韓國産業保安硏究 – 第13卷 第1號 (2023) : 7–28 투고일 2023.02.08 / 심사일 2023.02.27 / 게재확정일 2023.03.13
https://doi.org/10.33388/kais.2023.13.1.007

중소기업의 보안 활동이 사이버 침해사고 대응에 미치는 영향

김 은 정
(한성대학교 스마트융합컨설팅학과 박사과정)
박 인 채
(한성대학교 스마트경영공학부 조교수)

중소기업의 보안 활동이 사이버 침해사고 대응에 미치는 영향*

김 은 정** · 박 인 채***

【 요 약 】

본 연구는 국내 중소기업이 사이버 침해사고에 유연하게 대응하기 위하여 보안체계의 보안 활동이 사이버 침해사고 대응에 미치는 영향을 파악하여 효과적인 사이버 침해사고 대응체계를 구축하는 방안을 제시하는 데 목적이 있다. 중소기업에서 보안역량 강화를 위해 수행하는 보안 활동(보안정책 품질, 보안인력 품질, 보안인프라 품질, 보안프로세스 품질)이 사이버 침해사고 대응을 위한 관리체계 구축에 미치는 영향을 분석하고 중소기업의 관리방식에 따른 조절효과를 검증하였다. 국내 중소기업을 대상으로 한 2019년도 중소기업 기술보호 수준 실태조사의 데이터를 SPSS 23.0과 AMOS 22.0.0을 이용하여 분석하였다. 연구모형과 연구가설 검증을 위하여 신뢰도 분석, 타당성 검증, 구조방정식 모형 분석, 조절변수 효과를 분석하였다.

연구결과 중소기업의 사이버 침해사고 대응체계 구축에 영향도가 높은 보안 활동은 자산관리, IT관리 프로세스와 시스템관리 프로세스 순으로 나타났고, 보안정책이 기술보호 수준에 가장 큰 영향을 미친다는 선행연구들과 다르게 보안 인프라와 보안 프로세스 측면에서 더욱 영향이 큰 것으로 나타났다. 본 연구에서 지지된 가설 특히 영향도가 높은 순으로 보안 활동을 수행하고, 선행연구에서 의미 있다고 제시된 보안 정책이나 보안 인식에 대한 투자를 장기적인 계획으로 수립한다면, 장 · 단기적으로 의미 있는 사이버 침해사고 대응체계를 구축할 수 있을 것이다. 연구분석 결과가 효과적인 중소기업 맞춤형 사이버 침해사고 대응체계에 대한 기준을 수립하는 것에 도움을 줄 수 있기를 기대한다.

주제어: 사이버 침해사고, 침해사고 대응체계, 중소기업 지원사업, 보안책임자, 기업핵심정보 관리방식, 보안 활동

* 본 연구는 한성대학교 학술연구비 지원과제임
** 한성대학교 스마트융합컨설팅학과 박사과정 (제1저자)
*** 한성대학교 스마트경영공학부 조교수 (교신저자)

목 차

Ⅰ. 서 론
Ⅱ. 이론적 배경
Ⅲ. 연구방법
Ⅳ. 실증분석 및 결과
Ⅴ. 결 론

Ⅰ. 서 론

디지털 전환의 가속화로 인해 언제 어디서나 어떤 장치로나 인터넷에 접속할 수 있는 초연결 시대에 살고 있다. 또한, 코로나19 이후로 업무환경이 재택근무 등으로 다양화됨에 따라 보안 위험이 다양해지고 고도화되어 사이버 침해사고에 대한 이해와 대응방안이 더욱 필요해졌다. 기업들은 매년 기술유출과 탈취로 인한 피해를 보고 있으며, 이런 침해사고는 점점 더 복잡해지고 장기화되어 대응이 어려워지고 있다. 보안 인프라와 시스템이 상대적으로 잘 갖춰진 대기업에 비해, 중소기업들은 자산 보호에 대한 필요성은 느끼나, 자금 및 인력 부족으로 보안 인프라 구축 및 보안체계를 갖추는 것에 소홀할 수밖에 없어 정보보호에 더욱 취약한 상태가 되었다(대·중소기업·농어업 협력재단, 2020).

중소기업이 사이버 침해사고를 예방하고 침해사고 이후에도 내부적·외부적으로 유연하게 대처할 수 있으려면, 먼저 중소기업의 정보보호 현황을 알아야 한다. 그리고 중소기업의 사이버 침해사고의 특징을 파악하여야 효과적인 대응방안을 찾을 수 있다. 2009년 이후 2018년까지 산업기술 유출이 증가하였으며, 기술유출 예상 피해액이 50조 원에 달하였다. 616개 기업 중 86개 기업 영업비밀 침해되었고, 영업비밀 침해 경험이 있는 86개 기업 중 49개가 중소기업으로 확인되었다(국회정보위원회, 2019). 미국 정보보안 사이트 사이버시큐리티벤처스(CyberSecurity Ventures)의 보고서에 따르면 사이버범죄로 인한 피해액은 2021년까지 연간 6조 달러(7,170조원)이며, 2015년 3조 달러(3,585조원)의 두 배 수준에 이른다. 사이버보안 업체 사이레론(Cyleron)의 수전 레너 최고경영자(CEO)는 포브스(Forbes)에 "중소기업의 경우 보안 위협으로부터 회사를 보호할 자원이나 전문지식이 부족해 사이버 공격의 주 타깃이 된다"며 "중소기업의 사이버보안 중요성이 가장 커지는 때"라고 진단을 내놨다. 그는 이어 "악성 프로그램 공격 대상자의 58%가 중소기업이다"며 "피해 기업 중 94%가 어음, 송장, 메일 전송 실패 통지 등으로 위장한 악성 프로그램이나 피싱 메일로 피해를 본다"고 덧붙였다. KISA에서 발표한 2017년 기업 규모별 사이버침해 사고율을 보면 전체 피해기업 중 98%

가 중소기업으로 나타났다. 한국 랜섬웨어 침해대응센터에서 발표한 보고에서도 2019년 상반기 기준 랜섬웨어 업종별 피해분석 결과, 중소기업 43%와 소상공인 25%의 피해율이 대기업 1%보다 월등히 높다고 발표하였다(김평화, 2019).

중소기업은 기술보호 역량이 부족하고, 대기업에 비해 사이버 침해사고의 비중이 높다. 그리고 이러한 사이버 침해사고는 기업 성장의 걸림돌이 되고 있는 상황임에도 불구하고 대기업들이 보안사고 대응에 적극적인 대처를 하는 것에 비해 자금력과 보안의식이 부족한 중소기업은 여전히 소극적인 자세를 보이고 있다. 인력 및 자금력이 상대적으로 부족한 중소기업은 보안역량이 낮아 사이버 침해사고를 당할 확률이 높으며, 중소기업 스스로 보안 인프라나 시스템 구축에 투자한다고 하지만 적절한 보안체계가 아닌 대부분이 사후 대응방식으로 사업이 이루어지다 보니 투자의 범위가 제한적이며, 효율적이지 못하다(곽재연, 2019). 이에 중소기업의 보안 활동, 보안 활동과 기술보호 수준 간의 영향 관계 분석에 주안점을 두고 중소기업과 정책 지원기관의 관점에서의 연구도 중요한 것으로 제시하였다(김택영, 2022). 중소기업을 대상으로 사이버 침해사고 관련하여 다양한 연구를 하고 있다. 보안 정책과 보안 활동 측면에서 주로 연구되었으며, 보안 활동 측면에서는 보안 인프라, 보안 프로세스, 임직원의 보안인식 개선에 관한 연구 등으로 확인된다(김경선, 2016; 이홍배, 2022; 이민형, 2018). 보안 인프라가 상대적으로 취약한 중소기업에게 실질적인 혜택과 도움을 줄 수 있는 정보보호 관리체계를 구축하기 위해서 중소기업의 기술유출 및 탈취 실태 파악 등 사이버 침해사고를 연구하고, 중소기업의 정보보호 역량 수준에 대한 평가, 진행되고 있는 중소기업 정보보호 지원사업의 실효성 분석 조사가 반드시 선행되어야 한다.

본 연구는 선행연구들과 비교하여 다음과 같은 차별성을 가지고 있다. 먼저, 보안 활동을 세분화하여 구체적으로 사이버 침해사고 대응에 영향을 미치는 활동을 분석함으로써 중소기업이 사이버 침해사고 대응체계 구축에 있어 효과적인 구축 기준을 수립하는 것에 도움을 주고자 하였다. 또한, 사이버 침해사고 대응체계의 영향요인을 중소기업 지원사업 수혜 여부, 보안책임자의 역할 수행자, 기업의 핵심정보를 관리하는 방식에 따라 어떤 조절 효과를 주는지 분석하여, 사이버 침해사고 대응체계 구축에 영향을 미치는 보안요소는 무엇인지 연구하였다.

Ⅱ. 이론적 배경

1. 중소기업의 사이버 침해사고 대응체계

정보보호 관리체계를 기반으로 구축한 체계가 효과적으로 사이버 침해사고를 대응할 수

있는지 연구하였다. 안종하(2013)는 국내 사이버보안 대응체계를 위한 정책적 방안을 정부 차원에서 사이버보안 대응조직 체계화 및 위상 제고, 국가 사이버보안 관련 법령/제도 정비, 사이버보안 소요예산 확보 및 효율성 제고, 사이버보안 인력양성 및 R&D 로드맵 구축 등을 제시하였다. 강신범, 이상진, & 임종인(2012)은 제도적으로 시행되고 있는 관리적 보안, 기술적 보안, 물리적 보안 조치가 실제 침해사고 대응에 완벽한 예방책이 되지는 못하여, 현행 제도적 보호조치의 예방 효과를 알아보고 제도적 한계와 개선점을 도출하여 기업들이 실질적인 목표 정보보호 수준을 유지하기 위한 효과적인 침해사고 예방 및 대응책으로써의 선행 위협 관리 모델을 제안하였다. 성욱준(2018)은 사이버 침해사고 발생과 복구에 영향을 미치는 요인을 연구하여 정보보호 아웃소싱, 데이터 백업, 최고 경영진 및 직원의 정보보호 인식이 정보보호에 중요한 영향을 미치는 변수를 연구하였다.

보안 활동은 기본적으로 정보보호 관리체계인 ISMS-P, ISO 27001, CSF의 분류체계를 참고하여 도출하였다. 또한, 기업의 특징에 따라 보안정책이 정해지고 보안업무 성격 또한 다양하게 변경된다. 이에 따라 조직 차원에서 보호해야 할 가치를 정하고 그것에 상응하는 보안 프로세스를 확립하는 것이 중요하다(차재원, 2016). 기술과 시스템 관리만으로는 정보보호의 안정성을 유지하기 어렵고 정보보호의 효과적인 수행을 위해 정보보호 정책과 제도가 조직의 정보보호를 실질적으로 운영될 수 있도록 구성할 필요가 있다(성욱준, 2018). 이와 더불어 포스트 코로나 시대 디지털 가속화에 따라 능동적, 자발적으로 산업보안 규정 준수를 이행하는 중소기업 산업보안 강화방안으로 관리적보안, 기술적보안, 물리적보안, 인적보안을 제시하였다(송재혁, 2021). 중소기업의 현실상 보안시설 구축에 많은 비용을 투자할 수 없는 관계로 내부인, 외부 출입자 등을 관리 위주로 점검할 수 있도록 관리적보안, 기술적보안, 물리적보안으로 중소기업 산업보안 점검 체크리스트를 제시하였다(이호준, 2020). 이와 같이 본 연구에서는 기존 연구를 기반으로 보안 활동을 좀 더 세분화하여 구체적으로 사이버 침해사고 대응에 영향을 미치는 활동을 분석하였다.

2. 중소기업의 사이버 침해사고 대응체계의 영향요인 연구

1) 중소기업지원사업 수혜 여부

중소기업은 정보보호 조직이 부재하고 조직구성원들의 정보보안 인식이 현저히 낮으며, 정보보호 내부통제 시스템이 미비한 것으로 조사 되었다(이인선, 2021). 대기업 대비 전문인력과 자금의 한계로 인하여 정보보호에 투자할 수 있는 역량이 부족하다. 이러한 한계를 극복하고 중소기업에 맞는 정보보호 환경을 구축할 수 있도록 정부는 많은 지원사업을 추진하고 있다. 이러한 지원사업이 중소기업에 도입되어 효과적으로 상호작용하는지에 대하여

많은 연구가 이루어지고 있다(David 외, 2000; Zahra 외, 2002; 신진교, 최영애, 2008; 박상훈, 조남욱, 2017). 이에 국내 중소기업의 지원사업 수혜 여부가 가지는 효과를 확인하였다.

2) 보안책임자의 역할 수행자

전문적인 능력이 요구되는 보안책임자의 역할을 누가 수행하는가에 따라 그 기업의 보안 역량은 크게 달라질 것이다. 보안책임자에 관하여 주로 보안인식에 대한 연구(권재성, 2021; 김택영, 2022; 안병구, 2018) 또는 경영진의 보안 참여에 관한 연구(소현철, 2018; 신혁, 2018; 박성환, 2020) 등 보안책임자나 경영진의 보안인식에 따른 보안성과에 대하여 주로 연구되었으나, 본 연구에서는 이를 포함하여 보안책임자의 역할 수행자가 외부전문가, 부서책임자, 보안전담팀 또는 경영진이 직접 참여한 경우에 대한 연구를 통하여 어떻게 침해사고 대응이 달라지는지를 연구하였다.

3) 기업핵심정보 관리방식

시스템이나 데이터에 대한 백업은 기술 관리적 관점에서 매우 기본적이면서도 핵심적인 사항이다. 백업은 조직 내 정보의 지속성과 연속성을 보장하며, 유사시 침해사고가 발생할 경우 문제의 원인을 파악하고 조속한 문제해결에 매우 중요하게 작용한다(송정석 외, 2011). 기업이 핵심자산이 되는 중요정보를 관리할 때, 아웃소싱을 통해 관리하는 경우 사고침해인지까지 걸리는 시간이 더 길며, 데이터 백업을 주기적으로 시행할 경우에는 사고침해 인지, 사고원인 파악까지 걸리는 시간 및 복구까지 걸리는 시간을 줄일 수 있는 것으로 나타났다(성욱준, 2018). 기업의 중요정보를 자산관리 측면에서 보안체계의 하나로 관리하는 연구(이대권 외, 2021; 김양훈, 2014)로서 핵심자산에 대한 관리에 따른 보안 성과를 연구하는 것에는 부족한 부분이 있었다, 본 연구에서는 기업의 핵심정보를 관리하는 방식을 외부서비스로 관리하는가 또는 자체적인 체계를 갖추어 관리하는가에 따라 각 보안 활동이 침해사고 대응에 어떤 조절 효과를 주는지 분석하였다.

Ⅲ. 연구방법

1. 연구모형

본 연구는 국내 중소기업이 사이버 침해사고에 유연하게 대응하기 위한 보안체계를 제시

하고, 보안체계의 각 보안 활동이 사이버 침해사고 대응에 미치는 영향을 파악하여 효과적인 사이버 침해사고 대응체계를 구축하는 방안을 제시하는 것에 목적이 있다. 연구모형은 보안 활동이 보안 성과 및 수준에 영향을 미친다는 Layton (2005)의 연구모형을 참고하여 중소기업 기술보호 관점에서 설계하였다. 중소기업에서 보안역량 강화를 위해 수행하는 보안 활동이 사이버 침해사고 대응을 위한 관리체계 구축에 미치는 영향 분석과 중소기업의 관리방식에 따른 조절효과를 검증하고자 아래 연구가설과 연구모형을 구성하였다 <그림 1>.

H1: 보안 정책 품질은 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H1-1: 보안관리정책는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H1-2: 인력관리정책은 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.

H2: 보안 인력 품질은 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H2-1: 보안인식관리는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H2-2: 인력관리는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.

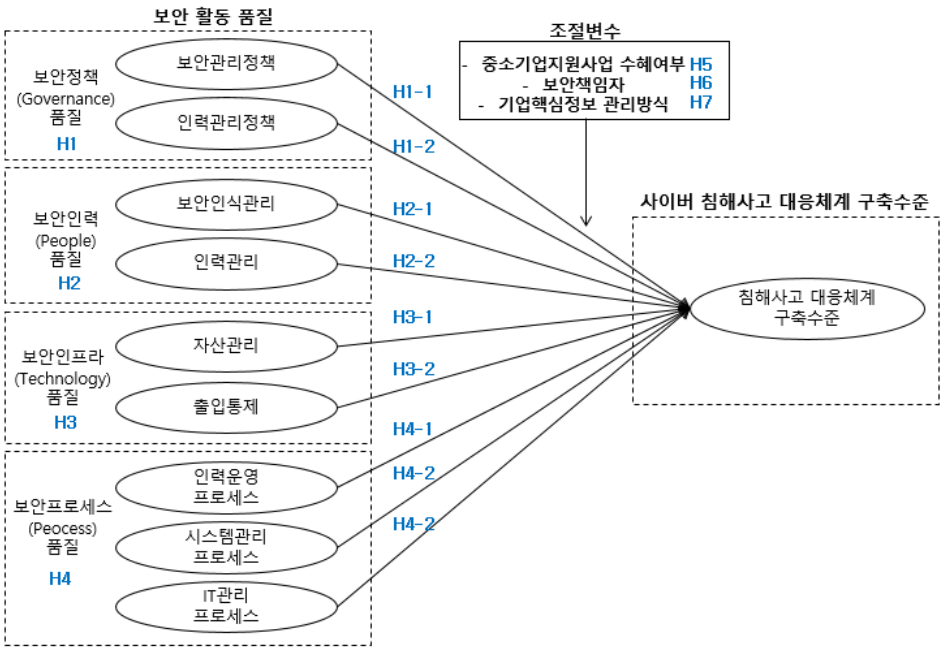
H3: 보안 인프라 품질은 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H3-1: 자산관리는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H3-2: 출입통제는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.

H4: 보안 프로세스 품질은 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H4-1: 인력 운영 프로세스는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H4-2: 시스템관리 프로세스는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.
  H4-3: IT관리 프로세스는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.

H5: 보안 활동이 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H6: 보안 활동이 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H7: 보안 활동이 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.



〈그림 1〉 연구모형

2. 연구방법 및 표본의 특성

보안체계의 각 보안 활동이 사이버 침해사고 대응에 미치는 영향에 대한 연구모형 및 가설을 검증하기 위해, 중소기업을 대상으로 매년 대·중소기업·농어업협력재단에서 조사하고 있는 '2019년 중소기업 기술보호 수준 실태조사'의 데이터를 활용하였다. 중소기업 기술보호 수준 실태조사는 성장 동력 핵심기술을 보유한 중소기업의 기술유출 및 탈취 실태를 파악하고, 기업(중소기업, 중견기업, 대기업)들의 기술자료 보안 역량 수준에 대한 정확한 진단을 통해 향후 정부에서 기술보호 지원제도 개선 및 보안역량 강화를 위한 중장기적 정책 수립 시 기초자료로 활용하고자 매년 실시하는 사업이다.

연구 데이터의 경우, 다년간의 실태조사 데이터를 활용할 수 있으나 년도간 참여기업의 식별이 보장되지 않아 연구에 적합한 특정 연도(2019년)를 선정하여 활용하였다. 이는 연구하고자 한 연구모형과 가장 근접한 설문 데이터를 가지고 있는 점에서 2019년 데이터를 특정하였다. 2019년 중소기업 기술보호 실태조사의 데이터의 실태조사 대상 및 방법 등 조사 개요는 <표 1>와 같다.

〈표 1〉 2019년도 중소기업기술보호 수준 실태조사 개요

구분	내용
모집단	- 기업부설연구소 및 연구개발전담부서를 보유한 국내 중소기업·중견기업·대기업
조사 대상	- 기업 내 보안 관련 총괄 책임자, 담당자 등 실무자 / 대표, 책임연구원
조사 지역	- 전국 17개 광역시도
조사 방법	- Multi-Method (전화 사전 접촉 후 응답자의 편의에 따라 방문, Fax, 이메일 조사)
표본추출	- 기업규모, 업종을 고려한 층화 추출
조사 기간	- 2020.1.14.~2.14
유효 표본	- 총 2,900개 업체 (중소기업 2,500개, 중견기업 200개, 대기업 200개)

※ 출처: 대 · 중소기업 · 농어업 협력재단(2020)

보안체계의 각 보안 활동이 사이버 침해사고 대응에 미치는 영향에 대한 연구모형 및 가설을 검증하기 위해, 중소기업 기술보호 실태조사의 데이터를 활용하여, 표본의 특성 도출 및 기술적 통계, 측정항목의 분석, 연구모형 및 가설에 대한 검증을 진행하였다. 측정항목의 검증을 위하여 SPSS 23.0로 신뢰도 분석과 타당성 분석을, 연구모형과 연구가설 검증을 위하여 AMOS로 구조방정식 모형을 분석하였다. 조절변수의 효과는 χ^2 차이 검정 및 경로별 표준화경로계수를 비교하여 분석하였다.

Ⅳ. 실증분석 및 결과

1. 측정항목의 신뢰도 분석 및 타당도 분석

신뢰도와 집중타당도 분석 결과는 아래 <표 2>와 같이 개별 측정변수들의 표준화 경로계수는 대부분 0.7 이상으로 나타났고, 통계적으로 유의한 것으로 확인되었다. CR과 Cronbach's α값은 0.7 이상으로 신뢰도가 높은 것으로 나타났다. 그리고 AVE는 0.5 이상이므로 집중타당도는 확보되었다고 평가할 수 있다.

〈표 2〉 연구변수의 신뢰도와 집중타당도 분석결과

항목		표준화계수	S.E.	t값	p값	C.R.	AVE	Cronbach's α
보안 정책	Policy1	0.887				0.978	0.908	0.822
	Policy2	0.931	0.027	35.512	***			
	Policy3	0.421	0.033	12.21	***			
	Policy4	0.661	0.046	21.445	***			
	Policy5	0.484	0.035	14.36	***			
보안 인력	People1	0.895				0.992	0.943	0.851
	People2	0.849	0.027	33.8	***			
	People3	0.836	0.028	32.749	***			
	People4	0.81	0.029	30.721	***			
	People5	0.826	0.028	31.945	***			
	People6	0.858	0.028	34.548	***			
	People7	0.316	0.052	8.994	***			
	People8	0.235	0.07	6.587	***			
보안 인프라	Infra1	0.53				0.928	0.767	0.703
	Infra2	0.534	0.109	10.936	***			
	Infra3	0.536	0.092	10.967	***			
	Infra4	0.713	0.113	12.837	***			
보안 프로세스	Process1	0.891				0.977	0.859	0.803
	Process2	0.218	0.028	6.022	***			
	Process3	0.404	0.04	11.674	***			
	Process4	0.818	0.03	30.326	***			
	Process5	0.812	0.033	29.895	***			
	Process6	0.859	0.027	33.134	***			
	Process7	0.683	0.034	22.581	***			
	Process8	0.041	0.049	1.118	***			
	Process9	0.213	0.04	5.878	***			
대응체계	Response1	0.8				0.897	0.814	0.737
	Response2	0.715	0.059	16.753	***			

*p<0.01 수준에서 유의함

판별 타당성 분석 결과, 아래 <표 3>와 같이 AVE의 제곱근 값이 모두 0.7 이상으로 나타났다. 또한, 해당 변수와 그 외의 다른 변수들 사이의 상관계수를 비교하였을 때, 각 변수의 평균추출분산값(AVE)의 제곱근 값이 상관계수를 상회하였다. 잠재변수 간 상관계수 중에서 가장 큰 것은 0.76(인프라와 대응체계 간)이다. 이 값의 상관계수 제곱, 즉 결정계수는

0.578(0.76 x 0.76)이다. 잠재변수 간에 구한 AVE의 제곱근 값이 결정계수 0.578보다 크므로 판별 타당도를 확보하고 있다고 할 수 있다(Chin, 1998).

〈표 3〉 구성개념 간의 판별 타당도 분석결과

구분	정책	인력	인프라	프로세스	대응체계
정책	**0.953**				
인력	0.42	**0.972**			
인프라	0.68	0.467	**0.928**		
프로세스	0.309	0.333	0.51	**0.876**	
대응체계	0.598	0.335	0.76	0.521	**0.903**

*대각선 진한 부분은 AVE의 제곱근 값을, 비 대각선의 값은 변수들 간의 상관계수를 나타냄
*모든 상관계수는 p=0.01수준에서 유의함

2. 구조모형 분석과 조절효과 분석 및 결과

1) 중소기업의 사이버 침해사고 대응체계 구축의 영향분석 및 가설검증

연구 모델의 요인들 간의 인과관계를 분석을 위해 Amos 구조방정식 모형을 분석한 결과는 <표 4>과 같다. 가설검증 결과는 H2-1: 보안인력의 보안인식관리→침해사고 대응체계(t값=-0.875, p=0.381)만이 유의한 영향을 미치지 않는 것으로 나타나 지지되지 못하였고, 이외의 연구가설은 p값이 모두 유의수준으로 확인되어 지지되었다. 보안인프라 품질(H3)의 자산관리(β=0.176, t값=9.432)와 보안프로세스 품질(H4)의 시스템관리 프로세스(β=0.15, t값=9.455), IT관리 프로세스(β=0.173, t값=9.769)는 대응체계 구축에 영향도가 높은 것으로 분석되었다.

보안 활동 중 보안정책이 기술보호 수준에 가장 큰 영향을 미친다는 앞선 연구들(김택영, 2021, 정성배 외, 2015)과 다르게 중소기업을 대상으로 한 본 연구에서는 보안인프라와 보안프로세스가 더욱 영향이 큰 것으로 나타났다. 또한, 내부/외부 인력의 보안 준수를 위한 원칙이나 규율 등의 '인력관리정책'은 상대적으로 낮게 나와 중소기업의 인력에 관한 정책은 미흡하게 관리되는 것으로 분석된다. 중소기업이 기술인력 유출 비중도 상대적으로 높음을 감안할 때, 장기적인 관점에서 근무하는 기술인력에 대한 예방적 보안도 필요하고, 인력에 대한 보안교육, 윤리 교육을 정기적으로 진행하여, 보안인식을 관리하고 보안 전문인력 양성을 하는 것도 중요하게 고려하여야 할 것이다.

〈표 4〉 구조방정식분석에 의한 가설검증 결과

구분	경로	Estimate		S.E.	C.R.	p값	검증결과
		B	β				
보안정책 품질	대응체계 ← 보안관리정책	0.157	0.121	0.028	5.688	***	지지
	대응체계← 인력관리정책	0.072	0.059	0.025	2.915	0.004	지지
보안 인력 품질	대응체계← 보안인식관리	-0.023	-0.014	0.026	-0.875	0.381	기각
	대응체계← 인력관리	0.141	0.124	0.022	6.338	***	지지
보안 인프라 품질	대응체계← 자산관리	0.194	**0.176**	0.021	9.432	***	지지
	대응체계← 출입통제	0.087	0.078	0.019	4.627	***	지지
보안 프로세스 품질	대응체계← 인력운영	0.07	0.059	0.018	3.834	***	지지
	대응체계← 시스템관리	0.169	**0.15**	0.018	9.455	***	지지
	대응체계← IT 관리	0.229	**0.173**	0.023	9.769	***	지지

*p<0.05 수준에서 유의함

2) 조절 효과 분석결과 및 가설검증

연구모형에서 중소기업이 구축한 정보보호 관리체계의 각 보안 활동이 사이버 침해사고 대응체계에 미치는 영향에 있어서, 먼저 중소기업 지원사업의 수혜 여부와 보안책임자의 역할 수행자 그리고 기업의 핵심정보를 관리방식에 따른 조절 효과를 분석하였다. 비제약모형과 제약모형의 차이는 DF=1(10-9)일 때, $\Delta\chi 2$=11.626(28.724-17.098)이고 p값은 0.001로 통계적으로 유의하게 나타났다. 따라서 지원사업 수혜여부는 조절 효과가 있다고 할 수 있다. 각 보안 활동이 침해사고 대응체계에 미치는 유의한 영향도를 파악하고자 표준화경로계수 β와 p값을 확인한 결과는 <표 5>와 같다. 비수혜기업과 비교하여 수혜 기업이 의미있게 조절효과를 나타낸 활동은 시스템관리 프로세스(β=0.181, t값=5.887***), 보안관리정책(β=0.176, t값=4.224***)과 자산관리(β=0.164, t값=4.589***)로 나타났다.

본 연구의 조절 효과 결과는 관리적 보호 방안보다는 물리적 보호 방안의 '출입통제'와 기술적 보호 방안의 '시스템관리 프로세스'에서 수혜의 조절 효과가 있는 것으로 나타났다.

이는 연구가설에 적합하게 세분화하고 조절한 연구의 분석에 의하면 중소기업지원사업은 임직원의 보안인식변화 등의 장기적인 투자에 대한 효과보다는 인프라 도입 등 물리적 보안을 통한 보안 인프라·프로세스 수립 같은 좀 더 단기적인 투자에 효과가 나타나는 것으로 분석된다.

〈표 5〉 지원사업 수혜여부에 따른 조절효과 가설검증 결과

구분	경로	비수혜 기업(C1)			수혜 기업(C2)		
		β	C.R.	p값	β	C.R.	p값
보안정책 품질	대응체계 ← 보안관리정책	0.107	4.299	***	**0.176**	4.224	***
	대응체계← 인력관리정책	0.054	2.258	0.024	0.067	1.736	0.083
보안인력 품질	대응체계← 보안인식관리	-0.006	-0.304	0.761	-0.036	-1.152	0.249
	대응체계← 인력관리	0.132	5.828	***	0.088	2.325	0.02
보안 인프라 품질	대응체계← 자산관리	0.18	8.219	***	**0.164**	4.589	***
	대응체계← 출입통제	0.07	3.551	***	0.102	3.163	0.002
보안 프로세스 품질	대응체계← 인력운영	0.06	3.272	0.001	0.061	2.112	0.035
	대응체계← 시스템관리	0.14	7.51	***	**0.181**	5.887	***
	대응체계← IT 관리	0.194	9.278	***	0.116	3.457	***

*p<0.05 수준에서 유의함

보안책임자의 역할을 누가 수행하는가에 따른 조절 효과의 가설검증은 책임자 없음(C1), 외부전문가(C2), 부서책임자(C3), 보안전담팀(C4), 경영진참여(C5)에 따른 영향을 분석하였다. 비제약모형과 제약모형의 차이는 DF=4(40-36)일 때, $\Delta\chi2$=11.908(100.527-88.619)이고 p값은 0.018로 통계적으로 유의함을 알 수 있다. 따라서 보안책임자는 조절 효과가 있다고 할 수 있다. 각 보안 활동이 침해사고 대응체계 구축수준에 미치는 유의한 영향도를 파악하고자 표준화경로계수 β와 p값을 확인한 결과는 <표 6>, <표 7>와 같이 나타났다. 보안책임자의 역할을 외부전문가(C2)가 수행할 경우 보안관리정책(β=0.346, t값=3.445***), 인력운영 프로세스(β=0.423, t값=2.561, p값=0.01), IT관리 프로세스(β=0.579, t값=3.894***)에서 의미

있는 조절 효과가 나타났다. 보안책임자의 역할을 보안전담팀(C4)이 수행할 경우 시스템관리 프로세스(β=0.311, t값=5.668***)에서 의미 있는 조절 효과가 나타났다. 그리고, 보안책임자의 역할을 경영진이 참여(C5)하여 수행할 경우 자산관리(β=0.206, t값=8.652***)에서 의미 있는 조절 효과가 나타났고, IT관리 프로세스(β=0.192, t값=8.482***)도 유의미한 결과가 나왔으나 외부전문가(C2)가 수행할 경우보다 낮게 나타났다.

본 연구에서는 경영진이 참여(C5)한 경우는 자산관리에서만 다른 그룹에 대비해 높은 조절효과를 보였으며, 외부전문가(C2)가 수행할 경우가 대부분의 활동에서 다른 그룹에 대비해 유의미하게 조절 효과가 높게 나온 것을 알 수 있다. 중소기업 내에 보안 전문가가 없는 경우가 많아 외부 보안 컨설팅을 받거나 보안서비스를 이용하는 경우가 조직 내부에서 보안책임자를 맡는 경우보다 효과가 높은 것으로 나타난 것으로 보인다.

〈표 6〉 보안책임자에 따른 조절효과 가설검증 결과(1)

구분	경로	챔임자없음(C1)			외부전문가(C2)			부서책임자(C3)		
		β	C.R.	p값	β	C.R.	p값	β	C.R.	p값
보안정책 품질	대응체계 ← 보안관리정책	0.229	3.912	***	**0.346**	3.445	***	0.128	2.611	0.009
	대응체계← 인력관리정책	0.01	0.168	0.867	-0.366	-3.357	***	-0.045	-0.979	0.328
보안인력 품질	대응체계← 보안인식관리	0.015	0.333	0.739	-0.978	-4.889	***	-0.094	-2.299	0.022
	대응체계← 인력관리	0.034	0.615	0.538	0.376	1.811	0.07	0.167	3.538	***
보안 인프라 품질	대응체계← 자산관리	0.172	3.289	0.001	-0.951	-4.153	***	0.145	3.063	0.002
	대응체계← 출입통제	0.015	0.32	0.749	-0.12	-1.273	0.203	0.124	2.877	0.004
보안 프로세스 품질	대응체계← 인력운영	0.171	3.706	***	**0.423**	2.561	0.01	0.112	2.878	0.004
	대응체계← 시스템관리	0.227	4.676	***	1.03	3.857	***	0.17	4.277	***
	대응체계← IT 관리	0.1	2.018	0.044	**0.579**	3.894	***	0.118	2.745	0.006

*p<0.05 수준에서 유의함

〈표 7〉 보안책임자에 따른 조절효과 가설검증 결과(2)

구분	경로	보안전담팀(C4)			경영진참여(C5)		
		β	C.R.	p값	β	C.R.	p값
보안정책 품질	대응체계 ← 보안관리정책	0.012	0.212	0.832	0.081	3.169	0.002
	대응체계← 인력관리정책	-0.027	-0.553	0.581	0.101	4.142	***
보안인력 품질	대응체계← 보안인식관리	0.003	0.062	0.951	0.009	0.412	0.68
	대응체계← 인력관리	0.162	2.859	0.004	0.113	4.67	***
보안 인프라 품질	대응체계← 자산관리	0.087	1.578	0.115	**0.206**	8.652	***
	대응체계← 출입통제	0.069	1.221	0.222	0.085	3.895	***
보안 프로세스 품질	대응체계← 인력운영	0.058	1.226	0.22	0.017	0.833	0.405
	대응체계← 시스템관리	**0.311**	5.668	***	0.115	5.642	***
	대응체계← IT 관리	0.187	3.284	0.001	**0.192**	8.482	***

*p〈0.05 수준에서 유의함

기업핵심정보 관리방식에 따른 조절 효과의 가설검증은 관리 안함(C1), 외부 전문서비스 이용(C2), 자체적으로 백업 관리(C3)에 따라 구분하여 영향을 분석하였다. 비제약모형과 제약모형의 차이는 DF=2(20-18)일 때, Δχ2=62.005(107.023-45.018)이고 p값은 0.000로 통계적으로 유의함을 알 수 있다. 따라서 기업핵심정보 관리방식은 조절 효과가 있다고 할 수 있다. 각 보안 활동이 침해사고 대응체계 구축수준에 미치는 유의한 영향도를 파악하고자 표준화 경로계수 β와 p값을 확인한 결과는 <표 8>와 같이 나타났다. 기업핵심정보를 외부서비스(C2)를 이용하여 관리할 경우는 다른 집단에 비교하여 보안관리정책(β=0.173, t값=4.601***), 자산관리(β=0.255, t값=7.69***), IT관리 프로세스(β=0.167, t값=5.452***)에서 의미 있는 조절 효과를 나타냈다. 기업핵심정보를 자체적으로 관리(C3)하는 경우는 시스템관리 프로세스(β=0.181, t값=8.682***)에서 의미 있는 조절 효과를 나타냈으며, 외부서비스(C2)를 이용한 경우와 비교하였을 때 전반적으로 낮은 영향도를 보였다.

외부서비스(C2)를 이용하여 관리할 경우 자산 및 체계의 보안 활동을 지원하는 원칙이나 규율을 수립하는 '보안관리정책', 어플리케이션, 장비, 시설 등 기업의 주요자산을 관리하는

‘자산관리’, 정보시스템의 로그 및 최신 업데이트 등 보안관리 또는 보안 절차 등의 ‘IT관리 프로세스’에서 다른 집단보다 조절효과가 크게 나타났다. 이는 자체적으로 백업체계를 갖추기 어려운 중소기업이 외부 전문서비스 이용(C2)함으로써 외부서비스의 보안 전문가가 참여하여 자산에 대한 보안관리정책을 수립하여 보안 인프라와 보안 프로세스를 체계적으로 관리할 수 있게 지원하기 때문이라고 파악된다.

〈표 8〉 기업핵심정보 관리방식에 따른 조절효과 가설검증 결과

구분	경로	관리안함(C1)			외부서비스(C2)			자체적관리(C3)		
		β	C.R.	p값	β	C.R.	p값	β	C.R.	p값
보안정책 품질	대응체계 ← 보안관리정책	0.103	1.325	0.185	**0.173**	4.601	***	0.079	2.805	0.005
	대응체계← 인력관리정책	-0.044	-0.622	0.534	0.018	0.485	0.628	0.093	3.486	***
보안인력 품질	대응체계← 보안인식관리	0.02	0.356	0.722	-0.024	-0.815	0.415	0.005	0.208	0.835
	대응체계← 인력관리	0.216	3.215	0.001	0.088	2.565	0.01	0.126	4.872	***
보안 인프라 품질	대응체계← 자산관리	0.178	2.636	0.008	**0.255**	7.69	***	0.146	5.875	***
	대응체계← 출입통제	-0.007	-0.126	0.9	0.052	1.786	0.074	0.065	2.813	0.005
보안 프로세스 품질	대응체계← 인력운영	0.1	1.775	0.076	0.045	1.648	0.099	0.073	3.443	***
	대응체계← 시스템관리	-0.054	-0.939	0.348	0.079	2.742	0.006	**0.181**	8.682	***
	대응체계← IT 관리	0.257	4.109	***	**0.167**	5.452	***	0.153	6.435	***

*p<0.05 수준에서 유의함

3) 연구 결과 분석

중소기업은 보안 인프라와 시스템이 상대적으로 잘 갖춰진 대기업에 비해, 보안역량이 상대적으로 낮아 사이버 침해사고를 당할 확률도 높으며, 투자의 범위가 제한적이고 효율적이지 못하다. 이러한 중소기업 환경에서 효과적으로 사이버 침해사고를 대응하기 위하여 중소기업의 정보보호 실태를 연구하고, 사이버 침해사고에 유연하게 대응하기 위한 보안체계를 제시하고, 각 보안 활동 중 사이버 침해사고 대응체계에 미치는 영향도와 조절효과을

분석했다.

중소기업 업체는 그들의 맞는 보안체계를 구축함에 있어 단기적으로는 엄격한 물리적 보안과 기술적 보안을 통해 보안인프라와 보안 프로세스를 구축하여 효과적으로 구축하는 것도 중요하다. 하지만, 중소기업이 기술인력 유출 비중도 상대적으로 높음을 감안할 때, 장기적인 관점에서 근무하는 기술인력에 대한 예방적 보안도 필요하고, 인력에 대한 보안교육, 윤리 교육을 정기적으로 진행하여, 보안인식을 관리하고 보안 전문인력 양성을 하는 것도 중요하게 고려하여야 한다.

재정적인 제약뿐 아니라 전문인력이 부족한 환경에서 쉽게 분석결과에 따라 사이버 침해사고 대응을 위한 정보보호 관리체계를 구축하는 것은 쉬운 일은 아닐 것이다. 먼저 중소기업 정보보호 지원사업의 법제도 추진 체계를 이해하고, 각 기관에서 시행하는 다양한 중소기업 지원사업을 이용하는 것도 효율적인 구축방안이 될 수 있을 것이다. 하지만 이 또한 마구잡이식 시도가 아닌 기업의 위험을 분석하여 해당 조직의 중요자산에 대한 위험 관리 수준을 지정하고, 이러한 위험 관리 방안을 근거로 정보보호 관리체계 구축 계획을 수립해야 할 것이다.

Ⅴ. 결론 및 시사점

중소기업은 대기업에 비해 사이버 침해사고의 비중이 높고, 이에 반해 기술보호 역량이 부족하다. 대기업이 보안사고 대응에 적극적인 대처를 하는 것에 비해 산업보안에 투자가 부족한 중소기업은 여전히 소극적인 자세를 보이고 있다. 중소기업 스스로 보안 인프라나 시스템 구축에 투자한다고 하지만 적절한 보안체계가 아닌 대부분이 사후 대응방식으로 사업이 이루어지다 보니 투자의 범위가 제한적이며, 효율적이지 못하다(곽재연, 2019). 본 연구에서는 디지털 전환의 가속화로 인해 더욱 복잡해진 초연결 시대에 사이버 침해사고 대응을 위해 중소기업이 효과적으로 수행할 수 있는 보안 활동은 무엇인지 알아보고자 연구하였다.

중소기업 정보보호와 관련하여 보안 활동이 사이버 침해사고 대응에 영향을 미치는지 여부와 정도의 차이를 분석함으로써, 중소기업의 정보보호를 위한 방향을 제시하고자 하였다. 이를 위해 연구결과를 바탕으로 중소기업 정보보호의 문제점을 도출하고, 문제해결을 위한 개선 방향을 제시하고자 하였다. 분석 결과는 사이버 침해사고 대응체계 구축에 영향도가 높은 보안 활동은 자산관리, IT관리 프로세스와 시스템관리 프로세스 순으로 나타났다. 보안활동 중 보안정책이 기술보호 수준에 가장 큰 영향을 미친다는 선행연구들과 다르게 본 연구에서는 보안 인프라와 보안 프로세스 측면에서 더욱 영향이 큰 것으로 나타났다. 또한, 중소기업지원사업 수혜 여부에 따른 조절 효과는 시스템관리 프로세스, 보안관리정책, 출입통제

에서 주로 조절 효과가 나타난 것으로 확인되었다. 보안책임자의 역할 수행자에 따른 조절 효과는 경영진이 참여한 경우 출입통제 측면에서 영향도가 있는 것으로 보이나, 외부전문가가 수행할 경우가 더욱 많은 보안활동에서 유의미하게 조절 효과가 큰 것으로 나타났다. 기업핵심정보 관리방식에 따른 조절 효과도 중소기업 자체적으로 백업 관리체계를 구축하여 관리하는 경우보다 외부 전문서비스 이용하는 경우가 전반적으로 조절 효과가 큰 것으로 나타났다.

본 연구에서 지지된 가설 특히 영향도가 높은 순으로 보안 활동을 수행하고, 선행연구에서 의미 있다고 제시된 보안정책이나 보안인식에 대한 투자를 장기적인 계획으로 수립한다면, 장·단기적으로 의미 있는 관리체계를 구축하는 것이라 할 수 있다. 장기적인 수행을 위해 정보보호 로드맵을 수립하여 이를 기반으로 중소기업지원사업의 수행 결과를 분석하고 미흡한 부분에 대한 지속적인 보완을 통하여 사이버 침해사고 대응체계를 구축하는 것이 필요하다. 본 연구의 실증분석 결과가 정보보호 환경을 구축함에 있어 효과적인 중소기업 환경 맞춤형 사이버 침해사고 대응체계에 대한 기준을 수립하는 것에 도움을 줄 수 있기를 기대한다.

마지막으로 디지털 전환의 가속화로 인해 더욱 복잡해진 초연결 시대에 중소기업이 사이버 침해사고 대응을 위하여 정보보호 관리체계를 기반으로 하여 사이버탄력성을 갖출 수 있는 보안요소는 무엇인지 연구가 필요하나, 사용한 연구데이터는 연도별 기업을 추적해서 침해에 대한 복원력 분석을 할 수 없는 한계가 존재하였다. 향후에는 중소기업의 사이버탄력성을 갖출 수 있는 보안요소는 무엇인지 뉴노멀 시대에서 중소기업 보안체계의 방향에 대한 연구가 필요할 것이다.

참 고 문 헌

국내문헌

강신범 · 이상진 · 임종인. (2012). “기업의 침해사고 예방을 위한 관리 모델”, 「정보보호학회논문지」, 22(1):107-115.

곽재연. (2019). “중소기업의 정보보호 활동을 위한 지원정책의 방향성 연구”, 「석사학위논문」, 한양대학교 대학원.

권재성. (2021). “재택근무에 따른 정보유출 대책방안에 대한 기업 보안담당자들의 인식 연구”, 「석사학위논문」, 중앙대학교 대학원.

김건희 · 박준석 · 정성배. (2018). “중소기업 산업기술보호활동이 산업보안정책준수의지에 미치는 영향-보안인식의 매개효과를 중심으로”, 「한국산업보안연구」, 8(1):75-111.

김경선. (2016). “기술보호활동이 기업성과에 미치는 영향에 관한 실증연구”, 「박사학위논문」, 성균관대학교 대학원.

김양훈. (2014). “핵심기술 유출과 보안수준 상관관계 연구: 중소기업 기술유출을 중심으로”, 「한국산업보안연구」, 4(1):97-108.

김용재. (2017). “기업의 정보보호 활동에 관한 연구”, 「석사학위논문」, 서울대학교 대학원.

김택영 · 김태성 · 전효정. (2022). “중소기업의 기술보호 인식과 활동이 기술보호 수준에 미치는 영향”, 「한국산업보안연구」, 12(1):79-109.

박상훈 · 조남욱. (2017). “중소기업 기술보호지원제도에 대한 이용자와 정책담당자의 인식차이 분석”, 「디지털산업정보학회논문지」, 13(1):37-48

박성환. (2020). “금융기관의 정보보안문화와 경영진의 보안 리더십이 정보보안 행동에 미치는 영향”, 「석사학위논문」, 연세대학교 정보대학원.

박세락 · 이환수 · 박현애. (2020). “기술 보호 측면에서 보안교육실시빈도가 임직원 보안의식함양에 미치는 영향”, 「한국산업보안연구」, 10(1):55-79.

성욱준. (2018). “정보보호 침해 사고 발생과 복구의 영향 요인에 대한 연구”, 「한국지역정보화학회지」, 21(2):27-48.

소현철. (2018). “금융기관의 정보보호활동이 정보보호담당자의 보안자신감에 미치는 영향”, 「박사학위논문」, 호서대학교 대학원.

송재혁. (2021). “포스트 코로나 시대의 중소기업 산업정보 유출 방지를 위한 방안 연구”, 「석사학위논문」, 울산대학교 경영대학원.

송정석 · 전민준 · 최명길. (2011). “공공기관 정보보호 거버넌스 수준에 영향을 미치는 요인에 관한 연구”, 「한국전자거래학회지」, 16(1):133-151.

신진교 · 최영애. (2008). “중소기업의 R&D와 혁신-정부정책지원의 조절효과”, 「기업경영연구」,

15(1):119-132.
신혁. (2018). “계획행동 요인을 매개로 경영진 역할과 보호동기가 정보보안정책 준수에 미치는 영향”, 「박사학위논문」, 건국대학교 대학원.
안병구. (2018). “기업의 참여형 보안문화 프레임워크 개발 연구”, 「박사학위논문」, 중앙대학교 대학원.
안종하. (2013). “국내 사이버보안 체계 진단 및 정책적 대응방안 연구”, 「한국경찰연구」, 12(3):125-146.
이대권 · 양정훈 · 강원선 · 박준석. (2021). “산업보안 기술보호활동이 보안인식과 보안성과에 미치는 영향: 해외진출기업 (베트남) 을 중심으로”, 「한국산업보안연구」, 11(1):193-216.
이인선. (2021). “중소기업 정보보호 강화방안에 대한 연구”, 「석사학위논문」, 동국대학교 국제정보보호대학원.
이호준. (2020). “중소기업 산업보안 수준 개선에 관한 연구”, 「석사학위논문」, 동아대학교 대학원.
이흥배. (2022). “중소제조기업의 정보시스템 운영환경 요인과 성과와의 관계 연구”, 「박사학위논문」, 고려대학교 기술경영전문대학원.
정성배 · 박준석 · 최영호. (2015). “산업보안관리활동이 기업의 보안성과에 미치는 영향”, 「한국경찰연구」, 14(4):521-538.
차재원. (2016). “ISO 27001과 ISMS를 활용한 공공분야 보안관제 업무 향상에 관한 연구”, 「석사학위논문」, 건국대학교 대학원.

국외문헌

David, P., Hall, B., & Toole, A. (2000). Is public R&D a complement or a substitute for private R&D? A review of econometric evidence. *Research Policy*, 29(4-5):497-530.
Layton, T. P. (2015). *Information security awareness*, AuthorHouse.
Zahra, S. A., & Nielsen, A. P. (2002). Sources of capabilities, integration and technology commercialization. *Strategic Management Journal*, 23(5):377-398.

기타

국가사이버안전센터 홈페이지. http://www.ncsc.go.kr/
국가정보원 홈페이지. http://portal.nis.go.kr/
김평화 (2019. 11. 7.). 사이버 공격 피해 98%는 중소기업…"정부 · 기업 대책 시급하다". 「IT조선」, https://it.chosun.com/site/data/html_dir/2019/11/07/2019110700364.html
대·중소기업·농어업 협력재단. (2020. 2). 「2019년도 중소기업기술보호수준 실태조사 보고서」.
인터넷침해사고대응지원센터 홈페이지. http://www.krcert.or.kr/
중소기업 기술보호울타리 홈페이지. https://www.ultari.go.kr/portal/ptm/main.do
중소기업기술정보진흥원 홈페이지. https://www.tipa.or.kr/
한국정보보호진흥원 홈페이지. http://www.kisa.or.kr/

【Abstract】

The Impact of SMEs' Security Activities on Cyber Incident Response

Kim, Eun-Joung · Park, In-Chae

This study aims to propose an effective cyber incident response system for SMEs by understanding the impact of each security activity on cyber incident response. To investigate the impact of security activities on the establishment of a cyber incident management system, structural equation model is used with the 2019 SME technology protection level survey data set. In this research model, four independent variables presenting security activities (Govennance, People, Technology, Process for security) were selected and the level of cyber incident management system establishment was selected as a dependent variable. In addition, the moderating effect according to the management style of SMEs was analyzed.

As a result of the study, the security activities that have a high impact on the establishment of a cyber incident response system for SMEs were in the order of ‘asset management’, ‘IT management process’, and ‘system management process’. It is important that security infrastructure and security processes have a greater impact than security policies in terms of SME‘s cyber security activities that is a result contrary to previous studies that security policy has the greatest impact on the level of technology protection. The results from this study can contribute to establish standards for an effective cyber incident response system to SMEs in the future.

Key Words: Cyber Incidents, Cyber Incident Management System, SMEs’ Support Project, CISO(Chief Information Security Officer), Core Asset Management, Security Activities