4차 산업혁명 도입 촉진을 위한 정보보호 제도 개선방안 연구

- 사이버 보험의 역기능 분석 중심 -

2022년 7월

과학기술정보통신부

최우석

국외훈련 개요

1. 훈련국 : 미국

2. 훈련기관명 : University of California, San Diego

3. 훈련분야 : 정보통신정책

4. 훈련기간 : 2020년 8월 10일 ~ 2022년 6월 27일

훈련기관 개요

1. 기관명 : 캘리포니아대학교 샌디에고
(University of California, San Diego)
글로벌 정책&전략 학부
(School of Global Policy & Strategy)

2. 주소 및 연락처

ㅇ 주소 : 9500 Gilman Dr. La Jolla, CA 92093

ㅇ 홈페이지 : https://www.ucsd.edu/,
https://gps.ucsd.edu/

ㅇ 전화 : +1 (858) 534-7496

3. 설립목적

ㅇ 21세기 중대한 사회적 도전에 대응하기 위해 설립. 과학 기술을 실세계에 접목하고 새로운 세대의 글로벌 리더를 양성

4. 조직

ㅇ 르벨, 존 뮤어, 써굿 마셜, 얼 워런, 엘리너 루즈벨트, 식스 등 6개 캠퍼스로 구성

5. 연구분야 및 기능

ㅇ 과학분야의 급속한 발전에 힘입어 과학과 엔지니어링 분야의 대학원 중심 학교로 시작하여 기술집약적 고등교육에 집중

ㅇ 지구온난화, UCSD파스칼(프로그래밍 언어), 해양생물학, 해양군사기술, 정보통신기술, 슈퍼컴퓨터, 지진연구, 도시계획 및 설계 등 연구

6. 정책학과(MPP) 학위 이수 요건

ㅇ 총 92학점

- 전공필수 36학점(졸업프로젝트 포함)
- 특성화 분야 20학점(Specialized Area, 전필과 유사)
- 전공선택 36학점

7. MPP 핵심 커리큘럼 및 연구 영역

ㅇ 핵심 과정 : 정책학, 경제학, 재무, 계량경제학 등

ㅇ 특성화 분야 : 프로그램 디자인 및 평가, 미국 및 경쟁 규제, 환경 정책, 보건 정책, 불평등 및 사회 정책, 평화 및 보안 등

차 례

I. 서론

최근 전 세계적으로 4차 산업혁명 도입이 본격화되고 있다. 인공지능 등 최신 정보통신 기술이 잘 알려진 하이테크 산업 분야 뿐만아니라 전통산업에도 적용되면서 전 산업의 생산성 향상이 진행중이다. 이에 따라 우리나라도 4차 산업혁명 위원회를 설립하여 정부 정책을 4차 산업혁명에 적합하도록 심의·권고하는 등 사회·경제적 변화에 발빠르게 대응하려고 해온 바 있다.

그런데, 정보통신기술이 확산될수록 정보통신기술의 역기능인 사이버위협과 이에 따른 사회적 혼란 가능성이 대두되며 4차 산업혁명의 걸림돌로 작용하고 있다. 전력망 등 국가 기간 인프라에서 일상적으로 사용하는 사물인터넷 제품들에 이르기까지 인터넷에 연결되는 모든 것이 해킹을 당할 수 있는 가능성이 있기 때문이다. 특히 최근에는 주요 데이터를 인질로 삼아 금전을 요구하는 랜섬웨어 해킹 형태가 급증하면서 시민들의 우려를 낳고 있다.

이에 따라, 4차 산업혁명의 빠른 확산을 위해서는 사이버사고를 억제하고 정보통신기술로 연결된 경제사회시스템의 지속적인 운영 가능성을 보장할 수 있는 보다 진전된 사이버보안 체계 도입이 강조된다.

이런 가운데 최근 사이버보안 강화를 위한 한가지 수단으로 사이버보험이 부각되고 있다. 사이버보험(Cyber Insurance)은 사이버 활동 중 기업의 과실·태만 혹은 제3자의 사이버공격으로 발생하는 기업의 손실 위험을 담보하는 보험으로, 기업이 입은 재정적 손실과 제3자에 대한 배상책임 등을 보장하는 상품이다. 이 보험은 사이버사고 발생시 기업들의 빠른 회복을 돕고, 적절한 가격 전략을 통해 기업들의 사이버보안 투자를 유도하는 역할을 할 것으로 기대된다.

사이버보험은 미국, 영국 등을 중심으로 2000년대 초반부터 시장이 발달해왔으며, 한국의 경우 사이버사고에 의한 피해보상 사례가 부족해 사이버보험 시장 발달이 늦었으나, 2018년 정보통신서비스 제공자를 대상으로 사이버보험 가입 의무를 부과하면서 조금씩 시장이 확대되고 있다.

<참고자료>

○ 사이버 범죄로 인한 세계 경제 손실규모는 '14년 연간 4,450억 달러 수준(세계 GDP의 0.8%)

○ 사이버보험 시장 규모는 2016년 기준 약 35억 달러 수준(PwC, 2015)

○ 2016년 기준 미국의 사이버보험 시장 규모는 연간 32억 5천만 달러로 추산(PwC, 2015)

○ 미국 국토안보부는 사이버보험 활성화를 위해 '12년부터 정책연구 및 포럼 운영을 추진 중

출처: 과학기술정보통신부

그런데, 정책 및 시장에서의 이런 기대와 달리 학계의 이론 연구에 의하면 사이버보험은 경우에 따라 기업들의 보안 투자 유인을 낮추어 사회 전체적으로 사이버보안 수준을 열화시킬 가능성이 있는 것으로 나타났다.

Shetty, Khalili 등에 따르면, 사이버보험의 기업 보안에 대한 영향은 보험 시장의 환경에 따라 달라지는데, 보험 시장이 독점적인 경우에는 보험사가 가입자의 보안 투자를 유도할 수 있으며, 따라서 사회적으로 보안 수준이 높아질 수 있다. 하지만, 보험 시장이 경쟁적인 경우 보험사는 가입자에게 보안 투자를 유도할 수 없으며 사회 전체의 보안 수준이 낮아지게 된다.

Shetty et al. (2010)은 경쟁적인 시장에서 사이버보험이 기업들의 보안 수준에 어떤 영향을 미치는지 이론적으로 연구하였다. 이 연구는 정보 비대칭성의 유무에 따라 두 가지 상황을 분석하였다. 첫 번째로 보험사가 기업의 보안 수준을 확인할 수 없는 정보 비대칭성이 존재할 때를 분석하였는데, 이 때에는 보험 시장이 성립하지 못하였다. 두번째로 보험사가 기업의 사이버보안 수준을 완전히 관찰할 수 있는 상황, 즉 도덕적 해이가 없는 환경을 가정하였는데, 이 상황에서도 보험은 보험이 없는 상황에 비해 보안 수준을 악화시켰다. 사이버보험이 위험 회피적인 가입자의 효용을 높일 수는 있어도 보안 수준을 높이는 인센티브로서는 역할 하지 못했다.

Khalili et al. (2018)은 독점적 시장에서 사이버보험의 영향을 이론적으로 연구하였다. 이 연구는 최근 머신러닝 등 기술 발달로 보험사가 가입자를 사전에 충분히 검열할 수 있다고 보았다. 즉, 정보 비대칭성이 해소될 수 있다고 가정하였다. 이 가정 하에 이 연구는 독점적 시장에서 보험사가 적절한 가격 전략을 통해 보험사의 보안 투자를 유도할 수 있다는 것을 밝혀냈다.

만약 사이버보험이 시장에 미치는 역기능이 더 크다면 정부의 보험 도입 정책은 재검토되어야 할 것이다. 다만 현재까지 연구들은 모두 이론 연구로서 현실에서 실제 데이터를 바탕으로 사이버보험의 효과성에 대해 분석한 연구는 없었다. 실제 시장은 완전 독점이라거나 경쟁적이라고 단정할 수 없으며, 이론이 전제하고 있는 가정이 현실에서 성립하지 않는 경우가 많기 때문에 현실에서의 사이버보험의 효과는 이론과 다를 수 있다.

이에 따라, 이 연구는 국내에서 사이버보험이 확산됨에 따라 우리 시장 환경에서 사이버보험이 끼치는 역기능이 있는지 확인하기 위해 진행되었다.

한국에서는 2018년에 『정보통신망법』(현재는 『개인정보보호법』으로 관련 조항 이관됨) 개정을 통해 정보통신서비스 제공자를 대상으로 사이버보험이 일부 의무화되었다. 이에 따라 보험 의무화 정책 시행 전과 후에 정보통신서비스 제공자 집단과 기타 기업 집단을 비교함으로써 사이버보험이 기업의 사이버보안 투자에 미치는 영향을 분석할 수 있게 되었다.

분석 결과, 우리나라에서 사이버보험이 의무화된 이후 사이버보험 의무 가입 대상 기업들은 사이버보안 투자를 줄인 것으로 나타났다.

분석에는 한국 정부가 오랜기간 국내 기업들의 정보보호 실태를 체계적으로 조사하여 자료를 축적하고 있는 「정보보호 실태조사」를 활용하였으며, 사이버보험이 의무화된 2018년을 포함하는 5년간(2016~2020)의 실태조사 데이터를 활용하였다. 분석은 '이중차분법'(Difference in Differences)을 사용하였으며, 처치그룹은 정보통신업종, 통제그룹은 정보통신업을 제외한 모든 기업으로 설정하였다. 처치그룹이 사이버보험 의무 가입 대상인 정보통신서비스 제공

자와 정확히 일치하지는 않지만, 실태조사 데이터가 허용하는 가장 유사한 분류체계이기 때문에 이를 채택하고 이에 따른 오류 가능성을 고려하여 결과를 보정하였다. 이 연구에서 기업들의 사이버보안 수준을 가늠하는 변수로는 '기업이 사용중인 정보보호 제품의 종류의 수', '정보보호 제도 및 인프라 수준', '아웃소싱 중인 정보보호 서비스의 종류의 수' 등이 테스트되었으나, '정보보호 제품의 종류의 수' 변수만이 통계적으로 의미 있는 결과를 나타냈다.

구체적으로, 분석 결과 사이버보험 의무 가입 대상 기업들은 보험 가입 의무가 부과된 후 사용하는 정보보호 제품의 종류의 수를 최소 9% 감소시킨 것으로 나타났다.

이는 기업들이 보험을 통해 위험이 줄어든만큼 사이버보안 투자를 할 유인이 낮아진 것으로 해석할 수 있을 것이다. 또한 보험사들이 가입자들에 대해 사이버보안 투자를 유도할 수 있을 정도로 시장 지배력을 갖추지는 못했다는 것을 의미하기도 한다. 이와 같은 결과는 기존 이론 연구의 예상과 부합한다.

개별 기업들의 보안 투자 축소는 결과적으로 국가 네트워크 전반의 보안 수준 감소로 이어진다. 전체 네트워크는 개별 네트워크가 모여서 이루어지며, 네트워크의 연결성으로 인해 한 지점의 보안 약화는 곧 전체의 보안 위협으로 이어질 수 있기 때문이다.

사이버보험이 당초 의도했던 네트워크 보안 강화 효과를 내지 못하고 오히려 이를 열화시키고 있다는 것은 정부 당국이 주목해야 할 부분일 것이다. 사이버보험의 부정적인 외부성을 방치할 경우 사이버사고 가능성과 피해를 키우고 결과적으로 더 높은 사회적 비용을 발생시킬 우려가 있다.

사이버보험 도입 및 확산은 개별 기업 입장에서는 사이버보안

활동에 있어 선택권이 넓어지는 것을 의미하므로 이들에게 긍정적으로 작용할 수 있다. 보험이 과도한 수준으로 의무화되지 않는 한, 기업은 보험 상품과 보안 조치를 적절히 갖춤으로써 보험이 존재하지 않았을 때보다 높은 효용을 얻을 수 있을 것이다. 다만 개별 기업이 각자의 효용 극대화를 추구하는 과정에 사회 전체적으로는 보안 수준이 약화되는 부정적 외부성이 발생하는 것이다.

따라서, 정부는 사이버보험 도입은 장려하되 보험에 따른 부작용은 최소화될 수 있도록 제도를 보완할 필요가 있다.

정부는 사이버보험 가입자 확대를 통해 수익을 얻는 보험사가 보험에 가입한 기업들에 대해 사이버보안 점검을 실시하거나 보안 컨설팅을 하고, 사이버보안 사고에도 더욱 적극적으로 개입하도록 유도함으로써(침해사고 대응팀 운영 등) 전체 네트워크의 사이버보안 수준 향상에 기여할 수 있을 것이다.

Ⅱ. 사이버보안 정책 동향

1. 국내·외 사이버사고 현황

전세계적으로 사이버사고는 점점 다양화되며 피해규모가 지속적으로 커지고 있다. 90년대 후반 CIH 바이러스에서 시작하여 2003년 1.25인터넷 대란, 2009년 7.7 디도스 사건, 2011년 3.4 디도스 사건, 2013년 국내 주요 언론사와 금융권 전산망이 다운된 3.20 사이버테러, 2014년 한수원 해킹과 6.25 사이버공격, 2017년 IP카메라 해킹 공격 등 사이버사고는 끊이지 않고 발생해왔다.

특히 2018년도에는 국내 가상화폐 취급업소 해킹사고로 약 1,000억원의 손실이 발생하여 사회적 혼란이 있었고, 보안업계에 따르면 이 시기 전세계적으로는 약 6천억 달러(676조원)에 달하는 사이버사고 피해(맥아피, 2017)가 있었던 것으로 알려져 있다.

또한 2021년 5월에는 미국 송유관업체 '콜로니얼 파이프라인(Colonial Pipeline)'이 해킹을 당해 석유 운송이 마비되는 사태가 발생했다. 이는 '다크사이드'라는 조직의 랜섬웨어 공격으로 금전을 요구하면서 발생한 사건인데, 이 공격으로 콜로니얼사는 송유관 8,850킬로미터 구간을 폐쇄하였으며, 미국 교통부는 미국 동남부 18개 주에 긴급사태를 선언하고 석유의 육상 수송을 추진하기도 하였다.

폐쇄된 콜로니얼사의 송유관은 하루 250만 배럴의 원유를 운송, 미 동부지역 석유 수요의 45%를 담당하던 것으로, 송유관 폐쇄에 따라 미국 동남부 지역에서 기름 사재기가 발생하였으며, 결국 콜로니얼사는 '다크사이드'에 5백만불(56억원)을 가상화폐로 지불하고 송유관을 정상화시켰다. 다만, 미국 FBI는 지불한 가상화폐 중 230만불을 회수했다고 밝히기도 했다.

표 1 주요 사이버사고 현황

사고명	해킹유형	사고내용
빗썸정보유출 ('17.6)	정보유출	빗썸 회원정보 유출사고 발생
인터넷나야나 랜섬웨어 감염 ('17.6)	랜섬웨어 감염	인터넷나야나 호스팅서버(153대)가 랜섬웨어에 감염되어 이용기관 홈페이지가 랜섬웨어 협박화면으로 변조
워너크라이 랜섬웨어 ('17.5)	랜섬웨어 감염	워너크라이 랜섬웨어에 감염되어 데이터 암호화 피해발생
여기어때 개인정보유출 ('17.3)	개인정보 유출	SQL 인젝션 및 세션 변조 공격 등으로 개인정보 유출. 이를 악용하여 금전요구
인터파크 개인정보유출 ('16.5)	개인정보 유출	내부직원의 PC가 악성코드에 감염된 후 사내 확산 및 DB파일 탈취
뽐뿌해킹 ('15.9)	개인정보 유출	비정상DB질의에 대한 검증절차가 없는 보안취약점을 이용하여 개인정보유출
한수원해킹 ('14.12, '15.3,7,8)	정보유출	해커그룹(Who am I)이 원전중단을 요구하며 원자력 관련 자료를 인터넷에 공개
SKB DDoS공격 ('14.11)	DDoS	SKB DNS를 대상으로 DDoS 공격이 발생한 사고
KT정보유출 ('14.3)	해킹	KT 홈페이지의 타인여부 인증절차 보안취약점을 악용, KT고객 개인정보 유출 사고
6.25사이버공격 ('13.6)	해킹 DDoS	총 69개 기관·업체등에 대한 DDoS 공격 및 홈페이지 변조 사고 발생
3.20사이버공격 ('13.3)	해킹	방송·금융기관 등 서버·PC 등 악성코드 감염

출처: 사이버위험 관리를 위한 보험의 역할 및 과제, The Risk, 2017

2. 국내·외 사이버보안 정책 현황

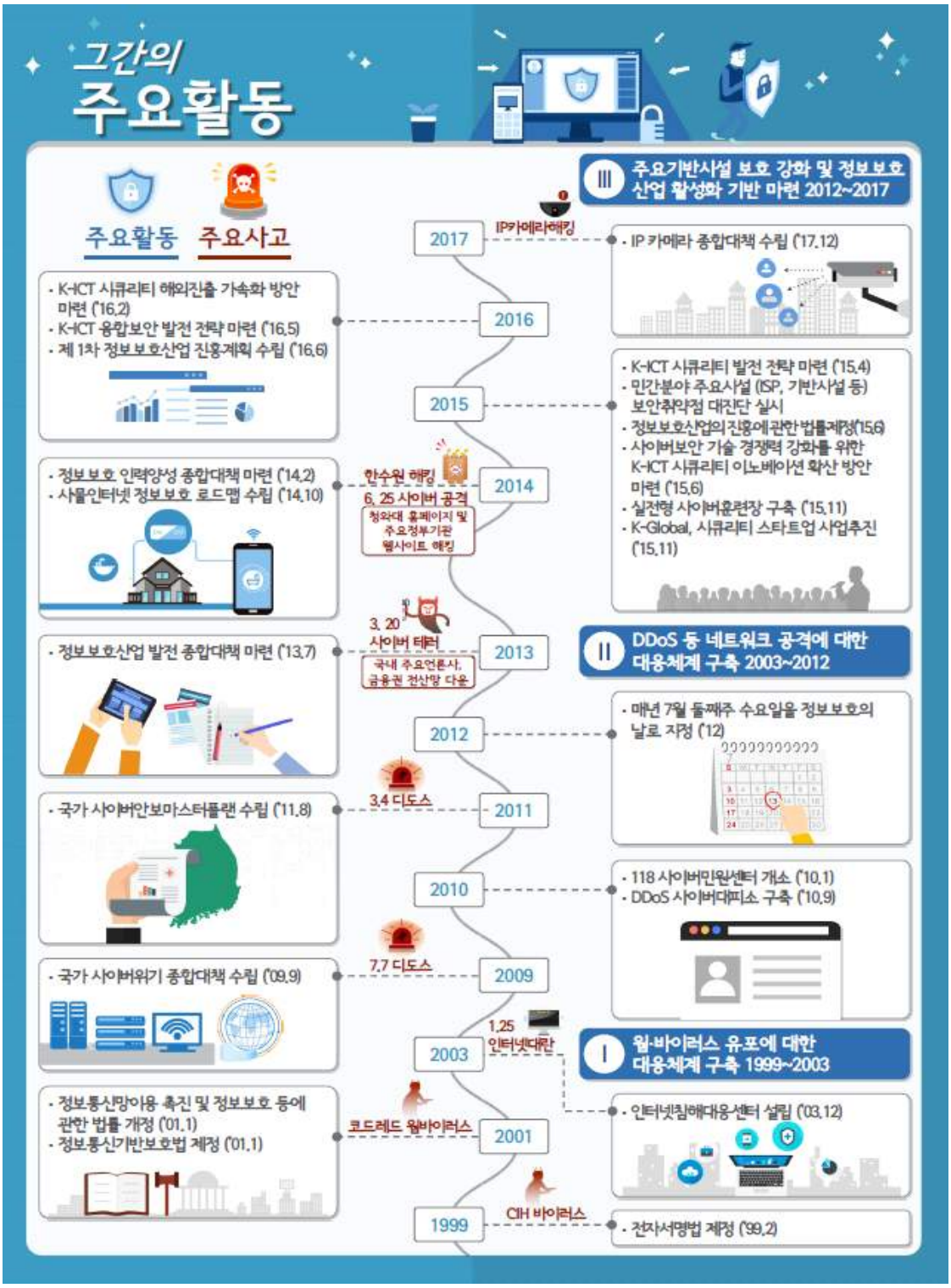
이렇게 점점 확대되는 사이버사고에 대응하기 위해 세계 각국은 사이버보안 대응체계를 고도화하고 관련 정책을 지속 발전시켜 왔다. 이 중 우리나라와 미국의 사이버보안 정책을 살펴보면 다음과 같다.

2.1. 국내 사이버보안 정책

우리나라는 발달된 정보통신인프라와 북한 등 지정학적 요소로 인해 과거부터 끊임없는 사이버사고를 겪어왔으며, 이에 따라 관련 사이버보안 대책을 지속적으로 발전시켜왔다.

그간 우리나라의 주요 사이버보안 정책을 보면, 2001년『정보통신망 이용 촉진 및 정보보호 등에 관한 법률』(정보통신망법)과『정보통신기반보호법』이 제정되면서 국가 정보통신망 및 기간 시설들에 대한 보안이 추진되었다. 이후 2003년 1.25 인터넷대란을 겪은 뒤 국가 차원에서 인터넷 침해대응센터를 설립(2003년 12월)하였고, 2009년 7.7 디도스 사태가 발생함에 따라 이와 같은 사태를 방지하고자 2009년 9월에「국가 사이버위기 종합대책」을 수립한 바 있다. 이후 2011년 3.4 디도스사태 발생 이후 동년 8월에「국가 사이버안보 마스터플랜」을 수립하였고, 2013년에는 정보보호 산업 발전 종합대책이 마련되면서 사고에 대한 대응 차원의 정책에서 보안 산업 기반을 강화하는 보다 근본적이고 지속적인 정책으로 전환하였다. 2014년에는「정보보호 인력양성 종합대책」과「사물인터넷 정보보호 로드맵」이 수립되었고, 2015년에는『정보보호산업의 진흥에 관한 법률』이 제정되면서 관련 정책 추진이 더욱 탄력을 받게 되었다. 2015년 4월에는「K-ICT 시큐리티 발전전략」이 마련되었고, 2016년에는「제1차 정보보호산업 진흥계획」,「K-ICT 융합보안 발전전략」 등이 마련되었다.

그림 1 주요 사이버사고 및 국내 사이버보안 대책 추진 경과



출처: 민간부문 정보보호 종합계획 2019, 과학기술정보통신부

가장 최근 마련된 사이버보안 정책으로는 「2019 민간부문 정보보호 종합계획」과 2020년 마련된 「K-사이버방역 추진전략」이 있다.

「2019 민간부문 정보보호 종합계획」은 당시 랜섬웨어, 가상화폐 취급업소 해킹 및 IP카메라 해킹 등 국민 일상생활에 영향을 주는 사이버사고 발생이 증가하면서 국민 불안감이 확산됨에 따라 이에 대응하기 위해 마련된 것이다. 드론, 자율차 등 정보통신기술이 발달하고 전방위로 접목·확산되면서 사이버위협이 디지털경제 발전의 걸림돌로 작용하고, 기존 PC·네트워크 중심의 사이버보안 대응체계로는 신기술 기반으로 새롭게 발생하는 사이버위협 대응에 한계가 나타나고 있다는 문제의식이 있었다.

이에 따라 이 대책은 '안전하고 신뢰할 수 있는 사이버환경 구현'이라는 비전 하에 사이버안전 확보와 정보보호 산업 발전이라는 두 가지 목표를 위해 사이버안전망 확대, 정보보호 산업 경쟁력 강화, 정보보호 기반 강화라는 세 가지 전략과 10여 가지 추진과제로 구성되었다.

추진과제로는 사이버안전망 확대를 위해 사이버위협 사전 탐지·대응 역량 강화, 사물인터넷 기기 보안성 강화, ICT 융합 영역까지 보호 범위 확대, 취약 부문 보안 강화 지원, 정보보호 산업 경쟁력 강화를 위해 공정하고 합리적인 시장 여건 조성, 정보보호 기업 성장 환경 조성, 융합보안 신시장 창출, 해외진출 본격화, 정보보호 기반 강화를 위해 정보보호 법제 개선, 미래 사이버보안 기술 확보, 정보보호 전문인력 양성, 국내·외 정보보호 협력 강화 등이 있다.

정부는 이를 통해 정보통신 침해사고에 대한 조기 대응능력을 확보하고, 정보보호 시장 50% 확대 및 글로벌 기술 경쟁력 확보 등의 목표를 설정한 바 있다.

그림 2 2019 정보보호 종합계획 비전, 전략 및 과제 체계도

정부가 2020년에 마련한 「K-사이버방역 추진전략」은 5G, 인공지능 등 4차 산업혁명 확산, 비대면 경제 활성화 등 우리 산업과 사회 전반에 걸쳐 디지털 전환이 빠른 속도로 진행됨에 따라 사이버 위협의 경계가 없어지고 정보보호를 필요로 하는 영역이 확대되고 있으며 무인상점 해킹, 인공지능을 활용한 공격 등 새로운 보안위협이 증가하는데 대응하기 위해 마련되었다.

표 2 디지털경제 시대의 정보보호 패러다임의 변화

구분		기 존		디지털경제
주체		**보안전문가** ◦ 보안관리자, 정보보호책임자 등	⇨	**누구나(Whoever)** ◦ 디지털을 활용하는 모든 이용자
방식		**위협발생(의심)시** ◦ 사이버위협 발생시 진단・점검・대응	⇨	**항상(Whenever)** ◦ 상시 진단・점검 및 선제적 탐지・대응
범위		**주요시설** ◦ 국가 중요시설, 주요자원 등 보호자산	⇨	**모든 곳(Wherever)** ◦ 디지털이 활용・결합되는 모든 기기・서비스

출처: K-사이버방역 추진전략, 과학기술정보통신부('20.2)

이 전략은 '안전하고 신뢰할 수 있는 세계 최고의 디지털안심 국가 실현'이라는 비전 하에 디지털경제 시대 정보보호 패러다임 변화를 반영한 대응체계의 선제적 확충과 안심할 수 있는 디지털 환경 조성을 통한 지속 가능한 성장을 뒷받침한다는 목표로 3대 전략 8대 과제로 구성되었다.

추진 과제는 디지털안심 국가 기반 구축을 위해 사이버보안 대응체계 고도화, 수요자 중심 디지털 보안 역량 강화, 보안 패러다임 변화에 대한 대응 강화를 위해 차세대 융합보안 기반 확충, 신종 보안위협 및 AI 기반 대응 강화, 디지털 보안 핵심기술 역량 확보, 정보보호산업 육성 기반 확충을 위해 정보보호산업 성장 지원 강화, 디지털보안 혁신인재 양성, 디지털보안 법제도 정비 등이다.

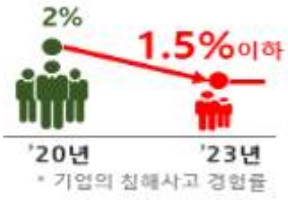
표 3 K-사이버방역 추진전략 비전, 전략 및 과제 체계도

【비전】 안전하고 신뢰할 수 있는 세계 최고의 디지털안심 국가 실현

【추진 방향 및 목표】

◈ **디지털경제** 시대 **정보보호 패러다임 변화**를 반영한 **대응체계 선제적 확충**

◈ 안심할 수 있는 **디지털 환경 조성**을 통한 **지속 가능한 성장** 뒷받침

글로벌 정보보호 역량 강화	기업 침해사고 발생 억제	정보보호시장 규모 확대
		

【추진 전략 및 과제】

1. 디지털안심 국가 기반 구축	① 사이버보안 대응체계 고도화 ② 수요자 중심 디지털보안 역량 강화
2. 보안 패러다임 변화 대응 강화	① 차세대 융합보안 기반 확충 ② 신종 보안위협 및 AI 기반 대응 강화 ③ 디지털보안 핵심기술 역량 확보
3. 정보보호산업 육성 기반 확충	① 정보보호산업 성장 지원 강화 ② 디지털보안 혁신인재 양성 ③ 디지털보안 법제도 정비

2.2. 미국의 사이버보안 정책

미국은 사이버보안 시장이 세계에서 가장 발달한 국가이자 가장 큰 경제규모를 가진 국가로서 사이버공격도 가장 많이 받는 국가로서 그동안 사이버보안 정책과 관련 산업이 발달해왔다.

미국은 자유주의를 중요시하는 국가로서 정부의 민간에 대한 개입을 최소화하는 움직임을 보여왔으나, 사이버보안 분야에서는 시장 실패를 극복하기 위해 산업 정책을 일부 도입하여 운영 중이다. 사이버보안 분야에서 발생하는 과소 공급 문제 등 해소를 위해 미국 정부도 민·관 협업의 필요성을 인식하고 있는 것으로 보인다[1].

사이버보안 분야에서 시장 실패 유형은 대표적으로 조정 실패, 정보 부족, 기업들의 도덕적 해이, 외부성 등이 있다. 조정 실패는 정보통신기업, 플랫폼기업과 사용자 간에 사이버보안 책임 소재가 불분명한 것을 의미하고, 정보 부족은 사이버보안이 정부나 기업의 입장에서 핵심 사업영역이 아니고 고도의 기술적 영역에 해당하기 때문에 정부나 기업이 충분한 정보를 갖기 어렵다는 것을 의미한다. 기업의 도덕적 해이는 기업들이 그들의 사이버보안 수준을 높이는 대신 이용자들이 단말 장치에서 사이버보안 수준을 강화하도록 책임을 전가하려 한다는 것을 의미하고, 외부성은 사이버범죄 및 사이버보안 취약성이 경제 발전을 가로막는 부정적 외부효과를 가지며, 이에 대응하는 사이버보안 활동은 시장 참여자들에게 공공재로 인식된다는 것을 의미한다. 이상의 특성에 따라 사이버보안은 시장에 맡겨질 경우 시장에서 필요로하는 것보다 과소 공급되고, 전문인력이 부족해지며, 이에 따라 자국 시장 내에서 수요 공급이 해소되지 않고 글로벌 공급사슬에 공급을 과의존하게 되는 문제가

1) W. Lynn 미 국방부 차관은 “정부나 산업계는 홀로 사이버보안에서의 도전을 해결할 수 없는데, 산업계가 중요한 국가 정보 인프라의 대부분을 소유·운영하고 있으며, 민간은 정부의 효과적 규제가 필요하기 때문”이라고 언급하였다. (2009)

발생하게 된다.

미국은 이런 사이버보안 분야의 시장 실패를 극복하기 위해 미국 벤처투자사와 협력, 인력양성 프로그램 운영, 민·관 협력, 무역 규제 완화 등 다양한 정책을 추진하고 있다.

미국 정부는 사이버보안 과소 공급 문제를 해결하기 위해 사이버보안 분야에 투자하는 벤처투자사와 협력을 하고 있다. 예를 들어, 전직 CIA 출신이 설립한 벤처투자사(인큐텔)와 협력하여 정부 수요를 충족시킬 수 있는 사이버보안 기업을 양성하고 있는데, 세계적인 보안 기업 '팔란티어'가 2003년에 인큐텔의 투자를 바탕으로 설립되기도 했다. CIA는 '디지털 혁신 부서'(Directorate of Digital Innovation)을 구성하여 벤처캐피털에 최신 이슈 및 요구사항을 전달하며 업계를 지원하고 있다.

미국은 사이버보안 분야 인력의 역량을 강화하기 위해 산학연관이 협력하여 교육기관을 설치·운영하고 교육 프로그램을 제공하는 등 다양한 인력양성 프로그램을 운영하고 있다. 미국 NIST 산하에 NICE(National Initiative for Cybersecurity Education)를 설치하여 2012년부터 운영하고 있으며, NICERC(National Integrated Cyber Education Research Centre)는 국토안보부와 협력하여 초중등 학교에 사이버보안 커리큘럼을 제공하고 있다. 또한, 미 국방부의 국방디지털서비스부(Defense Digital Service)는 'Hack the Pentagon', 'Hack the Army' 등의 프로그램을 운영하고 있다.

이와 함께 미국은 'Pentagon Highlands Forum', 'National Cyber Sercurity Alliance' 등을 통해 기업과 정부 기관 담당자가 교류할 수 있는 장을 마련하고 있으며, 중·러 등 적국 정부가 그들의 기업을 통해 미국에 침투하는 것을 막기 위해 전략적으로 중요한 분야에서는 해외 기업의 제품·부품 사용을 제한하는 등 무역

규제를 강화하고 있다.

한편, 미국은 2020년 5G의 중요성을 고려하여 「국가 5G 보안전략」을 마련하기도 했다. 미국은 5G 이동통신이 21세기 국가 번영을 이끌 성장동력(driver)으로서 10조 개의 기기를 연결시키며 우리의 삶을 변화시킬 것이나, 그 성과의 이면에는 새로운 위험과 취약점이 존재한다고 인식하고 있다. 이에 따라 미국은 안전하고 신뢰할 수 있는 5G 통신인프라의 개발, 구축 및 관리를 선도하기 위한 「5G 보안 전략」을 마련하였고, 2020년 9월 국토안보부 사이버 보안 및 기반시설 보호원(CISA)[2]이 구체적 실행전략을 마련하였다.

미국의 「국가 5G 보안 전략」에서 미국은 국내 차세대 통신 및 정보 통신 기반 구조의 신속한 개발과 확산을 촉진하는 한편 연방정부의 구매력을 이용하여 보다 안전한 공급망으로의 이동을 장려한다고 밝히고 있으며, 미국 정부는 민간 부문과 협력하여 5G의 진화 및 보안을 촉진하고, 기술 및 주파수 기반 솔루션을 관리할 것이라고 한다.

이를 위해 미 정부는 국내 5G 확산 촉진, 5G 인프라·응용의 보안 위험 평가 및 핵심 보안원칙 식별, 전세계 5G 인프라 개발 및 배치 중 미국 경제 및 국가 안보에 대한 위험 해결, 안전하고 신뢰할 수 있는 5G 인프라의 책임 있는 글로벌 개발 및 구축 촉진이라는 4가지 추진 전략을 마련하였다.

보다 구체적으로 살펴보면, 미국내 5G 확산 촉진을 위해서 연방통신위원회(FCC)는 더 많은 상업용 주파수를 확보, 5G 기반시설 승인 절차 간소화, 5G 네트워크 장비 규제 현대화를 추진하고, 5G 인프라·응용의 보안 위험 평가 및 핵심 보안 원칙 식별을 위해서

2) CISA : Cybersecurity and Infrastructure Security Agency

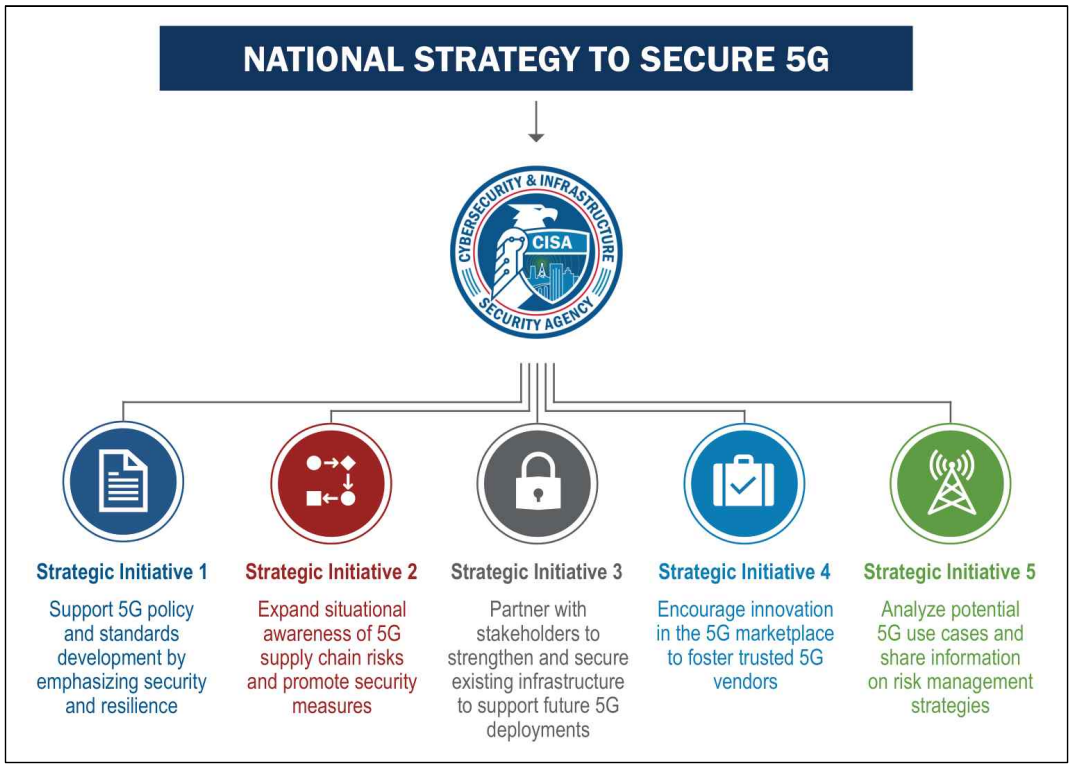
미국 정부는 각 지방정부 및 민간부문 협력사들과 함께 5G 기반시설의 취약점과 위협을 지속적으로 평가하고, 사이버보안, 공급망 위험 관리, 공공 안전 등 핵심 보안 원칙을 식별, 개발 및 적용한다. 전세계 5G 인프라 개발 및 배치 중 미국 경제 및 국가 안보에 대한 위험 해결을 위해서는 미국 정부는 공급망 위험 관리 표준 및 가이드라인을 마련하고, 적대적 국가·기관 등과의 거래를 금지할 수 있도록 미국 정부 기관에 권한 부여한다. 안전하고 신뢰할 수 있는 5G 인프라의 책임 있는 글로벌 개발 및 구축 촉진을 위해서 미국은 우호국가 및 민간 기업들과 함께 국제 5G 보안 원칙 개발 및 구현을 촉진하고, 5G 공급 시장의 경쟁력 및 다양성을 제고한다.

미국의 「5G 보안전략」의 실행계획 성격으로 2020년 9월에 국토안보부 사이버보안 및 기반시설 보호원이 마련한 「5G 전략」은 국가 안보, 기술 혁신, 경제적 기회를 개선·확대하는 5G 연결 보장을 비전으로 하여 5가지 이니셔티브를 마련하였다. 참고로 미국 국토안보부 산하의 사이버보안 및 기반시설 보호원(CISA)은 사이버 및 물리적 인프라의 보안, 복원력 및 신뢰성 향상을 담당하고 있으며, 미국 내 5G 관련 주요 시설 대부분이 민간 영역에 있어 5G 보안 활동은 민간의 자발적 참여와 CISA의 조언으로 이루어지고 있다.

5가지 이니셔티브의 세부 내용은 다음과 같다. 첫째, 보안 및 복원력에 중점을 둔 5G 정책 및 표준 개발 지원을 위해 5G 구조 설계시 악성 행위자가 영향을 미치지 못하도록, 많은 신뢰할 수 있는 기관·기업이 5G 관련 표준 제정에 참여하도록 독려한다. 둘째, 5G 공급망 보안 위험 인식 제고 및 보호방안 보급을 위해 연방 정부 내 ICT 공급망 위험에 대한 정보 공유를 확대하고 5G 공급망에 대한 공통 보안 프레임워크를 개발한다. 셋째, 기반시설 보호수준 제고를 위해 국가 연구소 등과 협력하여 5G 부품·장비의 취약점을 식별하고 이를 국내 및 해외 기관에 전파·공유한다. 넷째, 안전한

5G 공급사 육성을 위해 관계기관과 5G 관련 R&D 프로젝트 개발 및 '5G 혁신 챌린지' 등 대회를 개최하는 한편, 신뢰할 수 없는 공급사의 장기적 위험을 분석·보고한다. 다섯째, 가능한 5G 사용 사례를 분석하여 위험관리전략 정보를 공유하기 위해 실제 혹은 시뮬레이션 공간에서의 5G 기술 사용 사례를 분석하여 취약점을 식별·제공하고, 민간 전문가들이 더 많은 정보를 개발하도록 촉진한다.

그림 3 CISA 5G 전략 개요



이상의 미국 사이버보안 전략을 살펴보면, 미국은 악성 행위자가 새로운 통신 방식인 5G의 구조 설계 단계부터 취약점을 내재시키지 않도록 방지하는데 중점을 두고 있으며, 이를 달성하기 위해

국내외의 우호적인 국가·기관·기업과 광범위한 협력 및 공정경쟁을 촉진하고자 하고 있다. 미국은 주요 인프라 보호는 단일 기업이 전적으로 위험을 관리할 수 없다는 점을 고려, 보안성이 높은 생태계가 구축될 수 있도록 노력하고 있다.

한편, 미국은 2021년 5월 송유관업체 '콜로니얼 파이프라인'사의 해킹 사태 이후 국가의 사이버보안 수준 강화를 위해 1건의 행정명령과 2건의 각서에 서명을 하였다. '콜로니얼 파이프라인'사 해킹사태는 '다크사이드'라는 해킹 조직의 랜섬웨어 공격으로 송유관업체 '콜로니얼 파이프라인'사의 송유관 8,850킬로미터 구간이 폐쇄되었으며, 이에 따라 기름 사재기 등이 발생하는 등 미국 동남부 지역에 초유의 비상사태가 발생한 끝에 동 업체가 해킹조직에게 5백만불의 비용을 지불하고 송유관을 정상화시킨 사건이다. 이 사태는 미국의 바이든 행정부가 국가 사이보보안에 관심을 더 가지게 된 계기가 되었다.

이 사건으로 바이든은 「국가의 사이버 보안 향상에 관한 행정명령」(Executive Order on Improving the Nation's Cybersecurity, '21.5.12)에 서명하였다. 이 행정명령의 주요 내용은 ▲민·관 간의 사이버 위협 정보 공유에 장애가 되는 것을 제거 ▲연방정부내에 현대적이고 더 강한 사이버보안 표준 마련 ▲소프트웨어 공급망 보안 개선 ▲'사이버 안전 점검 위원회'(Cyber Safety Review Board)를 설치 ▲보안 취약점 및 사고에 대한 대응 매뉴얼 마련 ▲사이버보안 점검 및 대응 역량 강화 등이다.

바이든은 「주요기반시설 제어 시스템 사이버보안 개선에 관한 국가 보안 각서」(National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, '21.7.28.)에도 서명하였는데, 이 각서는 국토안보부의 CISA(Cyber Security & Infrastructure Security Agency) 및 상무부의

NIST(National Institute of Standards and Technology)가 다른 기관과 협력해서 주요기반시설에 대한 사이버 보안 성능 목표를 개발하도록 지시하는 내용을 담고 있다.

이어서 서명한 「국가 보안, 국방부, 정보 당국 시스템의 사이버 보안 개선을 위한 국가 보안 각서」(National Security Memorandum to improve the cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, ’22.1.19)는 ▲상기 행정명령을 국가 보안 시스템에 적용하는 방안 마련 ▲이 시스템들에 발생하는 사이버사고의 가시성 개선 ▲시스템 운영 기관들에 시스템을 사이버위협으로부터 보호하고 위협을 약화시키기 위한 활동 요구 ▲다양한 시스템간 정보를 공유할 수 있는 체계를 갖추도록 요구 등의 내용을 담고 있다.

이와 함께, 미국 정부는 IT업계[3]와의 파트너십을 강화하였으며 美 IT업계는 최소 35조원 규모의 사이버보안 분야 투자를 약속하기도 했다.(‘21.8.25)

미국의 이러한 움직임은 미국이 그동안 기업·기관 자율에 맡기던 사이버보안 정책 기조에서 벗어나 정보 공유 등을 보다 강력하게 강제하는 방향으로 정책을 수정하고 있다는 것을 보여준다. 미국은 사이버보안을 민간이나 관이 단독으로 성취할 수 없다는 점을 지속 강조하고 있으며, 이에 대해 민간도 화답하는 추세를 보이고 있다.

3. 사이버보험 정책 현황

이상으로 사이버사고에 대한 국가 차원의 대응 전략 차원의 정

3) ADP, 알파벳, 아마존, 애플, IBM, 마이크로소프트 등

책들을 살펴보았다. 이와 함께 비교적 최근부터 사이버사고에 의한 피해를 더 빠르게 구제하고 원상태로 복원시키기 위해 사이버보험 활성화 정책이 추진되어 왔다.

3.1. 해외 동향

전세계적으로 사이버위험이 증가하면서 국내외 사이버보험 시장 규모는 증가해 왔다. 사이버범죄로 인한 경제 손실규모는 2014년에 연간 4,450억 달러로 전세계 GDP의 0.8%에 이른다는 연구가 있었으며, 이에 따라 사이버보험 시장 규모는 2016년 기준 약 35억 달러 수준이라는 연구가 있었다.(PwC, 2015)

사이버보험은 미국과 영국을 중심으로 활성화 추세를 보이고 있는데, 미국은 개인정보침해사고 처벌이 강한만큼 전세계에서 사이버보험 확산이 가장 빠르게 진행되고 있다. 다양한 연구 보고서에 따르면 미국 기업의 사이버보험 가입률은 20~30%에 이르는 것으로 나타나며, 2017년 기준 미국 내 사이버보험 시장 규모는 연간 40억 달러로 추산된다. 미국은 사이버보험 활성화를 위해 2012년부터 오바마정부에서 '행정명령 13636'에 따라 국토안보부가 이해관계자 포럼을 운영하고 정책연구 등을 추진하고 있다.

영국의 경우 사이버보험 시장 규모는 2014년 2,000만~2,500만 파운드(약 296억원~369억원)에 이르는 것으로 추정된다(Marsh). 영국은 미국에 비해 사이버보험의 활성화 수준이 낮으나 사이버보험을 금융 산업을 이끌 새로운 분야로 인식하고 관련 가이드라인을 마련하는 등 집중 육성하기 시작했다.

그 외에 국제기구에서도 관련 움직임이 있는데, OECD는 2016년에 사이버보험 활성화르 위한 비공식 전문가 그룹을 구성하였으며, ISO도 관련 논의를 진행한 바 있다. 국제기구는 사이버보험을 중소기업 보안 수준 제고를 위한 현실적 대안으로 인식하고 있다.

3.2. 국내 현황

국내에서는 아직 사이버보험 가입률은 낮은데, 정보보호 실태조사에 따르면 2018년 사이버보험 가입률은 0.3%에서 2020년 0.4%로 아직 미미한 수준에 머물고 있다.

다만 2018년『정보통신망법』개정을 통해 정보통신서비스 제공자를 대상으로 사이버보험이 일부 의무화되면서 관련 시장이 조금씩 발달하고 있다.

2018년 도입된 정보통신서비스 제공자 대상 사이버보험 의무화 정책은 일정 수준 이상의 고객 개인정보를 보유하고 있으며, 전년도 매출액 5천만원 이상일 것 등 의무 부과 대상에 일정한 제한을 두고 있다. 또한, 기업이 이러한 조건에 해당이 되더라도 반드시 사이버보험에만 가입해야하는 것이 아니라 기업 내부에 관련 준비금을 적립하는 등의 방식으로도 의무를 이행할 수 있기 때문에 이 정책에 의한 사이버보험 가입률 증가에는 아직 한계가 있다. 하지만, 장기적으로 사이버보험 시장이 발달하게 되면 기업이 내부에 기금 형태로 준비금을 적립하는 방식보다 사이버보험 상품이 기업에게 주는 효익이 더 크게 될 것이며, 따라서 점차 사이버보험 가입률이 증가하고 관련 상품의 보장률이 개선되는 등 시장에 선순환 작용이 일어날 것이라 생각된다.

이 연구는 다양한 사이버보안 정책 중, 비교적 최근에 도입되었으며 기존의 단순 사고 대응 방식이나 기반 구축 성격에서 벗어나 복원력 강화라는 새로운 차원의 정책으로 대두되고 있는 사이버보험 정책에 관심을 두고 분석을 진행한다. 사이버보험은 기업들의 요구사항을 수용하여 보안 투자를 이끌어낼 수 있는 새로운 수단으로 생각되는 바 장려될 필요가 있으나, 충분히 준비되지 않으면 보험 상품의 특성상 모럴 해저드 등 역기능 발생이 가능하기 때문에 신중한 접근이 필요하다.

Ⅲ. 사이버보험 역기능 분석

1. 문헌 연구

그동안 사이버보험이 네트워크 보안[4]을 개선하는지에 대하여 다양한 연구가 있었다. 이 연구들은 모두 이론적 분석이며, 결과를 종합하면 다음과 같다. 사이버보험의 효과는 사이버보험 시장이 처한 환경에 따라 달라진다. 사이버보험 시장이 독점적인 경우 보험은 기업의 보안 투자를 유도할 수 있으나, 시장이 경쟁적인 경우 보험은 기업의 보안 투자를 유도할 수 없다.

사이버보험은 당초 적절한 가격 전략을 통해 기업들의 사이버보안 투자를 이끌어 낼 수 있을 것으로 생각되었다. Kesan et al. (2004)은 보험사와 기업이 효용을 극대화하기 위해 행동한다는 가정하에 사이버보험이 기업들의 보안 투자를 증가시킨다는 것을 이론적으로 증명하였다. 이 연구는 보험사가 기업의 보안 투자 수준을 정확히 파악할 수 있다는 가정하에 이루어졌다.

그런데, 이후의 연구들에서는 경우에 따라 사이버보험이 기업의 보안 투자를 유도하지 못한다는 결과가 나타났다. Shetty et al. (2010)은 경쟁적인 시장에서 사이버보험이 기업들의 보안 수준에 어떤 영향을 미치는지 이론적으로 연구하였다. 이 연구는 정보 비대칭성의 유무에 따라 두 가지 상황을 분석하였다. 첫 번째로 보험사가 기업의 보안 수준을 확인할 수 없는 정보 비대칭성이 존재할 때를 분석하였는데, 이 때에는 보험 시장이 성립하지 못하였다. 두 번째로 보험사가 기업의 사이버보안 수준을 완전히 관찰할 수 있는 상황, 즉 도덕적 해이가 없는 환경을 가정하였는데, 이 상황에서도

4) 이 연구에서 '네트워크 보안'은 사회 전체의 네트워크의 사이버보안을 의미한다. 이 네트워크는 각 기업 등 네트워크 가입자들이 개별적으로 영향을 미칠 수 있으므로, '네트워크 보안'은 기업들의 평균적인 사이버보안 수준에 영향을 받는다.

보험은 이것이 없는 상황에 비해 보안 수준을 악화시켰다. 사이버보험이 위험 회피적인 가입자의 효용을 높일 수는 있어도 보안 수준을 높이는 인센티브로서는 역할을 하지 못했다.

Martinelli et al. (2018) 또한 경쟁적 시장에서 사이버보험이 기업의 보안 투자를 낮춘다는 것을 이론적으로 보였다. 하지만, 이 연구는 비경쟁적 시장에서는 적절한 가격 전략이 있다면 기업의 사이버보안 투자가 최소한 사이버보험이 없을 때에 비해 더 적어지지는 않도록 보장하는 것이 가능하다는 것을 밝혔다.

Khalili et al. (2018)은 독점적 시장에서 사이버보험의 영향을 이론적으로 연구하였다. 이 연구는 최근 머신러닝 등 기술 발달로 보험사가 가입자를 사전에 충분히 검열할 수 있다고 보았다. 즉, 정보비대칭성이 해소될 수 있다고 가정하였다. 이 가정하에 이 연구는 독점적 시장에서 보험사가 적절한 가격 전략을 통해 보험사의 보안 투자를 유도할 수 있다는 것을 밝혀냈다.

이상의 연구들을 종합하면, 사이버보험이 각 조건에 따라 기업의 태도에 다양한 영향을 미칠 수 있다는 것을 추측할 수 있다. 하지만, 사이버보험이 실제 상황에서 이론들이 예측한 것과 같은 효과를 내는지는 아직 확인된 바가 없다. 특히, 현실에서 시장은 보통 완전히 경쟁적이거나 완전히 독점적이지 않으므로, 현재까지의 이론만으로 현실에서 어떤 효과가 나타날지 예측하는 것은 어렵다. 따라서, 기업들에 대한 설문조사 데이터를 바탕으로 사이버보험이 현실에서 어떤 효과를 더 강하게 나타내는지 확인해볼 필요가 있다.

2. 연구 설계

2.1. 연구 문제

이 연구는 사이버보험 의무화 정책이 기업의 사이버보안 투자를 증가시켰는지에 대하여 분석하였다.

2.2. 연구 방법

이 연구는 인과관계 추론을 위해 이중차분법(Difference in differences)을 이용하였다. 이중차분법은 처치집단과 통제집단의 특성이 동질적이라는 가정(평행 추세, parallel trend)이 성립할 경우 두 집단 간의 차이를 측정함으로써 어떤 사건과 그 효과 간의 인과적 관계를 밝히는 분석 방법이다.

한국에서는 2018년에『정보통신망법』개정을 통해 정보통신서비스 제공자에 대해 사이버보험이 일부 의무화되었다. 따라서 2018년을 전후하여 정보통신서비스 제공자의 사이버보안 투자 수준 변화를 대조군과 비교함으로써 사이버보험이 기업의 보안 수준에 미치는 영향을 파악할 수 있다. 처치 그룹인 정보통신서비스 제공자와 대조군인 기타 기업들간에 평행 추세 가정이 성립한다면 이중차분법은 이 연구 문제에서 인과관계를 올바르게 추론해낼 수 있을 것이다.

다만, 이 연구가 분석의 도구로 사용하고 있는 실태조사 데이터가 채택한 산업분류체계와 사이버보험 의무화 법이 정의하고 있는 법 적용 대상이 완전히 일치하지는 않기 때문에 분석에 일부 오류 가능성이 있으며, 이 오차 가능성에 대해서는 토의 부분에서 보다 자세히 다룬다.

2.3. 회귀식

$$y = \beta_0 + \beta_1 ICTcompanies_i + \beta_2 post2018_t$$
$$+ \beta_3 (ICTcompanies_i \times post2018_t)$$
$$+ size_{i,t} + Pdata_{i,t} + tech_{i,t} + accident_{i,t} + \epsilon_{i,t}$$

<변수 개요>

- y : 종속변수
- ICTcompanies : 정보통신업체
- post2018 : 정책시행(2018년) 이후를 나타내는 더미 변수
- size : 기업 규모(종업원 수 기준)
- Pdata : 고객의 개인정보 보유 수준
- tech : 신기술 이용 수준
- accident : 과거 사이버사고 경험 유무

2.4. 데이터

이 연구는 2016년부터 2020년까지의 한국 정보보호 실태조사 자료를 사용하였다. 이 실태조사는 한국인터넷진흥원 및 한국정보보

호산업협회가 한국 과학기술정보통신부의 지원하에 매년 실시하는 것으로, 2001년부터 조사가 시행되어왔으며 원데이터는 통계청을 통해 공개되고 있다.

< 정보보호 실태조사 내용 및 범위 >

ㅇ 정보보호 중요성 인식 현황

ㅇ 정보보호 정책 수립 및 정보보호 조직 구성 현황

ㅇ 임직원 대상 정보보호 교육 실시 현황

ㅇ 정보보호 예산 및 투자 현황

ㅇ 정보보호 제품 및 서비스 이용 현황

ㅇ 정보보호 관리 현황

ㅇ 침해사고 경험 여부 및 대응활동 현황

ㅇ 개인정보 수집 및 이용 현황

ㅇ 개인정보 침해사고 경험 여부 및 대응 현황

ㅇ 모바일, 무선랜, 클라우드 및 사물인터넷(IoT) 보안 현황

ㅇ 사이버(정보보호, 개인정보보호) 보험 이용 및 향후 계획 현황

ㅇ 주요서비스 정보보호 투자 계획 현황

출처: 2020 정보보호 실태조사 보고서

이 설문조사의 관측 단위는 기업이며, 평균적인 유효 응답 수는 매년 약 9,000개이다. 이 설문조사의 대상은 종사자 수 1명 이상이며 1대 이상의 네트워크에 연결된 컴퓨터를 보유한 사업체이다. 이 설문조사는 통계청의 '전국사업체조사'의 업종별, 규모별 사업체 수 및 분포와 정보화진흥원의 '정보화통계조사' 결과에서 파악된 네트워크 구축 비율을 이용하여 모집단을 구성하였으며, 조사를 위한 업종 분류는 OECD의 분류 권고안과 한국표준산업분류를 기준으로 13개 업종으로 구분하였다. 이 조사는 표본의 대표성을 확보하기 위해 표본 추출을 위해 다단계층화계통추출법을 사용하였다. 이 조사는 매년 유사한 규모로 실시 되었으나 기존 표본 기업을 추적관리하지 않고 매번 새로운 표본을 선정한 것으로 패널 데이터를 구성하지는 않는다.

다음 표 4는 이 연구에서 사용된 실태조사 데이터의 표본 수를 업종별로 나타낸 것이다. 처치그룹인 정보통신업은 매년 600~700여 개로, 총 3,200여개의 표본이 관측되었다. 통제그룹은 매년 약 8,100~8,800여개로 총 42,000여개의 표본이 관측되었다. 전체 표본의 수는 매년 약 9,000여 개이다.

표 5는 한국표준산업분류체계와 정보보호 실태조사의 업종 분류체계를 비교한 것이다. 실태조사에서는 한국표준산업분류체계에서 농업, 임업 및 어업과 광업을 농림수산업의 한 업종으로 통일하였고, 교육 서비스업, 보건업 및 사회복지 서비스업 등 5개 분류를 기타 서비스업으로 통합하여 한 업종의 표본 수가 다른 업종에 비해 지나치게 작아지지 않도록 하였다.

표 4 업종별 연도별 표본 수

업종		2016	2017	2018	2019	2020	계
처치그룹	정보통신업	711	693	613	621	628	3,266
통제그룹	농림수산업(광업 포함)	394	317	259	370	310	1,650
	제조업	1,242	1,123	1,117	1,178	1,178	5,838
	건설업	757	769	788	882	770	3,966
	도매 및 소매업	966	941	878	906	908	4,599
	운수 및 창고업	680	610	587	572	635	3,084
	숙박 및 음식점업	731	730	625	620	637	3,343
	금융 및 보험업	699	699	688	691	676	3,453
	부동산업	560	550	535	503	521	2,669
	전문, 과학 및 기술서비스업	765	745	773	730	753	3,766
	사업시설관리, 사업지원 및 임대서비스업	823	790	705	767	775	3,860
	협회 및 단체, 수리 및 기타 개인서비스업	605	608	510	471	485	2,679
	기타 서비스업	653	555	658	739	724	3,329
	소계	8875	8437	8123	8429	8372	42236
총계		9,586	9,130	8,736	9,050	9,000	45,502

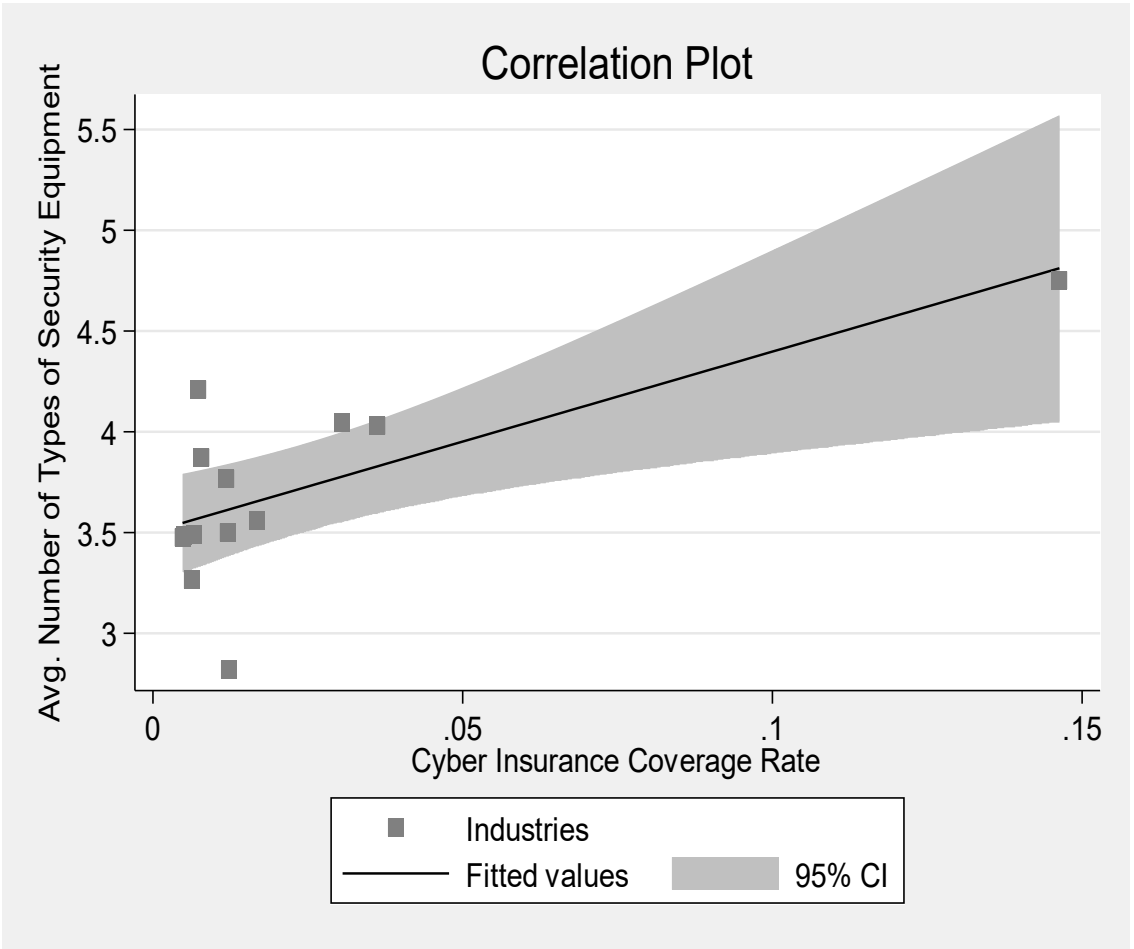
표 5 한국표준산업분류와 정보보호 실태조사의 업종 분류체계 비교

한국표준산업분류 (10차 개정)	업종 분류기준 (본조사)
A. 농업, 임업 및 어업	1. 농림수산업(광업포함)
B. 광업	
C. 제조업	2. 제조업
F. 건설업	3. 건설업
G. 도매 및 소매업	4. 도매 및 소매업
H. 운수 및 창고업	5. 운수 및 창고업
I. 숙박 및 음식점업	6. 숙박 및 음식점업
J. 정보통신업	7. 정보통신업
K. 금융 및 보험업	8. 금융 및 보험업
L. 부동산업	9. 부동산업
M. 전문, 과학 및 기술 서비스업	10. 전문, 과학 및 기술서비스업
N. 사업시설 관리, 사업 지원 및 임대 서비스업	11. 사업시설관리, 사업지원 및 임대 서비스업
S. 협회 및 단체, 수리 및 기타 개인서비스업	12. 협회 및 단체, 수리 및 기타 개인서비스업
D. 전기, 가스, 증기 및 공기 조절 공급업	13. 기타 (한국표준산업분류 중 좌변의 대분류에 해당하는 산업, 단 O는 제외)
E. 수도, 하수 및 폐기물 처리, 원료 재생업	
O. 공공 행정, 국방 및 사회보장 행정	
P. 교육 서비스업	
Q. 보건업 및 사회복지 서비스업	
R. 예술, 스포츠 및 여가관련 서비스업	

출처: 2020 정보보호 실태조사

그림 4는 업종 단위에서 사이버보험 가입률과 정보보호 수준 간의 상관관계를 보여주고 있다. 그림의 y축은 업종별 사용 중인 정보보호 제품의 종류의 수의 평균이고, x축은 업종별 사이버보험 가입률이다. y축 변수는 0에서 6까지의 값을 가질 수 있다. 이 그림이 보여주듯이, 업종 단위에서는 사이버보험 가입률이 높을수록 사용 중인 정보보호 제품 종류의 수, 즉 정보보호 준비 수준이 높아진다는 것을 알 수 있다.

그림 4 업종별 사이버보험 가입률과 정보보호 수준



2.5. 변수

종속변수

이 연구는 기업의 사이버보안 수준을 측정하기 위해 세 개의 종속변수를 사용하였다. 각각 기업이 사용중인 정보보호 장비의 종류의 수, 정보보호 제도 및 인프라, 아웃소싱 중인 정보보호 서비스의 종류의 수이다. 이 변수들이 측정된 방식은 다음과 같다.

종속변수 1 : 정보보호 장비의 종류의 수

이 변수는 정보보호 장비를 6개의 카테고리로 분류하여 각 기업이 얼마나 많은 종류의 장비를 사용하고 있는지 측정하였다. 각 카테고리는 1) 네트워크 보안(network security), 2) 시스템/단말 보안(terminal device security), 3) 콘텐츠/정보 유출 방지(content/information leakage prevention), 4) 인증(authentication security, such as account management, password, etc.), 5) 보안 관리(security management) 그리고 6) 기타이다. 분류 체계는 '정보보호 실태조사'가 이용하는 체계를 그대로 사용하였다. 각 카테고리별로 기업이 이에 속하는 장비를 하나라도 사용하고 있으면 1, 없으면 0의 값을 주고, 이 값들을 모두 더하여 이 변수의 최종 값을 얻는다. 카테고리가 총 6개이므로 이 변수의 값은 0~6의 범위를 갖는다.

기업이 사용하고 있는 정보보호[5] 장비의 양은 그 기업의 사이버보안 수준을 가늠할 수 있는 가장 직접적인 지표이다. 다양한 사이버보안 장비를 직접 갖추고 운용하는 기업은 그만큼 사이버보안 활

5) 이 연구에서는 '사이버보안'과 '정보보호'라는 용어를 특별히 구분하지 않고 혼용하고 있으며, 주로 '사이버보안'이라는 단어로 통일하여 사용하고 있다. 다만, '정보보호 실태조사'가 '정보보호'라는 용어를 사용하고 있기 때문에, 실태조사와 관련된 내용을 언급할 때는 이 연구에서도 '정보보호'라는 단어를 사용하고 있다.

동에 대한 이해도가 높고 많은 투자를 하고 있다는 것을 나타낸다. 사이버보안 장비는 종류와 가격이 다양하기 때문에 일반적으로 장비를 갖추고 운용하는데 적지 않은 예산이 필요하며, 장비를 많이 운용할수록 더 많은 사이버보안 인력을 고용할 필요가 있다. 따라서 이 연구에서는 기업이 사용하는 정보보호 장비의 양을 기업의 사이버보안 수준을 측정하기 위한 지표로 사용하였다.

이제 정보보호 장비의 양을 구체적으로 어떻게 측정할 것인가 하는 문제가 있는데, 이 연구는 기업이 사용하고 있는 정보보호 제품의 수를 단순히 합하는 대신 기업이 사용하고 있는 정보보호 장비의 종류를 기능별로 구분하고 기업이 해당 종류를 사용하고 있는지 카운트하는 방식으로 측정하였다. 이런 방식을 활용한 이유는 첫째, 이 방식이 조사가 용이한 만큼 조사된 데이터의 신뢰성이 높을 것으로 예상되고, 둘째, 정보보호 예산을 단순 비교하는것에 비해 얼마나 많은 보안 요소를 고려하고 있는지가 더 실질적인 사이버보안 수준을 나타낸다고 볼 수도 있기 때문이다. 예를들어 어떤 기업이 비싼 정보보호 장비 1세트를 구매하여 수년간 사용한다고 할 경우, 단순히 정보보호 예산을 조사한다면 구매한 당해연도에만 투자비용이 인식되고 이후 수년간은 투자가 없는 것으로 인식될 것이므로 기업의 보안 투자를 올바르게 조사하고 있다고 보기 어려울 것이다. 또한, 만약 정보보호 제품의 개수를 계산한다면 기업의 설문조사 담당자가 여러개의 장비가 모여서 이루어진 장비 1세트를 제품 1개로 응답하는 방식의 측정 오류가 발생할 가능성이 있다. 이에 반해, 사용하고 있는 정보보호 제품의 종류를 체크한다면 기업의 설문조사 담당자가 해당 기업이 보유한 정보보호 장비의 기능을 제대로 인식하고 있기만 하다면 측정 오류가 발생할 가능성이 적다.

그림 5 정보보호 장비의 종류의 수 평균

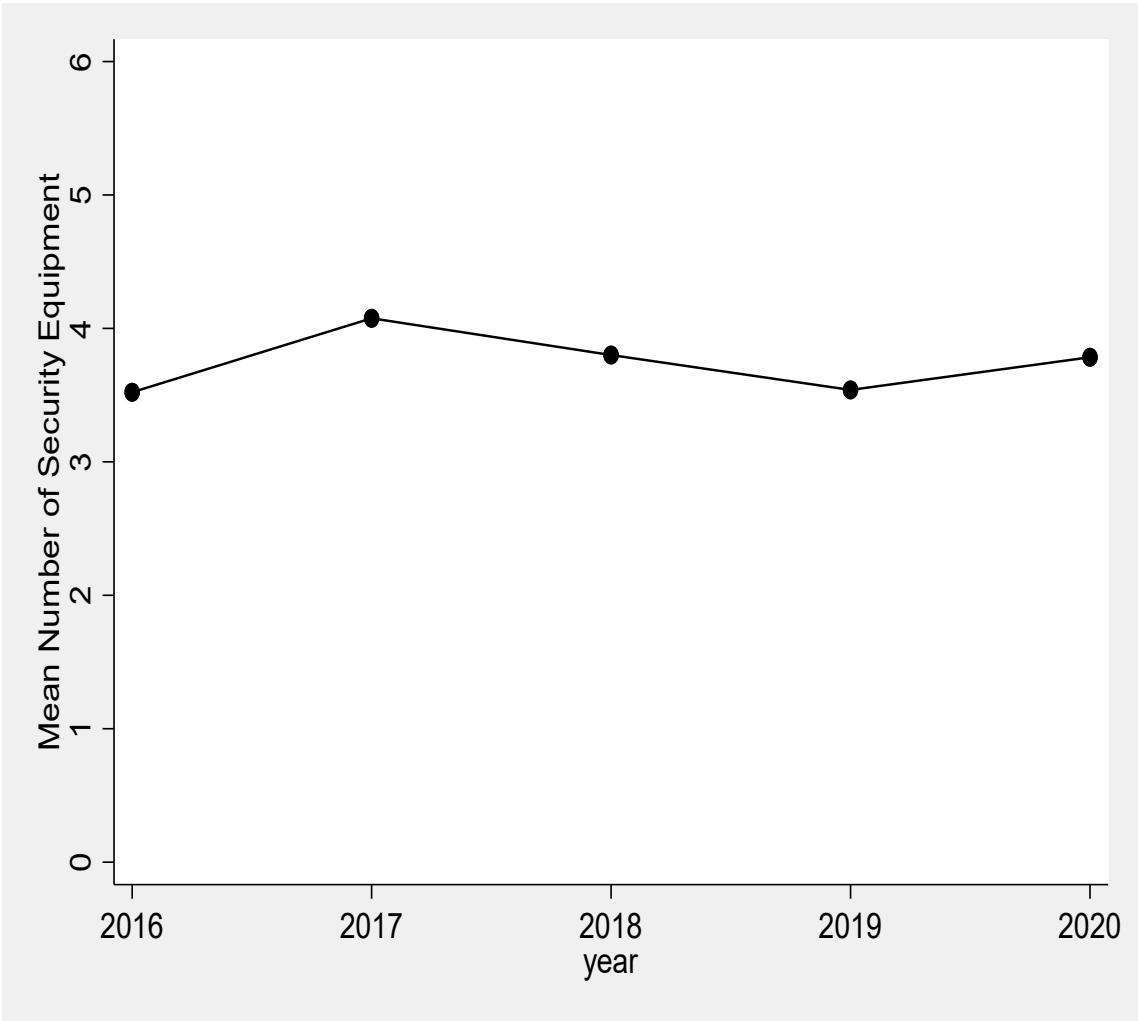
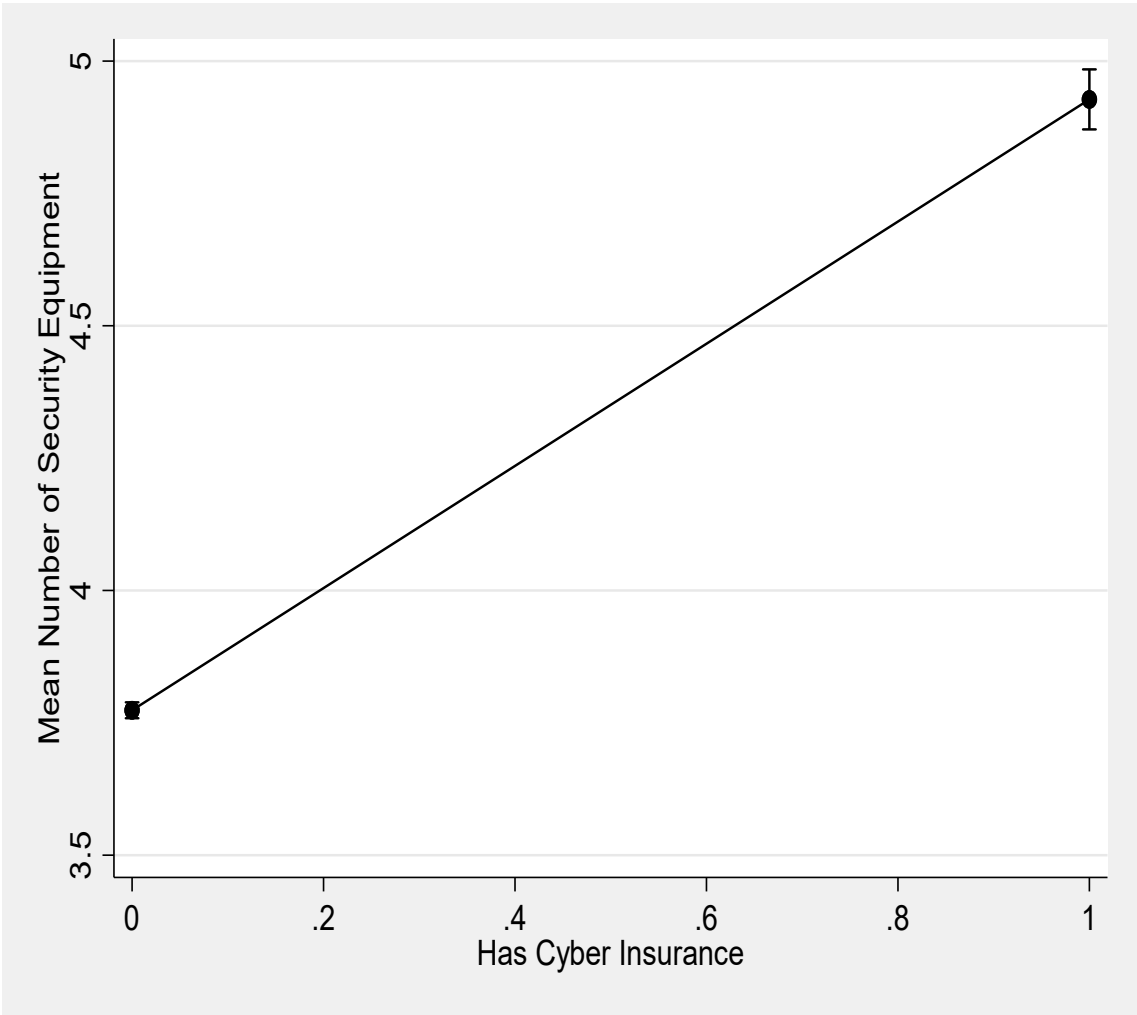


그림 6 사이버보험 가입과 정보보호 장비의 종류의 수 간 상관관계



종속변수 2 : 정보보호 제도 및 인프라

이 변수는 기업이 정보보호 제도 및 인프라와 관련하여 준비된 수준을 측정하였다. 구체적으로, 다음 4가지 항목 중 기업이 갖추고 있는 항목의 수를 측정하였다. 각 항목은 1) 정보보호 제도 수립 여부(whether each company establishes information protection policies), 2) 정보보호 전담 조직 운영 여부(operates a dedicated organization), 3) 정보보호 담당관 임명 여부(designates an information protection officer), 그리고 4) 고위급 및 실무자급 직원에 대한 정보보호 교육 시행 여부(educates executives and employees about information protection) 이다. 각 카테고리별로 기업이 제도 및 조직을 갖춘 경우 1, 아닌 경우 0의 값을 할당하고 이 값을 모두 더하여 변수의 값을 측정하였다. 카테고리가 총 4개이므로 이 변수의 값은 0~4의 범위를 갖는다.

기업의 사이버보안에 대한 투자는 반드시 제품 구매로만 이루어지지 않는다. 기업이 내부적으로 사이버보안 관련된 규율을 만들고 이를 실천하고 있는지, 종사자 구성원들에게 지속적으로 사이버보안 인식률을 높이기 위한 활동을 하고 있는지 등은 금액으로 환산하기는 어려우나 기업의 사이버보안 수준에 큰 영향을 미치는 요소이다. 이에 따라 기업의 사이버보안 관련 제도적 인프라에 해당하는 항목들을 일부 선택하여 하나의 지수로 만들었다.

'정보보호 실태조사'에서는 조사의 목적상 일반적인 '정보보호'와 '개인정보보호'를 구분[6]하고 있으며, 이에 따라 '정책' 혹은 '전담조

6) 정보보호 실태조사는 '정보보호'를 '정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 조치'라고 설명하고 있으며, '개인정보보호'는 '개인정보 침해 문제 방지를 위한 종합적 접근 및 대책을 위한 관리적· 기술적 수단 또는 그러한 수단으로 이루어지는 조치'라고 설명하고 있다. (출처: 2020 정보보호 실태조사 기업부문 조사표)

직’ 등에 있어서 일반적인 ‘정보보호 정책’과 ‘개인정보보호 정책’, ‘정보보호 전담조직’과 ‘개인정보보호 전담조직’ 등을 구분하여 조사하였다. 이 실태조사에서 개인정보보호와 관련된 항목들은 일반 정보보호와 구분되는 좀 더 구체적인 활동들을 인식하고 있는데, 이 연구에서는 ‘정보보호’와 ‘개인정보보호’를 구분할 특별한 실익이 없으므로 이 두 가지를 하나로 통합하여 인식하였다. 따라서, 일반 ‘정보보호’와 ‘개인정보보호’ 중 하나라도 해당되는 경우에는 1로, 둘 모두 해당되지 않는 경우에는 0으로 수치를 할당하였다. 예를들어, 어떤 기업이 정보보호 정책과 개인정보보호 정책 중 하나를 수립하고 있는 경우 수치 1을 할당하고, 둘 모두 수립하고 있지 아니할 때는 0을 할당하였다. 특히, 정보보호 정책과 개인정보보호 정책을 모두 수립하고 있는 경우에도 수치는 1만 할당하였다. 즉, 두 가지 정책을 세부적으로 구분하여 수립하고 있는 경우에도 사이버보안 수준이 특별히 더 높다고 인식하지 않았다. 왜냐하면 첫째, 대부분의 경우 기업들이 정보보호 관련 사항을 구비하고 있을 때에는 개인정보보호와 관련된 사항을 갖추고 있었으며, 둘째, 기업이 하나의 정책 속에 정보보호 및 개인정보보호에 관련된 내용을 모두 포괄하고 있는 경우에도 기업측의 설문조사 담당자가 착오로 한가지 정책만을 수립하고 있다는 등의 오류를 범할 가능성이 우려되기 때문이다. 즉, 일반 정보보호와 개인정보보호를 구분할 경우의 이익보다 측정오류가 포함됨으로 인한 손해가 더 클 것으로 우려되어 해당 항목을 단순화시켰다.

그림 7 정보보호 제도 수준 평균

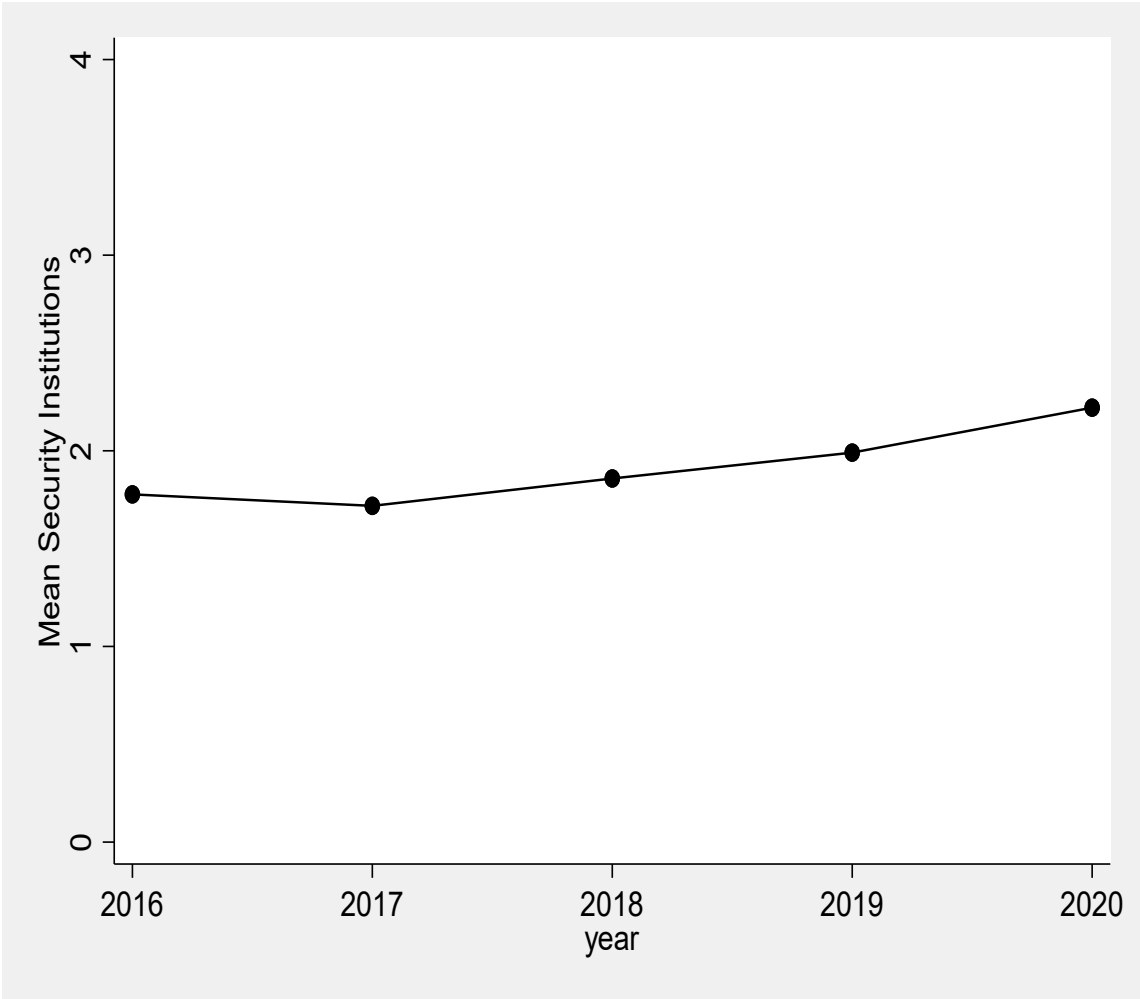
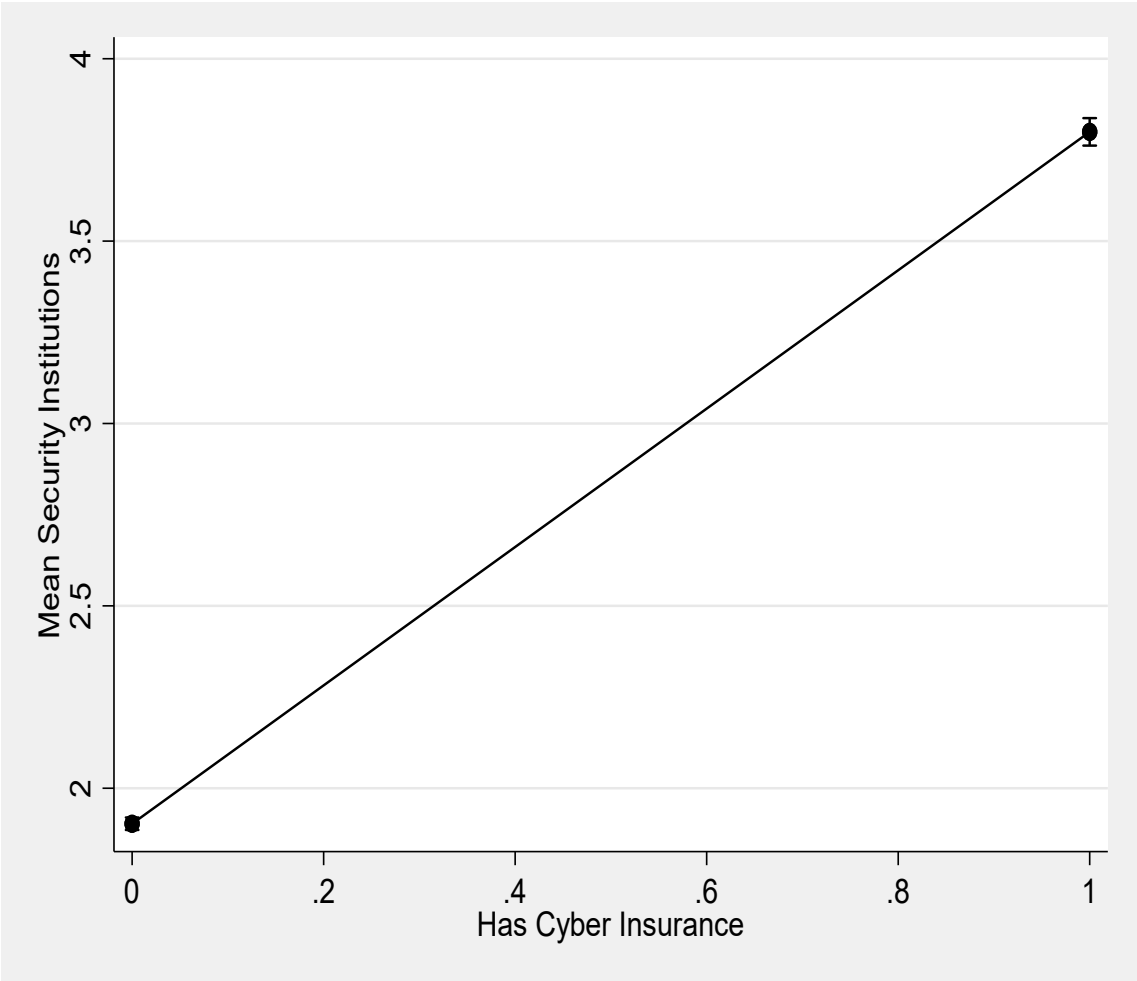


그림 8 보험 가입 여부와 정보보호 제도 수준 간 상관관계



종속변수 3 : 아웃소싱 중인 정보보호 서비스의 종류의 수

이 변수는 기업이 아웃소싱 할 수 있는 정보보호 서비스를 5개의 카테고리로 분류하고, 각 기업이 얼마나 많은 종류를 아웃소싱하고 있는지 측정하였다. 5개의 항목은 보안 컨설팅, 유지관리/보안성 지속 서비스, 보안 관제 서비스, 교육/훈련, 그리고 인증서 서비스이다. 다른 두 종속변수와 마찬가지로 기업이 각 카테고리별로 하나라도 해당되는 아웃소싱 서비스를 이용하고 있다면 1, 없다면 0의 값을 할당하고 이 값을 모두 더하여 변수의 값을 측정하였다. 총 5개의 카테고리가 있으므로 이 변수의 값은 0~5의 범위를 갖는다.

아웃소싱 중인 정보보호 서비스란, 정보보호 관련 제품이나 인력을 기업이 직접 구매하거나 고용하지 않고 정보보호 관련 업무 일체를 외부에 맡기는 것을 의미한다. 정보보호 업무가 일반적인 IT 업무에 비해 더 높은 전문성을 요하기 때문에 작은 기업일수록 직접 보안 업무를 수행하기 어려운 측면이 있으며, 이들에게는 서비스를 구매하는 것이 더 효과적일 수 있다. 정보보호 서비스를 이용하는 비율도 작지 않기 때문에(2020년 69.5%, 2019년 대비 42.5% 증가), 정보보호 제품을 직접 설치·이용하는 것과 별도로 서비스 구매를 기업의 사이버보안 투자를 가늠하는 지표로 활용하였다.

이 항목도 첫 번째 종속변수인 '정보보호 장비의 종류의 수'와 마찬가지로 아웃소싱 서비스의 유형을 기능별로 나누고, 기업이 얼마나 많은 유형의 서비스를 이용하고 있는지 카운트하여 지수화하였다.

그림 9 아웃소싱 서비스의 종류의 수 평균

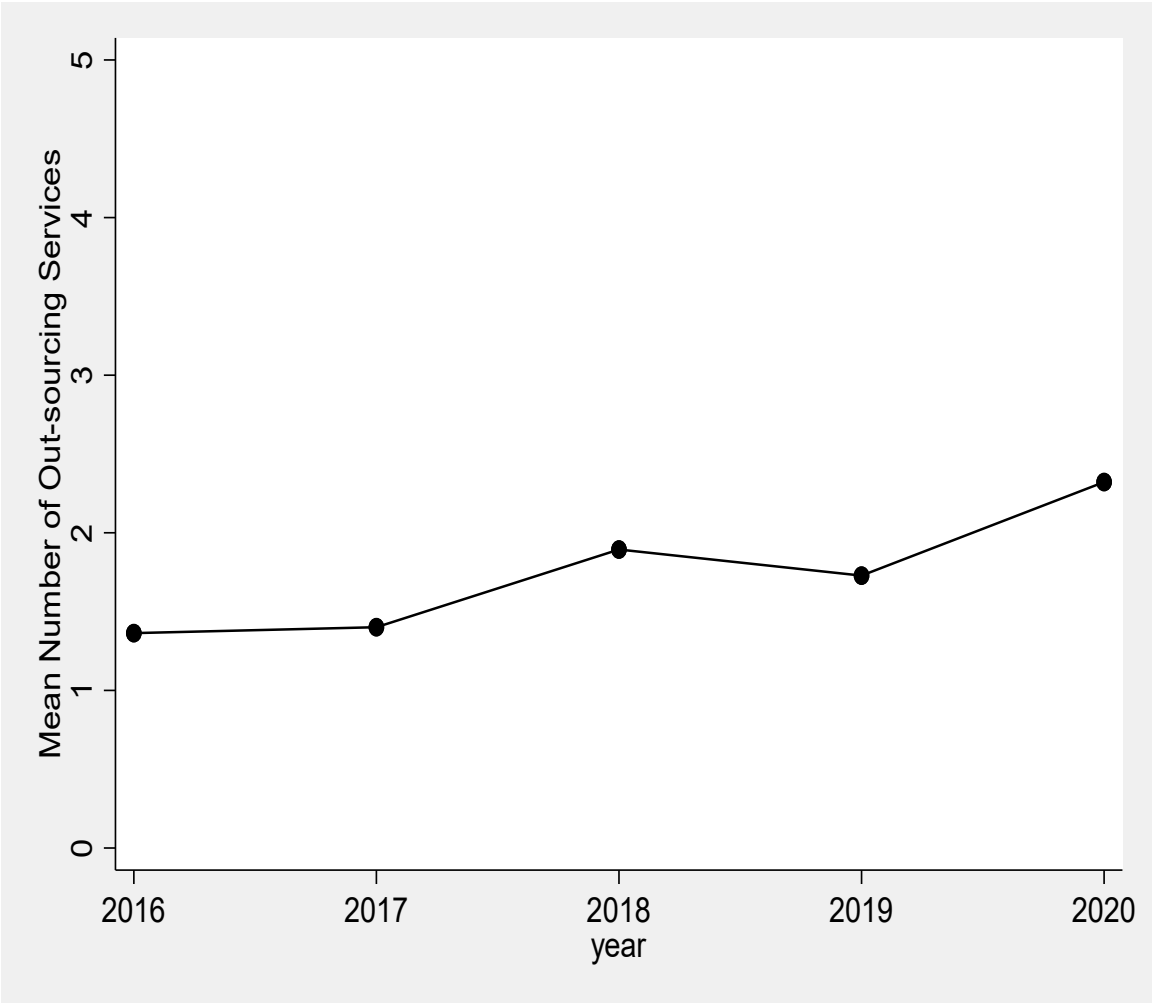
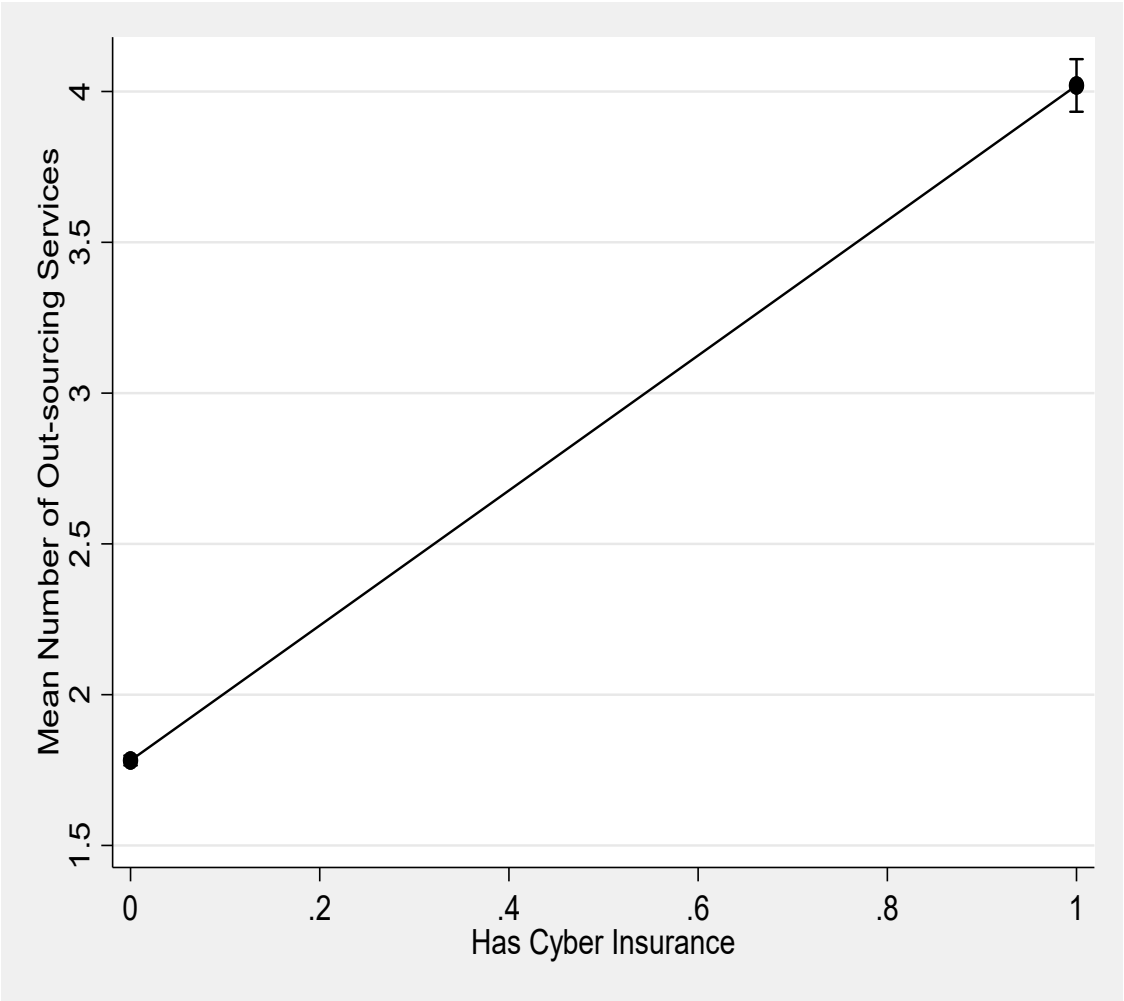


그림 10 이웃소싱과 보험가입여부와의 상관관계



처치그룹

이 연구에서 처치그룹은 정보통신기업이다. 이 분류는 정보보호 실태조사의 분류체계를 그대로 활용한 것이며, 정보보호 실태조사는 한국산업분류체계를 토대로 일부 수정한 업종 분류체계를 사용하고 있다. 이 정보통신기업 분류가 사이버보험 가입 의무 대상인 정보통신서비스 제공자와 범위가 완전히 일치하지는 않으나, 실태조사가 제공하는 업종 중 내용상 가장 유사한 그룹이기 때문에 이 업종을 처치그룹으로 채택하였다.

사이버보험은 2018년『정보통신망법』개정을 통해 정보통신서비스 제공자를 대상으로 의무화되었으며, 지금은 관련 법 조문이『개인정보보호법』으로 이관되어 현재는『개인정보보호법』을 통해 정보통신서비스 제공자가 관련 의무를 부과받고 있다(개인정보보호법 제39조의 9, 손해배상의 보장).

표 6 사이버보험 의무 가입 관련 법 조문

법령	조문
개인정보보호법	제39조의9(손해배상의 보장) ① 정보통신서비스 제공자등은 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다. ② 제1항에 따른 가입 대상 개인정보처리자의 범위, 기준 등에 필요한 사항은 대통령령으로 정한다.

개인정보보호법 시행령	제48조의7(손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등) ① 다음 각 호의 요건을 모두 갖춘 정보통신서비스 제공자등(이하 이 조에서 “가입 대상 개인정보처리자”라 한다)은 법 제39조의9제1항에 따라 보험 또는 공제에 가입하거나 준비금을 적립해야 한다. 1. 전년도(법인의 경우에는 전 사업연도를 말한다)의 매출액이 5천만원 이상일 것 2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 1천명 이상일 것 ② 가입 대상 개인정보처리자가 보험 또는 공제에 가입하거나 준비금을 적립할 경우 최저가입금액(준비금을 적립하는 경우 최소적립금액을 말한다. 이하 이 조에서 같다)의 기준은 별표 1의4와 같다. 다만, 가입 대상 개인정보처리자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우에는 보험 또는 공제 가입금액과 준비금 적립금액을 합산한 금액이 별표 1의4에서 정한 최저가입금액의 기준 이상이어야 한다. ③ 가입 대상 개인정보처리자가 다른 법률에 따라 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하

	거나 준비금을 적립한 경우에는 법 제39조의9 제1항에 따른 보험 또는 공제에 가입하거나 준비금을 적립한 것으로 본다.

이 법에서 말하는 '정보통신서비스 제공자'는 『정보통신망법』에서 정의하고 있는데, 이는 전기통신사업법에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. 여기서 전기통신사업자는 전기통신사업법에 따라 신고를 하고 전기통신역무(전기통신설비를 이용하여 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말함)를 제공하는 자를 말한다.

정보통신서비스 제공자는 관련 법이 다양한 조문을 통해 복잡하게 정의하고 있어, 실제로 어떤 기업이 정보통신서비스 제공자에 해당하는지 여부는 각 기업별로 영업의 내용 및 형태를 살펴 판단해야 한다. 다만, 일반적으로 KT와 같은 기간통신 기업과 NHN 등의 포털 기업은 당연히 정보통신서비스 제공자에 해당되며, 일반적으로 홈페이지를 사용하여 고객과 소통하는 사업체들은 대부분 정보통신서비스 제공자에 해당된다고 본다.

한편, 정보보호 실태조사에서 말하는 '정보통신업'은 한국표준산업분류체계에서 그 내용을 차용한 것으로, 정보 및 문화 상품을 생산하거나 공급하는 산업활동 등을 말한다. 한국표준산업분류체계에서 정보통신업의 하위 분류로는 출판업, 영상·오디오 기록물 제작 및 배급업, 방송업, 우편 및 통신업, 컴퓨터 프로그래밍, 시스템 통합 및 관리업, 정보서비스업 등이 있다.

표 7 정보통신업과 정보통신서비스 제공자 정의 비교

구분	정의
한국표준산업분류상 정보통신업	1. 개요 정보 및 문화 상품을 생산하거나 공급하는 산업활동; 정보 및 문화상품을 전송하거나 공급하는 수단을 제공하는 산업활동; 통신 서비스 활동; 정보 기술, 자료 처리 및 기타 정보 서비스를 제공하는 산업활동을 말한다. 여기에는 출판, 소프트웨어 제작.개발.공급, 영상 및 오디오 기록물 제작.배급, 라디오 및 텔레비전 방송, 방송용 프로그램 공급, 전기 통신, 정보 기술 및 기타 정보 서비스 활동 등을 포함한다. 가. 출판업 학습 서적, 만화, 소설 및 수필집 등의 일반 서적과 신문, 주간지, 월간지, 연보 등의 정기 간행물 등을 발간하거나 소프트웨어를 출판하는 산업활동을 말한다. 출판물은 자사에서 직접 창작되거나 다른 사람에 의하여 제작된 창작물을 구입 또는 계약에 의하여 출판할 수도 있다. 나. 영상.오디오 기록물 제작 및 배급업 영화 및 방송 프로그램을 제작, 배급 및 상영하거나 영화 제작과 관련된 필름 가공, 더빙 등의 제작 후 서비스를 제공하는 산업활동과 음반 등 오디오 기록물의 원판 및 출판활동을 말한다.

	다. 방송업 라디오 및 텔레비전 등의 방송 프로그램을 지상파, 유선 및 위성 등의 각종 전송 방식에 의하여 송출하는 산업활동을 말한다. 라. 통신업 유선, 무선 및 기타 전자적 방법에 의하여 음성, 자료, 문자, 영상 등의 각종 정보를 송.수신하거나 전달하는 통신 서비스를 제공하는 산업활동을 말한다. 마. 컴퓨터 프로그래밍, 시스템 통합 및 관리업 컴퓨터 시스템을 통합 구축하는 산업활동과 컴퓨터 시스템의 관리 및 운영관련 기술 서비스를 주로 제공하는 산업활동을 말한다. 바. 정보 서비스업 정보 처리, 호스팅 서비스 및 온라인 정보 제공 서비스를 제공하는 산업활동을 포함한다. 뉴스 제공 등의 기타 정보 서비스를 제공하는 활동도 포함한다. 2. 타산업과 관계 가. 출판권 없이 각종 서적이나 정기 간행물을 인쇄하는 산업활동 “1811” 나. 소프트웨어 및 오디오 기록물을 복제하는

	산업활동 “1820” 다. 온라인 방법을 통하여 특정한 산업활동을 수행하는 경우는 해당 산업의 특성에 따라 분류 - 온라인 증권 중개(66121), 온라인 부동산 중개(68221), 온라인 인력 알선(75110) 등
사이버보험 의무 가입 대상	ㅇ 정보통신서비스 제공자 중 개인정보보호법이 정하는 기준을 충족하는 자 ㅇ 정보통신서비스 제공자: 정보통신망법 제2조(정의) “정보통신서비스 제공자”란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. ㅇ「전기통신사업법」 제2조제8호에 따른 전기통신사업자: “전기통신사업자”란 이 법에 따라 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무를 제공하는 자를 말한다. ㅇ 전기통신역무: “전기통신역무”란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다. ㅇ 개인정보보호법상 사이버보험 의무 가입 대상자: 제39조의9(손해배상의 보장) ① 정보

	통신서비스 제공자등은 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다. ② 제1항에 따른 가입 대상 개인정보처리자의 범위, 기준 등에 필요한 사항은 대통령령으로 정한다. ㅇ 개인정보보호법 시행령: 제48조의7(손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등) ① 다음 각 호의 요건을 모두 갖춘 정보통신서비스 제공자등(이하 이 조에서 “가입 대상 개인정보처리자”라 한다)은 법 제39조의9제1항에 따라 보험 또는 공제에 가입하거나 준비금을 적립해야 한다. 1. 전년도(법인의 경우에는 전 사업연도를 말한다)의 매출액이 5천만원 이상일 것 2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 1천명 이상일 것

표 8 사례별 정보통신서비스 제공자 해당 여부

구분	정보통신서비스 제공자 해당 여부
상법상의 상인 및 회사	•상법상의 상인 및 회사는 영리를 목적으로 사업을 영위 •따라서, 회사 등은 구체적 영리행위가 없더라도 영리목적으로 서비스를 제공하므로 기본적으로 정보통신서비스 제공자에 해당
비영리법인	•비영리법인이 학술, 종교, 자선, 기예, 사교 등 영리 아닌 사업을 목적으로 정보통신서비스를 제공하는경우에는 정보통신서비스 제공자에 해당되지 않음 - 다만, 비영리법인이라 하더라도 수익사업을 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당 ▶ 법인세법 시행령 제3조는 비영리내국법인에 적용되는 수익사업의 범위를 규정
특수법인	•농협, 한국마사회 등 특수법인이 법률상 목적 중 비영리사업을 위해 정보통신서비스를 제공하는 경우정보통신서비스 제공자에 해당하지 않음 - 다만, 특수법인이 목적사업으로 수행하는 영리사업을 위해 정보통신서비스를 제공하는 경우에는

	정보통신서비스 제공자에 해당 ▶ 농협이 유통업을 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당
공공기관	•공공기관은 공기업, 준정부기관, 기타 공공기관으로 구분 - 공기업은 기본적으로 영리를 목적으로 사업을 영위하므로 해당 사업을 목적으로 서비스를 제공하는경우에는 정보통신서비스 제공자에 해당 - 준정부기관은 정부 업무의 수탁 수행 또는 기금관리 업무를 수행하므로 기본적으로 정보통신서비스 제공자에 해당하지 않음 - 기타 공공기관은 개별적으로 “영리 목적의 정보통신서비스 제공 여부”를 판단하여 정보통신서비스 제공자 여부를 판단하며, - 연구개발목적기관으로 분류된 경우 정보통신서비스 제공자에 해당하지 않는 것으로 판단 ▶ 정보통신서비스를 제공하는 공영홈쇼핑은 정보통신서비스 제공자에 해당(기타 공공기관) ※ 정보통신서비스 제공자 여부와 관계없이 방송사업자는 정보통신망법 제4장(개인정보의 보호)이 준용됨 ▶ 한국과학기술연구원은 정보통신서비스 제공자

	에 해당하지 않음(기타 공공기관)
병원 등 의료기관	•의료기관이 제공하는 의료업의 경우 실비보전 수준 이상의 수입이 발생하고 있다면 영리행위로 볼 수있으므로, - 의료기관의 의료업을 위해 정보통신서비스를 제공하는 경우에는 정보통신서비스 제공자에 해당
학교	•학교는 교육 실시기관으로 교육은 비영리 목적에 해당하므로 정보통신서비스 제공자에 해당하지 않음 - 다만, 사립학교가 상행위 등 영리 목적으로 정보통신서비스를 제공하는 경우에는 정보통신서비스 제공자에 해당
금융회사	•금융회사는 영리목적의 금융업을 영위하는 자이므로 기본적으로 정보통신서비스 제공자에 해당 - 다만, 정보보호 최고책임자에 관한 규정 등에 있어서 정보통신망법은 일반법, 「전자금융거래법」은 특별법으로 볼 수 있으므로, 「전자금융거래법」의 적용을 받는 정보통신서비스 제공자인 금융회사 등은「전자금융거래법」을 우선 적용

출처: 정보보호 최고책임자 지정·신고 안내서, 한국인터넷진흥원(2019.12)

이상의 용어 정의에서 알 수 있듯이, 정보보호 실태조사에서 구분하고 있는 정보통신업종과『정보통신망법』이 규정하고 있는 정보통신서비스 제공자는 서로 다를 수 있다. 간단히 예를 들어 생각해보면, SK텔레콤이나 다음 포털 사업자의 경우에는 정보통신서비스 제공자에 속함과 동시에 정보통신업에 속할 것이다. 하지만 예를 들어 현대자동차는 정보통신업에는 속하지 않지만 홈페이지를 운영하여 영리활동을 펼치고 있으므로 정보통신서비스 제공자에는 속할 수 있을 것이다.

이와 같은 차이에도 불구하고 이 연구는 실태조사의 정보통신업을 처치그룹으로 정했는데, 이는 첫째, 이보다 더 나은 분류방법이 없으며, 둘째, 정보통신업에 속하며 이 실태조사에 응답한 기업들은 대부분 정보통신서비스 제공자에 속할 가능성이 높으므로 처치그룹과 통제그룹 중 최소한 처치그룹 내에 비 정책대상이 포함될 가능성을 가장 낮출 수 있는 방법이기 때문이다.

이와 같은 이유로 이 연구에서는 정보보호 실태조사의 '정보통신업'을 사이버보험 의무화 정책의 적용을 받은 '처치그룹'으로 설정하여 분석을 진행하였다. 처치그룹의 샘플 수는 연도별로 약 600~700개이다.

통제그룹

이 연구에서 통제그룹은 정보보호 실태조사에서 정보통신업을 제외한 나머지 모든 기업이다. 통제그룹의 샘플 수는 연도별로 약 8,400개 내외이다.

정책 시행 더미 변수

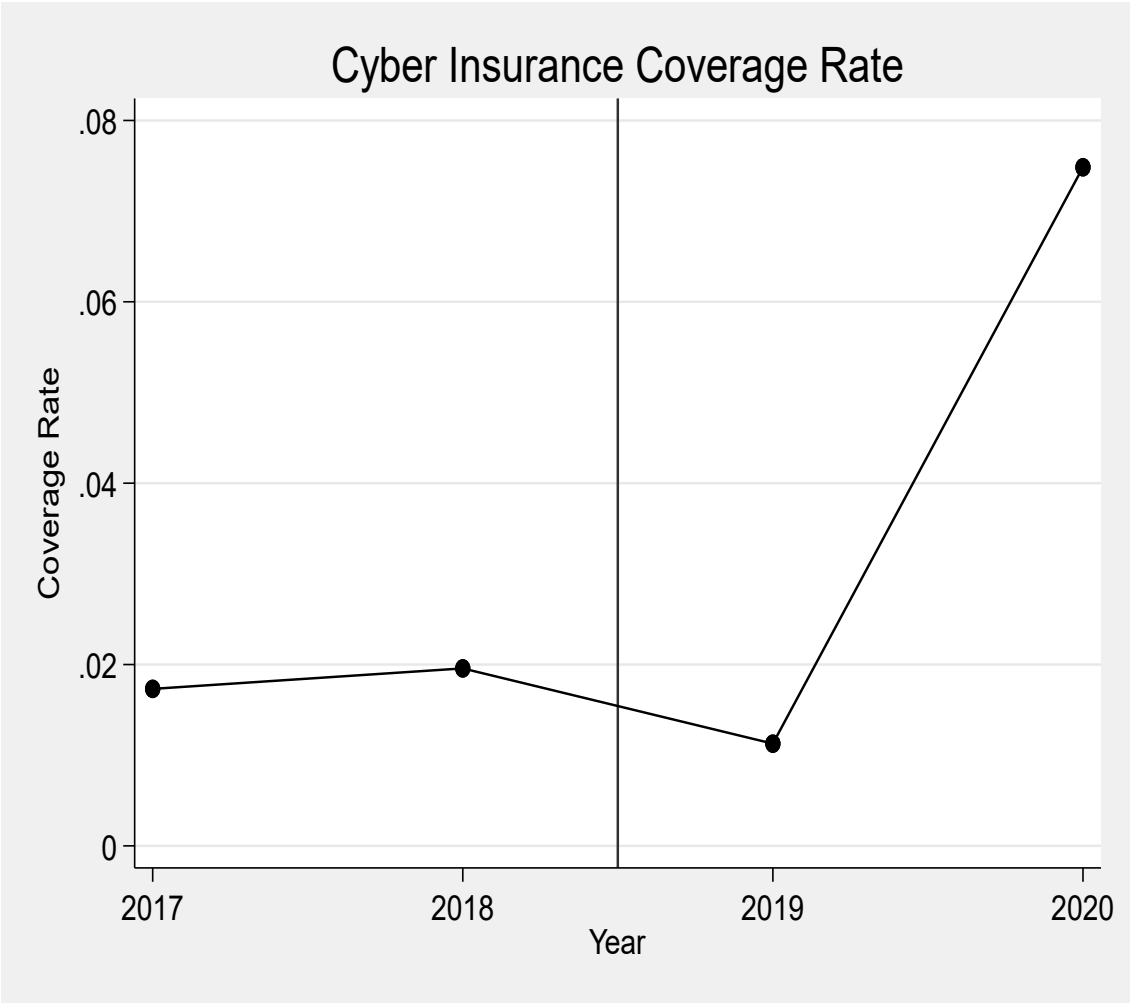
사이버보험 의무화 관련 법은 2018년에 개정되어 2019년에 발효되었다. 이에 따라 2016년부터 2018년까지를 정책 시행 이전으로 보고, 2019년과 2020년을 정책 시행 이후로 보았다.

법이 개정된 해인 2018년을 정책 시행 이전으로 볼 것인지, 이후로 볼 것인지, 혹은 분석에서 제외할 것인지에 대해 판단이 필요한데, 이 연구에서는 2018년을 정책 시행 이전으로 분류하여 분석을 진행하였다. 법의 발효 시점이 2019년이더라도 법 개정만으로 기업들의 태도 변화를 이끌어냈다면 법 개정 시점인 2018년을 정책 시행 이후 기간에 포함시켜야 할 것인데, 이 사안에서는 오히려 개정된 법이 법 적용 대상 범위 획정을 시행령으로 위임하였고, 이 시행령이 마련되는데 상당한 시간이 걸렸으며, 시행령이 마련된 이후에도 행정부가 한동안 처벌을 하지 않고 계도기간을 가짐으로써 기업들이 법 개정시 바로 태도를 바꾸기 어려웠다. 특히, 법이 발효되는 시점에 이르러서도 관련 사이버보험 상품이 부족하다는 의견도 있었기 때문에 결과적으로 기업들이 법 개정시 자신들이 의무부과 대상인지 명확하지 않았고 부과 대상이라고 할지라도 사이버보험에 가입하지 않고 보험 상품이 더 출시되기를 기다리는 등 관망세를 유지했을 가능성이 높다. 실제로 그림 11의 보험 가입율 그래프를 보면 정보통신기업들의 사이버보험 가입율은 2020년에 이르러서야 분명한 상승세를 보이고 있다.

통제변수

통제변수로는 정보보호 실태조사가 제공하는 데이터 중 기업의 사이버보안 준비 수준에 영향을 미칠 수 있는 요인들을 설정하였다. 이 연구에서 설정한 통제변수는 총 4개로, 기업의 규모(종업원 수 기준), 고객의 개인정보 보유 수준, 정보통신 기술을 업무에 활용하는 수준, 그리고 지난 1년간 사이버사고 경험 유무이다.

그림 11 정보통신기업의 보험 가입율 그래프



통제변수 1 : 기업 규모

기업 규모는 기업이 사이버보안 활동에 투자하는 규모에 큰 영향을 차지하는 변수이다. 이 연구가 선택한 종속변수는 투입한 예산 규모 등의 수치적인 성격이 아니라 얼마나 다양한 활동이나 장비를 구비하고 있는지 기능적인 부분을 보기 때문에 기업의 매출액이나 운영비용 등에 직접적인 영향을 받는 것은 아니다. 하지만 기업에 더 많은 인력이 종사하는 등 규모가 커질수록 사이버보안 분야에 투입할 수 있는 인력이 증가하고, 이에 따라 사이버보안 정책 수립이나 더 다양한 장비 구입·운용 등 다양한 활동이 가능해질 수 있다. 따라서 정확한 인과관계 분석을 위해 기업 규모는 통제되어야 한다.

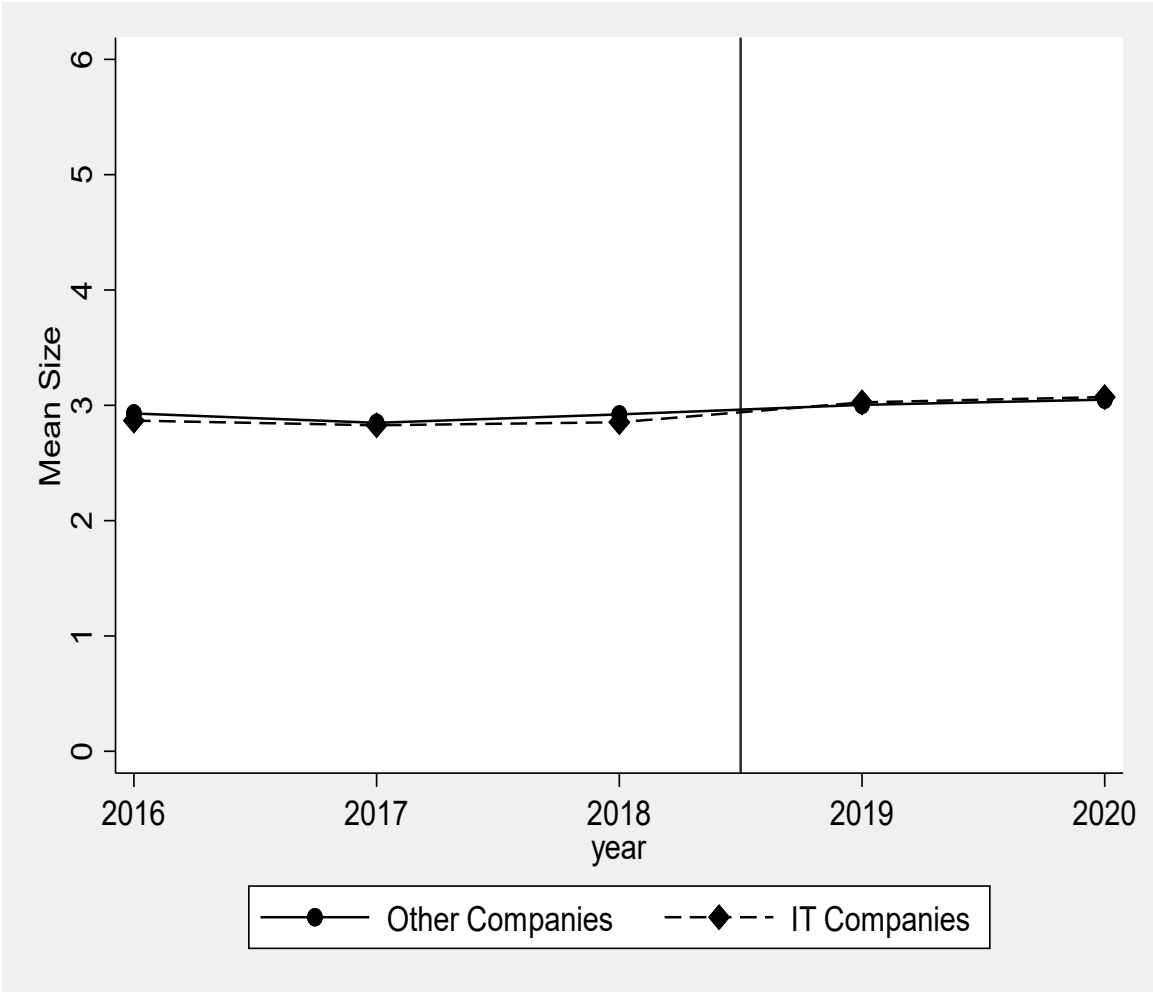
이 연구에서 통제변수 '기업 규모'는 정보보호 실태조사가 제공하는 종업원 수 기준의 기업 규모를 사용하고 있다. 정보보호 실태조사는 종업원 수를 5단계로 구분하여 조사하였는데, 각 구간 구분은 다음 표와 같다.

표 9 정보보호 실태조사 업종 구분 기준 및 해당 사업체 수

구분	업종/규모	사업체 수	컴퓨터 보유/네트워크 구축 사업체 수
규모별	1~4명	3,272,417	928,270
	5~9명	489,710	313,650
	10~49명	280,615	230,135
	50~249명	43,235	38,104
	250명 이상	4674	4319
전체		4,090,651	1,514,478

※ 출처: 2018년 기준 전국사업체조사(통계청),
2019년 정보화통계조사(한국정보화진흥원)

그림 12 기업 규모 비교


Mean Size
0
1
2
3
4
5
6
2016
2017
2018
2019
2020
year
Other Companies
IT Companies

통제변수 2 : 개인정보 보유 수준

고객의 개인정보 보유 수준 또한 기업의 사이버보안에 대한 투자에 직접적인 영향을 미치는 요인이다. 사이버사고로 인한 피해는 크게 두 가지로 구분될 수 있다. 한 가지는 기업 자신에 대한 피해이고, 다른 한 가지는 제 3자에 대한 피해이다. 기업 자신에 대한 피해란, 사이버사고가 발생하면 정보통신 시스템이 제 기능을 못하게 되는 경우가 많은데 이때 이를 복구하는 복구비용과 이를 복구하는 기간 동안 영업을 하지 못하게 되면서 발생하는 영업손실이 있다.

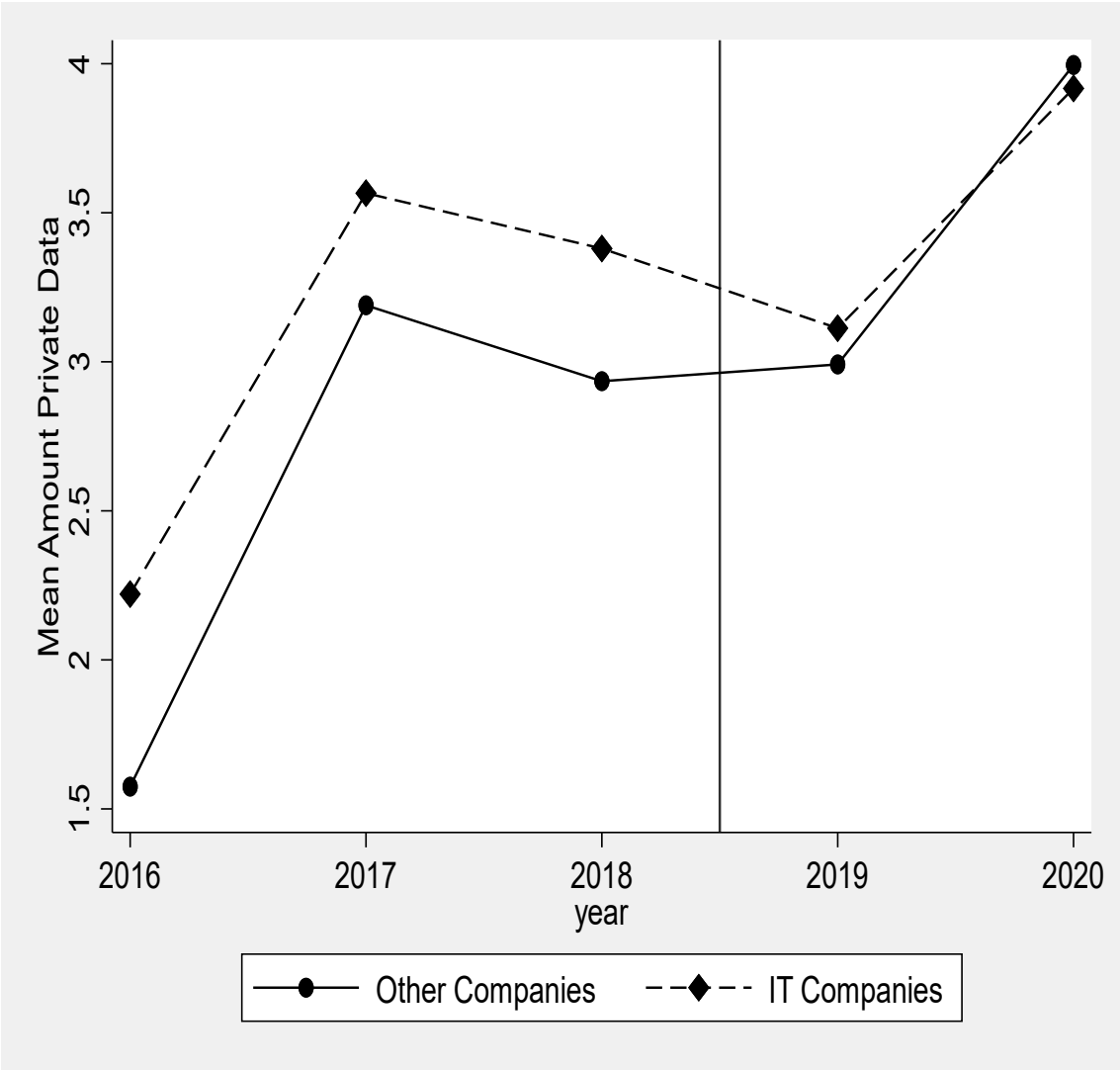
다른 한 편으로 제 3자에 대한 피해는 기업이 사이버사고로 보유하고 있던 고객의 개인정보가 유출되면서 발생하는 고객의 피해이다. 여기서 일반적으로 사이버사고에서 정말 문제가 되는 것은 제 3자에 대한 피해로, 유출된 개인정보의 양이 클수록 피해보상액은 한계가 없이 기하급수적으로 증가할 수 있으며, 피해사실을 고객에게 알리면서 기업이 사이버사고를 당했다는 사실이 대외적으로 공개되기 때문에 기업 이미지가 훼손되는 부수적인 피해도 함께 발생하게 된다. 특히 많은 경우 고객들과 기업이 유출된 개인정보에 대한 보상의 적정 규모를 서로 다르게 인식하기 때문에 긴 법정 공방을 벌이게 되므로 직·간접적인 피해 규모는 매우 커지게 된다. 따라서 고객의 개인정보를 많이 보유한 기업은 사이버보안에 특별히 더 신경을 쓸 수밖에 없고, 따라서 이 변수는 통제되어야 한다.

기업의 개인정보 보유 수준은 보유하고 있는 개인정보에 포함된 고객의 수와 개인정보의 다양성, 민감성 등으로 판단할 수 있을 것이다. 하지만 개인정보를 보유하고 있는 고객의 수는 기업이 설문조사시에 공개하기 어려운 측면이 있기 때문에 이 연구에서는 기업이 보유하고 있는 개인정보의 유형을 파악하여 더 많은 유형을 가지고 있을수록 높은 점수를 할당하는 방식으로 개인정보 보유 수준으르 지수화하였다.

표 10 정보보호 실태조사, 개인정보 보유 유형 조사표

개인정보 유형		수집/이용여부	
		예	아니오
일반 정보	1) 성명	①	②
	2) 주민등록번호	①	②
	3) (집 또는 회사) 주소	①	②
	4) (집 또는 회사) 전화번호 등 연락처	①	②
	5) 휴대전화 번호	①	②
	6) 이메일 주소	①	②
	7) 회원ID 및 비밀번호	①	②
	8) 계좌번호	①	②
	9) 신용카드 번호	①	②
	10) 생년월일	①	②
특화 정보	11) 가족정보(가족이름, 출생지, 생년월일 등)	①	②
	12) 신용정보(대부잔액, 지불상황, 저당, 지불연기 및 미납의 수 등)	①	②
	13) 고용정보(현재 고용주, 회사주소, 상급자이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록 등)	①	②
	14) 통신정보(전자우편, 전화 통화내용, 로그파일 등)	①	②
	15) 소득정보(월수입, 소유주택, 자동차 등 재산 관련 정보)	①	②
	16) 의료정보(과거 의료기록, 가족병력, 의약이력 등)	①	②
	17) 위치정보(GPS나 휴대폰에 의한 개인의 위치정보)	①	②
	18) 기타(적을것 : _____)	①	

그림 13 개인정보 보유 수준 비교



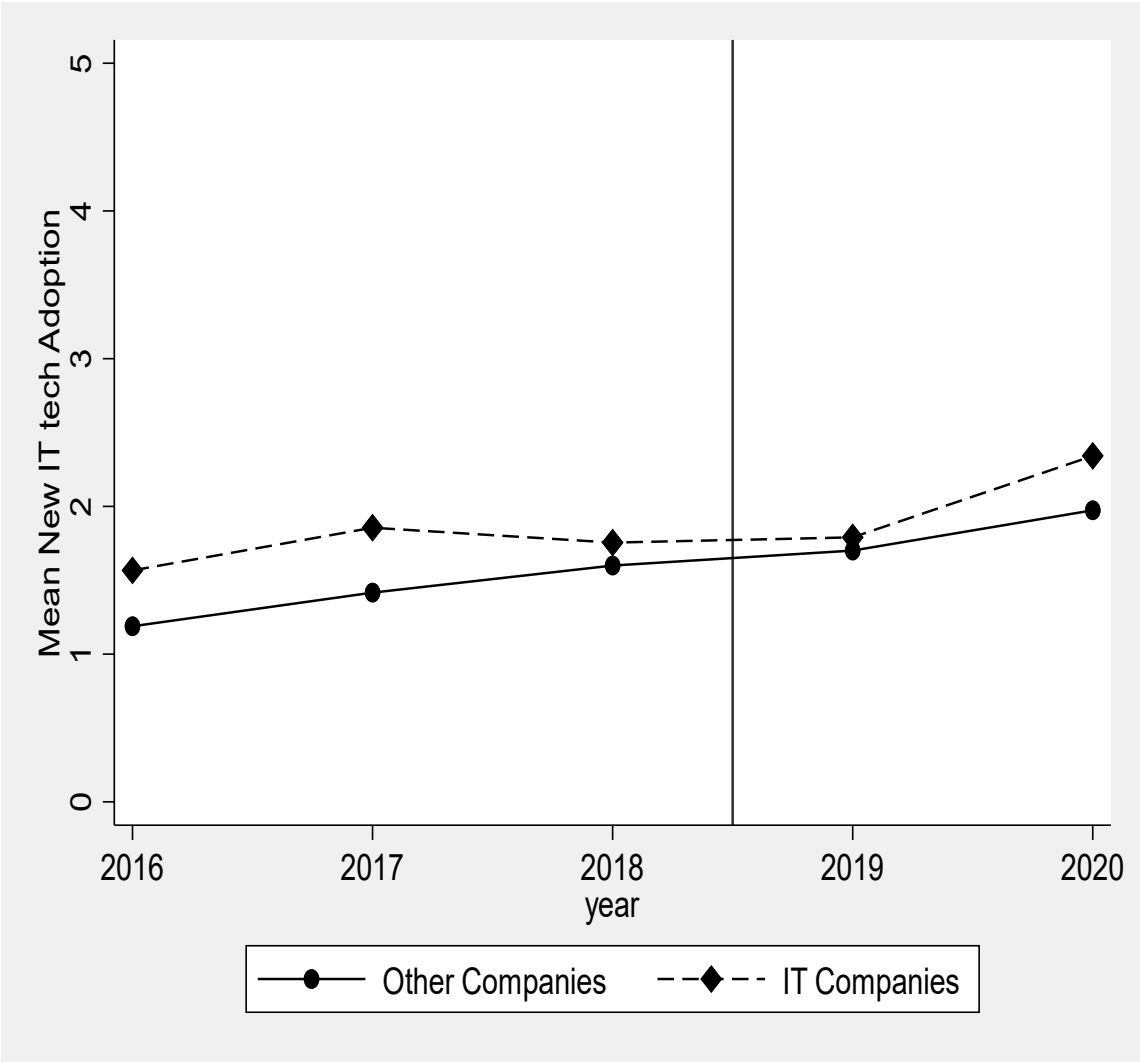
위 표 10은 정보보호 실태조사에서 기업이 수집하는 개인정보의 유형을 나열한 것이다. 이 연구에서는 기업이 아래 표에서 '예'를 선택한 수를 카운트한 값을 개인정보 보유 수준 변수의 값으로 사용하였다. 이 실태조사가 조사하는 개인정보의 유형이 총 18개이므로 이 통제변수 '개인정보 보유 수준'은 0에서 18까지의 범위를 갖는다.

통제변수 3 : 정보통신기술 업무 활용 수준

'정보통신 기술을 업무에 활용하는 수준' 또한 기업의 사이버보안에 대한 투자 활동에 영향을 미치는 요소로서 통제될 필요가 있다. 기업이 더 많은 정보통신 기술을 사용할수록 더 많은 취약점을 갖게 되고 더 많은 사이버위협에 노출되게 된다. 이에 따라 더 많은 정보통신 기술을 사용하는 기업일수록 자연스럽게 사이버보안 활동에 더 많은 관심을 기울이게 된다. 또한, 다양한 정보통신기술을 업무에 활용하고 있다는 것은 기업 구성원들의 정보통신기술에 대한 이해가 상대적으로 높다는 것을 의미하므로, 사이버보안에 대한 인식 수준도 더 높을 가능성이 있다. 따라서 이 부분 또한 통제되어야 한다.

이 연구에서 기업이 '정보통신 기술을 업무에 활용하는 수준'은 기업이 일반적인 유선 PC 네트워크를 이용하는 것 보다 진보된 형태의 정보통신 수단 유형을 정하고 해당 기업이 이 중 몇 가지를 업무에 활용하는지 카운트하는 방식으로 지수화하였다. 일반 유선 네트워크보다 진보된 형태의 정보통신 수단으로는 '무선랜', '모바일 기기', '클라우드', '사물인터넷' 등 4가지로 구성하였다. 기업이 이 중 1개를 이용할 때마다 이 변수의 값을 1씩 증가시키는 형태로 이 지수를 측정하였다. 총 4개의 항목이 있으므로, 이 변수는 0에서 4까지의 값을 가진다.

그림 14 정보통신기술 업무 활용 수준 비교



통제변수 4 : 사이버사고 경험 여부

마지막으로, 기업의 사이버사고 경험 유무를 통제변수로 활용하였다. 2020년 정보보호 실태조사 결과 기업의 약 2.0%는 지난 1년간 사이버사고를 경험한 것으로 나타났다. 사이버사고를 경험한 기업은 자연스럽게 향후 같은 일이 반복되지 않도록 사이버보안 조치를 강화할 것으로 기대된다. 따라서 회귀분석시 사이버사고 경험 여부를 통제하였다.

이 변수에서 사이버사고 경험 유무를 파악할 때 기준은 지난 1년간으로 설정하였다. 오래된 경험일수록 현재 기업의 태도에 미치는 영향이 낮아질 것이므로 과거의 경험을 적당한 수준에서 필터링할 필요가 있고, 실태조사 데이터가 지난 1년간의 경험에 대해 제공하고 있기 때문에 이와 같은 기준을 차용하였다.

다음 그림 15의 그래프는 각 그룹별로 사이버사고 경험률을 비교한 것이다. 집단간 경험률 차이가 거의 없다.

표 11은 지금까지 서술한 변수들의 기본적인 기술통계를 나타낸 것이다. 이 표는 각 집단별/연도별로 변수의 평균값과 표준편차를 보여주고 있다.

그림 15 기업의 사이버사고 경험률

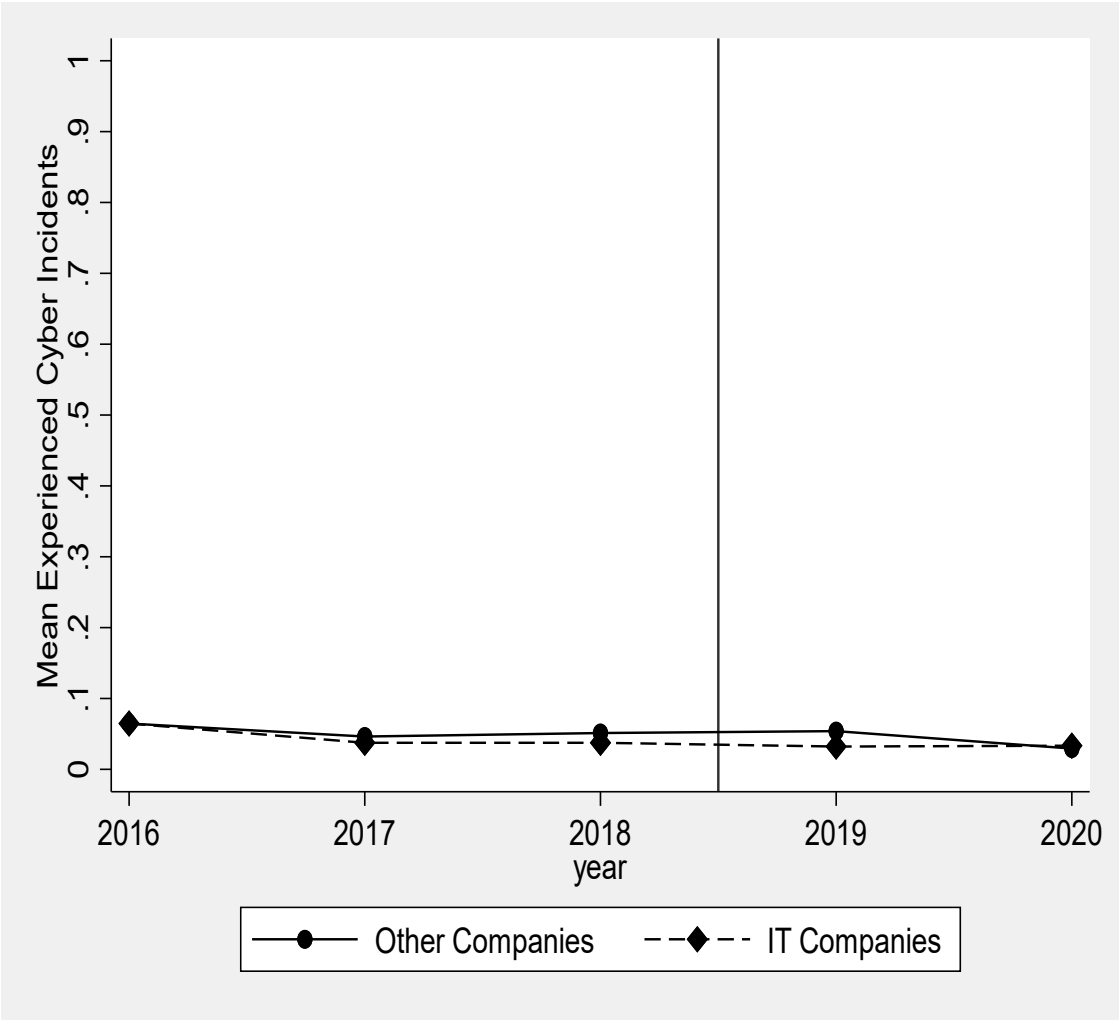


표 11 주요변수 기술통계

	연도		2016	2017	2018	2019	2020	전체
통제그룹	표본 수		8,875	8,437	8,123	8,429	8,372	42,236
	정보보호 장비의 종류의 수	평균	3.49	4.04	3.77	3.53	3.78	3.72
		표준편차	1.66	1.68	1.36	1.34	1.32	1.50
	정보보호 제도 수준	평균	1.72	1.66	1.82	1.94	2.17	1.86
		표준편차	1.78	1.62	1.58	1.65	1.67	1.67
	아웃소싱 서비스의 종류의 수	평균	1.32	1.39	1.88	1.70	2.31	1.71
		표준편차	1.58	1.52	1.60	1.57	1.61	1.62
	기업 규모	평균	2.93	2.85	2.92	3.00	3.05	2.95
		표준편차	1.34	1.39	1.38	1.39	1.42	1.39
	고객정보 보유 수준	평균	1.57	3.19	2.93	2.99	4.00	2.92
		표준편차	3.23	3.76	3.57	3.73	3.54	3.65
	신IT기술 업무 활용 수준	평균	1.19	1.42	1.60	1.70	1.97	1.57
		표준편차	1.04	1.08	1.06	1.10	1.27	1.14
	사이버사고 경험율	평균	6.47%	4.63%	5.13%	5.40%	2.94%	4.93%
		표준편차	24.60%	21.02%	22.07%	22.60%	16.89%	21.65%
처치그룹	연도		2016	2017	2018	2019	2020	전체
	표본 수		711	693	613	621	628	3,266
	정보보호 장비의 종류의 수	평균	3.94	4.56	4.19	3.60	3.90	4.04
		표준편차	1.58	1.42	1.15	1.19	1.29	1.38
	정보보호 제도 수준	평균	2.48	2.46	2.41	2.63	2.88	2.57
		표준편차	1.72	1.63	1.52	1.51	1.41	1.58
	아웃소싱 서비스의 종류의 수	평균	1.90	1.50	2.12	2.09	2.46	2.00
		표준편차	1.81	1.46	1.66	1.48	1.63	1.65
	기업 규모	평균	2.87	2.83	2.85	3.03	3.07	2.93
		표준편차	1.25	1.41	1.41	1.39	1.46	1.38
	고객정보 보유 수준	평균	2.22	3.57	3.38	3.11	3.92	3.22
		표준편차	3.66	3.52	4.04	3.91	3.45	3.76
	신IT기술 업무 활용 수준	평균	1.57	1.86	1.76	1.79	2.34	1.86
		표준편차	1.20	1.32	1.08	1.21	1.33	1.26
	사이버사고 경험율	평균	6%	4%	4%	3%	3%	4%
		표준편차	25%	19%	19%	18%	18%	20%

3. 결과

이중차분법을 이용하여 사이버보험 의무화 정책이 기업들의 보안 투자에 미친 영향을 분석한 결과, 종속변수 중 '정보보호 제품의 종류의 수'는 통계적으로 유의미한 것으로 나타났으며, 처치그룹인 정보통신기업은 정책 시행 이후 정보보호 제품의 종류의 수를 줄인 것으로 나타났다. 표 12가 회귀분석 결과를 보여주고 있다.

구체적으로 살펴보면, 정보통신기업은 사이버보험 의무화 정책 시행 전에 비해 시행 후 이용하는 정보보호 제품의 종류의 수를 0.329만큼 줄였다. 정보통신기업이 사용하는 정보보호 제품의 종류의 수의 평균은 3.742로(최대값은 6), 0.329는 평균의 약 9%에 해당한다. 즉, 정보통신기업은 사이버보험 의무화에 따라 정보보호 제품 투자를 9% 줄인 것이다.

이 결과는 이론연구가 예측한 것과 유사한 방향성을 갖고 있다. 이론연구는 경쟁적인 시장 환경에서 사이버보험이 기업들의 보안 투자를 유인하지 못하고 기업들의 모럴 해저드를 막지 못해 사이버 보안 수준을 열화시킬 것이라고 보았다. 현재 한국의 사이버보험 시장은 초기상태로서 경쟁 수준을 판단하기 어렵지만, 이 연구 결과를 볼 때 보험사들이 가입자에 대해 가격차별을 통해 보안 투자를 유인할 수 있을 정도의 시장 지배력을 갖추지 못했을 것이므로 이론연구의 경쟁적 시장환경에 해당하는 효과가 나타난 것으로 보인다.

이 회귀분석 결과는 해석하기에 앞서 분석의 실효성을 판단해볼 필요가 있다. 먼저, 이중차분법이 사용되었으므로 처치집단과 통제집단 간에 평행 추세의 가정이 성립하는지 확인하는 것이 중요하다. 또한, 통제변수가 적절히 사용되었는지 확인하고 샘플이 처치그룹과 통제그룹에 적절히 할당되었는지도 검토하여 문제가 있다면 결과를 보완할 필요가 있다. 다음 토의 부분에서 이에 대하여 다룬다.

표 12 회귀분석 결과

	(1) Num of Types of Security Equipment	(2) Security Institutions	(3) Num of Types of Services Outsourcing
IT Companies × Post 2018	**-0.329***** **(0.0482)**	**0.0126** **(0.0445)**	**0.0207** **(0.0499)**
IT Companies	0.372*** (0.0299)	0.638*** (0.0276)	0.189*** (0.0310)
Post 2018	-0.326*** (0.0131)	0.0503*** (0.0121)	0.214*** (0.0136)
Size	0.332*** (0.00469)	0.630*** (0.00432)	0.361*** (0.00484)
Amount Private Data	0.102*** (0.00171)	0.140*** (0.00158)	0.144*** (0.00177)
New IT tech Adoption	0.182*** (0.00573)	0.141*** (0.00529)	0.197*** (0.00593)
Experienced Cyber Incidents	-0.123*** (0.0284)	-0.0720** (0.0262)	-0.0798** (0.0294)
Constant	2.292*** (0.0155)	-0.648*** (0.0143)	-0.159*** (0.0160)
Mean	3.742	1.911	1.735
S.D.	1.491	1.677	1.620
Observations	45502	45502	45502
Adjusted R^2	0.249	0.495	0.321

Standard errors in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

4. 토의

4.1. 평행 추세 가정(Parallel-Trend Assumption)

이 연구는 분석을 위해 이중차분법 모델을 사용하였으므로, 분석 결과가 의미를 가지기 위해서는 처치그룹과 통제그룹 간 평행 추세가 존재한다는 가정이 성립하여야 한다. 이에 따라 각 종속변수별로 평행 추세의 존재를 확인해보았다.

그림 16은 이 연구가 테스트한 종속변수들 중 유의미한 결과가 나온 '정보보호 제품의 종류의 수' 변수에 대해 처치그룹과 통제그룹 간 추세를 보여주고 있다. 평행 추세가 존재한다는 것을 육안으로도 확인할 수 있다. 하지만, 보다 정확한 분석을 위해 평행 추세를 회귀분석을 통해서도 검증해 보았다.

아래 표 13은 평행 추세가 있는지 회귀분석을 이용해 테스트한 결과이다. 분석 결과, 정책이 도입된 2018년을 기준으로 정책 변화 이전 기간에는 처치그룹과 통제그룹 간 평균 차이에 통계적으로 유의미한 변화가 없다. 즉, 처치그룹과 통제그룹이 같은 추세를 가지고 있다. 하지만, 2018년 이후에는 처치그룹과 통제그룹 간의 평균 차이가 기준인 2018년에 비해 통계적으로 유의미한 차이를 나타내고 있다. 즉, 정책 시행 이후에는 두 집단간 추세에 차이가 나타나고 있는 것이다.

이중차분법에서 가정하는 평행 추세는 우리가 관심을 가지는 특별한 이벤트가 발생하지 않았을 경우 처치그룹과 통제그룹이 우리가 관심을 가지는 분야에서 같은 특성을 가져야 한다는 것이다. 위 분석에서 이 연구의 처치그룹과 통제그룹은 정책 변화가 발생하기 전에 정보보호 장치의 종류의 수에 있어 같은 추세를 나타내고 있다. 따라서 이 종속변수는 처치그룹과 통제그룹 간 평해추세가 성립한다.

그림 16 그룹별 정보보호 장비의 종류의 수 평균

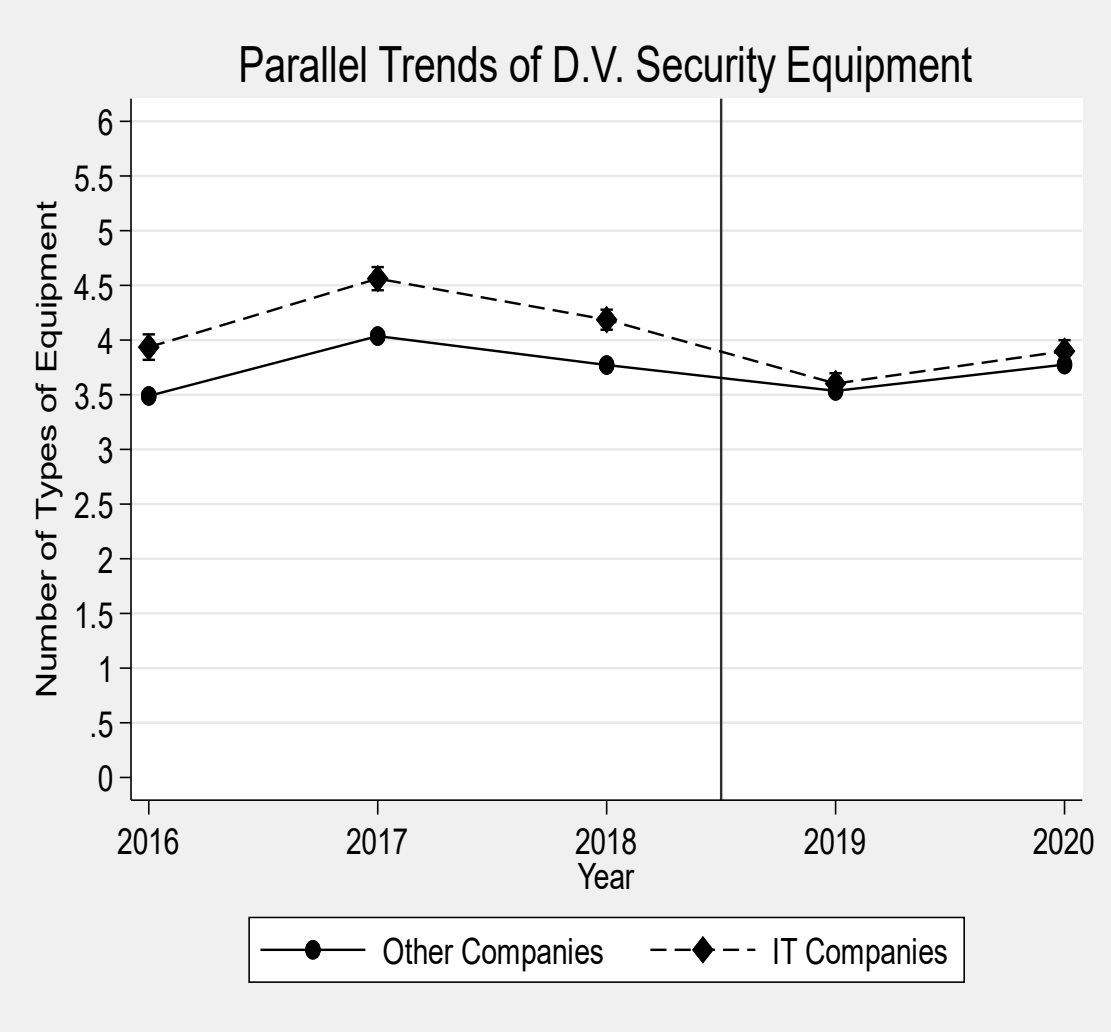


표 13 종속변수 1 평행 추세 테스트 결과

	(1) Num of Types of Security Equipment
IT Companies × year 2016	**-0.0273** **(0.0735)**
IT Companies × year 2017	**0.0520** **(0.0740)**
IT Companies × year 2019	**-0.335***** **(0.0758)**
IT Companies × year 2020	**-0.307***** **(0.0757)**
IT Companies	0.365*** (0.0538)
Years	Y
Controls	Y
Observations	45502
Adjusted R^2	0.257

NOTE: Baseline is the year 2018.
Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

그림 17 그룹별 정보보호 제도 수준

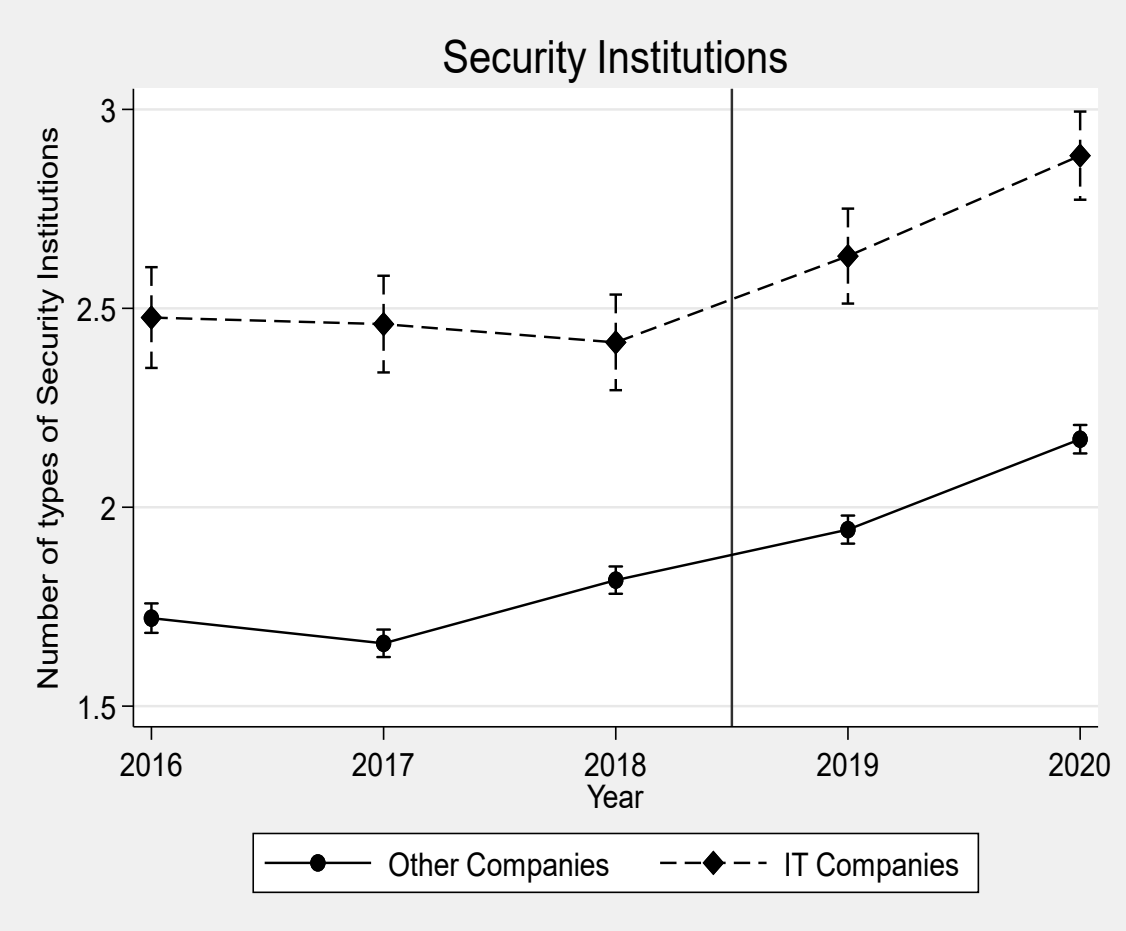


표 14 종속변수 2 평행 추세 테스트 결과

	(1) Security Institutions
IT Companies	0.552***
	(0.0498)
IT Companies # year=2016	0.0936
	(0.0680)
IT Companies # year=2017	0.144*
	(0.0684)
IT Companies # year=2019	0.0891
	(0.0701)
IT Companies # year=2020	0.104
	(0.0699)
Years	Y
Controls	Y
Observations	45502
Adjusted R^2	0.498

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

그림 18 그룹별 아웃소싱 서비스의 종류의 수

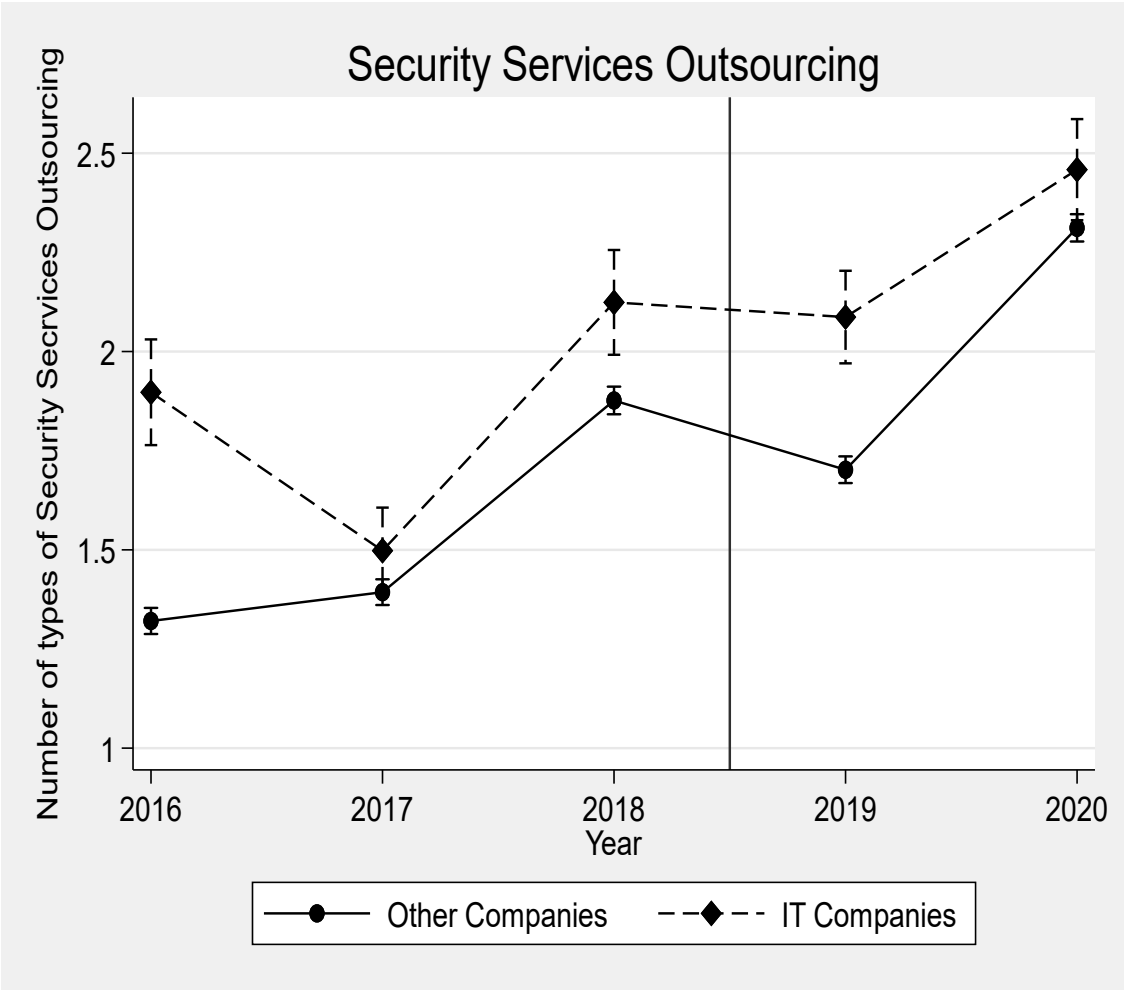


표 15 종속변수 3 평행 추세 테스트 결과

	(1)
	Security Services Outsourcing
IT Companies	0.180**
	(0.0553)
IT Companies # year=2016	0.259***
	(0.0756)
IT Companies # year=2017	-0.201**
	(0.0761)
IT Companies # year=2019	0.162*
	(0.0780)
IT Companies # year=2020	-0.0969
	(0.0778)
Years	Y
Controls	Y
Observations	45502
Adjusted R^2	0.335

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

위 그림 17, 18, 표 14, 15는 종속변수 2와 3을 테스트한 것이다. 그림과 표에서 모두 볼 수 있듯이 종속변수 2와 3은 두 집단간 평행 추세가 성립하지 않는다. 따라서 이 변수들은 이중차분법을 이용한 분석 결과를 신뢰할 수 없다.

4.2. 통제 변수의 유효성 확인

이 연구에서는 기업의 사이버보안 준비 태도에 영향을 미칠 개연성이 높은 기업의 특성을 선별하여 통제하였다. 이 통제변수는 각각 기업 규모(종업원 수 기준), 기업의 고객 프라이버시 데이터 보유 수준, 업무에 정보통신기술을 활용하는 수준, 그리고 지난 1년간 사이버사고 경험 유무 등이다.

그런데, 통제변수가 잘못 설정될 경우 회귀분석 결과는 전혀 다르게 나올 수 있다. 만약 통제변수가 독립변수나 종속변수에 영향을 미치는 변수였을 경우, 통제변수가 회귀분석에 추가됨으로써 우리가 관심을 가지는 계수의 크기나 방향 또는 유의성에 영향을 미치게 된다. 이에 따라, 회귀식에서 통제변수를 변경하면서 회귀 결과에 유의미한 변화가 있는지 확인해보았다.

아래 표 16은 통제변수의 수를 변경하면서 회귀식을 테스트한 결과이다. 테이블 4의 (1)번은 통제변수를 모두 제거한 경우이다. 회귀 계수의 값에는 큰 차이가 없으나, 회귀식의 설명도를 나타내는 수정 R^2 값은 0.006으로 매우 낮아졌다. 즉, 통제변수를 제거함으로써 회귀식의 적합성이 낮아진 것이다. 테이블4의 (2)번에서 (5)번까지는 통제변수를 하나씩 추가하면서 회귀식을 테스트한 결과이다. 통제변수의 수가 늘어나면서 상호작용항의 회귀계수의 크기에 약간의 변화가 있지만, 회귀계수의 방향성이나 유의도에는 영향을 미치지 않고 있다. 이와 달리, 회귀식의 설명도를 나타내는 수정

표 16 통제변수 유효성 테스트 결과

	(1)	(2)	(3)	(4)	(5)
	Security Equipment	Security Equipment	Security Equipment	Security Equipment	Security Equipment
IT Companies × Post 2018	**-0.370*** **	**-0.401*** **	**-0.347*** **	**-0.329*** **	**-0.329*** **
	(0.0555)	**(0.0509)**	**(0.0488)**	**(0.0483)**	**(0.0482)**
IT Companies	0.466***	0.488***	0.432***	0.374***	0.372***
	(0.0344)	(0.0315)	(0.0302)	(0.0299)	(0.0299)
Post 2018	-0.106***	-0.160***	-0.256***	-0.324***	-0.326***
	(0.0148)	(0.0136)	(0.0131)	(0.0131)	(0.0131)
Size		0.430***	0.375***	0.330***	0.332***
		(0.00461)	(0.00450)	(0.00468)	(0.00469)
Amount Private Data Retention			0.109***	0.102***	0.102***
			(0.00172)	(0.00171)	(0.00171)
New IT tech Adoption				0.180***	0.182***
				(0.00571)	(0.00573)
Experienced Cyber Incidents					-0.123***
					(0.0284)
Constant	3.761***	2.515***	2.396***	2.292***	2.292***
	(0.00932)	(0.0159)	(0.0153)	(0.0155)	(0.0155)
Observations	45502	45502	45502	45502	45502
Adjusted R^2	0.006	0.165	0.233	0.249	0.249

Standard errors in parentheses

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

R^2 값은 통제변수의 수가 늘어날수록 점차 커지는 것을 볼 수 있다. 즉, 통제변수를 추가할수록 모델 적합도가 높아지는 것이다.

분석 결과를 종합하면, 통제변수의 유무가 우리가 관심을 가지는 상호작용항의 회귀계수의 방향성이나 유의성, 크기에 큰 영향을 미치지 않는 반면 통제변수가 추가될수록 회귀식의 설명력은 높아지고 있는 바, 이 연구에서 설정한 4개의 통제변수의 활용은 타당하다고 판단하였다.

다음의 표 17과 18은 종속변수 2와 3에 대한 통제변수 유효성 테스트 결과이다. 이 종속변수들은 통제변수가 추가될 때 상호작용항의 회귀계수의 방향이 변하고 있으며, 절대값도 큰 폭으로 변하고 있다. 따라서 이 종속변수들은 통제변수의 사용이 적절하지 못했다.

표 17 종속변수 2에 대한 통제변수 테스트 결과

	(1)	(2)	(3)	(4)	(5)
	Security Institutions	Security Institutions	Security Institutions	Security Institutions	Security Institutions
IT Companies	0.721***	0.759***	0.684***	0.639***	0.638***
	(0.0384)	(0.0302)	(0.0278)	(0.0276)	(0.0276)
Post 2018=1	0.326***	0.233***	0.104***	0.0519***	0.0503***
	(0.0165)	(0.0130)	(0.0120)	(0.0121)	(0.0121)
IT Companies # Post 2018=1	-0.0202	-0.0740	-0.00106	0.0126	0.0126
	(0.0620)	(0.0488)	(0.0448)	(0.0445)	(0.0445)
Size		0.737***	0.665***	0.630***	0.630***
		(0.00443)	(0.00414)	(0.00431)	(0.00432)
Amount Private Data			0.145***	0.140***	0.140***
			(0.00158)	(0.00158)	(0.00158)
New IT tech Adoption				0.140***	0.141***
				(0.00526)	(0.00529)
Experienced Cyber Incidents					-0.0720**
					(0.0262)
Constant	1.731***	-0.408***	-0.567***	-0.648***	-0.648***
	(0.0104)	(0.0152)	(0.0141)	(0.0143)	(0.0143)
Observations	45502	45502	45502	45502	45502
Adjusted R^2	0.021	0.392	0.488	0.495	0.495

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

표 18 종속변수 3에 대한 통제변수 테스트 결과

	(1)	(2)	(3)	(4)	(5)
	Security Services Outsource	Security Services Outsource	Security Services Outsource	Security Services Outsource	Security Services Outsource
IT Companies	0.307***	0.331***	0.253***	0.190***	0.189***
	(0.0370)	(0.0336)	(0.0313)	(0.0310)	(0.0310)
Post 2018=1	0.484***	0.422***	0.289***	0.216***	0.214***
	(0.0159)	(0.0145)	(0.0135)	(0.0136)	(0.0136)
IT Companies # Post 2018=1	-0.0387	-0.0740	0.00164	0.0207	0.0207
	(0.0598)	(0.0543)	(0.0505)	(0.0499)	(0.0499)
Size		0.484***	0.408***	0.360***	0.361***
		(0.00492)	(0.00466)	(0.00483)	(0.00484)
Amount Private Data			0.151***	0.144***	0.144***
			(0.00178)	(0.00177)	(0.00177)
New IT tech Adoption				0.196***	0.197***
				(0.00590)	(0.00593)
Experienced Cyber Incidents					-0.0798**
					(0.0294)
Constant	1.522***	0.119***	-0.0464**	-0.159***	-0.159***
	(0.0100)	(0.0169)	(0.0159)	(0.0160)	(0.0160)
Observations	45502	45502	45502	45502	45502
Adjusted R^2	0.023	0.194	0.305	0.321	0.321

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

4.3. 부적절한 할당의 오류 확인

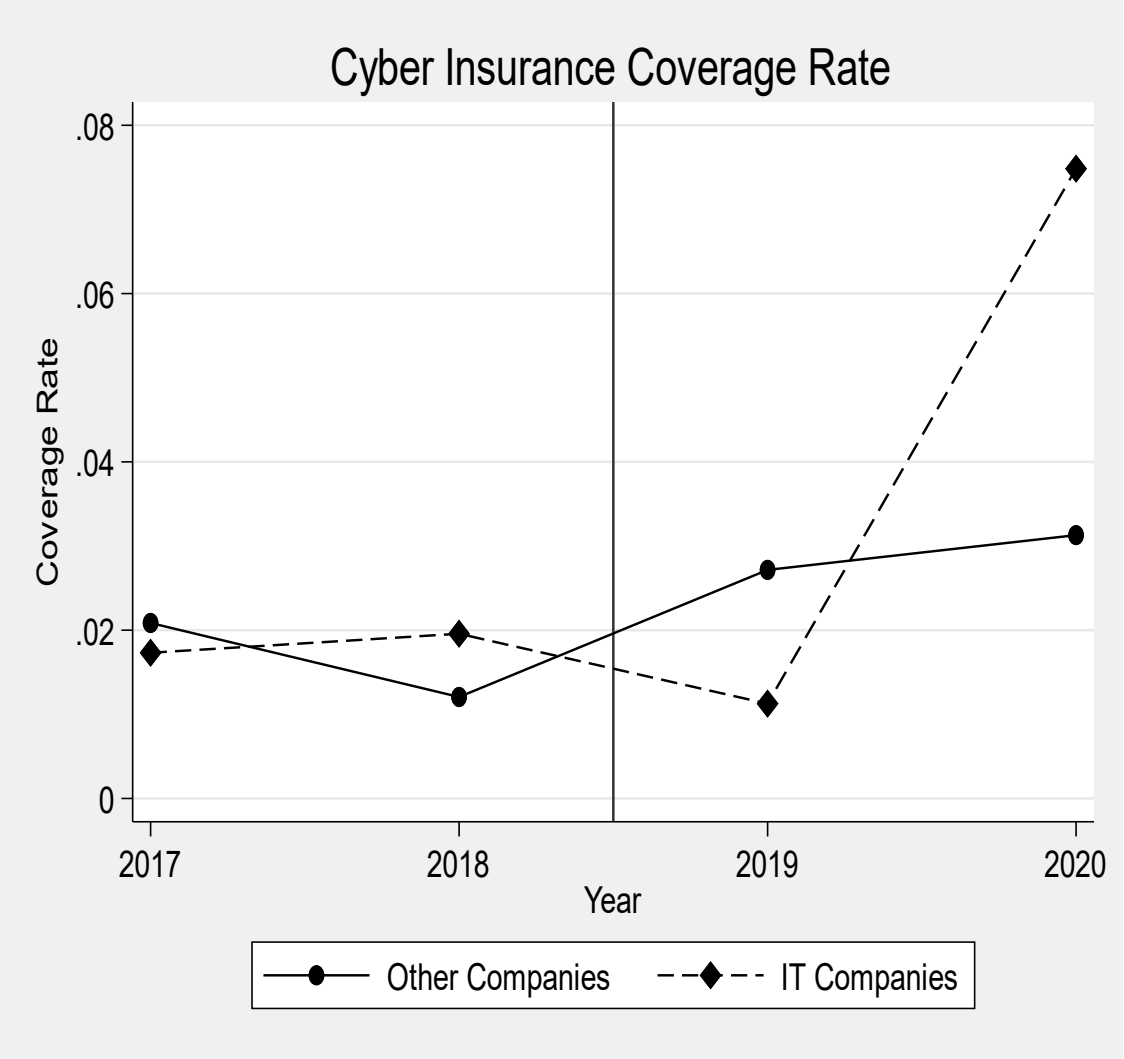
이 연구는 기본적으로 정부의 정책 변화를 바탕으로 정책 대상과 그 외 집단을 비교 분석하는 틀을 가지고 있다. 따라서, 정확한 분석을 위해서는 정책 대상 기업과 그렇지 않은 기업들을 정확히 구분하여 처치그룹과 통제그룹을 설정하는 것이 가장 이상적일 것이다. 하지만, 이 연구에서 사용한 설문조사가 기업을 분류하는 방식은『정보통신망법』혹은『개인정보보호법』에서 정하고 있는 정책 대상을 정확히 분류해내는데 한계가 있다. 따라서, 이 연구는 설문조사가 제공하는 기업 분류 중 정책 대상을 가장 많이 포함하고 있을 것으로 생각되는 집단인 정보통신기업군을 처치그룹으로 설정하였다.

이렇게 실제 정책 대상과 이 연구가 설정한 처치그룹인 정보보호 실태조사의 분류에 따른 정보통신업은 차이가 있다. 예를 들어, SK텔레콤이나 다음 포털 사업자의 경우에는 정보통신서비스 제공자에 속함과 동시에 정보통신업에 속할 것이다. 하지만, 예를 들어 현대자동차는 정보통신업에는 속하지 않지만 홈페이지를 운영하여 영리활동을 펼치고 있으므로 정보통신서비스 제공자에는 속할 수 있을 것이다.

이와 같은 처치그룹과 통제그룹 설정 오류는 그래프를 통해서도 확인할 수 있다. 아래 그림 3은 처치그룹과 통제그룹의 사이버보험 가입률 변화 추이를 비교한 것이다.

그림 19의 그래프를 보면, 정책 시행 이후 약 1년의 시차를 두고 처치그룹의 보험 가입률이 가파르게 상승하는 것을 확인할 수 있다. 보험가입률이 1년의 시차를 두고 나타나는 이유는 법 개정과 발효에 시차가 있었기 때문이다. 사이버보험을 의무화시키는『정보통신망법』개정은 2018년에 이루어졌지만 실제로 적용된 것은 2019년이었다. 이 법은 제도를 관리할 정부 당국과 법에 따른 의무가 발생한 기업들에게 준비할 시간을 보장하기 위해 6개월의 계도기간을 두었다.

그림 19 그룹별 보험 가입률



그런데, 이 그래프를 보면 통제집단에서도 정책 시행 후 보험가입률이 상승한 것을 볼 수 있다. 단순히 시간이 흐르면서 발생한 트렌드일 수도 있지만, 통제집단 내에 정책의 영향을 받은 기업이 포함되었기 때문에 발생했을 가능성을 배제할 수 없다.

보다 정확한 분석을 위해, 통제집단을 산업 분야별로 세분화하여 연도별 보험가입률 변화를 관찰해보았다. 그래프 4와 5가 이를 보여주고 있다.

그림 20은 전체 13개 업종의 보험가입률 그래프를 모두 보여주고 있으며, 그림 5는 이 중 보험가입률이 높은 4개 업종만을 추려내어 그래프로 나타낸 것이다. 다만, 금융 및 보험업(Finance and Insurance)의 경우 보험가입률이 높지만 이 연구에서 고려하는 법 및 정책의 변화와는 명백하게 관계없기 때문에 고려하지 않았다. 금융 및 보험업의 경우 금융 관련 법에서 오래전부터 보험 가입을 의무화한 경우가 많다.

그림 21을 보면 기타업종의 경우 처치그룹인 정보통신업종보다 사이버보험 가입률 상승 기울기가 더 높으며, 도소매업과 전문 및 과학기술 서비스업도 정도의 차이는 있으나 정책 시행 이후 가입률이 상승하는 것이 눈에 띈다. 따라서, 통제그룹 내에 정책의 영향을 받은 기업이 존재할 가능성이 높다.

한편, 사이버보험 의무 가입 정책 적용 대상의 정의에서 보듯이, 처치그룹 내에도 정책의 대상이 아닌 경우가 있을 것으로 예상할 수 있다. 『개인정보보호법』은 시행령에서 정보통신서비스 제공자 중 고객 1000명 이상의 개인정보를 보유한 기업 및 전년도 매출액 5천만원 이상인 기업으로 의무 가입 대상을 제한하고 있다. 하지만 이 연구에서는 모든 정보통신기업을 처치그룹으로 설정하였기 때문에 오류 가능성이 높다.

그림 20 업종별 보험 가입률

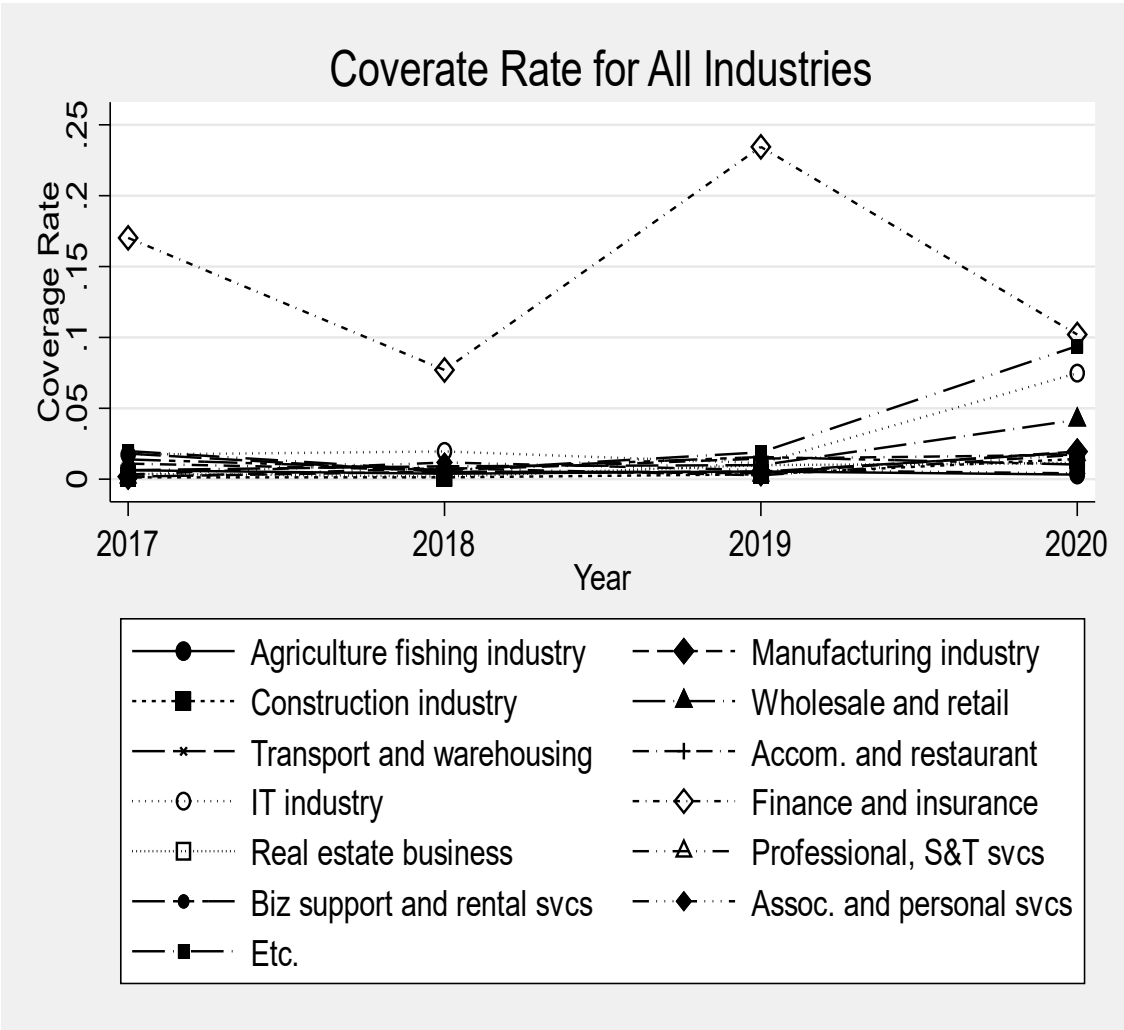
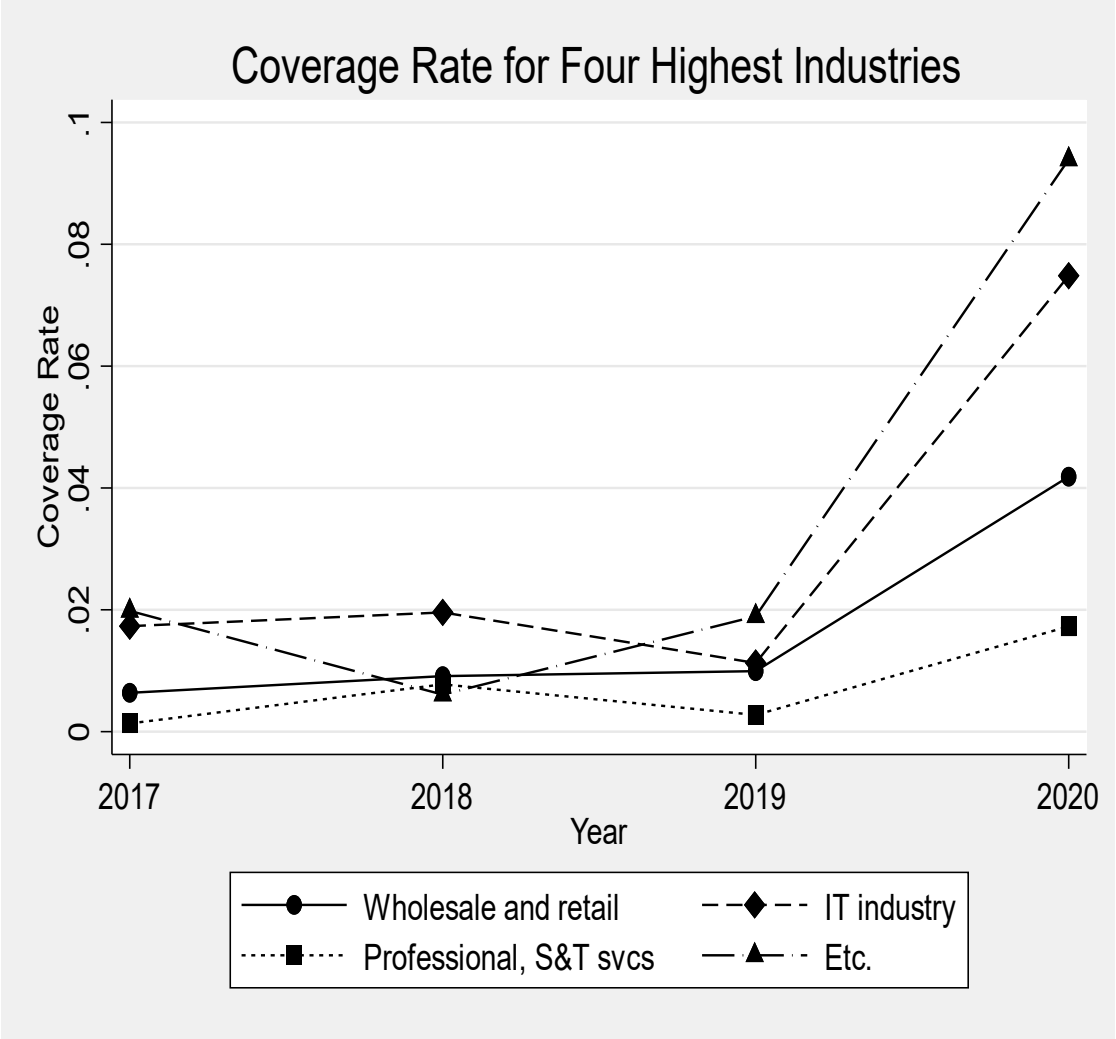


그림 21 주요 상위 업종별 보험 가입률



이중차분법 분석에서 샘플들을 처치그룹과 통제그룹으로 정확히 분류해내지 못하는 할당 오류는 회귀분석 결과를 희석시킬 것이다. 만약 부적절한 할당 오류가 어떤 이유로든 체계적으로 발생했다면 회귀 결과를 반드시 희석시키는 것이 아닐 수 있으나, 이 연구에서 특별히 부적절한 오류가 체계적으로 발생했을 가능성이 보이지는 않는다. 따라서 처치그룹과 통제그룹에 들어갈 기업들이 일부 부적절하게 섞인 오류는 회귀 계수의 크기를 줄이는 효과를 냈을 것으로 본다. 따라서, 회귀분석 결과 회귀 계수의 절대값은 하한선으로서 기능한다.

아래 표 19는 보험가입률이 가장 가파르게 상승한 기타업종을 정보통신업종과 함께 처치그룹으로 포함시켜서 분석한 회귀결과이다. 이 표를 보면, 상호작용항의 회귀계수값이 -0.406으로서 기존 회귀계수값인 -0.329보다 절대값이 더 큰 것을 알 수 있다. 이 결과는 기존의 회귀계수값인 -0.329가 하한선으로 작용한다는 위 판단을 지지해준다.

이상의 결과를 종합하면 연구 결과는 다음과 같이 해석할 수 있다. 의무 사이버보험 정책은 기업의 정보보호 장비 사용 종류의 수를 0.329 (정보보호 장비 사용 종류의 수의 평균은 3.7) 혹은 9% 이상 줄인다.

표 19 기타업종을 처치그룹으로 추가했을 때의 회귀분석 결과

	(1) Number of Types of Security Equipments
isITetc=1	0.234***
	(0.0226)
Post 2018=1	-0.292***
	(0.0137)
isITetc=1 # Post 2018=1	-0.406***
	(0.0350)
Size	0.330***
	(0.00468)
Amount Private Data	0.101***
	(0.00173)
New IT tech Adoption	0.185***
	(0.00573)
Experienced Cyber Incidents	-0.133***
	(0.0284)
Constant	2.288***
	(0.0156)
Observations	45502
Adjusted R^2	0.249

Standard errors in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Ⅳ. 결론

최근 인공지능과 5G 등 정보통신기술의 발달은 사회 경제 전반의 정보화를 이끌고 있다. 특히 최근의 코로나 바이러스로 인한 공중보건비상사태는 일상 생활의 비대면화를 촉진하면서 정보통신기술의 일상에의 침투가 가속화되고 있다.

이런 시대적 흐름은 자연스럽게 사이버위협이라는 정보통신기술의 역기능에 대한 우려로 이어지고 있으며, 국가적으로 이를 개선할 수 있는 방안을 마련하는 것은 세계 속에서 우리나라가 경쟁력을 가지기 위해 필수적이다. 전력망, 금융 인프라 등 국가 기반시설에서 IP카메라 등 일상 생활 주변에서 찾을 수 있는 사물인터넷 제품에 이르기까지 인터넷에 연결되는 모든 것들은 해킹의 위험에 노출되어 있어, 이제는 사이버위협이 국민의 일상에서 안전에 위협을 주는 수준까지 이르고 있다.

이에 따라 세계 각 국은 다양한 사이버위협 대응 전략을 마련하고 있는데, 이 중 사이버보험이 경제·사회의 복원력 강화를 위해 좋은 수단으로 인식되고 있다. 사이버보험은 사이버위협에 의한 피해를 보상해주는 보험 상품으로서 기업 등 가입자의 사이버 위험을 효과적으로 분산시켜주는 수단이다. 여기에 더하여, 사이버보험 상품이 적절한 가격 차별 전략을 통해 가입자에게 사이버보안 투자를 이끌어 낸다면 국가 전체적으로 사이버보안 수준이 높아지게 되므로 사이버보험은 민간의 사이버보안 투자를 이끌어냄과 동시에 유사시 피해로부터 빠르게 복구할 수 있는 수단으로 부각되었다.

사이버보험은 미국, 영국 등을 중심으로 2000년대 초반부터 시장이 발달해왔으며, 한국의 경우에는 2018년 사이버보험이 정보통신서비스 제공자를 대상으로 일부 의무화되면서 현재 시장이 서서

히 형성되고 있다.

그런데, 사이버보험의 기능에 대한 시장에서의 기대와 달리 학계에서는 경우에 따라 사이버보험이 사회적으로 보안 수준을 열화시키는 악영향을 일으킬 수 있다는 연구 결과가 보고되고 있다. Shetty, Khalili 등에 따르면, 사이버보험의 기업 사이버보안에 대한 영향은 보험 시장의 특성에 따라 달라지는데, 보험 시장이 독점적인 경우에는 보험사가 가격 차별 전략을 통해 보안 투자를 유도할 수 있으나, 보험 시장이 경쟁적인 경우에는 보험사가 가입자에게 보안 투자를 유도할 수 없으면 이에 따라 사회 전체의 보안 수준이 낮아지게 된다.

만약 사이버보험이 당초 기대와 달리 이와 같은 부작용을 만들어낸다면 정부의 정책이 재검토되어야 할 것이다. 이에 따라 본 연구에서는 한국의 시장 환경에서 사이버보험 의무화 정책이 기업의 보안 투자 태도에 어떤 영향을 미치는지 실증 분석을 진행해보았다.

한국에서는 2018년에『정보통신망법』개정을 통해 정보통신서비스 제공자를 대상으로 사이버보험이 일부 의무화되었다. 전년도 매추 5천만원 이상이며 고객의 개인정보를 1,000건 이상 보유한 기업에 한해 손해배상의 보장을 위해 기업이 보험, 공제 또는 준비금을 적립하도록 의무화한 것으로, 해당되는 기업들이 보험에 가입하지 않고도 의무를 이행할 수 있기 때문에 이 정책에 의한 보험 가입률이 매우 높지는 않으나 정책 시행 이전에 비해 이후 기간에 정책 대상 집단의 보험 가입률은 눈에 띄게 늘어났고, 이를 바탕으로 본 연구가 진행되었다.

이 분석에는 한국 정보보호산업협회가 시행하는 '정보보호 실태조사' 데이터가 활용되었으며, 사이버보험이 의무화된 2018년을 전

후한 5개년 데이터를 바탕으로 이중차분법 모델을 사용하였다. 분석에서 처치그룹은 정보보호 실태조사의 분류에 따른 정보통신업으로 설정하고, 통제그룹은 이 업종을 제외한 나머지 모든 기업으로 설정하였다. 처치그룹인 정보통신업종이 정책 대상인 정보통신서비스 제공자와 완전히 일치하지는 않지만 실태조사의 분류체계 내에서 가장 유사한 그룹이기 때문에 이 업종이 처치그룹으로 설정하였으며, 기업의 사이버보안 수준을 측정하는 종속변수로는 기업이 사용하는 '정보보호 제품의 종류의 수', '정보보호 제도 수준', 그리고 '아웃소싱 중인 정보보호 서비스의 종류의 수'를 설정하였다.

분석 결과, 우리나라에서 2018년 도입된 사이버보험 의무화 정책은 기업들의 보안 투자를 9% 이상 줄이는 것으로 나타났다. 테스트한 종속변수 3가지 중 '정보보호 제품의 종류의 수'만이 통계적으로 유의미한 것으로 나타났고, 나머지 두 변수는 통계적으로 의미가 없었다. 분석 결과를 다시 말하면, 기업들은 사이버보험 의무화 정책 시행 후 사용하는 정보보호 제품의 종류를 9% 줄였다.

이 분석의 실효성을 확인하기 위해 이 연구에서 우리는 평행 추세 가정의 성립 여부, 통제 변수의 유효성, 샘플의 처치그룹 할당 오류 등을 검토하였다. 평행 추세의 경우, 이중차분법 모델의 필수 조건으로서 처치그룹과 통제그룹이 동질적인 특성을 갖는다는 가정이다. 확인 결과 이 연구에서 관심이 있는 종속변수인 '정보보호 제품의 종류의 수'에 있어 처치그룹과 통제그룹은 정책 시행 이전 3년 동안 평행 추세를 보였다. 따라서 이 연구에서 평행 추세 가정은 성립한다.

통제 변수의 유효성의 경우, 독립변수나 종속변수에 영향을 미치는 변수가 통제변수로 잘 못 삽입될 경우 회귀계수가 전혀 다른 값이 도출될 수 있으므로 통제변수가 잘 설정된 것인지 검증하는

과정을 거칠 필요가 있다. 이 연구에서 통제변수는 기업 규모, 기업이 보유한 개인정보의 양, 신 정보통신 기술의 업무 적요요 수준, 지난 1년간 사이버사고 경험 여부를 설정하였는데, 모두 기업의 업종이나 사업 모델과 별도로 기업의 사이버보안 투자 태도에 직접적인 영향을 미치는 변수이기 때문이다. 이 통제변수들이 이 연구의 분석 모델에서 적절한 역할을 한 것인지 분석하기 위해 통제변수를 제외한 상태에서 같은 회귀분석을 진행하였는데, 통제변수가 모두 제거된 상태에서 하나씩 통제변수가 추가될 때마다 회귀계수값에 미세한 변동은 있었지만 회귀계수의 방향성은 유지되었고, 그 절대값도 큰 변화가 없었다. 이에 더하여, 통제변수가 하나씩 추가될수록 모델의 설명력을 의미하는 수정 R^2 값이 점점 높아졌다. 이에 따라, 이 연구에서 통제변수는 적절하게 설정된 것으로 판단하였다.

샘플의 그룹 할당 오류의 경우, 이 연구가 처치그룹으로 설정한 것은 정보보호 실태조사 분류 상 정보통신업종인데 반해 실제 정책 적용 대상은『정보통신망법』상 정보통신서비스 제공자 중 직전년도 매출액 5,000만원 이상이며 고객의 개인정보를 1,000건 이상 보유한 경우에 한정되기 때문에 상호 불합치가 발생할 가능성이 매우 높기 때문에 검토되었다.

실제로 두 그룹의 사이버보험 가입률을 시계열로 확인한 결과 처치그룹의 보험 가입률이 정책 시행 이후 뚜렷하게 증가하였으나, 통제그룹도 어느정도 상승 추세를 보였다. 보다 구체적으로 통제그룹을 업종별로 나누어 분석한 결과, 정보보호 실태조사 분류 상 기타업종의 경우 정책 시행 후 사이버보험 가입률 상승 기울기가 처치그룹인 정보통신업보다 더 큰 것으로 나타났다. 따라서 통제그룹에 정책의 영향을 받은 대상이 어느 정도 포함되었다고 판단하였으며, 이에 따라 이 연구에서의 회귀 분석 결과값은 실제 현상보다 희석될 것으로 해석하였다. 즉, 실제 정책 효과는 이 연구가 도출

한 회귀계수값의 절대값을 '하한선'으로 한다. 이에 따라 이 연구는 사이버보험 의무화 정책이 기업들의 보안 투자를 9% '이상' 감소시킨다고 해석하였다.

이 연구는 사이버보험의 기업 보안에 대한 영향을 분석한 첫 번째 실험 연구이다. 그간 이론 연구는 여러 건 이루어졌으나 실제 정책 시행 데이터를 바탕으로 사이버보험의 영향에 대한 실증 분석이 이루어진 사례는 없으며, 이는 사이버보안 분야에서 정책 효과를 분석하기에 충분한 데이터가 체계적으로 축적되지 않기 때문이기도 하다.

이 연구에서 사이버보험 가입률은 처치그룹에서도 10% 미만으로서 저조하다. 따라서, 이 연구가 사이버보험 의무화 정책의 효과로서는 충분히 기능할 수 있으나, 사이버보험 자체의 기업 보안 투자에 대한 효과로 확대 해석하는 것은 경계할 필요가 있다. 우리나라에서 2018년 도입된 사이버보험 의무화 정책은 기업에게 보험 가입 외에도 준비금 적립 등 다른 의무 이행 수단을 허용하고 있기 때문에 사이버보험 가입률이 어느 수준 이상으로 올라가지 않을 것이며, 사이버보험에 가입하지 않는 기업들이 무작위적이지 않고 체계적일 가능성이 있다. 예를들어, 보험에 가입한 기업들은 보안 수준을 높였으나, 보험에 가입하지 않은 기업들이 어떤 체계적인 이유에 의해 보안 수준을 낮췄을 경우 분석 결과는 부정적으로 나오게 될 것이다. 이 경우, 이 연구는 한국의 사이버보험 의무화 정책의 효과를 분석한 것으로 의미가 제한되어야 할 것이다. 즉, 이 연구결과를 사이버보험의 효과로 바로 연결시킬 수 없다.

또한, 이 연구는 실험 대상을 관찰한 기간이 짧고 데이터의 양이 제한적이기 때문에 연구의 신뢰성에 한계를 가진다. 향후 몇 년간 데이터를 더 축적하고 처치 그룹을 더 분명히 설정하여 유사한 실험연구를 진행한다면 보험의 효과를 더욱 분명히 알 수 있을 것

이다.

사이버보험이 당초 의도했던 기업의 보안 투자 강화 효과를 내지 못하고 오히려 이들의 투자 의욕을 저하시켜 결과적으로 전체 정보통신 네트워크의 보안 수준 열화를 일으키고 있다는 것은 정부가 유념해야할 부분이다. 사이버보험의 부정적인 효과를 방치할 경우 낮아진 사이버보안 수준은 결과적으로 더 큰 사회적 비용으로 다가오게 될 것이다.

사이버보험의 도입 및 확산은 개별 기업의 입장에서는 사이버보안 정책을 수립함에 있어 선택권이 넓어지는 것을 의미하므로 미시적 관점에서는 긍정적이다. 우리나라의 경우 사이버보험이 일부 의무화되면서 강제적으로 보험이 확산되게 되었으나, 가입 대상을 협소하게 지정하고 있으며 가입 규모 기준도 낮게 설정하고 있어 기업들에게 과도한 규제로 작용하지 않을 것으로 기대된다. 보험이 과도하게 의무화되지 않는 한, 향후 보다 합리적인 사이버보험 상품의 출현은 기업들에게 더 다양한 기회를 부여함으로써 기업들의 효용을 극대화하는데 기여할 수 있다.

하지만, 거시적으로는 사이버보험 확산에 따라 사회 전체의 사이버보안 수준이 열화되어 사이버사고가 늘어나게 될 것이며, 네트워크의 연결성으로 인해 네트워크상의 확대된 취약점은 결국 네트워크에 접속한 모든 가입자의 보안 위협으로 다가오게 될 것이다.

이에 따라 정부는 기업들의 사이버보험 선택권은 유지하되 전체 네트워크의 보안 수준은 유지시킬 수 있도록 적절한 정책을 마련할 필요가 있다.

사이버보험 가입자가 늘어나고 시장이 확대되면 보험사는 비례하여 수익을 늘리게 된다. 따라서 정부는 이들 보험사에게 기업들

에 대한 사이버보안 점검 의무를 부여하거나 주기적인 사이버보안 컨설팅을 실시하도록 유도하고, 일정 규모 이상의 사이버보험 매출을 얻는 보험사에게는 사이버사고에 직접 대응하는 체계를 갖추도록 함으로써 전체 네트워크의 사이버보안 수준 향상에 기여할 수 있을 것이다.

참고문헌

Hofmann, A. (2007). Internalizing externalities of loss prevention through insurance monopoly: An analysis of interdependent risks. *GENEVA Risk and Insurance Review*, *32*(1), 91–111. https://doi.org/10.1007/s10713-007-0004-2

Kang, S. (2018). “Baby steps” Cyber Insurance Market, Dominated by foreign firms “A matter of Time.” *Economic Review*. http://www.econovill.com/news/articleView.html?idxno=347566

Kesan, J. P., Majuca, R. P., & Yurck, W. J. (2004). *The Economic Case for Cyberinsurance*.

Khalili, M. M., Naghizadeh, P., & Liu, M. (2018). Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security*, *13*(9), 2226–2239. https://doi.org/10.1109/TIFS.2018.2812205

Kuru, D., & Bayraktar, S. (2017). The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime*, *24*(2), 329–346. https://doi.org/10.1108/JFC-05-2016-0035

Lelarge, M., & Bolot, J. (2009). Economic incentives to increase security in the internet: The case for insurance. *Proceedings - IEEE INFOCOM*, 1494–1502. https://doi.org/10.1109/INFCOM.2009.5062066

Martinelli, F., Orlando, A., Uuganbayar, G., & Yauntsiukhin, A. (2014). Preventing the Drop in Security Investments for Non-competitive Cyber-Insurance Market. In *Risks and Security of Internet and Systems*. Springer International Publishing. https://doi.org/10.1007/978-3-319-76687-4

Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). *Will Cyber-Insurance Improve Network Security? Market Analysis*. 235–243.

Schwartz, G. A., & Sastry, S. S. (2014). Cyber-insurance framework for large scale interdependent networks. *HiCoNS 2014 - Proceedings of the 3rd International Conference on High Confidence Networked Systems (Part of CPS Week)*, 145–153. https://doi.org/10.1145/2566468.2566481

Shetty, N., Schwartz, G., & Walrand, J. (2010). Can Competitive Insurers Improve Network Security? In *Lecture Notes in*.

Sridevi, J., & Priyanka, L. (2018). An empirical study on the factors affecting employee engagement. *Eurasian Journal of Analytical Chemistry*, *13*(01), 254–260.

Uuganbayar, G., Yautsiukhin, A., & Martinelli, F. (2018). Cyber insurance and security interdependence: Friends or foes? *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018*, *Section IV*. https://doi.org/10.1109/CyberSA.2018.8551447

Yang, Z., & Lui, J. C. S. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, *74*, 1–17. https://doi.org/10.1016/j.peva.2013.10.003

Zhang, R., Zhu, Q., & Hayel, Y. (2017). A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks. *IEEE Journal on Selected Areas in Communications*, *35*(3), 779–794. https://doi.org/10.1109/JSAC.2017.2672378

한국인터넷진흥원. (2017). *2016 정보보호 실태조사*.

한국인터넷진흥원. (2018). *2017 정보보호 실태조사*.

한국인터넷진흥원. (2019). *2018 정보보호 실태조사*.

한국정보보호산업협회. (2020). *2019 정보보호 실태조사*.

한국정보보호산업협회. (2021). *2020 정보보호 실태조사*.

과학기술정보통신부. (2019). *2019 정보보호 종합대책*.

과학기술정보통신부. (2021). *K-사이버방역 추진 전략*.

최우석. (2017). 사이버위험 관리를 위한 보험의 역할 및 과제. *The Risk*, *4*.