https://doi.org/10.33778/kcsa.2019.19.2.039

행동경제학 기반 정보보안 연구 동향 분석★

오 명 옥*, 김 정 덕**

요 약

최근 피싱(Phishing)과 같은 새로운 유형의 악성코드를 이용한 사회공학 공격이 빈번해짐에 따라 정보보안 사고가 점차 고도화되고 있다. 조직에서는 정보보안 사고를 예방하기 위하여 다양한 노력을 하고 있지만 대부분 기술적 보안솔루션에 의존하는 경향이 있다. 그럼에도 불구하고 모든 보안사고를 완벽하게 예방할 수 없다. 최근에는 보안기술 기반 정보보안 접근방법의 한계를 극복하기 위하여 새로운 접근방법인 인간 중심 보안에 대한 관심이 높아지고 있다. 이러한 노력의 일환으로 일부 연구자들은 인간의 실제적 행동을 이해하고 그 행동에 따른 결과를 규명하는 행동경제학을 정보보안 분야에 접목시키고 있다. 본 연구는 행동경제학의 개념과 방법을 정보보안에 적용한 최근의 연구 흐름을 파악하는 동향 분석 연구로서, 141개의 관련 논문을 대상으로 연구 추세, 연구 주제, 연구방법론 등을 분석하였다. 분석 결과, 행동경제학의 개념과 아이디어를 '운영 보안' 분야에 적용한 실증연구가 대다수이며, 향후 폭넓은 연구 주제 선정과 문헌연구를 통해 실제로 사람의 행동을 바꾸는 문제에 행동경제학을 적용하여 프레임워크 정립, 영향 요인을 식별하는 연구가 수행되어야 한다.

An Analysis of Research Trends in Information Security Based on Behavioral Economics

Oh Myeong Oak*, Kim Jung Duk**

ABSTRACT

Recently, information security accidents are becoming more advanced as social engineering attacks using new types of malicious codes such as phishing. Organizations have made various efforts to prevent information security incidents, but tend to rely on technical solutions. Nevertheless, not all security incidents can be prevented completely. In order to overcome the limitations of the information security approach that depends on these technologies, many researchers are increasingly interested in People-Centric Security. On the other hand, some researchers have applied behavioral economics to the information security field to understand human behavior and identify the consequences of the behavior. This study is a trend analysis study to grasp the recent research trend applying the concept and idea of behavioral economics to information security. We analyzed the research trends, research themes, research methodology, etc. As a result, the most part of previous research is focused on 'operational security' topics, and in the future, it is required to expand research themes and combine behavioral economics with security behavioral issues to identify frameworks and influencing factors.

Keywords : Information Security, Behavioral Economics, Heuristics, Bias, Nudge, Research Trends

접수일(2019년 1월 28일), 수정일(2019년 3월 19일),
게재확정일(2019년 3월 30일)

★ This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2014-1-00636) supervised by the IITP(Institute forInformation & communications Technology Promotion)

* 중앙대학교 융합보안학과(주저자)
** 중앙대학교 산업보안학과(교신저자)

1. 서 론

인터넷과 IT 환경의 급속한 발전으로 정보화 사회로의 빠른 변화가 진행됨에 따라 동시에 정보화 역기능이 큰 위협으로 등장하기 시작했다[1]. 피싱(Phishing)과 같은 새로운 유형의 악성코드를 이용한 사회공학 공격이 빈번해지고 각종 보안사고가 점차 고도화되고 복잡해지고 있다. 조직에서는 보안사고를 예방하기 위하여 다양한 노력을 하고 있지만 기술적인 솔루션에 의존하는 경향이 있으며, 그럼에도 불구하고 보안사고를 완벽히 예방하는 것은 불가능하다. 즉 급격한 IT환경의 변화와 외부 위협의 증가로 인하여 기존의 기술 기반의 정보보호 대책으로는 그 한계가 있으며 인간 중심의 정보보호 전략이 필요하다[2]. 임직원 개인에게 권한과 책임을 명확히 하고 신뢰와 원칙 기반의 보안활동을 추진하여야 하며, 이를 위해서는 정교한 교육 인식프로그램의 시행과 행위기반 모니터링 시스템의 적용이 수반될 필요가 있다[3].

기업 규모와 상관없이 대부분의 기업에서 보안사고 예방을 목적으로 다양한 조직원의 인식 제고 활동을 진행하고 있다. 하지만 그 효과는 이상적이지 않은 경우가 많다. 그 중에는 보안담당자의 전문성 부족 등의 이유로 보안인식 프로그램이 실패할 수 있지만 조직원의 이해 부족과 저조한 참여도가 가장 큰 원인으로 작용한다. Osterman Research에서 실시한 '조직원의 보안인식 훈련 프로그램에 대한 태도 조사'에 따르면, 조직에서 전개한 보안활동에 '적극적으로 반대'하는 직원은 없지만 전체의 38%는 '중립적'이거나 그들이 받은 훈련에 대해 '다소 반대'하는 입장을 보였다[4]. 보안의 중요성을 인정하나 그 전달 방식이나 내용에 대해 찬성을 하지 못하거나 '귀찮은' 감정적인 요인 때문이다[4]. 이렇게 사람들이 보안의 중요성을 알고 있으나 소극적인 반응을 보이는 것은 사람이 주변 상황을 인식할 때 이성적이고 엄격한 객관성을 유지하지 못하고 때론 감정적이고 이기적이기 때문이다.

이러한 사람의 이성적이고 합리적인데 반해 때로 감정적이고 이기적인 행동에 대한 연구는 심리학에서 태동한 행동경제학(Behavioral Economics)에서도 다루고 있다. 행동경제학은 이성적이고 이상적인 경제적 인간 (Homo Economics)을 전제로 한 경제학이 아닌 실제적인 인간의 행동과 그 행동에 따른 결과들을 규명하기 위한 경제학이다[5].

최근 인간 중심의 보안에 대한 관심이 높아짐에 따라 사람의 심리적 특징과 행동을 연구하는 행동경제학을 정보보안에 적용하는 시도가 일부 연구자에 의해 진행되고 있다. 본 연구는 행동경제학의 개념과 아이디어를 정보보안에 적용한 최근의 연구 흐름을 파악하는 동향 분석 연구로서, 141개의 논문을 대상으로 연구 추세, 연구 주제, 연구 방법론을 살펴보고 이에 대한 시사점과 향후 연구 방향을 제시하고자 한다.

2. 이론적 배경

2.1 정보보안의 동향

4차 산업혁명과 함께 사람과 사물은 보다 촘촘히 연결되고 물리적 현실 환경과 디지털 환경의 경계는 희미해진다. 이러한 변화를 주도하는 것은 디지털 기술이라고 볼 수 있다. 데이터의 증가량, 네트워크에 연결되는 기기의 수, 알고리즘 성능, 반도체 집적도 등 디지털 DNA(Data, Network, Algorithm/Architecture)[6] 영역의 발전 속도는 우리의 예상을 훨씬 앞서가고 있다. 지능정보 기술의 발전은 풍요로운 생활을 만들어 주지만 보안 측면에서는 많은 문제를 일으키고 있다. 이는 지능정보기술의 발전과 보안의 위협은 비례적으로 증가하기 때문이다.

4차 산업혁명 시대의 정보보안 정책은 네트워크나 기기를 경계로 보안기술을 적용하기보다는 사람을 중심으로 경계선을 선정하고 차별적 대응 전략을 적용하는 방향으로 전환되어야 한다[7]. 김은지 등(2016)은 정보보안 사건이 증가함에 따라

내부자에 의한 정보시스템 오남용은 조직의 지속적인 위협 요소로 존재할 것으로 추측 하였으며[8], 이는 인간 요소가 정보보안에 주는 영향을 강조하였다. 이외에도 고도화되고 있는 보안위협에 대응하기 위해서는 인공지능, 블록체인 등 신기술 도입으로 한층 더 지능화된 각종 위협에 대비한 차세대 정보보안 기술의 마련도 필요하다.

2.2 행동경제학의 발전과정

경제학에서는 합리적이고 이기적이고 빠른, 그래서 자신의 선택에서 고려하는 모든 대상이 얼마나 가치가 있는지를 계산하여 가장 가치가 큰 대상을 선택하는 경제 주체를 상정하고 이론을 전개해 나간다. 합리적이라 함은 선택 대상이 자신에게 얼마나 가치가 있는지를 정확하고 일관되게 판단을 내릴 수 있음을 의미하고, 이기적이라 함은 그 판단이 '자신'에게 얼마나 가치가 있는지를 기준으로 할 뿐 '타인' 혹은 '우리'에게 얼마나 가치가 있는가는 따지지 않는다는 말이다. 행동경제학은 경제이론의 출발점이라 할 수 있는 경제인이라는 가정, 즉 경제 주체의 합리성과 이기성에 대해 문제를 제기한다[9].

행동경제학이라는 용어가 공식적으로 사용되기 시작한 것은 1958년경으로 확인된다. 당시의 주류경제학의 합리성의 체계에 의문을 제기하면서 발전한다. 초기 행동경제학의 선두 주자로서 허버트 사이먼과 조지 카토나는 정통 경제학자가 아니라, 심리학자이자 인지과학자였다. 이들의 심리학과 인지과학에 대한 전문성은 기존 주류경제학이 간과하였던 인간의 비합리적인 심리 특성에 주목할 수 있었다. 이들 다음으로 2002년 노벨경제학상을 수상한 다니엘 카너먼과 그의 절친한 공동연구자인 아모스 트버스키(Amos Tversky)는 신행동경제학 시대를 연 대표 학자로 거론된다. 이 두 명의 학자가 공동으로 수행한 대표적인 연구 성과 습관적 생각에 기인한 행동과 오류 문제를 다룬 1974년 Science 출간 논문, 'Judgement under Uncertainty: Hueristics and Biases는 인간의 비합리적 심리 특성의 경제이론 모형 및 실증분석 모형 속으로 적용시키면서 행동경제학 발전에 지대한 공헌을 세운다[10]. 또한 행동경제학을 언급하면서 빼놓을 수 없는 학자는 2017년 노벨경제학상 수상자 세일러 교수이다. 세일러 교수가 집필한 '넛지'에서는 심리학적인 가정을 통해 경제적 의사결정 과정을 설명하는 근거를 마련하였으며 제한적 합리성과 공정성 선호, 자제력 결여 등의 인간의 특성이 시장뿐 아니라 개인의 의사결정에 어떻게 영향을 미치는지 체계적으로 분석해냈다.

2.3 연구 동향 분석

연구 동향 분석은 일종의 메타분석으로, 기존에 수행된 다양한 개별 연구들을 분석 및 종합하여 연구자에게 통합된 관점의 연구 동향을 제동하기 위한 연구 방법이다[11]. 분석방법은 크게 기본 분석과 상세 분석으로 구분할 수 있으며, 기본 분석에는 분야별 논문 건수, 논문 게재 추세 등이 해당되며, 논문 주제, 연구방법론, 교차분석 등 이 상세 분석에 해당된다. 연구동향 분석을 위한 자료의 수집은 특정 저널이나 학술대회에 게재된 논문을 대상으로 하거나 연구검색을 위한 학술 데이터베이스를 활용하여 수집할 수 있다[12]. 검색 방법은 일반적으로 논문 제목, 키워드, 요약 등에 특

<Table 1> Research type

Category	Description
Descriptive	Describes a phenomenon in its appearance without any use of theory
Philosophical	Reflects upon a phenomenon without data or reference to any theory
Theoretical	Reflects upon a phenomenon based on some theory but without empirical data or with only anecdotal and particular such
Theory generating	Attempts to analyse / interpret quantitative or qualitative data in a systematic manner for the purpose of model building.
Theory testing	Attempts to test a theory using quantitative or qualitative data in a systematic manner, i.e. not just strict theory testing

정 용어를 입력하는 형태로 수행되며, 이때 전 기간을 대상으로 하거나 희망하는 특정 기간으로 한정 지을 수 있다. 수집된 논문은 연구자가 검토하여 참고문헌의 기준을 인용하여 연구 방법론, 주제 등을 분석한다.

따라서 본 연구의 연구 주제는 ISO 27002의 14개 통제항목 (정보보호 정책, 정보보호 조직, 인적자원보안, 자산관리, 접근통제, 암호화, 물리적 및 환경적 보안, 운영 보안, 통신 보안, 시스템 도입·개발·유지 보수, 정보보호 사고 관리, 업무 연속성 관리의 정보보호 측면, 준거성)을 참고하여 분류하였다[8]. ISO 27002를 참고한 이유는 행동경제학의 아이디어를 적용한 정보보안의 특정 분야가 아닌 정보보안의 전반에 대한 연구 동향 분석이 목표이기 때문이다. 또한 연구방법론은 Gronlund의 기준을 참고하였다. Gronlund는 연구의 유형을 '기술적(Descriptive)', '철학적(Philosophical)', '이론적(Theoretical)', '이론 생성(Theory generating)', '이론 테스트(Theory testing)'으로 분류된 바가 있으며, 세부 설명은 <표 1>과 같다[13]. 이는 크게 두 개의 종류의 연구로 분류가능한데, 이론들만을 통해 현상이나 항목도출 및 정의까지를 의미하는 문헌연구와 연구의 주제와 가설에 대해서 정량적인 수치를 통해 테스트 및 입증까지 하는 실증 연구로 분류할 수 있다[16].

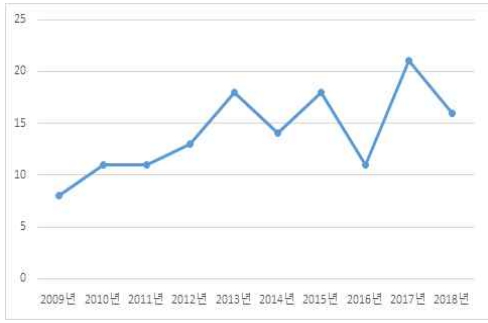
3. 연구대상 및 방법

본 연구는 J. Webter의 연구 방법에 따라 포괄적인 조사를 진행하기 위하여 특정 저널에 한정하지 않고 학술 검색 엔진을 활용하여 2009년부터 2018년까지의 행동경제학의 아이디어를 보안에 적용한 연구를 검색하였다[14]. 검색엔진은 'Google Scholar', 'IEEE', 'Emerald Insight', 'RISS'를 이용하여 자료를 수집하였다[16]. 선정된 검색엔진에 'behavioral economics, information security', 'heuristics, information security', 'bias, information security', 'nudge, information security', '행동경제학, 정보보안', '휴리스틱, 정보보안', '편향, 정보보안', '넛지, 정보보안'을 입력하여 행동경제학의 아이디어를 정보보안에 적용한 관련 연구 총 189개를 수집하였으며, 이 중에서 행동경제학을 단순 언급, 정보보안을 연구의 변수로 사용하는 논문을 제외 한 141개를 연구대상으로 선정하였다. 또한 선정된 논문은 전문을 검토하여 연구 주제와 연구 방법론으로 분류하고 교차 확인하였으며 이때 분류기준의 객관성 확보를 위하여 유사분야의 분류기준을 참고하였다[15].

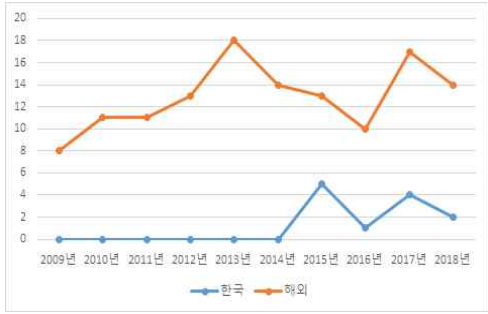
4. 연구 동향 분석 결과

4.1 연구 추세

행동경제학의 아이디어를 정보보안에 적용한 연구의 동향을 살펴보면 (그림 1)과 같이 전반적인 연구 추세는 증가와 감소를 반복하지만 지속적인 연구가 이루어져 왔음을 알 수 있다.



(Fig. 1) Publication Trend

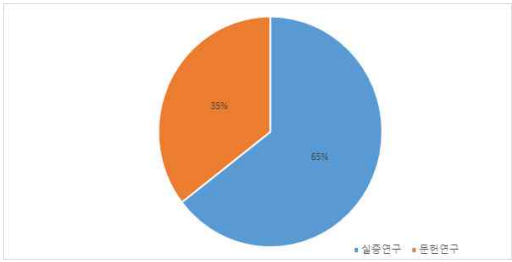


(Fig. 2) Domestic and Foreign Publishing Trends

4.2 연구 방법론

연구방법론에 대한 분류기준은 Gronlund의 기준을 참고하여 분류하였으며, 본 연구에서는 (그림 3)과 같이 크게 두 종류의 연구로 분류하였다[13].

행동경제학을 정보보안에 적용한 연구의 목적별로 크게 두 가지로 분류하였을 때 문헌연구는 37% (50편)을 차지하고, 실증연구는 63% (91편)으로 실증연구가 주를 이루었음을 알 수 있다.



(Fig. 3) Research Methodology

4.3 연구의 주제

행동경제학의 아이디어를 정보보안에 적용한 연구들을 대상으로 동향 분석을 진행한 연구는 아직까지 부족한 실정이다. 행동경제학의 개념과 아이디어를 적용하기 어려운 항목 제외하고 총 9 개의 주제 '정보보호 정책', '정보보호 조직', '인적자원 보안', '통신 보안', '도입·개발·유지보수', '개인정보 보호'로 최종 분류하였다. 연구의 주제를 9개의 기준으로 분석한 결과, <표2>와 같이 운영 보안(56개), 개인정보보호(21개), 인적자원 보 안(20개), 접근 통제(16개), 시스템 도입·개발·유지보수(10), 정보보호 조직(7개), 통신 보안(6개), 정보보호 정책 (3개), 암호화(2개) 순으로 연구가 수행된 것을 알 수 있었다.

<Table 2> Research Theme

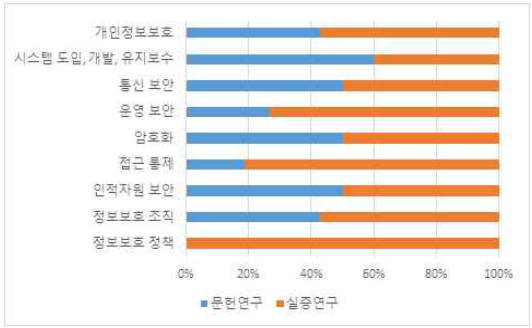
Research Theme	Number of Research
Information security policies	3
Organization of information security	7
Human resource security	20
Access control	16
Cryptography	2
Operations security	56
Communications security	6
System acquisition, development and maintenance	10
protection of personally identifiable information	21
Total	141

4.4 연구의 주제와 연구의 방법론 교차분석

끝으로 <표3>과 (그림4)에서 보여준 듯이 향후 유망한 연구의 주제와 방법론을 찾기 위해, 주제와 연구 방법론을 교차분석 하였다.

<Table 3> Research Methodology and Theme

Theme/ Methodology	Literature study	Empirical study	Total
Information security policies	0	3	3
Information security policies	3	4	7
Human resource security	10	10	20
Access control	3	13	16
Cryptography	1	1	2
Operations security	15	41	56
Operations security	3	3	6
System acquisition, development and maintenance	6	4	10
Protection of personally identifiable information	9	12	21
Total	50	91	141



(Fig. 4) Research Methodology and Research Theme

우선 운영 보안, 접근통제, 개인정보보호, 정보보호 조직, 정보보호 정책 분야의 경우 문헌연구보다 실증 연구이 더 많이 사용되고 있었다. 인적자원 보안, 통신 보안, 암호화 분야는 실증연구와 문헌연구 두 가지 방법의 사용 비중이 같았으며 시스템 도입·개발·유지보수 분야는 실증연구보다 문헌연구를 더 많이 수행한 것으로 나타났다.

5. 결론

본 연구는 행동경제학의 개념과 아이디어를 정보보안에 적용한 연구 동향을 파악하기 위하여 기존에 수행했던 연구를 분석하였다. 또한 향후 발전 방향을 제시하고 국내외 141개의 논문을 대상으로 연구의 추세, 주제, 방법론을 중심으로 정량적 분석을 실시하였다. 전반적인 추세를 볼 때, 행동경제학의 아이디어를 정보보안에 적용하는 연구들은 꾸준히 진행되고 있었고, 상세분석을 통해 도출된 시사점은 다음과 같다. 첫째, 정보보안의 가장 취약한 링크는 인간이고, 사람의 심리를 이해하고 행동을 유도하는 행동경제학의 이론은 조직원의 자발적인 정보보안 정책 준수 실현이 가능하다고 본다. 하지만 행동경제학의 이론을 정보보안에 적용한 연구는 전반적으로 부족한 편이고, 특히 국내에 더 많은 연구가 필요할 것으로 보인다. 본 연구에서 사용한 키워드로 검색한 결과, 해외의 129건에 비해 국내의 연구는 12건에 불과하였다. 둘째, 행동경제학의 아이디어를 정보보안에 적용한 연구에 사용된 연구 방법론에 대해서는 정량적인 수치를 통해 테스트 및 입증까지 하는 실증연구가 상대적으로 많이 수행되었는데, 문헌연구를 통해 인간의 태도와 행동 문제를 행동경제학을 접목하여 프레임워크 정립, 정보보안에 영향주는 요인을 식별하는 연구가 수행되어야 한다. 셋째, 현재까지 수행된 연구의 주제 중 운영 보안이 상대적으로 많이 수행되었다. 휴리스틱 기법을 통한 악성코드 탐지 프로그램 개발 및 실효성 검증, 발견적 평가방법을 통해 컴퓨터 프로그램이나 웹사이트 등 복잡한 시스템을 위한 사용자 인터페이스 디자인 개발에 사용성 문제를 탐지를 목적으로 시스템을 개발 및 평가하는 연구가 상당수인 것으로 파악이 되었다. Kozachok외 2명은 실행파일에 대한 정적분석을 바탕으로 휴리스틱 기법을 활용하여 악성코드 탐지 메커니즘을 제안하였다 [17]. 이진이 외 2명은 피싱 유형에 대한 대응방안을 제시하고, 대응방안의 유효성을 판단하기 위하여 휴리스틱 기반 악성 사이트 분류 모델을 생성하고, 각 모델의 정확도를 검증하였다[16]. 또한 신경민 외 3명은 휴리스틱 기법을 이용하여 보안 애플리케이션을 설계하였다[18]. 향후에는 운영보안 이외의 다른 분야에 대한 연구도 많이 이루어질 필요가 있을 것으로 보인다. 마지막으로, 본 연구에서는 일부 국제표준 ISO 27002의 주제를 참고하고 연구주제 분류기준을 설정하였다. 아직 다루지 못한 주제(‘물리적 및 환경적 보안’, ‘자산 보안’, ‘공급자 관계’, ‘보안사고 관리’, ‘업무 연속성 관리의 정보보호 측면’)에 행동경제학의 개념과 아이디어의 적용 타당성 및 기여점을 찾아볼 필요가 있을 것으로 판단된다.

본 연구에서는 검색의 범위에 있어 특정 용어만을 검색한 것으로 다른 용어로 이루어진 연구를 분석하지 못했다는 점, 연구자의 주관적인 판단으로 분류하였다는 점에서 한계가 존재한다. 하지만, 본 연구는 국내뿐만 아니라 해외 연구를 대상으로 종합적인 관점에서 정량적인 분석을 통해 행동경제학을 정보보안 분야에 활용한 논문의 주제를 식별하고 연구 동향을 파악하였다는 의의를 가진다. 이는 행동경제학의 개념과 아이디어의 정보보안

적용에 관심 있는 연구자들이 관련 연구 동향을 파악하고, 연구 방향을 설정하는데 도움이 될 것이다. 또한 행동경제학은 사람의 심리적 특징과 행동을 연구하는 학문이므로 이를 인간 중심의 정보보호 전략 수립에 활용할 수 있을 것으로 기대된다.

참고문헌

[1] Min Sik Kim, Jong In Lim, " The Best Model to Optimize Security Investments with Considering a Corelation of Response Techniques Against Each Threat", Jouranl of Information and Security, Vol. 16, NO. 05, 2016.

[2] Jaewon Jun, Jung-hoon Le. Chae-ri Ki, "A Study on the influence of firm's Information Security Activities on the Information Security Compliance Intention of Employee", Jouranl of Information and Security, Vol.6, NO.7, pp. 51-59, 2016.

[3] Kunwoo Kim, Jungduk Kim, "The Values and Strategies of Industrial Security in Digital Economy", Korean Journal of Industry Security, Vol.8, NO.1, pp. 61-74, 2018

[4] Osterman Research, "Best Practices for Implementing Security Awareness Training", Osterman Research, 2008.

[5] Wan Soo, Lee, Chan Souk, Kim, Chong-Ryul, Park, "'Combination of 'Econ' and 'Nudge' : The Applicability of Concepts and Theories of Behavioral Economics in Communication Effect Researches", Korean Society For Journalism And Communication Studies, Vol. l, NO. 2, pp. 129-164, 2016.

[6] Future Technology Research Center, "ECOsight 3.0: Future Technology Outlook", Electronics and Telecommunications Research Institute, 2015

[7] Seung-min Lee, Geun-Hye Song, "Information security trends and security threat analysis", Electronics and Telecommunications Research Institute, 2017

[8] Kim Eun Ji, Lee Joon Tai, "The Empirical Study on the Misuse Intention Using Information System : Focus on Healthcare Service Secto" Jouranl of Information and Security, Vol. 16, No. 5, pp. 23-31, 2016.

[9] Kahneman, "Maps of bounded rationality: Psychology for behavioral economics", American Economic Review, Vol. 93, NO. 5, pp. 1449-1475, 2003.

[10] Seon-gil Yun, 'Heuristics and Persuasion', Communication Books, 2015

[11] Hang-Bae Chang, "An Exploratory Study of Industrial Security Studies for Science and Technologies Protection", The Korea navigation institute, Vol. 17, NO.1, pp. 123-131, 2013.

[12] Mi-Hwa Kang, Tae-Sung Kim, "Research Trends in Information Security Economics: Focused on the Articles Presented at WEIS", Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, NO. 6, pp. 1561-1570, 2015.

[13] A. Gronlund, Editors, "State of the art in e-Gov Research-A survey", Proceeding of the 3rd International Conference of Electronic government, pp. 178-185, 2004.

[14] J. Webter, R. T. Watson, "Analyzing the Past to Prepare for the Future : Writing a Literature Review, Management Information System Quarterly", Vol.26, No.2, pp.13-23, 2002.

[15] Kunwoo Kim, Jungduk Kim, "An Analysis of Research Trends in Information Security Education", Journal of The Korea Institute of Information Security & Cryptology, VOL.26, NO.2, pp. 489-497, 2016.

[16] Myeong-gyun Song, Jungduk Kim, "An analysis of literature review about information security culture: Setting a direction for future study", Journal of Security Engineering, Vol. 12, NO. 5, pp. 515-524, 2015.

[17] A.V. Kozachok, M.V. Bochkov, E.V. Kochetkov, "Heuristic Malware Detection Mechanism Based on

Executable Files Static Analysis", Proceeding of the 3rd International Conference of Information Technology and Nanotechnology, 2017.
[18] Lee-Jin Lee, Doo-Ho Park, Chang-Hoon Lee, "Information Security : Phishing Detection Methodology Using Web Sites Heuristic", Korea Information Processing Society, Vol. 4, NO. 10, pp. 349-360, 2015.
[19] Kyung-min Shim, Hoon-beom Hyun, Yong-tae Jeon, Hyun-sik Lee, "A Smishing Analysis and Correspondence method based on Heuristic", Korean Conference on Computers, pp. 1823-1825, 2015.

〔저자소개〕

오 명 옥 (Myeong-oak Oh)
2014년 6월 YANBIAN University 학사
2017년 9월 ~ 중앙대학교 융합보안학과 석사
email : ohmoak91@gmail.com

김 정 덕 (Jung-duk Kim)
1979년 2월 연세대학교 정치외교학과
1981년 8월 연세대학교 경제학과 석사
1986년 5월 University of S. Carolina, MBA
1990년 12월 Texas A&M University, Ph.D. in MIS
2014년 8월 중앙대학교 정보시스템학과 교수
2014년 9월 ~ 중앙대학교 산업보안학과 교수
email : jdkimcau@gmail.com