 접목이 기대된다[15]. 양질의 데이터를 기반으로 인공지능은 객관성, 일관성이 있는 판단을 할 수 있을 것이다. 약한 AI의 정밀함과 객관성은 명확한 매뉴얼의 업무, 최적 상품 추천, 신용평가 등에서 활용할 수 있다. 물론 대출 고객의 상환 의지는 상담 과정에서 인간의 융통성, 경험, 직관을 통해 파악하는 것이 더 나을 수 있다. AI를 통해 인간의 주관적 판단으로 인한 금융 사고, 보안 문제를 방지하고, 인간이 AI를 보완하기도 하며 상호 협력할 수 있다.

6.3.2 보안 관제, 통제, 모니터링

이상 징후와 침입 탐지 업무 경험이 있는 인간의 유연한 대응과 의사 결정은 중요하다. AI의 과거 데이터를 활용한 미래 위협 예측은 인간의 경험, 직관을 통한 예측에 비해 부족한 측면이 있다. 한편 인간의 편향적 사고와 편리함 추구, 시간적 한계라는 휴먼팩터를 고려하여 금융 보안에서 AI를 활용할 수 있다. 기계의 정확성과 사람에 비해 시간적 제약이 덜하다는 강점을 인간의 유연성과 결합해 시너지 효과를 낼 수 있다.

인공지능은 지능적 위협 탐지, 분석, 대응과 향후 발생 가능한 보안 위협을 예측하는 데 활용 가능하다. APT 공격은 장기간의 지속적인 데이터 수집과 내부 감염을 통해 수행되기에 지속적인 모니터링이 필요하다. 직원의 개인 정보 오남용 모니터링을 인간이 장시간 수행하기에 한계가 있다. 24시간 분석과 모니터링을 위한 인공지능의 활용이 가능할 것이다. AI는 보안 모니터링 담당 직원의 업무 행위에 대해 그 특성을 분석하고 학습할 수 있다[20]. 한편 AI는 악성코드 리스트와 영향의 정도를 인간에게 제공할 수도 있다. 인공지능은 최신 트랜드를 반영하고, 자동적인 업데이트가 가능해야 한다. 이와 같이 AI는 효율적 보안 시스템을 제공할 것이다[13].

금융ISAC에 의하면 금융회사로부터 수집한 침해 데이터 탐지 건수는 2017년 3월 기준 매월 약 85만 건이었다[20]. 금융권에 FDS(Fraud Detection System)를 도입할 필요가 있고, 국내외 활용 사례가 있다. Paypal은 딥러닝 기반 FDS에 고객의 금융 거래 정보를 학습시켜 사기 탐지를 수행했다. 한국스마트카드의 경우 딥러닝 기반 FDS를 구축하여 이상 거래 탐지를 했다. 그러나 시스템 오류를 이상 거래로 탐지하는 등 오탐이 발견되었다[45]. 해당 분야의 지속적인 기술 개선이 필요해 보인다.

인간과 인공지능이 협업하여 기계의 긍정 오류(False Positive)를 줄인 연구 사례가 있다. 긍정 오류는 위협이 아닌 것을 위협으로 식별하는 것이다. 우선 기계는 비지도 학습의 머신러닝을 이용하여 선별한 비정상적 이벤트를 분석가에게 보낸다. 그 후 분석가로부터 실제 공격이 무엇인지 라벨링을 한 피드백을 받는다. 이 피드백으로 지도 학습을 한다. 해당 과정을 반복한 결과 기계 예측의 정확성이 점차

개선되었다[46]. 이는 인간 분석가의 경험, 직관을 기계 학습에 결합하여 기술적으로 성과가 있음을 보여주는 의미 있는 연구이다.

보안에서 AI는 기존 사건을 기반으로 비정상적 거래의 특성을 유추하고, 패턴을 찾도록 구현해야 한다[20]. 신기술 시대에는 보안 문제로 인한 피해가 가상의 공간을 넘어 물리적 세계로 확장된다. 공격이 정교화되고 있고, 보안 위협을 인간이 모두 대응하기에는 한계가 있다. 사람이 직접 확인하고 방어하면 대응이 늦어질 수 있다. AI가 규칙에 의존하지 않는 공격의 특징을 도출하면 기존에 알려지지 않은 공격에도 대응 가능할 것이다. 새로운 유형의 공격에도 AI와 인간이 협력하여 대응해야 한다.

보안에 있어 예방이 사후 대응보다 낫다[10]. 그런데 금융 보안에서 탐지적, 교정적 통제 역시 중요하다. 제4장의 휴먼팩터 관련 도미노 모델, 스위스 치즈 모델에서 보았듯이 어느 하나에 허점이 생기면 전체의 보안 위험으로 이어진다. 입구와 출구뿐만 아니라 금융 서비스와 관련한 전체 과정에서 보안을 유지해야 한다. 취약점은 잠복해 있다가 어느 순간에 나타날 수 있기 때문에 실시간 감시와 대응이 필요하다. 그러나 인력과 시간은 한정되어 있고, 이때 인공지능을 활용할 수 있다.

6.3.3 레그테크

레그테크(RegTech)는 규제(Regulation)와 기술(Technology)의 합성어이고, IT를 활용해 컴플라이언스 업무를 효율화하는 기술이다. 예를 들어 금융회사와 감독기관의 규제, 투자, 금융시장 위험 정보를 수집하고, 이 데이터를 분석하여 규제 준수, 위험 예측, 이상 거래 여부 파악을 한다. 이 과정에서 인공지능과 같은 신기술을 활용하여 규제 업무를 자동화할 수 있다[41]. 즉, 레그테크는 금융회사가 금융 당국의 각종 법률 규제에 대응하여 규제 준수 수준을 향상시키기 위하여 신기술 활용을 통해 규제에 대응하는 것이다[20].

영국, 호주, 싱가포르는 금융 당국 주도로 레그테크 활성화를 위한 행사를 개최하고, 레그테크 프로젝트를 진행하고 있다. 미국 및 유럽은 규제 이슈로 관련 수요가 크고, 레그테크 업체가 증가하고 있다. 특히 유럽은 GDPR 적용 등으로 레그테크를 활용한 규제 준수의 자동화 필요성이 부각되었다[41].

레그테크는 금융소비자 보호와 통제 비용 감축, 내부 통제 기능 강화를 위한 것이다[20]. 내부 통제의 허점은 인간의 역할 수행 미흡, 윤리 의식 결여 등 휴먼팩터에 기인한다. 인공지능을 활용하여 복잡하게 변화하는 규제에 즉시 대응할 수 있을 것이다. AI를 활용한 레그테크는 장기간의 내부 통제 인력 양성에 비해 효율적일 수 있다. 규제, 컴플라이언스의 빈틈은 보안 문제와 직결된다. 내부 통제에서 문제가 되는 부분에 AI 기술을 우선 도입하여 문제를 줄여나갈 수 있다. 물론 레그테크 구축에 외부 업체가 참여하기도 할 것이고, 그 구축 과정에서의 휴먼팩터에도 관심을 가져야 한다. 인간은 레그테크에 신기술을 활용하는 동시에 레그테크 도입과 운영의 과정에서 발생 가능한 보안 위협을 경계해야 한다.

6.3.4 인증, 승인 단계 강화

사용자가 웹 브라우저의 반복적 보안 경고 메시지에 매번 확인 버튼을 클릭하면 중요한 설정 시에도 확인 버튼을 클릭하는 경우가 있다[7]. 5.3절에서 패스워드 공유, 바이러스 검사를 하지 않은 이메일 열람, 다소 쉬운 패스워드 구성에 대해 제시했다. 상위 결재자의 허술한 승인으로 인한 문제도 있다. 이 문제들의 원인은 부주의와 같은 불완전한 행동, 즉 휴먼팩터이다. 보안 교육 등으로 금융 관련 주체는 편리함 추구의 이익보다 보안 위협 발생 시 손실이 크다는 것을 알고 있다. 그러나 현실에서는 여전히 휴먼팩터와 관련한 보안 취약성이 나타나고 있다.

인공지능을 투입하여 2단계의 인증과 승인 구조로 보안을 강화할 수 있다. 우선 필요한 순간에 AI가 보안을 상기시킨다. 중요한 설정이나 정보에 접근할 때 이에 대한 접근자의 책임을 알려주는 문구를 보여주고, 이에 서명하며 동의 버튼을 클릭해야 접근을 허락한다. 패스워드 설정 시 쉬운 비밀번호 사용은 지양할 것을 안내한다. 공포소구 이론을 활용해 위협을 알리고 대응 방안을 권고하는 것이다[47]. 이메일 열람 시 바이러스 검사를 했는지를 AI가 확인하고, 열람을 승인할 수도 있다.

직접적인 업무 효율성을 제공하는 기술과 달리 보안 기술은 사용자에게 보안 위협을 막아주는 간접적 효익을 제공한다. 사용자는 보안 기술에 대해 귀찮음을 느낄 수 있다[47]. 인간이 편리함을 위해 승인 구조를 단순화하거나 허술하게 승인하는 행위를 승인 담당 AI를 통해 보완 할 수 있다. AI를 활용한 승인과 인증 구조는 유용할 것이다. 나아가 인공지능 기

술이 활성화되면 AI의 요청을 승인하는 상위의 AI를 두어 AI에 의한 오류를 한 번 더 막을 수 있다.

6.3.5 학습 데이터 및 AI 관리

인간은 학습 데이터의 수집과 선별, 운영, 폐기까지 관리를 해야 하고, 이는 인간이 AI를 보완해야 되는 측면이다. 금융 데이터는 학습에 대한 동의가 필요하거나 익명 처리 후 활용이 가능한 경우가 있다. 음성 인식 기술은 발전하고 있지만 국가별로 언어가 다르고, 각 언어도 시대에 따라 변한다. 국가, 문화, 산업에 따라 학습 데이터에 차이가 있다. 담당자는 양질의 데이터를 확보하고, 정제된 데이터를 주입하기 위해 관련 전문 지식을 습득해야 한다.

금융 보안에서 AI를 활용하기 위해서는 정확한 데이터를 입력해야 한다. 또한 운영 과정에서 업무 매뉴얼 개정 시 변경된 내용으로 학습 데이터를 업데이트하여 제공해야 한다. 6.2절에 제시한 기밀의 업무를 담당하는 AI의 경우 독립적이고, 접근이 어렵다. 그 AI가 저장하고 있는 내용을 삭제해야 할 때 인간은 해당 데이터 폐기를 엄격하게 해야 된다.

6.3.1항에서 약한 AI의 객관성과 관련하여 개선할 부분이 있다. 인간이 설계한 알고리즘과 학습 데이터가 반영된 AI가 정말 객관적일 수 있는지의 문제이다. 담당자의 편견과 주관성, 가치관을 배제한 공정한 알고리즘 설계가 어려운 경우가 있다. 알고리즘은 기획자, 설계자, 개발자 등 이를 만든 사람에 따라 다를 수 있다. 기계와의 상호 작용, AI의 이용 주체에 따른 수정 가능성도 있다. 휴먼팩터의 한계를 보완하기 위해 활용할 AI는 객관적이고 편향적이지 않도록 설계해야 한다.

한편 학습 데이터를 제공하는 사람의 실력이 AI에 반영될 수 있다. [48]은 'good'이라는 영단어가 문장에 따라 주관적, 객관적 의미로 쓰이는 사례를 제시했다. 'good'이 항상 감정과 관련된 주관적 단어라고 판단하는 것은 오류임을 보여준다. 6.3.1항과 관련하여 인공지능에 객관적인 데이터를 주입할 때 담당자는 객관적, 주관적인 문장과 용어를 구분해야 한다. 또한 인간 전문가는 AI 활용 시 6.2절에 제시한 데이터 중독 공격과 같은 문제를 경계해야 한다.

인공지능의 담당 업무, 버전 등에 대한 관리와 통제가 필요할 것이다. AI의 제조와 도입 시기, 생애주기를 관리해야 한다. 필요 시 대시보드로 인공지능의 운영 현황과 상태를 모니터링할 수 있다. 대시보드를 통해 AI의 예상치 못한 동작이 포착되면 인간이 해당 AI를 제어할 수 있어야 한다. AI 알고리즘을 주기적으로 평가하여 최적의 알고리즘이 설계되고 운영될 수 있도록 해야 한다.

6.4 인간과 인공지능의 역할 및 협업 최종 모델

금융 보안에서 인간과 인공지능 기계는 서로의 한계를 보완하며 협업할 수 있다. Fig. 7은 인간과 AI의 상호 작용 구조이다. 금융회사가 인간과 AI의 협업을 위해서 수행할 일련의 과정이 있다. 금융회사의 업무와 서비스 채널, 당면한 보안 위협을 분류하고, 관련된 이해관계자를 추출한다. 금융 업무 중 협업이 필요한 업무를 선별하고, 인간과 인공지능이 각각 더 잘 수행할 수 있는 업무로 나눈다. 객관적, 주관적 영역으로도 구분한다. 인간과 인공지능의 특징과 장단점, 역할을 파악하고 서로의 한계를 보완하도록 모델 설계를 해야 한다. Fig. 7을 확장하여 Fig. 8에는 인간과 AI의 역할 및 협업 모델을 도식화하였다.

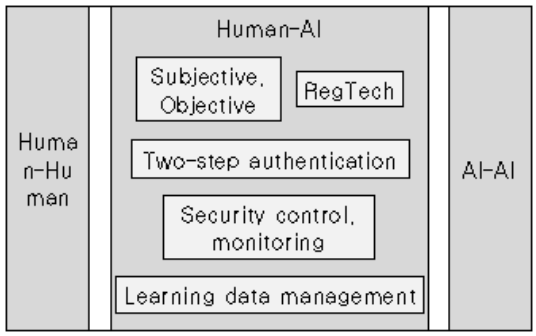

Fig. 7. Interaction between Human and AI

VII. 인공지능 활용 시 고려 사항

금융회사에서 인공지능을 활용할 때 다음과 같은 사항을 고려해야 한다. 금융권에 인공지능 도입 시 5가지 평가 기준을 [1]과 [49]를 활용하여 Table 7에 제시하였다. 무결성, 가용성, 기밀성은 기본이고, 요구사항 5가지로 CARRS 평가 기준을 제안한다. 한편 AI 기술 실현에 대비하여 인공지능 폐기와 같은 윤리적 문제에 대한 논의가 이루어지고 있다. 또한 인공지능 분야에 대한 국제적인 표준화 활동이 진행 중이다. 인공지능의 안전 요구 사항과 보안 가이드라인도 필요하다[49].

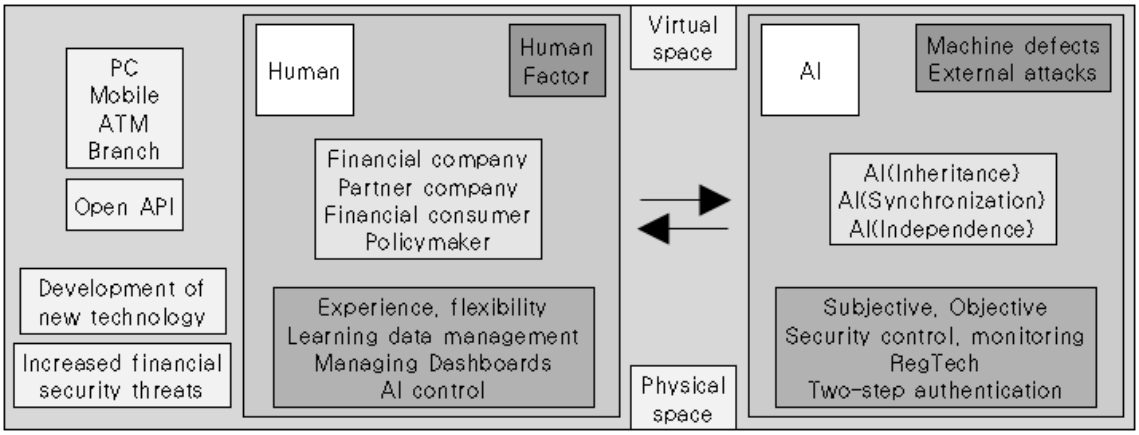

Fig. 8. Role and Collaboration Model of Human and Artificial Intelligence

Table 7. Five criteria for the introduction of Artificial Intelligence

Division	Content
Cooperation	Human and machine complement each other's weaknesses and increase efficiency
Autonomy	Self-diagnostics detect vulnerabilities or defects and take self-measures
Reliability	Associated with the issue of explainability and transparency
Resilience	Ability to recover from security threats
Safety	Safety of artificial intelligence requires high standard design and verification

VIII. 결 론

본 연구의 결과는 인공지능의 실현을 가정할 경우 금융 보안을 위해 인간과 인공지능이 상호 협력할 수 있다는 것이다. 금융업과 IT는 함께 발전해왔고, 금융 비대면 채널이 활성화되었다. 이와 함께 보안 위협은 진화하고 있고, 금융 보안에서 인간적 요인으로 인한 취약성이 나타나고 있다. 이는 사물인터넷, 인공지능의 신기술 도입이 본격화되면 더욱 심화되고, 사이버와 현실 세계에서 나타날 것이다.

위협에 대한 대안으로 인간과 인공지능의 역할 및 협업 모델을 제안하였다. 이를 위해 사전에 인공지능의 정의와 역사, 시장 규모, 기술에 대해 논하고, 휴먼팩터 관련 이론을 제시했다. 또한 인간, 약한 AI, 강한 AI를 비교하고, 본 연구에서 인공지능은 약한 AI로 한정하였다. 금융 서비스 채널과 주체가 다양해졌고, 이들 각각을 기준으로 위협을 분류했다. PC, 스마트폰, ATM 등 채널과 금융회사, 협력회사, 금융소비자, 정책 입안자의 주체별 위협을 보면 휴먼팩터와 연관이 있다.

인간과 인공지능의 역할 및 협업 모델을 크게 3가지로 구성하였다. 3가지는 인간의 역할(H-H), 인공지능의 역할(A-A), 인간과 인공지능의 협업(H-A)이다. H-H 모델에서는 금융회사 등 주체별로 위협요인을 극복하기 위한 인간의 역할을 기술했다. A-A 모델에서는 상속, 동기화, 독립성 유지, 공격대응 등 인공지능 기계의 역할을 기술했다. H-A 모델에서는 인간과 인공지능의 협업을 제시했다. 이를 객관과 주관적 업무, 관제와 모니터링, 레크테크, 2단계 인증과 승인, 학습 데이터 및 대시보드 관리로 나누어 구성했다. 인공지능 활용 시 고려할 사항에 대해서도 언급하였다.

본 연구의 한계점은 인공지능의 실현을 가정했기 때문에 실제 상황과 현실적 문제를 반영하지 못하는 측면이 있다는 것이다. 또한 역할 및 협업 모델을 도출한 과정과 근거를 제시하였지만 그에 대한 실증적인 입증에는 한계가 있었다. 본 연구의 의의는 AI 기술의 실현은 불분명하지만 이에 대한 사전 논의와 대응을 한다는 것이다. 또한 근본적인 것에 대해 상기시켰다는 의의가 있다. 기계를 만들고 활용하는 주체는 사람이다. 결국 본질은 인간이고, 인간에 대한 이해가 필요하다. AI 논문과 특허의 수에서 한국은 열위에 있다. 본 논문은 활발하게 진행 중인 인공지능 분야의 연구에 참여를 했다는 의의도 있다.

신기술 시대에는 복잡성이 증가하고, 위협의 원인도 한 가지로 설명하기 어렵다. 기술, 인증이 완벽해도 금융 보안에서 휴먼팩터가 문제가 될 수 있다. 한편으로는 부족한 기술을 사람이 보완할 수 있다. 신기술로 위험이 증가하지만 기술의 변화에는 적응해야 한다. 본 논문에서 제시하는 발전 방향은 기술을 받아들이면서 증가하는 위협 또한 AI로 보완하는 것이다. 물론 AI가 아니더라도 인간의 주관성과 시간적 한계를 보완할 수 있는 기계를 고안할 수 있고, 이와 같이 해결책을 찾으려는 시도는 의미가 있다. 앞으로의 연구 과제는 진정한 AI 구현이 가까워지면 그 시대에 맞게 현실적이고 구체적인 연구를 하는 것이다.

인공지능은 그 기술 실현의 확실한 시기를 알 수 없어도 시장의 흐름을 바꾸었다는 의미가 있다. 이에 대한 투자와 관심이 증가하고, AI 연구와 함께 음성인식 등 기술이 발전했다. AI에 대한 지나친 과열 양상과 막연한 낙관론을 경계하는 동시에 AI에 대한 공포심 유발과 무조건적인 비판론은 설득해야 한다.

각 산업에서 신성장 동력으로 간주되는 인공지능이 패러다임 전환일지 아니면 일시적 유행일지는 알 수 없다. 분명한 것은 부흥기와 침체기를 더 반복할 수 있지만 AI는 실현될 때까지 학계와 산업계의 목표 중 하나이며 그 논의는 계속될 것이라는 점이다. 따라서 신기술 시대에 금융회사는 시대에 맞게 수정 가능하되 일관성이 있는 기술 및 보안 전략을 마련해야 한다. 본 연구에서 제안한 인간과 인공지능의 역할 및 협업 모델처럼 인간과 인공지능은 상생의 방향으로 나아가야 한다.

References

[1] Bank of Korea's Financial Settlement Bureau, "The Future of Digital Innovation and Financial Services: Challenges," Payment Survey 2017-1, Jan. 2017.

[2] Financial Services Commission, "Notification No. 2015-18," Notification of Financial Services Commission, Jun. 2015.

[3] Stuart J. Russell and Peter Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall, 1995.

[4] Sung-il Ryu, "Artificial intelligence leading the fourth industrial revolution: Focusing on deep learning," DIGIECO REPORT Issue&Trend, Apr. 2017.

[5] Bank of Korea, "Domestic Internet banking service usage in the second quarter of 2016," Press Release No. 2016-8-6, Aug. 2016.

[6] Reza Alavi, "A Risk-Driven Investment Model for Analysing Human Factors in Information Security," Ph.D.Thesis, UNIVERSITY OF EAST LONDON, 2016.

[7] Su-mi Lee, "How Human Factors Affect Security," Financial Security Institute Issue Report, Vol. 2011-009, Jun. 2011.

[8] Financial Security Institute, "E-FINANCE AND FINANCIAL SECURITY," e-finance and financial security No. 2, Oct. 2015.

[9] Brian M. Bowen, Ramaswamy Devarajan, and Salvatore Stolfo, "Measuring the Human Factor of Cyber Security," IEEE International Conference on Technologies for HST, pp. 230-235, Nov. 2011.

[10] Gary Hinson, "Human factors in information security," White paper of IsecT Ltd, 2003.

[11] Kun-woo Kim, Myeong-gyun Song, and Jung-duk Kim, "A Research on Security Education Framework for Employee's Behavior Change," International Journal of Information and Education Technology, Vol. 8, No. 1, Jan. 2018.

[12] Sizwe M. Dhlamini, Michael O. Kachienga, T. Marwala, and Members, "Artificial Intelligence as an Aide in Management of Security Technology," IEEE Africon 2007, Massachusetts Institute of Technology, pp. 1-5, 2007.

〔13〕 Madhavi Dhingra, Manisha Jain, and Rakesh Singh Jadon, "Role of artificial intelligence in enterprise information security: A review," 2016 Fourth International Conference on PDGC, pp. 188-191, 2016.
〔14〕 Hyun-cheol Choi, Sun-yong Byun, Hyung-ju Kim, and Jin-kyu Jeong, "The Study on Logic of Designing and Ethical Programming the Behavior of AMA Robot 1," Ethics Education Research 46th, pp. 65-91, Oct. 2017.
〔15〕 Financial Security Institute, "Domestic and foreign artificial intelligence related policies and R & D trends," Security Research Department-2016-058, Dec. 2016.
〔16〕 Nils J. Nilsson, THE QUEST FOR ARTIFICIAL INTELLIGENCE: A HISTORY OF IDEAS AND ACHIEVEMENTS, Cambridge University Press, Sep. 2009.
〔17〕 John R. Searle, "MINDS, BRAINS, AND PROGRAMS," Behavioral and Brain Sciences, 1980.
〔18〕 Korea Meteorological Administration, "Utilizing meteorological fields with artificial intelligence," Weather Technology Policy Paper, 9(2), Dec. 2016.
〔19〕 Sang-soo Lee, "4th Industrial Revolution, What is Artificial Intelligence?," Education Union News, Jan. 2018.
〔20〕 Financial Security Institute, "E-FINANCE AND FINANCIAL SECURITY," e-finance and financial security No. 8, Apr. 2017.
〔21〕 MSIT and KISTEP, "Book 2 Artificial Intelligence Technology," 2015 Technology Impact Assessment, Jan. 2016.
〔22〕 Young-il Kong, Hyung-suk Choo, and Kyung-bok Lee, "China, the dominant partner of artificial intelligence," SPRi Issue Report No. 2017-005, Oct. 2017.
〔23〕 Hye-jung Shim and Kun-woo Kim, "Business model that utilizes AI of our enterprise," KITA Report, Jan. 2018.
〔24〕 Doopedia, "human factor" http://www.doopedia.co.kr/doopedia/master/master.do?_method=view&MAS_IDX=101013000774253, 2018.
〔25〕 Zahid H. Qureshi, "A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems," Defence Science and Technology Organisation, Jan. 2008.
〔26〕 Scott A. Shappell and Douglas A. Wiegmann, "The Human Factors Analysis and Classification System-HFACS," U.S. Department of Transportation, Feb. 2000.
〔27〕 Geun-hye Song and Seung-min Lee, "Fourth Industrial Revolution and Security Paradigm Shift," IITP Weekly ICT Trends No. 1847, May. 2018.
〔28〕 Su-jin Lee, Sang-Yong Choi, Jae-Kyoung Kim, Chung-shick Oh, and Chang-ho Seo, "A Study for Limitations and Improvement of Information Security Management System," Journal of Digital Convergence, pp. 563-570, Feb. 2014.
〔29〕 Kang-yoo Cho, Sang-sik Min, and Jae-mo Sung, "Promotion plan of countermeasure technology research related to electronic financial security threat," korea institute of information security & cryptology, pp. 49-53, Dec. 2013.
〔30〕 Financial Security Institute, "Analysis of major countries for electronic finance policy and supervision advancement," Financial Security Institute Report, Nov. 2012.
〔31〕 Mark Evans, Leandros A. Maglaras, Ying He, and Helge Janicke, "Human

Behaviour as an aspect of Cyber Security Assurance," Security and Communication Networks, 2016.
[32] Jung-ho Lee, "Measures to Prevent and Respond to Electronic Financial Infringement Accidents," korea institute of information security & cryptology, pp. 1-20, Oct. 2008.
[33] Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus, and Rafael Timóteo de Sousa Jr, "A FORMAL CLASSIFICATION OF INTERNET BANKING ATTACKS AND VULNERABILITIES," IJCSIT, Vol. 3, No. 1, pp. 186-197, Feb. 2011.
[34] Dae-kyung Jung, "Comparative study of the privacy information protection policy: Privacy information basic laws and dedicated organizations," korea institute of information security & cryptology, pp. 923-939, Aug. 2012.
[35] Karin Hone and J.H.P. Eloff, "Information security policy: what do international information security standards say?," Computers & Security, pp. 402-409, 2002.
[36] Myung-seong Yim, Tae-seog Jeong, and Jung-min Lee, "A Suggestion for Information Security Awareness of Finance Firms," Journal of Security Engineering, 11(6), pp. 479-498, Dec. 2014.
[37] Xiuquan Li and Tao Zhang, "An Exploration on Artificial Intelligence Application: From Security, Privacy and Ethic Perspective," IEEE ICCCBDA, pp. 416-420, 2017.
[38] Zeynep Ozguner and Mert Ozguner, "A Managerial Point of View on the Relationship between of Maslow's Hierarchy of Needs and Herzberg's Dual Factor Theory," International Journal of Business and Social Science, Vol. 5, No. 7, Jun. 2014.
[39] Chun-soo Park, Min-soo Jang, Dong-wook Lee and Jae-hong Kim, "Cognition·Expression Technology Trend for Human and Robot Interaction," Electronics and Telecommunications Trends, 28th issue, No. 4, pp. 86-96, Aug. 2013.
[40] Nick Bostrom and Eliezer Yudkowsky, "The ethics of artificial intelligence," The Cambridge Handbook of Artificial Intelligence, Cambridge University Press, pp. 316-334, 2014.
[41] Financial Security Institute, "E-FINANCE AND FINANCIAL SECURITY," e-finance and financial security No. 13, Jul. 2018.
[42] IEC Future Factory Project team, "Factory of the future," IEC White Paper, pp. 214-285, 2015.
[43] Hyun-ki Kim, "Exobrain: Language intelligence SW for communication of human and machine knowledge," https://www.etri.re.kr/webzine/20160318/05.html, ETRI webzine, Vol.58, Mar. 2016.
[44] Justice Institute of BC, "Subjective vs. Objective," JIBC, Sep. 2012.
[45] Financial Security Institute, "Trend of Fraud Detection System based on machine learning," Security Research Department-2017-032, Aug. 2017.
[46] Kalyan Veeramachaneni and Ignacio Arnaldo, "AI² : Training a big data machine to defend," IEEE International conference on BigDataSecurity, 2016.
[47] Sang-hoon Kim and Gab-su Lee, "An Empirical Study on Influencing Factors of Using Information Security Technology," The Journal of Society for e-Business Studies, 20(4), pp. 151-175, Nov. 2015.
[48] Ahmad Kamal, "Subjectivity Classification using Machine Learning

Techniques for Mining Feature-Opinion Pairs from Web Opinion Sources," International Journal of Computer Science Issues (IJCSI), Vol. 10, Issue 5, pp. 191-200, 2013.

[49] Jong-hong Jeon and Seung-yoon Lee, "Technical standardization trend of open and human-friendly artificial intelligence system," TTA Journal, Vol.169, pp. 46-54, 2017.

〈저자소개〉

이 보 라 (Bo-ra Lee) 정회원
2016년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 금융, 컴퓨터공학

김 인 석 (In-seok Kim) 정회원
2008년: 고려대학교 정보경영공학과 박사
2009년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT 감사, 전자금융법규