Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1233

사이버보험의 위험관리 요구사항*

이 송 하,[1†] 전 효 정,[2] 김 태 성[1‡]
[1]충북대학교 경영정보학과, [2]충북대학교 정보보호경영학과

Risk Management Requirements for Cyber Insurance*

Song-ha Lee,[1†] Hyo-Jung Jun,[2] Tae-Sung Kim[1‡]
[1]Department of MIS, Chungbuk National University,
[2]Department of ISM, Chungbuk National University

요 약

지능정보사회를 선도하는 핵심 기술이자 서비스인 사물인터넷의 초연결성으로 인해 사이버리스크가 급증하면서 사이버리스크의 전가(Risk transfer)를 통해 경영환경의 안정성을 높이는 새로운 위험관리 방안으로 사이버보험(Cyber insurance)이 주목받고 있다. 그러나, 사이버보험은 아직 국내에서는 비교적 생소한 개념이다. 이에 본 연구에서는 국내 상황에서 우선적으로 요구되는 보장사항을 도출하여 국내 수요에 적합한 사이버보험의 개념을 제안하고자 하였다. 연구 결과 사이버보험의 수요자들은 사업손실과 배상책임에 가장 많은 필요성을 보이고 있는 것으로 나타났다.

ABSTRACT

Cyber risk is rapidly increasing due to the hyperconnectivity of the IoT in the intelligent information society. Therefore cyber insurance has been attracting attention as a new risk management countermeasure by transferring cyber risk. However, cyber insurance is still a new concept in South Korea. The purpose of this study is to propose the concept of cyber insurance suitable for domestic demand by deriving the priority of cyber insurance coverage. Research results suggest that the most requisite cyber insurance types are business interruption and liability.

Keywords: Cyber Insurance, Cyber-security Insurance, Risk Management, Cyber Security, AHP

I. 서 론

지능정보사회를 선도하는 핵심 기술이자 서비스인 사물인터넷(Internet of Things, IoT)의 '초연결성'에 따른 취약포인트의 증가로 사이버리스크(cyber risk)가 급증하고 있다[1]. 은행, 보험, 에너지, 소매, 제약, 헬스케어, 자동차 등의 산업분야의 최고 임원 959명 중 63%가 자신의 회사가 매일 혹은 매주 중대한 사이버공격을 일상적으로 경험하고 있으며[2], 사이버범죄로 인한 세계경제의 손실규모는 연간 약 4,450억 달러로, 2019년에는 손실액이 최대 2.1조 달러에 이를 것으로 전망된다[3,4]. 또한 스위스 보험사인 Zurich는 이미 2014년 정보사회의 사이버위험 수준이 미국의 서브프라임모기지 사태와 유사한 규모라고 제시하였으며[5], Lloyd's는 미국 전력망에 대한 사이버공격으로 피해규모가 1조 달러에 달할 수 있다고 경고하였다[6].

특히 현재의 사이버리스크는 정보통신기술(ICT)을 활용해 기밀성·무결성·가용성을 침해하여 단순한 데이

Received(08. 22. 2017), Modified(08. 29. 2017), Accepted(09. 29. 2017)
* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 2017 정보보호 특성화대학 지원사업과 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015S1A5A2A01009763).
† 주저자, lsh914@naver.com
‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

터의 손실 뿐 만 아니라, 사생활 침해, 평판 훼손 등의 범위를 넘어 기업에 직접적인 재무적 손실, 경영손실, 사업 중단까지 초래한다[7, 8]. 더불어, 2016년 영국과 웨일스 내에서 발생한 사기범죄의 68%가 은행계좌 및 신용정보와 관련하여 발생하였고[9], 2016년 초 방글라데시 중앙은행은 해커그룹으로부터 부정이체를 통해 8,100만 달러를 탈취 당하는 등[10] 금전 탈취를 목적으로 하는 공격이 증가하고 있다.

우리나라의 경우 IT기반 구축 수준에 비해 보안 관련 대응능력과 인프라 수준이 상대적으로 하위권에 머물면서 아시아태평양 지역 18개국 중에서 사이버 공격에 가장 취약한 것으로 나타났다[11]. 또한 2016년을 기준으로 국내 종사자 1인 이상 기업 9,586개 중 IT 예산에 정보보호 예산을 편성한 기업은 32%로 그 비중이 5% 이상인 기업은 1.1% 수준에 불과하다[12]. 더불어, 사이버보안 대책을 수립하더라도 사이버리스크의 특성상 100% 완벽한 사이버보안을 구현하는 것은 어려운 실정이다.

이에 최근 사이버보험(cyber insurance)이 새로운 위험관리수단으로 주목받고 있다. 그러나, 사이버보험은 아직 국내에서는 비교적 생소한 개념으로 각 연구자 혹은 보고서마다 용어도 통일되어 있지 않은 실정이다. 따라서 본 연구에서는 최우선적으로 요구되는 보장사항(coverage)을 도출하여 국내의 상황에 맞는 사이버보험의 개념을 제안하고자하며, 이를 통해 사이버보험 활성화를 통한 사이버보안 경쟁력 향상에 도움이 되고자 한다.

II. 이론적 논의

2.1 사이버보험

2.1.1 사이버보험 개념의 재정의

사이버보험은 컴퓨터나 네트워크 등 사이버보안과 관련된 사고로부터 발생한 당사자 및 제 3자의 유·무형 자산의 손실을 보장하는 보험 상품의 포괄적인 개념이다[14,15,16,17].

또한 사이버보험은 예측 불가능한 위험에 대한 대비책으로 경영환경의 안정성을 높이는 위험관리수단으로 볼 수 있다. 일반적으로 위험관리는 자산, 취약점, 위협 등을 고려해 위험을 분석 및 평가하고 그에 따른 위험처리 방안을 수립하여 위험을 받아들일 수 있는 수준 이하로 낮추는 것을 말한다. 위험처리

Table 1. Definition of Cyber Insurance

Classification		Ref.
KIRI	Insurance that provides tangible and intangible financial loss resulting from IS threat events	[14]
ENISA	Insurance to ensure the risks associated with cybersecurity and third-party risks	[15]
ABI	Insurance to insure loss of information or damage to IT systems and networks	[16]
MARSH	Insurance that provides financial protection for information and technical risks	[17]

전략은 위험보유, 위험축소, 위험전가, 위험회피 등으로 나눌 수 있는데, 사이버보험의 경우 위험전가(risk transfer)에 해당한다[Table 2.].

실제로 미국의 대형유통업체인 Target은 2013년 4사분기에 해커집단에 의해 최소 1억 1천 건 이상의 고객정보가 유출되어 2015년 1월을 기준으로 총합 2억 5,200만 달러의 피해비용이 발생하였으나, 이 중 약 1/3 수준인 9,000만 달러를 사이버보험으로 커버하였다[20, 21].

현재 사이버보험은 각 보험사 및 연구자별로 사이버배상책임보험(Cyber liability insurance), 사이버보안(보증)보험(Cyber security insurance), 사이버리스크보험(Cyber risk insurance), 디지털리스크보험(Digital risk insurance), 사이버 및 프라이버시보험(Cyber and privacy insurance)등 여러 용어로 불리며 아직 표준화되지 않은 것으로 판단되나[1], 최근에는 사이버보험(Cyber insurance)이라는

Table 2. Types of Risk Management

Classification	Definition
Risk acceptance	Accepting risk and bearing potential loss cost
Risk mitigation	Controling risk through technical and/or administrative security countermeasure
Risk transfer	Preparing the funds as contract with other company to cover potential loss cost
Risk avoidance	Giving up risky process or business

Reconstruction by referring to [18] and [19]

1) Google에서 Cyber Insurance 등의 키워드 검색을 통해 보험사 홈페이지를 직접 방문하여 사이버보험 관련 상품의 명칭을 조사함

용어를 주로 사용하는 추세로 보인다.

2.1.2 사이버보험 관련 연구

사이버보안 투자와 관련하여 기존에는 기술적 보안 대책(firewall 설치, IDS 도입 등) 구현에 대한 투자의 적절성, 각 대책들 간의 비용효과 분석에 대한 연구[22, 23], CISO가 보안투자 예산과 관련하여 CFO를 효과적으로 설득 하도록 지원하는 방법과 관련된 연구[24]가 진행 되었다.

그러나 제한된 자원에서 기술적 보안투자가 항상 효율적인 것은 아니다[25]. 또한 위험관리수단을 구현한 경우에도 사이버 침해사고 발생 시 기업의 이미지 훼손 등의 잔여위험이 존재하기 때문에 완벽한 보안은 없으며, 사이버 보안사고의 경우 사후처리를 위해 발생하는 비용이 크기 때문에 Gordon et. al.[13]은 기술적 보안대책과 더불어 보험을 이용한 위험관리 프레임워크를 제시하였다. 추가적으로 사이버보험은 기술적 보안 대책을 구현하는 것보다 시간 및 비용 측면에서 효과적이라고 주장하였다. 더불어 Kumar et. al. [26]은 기존의 정보시스템 보안 투자관련 연구들은 침입탐지와 예방에만 중심을 두고 있다는 점을 비판하며, 자신들의 연구에서 재난복구계획으로써 사이버보험까지 고려한 통합적인 보안투자결정 모델을 개발하고자 하였다.

국내에서는 주로 전자상거래로 발생할 수 있는 사이버 침해 사고를 배경으로 전자상거래보험이라는 이름으로 사이버보험에 대한 연구가 진행되었으나, 사이버보험의 범위를 배상책임에만 초점을 두고 연구하였다는 점에서 한계가 있다.

라공우[27]는 전자상거래의 여러 위험 요인에 대한 피해구제 방안으로 전자상거래 보험의 활용을 적극 검토해야 하며, 보험업계의 다양한 보험 상품 개발 및 담보 범위의 표준화가 필요하며, 이를 위해 정부차원의 정책적인 대책이 필요하다고 주장하였다.

또한 무역기업은 전자상거래 환경에서의 새로운 위험에 대비하여 방화벽, 안티 바이러스와 같은 기술적인 장치는 물론이고 제도적인 장치로서 보험을 이용하는 것이 필수적이라고 주장하는 연구도 진행되었다[28].

홍진희[29]는 전자상거래보험이 적은 보험료로 고액의 손해배상책임과 소송비용을 해결함으로써 사업자의 왕성한 활동을 뒷받침하게 한다고 주장하며, 정부에서 보험의 가입을 적극 유도하고, 보험업계에서 다양한 상품을 개발해야 한다고 주장하였다.

정보보호의 관점에서는 권홍과 김태성[30]은 기술적 위험관리의 한계를 보완하고 불확실성을 상쇄하기 위해 보험을 이용한 정보보안 위험관리에 대한 인식을 제고하고 활용방안 및 투자전략을 제시하기 위한 연구가 필요하다고 주장하였다.

2.1.3 사이버보험의 국내외 현황

사이버보험은 2000년대 초반에 등장하여 주로 제3자(Third party)에 대한 보상을 담보하였으나, 2003년 CA Security Breach Information Act[2]의 시행으로 인해 당사자(first party)에 대한 보상이 추가되었다. 현재 국외에는 다양한 보장내용(coverage)과 보상규모(limit)의 사이버보험이 존재하며, 2016년 기준 미국에만 60개 이상의 사이버보험 공급자가 존재한다[31]. 2015년을 기준으로 미국의 사이버보험 시장은 약 23억 달러에서 24억 8천만 달러 사이인 것으로 조사되었으며[32, 33], 2020년 미국 사이버보험의 시장규모가 약 75억 달러 까지 성장 할 것으로 전망된다[34].

더욱이 Allianz Life Korea[35]는 정보침해로 인한 처벌과 정보보호 규제 강화는 글로벌 추세로써 이에 따른 기업의 책임 수준이 강화되면서 사이버보험의 성장세가 가속화될 것이라고 전망하였다.

또한 기존의 IT 관련 보험은 기업정보훼손이나 개인정보침해에 관한 위협에만 주로 초점을 두고 있어 점차 다변화되는 사이버리스크에 대한 실질적인 대응력이 부족한 것으로 평가되고 있다. 일례로 2011년 고객정보유출로 피해를 입은 소니가 보험금을 받기 위한 지급요청 소송에서 패소하면서 일반 IT 보험으로는 사이버 공격에 대한 피해보상을 받는 것이 더 이상 어렵게 되었다는 견해가 우세하다[36].

해외 추세와 마찬가지로 국내에서도 법정손해배상 및 징벌적손해배상제도가 발효되면서 기업의 사이버 침해사고에 대한 부담이 커질 것으로 예상되어 사이버보험 수요가 증가 할 것으로 예상된다[Table 3.]. 실제로, 2016년 12월 인터파크는 방송통신위원회로부터 개인정보 유출사고 중 최대금액인 44억 8,000만원의 과징금 및 2,500만원의 과태료 처분을 받았으며[37], 개인정보가 유출 된 고객으로부터 집단

2) 2003년 개인정보유출고지법(Data Breach Notification Law)을 도입한 이후 보험시장이 급속도로 성장. 동법의 개인정보유출시 통지의무조항으로 인해 법 시행 후 개인정보유출사고 통계가 급격히 증가함[31]

Table 3. Domestic Cyber Security Related Acts

	Act 1[3]	Act 2[4]	Act 3[5]
Exemplary damages	Damage claim suit is available below three times of actual loss		
Statutory damages	Damage claim suit is available below 3 million won		
Penalty	less than 3% of sales	less than 5 billions	less than 50 billions
Fine	less than 30 million	less than 50million	less than 20 million

소송도 진행 중이다.

더불어 현행 법률에 의무화된 금융기관 대상의 전자금융거래 배상책임보험은 정보유출로 인한 2차 피해가 발생한 경우에만 보장하며[38], 보상한도액이 20억~50억 원에 불과해 실효성이 낮아[39] 새로운 사이버보험에 대한 요구가 증가할 것으로 보인다.

이처럼 사이버보험은 기존의 IT 보험보다 광범위한 사이버리스크에 대한 피해를 보상한다는 점에서 주목을 받고 있으나, 아직 성숙한 시장으로 볼 수는 없는데 그 이유는 다음과 같다.

첫째, 사이버보험의 보험료 산정을 위해서는 다년간의 사고의 유형, 사고에 따른 피해, 보상금액 등과 관련된 데이터가 필요하지만, 기업들이 사고 데이터 개방을 꺼려하기 때문에 현재의 보험료 산정이 산업 분류와 지역, 기업규모 등에 매우 의존적으로 보험료 산정이 합리적이지 못하다[31, 40, 41].

둘째, 보험사들은 우후죽순으로 보험상품을 내놓고 경쟁하는데 집중하고 있으나, 정작 수요 기업들의 사이버보험에 대한 이해는 부족하다. 일례로 사이버보험의 보험료와 보장사항이 매우 다양한데, 이는 사이버보험을 객관적으로 비교하기 어렵게 만드는 요인이 된다. 또한 제공되는 보장사항이 모든 사이버 위협에 대한 고려를 하고 있지 않음에도 불구하고, 기업들은 자신이 가입한 보험이 어떤 위협에 대해 얼마를 보상해 주는지를 정확히 모르고 있으며, 모든 사고에 대한 비용을 처리해 주는 것으로 착각하고 있다[42].

더불어 공급자(보험사) 측면에서는 사이버리스크는 발생빈도는 낮으나 1회 발생 시 피해규모가 큰점, 사이버사고 관련 소송 수행 관련 비용 추정이 어려운 점, 보험 계약자 간 사이버리스크 관리 수준에 큰 편차가 존재해 일괄적인 요율 책정이 불가능 한 점 때문에 다양한 보험 상품 개발을 주저하고 있으며, 안전할증을 위해 높은 보험료를 부과하고 있다. 수요자(기업) 측면에서는 사이버보험의 약관에 다양한 면책사유가 포함되어 있고, 낮은 위자료 판결 등 실제 손해 발생 사례가 부족하고, 아직은 사이버보험이 담보하는 리스크의 다양성이 부족해 보험 가입의 필요성을 체감하지 못하고 있다. 이 같은 요인들이 사이버보험 시장의 활성화를 저해한다고 볼 수 있다.

3) 정보통신망 이용촉진 및 정보보호 등에 관한 법률(시행 2017. 3. 23)
4) 개인정보보호법(시행 2017. 3. 30)
5) 신용정보보호법(시행 2016. 9. 30)

2.2 사이버보험 보장범위(Coverage)

다양한 문헌들에서 사이버보험의 주된 보장범위를 설명하고 있으나, 문헌에 따라 용어와 내용이 상이한 실정이다. 일례로 개인정보 유출에 따른 비용(breach of privacy)을 큰 범주의 보장범위로 설명하는 문헌이 있는 반면, 개인정보 유출에 따른 배상책임(privacy liability), 개인정보유출알림비용(breach notification costs), 신용정보모니터링 서비스(credit monitoring) 등으로 나누어 설명하는 문헌도 있다. 이에 본 연구에서는 국제기구와 은행, 보험, 컨설팅 업계 등에서 발표한 사이버보험의 보장범위들을 모두 망라하여 현재 국외에서 중요하게 생각되고 있는 보장범위들을 파악하고자 하였다[Table 4.]. 그 결과 국외에서는 개인정보유출에 따른 비용, 자사사업중단(business interruption), 사이버 강탈(cyber ransom and extortion), 데이터 및 S/W 손실(data and software loss)에 대한 보장범위를 가장 많이 언급하는 것으로 나타났다.

2.3 AHP 모형

AHP(Analytic Hierarchy Process, 계층분석기법)는 의사결정의 계층구조를 구성하고 있는 요소간의 쌍대비교를 통해 평가자의 지식, 경험, 직관 등을 기반으로 하는 의사결정방법론 중 하나로서, Thomas. L. Saaty 교수에 의해 1970년 초반에 개발되었다[49]. AHP 방법론은 정량적인 분석이 어려운 의사결정을 위해 관련 전문가들의 정성적 지식을 이용하여 평가 요소의 중요도를 결정함으로써, 상충되는 다수의 평가 기준(다속성) 하에서 합리적으로 최적의 대안을 선택할 수 있도록 설계된 포괄적인 틀이라고 볼 수 있다[49]. 사이버보험의 보장범위는 아직 다수의 의견수렴이 이루어지지 않은 분야로, AHP 방법론을 활용하여 다양하고 복잡한 보장범위

Table 4. Classification of Cyber Insurance Coverage

Classification	[43] OECD (2017)	[44] ABA (2016)	[45] CRS-RMS(2016)	[46]Deloitte (2015)	[47] RIMS (2017)	[48]Advisen&PartnerRe(2016)	Freq.
Assistance coverage - psychological support	-	-	-	-	-	-	-
Bodily injury and death	-	-	Death and bodily injury	-	-	Cyber-related bodily injury and/or property damage	2
Breach of privacy [compensation]	Breach of privacy [compensation]	Privacy liability	Breach of privacy event	Privacy Breach/ Breach Notification	Privacy liability/ Breach notification costs/ Credit monitoring	Data breach	6
Business interruption(BI)/ Interruption of operations	Business interruption/ Interruption of operations	Network Business interruption	Business interruption	Business interruption loss/ Business interruption	Network interruption/ Business interruption	Cyber-related business interruption	6
Communication and media	Communication and media	-	Multi-media liabilities	Media liability	Media liability	Internet media liability	5
Contingent business interruption (CBI) for nonphysical damage	-	-	Contingent business interruption	-	-	Cyber-related contingent business interruption	2
Cyber ransom and extortion	Cyber ransom and extortion	Cyber Extortion	Cyber extortion	Extortion	Cyber extortion& ransom	Cyber extortion	6
Data and software loss	Data and software loss	Data Asset Protection	Data and software loss	Damage to Data	Data loss and restoration	Data restoration	6
D&O	-	-	Liability - D&O	-	-	-	1
Environmental damage	-	-	Environmental damage	-	-	-	1
Financial theft and/ or fraud	Financial theft and/ or fraud	-	Financial theft & fraud	-	Theft&fraud	Funds transfer fraud/ Cyber-related bodily injury and/or property damage	4
Fines and penalties	Fines and penalties	Crisis management & Identity theft response	Regulatory and defence coverage	-	Regulatory fines	Regulatory fines& penalties	5
Incident response costs	Incident response costs	Crisis management & Identity theft response	Incident response costs	-	Reputation& crisis management/ Forensic investigation costs	-	4
Intellectual property theft	-	-	Intellectual property theft	-	-	-	1
Legal protection - Lawyer fees	-	-	-	-	-	-	-
Network security/ Security failure	Network security/ Security failure	Network security liability	Network service failure liabilities	Network security/ Virus transmission	Transmission of viruses or malicious code	-	5
Physical asset damage	-	-	Physical asset damage	-	-	-	1
Products	-	-	Liability - product and operations	-	-	-	1
Professional services E&O.	-	-	Liability - professional services errors & omissions	Professional services			2
Regulatory & legal defense costs (excluding fines and penalties)	Regulatory & legal defense costs(excluding fines and penalties)	Crisis management & Identity theft response	Regulatory and defence coverage	Regulatory investigation	Forensic investigation costs	-	5
Reputational damage (excluding legal protection)	-	Crisis management & Identity theft response	Reputational damage	-	Reputation& crisis management	-	3
Tech E&O	-	-	Liability - tech E&O	-	-	-	1

들을 구조화하고, 비율척도를 통해 우선순위 및 가중치를 도출·통합·분석함으로써 보장범위에 대한 평가를 실시하였다.

AHP 방법론을 이용할 경우 무엇보다 분석결과를 신뢰할 수 있는지를 판단할 수 있는 기준인 일관성 비율(consistency ratio, CR)을 확인하는 것이 필요하다. 일관성 비율은 그 값이 0.1 보다 작을 경우 응답자가 비교적 일관성 있게 응답하였다고 판단한다. 그러나, 사회과학 연구에서는 상·하위 기준간의 독립성 확보가 쉽지 않다는 점을 감안하여 일관성 비율을 0.2 이하로 보는 경우도 많다[50, 51]. 이에 본 연구에서는 사이버보험이 국내 시장에서 매우 생소한 개념이라는 점을 감안하여 일관성 비율의 기준을 0.2 이하로 정하였다.

III. 연구모형

본 연구모형의 목적은 지능정보사회의 보안성 향상을 위해 최근 주목받고 있는 위험관리수단이자 정보보호 분야의 보편적 서비스로써 활용될 수 있는 사이버보험의 보장사항(coverage) 중 가장 우선적으로 필요시 되는 분야를 선정하는 것이다.

3.1 위험관리 세부사항 도출

평가기준의 도출을 위해 문헌연구를 통해 제시된 22개 사이버보험 보장사항(coverage)[Table 4.]을 비슷한 유형별로 분류하여 6개 그룹으로 나누었다. 분류된 그룹은 사이버보험의 보장범위로 볼 수 있으며, 특성을 반영하여 명명하고 상위평가기준으로 사용하였다. 이를 통해 조사대상자들이 AHP설문 응답 시에 먼저 간소화된 상위평가기준에 대한 자신의 중요도를 생각하도록 함으로써 응답의 신뢰도를 높이고자 하였다. 더불어 연구결과를 활용 할 때, 상위평가기준 간의 비교를 통해 큰 흐름에서 어떤 사이버보험 보장범위가 가장 필요시 되는지, 하위평가기준을 통해 구체적으로는 어떤 세부 보장사항이 가장 시급하게 필요시 되는지 도출하고자 하였다. 단, 하위기준으로 사용된 22개 세부보장사항 중 정보 및 네트워크 기술에 대한 전문인 배상책임(professional services errors or omissions liability)과 기술에 대한 전문인 배상책임(technology errors or omissions liability)는 서로 상관관계가 있으며, 하나의 기준으로 보아도 무방하다고 판단되어 정보네트워크 기술에 대한 전문인 배상책임(errors or omissions liability; E&O)으로 조사하였다. 더불어 상위평가기준 중 사고대응비용은 일면 사이버보험의 모든 보장사항에 포함된다고 볼 수 있어 특화된 하위기준이 없기 때문에, 최종적으로 하위평가기준으로 총 20개의 지표를 활용하였다[Table 5.].

3.2 연구모형: 위험관리 요구사항 체계화

본 연구에 사용된 모형은 제 1계층은 모델의 목표인 사이버보험 보장사항의 우선순위 결정, 제 2계층은 사이버보험의 보장범위인 6개 상위평가기준, 제 3계층은 사이버보험의 세부 보장사항으로 볼 수 있는 20개의 하위평가기준 등으로 구성되어 있다[Fig. 1.].

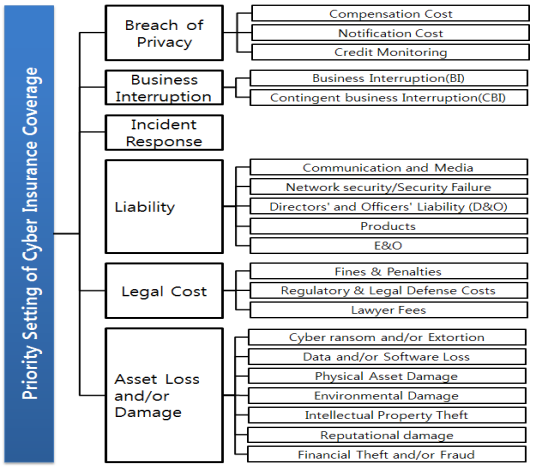

Fig. 1. AHP Model

IV. 실증분석

데이터 수집은 Saaty가 제시한 9점 척도법[49]을 활용한 설문을 바탕으로 사이버보험 수요자로서의 전문성을 보유한 재직자를 중심으로 진행되었다. 1차적으로 2017년 7월 19일에 개최된 정보보호 GRC 연구회 참석자를 대상으로 오프라인으로 25부를 배포하여 10부를 회수하였다. 2차적으로 보안컨설팅전문기업의 본부장급 이상 및 제조업, 금융업, 통신서비스업 등에 해당하는 업체의 정보보안 부문 책임자 등을 대상으로 2017년 7월 28일부터 2017년 8월 10일까지 온라인으로 배포하여 총 12부를 회수하였다. 이에 총 회수된 설문지는 22부이며,

Table 5. Evaluation Criteria of AHP Model

Upper Criteria	Lower Criteria	Operational Definition
Breach of privacy	Compensation cost	Compensation costs after leakage of private and/or sensitive data, including psychological support, bodily injury and death, property damage, etc.
	Notification cost	Cost for notifying the customer about leakage of their private and/or sensitive data
	Credit monitoring	Cost for providing credit monitoring services as a follow-up of the customer's private and/or sensitive data leakage
Business interruption	Business interruption(BI)	Lost profits or extra expenses of insured caused by a unavailability of IT systems or data as a results of cyber attacks or other non-malicious IT failures
	Contingent business interruption(CBI)	Reimbursement for the lost profits of the third parties caused by a unavailability of IT systems or data as a results of cyber attacks or other non-malicious IT failures of insured
Incident response	N/A	Direct costs incurred to investigate and close the incident to minimise postincident losses
Liability	Communication and media	Compensation due to misuse of communication media at the insured resulting in defamation, libel, slander, copyright/ trademark infringement, negligence in publication of any content in electronic or print media
	Network security failure	Compensation for damages caused to third parties through the policyholder/observed company's IT network.(the policy-holder/observed company may not have any damage but has been used as a vector or channel to reach a third party)
	Directors and officers liability (D&O)	Compensation in case of claims made by a third party against the insured directors and officers, including breach of trust or breach of duty resulting from cyber event
	Errors or omissions liability (E & O)	Compensation costs related to the failure in providing adequate professional/technical services or (technical) products resulting from a cyber-event
	Products	Compensation in case delivered products or operations by the insured are defective or harmful resulting from a cyber-event
Legal cost	Fines and penalties	Cost for fines and penalties imposed on the insured
	Regulatory and legal defense costs	Regulatory costs: costs incurred to the insured when responding to governmental or regulatory inquiries related to a cyber-attack Legal defense costs: own defense costs incurred to the insured facing legal action in courts following a cyber-attack
	Lawyer fees	Costs of legal action brought by or against the policyholder including lawyer fees costs in case of trial
Asset loss and/or damage	Cyber ransom and/or extortion	Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment
	Data and/or Software loss	Cost of reconstituting data or software that have been lost, deleted, stolen, encrypted or corrupted
	Physical asset damage	Cost of insured's loss due to the destruction of physical property resulting from cyber attacks
	Environmental damage	Costs of clean up, recovery and liabilities after leakage of toxic and/or polluting products consecutive to a cyber-event
	Intellectual property theft	Insured's loss of value of an IP asset, expressed in terms of loss of venue as a result of reduced market share
	Reputational damage	Compensation for loss of profits due to a reduction of trade/ clients because they lost confidence in the impacted company
	Financial theft and/or fraud	Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets

※Main reference: 'Categories and Definitions' of OECD(2017)[43]
Sub reference: 'Cyber Insurance Loss Coverage Categorization' of CRS-RMS(2016) [45]

Expert Choice 2000 소프트웨어를 이용하여 분석하였다. 일관성 지수 계산 결과, 0.20을 기준으로 13부가 채택되었다. 응답자 13명의 의견을 기하평균을 이용하여 종합하여 분석한 결과, 일관성 비율은 0.02로 도출되었다.

4.1 설문 응답자 일반사항

채택된 설문 응답자의 일반사항은 〔Table 6.〕과 같다. 응답자는 모두 민간기업 소속으로, 주로 중소/중견기업에 재직 중인 것으로 나타났다.

응답자가 재직 중인 회사의 업종은 정보통신업의 비율이 절반이상을 차지하였다. 응답자의 대부분이 관리자 및 책임자 급으로 실제 의사결정이 가능하거나 사내의 현황에 대한 이해도가 높은 직위에 위치하고 있으며, 응답자 전부가 정보보호 업무취급자로 나타났다. 이에 본 연구의 응답자들은 설문 내용에 대해 상당한 전문성(이해도)을 보유하고 있다는 점에서 연구에 활용된 응답의 신뢰성이 매우 높다고 볼 수 있다.

본 설문 응답자의 절대다수가 사이버보험을 이미 알고 있는 것으로 나타났으며, 극히 일부 응답자의 소속기관이 사이버보험 혹은 전산/IT 관련 보험을 보유하고 있는 것으로 나타났다. 응답자 대부분이 사이버보험 도입이 보안사고 발생 시 사후대응 비용마련(preparing for post-response costs)에 도움을 줄 것이라고 응답하였으며, 예외적으로 금융보험업에 종사하는 응답자의 경우 내부자의 고의적인 보안사고 및 방어에 효과를 볼 것이라고 응답하였다. 사이버 보험 가입 시 주요 고려사항으로는 응답자의 절반 이상이 보험의 보장사항(coverage)의 다양성을 가장 중시하는 것으로 나타났다〔Table 7.〕.

Table 6. Details of the Respondents

Classification	Category	Freq.(%)
Affiliation	Small and Medium Enterprise	8(61%)
	Large Enterprise	5(39%)
Total		13(100%)
Industry	Retail	-
	Healthcare	-
	IT	7(54%)
	Finance/Insurance	1(8%)
	Educational Service	1(8%)
	Manufacturing	2(15%)
	Government&Public	-
	Etc.	2(15%)
Total		
Position	Practitioner	-
	Project Manager	4(31%)
	Decision Maker	8(61%)
	Etc.	1(8%)
Total		13(100%)
Relation of IS task	Related	13(100%)
	Unrelated	-
Total		13(100%)

Table 7. Details of the Responses

Classification		Freq.(%)
Cyber insurance awareness	Yes	12(92%)
	No	1(8%)
Total		13(100%)
Whether to join cyber insurance	Yes	2(15%)
	No	11(85%)
	Unfamiliar	-
Total		13(100%)
Whether to join IT insurance	Yes	3(23%)
	No	6(46%)
	Unfamiliar	4(31%)
Total		13(100%)
Major expected effects of cyber insurance	Complement for lack of IS skills and expertise	-
	As parts of IS investment technology introduction	2(15%)
	Countermeasures against insider security threat	1(8%)
	Countermeasures against outsider security threat	-
	Preparing for post-response costs	10(77%)
	Minimizing IS investment	-
	Etc.	-
Total		13(100%)
Key considerations	Premium	4(31%)
	Limit	2(15%)
	Coverage	7(54%)
	Etc.	-
Total		13(100%)

4.2 사이버보험 보장범위 간 가중치 비교 결과

사이버보험의 유형이라고 볼 수 있는 상위평가기준 중에서는 배상책임(liability), 사업손실(business interruption), 법적비용(legal cost) 순으로 나타났으며, 자산손실(asset loss and/or damage)에 따른 비용이 가장 낮은 순위로 나타났다〔Table 8.〕.

Table 8. Weights of Upper Criteria

Classification	Weight	Rank
Breach of privacy	0.109	5
Business interruption	0.196	2
Incident response	0.118	4
Liability	**0.339**	**1**
Legal cost	0.165	3
Asset loss and/or damage	0.073	6
Total	1.000	

세부 보장사항 중에서는 자사사업중단(business interruption; BI) 및 제3자사업중단(contingent business interruption; CBI)의 우선순위가 가장 높게 나타났으며, 정보/네트워크 배상책임(errors or omissions liability; E&O), 제3자 네트워크 피해(network security failure) 및 임원배상책임(directors and officers liability; D&O) 등이 그 뒤를 이었다[Table 9.].

더불어 개인정보유출에 따른 물질적/정신적 손해배상(compensation cost) 및 사이버보안 침해사고에 따른 규제 및 법에 따른 방어를 위한 비용(regulatory & legal defense costs)도 높은 순위로 나타났다. 반면 최근 화두가 되고 있는 랜섬웨어/강탈에 대한 복구비용(cyber ransom and/or extortion)을 상쇄할 수 있는 사이버보험 보장사항에 대한 필요성은 비교적 낮게 나타났다[Table 9.].

이를 통해, 사이버보험의 수요자들은 사업 손실과 배상책임 부분에 가장 많은 관심과 필요성을 느끼고 있음을 알 수 있다.

Table 9. Weights of Lower Criteria

Classification		Weight	Rank
Breach of privacy	Compensation cost	0.073	6
	Notification cost	0.020	14
	Credit monitoring	0.031	12
Business interruption	Business interruption	**0.103**	**1**
	Contingent business interruption	**0.103**	**1**
Incident response		0.019	15
Liability	Communication and media	0.042	11
	Network security failure	**0.079**	**4**
	D&O	**0.079**	**4**
	E&O	**0.092**	**3**
	Product	0.071	8
Legal cost	Fines & penalties	0.059	9
	Regulatory & legal defense costs	0.073	6
	Lawyer fees	0.048	10
Asset loss and/or damage	Cyber ransom and/or extortion	0.014	18
	Data and/or software loss	0.018	17
	Physical asset damage	0.011	20
	Environmental damage	0.010	21
	Intellectual property theft	0.012	19
	Reputational damage	0.024	13
	Financial theft and/or fraud	0.019	15
Total		1.000	

V. 결 론

지능정보사회가 도래함에 따라 지금까지는 경험하지 못한 사이버 침해사고가 빈번하게 발생하는 등 사이버리스크가 폭발적으로 증가하고 있다. 더불어 최근의 비즈니스 환경은 기업의 규모와 관계없이 사이버보안 위협에 직면하고 있으며, 특히 중소기업은 상대적으로 사이버보안에 대한 지식 및 이를 위한 인력이 부족하여 관리가 허술하며, 투자할 여력이 없는 경우가 많기 때문에 사이버보안에 더욱 취약하다[52]. 이러한 상황 속에서 사이버보험은 사이버리스크의 전가를 통한 위험관리수단 중 하나로 급부상하고 있다. 더불어 사이버보험은 기술적 위험관리수단을 수립하는 것 보다 시간적·비용적 측면에서 우위를 지니며, 전문가가 아니더라도 비교적 쉽게 접할 수 있는 위험관리수단이라는 점에서 정보보호 분야의 보편적 서비스로써 활용이 가능하다. 그러나, 사이버보험은 아직 국내에서는 생소한 개념으로 정확한 정의조차 되어있지 않으며, 사이버보험의 활성화 및 그 효과성 향상을 위해서는 다수의 연구가 진행되어야 한다.

이에 본 연구에서는 지능정보사회의 사이버보안 향상에 기여하고자, 사이버보험의 개념 및 보장사항(coverage)에 대한 문헌연구를 진행하였으며, AHP분석을 통해 가장 우선적으로 요구되는 사이버보험의 보장사항을 조사하여 국내 수요 맞춤형 사이

버보험의 유형을 도출하고 초기 사이버보험의 발전방향을 제시하고자 하였다.

연구결과 기업의 책임자 이상에서 사이버보험에 대한 인지도가 매우 높은 것으로 나타났으며, 이를 통해 국내에서도 사이버보험에 대한 관심이 증가하고 있는 것을 알 수 있다. 국내 기업의 사이버보험 도입 유인은 주로 '보안사고 발생 시 사후대응 비용마련(preparing for post-response costs)' 으로 나타났다. 더불어 사이버보험 가입 시 사이버보험 보장사항(coverage)의 다양성을 가장 중시하며 그 다음으로는 보험료(premium), 보험금(limit) 순으로 나타났다.

또한 국내 기업이 현재 요구하는 사이버보험의 유형은 배상책임(liability)과 사업손실(business interruption) 순으로 나타났다. 세부적으로는 먼저, 배상책임의 경우 정보/네트워크 배상책임(E&O), 제3자 네트워크 피해(network security failure), 임원배상책임(D&O) 등이 높은 순위를 차지하였다. 다음으로 사업손실의 경우에는 자사사업중단(BI)과 제3자사업중단(CBI)에 따르는 피해에 대한 보상이 중요한 것으로 나타났다.

이 같은 이유는 최근 국내 기업들이 해킹이나, DDoS 공격, 랜섬웨어 등을 통해 시스템이 마비되어 자사 및 제3자(고객)의 업무마비에 따른 자사의 영업 손실과 더불어 계약에 따른 IT 서비스를 제대로 이행하지 못하여 발생하는 추가적인 배상요구가 증가하고 있기 때문으로 판단된다. 일례로 7.7 DDoS 공격 이후 최근까지도 금융권, 정부기관, 일반기업 등을 대상으로 한 DDoS공격 협박이 심심치 않게 일어나고 있으며, 최근에는 랜섬웨어에 감염되거나 감염을 막고자 기업들이 업무를 일부 중지하면서 직접적인 영업손실이 발생하고 있다. 더불어 2017년 6월 10일 호스팅업체인 '인터넷나야나'의 호스팅 서버가 랜섬웨어에 감염되어 병원과 쇼핑몰등 다양한 사이트가 마비되면서 10%의 고객들이 이탈하였으며, 피해보상으로 고객에게 호스팅 사용기간을 무료로 연장해주거나, 영구적으로 무료 제공하는 등의 조치를 제공하는 등 사이버침해사고로 인한 기업휴지에 따른 사업영업 손실 및 배상책임이 발생하였다[53].

추가적으로 랜섬웨어에 따르는 자산손실 및 개인정보유출에 따른 위자료 등에 대한 보장사항이 비교적 낮은 순위를 보인 것은 국내에서는 아직 주목할 만한 랜섬웨어의 몸값 지불 사례가 다수 발생하지 않았으며, 개인정보 유출에 따른 손해배상 소송이 기각되거나 일반적으로 10만 원 선에서 결정되고 있으며, 국내의 경우 소송에 참여한 사람들에게만 배상이 이루어지기 때문에 기업들의 이에 대책 마련의 시급성이 아직 부족하기 때문으로 해석된다.

위와 같은 결과를 바탕으로 사이버보험의 실효성 확대 및 활성화를 위한 몇 가지 제안사항을 도출하였다.

첫째, 사이버보안 침해사고는 기존보험으로 커버하기 어려우며, 특화된 보장사항의 제공이 필요하다. 사업중단과 관련된 보험 및 배상책임관련 보험은 이미 일부 존재하지만, 기존의 보험으로는 사이버보안과 관련된 침해사고를 보장받지 못하기 때문에 여전히 IT/사이버보안 관련 기업들이 위 유형의 침해사고에 대한 보장의 필요성을 느끼고 있는 것으로 보인다. 이에 단기적으로는 기존의 보험에 사이버사고와 관련하여 보상이 가능하도록 추가담보를 제공하거나, 장기적으로는 사업중단 및 배상책임을 커버하는 단독 사이버보험의 신설이 필요하다.

둘째, 사이버보험은 타 보험보다 유연성을 지녀야 한다. 지능정보사회의 사이버보안침해사고 유형은 매우 빠르게 변화한다. 본 연구결과에서 사업중단과 배상책임이 높은 우선순위를 보인 이유는 최근에 발생한 침해사건사고의 유형이 반영되었기 때문으로 판단된다. 이에 사이버보험은 전통적인 보험보다는 사이버보안 상황에 민감하게 반응해야 할 필요가 있다.

셋째, AHP 분석의 결과를 활용하여 기업이 조금 더 손쉽게 사이버보험을 선택하도록 도울 수 있다. 사이버보험은 매우 다양한 보장사항을 지니고 있으며, 단독보험으로 나타날 수도 있지만 기존의 보험에 사이버보안침해사고 관련 보장사항을 추가하는 형태로 활용될 수도 있다. 이 같은 점은 고객들이 사이버보험을 선택 할 때 혼란을 주거나, 이미 가입하고 있다고 착각하게 만드는 요인이다[42]. 이에 본 연구와 같이 AHP 분석을 활용하여 도출된 상위 보장사항들을 사이버보험의 기본사항으로 설정하여 보편적 서비스로 제공하고, 이외의 보장사항은 고객사의 성격에 맞게 추가할 수 있도록 한다면 조금 더 손쉽게 기업맞춤형 단독 사이버보험을 설계할 수 있을 것이다.

더불어 향후 연구에서는 다양한 업종별, 실제 사건 혹은 사건 시나리오 별로 필요시 되는 사이버보험에 대하여 심화 연구를 진행하고자 한다. 일례로 기관분류 및 업종에 따른 사이버보험 관련 요구사항의 차이정도, 사이버보험 수요자의 사이버보안 이슈에

따른 요구사항(보장사항, 보험료 등) 변화의 민감도, 최적보험료 수준 평가 등의 다각적인 연구를 통해 더욱 다양한 수요에 적합하고 구체적이며, 실효성 있는 사이버보험의 활성화 방안을 도출 할 수 있을 것이다.

결과적으로 본 연구는 최근 화두가 되고 있는 사이버보험의 혼재된 개념 및 보장사항(coverage) 관련 용어와 내용을 정리였으며, 가장 시급하게 요구되는 사이버보험의 유형 및 보장사항을 도출하였다. 이에 본 연구결과는 사이버보험의 실효성 극대화를 통해 궁극적으로 기업 및 국가의 보안성 향상에 활용될 수 있을 것이다.

References

[1] AGCS, Allianz risk barometer top business risks 2016, 2016.

[2] R. Ostvold and B. Walker, Business resilience in the face of cyber risk Accenture, 2015.

[3] AGCS, A guide to cyber risk: managing the impact of increasing interconnectivity, Sep. 2015.

[4] G. Stephen, Lloyd's CEO: cyber attacks cost companies $400 billion every year, Fortune, Jan. 2015.

[5] Jason Healey and Goldman Sachs, Beyond data breaches: global interconnections of cyber risk, Zurich, Apr. 2014.

[6] S. Basak, Attack on U.S. power grid could cost $1 trillion, Lioyd's says, Bloomberg Business, Jul. 2015.

[7] Hye-Eun Lee, Current status and future tasks of cyber risk and cyber insurance, KIRI Report, Jan. 2017.

[8] P. Daniele, A. Maugeri and A. Nagurney, In Operations Research, Engineering, and Cyber Security, Springer International Publishing, pp. 117-134, Mar. 2017.

[9] Office for National Statistics, Crime in england and wales: year ending sept 2016, Jan. 2017.

[10] Byeong-Cheol One, Lazarus, a suspect to bank of bangladesh hacking is belonging to north korea?, Boannews, Apr. 2017.

[11] R. Arash, C. Cloud, J. Midgley, J. M. Moyer and B. Strauss, 2016 deloitte asia-pacific defense outlook, Deloitte, 2016.

[12] Ministry of Science and ICT and Korea Internet Security Agency, Survey on information security(business), Feb. 2017.

[13] L. A. Gordon, M. P. Loeb and T. Sohail, "A framework for using insurance for cyber-risk management," Communications of the ACM, Vol. 46, No. 3, pp. 80-85, Mar. 2003.

[14] A-leum Lee, Influence and implications of reputation risk on insurance companies, Global Issue, KIRI Weekly, Jun. 2015.

[15] ENISA, Incentives and barriers of the cyber insurance market in europe, Jun. 2012.

[16] https://www.abi.org.uk/Insurance-and-savings/Products/Business-insurance/Cyber-risk-insurance(visited in 2017.4.19.)

[17] https://www.marsh.com/ca/en/services/cyber-risk.html(visited in 2017.4.19.)

[18] Jae-Bock Lee, Principles of insurance, Dunam, 2008.

[19] Sang-Soo Jang, Tae-Hee Cho, Seung-ho Shin, Dae-Hyun Sin, ISMS build and utilize, Life and Power Press, 2013.

[20] Target, Form 10-K(Fiscal year 2015.1.31.), United States Security and Exchange Commission Fillings, 2015.

[21] K. McGinty, Target data breach price tag: $252 million and counting, Advisen Cyber FPN, Feb. 2015.

[22] H. Cavusoglu, B. Mishra and S. Raghunathan, "A model for evaluating IT security investments," Communications of the ACM, vol. 47, no. 7, pp. 87-92, 2004.

[23] H. Cavusoglu, B. Mishra and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture," Information Systems Research, vol. 16, no. 1, pp. 28-46, Mar. 2005.
[24] L. D. Bodin, L. A. Gordon and M. P. Loeb, "Evaluating information security investments using the Analytic Hierarchy Process," Communications of the ACM, vol. 48, no. 2, pp. 78-83, Feb. 2005.
[25] L. A. Gordon and M. P. Loeb, "The economics of information security investment," ACM Transactions on Information and System Security (TISSEC), vol. 5, no. 4, pp. 438-457, Nov. 2002.
[26] R. L. Kumar, S. Park, and C. Subramaniam, "Understanding the value of countermeasure portfolios in information systems security," Journal of Management Information Systems, vol. 25, no. 2, pp. 241-280, 2008.
[27] Kong-Woo La, "A Study on relations of Insurance and damage of Electronic Commerce," The Journal of Korea Research Society for Customs, 4(1), pp.199-224, Dec. 2003.
[28] Gun-Hoon Shin, "A Study on the Market Status and Issues of e-Commerce Insurance," International Commerce and Information Review, 7(3), pp. 27-51. 2005.
[29] Jin-Hee Hong, "Legal Issues of Insurance on Liability from Electronic Commerce," Institute for the Study of Law Dong-A University, (59), pp.325-359, May 2013.
[30] Hong Kwon and Tae-Sung Kim, "A study on information Security Risk Management Using Insurance," Proceedings of the 2009 Korean Management Symposium, pp. 1-3, June 2009.
[31] L. John, "Cyber-insurance—I do not think that word means what you think it mean," San Francisco, RSA Conference 2017, Feb. 2017.
[32] Aon Benfield, Cyber—the fast moving target: benchmarking views and attitudes by industry, 2016.
[33] So-Yang Lee, The latest trends in the US cyber insurance market, KIRI Report, June 2015.
[34] PwC, Insurance 2020 & beyond: reaping the dividends of cyber resilience, 2015
[35] Allianz Life Korea, Now is the time to prepare for the new cyber risk era, Sep. 2015.
[36] Byeong-Cheol Won, Pay attention to cyber insurance in the information protection market in 2017, Boannews, Jan. 2017.
[37] In-Soon Kim, Interpark, filed an administrative suit against 500 million penalty charges to korea communications commission, Etnews, Feb. 2017.
[38] Yong-Sup Han, Personal information liability insurance 'nominal thing' (?), Joseilbo, Feb. 2014.
[39] Byung-Hwan Bae and Kyung-Sik Min, Policy suggestions on how to activate the domestic information security insurance market, Internet & Security Focus, Jul. 2013.
[40] Chang-Hee Choi and Hye-Ran Kim, Implications of overseas cyber liability insurance market growth, KIRI Weekly, Sep. 2014.
[41] Hye-Won Byeon, Considerations for improving cyber insurance trends and cyber risk management, KIRI Weekly, Nov. 2015.
[42] D. Nathans, "Cyber-insurance: fraud, waste or abuse?," San Francisco, RSA Conference 2017, Feb. 2017.
[43] OECD, Supporting an effective cyber insurance market, 2017.
[44] American Bankers Association, 2016 cyber insurance buying guide, 2016.

[45] Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, Managing cyber insurance accumulating risk, 2016.
[46] Deloitte, Inside, 7, Quarterly Insights from Deloitte, 2015 .
[47] RIMS, Cyber insurance: considerations for businesses, 2017.
[48] Advisen&PartnerRe, 2016 survey of cyber insurance market trends, 2016.
[49] T. L. Satty, The analytic hierarchy process, New York: McGraw-Hill, 1980.
[50] T. L. Satty and K. P. Kearns, Analytic planning-the organization of systems, lst Ed., Pergamon Press, Jan. 1985.
[51] T. L. Saaty, "How to make a decision: the analytic hierarchy process," European Journal of Operational Research, vol. 48, no. 1, pp. 9-26, Sep. 1990.
[52] NIST, Small business information security: the fundamentals, NISTIR 7621(Rev.1), 2016.
[53] So-In Byeon, Internet nayana offers compensation for ransomware, Sisajournal-E, Oct. 2017.

〈저자소개〉

이 송 하 (Song-ha Lee) 학생회원
2015년 2월: 충북대학교 경영정보학과 학사
2017년 2월: 충북대학교 경영정보학과 석사
2017년 3월~현재: 충북대학교 경영정보학과 박사과정
〈관심분야〉 정보보호 교육 및 인력, 정보보호정책, 보안경제성 및 사이버보험, 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
〈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, 행정자치부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, ISMS/PIMS 인증위원회 위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책 의사결정