

보안경제성 연구동향 분석: WEIS 발표 논문을 중심으로*

강 미 화,^{1*} 김 태 성^{2*}
¹(주)에이쓰리, ²충북대학교

Research Trends in Information Security Economics: Focused on the Articles Presented at WEIS*

Mi-Hwa Kang,^{1*} Tae-Sung Kim^{2*}
¹A3 Co., Ltd., ²Chungbuk National University

요 약

정보보호 침해사고로 인한 피해를 예방하거나 감소시키기 위해 많은 관심과 투자가 검토되고 있지만, 투자, 관리 등의 정보보호 의사결정을 경제적으로 합리적으로 하기 위한 연구에 대해서는 국내에 본격적으로 소개되지 않았다. 정보보호의 경제적 의사결정에 대한 연구자들은 보안경제성워크샵(Workshop on the Economics of Information Security, WEIS)을 중심으로 활동하고 있으며, 본 연구는 WEIS에 2002년부터 2014년까지 발표된 논문들의 연구주제와 연구방법을 분석하였다. 연구결과는 국내의 관련 연구 활성화에 도움이 될 수 있고, 기업과 정부의 경제적 정보보호 의사결정에 참고가 될 수 있을 것이다.

ABSTRACT

Even though much investment to prevent or mitigate damage from information security breaches have been considered, researches on economically rational information security decision-making such as investment, management, etc. are not introduced in Korea. This study analyzes research themes and methodologies of articles presented at the Workshop on the Economics of Information Security (WEIS) for 2002 - 2014. Results of the study can suggest future research topics for researchers, and help make rational information security decision-making for practitioners.

Keywords: Security Economics, Decision-Making, WEIS, Research Trends

1. 서 론

2014년 1월에 발생한 3개 신용카드 회사의 고객 정보 유출 사태로 카드사들의 주가는 엇갈린 반응을 보였다. 고객의 정보가 유출됨으로 인해 KB금융의 주가는 약세를 보였던 반면, 카드 3사가 3개월간 영

업을 할 수 없게 됨에 따라 상대적으로 혜택을 볼 것으로 예상되었던 삼성카드의 주가는 연일 상승했었다 [1]. 또한, 3개 카드사들의 고객정보 유출 사태에 따른 손실액이 1,600억원 수준인 것으로 파악됐으며, 그 외에도 정보유출과 관련한 소송으로 인해 추가적으로 손실이 발생할 가능성이 높았다[2]. 한 기업의 개인정보유출은 사고수습처리 비용의 발생에서 그치지 않고 수많은 기존고객 이탈 그리고 잠재고객까지 잃게 되며 그로 인한 매출감소, 기업 이미지 및 가치 하락과 신뢰저하로까지 이어지며 중국에는 기업의 도산 가능성까지 확산되어가고 있다[3].

조직에게 정보보안 투자를 위한 의사결정은 매우 중요하며, 조직은 제한된 자원으로 최적의 투자를 하

Received(07. 14. 2015), Modified(09. 23. 2015),
Accepted(09. 23. 2015)

* 본 연구는 2014년 한국정보보호학회 동계학술대회에서 발표한 내용을 수정 및 보완한 것임. 이 논문은 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015S1A5A2A01009763).

† 주저자, noltkatnsdl@hanmail.net

‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

기위해 노력한다. 투자 의사결정 이외에도 관리 방법의 선택 등 정보보호 활동 전반에 대해 경제적으로 합리적인 의사결정이 절실하게 필요한 현실이다[4~6].

2000년대 초기부터 컴퓨터공학, 경제학 등 다양한 학문 분야의 연구자들이 보안경제성에 대해 많은 연구를 해오고 있지만, 국내에는 관련 연구를 체계적으로 수행하고 있는 사례가 많지 않은 것으로 판단된다.

본 연구는 보안경제성 분야의 가장 활발한 학술모임인 WEIS(Workshop on the Economics of Information Security)에서 2002년부터 2014년까지 총 13개년 동안 발표된 논문들을 대상으로 연구의 주제와 방법론을 기준으로 연구동향을 파악한다. 이를 통해 연구자들에게는 향후 유망한 연구 주제를 제공하고, 실무자들에게는 합리적인 정보보호 의사결정에 대한 지침을 제공하고자 한다.

II. 이론적 배경

2.1 보안경제성 관련 연구

상당수의 학자들이 정보보호와 경제학의 밀접한 연관성에 대해 주장하였다. Anderson[4]은 정보보안의 많은 문제가 미시경제학으로 보다 명확하고 설득력 있게 설명될 수 있으며, 보안 공학은 합리적인 위험 관리의 문제이므로 정보보호 평가자는 기술적인 도구뿐만 아니라 경제적 도구도 활용해야 한다고 주장하였다. Odlyzko[5]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 등[7]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, 책임 회피, 다양성의 부족, 법률과 법 집행의 분열의 5가지로 분류하고, 보안경제학을 기반으로 분석하였다. Moore[8]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 도메

인인 일반적인 보안의 경제성, 신뢰성의 경제성 등에 파급되고 있다[6]. Anderson과 Moore[6]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 정보 보안 분석 등을 중점으로 검토하였다. Moore와 Anderson[9]은 보안경제성 연구들의 4가지 주요 영역을 공격과 방어에 대한 모델링, 개인정보 침해, 악성코드와 봇넷, 지불 시스템 보안으로 보고, 각 영역별로 이론적 연구, 경험적 연구, 행동적 연구, 연구와 정책의제 등 4가지 방법론으로 분류한 후, 4가지 영역의 연구동향을 분석하였다.

본 연구는 Moore와 Anderson[9]의 기술적인(descriptive) 성격의 연구를 WEIS 발표 논문에 대한 정량적인(quantitative) 분석으로 확장한 것이다.

2.2 정보시스템 및 정보보호 분야의 리뷰 연구

리뷰 연구를 위한 방법론에 대한 고찰을 하기 위해, 정보보호 및 정보시스템 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[10]. 연구범위는 크게 저널 및 컨퍼런스(프로시딩)을 선정할 경우와 연구검색용 데이터베이스를 선정할 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[11]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[12], 명사구[13]를 활용한 경우도 있었다. 분석방법은 크게 정량적인 분석과 정성적인 분석으로 나누어볼 수 있다(Table 1).

Table 1. Review Research of Information Systems and Information Security

Author	Research Field	Research Scope	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, ...	unlimited	
Palvia et al. (2007)			1 Theme, Methodology, ...	8	
Mustafee (2011)			2 Noun phrase	14	Quantitative Analysis
Córdoba et al. (2012)			2 Co-citation	14	
Davies (2012)			3 Methodology, Researchers, ...	3	
Siponen and Willison (2007)	Information Systems Security		21 Theme, Methodology	15	
Smith et al. (2011)	Information Systems Privacy	Research Database	3 Theme, Methodology, ...	unlimited	
Bélanger and Crossler (2011)			3 Theme, Methodology, ...	unlimited	

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 1280개까지, 평균 약 542개였다. 분류기준은 방법론, 주제, 저자정보, 분석수준, 학문분야 순으로 많았다(Table 2). 상위 33명 저자의 연구주제, 선호 연구방법론, 소속을 분류한 경우[14], 정보유형, 기술적 속성, 프라이버시 정의 유형을 분류한 경우[15]도 있었다. 분류에서 중복을 허용한 경우도

Table 2. 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	

있다. Palvia 등[14]은 연구 당 주제는 3개까지, 방법론은 2개까지 중복을 허용하였다.

III. 연구범위 및 연구방법

3.1 용어정의

보안경제성 관련 연구동향을 파악하기 전에 먼저 '보안경제성 관련 연구가 무엇인지 정의하고자 한다. 정보보안¹⁾을 경제적 관점으로 접근한 연구들을 포괄하는 용어가 명확하지 않아 본 연구에서는 이를 '보안경제성'이라 명명하였고, 사전적 의미 등을 참고하여 다음과 같이 정의하였다. 보안경제성이란 '컴퓨터 또는 네트워크상의 정보의 훼손, 변조, 유출 등을 방지하기 위한 재물, 자원, 노력, 시간 따위가 적게 들면서도 이득이 되는 성질'을 의미하고,²⁾ 보안경제성 관련 연구란 '정보보안 관련 현상 및 문제를 경제적 관점으로 분석한 연구 또는 연구결과가 개인 및 조직의 정보보안 관련 의사결정에 도움이 되는 연구를 의미하며,³⁾ 이를 기반으로 본 연구를 진행하였다.

- 1) 본 연구에서 '정보보안'과 '정보보호'를 동일한 의미로 문맥에 맞게 혼용하여 사용하였다.
- 2) 지식경제부(현 산업통상자원부)의 '정보보안' 정의[20], 국립국어원의 '경제성' 정의[21]를 참고하여 보안경제성을 정의하였다.
- 3) 온라인 백과사전인 위키피디아(Wikipedia)에서는 'Economics of security'가 컴퓨터 보안 및 개인정보 보호와 관련한 경제적 측면, 개인/조직의 의사결정 및

3.2 연구범위

본 연구는 WEIS에서 2002년부터 2014년까지 총 13개년 동안 발표된 논문들을 대상으로 진행하였다. WEIS는 보안경제성 관련 연구결과를 발표하는 학술 대회이기 때문에, WEIS에서 발표된 논문들은 모두 분석대상 논문에 포함될 수 있다는 이점을 가지고 있다. WEIS는 2002년을 시작으로 매년 한번씩, 2014년 말까지 총 13번 개최 되었고, 한 해에 24편 정도의 논문이 발표되며, 경제학, 사회 과학, 비즈니스, 법률, 정책, 컴퓨터 과학 등 다양한 분야의 전문 지식과 정보보안이 결합된 논문들을 다루고 있다[22~34].

본 연구는 보안경제성 관련 연구를 개괄적으로 파악하는데 중점을 두어, 개별 논문이 분석단위가 되며, 세부적으로는 주제, 방법론 등에 관심을 갖는다. 분석대상 논문 수는 논문 파일이 확인 불가능(20개)하거나 프리젠테이션 파일만 존재(8개)한 경우를 제외한 총 284개로, 2002년 24개, 2003년 14개, 2004년 17개, 2005년 38개, 2006년 29개, 2007년 21개, 2008년 22개, 2009년 19개, 2010년 21개, 2011년 19개, 2012년 20개, 2013년 20개, 2014년 20개이다. 분석대상 논문 중 요약만 확인 가능한 경우는 총 19개로, 2002년 13개, 2003년 4개, 2005년 1개, 2013년 1개이다.

3.3 연구방법

본 연구는 2명의 연구자가 각각 연구의 주제와 방법론을 분류기준에 따라 분류하였다. 분류가 분명하게 될 때까지 요약, 결론, 서론, 전문 순으로 범위를 확대하면서 논문을 검토하였다. 요약만 확인가능한 경우는 요약을 검토한 후 분류하였고, 연구의 주제 또는 방법론이 복합적인 경우는 연구에서 차지하는 비중이 더 큰 주제 또는 방법론으로 분류하였다. 분류결과가 연구자 간에 상이한 경우는 주제가 한 해당 평균 4개, 방법론이 한 해당 평균 0.5개였는데, 이는 재검토를 통해 의견일치를 보았다.

보안경제성 관련 연구들을 주제와 방법론으로 분류하기 위해, 주제와 방법론의 분류기준을 각각 정하였다. 보안경제성 관련 연구들의 세부분야 등이 명확하지 않아, 본 연구에서는 WEIS의 연구주제를 참고하여 주제 분류기준을 추출하였다. WEIS의 연구주

제를 파악하기 위하여 WEIS의 13개년(2002~2014년) 동안의 Call for Paper를 분석하였고, 그 결과 2011년부터 2014년까지의 Call for Paper가 일관된 패턴을 보이는 것을 발견할 수 있었다 (Table 3).

2011~2014년에는 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

Table 3. Research Theme of WEIS (2011~2014)

Ref.	Research Theme	2011	2012	2013	2014
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	

행동, 공학설계 의사결정 등을 해결한다고 설명하고 있다[35].

and Security)를 제외한 연구주제 9개를 주제 분류기준으로 추출하였다. 분석대상 논문 수(284개) 대비 주제 분류기준 수(9개)가 많아 전반적인 연구 동향을 파악하는데 어려움이 있을 것이라 판단되어, 연관성을 고려하여 9개의 주제 분류기준을 5개로 그룹화 하였고, 모든 주제를 포괄할 수 있으면서 분류 기준 간에는 배타적일 수 있도록 일부 단어를 수정하였다.

본 연구의 주제 분류기준은 위험 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, 세부분류 기준은 Table 4와 같다.

각 주제 분류기준에 포함된 연구는 다음과 같다. '위험 평가 및 보안 투자'는 조직 내의 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(9)의 방법론 분류기준을 참고하였다. Moore와 Anderson(9)은 분석적 연구, 경험적 연구, 행동적 연구, 연구와 정책 의제 등 총 4개의 방법론으로 분류하였는데, 본 연구는 크게 분석적 연구, 경험적 연구, 연구 및 정책 의제 등 총 3개의 방법론으로 분류하였다(Table 5).

각 방법론 분류기준에 포함된 연구는 다음과 같다. '분석적 연구'는 수리적 모델링, 비수리적 모델링 등을 사용한 연구를 포함하며, '경험적 연구'는 설문조사, 사례조사, 실험 등을 사용한 연구를 포함한다. 마지막으로 '연구 및 정책 의제'는 분석적 연구 및 경험적 연구를 제외한 연구로 이슈, 현상, 정책 등에 대해 기술한 연구를 포함한다.

Table 4. Classification Standard of Theme

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

Table 5. Classification Standard of Methodology

Code	Methodology
R&PA	Research and Policy Agenda
ER	Empirical Research
AR	Analytical Research

IV. 연구동향 분석결과

4.1 주제

5개의 기준으로 분류하여 빈도 분석한 결과, 보안 표준 및 정책(31%)이 가장 많으며, 위험 평가 및 보안 투자(28%), 사이버 범죄와 방어 전략(18%), 프라이버시 및 익명의 경제성(13%), 취약점 관리(11%) 순으로 그 뒤를 따른다(Fig.1).

분석대상 논문 수(284개) 대비 검색 연도(13개년)가 많아 전반적인 연구동향을 파악하는데 어려움이 있어, 3~4년 단위로 그룹지어 그룹 당 빈도수를

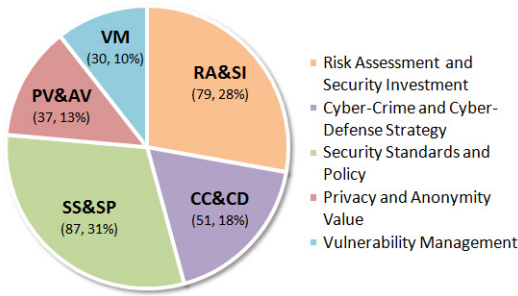


Fig. 1. Frequency of Research Theme

높았다. 2002~2004년(2000년대 초반), 2005~2007년(2000년대 중반), 2008~2010년(2000년대 후반), 2011~2014년(2010년대 초반) 등 총 4개로 그룹화 하였다.

주제별로 연도에 따른 변화를 살펴보면, 2000년대에는 위험 평가 및 보안 투자와 보안 표준 및 정책이 다른 주제들보다 약 2배정도 많이 나타났다. 2010년대 초반에 접어들면서 보안 표준 및 정책은 꾸준히 상위권을 유지한 반면, 위험 평가 및 보안 투자는 하위권으로 진입하였다. 사이버 범죄와 방어 전략, 프라이버시 및 익명의 경제성, 취약점 관리는 2000년대 초반부터 중반까지 하위권을 유지하였다. 사이버 범죄와 방어 전략은 2000년대 후반부터 상승세를 보이면서 2010년대 초반에는 상위권으로 진입하였다. 프라이버시 및 익명의 경제성, 취약점 관리는 2000년대 후반까지도 하위권을 유지하다가, 2010년대에 접어들면서 프라이버시 및 익명의 경제성은 급증하여 중위권에 진입한 반면, 취약점 관리는 변함없이 하위권에 머물렀다(Fig.2, Table 6).

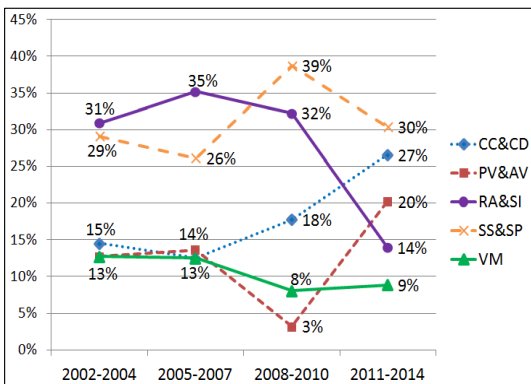


Fig. 2. Research Theme Trends

Table 6. Frequency Table of Research Theme

Year Theme	2002~ 2004	2005~ 2007	2008~ 2010	2011~ 2014	Total
CC&CD	8 15%	11 13%	11 18%	21 27%	51 18%
PV&AV	7 13%	12 14%	2 3%	16 20%	37 13%
RA&SI	17 31%	31 35%	20 32%	11 14%	79 28%
SS&SP	16 29%	23 26%	24 39%	24 30%	87 31%
VM	7 13%	11 13%	5 8%	7 9%	30 11%
Total	55 100%	88 100%	62 100%	79 100%	284 100%

Year Theme	02	03	04	05	06	07	08	09	10	11	12	13	14	Total
CC&CD	4	0	4	5	4	2	5	2	4	4	7	2	8	51
PV&AV	3	3	1	5	4	3	2	0	0	4	3	6	3	37
RA&SI	8	6	3	14	8	9	7	10	3	3	5	1	2	79
SS&SP	8	4	4	8	11	4	8	6	10	7	3	9	5	87
VM	1	1	5	6	2	3	0	1	4	1	2	2	2	30
Total	24	14	17	38	29	21	22	19	21	19	20	20	20	284

※ Theme Classification Standard
 CC&CD : Cyber-Crime and Cyber-Defense Strategy
 PV&AV : Privacy and Anonymity Value
 RA&SI : Risk Assessment and Security Investment
 SS&SP : Security Standards and Policy
 VM : Vulnerability Management

4.2 방법론

3개의 기준으로 분류하여 빈도 분석한 결과, 분석적 연구(44%)가 가장 많으며, 경험적 연구(39%), 연구와 정책 의제(17%) 순으로 그 뒤를 따른다(Fig.3).

방법론별로 연도에 따른 변화를 살펴보면, 2000년대 초반에는 연구와 정책의제와 분석적 연구가 각각 40%대로 대부분을 차지하였으나, 2000년대 중반에는 연구와 정책의제가 급감하고, 경험적 연구가 급증하면서 분석적 연구와 경험적 연구가 각각 40%대로 대부분을 차지하였다. 2000년대 후반에는 경험적 연구가 하락하면서 분석적 연구가 50%이상을 차지하고, 경험적 연구가 34%로 그 뒤를 따랐다. 2010년대 초반에는 경험적 연구가 상승하고, 분석적

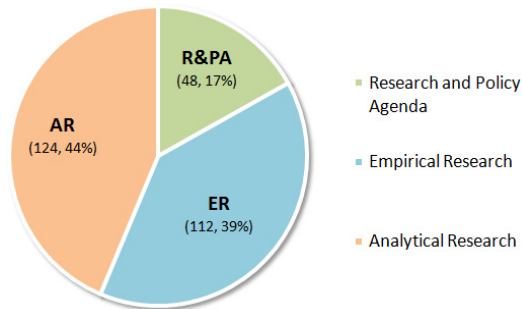


Fig. 3. Frequency of Research Methodology

연구가 하락하면서 경험적 연구가 50%이상을 차지하고, 분석적 연구가 35%로 그 뒤를 따랐다. 연구와 정책의제는 2000년대 중반에 급감한 이후 10% 내외의 낮은 수치를 유지한다(Fig.4, Table 7).

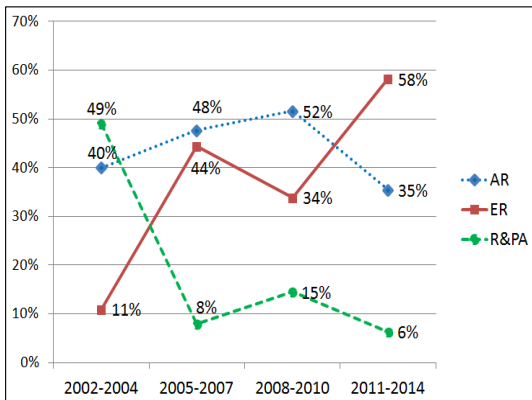


Fig. 4. Research Methodology Trends

Table 7. Frequency Table of Research Methodology

Year Method	2002~2004	2005~2007	2008~2010	2011~2014	Total
AR	22 40%	42 48%	32 52%	28 35%	124 44%
ER	6 11%	39 44%	21 34%	46 58%	112 39%
R&PA	27 49%	7 8%	9 15%	5 6%	48 17%
Total	55 100%	88 100%	62 100%	79 100%	284 100%

Year Method	02	03	04	05	06	07	08	09	10	11	12	13	14	Total
AR	5	7	10	19	12	11	13	9	10	5	8	8	7	124
ER	1	0	5	13	16	10	6	7	8	13	11	10	12	112
R&PA	18	7	2	6	1	0	3	3	3	1	1	2	1	48
Total	24	14	17	38	29	21	22	19	21	19	20	20	20	284

※ Methodology Classification Standard
 AR: Analytical Research
 R&PA: Research and Policy Agenda
 ER: Empirical Research

4.3 주제와 방법론의 교차분석

보안경제성 관련 연구들의 종합적인 흐름을 파악하고, 향후 유망한 연구의 주제와 방법론을 찾기 위해, 주제와 방법론을 교차분석 하였다.

주제로서 사용한 방법론을 살펴본 결과, '사이버 범죄와 방어 전략', '위험 평가 및 보안 투자', '취약점 관리' 관련 주제를 다룬 연구들은 '분석적 연구' 방법론을 가장 많이 사용하였고, '프라이버시 및 익명의 경제성', '보안 표준 및 정책' 관련 주제를 다룬 연구들은 '경험적 연구' 방법론을 가장 많이 사용한 것으로 나타났다(Fig.5).

전반적으로 '위험 평가 및 보안 투자' 관련 주제에 '분석적 연구' 방법론을 사용한 연구(44개, 15%)가 가장 많았고, '보안 표준 및 정책' 관련 주제에 '경험적 연구' 방법론을 사용한 연구(37개, 13%), 동일한 주제에 '분석적 연구' 방법론을 사용한 연구(30개, 11%)순으로 그 뒤를 따른다. '사이버 범죄와 방어 전략' 관련 주제에 '연구와 정책 의제' 방법론을 사용한 연구(2개, 1%)가 가장 적었고, 동일한 방법론으로 '프라이버시 및 익명의 경제성과 '취약점 관리' 관련 주제를 다룬 연구가 각각 2%(5개)로 그 뒤를 따

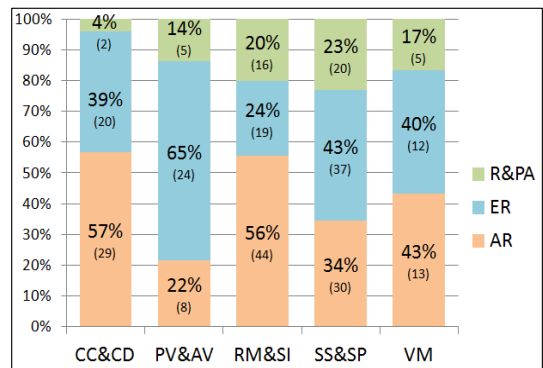


Fig. 5. Cross-analysis of Theme and Methodology

Table 8. Matrix of Theme and Methodology

Theme Method	CC&C D	PV&A V	RA&SI	SS&SP	VM	Total
AR	29 (10%)	8 (3%)	44 (15%)	30 (11%)	13 (5%)	124 (44%)
ER	20 (7%)	24 (8%)	19 (7%)	37 (13%)	12 (4%)	112 (39%)
R&PA	2 (1%)	5 (2%)	16 (6%)	20 (7%)	5 (2%)	48 (17%)
Total	51 (18%)	37 (13%)	79 (28%)	87 (31%)	30 (11%)	284 (100%)

※ Theme Classification Standard

CC&CD : Cyber-Crime and Cyber-Defense Strategy

PV&AV : Privacy and Anonymity Value

RA&SI : Risk Assessment and Security Investment

SS&SP : Security Standards and Policy

VM : Vulnerability Management

※ Methodology Classification Standard

AR : Analytical Research

ER : Empirical Research

R&PA : Research and Policy Agenda

른다(Table 8.).

V. 결 론

본 연구는 보안경제성 관련 연구에서 그동안 진행 된 연구의 흐름을 파악하고 향후 유망한 연구의 주제와 방법론을 찾고자, WEIS에서 2002년부터 2014년까지 총 13개년 동안 발표된 논문들을 대상으로 연구의 주제와 방법론을 중심으로 보안경제성 관련 연구에 대한 정량적인 분석을 시도하였다.

본 연구의 결과, 보안경제성 관련 연구들은 '위험 평가 및 보안 투자' 관련 주제에 '분석적 연구' 방법론을 사용한 연구, '보안 표준 및 정책' 관련 주제에 '경험적 연구' 방법론을 사용한 연구, 동일한 주제에 '분석적 연구' 방법론을 사용한 연구 순으로 많았다. 가장 선호하는 주제는 '보안 표준 및 정책'이고, 가장 선호하는 방법론은 '분석적 연구' 방법론이다. 주제별로 선호하는 방법론은 '사이버 범죄와 방어 전략', '위험 평가 및 보안 투자', '취약점 관리' 관련 주제를 다룬 연구들은 '분석적 연구' 방법론, '프라이버시 및 익명의 경제성', '보안 표준 및 정책' 관련 주제를 다룬 연구들은 '경험적 연구' 방법론이다.

주제와 방법론의 증감추세, 주제와 방법론의 교차 분석 결과 등을 고려하여 향후 유망한 보안경제성 관

련 연구들을 예측해보았다. '프라이버시 및 익명의 경제성' 관련 주제에 '분석적 연구' 방법론을 사용한 연구, '사이버 범죄와 방어 전략', '위험 평가 및 보안 투자' 관련 주제에 '경험적 연구' 방법론을 사용한 연구 등이 향후 유망한 연구가 될 것이라 판단된다.

본 연구는 연구대상에 특정 포럼만을 포함하였다는 점, 연구자의 주관적인 판단으로 분류하였다는 점, 주제 및 방법론만으로 분석하였다는 점으로 인해 한계가 있으나, 정량적인 분석을 통해 보안경제성 관련 연구동향을 파악하였다는 점에서 의의를 가진다. 본 연구의 결과는 보안경제성 관련 연구에 관심이 있는 연구자들이 연구동향 파악, 연구방향 설정 등을 하는데 도움이 될 것이다.

향후 연구에서는 보안경제성 관련 연구가 발표되었을 것으로 예상되는 정보시스템 및 정보보안 관련 저널, 경영/경제 관련 저널 등으로 연구범위를 확대하고자 하는데, 이는 각 저널에서 보안경제성 관련 연구를 찾아내는 과정에 어려움이 따를 것이라 예상된다. 향후 연구에서는 분류기준을 다양화하여 저널, 학문분야, 저자정보 등에 따른 보안경제성 관련 연구동향을 분석하고자 하며, 이를 통해 향후 보안경제성 관련 연구동향을 예측해보고자 한다. 또한, 정량적인(quantitative) 분석에 기술적인(descriptive) 성격을 더한다면 더욱 의미 있는 연구가 될 것으로 기대된다.

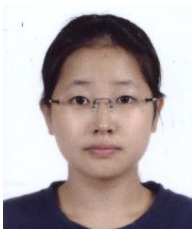
References

- [1] Digital Times, "Stock price of credit card companies, 'joy and sorrow'." 2014.01.23.
- [2] Maeil Business Newspaper, "Three card companies which disclosed personal information would make a loss of over 160 billion," 2014.05.19.
- [3] Korean Bar Newspaper, "Privacy, now when you need to invest," 2014.04.21.
- [4] R. Anderson, "Why information security is hard - an economic perspective," In Computer Security Applications Conference, pp. 358-365, IEEE, Dec. 2001.
- [5] A. Odlyzko, "Economics, psychology, and sociology of security," In Financial Cryptography, pp. 182-189, Springer

- Berlin Heidelberg, Jan. 2003.
- [6] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, pp. 610-613, Oct. 2006.
- [7] R. Anderson, R. Böhme, R. Clayton, and T. Moore, "Security economics and european policy," *Managing Information Risk and the Economics of Security*, Springer US, pp. 55-80, 2009.
- [8] T. Moore, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 103-117, Dec. 2010.
- [9] T. Moore and R. Anderson, "Economics and internet security: A survey of recent analytical, empirical and behavioral research," *Harvard University Computer Science Group*, 2011.
- [10] Hyo-Jung Jun, Hye-Won Yoo, and Tae-Sung Kim, "Analysis on knowledge and skills for information security professionals," *Information Systems Review*, 10(2), pp. 253-267, Aug. 2008.
- [11] F. Belanger and R.E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly*, vol. 35, no. 4, pp. 1017-1042, Dec. 2011.
- [12] J.R. Córdoba, A. Pilkington, and E. WN Bernroider, "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, pp. 479-495, Jan. 2012.
- [13] N. Mustafee, "Evolution of IS research based on literature published in two leading IS journals-EJIS and MISQ," In 19th European Conference on Information Systems, pp. 2658-2668, Jul. 2011.
- [14] P. Palvia, P. Pinjani, and E.H. Sibley, "A profile of information systems research published in *Information & Management*," *Information & Management*, vol. 44, no. 1, pp. 1-11, Jan. 2007.
- [15] H.J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quarterly*, vol. 35, no. 4, pp. 989-1016, Dec. 2011.
- [16] E.B. Swanson and N.C. Ramiller, "Information systems research the-matics: Submissions to a new journal, 1987 - 1992," *Information Systems Research*, vol. 4, no. 4, pp. 299-330, Dec. 1993.
- [17] R.D. Banker and R.J. Kauffman, "The evolution of research on information systems: A fiftieth-year survey of the literature in management science," *Management Science*, vol. 50, no. 3, pp. 281-298, Mar. 2004.
- [18] K. Davies, "Content analysis of research articles in information systems (LIS) journals," *Library and Information Research*, vol. 36, no. 112, pp. 16-28, 2012.
- [19] M. Siponen and R. Willison, "A critical assessment of IS security research between 1990-2004," *Copenhagen Business School*, Feb. 2007.
- [20] Ministry of Knowledge Economy (Current Ministry of Trade, Industry and Energy), "By 2013, Knowledge Information Security Industry 18 trillion won Market Creation", Dec. 2008.
- [21] Standard Korean Dictionary of The National Institute of The Korean Language, <http://stdweb2.korean.go.kr/>
- [22] WEIS 2002, <http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/>
- [23] WEIS 2003, <http://www.cpppe.umd.edu/rhsmi th3/agenda.htm>
- [24] WEIS 2004, <https://www.dtc.umn.edu/seminars/events.php?eventdesc=207&menuid=2>

- [25] WEIS 2005, <http://infosecon.net/workshop/schedule.php>
- [26] WEIS 2006, <http://weis2006.econinfosec.org/program.html>
- [27] WEIS 2007, <http://weis2007.econinfosec.org/program.htm>
- [28] WEIS 2008, <http://weis2008.econinfosec.org/program.htm>
- [29] WEIS 2009, <http://weis09.infosecon.net/programme.html>
- [30] WEIS 2010, <http://weis2010.econinfosec.org/>
- [31] WEIS 2011, <http://weis2011.econinfosec.org/>
- [32] WEIS 2012, <http://weis2012.econinfosec.org/>
- [33] WEIS 2013, <http://weis2013.econinfosec.org/>
- [34] WEIS 2014, <http://weis2014.econinfosec.org/>
- [35] Wikipedia, https://en.wikipedia.org/wiki/Economics_of_security

〈저자소개〉



강 미 화 (Mi-Hwa Kang) 정회원
 2013년 2월: 충북대학교 경영학부 졸업
 2015년 2월: 충북대학교 정보보호경영학과 석사
 2015년 3월~현재: ㈜에이쓰리 정보보호컨설팅
 <관심분야> 정보보호투자, 정보보호교육, 정보보호컨설팅



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 및 학과장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 금융보안원 금융보안컴플라이언스 자문위원, 전자정부 민관협력포럼 자문위원
 <관심분야> 정보통신과 정보보호 분야의 경영 및 정책 의사결정