디지털산업정보학회 논문지 제20권 제1호 - 2024년 3월
http://dx.doi.org/10.17662/ksdim.2024.20.1.119

디지털 전환(DX) 시대에 기업의 정보보안 투자 수준에 따른 운영성과에 관한 연구*

정 병 호** · 주 형 근***

A Study on the Operational Performance by the Investment Level of Companies Information Security in the Digital Transformation(DX) Era

Jung Byoungho · Joo Hyungkun

〈Abstract〉

The purpose of this study is to examine the operational performances by the investment level of information security in companies. The theoretical background summarized the meaning of information security, management information security, and network security. The research process was carried out in four stages.

As a result of the analysis, the level of information security was classified into four groups, and the difference in operational performance was confirmed. According to the categorical regression analysis of the three dependent variables, independent variables such as network threats, non-network threats, executive information security awareness, industry, organizational size, and information security education all affected information security regulations, in-house information security checks, and information security budget investments. The theoretical implications of this study have contributed to updating the latest information security theory. Practical implications are that rational investments should be made on the level of information security of companies.

Key Words : Information Security, Confidential Information, Information Security Investment, Administrative Security, Information Security Competence

Ⅰ. 서론

전 세계는 디지털 전환 시대를 맞이하면서 인공지능과 로봇 기술이 보편화되었고, 기업들의 빅데이터 수집과 활용도 계속 증가하고 있다. 기업들은 디지털 전환 시대에 데이터과학, 인공지능 등 다양한 디지털 기술을 활용하여 기존 산업의 구조를 변화시키거나 고도화하는 등의 새로운 전환과정을 맞이하고 있다[1]. 기업들은 인공지능 기술을 활용하여 기업의 생산성을 강화하고 있으며 빅데이터 수집을 통해서 인공지능을 학습시켜 기업의 생산성에 도움을 받고 있다[2]. 인공지능과 빅데이터는 경

* 본 연구는 한성대학교 교내학술연구비 지원과제임
** 한성대학교 지식서비스&컨설팅대학원 초빙교수 (주저자)
*** 한성대학교 지식서비스&컨설팅대학원 교수 (교신저자)

제, 의료, 행정, 예술 등 전 분야에서 추천 시스템으로 고객 맞춤형 서비스를 제공하고, 행정업무의 간소화 서비스, 고객 행동을 사전에 예측하는 등의 가치를 제공하고 있다[2, 3]. 이처럼 빅데이터와 인공지능은 사회문화, 경제적으로 부가가치를 창출해주는 역할을 하고 있다.

하지만, 기업들의 인공지능과 빅데이터가 활용이 강조되고 있는 반면에 정보기술의 활용 숙련도와 기밀정보를 매우 잘 보호해야 하는 책임감도 뒤따르게 된다[4]. 빅데이터는 기업의 경쟁력뿐만 아니라 국가 경제에도 영향을 제공한다. 최근 대기업들은 기밀 빅데이터가 협력회사를 통한 침해사고로 발생하고 있으며 22년부터 5배 증가했다는 통계 발표도 있다. 중소기업의 사이버 보안 취약 문제로 대기업 기밀정보 유출이 발생하였고, 협력사를 통해서 대기업 서버를 해킹하거나 메일 탈취 등의 기밀정보를 확보했다고 한다[5]. 또한 방사청의 전투기 군사 기밀을 USB에 저장하여 유출하는 사건이 발생하는 등의 정보보안 사고는 지속해서 발생하고 있다[6]. 이렇듯 기업의 정보보호의 중요성은 꾸준히 강조되고 있지만, 최근까지도 고객들의 개인정보 누출, 반도체 기술 누출, 국방 기술 누출, 배터리 기술 유출 등은 계속 발생하고 있다[7, 8].

이에 본 연구는 기업들의 정보보안 투자 수준을 강화해주는 중요 요인이 무엇인지 살펴보는 데 있다. 정보보안의 운영 수준과 정보보안의 규정, 정보보안 점검, 정보보안 예산을 강화하는 요인이 무엇인지 분석할 것이다.

Ⅱ. 이론적 배경

2.1 정보보안의 의미와 인식 수준

정보보안은 기업에서 중요시하는 기밀정보를 보호하기 위한 장치이자 특정 목적에 사용 및 분석되는 정보를 보호하는 것을 말한다[4]. 기업은 기밀정보를 보호하기 위해서 기밀성, 무결성, 가용성으로 정보 접근의 권한과 통제를 강화하고 있으며 데이터의 안전을 보장하고 있다[9]. 최근 기업 내 인공지능의 활용과 비대면 정보 접근이 증가하면서 정보보안 인식의 중요성이 더욱 강조되고 있다. 이러한 정보기술의 발달로 기업의 정보보안 인식은 지속해서 중요해졌다. 이에 조직 내 구성원은 기밀 데이터의 정보 보안성을 인지해야 한다[10]. 정보보안의 인식은 기업의 정보보안 규칙 수준을 의미하며, 정보보안 준수 행동과도 관련되어 있다. 정보보안 인식은 개인의 정보보안 행동에 직접적인 영향을 주는 요인이라고 할 수 있다[11].

2.2 관리적 정보보안 활동과 보안 준수

기업의 정보보안 활동은 기술적 보안과 함께 관리적, 물리적 보안 활동을 포함한다[12]. 이중 관리적 보안은 무형 자산의 개념으로서 보안 정책과 제도, 보안조직, 인사 보안, 정보보호 교육, 보안 교육훈련, 복구절차 등을 포함하고 있다. 관리적 보안은 데이터 보호를 위한 기술적인 방법뿐만 아니라 종합적이며 체계적으로 정책 및 관리, 지침을 구성하게 하여 기업의 기밀 데이터 보호를 강화해준다[13].

관리적 보안은 기업의 정보보안의 중요한 통제 요소로서 기술 보안과 물리 보안을 더욱 강화할 수 있는 요인으로 중요하다[14]. 관리적 보안은 기업 거버넌스 차원에서 보안 활동의 효율성과 효과성을 제공하며, 기밀정보가 사전에 누출되는 위협을 파악해주고, 조직 내 구성원들이 자발적으로 기밀정보를 보호하고 관리하는 의지를 강화해준다[15].

한편, 관리적 보안에서도 정보보안 정책은 조직의 정보와 기술 자원을 보호하기 위한 조직구성원의 역할과 책임을 명시해 놓은 것이다[10]. 이에 기업의 정보보안 정책은 우선 조직구성원이 쉽게 이해하고 정책을 실행하는데 혼선이 없도록 행동 지침이 구체적이고 명확해야 한다[16]. 또한 정보보안 교육훈련도 정보보호의 인식 강

화하는 데 도움을 제공한다. 정보보안 교육은 조직의 기밀정보에 대한 인식과 관리 책임 의식을 높이고, 기밀정보를 이용하는 데 필요한 권한과 사용에 대한 인식을 강화하는 활동을 말한다[17]. 정보보안 교육은 조직구성원이 기밀정보를 보호하지 않는 미준수 행동을 변화시킬 수 있으며 심리적 관점에서 정보보안 준수가 조직 데이터 관리에 긍정적 효과를 높이는데 기여할 수 있다[18]. 즉, 조직이 보호하려는 빅데이터에 대해서 발생 가능한 위협을 파악하고, 개인 스스로 데이터를 보호하고 관리하려는 의지로 정의할 수 있다[10].

2.3 네트워크 보안

네트워크 보안은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 조작, 유출, 무단침입 등의 불법 행위로부터 기밀정보를 보호하는 것을 의미한다[19]. 컴퓨터 네트워크는 각종 프로토콜이나 네트워크로 연결된 수많은 호스트 사이로 정보가 교류시킨다. 이 과정에서 정보의 유출과 불법적인 사용이 발생할 수 있으며 이를 보호하는 것이 네트워크 보안의 목적이 된다[20]. 즉, 네트워크 보안은 네트워크 경계에서 침입자로부터 데이터를 보호하는 것이다. 네트워크 보안은 외부의 공격과 데이터 유출로부터 내부의 네트워크를 보호하는 임무를 수행하는 것이 최우선이다[21].

네트워크 환경에서 발생할 수 있는 보안 위협으로는 장치의 절도, 장치 분실, Rogue AP, IP 스푸핑, 디도스 공격, 트로이목마, 웜, 바이러스, 신호 방해 공격, 배터리 소진 공격 등이 있다[22]. 네트워크 보안은 침입자가 네트워크 액세스 권한을 확보하여 공격에 성공하는 것을 네트워크에 보호 전문 소프트웨어와 하드웨어로 활용하여 침입을 방지시켜준다. 네트워크 보안 도구는 인프라 파괴, 운영 지연, 리소스 악용, 민감 데이터의 손상을 의도하는 모든 침입자를 탐지하여 데이터를 보호한다[19].

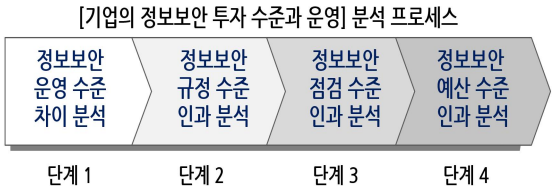
이처럼 네트워크 보안의 목적은 비인가의 침입으로 정보가 외부로 유출되지 않도록 하기 위해서이며[23], 보안 데이터가 전달되는 네트워크 경로에서 데이터를 불법적으로 훔쳐내 악용하는 것을 방지하기 위해서 중요하다[9]. 그리고 외부 침입자가 기밀 데이터의 내용을 위조와 변조하지 않도록 보호하기 위해서다[21].

Ⅲ. 연구방법론

3.1 연구 프로세스

본 연구는 기업 정보보안의 수준을 파악하고, 정보보안의 역량을 높이는데 중요한 변수가 무엇인지 확인할 것이다. 2022년은 포스트 코로나19로 접어들면서 기업들이 인공지능과 로봇 기술에 대해 대대적으로 투자 및 개발하는 시기였고, 디지털 전환 시대로 세계적으로 모든 기업이 새로운 정보기술에 투자가 활발한 시기였다[1]. 즉, 빅데이터와 인공지능이 기업 핵심 경쟁력으로 중요 자산으로 자리매김하고 있는 상황에서 기업들의 정보보안 중요성을 강조하는 연구가 되겠다.

이에 본 연구는 총 4단계의 분석 프로세스를 진행하여 기업의 정보보안 투자 수준과 운영성과를 확인할 것이다. 연구 프로세스는 <그림 1>에 제시하였다.



〈그림 1〉 연구 프로세스

첫 번째 단계에서는 기업의 정보보안 수준을 구분하여, 정보보안의 운영성과 차이가 있는지를 확인할 것이다. 정보보안 운영성과는 정보보안 규정 제정, 사내 정보보안 점검, 정보보안 예산투자 등으로 구성하였다.

· 연구단계 1 : 정보보안 수준별로 정보보안 성과 차이를 보이고 있는가?

연구단계 1에서는 정보보안 수준별로 정보보안 운영성과를 분석하기 위해서 비 계층적 군집분석과 함께 분산분석을 활용하여 연구단계 1을 검정할 것이다. 그리고 다음 연구단계 2~4 에서는 연구단계 1에서 분석한 세 가지 정보보안 운영성과를 높이기 위한 중요 독립변수가 무엇인지 범주형 회귀 분석을 통해서 확인하고자 한다. 연구단계 2에서는 정보보안 규정 제정에 중요 독립변수를 탐색하고, 연구단계 3에서는 사내 정보보안 점검에 중요 독립변수가 무엇인지 탐색할 것이다. 마지막 연구단계 4에서는 예산투자 수준에 중요 독립변수가 무엇인지 탐색할 것이다.

· 연구단계 2~4 : 정보보안 규정 제정, 사내 정보보안점검, 정보보안 예산투자에 영향을 제공하는 중요 변수는 무엇인가?

연구단계 2~4에서는 정보보안 운영성과의 영향을 미치는 중요 변수를 탐색하고 또한 산업별로 운영성과에 대한 차이가 있는지도 살펴볼 것이다.

이러한 분석 프로세스를 위해서 본 연구에서 사용할 분석 데이터는 2022년도 과학기술정보통신부와 한국정보보호산업협회에서 조사한 '2022년 정보보호 실태조사(기업)'을 활용하였다[24]. 설문 조사된 기간은 2022년 9월이었으며 IT 관련 기술이 중요하다고 응답한 기업만을 대상으로 분석에서 사용하였다. 분석에 사용된 총 데이터 수는 4,331개 데이터이다.

〈표 1〉 구성요인별 측정항목

변수명		아이템명		척도	참고문헌
독립변수	네트워크 보안 위협	IA1	인터넷을 통해 사내 전산 시스템 침해사고 위협	구간	[19, 20, 21, 22 ,23, 24]
		IA2	시스템 및 네트워크 장애로 인한 서비스 마비 위협	구간	
		IA3	시스템 및 네트워크 침입을 통한 해킹의 위협	구간	
	비 네트워크 보안 위협	IB1	인적 요인에 의한 정보 유출 위협	구간	[10, 12, 13, 15, 24, 26]
		IB2	불법적인 사내 침입 등에 의한 물리적 위협	구간	
		IB3	사내에 가이드, 규정 등의 미비로 인한 우려	구간	
	임원진 정보보안 인식	귀사의 임원들은 정보보호에 대해 얼마나 중요하게 생각하는가?		구간	
	업종(산업)	산업(업종) : 농림수산업 ~ 협회/단체업 (총 16개 항목)		명목	
	조직규모	조직규모 (총 5개 항목)		명목	
	정보보안 교육	2021년 1월 이후 임직원 대상으로 정보보호 교육 ① 예 ② 아니오		명목	
종속변수	정보보안 규정 제정	귀사에 정보보호 관련 규정이 제정, 변경 또는 강화되었을 시, 귀사의 조직구성원에게 엄격하게 적용하고 있는가?		구간	[4, 12, 13, 15, 24, 26]
	사내 정보보안 점검	귀사에서는 최근 사내 IT 시스템 및 네트워크에 대해 보안점검을 언제 실시하였는가? ① 실시하지 않음 ② 1개월 미만 ③ 1개월~6개월 미만 ④ 6개월 ~ 1년 미만 ⑤ 1년 ~ 2년 미만 ⑥ 2년 이상		명목	
	정보보안 예산투자	귀사의 정보보호 관련 예산 소비는 적절하다고 생각하십니까?		구간	
집단변수	정보보안 정책	공식 문서로 작성된 사내 정보보호 정책 또는 규정집이 있는가?		명목	[12, 13, 15, 24]
	정보보안 운영조직	귀사에서 정보보호 조직을 운영하는 방식은 무엇입니까? ① 전담조직 ② 겸임조직 ③ 운영하지 않음		명목	
	정보보안 최고책임자	CISO 책임자 임명 여부 ① 예 ② 아니오		명목	
	정보보안 사전 예방 능력	정보보호 침해사고의 정보보안 사전예방 능력		구간	
	정보보안 중요성	정보보호에 대하여 얼마나 중요하게 생각하는가?		구간	
	정보보안 침해사고 발생 가능성	귀사에서는 정보보호 관련 침해사고가 발생할 가능성이 크다고 생각하십니까?		구간	

3.2 조작적 정의 및 변수 설정

연구 프로세스를 분석하기 위해서 이론적 배경의 관리적 정보보안, 보안 준수, 네트워크 보안 등을 토대로 변수들을 구성하였다. 변수들은 <표 1>에 제시하였다.

연구에서 사용되는 독립변수로는 네트워크 위협요인, 비 네트워크 위협요인, 임원진 정보보안 인식, 정보보안 교육, 업종(산업), 규모 등으로 구성하였다. 종속변수로는 정보보안 규정 제정, 사내 정보보안 점검, 정보보안 예산 투자로 구성하였다. 집단변수는 정보보안 정책, 정보보안 운영조직, 정보보안 최고책임자, 정보보안 사전 예방 능력, 정보보안 중요성, 정보보안 침해사고 발생 가능성 등으로 구성하였다. 연구 프로세스 분석을 위해서 변수들의 척도는 구간변수, 명목변수 등으로 구성하였다.

Ⅳ. 연구 결과

4.1 표본 특성

본 연구의 표본 특성을 살펴보고자 인구통계학을 분석하였다. 분석 결과, 지역은 서울이 1,826개(42.2%)로 응답 비율이 가장 높게 나타났다. 그다음은 경기로 811(18.7%)로 나타났다. 기업규모는 50-249명이 1,351개(31.2%)로 높게 나타났다. 산업은 전문, 과학, 과학기술서비스업이 544(12.6%)로 높게 나타났고 다음으로 제조업이 504개(11.6%)로 나타났다. 사업 형태는 단독사업체가 2,533개(58.5%)로 나타났고, 조직 형태는 회사법인이 3,663개(84.6%)로 높게 나타났다. 이에 대한 세부적인 분석 결과 내용은 <표 2>에 제시하였다.

〈표 2〉 인구통계학 특성

구분		빈도	비율	구분		빈도	비율
지역	서울	1826	42.2	산업	① 농림수산업	43	1.0
	부산	244	5.6		② 제조업	504	11.6
	대구	79	1.8		③ 전기, 가스업	107	2.5
	인천	167	3.9		④ 건설업	404	9.3
	광주	120	2.8		⑤ 도매 및 소매업	340	7.9
	대전	93	2.1		⑥ 운수 및 창고업	279	6.4
	울산	62	1.4		⑦ 숙박 및 음식점업	123	2.8
	세종	17	0.4		⑧ 정보통신업	371	8.6
	경기	811	18.7		⑨ 금융 및 보험업	348	8.0
	강원	79	1.8		⑩ 부동산업	247	5.7
	충북	101	2.3		⑪ 전문, 과학, 과학기술서비스업	544	12.6
	충남	136	3.1		⑫ 사업시설관리업	447	10.3
	전북	123	2.8		⑬ 교육서비스업	118	2.7
	전남	165	3.8		⑭ 보건 및 사회복지 서비스업	249	5.7
	경북	86	2.0		⑮ 예술, 스포츠, 여가서비스업	112	2.6
	경남	170	3.9		⑯ 협회, 단체, 수리 서비스업	95	2.2
	제주	52	1.2	사업 형태	단독사업체	2533	58.5
조직 규모	10~49명	1184	27.3		본사/본점	1798	41.5
	50~249명	1351	31.2	조직 형태	개인사업체	369	8.5
	250~499명	921	21.3		회사법인	3663	84.6
	500~999명	178	4.1		회사 이외의 법인	194	4.5
	1000명 이상	697	16.1		비법인단체	105	2.4

4.2 신뢰성과 타당성 검정

본 연구에서 독립변수로 활용할 네트워크 위협요인과 비네트워크 위협요인에 대해서 타당성과 신뢰성을 검정하였다. 신뢰성 검정은 Cronbach's a의 값으로 분석하였고, 타당성 검정은 요인분석으로 분석하였다. 요인분석은 주성분 분석 방식으로 배리맥스 회전을 이용하였다[25].

요인분석 결과, KMO와 Bartlett의 검정에서 Kaiser-Meyer-Olkin 측도는 0.892로 나타났고, Bartlett 구형성 검정의 카이제곱은 12315.666으로 나타났고, 유의확률은 0.000으로 나타났다. 그리고 모든 아이템은 0.7 이상의 요인값을 보여주었고, 공통성은 0.6 이상으로 나타났으며, 신뢰성은 0.8 이상으로 나타나 타당성과 신뢰성을 확보하였다. 이에 대한 상세 내용은 <표 3>에 제시하였다.

〈표 3〉 변수의 신뢰성과 타당성

변수명		요인값	공통성	신뢰성
네트워크 보안 위협	IA1	.869	.799	.822
	IA2	.756	.725	
	IA3	.719	.706	
비 네트워크 보안 위협	IB1	.736	.688	.810
	IB2	.872	.805	
	IB3	.720	.701	

4.3 프로세스 1 검정 : 정보보안 운영 수준 차이 분석

다음은 프로세스별로 분석을 진행하였다. 우선 프로세스 1 검정을 위해서 기업들의 정보보안 운영 수준을 집단별로 구분하였다. 이때 집단은 비 계층적 군집분석으로 진행하였다. 비 계층적 군집분석에서는 총 6개의 변수를 기준으로 분석을 진행하였다.

비 계층적 군집분석의 결과를 살펴보면 군집의 모형 분석인 ANOVA에서 정보보안 정책의 F값은 508.771로 나타났고 p값은 0.001로 나타났다. 정보보안 운영조직의 F값은 597.233이며 p값은 0.000으로 나타났다. 정보보안 최고책임자의 F값은 815.335이며 p값은 0.000으로 나타났다. 정보보안 사전 예방 능력의 F값은 304.768이며 p값은 0.001로 나타났다. 기업 정보보안 인식의 F값은 4309.169이며 p값은 0.000으로 나타났다. 정보보안 침해사고 발생 가능성의 F값은 1630.375이었고, p값은 0.000으로 나타났다.

최종 4개의 집단으로 분석된 군집분석의 내용을 살펴보면 군집1은 853개, 군집2는 452개, 군집3은 1,801개, 군집4는 1,225개로 나타났다. 이중 군집3이 정보보안 운영 역량이 가장 높은 것으로 해석되었고, 군집4는 정보보안 운영 역량이 가장 낮은 집단으로 해석되었다. 이에 대한 세부 내용은 <표 4>와 <표 5>에 제시하였다.

군집으로 분류한 4개의 정보보안 수준 집단 차이가 있는지를 살펴보고자 분산분석(ANOVA)을 실시하였다. 분산분석은 정보보안 규정 제정, 사내 정보보안 점검, 정보보안 예산투자 등 3개의 정보보안 수준에 대해서 집단별 차이를 분석하였다. 세부적인 결과 내용은 <표 6>에 제시하였다.

〈표 4〉 정보보안 역량 수준에 대한 군집분석

구분	군집 유형			
	군집1 (n=853)	군집2 (n=452)	군집3 (n=1801)	군집4 (n=1225)
정보보안 정책	1 (보유)	1 (보유)	1 (보유)	2 (미보유)
정보보안 운영 조직	2 (겸임)	2 (겸임)	2 (겸임)	3 (없음)
정보보안 최고 책임자 CISO	2 (없음)	1 (있음)	1 (있음)	2 (없음)
정보보안 사전 예방 능력 (정보보안)	3 (보통)	3 (보통)	4 (높음)	3 (보통)
기업 정보보안 인식	4 (높음)	2 (낮음)	4 (높음)	4 (높음)
정보보안 침해사고 발생 가능성	4 (높음)	3 (보통)	2 (낮음)	3 (보통)

〈표 5〉 군집별 특징 정의

집단 구분		군집 정의
A	군집1 (n=853)	정보보안 정책을 보유하고 있으며 정보보안을 운영하는 겸직조직이 있음. 기업의 정보보안 인식은 높지만, 정보보안 관리책임자는 없고 정보보안 침해사고 발생 가능성이 큰 집단임
B	군집2 (n=452)	정보보안 정책을 보유하고 있으며 정보보안을 운영하는 겸직조직이 있음. 기업의 정보보안 인식은 낮지만, 정보보안 관리책임자가 있으며 정보보안 침해사고 발생 가능성이 준수한 수준을 보유한 집단임
C	군집3 (n=1801)	정보보안 정책을 보유하고 있으며 정보보안을 운영하는 겸직조직이 있음. 정보관리책임자가 있으며 정보보안 인식과 정보보안 사전 예방이 높고 침해사고 발생 가능성도 낮은 집단임
D	군집4 (n=1225)	정보보안 정책을 미보유하고 있으며 정보보안을 운영하는 조직과 정보관리책임자가 없음. 정보보안 침해사고 발생 가능성이 준수한 수준을 보유한 집단임

분산분석은 총 3가지로 분석하였다. 첫 번째는 정보보안 규정 제정에 대한 집단 간 차이를 분석하였다. F값은 84.575로 나타났으며, p값은 0.001로 나타나 집단 간의 차이가 있다고 나타났다. C 집단이 3.94로 다른 집단에 비해 정보보안 규정에 대해 높은 수치를 보여주었다. 그리고 D 집단은 3.54로 나타나 다른 집단에 비해 낮은 정보보안 규정을 제정하는 것으로 나타났다. LSD 사후검정 방법을 사용하여 세부적으로 차이를 살펴보면 A와 B 집단은 동질 하다고 나타났고, C와 D 집단은 차이가 있다고 나타났다. 두 번째는 사내 정보보안 점검을 분석하였다. F값은 48.589로 나타났고 p값은 0.001로 나타나 집단 간 차이가 있다고 나타났다. 사내 정보보안 점검은 점수가 낮을수록 보안점검을 다른 집단에 비해 더 많이 실시하는 것으로 해석할 수 있다. 분석에서는 C 집단이 3.13으로 나타나 사내 정보보안 점검을 다른 집단이 비해 자주 하는 것으로 나타났고 D 집단이 3.58로 다른 집단보다 정보보안 점검이 빈도수가 낮은 것으로 나타났다. LSD 사후검정 방법을 살펴보면 네 개의 집단 모두 차이가 있다고 나타났다. 마지막은 정보보안 예산투자에 대한 집단 간 차이를 분석하였다. F값은 109.322로 나타났고, p값은 0.001로 나타나 집단 간 차이가 있다고 나타났으며 C 집단이 3.77로 가장 높은 예산투자를 보여주고 있다. LSD 사후검정 방법을 살펴보면 네 개의 집단 중 A와 B 집단은 동질 하다고 나타났고, C 집단과 A, B 집단은 차이가 있다고 나타났다. 그리고 D 집단은 C 집단과 A, B 집단과 차이가 있다고 나타났다.

〈표 6〉 정보보안 수준에 대한 집단별 차이 검정

종속변수	집단	N	평균	표준편차
정보보안 규정 제정	A 집단	853	3.72	.773
	B 집단	452	3.77	.652
	C 집단	1801	3.94	.569
	D 집단	1225	3.54	.777
	F	84.575		
	유의확률	0.001		
	사후검정	C > A=B > D		
사내 정보보안 점검	A 집단	853	3.49	1.17
	B 집단	452	3.29	1.04
	C 집단	1801	3.13	1.03
	D 집단	1225	3.58	1.15
	F	48.589		
	유의확률	0.001		
	사후검정	C > B > A > D		
정보보안 예산투자	A 집단	853	3.48	.683
	B 집단	452	3.56	.695
	C 집단	1801	3.77	.754
	D 집단	1225	3.32	.567
	F	109.322		
	유의확률	0.001		
	사후검정	C > A=B > D		

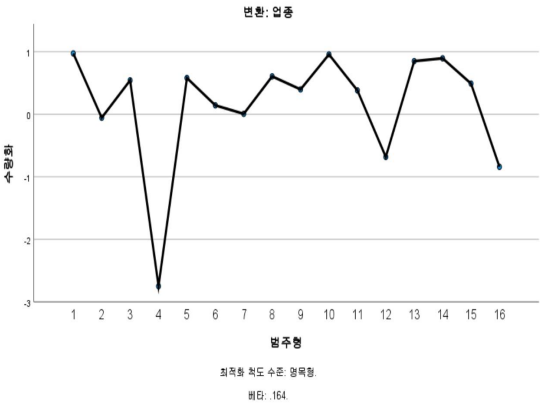
4.4 프로세스 2 검정 : 정보보안 규정 수준 인과 분석

다음 프로세스 2 검정으로서 기업들의 보안규정 제정을 위한 중요 독립변수가 무엇인지 확인하고자 범주형 회귀 분석을 진행하였다. 독립변수는 네트워크 보안 위협, 비 네트워크 보안 위협, 임원진 정보보안, 산업, 조직규모, 정보보안 교육으로 설정하였다. 회귀 분석 결과를 살펴보면, 분석 모형의 설명력은 27.1%이며 F값은 71.073(p=0.000)으로 나타났다. 분석 모형에서 모든 독립변수는 정보보안 규정을 제정하는데 긍정적 영향을 제공하는 것으로 나타났다. 특히 임원진의 정보보안 인식이 정보보안 규정을 제정하는 데 제일 중요한 변수로 나타났으며 다음으로 업종(산업)이 정보보안 규정 제정에 긍정적 영향을 제공한다고 나타났다. 그리고 네트워크와 비 네트워크의 보안 위협도 위협이 높아질수록 정보보안 규정을 제정하는데 긍정적 영향을 제공하는 것으로 나타났다. 조직규모와 정보보안 교육도 정보보안 규정을 제정하는데 긍정적 영향을 제공하는 것으로 나타났다.

〈표 7〉 정보보안 규정 제정 – 범주형 회귀 분석 결과

독립변수	B	표준 오차	F	유의 확률	중요도
네트워크 위협	.065	.018	12.905	.001	.055
비 네트워크 위협	.043	.017	6.122	.013	.026
임원진 정보보안	.408	.016	675.698	.000	.706
업종(산업)	.164	.016	103.212	.000	.132
조직규모	.098	.014	52.764	.000	.047
정보보안 교육	.043	.016	7.644	.006	.034
R^2=0.275, 수정된 R^2=0.271, F=71.073(p=0.000)					

이에 대한 세부 내용은 <표 7>과 <그림 2>에 제시하였다. 특히 업종(산업)에 대해서 세부적으로 살펴보면 다수의 산업이 0 이상의 양적인 수량값을 보이고 있다. 하지만 4번인 건설업, 12번인 사업시설관리업, 16번인 협회 및 단체업은 다른 산업에 비해 정보보안 규정 제정이 미흡한 것으로 나타났다. 특히 2021년 데이터로 분석한 연구와 비교해 보면, 2021년 결과에서는 건설업, 협회 및 단체업이 다른 산업에 비해 정보보안 규정 제정을 강하게 한다고 나타났으나[26] 2022년 데이터로 분석된 결과에서는 반대의 결과를 보여주었다. 또한 다른 산업군도 마찬가지로 2021년 데이터에서는 음의 수량화에 있었으나 2022년 데이터에서는 양의 수량화를 보여주었다. 즉, 2021년 결과와 2022년 결과가 정반대되는 모습을 보여주고 있다. 산업 비교에서 고찰해보았을 때 2021년에 정보보안 규정 제정이 미흡한 산업들이 정보보안 규정을 강화하는데 건설업, 협회 및 단체업 등보다 노력한 것으로 판단된다.



〈그림 2〉 정보보안 규정 제정 - 산업별 현황

4.5 프로세스 3 검정 : 정보보안 점검 수준 인과 분석

다음 프로세스 3 검정에서는 기업들이 사내 정보보안

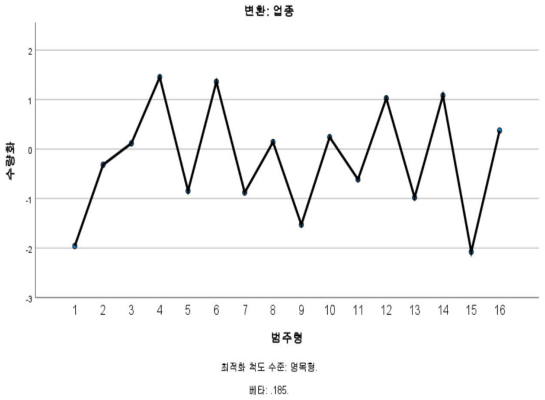
점검에서 어떤 독립변수가 강력한 영향을 제공하는지 범주형 회귀 분석을 진행하였다. 분석 결과를 살펴보면, 분석 모형의 설명력은 14.0%이며 F값은 31.545 (p=0.000)으로 나타났다. 분석 모형에서 모든 독립변수는 사내 정보보안 점검에 영향을 제공하는 것으로 나타났다. 이중 네트워크 보안 위협과 임원진 정보보안은 음의 효과를 보여주고 있다. 이는 네트워크 보안 위협이 감소되고, 임원진의 정보보안 인식이 감소될 때 기업들은 위기의식을 가지고 정보보안 점검을 더 집중해야 하는 것으로 해석할 수 있겠다. 반대로 비 네트워크 보안 위협은 정의 효과로 나타나 인적 요인에 의한 정보 유출, 물리적 위협, 사내 정보 가이드, 규정이 미흡할 때 사내 보안점검을 더 자주 해야 하는 것으로 볼 수 있다.

본 분석 모형에서는 조직규모, 업종(산업)이 사내 정보보안 점검에 가장 높은 중요도를 보여주고 있으며, 정보보안 교육도 다른 변수에 비해 높은 중요도를 보여주고 있다. 세부 내용은 <표 8>과 <그림 3>에 제시하였다.

〈표 8〉 사내 정보보안 점검 – 범주형 회귀 분석 결과

독립변수	B	표준 오차	F	유의 확률	중요도
네트워크 위협	-.051	.019	7.003	.008	.022
비 네트워크 위협	.069	.020	11.808	.001	-.001
임원진 정보보안	-.100	.018	30.052	.001	.129
업종(산업)	.185	.015	148.614	.000	.264
조직규모	.211	.016	180.941	.000	.365
정보보안 교육	.128	.017	57.300	.001	.220
R^2=0.144, 수정된 R^2=0.140, F=31.545(p=0.000)					

업종(산업)을 세부적으로 살펴보면 4번 건설업, 6번 운수 및 창고업, 12번 사업시설관리업, 14번 보건업이 다른 산업에 비해 높은 수량을 보였다. 특히 4번 건설업과 12번 사업시설관리업은 정보보안 규정 제정에 다른 산업보다 미흡한 모습을 보였다면 사내 정보보안 점검에 대해서는 다른 산업보다 사내 정보보안 점검을 자주 하는 것으로 나타났다. 그리고 1번 농림수산업, 9번 금융 및 보험업, 15번 예술 및 스포츠업이 사내 정보보안 점검에서 다른 산업보다 낮은 수량값을 보여주고 있다.



〈그림 3〉 사내 정보보안 점검 - 산업별 현황

4.6 프로세스 4 검정 : 정보보안 예산 수준 인과 분석

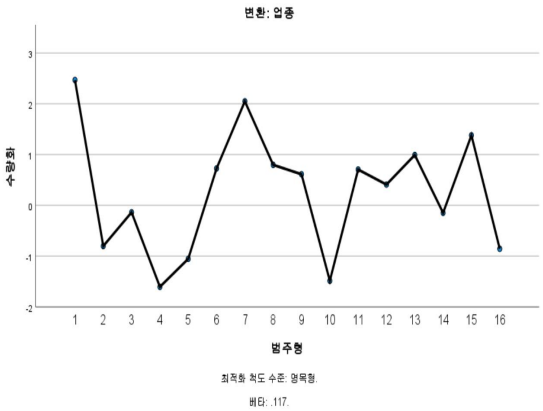
마지막 프로세스 4 검정에서는 기업들의 정보보안 예산투자에 강력한 영향을 제공하는 중요 독립변수가 무엇인지 확인하고자 범주형 회귀 분석을 진행하였다. 분석 결과를 살펴보면, 분석 모형의 설명력은 10.8%이며 F값은 23.871(p=0.000)으로 나타났다. 분석 모형에서 모든 독립변수는 정보보안 예산투자에 영향을 제공하는 것으로 나타났다. 이중 비 네트워크 보안 위협은 음의 영향을 보여주었고, 나머지 모든 독립변수는 정의 영향을 보여주고 있다. 종속변수에 영향이 가장 큰 독립변수는 임원진 정보보안, 정보보안 교육, 비 네트워크 보안 위협, 업종

(산업) 순으로 나타났다. 즉, 임원진의 정보보안 인식이 적절한 정보보안 예산투자에 긍정적 영향을 제공한다고 나타났다. 두 번째로는 비 네트워크 보안 위협이 적을수록 정보보안 예산투자에 긍정적 영향이 있다고 나타났다. 즉, 인적 요인에 의한 정보 유출이 없고, 물리적 위협이 없고, 사내 가이드 및 규정 등이 잘 운영될수록 정보보안 예산투자에 긍정적 영향을 제공한다고 해석할 수 있겠다. 반대로 네트워크 보안 위협인 정보기술 네트워크 침해사고의 위협이 강해질수록 정보보안 예산투자는 크게 높아진다고 해석할 수 있다. 세부 내용은 <표 9>와 <그림 4>에 제시하였다.

〈표 9〉 정보보안 예산투자 – 범주형 회귀 분석 결과

독립변수	B	표준 오차	F	유의 확률	중요도
네트워크 위협	.064	.022	8.258	.004	.006
비 네트워크 위협	-.189	.021	81.372	.000	.178
임원진 정보보안	.204	.016	156.465	.000	.429
업종(산업)	.117	.013	76.615	.000	.147
조직규모	.058	.014	16.487	.001	.049
정보보안 교육	.112	.015	53.204	.001	.190
R^2=0.113, 수정된 R^2=0.108, F=23.871(p=0.000)					

업종(산업)을 세부적으로 살펴보면, 1번 농림수산업, 7번 금융 및 보험업은 수량화에서 2 이상의 양의 값을 보여주어 다른 산업에 비해 정보보안 예산투자에 더 적극적인 모습을 보여주고 있다. 이와 반대로 수량화에서 -1 이하의 값을 보여주고 있는 2번 제조업, 4번 건설업, 5번 도매 및 소매업, 10번 부동산업, 16번 협회 및 단체업 등은 다른 산업에 비해 정보보안 예산투자에 대해서 소극적인 모습을 보여주고 있다.



〈그림 4〉 정보보안 예산투자 - 산업별 현황

Ⅴ. 연구 결론

5.1 연구 결론과 시사점

디지털 전환 시대에 접어들면서 인공지능과 빅데이터, 로봇의 기술이 빠르게 발전하면서 데이터의 관리와 보호의 중요성은 더욱 커지고 있다. 하지만 정보보안을 불완전하게 운영하는 기업들에서 기밀정보 누출이 자주 발생하고 있으며 이는 기업뿐만 아니라 국가와 개인의 재산적 피해를 발생시키고 있다. 이에 본 연구에서는 디지털 전환 시대 기점으로 기업들의 정보보안 수준을 진단하였고, 운영성과 역량을 높이는 중요 변수가 무엇인지 확인하였다. 이러한 연구 결과를 요약하면 다음과 같다.

4개의 집단으로 정보보안 수준을 분류하여 상호 집단을 비교하였을 때 정보보안 정책을 보유하고, 정보보안 최고책임자가 선임되어 있으며 정보보호 침해사고 발생 가능성을 항상 예의주시하고 있는 집단이 정보보안 운영성과가 높게 나타났다. 그리고 네트워크 보안 위협, 비 네트워크 보안 위협, 임원진 정보보안 인식, 산업, 조직규모, 정보보안 교육 등 모든 변수는 정보보안 규정, 사

내 정보보안 점검, 정보보안 예산투자에 영향을 제공하는 변수로 나타났다. 이중 네트워크 보안 위협 변수는 침해사고 위협이 높아질수록 정보보안 규정과 정보보안 예산투자를 높여주는 요인으로 나타났다. 하지만 사내 정보보안 점검에서는 반대의 효과를 보였다. 네트워크 침해사고 보안 위협이 높아지면 사내 정보보안 점검이 자주 되지 않았다는 결과를 보여주었다.

다음 비 네트워크 보안 위협에서는 침해사고 위협이 높아질 때 정보보안 규정과 사내 정보보안 점검을 높여준다고 나타났다. 하지만 예산투자에서는 반대의 결과를 보여주었다. 비 네트워크 보안 위협이 높아지면 적절한 예산투자가 되지 못했다는 결과를 보였다. 임원진의 정보보안 인식에서는 정보보안 규정과 정보보안 예산에서 긍정적 영향을 제공한다고 나타났다. 하지만 임원진의 정보보안 인식이 낮아지면 사내 정보보안 점검이 더 높아진다고 나타났다. 이는 임원진의 정보보안에 대한 관리·감독 관점에서 소홀해질 때 오히려 정보보안 점검에 더 필요하다는 관점으로 해석할 수 있겠다. 한편, 정보보안 규정 제정과 사내 정보보안 점검, 정보보안 예산투자를 각각의 산업별로 살펴보면 각각 집중하여 투자하는 보안 요소들이 다른 것을 확인할 수 있었다. 예를 들어 건설업은 정보보안 규정 제정과 예산투자에서 다른 산업보다 낮은 선호도를 보였지만 보안점검에서는 다른 산업보다 높은 선호도를 보여주었다. 농림수산업은 건설업과 반대로 정보보안 규정 제정과 예산투자에서 다른 산업보다 높은 투자 선호를 보였지만 보안점검에서는 다른 산업에 비해 낮은 선호를 보여주고 있다. 이렇듯 산업별로도 정보보안 투자 선호가 다른 것을 확인할 수 있다.

본 연구의 이론적 시사점은 다음과 같다. 기업들의 정보보안 운영에 필요한 중요 변수가 무엇인지 설명하기 위해서 정보보안의 의미, 관리적 정보보안, 네트워크 보안 등의 이론을 정리하고 활용하였다. 해당 정보보안 이론을 토대로 향후 기업 의사결정 연구과 경영전략 연구 등의 경영학 연구와 IT 투자와 활용 등의 경영정보 연구에 적용할 수 있도록 본 연구는 기여하였다.

실무적 시사점은 다음과 같다. 첫째, 기업들은 정보보안 규정을 제정하거나 예산투자 시 임원진의 정보보안 인식을 우선으로 강화할 필요가 있겠다. 이에 정기적인 정보보안 교육이 정보보안 인식 강화에 도움이 될 수 있다. 둘째, 조직구성원들의 정보보안 교육은 정보보안 제정, 예산투자, 점검 활동에 긍정적 영향을 제공하므로 기업은 정기적인 보안 교육활동을 투자할 필요가 있겠다. 마지막, 기업들은 정보전략 수립 시 정보보안 활동을 비용이 아닌 투자의 개념으로 인식하여 네트워크 위협과 비 네트워크 위협을 회피할 수 있어야 한다.

5.2 향후 연구과제

본 연구는 2022년도 과학기술정보통신부와 한국정보보호산업협회에서 수집한 '2022년 정보보호 실태조사(기업)' 데이터를 활용하여 정보보안을 분석하였다. 분석 결과를 살펴보면 2021년 데이터 분석 결과와 2022년 데이터 결과에서 정보보안 규정이 산업별로 차이를 보였다. 이에 향후 2023년 정보보안 데이터를 토대로 정보보안 규정이 산업별로 지속해서 변동을 보이는지 확인할 필요가 있겠다.

참고문헌

[1] 한국과학기술기획평가원, 디지털 전환 시대의 과학기술혁신정책 : 산업 고도화와 융복합 신산업 창출을 위한 10대 정책과제, 2022.12.31

[2] 정병호·주형근, "인공지능 기술 위험관리에 따른 과학기술 정책과 활용 불안감," e-비즈니스연구, 제21권, 제3호, 2020, pp.91-104.

[3] 박새한·이상엽·한기현·김지연·구지현·정병호, "의료 빅데이터로 분석한 만성질환자의 건강정보 수준별 차이 연구," 디지털산업정보학회 논문지, 제

19권, 제4호, 2023, pp.73-86.

[4] 정병호, “기밀정보 유출 경험을 가진 기업들의 정보사고 대응역량 강화에 관한 연구,” 디지털산업정보학회 논문지, 제12권, 제2호, 2016, pp.73-86.

[5] 한국경제, “[단독] 협력사 뚫리면 속수무책...대기업 정보보안 비상,” https://www.hankyung.com/article/2024021277731i, 2024.02.13.

[6] News1, 방사청, “KF-21 기밀 유출 시도에 엄중하게 주시… 합동조사 중,” https://www.news1.kr/articles/5312127, 2024.02.05.

[7] 디지털데일리, “LG엔솔 비밀 누출한 前직원 구속…’자문’에 ’가명’까지 수단방법 안 가려,” https://www.ddaily.co.kr/page/view/20230816143641322600, 2023.08.16.

[8] BreakNews, “군 기밀 문서 누출 HD현중 직원, 항소심서 일부 무죄 유죄 판결,” https://www.breaknews.com/1001640, 2023.11.30.

[9] NIST, Information Security Handbook: A Guide for Managers, 2006.

[10] Bulgurcu, B., Cavusoglu, H. and Benbasat, I., “Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness,” MIS Quarterly, Vol.34, No.3, 2010, pp.523-548.

[11] Mamonov, S. and Benbunan-Fich, R., “The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors,” Computers in Human Behavior, Vol.83, 2018, pp.32-44.

[12] Solms, B., “Information security management: The second generation,” Computer and Security, Vol.15, No.4, 1996, pp.281-288.

[13] Hone, K. and Eloff, J. H., “Information Security Policy: What do International Information Security Standards Say?,” Computers and Security, Vol.21, No.5, 2002, pp.402-409.

[14] Hsu, Jack Shih-Chieh, et al., “The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness,” Information Systems Research, Vol.26, No.2, 2015, pp.282-300.

[15] NIST, Risk management guide for information technology systems. ist Special Publication, 2002.

[16] Vance, A., Siponen, M. and Pahnila, S., “Motivating IS Security compliance: Insights from Habit and Protection Motivation Theory,” Information & Management, Vol.49, 2012, pp.190-198.

[17] McIlwraith, A., Information security and employee behaviour: how to reduce risk through employee education, training and awareness, Routledge, 2021.

[18] Hwang, I., Kim, D., Kim, T. and Kim, S., “Why Not Comply with Information Security? An Empirical Approach for the Causes of Non-compliance,” Online Information Review, Vol.41, No.1, 2017, pp.2-18.

[19] 김봉현・조동욱, “네트워크 보안 기술 동향과 전망,” 한국통신학회지(정보와 통신), 제31권, 제4호, 2014, pp.99-106.

[20] 김시홍・구자환・박병연・박학수・최장원・이재용, “IP 통합 관리를 통한 유·무선 네트워크의 생존성 향상에 관한 연구,” 정보보증논문지, 제3권, 제3호, 2003, pp.43-50.

[21] Yeh, Quey-Jen, and Arthur Jung-Ting Chang., "Threats and countermeasures for information system security: A cross-industry study," Information & Management, Vol. 44, No. 5, pp. 480-491, 2007.

[22] 이대식・윤동식, “유비쿼터스 컴퓨팅 및 네트워크의 보안연구,” 정보보증논문지, 제5권, 제4호, 2005,

pp.59-65.
[23] Vacca, John R. Computer and information security handbook. Newnes, 2012.
[24] 과학기술정보통신부・한국정보보호산업협회, 2022년 정보보호 실태조사(기업), https://kisia.or.kr
[25] Hair, Joseph F., Multivariate data analysis, 2010.
[26] 정병호・주형근, “산업별 정보보안의 투자 수준과 관리 역량에 관한 연구,” 디지털산업정보학회 논문지, 제19권, 제2호, 2023, pp.89-102.

■ 저자소개 ■

정 병 호
(Jung Byoungho)

2024년 현재 한성대학교 지식서비스&컨설팅 대학원 초빙교수
2015년 8월 한국외국어대학교 경영학 박사
2011년 3월 한국외국어대학교 경영학 석사

관심분야 : IT투자, 정보윤리, 빅데이터, 신기술 혁신, 조직변화 관리
E-mail : jung.hmis@gmail.com

주 형 근
(Joo Hyungkun)

2024년 현재 한성대학교 교수
2021년 현재 기술표준원 평가위원. 상사중재인

관심분야 : e-비즈니스, 중소기업혁신
E-mail : hkjoo@hansung.ac.kr

논문접수일 : 2024년 2월 21일
수정접수일 : 2024년 3월 08일
게재확정일 : 2024년 3월 15일