Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.695

교차영향분석을 이용한 국내 ICT 융합산업의 정보보호정책 우선순위 분석*

이 동 희,[1†] 전 효 정,[2] 김 태 성[2‡]
[1]충북대학교 정보보호경영학과, [2]충북대학교 경영정보학과/보안경제연구소

Priority Analysis of Information Security Policy in the ICT Convergence Industry in South Korea Using Cross-Impact Analysis*

Dong-Hee Lee,[1†] Hyo-Jung Jun,[2] Tae-Sung Kim[2‡]
[1,2]Chungbuk National University and Cybersecurity Economics Research Institute (CERI)

요 약

최근 제조업을 시작으로 농업, 금융업 등의 전 산업 영역에서 ICBM(IoT, Cloud, Bigdata, Mobile)을 중심으로 한 신산업과의 융합이 급속도로 진행되고 있다. 향후 융합산업의 가장 큰 문제 중 하나인 사이버 위협에 대비하기 위해 정보보호를 고려한 융합산업의 발전이 매우 중요한 상황이다. 이에 본 연구에서는 현재 발표된 산업발전 정책과 이와 관련된 정보보호정책들의 세부 내용을 교차영향분석으로 분석하고 전문가 설문을 통해 정책의 우선순위를 제시하였다. 이를 통해 정보보호정책 내의 우선순위 및 상호 연관성을 밝히고, 효과적인 정책 시행방향에 대해서 제시하고자 하였다. 결과적으로 본 연구에서 도출한 6개의 정보보호정책과제들은 모두 핵심 동인에 속하며, 정책의 중요도를 고려한다면 보안 산업의 체질개선 및 지원 강화, 정보보호 인재양성, 정보보호산업 투자확대 등의 정책이 상대적으로 우선 시행될 필요가 있는 것으로 나타났다.

ABSTRACT

In recent years, industrial convergence centered on ICBM (internet of things (IoT), cloud, big data, mobile) has been experiencing rapid development in various fields such as agriculture and the financial industry. In order to prepare for cyber threats, one of the biggest problems facing the convergence industry in the future, the development of the industry must proceed in tandem with a framework of information security. In this study, we analyze the details of the current industrial development policy and related information protection policies using cross impact analysis and present policy priorities through the expert questionnaire. The aim of the study was to clarify the priorities and interrelationships within information security policy as a first step in suggesting effective policy direction. As a result, all six information security policy tasks derived from this study belong to key drivers. Considering the importance of policies, policies such as improving the constitution of the security industry and strengthening of support, training of information protection talent, and investing in the information security industry need to be implemented relatively first.

Keywords: ICT convergence Industry, Information security policy, Cross-impact analysis

Received(02. 20. 2018), Modified(105. 24. 2018), Accepted(05. 25. 2018)

* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"(과제번호 H2101-17-1001)의 지원을 받아 수행된 연구임

† 주저자, iluy3082@gmail.com
‡ 교신저자, kimts@chungbuk.ac.kr(Corresponding author)

I. 서 론

'제4차 산업혁명(the 4th industrial revolution)'은 2016년 다보스포럼(WEF, World Economic Forum)에서 언급되면서 국내외적으로 큰 화제가 되었다. 4차 산업혁명이란 표현 이전에는 독일의 'High-tech Strategy 2020' 의 10가지 프로젝트 중 하나인 Industry 4.0이 4차 산업혁명의 시초라고 할 수 있다. Industry 4.0은 제조업 분야에서 정보통신기술이 융합되는 단계를 의미하였으나, WEF의 주제로 선정되면서 본격적으로 논의되기 시작하였다[1]. WEF의 창립자 클라우스 슈밥(Klaus Schwab)은 4차 산업혁명을 '디지털 혁명인 3차 산업혁명을 기반으로 하여 산업 간 경계를 허무는 기술의 융합'이라고 정의하였다[2]. 결국 4차 산업혁명이란 3차 산업혁명까지의 제조, 전기, 컴퓨터와 인터넷 등을 기반으로 한 기존의 산업들과 ICBM(IoT, Cloud, Big data, Mobile)을 중심으로 한 신기술이 융합하여 혁신적인 제품 및 서비스를 창출하는 것을 의미한다. 이처럼 기존 산업과 정보통신기술의 융합을 통한 혁신은 무궁한 잠재력을 내포하고 있으나, 한편으로 기존에는 정보통신기술이 활용되지 않았던 산업 또는 생활의 영역에서 까지 연결되어 사생활 침해의 가능성, 랜섬웨어(Ransomware)의 증가 그리고 극단적인 경우 사람의 생명을 위협하는 일마저 발생할 것으로 우려되고 있다. 예를 들어 커넥티드 카의 보안위협 시나리오를 가정한다면 다음과 같다. 커넥티드 카(Connected Car)는 다른 차량이나 도로, 신호 체계 및 기타 스마트 장치와 통신하면서 실시간 데이터 수집과 전송이 가능한 차량을 의미한다. 이를 통해 커넥티드 카는 안전, 유희, 자율 주행 등의 새로운 편의를 제공할 것으로 기대되고 있는 한편, 해킹에 의해 열쇠 없이 차의 문을 열거나, 차량 주행 중 발생하는 위치 정보 등의 탈취, 심지어는 차량의 조향기능 및 제동기능을 원격으로 제어하여 운전자의 안전을 위협하는 상황 등이 발생할 수 있을 것으로 우려되고 있다[3]. 이처럼 기존에는 정보통신기술이 접목되지 않은 제품이나 서비스들은 비교적 해킹의 위협에서 안전했으나, 초연결(Hyperconnectivity)을 특징으로 하는 4차 산업혁명 시대로 진입하면서 향후 네트워크에 연결되는 제품, 기반 시설, 공장, 일반 가정의 모든 곳으로 현존하는 보안 취약점이 그대로 이전된다는 것에 문제가 있다. 이 같은 이유로 4차 산업혁명시대의 정보보호 문제는 그 범위와 영향력에 있어서 전례를 찾아보기 힘든 엄청난 사회적 문제로 대두될 것으로 예상된다. 따라서 향후 보안 위협에 대해 효과적으로 대응하기 위해서는 4차 산업혁명의 신산업과 융합산업의 발전과정에서 정보보호를 고려할 수 있도록 정책적 노력이 필요한 시점이다. 그러나 미래창조과학부 및 관계부처에서 발표한 융합산업과 ICBM 등의 신산업에 관련된 정보보호정책들은 정보보호정책과제들을 병렬적으로 제시하고 있다. 따라서 어떤 정책과제가 상대적으로 더 중요한지, 어떤 정책과제가 다른 것보다 선행적으로 수행되어야 할지에 등에 대한 사항을 확인하기 어렵다. 본 연구에서는 ICBM을 중심의 국내 융합산업 관련 발전정책과 정보보호정책의 분석을 통해 융합산업 발전에 고려해야 할 정보보호의 과제들을 연계하고자 하였다. 또한 융합산업 관련 정보보호정책들 간의 우선순위를 제시함으로써 정보보호를 고려한 융합산업의 균형 발전이라는 과제를 효과적으로 달성하기 위한 정책적 방향을 제시하고자 한다.

II. 이론적 배경

2.1 정보보호정책 관련 연구

본 연구에 앞서 정보보호정책에 대한 연구들을 크게 두 가지로 분류할 수 있다. 첫째는 현재 당면한 보안 문제를 해결하기 위해 필요한 정책을 제안하기 위한 연구이며, 둘째는 정보보호정책들 간의 우선순위에 관한 연구가 주로 진행되었다. 정보보호정책을 제안한 연구로 류현숙[4]은 인증제도를 중심으로 국내외 사례연구 및 계층화의사결정방법(AHP)을 활용하여 사이버보안 핵심 가이드라인과 전략을 제시 하였으며, 특히 국내에서는 새로운 개념인 사이버 복원력이라는 개념을 통해 향후 정보보호정책의 방향을 제안하였다. 김정덕[5]은 국가 정보보안의 주체를 정부, 기업 및 산업, 개인, 환경 등의 네 가지로 나누고 각각의 주체들이 해결해야 할 보안 이슈 도출과 해결방안을 제시하였다. 구체적인 내용으로는 국가 정보보안 거버넌스의 개선, 정보보안 산업 육성, 기업 보안수준 제고, 정보보호 인력 양성, 법제도 정비 및 문화 형성 등의 문제점과 정책 대안을 제안하였다. 김병운[6]은 국내외의 주요국가의 사이버 보안정책 동향분석을 통해 국내 정보보호 현황을 진단하고, 거버넌스, 법제도, 연구개발, 인력양성 등의 정책을 제안하였다. 한편, 정보보호정책 간의 우선순위에 대한 연

구로 신영진과 김성태[7]는 기존 정보보호관련 연구와 2002년 '정보보호 중장기 계획'의 내용을 중심으로 법제도, 물리적· 기술적 측면, 조직적· 관리적 측면으로 분류하고, AHP를 통해 정보 보호정책의 우선순위를 전문가 대상으로 설문하였다. 이를 통해 우리나라의 정보보호에 대한 통합적 관점에서의 정책방향을 제시 하고자 하였다. 성욱준과 김동욱[8]은 정보보호정책을 정보보호 기반분야, 정보보호 정책활동 분야로 계층을 구분하였다. 이를 다시 정보보호 기반 분야는 법제도 기반, 인적기반, 기술적 기반, 사회적 인식으로 구분 하였고 정보보호 정책활동은 주요기반 시설보호, 개인정보보호, 정보보호 산업진흥, 국가안보활동으로 구분하였다. 이를 AHP 통하여 정책의 중요도에 따른 우선순위를 제시하였다. 신영진 외[9]는 공공분야의 개인정보보호를 위해 우선적으로 추진되어야 할 정책과제를 도출하기 위한 연구를 진행하였다. 개인정보보호를 정책적· 기술적 측면, 처리단계별 개인정보 관리, 개인정보 침해대응의 측면으로 구분하고 AHP 방법을 통해 정책의 중요도에 따른 우선순위를 제시하였다.

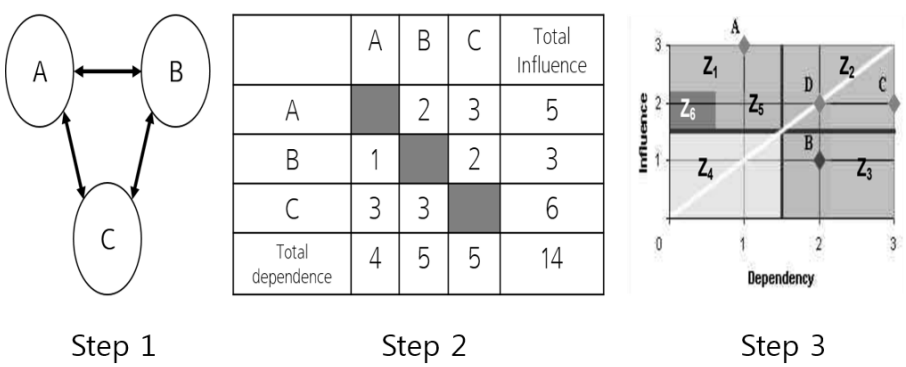
2.2 교차영향분석을 활용한 연구

교차영향분석(CIA, Cross Impact Analysis)이란 특정 사건들의 추세나 상호관계를 분석하여 변수들 간의 의존성, 핵심 변수, 영향력 등을 추정하기 위해 사용되는 방법이다[10]. 전문가들의 의견을 통해 유의미한 결과를 도출한다는 점에서 유사하나, 예측하고자 하는 변수들 간의 상호 영향을 고려한다는 점에서 차이가 있다. 선행 연구에서 교차영향분석은 크게 두 가지의 목적으로 사용되고 있었다. 하나는 미래 예측을 위해 사건 사이의 영향관계를 분석하여 향후 특정 사건의 발생 가능성을 파악하기 위해 사용하였으며, 다른 하나는 정책, 기술, 사건 등의 변수 간 영향의 방향, 세기, 시차 등을 추정하고, 향후 중요 변수를 도출하기 위한 목적으로 사용되었다. 김진한과 김성홍[11]은 정보통신산업의 발전방향을 제시하기 위해 미래 IT 환경의 시나리오를 개발하였고, 이를 CIA 방법을 활용하여 가장 유력한 시나리오를 도출하였다. Choi et al.[12]은 특허 분석과 CIA방법을 활용하여 복잡한 정보통신기술 간의 관계를 파악하고 기술 간 교차영향점수를 분석하여 향후 융합기술의 동향을 예측하고자 하였다. 연승준 외[13]는 국내외 미래 연구와 문헌고찰을 통해 방송통신정책의 문제점을 분석하여 정책과제를 도출하고, CIA 방법을 활용하여 정책과제들의 상호 영향관계와 중요도를 고려한 방송통신 융합정책 패키지를 제안하였다. 유준상과 이희상[14]은 특허와 특허에 인용된 논문, 특허 분류, 산업 분류체계를 종합하여 융합기술에 영향을 미친 과학 분야를 제시하고, 융합기술의 원천 기술 및 핵심 분야를 분석하였다. 또한 특허의 분류체계를 따라 CIA 방법을 적용하여 각 기술 분야들의 영향력 지수를 측정함으로써 융합 기술의 진행 양상을 제시하였다.

III. 연구 방법

3.1 연구 설계

본 연구에서 활용한 교차영향분석방법은 Fig. 1.과 같은 프로세스로 수행된다[10]. 1 단계에서는 교차영향분석에 적용할 사건들을 정의한다. 분석에 포



	A	B	C	Total Influence
A		2	3	5
B	1		2	3
C	3	3		6
Total dependence	4	5	5	14

Fig. 1. Process of Cross Impact Analysis

함되는 개수가 많아질수록 사건들 사이의 상호작용이 기하급수적으로 증가하여 분석이 불가능하게 될 수 있다. 따라서 불필요한 부분이 포함되지 않도록 만드는 것이 중요하며, 일반적으로 교차영향분석 연구들에서는 10개에서 40개로 사건을 제한하여 분석한다. 본 연구에서는 국내 융합산업 정보보호정책을 수집하여 그 세부 내용을 분석하였다. 이를 통해 주요 정보보호정책과제들을 나열하고, 내용에 따라 병합하거나 수정·삭제하는 과정을 통해 최종적으로 6개의 정보보호정책과제를 교차영향분석에 활용하였다. 한편 국내 융합산업 발전정책을 수집하고, 마찬가지로 6개의 핵심 정책과제로 분류하였다. 결과적으로 융합산업의 정보보호정책은 상호 영향성을 묻는 설문 응답을 통해 직접영향 매트릭스를 작성하기 위해 활용된다. 이를 통해 영향성, 의존성 등을 도출할 수 있다. 한편, 융합산업의 발전정책과의 연계를 위해 총 6개의 발전정책과제 각각에 대해 정보보호 정책과제의 중요 순위를 묻는 문항을 구성하였다. 이를 통해 각 산업의 발전정책에서 중요하게 고려해야 할 정보보호정책이 무엇인지에 대해 전문가 의견을 통해 추정하고자 하였다. 교차영향분석 프로세스 2 단계에서는 1 단계에서 정의한 발전정책과제 및 정보보호정책과제를 통해 설문지를 구성하고, 이를 통해 전문가의 의견을 묻는 단계이다. 설문 대상은 융합산업과 정보보호, 그리고 관련 정책에 대한 이해를 갖춘 연구기관·학계·산업계 종사자를 대상으로 배포하였다. 3 단계에서는 설문 응답을 회수하여 직접영향 매트릭스와 직접 영향성-의존성 맵을 작성한다. 이를 통해 융합산업 정보보호 정책과제의 핵심 정책과 정책 시행의 간격 등의 시사점을 도출하고자 하며, 융합산업 발전정책과제에서 중요하게 고려해야 할 정보보호정책이 무엇인지에 대해 제시하고자 하였다.

3.2 사건 리스트 정의

교차영향분석을 위해 분석에 활용될 사건의 리스트를 정의해야 한다. 본 연구에서는 국내 ICT 융합산업의 발전정책과 정보보호정책을 수집하여 분석하였다. 사건 리스트 정의를 위해 참고한 ICT 융합산업 정보보호정책으로는 K-ICT 시큐리티 발전전략[15], 사물인터넷 정보보호 로드맵 3개년 시행계획[16], 클라우드 서비스 활성화를 위한 정보보호대책[17], K-ICT 융합보안 발전전략[18], 제1차 정보보호산업 진흥계획[19] 등 5개 정책을 분석하였다. 이를 통해 융합산업의 정보보호 정책과제를 선정하였다(Fig. 2.). 최초 총 12개의 융합산업 정보보호정책과제를 선정하였고, 그 중요성을 고려하여 최종 6개의 정책과제로 확정하였다. 최초 선정한 12개의 융합산업 정보보호 정책과제는 '정보보호 산업투자 확대', '정보보호 산업 체질개선', '원천 보안기술 개발', '융합산업 보안 인재 양성', '정보보호 실천문화 및 인식 확산', '침해사고 대응 및 복구 체계 구축', '핵심 시설의 보안 역량 강화', '보안 사각지대에 대한 지원 및 격차해소', '보안 산업 경쟁력 강화를 위한 지원', '보안을 고려한 제품 및 서비스 개발(보안 내재화)', '보안 요구사항 표준화', '정보보호 진흥을 위한 거버넌스 및 법제도 개선' 등이다. 그러나 교차영향분석에 활용되는 사건(event)이 많아질수록 분석이 어려워진다. 때문

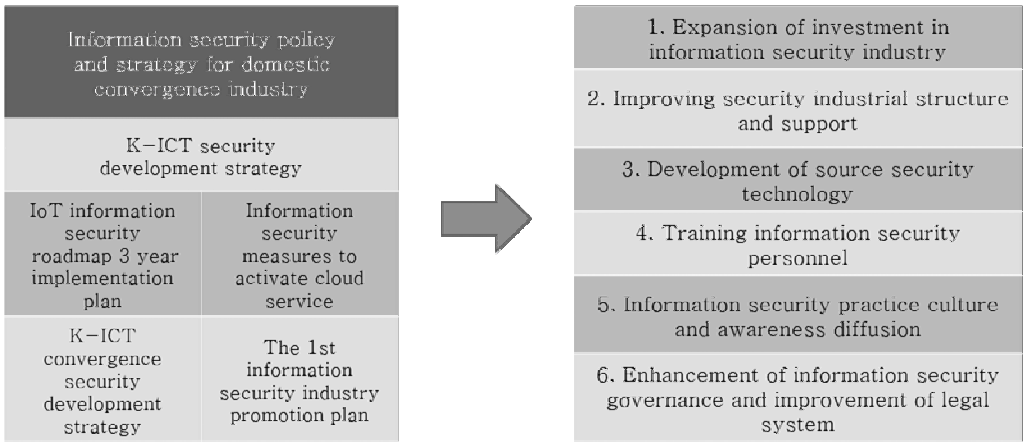


Fig. 2. Information security policy and strategy for domestic convergence industry

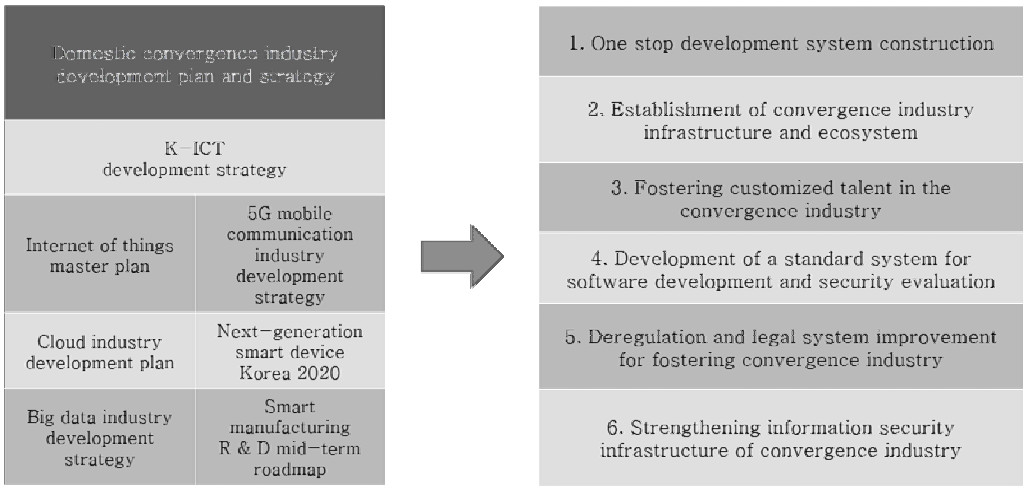


Fig. 3. Domestic convergence industry development plan and strategy

에 융합산업 정보보호정책의 내용과 관련성을 고려하여 최종적으로 6개의 정보보호 정책과제로 확정하였다. 한편 ICT 융합산업의 발전정책으로는 K-ICT 발전전략[20], 스마트 제조 R&D 중장기 로드맵[21], 사물인터넷 기본계획[22], 5G 이동통신산업 발전전략[23], 클라우드 산업 육성계획[24], 빅데이터 산업 발전전략[25], 차세대 스마트 디바이스 코리아 2020[26]등 7개의 정책의 핵심 과제 및 중점 추진과제를 분석하였다. 이를 정보보호 정책과제와 마찬가지로 그 세부 내용에 따라 11개의 정책 키워드로 축약하였다. 융합산업 발전정책의 11가지 중점 추진과제로는 '신기술 개발 지원', '산업인프라 및 생태계 구축', '융합산업의 제품 및 서비스 발굴·확산', '융합산업 맞춤 인재 육성', '개발 및 보안성 평가 등의 표준화', '신산업 육성을 위한 법제도 정비', '중소기업 성장 촉진', '신기술의 제품화·사업화 촉진', '국제 협력 및 해외진출 지원', '공공부문의 수요 확대', '정보보호 인프라 강화'로 나타났다. 이 또한 정보보호 정책과제와 같은 이유로 최종 6개의 발전전략과제를 확정하였다(Fig. 3.).

3.3 융합산업 관련 전문가 대상 설문

앞서 정의한 사건들 사이의 의존성과 영향성을 파악하기 위해 전문가 대상으로 설문을 진행하였다. 전문가 설문은 크게 두 개의 질문으로 구성하였다. 첫 번째는 기준이 되는 한 정보보호 정책과제가 다른 나머지 정보보호 정책과제들과 얼마나 연관성이 있는지에 대해 전문가의 주관적인 판단을 통해 1에서 10 사이의 값 중 하나로 응답하도록 구성하였다. 이를 통해 설문 응답자는 Table 1.의 예시와 같이 정보보호정책과제들의 관계를 묻는 총 6개의 설문에 응답한다. 응답의 기준은 특정 정보보호 정책과제의 시행에 대해 다른 정보보호 정책과 선행·후행적으로 시행이 필요하다거나, 또는 동시에 시행될 필요가 있다고 판단되는 경우 관계의 정도가 큰 것으로 판단하도록 제시하였다. 한편 두 번째 질문은 융합산업의 발전정책과 더불어 가장 중요하게 고려해야 할 정보보호정책이 무엇인지를 질문하였다. 설문 문항의 예시는 Table 2.와 같다. 이를 통해 융합산업에서의 발전과 함께 우선적으로 고려해야 할 정보보호의 과제가 무엇인지 파악하고자 하였다.

설문은 융합산업과 정보보호분야에 관련된 연구기관·산업계·학계 종사자를 대상으로 배포하였다. 설문지에는 설문응답 내용과 예시, 그리고 응답의 기준을 제시하였다. 또한 본 설문지에서 말하는 융합산업의 정의, 본 설문지에서 정의한 국내 융합산업 정보보호 정책과제들의 세부 설명을 추가하여 응답에 참고할 수 있도록 하였다. 설문은 2017년 11월 10일부터 배포하여 12월 5일까지 설문 응답 12부를 회수하였다. 응답자는 연구기관 종사자 5명, 정보보호 관련 공공기관 종사자 (또는 종사한 경력이 있는 자) 5명, 학계 2명으로 구성되었다.

Table 1. Example of survey response in cross impact analysis

Survey example	Relevance of '① expansion of investment in information protection industry' Low ← → High									
	1	2	3	4	5	6	7	8	9	10
② Improving security industrial structure and support								√		

Table 2. Example of a survey on the priority of information security policy within development policy

Survey example		Information security policy					
		①	②	③	④	⑤	⑥
Development policy	①	3	2	4	6	5	1
	②	2	4	3	5	6	1

IV. 연구 결과

4.1 설문 응답 분석

4.1.1 ICT 융합산업의 정보보호정책과제 간 교차영향 분석

회수한 설문응답 12부를 통해 직접영향 매트릭스와 직접영향 맵을 구성하여 설문응답을 분석하였다. 설문 응답을 통해 작성한 직접영향 매트릭스는 Table 3.과 같다. 직접영향 매트릭스에서 총 영향성(total influence)은 특정 정보보호 정책과제가 다른 과제에 직접적으로 미치는 영향의 정도를 나타내며, 영향성이 높을수록 선행적으로 실행될 필요가 있는 중요 정책이라고 볼 수 있다. 한편, 총 의존성(total dependency)은 다른 정책의 수행의 여부 또는 성공적인 수행 여부에 의해 영향을 받는 정도는 의미한다. 의존성이 높은 정책과제는 다른 정책과제의 성패에 영향을 크게 받는 정책 과제라고 볼 수 있다. 정보보호 정책과제 중 ② 보안 산업의 체질개선 및 지원 강화, ④ 정보보호 인재양성의 총 영향성이 가장 높은 것으로 나타났다. 이어서 ⑤ 정보보호 실천문화 및 인식 확산, ① 정보보호산업 투자확대, ⑥ 정보보호 거버넌스 강화 및 법제도 개선 순으로 총 영향성이 높은 것으로 나타났으며, ③ 원천 보안기술 개발은 가장 영향성이 낮은 것으로 나타났다. 한편 총 의존성 측면에서는 ① 정보보호산업 투자확대가 426점으로 의존성이 가장 높은 정책과제로 나타났다. 이어서 ⑥ 정보보호 거버넌스 강화 및 법제도 개선, ② 보안 산업의 체질개선 및 지원 강화, ④ 정보보호 인재양성, ⑤ 정보보호 실천문화 및 인식 확산, ③ 원천 보안기술 개발의 순으로 의존성이 높은 것으로 나타났다. 또한 앞서 계산한 직접영향 매트릭스의 결과를 통해 직접 영향성-의존성 맵(direct influence-dependency map)을 작성하였다. 직접 영향성-의존성 맵을 작성함으로써 분석하고자하는 시스템 내에서 요인들이 갖는 함의를 도출할 수 있다[27]. 직접영향 매트릭스를 통해서 계산한 영향성과 의존성의 점수에 따라서 직접 영향성-의존성 맵에 각 정책과제들을 위치시킬 수 있으며, 정책들의 위치에 따라서 정책특성을 파악할 수 있다. 맵은 총 6개의 영역으로 나누어진다. Z1(Zone 1) 영역은 영향 동인(influence drivers)으로 시스템의 상태를 설명하는 동인이다. Z2 영역은 핵심 동인(key drivers)으로 영향성과 종속성이 모두 높고 불안정한 동인이다. Z3 영역은 결과 동인(resultant drivers) 으로 결정 동인, 지연 동인에 의해 영향을 받는다. Z4 영역은 자율 동인(autonomous drivers)로 전체 시스템과 상대적으로 동떨어진 동인이다. Z5 영역은 규제 동인(regulating drivers)으로 향후 발전 사항에 대해서 설명하기 어려운 동인이다. 마지막으로 Z6 영역은 주변 동인(neighboring drivers)으로 보통의 경우 주변에 머무르다가 Z1 영역으로 움직이면서 지배적인 동인으로 진화할 수 있는 동인이다. 직접영향

Table 3. Direct impact matrix of information security policy for convergence industry

Policy task	①	②	③	④	⑤	⑥	Total influence
① Expansion of investment in information security industry		81	84	85	70	82	402 (3^{rd})
② Improvement of security industrial structure And support	90		80	73	83	91	417 (1^{st})
③ Development of source security technology	85	82		81	53	67	368 (6^{th})
④ Training information security personnel	88	80	83		78	83	412 (2^{nd})
⑤ Information security practice culture and awareness diffusion	77	83	57	81		90	388 (5^{th})
⑥ Enhancement of information security governance and improvement of legal system	86	87	66	73	82		394 (4^{th})
Total dependancy	426 (1^{st})	413 (2^{nd})	370 (4^{th})	393 (3^{rd})	366 (5^{th})	413 (2^{nd})	2381

매트릭스의 결과에 따라 직접 영향성-의존성 맵에 정책과제들을 위치시킨 결과는 Fig. 4.와 같다. 그 결과 정책 1부터 6은 모두 Z2(핵심 동인)에 위치하였다. 즉 설문 응답자들은 본 연구에서 제시한 6개의 융합산업 정보보호 정책과제가 모두 핵심적인 요인이라고 판단하였다. 또한 정책간 상호 의존도가 높아 제시된 정보보호 정책과제들 이 빠짐없이 시행되어야만 융합산업의 정보보호를 달성할 수 있다고 판단하였다. 그 중에서도 상대적으로 가장 영향성이 높은 정책은 '② 보안 산업의 체질개선 및 지원 강화'로 나타났다. 그 다음으로는 '④ 정보보호 인재양성', '① 정보보호산업 투자확대'인 것으로 나타났다. 가장 높은 의존성을 갖는 것으로 나타난 정책은 '① 정보보호 산업 투자확대'으로 나타났다. 그 다음으로는 '② 보안 산업의 체질개선 및 지원 강화', '⑥ 정보보호 거버넌스 강화 및 법제도 개선', '④ 정보보호 인재양성'이 높은 의존성을 갖는 정책인 것으로 나타났다. 직접영향 매트릭스와 직접 영향성-의존성 맵을 작성한 결과를 종합하면 다음과 같다. 첫째, 가장 영향성이 높은 정보보호 정책과제는 ②보안 산업의 체질개선 및 지원 강화였다. 설문에 응답한 전문가들은 보안 산업의 체질 개선과 지원 강화를 가장 중요하고 시급한 정보보호 정책과제인 것으로 판단하였다. 반면 ③원천 보안기술 개발을 가장 낮은 영향성을 갖는 것으로 판단하였다. 이는 '보안 선도 기술', '원천 기술 개발', '정보보호 핵심 기술 개발' 등이 다른 정보보호 정책과제에 비해 상대적으로 덜 중요하다고 판단하였거나, 핵심 보안 기술의 개발이 사실상 실현 가능성이 낮을 것이라고 예측한 것으로 판단된다. 둘째, 총 의존성이 가장 높은 정보보호 정책과제는 ① 정보보호산업 투자확대이며, 총 의존성이 가장 낮은 정책과제는 ③원천 보안기술 개발로 나타났다. 즉, 정보보호 거버넌스 강화와 법제도 개선이라는 정책과제는 다른 정책과제들의 성패 또는 시행 자체에 의해 큰 영향을 받는 정책과제라고 해석할 수 있다. 셋째, 앞서 살펴본 영향성과 의존성 결과는 정보보호 정책과제들 간의 상대적인 평가이며, 직접 영향성-의존성 맵을 작성한 결과 6개의 모든 정보보호 정책과제들이 Z2(핵심 동인, key drivers)에 속하는 것으로 나타났다. 핵심 동인(Key drivers)은 높은 영향성과 의존성을 지니고 있어 근본적으로 불안정한 요인이다. 따라서 본 연구에서 제시하였던 6개의 정보보호 정책과제들 모두는 정보보호목표 달성에 있어 매우 중요한 요인들인 것으로 분석되었다. 또한 각각의 정보보호 정책과제들의 시행이나 정책 성패에 따라서 다른 정책과제들이 큰 영향을 받게 될 것이라고 예상할 수 있다. 즉, 6개의 정보보호 정책과제들을 균형적으로 발전시킬 때에만 정보보호라는 목표를 온전히 달성할 수 있다고

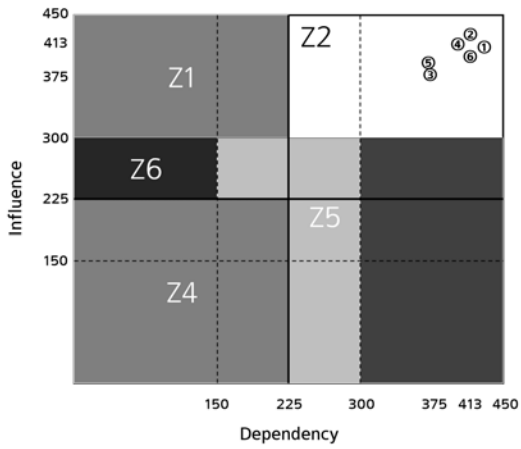


Fig. 4. Direct influence-dependency map of information security policy task for convergence industry

판단한 것으로 분석된다. 결과적으로 국내 ICT 융합산업의 정보보호정책을 분석하여 도출한 6개의 정보보호 정책과제들은 병렬적으로 동시 시행하는 것이 가장 바람직하다. 그러나 시간, 예산 등의 한계로 인하여 상대적인 우선순위를 판단하여 시행하여야 하는 경우라면 앞서 제시한 정보보호 정책과제의 영향성 순위에 따라 ②, ④, ①, ⑥, ⑤, ③의 순서로 시행하는 것이 바람직한 것으로 분석되었다.

4.1.2 ICT 융합산업 발전정책 내 정보보호정책의 우선순위

앞서 진행한 교차영향분석은 거시적인 관점에서 ICT 융합산업 전 분야의 정보보호 정책과제를 정의하고, 정보보호 정책과제 내에서 상대적인 영향성을 파악하고자 하였다. 한편, ICT 융합산업 발전정책의 개별 과제에서 요구되는 정보보호 정책과제는 ICT 융합산업 전 분야를 대상으로 하는 경우와는 상이할 것이라고 예상하였다. 따라서 이를 확인하기 위해 Table 2.와 같이 융합산업 발전정책에 따라 정보보호정책의 중요 순위를 1위부터 6위까지 매기는 방식으로 설문하였다. Table 2.의 설문응답 예시는 다음과 같이 해석된다. ICT 융합산업 발전정책 ①에서 가장 중요하게 고려해야 할 정보보호 정책과제는 ⑥번 정보보호 정책과제이며, 중요 순위대로 ②, ①, ③, ⑤, ④번 정보보호 정책과제가 시행되어야 한다고 판단한 것이라고 할 수 있다. Table 4.는 본 연구의 설문에 응답한 전문가 12명의 응답결과를 분석한 표이다. ICT 융합산업의 발전정책에 따라 함께 시행되어야 하는 정보보호정책을 설문하였으며, 설문 응답결과의 평균을 통해 응답자들의 의견을 종합하였다. 주요 결과를 살펴보면 다음과 같다. 먼저 '① 원스톱 개발체계 구축'에서 가장 중요하게 고려해야 하는 정보보호정책은 '② 보안 산업의 체질 개선 및 경쟁력 강화'라는 의견이 가장 높았다. '② 융합산업 인프라 및 생태계 구축'에서는 '② 보안 산업의 체질 개선 및 경쟁력 강화'가 중요하다는 의견이 가장 높았으며, 근소한 차이로 '① 정보보호 산업투자 확대'가 중요하다는 의견이 많았다. '③ 융합산업 맞춤인재 육성'이라는 정책에서는 '④ 정보보호 인재양성'가 가장 높은 우선순위를 차지하였다. '④ 개발·보안성 평가 등의 표준체계 개발'에서는 '⑥ 정보보호 거버넌스 강화 및 법제도 개선'이 가장 중요하다고 나타났다. '⑤ 신산업 육성을 위한 법제도 정비'에서는 '⑥ 정보보호 거버넌

Table 4. Priority of information security policy in ICT convergence industry development policy

Policy task		information security policy for ICT convergence industry					
		①	②	③	④	⑤	⑥
ICT convergence industry development policy	①	3.08 (2^{nd})	1.50 (1^{st})	3.50 (4^{th})	4.17 (5^{th})	5.08 (6^{th})	3.33 (3^{rd})
	②	2.58 (2^{nd})	2.50 (1^{st})	3.83 (4^{th})	3.92 (5^{th})	4.92 (6^{th})	3.25 (3^{rd})
	③	3.08 (2^{nd})	3.92 (4^{th})	3.75 (3^{rd})	1.83 (1^{st})	4.67 (5^{th})	3.75 (3^{rd})
	④	2.75 (2^{nd})	3.08 (3^{rd})	4.17 (4^{th})	4.75 (6^{th})	4.67 (5^{th})	1.58 (1^{st})
	⑤	3.42 (3^{rd})	3.00 (2^{nd})	4.50 (6^{th})	4.25 (4^{th})	4.33 (5^{th})	1.50 (1^{st})
	⑥	2.67 (2^{nd})	3.25 (3^{rd})	4.25 (5^{th})	4.17 (4^{th})	4.25 (5^{th})	2.42 (1^{st})

스 강화 및 법제도 개선'이 가장 중요하다는 의견이 많았으며, '⑥ 융합산업의 정보보호 인프라 강화'에서는 '⑥ 정보보호 거버넌스 강화 및 법제도 개선'과 '① 정보보호 산업투자 확대'가 중요하다는 의견이 높았다. 앞선 Fig. 4.의 교차영향분석 결과와 Table 4.를 통해 확인한 주요 내용은 다음과 같다. 첫째, 영향성 및 의존성이 가장 높은 것으로 나타난 정보보호 정책과제 ②, ④, ①, ⑥은 ICT 융합산업 발전정책 내의 우선순위 역시 상대적으로 높은 것으로 나타났다. 이는 ICT 융합산업의 전체를 대상으로 했을 때 중요한 정보보호 정책과제와 융합산업의 개별 발전정책을 대상으로 했을 때 중요한 정보보호 정책과제가 크게 다르지 않다는 것을 나타낸다. 둘째, 각 발전정책마다 정보보호 정책과제의 중요 순위가 상이하다. 발전정책 ①, ②에서는 정보보호 정책과제 ②가 가장 중요하며, 발전정책 ③에서는 정보보호 정책과제 ④가 가장 중요하다는 의견이 많았다. 그리고 발전정책 ④, ⑤, ⑥에서는 정보보호 정책과제 ⑥이 가장 중요한 것으로 나타났다. 즉, 정보보호 정책과제만을 비교하는 경우 상대적으로 중요도가 높은 정책과제는 ②, ④, ①, ⑥이지만, ICT 융합산업 발전정책을 고려하는 경우엔 정보보호 정책과제의 중요 순위가 달라질 수 있다는 것을 의미한다. 따라서 각 산업에서는 효과적인 정보보호 정책시행을 위해 중요한 정보보호 정책과제를 선별하여 우선 시행해야 할 필요가 있다는 것을 의미한다.

V. 결 론

본 연구의 결과를 요약하자면 다음과 같다. 본 연구는 정보보호를 고려한 ICT 융합산업의 균형발전이라는 목표를 달성하기 위해 필요한 효과적인 정보보호정책의 시행방향에 대한 시사점을 도출하고자 하였다. 이를 위해 국내 ICT 융합산업의 발전정책과 정보보호정책을 수집하여 각각 6개의 정책과제로 축약하였다. 이를 통해 설문지를 구성하여 총 12명의 전문가 의견을 종합하였고, 교차영향분석 방법을 통해 직접영향 매트릭스와 직접 영향성-의존성 맵을 작성하여 분석하였다. 그 결과 ICT 융합산업의 정보보호 정책과제 중 상대적으로 중요성이 높은 정책으로는 '보안 산업의 체질 개선 및 경쟁력 강화', '정보보호 인재양성', '정보보호 산업투자 확대', '정보보호 거버넌스 강화 및 법제도 개선' 등의 순서로 중요도가 높은 것으로 나타났다. 한편 상대적으로 의존성이 높은 정책과제와 의존성이 낮은 정책과제를 분류하여 동반 시행이 필요한 정보보호정책그룹을 제시하였다. 또한 ICT 융합산업의 발전정책과 더불어 시행이 필요한 정보보호 정책과제가 무엇인지 제시하였다. 그 결과, 각 발전정책 별 중요 정보보호 정책이 달라진다는 결과를 얻었다. 이를 통해 정보보호 정책과제 중 상대적으로 더 중요한 정책은 무엇이며, ICT 융합산업의 발전정책과 정보보호정책의 연계를 고려하는 경우 각 발전정책 별로 중요시해야 할 정보보호 정책과제는 무엇인지에 대해 제시하였다. 본 연구의 시사점은 다음과 같다. 융합산업 또는 4차 산업혁명의 진행이 가속화되면서 정보보호의 중요성은 날로 강조되고 있다. 그러나 산업 발전이 우선시되고 정보보호가 산업의 발전을 저해할 수 있다는 인식 때문에 정보보호는 그 중요성에 비해 등한시되는 경향이 있다. 이 같은 상황이 지속된다면 향후 정보보호에 실패할 가능성이 더욱 높아질 것으로 우려된다. 현실과 가상이 밀접하게 연결된 미래 사회에서 정보보호의 실패는 단순히 정보의 기밀성, 무결성, 가용성의 침해가 아니라 개인의 재산과 생명, 그리고 한 기업의 존폐까지 위협하는 위험으로 진화할 것이다. 이에 본 연구는 ICT 융합산업의 효과적인 정보보호 정책의 시행을 위한 우선순위와 병행 시행되어야 하는 정책들의 그룹을 제시하였다는 것에 의의가 있다. 또한 ICT 융합산업의 세부 정책과제와 더불어 특히 중요하게 고려해야 할 정보보호 정책과제가 무엇인지 제시하였다. 이를 통해 산업의 발전정책과 정보보호정책이 이원화되어 진행됨으로 인해 발생하는 불합리성을 감소시킬 수 있는 방향을 제시하고자 하였다. 즉 중요한 부분에 인력과 자원이 먼저 투입될 수 있도록 함으로써 효과적인 정보보호의 달성에 도움이 될 것으로 기대한다.

한편 본 연구의 한계는 다음과 같다. 첫째, ICT 융합산업의 전체를 광범위하게 다루었기 때문에 특정 산업에서 요구되는 정보보호정책의 우선순위에 대해서는 파악하기 어렵다는 한계가 있다. 예를 들어 스마트 팩토리 운영에 있어서 정보보호정책의 우선순위는 본 연구의 결과를 참고할 수 있으나 직접적으로 제시하고 있지는 않다. 둘째, 본 연구의 설문에 응답 가능한 모집단이 매우 제한되어 있어 많은 수의 설문 응답을 수집할 수 없었다. 물론 각 분야의 전문가들의 의견이라는 점에서 본 연구의 결과를 수용할 수 있으나, 상대적으로 적은 수의 응답을 통해 분석하였으므로 특정 개인의 의견이 과대 반영되었을 가능성이 있다. 셋째, 본 연구에서 활용한 방법론인 교차영

향분석은 다소 생소한 방법론이다. 따라서 응답자들이 설문의 내용과 설문응답 방법을 충분히 이해하지 못하였을 가능성이 있다. 또한 교차영향분석의 방법론적인 특징으로 인하여 유사한 형태의 질문이 반복적으로 제시되어 설문응답자들에게 '피로효과'가 발생되었을 가능성이 있다[28]. 피로효과란 설문응답자가 설문 도중에 지치거나 응답하기 어려운 문항을 마주하게 되어 설문 후반부에 부정확한 응답을 보이는 경우를 말한다. 본 연구에서는 피로효과를 억제하기 위해 설문 내용의 모호함을 없애고, 중복되는 것처럼 느껴지지 않도록 노력하였다. 그러나 향후 연구에서는 응답자의 응답신뢰도를 향상시킬 수 있는 추가적인 대책을 마련해야 할 필요성이 있다. 이에 향후연구에서는 다음과 같은 점을 보완할 필요가 있다. 첫째, 본 연구에서 ICT 융합산업을 거시적 관점에서 다룬 것과 달리, 특정 산업으로 한정하여 정보보호 정책의 우선순위를 제시하는 연구가 진행될 필요가 있다. 둘째, 김도관과 홍성희[29]의 미래연구 방법론에 관한 연구에 의하면 복수의 방법론을 함께 사용하는 것이 예측의 효율성과 정확성 측면에서 유리하다고 주장하였다. 따라서 향후 연구에서는 교차영향분석 이외에 다양한 예측 기법을 동시에 활용하여 연구를 진행할 필요가 있다.

References

[1] Korea Institute of Science and Technology Evaluation and Planning, Seeking Strategic Response to Future Society Changes in the Age of the Fourth Industrial Revolution, 2016.

[2] Schwab, K., The Fourth Industrial Revolution, Crown Business, 2017.

[3] Coppola, R. and Morisio, M., "Connected car: technologies, issues, future trends," ACM Computing Surveys (CSUR), vol. 49, no. 3, pp. 1-36, Dec. 2016.

[4] Hyun-Sook Ryu, "A study on cyber security policy and governance for ICT convergence environments," Basic Research Projects, pp. 1-349, 2015.

[5] Jung-Deok Kim, "A study on national information security issues and policy plans," Journal of Digital Convergence, vol. 10, no. 1, pp. 105-111, 2012.

[6] Byung-Woon Kim, "Secured connected industrial society, cyber security policy," Science and Technology Research, vol. 22, no. 3, pp. 85-122, 2016.

[7] Young-Jin Shin and Sung-Tae Kim, "Strategic priority analysis of information security policy - focusing on policy comparison using AHP technique," Korea Policy Review, vol. 13 no. 3, pp. 29-63, 2004.

[8] Wook-Jun Sung, and Dong Wook Kim, "A study on the priority of information security policy using analytic hierarchy process," Academic Publications of The Korean Association for Public Administration, pp. 1614-1634, June. 2011.

[9] Young-Jin Shin, Hyung-Chul Jung, & Won-Young Kang, "Priority analysis of public information privacy policy enforcement tasks," Journal of the Korea Institute of Information Security and Cryptology, vol. 22, no.2, pp. 379-390, 2012.

[10] Korea Information Technology Promotion Agency, Future Strategic Research Methodology for Establishing Successful Public Policy (FROM) version 1.0. 2009.

[11] Jin-Han Kim and Sung-Hong Kim, "A study on the domestic IT environment scenarios through the application of cross-impact analysis," Korean Management Science Review, vol. 21, no. 3, pp. 129-147, 2004.

[12] Choi, C., Kim, S., and Park, Y, "A patent-based cross impact analysis for quantitative estimation of technological impact: The case of information and communication technology," Technological Forecasting and Social Change, vol. 74, no. 8, pp. 1296-1314,

2007.
〔13〕 Seung-Jun Yeon, Seong-Hyun Hwang, Hyo-Jung Jun, and Tae-Sung Kim, "Design of broadcasting convergence policy package through cross impact analysis," Telecommunications Review, vol. 20, no. 1, pp. 10-20, 2010.
〔14〕 Jun-Sang Yoo and Hee-Sang Lee, "Analysis of technology convergence based on patent," Proceedings of KIIS Fall Conference, pp. 1105-1133, 2013.
〔15〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, K-ICT Security Development Strategy for Industrialization of Creative Economy Food for Food Industry, 2015
〔16〕 Ministry of Science, ICT and Future Planning, Three-Year Implementation Plan for Internet Information Protection Roadmap, 2015
〔17〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, "Information Protection Measures for Activating Cloud Services," 2015
〔18〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, K-ICT Convergence Security Development Strategy for the Implementation of ICT Convergence Trusted Society and Fostering New Information Industry, 2016.
〔19〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, The First Information Security Industry Promotion Plan for Fostering the Information Security Industry and Creating Professional Jobs, 2016.
〔20〕 Ministry of Science, ICT & Future Planning, K-ICT Strategy for Realizing Creation Economy, 2015.
〔21〕 Ministry of Trade, Industry and Energy and Ministry of Science, ICT & Future Planning, Smart Manufacturing R&D Mid-term Roadmap, 2016.
〔22〕 Ministry of Science, ICT & Future Planning, Basic Internet of Things for Realizing the Leading State of Digital Revolution, 2014.
〔23〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, 5G Mobile Communication Industry Development Strategy, 2015.
〔24〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, Cloud Industry Development Plan (draft), 2014.
〔25〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, Big Data Industry Development Strategy for Creative Economy and Government 3.0 Support, 2013.
〔26〕 Ministry of Science, ICT & Future Planning and Ministry of Relations, Next-Generation Smart Device Korea 2020 Prepares for Super-Connected Age, 2015.
〔27〕 Miles, I., Keenan, M., and Kaivo-Oja, J, Handbook of Knowledge Society Foresight, PREST and FFRC, 2002.
〔28〕 Bradburn, N. M., and Mason, W. M., "The effect of question order on responses," Journal of Marketing Research, vol. 1, no. 4, pp. 57-61, Nov. 1964.
〔29〕 Do-Kwan Kim and Sung-Hee Hong, Future Trend and Future Research Methodology, Future Economic Research Center, Busan Development Institute, 2007.

〈저자소개〉

이 동 희 (Dong-Hee Lee) 학생회원
2015년 8월 : 충북대학교 경영정보학과 학사
2018년 2월 : 충북대학교 정보보호경영학과 석사
2018년 3월~현재: (주)싸이버원 재직
〈관심분야〉 정보보호정책, 정보보호관리체계, 개인정보보호

전 효 정 (Hyo-Jung Jun) 정회원
2001년 2월: 충북대학교 경영정보학과 학사
2003년 8월: 충북대학교 경영정보학과 석사
2003년 9월~2007년 5월: 한국전자통신연구원 사업기획팀 기술원
2014년 2월: 충북대학교 경영정보학과 박사
2014년 3월~ 2017년 2월: 충북대학교 정보보호경영학과 Post-Doc
2018년 1월~ 현재: 충북대학교 글로컬 보안컨설팅 전문인력 양성사업단 Post-Doc
〈관심분야〉 정보보호정책, 정보보호인력, 정보자원관리, 보안경제성

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수, 보안경제연구소장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, ISMS/PIMS 인증위원회 위원, 한국전력 정보보호 자문위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책의사결정