

보안경제성 연구동향 분석 : IS 저널 중심으로

강미화* · 김태성**

Research Trends in Information Security Economics : Focused on Information Systems Journals

Mi-Hwa Kang* · Tae-Sung Kim**

Abstract

As numerous security breaches on a variety of information assets such as personal information, corporate secrets, computer servers, and networks have occurred, information security has emerged as a critical social issue. However, researches on economically rational information security decision-making have been few. Such researches are especially rare in South Korea where information security is considered to be a discipline of engineers. This study aims to identify the preferred themes and methodologies of information security economics research in the field of information systems by reviewing papers published in *Management Information Systems Quarterly (MISQ)*, *Information Systems Research (ISR)*, *European Journal of Information Systems (EJIS)*, *Management Science (MS)*, and *Information and Management (I&M)*. We hope that the results of the study will be helpful in rational managerial or policy decision-making for practitioners and suggest future research topics for researchers.

Keywords : Information Security Economics, Decision-Making, Information Systems Journal, Research Trends

Received : 2016. 02. 12. 1st Revised : 2016. 03. 04. 2nd Revised : 2016. 03. 20. Final Acceptance : 2016. 03. 22.

* We appreciate Sangsan Brick Co. supporting this research by the development fund of the Chungbuk National University.

본 논문은 2015년 한국경영정보학회 춘계학술대회에서 발표된 내용을 수정 및 보완한 것임.

* A3 Co., Ltd., e-mail : no1tkatnsdl@hanmail.net

** Corresponding Author, Department of Management Information Systems, Graduate Program of Information Security Management, Chungbuk National University, 1, Chungdae-ro, Seowon-gu Cheongju-si, Chungcheongbuk-do, 28644, Korea, Tel : +82-43-261-3343, e-mail : kimts@cbnu.ac.kr

1. 서론

정보유출사고는 한 개인의 문제를 넘어서서 사회적인 문제로 대두되었다. 2014년 한 해에 발생한 정보유출사고만 해도 피해비용이 9조 원을 넘는 것으로 파악되었다[National Disaster Management Institute, 2015]. 정부는 정보유출 사고를 예방하기 위해 정보보호산업 기반 강화, 글로벌 원천 보안기술 개발, 최고 보안인재 양성 및 정보보호 실천문화조성, 사이버 보안 복원력 제고 등 정보보호산업 발전 전략을 제시하고 있다[Ministry of Science, ICT and Future Planning, 2015]. 그러나 정보보안 관련 문제는 다양한 요소들이 복잡하게 얽혀있어서 해결하기 쉽지 않다. 이를 해결하기 위해서는 정보보안을 공학적 관점으로만 접근하는 것이 아닌, 경제학, 심리학, 사회학 등의 관점으로 접근할 필요가 있다[Odlyzko, 2003]. 특히, 정보보안은 합리적인 위협 관리의 문제이므로 경제학적 관점을 활용할 필요가 있다[Anderson, 2001].

정보보안을 경제학적 관점으로 분석할 필요성을 느낀 연구자들은 다양한 주제와 방법론으로 활발하게 연구결과를 발표하였고, 보안경제성 관련 연구들이 상당수 진행됨에 따라 보안경제성 관련 연구에 대한 리뷰 연구도 시도되었다. 리뷰 연구의 결과는 보안경제성 관련 연구가 시작된 시점부터 현재까지의 연구현황을 한눈에 파악할 수 있게 한다. 그러나 이전 연구들은 주로 특정 시점에서 연구현황을 보여주는 정성적인 분석을 시도하였고, 이로 인해 시간흐름에 따른 연구동향을 파악하기 어렵다는 한계점을 가진다.

본 연구에서는 정량적인 분석으로 보안경제성 관련 연구동향을 파악하기 위해, Management Information Systems Quarterly(MISQ), Information Systems Research(ISR), European Journal of Information Systems(EJIS), Manage-

ment Science(MS), Information and Management(I&M) 등 5개의 IS 저널에서 발표된 보안경제성 관련 논문들을 검토하였고, 논문별로 주제 및 방법론을 분류한 정량적 데이터를 기반으로 보안경제성 관련 연구들이 선호하는 주제 및 방법론을 분석하였으며, 이를 통해 보안경제성 관련 연구자들이 향후 선호하게 될 주제 및 방법론을 예측하였다. 본 연구의 결과로 연구자들에게는 향후 유망한 연구 주제를 제공하고, 실무자들에게는 합리적인 정보보호 의사결정에 대한 지침을 제공하고자 한다.

2. 이론적 배경

2.1 보안경제성 관련 연구

상당수의 학자들이 정보보호¹⁾와 경제학의 밀접한 연관성에 대해 주장하였다. Anderson[2001]은 정보보안의 많은 문제가 미시경제학으로 보다 명확하고 설득력 있게 설명될 수 있으며, 보안 공학은 합리적인 위협 관리의 문제이므로 정보보호 평가자는 기술적인 도구뿐만 아니라 경제적 도구도 활용해야 한다고 주장하였다. Odlyzko[2003]은 정보보호는 고립된 제품이 아니고 복잡한 경제의 한 구성 요소이며, 사람과 기술이 조화되지 않으면 구현하는데 많은 비용이 들기 때문에 심리학과 사회학을 고려한 요인들과의 경제적 절충이 필요하다고 주장했다.

정보보호를 경제학적 관점으로 분석한 연구들도 상당수 등장하였다. Anderson et al.[2009]은 유럽 연합(EU) 내에서 안전한 전자 통신에 대한 시장의 실패를 조사하고 정책 권고 사항을 마련하기 위해, 네트워크 및 정보보호에 대한 실질적인 문제를 정보의 비대칭성, 외부 효과,

1) '정보보호'와 '정보보안'에 해당하는 영문 용어는 information security이다. 본 연구에서는 두 가지 용어를 동일한 의미로 문맥에 적합하게 혼용하였다.

책임 회피, 다양성의 부족, 법률과 법 집행의 분열의 5가지로 분류하고, 보안경제학을 기반으로 분석하였다. Moore[2010]은 사이버 보안에 대한 경제 문제인 왜곡된 인센티브, 정보의 비대칭, 외부 효과를 설명하고, 이를 해결 할 수 있는 정책을 제안하였다.

보안경제성 관련 연구는 활발하게 진행되고 있으며, 보안경제성 관련 연구자들의 작업은 새로운 도메인인 일반적인 보안의 경제성, 신뢰성의 경제성 등에 과급되고 있다[Anderson and Moore, 2006]. Anderson과 Moore[2006]은 보안경제성 관련 연구에서 최근의 결과와 실제 연구 과제를 컴퓨터 시스템의 설계 및 구축에 왜곡된 인센티브, 외부 효과의 영향, 취약점의 경제학, 프라이버시의 경제학, 네트워크 토폴로지의 정보보안 분석 등을 중점으로 검토하였고, Moore와 Anderson[2011]은 보안경제성 연구들을 4가지 주요 영역(공격과 방어에 대한 모델링, 개인정보 침해, 악성코드와 봇넷, 지불 시스템 보안) 및 4가지 방법론(이론적 연구, 경험적 연구, 행동적 연구, 연구와 정책의제)으로 분류하여 연구동향을 분석하였다.

본 연구는 Moore와 Anderson[2011]의 기술적인(descriptive) 성격의 연구를 IS 저널 발표 논문에 대한 정량적인(quantitative) 분석으로 확장한 것이다.

2.2 정보시스템 및 정보보호 분야의 리뷰 연구

리뷰 연구를 위한 방법론에 대한 고찰을 하기 위해, 정보시스템 및 정보보호 분야의 리뷰 연구들을 대상으로 연구범위, 검색방법, 분류방법, 분류기준, 분석방법 등을 중심으로 살펴보았다. 정보보호 분야의 리뷰 연구가 많지 않아, 관리적 측면의 정보보호 연구가 많이 수행된 정보시스템 분야의 리뷰 연구들도 살펴보았다[Jun et al., 2008].

연구범위는 크게 저널 및 컨퍼런스(프로시딩)

을 선정할 경우와 연구검색용 데이터베이스를 선정한 경우로 나누어 볼 수 있다. 선정된 저널 및 컨퍼런스 또는 연구검색용 데이터베이스의 수는 적게는 1개부터, 많게는 21개까지 있었고, 평균 약 4개가 선정되었다. 검색방법은 용어를 입력하여 검색한 경우가 대부분이었으며, 검색된 논문들이 인용한 논문들을 포함한 경우[Belanger and Crossler, 2011]도 있다. 검색기간은 크게 특정 기간으로 제한하여 검색하거나, 제한하지 않고 전체를 대상으로 검색하는 경우로 나누어 볼 수 있다. 특정기간으로 제한하여 검색하는 경우는 짧게는 3년부터, 길게는 15년까지 있었고, 평균 약 10년으로 검색기간을 제한하였다. 분류방법은 2~3명의 연구자가 직접 검토한 후 분류한 경우가 대부분이었다. 분류기준은 주제, 방법론, 분석수준, 학문분야, 저자정보 등을 활용한 경우가 대부분이었으며, 동시인용[Córdoba, 2012], 명사구[Mustafee, 2011]를 활용한 경우도 있었다. 분석방법은 크게 정량적인 분석과 정성적인 분석으로 나누어볼 수 있다(<Table 1> 참조).

본 연구는 분류기준에 해당되는 논문의 수를 파악하는 정량적인 분석을 목적으로 하고 있기 때문에, 정량적인 분석을 한 연구들을 중심으로 좀 더 상세하게 살펴보았다. 그 중에서도 주제와 방법론 등을 중심으로 분석한 연구들을 집중적으로 살펴보았다. 분석대상으로 사용된 논문 및 책은 적게는 142개부터, 많게는 1,280개까지, 평균 약 542개였다. 분류기준은 방법론, 주제, 저자정보, 분석수준, 학문분야 순으로 많았다(<Table 2> 참조). 상위 33명 저자의 연구주제, 선호 연구방법론, 소속을 분류한 경우[Palvia et al., 2007], 정보유형, 기술적 속성, 프라이버시 정의 유형을 분류한 경우[Smith et al., 2011]도 있었다. 분류에서 중복을 허용한 경우도 있다. Palvia et al. [2007]은 연구 당 주제는 3개까지, 방법론은 2개까지 중복을 허용하였다.

〈Table 1〉 Review Research of Information Systems and Information Security

Author	Research Field	Research Scope (Number of DBs or journals)		Classification Standard	Research Period (years)	Analysis Method
Swanson and Ramiller[1993]	Information Systems	Journals and Conferences	1	Theme	6	Qualitative Analysis
Banker and Kauffman[2004]			1	Theme, Methodology, etc.	unlimited	
Palvia et al.[2007]			1	Theme, Methodology, etc.	8	Quantitative Analysis
Mustafee[2011]			2	Noun phrase	14	
Córdoba et al.[2012]			2	Co-citation	14	
Davies[2012]			3	Methodology, Researchers Information, etc.	3	
Siponen and Willison [2007]	21	Theme, Methodology	15			
Smith et al.[2011]	Information Systems Privacy	Research Database	3	Theme, Methodology, etc.	unlimited	
Bélanger and Crossler[2011]			3	Theme, Methodology, etc.	unlimited	

〈Table 2〉 Preference of Classification Standard

Author	Theme	Methodology	Level of Analysis	Researchers Information	Academic Field
Palvia et al.[2007]	O	O		O	
Siponen and Willison [2007]	O	O			
Bélanger and Crossler[2011]	O	O	O		
Smith et al.[2011]	O	O	O		O
Davies[2012]		O		O	

3. 연구방법

3.1 용어정의

보안경제성 관련 연구동향을 파악하기 전에 먼저 ‘보안경제성 관련 연구’가 무엇인지 정의하고자 한다. 정보보안을 경제적 관점으로 접근한 연구들을 포괄하는 용어가 명확하지 않아 본 연구에서는 이를 ‘보안경제성’이라 명명하였고, 사전적 의미 등을 참고하여 다음과 같이 정의하

였다. 보안경제성이란 ‘컴퓨터 또는 네트워크상의 정보의 훼손, 변조, 유출 등을 방지하기 위한 재물, 자원, 노력, 시간 따위가 적게 들면서도 이득이 되는 성질²⁾’을 의미하고, 보안경제성 관련 연구란 ‘정보보안 관련 현상 및 문제를 경제적 관점으로 분석한 연구 또는 연구결과가 개인 및 조직의 정보보안 관련 의사결정에 도움이 되는

2) 지식경제부(현 산업통상자원부)의 ‘정보보안’ 정의, 국립국어원의 ‘경제성’ 정의를 참고하여 보안경제성을 정의하였다[Ministry of Knowledge Economy, 2008].

〈Table 3〉 Preference of IS Field Journal

Code	Journal Name	Frequency	References (Research which included each journal in its review scope.)
MISQ	Management Information Systems Quarterly	5	Culnan and Swanson[1986], Siponen and Willison[2007], Mustafee[2011], Davies[2012], Córdoba et al.[2012]
ISR	Information Systems Research	3	Swanson and Ramiller[1993], Siponen and Willison[2007], Davies[2012]
EJIS	European Journal of Information Systems		Siponen and Willison[2007], Mustafee[2011], Córdoba et al.[2012]
MS	Management Science	2	Culnan and Swanson[1986], Banker and Kauffman[2004]
I&M	Information and Management		Palvia et al.[2007], Siponen and Willison[2007]

연구³⁾를 의미하며, 이를 기반으로 본 연구를 진행하였다.

3.2 연구범위

본 연구는 Management Information Systems Quarterly(MISQ), Information Systems Research (ISR), European Journal of Information Systems (EJIS), Management Science(MS), Information and Management(I&M) 등 정보시스템 분야의 저널 5개를 대상으로 정보보호경제성 관련 연구를 검색하였다. 연구 대상으로 선정된 5개 저널은 정보보호 및 정보시스템 관련 리뷰연구의 연구범위에 포함된 횟수가 많은 상위 5개의 저널이다(<Table 3> 참조). MS는 1954년부터 매월, MISQ는 1977년부터 매분기, I&M은 1977년부터 1~2개월마다, ISR은 1990년부터 매분기, EJIS는 1991년부터 격월로 발행되고 있다. 본 연구에서는 2014년 10~11월 동안 검색된 논문을 대상으로 분류를 하였는데, 검색기간은 제한을 두지 않고 전체 발행기간을 범위로 하였으며, 검색경로는 각 저널에서 운영하거나 연계된 사이트를 범위로 진행하였다.

3.3 연구방법

본 연구는 정량적인 분석으로 보안경제성 관련 연구동향을 파악하기 위해, MISQ, ISR, EJIS, MS, I&M 등 5개의 IS 저널에서 발표된 보안경제성 관련 논문을 찾아내었고, 발견된 보안경제성 관련 논문들을 대상으로 주제 및 방법론을 분류하였으며, 분류된 정량적 데이터를 기반으로 선호되는 주제 및 방법론을 분석하였다. 본 연구는 보안경제성 관련 연구를 개괄적으로 파악하는데 중점을 두어, 개별 논문이 분석단위가 되며, 세부적으로는 주제, 방법론 등에 관심을 갖는다.

본 연구에서는 보안경제성 관련 논문을 찾아내기 위해, 보안경제성 관련 검색용어⁴⁾를 기반으로 각 저널 사이트를 직접 검색하였고, 검색된 논문들의 초록 또는 전문을 검토하여 보안경제성 관련 연구를 선별하였다. 보안경제성 관련 검색용어는 보안경제성 관련 주제만을 다루고 있는 학술대회인 Workshop on the Economics of Information Security(WEIS)에서 발표된 논문들의 키워드에서 추출한 보안 관련 용어와 경제성 관련 용어를 조합하여 만들었다(<Table 4> 참조).

3) 온라인 백과사전인 위키피디아(Wikipedia)에서는 'Economics of security'가 컴퓨터 보안 및 개인정보보호와 관련한 경제적 측면, 개인/조직의 의사결정 및 행동, 공학설계 의사결정 등을 해결한다고 설명하고 있다.

4) 기존 발간된 논문들의 키워드(keyword)와 본 연구에서 사용한 논문 검색 기준과 구분하기 위해 '검색용어'라는 용어를 사용하였다.

〈Table 4〉 Security and Economics Related Terms

Area	Term	Frequency
Security	security, anonymity, attack, bitcoin, botnet, breach, crime, cryptology, denial of service attacks, digital forensics, DRM(Digital Rights Management), encryption, hackers, malware, phishing, privacy, protection, spam, virus, vulnerability	23
Economics	economic, accounting, benefits, cost, decision making, demand, e-commerce, finance, incentive, insurance, investment, loss, manage, money, moral hazard, Nash equilibrium, optimal, policy, price, regulation, risk, ROI(Return On Investment), standard	20

검색의 편의성을 높이기 위해, 사전 검색과정을 통해 보안 관련 용어와 경제성 관련 용어를 각각 축소하였다. 용어 축소를 인해 보안경제성 관련 연구가 검색결과에서 누락되는 일이 없도록 주의하였다. 보안 관련 용어 축소의 경우, 보안 관련 용어(23개)와 경제성 관련 용어를 대표할 수 있는 'Economic'을 조합한 용어(23개)들로 검색을 한 후, 검색결과가 다른 용어의 검색결과에 포함되는 보안 관련 용어를 제외하는 방식으로 진행하였다. 예를 들면, 아래와 같은 경우 보안 관련 용어 중 'Cryptology'를 제외하였다.

- 'Security Economic'으로 검색한 논문 목록 :
논문 A, 논문 B, 논문 C, 논문 D, 논문 E,
논문 F, 논문 G, 논문 H (총 8개)
- 'Cryptology Economic'으로 검색한 논문 목록:
논문 B, 논문 C, 논문 F (총 3개)

위와 동일한 방법으로 경제성 관련 용어(20개)와 보안 관련 용어를 대표할 수 있는 'Security'를 조합하여 경제성 관련 용어도 축소하였다. 저널마다 사전 검색과정을 진행하여 보안 및 경제성 관련 용어를 축소하였고, 그 결과로 축소된 용어는 저널마다 달랐다. 축소된 용어를 기반으로 '보안 관련 용어(N개)'와 '경제성 관련 용어(M개)'를 조합하여 보안경제성 관련 검색용어(M×N개)를 만들었다.

축소된 보안경제성 관련 검색용어를 기반으로 논문을 검색한 결과, MISQ가 48개, ISR이 42개, EJIS가 26개, MS가 217개, I&M이 79개로 총

412개가 검색되었다. 검색된 논문들의 초록 또는 전문을 검토하여 보안경제성 관련 논문을 선별한 결과, MISQ가 29개, ISR이 33개, EJIS가 21개, MS가 27개, I&M이 30개로 총 140개가 선별되었다. 저널별로 논문 수는 큰 차이가 없으며, 한 저널 당 평균 약 28개의 논문이 발견되었다. 보안경제성 관련 논문 수(A)에 검색된 논문 수(B)를 나누어 검색정확도(A/B)를 구한 결과, MISQ가 60%, ISR이 79%, EJIS가 81%, MS가 12%, I&M이 38%의 검색정확도를 보였으며, 전체적으로는 34%의 검색정확도를 보였다. 검색정확도가 낮아진 주된 이유는 Security를 국가안보 또는 증권의 의미로 사용한 경우가 많았기 때문이다. 전문을 구하지 못하여 초록만 확인이 가능한 경우는 MISQ가 1개(3%), ISR이 5개(15%), EJIS가 13개(62%), MS가 3개(11%), I&M이 6개(20%)로 총 28개(20%)이다.

발견된 보안경제성 관련 논문들의 초록 또는 전문을 연구자가 직접 검토하여 주제 및 방법론을 분류하였다. 초록만으로 분류하기 어려운 경우에만 전문을 검토하여 분류하였으며, 초록만 확인이 가능한 경우에는 초록만 검토하여 분류하였다. 연구의 주제와 방법론은 각각 1개씩만을 허용하였으며, 연구의 주제 또는 방법론이 복합적인 경우는 연구에서 차지하는 비중이 더 큰 주제 또는 방법론으로 분류하였다.

보안경제성 관련 연구들을 주제와 방법론으로 분류하기 위해, 주제와 방법론의 분류기준을 각각 정하였다. 보안경제성 관련 연구들의 세부 분야 등이 명확하지 않아, 본 연구에서는 WEIS

〈Table 5〉 Research Themes of WEIS(2011~2014)

Ref.	Research Theme	11	12	13	14
CfP1	Optimal Investment in Information Security	0	0	0	0
CfP2	Models and Analysis of Online Crime	0	0	0	0
CfP3	Risk Management and Cyber-Insurance	0	0	0	0
CfP4	Security Standards and Regulation	0	0	0	0
CfP5	Cyber-Security and Privacy Policy	0	0		0
CfP6	Cyber-Defense Strategy and Game Theory	0	0	0	0
CfP7	Security and Privacy Models and Metrics	0	0	0	0
CfP8	Economics of Privacy and Anonymity	0	0	0	0
CfP9	Behavioral Security and Privacy	0	0	0	0
CfP10	Vulnerability Discovery, Disclosure, and Patching	0	0	0	0
CfP11	Incentives for Information Sharing and Cooperation	0	0	0	0
CfP12	Incentives Regarding Pervasive Monitoring Threats				0
CfP13	Psychology of Risk and Security	0		0	

〈Table 6〉 Classification Standard of Theme

Code	Theme	Detailed Theme	Code	Ref.
RA&SI	Risk Assessment and Security Investment	Optimal Security Investment	OSI	CfP1
		Risk Assessment and Cyber-Insurance	RA&CI	CfP3
CC&CD	Cyber-Crime and Cyber-Defense Strategy	Models and Analysis of Online Crime	CM&CA	CfP2
		Cyber-Defense Strategy and Game Theory	DS>	CfP6
SS&SP	Security Standards and Policy	Security Standards and Regulation	SS&SR	CfP4
		Security and Privacy Policy	SP&PP	CfP5
PV&AV	Privacy and Anonymity Value	Privacy and Anonymity Value	PV&AV	CfP8
VM	Vulnerability Management	Vulnerability Discovery, Disclosure, and Patching	V-DDP	CfP10
		Incentives for Vulnerability Disclosure and Cooperation	I-V-DC	CfP11

의 연구주제를 참고하여 주제 분류기준을 추출하였다. WEIS의 연구주제를 파악하기 위하여 WEIS의 13개년(2002년~2014년) 동안의 Call for Paper를 분석하였고, 그 결과 2011년부터 2014년까지의 Call for Paper가 일관된 패턴을 보이는 것을 발견할 수 있었다(<Table 5> 참조).

2011년~2014년에는 해마다 11~12개의 연구주제가 제시되었고, 중복을 제거하면 총 13개이다. 13개의 연구주제 중 방법론적인 내용을 담고 있는 연구주제 2개(Behavioral Security and Privacy, Security and Privacy Models and Metrics)와 4개년 동안 2번 이하로 제시된 연구주제 2개(Incentives Regarding Pervasive Monitoring Threats,

Psychology of Risk and Security)를 제외한 연구주제 9개를 주제 분류기준으로 추출하였다. 분석대상 논문 수 대비 주제 분류기준 수가 많아 전반적인 연구동향을 파악하는데 어려움이 있을 것이라 판단되어, 연관성을 고려하여 9개의 주제 분류기준을 5개로 그룹화 하였고, 모든 주제를 포괄할 수 있으면서 분류기준 간에는 배타적일 수 있도록 일부 단어를 수정하였다.

본 연구의 주제 분류기준은 위협 평가 및 보안 투자(RA&SI), 사이버 범죄와 방어 전략(CC&CD), 보안 표준 및 정책(SS&SP), 프라이버시 및 익명의 경제성(PV&AV), 취약점 관리(VM)이며, 세부 분류기준은 <Table 6>과 같다.

각 주제 분류기준에 포함된 연구는 다음과 같다. ‘위험 평가 및 보안 투자’는 조직 내에 존재하는 보안 위험을 평가하는 연구, 보안 관련 의사결정을 함에 있어 최적의 투자를 분석하는 연구 등을 포함하고, ‘사이버 범죄와 방어 전략’은 사이버 상에 존재하는 범죄를 분석하는 연구, 사이버 범죄에 대응하기 위한 방어 전략을 분석한 연구 등을 포함한다. ‘보안 표준 및 정책’은 보안 관련 표준 및 가이드라인을 제시하는 연구, 보안 관련 정책 및 규정을 분석한 연구 등을 포함하고, ‘프라이버시 및 익명의 경제성’은 개인의 프라이버시가 가지는 경제적 가치에 대한 연구, 사이버 상에서 익명성이 가지는 경제적 가치에 대한 연구 등을 포함한다. 마지막으로 ‘취약점 관리’는 취약점에 대한 발견, 공개 및 패치에 대한 최적의 정책에 대한 연구, 조직의 취약점을 공개하거나 또는 조직 간에 취약점 관련하여 협력하는 것에 대한 인센티브를 분석한 연구 등을 포함한다.

방법론 분류기준은 Moore와 Anderson[2011]의 방법론 분류기준을 참고하였다. Moore와 Anderson [2011]은 분석적 연구, 경험적 연구, 행동적 연구, 연구와 정책의제 등 총 4개의 방법론으로 분류하였는데, 본 연구는 크게 분석적 연구, 경험적 연구, 연구 및 정책 의제 등 총 3개의 방법론으로 분류하였다(<Table 7> 참조).

<Table 7> Classification Standard of Methodology

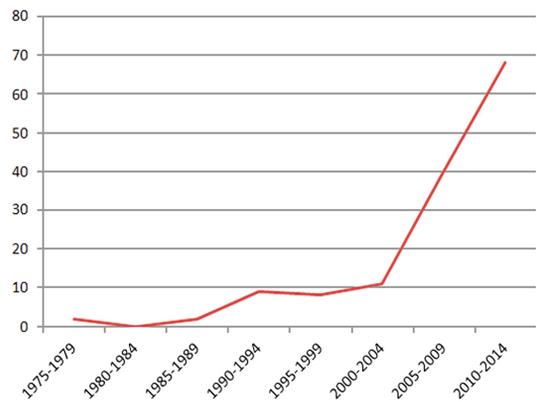
Code	Methodology	Detailed Methodology	Code
R&PA	Research and Policy Agenda	Research and Policy Agenda	R&PA
ER	Empirical Research	Primary Data	1D
		Secondary Data	2D
AR	Research and Policy Agenda	Mathematical Modeling	MM
		Non-mathematical Modeling	NM

각 방법론 분류기준에 포함된 연구는 다음과 같다. ‘분석적 연구’는 수학 이론에 기초하여 모델링한 연구, 메커니즘, 관리체계 등을 모델링한 연구를 포함하며, ‘경험적 연구’는 설문조사, 사례조사 등의 방법으로 직접 수집한 데이터를 활용한 연구, 조직 및 기업 등을 통해서 간접 수집한 데이터를 활용한 연구를 포함한다. 마지막으로 ‘연구 및 정책 의제’는 분석적 연구 및 경험적 연구를 제외한 연구로 이슈, 현상, 정책 등에 대해 기술한 연구를 포함한다.

4. 연구동향 분석결과

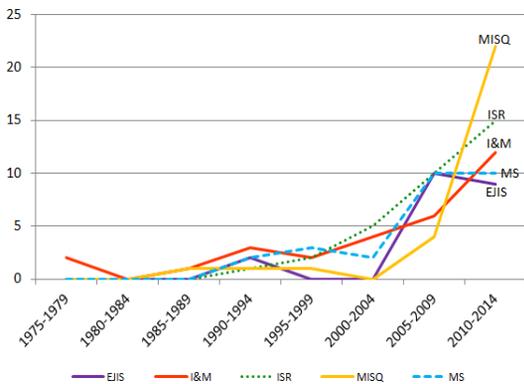
4.1 연도별 논문 빈도 분석

연도별로 발표된 보안경제성 관련 논문의 분포를 살펴보았다. 종합적으로 발표된 논문의 분포를 살펴본 결과, 1970년대 후반에 처음 나타났고, 이후 10년 정도 발표된 논문이 없다가, 1980년대 후반에 다시 나타난 이후부터는 거의 지속적으로 발표되었다. 1990년대 전반에 연구가 증가하다가 주춤하였고, 1990년대 후반부터 상승세를 계속 이어가고 있다. 특히, 2000년대 후반부터 높은 상승세를 보이고 있다(<Figure 1> 참조).



<Figure 1> Research Theme Trends(Sum of 5 Journals)

저널별로 발표된 논문의 분포를 살펴본 결과, I&M은 1970년대 후반에 처음 나타났고, 1980년대 후반에 다시 나타난 이후 전반적으로 증가하는 추세를 이어가고 있다. MISQ는 1980년대 후반에 처음 발표된 이후 1990년대 후반까지 지속적으로 발표되었다. 2000년대부터 상승세를 계속 이어가고 있으며, 특히 2010년대 전반에 급증하였다. ISR은 1990년대 전반에 나타난 이후 계속 상승세를 이어가고 있다. EJIS는 1990년대 전반에 나타났고, 2000년대 후반에 다시 나타날 때 다소 큰 폭으로 증가하였다가, 2010년대 전반에 소폭 감소하였다. MS는 1990년대 전반에 나타난 이후 지속적으로 발표되었고, 2000년대 후반에 다소 큰 폭으로 증가하였다(<Figure 2> 참조).



<Figure 2> Research Theme Trends(Each Journal)

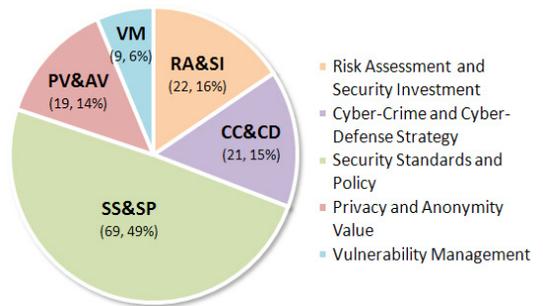
저널별로 발표된 논문에 스페셜 이슈의 영향이 있었던 것은 아닌지 확인해보았다. 5개 저널 중 보안 관련 스페셜 이슈가 있던 것은 MISQ, EJIS 등 총 2개 저널이다. MISQ는 2010년에 'Information Systems Security'를 스페셜 이슈로 발표하였고, 이 영향으로 2010년에 보안경제성 관련 연구가 평년보다 5배 가량 많이 발표된 것으로 추측된다. EJIS는 'Behavioural and Policy Issues in Information Systems Security'를 스페셜 이

슈로 논문을 모집했었고, 이 영향으로 2009년에 보안경제성 관련 연구가 평년보다 3배 가량 많이 발표된 것으로 추측된다. 또한, EJIS는 2016년 1월까지 'Security and Privacy in 21st Century Organisations'를 스페셜 이슈를 모집하고 있으므로, 2016년 즈음에는 보안경제성 관련 연구가 평년보다 더 많이 발표될 것으로 예상된다.

4.2 주제 및 방법론 빈도 분석

논문별로 주제 및 방법론을 분류한 정량적 데이터를 기반으로 보안경제성 관련 연구들이 선호하는 주제 및 방법론을 분석하였다.

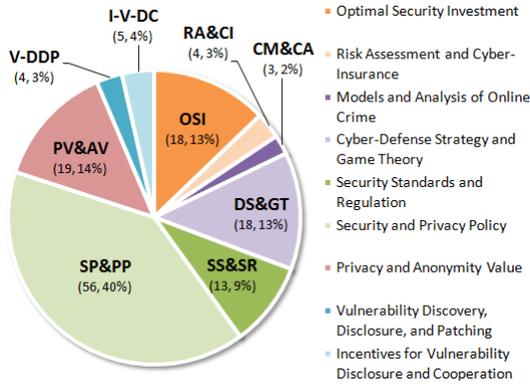
종합적으로 선호하는 주제를 살펴본 결과, '보안 표준 및 정책(49%)'이 가장 많았으며, '위험 관리 및 보안 투자(16%)', '사이버 범죄와 방어 전략(15%)', '프라이버시 및 익명의 경제성(14%)', '취약점 관리(6%)' 순으로 뒤를 잇고 있다(<Figure 3> 참조).



<Figure 3> Frequency of Research Theme(Sum of 5 Journals)

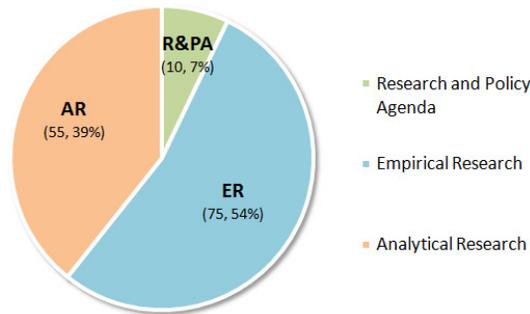
세부 분류기준으로 살펴본 결과, '사이버 보안 및 프라이버시 정책(40%)'이 가장 많았으며, '프라이버시 및 익명의 경제성(14%)', '정보보안에 대한 최적의 투자(13%)', '사이버 방어 전략과 게임 이론(13%)' 순으로 뒤를 잇고 있다. '보안 표준 및 정책' 내에서는 '사이버 보안 및 프라이버시 정책', '위험 관리 및 보안 투자' 내에서는

‘정보보안에 대한 최적의 투자’, ‘사이버 범죄와 방어 전략’ 내에서는 ‘사이버 방어 전략과 게임 이론’이 압도적으로 많았다(<Figure 4> 참조).



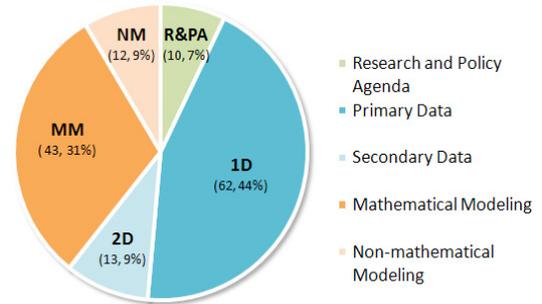
<Figure 4> Frequency of Detailed Research Theme(Sum of 5 Journals)

종합적으로 선호하는 방법론을 살펴본 결과, ‘경험적 연구(54%)’가 가장 많았으며, ‘분석적 연구(39%)’, ‘연구와 정책 의제(7%)’ 순으로 뒤를 잇고 있다(<Figure 5> 참조).



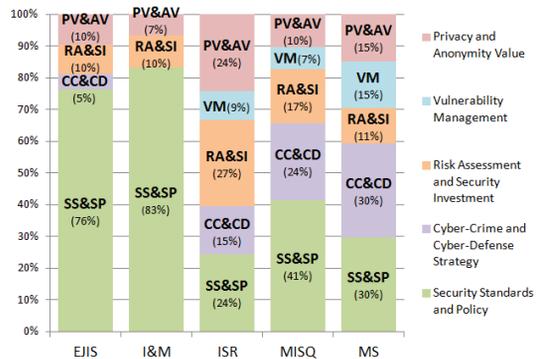
<Figure 5> Frequency of Research Methodology(Sum of 5 Journals)

세부 분류기준으로 살펴본 결과, ‘1차 데이터 활용(44%)’이 가장 많았으며, ‘수리적 모델링(31%)’이 뒤를 잇고 있다. ‘경험적 연구’ 내에서는 ‘1차 데이터 활용’, ‘분석적 연구’에서는 ‘수리적 모델링’이 압도적으로 많았다(<Figure 6> 참조).



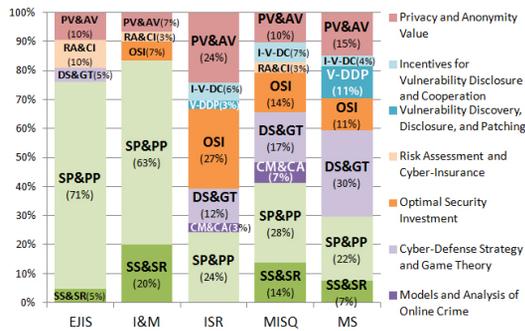
<Figure 6> Frequency of Detailed Research Methodology(Sum of 5 Journals)

저널별로 선호하는 주제를 살펴본 결과, EJIS와 I&M은 ‘보안 표준 및 정책’이 각각 76%, 83%로 거의 대부분을 차지한다. MISQ도 ‘보안 표준 및 정책’이 45%로 가장 많으며, ‘사이버 범죄와 방어 전략(24%)’, ‘위험 평가 및 보안 투자(17%)’ 순으로 뒤를 잇고 있다. MS는 ‘보안 표준 및 정책’과 ‘사이버 범죄와 방어 전략’이 각각 30%로 가장 많으며, ‘프라이버시 및 익명의 경제성’과 ‘취약점 관리’가 각각 15%로 뒤를 잇고 있다. ISR은 ‘위험 평가와 보안 투자(27%)’가 가장 많으며, ‘프라이버시 및 익명의 경제성’과 ‘보안 표준 및 정책’이 각각 24%로 근소한 차이로 뒤를 잇고 있다. I&M은 ‘사이버 범죄와 방어 전략’과 ‘취약점 관리’를 제외한 3개의 주제만 다루어졌고, EJIS는 ‘취약점 관리’를 제외한 4개의 주제만 다루어졌으며, ISR, MISQ, MS는 5개 주제가 모두 다루어졌다(<Figure 7> 참조).



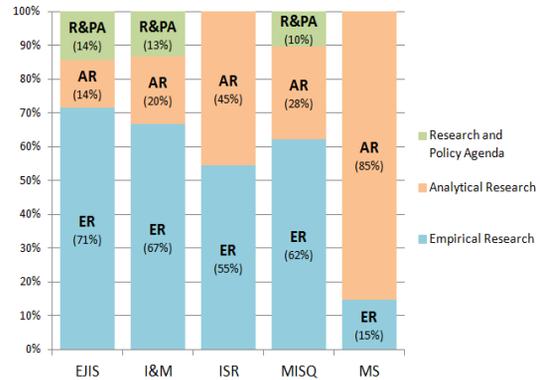
<Figure 7> Frequency of Research Theme(Each Journal)

세부 분류기준으로 살펴본 결과, EJIS와 I&M은 ‘사이버 보안 및 프라이버시 정책’이 각각 71%, 63%로 거의 대부분을 차지한다. ISR은 정보보안에 대한 최적의 투자(27%)가 가장 많았으며, 근소한 차이로 ‘사이버 보안 및 프라이버시 정책(24%)’과 ‘프라이버시 및 익명의 경제성(24%)’이 뒤를 잇고 있다. MISQ는 ‘사이버 보안 및 프라이버시 정책(28%)’이 가장 많았으며, ‘사이버 방어 전략과 게임 이론(17%)’이 뒤를 잇고 있다. MS는 ‘사이버 방어 전략과 게임 이론(30%)’이 가장 많았으며, ‘사이버 보안 및 프라이버시 정책(22%)’이 뒤를 잇고 있다. MISQ는 ‘취약점 발견, 공개 및 패치’를 제외한 8개의 주제만을 다루었고, ISR은 ‘보안 표준 및 규정’, ‘위험 평가 및 사이버 보험’을 제외한 7개의 주제만 다루었으며, MS는 ‘온라인 범죄에 대한 모델 및 분석’, ‘위험 평가 및 사이버 보험’을 제외한 7개의 주제만을 다루었다. EJIS는 ‘온라인 범죄에 대한 모델 및 분석’, ‘정보보안에 대한 최적의 투자’, ‘취약점 발견, 공개 및 패치’, ‘취약점 공개 및 협력의 인센티브’를 제외한 5개의 주제만 다루었으며, I&M은 ‘온라인 범죄에 대한 모델 및 분석’, ‘사이버 방어 전략과 게임 이론’, ‘취약점 발견, 공개 및 패치’, ‘취약점 공개 및 협력의 인센티브’를 제외한 5개 주제만 다루었다(<Figure 8> 참조).



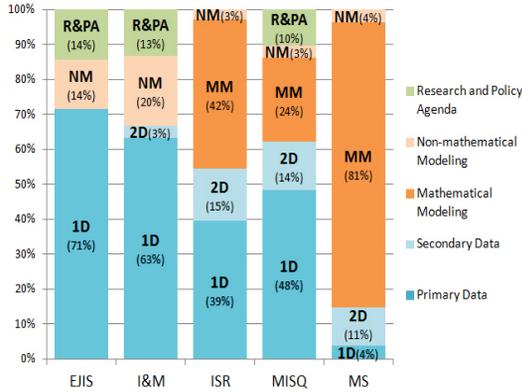
<Figure 8> Frequency of Detailed Research Theme(Each Journal)

저널별로 선호하는 방법론을 살펴본 결과, EJIS, I&M, MISQ는 ‘경험적 연구’가 각각 71%, 67%, 62%로 거의 대부분을 차지하였다. ISR도 ‘경험적 연구(53%)’가 가장 많았으며, ‘분석적 연구(45%)’가 근소한 차이로 뒤를 잇고 있다. 반면, MS는 ‘분석적 연구’가 85%로 거의 대부분을 차지한다. ISR과 MS를 제외한 3개의 저널은 3개의 방법론이 모두 활용되었으나, ISR과 MS는 ‘연구와 정책 의제’ 방법론을 활용한 연구가 없었다(<Figure 9> 참조).

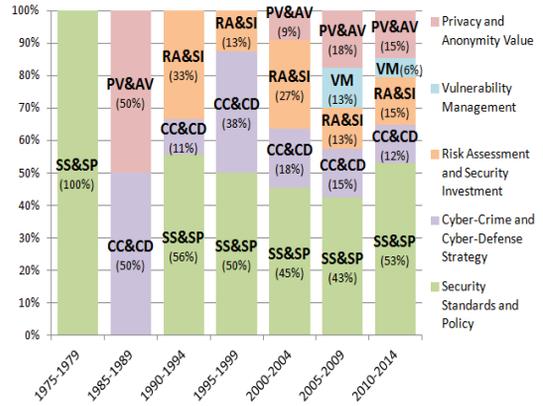


<Figure 9> Frequency of Research Methodology(Each Journal)

세부 분류기준으로 살펴본 결과, EJIS와 I&M은 ‘1차 데이터 활용’이 각각 71%, 63%로 거의 대부분을 차지하며, MS는 ‘수리적 모델링’이 81%로 대부분을 차지한다. MISQ는 ‘1차 데이터 활용(48%)’이 절반 가량을 차지하며, ‘수리적 모델링(42%)’이 가장 많았으며, ‘1차 데이터 활용(39%)’이 근소한 차이로 뒤를 잇고 있다. ISR은 ‘수리적 모델링(42%)’이 가장 많았으며, ‘1차 데이터 활용(39%)’이 근소한 차이로 뒤를 잇고 있다. MISQ는 모든 방법론을 다루었으며, ISR와 MS는 ‘연구와 정책 의제’를 제외한 4개 방법론만을 다루었다. I&M은 ‘수리적 모델링’을 제외한 4개 방법론만을 다루었으며, EJIS는 ‘2차 데이터 활용’, ‘수리적 모델링’을 제외한 3개 방법론만을 다루었다(<Figure 10> 참조).



<Figure 10> Frequency of Detailed Research Methodology(Each Journal)

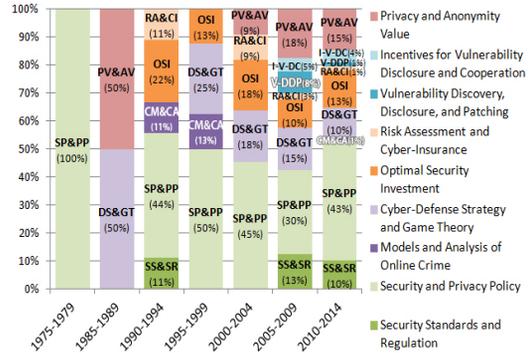


<Figure 11> Research Theme Trends(Sum of 5 Journals)

4.3 연도별 주제 및 방법론 빈도 분석

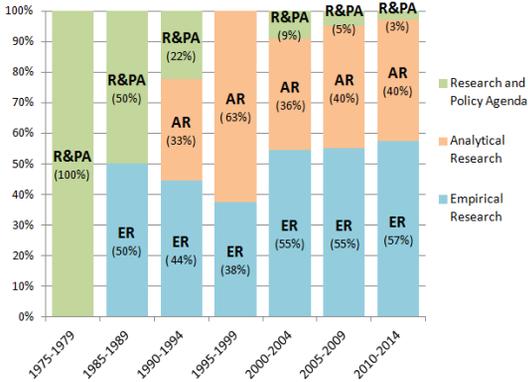
향후 선호하게 될 주제 및 방법론을 예측하기 위해, 연도별 주제 및 방법론의 비율을 살펴보았다. 연도별 주제의 비율을 살펴본 결과, 1980년대를 제외하면 모든 연대를 통틀어 ‘보안 표준 및 정책’이 가장 많았다. 가장 먼저 나타난 주제는 ‘보안 표준 및 정책’으로 1970년대 후반에 나타났고, 1980년대 후반에 ‘프라이버시 및 익명의 경제성’과 ‘사이버 범죄와 방어 전략’이 나타났다. 1990년대 전반에 ‘위험 평가 및 보안 투자’가 나타났고, ‘취약점 관리’는 가장 늦게 2000년대 후반에 나타났다. 1990년대부터 꾸준히 절반가량을 차지하고 있는 ‘보안 표준 및 정책’이 향후에도 가장 선호하게 될 주제로 예측된다(<Figure 11> 참조). ‘보안 표준 및 정책’ 중에서도 ‘사이버 보안 및 프라이버시 정책’ 관련 연구가 가장 활발하게 이루어질 것으로 전망되며, 그 외에도 ‘정보보안에 대한 최적의 투자’, ‘사이버 방어 전략과 게임 이론’, ‘프라이버시 및 익명의 경제성’ 관련 연구들이 꾸준히 발표될 것으로 전망된다(<Figure 12> 참조).

연도별 방법론 비율을 살펴본 결과, 연구가 처음 등장하던 시기에는 ‘연구와 정책의제’가 대

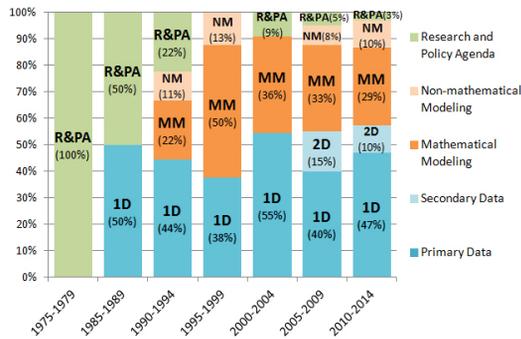


<Figure 12> Detailed Research Theme Trends(Sum of 5 Journals)

부분을 차지하였으나, 연구가 활발하게 이루어짐에 따라 ‘경험적 연구’와 ‘분석적 연구’가 급증하면서 대부분을 차지하였다. 가장 먼저 나타난 방법론은 ‘연구와 정책 의제’로 1970년대 후반에 나타났고, 1980년대 후반에는 ‘경험적 연구’가 나타났다. ‘분석적 연구’는 가장 늦게 1990년대 전반에 나타났다. 2000년대부터 꾸준히 절반 이상을 차지하고 있는 ‘경험적 연구’가 향후 가장 선호하게 될 방법론으로 예측된다(<Figure 13> 참조). ‘경험적 연구’ 중에서도 ‘1차 데이터 활용’ 관련 연구가 가장 활발하게 이루어질 것으로 전망되며, 그 외에도 ‘수리적 모델링’ 관련 연구가 활발하게 이루어질 것으로 전망된다(<Figure 14> 참조).



<Figure 13> Research Methodology Trends(Sum of 5 Journals)



<Figure 14> Detailed Research Methodology Trends(Sum of 5 Journals)

4.4 주제와 방법론의 교차분석

어떤 주제와 방법론을 주로 함께 활용하는 지 확인하기 위해 주제와 방법론을 교차 분석하였다. 종합적으로 살펴본 결과, ‘보안 표준 및 정책’ 관련 주제로 ‘경험적 연구’ 방법론을 활용한 연구가 31%로 가장 많았고, 동일한 주제로 ‘분석적 연구’ 방법론을 활용한 연구(14%), ‘위험 평가 및 보안 투자’ 관련 주제로 ‘분석적 연구’ 방법론을 활용한 연구(10%) 순으로 뒤를 잇고 있다. ‘사이버 범죄와 방어 전략’과 ‘취약점 분석’ 관련 주제로 ‘연구와 정책 의제’ 방법론을 활용한 연구는 없었다. 주제별로 선호하는 방법론을 살펴보면, ‘위험 평가 및 보안 투자’와 ‘취약점 관리’

관련 주제의 연구는 ‘분석적 연구’ 방법론을 가장 많이 활용하였으며, ‘사이버 범죄와 방어 전략’, ‘프라이버시 및 익명의 경제성’, ‘보안 표준 및 정책’ 관련 주제의 연구는 ‘경험적 연구’ 방법론을 가장 많이 활용하였다.

저널별로 살펴본 결과, ‘보안 표준 및 정책’ 관련 주제로 ‘경험적 연구’ 방법론을 활용한 연구를 가장 많이 선호하는 저널은 MISQ, EJIS, I&M 등 총 3개이다. ISR은 ‘프라이버시 및 익명의 경제성’ 관련 주제로 ‘경험적 연구’ 방법론을 활용한 연구를 가장 많이 선호하며, MS는 ‘사이버 범죄와 방어 전략’과 ‘보안 표준 및 정책’ 관련 주제로 ‘분석적 연구’ 방법론을 활용한 연구를 가장 많이 선호한다. 각각 저널별로 주제 및 방법론 교차결과를 좀 더 상세하게 살펴 보았다.

MISQ는 ‘보안 표준 및 정책’ 관련 주제로 ‘경험적 연구’ 방법론을 활용한 연구가 28%로 가장 많았으며, 동일한 방법론으로 ‘사이버 범죄와 방어 전략’ 관련 주제를 다룬 연구(21%), ‘위험 평가 및 보안 투자’ 관련 주제로 ‘분석적 연구’ 방법론을 활용한 연구(17%) 순으로 뒤를 잇고 있다. ‘위험 평가 및 보안 투자’ 관련 주제만 ‘분석적 연구’ 방법론을 가장 많이 활용하였고, 그 외의 모든 주제들은 ‘경험적 연구’ 방법론을 가장 많이 활용하였다. ‘보안 표준 및 정책’ 관련 주제만 모든 방법론이 활용되었다.

ISR은 ‘프라이버시 및 익명의 경제성’ 관련 주제로 ‘경험적 연구’ 방법론을 활용한 연구가 18%로 가장 많았고, ‘위험 평가 및 보안 투자’와 ‘보안 표준 및 정책’ 관련 주제로 ‘분석적 연구’ 방법론을 활용한 연구가 각각 15%로 뒤를 잇고 있다. ‘연구와 정책 의제’ 방법론을 활용한 연구는 없었다. ‘위험 평가 및 보안 투자’, ‘보안 표준 및 정책’ 관련 주제의 연구는 ‘분석적 연구’ 방법론을 가장 많이 활용하였고, ‘사이버 범

전략'(18%), '프라이버시 및 익명의 경제성'(13%), '취약점 관리'(11%)의 분포를 보였다. 연구방법의 측면에서는 주요 IS 저널에 게재된 논문이 '경험적 연구'의 비중(54%)이 높았던 것에 비해, WEIS에 발표된 논문은 '분석적 연구'의 비중(44%)이 높다는 차이가 있다. 연구주제의 측면에서는 주요 IS 저널에 게재된 논문도 '보안 표준 및 정책'의 비중(50%)이 WEIS에 발표된 논문의 해당 주제의 비중(31%)과 마찬가지로 가장 선호되는 연구주제인 것으로 나타났다. 다만 IS 연구자들이 발표한 논문의 주제는 '보안 표준 및 정책'(50%), '사이버 범죄와 방어 전략'(15%), '위험 관리 및 보안 투자'(15%), '프라이버시 및 익명의 경제성'(14%), '취약점 관리'(7%)의 분포를 보여서, 특정 주제로 편중되고 있는 것을 알 수 있다. 저자의 학문 분야의 구성을 분석하면 더 분명하게 알 수 있겠지만, WEIS에 발표하는 논문들은 다학제적으로 연구되고 있기 때문에 연구방법이나 연구주제가 비교적 고르게 분포하고 있는 것으로 판단되며, IS 분야의 보안경제성 관련 연구자들도 타학제의 연구자들과의 협력이 증가하게 되면 이러한 성향을 보이게 될 것으로 추측된다.

5. 결 론

본 연구에서는 보안경제성 관련 연구동향을 파악하기 위해, Management Information Systems Quarterly(MISQ), Information Systems Research(ISR), European Journal of Information Systems(EJIS), Management Science(MS), Information and Management(I&M) 등 5개의 IS 저널에서 발표된 보안경제성 관련 논문들을 검토하였고, 논문별로 주제 및 방법론을 분류한 정량적 데이터를 기반으로 보안경제성 관련 연구들이 선호하는 주제 및 방법론을 분석하였다.

연구결과, 보안경제성 관련 연구들은 '보안 표준 및 정책' 관련 주제와 '경험적 연구' 관련 방법론을 가장 선호하였고, 세부적으로는 '보안 표준 및 정책' 관련 주제와 '1차 데이터 활용' 관련 방법론을 가장 선호하였다. 주제별로 선호하는 방법론의 경우, '위험 평가 및 보안 투자'와 '취약점 관리' 관련 주제의 연구는 '분석적 연구' 방법론을 가장 많이 활용하였으며, '사이버 범죄와 방어 전략', '프라이버시 및 익명의 경제성', '보안 표준 및 정책' 관련 주제의 연구는 '경험적 연구' 방법론을 가장 많이 활용하였다. 종합적으로 선호하는 주제 및 방법론의 조합을 살펴본 결과, '보안 표준 및 정책' 관련 주제로 '경험적 연구' 방법론을 활용한 연구, 동일한 주제로 '분석적 연구' 방법론을 활용한 연구, '위험 평가 및 보안 투자' 관련 주제로 '분석적 연구' 방법론을 활용한 연구 순으로 높은 선호도를 보였다. 저널별로 선호하는 주제 및 방법론의 조합을 살펴본 결과, MISQ, EJIS, I&M는 '보안 표준 및 정책' 관련 주제로 '경험적 연구' 방법론을 활용한 연구, ISR은 '프라이버시 및 익명의 경제성' 관련 주제로 '경험적 연구' 방법론을 활용한 연구, MS는 '사이버 범죄와 방어 전략'과 '보안 표준 및 정책' 관련 주제로 '분석적 연구' 방법론을 활용한 연구를 가장 많이 선호하였다.

본 연구는 연구범위에 일부 저널만을 포함하여 전반적인 보안경제성 관련 연구동향과 다소 차이가 있을 수 있다는 점, 연구자의 주관적인 판단으로 분류하는 과정에서 오류가 발생했을 가능성이 존재한다는 점으로 인해 한계가 있으나, 정량적인 분석을 통해 보안경제성 관련 연구동향을 파악하고 저널별로 선호하는 연구주제 및 연구방법론의 경향을 제공한다는 점에서 의의를 가진다. 본 연구의 결과는 보안경제성 관련 연구에 관심이 있는 연구자들이 연구동향

과약, 연구방향 설정 등을 하는데 도움이 될 것이다. 또한, 국내의 관련 연구 활성화에 도움이 될 수 있고, 기업과 정부가(경제적으로) 합리적인 정보보호 의사결정을 하는데 참고가 될 수 있을 것이다.

향후 연구에서는 논문검색용 데이터베이스를 연구범위로 검색된 논문이 인용한 논문도 검토하여 보안경제성 관련 연구를 포괄적으로 수집하고, 주제 및 방법론 외에도 학문분야, 저자정보 등 분류기준을 확대하여 정량적인 분석으로 보안경제성 관련 연구동향을 파악하고자 한다. 이는 보안경제성 관련 연구를 찾아내고 분류기준에 따라 기초 데이터를 정리하는 과정에 어려움이 따를 것이라 예상된다. 인용수가 높은 연구를 중심으로 보안경제성 관련 분야에서 어떤 연구가 이루어졌는지에 대한 기술적인(descriptive) 성격을 더한다면, 더욱 의미 있는 연구가 될 것으로 기대된다. 이를 통해 전반적인 보안경제성 관련 연구동향을 파악할 수 있을 것으로 기대된다.

References

- [1] Anderson, R., "Why Information Security is Hard-An Economic Perspective", In Computer Security Applications Conference, 2001, ACSAC 2001, Proceedings 17th Annual, IEEE, 2001, pp. 358-365.
- [2] Anderson, R. and Moore, T., "The Economics of Information Security", *Science*, Vol. 314, No. 5799, 2006, pp. 610-613.
- [3] Anderson, R., Böhme, R., Clayton, R., and Moore, T., "Security Economics and European Policy", *Managing Information Risk and the Economics of Security*, 2009, pp. 55-80.
- [4] Banker, R. D. and Kauffman, R. J., "The Evolution of Research on Information Systems : A Fiftieth-year Survey of the Literature in Management Science", *Management Science*, Vol. 50, No. 3, 2004, pp. 281-298.
- [5] Belanger, F. and Crossler, R. E., "Privacy in the Digital Age : A Review of Information Privacy Research in Information Systems", *MIS Quarterly*, Vol. 35, No. 4, 2011, pp. 1017-1042.
- [6] Córdoba, J. R., Pilkington, A., and Bernroider, E. W., "Information Systems as a Discipline in the Making : Comparing EJIS and MISQ between 1995 and 2008", *European Journal of Information Systems*, Vol. 21, No. 5, 2012, pp. 479-495.
- [7] Davies, K., "Content Analysis of Research Articles in Information Systems(LIS) Journals", *Library and Information Research*, Vol. 36, No. 112, 2012, pp. 16-28.
- [8] Jun, H.-J., Yoo, H.-W., and Kim, T.-S., "Analysis on Knowledge and Skills for Information Security Professionals", *Information Systems Review*, Vol. 10, No. 2, 2008, pp. 253-267.
- [9] Kang, M.-H. and Kim, T.-S., "Research Trends in Information Security Economics : Focused on the Articles Presented at WEIS", *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 25, No. 6, Dec. 2015, pp. 1561-1570.
- [10] Ministry of Knowledge Economy, "By 2013, Knowledge Information Security Industry 18 trillion won Market Creation", 2008.
- [11] Ministry of Science, ICT and Future Plan-

- ning, “K-ICT Security Development Strategy”, 2015.
- [12] Moore, T., “The Economics of Cybersecurity : Principles and Policy Options”, *International Journal of Critical Infrastructure Protection*, Vol. 3, No. 3, 2010, pp. 103-117.
- [13] Moore, T. and Anderson, R., “Economics and Internet Security : A Survey of Recent Analytical, Empirical and Behavioral Research”, Harvard University Computer Science Group, 2011.
- [14] Mustafee, N., “Evolution of IS Research Based on Literature Published in Two Leading IS Journals-EJIS and MISQ”, In 19th European Conference on Information Systems, 2011, pp. 2658-2668.
- [15] National Disaster Management Institute, “Analysis of Social Disaster and the Damage Costs due to Leakage of Personal Information”, *Disaster and Safety*, Vol. 17, No. 1, 2015, pp. 21-28.
- [16] Odlyzko, A., “Economics, Psychology, and Sociology of Security”, *Financial Cryptography*, 2003, pp. 182-189, Springer Berlin Heidelberg.
- [17] Palvia, P., Pinjani, P., and Sibley, E. H., “A Profile of Information Systems Research Published in Information and Management”, *Information and Management*, Vol. 44, No. 1, 2007, pp. 1-11.
- [18] Siponen, M. and Willison, R., “A Critical Assessment of IS Security Research between 1990~2004”, Copenhagen Business School, 2007.
- [19] Smith, H. J., Dinev, T., and Xu, H., “Information Privacy Research : An Interdisciplinary Review”, *MIS Quarterly*, Vol. 35, No. 4, 2011, pp. 989-1015.
- [20] Swanson, E. B. and Ramiller, N. C., “Information Systems Research Thematics : Submissions to a New Journal, 1987~1992”, *Information Systems Research*, Vol. 4, No. 4, 1993, pp. 299-330.
- [21] Standard Korean Dictionary of The National Institute of The Korean Language, <http://stdweb2.korean.go.kr/>.
- [22] EJIS(European Journal of Information Systems), <http://www.palgrave-journals.com/ejis/index.html>.
- [23] ISR(Information Systems Research), <http://pubsonline.informs.org/journal/isre>.
- [24] I&M(Information and Management), <http://www.sciencedirect.com/science/journal/03787206>.
- [25] MISQ(Management Information Systems Quarterly), <http://www.misq.org/>.
- [26] MS(Management Science), <http://pubsonline.informs.org/journal/mnsc>.
- [27] WEIS(Workshop on the Economics of Information Security) 2011, <http://weis2011.econinfosec.org/>.
- [28] WEIS(Workshop on the Economics of Information Security) 2012, <http://weis2012.econinfosec.org/>.
- [29] WEIS(Workshop on the Economics of Information Security) 2013, <http://weis2013.econinfosec.org/>.
- [30] WEIS(Workshop on the Economics of Information Security) 2014, <http://weis2014.econinfosec.org/>.

■ 저자소개



강 미 화

충북대학교 정보보호경영학과 석사학위를 취득하고, 현재 (주)에이쓰리에서 정보보안 컨설턴트로 재직 중이다. Information Systems Review, 정보보호학회논문지 등에 논문을 발표하였다. 주요 관심분야는 정보보호 투자, 정보보호 교육, 정보보호 컨설팅 등이다.



김 태 성

한국과학기술원 경영학과에서 박사를 취득하고, 한국전자통신연구원 정보통신기술경영연구소에서 근무한 후, 현재 충북대학교 경영정보학과에서 정교수로 재직하고 있으며 대학원 정보보호경영전공 주임교수를 맡고 있다. University of North Carolina at Charlotte과 Arizona State University에서 Visiting Professor와 Visiting Scholar로 각각 근무하였다. OR Letters, European Journal of Operational Research, Journal of the Operational Research Society 등 국내 외 경영과학, 정보통신, 정보보호 관련 학술지 및 학술대회에 논문을 발표하였으며, 주요 관심분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.