박 사 학 위 논 문

중소기업의 보안 활동이 사이버 침해사고 대응체계 구축에 미치는 영향 연구

2023년

한성대학교 대학원
스마트융합컨설팅학과
스마트융합컨설팅전공
김 은 정

박 사 학 위 논 문
지도교수 박인채

중소기업의 보안 활동이 사이버 침해사고 대응체계 구축에 미치는 영향 연구

A Study on the Impact of SMEs' Security Activities on the Establishment of Cyber Incident Management System

2022년 12월 일

한성대학교 대학원
스마트융합컨설팅학과
스마트융합컨설팅전공
김 은 정

박 사 학 위 논 문
지도교수 박인채

중소기업의 보안 활동이 사이버 침해사고 대응체계 구축에 미치는 영향 연구

A Study on the Impact of SMEs' Security Activities on the Establishment of Cyber Incident Management System

위 논문을 컨설팅학 박사학위 논문으로 제출함

2022년 12월 일

한성대학교 대학원
스마트융합컨설팅학과
스마트융합컨설팅전공
김 은 정

김은정의 컨설팅학 박사학위 논문을 인준함

2022년 12월 일

심사위원장 이 석 기 (인)

심 사 위 원 이 상 복 (인)

심 사 위 원 박 상 선 (인)

심 사 위 원 천 성 용 (인)

심 사 위 원 박 인 채 (인)

국 문 초 록

중소기업의 보안 활동이 사이버 침해사고 대응체계 구축에 미치는 영향 연구

한성대학교 대학원
스마트융합컨설팅학과
스마트융합컨설팅전공
김 은 정

디지털 전환의 가속화로 인해 언제 어디서나 어떤 장치로나 인터넷에 접속할 수 있는 초연결 시대에 보안 위험이 다양해지고 고도화되어 사이버 침해사고에 대한 이해와 대응방안이 더욱 필요해졌다. 중소기업은 보안역량이 낮아 사이버 침해사고를 당할 확률도 높으며, 침해사고 후에도 사후 처리에 대한 투자범위가 제한적이며, 효율적인 대응이 어렵다.

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. 국내 중소기업을 대상으로 한 2019년도 중소기업 기술보호 수준 실태조사의 데이터를 SPSS 23.0과 AMOS 22.0.0을 이용하여 분석하고, 연구모형 및 가설을 검증하여 연구하였다. 연구데이터 적정성 검토를 위해 탐색적 요인분석을 한 후 그룹화된 요인분석과 신뢰도 분석을 하

였고, 측정 모델 검정과 구조 모델 검정을 수행하기 위하여 타당성 검증을 수행하였다. 연구모형과 연구가설 검증을 위하여 구조방정식 모형을 분석하였고, 조절변수의 효과는 χ^2 차이 검정 및 경로별 표준화경로계수를 비교하여 분석하였다.

분석결과는 사이버 침해사고 대응체계 구축에 영향도가 높은 보안 활동은 자산관리, IT관리 프로세스와 시스템관리 프로세스 순으로 나타났다. 보안 활동 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, 출입통제에서 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 보안 정책이나 보안 인식에 대한 투자를 장기적인 계획으로 수립한다면, 장·단기적으로 의미 있는 관리체계를 구축하는 것이라 할 수 있을 것이다. 장기적인 수행을 위해 정보보호 로드맵을 기반으로 중소기업지원사업의 수행 결과를 분석하고 미흡한 부분에 대한 지속적인 보완을 통하여 사이버 침해사고 대응체계를 구축하는 것이 필요할 것이다. 본 연구의 실증분석 결과가 정보보호 환경을 구축함에 있어 효과적인 중소기업 환경 맞춤형 사이버 침해사고 대응체계에 대한 기준을 수립하는 것에 도움을 줄 수 있기를 기대한다.

【주요어】 사이버 침해사고, 침해사고 대응체계, 중소기업 지원사업, 보안 책임자, 기업핵심정보 관리방식, 보안 활동

목 차

<표 목차>

<그림 목차>

Ⅰ. 서론

3.1. 연구의 배경 및 필요성

디지털 전환의 가속화로 인해 언제 어디서나 어떤 장치로나 인터넷에 접속할 수 있는 초연결 시대에 살고 있다. 또한, 코로나19 이후로 업무환경이 재택근무 등 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).

4차 산업혁명 시대가 도래한 지금, 기업 성장의 원동력이 되는 핵심기술 정보가 담긴 기업 자산에 대한 보호 역량은 기업의 중요한 경쟁력이 될 수 있다. 기업의 기술유출 및 탈취로 인한 피해를 줄이고자 정부에서도 다양한 정보보호 지원사업, 사후 대응전략 교육 등을 통해 정보보호 역량 강화를 도모하고 있다. 기업들의 정보자산 보안 강화를 위한 자체 노력과 정부의 다양한 지원사업 실시에도 불구하고 여전히 기술자료 유출 및 탈취는 일어나고 있다. 기업의 성장 및 발전에 있어 절대적 저해요인이 되는 기술자료 유출 및 탈취를 예방하고 방지하는 것은 각 기업 차원을 넘어 국가 차원에서 정책적으로 아낌없는 지원 및 보안 관련 법안 제정 등 제도적 장치 마련이 필요하다.

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 중소기

업은 보안역량이 낮아 사이버 침해사고를 당할 확률이 높으며, 중소기업 스스로 보안 인프라나 시스템 구축에 투자한다고 하지만 적절한 보안체계가 아닌 대부분이 사후 대응방식으로 급급하게 사업이 이루어지다 보니 투자의 범위가 제한적이며, 효율적이지 못하다(곽재연, 2019). 기업들, 특히 보안 인프라가 상대적으로 더 취약한 중소기업에게 실질적인 혜택과 도움을 줄 수 있는 정보보호 관리체계를 구축하기 위해서 중소기업의 기술유출 및 탈취 실태 파악, 실제 사이버 침해사고 피해사례 수집, 중소기업의 정보보호 역량 수준에 대한 평가, 진행되고 있는 중소기업 정보보호 지원사업의 실효성 분석 조사가 반드시 선행되어야 한다.

3.2. 연구의 목적

중소기업은 보안역량이 낮아 사이버 침해사고를 당할 확률도 높으며, 중소기업 스스로 보안 인프라나 시스템 구축에 투자한다고 하지만 적절한 보안체계가 아닌 대부분이 사후 대응방식으로 사업이 이루어지다 보니 투자의 범위가 제한적이며, 효율적이지 못하다. 이러한 중소기업의 현황에서 국내 중소기업이 사이버 침해사고에 유연하게 대응하기 위하여 보안체계의 보안 활동이 사이버 침해사고 대응에 미치는 영향을 파악하여 효과적인 사이버 침해사고 대응체계를 구축하는 방안을 제시하고자 한다.

본 연구의 목적을 제시하면 다음과 같다.

첫째, 중소기업의 기술유출 및 탈취 실태 및 중소기업의 정보보호 역량 수준을 선행연구를 통해 현재 중소기업의 산업보안 수준을 이해하고자 한다. 이를 통해 중소기업 사이버 침해사고의 특징을 파악하여 중소기업 사이버 침해사고의 대응을 위한 핵심요소가 무엇인지 제시한다.

둘째, 중소·중견기업의 산업보안 환경을 고려한 정보보호 관리체계를 구축하기 위하여, ISMS-P, ISO 27001, CSF 등의 정보보호 관리체계를 연

구하고, 효과적인 중소기업의 사이버 침해사고 대응체계 구축을 위한 보안요소를 도출하고자 한다.

셋째, 중소기업 기술보호수준 실태조사 데이터를 기반으로 효과적인 중소기업의 사이버 침해사고 대응체계 구축을 위한 보안 활동은 무엇인지 영향에 대해 실증 분석하고자 한다.

넷째, 중소기업의 사이버 침해사고 대응체계 구축에 있어 중소기업 지원사업의 수혜 여부, 보안책임자는 누가 수행하는지, 기업핵심정보를 어떻게 관리하는지에 따른 조절 효과를 연구하고자 한다.

본 연구는 중소기업의 정보보호에 대한 선행연구를 수행하고, 사이버 침해사고를 유연하게 대응하기 위하여 보안체계의 각 보안 활동이 사이버 침해사고 대응체계 구축에 미치는 영향을 분석하여 중소기업에게 효과적인 보안 활동이 무엇인지 제시하고자 한다. 이를 통해 인력 및 자금력이 상대적으로 부족한 중소기업이 효과적으로 중소기업 환경 맞춤형 사이버 침해사고 대응체계를 구축하여 중소기업의 정보보호 역량이 향상될 수 있기를 기대한다.

3.3. 논문의 구성

3.3.1. 연구방법

본 연구는 중소기업에서 보안 정책, 보안 인력, 보안 인프라, 보안 프로세스로 정보보호 관리체계를 구축함에 있어 각 보안 활동이 사이버 침해사고 대응에 미치는 영향을 검증하는 데 목적이 있다. 이를 위하여, 정보보안, 기술보호 및 기술유출 등 침해사고 대응에 대한 선행연구를 수행하였고, 중소기업의 정보보호 활동이 침해사고 대응체계 구축에 미치는 영향을 연구하기 위해 연구모형 및 가설을 도출하였다. 그리고 국내 중소기업을 대상으로 한 2019년도 중소기업 기술보호 수준 실태조사의 데이터를 SPSS 23.0과 AMOS 22.0.0을 이용하여 분석하고, 연구모형 및 가설을 검증하여 연구의 함의를 도출하였다. 연구데이터 적정성을 검토하기 위하여 탐색적 요인분석을 한 후 그룹화된 요인분석과 신뢰도 분석을 하였고, 측정 모델 검정과 구조 모델 검정을 수행하기 위하여 타당성 검증을 수행하였다. 연구모형과 연구가설 검증을 위하여 구조방정식 모형을 수행하였고, 조절변수의 효과는 χ^2 차이 검정 및 경로별 표준화경로계수를 비교하여 분석하였다.

3.3.2. 논문의 구성체계

이 연구의 구성은 총 5장으로 구성하였다. 제 Ⅰ장은 서론으로 연구의 배경 및 필요성, 연구의 목적, 논문의 구성이다. 제 Ⅱ장은 이론적 배경으로 중소기업 사이버 침해사고의 위험, 중소기업 측면의 사이버 침해사고 대응, 사이버 침해사고의 대응체계로 구성하였다. 제 Ⅲ장은 연구모형, 연구변수의 조작적 정의, 연구가설을 통하여 연구설계 하였다. 제 Ⅳ장은 설계한 연구모델을 실증분석하여 가설검증과 실증분석 결과를 제시하였다. 마지막 제 Ⅴ장은 이 연구의 결론 및 시사점으로 연구의 요약, 논의 및 시사점, 한계점과 향후 연구방향으로 구성하였다. 자세한 구성 내용은 [표

1-1]에서 정리하였다.

[표 1-1] 논문의 구성

<table>
<tr><th colspan="4">Ⅰ. 서론</th></tr>
<tr><td>연구의 배경 및 필요성</td><td colspan="2">연구의 목적</td><td>논문의 구성</td></tr>
<tr><td colspan="4">⇩</td></tr>
<tr><th colspan="4">Ⅱ. 이론적 배경</th></tr>
<tr><td>중소기업 사이버 침해사고의 위험</td><td colspan="2">중소기업의 사이버 침해사고 대응체계</td><td>선행연구의 분석과 연구의 차별성</td></tr>
<tr><td colspan="4">⇩</td></tr>
<tr><th colspan="4">Ⅲ. 연구설계</th></tr>
<tr><td>연구모형</td><td colspan="2">연구변수의 조작적 정의</td><td>연구가설</td></tr>
<tr><td colspan="4">⇩</td></tr>
<tr><th colspan="4">Ⅳ. 실증분석 및 결과</th></tr>
<tr><td rowspan="2">연구방법</td><td colspan="3">구조방정식모형을 통한 실증분석</td></tr>
<tr><td>측정항목 분석</td><td>가설검증</td><td>연구결과 분석</td></tr>
<tr><td colspan="4">⇩</td></tr>
<tr><th colspan="4">Ⅴ. 결론 및 시사점</th></tr>
<tr><td colspan="4">연구의 요약</td></tr>
<tr><td colspan="4">논의 및 시사점</td></tr>
<tr><td colspan="4">한계점과 향후 연구방향</td></tr>
</table>

Ⅱ. 이론적 배경

4.1. 중소기업 사이버 침해사고의 위험

4.1.1. 사이버 침해사고의 의미와 특징

사이버 침해사고는 사이버상에서 범죄로 규정되고 있는 행위뿐만 아니라, 법적으로 규제하고 있지 않은 행위까지 포함하여 모든 침해 행위를 말한다. 사이버범죄는 컴퓨터시스템을 이용한 수많은 유형의 범죄로 그와 관련하여 다양하게 발생하고 있어 단적으로 정의하기가 어렵다.

정보통신망법에서는 종전에는 침해사고를 구성하는 공격행위는 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법에 의한 것으로 한정되었으나, 2020년 6월 9일 개정법에 의하여 현행법과 같이 “정보통신망에 접근할 수 있도록 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법에 의하여 공격하는 행위”를 추가하고 있다. 이른바 백도어 설치행위 등으로 발생하는 사고가 기존법에서는 침해사고에 해당되지 않아 이에 대한 대응 및 관련 조치를 할 수 없다는 한계가 지적되면서 도입된 규정이다(한국인터넷진흥원, 2021.12).

본 논문에서는 정보통신망법의 정의를 기반으로 사이버범죄를 사이버공간 즉, 컴퓨터, 모바일, 네트워크 장치 등에서 발생하는 모든 범죄 활동으로 정의하고자 한다[표 2-1].

[표 2-1] 사이버 침해사고의 정의

구분	정의
정보통신망법	- 제2조 제1항 7. "침해사고"란 다음 각 목의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다. 가. 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법 나. 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법

구분	정의
한국인터넷진흥원 (2021.12)	- 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생하는 사태를 의미
구중모 (2020)	- 사이버환경 속에서 일어날 수 있는 모든 침해 사고 사건과 이로 인해 발생되는 모든 피해를 총칭
조호대 외 (2008.11)	- 법적으로 규제하고 있지 않은 행위들 중 침해하는 모든 행위를 포함하여 사이버상에서 범죄로 규정되고 있는 행위 연구
inet (2021)	- 정보통신시스템에 대한 비인가된 행위 또는 위협을 의미. 비인가된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행, 정보 서비스의 방해 등이 해당됨. 또한, 회사의 보안정책에 위반되는 행위 역시 침해사고로 정의

출처: 선행연구 논문을 토대로 연구자 정리

사이버 침해사고는 주로 다음과 같은 특징을 보인다.

첫째, 침해사고는 주로 네트워크 등 가상공간에서 발생하므로 피해자는 가해자가 누구인지 정확히 드러나지 않는 특성인 익명성과 비대면성을 가진다.

둘째, 사이버 침해사고의 원인을 분석하거나 대응이 어렵고, 사이버공간에서 이루어지므로 빠른 전파력과 천문학적 재산피해를 가져올 수 있다.

셋째, 현실 공간에서 벌어지는 사고와는 다르게 달리 피해자가 인지하기가 어려워 인지하여 대응하기까지 시간이 오래 걸리며, 원인을 규명하고 증거 확보를 하기가 여려운 특징이 있다.

넷째, 사이버 침해사고는 현실과 달리 인터넷이 연결된 디지털 환경이라면 어디에서든지 범할 수 있으므로 장소나 시간적인 제약이 없다(조호대, 박동균, 조현빈, 2008.11).

4.1.2. 사이버 침해사고의 유형

사이버 침해사고는 '우연한 사고로 인한 침해'와 '악의적 목적을 지닌 침해'로 분류가 가능하다(박도권, 2007). '우연한 사고로 인한 침해'의 경우는 주로 실수로 인해 발생하는 경우가 많다. 피해를 입히려는 의도가 없이 우연히 행한 행동들이 사이버 환경에서 피해를 입히거나 시스템을 마비시키는 등의 사고들이 이에 해당된다. 하지만 우연한 사고로 인한 침해는 악의적 의도

가 없기 때문에 반복성이 없고 경제적 피해를 야기하는 것이 목적이 아니기 때문에 기업에 큰 피해를 입히는 유형은 아니다. 하지만 '악의적 목적을 지닌 침해'는 문제가 되는 유형이라고 할 수 있다. 이러한 유형의 경우 목표 시스템의 취약점을 공격함으로써 시스템의 관리 권한을 획득하여 내부로 침입하고 시스템을 파괴하고 마비시켜 정상적인 서비스를 불가능하게 사고를 발생시키는 행동을 일컫는다. 이는 해킹, 컴퓨터 바이러스 유포, 스팸, 피싱, 산업스파이 활동 등 여러가지 양상으로 나타나고 있다. 이렇게 범죄의 양상이 다양화 되고 있기 때문에 이러한 피해를 입히는 원인을 사전에 파악하고, 이에 적합한 대응책이 필수로 수반되어야 한다(구중모, 2020).

통계청에서 발표한 정보보호 침해사고 대응지침에서 분류한 사이버 침해사고의 유형은 크게 공격 방식에 따라 악성코드공격, 서비스거부공격, 비인가접근공격, 복합구성공격 등으로 구분하였다[표 2-2].

[표 2-2] 사이버 침해사고 유형 분류1

구분	내용
악성코드공격	컴퓨터바이러스, 웜(Worm), 트로이목마, 백도어, 봇(Bot), 스파이웨어 등이 사용자 동의 없이 컴퓨터에 설치되어 사용자의 정보를 탈취하거나 오작동시키고 네트워크를 마비시킬 수 있는 악의적인 행위
서비스거부공격	시스템에 과도한 부하를 유발하여 정상적인 서비스를 불가능하게 차단하거나 성능을 저하시키는 공격
비인가접근공격	목표 시스템의 데이터 또는 기타 자원 등에 접근을 위해 인가 받지 않는 자가 관리 권한을 획득하여 논리적 또는 물리적으로 불법적으로 접근하는 공격
복합구성공격	악성코드공격, 서비스거부공격(DDos), 비인가 접근공격 등의 요소를 복합적으로 이용하는 공격유형

출처: 정보보호 침해사고 대응지침 (2012).

안철수연구소에서는 사이버 침해사고의 유형을 고객정보 및 기밀정보 유출(기밀성 침해), 서비스 지연 및 중단(가용성 침해), 침입에 의한 정보 변조(무결성 침해)로 구분하였다[표 2-3].

[표 2-3] 사이버 침해사고 유형 분류2

구분	주요 내용
고객정보 및 기밀정보 유출(기밀성 침해)	▪ 비인가된 시스템 접근, 파일접근, 네트워크 정보수집을 포함한 네트워크 정보의 접근을 통한 정보 유출 ▪ 정보에 접근 가능한 내부자 또는 외부자에 의한 고객정보, 회사 기밀정보를 보유한 시스템의 해킹으로 인한 정보의 유출 ▪ 중요 장비 또는 정보 저장 매체(디스크, CD, USB 등)의 도난 또는 불완전한 폐기로 인한 정보의 유출 ▪ 도청, 감청, 네트워크 스니핑에 의한 정보의 유출 ▪ 외부 협력업체를 통한 정보의 유출
서비스 지연 및 중단(가용성 침해)	▪ 웜/바이러스, 트로이목마, 백도어 등의 악성코드를 유포 및 실행시켜 피해를 일으키는 공격에 의한 서비스 중단 ▪ 정보자산에 대한 물리적인 손상에 의한 서비스 중단 ▪ 서비스 거부(DoS) 공격, 웜/바이러스로 인해 정보자산의 일부/전체 서비스 중단
침입에 의한 정보 변조(무결성 침해)	▪ 고객 정보 및 기밀정보를 내부자 또는 외부자가 승인을 받지 않고 의도적으로 조작 ▪ 거래정보, 계좌 정보 등 중요정보를 보유한 시스템에 대한 해킹 ▪ 인터넷 서비스 관련 배너 정보의 변경

출처: 안철수연구소 (2007).

임채태(2012)는 해킹 동기가 과거엔 호기심, 자기과시형(2000～2004) 이었고 최근에는 기존 범죄조직과 연루된 범죄형 해킹과 금전적 이득이 목적인 공격(2004～현재)이 두드러진다고 보았고, [표 2-4]과 같이 정치·사회적 목적, 금전적 이득 목적, 범죄형 침해사고 등으로 나누었다.

[표 2-4] 사이버 침해사고 유형 분류3

구분	방법	국내 사례
정치·사회적 목적	▪ 전산망 장애 발생	▪ 농협 디도스공격 ▪ 한일 사이버전쟁
금전적 이득 목적	▪ 서버 다운 협박 ▪ 중요정보 거래 ▪ 금융범죄 위한 정보수집 수단	▪ SK커뮤니케이션즈(3,500만), 현대캐피탈(175만) ▪ 중국해커, 서버다운 협박으로 금품 갈취
범죄형 침해사고	▪ 경쟁사 서버 디도스공격 ▪ 경쟁사 사이트 부정클릭 ▪ 경쟁사 전산망 임의 침입	▪ 중국 해커 통한 경쟁사 서버 공격 ▪ 부정 클릭으로 포털 광고비 과다 지급유발 ▪ 보험사 긴급 출동업체 정보 임의 변경

출처: 임채태 (2012). 재구성.

또한, 목적 측면에서 사이버 침해사고를 구분하면 크게 정보를 탈취하기 위한 목적의 침해사고와 시스템을 마비시키기 위한 침해사고로도 분류할 수 있다(구중모, 2020). 기업에서 주요 자산을 어떤 관점에서 관리할 것인가를 고려한다면 사이버 침해사고를 어떻게 구분하여 관리할지도 판단할 수 있을 것이다.

최근 발생하고 있는 침해사고는 지능형지속공격(Advanced Persistent Threats, APT)의 형태를 가지고 있다. 지능형 지속공격은 공격 의도를 가진 공격자가 공격대상을 선정한 뒤 지속적으로 공격하는 공격 방식이다. 이는 지속적으로 목표대상을 감시하여 가장 취약한 지점에 대한 초기 침해를 성공시킨 후 이를 통해 점유한 컴퓨터에 접근할 수 있는 명령제어 체계를 구축하고, 동일 네트워크에 위치한 공격대상 컴퓨터로의 내부이동, 정보탈취, 시스템 파괴 등의 일련의 작업을 수행하게 된다. 이런 침해사고는 복합구성공격의 유형으로 더욱 복잡해지고 장기화된 공격형태를 띤다.

4.1.3. 중소기업의 사이버 침해사고 연구

2009년 이후 2018년까지 산업기술 유출이 증가하였으며, 기술유출 예상 피해액이 50조 원에 달하였다. 2013년 이후 중소기업 기술유출 건수 감소하였으나, 2017년에 다시 증가하는 것으로 보인다(국회정보위원회, 2019). 특히, 5G, 인공지능 등 4차 산업혁명의 확산과 비대면 경제의 활성화 등으로 우리 사회와 산업 전반에서는 디지털 대전환이 빠른 속도로 진행되고 있다. 무인상점 해킹, 인공지능을 활용한 공격 등과 같은 새로운 보안 위협이 증가하고 있어 정보보호를 필요로 하는 영역이 확대되고 있다(한국인터넷진흥원, 2021.12). 사이버 침해사고를 효과적으로 대응하기 위한 개인정보보호법 등 관련 법률이 재개정 되었음에도 불구하고 정보보호의 사각지대에 놓여 있는 기업이 대다수이고, 업종 등 기업의 특성에 따라 정보보호 수준의 편차가 크다는 사실을 알 수 있다(김용재, 2017).

국내 중소기업의 사이버 침해사고 현황을 파악하기에 앞서 사이버 침해사고에 대하여 선행연구하였고, [표 2-5]와 같이 정리하였다. 업무환경 측면에

서는 주로 금융권, 클라우드, 모바일 등에서의 침해사고에 대한 연구가 되었고, 조직 기반 측면에서는 조직원의 보안인식에 따른 영향도 등에 대한 연구가 다수 수행되었다.

[표 2-5] <사이버 침해사고>에 관한 선행연구

구분	연구자(연도)	연구내용
업무환경 기반 연구	김양훈 (2014)	- 핵심기술 유출기업군과 일반기업군들 사이의 보안역량을 측정하고 상관관계를 실증분석
	김영근 (2018)	- 클라우드 환경에 대한 정의를 기반으로 클라우드 환경에서 더욱 중요시되고 있는 Shadow IT 와 내부자 위협에 대한 연구
	김용재 (2017)	- 기업의 정보보호 수준과 직결되는 정보보호 교육 및 정보보호 점검 활동을 정보보호 활동으로 명명하고, 이에 영향을 미치는 요인을 규명
	박병우 (2018)	- 기업의 BYOD 환경에서 모바일 오피스 정보보안에 대한 고찰을 통해 모바일 오피스 정보보안 대응방안을 연구
	서동진 (2016)	- '2014 중소기업 기술 보호 역량 및 수준 조사'에서 수집된 데이터를 활용하여 기술유출방지 경영검토, 특허활동, 연구개발 활동 등에 따라 국내 기업의 기술 보호 역량에 영향을 주는 요인
	소현철 (2018)	- 금융기관의 정보보호 활동 중 어떤 활동이 보안담당자들의 보안자신감에 영향을 미치는지와 임직원 및 경영진의 정보보호의식이 보안자신감에 미치는 매개효과를 연구 실증분석
	왕린린 (2019)	- 중국의 실제 상황에 기초하여 정부지원금, 수명주기 단계 및 기업숙성에 따른 기업 연구개발 투자가 기업 경영성과와 기업가치에 미치는 영향 연구
	우순규 (2018)	- 금융산업에서 개인정보 비식별 조치를 위하여 국내·외 비식별 조치에 대한 사례와 제도, 기술 및 정책동향과 실태를 조사·연구
	유인진 외 (2018)	- 중소기업의 기술유출에 대해 정보보안 및 기술보호 관련 정책에 대한 접근을 통해 보다 효율적인 대안 제시
	윤태호 (2019)	- 인터넷전문 은행 서비스에 대한 최근 핀테크 관련 분야에 많이 활용되고 있는 통합기술수용 이론을 바탕으로 위험요인인 인지된 위험과 혁신저항을 추가하여 수용의도와 이용에 영향을 미치는 요인 분석
	이길호 (2019)	- 공공기관, 일반기업, 중소기업 등 보안성 향상을 위한 사이버 침해사고 예방을 위하여 정보보호 취약점 개선 및 효율적인 개인정보보호 관리 관련 연구
	이대권 외 (2021)	- 베트남의 해외진출기업을 중심으로 기업의 핵심정보 유출을 예방하고 보안 인식과 보안 성과를 제고하기 위한 방안을 제시
조직 기반 연구	김택영 외 (2020)	- 외부 연구자가 접근할 수있는 언론 매체 및 정부의 보도 자료를 통해 2005년부터 2019년까지 발생한 개인정보 유출 사고에 대한 정보를 수집하고, 개인정보유출사고 요소간의 관계와 기업의 특성간 영향관계 분석

구분	연구자(연도)	연구내용
	김택영 (2021)	- 이성적 행동 이론, 계획 행동 이론, 기술 수용 모형에 기안하여 연구모형을 설계 연구
	박세락 (2020)	- 보안교육 빈도와 보안역량 또는 보안의식 제고와의 관계를 검증하는 연구 필요성을 제기
	박재곤 (2016)	- 조직화이론 관점에서 내부자 보안위협에 대한 보안성과에 미치는 영향을 구조방정식모형을 통한 실증분석
	신현구 (2015)	- 산업기술 보유기관 보안담당자를 대상으로 보안정책 준수의지의 인과경로를 규명함으로써 효과적인 인적 경영을 위한 방향성 제시
	하태경 (2019)	- 온라인 서비스의 사용자 보안인식과 정보보안제도가 개인정보 제공의도에 미치는 영향을 파악 위해 사용자 보안인식과 이용갈등, 정보보안제도와 대한 지각된 신뢰성을 검증 및 개인정보 제공의도를 확인
	황성민 (2018)	- 보안관제에서의 보호동기요인들에 대해 파악하고 이들 요인이 자기효능감과 보안신뢰를 통하여 정보보안성과에 대한 영향요인 실증 검증

출처: 선행연구 논문을 토대로 연구자 정리

중소기업이 사이버 침해사고를 예방하고 침해사고 이후에도 내부적·외부적으로 유연하게 대처할 수 있으려면, 먼저 중소기업의 정보보호 현주소는 어떻게 되는지 알아볼 필요가 있다. 그리고 중소기업의 사이버 침해사고의 특징을 파악하여야 효과적인 대응방안을 찾을 수 있을 것이다.

2009년 이후 2018년까지 산업기술 유출이 증가하였으며, 기술유출 예상 피해액이 50조 원에 달하였다. 2013년 이후 중소기업 기술유출 건수 감소하였으나, 2017년에 다시 증가하는 것으로 보인다. 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 악

성 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).

국내 산업보안 중에서도 중소기업을 대상으로 피해실태와 보안예산 편성 등의 조사가 실시된 적은 거의 없어 정확한 현황과 피해 상황은 파악이 어려운 것으로 보인다. 하지만, 2020년 중소기업 기술보호수준 실태조사 자료를 보면 아래 [표 2-6]와 같이 중소기업의 기술보호 역량점수는 48.6점으로 나타난 것에 비해 상대적으로 낮게 조사되었다. 기업규모, 매출액, 종업원 수가 적을수록 기술 보호 수준 평가점수도 낮았으며, 영세한 중소기업일수록 산업보안에 대한 관리, 예산, 조직, 인력에 대한 투자는 미비한 것으로 나타났다. 특히, 10인 미만의 소규모 기업은 50점 미만으로 결과가 나타나서 보안 역량이 상당히 낮은 수준에 있음을 알 수 있다. 중소기업의 평가부문별 역량점수는 '기술보호 정책(57.2점)'이 가장 높고, 다음으로 '물리적 보호방안(49.6점)', '사고/재해 관리(47.8점)' 등의 순으로나타났다. 중견기업, 대기업 대비 중소기업 상대지수가 가장 큰 부문은 '기술보호 정책'으로 정책이 잘 수립되어 역량점수가 높은 것으로 보여지나, '물리적 보호방안' 이나 '사고/재해 관리'가 상대적으로 낮은 원인도 있다고 판단된다.

[표 2-6] 중소/중견/대기업 역량점수 및 상대지수 결과

구분	중소기업 점수(점)	중견기업 점수(점)	대기업 점수(점)	중견기업 대비 중소기업 상대지수(%)	대기업 대비 중소기업 상대지수(%)
종합	48.6	64.3	69.4	75.7	70.1
기술보호 정책	57.2	64.5	70.2	88.7	81.4
관리적 보호방안	40.1	56.1	60.7	71.6	66.1
물리적 보호방안	49.6	70.4	79.2	70.5	62.7
기술적 보호방안	47	68.1	69.8	69	67.3

구분	중소기업 점수(점)	중견기업 점수(점)	대기업 점수(점)	중견기업 대비 중소기업 상대지수(%)	대기업 대비 중소기업 상대지수(%)
사고/재해 관리	47.8	70.8	76.7	67.6	62.4

* 중견기업 대비 중소기업 상대지수 = (중소기업 역량점수/중견기업 역량점수)*100
* 대기업 대비 중소기업 상대지수 = (중소기업 역량점수/대기업 역량점수)*100
출처: 2020년 중소기업 기술보호수준 실태조사 (2021).

중소기업에 대한 공격이 위협적인 이유는 하청업체가 많은 중소기업의 특성상 이들 기업에 대한 해킹은 결국 정부 혹은 대기업에 대한 해킹으로 이어지기 때문이다. 최근 정부 기관 등을 목표로 발생한 해킹 시도 역시 소규모 외주업체의 보안 취약점을 노린 공격으로 전문가들은 분석했다. 2022년 9월 전쟁기념관 침해사고는 해커 공격으로 일주일간 홈페이지 등 전산망이 마비됐는데 이 역시 그동안 전산망 서버를 관리했던 민간 용역업체의 보안 취약점이 드러난 것으로 업계는 추정하고 있다. 인력과 보안투자가 가능한 대기업과 정부 주요 내부망 같은 경우는 사이버 침해사고에 비교적 대응이 용이하나, 이들과 연관된 중소기업의 보안이 허술하면 보안피해를 피해가기는 어렵다. 주로 협력업체를 통해 주요 정보가 새어 나가기도 하기 때문에 결국 중소기업 보안이 강화되어야 정부와 전체 산업 보안도 강화될 수 있다고 할 수 있다. 이렇듯 중소기업의 사이버 침해사고는 중소기업 내의 문제뿐만이 아니라 협업을 하는 대기업, 공공기업에도 많은 영향을 미치는 것으로 나타났다(이소연, 2022).

국내 중소기업의 사이버 침해사고의 특징을 파악하기 위하여 중소기업 사이버 침해사고의 주요 원인을 알 필요가 있다. 2019년 중소기업 기술보호수준 실태조사에서는 중소기업의 기술유출 사고가 발생하는 주된 이유에 대해 '보안관리 감독체계 미흡(34.9%)' 응답이 가장 많고, 다음으로 '임직원들의 보안인식 부족(32.4%)', '보안 관련 투자 미흡(30.6%)' 등의 순으로 나타났다[표 2-7]. 이러한 결과는 중소기업이 대기업에 비해 기술유출에 관한 경각심이 부족하거나 안이한 대처를 하고 있음을 의미하고, 손실에 대한 고려 없이 비용, 예산 등을 이유로 보안업무에 투자를 하지 않고 있음을 의미한다. 또한, 내부자를 통한 기술 유출도 많은데, 이 이유도 기업이 직원 대상으로

보안교육에 대한 투자가 미흡한 현실을 반영한다(송재혁, 2021).

[표 2-7] 기술유출 사고 발생 주된 이유(2017~2019년)

구분	2017년	2018년	2019년
보안관리, 감독체계 미흡	46.5	44.4	34.9
보안 관련 투자 미흡	11.6	24.5	30.6
보안전담 인력의 부재	3.8	14.5	21.7
임직원들의 보안의식 부족	23.5	35.9	32.4
개인의 금전적 이익추구	5.1	20.2	29.6
회사의 처우에 대한 불만	3.1	17	15.4
회사 운영난에 따른 감원 등 직업 불안정	3	5.9	12.9
기타	1.5	0.3	0.1

출처: 2019년 중소기업 기술보호수준 실태조사 (2020).

또한, 중소기업 정보유출 원인 중 국가 차원의 기술보호 종합시스템 및 체계적 관리 부재도 주요 원인으로 파악된다. 중소기업 산업기술 보호 정책을 살펴보면 여러 부처에서 많은 정책적 방안을 제공하고 있지만, 기업에서는 정책에 대한 인지를 제대로 못하고 있는 실정이다. 이러한 점에서 정부 차원의 산업기술보호 체계가 제 역할을 못하는 것으로 파악할 수 있다. 이와 관련하여 조사결과에 따르면 기업 입장에서의 각종 지원정책에 대한 기업 인지도는 24.5%로 낮은 상황이다(고찬석, 2021). 2020년 중소기업 기술보호수준 실태조사에 따르면 중소기업 정보보호 담당자의 사이버 침해사고 대응을 위해 시급하다고 느끼는 부분 중 '중소기업 기술보호 지원정책 마련'도 포함된다[표 2-8].

[표 2-8] 중소기업 기술자료 유출 및 탈취 방지를 위해 시급한 부분

구분	결과(%)
자체적인 보안 노력	37.1
안전한 기술거래 계약 체결	15.1

구분	결과(%)
공정기술거래 환경 조성	12.3
강력한 법제도 마련 및 처벌	22.7
중소기업 기술보호 지원정책 마련	12.7

출처: 2019년 중소기업 기술보호수준 실태조사 (2020).

기술유출 사고가 발생하는 이유로는 임직원들의 보안의식 부족(1순위: 38.8%), 보안관리/감독체계 미흡(2순위:29.7%), 보안 관리투자 미흡(3순위: 9.9%), 회사처우에 대한 불만(4순위:7.7%), 임직원 금전적 이익 추구(5순위: 6.7%), 회사운영난에 따른 감원 등 직업불안정(6순위: 5.3%) 순으로 나타나고 있다(김태형, 2019). 이러한 중소기업의 사이버 침해사고 관련 선행연구는 아래와 같이 정리하였다[표 2-9].

[표 2-9] <중소기업보안>에 관한 선행연구

구분	연구자(연도)	연구내용
보안 정책 연구	김미래 (2018)	- 개인정보 유출사고가 발생하는 원인분석과 해당 원인으로 분류되는 주요 보안 위협을 선정하고, 보안 위협을 법적으로 제재할 수 있도록 기술적 보호조치 대응규제 제시
	김태형 (2019)	- 현재 중소기업 산업보안의 현 수준과 보안 방법론에 대해 언급하고 국가 지원 정책 및 법률의 실효성에 대한 문제점을 찾아 강화 방안들을 연구
	최성욱 (2016)	- 국내외에서 운영 중에 있는 산업보안관련 정책을 알아보고, 국내 중소기업의 산업 보안정책 문제점을 해결하기 위한 과제로 국가 기술보호통합센터 설립을 중심으로 국내 중소기업 산업보안방안에 대한 단계적 지원방안을 제시
	홍준석 (2021)	- 중소기업 임직원들의 정보 보안 정책 준수에 영향을 미치는 인자들을 선택하였고, 이를 바탕으로 정보 보안 수준을 향상시킬 수 있는 인자에 대한 연구
보안 인프라 연구	김신석 (2020)	- 중소기업에 맞는 개인정보 기술적 보호조치 방안을 제시하고, 중소기업 중 온라인쇼핑몰에서 수집 및 사용하고 있는 개인정보, 개인정보 사용 환경을 분석하여 이에 대한 개인정보 보호조치 방안을 제시
	이찬우 (2018)	- 중소·중견기업의 기술유출방지를 위한 디지털 정보 분석 기반의 객관화된 보안수준 평가를 지원할 수 있는 자동화 진단 도구를 제시

구분	연구자(연도)	연구내용
보안 프로세스 연구	유정은 (2017)	- 기존의 내부자 중심 기술유출 방지 방안의 한계점, 중소기업과 협력업체 간 기술유출을 분석하여 협업 프로세스 개선방안 제시
정보보호 성과 연구	김경선 (2016)	- 기술보호활동의 영향요인과 기술보호 성과, 기술보호 및 지식재산권화 활동과 기업성과를 연구
	박상복 (2022)	- 중소기업의 보안수준 향상을 위한 우선순위 항목에 대한 타당성 검증 및 중소기업의 보안수준 향상을 위한 우선순위 항목 도출
	이홍배 (2022)	- 정보시스템 운영 환경이 정보시스템 품질 수준과 순차적 매개변수인 기업 생산성을 거쳐 BSC성과에 미치는 영향에 관하여 구조 모형을 이용하여 실증적으로 분석
	장동원 (2020)	- 자산이 IT서비스 가치에 영향을 미치는 관계를 연구
	조재완 (2022)	- 중소기업의 ESG 경영환경에 따른 보안관리체계를 연구하고자 하고 전문가 인터뷰를 통해 도출하고 타당성 검증한 주요항목에 대한 중요도를 선정
	최영환 (2019)	- 6개 Domains (조직, 시스템, 프로세스, 통합, 설비, 그리고 Data)를 포함하고 있는 새로운 스마트 팩토리 운영시스템 성숙도 수준평가 모델을 제안
	한규왕 (2017)	- 자율점검 체크리스트를 통하여 기본적인 보안환경을 조성하고 중소기업의 정보보안 보호수준을 높이기 위해 체크리스트를 개발
	박양모 (2017)	- 중소기업의 정보보호 위험 요소 분석하고, 중소기업 특화 정보보호 점검 항목 선별 및 타당성 조사

출처: 선행연구 논문을 토대로 연구자 정리

김경선(2016)은 기술보호 성과를 위한 기술보호 활동을 기술보호 노력 정도에 따른 매개효과 중심으로 연구하였고, 이홍배(2022)는 중소기업의 성과를 위하여 조직원의 교육, 정보보안 등 중소제조기업의 정보시스템 운영환경 요인과 성과와의 관계를 연구하였다. 이와 같이 중소기업보안 관련 선행연구는 보안 정책과 정보보호 성과에 관한 연구가 주로 수행되었으며, 정보보호 성과 관련 연구도 보안활동이 조직의 구성 인력에 집중된 정보보호 노력 정도나 정보보호 인식향상 등의 연구가 주로 수행되는 것으로 확인하였다. 중소기업의 보안체계 향상을 위하여 중소기업 특성을 고려한 구체적으로 세분화된 중소기업의 보안 활동 분석은 부족한 것으로 파악되었다.

4.2. 중소기업의 사이버 침해사고 대응체계

4.2.1. 사이버 침해사고 대응체계 연구

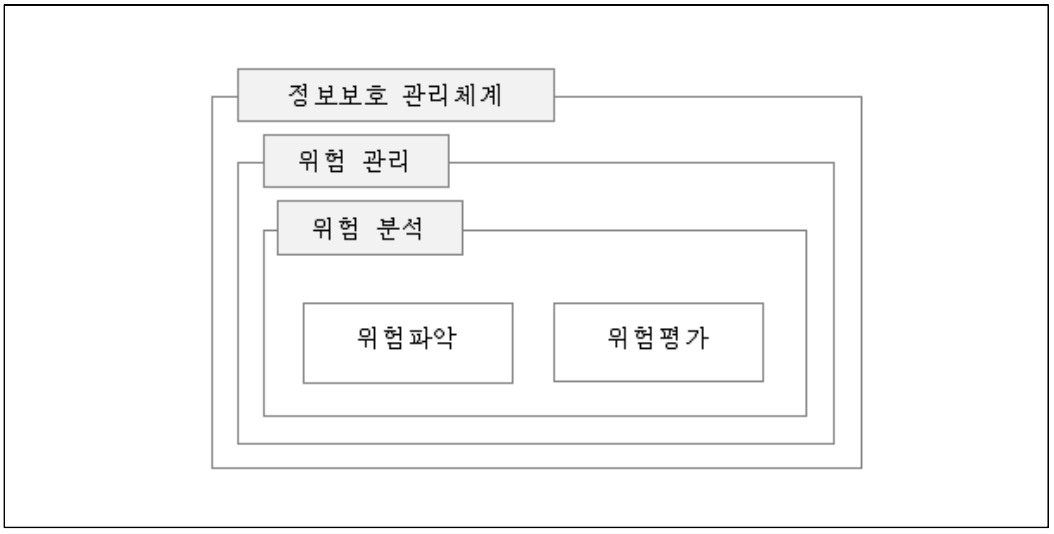
사이버 침해사고를 효과적으로 대응한다는 의미는 무엇인가. 사이버 침해사고 대응방안을 이야기하기에 앞서 대응방안이 적절한지, 효과적인지를 판단할 수 있는 기준이 필요할 것이다. 미국 연방정부 보안수준은 효과성(Effectiveness), 효율성(Efficiency), 책임 추적성(Accountability), 법적준수사항 확인(Compliance) 등이다[표 2-10](안종하, 2013). 계량화된 보안통제는 조직의 보안 역량으로 나타나는데, 이는 주어진 보안통제의 수량 중 효과적인가, 효율적인가, 책임 추적성이 있는가, 법적준수사항이 이행되고 있는가의 여부를 보안통제로 나누고 백분율을 하여 표준점수(Normalized degrade)로 산정한다.

[표 2-10] 미국 연방정부 보안수준 평가기준

평가항목	내용
효과성(Effectiveness)	적용한 통제 적절성 파악
효율성(Efficiency)	적용한 통제 성능여부 파악
책임 추적성(Accountability)	통제가 적절치 못할 경우 개선여지 파악
법적준수사항 확인(Compliance)	법에서 요구사항 준수여부 파악

출처: 안종하 (2013). 국내 사이버보안 체계 진단 및 정책적 대응방안 연구

기업에서 발생하는 사이버 침해사고를 효과적으로 대응 및 관리하기 위하여 위험을 분석하고 식별한 위험을 우선순위로 위험을 관리하는 정보보호 관리체계를 구축하는 것이 중요하다(김민수, 2014). 조직의 자산에 대한 위험을 관리할 수 있는 수준으로 유지하기 위하여 자산에 대한 위험을 분석하고, 보호되어야 할 자산과 조직의 위험을 측정하고 측정된 위험이 허용 가능한 수준인지 아닌지 판단하여 위험을 관리할 수 있는 기준을 만들어야 한다[그림 2-3].



[그림 2-1] 보안관리의 구성

출처: 김민수 (2014)

침해사고는 예측하기 어렵기 때문에 불시에 일어날 수 있는 침해사고 또는 실시간 이루어지는 침입에 대해 선제 대응을 하기 위해 준비가 필요하다. 조직의 위험을 분석하여 위험을 관리할 수 있는 보안정책과 전문적인 보안 인력, 보안 인프라, 보안 프로세스 등의 방법론을 가지고 상시 발생할 수 있는 위협에 대해 유연하게 대응할 수 있는 정보보호 관리체계가 필요하다. 단순히 보안 인프라의 구축만으로 보안성을 높일 수 없는 이유가 정보보호 관리체계를 구축하여 체계적으로 이루어진 관리활동이 필요하기 때문이다. 따라서 침해사고를 예방하기 위해서는 효율적인 정보보호 관리체계가 필요하다.

중소기업이 보안역량을 확보하고 기술보호역량을 키우기 위하여 효과적인 정보보호 관리체계를 기반으로 초석을 마련하는 것이 필요하다. 보안은 일반적으로 관리적 보안, 물리적 보안, 기술적 보안으로 구분하여 관리한다. 이를 기반으로 정보보호 관리체계 인증(ISMS-P), 국제표준 정보보안경영시스템 인증(ISO 27001), NIST의 사이버보안 프레임워크(CSF) 등 다양한 표준 또는 인증체계로 정보보호 관리체계를 제시한다. 이런 관리체계를 중소기업에 효과적으로 적용하기 위하여 아래와 같이 선행연구를 하였다[표 2-11].

[표 2-11] <정보보호 관리체계>에 관한 선행연구

연구자(연도)	연구내용
강만성 (2018)	- 기업이 물리적 보안수준을 평가하여 보안수준의 향상과 효율적인 보안관리가 가능하게 할 수 있도록 객관적이고 수치화된 기업의 보안수준 평가지표 개발
김광민 (2019)	- 중소·중견기업의 산업보안 환경을 고려한 정보보호 관리체계에 대한 조사 및 분석을 통해 중소·중견기업에 특화된 정보보호 관리체계 모형을 개발하고 지속적으로 관리할 수 있는 맞춤형 정보보호 관리체계 제시
김동희 (2019)	- 국내·외 정보보호 이슈와 정보보호 관련 법·제도를 파악하여 국내 정보보호 관리체계에 대한 통합 개선제도를 구현하기 위하여 정보보호 관리체계 통합개선 제도 구현
박윤식 (2018)	- 국내외 정보보호 관리체계 중 ISMS, ISO27001을 선정하여 공통된 통제항목을 비교·분석하고, 한계점을 찾아 반도체 산업에 적용하기에 필요한 S-ISMS (Semiconductor - ISMS)를 제안
김이헌 (2021)	- 실제 중소기업 대상 정보보호 관리체계 컨설팅 결과를 바탕으로 중소기업의 특성을 고려한 정보보호 관리체계 평가 모델 개선
박장영 (2018)	- ISO 22301 운영전략 8대 자원 요구사항을 중심으로 기업의 산업분야를 제조업, 비제조업에 따라 재난 발생 시 신속한 업무 재개를 위해 중요시하는 자원의 중요도에 차이가 있음을 검증
박재성 (2022)	- 국내 대표적인 정보보안 제도인 ISMS 와 정보통신기반 보호법(주요정보통신기반시설 취약점 분석평가)을 비교하여 중소기업을 대상으로 한 정보보안 요건을 도출하여 예산과 인력을 기준으로 정보보호 관리체계 점검항목을 제안
박종승 (2020)	- 국내·외 정보보호 관리체계를 연구하여 스마트워크 정보보호 감리 모형 연구
박찬규 (2021)	- 재택근무를 시행하는 중소기업의 재택근무환경 보안실태를 파악하고, ISMS-P와 주요정보통신기반시설 취약점 분석평가를 참고해 보안 위협에 대한 점검항목을 연구하여 업무 PC의 재택근무에 적합한 보안 점검항목 도출
안종훈 (2021)	- ICT 공급망 위험도 영향평가 결과에 따라 사이버보안프레임워크(CSF, Cyber Security Framework)와 NIST SP800-161 (연방정부기관 ICT 공급망 보안관리 지침)의 보안 통제항목을 이용하여 효과적인 공급망 위험 통제 방안 연구
이병주 (2019)	- 침해사고 대응을 위해서 정보보호 관리체계(ISMS)와 ISO27001을 기반으로 디지털 포렌식 지침 적용 수행에 대하여 연구하고 정보보호 관리체계의 절차 및 통제항목을 점검하여 디지털 포렌식에 적합한 점검 항목 제안
오은 (2016)	- 금융 산업의 특성을 반영하기 위해 금융 IT・정보보호 관련 법규에서 도출한 신규 통제항목을 SMS, PIMS, PIPL 등 정보보호 인증제도 통합모형에 추가하여 금융권 정보보호 관리수준 평가모형 제안
이호준 (2020)	- 기술보호 지침과 산업기술 보호지침, ISMS 등의 통제항목을 연구하고, 국내 기업들 중 중소기업의 산업보안 수준을 강화시킬 수 있는 방안을 제공하기 위하여 자율점검 체크리스트 개발하여 제시
조경재 (2018)	- 콜센터에 적용되어야 할 정보보호 관리체계 항목을 파악하기 위해 콜센터 전문가 및 정보보호 전문가의 두 집단으로 구성하여 각 집단에서 중요하게 판단하는 정보보호 관리체계의 13개의 정보보호대책 관리항목의 우선순위를 분석
주영국 (2020)	- 2011년 이후에 발생한 정보보안 사고 사례를 분석하고, 원인을 파악하여, 정보보안 위협 사항을 제거하기 위한 정보보안 사고 기반의 평가항목 제안

연구자(연도)	연구내용
차재원 (2016)	- 공공분야 보안관제 업무향상을 위한 지표나 표준 통제항목을 연구하여 보안관제 전문업체 지정심사 기준과 보안관제 수행능력 평가를 개발
황연석 (2016)	- 정보보호 준비도 평가와 미국의 정보보호 성숙도 모델(C2M2)을 비교 분석하여 기존의 정보보호 준비도 평가의 제한사항을 고찰하고 개선방안을 모색하여 정보보호 준비도 평가의 개선방안 연구

출처: 선행연구 논문을 토대로 연구자 정리

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 선행위협 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. 다양한 사이버 침해사고 대응방안에 대한 선행연구는 아래와 같이 정리하였다[표 2-12].

[표 2-12] <사이버 침해사고 대응방안>에 관한 선행연구

구분	연구자(연도)	연구내용
관리체계 제시	강신범 외 (2012)	- 기업이 실질적인 정보보호 목표 수준을 준수하기 위하여 필요한 효과적인 기업의 침해사고 예방을 위한 관리 모델 제안
	구중모 (2020)	- 국내 침해사고 특징과 침해 사고 대응 시 문제점 및 한계와 침해 사고 대응 업무 체계 향상 방안 연구
	권재성 (2021)	- 보안전문가 FGD 및 기업 보안담당자들 대상 설문조사를 통해 재택근무 환경에서 정보유출 위험도와 관련 보안위협의 변화, 정보유출 위험에 대응하기 위해 강화되어야 할 보안대책 항목들을 실증적으로 파악

구분	연구자(연도)	연구내용
	안종하 (2013)	- 사이버보안 사고를 진단하고 국가 차원의 정책적 대응전략을 연구하여 국내 사이버보안 체계 진단 및 정책적 대응방안 연구
원인분석에 따른 대응방안	김기윤 (2019),	- 기업이 이미지를 회복하기 위해 사전적으로 기업의 보안 수준과 사후적으로 기업의 유출통지 활동에 따라서 소비자의 행동에 미치는지 영향 연구
	김지수 (2017)	- 개인정보 유출사고 발생 시 기업들이 행하게 되는 대응활동에 기반을 두고 직접적으로 산출이 가능한 모든 피해액 산출요소를 계산함으로써 보다 정확하고 현실적인 모델 제시
	박관수 (2019)	- 산업 환경에서의 IoT 침해 대응 현황과 현재 스마트 홈 환경에서 침해 대응 현황을 비교 분석
	백성현 (2019)	- 사이버 침해사고에 대해 세부 피해 요소에 대한 계산식을 대입하여 호스팅 사업자와 이용자에게 발생하는 피해액을 더하여 총 피해액 산출
	성욱준 (2018)	- 정보보호 침해사고 발생과 복구에 영향을 미치는 요인에 대한 경험적 연구
	신혜은 (2016)	- 최근 년간 금융기관에서 일어났던 개인정보 유출 현황 및 개인정보 유출 문제점을 바탕으로 개인정보 유출의 대응방안 제시
	위초롱 (2017)	- 유출의 원인을 중심으로 개인정보 유출 상황에서 나타나는 고객의 부정적 감정과 행위 연구
	유하랑 (2020)	- 보안사고 발생에 따른 기술유출의 피해규모를 객관적으로 추정하기 위해 고려되어야하는 핵심요인 도출하여 기술가치평가방법 분석
피해분석에 따른 대응방안	조성필 (2017)	- 제4차 산업혁명의 시대에 위협요인과 관련해 데이터 사고나 유출에 대한 전반적인 추이를 알아보고 구체적으로 어떤 산업분야에서 가장 많은 피해를 입었는지 연구
	조혜선 (2017)	- 침해사고 공격정보의 위협수준을 판단하기 위한 요구사항을 파악하고, 이에 대한 위협분석 기준을 추출하여 가중치 기반의 연산을 통해 위협수준을 도출
	최찬영 (2019)	- 금융기관 사이버보안 투자와 피해 예측 모델 설계에서는 기존 사이버사고 피해액 계산 방법에 대해 분석하고, 계산된 타 금융기관의 피해액을 이용해 해당 금융기관의 예상 피해액 추산

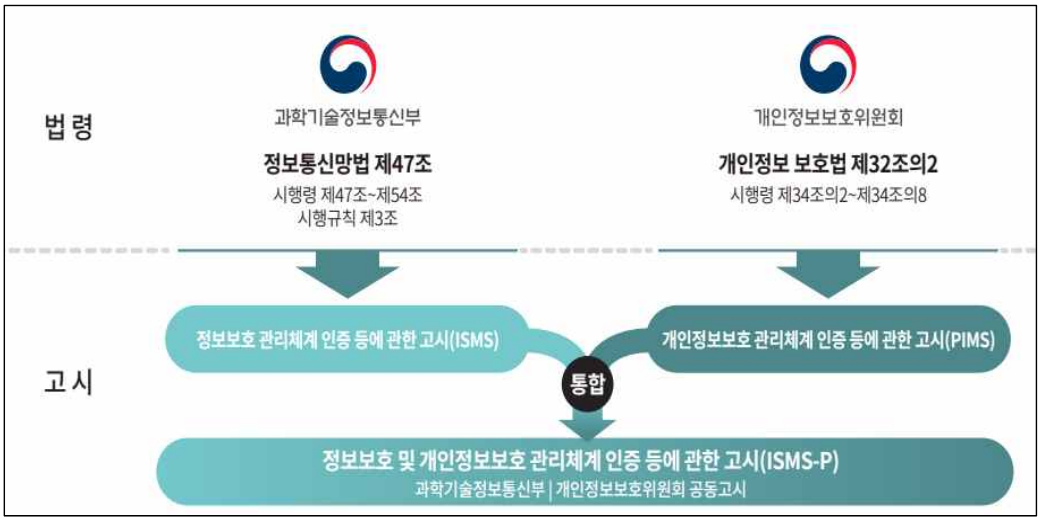
출처: 선행연구 논문을 토대로 연구자 정리

4.2.2. 정보보호 관리체계

1) 정보보호 관리체계 인증(ISMS-P)

국내 정보보호 관리체계(ISMS)는 기업의 자산에 대한 안전성과 신뢰성을 향상시키기 위해 정보보호 관리 절차 및 과정을 수립하고 문서화하여 지속적인 관리 및 운영을 하고, 이를 통해 기업에서 추구하는 정보의 기밀성, 무결성, 가용성 등을 실현하는 일련의 과정 또는 지속적인 개선활동 과정이라고 할 수 있다.

정보보호 및 개인정보보호 관리체계 인증제도는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 함) 제47조와 제47조의2, 같은 법 시행령 제47조부터 제54조까지의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과 「개인정보 보호법」 제32조의2, 같은 법 시행령 제34조의2부터 제34조의8까지의 규정에 따른 개인정보보호 관리체계 인증을 법적근거로 하고 있다. 법령에서 정한 인증의 통합을 위해 과학기술정보통신부와 개인정보보호위원회는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」를 공동으로 개정하여 시행하고 있다[그림 2-4].



[그림 2-2] ISMS-P의 법령 · 공시 현황
출처: 한국인터넷진흥원(https://isms.kisa.or.kr/)

정보보호 및 개인정보보호 관리체계 인증기준은 크게 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항', '3. 개인정보 처리 단계별 요구사항' 3개 영역에서 총 102개의 인증기준으로 구성되어 있다. 정보보호 관리체계(ISMS) 인증을 받고자 하는 신청기관은 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항' 2개 영역에서 80개의 인증기준을 적용받게 되며, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 '3. 개인정보 처리 단계별 요구사항'을 포함하여 102개의 인증기준을 적용받게 된다[그림 2-5].

[그림 2-3] ISMS-P의 인증기준 구성
출처: 한국인터넷진흥원(https://isms.kisa.or.kr/)

'관리체계 수립 및 운영' 영역은 관리체계 기반 마련, 위험 관리, 관리체계 운영, 관리체계 점검 및 개선의 4개 분야 16개 인증기준으로 구성되어 있다. 이러한 관리체계 수립 및 운영은 정보보호 및 개인정보보호 관리체계를 운영하는 동안 지속적이고 반복적으로 실행되어야 한다[표 2-13].

[표 2-13] ISMS-P 세부점검항목(관리체계 수립 및 운영)

영역	분야	항목
관리체계 수립 및 운영 (16개)	관리체계 기반 마련	경영진의 참여
		최고책임자의 지정
		조직 구성
		범위 설정
		정책 수립
		자원 할당
	위험 관리	정보자산 식별
		현황 및 흐름분석
		위험 평가
		보호대책 선정
	관리체계 운영	보호대책 구현
		보호대책 공유
		운영현황 관리
	관리체계 점검 및 개선	법적 요구사항 준수 검토
		관리체계 점검
		관리체계 개선

출처: 정보보호 및 개인정보보호 관리체계 (ISMS-P) 정보보호 및 인증기준 안내서 (2021).

'보호대책 요구사항' 영역은 12개 분야 64개 인증기준으로 구성되어 있다. 보호대책 요구사항에 따라 신청기관은 관리체계 수립 및 운영 과정에서 수행한 위험평가 결과와 조직의 서비스 및 정보시스템 특성 등을 반영하여 정책, 조직, 자산 관리 등 12개 분야의 체계적인 보호대책을 수립·이행하여야 한다 [표 2-14].

[표 2-14] ISMS-P 세부점검항목(보호대책 요구사항)

영역	분야	항목
보호대책 요구사항 (64개)	정책, 조직, 자산 관리	정책의 유지관리
		조직의 유지관리
		정보자산 관리
	인적 보안	주요 직무자 지정 및 관리

영역	분야	항목
		직무 분리
		보안 서약
		인식제고 및 교육훈련
		퇴직 및 직무변경 관리
		보안 위반 시 조치
	외부자 보안	외부자 현황 관리
		외부자 계약 시 보안
		외부자 보안 이행 관리
		외부자 계약 변경 및 만료 시 보안
	물리 보안	보호구역 지정
		출입통제
		정보시스템 보호
		보호설비 운영
		보호구역 내 작업
		반출입 기기 통제
		업무환경 보안
	인증 및 권한관리	사용자 계정 관리
		사용자 식별
		사용자 인증
		비밀번호 관리
		특수 계정 및 권한 관리
		접근권한 검토
	접근통제	네트워크 접근
		정보시스템 접근
		응용프로그램 접근
		데이터베이스 접근
		무선 네트워크 접근
		원격접근 통제
		인터넷 접속 통제
	암호화 적용	암호정책 적용
		암호키 관리

영역	분야	항목
	정보시스템 도입 및 개발 보안	보안 요구사항 정의
		보안 요구사항 검토 및 시험
		시험과 운영 환경 분리
		시험 데이터 보안
		소스 프로그램 관리
		운영환경 이관
	시스템 및 서비스 운영관리	변경관리
		성능 및 장애관리
		백업 및 복구관리
		로그 및 접속기록 관리
		로그 및 접속기록 점검
		시간 동기화
		정보자산의 재사용 및 폐기
	시스템 및 서비스 보안관리	보안시스템 운영
		클라우드 보안
		공개서버 보안
		전자거래 및 핀테크 보안
		정보전송 보안
		업무용 단말기기 보안
		보조저장매체 관리
		패치관리
		악성코드 통제
	사고 예방 및 대응	사고 예방 및 대응체계 구축
		취약점 점검 및 조치
		이상행위 분석 및 모니터링
		사고 대응 훈련 및 개선
		사고 대응 및 복구
	재해복구	재해, 재난 대비 안전조치
		재해 복구 시험 및 개선

출처: 정보보호 및 개인정보보호 관리체계 (ISMS-P) 정보보호 및 인증기준 안내서 (2021).

‘개인정보 처리 단계별 요구사항’ 영역은 개인정보 생명주기에 따른 개인정보 수집 시 보호조치, 개인정보 보유 및 이용 시 보호조치, 개인정보 제공 시 보호조치, 개인정보 파기 시 보호조치와 정보주체 권리보호를 포함하여 5개 분야 22개의 인증기준으로 구성되어 있다. 이 영역은 대부분 법적 요구사항과 직접적으로 관련되어 있으므로 개인정보 흐름분석을 바탕으로 조직이 적용받는 법규 및 세부 조항을 명확히 파악하여 이를 준수하여야 한다[표 2-15].

[표 2-15] ISMS-P 세부점검항목(개인정보 처리 단계별 요구사항)

영역	분야	항목
개인정보 처리 단계별 요구사항 (22개)	개인정보 수집 시 보호조치	개인정보 수집 제한
		개인정보의 수집 동의
		주민등록번호 처리 제한
		민감정보 및 고유식별정보의 처리 제한
		간접수집 보호조치
		영상정보처리기기 설치·운영
		홍보 및 마케팅 목적 활용 시 조치
	개인정보 보유 및 이용 시 보호조치	개인정보 현황관리
		개인정보 품질보장
		개인정보 표시제한 및 이용 시 보호조치
		이용자 단말기 접근 보호
		개인정보 목적 외 이용 및 제공
	개인정보 제공 시 보호조치	개인정보 제3자 제공
		업무 위탁에 따른 정보주체 고지
		영업의 양수 등에 따른 개인정보의 이전
		개인정보의 국외이전
	개인정보 파기 시 보호조치	개인정보의 파기
		처리목적 달성 후 보유 시 조치
		휴면 이용자 관리
	정보주체 권리보호	개인정보처리방침 공개
		정보주체 권리보장

영역	분야	항목
		이용내역 통지

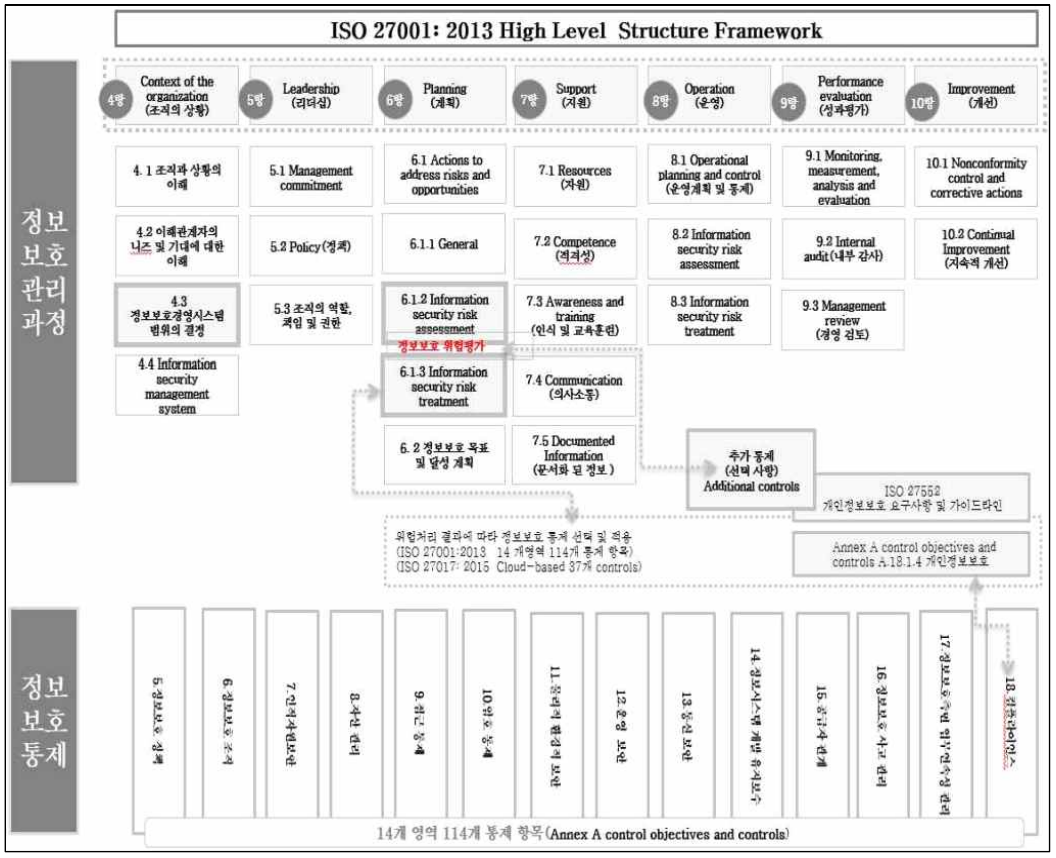
출처: 정보보호 및 개인정보보호 관리체계 (ISMS-P) 정보보호 및 인증기준 안내서 (2021).

2) 국제표준 정보보안경영시스템 인증(ISO 27001)

ISO 27001 인증은 국제표준화기구인 ISO와 국제전기기술위원회인 IEC에서 제정한 정보보호 관리를 위한 국제표준으로 정보보호 분야에서 권위있는 국제 인증제도이다. ISO/IEC27000 Family에는 용어, 요구사항, 지침 등을 규정하고 있고, 관리영역, 세부 통제항목에 대한 엄격한 심사를 거쳐 인증서를 부여한다. 정보보호 경영시스템의 수립, 구현, 유지, 지속적 개선에 필요한 요구사항을 제공하기 위해 개발되었다고 할 수 있고, 위험 관리 프로세스 적용을 통해 정보의 기밀성, 무결성, 가용성을 보존하고 위험을 관리하는 체계를 제공한다.

ISO27001은 조직의 정보보호를 위해 '무엇'을 해야 하는가를 정의하는데 목적을 갖는다. 또한 조직 내 정보 자산을 기준으로 자산 평가, 위협 평가, 취약성 평가를 산정하고 수용 가능한 위험 수준인 위험을 정의한다(이병주, 2019). ISO 27001 정보보호 관리체계는 비즈니스 목표를 달성하기 위해 조직의 정보보안을 수립·구현하고, 운영·모니터링하고, 검토·유지하고, 지속적인 개선을 위한 체계적인 Process Approach (Plan -> Do -> Check -> Act) 접근 방법이다. ISO 27001 은 조직의 상황, 리더십, 기획, 지원, 운영, 성과평가, 개선으로 7개 관리과정 요구사항으로 구성되어 있으며, 정보보호 통제 요구사항은 관리영역 14개, 세부 통제항목 114개로 구성되어 있다[그림 2-6][표 2-16].

- Process Approach(PDCA 접근): Plan -> Do -> Check -> Act
- HLS(High Level Structure): 조직 상황, 리더십, 기획, 지원, 운영, 성과평가, 개선의 7개 구조로 구성
- Risk-based Approach: ISO 31000 기반 원칙, 프레임워크, 프로세스 3가지 축으로 구성



[그림 2-4] ISO 27001:2013 통제항목 구성

출처: ISO/IEC 27001:2013

[표 2-16] ISO 27001:2013 통제항목

구분	통제항목	설명	항목수
통제 목적 및 통제	정보보호 정책 (Information security policies)	정보보호 정책에 대한 경영방침, 지원사항에 대한 통제가 적절히 진행되는지 체크	2
	정보 보호 조직(Organization of Information Security)	보안 관리를 위한 보안조직의 구성 및 각 조직원의 책임과 역할이 지정되었는지 체크	7
	자산 관리 (Asset management)	조직 내 자산에 대한 등급분류 및 적절한 보호되는지 체크 (프로세스 등)	10
	인력 자원 보안(Human Resource Security)	인적정보의 변동 및 시설의 절도, 사기, 오용에 대한 위험관리가 잘 수행되는지 체크	6
	물리적 및 환경적 보안 (Physical and	허가되지 않은 사용자 및 그룹의 접근 및 통제가 물리적, 환경적으로 대응하고 있는	15

구분	통제항목	설명	항목수
	Environmental Security)	지 체크	
	통신 보안 (Communications security)	정보 통신시설이 정확하고 안전하게 운영되는지에 대한 대응방안 확인	7
	접근 통제 (Access control)	정보에 대한 접근을 통제하기 위한 대응방안이 적절한지 체크	14
	정보 시스템 개발 및 유지보수 (System acquisition, development & maintenance)	정보시스템의 도입, 개발 유지보수가 정보보호를 위해 잘 수립되어 진행되는지 체크	13
	정보 보안 사고의 관리(Information security incident management)	침해사고의 탐지, 교정, 대응 등의 조치가 잘 진행되는지 체크	7
	정보보호 측면 업무 연속성 관리 (Information security aspects of business continuity management)	기업활동에 대한 방해요소의 최소화 및 시스템 실패 및 재난에 대해 사업의 연속성을 보호하는 프로세스가 있는지 체크	4
	준거성 (Regulatory compliance)	범죄 및 민형사상의 법률, 법규를 잘 준수하는지, 계약 의무사항 및 보안 요구사항에 불일치 및 회피 대응책 확인(법률위반, 계약의무 위반 등에 따른 피해를 피하기 위함)	8
	공급자 관계(5 Supplier relationships)	공급자가 접근할 수 있는 조직 자산에 대한 보호 보장	5
	암호 통제 (Cryptography)	암호 통제는 모든 관련 협약, 법규, 규제를 준수하며 사용	2
	운영 보안 (Operations security)	정보처리 시설의 정확하고 안전한 운영 보장	14
합계			**114**

출처: ISO/IEC 27001:2013

ISO 27001는 최근 2022년에 업데이트하여 114개의 통제항목이 93개로 정리되었다[표 2-17].

[표 2-17] ISO 27001:2022 변경항목

ISO 27001:2022	ISO 27001:2013
A.5.7 Threat intelligence	A.6.1.4 Contact with special interest groups
A.5.16 Identity management	A.9.2.1 User registration and de-registration
A.5.23 Information security for use of	A.15.x Supplier relationships

ISO 27001:2022	ISO 27001:2013
cloud services	
A.5.29 Information security during disruption	A.17.1.x Information security continuity
A.5.30 ICT readiness for business continuity	A.17.1.3 Verify, review and evaluate information security continuity
A.7.4 Physical security monitoring	A.9.2.5 Review of user access rights
A.8.9 Configuration management	A.14.2.5 Secure system engineering principles
A.8.10 Information deletion	A.18.1.3 Protection of records
A.8.11 Data masking	A.14.3.1 Protection of test data
A.8.12 Data leakage prevention	A.12.6.1 Management of technical vulnerabilities
A.8.16 Monitoring activities	A.12.4.x Logging and monitoring
A.8.23 Web filtering	A.13.1.2 Security of network services
A.8.28 Secure coding	A.14.2.1 Secure development p

출처: ISO/IEC 27001:2013, ISO/IEC 27001:2022 참조하여 연구자 정리

3) NIST의 사이버보안 프레임워크(CSF)

NIST(미국 국립표준기술연구소)의 사이버보안 프레임워크(CSF)는 사이버보안 관련 리스크를 관리하기 위한 표준, 지침 및 모범 사례로 구성된 자발적 프레임워크이다. 사이버보안 프레임워크는 우선순위 결정, 유연하고 비용효율적 접근 방식을 통해 공중 보건, 미국 경제 및 국가 안보에 중요한 핵심 인프라 및 기타 분야를 보호하고, 레질리언스 제고를 지원한다.

NIST의 지도 하에 글로벌 산업의 니즈를 대표하는 여러 분야의 팀들이 모여 일련의 워크샵을 통해 CSF가 구축되었다. 오늘날, 이 프레임워크는 주요 인프라 및 기타 독립체의 운영자에게 정보보호 및 사이버보안 조치의 구축과 적용에 대한 비용 효율적이고 유연하며 우선순위에 따른 반복 가능한 접근법을 제공한다.

이 프레임워크는 리스크 기반이며 프레임워크 코어 (Framework Core), 프레임워크 프로파일 (Framework Profile), 프레임워크 구현 계층 (Framework implementation Tiers) 세 부분으로 구성된다.

‘프레임워크 코어’는 조직이 특정 사이버보안 결과를 달성하도록 돕는 일련의 활동으로 구성된다. 또한, 여기에는 이해관계자가 사이버보안 리스크 관리에 유용하며, 원하는 결과를 달성하기 위한 용도로 사용할 수 있는 지침 사례들이 포함된다. 프레임워크 코어는 4가지 요소로 기능, 카테고리, 하위 카테고리, 정보 참조 자료로 구성되며, 동시적이고 연속적인 5가지 기능은 식별, 보호, 탐지, 대응 및 복구가 포함된다. 이 다섯 가지가 함께 고려될 때, 사이버보안 수명주기 및 조직의 사이버보안 리스크 관리에 대한 높은 수준의 전략적 관점을 제공한다.

‘프레임워크 프로파일’은 기능, 카테고리 및 하위 카테고리를 조직의 특정 비즈니스 요구사항, 리스크 허용 수준 및 자원과 일치시키는 데 도움이 됩니다. ‘프레임워크 구현 계층’은 조직이 사이버보안 리스크를 바라보는 방식과 그 리스크를 관리하기 위해 보유하고 있는 프로세스에 대한 맥락을 제공한다. 계층의 범위는 부분(Tier 1)부터 적응(Tier 4)까지가 해당되며, 이 계층 단계는 사이버보안 리스크 관리 관행의 엄격성과 정교함이 증가되는 정도를 설명한다. 또한, 조직의 필요에 의해 사이버보안 리스크 관리가 어느 정도까지 공유되는지, 그것이 전체 리스크 관리 관행에 얼마나 잘 통합되는지를 설명한다. 이 모든 요소들이 함께 작용하면서, 프레임워크는 조직의 정보보안 투명성을 높이며, 이는 결국 개인의 프라이버시와 시민의 자유뿐만 아니라 그 기밀성을 차례로 보호할 수 있게 한다[표 2-18].

[표 2-18] NIST의 CSF 프레임워크 구성항목

기능	카테고리	세부 카테고리 수
Identify	Asset Management	6
	Business Environment	5
	Governance	4
	Risk Assessment	6
	Risk Management Strategy	3
	Supply Chain Risk Management PR	5
Protect	Identity Management and Access Control	7
	Awareness and Training	5

기능	카테고리	세부 카테고리 수
	Data Security	8
	Information Protection Processes and Procedures	12
	Maintenance	2
	Protective Technology DE	5
Detect	Anomalies and Events	5
	Security Continuous Monitoring	8
	Detection Processes RS	5
Respond	Response Planning	1
	Communications	5
	Analysis	5
	Mitigation	3
	Improvements RC	2
Recover	Recovery Planning	1
	Improvements	2
	Communications	3
합계		**108**

출처: NIST, Framework for Improving Critical Infrastructure Cybersecurity (2018.04.16.).

4) 사이버탄력성 있는 정보보호 관리체계

현재의 복잡하고 불확실성이 만연한 경영, 기술 환경하에서 기술적 보안대책 중심의 통제 접근방법으로 이와 같은 목표 달성이 가능할 것인가에 대한 의문을 지울 수 없다(김정덕, 2021). 또한, 다양하고 복잡해진 사이버 침해사고에 대응하는 방안이 정보보호 관리체계를 구축하는 것만은 아닐 것이다. 특히 보안환경을 충분히 갖추지 못하는 중소기업은 침해사고를 유연하게 극복 가능한 사이버탄력성을 갖출 수 있는 방안를 고려하여야 한다.

기존 정보보호 중심 보안의 한계와 디지털 비즈니스 환경에서의 위험을 극복하기 위해 고안된 개념이 사이버탄력성(Cyber Resilience)다. 사이버탄력성은 2012년 다보스에서 개최된 세계경제포럼(WEF:World Economic Forum)에서 처음 사용되었다(김정덕, 2016). 당시 세계경제포럼에서는 보안에 대한 완벽한 예방은 불가능하며, 보안사고의 발생을 기정 사실로하고 손

실을 최소화하기 위해, 사고 이전의 상태로 신속하게 복구하는 역량 구축을 강조하였으며 이를 사이버탄력성이라고 통칭하였다(WEF, 2012).

COVID-19 팬데믹 발생 이후 디지털 비즈니스 환경의 복잡성 및 불확실성이 더욱 증가하게 되었으며 이를 타개할 역량으로 사이버탄력성이 대두되고 있다(KPMG, 2020). 이처럼 산업보안의 중요성이 증가하고, 기존 정보보호 대응 체제에 한계점이 드러난 상황에서, 새로운 보안 패러다임인 사이버탄력성이 침해사고 대응체계로서 적용 필요성 및 중요성에 대한 인식이 증가하고 있다. 특히, 중소기업에 있어 더욱 유연한 사이버 침해사고 대응을 위한 사이버탄력성 있는 보안환경이 필요하며, 이런 보안환경 구축에 필요한 것은 무엇인지 알 필요가 있다(고영현, 2021).

사이버탄력성 영역은 티어니와 브루너(Tierney&Bruneau, 2007)의 연구를 참고하여 기술, 조직, 사회, 경제에서 보다 구체적인 기술, 제도·거버넌스, 리더십·인식, 예산으로 구분한다. 또한 이재열(2009)이 [표 2-19]에서 제시한 사이버탄력성의 구성요소와 예시를 참고하여 사이버탄력성에 알맞게 시스템 견고성, 자원동원성, 신속성, 적응성 등 총 네 가지 사이버탄력성 영역을 도출하였다.

[표 2-19] Tiernery & Bruneau의 복원력의 네 가지 영역

구분	내용
기술영역	피해를 줄이고 기능 손상을 줄이는 시스템의 물리적 속성
조직영역	시스템의 물리적 요소를 관리하는 조직이나 제도
사회영역	사회집단이나 개인의 특성
경제영역	지역경제 및 기업의 특성

출처: Tiernery & Bruneau (2007)

사이버탄력성의 구성요소와 영역은 시스템견고성(Robustness), 자원동원성(Resourcefulness), 신속성(Rapidity), 적응성(Adoptability)으로 이루어진다.

첫째, '시스템견고성'은 침해 상황에서도 업무 연속성을 유지하는 견고한 시스템을 가리킨다. 따라서 기술적으로는 강한 보안시스템과 사이버침해를 예측할 수 있는 역량을 기반으로 하여, 취약성, 복원성에 대해 정의가 되어

있고, 이에 상응한 취약성 관리에 대하여 법적 절차가 제도적으로 마련되어야 한다. 보안시스템 구축과 개선을 위한 투자는 보안 정책을 담당하는 보안 책임자가 중요하며, 조직은 체계적으로 사이버탄력성 관련 정책을 확대해 나가야 한다.

둘째, '자원동원성'은 취약성 관리를 위한 자원뿐 아니라 관리 담당자의 역량에 대한 내용이다. 보안기술을 갖고 있는 전문인력 확보가 중요하며, 이러한 보안 전문가를 양성·지원하는 예산이 필요하다. 또한, 보안 전문인력의 역량조건 기준과 의무 및 역할을 규정하여 효율적인 인력관리하는 것이 필요하다. 조직적으로는 이런 환경을 제시할 수 있는 거버넌스 체계가 마련되어야 한다.

셋째, '신속성'은 가능한 한 신속하게 정상 또는 원래 상태로 돌아가는 능력을 말한다. 기술적으로는 최초복구까지 걸린 시간의 단축이 중요하며, 생산이나 예산을 복구하는 데 드는 시간의 단축도 중요하게 관리되어야 한다. 조직적으로 신속성을 관리할 수 있는 '컨트롤타워'와 명확한 책임과 역할을 정의하고, 제도적으로는 복구에 대한 절차나 매뉴얼을 기반으로 제시하여 시간을 단축할 수 있어야 한다.

넷째, '적응성'은 사이버침해 결과를 받아들이고 시스템견고성, 자원동원성, 신속성을 기준으로 개선 또는 제고하는 능력이다. 기술적으로 더 나은 보안시스템을 구축하고, 이를 위한 새로운 수단과 기술 소개 및 투자가 필요하다. 새로운 사이버침해에 대비하여 제도 개선과 신종 위협에 대비하기 위한 조직체계가 마련되어야 한다.

외부의 사이버침해에 대응하는 복원력을 심화시키는 것이 사이버탄력성의 궁극적 목적이기 때문에 네 가지 사이버탄력성 영역과 이에 대응하는 구성요소를 강화하는 방향으로 나아가야 한다(류현숙, 조희정, 이헌아, 2015).

대표적인 사이버탄력성 모델은 카네기 멜론 대학(CMU)의 CERT-RMM (Resilience Management Model), WEF(World Economic Forum)의 사이버탄력성 성숙도 평가항목, 컨설팅 기업인 PwC(PriceWaterhouseCoopers)의 사이버탄력성 검토항목 등이 있다. 먼저, 카네기 멜론 대학의 CERT-RMM은 4가지 Asset으로 구분하여 People, Information,Technology, Facilities 운

영관리를 구축하며, Engineering, Enterprise Management, Operations Management, Process Management 4개의 카테고리의 프로세스로 구성된다 [표 2-20].

[표 2-20] CMU의 CERT-RMM 구성요소

구분	내용
자산 분류	- People - 경영진, 임직원, 보안조직, 외부 조직 등 관계 구성원 - Information - 데이터, 핵심 지식, 정보 자원 등 - Technology - 소프트웨어, 시스템, 영상보안장비, 네트워크 등 - Facilities - 사무실, 데이터 센터 등 물리적 보안 요소
프로세스 분류	- Engineering : 조직 자산, 비즈니스 프로세스 및 서비스의 탄력성을 확립 - Enterprise Management : 복원력 관리 프로세스를 지원 - Operations Management: 복원력의 운영 측면을 관리 - Process Management : 운영 탄력성 관리 프로세스

출처: Software Engineering Institute, Carnegie Mellon University (https://resources.sei.cmu.edu/)

WEF(World Economic Forum)는 경영진의 사이버탄력성 성숙도 평가를 위한 체크리스트를 제공하여 평가를 지원한다. 이 체크리스트는 크게 최고경영자 및 경영진의 사이버리스크 관리 책임, 적극적 참여, 보안정책 등의 'Governance', 규칙 및 규정 준수 주기적 점검, 보안관련 교육, 보안 영향평가 실시 등의 'Programme', 사이버 위험 공동 관리, 업계 베스트프렉티스 반영, 리스크 관리 위한 제3자와 관계 구축 등의 'Network'으로 구성하여 관리하고 있다. 컨설팅 기업인 PwC(PriceWaterhouseCoopers)는 PPT(People, Process, Technology)관점을 이용하여 사이버탄력성을 검토하는 항목을 제시하였다. 또한, 사이버탄력성 교육재단인 RESILIA는 PPT(People, Process, Technology)모델과 ITIL lifecycle을 이용하여 사이버탄력성 수행의 BestPractive를 제시하였다. 중소기업이 급속히 변화하는 환경에서 예측 불가능한 위협까지 대처하여 효과적인 사이버 침해사고 대응을 위하여 앞에서 제시한 사이버탄력성 모델을 고려하여 체계를 구축하는 것도 중요한 성공요인이 될 수 있을 것이다.

4.2.3. 국내 중소기업 정보보호 지원사업

1) 중소기업 정보보호 지원사업의 중요성

중소기업 정보보호 지원사업의 법제도 추진 체계로는 과학기술정보통신부 소관 법률로서 정보보호 산업의 진흥에 관한 법률과 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등의 근거를 가지고 수행하고 있으나, 중소기업의 정보보호 지원사업에 대한 지원 근거는 명확하게 규정되어 있지 않다. 산업통상자원부 소관 법률 산업기술의 유출방지 및 보호에 관한 법률과 중소벤처기업부 소관 법률 중소기업기술 보호 지원에 관한 법률, 중소기업기술 촉진법에서도 중소기업의 정보보호 지원사업에 대한 지원 근거는 명확하지 않다(배영식, 장상수. 2021).

정보보호 실태조사 결과에 보는 바와 같이 많은 중소기업이 정보보호를 위한 기술적 조치를 마련하지 않았거나, 보안규정이 있음에도 이를 철저히 지키지 못하고 있다. 이는 법적 지원에도 문제가 있겠지만, 중소기업들의 정보보호 인식이 대기업보다 낮다는 것을 의미한다. 중소기업의 중요정보나 기술이 유출되면, 그것은 곧 그 기업의 재정적 문제에도 직결될 정도로 치명적이다. 실질적인 문제는 침해사고나 악성코드 감염 등으로 정보가 유출됐는지도 모른 채 손해를 입을 수 있다는 것이다. 국가 경제의 큰 축을 담당하고 있는 중소기업이 안전한 환경에서 비즈니스를 할 수 없다면, 경기가 어려운 시기에 경제적으로 더욱 큰 타격을 입을 수 있을 것이다. 중소기업은 대부분 동원할 수 있는 자원의 한계로 인하여 자력으로 필요한 정보보호 수준을 유지하는 것이 매우 어렵다. 특히 규모가 작은 영세기업의 경우에는 정보기술을 활용한 경영지원 업무와 침해 위협에 대한 대응 업무 등 서로 상충된 업무를 담당이 없거나 한 사람이 동시 수행하여 더욱 침해사고 위협에 취약할 수밖에 없다. 이러한 이유로 중소기업의 정보보호 문제는 적극적으로 정부의 지원이 필요하다(HIIC, 2020).

또한, 중소기업은 정부에서 제공하는 다양한 중소기업 지원사업을 이용하기는 접근성 측면에서 어려움이 많다. 중소기업이 사이버 침해사고에 대한 예방 및 대응체계를 수립하기 위해서는 정보보호 관리체계를 구축하는 것과

함께, 각 기관에서 제공하는 정보보호 지원사업을 적극적으로 알아보고 이용하는 것도 성공적인 보안체계를 구축하는 것만큼 중요하다고 볼 수 있다.

2) 한국인터넷진흥원의 중소기업 정보보호 지원사업

과학기술정보통신부 및 한국인터넷진흥원(KISA: Korea Internet & Security Agency, 이하 KISA)에서는 2014년부터 본격적으로 지역 중소기업의 정보보호 수준 제고 및 침해사고 예방·대응 역량 강화, 정보보호 산업 활성화를 위하여 '지역 중소기업 정보보호 지원' 사업을 추진하고 있다.

한국인터넷진흥원(KISA)이 주관하여 중소기업의 정보보안 역량 강화를 위해 전국 ICT중소기업을 대상으로 정보보호 컨설팅 및 보안솔루션 도입비용을 지원해주는 사업이다. 컨설팅 보안솔루션 지원사업은 일정 규모 이상의 ICT 인프라를 보유한 중소기업 대상, 정보보호 컨설팅 기반 보안솔루션 지원을 통해 기업 자체적인 정보보호 체계 구축 및 투자 기반 마련하는 것이 목적이다. 또한, 보안서비스 지원사업은 자체적인 보안솔루션 운영이 어려운 영세 중소기업 대상, 저예산으로 지속관리 가능한 클라우드 기반 보안 서비스(SECaaS) 지원을 통해 정보보호 인식 개선 및 투자기반 마련하는 것이다.

이를 위하여 지자체 및 지역 관계기관과 협력 모델로서 지역 중소기업의 정보보호 활동을 지원하기 위하여 「지역정보보호지원센터」를 구축·운영 중이다. 주요 사업 내용으로는 다음과 같다.

① 정보보호 맞춤형 현장컨설팅, 웹 취약점 점검 및 보호조치 지원, 민감정보보호 조치 지원
② 지역 중소기업 재직자 중심의 정보보호 전문교육, 정보보호 세미나 개최, 지역정보보호 컨퍼런스 개최
③ 지역 전략산업에 대한 설계단계부터의 보안 위한 보안 테스트베드 운영
④ 중소기업 대상 정보보호 맞춤형 종합컨설팅, 보안솔루션 도입 지원
⑤ 지역 유관기관과의 협력 네트워크 구축을 통한 상생 협력 방안 마련 등

3) 중소벤처기업부, 대·중소기업·농어업협력재단의 기술보호 지원사업

중소벤처기업부와 대·중소기업·농어업협력재단에서 시행하는 '중소기업 기술보호 지원사업'은 중소기업들의 기술보호 기반과 역량을 강화해 안정적인 기술개발 여건을 조성하자는 취지로 시행되며, 기업의 기술경쟁력 제고 및 관련 산업발전에 기여를 목적으로 하고 있다. 주요 지원사업은 사전예방 측면에서 '기술보호 전문가 현장자문', '중소기업 기술보호 정책보험', '기술자료 임치제도', '기술유출방지시스템구축 지원' 등이 있다. 피해주제 측면의 지원사업은 '부처통합 상담신고센터', '중소기업 기술침해 신고·조사' 등이 있다.

본 논문에서는 지원사업 중 중소기업의 핵심자산을 안전하게 지킬 수 있는 '기술자료 임치제도'에 대해 간단히 소개하고자 한다. 기술자료 임치제도는 '대·중소기업 상생협력 촉진에 관한 법률 제24조의 2(기술자료 임치제도)'를 근거로 대·중소기업·농어업 협력재단의 기술자료임치센터에서 수행하는 제도다. 거래 관계에 있는 대기업과 중소기업이 일정한 조건하에 서로 합의하여 핵심 기술자료를 신뢰성 있고 임치 설비를 갖춘 대·중소기업·농어업협력재단에 안전하게 보관해 둠으로써 중소기업은 기술유출 위험을 줄일 수 있고 대기업은 해당 중소기업의 파산·폐업 시 해당 임치물을 이용하여 관련 기술을 안전하게 활용할 수 있도록 하는 제도이다.

개발기술의 효율적인 보호를 위하여 개발기업의 기술자료가 유출되었을 경우 기술자료 임치물을 통해 개발기업의 기술 개발 사실을 입증하고, 내부직원 및 산업스파이 등에 의해 기술자료가 유출되더라도 임치물을 통해 개발기업은 해당 기술의 개발 사실을 입증한다. 중소기업은 개발기술이 유출되지 않음에 따라 개발기술에 대해 기술경쟁력을 유지할 수 있고, 사용기업도 개발기업의 파산·폐업, 유지보수 불가 시 임치물을 이용하여 안전한 유지보수가 가능하여, 기술보호 효과와 보험적 효과를 모두 지원할 수 있다[표 2-21].

[표 2-21] 기술자료임치센터 기술자료 임치제도

구분	내용
기술상 정보	- 시설 및 제품의 설계도 / 물품의 생산·제조방법 - 물질의 배합방법 / 연구개발 보고서 및 데이터 - SW 소스코드 및 디지털 콘텐츠 등 * 특히 소프트웨어의 발주시 기술자료 임치제도를 이용하면 사용기술에 대한 안정성을 보장

구분	내용
경영상 정보	- 기업의 운영 및 관리와 관련된 기밀서류 - (재무, 회계, 인사, 마케팅, 노무, 생산) 기업의 매출과 관련된 기밀서류 - (원가, 거래처, 각종 보고서 및 매뉴얼)

출처: 대·중소기업·농어업 협력재단 (https://www.kescrow.or.kr/)

중소기업 정보보호를 위한 지원사업은 여러 가지 다양하게 지원하고 있으나, 정보보호 실태조사 등의 분석에 근거하여 실효성이 불투명함을 알 수 있다. 또한, 현실적으로 기술 보호 지원 사업을 받고 있는 중소기업은 그리 많지 않은 것으로 보인다(국회정보위원회, 2019).

중소기업의 기술보호 지원사업별 인지도는 '전문가 현장자문(82.7%)'이 가장 높고, '통합상담신고센터(82.0%)', '기술자료 임치(77.4%)' 등의 순으로 나타났다[표 2-22]. 중소기업 기술보호 지원사업의 '효과 있음' 응답은 '기술자료 임치'가 24.9%로 가장 높고, 다음으로 '기술유출방지시스템 구축사업(20.0%)', '중소기업 기술지킴서비스(보안관제)(19.1%)' 등의 순으로 높은 것으로 나타났다[표 2-23](대·중소기업·농어업 협력재단, 2021).

[표 2-22] 기술보호 역량강화 지원사업별 인지도

조사연도	통합상담 신고센터	전문가 현장자문	기술자료 임치	기술유출 방지시스템 구축사업	기술분쟁 조정·중재	기술지킴 서비스 (보안관제)	증거지킴 서비스 (TTRS)
2020년	82	82.7	77.4	67.7	64	72.1	13.3
2019년	77.3	76.1	68	59.8	53.7	64.2	-
2018년	84.9	81.1	79.1	-	68	76.1	-

출처: 2020년 중소기업 기술보호수준 실태조사 (2021).

[표 2-23] 기술보호 역량강화 지원사업별 효과

조사연도	통합상담 신고센터	전문가 현장자문	기술자료 임치	기술유출 방지시스템 구축사업	기술분쟁 조정·중재	기술지킴 서비스 (보안관제)	증거지킴 서비스 (TTRS)
2020년	14.1	15.4	24.9	20.0	11.2	19.1	9.5

출처: 2020년 중소기업 기술보호수준 실태조사 (2021).

4.3. 선행연구의 분석과 연구의 차별성

중소기업을 대상으로 사이버 침해사고 관련하여 다양한 연구를 하고 있다. 보안 정책 측면의 연구는 정부 차원에서 중소기업을 위한 보안 정책은 무엇인지 연구하는 내용과 중소기업 임직원의 보안 정책 준수 의지에 관한 연구로 구분할 수 있다. 보안 활동 측면에서는 보안 인프라, 보안 프로세스 또는 임직원의 보안인식 개선에 관한 연구 등으로 확인된다. 보안 성과 측면에서는 보안성과 평가 방안과 성과에 영향을 미치는 요소를 연구하는 선행연구 등으로 확인되었다.

선행연구들과 비교하여 본 연구는 다음과 같은 차별성을 가지고 있다.

첫째, 선행연구에서는 보안 활동을 물리적 보안, 기술적 보안, 관리적 보안 등으로 크게 분류하여 연구가 진행되었거나(고찬석, 2021; 박양모, 2017; 김용재, 2017; 문건웅, 2017; 김택영, 2021) 좀 더 집중된 일부 보안영역에서의 연구(이민형 외, 2015; 강만성, 2018)를 수행하였으나, 본 연구에서는 보안 활동을 좀 더 세분화하여 구체적으로 사이버 침해사고 대응에 영향을 미치는 활동을 분석해 보았다.

둘째, 선행연구는 사이버 침해사고에 대한 영향을 지원사업의 수혜여부, 침해사고 경험여부, 보안담당자의 유무 등 수행 여부에 따른 조절 효과를 연구(이대권 외, 2021; 소현철, 2018; 이홍배, 2022; 우순규, 2018)하였으나, 본 연구에서는 보안책임자의 역할 수행자가 누구인지 그리고 기업의 핵심정보를 관리 방식에 따라 조절효과가 있는지 모든 보안 활동에 대하여 침해사고 대응에 대한 조절 효과를 분석하였다,

셋째, 선행연구는 보안책임자에 관하여 주로 보안인식에 대한 연구(권재성, 2021; 김택영, 2021; 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.

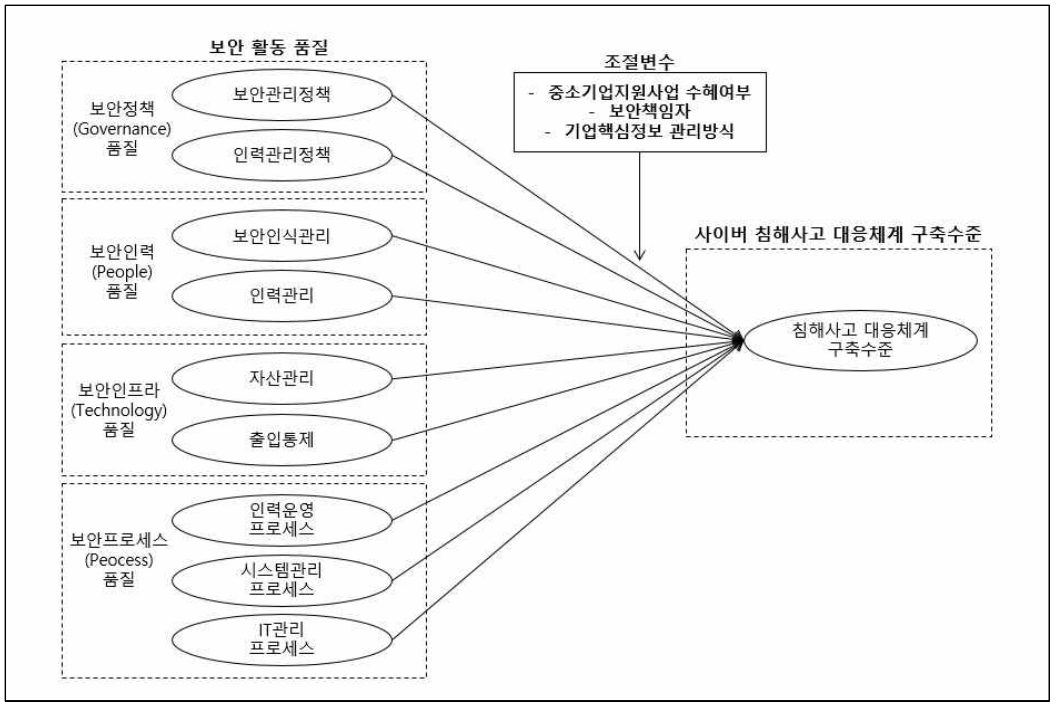
넷째, 선행연구는 기업의 중요정보를 자산관리 측면에서 보안체계의 하나로 관리하는 연구(차재원, 2016; 이대권 외, 2021; 김양훈, 2014)로서 핵심자산에 대한 관리에 따른 보안 성과를 연구하는 것에는 부족한 부분이 있었다, 본 연구에서는 이를 보완하여 기업의 핵심정보를 관리하는 방식을 외부서비스로 관리하는가 또는 자체적인 체계를 갖추어 관리하는가에 따라 각 보안 활동이 침해사고 대응에 어떤 조절 효과를 주는지 분석하였다.

Ⅲ. 연구설계

5.1. 연구모형

본 연구는 국내 중소기업이 사이버 침해사고에 유연하게 대응하기 위한 보안체계를 제시하고, 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 중소기업기술보호 관점에서 설계하였다. 중소기업에서 보안역량 강화를 위해 수행하는 보안 활동이 사이버 침해사고 대응을 위한 관리체계 구축에 미치는 영향 분석과 중소기업의 관리방식에 따른 조절효과를 검증하고자 아래와 같은 연구모형을 구성하였다.



[그림 3-1] 연구모형

보안 활동이 사이버 침해사고 대응을 위한 관리체계 구축에 미치는 영향에 대하여 중소기업 관점에서 분석하기 위해, 보안 활동(보안정책 품질, 보안인력 품질, 보안인프라 품질, 보안프로세스 품질)를 독립변수로 설정하고 침해사고 대응체계 구축수준을 종속변수로 설정하였다. 중소기업의 사이버 침해사고 대응체계 구축에 있어 각 보안 활동이 미치는 영향의 정도가 다를 것으로 보고, 보안 활동을 하나의 변수로 설정하지 않고 보안 정책 품질, 보안 인력 품질, 보안 인프라 품질, 보안 프로세스 품질로 변수를 구성하였고, 이를 한단계 더 세분화하여 독립변수를 구성하였다. 보안 정책 품질은 보안관리정책과 인력관리정책, 보안 인력 품질은 보안인식관리와 인력관리, 보안 인프라 품질은 자산관리와 출입통제, 보안 프로세스 품질은 인력운영 프로세스, 시스템관리 프로세스, IT관리 프로세스로 세분화하여 구성하였다. 또한, 중소기업 지원사업의 수혜 경험과 보안책임자의 역할과 책임 그리고 기업의 핵심정보를 관리방식이 보안 활동과 사이버 침해사고 대응체계 간 관계에 작용한다고 보고 조절변수로 설정하였다.

5.2. 연구변수의 조작적 정의

연구변수는 기존 문헌 연구의 정의를 참고하여 보안 활동, 침해사고 대응체계 간의 영향 관계를 도출한다는 본 연구의 목적에 적합하도록 수정·보완하였다. 본 연구에서 독립변수는 보안 활동으로 보안 정책 품질(보안관리정책, 인력관리정책), 인적 보안 품질(보안인식관리, 인력관리), 보안인프라 품질(자산관리, 출입통제), 보안 프로세스 품질(인력운영 프로세스, 시스템관리 프로세스, IT관리 프로세스)이고, 종속변수는 침해사고 대응체계 구축수준이다. 조절변수는 중소기업지원사업 수혜여부와 보안책임자, 기업핵심정보 관리 방식이다. 보안 활동이 중소기업의 사이버 침해사고 대응체계 구축에 미치는 영향을 검증하기 위해 수립한 연구변수의 정의는 아래와 같다[표 3-1].

[표 3-1] 연구변수의 개념적 정의

구분	변수명	세부 변수명	변수 내용	선행연구
독립변수	보안정책 품질	보안관리 정책	- 조직의 안전한 보안체계를 위하여 자산 및 체계의 보안 활동을 지원하는 원칙이나 규율	최연준 (2018) 신현구 (2015) 성욱준 (2018) 우인진 외 (2018) 김양훈 (2014) 전재찬 (2018)
		인력관리 정책	- 내·외부 인력의 보안 준수를 위한 원칙이나 규율	
	보안인력 품질	보안인식 관리	- 조직의 보안정책을 중심으로 교육 및 보안인식 관리	성욱준 (2018) 전재찬 (2018) 정혜인 (2016) 김양훈 (2014) 정점영 (2022)
		인력관리	- 내부 임직원의 비밀유지 및 퇴사 직원 관리 - 외주업체 및 외주용역 등 외부자 보안규정 수립 및 관리	
	보안 인프라 품질	자산관리	- 기업의 보안을 위하여 구축한 어플리케이션, 장비, 시설 등 보유자산 및 장비의 보안체계	최연준 (2018) 차재원 (2016) 이대권 외 (2021) 김양훈 (2014) 정진우 (2021)
		출입통제	- 내·외부 인력의 중요자산 보호를 위한 출입통제 및 정보화 기기 반입/반출 통제	
	보안 프로세스 품질	인력운영 프로세스	- 임직원의 보안 활동 관리 또는 보안 절차	송재혁 (2021) 김태형 (2019) 이호준 (2020) 고찬석 (2021)
		시스템관리	- 중요 자산 보호 위한 보안시스템 운영, 정기	

구분	변수명	세부 변수명	변수 내용	선행연구
		프로세스	적 보안감사 등 정보시스템 전반 보안관리 또는 보안 절차	김양훈 (2014) 유정은 (2017) 최영환 (2019) 차재원 (2016) Hayden (2015)
		IT 관리 프로세스	- 정보시스템의 로그 및 최신 업데이트 등 보안관리 또는 보안 절차	
종속변수	침해사고 대응체계 구축수준	침해사고 대응체계 구축수준	- 침해사고 대응을 위한 대응절차, 복구대책, 위기관리체계 등 수립·시행하는 보안관리 체계 구축에 대한 수준	강신범 외 (2012) 안종하 (2013) 문건웅 (2017) 김종원 (2018) 차재원 (2016)
조절변수	중소기업 지원사업 수혜여부	중소기업지원 사업 수혜여부	- 중소기업의 기술보호 역량을 강화하여 기술개발 여건을 조성하고, 기업의 기술경쟁력 제고 및 관련 산업발전에 기여하기 위한 목적으로 중소벤처기업부에서 수행하는 지원사업에 참여한 경험 여부 - 중소기업지원사업 수혜여부 (수혜/비수혜)	김택영 (2021) 서동진 (2016) 이인선 (2021) 곽재연 (2019) 신혁 (2018)
	보안 책임자	보안책임자의 역할 수행자	- 기업의 정보보호 관리체계를 관리하는 역할과 책임을 맡은 담당자 - 보안책임자(책임자 없음/외부전문가/부서책임자/보안전담팀/경영진참여)	김상균 외, 2016 박성환 (2020) 이은섭 (2020) 이홍제 (2018)
	기업 핵심정보 관리방식	기업 핵심정보 관리방식	- 기업 핵심자산인 중요정보를 보호하기 위한 관리방식 - 기업의 핵심 데이터 보호 위한 관리방식 (관리 안함/ 외부 전문서비스 이용/ 자체적으로 백업 관리)	성욱준 (2018) 이명렬 (2017) 이은섭 (2020)

보안 정책 품질, 보안 인력 품질, 보안 인프라 품질, 보안 프로세스 품질 등 독립변수의 의미는 다음과 같다. 보안 정책 품질은 보안관리정책과 인력관리정책으로 분류하였고, 보안관리정책은 조직의 안전한 보안체계를 위하여 자산 및 체계의 보안 활동을 지원하는 원칙이나 규율을 의미하고, 인력관리정책 내부/외부 인력의 보안 준수를 위한 원칙이나 규율을 의미한다. 보안 인력 품질은 보안인식관리과 인력관리로 분류하였고, 보안인식관리는 조직의 보안정책을 중심으로 교육 및 보안인식 관리를 말하며, 인력관리는 내부 임직원의 비밀유지와 퇴사 직원 및 외주업체 및 외주용역 등 외부자 보안규정 수립 및 관리를 의미한다. 보안인프라 품질은 자산관리와 출입통제로 분류하였고, 자산관리는 기업의 보안을 위하여 구축한 어플리케이션, 장비, 시설 등 보유 자산 및 장비의 보안체계를 뜻하며, 출입통제는 내·외부 인력의 중요자

산 보호를 위한 출입통제 및 정보화 기기 반입/반출 통제 전반을 뜻한다. 보안 프로세스 품질은 인력운영 프로세스, 시스템관리 프로세스, IT관리 프로세스로 분류하였고, 인력운영 프로세스는 임직원의 보안 활동 관리 또는 보안 절차를 말하며, 시스템관리 프로세스는 중요 자산 보호 위한 보안시스템 운영, 정기적 보안감사 등 정보시스템 전반 보안관리 또는 보안 절차를 의미하고, IT관리 프로세스는 정보시스템의 로그 및 최신 업데이트 등 보안관리 또는 보안 절차 등을 말한다.

종속변수인 침해사고 대응체계 구축수준의 의미는 다음과 같다. 침해사고 대응체계는 침해사고 대응을 위한 대응절차, 복구대책, 위기관리체계 등 수립 · 시행하는 보안관리 체계 등을 포함하였다. 중소기업지원사업 수혜여부와 보안책임자, 기업핵심정보 관리방식이다.

중소기업지원사업 수혜여부와 보안책임자, 기업핵심정보 관리방식 등 조절변수의 의미는 다음과 같다. 중소기업지원사업 수혜여부는 중소기업의 기술보호 역량을 강화하여 기술개발 여건을 조성하고, 기업의 기술경쟁력 제고 및 관련 산업발전에 기여하기 위한 목적으로 중소벤처기업부에서 수행하는 지원사업에 참여한 경험 여부이고, 수혜, 비수혜로 구분하여 조절효과를 검증하고자 한다. 보안책임자는 기업의 정보보호 관리체계를 관리하는 역할과 책임을 맡은 담당자를 의미하며, 책임자 없음, 외부전문가, 부서책임자, 보안전담팀, 경영진참여로 분류하여 조절효과를 검증하고자 한다. 기업핵심정보 관리방식은 기업 핵심자산인 핵심 데이터를 보호하기 위한 관리방식을 의미하며, 관리 안함, 외부 전문서비스 이용, 자체적으로 백업 관리로 분류하여 조절효과를 검증하고자 한다.

2019년 중소기업 기술보호 수준 실태조사의 설문조사 항목을 분석 데이터로 사용하였으며, 변수별 조작적 정의와 사용된 설문 문항에 대한 설명은 다음과 같다[표 3-2].

[표 3-2] 연구변수의 조작적 정의 및 연구변수별 적용 데이터

변수명	세부 변수명	조작적 정의	설문문항
보안 정책 (Governance)	보안관리정책	- 기술보호 및 보안규정 보유 여부 - 기술보호 및 보안 규정 정기적 검토 및 개정	Q1, Q6, Q24

변수명	세부 변수명	조작적 정의	설문문항
품질		- 정기적 보안감사 점검 실시 여부	
	인력관리정책	- 보안규정 위반 직원에 대한 징계절차 - 기술보호와 보안 담당 부서 및 인력 보유 여부	Q2, Q3_1
보안 인력 (People) 품질	보안인식관리	- 기술보호 필요성 인식 - CEO/임원/부서장/직원 - 기술보호방안/체계 추진의지 - CEO/임원/부서장/직원	Q7_1_1, Q7_1_2, Q7_1_3, Q7_2_1, Q7_2_2, Q7_2_3
	인력관리	- 기술보호 보안교육 실시 - 외주업체 및 외주용역 등 관리 보안규정	Q8, Q13
보안 인프라 (Technology) 품질	자산관리	- 보유자산 관리지침 마련 및 정기적 개정 - 중요 기술상/경영상 영업 비밀 자료 별도 보관	Q15, Q16
	출입통제	- 보안구역(통제구역/제한구역) 지정 · 운영 - 정보화기기(노트북, 스마트폰, 태블릿, USB, 외장하드, 디지털카메라 등) 반입 및 반출 통제	Q20, Q21
보안 프로세스 (Peocess) 품질	인력운영 프로세스	- '비밀유지서약서' 관리 - 핵심인력 '경쟁업체 전직금지 서약서' 체결	Q9, Q10
	시스템 관리 프로세스	- 물리적 보안 활동 실시 - 출입문, 캐비닛, 개인서랍 시건 여부 확인 - 문서 및 도면 방치여부 확인 - 노트북 방치 여부 확인 - PC전원 OFF 여부 확인 - 화면보호기설정 및 패스워드사용 여부확인	Q23_1, Q23_2, Q23_3, Q23_4, Q23_5
	IT 관리 프로세스	- 정보시스템 사용 로그(Log) 관리 - OS(운영체제), 백신 등 최신버전 업데이트 관리	Q25, Q26_1
침해사고 대응체계 구축효과	침해사고 대응체계 구축효과	- 기술유출 관련 사고 대응절차 - 주요시설 보호를 위해 자연재해, 재난, 전력장애, 보안사고 발생에 대비한 재해복구 및 위기관리체계 수립 · 시행	Q29, Q31
수혜여부	중소기업지원 사업 수혜여부	- 중소기업지원사업 수혜여부 (수혜/비수혜)	수혜여부
보안책임자	보안책임자의 역할 수행자	- 보안책임자 (책임자 없음/외부전문가/부서책임자/보안전담팀/ 경영진참여)	Q5_1
기업핵심정보 관리방식	기업 핵심정보 관리방식	- 기업의 핵심 데이터 보호위한 관리방식 (관리 안함 / 외부 전문서비스 이용/ 자체적으로 백업 관리)	Q22

5.3. 연구가설

1) 보안 활동과 침해사고 대응체계 구축수준과의 관계

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, 인적보안으로 제시하였다(송재혁, 2021). 중소기업의 현실상 보안시설 구축에 많은 비용을 투자할 수 없는 관계로 내부, 출입자 등의 관리 위주의 점검할 수 있도록 관리적보안, 기술적보안, 물리적보안으로 중소기업 산업보안 점검 체크리스트를 제시하였다(이호준, 2020). 이와 같은 기존 연구를 기반으로 사이버 침해사고 대응을 위한 관리체계 구축에 미치는 영향을 구체화하여 분석하기 위하여 보안 활동을 세분화 하였다.

침해사고 대응체계는 사후대응 체계에서 예방과 사전탐지 중심으로 바뀌어야한다. 기업의 침해사고 예방을 위한 제도적 보완장치가 모든 기업들의 정보보호 이슈를 제거하지는 못한다. 대부분의 제도적 보완장치는 수행기관과 대상자간의 점검 및 목표 설정, 모델 적용이 한계이고 실제 상황에서는 진단대상자 내부의 실행조치가 더욱 중요하다. 또한, 보호조치가 시행 중인 기업의 침해사고 대응 모델의 효율을 극대화시키기 위해서는 위협 발생 상황에 대한 초기 대응이 중요하다(강신범 외, 2012). 침해사고대응활동은 크게 3가지로 구분하는 바, 사이버공간의 안정성 확보를 위한 예방활동으로 안전대책 수립 시행, 정보보호시스템 도입운영, 취약점 분석 및 평가 등이며 탐지 및 대응활동으로는 보안관제와 예·경보, 사고조사 및 복구, 마지막으로 연구 개

발활동으로 분류된다(안종하, 2013). 이와 같은 기존 연구를 기반으로 사이버 침해사고 대응체계 구축에 대한 연구가설을 설정하여 분석하고자 한다.

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.

2) 중소기업지원사업 수혜 여부에 따른 조절 효과

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). 본 연구에서는 중소기업 지원사업 수혜 경험이 각 보안 활동과 침해사고 대응체계 구축 간의 영향관계를 알아보고자 한다. 정부 지원사업은 단순 재정적 지원뿐만 아니라, 중소기업의 현황 파악은 물론 정보보호 인식개선의 효과, 보안교육의 효과를 가져올 수 있기 때문이다(중소기업연구원, 2017). 이에 중소기업 지원사업 수혜 여부가 가지는 효과를 확인하고자 한다.

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

H5-1-1: 보안관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-2: 인력관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-3: 보안인식관리가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-4: 인력관리가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-5: 자산관리가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-6: 출입통제가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-7: 인력 운영 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-8: 시스템관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

H5-1-9: IT관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.

3) 보안책임자의 역할 수행자에 따른 조절 효과

기업들이 아웃소싱을 고려하는 이유를 간단히 설명하면 비용절감과 위험분산, 정보시스템의 성과향상을 통해 기업 운영의 생산성과 효율성을 극대화하여 고유의 핵심 업무에 집중할 수 있도록 지원하는 것에 있다. 수익성과 차별화된 서비스를 제공해 주는 외주용역 업체와 계약을 하지 않을 수 없게 되었다. 이에 따라 대다수의 기업에서 정보시스템의 관리, 보안, 운용을 위한 외주용역 활용이 증가하고 있다(이은섭, 2020). 전문적인 능력이 요구되는 보안책임자의 역할을 누가 수행하는가에 따라 그 기업의 보안역량은 크게 달라질 것이다. 경영진이 직접 참여하여 보안정책과 보안관리체계가 일관성 있게 관리 할 수 있는 환경을 갖출 수 있는가, 사내의 보안전담팀을 둘 것인가 아니면 부서에 어느 정도 보안지식을 갖은 보안책임자를 둘것인가, 또는 아웃소싱을 통한 외부전문가를 통한 관리를 받을 것인가. 보안책임자의 역할을 누가 수행하는가에 따른 효과를 확인하고자 한다.

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

H6-1-1: 보안관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-2: 인력관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-3: 보안인식관리가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-4: 인력관리가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-5: 자산관리가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-6: 출입통제가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-7: 인력 운영 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-8: 시스템관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

H6-1-9: IT관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.

4) 기업핵심정보 관리방식에 따른 조절 효과

시스템이나 데이터에 대한 백업은 기술 관리적 측점에서 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 복구 까지 걸리는 시간을 줄일 수 있는 것으로 나타났다(성욱준, 2018). 이런 선행연구를 바탕으로 기업 핵심자산인 중요정보를 보호하기 위한 관리방식을 외부 전문서비스 이용하는지, 자체적으로 백업관리를 하는지에 따른 효과를 분석하고자 한다.

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

H7-1-1: 보안관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-2: 인력관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-3: 보안인식관리가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-4: 인력관리가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-5: 자산관리가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-6: 출입통제가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-7: 인력 운영 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-8: 시스템관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

H7-1-9: IT관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.

Ⅳ. 실증분석 및 결과

6.1. 연구방법

6.1.1. 자료분석 도구 및 방법

본 연구는 보안체계의 각 보안 활동이 사이버 침해사고 대응에 미치는 영향에 대한 연구모형 및 가설을 검증하기 위해, 중소기업 기술보호 실태조사의 데이터를 활용하여, 표본의 특성도출 및 기술적 통계, 측정항목의 분석, 연구모형 및 가설에 대한 검증을 진행하였다. 분석결과를 바탕으로 중소기업의 사이버 침해사고 대응에 영향을 미치는 요인들을 SPSS 23.0과 AMOS 22.0.0을 이용하여 분석하였다.

연구데이터가 제대로 된 것인지 확인하기 위하여 SPSS를 이용하여 탐색적 요인분석(Exploratory Factor Analysis, EFA)을 한 후에 그룹화된 요인분석과 신뢰도 분석을 하였다. 탐색적 요인분석에 더불어 측정 모델 검정과 구조모델 검정을 수행하기 위하여 타당성 검증을 수행하였다. 연구모형과 연구가설 검증을 위하여 AMOS으로 구조방정식 모형을 분석하였고, 조절변수의 효과는 χ^2 차이 검정 및 경로별 표준화경로계수를 비교하여 분석하였다.

6.1.2. 연구 대상 및 표본의 특성

본 연구는 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 사업이

다.

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 4-1]와 같다.

[표 4-1] 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 2,700개, 중견기업 200개, 대기업 200개)

2019년 중소기업 기술보호 수준 실태조사의 인구통계적 특징은 아래와 같다[표 4-2].

[표 4-2] 표본의 인구통계적 특징

구분			표본 수	비율
전체			2,900	100
기업규모	중소기업	수혜기업	750	25.9
		비수혜기업	1,750	60.3
	중견기업		200	6.9
	대기업		200	6.9
상시	1~9인		597	20.6

구분		표본 수	비율
종업원 수	10~19인	721	24.9
	20~49인	755	26
	50~99인	323	11.1
	100~299인	273	9.4
	300인 이상	231	8
총 매출액	10억 원 미만	409	14.1
	10~50억 원 미만7	1,090	37.6
	50~100억 원 미만	425	14.7
	100~500억 원 미만	541	18.7
	500억 원 이상	435	15
주력업종	전기/전자	619	21.3
	화학/섬유	408	14.1
	기계/소재	637	22
	정보/통신	347	12
	바이오/의료	232	8
	에너지자원	67	2.3
	지식서비스	102	3.5
	기타	488	16.8

2019년 중소기업 기술보호 수준 실태조사의 역량평가 모형은 기술보호 정책 수립 및 운영, 기술보호 정책 관리, 인력 관리, 외부자 관리, 자산 및 장비 관리, 출입통제, 운영관리, IT관리, 사고/재해 관리의 총 9개 부문으로 구성하였다. 표본추출 조사대상 적합성 검토, 표본설계, 설문지 개편, 시계열 연속성 보전방안 등 문제점 개선을 위해 중소기업 기술보호수준 실태조사 개선 용역 및 연구회 운영을 통해 2019년 최종 역량평가 모형을 확정하였다. 기술보호 역량평가 모형의 배점 기준과 역량평가 모형은 다음과 같다[표 4-3]. 해당 조사는 핵심기술을 보유한 중소기업의 기술유출 실태를 파악하고 기업들의 기술보호 역량 수준에 대한 정확한 진단을 위해 실시하는 실태조사이다.

[표 4-3] 2019년 중소기업 기술보호수준 실태조사 역량평가 기준

구분	평가부문		점수(점)	가중치(%)
역량평가 배점 기준	기술보호 정책	기술보호 정책 수립 및 운영	20	22
		기술보호 정책 관리	8	8
	관리적 보호방안	인력 관리	28	17.5
		외부자 관리	8	10
	물리적 보호방안	자산 및 장비 관리	8	7.5
		출입 통제	20	7.5
	기술적 보호방안	운영 관리	16	10
		IT관리	16	10
	사고/재해 관리		12	7.5
총계			**136**	**100**

6.1.3. 연구 데이터 전처리

중소기업 기술보호 수준 실태조사는 중소기업의 기술보호 수준을 파악할 수 있는 지표로서, 실태조사에 대하여 중소기업이 느끼고 있는 응답시간에 대한 부담, 응답 시 설문지 문항 및 보기의 용어에 대한 어려움 등으로 인하여 설문 문항과 보기가 이해하기 쉽도록 단순화되어 있다. 또한, 각 문항별로 묻고 있는 기술보호 내용과 수준이 다르기 때문에 문항의 척도가 균일하지 않다. 이에 따라 중소기업 기술보호 수준 실태조사의 2차 데이터를 활용하기 위해서 일부 정제하여 연구 데이터로 사용하였다. 일관성 있는 변수의 활용 및 분석을 위해 비율척도 데이터는 제거하였고, 5점 척도로 구성되지 않은 데이터를 제거하거나 5점 척도에 맞추어 변환 및 정제하였다[표 4-4].

[표 4-4] 실태조사 데이터 구성 및 연구 적용 현황

실태조사 구분			연구 항목
기술보호역량 및 수준	기술보호 정책	기술보호 정책 수립 및 운영	보안관리정책
			인력관리정책

실태조사 구분			연구 항목
		기술보호 정책 관리	인력관리정책
			보안인식관리
	관리적 보호 방안	인력 관리	인력관리
			인력운영 프로세스
		외부자 관리	인력관리
	물리적 보호 방안	자산 및 장비 관리	자산관리
		출입통제	출입통제
	기술적 보호 방안	운영관리	시스템 관리 프로세스
		IT보안 관리	IT관리 프로세스
	사고/재해 관리	사고/재해 관리	침해사고 대응체계 구축수준

특히 조절효과를 확인하기 위한 설문문항은 아래와 같이 코딩하여 정리하였다[표 4-5].

[표 4-5] 조절변수의 데이터 코딩 사례

연구변수	측정방법	데이터 전처리 결과	
중소기업지원 사업 수혜여부	비수혜	비수혜	1
	수혜	수혜	2
보안책임자	보안감사 실시 책임자 없음	책임자 없음	1
	외부 전문가	외부전문가	2
	부서별 보안관리자	부서책임자	3
	보안전담부서 및 보안전담관리자	보안전담팀	4
	대표이사 및 임원급	경영진참여	5
기업 핵심정보 관리방식	관리 안함	관리 안함	1
	외부 전문서비스 이용	외부 전문서비스 이용	2
	자체적으로 비정기적 백업 관리	자체적으로 백업 관리	3
	자체적으로 정기적 백업 관리		

6.1.4. 표본의 기술적 통계

연구 데이터가 평균을 중심으로 퍼져 있는 정도를 확인하고, 데이터의 대칭도와 정규분포와 어떻게 다른지 확인하고자 표준편차와 왜도, 첨도를 확인하였다. 왜도는 데이터의 대칭도를, 첨도는 정규분포곡선에 분포의 중간이나 꼬리에 있는 점수의 비율이 상대적으로 어느 정도인가를 의미한다. 왜도는 절대값이 3보다 큰 경우, 첨도가 절대값이 8.0 이상은 극단적인 첨도로 해석할 수 있다.

보안 활동과 침해사고 대응체계 구축수준에 대한 평균과 표준편차를 살펴보면, 보안 정책 품질은 평균 3.53, 표준편차 1.38, 보안 인력 품질은 평균 3.23, 표준편차 1.19, 보안 인프라 품질은 평균 2.92, 표준편차 1.53, 보안 프로세스 품질은 평균 2.98, 표준편차 1.53, 침해사고 대응체계 구축수준은 평균 3.09, 표준편차 1.65로 나타났다. 보안 활동 중 보안 인프라 품질와 보안 프로세스 품질이 3 이하로 나타났으며, 보안정책 품질이 3.53으로 가장 높은 것으로 확인되었다.

본 연구에서는 표준편차가 3 이상, 왜도의 절대값이 3보다 큰 경우 그리고 첨도의 절대값이 8.0 이상이 없으므로 개별 측정변수들은 정규분포를 가지는 것으로 볼 수 있다[표 4-6].

[표 4-6] 연구변수의 기술적 통계

구분		평균	표준편차	평균	표준편차	왜도	첨도
보안 정책 품질	Policy1	3.53	1.38	4.128	1.426	-1.421	.473
	Policy2			3.297	1.758	-.293	-1.643
	Policy3			3.782	1.301	-1.164	.287
	Policy4			3.080	1.179	-.009	-.131
	Policy5			3.359	1.222	-.120	-.473
보안 인력 품질	People1	3.23	1.19	3.437	1.038	-.299	-.407
	People2			3.374	1.061	-.426	-.266
	People3			3.242	1.076	-.366	-.356

구분		평균	표준편차	평균	표준편차	왜도	첨도
	People4			3.298	1.002	-.237	-.294
	People5			3.191	1.049	-.308	-.333
	People6			3.096	1.054	-.260	-.415
	People7			3.590	1.429	-.501	-.933
	People8			2.592	1.788	.411	-1.624
보안 인프라 품질	Infra1	2.92	1.53	3.198	1.573	-.176	-1.364
	Infra2			3.858	1.493	-.883	-.673
	Infra3			2.675	1.637	.353	-1.474
	Infra4			1.936	1.404	1.176	-.102
보안 프로세스 품질	Process1	2.98	1.53	3.976	1.657	-1.114	-.616
	Process2			2.328	1.762	.638	-1.487
	Process3			2.874	1.549	.204	-1.443
	Process4			2.758	1.432	.329	-1.198
	Process5			2.751	1.535	.323	-1.378
	Process6			3.092	1.658	-.041	-1.645
	Process7			2.699	1.514	.385	-1.292
	Process8			2.986	1.577	.013	-1.392
	Process9			3.314	1.065	.131	.156
침해사고 대응체계 구축수준	Response1	3.09	1.65	3.139	1.573	-.250	-1.410
	Response2			3.048	1.729	-.046	-1.662

6.2. 구조방정식모형을 통한 실증 분석

6.2.1. 측정항목 분석

6.2.1.1. 탐색적 요인분석과 신뢰성 분석

본 연구모형의 구성요소는 추상적인 개념을 포함하고 있어, 연구 조사의 타당성과 신뢰성을 확보하는 것이 매우 중요하다. 신뢰성(reliability)은 연구자가 설문 조사를 다시 반복한다고 가정할 때 그 결과가 얼마나 원래 측정치와 일치하는지를 나타내는 척도이고, 타당성(validity)은 측정하려는 추상적인 개념이 측정 도구에 의해 얼마나 정확하게 측정되었는지를 판단하는 기준이다(이홍제, 2018).

이를 위해 연구모형의 검정을 위한 구조방정식 경로 모형의 분석에 앞서 SPSS를 이용하여 탐색적 요인분석을 한 후에 그룹화된 요인분석과 신뢰도 분석을 하였다. 측정도구의 타당성 검정을 위하여 주성분분석(principal component analysis)을 수행하였고, KMO와 Bartlett의 구형성 검정, 직교회전(varimax)방법을 적용하여 실시하였다. KMO와 Bartlett의 구형성 검정은 요인분석 모형의 적합도를 파악하는 것으로, KMO 값은 0.6 이상일 때, 엄격하게는 0.7 이상일 때 받아들일 수 있는 수준으로 내적 일관성이 있다고 판단하고(Hair et al., 1998), Bartlett의 구형성 검정에서는 p값이 유의수준인 .05 미만으로 나타나면 요인분석 모형이 적합한 것으로 판단한다.

본 연구에서는 KMO 측도는 .912로 나타났고, Bartlett의 구형성 검정 결과도 유의확률이 .05미만으로 나타나 요인분석 모형이 적합한 것으로 판단하였다. 또한, 누적분산이 59.019%로 나타나, 60%가 조금 안되긴 하지만 60%에 근사하므로 구성된 4개 요인의 설명력이 진행 가능한 수준인 것으로 판단하였다[표 4-7].

신뢰도 분석은 요인분석 결과를 어느 정도 신뢰할 수 있는가를 확인하는 과정이다(노경섭, 2019). 요인별로 상호 비교가 가능한 독립된 측정방식에 대하여 측정된 결과가 서로 유사하게 나타나는 것으로 의미한다. 각 변수에 대한 크론바흐 알파(Cronbach's α) 값이 0.7보다 높아야 한다(Hair et al.,

1998). 분석결과 각 변수들의 Cronbach's α값은 [표 4-7]과 같이 모든 요인이 0.7 이상으로 신뢰성을 가지고 있는 것으로 나타났다.

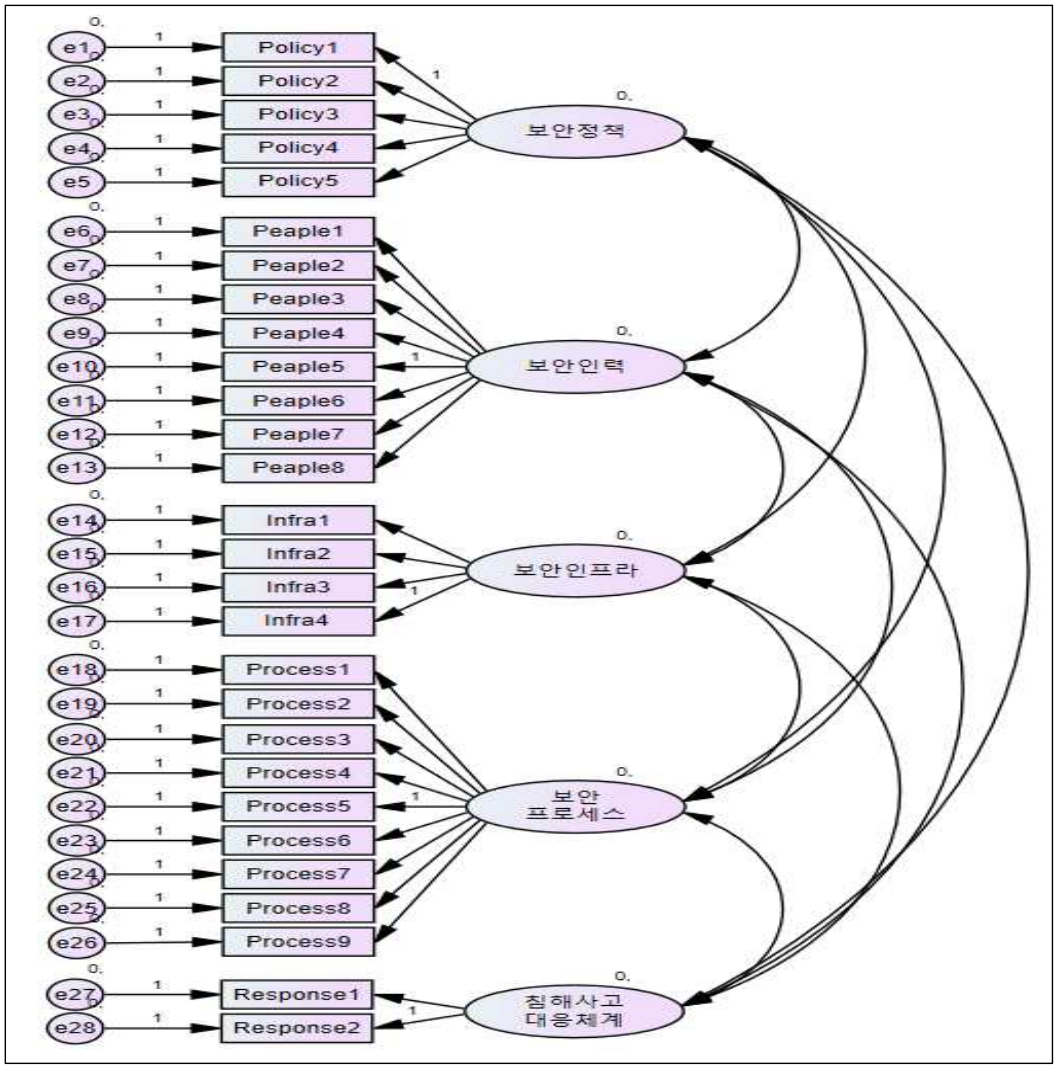
[표 4-7] 탐색적 요인분석과 신뢰도 분석결과

항목	1	2	3	4	Cronbach's α
Policy1	.822	.214	-.124	.097	0.822
Policy2	.688	.240	.025	.029	
Policy3	.435	.300	.107	.239	
Policy4	.854	.189	-.079	.077	
Policy5	.639	.135	.182	.134	
People1	.285	.811	.065	.094	0.851
People2	.241	.826	.056	.091	
People3	.219	.837	.061	.115	
People4	.176	.850	.097	.113	
People5	.097	.881	.113	.138	
People6	.057	.857	.107	.168	
People7	.612	.174	.093	.133	
People8	.490	.058	.408	.131	
Infra1	.693	.045	.331	.115	0.703
Infra2	.498	.003	.342	.072	
Infra3	.261	.202	.665	.154	
Infra4	.244	.146	.657	.189	
Process1	.488	.179	.168	.111	0.803
Process2	-.003	.024	.460	.030	
Process3	.072	.158	.139	.769	
Process4	.243	.092	.120	.813	
Process5	.180	.161	.101	.843	
Process6	.115	.142	.041	.840	
Process7	.162	.086	.158	.827	
Process8	.582	.052	.266	.204	
Process9	.351	.045	.315	.132	
Eigen Value	5.017	4.742	3.719	1.868	-
공통분산(%)	19.296	18.238	14.302	7.183	
누적분산(%)	19.296	37.533	51.836	**59.019**	
KMO=.912, Bartlett's X^2= 44,449.488(p=0.000)					

$p^{*}<0.1$, $p^{**}<0.05$, $p^{***}<0.01$

6.2.1.2. 타당성 분석

위의 탐색적 요인분석에 더불어 측정 모델 검정과 구조 모델 검정을 수행하기 위하여 타당성 검증을 수행하였다. 타당성 검증은 집중 타당성(Convergent Validity)과 판별 타당성(Discriminant Validity)으로 검토하였다(Gefen et al., 2005). 집중 타당성, 판별 타당성을 검증하기 위해 Amos를 이용하여 확인적 요인분석(Confirmatory Factor Analysis, CFA)을 하였다[그림 4-1].



[그림 4-1] 확인적 요인분석 모형

본 연구에서는 2019년도 중소기업 기술보호 수준 실태조사의 2차 데이터를 활용하고 있다. 이에 실태조사에서 구성한 설문문항을 연구자의 판단과 탐색적 요인분석을 통하여 연구모형에 적용을 하여, 본 논문에서 수립한 연구변수와 연구모형이 적정한지 1차적으로 보안전문가를 통하여 정성적인 검증을 수행하였고, 2차적으로 모형 적합도 및 확인적 요인분석을 수행하여 적정성을 검증하였다. 정성적 검증을 위한 보안 전문가는 보안 분야에서 5년 이상 경력을 가진 보안 컨설턴트 5명이 참여하여 독립변수로 사용하는 각 보안 활동의 세분화된 분류 구분의 적정성과 보안활동과 사이버침해사고 대응체계 구축수준 간의 영향 분석에 대한 연구모형의 적정에 대한 검증을 수행하여 모형적합도를 확보하였다.

모형적합도 지수(goodness of fit index)는 연구모형이 자료에 어느 정도 적합한지를 알려주는 지수로, 크게 절대 적합도 지수(absolute fit index), 증분 적합 지수(incremental fit index) 등으로 구분이 된다. 절대 적합도 지수는 수집된 자료와 연구 모델이 부합되는 정보를 절대적으로 평가하는 지수로 CMIN(χ^2), CMIN/df, RMR, RMSEA 등의 지수를 이용하여 측정하며, 연구모델과 구조 모형에 대하여 전반적인 모델의 적합도를 평가한다. 증분 적합도 지수는 연구자의 구조방정식 모델과 변수 간 상관을 설정하지 않는 모델(영모델)을 비교하여 얼마나 정확하게 측정되었는지를 나타내는 지수로 NFI, TLI, CFI, IFI 등이 있다(배병렬, 2011). 확인적 요인분석에 의한 적합도 분석결과는 아래 [표 4-8]와 같이 각각 RMSEA=0.092, NFI=0.8, TLI=0.795, CFI=0.815, IFI=0.816인 것으로 분석되었다. 분석결과 각 적합도 지수는 최적의 임계치 기준에는 다소 벗어난 보통 수준이나 선행연구 결과 허용한 수준으로 확인하였다(박병우, 2018).

[표 4-8] 확인적 요인분석의 모형 적합도

적합도 지수		임계치 기준	결과 값	판정
절대적합도 지수	CMIN(χ^2)	-	340	-
	CMIN/df	1.0~2.0	3.737	수용가능
	p-value		0.000	적절

적합도 지수		임계치 기준	결과 값	판정
	RMSEA	0.05~0.08	0.092	수용가능
증분적합도 지수	NFI	> 0.90	0.8	수용가능
	TLI	> 0.90	0.795	수용가능
	CFI	> 0.90	0.815	수용가능
	IFI	> 0.90	0.816	수용가능

1) 집중 타당성 분석

집중 타당성은 한 변수에 대하여 측정한 여러 개의 항목들이 보이는 상관관계의 정도를 나타내는 것으로, 그 값이 클수록 타당성이 높다고 할 수 있다. 본 연구에서는 집중타당성을 다음과 같이 검정하였다. 먼저, 해당 잠재변수와 각 항목과의 관련 정도를 나타내는 표준화 경로계수(Standardized Path Loadings)값이 0.7보다 높고 통계적으로 유의해야 한다(Gefen et al., 2000). 다음으로, 각 변수에 대한 평균추출분산(AVE)가 0.5를 상회해야 한다(Fornell et al,, 1981). 분석결과, 개별 측정변수들의 표준화 경로계수는 대부분 0.7 이상으로 나타났고, 통계적으로 유의한 것으로 확인되었다. CR은 0.7 이상으로 나타났다. 그리고 AVE는 0.5 이상이므로 집중타당도는 확보되었다고 평가할 수 있다[표 4-9].

[표 4-9] 연구변수의 집중 타당도 분석결과

항목		표준화계수	S.E.	t값	p값	C.R.	AVE
보안 정책	Policy1	0.887				0.978	0.908
	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	***		

항목		표준화계수	S.E.	t값	p값	C.R.	AVE
보안 인력	People1	0.895				0.992	0.943
	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
	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
	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	***		
대응 체계	Response1	0.8				0.897	0.814
	Response2	0.715	0.059	16.753	***		

*p<0.01 수준에서 유의함

2) 판별 타당성 분석

다음으로 판별 타당성을 확인하였다. 판별 타당성은 서로 다른 잠재변수 간의 차이를 나타내는 정도를 말하는데, 잠재변수 간에 상관관계가 낮아야 한다. 잠재변수 간에 높은 상관을 보이면 두 구성 개념 간에는 차별성이 떨어지는 것을 의미하기 때문에 잠재변수 간에 판별 타당성이 없다는 것이다(우종필, 2012). 구조방정식 모형의 판별 타당성을 확보하기 위해서는 두 요인 사이에서 구한 평균 분산 추출(AVE) 값이 개념 간 상관계수의 제곱 값보다 반드시 커야 한다(Fornell & Larcker, 1981).

분석결과, 아래 [표 4-10]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 4-10] 구성개념 간의 판별 타당도 분석결과

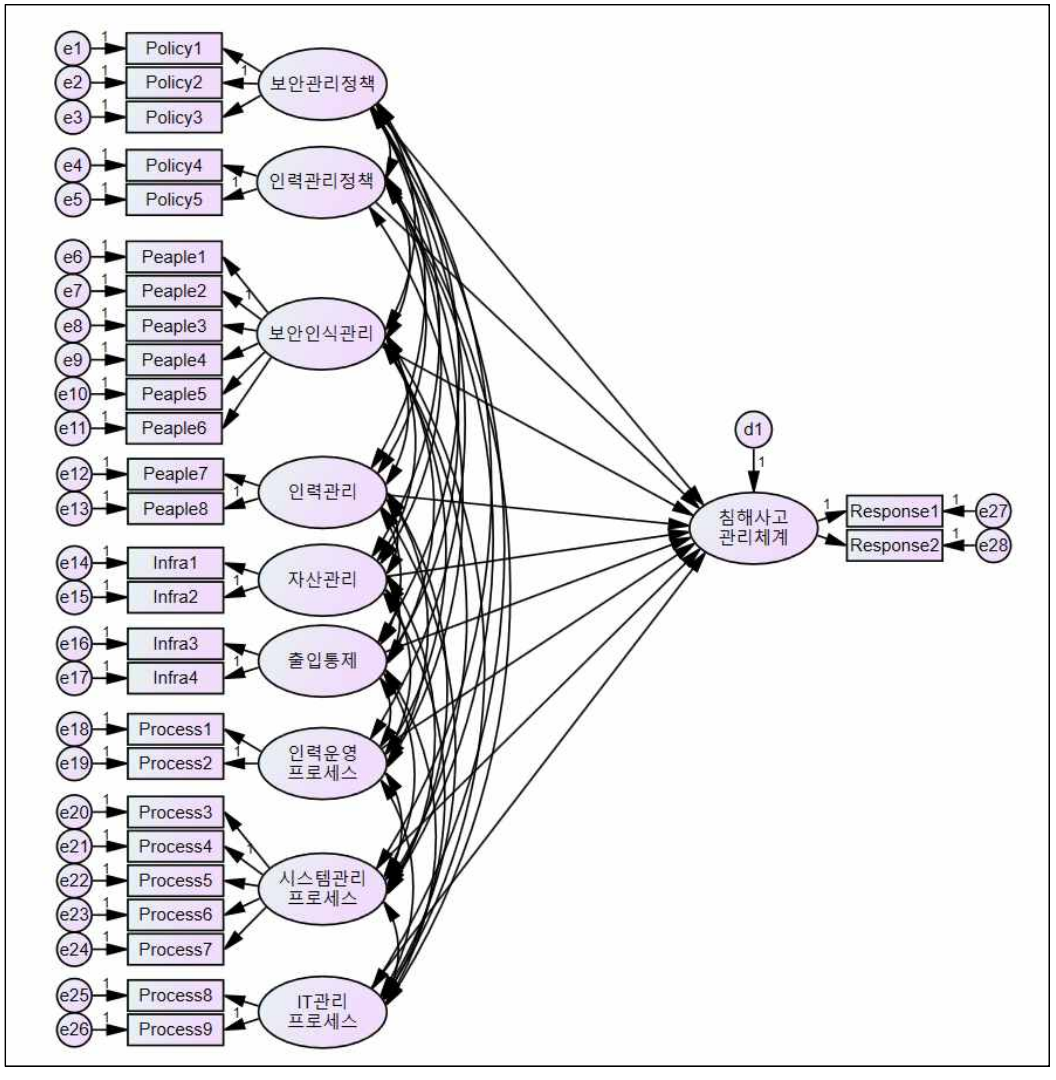
구분	정책	인력	인프라	프로세스	대응체계
정책	**0.953**				
인력	0.42	**0.972**			
인프라	0.68	0.467	**0.928**		
프로세스	0.309	0.333	0.51	**0.876**	
대응체계	0.598	0.335	0.76	0.521	**0.903**

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

6.2.2. 가설검증

6.2.2.1. 구조모형 분석과 가설 검증

본 연구는 각 보안 활동과 침해사고 대응체계 구축수준 간의 관계에 대한 가설을 검증하기 위해 [그림 4-2]와 같이 구조방정식 모형을 구성하였다.



[그림 4-2] 구조방정식 모형

본 연구모형의 구조방정식 모형 분석에 의한 적합도 분석결과는 각각 RMSEA=0.1, NFI=0.8, TLI=0.728, CFI=0.749, IFI=0.75인 것으로 분석되었다. 적합도 평가에 있어서 연구모형의 변수의 크기, 연구표본에 대한 설문에 의한 크기 등에 따라서 직접적인 영향을 받는다고 볼 수 있다. 본 연구모형에 대한 분석모형과 적합성 분석현황을 요약한 결과는 [표 4-11]과 같다. 분석결과 각 적합도 지수는 최적의 임계치 기준에는 다소 벗어난 보통 수준이나 선행연구 결과 허용한 수준으로 확인하였다(박병우, 2018).

[표 4-11] 구조모형 분석의 모형 적합도

적합도 지수		임계치 기준	결과 값	판정
절대적합도 지수	CMIN(χ^2)	-	1385.1	-
	CMIN/df	1.0~2.0	3.184	수용가능
	p-value		0.000	적절
	RMSEA	0.05~0.08	0.1	수용가능
증분적합도 지수	NFI	> 0.90	0.8	수용가능
	TLI	> 0.90	0.728	수용가능
	CFI	> 0.90	0.749	수용가능
	IFI	> 0.90	0.75	수용가능

구조모형 분석에서 비표준화경로계수는 회귀분석(regression analysis)의 B계수이며, 표준화경로계수는 베타계수 (beta coefficient)와 같다. 즉, 비표준화경로계수의 수치는 원인변인이 한 단위 변화할 때 영향을 받는 결과변인의 변화량을 의미한다. 그리고 하나의 결과변인에 두개 이상의 원인변인이 존재한다면, 계수는 다른 원인변인들의 효과를 통제한 상태에서, 한 원인이 변화할 때 영향을 받는 결과변인의 정도를 말한다. 즉, 원인변인의 고유한 직접효과크기를 의미한다. 구조모형의 표준화경로계수 β와 p값을 확인하여 가설의 유의한 영향도를 파악할 수 있다.

연구 모델의 요인들 간의 인과관계를 분석을 위해 [그림 4-2]와 같이

Amos 구조방정식 모형을 구성하였고, 분석 결과는 [표 4-12]과 같다. 가설 검증 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. 구조방정식 모형에서 설명력은 독립변수에 의해 설명되는 종속변수의 분산 양을 의미하는 R^2를 이용한다. 본 연구의 경우 독립변인인 보안 활동이 종속변인 침해사고 대응체계(43.8%)에 유의한 영향을 미치는 것으로 확인되고 있다.

[표 4-12] 구조방정식분석에 의한 가설검증 결과

경로		Estimate		S.E.	C.R.	p값	검증결과	R^2
		B	β					
보안정책 품질	대응체계 ← 보안관리정책	0.157	0.121	0.028	5.688	***	지지	.438
	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

보안정책 품질(H1)은 보안관리정책(β=0.121, t값=5.688)과 인력관리정책(β=0.059, t값=2.915)이 모두 유의수준 내에 있는 것으로 확인되어, 침해

사고 대응체계 구축수준에 정(+)으로 유의한 영향을 주는 것으로 분석되었다. 보안정책 중에서는 보안관리정책이 인력관리정책보다 침해사고 대응체계 구축수준에 영향도가 큰 것으로 나타났다. 보안인력 품질(H2)은 보안인식관리(β=−0.014, t값=−0.875)가 유의하지 않는 것으로 확인되어, 인력관리(β=0.124, t값=6.338)만이 침해사고 대응체계 구축수준에 정(+)으로 유의한 영향을 주는 것으로 분석되었다. 보안인프라 품질(H3)은 자산관리(β=0.176, t값=9.432)와 출입통제(β=0.078, t값=4.627)가 모두 유의수준 내에 있는 것으로 확인되어, 침해사고 대응체계 구축수준에 정(+)으로 유의한 영향을 주는 것으로 분석되었다. 보안인프라 중에서는 자산관리가 출입통제보다 침해사고 대응체계 구축수준에 영향도가 큰 것으로 나타났다. 보안프로세스 품질(H4)은 인력운영 프로세스(β=0.059, t값=3.834), 시스템관리 프로세스(β=0.15, t값=9.455), IT관리 프로세스(β=0.173, t값=9.769)가 모두 유의수준 내에 있는 것으로 확인되어, 침해사고 대응체계 구축수준에 정(+)으로 유의한 영향을 주는 것으로 분석되었다.

6.2.2.2. 조절효과 검증

연구모형에서 중소기업이 구축한 정보보호 관리체계의 각 보안 활동이 사이버 침해사고 대응체계에 미치는 영향에 있어서, 중소기업 지원사업의 수혜 여부와 보안책임자의 역할 수행자 그리고 기업의 핵심정보를 관리방식에 따른 조절 효과를 분석하고자 한다.

조절변수는 종속변수에 대한 독립변수의 효과를 조절하는 변수이다. 조절변수는 독립변수와 종속변수 간에 영향을 주는 외부변수로서 독립변수와의 상호작용을 통해 종속변수의 영향력에 변화를 주는 것으로 해석할 수 있다. 즉, 조절변수의 투입으로 인해 종속변수의 결과에 변화를 주는지를 확인하여 조절 효과를 확인할 수 있다.

본 논문에서는 AMOS에서 조절 효과 분석은 교차타당성을 검증하기 위해 모형별 χ^2 검정을 비교하고, 경로별 차이를 검증하는 방법으로 분석하였다(노경섭, 2019). 기본 구조방정식 모형에 기초하여 서로 다른 집단의 경로계수의 크기를 가지고 서로 통계적으로 유의한 차이가 있는지를 보고자 한다.

동일한 모 집단에서 추출한 두 표본에서 동일한 분석결과를 얻을 수 있는가를 판단하기 위해서 다중집단 확인요인분석을 통해서 교차타당성을 검증한다. 교차타당성을 검증하기 위해서는 측정동일성(measurement equivalence)에 대한 분석이 필요하다. 측정동일성을 확인하기 위해 형태의 동일성으로 비제약 모델(unconstrained model)형태로 집단 간 어떠한 제약도 하지 않은 모델과 요인부하량 동일성으로 요인부하량 제약모델(λ constrained model) 형태로 집단 간 요인 부하량을 동일하게 제약하는 모델의 차이를 보았다(윤태호, 2019).

1) 중소기업 지원사업 수혜 여부에 따른 조절 효과

중소기업 지원사업 수혜 여부에 따른 따른 조절 효과의 가설검증 결과는 비수혜기업(C1)와 수혜기업(C2)에 따라 모형별 χ^2 검정을 비교는 [표 4-13], 경로별 차이를 검증에 따른 가설검증 결과는 [표 4-14]와 같이 나타났다.

[표 4-13] 지원사업 수혜여부에 따른 모형 비교

모형	χ^2	DF	P값	χ^2/DF	RMSEA	NFI	TLI	CFI
비제약	17.098	9	0.047	1.9	0.027	0.996	0.978	0.998
제약	28.724	10	0.001	2.872	0.039	0.993	0.955	0.995
차이비교	11.626	1	0.001					

*p<0.05 수준에서 유의함

[표 4-14] 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←	0.054	2.258	0.024	0.067	1.736	0.083

구분	경로	비수혜 기업(C1)			수혜 기업(C2)		
		β	C.R.	p값	β	C.R.	p값
	인력관리정책						
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

모형별 χ^2 검정을 비교 결과는 비제약모형과 제약모형 모두 P값이 유의수준이고, χ^2/DF는 1.9와 2.872로 적정수준으로 나타났다. 비제약모형과 제약모형의 차이는 DF=1(10-9)일 때, $\Delta\chi2$=11.626(28.724-17.098)이고 p값은 0.001로 통계적으로 유의함을 알 수 있다. 따라서 지원사업 수혜여부는 조절 효과가 있다고 할 수 있다.

중소기업 지원사업 수혜 여부에 따른 조절 효과를 검증한 결과, 보안인식관리→침해사고 대응체계는 비수혜기업(β=-0.006, t값=-0.304, p값=0.761), 수혜기업(β=-0.036, t값=-1.152, p값=0.249) 모두 p값이 유의수준에 미치지 못하여 가설이 지지되지 못하였고, 인력관리정책→침해사고 대응체계(β=0.067, t값=1.736, p값=0.083)는 수혜기업에서 p값이 유의수준에 미치지 못하여 가설이 지지되지 못하였다. 이외의 경로는 중소기업지원사업 수혜 여부에 따른 조절 효과가 유의하게 나타나서 가설이 지지되었다.

각 보안 활동이 침해사고 대응체계에 미치는 유의한 영향도를 파악하고자 표준화경로계수 β와 p값을 확인한 결과, 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 타나났다.

2) 보안책임자의 역할 수행자에 따른 조절 효과

보안책임자의 역할을 누가 수행하는가에 따른 조절 효과의 가설검증 결과는 책임자 없음(C1), 외부전문가(C2), 부서책임자(C3), 보안전담팀(C4), 경영진참여(C5)에 따라 모형별 χ^2 검정을 비교는 [표 4-15], 경로별 차이를 검증에 따른 가설검증 결과는 [표 4-16], [표 4-17]와 같이 나타났다.

[표 4-15] 보안책임자에 따른 모형 비교

모형	χ^2	DF	P값	χ^2/DF	RMSEA	NFI	TLI	CFI
비제약	88.619	36	0.000	2.462	0.022	0.988	0.954	0.993
제약	100.527	40	0.000	2.513	0.023	0.986	0.953	0.992
차이비교	11.908	4	0.018					

*p<0.05 수준에서 유의함

[표 4-16] 보안책임자에 따른 조절효과 가설검증 결과(1)

구분	경로	책임자없음(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	대응체계←	0.172	3.289	0.001	-0.951	-4.153	***	0.145	3.063	0.002

구분	경로	책임자없음(C1)			외부전문가(C2)			부서책임자(C3)		
인프라 품질	자산관리									
	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 4-17] 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

모형별 χ^2 검정을 비교 결과는 비제약모형과 제약모형 모두 P값이 유의수준이고, χ^2/DF는 2.462와 2.513로 적정수준으로 나타났다. 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 조절효과가 있다고 할 수 있다.

보안책임자의 역할 수행자에 따른 조절 효과를 검증한 결과, 보안책임자의 역할 수행자에 따른 조절 효과는 모든 가설이 지지 되었으나, 다음 보안활동은 일부 집단에서만 유의한 효과를 확인할 수 있었다. 인력관리정책은 외부전문가(C2)와 경영진참여(C5)에서, 보안인식관리는 외부전문가(C2)와 부서책임자(C3)에서, 출입통제는 부서책임자(C3)와 경영진참여(C5)에서만 p값이 유의하게 나타났다. 각 보안 활동이 침해사고 대응체계 구축수준에 미치는 유의한 영향도를 파악하고자 표준화경로계수 β와 p값을 확인한 결과, 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.

3) 기업핵심정보 관리방식에 따른 조절 효과

기업핵심정보 관리방식에 따른 조절 효과의 가설검증 결과는 관리 안함(C1), 외부 전문서비스 이용(C2), 자체적으로 백업 관리(C3)에 따라 모형별 χ^2 검정을 비교는 [표 4−18], 경로별 차이를 검증에 따른 가설검증 결과는 [표 4−19]와 같이 나타났다.

[표 4-18] 기업핵심정보 관리방식에 따른 모형 비교

모형	χ^2	DF	P값	χ^2/DF	RMSEA	NFI	TLI	CFI
비제약	45.018	18	0.000	2.501	0.023	0.995	0.978	0.997
제약	107.023	20	0.000	5.351	0.039	0.989	0.937	0.991
차이비교	62.005	2	0.000					

*p<0.05 수준에서 유의함

[표 4-19] 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

모형별 χ^2 검정을 비교 결과는 비제약모형과 제약모형 모두 P값이 유의수준이고, χ^2/DF는 2.501와 5.351로 적정수준으로 나타났다. 비제약모형과 제약모형의 차이는 DF=2(20−18)일 때, $\Delta\chi2$=62.005(107.023−45.018)이고 p값은 0.000로 통계적으로 유의함을 알 수 있다. 따라서 기업핵심정보 관리방식은 조절 효과가 있다고 할 수 있다.

기업핵심정보 관리방식에 따른 조절 효과를 검증한 결과, 기업핵심정보 관리방식에 따른 조절효과 검증결과는 인력관리정책, 보안인식관리, 출입통제, 인력 운영 프로세스에서 기각 되었다. 각 보안 활동이 침해사고 대응체계 구축수준에 미치는 유의한 영향도를 파악하고자 표준화경로계수 β와 p값을 확인한 결과, 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 의미있는 조절 효과를 나타냈다. 기업핵심정보를 자체적으로 관리(C3)하는 경우는 시스템관리 프로세스(β=0.181, t값=8.682***), 인력관리(β=0.126, t값=4.872***)에서 의미 있는 조절 효과를 나타냈으며, 외부서비스(C2)를 이용하여 관리할 경우와 비교하였을 때 전반적으로 낮은 영향도를 보였다.

6.2.3. 연구 결과 분석

6.2.3.1. 중소기업의 사이버 침해사고 대응체계 구축의 영향분석

중소기업이 사이버 침해사고 대응체계를 구축함에 있어 수행한 보안 활동이 유의미하게 영향을 미치는지를 확인하기 위하여 연구가설을 수립하였다. 이를 검증하기 위하여 구조방정식 모형분석을 통하여 가설검증 하였다. 연구모형 분석결과는 아래 [표 4-20]과 같다

[표 4-20] 연구모형 가설검증 결과(1)

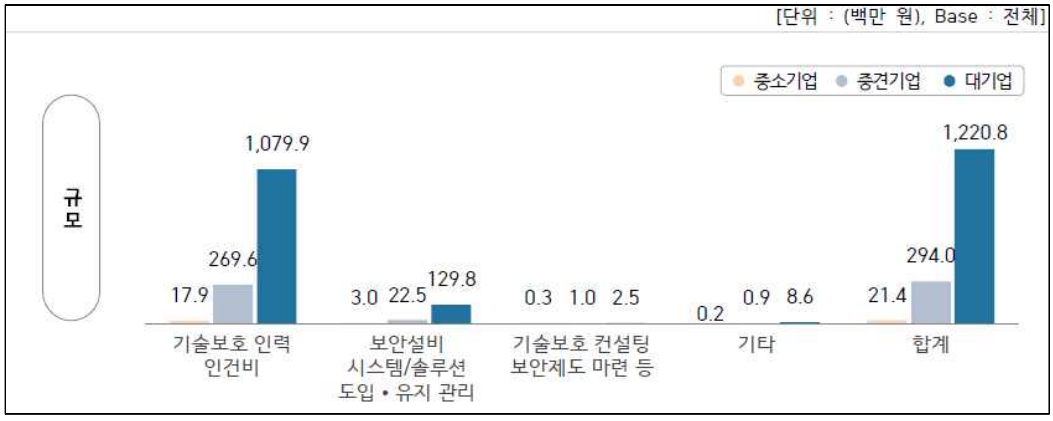
구분		연구가설	검증결과
H1	H1-1	- 보안관리정책는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지
	H1-2	- 인력관리정책은 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지
H2	H2-1	- 보안인식관리는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	기각
	H2-2	- 인력관리는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지
H3	H3-1	- 자산관리는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지
	H3-2	- 출입통제는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지
H4	H4-1	- 인력 운영 프로세스는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지
	H4-2	- 시스템관리 프로세스는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지
	H4-3	- IT관리 프로세스는 침해사고 대응체계 구축수준에 정(+)의 영향을 미칠 것이다.	지지

사이버 침해사고 대응체계 구축에 영향도가 높은 보안 활동은 자산관리, IT관리 프로세스와 시스템관리 프로세스 순으로 나타났다. 보안 활동 중 보안정책이 기술보호 수준에 가장 큰 영향을 미친다는 앞선 연구들(김택영,

2021, 정성배 외, 2015)과 다르게 중소기업을 대상으로 한 본 연구에서는 보안 인프라와 보안 프로세스가 더욱 영향이 큰 것으로 나타났다. 보안 인프라 중 기업의 보안을 위하여 구축한 어플리케이션, 장비, 시설 등 보유자산 및 장비의 보안체계인 '자산관리' 활동이 가장 높게 나타났는데, 물리적 보안 활동은 내외부의 불법적인 접근과 기술 유출 등을 방지하는데 가장 기본이 되는 활동으로서 기술보호 수준을 결정하는 데에 큰 영향을 미친 것으로 분석된다(김택영, 2021). 국가 중요시설을 중요자산 레벨에 따라 보안관리 계획을 수립하고 이에 따라 보안관리 활동을 수행하는 물리적 보안은 보안성과를 높인다는 연구(최연준, 2018)와 같이 중소기업도 규모에 차이는 있으나 중요자산을 식별하여 보안관리를 하는 활동은 중요하다고 할 수 있다.

보안 인력 관련 보안 활동이 가장 낮게 영향을 미치는 것은 이전 선행연구와 같다. 이는 중소기업이 현재 인적 요소에 대한 관리 및 통제 어려움으로 인하여 인적보안 활동이 취약하고, 그로 인해 기술유출 사고가 발생할 수 있음을 대변하고 있다(김택영, 2021). 선행연구에서 영향력이 높게 나온 보안정책 중 보안관리정책 측면에서는 높게 나타났으나, 내부/외부 인력의 보안 준수를 위한 원칙이나 규율 등의 '인력관리정책'은 상대적으로 낮게 나와 중소기업의 인력에 관한 정책은 미흡하게 관리되는 것으로 분석된다.

하지만, 2020년 중소기업 기술보호수준 실태조사 자료를 보면 중소기업이 기술보호를 위해 가장 많이 투자하는 항목이 '기술보호 인력 인건비' 이고, 그다음이 '보안설비 시스템/솔루션 도입유지관리' 항목으로 나타났다[그림 4-3]. 이는 보안 인력에 투자는 하고 있으나 투자 효과를 얻지 못하고 있는 것으로 판단할 수 있다. 원인은 찾아보자면, 형식적으로 수행되는 보안교육이나 외부 전문인력을 통해 보안 문제를 해결하는 등 간단히 생각할 수 있으나, 보안 인력에 대한 투자 효과 장기적인 측면에서 접근하여 계획할 필요가 있다는 것을 고려하여야 한다(이인선, 2021).



[그림 4-3] 기술보호 투자 비교
출처: 2020년 중소기업 기술보호수준 실태조사 (2021).

중소기업이 사이버 침해사고에 효과적으로 대응하기 위해서는 조직의 직무의 성격과 형태가 상이함을 감안하여 각 부서 특성에 맞춤화된 보안체계를 구성해야 한다(송재혁, 2021). 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 보안전문인력 양성을 하는 것도 중요하게 고려하여야 한다.

6.2.3.2. 중소기업의 사이버 침해사고에 대한 조절효과 분석

중소기업이 보안 활동을 통해 사이버 침해사고 대응체계를 구축함에 있어 중소기업 지원사업의 수혜 여부와 보안책임자의 역할 수행자 그리고 기업의 핵심정보를 관리방식에 따라 조절 효과가 있는지 분석하였다. 조절 효과에 관련한 가설은 다음과 같이 확인되었다.

1) 중소기업지원사업 수혜 여부에 따른 조절 효과 분석결과

본 논문에서 다루는 중소기업지원사업은 중소벤처기업부에서 대·중소기업·

농어업협력재단을 통해 중소기업을 대상으로 기술보호 지원을 목적으로 수행하는 지원사업이다. 기존 많은 선행연구에서는 지원사업의 수혜 경험이 보안활동과 기술보호 관리체계 간에 유의미한 영향을 미친 것으로 연구되었다(David 외, 2000; Zahra 외, 2002; 신진교, 최영애, 2008; 박상훈, 조남욱, 2017). 정부 지원사업은 단순 재정적 지원뿐만 아니라 중소기업의 정보보호 인식개선의 효과, 보안교육의 효과를 가져오는 것으로 나타났다(중소기업연구원, 2017). 하지만 본 연구에서 조절 효과를 검증한 결과는 [표 4-21]과 같이 나타났다.

[표 4-21] 연구모형 가설검증 결과(2)

구분		연구가설	검증결과
수혜 여부	H5-1-1:	- 보안관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	지지
	H5-1-2:	- 인력관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	기각
	H5-1-3:	- 보안인식관리가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	기각
	H5-1-4:	- 인력관리가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	지지
	H5-1-5:	- 자산관리가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	지지
	H5-1-6:	- 출입통제가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	지지
	H5-1-7:	- 인력 운영 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	지지
	H5-1-8:	- 시스템관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	지지
	H5-1-9:	- IT관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 중소기업지원사업 수혜 여부에 따라 증가할 것이다.	지지

중소기업지원사업 수혜 여부에 따른 조절효과 검증결과는 인력관리정책, 보안인식관리에서 기각 되었다. 비수혜기업과 수혜기업의 표준화경로계수(β)의 차이를 비교하면, 중소기업지원사업 수혜를 받았을 경우 보안관리정책, 시스템관리 프로세스, 자산관리가 유의미한 조절 효과가 나타난 것으로 확인되

었다. 이는 중소기업은 중소기업 지원사업을 통하여 보안 정책이나 보안 인력 측면에서의 효과보다는 출입문, 캐비닛, 개인서랍 시건 여부 확인, 화면보호기설정 및 패스워드사용 여부확인 등 물리적 보안 활동을 실시하는 '시스템관리 프로세스', 기술보호 및 보안규정을 수립하고 정기적 보안감사 점검을 실시하는 등의 '보안관리정책'과 보안구역 운영 및 정보화기기 반출입 통제 등 '출입통제'에 주로 효과를 가져온 것으로 나타났다.

중소기업 기술보호수준 실태조사에 따르면 중소기업(48.0점)은 대기업(69.4점)에 비해 역량 수준이 낮으나, 지원사업 수혜를 통해 54.4점으로 78.5%까지 역량점수를 올리는 효과를 얻고 있다. 정부지원사업의 수혜 여부에 따른 중소기업 기술보호 상대지수는 수혜기업(78.4%)이 비수혜기업(69.2%)에 비해 9.2%p 높다. 평가부문별 역량점수는 모든 부문에서 수혜기업의 점수가 비수혜기업보다 높게 나타났고, '관리적 보호 방안' 부문에서 수혜기업(48.6점)과 비수혜기업(39.3점)의 차이가 가장 크게 나타났다[표 4-22].

[표 4-22] 평가부문별 수혜/비수혜기업 역량점수 및 상대지수

연도	종합	기술보호 정책	관리적 보호방안	물리적 보호방안	기술적 보호방안	사고'재해 관리
대기업(A)	69.4	70.2	60.7	79.2	69.8	76.7
수혜기업(B)	54.4	60.8	48.6	56.6	50.3	56.1
비수혜기업(C)	48	56.8	39.3	48.9	46.7	47
대기업 대비 수혜기업상대지수 (B/A*100)	78.4	86.6	80.1	71.5	72	73.2
대기업 대비 비수혜기업상대지수 (C/A*100)	69.2	80.9	64.7	61.8	66.8	61.3

출처: 2020년 중소기업 기술보호수준 실태조사 (2021).

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. 중소기업지원사업 수혜기업은 장기적인 투자 효과를 가지기 위해서 적절한 정보보호 로드맵을 가지고 보안 정책과 관리적 보호 방안을 통한 정보보호 투자방안을 가지는 것도 중요하다(배영식, 장상수. 2021). 이러한 정보보호 로드맵을 기반으로 중소기업지원사업의 수행 결과를 분석하고 미흡한 부분에 대한 지속적인 보완을 통하여 사이버 침해사고 대응체계를 구축하는 것이 필요하다.

2) 보안책임자의 역할 수행자에 따른 조절 효과 분석결과

보안책임자의 역할 수행자에 따른 조절 효과를 검증한 결과는 [표 4-23]과 같이 나타났다. 보안책임자의 역할 수행자에 따른 조절 효과는 외부전문가가 수행할 경우가 다수의 보안 활동에서 유의미하게 영향도가 높게 나타난 것을 알 수 있다.

[표 4-23] 연구모형 가설검증 결과(3)

구분		연구가설	검증결과
보안책임자	H6-1-1:	- 보안관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지
	H6-1-2:	- 인력관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지
	H6-1-3:	- 보안인식관리가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지
	H6-1-4:	- 인력관리가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지
	H6-1-5:	- 자산관리가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지
	H6-1-6:	- 출입통제가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지
	H6-1-7:	- 인력 운영 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지
	H6-1-8:	- 시스템관리 프로세스가 침해사고 대응체계 구축수준에 미치는	지지

구분		연구가설	검증결과
		영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	
	H6-1-9:	- IT관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 보안책임자의 역할 수행자에 따라 증가할 것이다.	지지

최고 보안책임자는 회사 보안 비전에 대한 관리, 전략과 프로젝트에 대해 책임지는 비즈니스 리더로서의 역할을 수행한다. 그들은 위험을 경감시키고, 사고에 대응하며, 재무적, 물리적, 인적 위험 등 모든 분야 안에서 유출될 수 있는 경향을 감소하기 위해 보안 프로세스를 식별하고, 개발하고, 구현하고 유지하는 일에 대한 직접적인 명령권자이다. 이들은 지적인 자산에 관련된 적합한 표준과 위험 통제들을 수립하고 중요 정보에 대한 보안과 관련된 정책과 절차의 수립과 구현을 명령한다. 정보보호를 우선적으로 책임지는 이들은 직책을 구별짓기 위해서 최고 정보보호 책임자의 직함을 가지기도 한다(위키백과, https://ko.wikipedia.org/wiki/). 또한, 최고 보안책임자는 비즈니스 연속성 계획(business continuity planning), 유출 방지, 감사 및 위험 관리, 개인정보 보호와 같은 관련 영역을 담당하거나 밀접하게 참여한다. 물론 현실 세계에는 이런 보안 활동에 대한 부담을 짊어지지 않으면서도 공식 CSO 직함을 가진 사람들이 많이 있다. 최고 보안책임자의 자격으로 고위 경영진에서 효과적인 역할을 할 수 있고, 광범위한 기술 및 비기술 직원에게 보안 관련 개념을 전달할 수 있는 지능적이고 명료하며 설득력 있는 리더여야 한다. 비즈니스 연속성 계획, 감사 및 위험 관리에 대한 경험이 있어야 한다. 관련 법률 및 법 집행 기관에 대한 강력한 실무 지식이 있어야 한다[표 4-24]. 정보기술 및 정보보안에 대한 확실한 이해가 있어야 한다(Josh Fruhlinger, 2021).

[표 4-24] 국내법률에서의 정보보호 관련 책임자 직책 비교

직책	근거	대상	역할	직위	비고
정보보호 최고책임자 (CISO)	정보통신망법 제45조의3	정보통신서비스 제공자	정보통신시스템 등에 대한 보안 및 정보의 안전한 관리	임원급	신고

직책	근거	대상	역할	직위	비고
정보보호 최고책임자 (CISO)	전자금융거래법 제21조의2	금융회사, 전자금융업자	전자금융업무 및 기반 정보 기술부문 보안 총괄	임원 (차등)	-
정보보호 책임자 (CISO)	정보통신기반 보호법 제5조	주요정보통신기반시설 관리기관	시설 보호에 관한 업무 총괄	임원급, 영관급 장교 등	통지
개인정보 보호책임자 (CPO)	개인정보 보호법 제5조	개인정보처리자	개인정보의 처리에 관한 업무 총괄 책임	대표자, 임원, 부서장 등	공개
신용정보 관리보호인	신용정보법 제20조	신용정보회사, 금융회사 등	신용정보의 관리 및 보호에 관한 업무	임원 (차등)	공시
고객정보 관리인	금융지주회사법 제48조의2	금융지주회사 등	고객정보의 엄격한 관리	임원	-
정보화 책임관(CIO)	국가정보화 기본법 제11조	국가기관, 지방자치단체	국가정보화 시책 수립· 시행과 국가정보화사업 조정 등의 업무 총괄		통보

출처: IT위키: 정보보호 최고책임자 (https://itwiki.kr/)

본 연구에서 알아보고자 하는 보안책임자는 중소기업에서 정보보호에 대한 총 책임을 가지고 정책을 수립하고 정보보호 관리체계를 구축함에 있어 정보기술 및 정보보안에 대한 확실한 이해를 가지고 수행하는 책임자라고 할 수 있다. 하지만 많은 중소기업에서 보안전문가를 보안책임자로 두기 힘들기 때문에, 대부분이 실제 보안책임자의 역할자는 없고 보안실무자 역할을 수행하는 담당자만 있다고 할 수 있다. 보안담당자는 82%가 겸직을 하고 있었으며, 66%는 별도의 보안조직을 갖추고 있었다. 또한, 대부분 경영지원부서에 속해 있는 경우가 대부분이라 정보보안 업무보다는 다른 업무를 우선시하는 경우도 많았다. 중소기업에서 정보보호 업무는 IT관련 부서에서 한다고 생각하는 경향이 많아 정보보호 담당이 대부분 전산 업무까지 수행하고 있다. 보통 중소기업에는 보안전문가가 없어 방화벽, 출입통제 등의 네트워크보안은 외부 관제 서비스를 받는 경향이 많다. 만약 외부서비스를 받지 않는다면 직

접 위협에 대한 수많은 공격 이벤트 분석 등을 직접 수행해야 한다. 그리고 사내 정보유출 방지시스템, 백신 등의 보안솔루션 운영까지 수행해야 하므로 실제로는 보안관리를 못 하고 있다고 봐야 한다(이익선, 2021). 일반적으로 이런 관점에서 경영진이 참여(C5)하여 수행할 경우 보안체계 운영에 효과적이라고 한다(대·중소기업·농어업 협력재단, 2020). 국가정보원법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보보호산업의 진흥에 관한 법률 등에서도 보안 및 정보의 안전한 관리를 위하여 임원급을 정보보호 최고책임자로 제시하고 있다(국가정보원 외, 2022).

하지만 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. 특히 외부전문가(C2)가 수행할 경우, 정보시스템의 로그 및 최신 업데이트 등 보안관리 또는 보안 절차 수행하는 'IT관리 프로세스'와 임직원의 보안 활동 관리 또는 보안 절차를 수행하는 '인력운영 프로세스' 등 보안 프로세스에서 효과가 높은 것으로 나타났다. 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. 효과적인 측면에서 외부전문가는 사이버 침해사고 대응체계 구축에 유의미하다고 볼 수 있으나, 보안컨설팅이나 서비스를 통한 실무지식 등을 전수받아 보안전문가, 보안책임자를 양성하는 것도 중요할 것이다.

다음으로 보안전담팀(C4)이 수행하는 경우는 보안전담팀이 정보시스템 전반 보안관리을 관리하는 '시스템관리 프로세스' 등 보안 프로세스 측면에서 효과가 있는 것으로 나타났다. 중소기업 내에서 보안전담팀을 운영한다는 의미는 적어도 보안전문가 또는 보안 인력을 양성하고자 하는 의지가 있다는 의미로 해석할 수 있겠다. 이런 의미에서 보안책임자의 역할 수행자가 외부전문가(C2)인 경우가 효과가 높다고 해서 보안 취약점이 존재하는 외부 서비스에 의존하는 것 보다, 기업 내에 보안전담팀을 만들어 기업특성에 맞는 정보보호 관리체계를 운영하려고 노력한다면 장기적으로는 침해대응에 효과적일 수 있을 것이다.

3) 기업핵심정보 관리방식에 따른 조절 효과 분석결과

성욱준(2018)은 정보보호 침해사고 발생과 복구에 영향을 미치는 요인 중 정보보호 아웃소싱, 데이터 백업, 최고 경영진 및 직원의 정보보호 인식이 정보보호에 중요한 영향을 미치는 변수로 연구하였다. 시스템이나 데이터에 대한 백업은 기술 관리적 측점에서 매우 기본적이면서도 핵심적인 사항이다. 백업은 조직 내 정보의 지속성과 연속성을 보장하며, 유사시 침해사고가 발생할 경우 문제의 원인을 파악하고 조속한 문제해결에 매우 중요하게 작용한다. 기업의 핵심 데이터를 어떻게 관리하는가는 사이버 침해사고 대응에 중요한 요소로 판단하였고, 해당 조절 효과를 연구가설에 포함하여 [표 4-25]과 같이 분석하였다.

[표 4-25] 연구모형 가설검증 결과(4)

구분		연구가설	검증결과
기업핵심정보관리방식	H7-1-1:	- 보안관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	지지
	H7-1-2:	- 인력관리정책이 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	기각
	H7-1-3:	- 보안인식관리가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	기각
	H7-1-4:	- 인력관리가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	지지
	H7-1-5:	- 자산관리가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	지지
	H7-1-6:	- 출입통제가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	기각
	H7-1-7:	- 인력 운영 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	기각
	H7-1-8:	- 시스템관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	지지
	H7-1-9:	- IT관리 프로세스가 침해사고 대응체계 구축수준에 미치는 영향은 기업핵심정보 관리방식에 따라 증가할 것이다.	지지

기업핵심정보 관리방식에 따른 조절효과 검증결과는 인력관리정책, 보안인식관리, 출입통제, 인력 운영 프로세스에서 기각 되었다. 기업핵심정보 관리방식의 그룹별 표준화경로계수(β)의 차이를 비교하면, 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 핵심정보를 다루는 외부서비스의 자산관리 노하우를 이용하여 효과가 있다는 결과가 나타난 것으로 판단된다. 기업핵심정보를 자체적으로 관리(C3)하는 경우는 중요자산 보호를 위한 보안시스템 운영, 정기적 보안감사 등 정보시스템 전반으로 보안관리하는 '시스템관리 프로세스'에서 다른 집단보다 조절효과가 크게 나타났다. 이는 중소기업의 규모와 구축한 백업 방식에 따른 차이는 있겠으나 자체적인 관리를 위하여 운영 및 정기적인 점검 체계를 갖추게 되었을 경우 자체적인 관리가 의미 있다고 판단할 수 있다.

결과에 대한 정량적인 근거를 제시하고 싶었으나, 중소기업의 백업에 대한 관련 실태조사나 연구는 거의 없고 백업이 미비한 중소기업이 사이버 침해사고에 취약하다는 조사가 대다수였다. 2022년도 9월 기사에 의하면 중소기업 64%가 백업체계가 없고 국내 랜섬웨어 피해기업의 80%가 중소기업이라는 기사를 볼 수 있다(길민권, 2022). 기업핵심정보 관리방식을 관리 안함(C1), 외부 전문서비스 이용(C2), 자체적으로 백업 관리(C3)간의 표준화경로계수(β)의 차이를 비교하면 외부 전문서비스 이용(C2)하는 경우가 전반적으로 영향도가 높게 나타났다. 일반적으로 외부업체를 통한 시스템 관리의존도가 높아지면 그만큼 취약점이 높다고 판단하는데(국가정보원 외, 2022), 자체적으로 백업체계를 갖추기 어려운 중소기업으로서 외부 전문서비스 이용(C2)함으로써 외부서비스의 보안 전문가가 참여하여 자산에 대한 보안관리정책을 수립하여 보안 인프라와 보안 프로세스를 체계적으로 관리할 수 있게 지원하기 때문이라고 파악된다. 다만, 외부 전문서비스 이용(C2)함에 따른 보안취약점을 보안하기 위해 중소기업은 보완책을 마련하기 위해 노력이 필요할 것이다. 이를 위해서 중소기업지원사업의 보안컨설팅을 활용하여 체계적인 보

안정책을 수립하여 운영한다면 외부 전문서비스 이용에 대한 위험관리도 충분히 할 수 있을 것으로 판단된다.

또한, 자체적으로 백업 관리(C3)체계를 구축하여 정기적으로 기업핵심정보를 백업 관리하는 방식은 이상적인 방식이라고 제시하고 있으나, 중소기업에서 자체적으로 보안에 안정적인 환경을 구축하기에는 제약이 크다고 볼 수 있다. 이를 위해서는 중소기업지원사업인 과학기술정보통신부, 한국인터넷진흥원에서 지원하는 '클라우드 기반 보안서비스(SECaaS) 도입 지원사업' 또는 대·중소기업·농어업 협력재단의 '기술자료 임치제도' 등을 이용하는 것도 효과적인 방법이라고 할 수 있겠다. 중소기업 기술임치제도는 이용기업들의 사업인지도, 사업수요 등의 조사결과를 놓고 볼 때, 단순히 임치제도만을 이용하기 위해서라기보다는 중소기업청이 운영 중인 타사업(기술보호 전문가 상담 및 자문, 중소기업 기술지킴이 서비스, 보안시스템 구축 지원사업, 기술분쟁 조정·중재제도)과 연계되어 지원이 이루어지는 것으로 판단된다(오세영, 2017). 따라서 종합적인 중소기업의 기술지원이 이루어지기 위해 제도를 이용하여 기업의 핵심정보를 보호하는 방안으로 이용하는 기반으로 삼는 것도 효과적일 것으로 보인다.

6.2.3.3. 중소기업의 사이버 침해사고의 대응 방안

중소기업은 보안 인프라와 시스템이 상대적으로 잘 갖춰진 대기업에 비해, 보안 역량이 상대적으로 낮아 사이버 침해사고를 당할 확률도 높으며, 중소기업 스스로 보안 인프라나 시스템 구축에 투자한다고 하지만 적절한 보안체계가 아닌 대부분이 사후 대응하기에 급급하여 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 조절 효과들을 분석해 보았다.

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 중요 자산에 대한 위험 관리 수준을 지정하고, 이러한 위험 관리 방안을 근거로 정보보호 관리체계 구축 계획을 수립해야 할 것이다.

또한, 디지털 전환의 가속화로 인해 더욱 복잡해진 초연결 시대에 사이버 침해사고의 다양성과 복잡성에 유연하게 대응할 수 있는 방안은 정보보호 관리체계를 기반으로 하여 사이버탄력성을 갖출 수 있는 방안를 고려하여야 한다. 최근 인간 중심의 보안(PCS, People Centric Security), 사이버탄력성(Cyber Resilience), 제로 트러스트(Zero Trust) 등의 보안이 회자 되는 이유도 같을 것이다. 중소기업의 한계로 인해 이런 보안 방법론들에 소극적인 것이 아니라 오히려 중소기업에 필요한 요소들임을 인지하고 적극 받아들이는 자세가 필요하다.

Ⅴ. 결론 및 시사점

7.1. 연구의 요약

본 논문은 중소기업의 보안 활동이 사이버 침해사고 대응체계 구축에 미치는 영향에 대하여 결과를 도출하고, 중소기업 사이버 침해사고 대응체계 구축의 문제점을 분석하여 기업의 정보보호 관리체계 구축하는 방향을 제시하는 것에 목적이 있다. 본 연구에서는 사이버범죄를 사이버공간 즉, 컴퓨터, 모바일, 네트워크 장치 등에서 발생하는 모든 범죄 활동으로 정의하였고, 중소기업에서 이런 다양한 사이버범죄에 의한 사이버 침해사고에 대응하기 위해 수행해야 하는 보안 활동을 연구하는 것으로부터 출발하였다.

보안 활동은 정보보호 관리체계를 구성하는 보안정책, 보안 인력, 보안 인프라, 보안 프로세스로 구분하였고, 이 보안 활동이 사이버 침해사고 대응체계 구축에 미치는 영향을 밝히는 연구모형과 가설을 도출하였다. 연구모형과 가설을 검증하기 위해 2019년 중소기업 기술보호 수준 실태조사의 데이터를 활용하였다. SPSS 23.0과 AMOS 22.0.0을 통해 구조방정식 모형을 분석하였고, 조절변수의 효과는 χ^2 차이 검정 및 경로별 표준화경로계수를 비교하여 분석하였다. 주요 분석결과는 다음과 같다.

사이버 침해사고 대응체계 구축에 영향도가 높은 보안 활동은 자산관리, IT관리 프로세스와 시스템관리 프로세스 순으로 나타났다. 중소기업을 대상으로 한 본 연구에서는 보안정책보다는 보안 인프라와 보안 프로세스가 더욱 영향이 큰 것으로 나타났다. 보안 인프라 중 기업의 보안을 위하여 구축한 어플리케이션, 장비, 시설 등 보유자산 및 장비의 보안체계인 '자산관리' 활동이 가장 높게 나타났는데, 물리적 보안 활동은 내외부의 불법적인 접근과 기술 유출 등을 방지하는데 가장 기본이 되는 활동으로서 기술보호 수준을 결정하는 데에 큰 영향을 미친 것으로 분석된다. 기술 보호를 위한 정보시스템을 보호하기 위한 활동으로서 'IT관리 프로세스'와 '시스템관리 프로세스'가 다음으로 영향을 미쳤다. 보안 인력 관련 보안 활동이 가장 낮게 영향을 미치는 것으로 분석되었는데, 이는 중소기업이 현재 인적 요소에 대한 관리 및

통제 어려움으로 인하여 인적보안 활동이 취약하고, 그로 인해 기술유출 사고가 발생할 수 있음을 대변하고 있다(김택영, 2021). 선행연구에서 영향력이 높게 나온 보안정책 중 보안관리정책 측면에서는 높게 나타났으나, 내부/외부 인력의 보안 준수를 위한 원칙이나 규율 등의 '인력관리정책'은 상대적으로 낮게 나타나 중소기업의 인력에 관한 정책은 미흡하게 관리되는 것으로 분석된다. 중소기업이 사이버 침해사고에 효과적으로 대응하기 위해서는 조직의 직무 성격과 형태가 상이함을 감안하여 각 부서 특성에 맞춤화된 보안체계를 구성해야 한다(송재혁, 2021). 중소기업 업체는 그들에게 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.

보안 활동을 통해 사이버 침해사고 대응체계를 구축함에 있어, 중소기업 지원사업의 수혜 여부, 보안책임자, 기업핵심정보 관리방식 등의 각 조절변수가 조절 효과를 보이는지에 대한 분석결과는 다음과 같다.

첫째, 중소기업지원사업 수혜를 받았을 경우 조절 효과 결과는 관리적 보호 방안보다는 물리적 보호 방안의 '출입통제'와 기술적 보호 방안의 '시스템 관리 프로세스'에서 의미 있는 조절 효과가 있는 것으로 나타났다. 이는 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. 장기적인 보안체계 구축을 위해 인프라·프로세스 수립 등의 투자를 기반으로 중소기업지원사업의 수행 결과를 분석하여 미흡한 부분에 대한 지속적인 보완을 통하여 사이버 침해사고 대응체계를 구축하는 것이 필요하다.

둘째, 보안책임자의 역할 수행자에 따른 조절 효과는 외부전문가가 수행할 경우 다수의 보안 활동에서 유의미하게 영향도가 높게 나온 것을 알 수 있다. 특히 정보시스템의 로그 및 최신 업데이트 등 보안관리 또는 보안 절차

수행하는 'IT관리 프로세스'와 임직원의 보안 활동 관리 또는 보안 절차를 수행하는 '인력운영 프로세스' 등 보안 프로세스에서 다른 집단보다 효과가 높은 것으로 나타났다. 경영진이 참여한 경우 출입통제 측면에서 영향도가 있는 것으로 보이나, 외부전문가가 수행할 경우가 더욱 영향도가 높게 나온 것을 알 수 있다. 중소기업 내에 보안전문가가 없는 경우가 많아 외부 보안 컨설팅을 받거나 보안서비스를 이용하는 경우가 조직 내부에서 보안책임자를 맡는 경우보다 효과가 높은 것으로 나타난 것으로 보인다. 효과적인 측면에서 외부전문가는 사이버 침해사고 대응체계 구축에 유의미하다고 볼 수 있으나, 보안컨설팅이나 서비스를 통한 실무 지식 등을 전수받아 기업 내부에 보안전문가, 보안책임자를 양성하는 것도 중요할 것이다.

셋째, 기업핵심정보 관리방식에 따른 조절 효과는 외부서비스를 이용하여 관리할 경우 어플리케이션, 장비, 시설 등 기업의 주요자산을 관리하는 '자산관리', 자산 및 체계의 보안 활동을 지원하는 원칙이나 규율을 수립하는 '보안관리정책', 정보시스템의 로그 및 최신 업데이트 등 보안관리 또는 보안 절차 등의 'IT관리 프로세스'에 크게 영향을 미치는 것으로 나타났다. 일반적으로 외부업체를 통한 시스템 관리의존도가 높아지면 그만큼 취약점이 높다고 판단하는데(국가정보원 외, 2022), 자체적으로 백업체계를 갖추기 어려운 중소기업이 외부 전문서비스 이용함으로써 외부서비스의 보안전문가가 참여하여 자산에 대한 보안관리정책을 수립하여 보안 인프라와 보안 프로세스를 체계적으로 관리할 수 있게 지원하기 때문이라고 파악된다. 다만, 외부 전문서비스 이용함에 따른 보안취약점을 보완하기 위해 중소기업은 보완책을 마련하려는 노력이 필요할 것이다. 이를 위해서 중소기업지원사업의 보안컨설팅을 활용하여 체계적인 보안정책을 수립하고 운영한다면 외부 전문서비스 이용에 대한 위험 관리도 충분히 할 수 있을 것으로 판단된다.

7.2. 논의 및 시사점

중소기업은 대기업에 비해 사이버 침해사고의 비중이 높고, 이에 반해 기술보호 역량이 부족하다. 대기업들이 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. 보안 활동과 사이버 침해사고 대응체계 간의 영향을 확인한 결과는 자산관리, IT관리 프로세스와 시스템관리 프로세스 순으로 나타나, 선행연구에서 연구된 보안 정책과 보안 인력의 영향도와는 다른 결과가 나타났다. 또한, 중소기업 지원사업의 수혜 여부와 보안책임자의 역할 수행자 그리고 기업의 핵심정보를 관리방식에 따라 조절 효과에서도 보안 인프라 관련 보안 활동에서 주로 영향도가 높은 것으로 나타났다.

연구의 시사점은 다음과 같다.

첫째, 사이버침해사고 대응체계 구축에 있어 단기 계획과 장기 계획으로 구분하여 이원화된 로드맵 수립을 고려할 수 있다. 중소기업이 중소기업 지원사업의 수혜를 받거나 보안책임자를 경영진으로 하여 보안활동을 수행하거나 기업의 핵심정보를 기업 자체의 관리정책을 통해 통제할 수 있게 구축하였다고 해서 의미 있는 효과를 단시일 내에 얻기는 어려울 수 있다. 본 연구에서 지지된 가설 중 영향도가 높은 순으로 보안 활동을 수행하여 단기적인 효과를 얻고, 선행연구에서 의미 있다고 제시된 보안 정책이나 보안 인력에

대한 투자를 장기적인 관점에서 수행하는 것도 의미 있는 효과를 얻을 수 있는 관리체계 구축이라고 할 수 있을 것이다. 하지만, 이는 장기적인 관점으로 보안정책이나 보안 인력에 투자한다고 해서 보안 정책과 보안 인력에 대한 보안 활동이 전혀 없이 관리한다는 의미는 아니다. 대기업처럼 충분한 컨설팅을 통한 기업의 보안정책과 보안 인력 관리방안을 수립하기는 어려우니, 중요한 보안정책이나 보안 인력을 먼저 수립하고 장기적으로 초기 수립한 정책을 보완 관리하는 것을 목표로 한다는 뜻이다. 장기적인 수행을 위해 정보보호 로드맵을 기반으로 중소기업지원사업의 수행 결과를 분석하고 미흡한 부분에 대한 지속적인 보완을 통하여 사이버 침해사고 대응체계를 구축하는 것이 필요할 것이다.

둘째, 보안 인력관리 측면에서 명확한 보안 인력 관리정책을 수립하여 지속적인 관리를 할 필요가 있다. 본 연구에서 보안 인력에 관한 보안 활동으로 '인력관리정책', '보안인식관리', '인력관리', '인력운영 프로세스' 등으로 구분하여 분석하였고, 이 활동 중 의미 있는 효과가 나타난 활동은 '인력관리'로서 내부 임직원의 비밀유지와 퇴사 직원 및 외주업체 및 외주용역 등 외부자 보안규정 수립 및 관리하는 항목이다. 이외의 다른 보안 인력에 관한 보안 활동은 선행연구에서와는 다르게 낮은 영향도를 나타내었다. 보안책임자의 역할 수행자 측면에서도 경영진이 역할을 담당하는 것이 효과적이라는 선행연구(국가정보원 외, 2022)와는 다르게 주로 외부전문가가 역할을 수행할 경우 더 효과를 보이는 것으로 나타났다. 중소기업이 정보보호 관리체계를 구축하여 성공적으로 관리하기 위해서는 보안 인력은 중요한 관리요소이다(이홍제, 2018). 보안 인력에 대한 보안 활동에 효과를 나타낼 수 있게 하려면 형식적인 활동이 아닌 명확하게 수립한 보안 인력관리 정책하에 인력운영 프로세스를 수행하고, 보안인식을 향상시킬 수 있는 방안을 모색하는 것이 중요한 과제가 될 것이다.

셋째, 보안 투자에 제한적인 중소기업은 중요자산을 관리하기 위하여 자사의 중요자산을 식별하고, 중요도 및 핵심정보의 특징에 따라 외부서비스를 이용할지 기업 내 시스템에서 관리할지를 구분하고, 이에 따른 차별화된 관리방안을 고려하는 것이 필요할 것이다. 본 연구에서는 사이버 침해사고에서

중요하게 관리되어야 하는 기업핵심정보에 대해 어떻게 관리해야 할지 사이버침해사고 대응체계 구축에 미치는 조절 효과를 통하여 연구하였다. 연구결과는 외부 전문서비스를 이용하는 경우가 전반적으로 영향도가 높게 나타났다. 일반적으로 외부업체를 통한 시스템 관리의존도가 높아지면 그만큼 취약점이 높다고 판단하는데(국가정보원 외, 2022), 자체적으로 백업체계를 갖추기 어려운 중소기업으로서 외부 전문서비스를 이용함으로써 외부서비스의 보안전문가가 참여하여 자산에 대한 보안관리정책을 수립하여 보안 인프라와 보안 프로세스를 체계적으로 관리할 수 있게 지원하기 때문이라고 파악된다. 외부 전문서비스를 이용함에 따른 보안취약점을 보완하기 위해 중소기업은 보완책을 마련하기 위해 노력이 필요할 것이다. 이를 위해서 중소기업지원사업의 보안컨설팅을 활용하여 체계적인 보안정책을 수립하여 운영한다면 외부 전문서비스 이용에 대한 위험 관리도 충분히 할 수 있을 것으로 판단된다. 또한, 자체적으로 백업 관리체계를 구축하여 정기적으로 기업핵심정보를 백업 관리하는 방식은 이상적인 방식이라고 제시하고 있으나, 중소기업에서 자체적으로 보안에 안정적인 환경을 구축하기에는 제약이 크다고 볼 수 있다. 이를 위해서는 중소기업지원사업인 과학기술정보통신부, 한국인터넷진흥원에서 지원하는 ‘클라우드 기반 보안서비스(SECaaS) 도입 지원사업’ 또는 대·중소기업·농어업 협력재단의 ‘기술자료 임치제도’ 등을 이용하는 것도 효과적인 방법이라고 할 수 있겠다.

7.3. 한계점 및 향후 연구방향

중소기업에서 효과적인 정보보호 관리체계 구축을 위한 보안 활동을 검증하기 위하여 최대한 많은 중소기업의 참여와 객관성을 가질 수 있는 '2019년 중소기업 기술보호 수준 실태조사'의 2차 데이터를 활용하였다. 다만, 2차 데이터의 특성상 비식별화 처리에 의해 기업의 특성이 대부분 삭제되어 다양한 관점의 분석을 하기에는 제약이 있었다.

그리고 다년간의 데이터를 이용하여 연구하고 싶었으나, 연도별로 조사 항목과 내용, 조사 수준, 척도가 서로 상이하고, 조사대상의 중복성 역시 확인할 수가 없고 연도별 기업을 추적해서 분석할 수 없는 한계가 존재하였다. 다년간의 데이터를 통하여 침해사고 기업의 추적분석을 통해 중소기업의 침해를 유연하게 복구할 수 있는 사이버탄력성 있는 보안체계 구축에 대한 연구도 포함하고 싶었으나 본 연구에는 수행하지 못하였다. 향후에는 디지털 전환의 가속화로 인해 더욱 복잡해진 초연결 시대에 사이버 침해사고 대응을 위하여 정보보호 관리체계를 기반으로 하여 사이버탄력성을 갖출 수 있는 보안요소는 무엇인지 연구가 필요하다. 이를 위하여 다년간의 대상 추적이 가능한 사이버 침해사고 기업의 대응 결과 데이터를 활용하는 것이 필요하다.

마지막으로 본 연구가 중소기업의 정보보호 환경을 구축함에 있어 효과적인 중소기업 환경 맞춤형 사이버 침해사고 대응체계 기준을 제시하는 과학적인 연구가 되기를 기대한다.

참 고 문 헌

1. 간행물

과학기술정보통신부 정보통신산업기반과. (2020.01), 2019 ICT 중소기업 실태조사

과학기술정보통신부. (2021.02), 2020 정보보호 실태조사, 한국정보보호산업협회

국가정보원, 과학기술정보통신부, 행정안전부, 개인정보보호위원회, 금융위원회, 외교부. (2022.05), 2022 국가정보보호백서

국회정보위원회. (2019.12), 사이버공격을 통한 첨단산업비밀 유출 실태 및 대응방안 보고서

노경섭. (2019). 제대로 알고 쓰는 논문 통계분석: SPSS & AMOS (개정증보판). 한빛아카데미

대·중소기업·농어업 협력재단. (2020.02), 2019년도 중소기업기술보호수준 실태조사 보고서

대·중소기업·농어업 협력재단. (2021.02), 2020년도 중소기업기술보호수준 실태조사 보고서

류현숙, 조희정, 이헌아. (2015), ICT 융합환경에 적합한 사이버 보안정책 및 거버넌스 연구. 한국행정연구원

배병렬. (2011). Amos 19 구조방정식 모델링: 원리와 실제. 청람

우종필. (2012). 구조방정식모델 개념과 이해. 한나래출판사

조호대, 박동균, 조현빈. (2008.11), 사이버 침해사고 예방 및 대응을 위한 법·제도적 개선방향. 국회입법조사처

중소벤처기업연구원. (2021.12), 국내외 재창업 지원 정책 비교 및 시사점. KOSI 중소기업 포커스

통계청. (2012.5.18), 정보보호 침해사고 대응지침, 통계청예규 제78호
한국인터넷진흥원, 국가보안기술연구소, 금융보안원. (2022.05), 2021 국가 정보보호백서
한국인터넷진흥원. (2021.12), 침해사고 예방·대응 및 피해확산 방지를 위한 정보통신망법 개선방안 연구
CISA. (2020.04), CYBER RESILIENCE REVIEW (CRR), NIST Cybersecurity Framework Crosswalks
IDC(International Data Corporation). (2020.10), 사이버 복원력 프레임워크를 구현하기 위한 5가지 핵심 기술. IBM 백서
inet. (2021.7), 침해사고 대응 절차 및 사후관리. 아이네트호스팅
National Institute of Standards and Technology. (2018.04.16), Framework for Improving Critical Infrastructure Cybersecurity
NIS, 국가사이버안보센터. (2021.12), 2021 국가사이버안보센터 연례보고서
Scott Rose. (2022.05), Planning for a Zero Trust Architecture, NIST CYBERSECURITY WHITE PAPER
Software Engineering Instiyute. (2014.06). CERT® Resilience Management Model (CERT®-RMM) V1.1, NIST Special Publication Crosswalk
Tierney, K., & Bruneau, M. (2007). Conceptualizing and measuring resilience: A key to disaster loss reduction. TR news

2. 국내 문헌

강만성. (2018), DHP를 활용한 기업보안수준 평가지표 개발. 국내박사학위 논문 용인대학교
강신범, 이상진, 임종인. (2012). 기업의 침해사고 예방을 위한 관리 모델.

정보보호학회논문지, 22(1), 107-115.
고영현. (2021). ICT 공급망 사이버 레질리언스 대책 개발에 관한 연구. 국내석사학위논문 중앙대학교 대학원
고찬석. (2021), 중소기업의 산업정보 유출사고에 관한 실증분석 연구. 국내석사학위논문 한성대학교 지식서비스&컨설팅대학원
곽재연. (2019), 중소기업의 정보보호 활동을 위한 지원정책의 방향성 연구. 국내석사학위논문 한양대학교 대학원
구중모. (2020), 사이버 공격 대응 체계 향상 방안에 대한 연구: 침해대응 업무 중심으로. 국내석사학위논문 동국대학교
권재성. (2021), 재택근무에 따른 정보유출 대책방안에 대한 기업 보안담당자들의 인식 연구. 국내석사학위논문 중앙대학교 대학원
김건우, 김정덕. (2017). 인간 관점의 정보보호 연구동향 분석. 한국정보처리학회 학술대회논문집, 24(1), 332-335.
김경선. (2016). 기술보호활동이 기업성과에 미치는 영향에 관한 실증연구. 성균관대학교 박사학위논문.
김광민. (2019). 중소·중견기업의 산업기술 보호를 위한 산업보안 관리체계에 관한 연구. 국내석사학위논문 건국대학교 정보통신대학원
김기윤. (2019), 기업의 보안수준과 개인정보 유출 통지 활동이 개인정보 유출사고 대응 행동에 미치는 영향. 국내석사학위논문 연세대학교 정보대학원
김동희. (2017), 융합시대의 사이버보안 거버넌스 구축방안에 관한 연구. 국내박사학위논문 고려대학교 정보보호대학원
김동희. (2019). 국내·외 정보보호 관리체계 분석을 통한 통합개선제도에 대한 연구. 국내석사학위논문 건국대학교
김미래. (2018), 개인정보 유출사고의 원인분석을 통한 주요 보안위협 선정 및 활용방안에 관한 연구. 국내석사학위논문 서강대학교 정보통신대학

원

김민수. (2015). K-RAM을 이용한 산업기술유출 위험도 평가 방법론. 국내박사학위논문 경기대학교

김상균, 김인석. (2016). 공공기관 정보보안수준 향상을 위한 분임담당자 중심 업무분장 개선에 관한 연구. 한국정보통신학회논문지, 20(11), 2007-2013.

김신석. (2020), 중소기업의 개인정보와 스마트의료정보의 기술적 보호조치 방안 연구. 국내석사학위논문 세종사이버대학교 정보보호대학원

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

김영근. (2018), 클라우드 환경에서의 shadow IT와 내부자 위협. 국내석사학위논문 高麗大學校

김용재. (2017), 기업의 정보보호 활동에 관한 연구. 국내석사학위논문 서울대학교

김이헌. (2021), 중소기업의 특성을 고려한 정보보호 관리체계 평가 모델 개선. 국내석사학위논문 충북대학교

김종원. (2018), 보안역량진단이 기술보호대응책을 매개로 보안성과에 미치는 영향. 국내석사학위논문 부경대학교

김정덕. (2021). 디지털금융 혁신과 안정을 위한 인간중심보안. 전자금융과 금융보안, 25, 1-20.

김지수. (2017), 침해사고 대응활동에 기반한 개인정보 유출사고 피해액 산출에 대한 연구. 국내석사학위논문 상명대학교 일반대학원

김태형. (2019), 중소기업 산업기술유출방지 강화방안에 대한 연구. 국내석사학위논문 동국대학교

김택영, 김태성, 전효정. (2020). 기업의 특성이 개인정보 유출 사고에 미치는 영향. 한국 IT 서비스학회 학술대회 논문집, 485-488.

김택영. (2021), 조직의 기술보호 인식과 활동이 중소기업의 기술보호 수준에 미치는 영향. 국내박사학위논문 충북대학교

문건웅. (2017), 기업의 정보보호 활동과 정보침해사고 간의 관계. 국내석사학위논문 고려대학교 정보보호대학원

박관수. (2019), 스마트 홈 환경에서 사이버 침해대응 방향에 관한 연구. 국내석사학위논문 아주대학교

박병우. (2018), BYOD 환경에서 모바일 오피스 정보보안 제언을 위한 성공요인에 관한 실증 연구. 국내박사학위논문 전남대학교

박상복. (2022), 스마트공장 구축시 중소기업의 보안수준 향상을 위한 우선순위 도출에 관한 연구. 국내석사학위논문 한성대학교 지식서비스&컨설팅대학원

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. 국내석사학위논문 연세대학교 정보대학원

박세락. (2020), 기술보호 측면에서 보안교육 실시 빈도가 임직원 보안의식 함양에 미치는 영향. 국내석사학위논문 단국대학교 행정법무대학원

박양모. (2017), 중소기업에 특화된 정보보호 점검 항목에 관한 연구. 국내석사학위논문 건국대학교 정보통신대학원

박윤식. (2018), 정보보호 관리체계의 통제항목 적용 방안에 대한 연구. 국내석사학위논문 숭실대학교

박장영. (2018), 기업의 사업연속성 확보를 위한 자원 중요도에 대한 연구. 국내석사학위논문 숭실대학교

박재곤. (2016), 조직특성이 보안성과에 미치는 영향에 관한 근거이론적 해석과 모형화 연구. 국내박사학위논문 수원대학교

박재성. (2022), 중소기업을 위한 정보보호 관리체계 연구. 국내석사학위논

문 고려대학교 컴퓨터정보통신대학원
박종승. (2020), 스마트워크 환경에서의 ISMS-P 기반 정보보호 감리 모형 연구. 국내석사학위논문 건국대학교
박찬규. (2021). COVID-19 이후 증가하는 재택근무환경의 보안실태와 대책. 국내석사학위논문 숭실대학교 정보과학대학원
배영식, 장상수. (2021), 중소기업 정보보호 지원 사업 성과모델 및 측정 방법에 관한 연구. 한국전자거래학회지, 26.4, 37-52.
백성현. (2019), 호스팅 서비스의 인터넷 침해사고 발생 시 피해액 산출 방안에 대한 연구. 국내석사학위논문 상명대학교 일반대학원
서동진. (2016), 국내기업의 기술보호수준에 영향을 주는 요인에 관한 연구. 국내석사학위논문 충북대학교 일반대학원
성욱준. (2018). 정보보호 침해 사고 발생과 복구의 영향 요인에 대한 연구. 한국지역정보화학회지, 21(2), 27-48.
소현철. (2018), 금융기관의 정보보호활동이 정보보호담당자의 보안자신감에 미치는 영향. 국내박사학위논문 호서대학교
손효승. (2017), 소규모 사업자의 정보보호 수준 분석 및 정보보호 준비도 평가기준 개선방안 제시. 국내석사학위논문 순천향대학교
송재혁. (2021), 포스트 코로나 시대의 중소기업 산업정보 유출 방지를 위한 방안 연구. 국내석사학위논문 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 정보보안 정책 준수에 미치는 영향. 국내박사학위논문 건국대학교 대학원
신현구. (2015), 산업보안정책 준수의지의 영향요인에 관한 연구. 국내박사

학위논문 경기대학교
신혜은. (2016), 금융정보 보안 실태와 개선 방안 연구. 국내석사학위논문 고려대학교 정책대학원
안병구. (2018), 기업의 참여형 보안문화 프레임워크 개발 연구. 국내박사학위논문 중앙대학교 대학원
안종하. (2013). 국내 사이버보안 체계 진단 및 정책적 대응방안 연구. 한국경찰연구, 12(3), 125-146.
안종훈. (2021), C-SCRM을 이용한 ICT 공급망 위험영향평가 연구. 국내석사학위논문 건국대학교 대학원
오세영. (2017). 중소기업 기술역량 확보방안에 관한 연구 : 기술자료 임치제도를 중심으로. 국내석사학위논문 고려대학교 법무대학원
오은. (2016), 금융권 대상 정보보호 관리수준 평가모형 개발. 국내석사학위논문 충북대학교 일반대학원
왕린린. (2019), 중국 중소기업의 연구개발투자가 경영성과와 기업가치에 미치는 영향. 국내박사학위논문 호남대학교
우순규. (2018), 금융산업에서 빅데이터 기반의 개인정보 비식별 조치에 영향을 미치는 요인에 관한 연구. 국내박사학위논문 숭실대학교
위초롱. (2017), 개인정보 유출이 감정과 행위에 미치는 영향 : 통제가능성과 유출원인을 중심으로. 국내석사학위논문 충북대학교
유인진, 박도형. (2018). 중소기업 프로파일링 분석을 통한 기술유출 방지 및 보호 모형 연구. 정보시스템연구, 27(1), 171-191.
유정은. (2017), 중소기업 기술유출 방지 방안에 관한 연구. 국내석사학위논문 연세대학교 정보대학원
유하랑. (2020), 기술유출 피해규모 추정을 위한 핵심요인 도출연구. 국내석사학위논문 중앙대학교 대학원
윤태호. (2019), 인터넷전문은행 서비스에 대한 금융소비자의 수용의도 및

이용에 관한 연구. 국내박사학위논문 한성대학교
이길호. (2019), 사이버 침해사고 예방을 위한 정보보호 및 개인정보보호 강화 연구. 국내석사학위논문 高麗大學校
이대권, 양정훈, 강원선, 박준석. (2021). 산업보안 기술보호활동이 보안인식과 보안성과에 미치는 영향: 해외진출기업 (베트남) 을 중심으로. 한국산업보안연구, 11(1), 193-216.
이명렬. (2017). 정보보호 거버넌스 및 외부 위협 요인을 반영한 정보보호 위험분석 방법 연구. 국내박사학위논문 숭실대학교 대학원
이민형, 이정훈. (2015). 관리적 보안활동과 보안인력 전문성이 기술유출방지에 미치는 영향. 한국치안행정논집, 12(2), 165-182.
이병주. (2019), 침해사고 대응을 위한 디지털 포렌식 도구 활용 지침 적용 수행 방안 연구. 국내석사학위논문 건국대학교
이은섭. (2020), 정보시스템 구축·운영을 위한 외주용역기반 보안관리 강화에 관한 연구. 국내박사학위논문 한국산업기술대학교 지식기반기술·에너지대학원
이인선. (2021), 중소기업 정보보호 강화방안에 대한 연구. 국내석사학위논문 동국대학교 국제정보보호대학원
이찬우. (2018), 디지털 정보 분석 기반의 산업기술보호 수준진단 참조모델 설계 연구. 국내박사학위논문 중앙대학교 대학원
이호준. (2020), 중소기업 산업보안 수준 개선에 관한 연구. 국내석사학위논문 동아대학교 대학원
이홍제. (2018), 정보보호 투자 의도에 영향을 미치는 요인에 대한 연구. 국내박사학위논문 숭실대학교 대학원
이흥배. (2022), 중소제조기업의 정보시스템 운영환경 요인과 성과와의 관계 연구. 국내박사학위논문 고려대학교 기술경영전문대학원
임광수. (2017), 통제수용자에 의해 인지된 정보보안정책 특성요인이 보안스

트레스와 보안준수의도에 미치는 영향에 대한 연구. 국내석사학위논문 고려대학교 정보보호대학원

임채태. (2012). 최근 사이버침해 사고 동향 및 대응방안. 한국인터넷진흥원.

장동원. (2020), 중소기업의 IT서비스 가치평가모델에 관한 실증적 연구. 국내박사학위논문 숭실대학교 대학원

전재찬. (2018), 조직 구성원의 정보보안인식에 영향을 미치는 동기 및 심리적인 요인 분석. 국내석사학위논문 중앙대학교 대학원

정성배, 박준석, 최영호. (2015). 산업보안관리활동이 기업의 보안성과에 미치는 영향. 한국경찰연구, 14(4), 521-538.

정점영. (2022), 핵심인력의 산업기술 유출사고 수사 대응방안 연구. 국내박사학위논문 중앙대학교 대학원

정진우. (2021), 산업제어시스템 보안성 향상을 위한 보안 요구사항 및 적용방안 개발에 관한 실증 연구. 국내박사학위논문 중앙대학교 대학원

정혜인. (2016), 조직구성원들의 정보보안행동에 미치는 영향. 국내석사학위논문 남서울대학교 복지경영대학원

조경재. (2018). 콜센터 정보보호 관리체계(ISMS) 인증항목의 우선순위 선정에 관한 연구. 국내석사학위논문 서울과학기술대학교

조성필. (2017). 4 차 산업혁명 시대에 정보보안의 위협요인과 대응방안에 대한 연구. 시큐리티연구, 9-35.

조재완. (2022), 중소기업 ESG경영환경과 보안관리체계 연구. 국내석사학위논문 중앙대학교 대학원

조혜선. (2017), 침해지표 기반의 사이버 위협수준 분석. 국내석사학위논문 성균관대학교

주영국. (2020), 정보보안 사고 사례 분석을 통한 정보보호 평가항목 제안. 국내석사학위논문 高麗大學校

차재원. (2016). ISO 27001과 ISMS를 활용한 공공분야 보안관제 업무 향상

에 관한 연구. 국내석사학위논문 건국대학교
채정석. (2020), 경호·보안담당 공무원의 보안성과에 관한 연구. 국내박사학위논문 경기대학교 대학원
최성욱. (2016), 국내 중소기업 산업보안 향상 방안에 대한 연구. 국내석사학위논문 홍익대학교 대학원
최연준. (2018), 국가중요시설의 물리보안 수준과 보안정책 준수의지가 보안성과에 미치는 영향. 국내박사학위논문 경기대학교 대학원
최영환. (2019), 중소기업 스마트 팩토리 제조운영 성숙도 측정을 위한 평가모델. 국내박사학위논문 충북대학교
최찬영. (2019), 금융기관을 위한 효율적인 사이버보안 투자 및 피해 산출 예측 모델 연구. 국내박사학위논문 호서대학교
최홍선. (2017). 정보보호 위험관리를 위한 정보보호 관리체계(ISMS) 통제항목 개선 방안 연구. 국내석사학위논문 남서울대학교
하태경. (2019), 온라인 서비스의 사용자 보안인식과 정보보안 제도가 개인정보 제공의도에 미치는 영향. 국내석사학위논문 한성대학교 대학원
한규왕. (2017), 중소기업의 개인정보 보호를 위한 자율점검 체크리스트 연구. 국내석사학위논문 상명대학교 일반대학원
홍준석. (2021), 중소기업 임직원의 정보 보안 정책 준수에 미치는 주요 인자 연구 – 구조방정식 모형을 이용하여 –. 국내박사학위논문 서울과학기술대학교
황성민. (2018), 보안관제에서의 보호동기요인이 자기효능감과 보안신뢰를 통해 정보보안성과에 미치는 영향. 국내석사학위논문 건국대학교
황연석. (2016), 정보보호 역량 성숙도 모델과의 비교분석을 통한 정보보호 준비도 평가의 개선방안 연구. 국내석사학위논문 순천향대학교

3. 국외문헌

David, P., Hall, B., Toole, A.. (2000). Is Pubilc R&D a Complement or a Substitute for Private R&D? A Review of Econometric Evidence. Research Policy. 29(4-5), 497-530

Fornell, C. and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(1), 39-50.

Hair, J. F. Jr., R. E. Anderson, R. L. Tatham, and W. C. Black (1998). Multivariate Data Analysis. 5th ed, Prentice-Hall International.

Hayden, L. (2015). People-centric security: transforming your enterprise security culture. McGraw Hill Professional.

Kleij, R. V. D., & Leukfeldt, R. (2019, July). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In International conference on applied human factors and ergonomics (pp. 16-27). Springer, Cham.

Layton, T. P., Information security awareness. AuthorHouse, 2015.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In Cyber resilience of systems and networks (pp. 1-25). Springer, Cham.

Rashid, Z. (2019). Cybersecurity Information Sharing Ecosystems: From the Perspective of Value Creation and Security Investments (Doctoral dissertation, 서울대학교 대학원).

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). Developing cyber resilient systems: a systems security

engineering approach (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology.

Sarhan, N., Harb, A., Shrafat, F., & Alhusban, M. (2020). The effect of organizational culture on the organizational commitment: Evidence from hotel industry. Management Science Letters, 10(1), 183-196.

Zahra, S. A., Nielsen, A. P.. (2002). Sources of capabilities, integration and technology commercialization. Strategic Management Journal. 23(5), 377-398

4. 기타 자료

BSI korea. (2020.05.27), ISO/IEC 27002:2022 새롭게 출시된 정보보호시스템 통제 관련 지침사항_보안 표준 관련 중요 개정, BSI.Blog, http://bsiblog.co.kr/archives/30531

Josh Fruhlinger. (2021.05.26), "CSO 역할이 바뀌고 있다" 최고 보안 직무에 대한 책임과 요구사항, ITWORLD, https://www.itworld.co.kr/news/194959#csidx8d309eb87f205d39a4847c405079db6

곽중희. (2022.06.23), 2021년 정보 침해 사고 유형과 대응 현황 분석, CCTV뉴스, https://www.cctvnews.co.kr/news/articleView.html?idxno=232793

길민권. (2022.09.22), “국내 랜섬웨어 피해기업 80%가 중소기업...64%는 백업도 안 해”, 데일리시큐, https://www.dailysecu.com/news/articleView.html?idxno=139831

김평화. (2019.11.07), 사이버 공격 피해 98%는 중소기업…"정부 · 기업 대책

시급하다", IT조선, https://it.chosun.com/site/data/html_dir/2019/11/07/2019110700364.html

안철수연구소. (2007.09.28), 침해사고 대응절차, AhnLab, https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=10897

이소연. (2022.10.13), 사이버 침해사고 88% 중소기업… 협력업체 피해 정부·대기업으로 확산, 조선일보, https://biz.chosun.com/it-science/ict/2022/10/13/XOXSNJWOKVBBJMEOEHMINKI23E/

한호현. (2009.08.31). 정보보안책임자(CISO)의 역할과 사명, 아이티데일리, http://www.itdaily.kr/news/articleView.html?idxno=20156

CMU SW공학연구소, CERT® Resilience Management Model (https://resources.sei.cmu.edu/)

HIIC (https://www.hiic.re.kr/)

NIST (https://www.nist.gov/)

WEF(World Economic Forum) (https://www3.weforum.org/docs)

국가사이버안전센터 (http://www.ncsc.go.kr/)

국가정보원(http://portal.nis.go.kr/)

대·중소기업·농어업협력재단 (https://www.win-win.or.kr/)

대·중소기업·농어업협력재단 기술자료임치센터 (https://www.kescrow.or.kr/)

산업통상자원부(http://www.motie.go.kr/)

위키백과, https://ko.wikipedia.org/wiki/

인터넷침해사고대응지원센터 (http://www.krcert.or.kr/)

중소기업 기술보호울타리 (https://www.ultari.go.kr/portal/ptm/main.do)

중소기업기술정보진흥원 (https://www.tipa.or.kr/)

한국정보보호진흥원 (http://www.kisa.or.kr/)

한국인터넷진흥원 - ISMS-P (https://isms.kisa.or.kr/main/)

[부록] 설문지

본 조사의 개인정보는 통계법 제33조(비밀보호)와 제34조(통계종사자 의무)에 의해 비밀이 철저히 보장됩니다.	ID						

2019 중소기업 기술보호 수준 실태조사

안녕하십니까? 귀사의 평안과 무궁한 발전을 기원합니다.

중소벤처기업부과 대·중소기업·농어업 협력재단에서는 「중소기업기술 보호 지원에 관한 법률」에 따라 중소기업 기술보호 지원을 위한 중장기적인 정책 수립을 목적으로 매년 본 조사를 실시하고 있습니다. 설문조사는 조사 전문기관 (주)글로벌리서치가 수행하고 있으며, 귀사가 응답하신 내용은 통계분석에만 사용되고 통계법 제33조에 따라 절대 비밀이 보장됩니다.

2020년 1월

중소벤처기업부 · 대·중소기업·농어업 협력재단

■ 주관기관 : 중소벤처기업부
대·중소기업·농어업협력재단
■ 조사기관 : ㈜글로벌리서치
■ 문의전화 : 02-3438-1790 박혜란 대리
02-3438-1720 박주연 연구원

중소벤처기업부 대·중소기업 농어업협력재단

< 제출 방법 및 응답기준 시점>

■ 설문지 제출은 이메일, 팩스(수신번호: 02-3438-1710) 모두 가능합니다.

■ 응답기준 시점은 2018. 1. 1 ~ 2018. 12. 31 입니다.

Part 1. 기술보호 역량 및 수준

A-1. 기술보호 정책 - 기술보호 정책 수립 및 운영

☞ **중소기업 기술보호란?**
중소기업 및 중소기업자가 직접 생산하거나 생산할 예정인 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 독립된 경제적 가치를 가지는 기술 또는 경영상의 정보를 보호하는 행위

문1. 귀사는 임직원을 대상으로 한 **기술보호 및 보안 규정***을 **보유** 및 **공지**하고 있습니까?

기술보호 및 보안규정	기업별 특성에 맞는 기술정보 보호 및 운영에 관한 보안규정을 말하며, '보안정책서' 또는 '보안지침서' 등이 해당

① 보안규정 보유, 모든 직원에게 공지
② 보안규정 보유, 일부 직원에게 공지
③ 보안규정 보유, 공지하지 않음
④ 보안규정 없음

문2. 귀사는 보안규정을 위반하는 직원에 대한 **공식적 징계절차***가 마련되어 있습니까?

공식적 징계절차	보안규정에 근거한 '보안위반자 처리 지침'에 따라 해당 보안규정을 위반한 직원에게 문책 및 처벌을 가하는 적정한 과정

① 징계절차가 문서화되어 공지되고 있음
② 징계절차가 문서화되어 있으나, 공지되지 않음
③ 별도의 징계절차가 문서화되어 있지 않음

문3. 귀사는 **기술보호와 보안**을 담당하는 **부서 및 인력**을 **보유**하고 있습니까?
(※ 2018. 12. 31 기준으로 작성해 주시기 바랍니다)
① 내부의 전담 부서 및 인력을 통해 기술보호 활동을 수행
② 내부의 겸임직원 또는 외주관리를 통해 기술보호 활동을 수행
③ 별도의 부서 및 인력이 없음

구분	내부			외부		총 계
	1) 전담인력	+	2) 겸임직원	+	3) 외주관리*	=
인력수	□□□ 명		□□□ 명		□□□ 명	□□□ 명

외주관리	기술보호 및 보안을 담당하는 외부, 외주인력으로 일반경비원 등은 제외됨 예) 보안 시스템/솔루션 유지보수를 외부 전문업체가 관리

문4. 귀사는 기술보호를 위하여 매년 얼마나 **투자**하고 있습니까?
(※ 2018. 1. 1 ~ 2018. 12. 31 기간 기준으로 금액을 작성해 주시기 바랍니다)

구분	기술보호인력 인건비		보안설비·시스템/솔루션 도입·유지관리		기술보호 컨설팅 보안체도 마련 등		기타		합계 (총 기술보호 투자액*)	
금액	백억	십억	억	천만	백만	십만	만	원		

기술보호 투자액	기술보호 컨설팅, 기술유출 방지시스템 구축, 보안관제, 기술보호 인건비 등 기업의 보유 기술을 보호하기 위한 목적으로 지출되는 비용

문5. 귀사 내 **보안감사의 실시 책임자**는 누구입니까? (복수 응답 가능)

① 대표이사 및 임원급
② 보안전담부서 및 보안전담관리자
③ 부서별 보안관리자
④ 외부 전문기
⑤ 보안감사 실시 책임자 없음

A-2. 기술보호 정책 - 기술보호 정책 관리

문6. 귀사는 **기술보호 및 보안 규정**을 **정기적으로 검토 및 개정**하고 있습니까?

① 정기적으로 개정하고 있음
② 필요에 따라 비정기적으로 개정하고 있음
③ 규정 제정 후 개정하지 않음
④ 기술보호 및 보안 규정 없음

문7. 귀사의 임직원은 **기술보호의 필요성**에 대해 어떻게 인식하고 있습니까?

구 분	기술보호 필요성 인식					기술보호방안/체계 추진의지				
	매우 높음	높음	보통	낮음	매우 낮음	매우 높음	높음	보통	낮음	매우 낮음
1) CEO/임원	①	②	③	④	⑤	①	②	③	④	⑤
2) 부서장	①	②	③	④	⑤	①	②	③	④	⑤
3) 직원	①	②	③	④	⑤	①	②	③	④	⑤

B-1. 관리적 보호 방안 - 인력 관리

문8. 귀사는 직원들을 대상으로 얼마나 자주 **보안교육**을 **실시**하고 있습니까?

① 연1회 이상 정기적인 보안교육 실시 (☞문8-1로)
② 필요할 때 마다 비정기적으로 보안교육 실시 (☞문8-1로)
③ 보안교육 실시하지 않음

문8-1. **(문8의 ①, ② 응답 시)** 보안교육을 실시한다면, **누구**에 의해 실시되고 있습니까?
(복수 응답 가능)

① 대표이사 및 임원급
② 보안전담부서 및 보안전담관리자
③ 부서별 보안관리자
④ 외부 전문가 및 외부 교육기관

문9. 귀사는 임직원에게 '**비밀유지서약서**'를 작성하여 **제출**하도록 하고 있습니까?

비밀유지서약서	내부 직원에게 비밀유지의무를 부과하고, 보안정책 및 보안 세부 규정을 인지시켰다는 사실에 대한 서약서류로서 법적 증거로 활용 가능

① 비밀유지와 관련된 충분한 설명과 함께 비밀유지서약서를 작성 및 제출 받음 (☞문9-1로)
② 비밀유지서약서를 징구하고 있으나, 행정절차(통보식 절차)로서 존재함 (☞문9-1로)
③ 비밀유지서약서를 별도로 받지 않고 있음

문9-1. **(문9의 ①, ② 응답 시)** 비밀유지서약서를 작성하여 제출하는 경우, **작성 대상자**를 골라주십시오. (복수응답 가능)

① 현 직원(인턴, 임시직 포함) ② 퇴사자(퇴사예정자) ③ 고용외국인(연수생, 기술고문포함)
④ 기타( )

문9-2. **(문9의 ①, ② 응답 시)** 비밀유지서약서를 작성하여 제출하는 경우, **구체적으로 보안 대상 업무를 명시**하고 있습니까?

① 예 ② 아니오

문10. 귀사는 핵심인력에 대해 '**경쟁업체 전직금지 서약서**'를 체결하고 있습니까?

경쟁업체 전직금지 서약서 (경업금지약정)	근로자가 경쟁업체에 취업하거나, 스스로 경쟁업체를 설립·운영하는 등의 행위를 하지 않을 것을 약속하는 것으로, 이를 위반하면, 손해배상 청구, 위약금 반환 청구 등의 조치가 가능함

① 체결함 (☞문10-1로)
② 체결하지 않음

문10-1. **(문10의 ① 응답 시)** 경쟁업체 전직금지 서약서를 작성하여 제출하는 경우, **준수사항 위반 시 처벌 또는 배상책임**에 대해 **명시**하고 있습니까?

① 준수사항 위반 시 처벌 또는 배상책임에 대한 내용(의무, 기간, 대상정보, 범위 등)이 포함되어있음
② 준수사항 위반 시 처벌 또는 배상책임에 대한 명시만 포함되어 있음
③ 명시되어 있지 않음

문11. 귀사는 **퇴사자의 향후 진로 및 동향을 파악**하고 있습니까?

① 모든 퇴사자의 동향 파악 ② 주요 임·직원에 한하여 동향 파악 ③ 파악안함

문12. 귀사는 핵심인력의 장기 재직을 유도하기 위해 어떤 **인센티브 제도**'를 **운영 또는 지원**하고 있습니까? (복수 응답 가능)

내일채움공제	중소기업 핵심인력의 잦은 이직으로 인한 경영상 어려움을 해소하기 위해 장기재직(5년만기) 시 중소기업 및 근로자에게 세제 혜택 부여(중소벤처기업부)
청년내일채움공제	중소·중견기업의 우수인력 확보와 근로자의 장기근속을 유도하기 위해 근로자·기업·정부가 공동 적립(2년~3년)하여 만기 시 적립금 지급 (고용노동부)
직무발명보상제도	종업원의 직무발명을 기업이 소유하며, 발명자인 종업원에게 상당한 보상을 하는 제도
성과공유제	경영 목표 설정 및 목표달성에 따른 성과금 지급(우리사주 포함)을 사전에 약정하고 성과에 대해 보상하는 제도

① 내일채움공제 ② 청년내일채움공제 ③ 직무발명보상제도
④ 성과공유제 ⑤ 운영하고 있지 않음

B-2. 관리적 보호 방안 - 외부자 관리

문13. 귀사는 **외주업체 및 외주용역** 등을 관리하기 위한 **규정**이 **수립**되어 있습니까?
① 기술보호 내용이 포함된 규정이 수립되어 있음
② 업무를 위한 규정이 수립되어 있음
③ 별도의 규정 없음

문14. 기술보호를 위해 **제 3자(외부업체, 협력업체 등)**는 **어떻게 관리**를 하고 있습니까?
① 별도의 관리 방안이 마련되어 있으며, 대상자에 대한 비밀유지서약을 하고 있음
② 별도의 관리 방안은 마련되어 있지 않으나, 대상자에 대한 비밀유지서약을 하고 있음
③ 별도의 관리 방안이 마련되어 있지 않으며, 대상자에 대한 비밀유지서약을 하고 있지 않음

C-1. 물리적 보호 방안 - 자산 및 장비 관리

문15. 귀사는 **보유자산에 대한 관리지침**'을 마련하고 **개정 및 검토**하고 있습니까?

보유자산에 대한 관리지침	보유자산을 대내외의 부정한 행위로부터 지키기 위해서 주요 자산을 파악하여 분류하고 가치를 평가하기 위한 내부 규정

① 지침을 주기적으로 개정 및 검토하고 있음
② 지침이 수립되어 있으나, 필요할 때마다 비정기적으로 개정 및 검토하고 있음
③ 지침이 없으며, 체계적 관리를 하지 않음

문16. 내부에서 생성된 **중요 기술상/경영상 영업 비밀 자료의 보관**은 다른 문서와 구별하여 **보관**하십니까?
① 비밀 자료와 일반 자료를 구분하여 따로 보관함
② 비밀 자료와 일반 자료를 구분하지만 같이 보관함
③ 비밀 자료와 일반 문서를 별도로 구분하고 있지 않음

C-2. 물리적 보호 방안 - 출입통제

문17. 귀사에서 운영하고 있는 **유/무인 경비시스템**은 무엇입니까? (복수응답 가능)
① 상주경비인력 근무
② 무인경비시스템(에스원, ADT 캡스 등) 운영 중
③ 자체 CCTV 설치
④ 전혀 없음

문18. 귀사는 **외부인 접견실 또는 회의실을 운영**하고 있습니까?
① 예
② 아니오

문19. 귀사에서 운영하고 있는 **출입자 통제·관리 경비시스템**은 무엇입니까? (복수응답 가능)
① 출입자 관리대장 작성·관리
② 지문인식 또는 사원증/방문증(ID카드)을 통한 관리
③ 개발부서, 공장시설 등의 감시장치 설치·운영
④ X-Ray검색기 설치·운영
⑤ 전혀 없음

문20. 귀사는 **중요자산의 보호**를 위한 **통제구역을 운영**하고 있습니까?

① 통제구역 운영(CCTV 등 감시장치 설치), 한정된 직원만 출입가능
② 통제구역 운영(CCTV 등 감시장치 설치), 모든 직원 출입가능
③ 통제구역 운영(CCTV 등 감시장치 미설치), 한정된 직원만 출입가능
④ 통제구역 운영(CCTV 등 감시장치 미설치), 모든 직원 출입가능
⑤ 통제구역 없음

문21. 귀사는 **정보화기기**(노트북, 스마트폰, 태블릿, USB, 외장하드, 디지털카메라 등) **반입 및 반출 통제**를 하고 있습니까?

① 내부자 및 외부자의 모든 정보화기기 반출입 통제
② 내부자의 모든 정보화기기와 외부자의 일부 기기에 대하여 반출입 통제
③ 내부자의 모든 정보화기기 반출입 통제(외부자의 정보화기기에 대해 반출입 통제 하지 않음)
④ 내부자 및 외부자의 일부기기에 한해 반출입 통제
⑤ 반출입통제 없음

D-1. 기술적 보호 방안 - 운영관리

문22. 귀사는 **중요자산'의 보호**를 위한 **보안시스템'**을 **운영**하고 있습니까?

중요자산	기업 경쟁력의 원천이 되는 기술이나 경영노하우를 의미
보안시스템	CCTV 등 감시장치, 출입통제관리 시스템, 비밀관리 프로그램 등

① 회사 내부에 보안 시스템을 구축하여 운영 중이고, 필요에 따라 외부업체에 맡김(☞문22-1로)
② 외부 업체를 통해 보안 시스템을 운영 중(☞문22-1로)
③ 보안 시스템 없음

문22-1. **(문22 ①, ② 응답 시)** 보안시스템을 운영하고 있다면, 어떠한 시스템을 활용하고 있습니까? (복수응답 가능)

① CCTV 등 감시 카메라 장치
② 출입통제시스템(비밀번호, 출입카드, 지문/정맥인식 등)
③ 비밀관리 프로그램
④ 기타(　　)

문23. 귀사에서는 아래와 같은 **보안활동**을 하고 있습니까? 각 활동별 **실시 정도**를 선택하여 주십시오.

보안활동 실시 정도	매일	주 1회 이상	월 1회 이상	연 1회 이상	실시하지 않음
1) 출입문, 캐비닛, 개인서랍 시건 여부 확인	①	②	③	④	⑤
2) 문서 및 도면 방치여부 확인	①	②	③	④	⑤
3) 노트북 방치 여부 확인	①	②	③	④	⑤
4) PC전원 OFF 여부 확인	①	②	③	④	⑤
5) 화면보호기설정 및 패스워드사용 여부확인	①	②	③	④	⑤

문24. 귀사는 **정기적인 보안감사***를 **실시**하고 있습니까?

보안감사	보안시스템이 안전하게 운영되고 있는지를 조사하고 분석하는 행위 감사 대상은 기업의 보안 정책 수립부터 운영에 관련된 모든 사항을 포함함

① 정기적으로 실시 ② 필요시에만(비정기적) 실시 ③ 실시안함

D-2. 기술적 보호 방안 - IT(Information Technology)보안 관리

문25. 귀사는 정보시스템 사용 내용에 대한 **로그(Log)***를 **관리**하고 계십니까?

로그(Log)	시스템 접근 시 이용자가 행한 모든 행위를 기록한 파일로써 외부에서 침입을 해온 공격자 및 사용자가 시스템에서 어떤 일을 했는지, 어떠한 명령어를 사용했는지, 시스템에 보안상에 저촉이 되는 행동을 하지 않았는지 등에 대한 정보를 담고 있음

① 회사 자체적으로 정보시스템 사용 로그를 주기적으로 관리함
② 회사 자체적으로 정보시스템 사용 로그를 필요할 때마다 비정기적으로 관리함
③ 정보시스템 사용 로그를 별도로 저장 및 관리하지 않음

문26. 귀사는 외부침입방지를 위해 어떻게 **내부 무선 네트워크**를 **관리**하고 있습니까? (복수응답 가능)

① 내부, 외부 통신망 분리 ② 무선랜 사용 시 ID/PW부여
③ 무선IPS 등 무선보안을 하고 있음 ④ 무선랜 사용에 대한 제한이 없음

문27. 귀사에서 운영하고 있는 **보안솔루션**은 무엇입니까? (복수응답 가능)

① DRM(디지털 저작권 관리)
② DLP(데이터 유출방지 솔루션)
③ IPS(침입방지시스템) / IDS(침입탐지시스템)
④ 방화벽(firewall) 소프트웨어 혹은 하드웨어 장비
⑤ 기타 ( )
⑥ 전혀 운영 안함

DRM (Digital Rights Management : 디지털 저작권 관리)	문서 보안에 초점을 맞춘 기술로 자료를 저장할 때 권한을 설정하고 문서 열람/편집 /인쇄 시, 인증을 받지 못한 이용자에게는 사용을 제한하는 보안 프로그램
DLP (Data Loss Prevention : 데이터 유출방지 솔루션)	특정 데이터가 유출되는 과정을 모니터링하고 이를 선별적으로 차단하는 기능을 제공하는 프로그램
IPS (Intrusion Protection System : 침입방지시스템)	네트워크에서 공격 서명을 찾아내어 자동으로 모종의 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션
IDS (Intrusion Detection System : 침입탐지시스템)	정보시스템에 대한 침입이 발생할 경우 이를 탐지하고 대응하기 위한 프로그램 침입차단을 목적으로 하는 방화벽과는 달리 각종 해킹 수법을 이미 자체에 내장하고 있어 침입행동을 실시간으로 감시·제어·추적

문28. 귀사는 **OS(운영체제)', 백신** 등을 **최신버전**으로 **업데이트하여 관리**하고 있습니까?

OS(운영체제)	컴퓨터의 하드웨어를 제어하고 응용 소프트웨어를 위한 기반 환경을 제공하여, 사용자가 컴퓨터를 사용할 수 있도록 중재 역할을 해 주는 프로그램 예) 마이크로소프트社의 윈도우, 애플社의 맥OS 가 있음

① 보안 패치 자동 설정과 디불어, 이슈 발생 시 별도로 확인
② 패치기 나올 때 마다 적용될 수 있도록 자동 업데이트로 설정
③ 전혀 관리 안함

E. 사고/재해관리

문29. 귀사는 **기술유출 관련 사고**에 **대비**한 **대응절차가 마련**되어 있습니까?
① 구체적으로 마련되어 있으며, 숙지하고 있음 ② 구체적 마련되어 있으나, 내용은 미숙지
③ 일부 마련되어 있음 ④ 마련되어 있지 않음

문30. 귀사는 **중요자료**에 대한 **보호 대책을 수립·시행**하고 있습니까?
① 자체적으로 정기적 백업 관리 ② 자체적으로 비정기적 백업 관리
③ 외부 전문서비스 이용 ④ 관리 안함

문31. 귀사는 **주요시설의 보호**를 위해 재해방지대책 등 **위기관리체계를 수립·시행**하고 있습니까?
① 위기관리체계를 수립 및 시행하고 있음
② 위기관리체계를 수립하였으나 시행하고 있지 않음
③ 수립되어 있지 않음

Part 2. 기술유출 실태

☞ **기술유출이란?**
자사의 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 기술 또는 모든 경영상의 영업 비밀이 부정한 방법(핵심인력 유출, 해킹, 이메일 등)을 통해 경쟁업체 등으로 빠져나가는 모든 경우를 말함

문32. 귀사는 **기술유출 사고가 발생하는 주된 이유**가 무엇이라고 생각하십니까? (복수응답 가능)
① 보안관리, 감독체계 미흡 ② 보안관련 투자 미흡 ③ 보안 전담 인력의 부재
④ 임직원들의 보안의식 부족 ⑤ 개인의 금전적 이익추구 ⑥ 회사의 처우에 대한 불만
⑦ 회사 운영난에 따른 감원 등 직업 불안정
⑧ 기타( )

문33. 귀사는 **기술유출 방지**를 위해서 무엇이 가장 시급하다고 생각하십니까?
① 인력관리 ② 유출 시 처벌법규 강화 ③ 보안시설 장비도입
④ 기술보호 정부지원 강화 ⑤ 기타( )

문34. 기술보호를 위한 **보안관리**에 있어서 **귀사의 애로사항**은 무엇입니까? 아래 항목별로 귀사에서 느끼는 애로정도를 표시해 주십시오.

기술보호를 위한 보안관리 애로정도	매우 그렇다	그렇다	보통	그렇지 않다	전혀 그렇지 않다
1) 예산 부족	①	②	③	④	⑤
2) 보안전담 인력 부족	①	②	③	④	⑤
3) 보안 시설 부족	①	②	③	④	⑤
4) 기술인력의 이직	①	②	③	④	⑤
5) 법적, 제도적 장치 미흡	①	②	③	④	⑤
6) 보안관리에 대한 전문지식 부족	①	②	③	④	⑤
7) 보안관리에 대한 경영진의 중요성 인식 부족	①	②	③	④	⑤
8) 기타(구체적 기재 :)	①	②	③	④	⑤

문35. 귀사는 **최근 3년간** (2016년~2018년) **내부 기술정보가 외부로 유출**된 적이 있습니까?

① 국내로의 유출 있음
② 해외로의 유출 있음
③ 국내 및 해외로의 유출이 모두 있음
④ 유출 된 적이 없음 **(☞문54로)**

문36. **(문35 ①, ②, ③ 응답 시) 최근 3년간**(2016년~2018년) 발생한 **귀사의 기술유출 피해금액**을 **추산**한다면, 얼마 정도인지 국내 및 해외 △ **총 피해 건수**와 △ **총 피해 금액**을 말씀해 주십시오.

국내	유출 건수(합계)	총 피해금액
	건	백만원

(☞국내 유출 있는 경우 문37로 이동)

해외	유출 건수(합계)	총 피해금액
	건	백만원

(☞해외 유출만 있는 경우 문47로 이동)

문37. 귀사는 설립 이후, **최초로 기술정보가 유출된 시기**는 언제입니까?

① 1년 이내 ② 1~3년 이내 ③ 3~5년 이내
④ 5~7년 이내 ⑤ 7~10년 이내 ⑥ 10년 이상

문37-1. 귀사는 기술유출 발생 이후 **어느 시기**에 **인지**하셨습니까?

① 발생 직후 ② 발생 직후 ~ 3개월 이내 ③ 3~6개월 이내
④ 6개월~1년 이내 ⑤ 1~3년 이내 ⑥ 3~5년 이내
⑦ 5년 이상

문38. **누구에게** 기술정보를 **유출** 당했습니까? (복수응답 가능)

① 대기업 ② 중견기업 ③ 중소기업 ④ 정부
⑤ 공기업/공공기관 ⑥ 기타( ) ⑦ 잘 모르겠음

문38-1. 기술정보가 **유출된 곳**과의 **관계**는 무엇입니까? (복수응답 가능)

① 경쟁업체 ② 거래업체 ③ 관계없음 ④ 기타( )

문39. 귀사가 겪은 **기술유출 피해 경위**는 무엇입니까? (복수응답 가능)

① 기술자료 복사·절취 ② 핵심인력 스카웃 ③ 이메일, 휴대용장치 이용
④ 합작사업, 공동 연구 ⑤ 관계자 매수 ⑥ 시찰 및 견학
⑦ 기타 ( )

문40. 귀사의 기술정보를 외부로 **유출시킨 관계자**는 누구였습니까? (복수응답 가능)

① 현 직원(인턴, 임시직 포함) ② 퇴사자(퇴사예정자) (☞문40-1로) ③ 협력업체(하도급) 직원
④ 용역업체 직원 ⑤ 고용외국인(연수생, 기술고문포함) ⑥ 기타( )

문40-1. **(문40 ② 응답 시)** 기술정보 유출 이후 유출 **관계자의 진로 및 동향**은 어땠습니까?

① 국내 대기업으로 이직 ② 중견기업으로 이직 ③ 국내 중소기업으로 이직
④ 해외 대기업으로 이직 ⑤ 해외 중소기업으로 이직 ⑥ 창업
⑦ 계속 근무 ⑧ 기타( )

문41. 귀사에서 **외부로 유출된 기술정보는 어떤 종류**의 것이었습니까? (복수응답 가능)

① 연구과제 개발계획 ② 최종 연구결과 ③ 연구과제 결과데이터
④ 기술도입 및 이전계획 ⑤ 시제품 ⑥ 설계도면
⑦ 생산 중인 제품 ⑧ 기타( )

문42. 귀사의 기술정보는 **어떤 업무과정**에서 **유출**되었습니까? (복수응답 가능)

① 기술 협상 과정 ② 사업 제안 과정 ③ 거래 관계 중
④ 공동 연구 ⑤ M&A 과정 ⑥ 기타( )

문43. 귀사는 기술유출 당한 사실을 **어떻게 알게 되었습니까**? (복수응답 가능)

① 거래업체/고객을 통해 ② 타사에서 발견된 내부 문서를 통해
③ 영업사원/퇴사자의 창업 및 입찰 참가를 통해 ④ 현직원의 유출 사실 보고를 통해
⑤ 컴퓨터에 남은 유출 증거를 통해 ⑥ 출시된 제품을 통해
⑦ 기타( )

문44. 귀사는 기술유출 발생 이후에 **내부적으로 어떠한 조치**를 취하였습니까? (복수응답 가능)

① 보안 관리(자료관리, 출입자통제 등)강화 ② 보안장비 설치 강화 ③ 직원교육(보안의식)강화
④ 특별한 사후조치를 취하지 않음 ⑤ 기타( )

문45. 귀사는 기술유출 발생 시 **외부적으로 어떠한 조치**를 취하였습니까? (복수응답 가능)

① 민사법원에 손해배상 청구(소송) (☞문45-1로)
② 수사기관(경찰 등)에 수사 의뢰
③ 행정기관(중기부, 공정위, 특허청 등) 조사 의뢰
④ 보안 강화 관련 조치 시행
⑤ 조치하지 않음 (☞문45-4로)

문45-1. **(문45 ① 응답 시)** 귀사가 제기한 **소송의 결과**는 어떻게 되었습니까?

① 승소 ② 패소
③ 소송 진행중 ④ 소송 중 취하

문45-2. **(문45 ① 응답 시)** 제기한 소송의 '**소송 제기 시점부터 판결 확정 또는 소송 진행/취하**'까지 **얼마나** 걸렸습니까?

① 6개월 미만 ② 6개월 이상 - 1년 미만 ③ 1년 이상 - 2년 미만
④ 2년 이상 - 3년 미만 ⑤ 3년 이상 ⑥ 기타 ( )

문45-3. **(문45 ① 응답 시)** 제기한 소송의 '**소송 제기 시점부터 판결 확정 또는 소송 진행/취하**'까지 **지출한 비용**은 얼마입니까?

① 5천만 미만 ② 5천만원 이상 - 1억원 미만
③ 1억원 이상 - 2억원 미만 ④ 2억 이상 - 5억원 미만 ⑤ 5억원 이상

문45-4. **(문45 ⑤ 응답 시)** 기술유출 피해 발생 후, 귀사가 **별다른 조치를 취하지 않은 이유**는 무엇입니까? (복수 응답 가능)

① 거래축소/단절 우려 ② 증거 등 입증여력 부족 ③ 업계 이미지 약화 우려
④ 시간과 법적비용 부담 ⑤ 기타( )

☞ **이후 설문은 해외로 기술유출된 피해가 있는 경우에만 작성하여 주시기 바랍니다.**
해외 기술유출 경험이 없는 경우 문52로 이동하여 주시기 바랍니다.

문46. 기술정보가 **유출된 국가**는 어디입니까? (복수응답 가능)

① 중국 ② 동남아시아 ③ 일본 ④ 미국
⑤ 유럽 ⑥ 기타( )

문47. **누구에게** 기술정보를 **유출** 당했습니까? (복수응답 가능)

① 해외 대기업 ② 해외 중소기업 ③ 해외 정부 ④ 해외 공기업/공공기관
⑤ 기타( ) ⑥ 잘 모르겠음

문47-1. 기술정보가 유출된 곳과의 **관계**는 무엇입니까? (복수응답 가능)

① 경쟁업체 ② 거래업체 ③ 관계없음 ④ 기타( )

문48. 귀사가 겪은 기술유출 피해 유형은 무엇입니까? (복수응답 가능)

① 기술자료 복사·절취 ② 핵심인력 스카웃 ③ 이메일, 휴대용장치 이용
④ 합작사업, 공동 연구 ⑤ 관계자 매수 ⑥ 시찰 및 견학 ⑦ 기타 ( )

문49. 귀사의 기술정보를 외부로 **유출시킨 관계자**는 누구였습니까? (복수응답 가능)

① 현 직원(인턴, 임시직 포함) ② 퇴사자(퇴사예정자) (☞문49-1로) ③ 협력업체(하도급) 직원
④ 용역업체 직원 ⑤ 고용외국인(연수생, 기술고문포함) ⑥ 기타( )

문49-1. **(문49 ② 응답 시)** 기술정보 유출 이후 **유출 관계자의 진로 및 동향**은 어떠하였습니까?

① 국내 대기업으로 이직 ② 중견기업으로 이직 ③ 국내 중소기업으로 이직
④ 해외 대기업으로 이직 ⑤ 해외 중소기업으로 이직 ⑥ 창업
⑦ 계속 근무 ⑧ 기타( )

문50. 귀사에서 **해외로 유출된 기술정보**는 **어떤 종류**의 것이었습니까? (복수응답 가능)

① 연구과제 개발계획 ② 최종 연구결과 ③ 연구과제 결과데이터
④ 기술도입 및 이전계획 ⑤ 시제품 ⑥ 설계도면
⑦ 생산 중인 제품 ⑧ 기타( )

문51. 귀사는 기술유출 발생 시 **외부적으로 어떠한 조치**를 취하였습니까? (복수응답 가능)

① 국내 수사기관(경찰, 국정원 등)에 수사 의뢰 ② 현지 법원에 손해배상 청구(소송)
③ 행정기관(중기부, 공정위, 특허청 등) 조사 의뢰 ④ 보안 강화 관련 조치 시행
⑤ 조치하지 않음

Part 3. 기술탈취 실태

☞ **기술탈취란?**
자사의 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 기술 또는 모든 경영상의 영업비밀을 도급 기관(정부/공공기관 및 대기업 등) 혹은 거래업체가 부당한 방법으로 요구하여 탈취하는 모든 경우를 말함
거래관계 등을 이용한 부당한 요구로 인해 기술자료가 상대방으로 넘어가는 것이 기술유출과의 차이점임

문52. **최근 3년간** (2016년~2018년) 귀사는 **거래관계**에서 **기술자료**(영업비밀/경영정보/아이디어 등)에 대한 **탈취 피해를 경험하신 적**이 있습니까?

① 있다 ② 없다(☞문61로)

문53. **(문52 ① 응답 시)** **최근 3년간**(2016년~2018년) 발생한 **귀사의 기술탈취 피해금액**을 **추산**한다면, 얼마 정도인지 △ **총 피해 건수**와 △ **총 피해 금액**을 말씀해 주십시오.

탈취건수 (합계)	□□□ 건	총 피해금액	□□□□ 백만원

문54. 귀사는 설립 이후, **최초로 기술정보를 탈취 당한 시기**는 언제입니까?

① 1년 이내 ② 1~3년 이내 ③ 3~5년 이내
④ 5~7년 이내 ⑤ 7~10년 이내 ⑥ 10년 이상

문55. **누구에게** 기술자료를 탈취 당했습니까? (복수응답 가능)

① 대기업 ② 중견기업 ③ 중소기업 ④ 정부
⑤ 공기업/공공기관 ⑥ 기타 ⑦ 잘 모르겠음

문55-1. 기술자료를 탈취한 조직의 **관계**는 무엇입니까? (복수응답 가능)

① 원사업자 ② 위탁기업 ③ 기타( )
④ 관계 없음

문56. 기술자료에 대한 제공요구는 **어느 단계**에서 요구받으셨습니까? (복수응답 가능)

① 계약체결 전 단계 ② 계약체결 시점 ③ 계약기간 중
④ 재계약(계약갱신) 단계 ⑤ 계약종료 후

문57. 기술자료 제공요구를 받으셨다면, 귀사는 이에 대해 **어떻게 느끼셨습니까**?

① 거래를 위해 당연하다고 느낌 ② 불안하지만 어쩔 수 없다고 느낌 ③ 부당하다고 느낌

문58. 기술자료의 제공 요구가 있었을 경우, 귀사는 **어떻게 대응하였습니까**?

① 쌍방 합의(기술자료 임치* 등) 하에 조건부 제공 (☞문58-1로)
② 기술자료를 전부 제공 (☞문58-1로)
③ 기술자료의 제공 거부

기술자료 임치	중소기업은 핵심기술 정보를 제 3의 기관(대·중소기업·농어업협력재단, 기술보증기금)에 안전하게 보관하고 기술유출이 발생 하였을 경우 임치된 기술자료를 이용하여 해당 기술의 보유 사실을 입증할 수 있음 또한 중소기업과 함께 기술자료 임치제도를 이용한 대기업 등 거래기업은 중소기업이 폐업, 파산 등을 한 경우 기술자료를 교부받아 지속적인 유지보수 및 안정적인 사용이 가능함

문58-1. (문58 ①, ② 응답 시) 기술자료를 제공한 경우, 기술보호를 위해 귀사는 어떻게 **대응**하였습니까?

① 기술요구 서면요청 및 비밀유지 협약체결 ② 기술자료 임치(삼자간 또는 단독 임치)
③ 기술보호 조치 인함 ④ 기타( )

문59. 귀사에서 발생한 기술탈취 **피해 유형**은 무엇입니까? (복수응답 가능)

① 기술의 제3자 유출* ② 부당한 경영정보 요구* ③ 계약 전 기술유용*
④ 공동 지식재산 보유* ⑤ 핵심인력 탈취* ⑥ 기타( )

기술의 제3자 유출	대기업 등이 '공정 프로세스 및 설명서, 제품 설계도' 등 관련 기술자료 일체를 요구하여, 납품업체 다원화 및 납품단가 인하 등 목적으로 관련 기술자료를 경쟁사에 제공하여 동일한 부품을 제조토록 하는 행위
경영정보 요구	세부원가내역서 등 경영정보를 부당하게 요구·취득하여, 이를 활용해 계속된 단가인하로 최소한의 영업이익(1~2% 내외)만 보장하는 행위
계약 전 기술유용	납품 거래를 목적으로 제조방법·도면 등 기술 자료를 제출토록 요구해서 기술 자료만 획득한 후, 계약은 체결하지 않고 등 기술 자료를 유용해 유사제품을 제조·위탁생산하는 행위
공동 지식재산 보유	중소기업이 독자적으로 개발한 기술에 대해 거래계약 등의 이유로 공동 특허출원 등을 요구하여 지식재산권을 공유하는 행위
핵심인력 탈취	경쟁기업이 중소기업의 핵심기술을 취득하기 위해 관련인력을 채용하는 행위

문60. 귀사는 기술탈취 피해발생 이후 귀사는 **어떠한 조치**를 취하였습니까? (복수응답 가능)

① 정부·공공기관에 신고 ② 분쟁지원기관에 해결 요청
③ 민·형사상 법적소송 (☞문60-1로) ④ 기타( )
⑤ 조치하지 않음 (☞문60-4로)

문60-1. **(문60 ③ 응답 시)** 귀사가 제기한 **소송의 결과**는 어떻게 되었습니까?

① 승소 ② 패소
③ 소송 진행중 ④ 소송 중 취하

문60-2. **(문60 ③ 응답 시)** 제기한 소송의 **'소송 제기 시점부터 판결 확정 또는 소송 진행/취하'**까지 **얼마나** 걸렸습니까?

① 6개월 미만 ② 6개월 이상 ~ 1년 미만 ③ 1년 이상 ~ 2년 미만
④ 2년 이상 ~ 3년 미만 ⑤ 3년 이상 ⑥ 기타 ( )

문60-3. **(문60 ③ 응답 시)** 제기한 소송의 **'소송 제기 시점부터 판결 확정 또는 소송 진행/취하'**까지 지출한 **비용**은 얼마입니까?

① 5천만 미만 ② 5천만원 이상 ~ 1억원 미만 ③ 1억원 이상 ~ 2억원 미만
④ 2억 이상 ~ 5억원 미만 ⑤ 5억원 이상

문60-4. **(문60 ⑤ 응답 시)** 기술탈취 피해 발생 후, 귀사가 **별다른 조치를 취하지 않은 이유**는 무엇입니까? (복수 응답 가능)

① 거래축소/단절 우려 ② 증거 등 입증여력 부족 ③ 업계 이미지 악화 우려
④ 시간과 법적비용 부담 ⑤ 기타( )

Part 4. 정책지원 관련 활용실태 및 수요

■ 중소벤처기업부에서는 아래 7가지 기술보호지원사업을 운영중에 있습니다.
지원사업에 관한 자세한 내용은 www.ultari.go.kr를 참조하세요.

1) 기술보호 통합 상담·신고센터(02-368-8787) : 보안진단, 보안기술, 관련법률, 신고 및 수사에 관한 상담서비스 제공
2) 기술보호 전문가 자문(02-368-8787) : 기술보호 전문가가 직접 방문하여 보안전략, 보안시스템, 법률자문 등 교육 및 컨설팅 제공
3) 기술자료 임치(02-368-8787) : 기업간 합의에 의해 기술자료를 보관하여, 기술유출시 선개발 입증을 목적으로 함
4) 기술유출방지시스템 구축사업(02-368-8787) : 우수기술을 보유하고 있는 중소기업을 대상으로 기술유출 가능성을 정밀 진단하고 대책수립을 설계하여, 기업환경에 적합한 보안시스템 구축 지원
5) 중소기업기술분쟁 조정 · 중재(02-368-8787) : 기술유출 피해 기업을 대상으로 신속하고 원만하게 분쟁해결 지원
6) 중소기업 기술지킴서비스(02-3489-7050~3) : 24시간 실시간 온라인 기술유출 감시, 침해시도 분석 및 현장대응 서비스 제공
7) 보안시스템 구축지원(042-388-0758~60) : 기업의 보안인프라에 대한 정밀진단 및 설계 후, 기술유출방지 시스템 구축지원

문61. 귀사는 중소벤처기업부에서 지원하고 있는 아래의 **기술보호지원사업에 대해 알고 있습니까?**

구분	지원사업 인지도		활용 경험		이용 의향	
1) 기술보호 통합 상담 및 신고센터	① 알고 있음	② 모름	① 있음	② 없음	① 있음	② 없음
2) 기술보호 전문가 상담 자문	① 알고 있음	② 모름	① 있음	② 없음	① 있음	② 없음
3) 기술자료 임치	① 알고 있음	② 모름	① 있음	② 없음	① 있음	② 없음
4) 기술유출방지시스템 구축사업	① 알고 있음	② 모름	① 있음	② 없음	① 있음	② 없음
5) 중소기업 기술분쟁조정 · 중재	① 알고 있음	② 모름	① 있음	② 없음	① 있음	② 없음
6) 중소기업 기술지킴서비스(보안관제)	① 알고 있음	② 모름	① 있음	② 없음	① 있음	② 없음
7) 보안시스템 구축지원	① 알고 있음	② 모름	① 있음	② 없음	① 있음	② 없음

문61-1. **(문61 기술보호지원사업 '활용 경험' 1개 이상 ②없음 응답자)** 중소벤처기업부의 기술보호지원 사업을 이용한 적이 없다면 그 **이유는** 무엇입니까? (복수응답 가능)

① 지원사업에 대해 잘 몰라서
② 기술보호 관리 필요성이 없어서
③ 회사의 투자 우선순위가 낮아
④ 자체 보안시스템을 갖추고 있어서
⑤ 비용부담
⑥ 보안담당자가 없어서
⑦ 기타 ( )

문62. 다음 정책의 도입은 귀사의 '기술보호 역량강화'에 **얼마나 효과**가 있을 것이라고 생각하십니까?

구 분	효과성				
	매우 효과적	효과적	보통	비효과적	매우 비효과적
1) 온라인 기술보호 교육 컨텐츠 제공	①	②	③	④	⑤
2) 기업특성에 맞는 차별화된 보안교육(집합교육)	①	②	③	④	⑤
3) 기업 CEO, 임원대상 기술보호 인식교육	①	②	③	④	⑤
4) 기술보호지침(보안 매뉴얼) 제작 배포	①	②	③	④	⑤
5) 보안시스템 솔루션 구축 비용지원	①	②	③	④	⑤
6) 해킹방지, 자료유출방지 보안관제서비스 지원	①	②	③	④	⑤
7) 기술보호 자가진단 소프트웨어	①	②	③	④	⑤
8) 기술보호 전문가 방문진단, 자문 및 교육	①	②	③	④	⑤
9) 기술유출, 탈취 피해 시 법률자문 지원	①	②	③	④	⑤
10) 기술침해 소송비용의 일부 직접 지원	①	②	③	④	⑤
11) 기술실태조사	①	②	③	④	⑤

문63. 정부(중소벤처기업부, 산업통상자원부, 공정거래위원회, 특허청)는 2018년 2월 12일 중소기업 기술보호를 위한 **'중소기업 기술탈취 근절대책"**을 발표했습니다. **이 사실에 대해 알고 계십니까?**

① 예 ② 아니오

중소기업 기술탈취 근절대책	중소기업 기술탈취 근절로 공정한 기술거래 환경을 조성하기 위해 2018년 2월 중소벤처기업부, 산업통상자원부, 공정거래위원회, 특허청에서 발표하였음. 주요 내용은 행정부처 권한을 활용한 신속한 피해구제 실시, 대·중소기업 간 비밀유지협약서 체결 의무화, 기술탈취에 대한 징벌적 손해배상 강화 등이 있음

문63-1. '**중소기업 기술탈취 근절대책**'이 **얼마나 효과**가 있을 것으로 예상하십니까?

구 분	효과성				
	매우 효과적	효과적	보통	비효과적	매우 비효과적
1) 행정부처 권한을 활용한 신속한 피해구제 실시' (행정조사 제도 등)	①	②	③	④	⑤
2) 대·중소기업 간 비밀유지 협약서(NDA) 체결 의무화'	①	②	③	④	⑤
3) 기술탈취에 대한 징벌적 손해배상 강화'	①	②	③	④	⑤
4) 스마트공장 구축 위한 기술자료 임치 의무화'	①	②	③	④	⑤
5) 스마트공장 보안 매뉴얼 개발 및 보급	①	②	③	④	⑤
6) 핵심인력 등록제약 지원	①	②	③	④	⑤
7) 핵심인력 전직 신고제	①	②	③	④	⑤
8) 퇴직인력 하드디스크 임치	①	②	③	④	⑤
9) 퇴직인력 디지털 포렌식 지원	①	②	③	④	⑤
10) 일정기간 전직 및 경업금지 약정 지원	①	②	③	④	⑤
11) 해외진출기업 대상 기술보호방안 설명회	①	②	③	④	⑤

행정부처 권한을 활용한 신속한 피해구제 실시	① 중기부가 접수, 인지한 사건을 관련부처에 연계하고, 사후처리까지 모니터링 ② 범부처 공조체계를 수사기관으로 확대
대·중소 기업 간 비밀유지 협약서(NDA) 체결 의무화	대기업이 중소기업에게 기술 비밀자료를 요구하는 경우, 반드시 비밀유지협약서를 체결하도록 규정하고, 위반 시 벌칙 부과 • 『상생협력법』 개정 추진('18.하)
기술탈취에 대한 징벌적 손해배상 강화	징벌적 손해배상제도를 기술보호 관련 법률에 모두 도입하고, 배상액도 손해액의 최대 '10배 이내'로 강화('18년) • 『하도급법』상 징벌과징금 상한도 현행 '5억원→10억원'으로 상향 추진('18.상, 『하도급법』 시행령 개정)
스마트공장 구축 위한 기술자료 임치 의무화	스마트공장 도입기업과 공급기업은 사업성과물의 유지보수 및 안정적 사용을 보장하고 지식재산권을 보호하기 위해 공급기업의 용역수행에 따른 '기술자료'를 상호간 합의에 의해 임치기관에 2년 이상 임치하여야 함 • 『스마트공장 보급·확산사업 세부관리기준』

문64. 중소기업의 기술보호를 위한 지원정책에 대해 개선할 사항이나 추가지원이 필요하다고 생각되시는 부분을 말씀해 주십시오.

DQ. 회사 일반현황(2018년 기준)

※ 설문 통계처리에 필요한 내용입니다.

<table>
<tr><td>업체명</td><td colspan="3"></td><td>지역
(소재지)</td><td></td></tr>
<tr><td>설립년도</td><td>년</td><td>상시종업원 수</td><td>명</td><td>연구개발
인력 수</td><td>명</td></tr>
<tr><td>기업구분</td><td colspan="5">① 대기업 ② 중견기업 ③ 중소기업</td></tr>
</table>

<table>
<tr><th colspan="8">총매출액</th><th colspan="8">연구개발 투자액</th></tr>
<tr><td>십조</td><td>조</td><td>천억</td><td>백억</td><td>십억</td><td>억</td><td>천만</td><td>백만</td><td>십조</td><td>조</td><td>천억</td><td>백억</td><td>십억</td><td>억</td><td>천만</td><td>백만</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><td>주력업종
(매출비중)</td><td colspan="5">① 전기/전자 ② 화학/섬유 ③ 기계/소재 ④ 정보/통신
⑤ 바이오/의료 ⑥ 에너지자원 ⑦ 지식서비스 ⑧ 기타( )</td></tr>
<tr><td>기술유출관련
소송경험</td><td colspan="5">• 최근 3년(2016년 ~ 2018년) : (건)</td></tr>
<tr><td>연구소/전담부서
보유 여부
(복수응답)</td><td colspan="5">☐ 기업부설연구소 ☐ 연구개발 전담부서</td></tr>
<tr><td rowspan="2">응답자</td><td>성명</td><td></td><td>응답자 휴대폰 연락처</td><td colspan="2"></td></tr>
<tr><td>직위</td><td colspan="4"></td></tr>
<tr><td colspan="4">귀사는 중소벤처기업부의 기술보호 사전예방 및 피해예방을 위한 지원사업에 관하여 제공·안내(이메일, 전화수신 등) 받으시는 것에 대해 동의하십니까 ?</td><td colspan="2">서 명 (인)</td></tr>
</table>

● 응답자 성명 및 연락처는 상품권 지급 및 자료 검증 시 활용되며, 귀하의 개인 정보는 통계법에 의해 철저히 보호됩니다.

※ 설문에 참여해 주셔서 대단히 감사합니다.

ABSTRACT

A Study on the Impact of SMEs' Security Activities on the Establishment of Cyber Incident Management System

Kim, Eun Joung
Major in Smart Convergence Consulting
Dept. of Smart Convergence Consulting
Graduate School, Hansung University

Due to the acceleration of digital transformation, we are living in a hyper-connected era where we can access the Internet anytime, anywhere, with any device. As the work environment has diversified since COVID-19, such as working from home, security risks have diversified and advanced, further requiring understanding and countermeasures against cyber incidents. SMEs are likely to suffer from cyber accidents due to their low security capabilities. Even after the cyber accidents, the scope of investment is limited and it is responding

inefficiently as it is busy with post-processing.

This study proposes a security system for SMEs to respond to cyber incidents.It is intended to understand the impact of each security activity of the security system on responding to cyber incidents and to propose a plan to establish an effective cyber incident management system. The data of the 2019 SME technology protection level survey for SMEs were analyzed using SPSS 23.0 and AMOS 22.0.0, and the research model and hypothesis were verified and studied. After exploratory factor analysis was performed to review the adequacy of the research data, grouped factor analysis and reliability analysis were performed, and validity verification was performed to perform the measurement model test and structural model test. To verify the research model and research hypothesis, path analysis was performed using a structural equation model, and the effects of moderating variables were analyzed by group classification, free model, and constrained model.

As a result of the analysis, the security activities that had a high impact on the establishment of a cyber incident management system were in the order of 'asset management', 'IT management process', and 'system management process'. Previous studies have shown that security policies have the greatest influence on the level of technology protection among security activities. However, in this study, it was found that the security infrastructure and the security process were more influential. It was confirmed that the moderating effect according to whether or not to benefit from the SME support projects were mainly shown in 'system management process', 'security management policy', and 'access control'. The moderating effect of the security manager's role performer was found to be influential in 'access control' when management participated, but it was significantly. The moderating effect of the corporate core information management method was also found to have a higher overall

influence of using external professional services than in the case of SMEs establishing and managing their own backup management system.

If security activities are carried out in the order of the hypothesis adopted in this study, and investment in security policies or security awareness suggested in previous studies is established as a long-term plan, it can be said to establish a meaningful management system in the long and short term. For long-term performance, it will be necessary to analyze the results of SME support projects based on the information protection roadmap and establish a cyber incident management system through continuous supplementation of deficiencies. It is expected that the results of the empirical analysis of this study will help establish effective standards in establishing an information security environment.

【Keyword】 Cyber Incidents, Cyber Incident Management System, SMEs' Support Project, CSO(CISO), Core Asset Management, Security Activities