경영정보학연구
제25권 제4호, 2023년 11월 http://dx.doi.org/10.14329/isr.2023.25.4.205

정보보호 공시 데이터를 이용한 정보보호 관리체계 인증과 조직의 특성 분석

Analysis on ISMS Certification and Organizational Characteristics based on Information Security Disclosure Data

김 선 주 (SunJoo Kim) 충북대학교 대학원 융합보안협동과정 석사과정
김 태 성 (Tae-Sung Kim) 충북대학교 경영정보학과 교수/보안경제연구소장, 교신저자

요 약

정보보호 관리체계(Information Security Management System, ISMS)는 정보 자산의 기밀을 유지하고 결함이 없게 하며 언제든 사용할 수 있게 하는 보호 절차와 과정이고, 국내의 ISMS-P와 국외의 ISO/IEC 27001이 가장 대표적인 ISMS 인증제도이다.

본 논문에서는 ISMS 인증과 조직의 특성과의 관계를 파악하기 위해서 한국인터넷진흥원(KISA), 과학기술정보통신부 전자공시시스템(ISDS), 금융감독원 전자공시시스템(DART)로부터 데이터를 수집하고, Probit 회귀 분석을 실시하였다.

Probit 분석 시 ISMS-P 취득여부, ISO/IEC 27001 취득여부, ISMS-P와 ISO/IEC 27001 모두 취득여부의 세 가지 경우에 대해 독립변수 4개와의 관련성을 확인하였다. 분석 결과, ISMS-P, ISO/IEC 27001 모두 취득한 기업은 총 임직원 수와는 양의 상관관계, 업력과는 음의 상관관계가 있음을 알 수 있었다. 이외에도 ISMS-P 인증제도와 정보보호 공시제도의 개선방향에 대해서도 확인할 수 있었다.

키워드 : 정보보호 관리체계, ISMS, ISMS-P, ISO/IEC 27001, 조직 특성

Ⅰ. 서 론

정보보호 및 개인정보보호 관리체계 인증(Personal Information & Information Security Management System, ISMS-P)은 한국 내 기업의 정보보호 및 개인정보보호 수준을 확보하기 위해 법령에 명시된 인증제도이다. 2001년「정보통신망법」개정으로 정보보호 관리체계 인증제도(Information Security Management System, ISMS[1])가 도입되며 국내 기업 스스로 정보보호 관리체계를 구축, 운영하는데 활용할 수 있는 관리체계 모델이 개발되었다(한국인터넷진흥원, 2021). 이후 2018년 11월에 ISMS 인증제도와 개인정보보호 관리체계 인증(Personal

1) 본 논문에서 ISMS라는 용어는 세가지 의미로 사용된다. 첫 번째는 보편적인 정보보호 관리체계를 의미하는 일반명사로서의 ISMS이고, 두 번째는 2002년 최초 실시된 국내 정보보호 관리체계 인증제도를 의미하는 ISMS이고, 세 번째는 2018년 기존의 ISMS 인증제도와 PIMS 인증제도가 통합된 ISMS-P 인증제도에서 (개인정보를 제외한) 정보보호 관리체계에 한정된 인증을 의미하는 ISMS이다.

Information Management System, PIMS) 제도가 통합되어 ISMS-P 인증제도가 탄생하였다. 2020년 8월에는 ISMS-P 인증제도 소관부처가 행정안전부와 방송통신위원회에서 과학기술정보통신부와 개인정보보호위원회로 변경되었다.

현재 ISMS-P 제도에는 정보보호 중심의 '정보보호 관리체계(ISMS) 인증'과 개인정보 보호 영역이 추가된 'ISMS-P 인증'의 두 가지 버전이 있다. 대상에 따라 ISMS 인증은 의무일 수 있다. ISMS-P 인증기준은 '1.관리체계 수립 및 운영(16개)', '2. 보호대책 요구사항(64개)', '3.개인정보처리 단계별 요구사항(22개)'으로 구성되어 있다(한국인터넷진흥원, 2021).

ISMS-P가 대한민국 내 대표적인 정보보호 관리체계 인증이라면, 국제적으로 가장 권위 있는 정보보호 관리체계 인증은 ISO/IEC 27001이다. ISO(국제표준화기구)와 IEC(국제전기기술위원회)로부터 시작되었으며 정보보안 관리체계의 확립, 시행, 유지, 개선, 위험관리를 위해 개발된 7개 영역의 요구사항에 대해 심사한다(ISO, 2013). ISO에서는 매년 설문조사를 실시하는데, 2021년도 대한민국에 발급된 인증서는 총 460개이며, 조사대상 국가 중 인증서 발급 개수에 있어서 21위를 차지하고 있다(ISO, 2022).

ISMS-P와 ISO/IEC 27001은 모두 정보보호 관리체계 인증이며, 두 가지 인증을 모두 취득하는 기업들이 존재한다. Van Wessel and de Vries(2013)의 영국과 네덜란드의 사례 연구를 살펴보면 기업들이 품질 향상, 비용 절감과 같은 내부적인 요인과 법적 요구사항 및 고객 요구와 같은 외부적인 요인에 의해 ISO/IEC 27001과 ISO/IEC 27002를 취득한다. Mirtsch et al.(2021)의 독일 사례 연구에서도 기업들의 ISO/IEC 27001 취득에 대한 주된 동기가 법적 규제 준수와 고객 요구임을 알 수 있었다. 정보보호 관리체계(ISMS) 인증의 경우 의무 대상자임에도 불구하고 취득하지 않는다면 과태료 부과 대상이 될 수 있다. 한국인터넷진흥원에 따르면 ISMS-P 인증을 취득함으로써 정보보호 및 개인정보보호에 대한 관리수준 향상, 책임성과 신뢰성 향상, 대외 이미지 제고, 공공부문 사업 입찰 시 가산점 부여 등의 기대 효과가 있다(한국인터넷진흥원, 2021).

국내에서 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도에 관해 꾸준한 연구가 이루어지고 있으며, 그 중 특히 조직 특성을 고려한 ISMS-P 개선방안 탐색 시도가 있었다. 또한 조직 내 ISO/IEC 27001 적용에 관한 연구는 해외에서도 활발하게 연구가 진행되고 있다. 하지만 ISMS-P 인증제도에 대한 통제항목 개발 연구는 여러 차례 연구된 바 있지만, 기업 데이터 수집을 통한 조직 특성과의 관계 분석에 대한 연구는 아직 부족한 실정이다. 따라서 본 연구에서는 이러한 선행연구들에서 더 나아가 국내 기업의 사례를 이용해 조직특성과 ISMS-P 인증제도, ISO/IEC 27001 사이의 관계를 실증적으로 분석해보고자 하였으며, 정보보호 공시 데이터, ISMS(ISMS-P) 취득현황, 전자공시 데이터와 같이 신뢰성 있는 데이터를 사용하고자 한다.

기업들이 ISMS-P, ISO/IEC 27001을 모두 취득할 경우, 동일한 분야의 인증 취득을 위해 예산과 인력이 중복으로 투입되는 문제가 발생할 수 있다. 이러한 중복 투입이 불가피할 경우, 낭비가 되지 않도록 ISMS-P는 한국 기업 실정에 맞는 한국만의 정보보호 관리체계 인증이 될 필요가 있다. 본 연구에서는 그러한 점을 고려하여 정보보호 관리체계 인증 제도의 개선 방향도 제시하고자 하였다. 본 연구에서는 ISMS-P, ISO/IEC 27001 인증 취득에 영향을 주는 요인들에 대하여 파이썬으로 작성한 웹 스크래퍼로 데이터를 수집하고 Probit 회귀분석을 실시하였다. 분석을 위해 한국인터넷진흥원의 ISMS-P와 정보보호 공시 현황 데이터, 금융감독원 전자 공시 시스템으로부터 데이터를 수집하였다.

Ⅱ. 정보보호 관리체계 인증제도

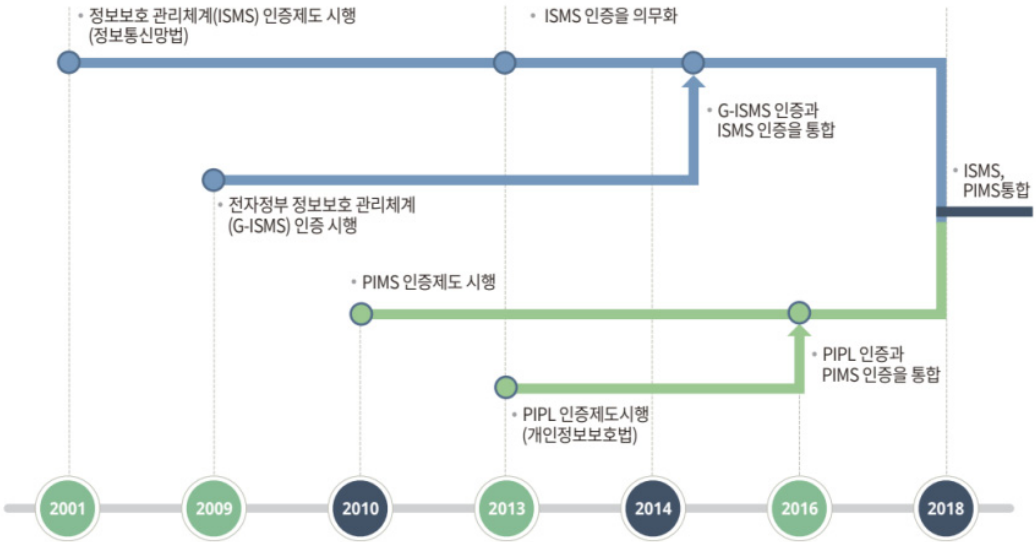
2.1 정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증제도의 추진 경과 (한국인터넷진흥원, 2021)

ISMS-P 인증제도의 변천 과정은 <그림 1>과 같다. 2001년 7월 「정보통신망법」개정을 통해 ISMS 인증제도가 도입되며 국내 기업들로 하여금 정보보호 관리체계를 구축·운영하게 하였다(구 정보통신망이용촉진및정보보호등에관한법률, 2001). 그리고 약 8년 후인 2009년 12월 「전자정부 정보보호관리체계 인증지침」이 제정되면서 공공부문의 인증제도인 G-ISMS(전자정부 정보보호 관리체계, Government Information Security Management System)도 시행되었다(구 전자정부 정보보호관리체계 인증지침, 2014). G-ISMS 제1호는 광주정부통합전산센터, 제2호는 정부통합전산센터이다(김정완, 2010).

2003년 1월 25일 인터넷 침해사고를 계기로 향후 사고 발생 시 경제적, 사회적 피해를 최소화하기 위해 2004년 7월 30일부터 「정보통신망법」에 따라 정보보호 안전진단 제도가 시행되었다(구 정보통신망이용촉진및정보보호등에관한법률, 2004). 이로 인해 조건에 해당되는 정보통신서비스제공자와 집적정보통신시설사업자는 정보보호 컨설팅전문업체로부터 매년 1회 안전진단을 받고 방송통신위원회에 결과를 제출해야 할 의무를 갖게 되었다(한국인터넷진흥원 전자서명인증관리센터, 2009).

개인정보 보호의 중요성이 대두되고 개인정보를 취급하는 조직들이 많아짐에 따라, 2010년 11월 방송통신위원회 의결(제2010-66-273호)로 PIMS (개인정보보호 관리체계 인증, Personal Information Management System) 인증제도가 시행되었다. 초기에는 주요 정보통신서비스 제공 사업자 대상으로 우선 실시하였지만 2013년 2월, 「정보통신망법」을 통해 PIMS 인증제도의 법률적 근거가 마련되었다(구 정보통신망이용촉진및정보보호등에관한법률, 2013; 한국인터넷진흥원, 2021).

2013년에는 ISMS 인증제도 의무화와 PIPL(개인정보보호 인증, Personal Information Production



〈그림 1〉 ISMS-P 인증제도의 변천 과정(한국인터넷진흥원, 2021)

Level) 제도가 실시되었다.「정보통신망법」개정으로 정보통신망서비스제공자(ISP), 집적정보통신시설(IDC)사업자, 정보통신서비스제공자 중 매출액, 이용자 수 등 일정 기준에 해당하는 기업들이 ISMS 인증 의무대상이 되었다(구 정보통신망이용촉진및정보보호등에관한법률, 2013). 또한「개인정보 보호법」개정을 통해 기존 PIMS 인증제도와는 별개로 PIPL이 11월 29일부터 시행되었다(구 개인정보 보호 인증제 운영에 관한 규정, 2021).

이후 ISMS, G-ISMS, 정보보호 안전진단, PIMS, PIPL 제도가 동시에 시행되며 기업들의 부담이 가중됨에 따라 인증 간 통합이 추진되었다. 먼저 2013년에 정보보호 안전진단과 ISMS 인증이 통합되었고, 2014년에 G-ISMS가 ISMS 인증으로 통합되며 민간부문과 공공부문에 동일한 인증제도가 적용되게 되었다. 그리고 2016년 1월, 행정안전부와 방송통신위원회의 공동고시를 통해 PIPL과 PIMS 인증제도가 통합되었다(구 개인정보보호 관리체계 인증 등에 관한 고시, 2021).

2016년 6월에는「정보통신망법」개정으로 연간 매출액 또는 세입 등이 1,500억 원 이상인 자 중 일정 요건에 해당하는 기업들이 ISMS 인증 의무대상에 포함되었다. 정보통신망에 대한 의존도가 높고 개인정보 등 다량의 민감정보를 다루는 기관들이 인증 의무대상에서 제외되는 문제를 반영한 것이다(구 정보통신망이용촉진및정보보호등에관한법률, 2016; 한국인터넷진흥원, 2021).

인증 간 통합을 거쳐 ISMS 인증과 PIMS 인증으로 운영되었지만 두 제도 간 요구사항 중복으로 인해 기업들의 부담은 여전하였고, 다시 ISMS 인증과 PIMS 인증의 통합이 추진되어 ISMS-P가 탄생하였다. 과학기술정보통신부와 행정안전부, 방송통신위원회의 공동고시를 통해 2018년 11월 시행되었다(구 (과학기술정보통신부) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시, 2018).

2020년 8월에는 ISMS-P 인증제도 소관부처가 과학기술정보통신부와 개인정보보호위원회로 변경되었다. 이로 인해 행정안전부, 방송통신위원회로 분산되어 있던 개인정보보호 기능이 개인정보보호위원회로 일원화되었다.

2.2 정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증 범위(한국인터넷진흥원, 2021)

ISMS-P 인증에는 ISMS 인증과, 개인정보 영역까지 심사받는 ISMS-P 인증의 두 가지 유형이 있다. 개인정보 보유 여부와 개인정보 보호 필요성 유무를 기준으로 선택할 수 있다. 현재 ISMS 인증의 경우 의무대상이 법령에 명시되어 있지만, ISMS-P 인증은 그렇지 않다. 다만 정보통신망법 제47조 제2항에 따른 인증 의무대상자는 ISMS 인증 또는 ISMS-P 인증을 취득한 경우 인증의무를 이행한 것으로 본다. 민간, 공공의 구분 없이 병원, 학교, 정보통신서비스제공자 중 일정 규모 이상을 충족하는 조직들이 ISMS 인증 취득 의무대상이다. 정보통신망서비스제공자(ISP), 집적정보통신시설(IDC) 사업자는 매출액 및 이용자 수와 관계없이 인증 의무대상자이다.

본 연구의 분석 대상인 ISO/IEC 27001과 ISMS-P를 비교하면 <표 1>과 같다. ISO/IEC 27001은 1995년부터 시행된 BS 7799의 개정 버전이며, ISMS-P는 2001년부터 시행된 정보보호 관리체계 인증과 2010년부터 시행된 PIMS의 통합 버전이다. ISO/IEC 27001과 ISMS-P의 채택 표준 영역과 개수에도 차이가 있는데, ISO/IEC 27001의 경우 조직, 인력, 물리적, 기술적 영역의 4가지로 구성되어 있고 93개의 통제항목이 있다. ISMS-P의 경우 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항으로 총 102개의 심사기준이 있다. 개인정보 영역을 제외하면 ISO/IEC 27001의 경우 4가지 영역, ISMS-P의 경우 2가지 영역으로 구성되어 있다.

〈표 1〉 ISO/IEC 27001과 ISMS-P 비교

항목	ISO/IEC 27001	ISMS-P
연혁	2005년 10월(BSI, 2005) - 1995년부터 시행된 BS 7799의 개정 버전	2018년 11월 시행 - 2001년부터 시행된 정보보호 관리체계 인증과 2010년부터 시행된 PIMS의 통합
통제(심사)항목	93개(BSI, 2022) - 4가지 영역(조직, 인력, 물리적, 기술적)	102개 - 관리체계 수립 및 운영(16개), 보호대책 요구사항(64개), 개인정보 처리단계별 요구사항(22개)
전체 취득 수	2021년 기준 유효 인증서 58,687개 - 2021년 BSI survey 기준(ISO, 2022)	2023.06.17. 기준 유효 인증서 1,032개 (한국인터넷진흥원, 2023)
2021년도 취득 수	2021년 대한민국 발급 인증서 14,339개 (ISO, 2022)	2021년 발급 인증서 326개(한국인터넷진흥원, 2023)
유효기간	3년 - 1년마다 사후심사, 3년 이후 갱신심사	3년 - 1년마다 사후심사, 3년 이후 갱신심사

또한 ISO/IEC 27001는 국제적 인증이므로 인증 취득 건수가 ISMS-P보다 많았다. 2021년 기준 ISO/IEC 27001 유효 인증서 58,687개에 비해 2023년 기준 ISMS-P(ISMS 포함) 유효 인증서는 1,032개였다. 21년도 기준으로 대한민국 내 발급된 ISO/IEC 27001 인증서는 14,339개, ISMS-P(ISMS 포함)는 326개였다. 국내 ISMS 인증 의무 대상이 아닌 조직들은 ISMS-P보다 ISO/IEC 27001을 더 많이 취득한다는 것을 알 수 있었다. 유효기간의 경우 ISO/IEC 27001과 ISMS-P의 정책이 동일하였다. 취득 후 3년 동안 유효하며 1년마다 사후심사를 받아야 한다.

2.3 정보보호 공시제도(한국인터넷진흥원, 2023)

정보보호 공시제도는 이용자의 안전한 인터넷 이용 및 정보보호 투자 활성화를 위해 정보보호 투자, 인력, 인증, 활동 등 기업의 정보보호 현황을 공개하는 제도이다. 「정보보호산업의 진흥에 관한 법률」제13조(정보보호 공시), 동법 시행령 제8조(정보보호 공시)로 인해 2021년 12월 9일부터 의무화가 시행되었다(구 정보보호산업의 진흥에 관한 법률, 2023; 구 정보보호산업의 진흥에 관한 법률 시행령, 2022). 이용자의 알 권리 보장과 더불어 객관적인 기업 선택의 기준을 제시할 수 있고, 기업에 자발적인 정보보호 투자를 유도할 수 있다.

자율공시와 의무공시로 나뉘며, 정보통신망을 통해 정보를 제공하거나 정보의 제공을 매개하는 사업자는 모두 자율공시가 가능하다. 이외에 사업 분야, 매출액, 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 사업자는 의무공시 대상이다(<표 2> 참고). 공시하여야 하는 내용에는 정보보호 투자 및 인력 현황, 정보보호 관련 인증·평가·점검 등에 관한 사항, 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황이 있다. 또한 과학기술정보통신부 전자공시시스템(ISDS)에 공시된 내용은 한국인터넷진흥원 웹사이트(isds.kisa.or.kr)에 공개되고 있다.

국내 기업·조직에 대해 의무적으로 시행되고 있는 정보보호 관련 제도 중 본 연구에 사용되는 제도들을 <표 3>과 같이 비교해보았다. 두 제도는 서로 다른 법률을 기반으로 하고 있는데, 의무화 시작에 있어 정보보호 공시제도는 2021년 12월 9일부터 시행된 반면 ISMS 인증제도는 2013년 2월 18일부터 시행되었다.

〈표 2〉 정보보호 공시 의무 및 제외대상 기준

구분	기준	상세 요건
의무	사업분야	- 회선설비 보유 기간통신사업자(「전기통신사업법」제6조제1항) - 집적정보통신시설 사업자(「정보통신망법」제46조) - 상급종합병원(「의료법」제3조의4) - 클라우드컴퓨팅 서비스제공자(「클라우드컴퓨팅법」시행령 제3조제1호)
	매출액	정보보호 최고책임자(CISO) 지정·신고하여야 하는 유가증권시장 및 코스닥시장 상장법인 중 매출액 3,000억 이상
	이용자 수	정보통신서비스 일일평균 이용자 수 100만 명 이상 (전년도말 직전 3개월간)
제외	공공기관	공기업 및 준정보기관 등(「공공기관운영법」)
	소기업	평균 매출액 120억 원 이하 기업(「중소기업기본법」시행령 제8조제1항) - 업종별 매출액 기준상이(10~120억 원), 정보통신업은 50억 원 이하
	금융회사	은행, 보험, 카드 등 금융회사(「전자금융거래법」제2조제3항)
	전자금융업자	정보통신업 또는 도·소매업을 주된 사업으로 하지 않은 전자금융업자(「전자금융거래법」제2조제4호, 한국표준산업분류)

〈표 3〉 ISMS 인증과 정보보호 공시제도의 대상 비교(한국인터넷진흥원, 2021; 한국인터넷진흥원, 2023)

		ISMS 인증	정보보호 공시제도
관련 법령		「정보통신망법」제47조 제2항 및 같은 법 시행령 제49조	「정보보호산업의 진흥에 관한 법률 시행령」 제8조
의무	서비스 분야	- 집적정보통신시설 사업자 (「정보통신망법」제46조) - 「전기통신사업법」제6조제1항에 따른 등록을 한 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자	- 집적정보통신시설 사업자 (「정보통신망법」제46조) - 회선설비 보유 기간통신사업자 (「전기통신사업법」제6조제1항) - 클라우드컴퓨팅 서비스제공자 (「클라우드컴퓨팅법」시행령 제3조제1호)
	병원	상급종합병원(「의료법」제3조의4) 중 연간 매출액 또는 세입이 1,500억 원 이상인 자	상급종합병원(「의료법」제3조의4)
	학교	직전연도 12월 31일 기준으로 재학생 수가 1만 명 이상인 「고등교육법」 제2조에 따른 학교 중 연간 매출액 또는 세입이 1,500억 원 이상인 자	-
	매출액	정보통신서비스 부문 전년도 매출액이 100억 원 이상인 자	정보보호 최고책임자(CISO) 지정·신고하여야 하는 유가증권시장 및 코스닥시장 상장법인 중 매출액 3,000억 이상인 자
	정보통신서비스 이용자 수	전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만 명 이상인 자	

〈표 3〉 ISMS 인증과 정보보호 공시제도의 대상 비교(계속)

		ISMS 인증	정보보호 공시제도
의무 제외	공공기관	-	공기업 및 준정보기관 등 (「공공기관 운영법」)
	소기업	-	평균 매출액 120억 원 이하기업 (「중소기업기본법」시행령 제8조제1항) ※ 업종별 매출액 기준상이
	금융회사	-	은행, 보험, 카드 등 금융회사 (「전자금융거래법」제2조제3)
	전자 금융업자	-	「전자금융거래법」제2조제4호, 한국표준산업분류에 따라 정보통신업 또는 도·소매업을 주된 사업으로 하지 않는 전자금융업자
임의신청자· 자율공시자		자발적으로 정보보호 및 개인정보보호 관리체계를 구축·운영하는 기업·기관	정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는자

정보통신서비스 분야에서의 차이점은 정보보호 공시제도에 클라우드컴퓨팅 서비스 제공자가 추가적으로 의무대상에 해당된다는 것이다. 병원의 경우 두 제도 모두 상급종합병원이 의무대상이지만 ISMS 인증제도에서는 매출액 및 세입액 기준이 있다. 정보보호 공시제도에서는 학교가 의무대상에 포함되지 않는다. 또한 매출액 기준 적용에 있어서 ISMS 인증제도에서는 정보통신서비스 부문에 대해 적용하는 반면, 정보보호 공시제도에서는 CISO 지정·신고하여야 하는 유가증권시장 및 코스닥시장 상장법인을 대상으로 하고 있다. 금액 기준도 정보보호 공시제도가 3,000억 원으로 더 높다. 정보통신서비스 이용자 수는 두 제도에서 모두 기준으로 적용하고 있다. ISMS 인증제도와 다르게 정보보호 공시제도에서는 의무 제외대상을 별도로 규정하고 있다. 또한 ISMS 인증제도에서 규정하는 임의신청자가 정보보호 공시제도의 자율공시자보다 그 범위가 더 넓다. 정보보호 공시제도에서는 정보통신망을 통해 정보를 제공하거나 매개하는 자로 한정하고 있다.

2.4 해외의 정보보호 관리체계 관련 정책

본 절에서는 타 국가들에서도 정보보호 관리체계 인증을 제도적으로 시행하고 있는지 조사하였다.

정보보호 관리체계 인증 중 국제적으로 가장 권위있는 인증은 ISO/IEC 27001이다. ISO/IEC 27001:2005 표준은 국제 표준화 기구(ISO, International Organization for Standardization)와 국제 전기 기술 위원회(IEC, International Electrotechnical Commission)가 2005년에 공동으로 발표하였다. 이것은 BS 7799-2:2002를 국제적 표준으로 개정한 것이다(BSI, 2005). 또한 2013년과 2022년에 개정되었다. 모든 규모·분야의 기업에 ISMS를 구축, 구현, 유지 및 지속적으로 개선하기 위한 필수 요구사항과 지침을 제공한다. 이 표준에 대한 준수는 곧 해당 기업이 소유 또는 취급하는 데이터의 보안과 관련된 위험을 관리하기 위한 시스템을 구축했음을 의미한다(ISO, 2023).

영국의 경우 1998년 자국의 표준으로 제정된 BS7799로 ISMS 인증이 시행되고 있다. 인정기관은 UKAS(UK Accreditation Service)이며 인증기관은 BSI, KPMG 등의 7개 기관이다(김원 등, 2022; 장상수, 2020). 또한 NCSC(National Cyber Security Centre)의 Cyber Essentials도 시행되고 있다. 2014년 10월 1일부터 개인정보나 특정 기술, 서비스 제공 또는 민감정보 관련 분야에서 정부와 계약 시 Cyber Essentials 인증을 의무적으로 요구하고 있다(GOV.UK, 2014). Cyber Essentials와 Cyber Essentials Plus의 두 가지 버전으로 운용되고 있으며 Plus 버전의 경우 기술검증이 추가된다. 2023년 3월 기준으로 120,000개의 인증서가

발행되었다(GOV.UK, 2023). IASME(Information Assurance for Small and Medium-sized Enterprises)에서 프로그램을 관리하며 총 9개의 심사영역(Insurance, Boundary Firewalls and Internet Gateways, Secure Configuration, Device Locking, Security update management, User Access Control, Administrative Accounts, Password-Based Authentication, Malware protection)으로 구성되어 있다(NCSC, 2022).

미국은 2002년부터 연방정부기관의 정보시스템에 대한 보호와 최소한의 통제 개발, 유지를 위해 FISMA(Federal Information Security Management Act)를 제정하였으며 인정기관은 OMB(Office of Management and Budget)이다. 인증대상은 81개 연방정부 기관이며 인증기준은 NIST의 정보보호관리 표준이다. 매년 의회에 연방정부기관 보고 시 보안 요구사항과 위협, 보안사고, 규정준수 등 세부사항을 보고하고 있다(김원 등, 2022; 장상수, 2020). NIST가 개발한 표준은 NIST SP(Special Publication) 800-53이며 2023년 6월 기준으로 revision 5까지 발행되었다. 20개 통제영역(Access Control, Awareness and Training, Audit and Accountability, ‘Assessment, Authorization, and monitoring’, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Planning, Program Management, Personnel Security, Personally Identifiable Information Processing and Transparency, Risk Assessment, System and Services Acquisition, System and Communications Protection, System and Information Integrity, Supply Chain Risk Management)으로 구성된다(NIST, 2020).

미국에는 NIST SP 외에도 HIPAA(Health Insurance Portability and Accountability Act)가 시행되고 있다(CDC, 2022). 1996년 HIPAA 법, Public Law 104-191로부터 시작된 연방 법률이며 환자의 민감 건강정보(PHI, Protected Health Information)가 환자의 동의나 지식없이 공개되지 않도록 보호하기 위한 연방법으로부터 시작되었다. 미 보건복지부(HHS)에서 HIPAA의 요구사항을 이행하기 위한 HIPAA 개인정보 보호규칙을 발표하였다. 적용 대상은 Healthcare providers, Health plans, Healthcare clearinghouses, Business associates이다. 2005년 4월 20일부터 적용 의무가 시행되었으며 Privacy, Security, Breach Notification, Compliance & Enforcement의 Rules로 구성된다(HHS, 2023).

일본은 2004년 4월부터 ISMS 적합성평가제도를 운영하고 있으며 인정기관은 경제산업성(METI, Ministry of Economy, Trade and Industry) 산하의 JIPDEC(Japan Information Processing Development Corporation)이다. 인증기준은 JIS Q 27001이며, 이것은 ISO/IEC 27001을 일본어로 번역한 것이다. 일본공업표준조사회(JISC)에 의한 일본공업규격(JIS)으로 지정되어 있다. ISMS 적합성평가제도는 모든 업종, 업무 분야를 대상으로 한다(김원 등, 2022; 다래나무 주식회사, 2020; 장상수, 2020).

독일에서는 IT-Grundschutz(IT Baseline Protection)을 시행하고 있다. 연방정보기술보안청(BSI, Bundesamt für Sicherheit in der Informationstechnik)에서 추진하고 있으며 취득 의무는 없다. IT Baseline Protection 감사 보고서를 제출하여 ISO/IEC 27001 획득 가능하다(Bundesamt für Sicherheit in der Informationstechnik, 2023). 10개 영역, 104개 모듈로 구성되며 10개 영역은 ISMS, ORP(Organisational and personnel security), CON(Crypto Concept and Data Protection), OPS(IT operations), DER(Security Incident Handling and Provisions for IT Forensics), APP(Applications), SYS(Systems), NET(Network), IND(Industrial IT), INF(Infrastructural Security)이다(Bundesamt für Sicherheit in der Informationstechnik, 2022). IT-Grundschutz 외에도 KRITIS Verordnung(BSI-KritisV) 제도가 운영되고 있다. Federal Office for Information Security Act(BSI-Act, BSIG), Regulation on the Designation of Critical Infrastructures pursuant to the BSIG(BSI Critical Infrastructure Regulation, BSI Kritis Regulation, BSI-KritisV)에 따른 중요 인프라에 대한 정보보안 적용 의무가 있으며 중요 인프라란

에너지, 수자원, 식품, 정보통신, 의료, 금융, 교통, 폐기물 등을 의미한다(Bundesamt für Sicherheit in der Informationstechnik, 2023).

EU의 경우, NIS Directive(Directive on Network and Information Security)를 시행하고 있다. NIS Directive는 정보보안에 대한 EU 법률이며 2016년 도입되었고 2023년 NIS2 지침으로 개정되었다(European Commission, 2023). ENISA(European Union Agency for Cybersecurity)에서 이행하고 있으며, EU 회원국의 에너지, 운송, 금융, 보건, 수자원, 디지털 인프라, 공공분야 등을 적용 대상으로 한다. EU 내 사이버위기 관리 체계(Cyclone), 보안 요구사항, 회원국들의 국가 사이버보안 전략 충족 등을 목표로 하고 10가지 핵심 요소 준수(사고 대응, 공급망 보안, 취약점 조치, 암호화 등)로 구성된다(ENISA, 2023; European Commission, 2023). EU 개인정보보호 분야에서는 GDPR(General Data Protection Regulation)이 있다. 2018.05.25.부터 시행되고 있는 EU 개인정보보호 법령이며 11장 99개 조항으로 구성된다. 대상은 EU 내 사업장을 운영하며 개인정보를 처리하거나, EU 거주자에게 재화나 서비스를 제공하거나, EU 거주자의 EU 내 행동을 모니터링하는 기업이다(한국인터넷진흥원, 2023).

Ⅲ. 관련 연구

3.1 조직특성과 정보보호 관리체계

조직 내 정보보호 관리체계에 대한 연구는 오래 전부터 연구되어왔다. Hsu(2009)은 조직에 정보보호 인증을 적용할 때 발생하는 문제점을 분석하였다. IS 보안 관리 개념이 조직의 업무 관행과 일상 업무에 완전히 포함되어 있지 않을 때 관리자와 인증 팀 그리고 그외 직원 간 인식 불일치가 발생한다고 보았다. Siponen and Willison(2009)은 ISMS 인증 기준에 대한 조직 특성 고려 필요성에 대한 연구를 수행하였다. 국제적 정보보안 관리 가이드라인(BS7799, BS ISO/IEC 17799:2000, GASPP/ GAISP, SSE-CMM)은 인증 범위가 일반적이고 보편적이어서 조직 간 다른 보안 요건이 고려되지 않고 있다고 하였다. Line *et al.*(2016)은 노르웨이 전력 산업의 소형 및 대형 배전시스템 사업자에 대해 정보보안 사고 관리에 대한 관행을 조사하였으며 소규모 유통 시스템 사업자는 대형 사업자에 비해 위험 인식이 낮은 경향을 보였다.

또한, 기업의 특성을 고려한 IT 및 정보보호 투자 전략을 제시함으로써 기업들의 의사결정에 도움이 되기 위한 연구도 꾸준히 진행되어 왔다. 강성민, 장강일(2005)은 기업들의 실제 IT 투자관리 사례 분석을 수행하였고 이를 통해 IT 투자관리체계를 구축하려는 기업들에게 실무적 가이드라인을 제시하였다. 김양훈 등(2012)은 소규모 IT 서비스 기업에 대해 보안관리 모델을 설계하고, 해당 기업의 비즈니스 특성을 고려하여 실증분석을 수행한 후 보안관리 추진전략을 제시하였다. 임정현, 김태성(2020)은 다양한 산업군의 기업에 대해 침해사고 유형 통계 분석, 유전자 알고리즘 적용, 설문조사를 실시하였다. 이를 통해 활용 가능한 예산 범위에서 구성할 수 있는 최적의 정보보호 대책 포트폴리오 구성을 제시하였다.

마찬가지로 기업의 특성을 고려하여 ISMS-P 인증 통제항목을 개발하고자 한 연구도 진행되어 왔다. 김동현, 이윤호(2020)는 경력과 회사규모가 다른 IT 종사자들에 대한 설문조사를 수행 후, 통계적 분석을 통해 ISMS-P 인증의 효과성에 대해 분석하였다. 그 결과로 경력과 회사규모에 무관하게 ISMS-P가 중요하게 인식되고 있다는 것을 알 수 있었다. 또한 박혁규 등(2021)은 중소기업의 특성에 맞게 변형한 ISMS-P 인증 통제항목을 제시하였으며, 신용녀(2023)는 하이퍼스케일 클라우드 환경의 특성을 고려하여 보다 더 특화된 ISMS-P 인증 통제항목 개선방안을 제시하였다.

3.2 ISMS 인증 취득에 영향을 미치는 요인

ISO/IEC 27001, ISMS-P 취득에 관해 연구한 문헌

들을 <표 4>에 요약하였다. Mirtsch *et al.*(2021)은 독일 내 ISO/IEC 27001 채택 현황에 대해 조사하였다. 웹 크롤링, 웹 마이닝, Probit 분석을 통해 취득 동인과 현황을 분석하였다. 그 결과 ISO/IEC 27001의 채택률이 기대보다 낮은 현상의 원인을 알 수 있었다. 인증 취득 대신 관리 시스템 표준 구현만 하거나, 인증된 파트너와의 협업을 통해 목적을 달성하는 경우가 있었기 때문이었다. Probit 분석 결과, 기업 규모(총 임직원 수)와는 양의 상관관계가 있었고 업력과는 음의 상관관계가 있었다. 특히 인증된 기업의 거의 절반이 ICT 분야에 속해있었다. 이외에 분석 대상 기업 웹 사이트 대부분이 ISO 9001을 참조하였다. 이외에도 Mirtsch *et al.*(2021)은 설문조사를 통해 동기, 영향, 취득 시의 장애물에 대해 알아보았다. ISO/IEC 27001 취득의 주요 동인은 법적 준수 보장과 정보보안 수준 향상으로 드러났다. ISO/IEC 27001 취득에 있어 ICT 부문 기업은 타 부문의 기업들에 비해 고객 요구사항에 더 많은 영향을 받았다.

Alshitri and Abanumy(2014)는 2013년 6월 기준 사우디아라비아 공공기관 137개를 대상으로 ISO/IEC 27001에 대한 낮은 채택의 원인에 대해 설문조사를 실시하였다. 가장 큰 걸림돌은 정보보안 전문성 부족, 교육 프로그램 부족, 보안 전문가에 대한 높은 급여 요구 등 인적자원 관리 문제로 나타났다. Longras *et al.*(2018)은 포르투갈 내 기업 25개를 대상으로 ISO/IEC 27001 표준 채택 시의 문제점과 한계에 대한 설문조사를 실시하였다. 조사 대상 기업들 중 91.7%가 ISO 9001 인증을 취득했다. 재정적 비용, 범위의 정의, 표준 및 문서의 해석, 변화에 대한 저항, 업무분장 등이 ISO/IEC 27001 채택 시의 어려움인 것으로 조사되었다.

〈표 4〉 ISMS 인증 취득에 관한 문헌고찰

인증	저자	연구목적	연구방법	분석대상	연구결과
ISO/IEC 27001	Mirtsch *et al.* (2021)	취득 동인, 현황 분석	웹 크롤링, 웹 마이닝, Probit 분석	독일 내 912,850개 기업	기업 업종, 규모와 유관
	Mirtsch *et al.* (2021)	동기, 영향, 장애물 통창	설문조사	독일 내 125개 인증기업	- 정보보안 수준 향상 - 법적 준수의 동기 - 재정적 이익은 미미함
	Alshitri and Abanumy(2014)	낮은 채택의 원인조사	설문조사	사우디아라비아 137개 공공기관	인적자원 관리 문제
	Longras *et al.* (2018)	장애물 분석	설문조사	포르투갈 내 25개 기업	예산, 범위 정의, 표준 해석, 변화 저항 등
ISMS-P 인증	Chang(2013)	경제적 효과 분석	재무정보 분석	대한민국 내 15개 기업	기업가치 상승, 고용창출
	김동현, 이윤호 (2020)	인증의 효과성 분석	설문조사	경력과 회사규모가 다른 IT 종사자 50명	경력, 회사규모에 무관하게 ISMS-P가 중요하게 인식됨
	박혁규 등(2021)	중소기업에 맞는 통제항목 제시	자료분석	ISMS-P 인증기준	- 중소기업에 적합한 평가 항목 도출 - 기존보다 28.4%의 항목 감소
	신용녀(2023)	하이퍼스케일 클라우드의 통제항목 개발	자료분석	ISMS-P 인증기준	클라우드에 특화된 통제항목 개선방안 제시

ISMS-P 인증 취득에 대한 연구도 찾을 수 있었다. Chang(2013)은 인증 취득에 따른 기업의 경제적 효과를 분석하였다. 대한민국 내 ISMS 인증을 취득한 A사와 유사 업종 및 규모의 다른 15개 기업을 표본으로 추출하여, 인증 취득 이후 3년(2006~2008) 동안의 재무정보를 기반으로 유사기업과의 성과 분석을 실시하였다. 그 결과, 인증기업은 ISMS 인증 후 인건비 상승률이 -1.69%로 낮아져 지난 해 증가율 대비 3.05%의 효율성을 보였으며 표준 업무 프로세스를 통해 효율성을 향상시켜 연간 4,270만 원 절감한 것으로 분석하였다. 이에 따라 조직 내 보안관리시스템 도입을 통한 경제적 효과는 연간 2억 2천만 원으로 측정하였고, 업계의 경제적 효과로 매출 증가액은 약 2억 1,600만 원, 일자리 창출은 약 2.47명이라고 하였다.

3.3 Probit 모델을 이용한 연구

종속변수가 이진 변수일 때 적용할 수 있는 회귀모형 중 하나인 Probit 모델은 그간 연구들에 <표 5>와 같이 다양하게 적용되어 왔다. Mirtsch *et al.*(2021)은 독일 내 ISO/IEC 27001 취득과 조직 특성과의 관계를 알아보았다. 모든 업종의 기업에 대해 Probit 모델을 적용하고, 이후 ICT 서비스 분야에 대한 기업들만을 대상으로 Probit 모델을 적용했다. 데이터셋은 912,850개의 기업 데이터로 구성하였고 4개의 독립변수를 사용하였다.

Nikita and Nikitas(2020)는 골격 성별 추정을 위한 로지스틱, 프로빗 및 누적 프로빗 회귀, 선형 및 2차 판별 분석, 인공 신경망 및 네이브 베이즈 분류 방법을 실시하고 성능을 비교하였다. 데이터셋은 225개의 해골로 구성된 그리스 카포디스트리아 대학교의 아테네 컬렉션 중 191개의 골격을 대상으로 하였다. Zhang and Ye(2013)는 중국 최고 경영진의 위험선호가 기업의 기술혁신 실패에 미치는 영향을 분석하였다. 데이터셋은 2011년부터 2017년까지 중국 제약상장기업 80개의 유효표본 480개를 대상

〈표 5〉 Probit 모델을 응용한 연구사례

저자	분야	연구방법
Mirtsch *et al.*(2021)	독일 ISO/IEC 27001	- 912,850개 기업 대상 - 독립변수 4개 사용 - 제2의 데이터셋과 분석결과 비교 - Correlation test
Nikita and Nikitas(2020)	골격성별추정	- 191개 골격 대상 - Correctly classified 값
Zhang and Ye(2021)	중국 경영진의 위험선호와 기술혁신 실패	- 80개 기업의 유효표본 480개 대상 - 독립변수 3개 사용 - $Pseudo\,R^2$ (0.05 ~ 0.1)
Ngenoh *et al.*(2019)	소규모 농업인의 제약 극복	- 독립변수 27개 사용 - Correlation test - 타 연구결과 비교
Sun and Lyu(2020)	중국 의료보험과 치명적인 의료 지출	- Probit, logit 분석결과 비교 - 타 연구결과 비교
Leśniak *et al.*(2019)	폴란드 교량특성과 프로젝트 지연	- Probit, logit 분석결과 비교 - Correctly classified 값 비교
Roberts *et al.*(2018)	환경태도와 통근방법	- $Pseudo\,R^2$ (0.05 ~ 0.1) - 제2의 데이터셋과 분석결과 비교 - 타 연구결과 비교 - Correctly classified(71.74 ~ 76.12)

으로 하였다. 독립변수는 3개를 사용하였다. Ngenoh *et al.*(2019)은 아프리카 시장에서 소규모 농업인의 제약 극복을 위한 동인, 인센티브를 분석하기 위해 Probit 모델을 적용하였다. 27개의 독립변수를 사용하였으며, 데이터셋은 총 1,232개의 농촌 및 도시 주변 토종채소 생산 가구의 가구 수준 데이터로 구성하였다. Sun and Lyu(2020)은 중국에서 의료보험이 치명적인 의료지출에 미치는 영향을 분석하기 위해 Random effects panel probit 회귀 모델을 적용하였다. Robustness test를 위해 random effects panel logit 회귀 모델을 수행하였으며 Probit, Logit 적용 결과가 일치하였다. 2012년, 2014년, 2016년에 수행된 중국 가족 패널 연구 데이터 중 5,768개의 샘플로 데이터셋을 구성하였다. Leśniak *et al.*(2019)은 폴란드 교량 특성과 프로젝트 지연 간의 관계를 분석하였다. Probit, Logit 분석을 모두 수행하여 correctly classified 값을 비교하였다. 데이터셋으로는 2005년~2017년 동안 폴란드에서 건설된 도로 및 철도 교량으로 구성된 총 109건의 사업 데이터가 사용되었다. Roberts *et al.*(2018)은 환경 태도가 통근 방법 선택에 미치는 영향을 분석하였다. Robustness test를 위해 두 개의 다른 데이터 셋으로 모델링을 복제하였으며, 타 연구결과들과 결과를 비교하였다. 데이터셋으로 영국 가정 연구(UKHLS) 데이터를 사용하여 표본 크기는 여성 6,883명과 남성 6,256명이다.

Ⅳ. 데이터 수집과 분석

4.1 데이터 수집

분석을 위해 파이썬으로 작성한 웹 스크래퍼를 사용하여 ISMS-P, ISO/IEC 27001 취득 현황에 대한 국내 기업들의 데이터를 수집했다. 데이터의 신뢰성을 보장하기 위해 ISMS-P 취득 현황은 한국인터넷진흥원에서 수집하고, ISO/IEC 27001 취득 정보는 정보보호 공시 데이터로부터 수집하였다. 정보보호 공시 데이터와 전자공시 데이터로부터 기업 특성 정보도 얻을 수 있었다.

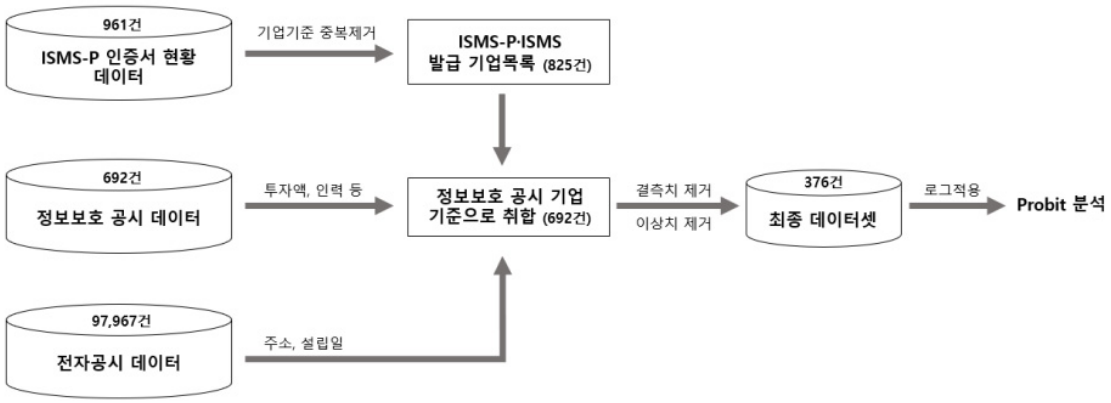
한국인터넷진흥원은 정보보호 관리체계 인증 및 ISMS-P를 위한 사이트를 운영하고 있다. 해당 사이트에서 2023년 4월 6일 기준 유효한 인증서 데이터 961건을 수집하였고 기업명, 발급번호(연도 포함), 유효 인증서 개수, 인증범위가 포함된다. 기업 기준으로 중복없이 분석하기 위해 가장 최신 데이터만 남기고, ISMS와 ISMS-P 모두 취득했을 경우 ISMS-P 데이터만 남기는 작업을 하였다.

과학기술정보통신부 전자공시시스템(ISDS)에 입력된 데이터는 한국인터넷진흥원 홈페이지(isds.kisa.or.kr)에서 확인할 수 있다. 해당 사이트에서 2023년 3월 25일 기준 공시현황 692건을 수집하였고 연도, 기업명, 업종, 정보기술부문 투자액, 정보보호부문 투자액, 주요 투자 항목, 총 임직원 수, 정보기술부문 인력, 정보보호부문 전담인력(내부, 외주), CISO 및 CPO 지정현황, 정보보호 관련 인증·평가·점검 등에 관한 사항, 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황 등이 포함되어 있다.

전자공시 데이터는 금융감독원 DART 시스템(전자공시 시스템, Data Analysis, Retrieval and Transfer System)에 저장되어 있고 Open DART (opendart.fss.or.kr)를 통해 수집 가능하다. 2023년 4월 8일 기준으로 기업개황 정보를 수집하였으며 기업 명칭, 종목명, 대표자명, 법인구분, 주소, 전화번호, 업종코드, 설립일, 결산월 등의 정보가 포함된다.

4.2 데이터 전처리

<그림 2>는 데이터 전처리 흐름도이다. 정보보호 공시데이터의 기업명 기준으로 수집한 데이터들을 매핑하였다. 분석에 사용할 변수는 <표 6>과 같이 정의하였다. 또한 업종 간 차이를 알아보기 위해 ICT 업종(정보통신업)과 비 ICT 업종으로 구분하여 분석을 시도하였고, 이를 위해 업종 데이터를 수집한 후 더미변수화 하였다. 정보통신업을 기준으로 하여 비 ICT 업종에 대한 0 또는 1 값을 독립변수로



〈그림 2〉 데이터 전처리 흐름도

〈표 6〉 분석에 사용한 변수

구분	변수명	내용
종속변수(Case)	both	인증 중복취득 여부(0 또는 1)
	ismsp	ISMS-P 취득여부(0 또는 1)
	iso27001	ISO/IEC 27001 취득여부(0 또는 1)
독립변수	budget_IS_weight	정보기술부문 대비 정보보호부문 투자액의 비중
	staff_IS_weight	정보기술부문 대비 정보보호부문 인력의 비중
	staff_all	기업의 규모 - 총 임직원 수(명, log)
	age	기업의 업력(년도)
	industry_dummy	업종 더미변수 (정보통신서비스 업종일 경우 0, 그렇지 않을 경우 1)

추가하였다. 투자액 혹은 인력 수를 공시하지 않은 결측치를 제거하고, 각 변수별 이상치를 제거하였다. 최종적으로 ISMS-P 취득여부, 투자액, 인력, 주소, 설립일 등을 종합한 376건의 데이터로 정리하였다.

정보보호 공시데이터 중, 한국만을 위한 정보보호 예산과 인력을 특정하기 어렵다고 공시내용을 기재한 글로벌 대기업 사례와 같은 결측치 148건을 제거하여 544건의 데이터셋이 되었다.

이상치 제거 시에는 Boxplot 규칙을 사용하였다. 정규분포에서 데이터들이 ±3σ 바깥에 존재하면 이상치로 처리하는 3-Sigma 규칙보다 데이터의 사분위수를 확인하여 처리하는 Boxplot 규칙이 더 적합하다고 판단하였기 때문이다. Zhao *et al.*(2013)에 따르면, 태양광 발전의 고장 감지를 위한 이상치 탐지 과정에서 3-Sigma 규칙, Hampel 식별자, Boxplot 규칙의 성능을 비교하였으며, 그 중 Boxplot 규칙이 가장 성능이 뛰어난 것을 확인할 수 있었다. Chen *et al.*(2023)에서도 Boxplot 규칙은 3-Sigma 규칙과 Z-fraction 방식에 비해 보편성이 좋다고 하였다.

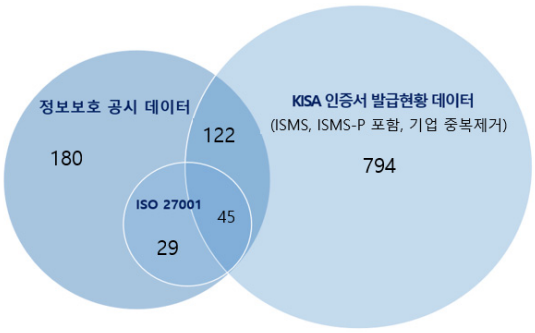
<표 7>에 이상치 제거 후 독립변수별 데이터 값 범위를 정리하였다. 데이터 값 단위에 큰 차이가 있는 staff_all 변수에만 로그를 적용하여 0.95 ~ 3.67로 조정하였다. 데이터들을 같은 비율의 수로 변환하여 데이터 간 편차를 줄이기 위함이다.

〈표 7〉 독립변수별 데이터 값 범위

변수 명	범위
budget_IS_weight	0.19 ~ 19.51
staff_IS_weight	0.33 ~ 21.43
staff_all	9 ~ 4664
staff_all(in logs)	0.95 ~ 3.67
age	1 ~ 89

고시개정에 영향 받은 ISMS-P 데이터를 제외하고자 하였다. 정보보호 관리체계 인증, PIMS 통합 시점은 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 개정일자인 2018년 11월 7일이다(구 (과학기술정보통신부) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시, 2018). 따라서 고시개정에 영향을 받아 제거가 필요한 인증서는 2015년 11월 7일 ~ 2018년 11월 7일 기간 내 발급된 인증서이다. ISMS-P 인증 유효기간은 3년이기 때문이다. 확인 결과, 분석에 사용한 데이터는 모두 2020년 4월 16일 이후 발급된 인증서였다.

<그림 3>은 Probit 분석에 사용되는 주요 데이터 수집원 간의 관계를 벤 다이어그램으로 표현한 것이다. 정보보호 공시를 한 기업들 중 정보보호 관리체계 인증 또는 ISMS-P를 취득하지 않은 기업들(55.59%, 209개)이 취득한 기업들(44.41%, 167개)보다 더 많았다. 또한 정보보호 관리체계 인증, ISMS-P를 취득한 기업들 중 정보보호 공시를 하지 않은 기업이 대다수였다(82.62%). 인증 취득현황은 <표 8>에 정리하였다. ISMS 분야의 인증을 중복으로 취득한 기업들의 비율을 확인해본 결과, ISMS-P와 ISO/IEC 27001을 모두 취득한 비율은 5.59% 이었으며 정보보호 관리체계 인증과 ISO/IEC 27001을 모두 취득한 비율은 6.38% 이었다. ISMS-P 최초 취득에 필요한 평균 비용 26,728,814원(원병철, 2020)을 고려하면, ISMS-P와 ISO/IEC 27001을 모두 취득하고 사후갱신하기 위해 적지 않은 금액이 필요한 것을 알 수 있다.



〈그림 3〉 주요 데이터 수집원 간 관계

수집한 데이터 중 동일한 내용임에도 기업명, 인증명이 제각기 입력된 경우가 상당수였다. 정보보호 공시 데이터를 규격화된 정형 데이터로 분석하기 위한 제도 개선이 필요함을 알 수 있었다.

〈표 8〉 인증 취득현황 비율

범위	구분	사례 수	비율(%)
Probit 분석 대상 데이터셋	ISMS-P만 취득	45건	11.97
	정보보호 관리체계 인증만 취득	122건	32.45
	ISMS-P 또는 정보보호 관리체계 인증 취득	167	44.41
	ISO/IEC 27001 취득	74건	19.68
	ISMS-P와 ISO/IEC 27001 취득	21건	5.59
	정보보호 관리체계 인증과 ISO/IEC 27001 취득	24건	6.38
정보보호 공시 데이터	정보보호 관리체계 인증 또는 ISMS-P 미 취득	209건	55.59
	정보보호 관리체계 인증 또는 ISMS-P 취득	167건	44.41
정보보호 관리체계 인증, ISMS-P 취득현황 데이터	정보보호 공시를 하지 않은 기업들	794건	82.62

〈표 9〉 Probit 분석대상 데이터셋 중 타 정보보호 인증 취득현황

인증명	인증내용	건수
ISO/IEC 27701	Privacy Information Management	18
ISO/IEC 27017	Security controls for cloud services	10
ISO/IEC 27018	Protecting personally identifiable information in the public cloud	6
ISO 27799	Health Informatics-Information Security Certification	3
ISO/IEC 29100	Privacy framework	1
ISO/IEC 22301	Business Continuity Management Certs	1
EMR 인증	전자의무기록시스템 인증	15
PCI DSS	Payment Card Industry Data Security Standard	12
CSAP	Cloud Security Assurance Program	8
CSA STAR	Cloud Security Alliance	8
ePRIVACY	국내 개인정보보호 민간 인증(개인정보보호협회)	7
ePRIVACY PLUS	국내 개인정보보호 민간 인증(개인정보보호협회)	3
SOC 2, SOC 3	Service Organization Control	3
BS10012	개인정보보호 경영시스템	2
TISAX	Trusted Information Security Assessment Exchange	1
MTCS	Multi-Tier Cloud Security	1
정보보호 준비도 평가(AAA)	과학기술정보통신부 주관 정보보호 수준평가	1

<표 9>는 Probit 분석대상 데이터셋 376건 중 타 정보보호 인증 취득 현황을 정리한 것이다. 주로 개인정보보호, 클라우드와 관련된 인증이 많았으며 국내 인증보다는 해외 인증 취득 수가 더 많았다. ISO/IEC 27001 취득에 비해 타 인증 취득 수는 크지 않았다. 또한 특정 업종(의료, 자동차, 금융) 분야에서의 정보보호 인증을 취득한 사례도 있었는데 그 중 의료 관련 인증 수가 가장 많았다.

Ⅴ. Probit 분석 결과

5.1 분석 결과

Mirtsch *et al.*(2021)의 연구에서 독일 기업의 ISO/IEC 27001 취득 현황에 대해 Probit 모델을 적용하였는데 본 연구에서는 대한민국과 독일의 결과를 비교해보고자 Probit 모델을 적용하였다. 또한 5.2절에서 결과 검증을 위해 로지스틱 모델을 사용하였다. 종속변수 세 가지의 경우에 대한 각 Probit 모델 적용 결과는 <표 10> ~ <표 12>에 정리하였다. 독립변수 ismsp와 종속변수들 간의 분석결과는 <표 10>이고, 독립변수 iso27001과 종속변수들 간의 분석결과는 <표 11>이며, 독립변수 both와 종속변수들 간의 분석결과는 <표 12>이다.

모든 경우에서 Coefficient의 방향은 동일하였지만, 값은 차이가 있었으며 유의정도가 달랐다. 세 가지 경우 모두 staff_all(기업 규모, 총 임직원 수)의 계수 값은 양의 방향이었고, age(업력)의 계수 값은 음의 방향이었다. budget_IS_weight(정보기술부문 대비 정보보호부문 투자액의 비중) 변수의 경우 iso27001을 종속변수로 설정한 분석에서만 유의성을 나타내었다. staff_IS_weight(정보기술부문 대비 정보보호부문 인력의 비중) 변수의 경우 모든 경우에서 유의미한 결과가 나오지 않았다.

staff_all 변수의 경우 iso27001 > both = ismsp 순으로 유의성이 높았으며 Coefficient 값은 both > iso27001 > ismsp 순으로 크게 나왔다. both를 종속변수로 한 분석에서 값이 양의 방향으로 가장 크게 나왔으며(0.874) 계수가 가장 작았던 경우는 ismsp를 종속변수로 한 경우이다(0.539).

〈표 10〉 Probit 분석 결과(ismsp)

ismsp (*Nagelkerke* R^2 = 0.12, Accuracy = 0.88)			
Variable	Coefficient	Std.error	Z value
budget_IS_weight	0.024	0.025	0.941
staff_IS_weight	-0.003	0.021	-0.159
staff_all (in logs)	**0.539****	0.190	2.828
age	**-0.016****	0.005	-2.985
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	**-0.653****	0.216	-3.017

*p<0.10, **p<0.05, ***p<0.001.

〈표 11〉 Probit 분석 결과(iso27001)

iso27001 (*Nagelkerke* R^2 = 0.16, Accuracy = 0.82)			
Variable	Coefficient	Std.error	Z value
budget_IS_weight	**0.037***	0.023	1.659
staff_IS_weight	-0.016	0.019	-0.850
staff_all (in logs)	**0.763*****	0.176	4.331
age	**-0.019*****	0.005	-4.118
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	**-0.626****	0.199	-3.151

*p<0.10, **p<0.05, ***p<0.001.

〈표 12〉 Probit 분석 결과(both)

both (*Nagelkerke* R^2 = 0.21, Accuracy = 0.94)			
Variable	Coefficient	Std.error	Z value
budget_IS_weight	0.054	0.034	1.601
staff_IS_weight	-0.015	0.030	-0.509
staff_all (in logs)	**0.874****	0.275	3.175
age	**-0.029*****	0.009	-3.342
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	**-0.719***	0.282	-2.550

*p<0.10, **p<0.05, ***p<0.001.

age 변수의 경우에는 iso27001 = both > ismsp 순으로 유의성이 높았으며, Coefficient 값은 both > iso27001 > ismsp 순으로 절대 값이 컸다. 마찬가지로 both를 종속변수로 한 분석에서 절대 값이 가장 크게 나왔다(-0.029). 계수는 ismsp를 종속변수로 한 경우에서 절대 값이 가장 작았다(-0.016).

Nagelkerke R^2 값을 계산한 결과 both를 종속변수로 한 분석에서 값이 가장 크게 나왔고(0.16), ismsp를 종속변수로 한 분석에서 값이 가장 작게 계산되었다(0.12). both > iso27001 > ismsp 순으로 값이 크게 나왔다.

Accuracy 값을 계산하였을 때도 both의 경우가 가장 크게 나왔다(0.94). 정분류율은 both > ismsp > iso27001의 순으로 값이 컸으며, 유의성 값의 추세나 Coefficient 값의 추세, 그리고 $Nagelkerke\,R^2$ 값과는 다르게 ismsp의 경우가 iso27001보다 컸다.

종속변수 세 가지 경우에 대한 각 Probit 분석 결과, 3가지 케이스 모두 기업규모(총 임직원 수)와는 양의 상관관계, 업력과는 음의 상관관계가 있었으며 정보통신서비스 업종과는 음의 상관관계가 있었다. 종합하면 ISMS-P, ISMS-P & ISO/IEC 27001 모두 취득의 경우 모두 기업규모가 클수록(총 임직원 수가 많을수록), 업력이 오래되지 않은 기업일수록, 정보통신서비스 업종일수록 취득할 가능성이 더 높아지는 것으로 판단할 수 있다. 또한 ISO/IEC 27001의 경우 정보기술 대비 정보보호 예산 비중과 기업규모가 클수록, 업력이 낮을수록, 정보통신서비스 업종일수록 취득할 가능성이 더 높아진다. 이외에 both를 종속변수로 했을 때 계수 절댓값이 가장 크므로, 두 인증 모두 취득하는 경우 업력과 기업규모, 그리고 업종으로부터 더 많은 영향을 받는 것을 알 수 있었다.

본 연구의 분석 결과는 Mirtsch *et al.*(2021)의 연구 결과와도 일치한다. 기업규모, 업력, 업종이 ISO/IEC 27001 인증 취득에 미치는 영향은 독일과 한국의 실증 결과가 동일하다는 것을 알 수 있었다.

5.2 결과 검증

분석결과 검증을 위해 <표 13> ~ <표 15>와 같이 Logistic 모델을 이용하여 동일한 데이터셋에 대해 분석해보았다. Logistic, Probit 모델 모두 분석결과의

〈표 13〉 Logistic 분석 결과(ismsp)

ismsp ($Nagelkerke\,R^2$ = 0.12, Accuracy = 0.88)			
Variable	Coefficient	Std.error	Z value
budget_IS_weight	0.043	0.047	0.920
staff_IS_weight	-0.008	0.040	-0.186
staff_all (in logs)	**0.991****	0.357	2.779
age	**-0.030****	0.010	-2.881
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	**-1.229****	0.392	-3.134

*p<0.10, **p<0.05, ***p<0.001.

〈표 14〉 Logistic 분석 결과(iso27001)

iso27001 ($Nagelkerke\,R^2$ = 0.16, Accuracy = 0.82)			
Variable	Coefficient	Std.error	Z value
budget_IS_weight	**0.066***	0.039	1.671
staff_IS_weight	-0.024	0.034	-0.698
staff_all (in logs)	**1.354*****	0.318	4.265
age	**-0.031*****	0.008	-3.828
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	**-1.148*****	0.343	-3.347

*p<0.10, **p<0.05, ***p<0.001.

계수 방향이 일치하였고 유의성도 유사한 모습을 보였다. staff_all 변수의 유의성 순위와 Coefficient 값 순위가 Probit 모델 적용 시와 동일하였으며 계수가 가장 작았던 경우도 ismsp 케이스로 동일하였다. age 변수의 경우 both를 종속변수로 했을 때 유의성이 감소하였다. 절대 값 순위와 Coefficient 값 순위는 Probit 모델 적용 시와 동일하였다. 또한 Probit 적용 시보다 Logistic 적용 시 Coefficient 값이 더 컸다. $Nagelkerke\,R^2$ 값도 거의 유사하였으며 Accuracy 값은 동일하였다.

일반적으로 VIF(분산 팽창 인수, Variance Inflation Factor)가 10 이상일 경우 다중공선성(Multicollinearity)이 있는 것으로 간주된다(O'Brien, 2027). Probit, Logistic 모델 적용시 각각에 대해 VIF를 계산하고 그 결과를 <표 16>, <표 17>에 정리하였다. 모든 값들이 1.4 이하이므로 다중공선성이 없는 것을 확인할 수 있었으며 Probit 모델을 적용했을 때와 Logistic 모델을 적용했을 때 모두 다중공선성이 발생하지 않았다는 것도 확인하였다.

〈표 15〉 Logistic 분석 결과(both)

both ($Nagelkerke\,R^2$ = 0.20, Accuracy = 0.94)			
Variable	Coefficient	Std.error	Z value
budget_IS_weight	0.106	0.067	1.593
staff_IS_weight	-0.038	0.062	-0.610
staff_all (in logs)	**1.686****	0.552	3.052
age	**-0.058****	0.018	-3.164
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	**-1.488****	0.552	-2.698

*p<0.10, **p<0.05, ***p<0.001.

〈표 16〉 Probit 분석 시 다중공선성(Multicollinearity) 확인 결과(VIF)

Case / Variable	ismsp	iso27001	both
budget_IS_weight	1.248	1.250	1.338
staff_IS_weight	1.266	1.257	1.322
staff_all (in logs)	1.378	1.387	1.361
age	1.110	1.128	1.069
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	1.374	1.367	1.355

〈표 17〉 Logistic 분석 시 다중공선성(Multicollinearity) 확인 결과(VIF)

Case / Variable	ismsp	iso27001	both
budget_IS_weight	1.268	1.270	1.388
staff_IS_weight	1.281	1.266	1.385
staff_all (in logs)	1.355	1.390	1.319
age	1.083	1.105	1.047
industry_dummy (정보통신서비스 업종이 아닐 경우 1)	1.364	1.378	1.347

Ⅵ. 결 론

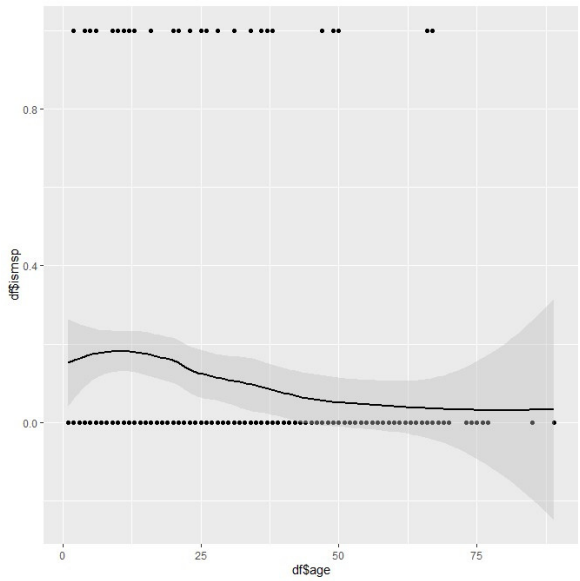
6.1 시사점

본 연구의 학술적 시사점은 ISMS 분야의 대표적인 인증 중 국내의 ISMS-P 인증제도, 해외의 ISO/IEC 27001에 대해 조직 특성과의 관계를 실증적으로 분석하였다는 것이다. 또한 이 때 한국인터넷진흥원(KISA), 과학기술정보통신부 전자공시시스템(ISDS), 금융감독원 전자공시시스템(DART)과 같이 정부기관에서 제공하는 신뢰성 있는 데이터를 사용하여 회귀분석을 하였다는 점에서 방법론적 의의도 찾을 수 있다.

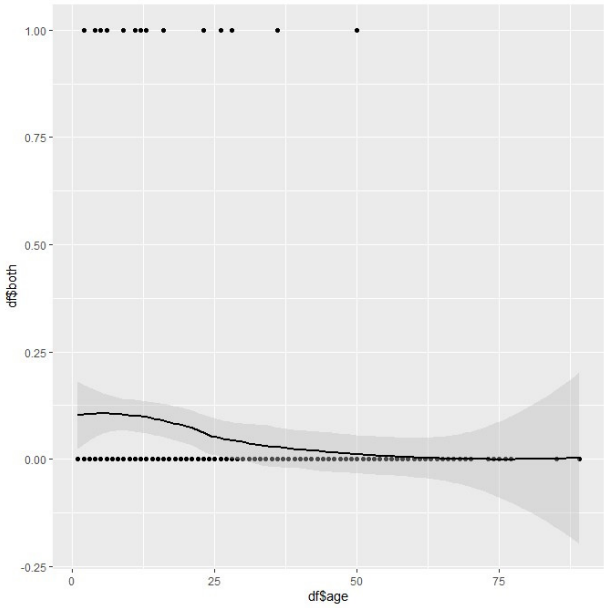
또한 본 연구의 실무적 시사점은 ISMS-P 인증제도의 개선방향을 탐색하였다는 것이다. 연구결과에 따르면 기업규모와 ISMS-P 취득과는 양의 상관관계가 있었으며 업력 및 비 ICT 업종과는 음의 상관관계가 있었다. 이를 통해 정보통신서비스 업종이 아닌 기업 중 규모가 작고 오래된 기업에 대해 ISMS-P 취득을 지원할 필요성을 도출할 수 있었다. ISMS-P 인증을 취득한다는 것은 단순 인증 취득만이 아닌, 해당 조직의 정보보호 및 개인정보보호 관리체계를 도입·유지하는 것을 의미한다. 따라서 그러한 기업에 대해 인증 취득을 넘어 관리체계 도입까지 지원한다면 정보보호 수준이 크게 향상될 것이다. 그리고 한국 내 성공적으로 정착한 ISMS-P 인증제도에 대해 신뢰성 있는 데이터로 분석한 결과를 제시하였기 때문에, 자국 내 정보보호 제도를 신설 및 정착 시키고자 하는 국가에 도움을 줄 수 있을 것이다.

그리고 기업규모가 커질수록, 신생 기업일수록 ISMS 분야 인증에 중복으로 투자할 가능성이 높다. ISMS-P와 ISO/IEC 27001은 각각의 이점이 있지만, 무작정 정보보호 관리체계 인증을 여러 개 취득할 경우 동일한 분야에 대해 예산과 인력을 낭비하는 것이 될 수 있다. 향후 연구에서 ISMS 분야 인증에 중복 투자한 기업들을 대상으로 ISO/IEC 27001을 먼저 취득하였는지, 혹은 ISMS-P 인증을 먼저 취득하였는지 등을 파악해보면 조직 특성에 대하여 보다 더 잘 이해할 수 있을 것이다.

중복 투자를 한 기업들을 대상으로, 어떠한 인증을 먼저 취득하였는지 파악해 볼 필요성은 <그림 4>, <그림 5>를 통해서도 알 수 있었다. 해당 그림들은



〈그림 4〉 독립변수, 종속변수 간 산점도(x축: age, y축: ismsp)



〈그림 5〉 독립변수, 종속변수 간 산점도(x축: age, y축: both)

독립변수 age와 종속변수 ismsp, both 사이의 관계를 산점도와 국소 회귀분석 방식의 추세선으로 나타낸 그래프인데, 특히 ISMS-P 인증과 ISO/IEC 27001을 모두 취득한 케이스의 추세선은 ISMS-P 인증 취득 케이스의 추세선과 유사하였다. ISMS-P 인증 취득 시 ISMS 분야 인증의 중복 취득의 비율이 높아지는 것인지, 또는 중복으로 취득하려다보니 ISMS-P 취득 비율이 높아지는 것인지 확인해보면 의미 있는 결과가 나올 것이다.

Probit 회귀분석을 통해 ISMS-P 인증 취득과 기업 규모와는 양의 상관관계가 있는 것을 알 수 있었는데 이것은 법령에 명시된 것처럼, 규모가 클 경우 인증 의무대상자에 해당될 가능성이 크기 때문인 것으로 보인다. ISMS-P는 병원・학교・정보통신서비스 제공자의 경우 일정 규모 이상일 시 정보보호 관리체계 인증 취득 의무대상자로 분류된다.

ISO/IEC 27001의 경우 Mirtsch *et al.*(2021)과 동일하게 ISO/IEC 27001 취득과 업력, 비 ICT 업종과 음의 상관관계가 있고, 기업규모(총 임직원 수)와는 양의 상관관계가 있는 것으로 드러났다. 이것은 ISO/IEC 27001 취득에 있어서 기업 규모와 업력 및 업종이 미치는 영향이 한국 기업, 독일 기업 모두에게 동일하다는 것을 의미한다. 그리고 정보기술 부문 대비 정보보호 투자액 비중과 양의 상관관계가 있는 것을 보아, 정보통신서비스 업종일수록, 정보보호 투자액 비중이 클수록 ISO/IEC 27001을 취득할 가능성이 높다는 것을 알 수 있었다.

비 ICT 업종과 인증 취득과는 음의 상관관계가 있었다. 2022년 공시된 기업 중 제조업의 비중이 50.72%, 정보통신업 비중은 17.22%로, 제조업(비 ICT 업종)의 비중이 높은 편이다(과학기술정보통신부, 2022). 2022년 정보보호 공시에 대한 업종별 현황을 <표 18>에 요약하였다. 업종은 한국표준산업분류의 대분류를 기준으로 구분하였다.

Mirtsch *et al.*(2021)에서는 전체 기업 데이터셋을 대상으로 분석한 결과 업력과 음의 상관관계가 있었지만, ICT 부문만을 대상으로 분석한 결과 업력과 양의 상관관계가 있었다. 향후 연구에서 업종 데이터를 보다 상세히 수집 및 분석하여 특정 업종과 양의 상관관계가 있는지 확인해볼 필요가 있다.

〈표 18〉 2022년 정보보호 공시제도 업종별 현황(과학기술정보통신부, 2022)

업종(대분류)	사례 수	비율(%)
건설업	32	5.10
광업	2	0.32
교육 서비스업	4	0.64
금융 및 보험업	13	2.07
농업, 임업 및 어업	3	0.48
도매 및 소매업	60	9.57
보건업 및 사회복지 서비스업	38	6.06
사업시설 관리, 사업 지원 및 임대 서비스업	8	1.28
숙박 및 음식점업	2	0.32
운수 및 창고업	21	3.35
전기, 가스, 증기 및 공기 조절 공급업	8	1.28
전문, 과학 및 기술 서비스업	9	1.44
정보통신업	108	17.22
제조업	318	50.72
협회 및 단체, 수리 및 기타 개인 서비스업	1	0.16
합 계	**627**	**100.00**

6.2 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도의 개선방향

ISMS-P는 한국 기업의 실정에 맞게 개발된 인증이므로, 국내에서 ISMS-P가 좀 더 적극적으로 확산되는 것이 바람직하다. 분석결과에 따르면 인증 취득이 기업규모, 업력, 업종과 관련이 있었다. 따라서 정보통신서비스 업종에 속하지 않은 기업 중 규모가 작고 오래된 소기업, 중소기업을 위한 대책 마련이 필요하다. 인증 간소화, 맞춤형 컨설팅 등이 해결방안이 될 수 있다. 이러한 방식으로 ISMS-P 취득률을 개선할 필요가 있으며, 향후 연구에서 상세한 업종에 따라 정보보호 인증 취득률이 달라지는지 확인이 필요하다. 상대적으로 부족한 업종을 찾고 해당 업종을 위한 해결방안을 찾아야 할 것이다. 주로 정보통신 분야의 기업들이 정보보호 관리체계 인증과 정보보호 공시 의무대상에 해당된다.

이 기준을 점차 비 ICT 기업들로 확대해나가면 업종에 따른 정보보호 수준 불균형도 해소될 수 있을 것이다. 또한 2022년 정보보호 공시 분석 보고서에 따르면 제조업 등 일부 업종의 경우 정보보호 활동이 평균에 미치지 못하여 향후 정보보호 최고책임자와 경영진 등 관심과 노력이 필요하다고 하였다(과학기술정보통신부, 2022). 제조업의 경우 정부주도의 스마트 팩토리 확산 사업 선정 시 정보보호 관리체계 인증 취득 또는 정보보호 공시를 의무화하거나 가산점 부여 항목으로 고려해볼 수 있을 것이다.

6.3 정보보호 공시제도 개선방향

데이터 수집과 전처리를 하며 정보보호 공시를 위한 개선점을 찾을 수 있었다. 기업마다 동일한 내용을 다르게 입력한 경우가 많아, 분석을 위한 가공이 필요하였다. 데이터 입력 시 기업들로부터 규격화된 정형 데이터를 입력받도록 개선할 필요가 있다. 그렇게 된다면 향후 데이터 기반 연구 및 정책 개선을 위한 분석 시 도움이 될 것이다. 그리

고 수집한 정보보호 공시 데이터 중 Probit 분석 시 활용하지 못한 독립변수(업종, 지역 등)가 있으므로 추가하여 분석이 필요하다. 이외에 DART 시스템에서 다양한 공시 데이터 수집이 가능하므로 독립변수를 추가 발굴한다면 또 다른 유의미한 결과가 나올 것이다.

참 고 문 헌

[1] 강성민, 장강일, “기업의 IT 투자 평가 효율화를 위한 지표 도출 및 투자관리체계에 관한 사례 연구”, *경영정보학연구*, 제7권, 제1호, 2005, pp. 219-239.

[2] 과학기술정보통신부, 2022 정보보호 공시 현황 분석보고서, 2022.

[3] 구 정보통신망이용촉진및정보보호등에관한 법률(2001. 12. 31. 법률 제6585호로 개정되기 전의 것) 제47조.

[4] 구 전자정부 정보보호관리체계 인증지침(2014. 4. 16. 안전행정부훈령 제39호로 폐지).

[5] 구 정보통신망이용촉진및정보보호등에관한 법률(2004. 12. 30. 법률 제7262호로 개정되기 전의 것) 제46조의3.

[6] 구 정보통신망이용촉진및정보보호등에관한 법률(2013. 3. 23. 법률 제11690호로 개정되기 전의 것) 제47조의3.

[7] 구 정보통신망이용촉진및정보보호등에관한 법률(2013. 3. 23. 법률 제11690호로 개정되기 전의 것) 제47조.

[8] 구 개인정보 보호 인증제 운영에 관한 규정(2021. 8. 30. 행정안전부고시 제2021-72호로 폐지).

[9] 구 개인정보보호 관리체계 인증 등에 관한 고시(2021. 8. 30. 행정안전부고시 제2021-72호 폐지).

[10] 구 정보통신망이용촉진및정보보호등에관한 법률(2016. 3. 22. 법률 제14080호로 개정되기 전의 것) 제47조.

[11] 구 정보보호산업의 진흥에 관한 법률(2023. 4. 18. 법률 제19351호로 개정되기 전의 것).

[12] 구 정보보호산업의 진흥에 관한 법률 시행령(2022. 3. 8. 대통령령 제32528호로 개정되기 전의 것).

[13] 구 (과학기술정보통신부) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(2018. 11. 7. 고시 제2020-37호로 개정되기 전의 것).

[14] 김동현, 이윤호, “보안 7대 위협을 이용한 ISMS-P 인증효과에 관한 연구: 기업규모와 경력 중심으로”, *한국정보기술학회논문지*, 제18권, 제4호, 2020, pp. 109-119.

[15] 김양훈, 나영섭, 장항배, “소규모 IT 서비스 기업 비즈니스 특성을 고려한 보안 관리모델 실증 연구”, *경영정보학연구*, 제14권, 제3호, 2012, pp. 131-141.

[16] 김원, 조용연, 강승찬, “정보보호 및 개인정보보호 관리체계의 인증 의무대상자 확대 방안 연구”, *차세대융합기술학회논문지*, 제6권, 제8호, 2022, pp. 1353-1364.

[17] 김정완, “공공부문 ’G-ISMS’ 인증 본격 개시!”, 보안뉴스, 2010년 7월 19일자, Available at https://www.boannews.com/media/view.asp?idx=22031, 2023년 7월 25일 접속.

[18] 다래나무주식회사, *해외보안인증제도 연구조사*, 한국인터넷진흥원, 2020.

[19] 박혁규, 강완석, 신광성, “정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 제도에서 중소기업 기반 평가항목 도출에 관한 연구”, *한국정보통신학회 종합학술대회 논문집*, 제25권, 제2호, 2021, pp. 578-579.

[20] 신용녀, “하이퍼 스케일 클라우드에 적합한 정보보호 및 개인정보보호 관리체계 인증 통제항목 연구”, *한국인터넷방송통신학회논문지*, 제23권, 제3호, 2023, pp. 19-26.

[21] 원병철, “ISMS-P 통합인증 본격 시행 1년, 개인정보보호수준↑ 인증비용↓”, 보안뉴스, 2020년 5월 7일자, Available at https://www.boannews.com/media/view.asp?idx=88037, 2023년 7월 29일

접속.

[22] 장상수, *정보보호 및 개인정보보호 관리체계 개론*, 생능출판사, 2020, pp. 31-37.

[23] 임정현, 김태성, "침해사고 통계 기반 정보보호 투자 포트폴리오 최적화 유전자 알고리즘 접근법", *경영정보학연구*, 제22권, 제2호, 2020, pp. 201-217.

[24] 한국인터넷진흥원, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내서. 2021.

[25] 한국인터넷진흥원 전자서명인증관리센터, "5월 7일, '방송통신융합 환경에서 기업정보보호 전략 세미나' 열려", 2009.05.05., Available at https://www.rootca.or.kr/kor/notice/dataView.jsp?p_No=8&b_No=8&d_No=313, 2023년 7월 25일 접속.

[26] 한국인터넷진흥원 정보보호 공시 종합 포털, "제도안내", Available at https://isds.kisa.or.kr/kr/subPage.do?menuNo=204924, 2023년 5월 7일 접속.

[27] 한국인터넷진흥원, GDPR 대응지원 센터, Available at https://gdpr.kisa.or.kr/index.do, 2023년 6월 11일 접속.

[28] 한국인터넷진흥원, 인증서 발급현황, Available at https://isms.kisa.or.kr/main/ispims/issue/, 2023년 6월 24일 접속.

[29] Alshitri, K. I. and A. N. Abanumy, "Exploring the reasons behind the low ISO 27001 adoption in public organizations in Saudi Arabia", *2014 International Conference on Information Science & Applications*, 2014, p. 1.

[30] Bartnes Line, M., I. Anne Tøndel, and M. G. Jaatun, "Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 12-26, 2016.

[31] BSI, "ISO/IEC 27001 International Information Security Standard published," 2005.11.02. Available at https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/, 2023년 5월 7일 접속.

[32] BSI, "ISO/IEC 27001 International Information Security Standard published", 2005.11.02., Available at https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/, 2023년 6월 24일 접속.

[33] BSI, "The new ISO/IEC 27001:2022 standard", Available at https://www.bsigroup.com/en-us/iso27001/revision/, 2023년 6월 24일 접속.

[34] Bundesamt für Sicherheit in der Informationstechnik, "ISO 27001 Zertifizierung auf Basis von IT-Grundschutz", Available at https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html, 2023년 6월 11일 접속.

[35] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Compendium, 2022.

[36] Bundesamt für Sicherheit in der Informationstechnik, "Was sind Kritische Infrastrukturen?", Available at https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html, 2023년 6월 11일 접속.

[37] CDC, "Health Insurance Portability and Accountability Act of 1996 (HIPAA)", Available at https://www.cdc.gov/phlp/publications/topic/hipaa.html, 2023년 6월 11일 접속.

[38] Chang, H., "Is ISMS for financial organizations effective on their business?", *Mathematical and Computer Modelling*, Vol.58, No.1-2, 2013, pp. 79-84.

[39] Chen, J., J. Zhang, R. Qian, J. Yuan, and Y. Ren, “An anomaly detection method for wireless sensor networks based on the improved isolation forest”, *Applied Sciences*, Vol.13, No.2, 2023, p. 702.

[40] ENISA, Supporting the implementation of Union policy and law regarding cybersecurity, Available at https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new, 2023년 6월 11일 접속.

[41] European Commission, “Directive on measures for a high common level of cybersecurity across the Union(NIS2 Directive)”, Available at https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, 2023년 6월 11일 접속.

[42] GOV.UK, “Government mandates new cyber security standard for suppliers”, 2014.09.26., Available at https://www.gov.uk/government/news/government-mandates-new-cyber-security-standard-for-suppliers, 2023년 6월 11일 접속.

[43] GOV.UK., “Cyber Essentials scheme: Overview”, Available at https://www.gov.uk/government/publications/cyber-essentials-scheme-overview, 2023년 6월 11일 접속.

[44] HHS, “Health Information Privacy”, Available at https://www.hhs.gov/hipaa, 2023년 6월 11일 접속.

[45] Hsu, C. W., “Frame misalignment: Interpreting the implementation of information systems security certification in an organization”, *European Journal of Information Systems*, Vol.18, No.2, 2009, pp. 140-150.

[46] ISO, ISO/IEC 27001:2013, Available at https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, 2023년 5월 7일 접속.

[47] ISO, ISO Survey 2021 results - Number of certificates and sites per country and the number of sector overall, Available at https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top, 2023년 5월 7일 접속.

[48] ISO, “ISO/IEC 27001”, Available at https://www.iso.org/standard/27001, 2023년 5월 7일 접속.

[49] Leśniak, A., M. Juszczyk, and G. Piskorz, “Modelling delays in bridge construction projects based on the logit and probit regression”, *Archives of Civil Engineering*, Vol.65, No.2, 2019, pp. 107-120.

[50] Longras, A., T. Pereira, P. Carneiro, and P. Pinto, “On the track of ISO/IEC 27001:2013 implementation difficulties in Portuguese organizations”, *2018 International Conference on Intelligent Systems*, 2018, pp. 886-890.

[51] Mirtsch, M., K. Blind, C. Koch, and G. Dudek, “Information security management in ICT and non-ICT sector companies: A preventive innovation perspective”, *Computers & Security*, Vol.109, 2021, p. 102383.

[52] Mirtsch, M., J. Kinne, and K. Blind, “Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis”, *IEEE Transactions on Engineering Management*, Vol.68, No.1, 2021, pp. 87-100.

[53] NCSC, IASME, Cyber Essentials Self-Assessment Preparation Booklet, 2022.

[54] Ngenoh, E., B. K. Kurgat, H. K. Bett, S. W. Kebede, and W. Bokelmann, “Determinants of the competitiveness of smallholder African indigenous vegetable farmers in high-value agro-food chains in Kenya: A multivariate probit regression analysis”, *Agricultural and Food Economics*, Vol.7, No.1, 2019, pp. 1-17.

[55] Nikita, E. and P. Nikitas, “Sex estimation: A comparison of techniques based on binary logistic, probit and cumulative probit regression, linear and quadratic discriminant analysis, neural networks, and naive Bayes classification using ordinal varia-

bles", *International Journal of Legal Medicine*, Vol.134, No.3, 2020, pp. 1213-1225.

[56] NIST Special Publication 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations, September, 2020.

[57] O'Brien, R. M., "A caution regarding rules of thumb for variance inflation factors", *Quality & Quantity*, Vol.41, No.3, 2007, pp. 673-690.

[58] Roberts, J., G. Popli, and R. J. Harris, "Do environmental concerns affect commuting choices?: Hybrid choice modelling with household survey data", *Journal of the Royal Statistical Society. Series A, Statistics in Society*, Vol.181, No.1, 2018, pp. 299-320.

[59] Siponen, M. and R. Willison, "Information security management standards: Problems and solutions", *Information & Management*, Vol.46, No.5, 2009, pp. 267-270.

[60] Sun, J. and S. Lyu, "The effect of medical insurance on catastrophic health expenditure: Evidence from China", *Cost Effectiveness and Resource Allocation*, Vol.18, No.1, 2020, pp. 10-10.

[61] Van Wessel, R. and H. J. de Vries, "Business impact of international standards for information security management. Lessons from case companies", *Journal of ICT Standardization*, Vol.1, 2013, pp. 25-40.

[62] Zhang, Y. and J. Ye, "Risk preference of top management team and the failure of technological innovation in firms-based on principal component analysis and probit regression", *Journal of Intelligent & Fuzzy Systems*, Vol.40, No.1, 2021, pp. 1161-1173.

[63] Zhao, Y., B. Lehman, R. Ball, J. Mosesian, and J. de Palma, "Outlier detection rules for fault detection in solar photovoltaic arrays", *2013 Twenty-Eighth Annual IEEE Applied Power Electronics Conference and Exposition*, 2013, pp. 2913-2920.

Information Systems Review
Volume 25 Number 4
November 2023

Analysis on ISMS Certification and Organizational Characteristics based on Information Security Disclosure Data

SunJoo Kim* · Tae-Sung Kim**

Abstract

The Information Security Management System (ISMS) is a protection procedure and process that keeps information assets confidential, flawless, and available at any time. ISMS-P in Korea and ISO/IEC 27001 overseas are the most representative ISMS certification systems.

In this paper, in order to understand the relationship between ISMS certification and organizational characteristics, data were collected from Korea Internet & Security Agency (KISA), Ministry of Science and ICT, Information Security Disclosure System (ISDS), Financial Supervisory Service, Data Analysis, Retrieval and Transfer System (DART), and probit regression analysis was performed.

In the probit analysis, the relationship with four independent variables was confirmed for three cases: ISMS-P acquisition, ISO/IEC 27001 acquisition, and both ISMS-P and ISO/IEC 27001 acquisition. As a result of the analysis, it was found that companies that acquired both ISMS-P and ISO/IEC 27001 had a positive correlation with the total number of employees and a negative correlation with business history. In addition, the improvement direction of the ISMS-P certification system and information security disclosure system could also be confirmed.

Keywords: Information Security Management System, ISMS, ISMS-P, ISO/IEC 27001, Organizational Characteristics

* Master's Course, Department of Convergence Security, Chungbuk National University
** Corresponding Author, Professor, Department of MIS; and Director, Cybersecurity Economics Research Institute, Chungbuk National University

◐ 저 자 소 개 ◑

김 선 주 (sunj@chungbuk.ac.kr)

충북대학교 융합보안협동과정에서 석사과정 재학 중이다. 현재 공공기관에서 정보보호, 개인정보보호, 시스템 운영 관련 업무를 하고 있고, 주요 관심 분야는 조직 특성과 정보보호 수준이다.

김 태 성 (kimts@cbnu.ac.kr)

KAIST 산업경영학과에서 박사를 취득하고, 한국전자통신연구원에서 선임연구원으로 근무한 후, 현재 충북대학교 경영정보학과에서 정교수, 보안경제연구소장, 보안컨설팅연계전공 및 대학원 융합보안전공 주임교수로 재직하고 있다. 국가정보원 보안관리실태평가 자문 및 평가위원, 행정안전부 전자정부 민관협력포럼 자문위원, 국방부 사이버보안 자문위원, 병무청 정책자문위원, 한국전력 정보보안 자문위원, 한국지역정보개발원 선임이사, ISMS-P 인증위원회 위원, 정보보호산업 분쟁조정위원회 위원, 금융감독원 데이터분야 외부평가위원으로 활동하고 있으며, 주요 관심분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.

논문접수일 : 2023년 08월 06일 **게재확정일 : 2023년 10월 06일**