정책학석사학위논문

기업의 정보보호 활동에 관한 연구

— 정보보호 체계 구축 수준에 따른 차이를 중심으로 —

2017년 8월

서울대학교 행정대학원

행정학과 정책학전공

김 용 재

국 문 초 록

오늘날 정보통신기술의 발달과 인터넷의 광범위한 보급으로 말미암아 전 영역의 산업 분야에서 급속한 정보화가 진행되고 있다. 이로써 기업 차원에서는 업무 프로세스의 효율화 및 비용 절감 등이 가능해졌으나, 동시에 보다 지능화·대규모화된 사이버 공격에 노출되고 있다. 실제로 2014년에는 KB국민카드, NH농협은행, 롯데카드 등 3개 카드사에서 대량의 고객 개인정보가 유출되는 사건이 일어나기도 하였다.

이러한 위험에 대응하기 위하여 2011년 개인정보보호법이 제정되는 등 정부 차원에서 기업의 정보보호에 대한 법·제도적인 보완책을 마련하고자 노력해왔다. 그러나 여전히 기업의 규모·업종 등 기업의 개별적인 특성과 상황을 고려한 세부적인 법적 기준이 미흡한 것이 실정이다.

또한 정보보호를 위한 인적자원 관리 활동으로서의 정보보호 교육, 그리고 정보 침해 사고의 예방 및 사후 조치를 위한 수단으로서의 정보보호 점검 활동이 갖는 중요성이 거듭 강조되어왔으나, 이에 대한 선행연구가 부족한 것이 현실이다.

이에 따라 이 논문은 기업의 정보보호 수준과 직결되는 정보보호 교육 및 정보보호 점검 활동을 아울러 '정보보호 활동'으로 명명하고, 이에 영향을 미치는 요인을 규명함으로써 기업 정보보호 정책의 방향성을 제시하고자 하였다. 이때 정보보호 활동에 영향을 미치는 독립변수로서 기업의 투입 요소(input)인 '정보보호 체계'를 선정하였다.

즉, 이 논문은 기업의 정보보호 체계의 구축 수준이 기업의 정보보호 활동 수준에 미치는 영향력을 통계적으로 검증하고자 하였으며, 이때 정보보호 체계는 '정보보호 정책', '개인정보보호 정책', '정보보호 조직', '정보보호 관리자 인력', '정보보호 담당 인력' 및 '정보보호 예산' 등 복수의 하위 변수로 구성된다.

분석 대상 자료로는 정부 주관 하에 한국인터넷진흥원이 총 9,586개의

민간 기업을 대상으로 수행한 '2016년 정보보호 실태조사(기업)'의 원 데이터(raw data)를 활용하였다.

다중회귀분석을 통한 가설 검증 결과, 첫 번째로 기업의 정보보호 체계 가운데 정보보호 정책을 제외한 모든 변수가 기업의 정보보호 교육에 정(+)의 영향을 미친다는 사실을 확인하였다. 즉, 기업 내 개인정보보호 정책이 수립되어 있을 때, 정보보호 조직이 구축되어 있을 때, 정보보호 관리자 인력이 많이 임명되어 있을수록, IT 인력 가운데 정보보호 담당 인력의 비중이 높을수록, IT 예산 가운데 정보보호 예산의 비중이 높을수록 기업의 연간(2015년) 정보보호 교육 시간의 총계가 증가하였다.

두 번째로 정보보호 점검 활동에 대하여는 정보보호 정책, 개인정보보호 정책, 정보보호 조직, 정보보호 관리자 인력, 정보보호 담당 인력, 정보보호 예산이 모두 정(+)의 영향을 미친다는 사실을 도출하였다. 다시 말해 정보보호 정책이 수립되어 있을 때, 개인정보보호 정책이 수립되어 있을 때, 정보보호 조직이 구축되어 있을 때, 정보보호 관리자 인력이 다수 임명되어 있을수록, IT 인력 가운데 정보보호 담당 인력의 비중이 높을수록, IT 예산 가운데 정보보호 예산의 비중이 높을수록 기업의 정보보호 점검 빈도가 높게 나타난 것이다.

이를 통해 정부가 기업의 정보보호 활동 관련 정책을 입안함에 있어 기업의 정보보호 체계 구축에 대한 법·제도적 규정을 강화하는 것이 정보보호 수준을 제고하는 데 효과가 있을 것이라는 점을 추론할 수 있다.

마지막으로, 이 논문은 기업의 규모·업종을 통제변수로 투입하여 살펴보았다. 그 결과, 기업의 규모가 클수록, 업종의 경우 금융 및 보험업에서 상대적으로 정보보호 활동 수준이 높게 나타남을 알 수 있었다. 따라서 정부는 규모·업종에 따라 발생하는 정보보호 수준의 편차를 개선하기 위한 노력 또한 기울여야 할 것이다.

주요어: 정보보호, 개인정보보호, 정보보호 체계, 정보보호 교육, 정보보호 점검

학 번: 2015-24509

목 차

표 목 차

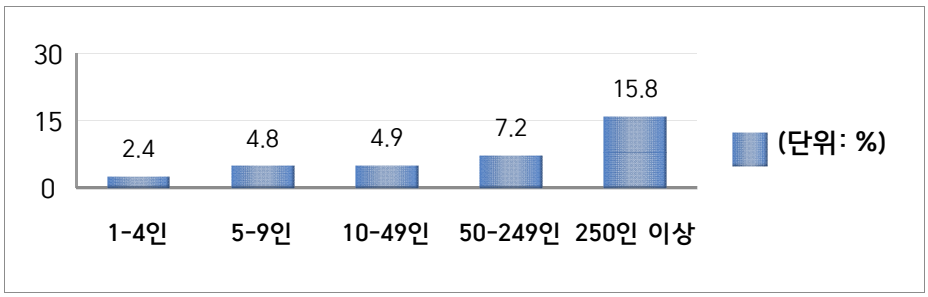
그 림 목 차

제 1 장 서 론

제 1 절 연구의 배경 및 목적

정보통신기술의 발달과 인터넷의 광범위한 보급으로 인해 모든 영역의 산업 분야에서 급속한 정보화가 진행되고 있다. 이러한 추세는 기업 업무 프로세스의 효율성 및 편의성 증대, 비용 절감 등과 같은 긍정적 효과를 낳았지만, 동시에 사이버 공격, 정보 유출 등의 역기능 또한 야기하였다(김지수 외, 2012; 임헌정 외, 2010).

한국인터넷진흥원(2016)에 따르면, 국내 사업체의 약 3.1%가 2015년 한 해 동안 해킹, 악성코드(웜·바이러스), DDoS 등의 침해사고를 경험한 것으로 드러났고, 규모별로는 250명 이상 규모 사업체의 15.8%가 침해사고를 겪은 것으로 나타나 기업 규모가 클수록 침해사고의 위협에 더 크게 노출되는 경향을 보였다.



[그림 1] 기업 규모별 정보보호 침해 사고 현황(2015년)

출처: 한국인터넷진흥원(2016)

특히 오늘날 보안 공격은 점차 지능화·대규모화하고 있으며(김동우 외, 2013), 일례로 2014년에는 KB국민카드, NH농협은행, 롯데카드 등 3개 카드사에서 대량의 고객 개인정보가 유출되는 사태가 벌어지기도 하

였다(국민일보, 2016). 또 같은 해, 국외에서는 인터넷 포털 야후(Yahoo)에 대한 해킹 공격으로 인해 가입 회원 약 5억 명의 개인정보가 유출되는 사건이 있었다(조선일보, 2016).

이로써 볼 때 금융 데이터 등의 민감한 정보가 기업에서 유출되는 것은 기업의 존립을 위협하는 요소이자, 광범위한 사회적 피해를 일으키는 요인이 된다(김지수 외, 2012). 실제로 2017년 2월, 법원은 롯데카드 개인정보유출 피해자 3,577명에게 기업 차원에서 10만원씩 배상하라는 판결을 내리기도 하였다(조선 비즈, 2017).

더욱이 최근 들어 클라우드, IoT, 스마트워크 등 새로운 기술이 보급되어 데이터의 이동이 자유로워지면서 정보 유출의 위험성 또한 한층 커지게 되었다(컴퓨터월드, 2016). 이러한 새로운 위협에 대응하기 위해 미국에서는 2009년부터 국가 차원에서 정보보호 교육과 관련한 종합적인 대책을 마련하여 시행하고 있다(김동우 외, 2013).

우리나라에서도 2011년 개인정보보호법이 제정되는 등 기업의 정보보호에 대한 법·제도적인 보완과 의식 제고를 위한 노력이 이어졌다(남길현, 2011). 그러나 여전히 기업의 규모·업종 등 기업의 개별적 특성과 상황을 고려한 보다 세부적인 법적 기준 및 기업의 정보보호 교육·훈련 등에 관한 명확한 규정이 없어 개인정보를 포함한 각종 정보가 유출될 위험성은 늘 존재한다(김진형 외, 2012).

이에 따라 이 논문은 기업 차원에서의 정보보호 활동 수준을 진단하고, 이에 영향을 미치는 요인을 규명함으로써 기업 정보보호에 관한 정책의 방향성을 모색하고자 한다.

제 2 절 연구대상과 범위

이 논문은 위와 같은 연구 배경 하에 기업의 정보보호 활동에 영향을 미치는 요인을 탐구하는 것을 주요 목표로 하고 있다. 그리고 이에 영향을 미치는 변수로서 '정보보호 체계'의 중요성에 주목하여, 기업의 정보보호 체계 구축 수준의 차이에 따라 기업의 정보보호 활동 수준에 통계적으로 유의미한 차이가 존재하는지를 검증하고자 한다. 이때 편의상 기업의 정보보호 교육과 정보보호 점검 활동을 아울러 '정보보호 활동'으로 정의한다.

아래에서 보다 자세히 논할 것이지만, 본 연구에서는 정부 주관 하에 한국인터넷진흥원이 전담하여 수행한 민간기업 정보보호 실태조사 데이터 가운데 2016년도의 데이터 및 자료를 활용할 것이다.

이 설문조사는 '종사자 수 1인 이상, 네트워크에 연결된 컴퓨터를 1대 이상 보유한 전국의 사업체'를 대상으로 이루어졌으며, 유효 응답자 수는 총 9,586개 사업체였다(한국인터넷진흥원, 2016).

그리고 해당 조사의 내용 및 범위는 정보보호 정책 수립 및 정보보호 조직 구성 현황, 임직원 대상 정보보호 교육 실시 현황, 정보보호 예산 및 투자 현황, 정보보호 제품 및 서비스 운영 현황, 정보보호 관리 현황, 침해사고 경험 여부 및 침해사고 대응활동 현황, 개인정보 수집 및 이용 현황, 개인정보보호 관리 및 개인정보 침해사고 대응 현황, 정보보호의 중요성 및 위협 요인에 대한 인식 현황, 신규서비스 정보보호 투자 현황 등을 아우르고 있다(한국인터넷진흥원, 2016).

이 가운데에서도 본 논문은 관련 선행연구 및 설문조사 내용을 근거로 하여 연구 범위를 제한하고자 한다.

우선 독립변수인 '정보보호 체계'의 수준을 측정하기 위한 세부 변수로서 정보보호 정책 및 개인정보보호 정책, 정보보호 조직, 정보보호 인력, 정보보호 예산 등을 채택하였으며, 종속변수인 '정보보호 활동'은 각각 '정보보호 교육'과 '정보보호 점검 활동'으로 세분화하여 정의한다. 이때 정보보호 교육은 기업에서 실시한 연간 교육시간의 총계로 측정하며, 정

보보호 점검 활동은 관련 문항을 근거로 하여 점검 빈도로써 측정한다.

변수의 정의 및 측정 방법과 관련하여서는 아래에서 보다 자세하게 기술하도록 한다.

제 2 장 이론적 논의와 선행연구

제 1 절 정보보호

1. 정보보호의 개념 및 의의

국내외 학계에서 '정보보호'는 '정보를 입력·저장·처리·출력·전송하는 등의 모든 단계에서 정보를 보호하기 위해 정보의 비밀성(confidentiality), 무결성(integrity), 가용성(availability) 등을 확보하는 것'(김용겸, 2009), '정보의 입력, 처리, 저장, 출력, 전송 등의 모든 단계에 걸쳐 시스템을 보호하는 것' 혹은 '다양한 내외적인 위협들로부터 조직의 손실을 최소화하고 이익을 극대화하는 것' 등으로 정의되고 있다(박준경 외, 2011). 이때 '정보보호'와 유사한 개념으로서 '정보보안'이 사용되기도 한다.[1)]

이로써 미루어볼 때, '정보보호'는 단지 정보 유출을 막기 위한 기술적인 수단을 마련하는 것에 국한되지 않으며, 조직 관리를 위한 일련의 조치를 포괄하는 개념이라고 할 수 있다.

이 논문이 연구하고자 하는 설문조사에서 또한 이러한 확장된 의미로서의 '정보보호' 개념을 사용하였다. 한국인터넷진흥원(2016)은 '정보보호'를 '정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 조치'로 정의하고 있다.

이에 더해 해당 설문조사는 '정보보호'와는 별개의 개념으로서 '개인정보보호'를 정의하여 활용하였다. '개인정보보호'는 '특정 개인을 알아볼

1) 한편 '정보유출'은 '종이나 전자적으로 된 문서의 정보가 불법적으로 국가나 조직 밖으로 나가는 것'(박종일, 2013) 등으로 정의되고 있다.

수 있는 정보(성명, 주민등록번호, 영상정보 등)가 유출되는 위협으로부터 보호하는 활동'으로 규정되고 있는데(한국인터넷진흥원, 2016), 이 논문은 일차적으로 '정보보호'라는 용어를 '개인정보보호'를 포함한 전반적인 정보보호 관련 활동 및 조치를 통칭하는 개념으로 사용하기로 한다.[2)]

다만 설문조사에서 정보보호와 개인정보보호의 개념을 명확히 분리하여 사용한 문항을 검증하는 경우, 그 사실을 명시함으로써 개념상의 혼동이나 분석 결과상의 왜곡이 없도록 할 것이다.

본 연구에서는 최종적으로 해당 설문조사에서 사용된 '정보보호' 및 '개인정보보호'의 개념을 채택하되, 선행연구 결과와 설문조사 문항을 고려하여 독립변수인 '정보보호 체계'의 내용을 정보보호 정책 및 개인 정보보호 정책, 정보보호 조직, 정보보호 인력, 정보보호 관련 예산 등의 범위로 한정하고자 한다.

그리고 앞서 롯데카드에 대한 법원의 판결 사례에서 유추할 수 있듯 오늘날 기업이 각종 위협으로부터 내부 정보를 보호하는 것은 기업의 법적 책임으로 인식되고 있으며, 정보보호 활동을 통해 잠재적인 보안 피해를 사전에 예방할 수 있다는 점에서 이는 큰 의의를 지닌다.

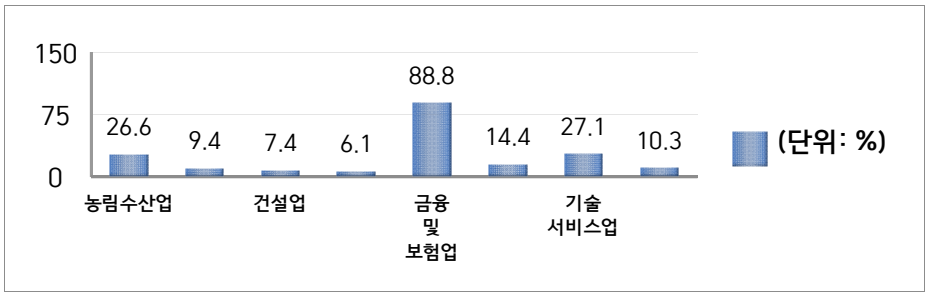
즉, 기업의 정보자산 및 정보보호 활동은 기업의 경쟁우위 및 조직적 가치와도 직결되는 요소라고 할 수 있는 것이다(김용겸 외, 2009; 조선비즈, 2017).

2. 기업의 정보보호 실태

한국인터넷진흥원(2016)에 의하면, 조사된 9,586개 기업 가운데 공식 문서로 작성된 정보보호 정책이 있는 사업체는 14.5%인 것으로 나타났다. 업종별로는 금융 및 보험 기업의 정보보호 정책 수립률이 88.8%로 가장 높았다.

---

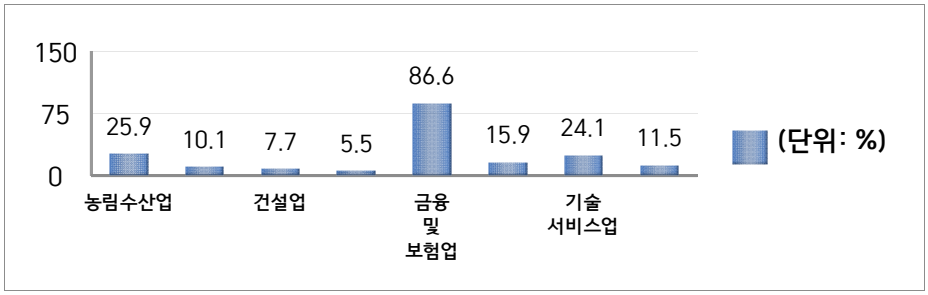
2) 본 논문에서는 독립변수인 '정보보호 체계'에 '개인정보보호 정책'을 포함시켰다.



[그림 2-1] 주요 업종별 정보보호 정책 수립 현황(2015년)

출처: 한국인터넷진흥원(2016)

한편 공식 문서로 작성된 개인정보보호 정책이 있는 사업체는 15.3%로 나타났다. 이 또한 마찬가지로 금융 및 보험업의 경우 개인정보보호 정책 수립률이 86.6%로 드러나 가장 높은 정보보호 수준을 보이고 있었다.



[그림 2-2] 주요 업종별 개인정보보호 정책 수립 현황(2015년)

출처: 한국인터넷진흥원(2016)

이어서 조사된 사업체의 약 11%가 공식적인 정보보호(개인정보보호 포함) 조직을 운영하고 있는 것으로 파악되었다.

한편 정보보호 관련 책임자 임명 비율은 정보관리책임자(CIO)의 경우 9.4%, 정보보호최고책임자(CIS)가 8.9%, 개인정보보호책임자(CPO)가 10.5%인 것으로 나타났다. IT 인력 가운데 정보보호를 담당하는 인력을 배정한 사업체는 14.6%로 조사되었다.

정보보호 관련 분야에 예산을 책정한 사업체는 32.5%인 것으로 드러났고, IT 예산 가운데에서 정보보호 예산이 차지하는 비중은 '1% 미만'이라고 한 응답한 사업체가 23.3%로 가장 높게 나타났다. 즉, 전체 IT 예산 가운데 정보보호 예산의 비중은 대체적으로 낮은 수준에 머무르고 있는 것이다. 정보보호 예산을 편성한 사업체는 주로 '정보보호 제품 구입(42.9%)'에 많은 예산을 투입한 것으로 파악되었다.

이러한 실태 조사 현황을 보았을 때, 정보보호 관련 정책의 수립 비율은 14~15%대, 조직 운영 비율은 11%대, 정보보호 관련 인력의 임명 및 배정 비율은 8~14%대의 분포를 형성하고 있음을 알 수 있다. 관련 예산을 편성한 사업체가 32.5%로 나타난 것을 제외하고는 기업의 정보보호 활동 수준이 현저히 낮은 것을 알 수 있다.

이는 개인정보보호법 등 관련 법률이 제·개정되었음에도 불구하고 정보보호의 사각지대에 놓여 있는 기업이 대다수임을 시사하며, 업종 등 기업의 특성에 따라 정보보호 수준의 편차가 크다는 사실 또한 파악할 수 있다.

3. 기업 정보보호에 관한 선행연구

(1) 정보보호에 영향을 미치는 변수에 관한 연구

앞서 밝힌 바와 같이 '정보보호'는 다양한 의미로 정의되고 있으며, 기업의 정보보호에 관한 선행연구에서도 기업의 정보보호와 그에 영향을 주는 요인들이 각기 다르게 개념화되고 있었다.

이때 기업의 정보보호에 영향을 미치는 요인에 관한 선행연구는 조직 구성원의 인식·태도, 관련 법·제도 등의 독립변수를 중심으로 진행되었다.

먼저 많은 연구에서 조직 구성원들의 정보보호 인식 및 태도를 기업

정보보호에 영향을 미치는 요소, 즉 독립변수로서 규명하고 있었다.

박준경 외(2011)는 기업을 분석 단위로 하여 조직원들의 인식 및 태도가 기업의 정보보호에 중요한 영향을 미친다고 가정하고, 다시 조직원들의 인식과 태도에 영향을 주는 요인을 규명하였다.

이 연구는 기업의 '정보보호'를 정보 유출에 대비되는 개념으로 정의하여, 이것이 기술적·하드웨어적 요소와 관리적 조치를 통해 달성 가능한 것이라고 보았다. 이때 박준경 외(2011)는 특히 기술적 조치보다 조직 구성원에 대하여 교육 및 홍보활동 등을 시행함으로써 조직원들에게 정보보호를 위한 동기를 부여하는 것이 중요하다고 주장하였다.

박준경 외(2011)에 따르면 인지된 보안교육이 기업 정보보호에 대한 조직 구성원의 태도에 직접적이고 긍정적인 영향을 미친다는 것이 실증적으로 입증되었다. 그 가운데에서도 특히 정보보호와 관련한 인지된 보상 및 처벌의 유용성이 조직 구성원의 정보보호 태도에 직접적·긍정적 영향을 준다는 사실을 도출하였다.

김지수 외(2012)는 기업 내 정보보호최고책임자(CISO)의 역할인식이 조직의 정보보호 성과에 영향을 미친다는 사실을 확인하였다. 이 연구는 정보보호의 필요성이 증대됨에 따라 정보보호최고책임자의 역할이 중요해지고 있다고 보고, 그 영향력을 파악하고자 하였다.

김지수 외(2012)는 우선 정보보호 성과를 정보보호 안전 성과와 정보보호 기반 성과로 분류한 뒤, 이를 고객정보 안전, 법적 요구 준수, 정보보호 인식 제고, 침해 사고에 대한 조치, 보안통제 구현 등의 세부 요인을 통해 측정하였다.

이후 정보보호최고책임자의 역할인식의 유형을 분류하여 각 역할인식에 따라 정보보호 성과가 어떻게 달리 나타나는지를 분석하였다. 이때 역할인식 유형은 크게 '지적자산 가치 평가자', '정보통신 인프라의 전략적 활용 촉진자', '변화 관리자', '정보보안, 전략, 정책, 표준기술 확보자' 등 네 가지로 분류되었다.

그리고 통계적 검증 결과, 이 논문이 정의한 모든 유형의 역할인식이 정보보호 성과에 정(+)의 영향을 미친다는 사실이 확인되었다.

김민정 외(2014)는 중소기업을 분석 대상으로 하여 CEO의 개인정보보호 제도에 대한 의지, 기업의 매출규모 및 고객 개인정보 보유량이 개인정보보호 대책 활동과 개인정보보호 제도의 이해에 미치는 영향을 검증하였다.

이때 해당 논문에서 개인정보보호 대책 활동은 '개인정보보호를 위한 조직 및 인력 구성, 교육활동, 기술적 조치활동, 개인정보 침해사고의 예방 및 사후 처리를 위한 조치 활동'으로 정의되었으며, 이는 개인정보보호관리체계(PIMS)의 개인정보보호대책 항목을 통해 측정되었다. 구체적 지표로는 개인정보 관리 책임자의 지정, 개인정보 보호 조직의 구성 및 운영, 개인정보 취급자에 대한 교육, 백신 소프트웨어의 설치 및 주기적 점검, 개인정보 침해사고 예방에 관한 매뉴얼 수립 등이 있다.

한편 CEO의 개인정보보호에 대한 의지는 '경영계획을 수립할 때 개인정보보호에 대하여 중요하게 고려하는 정도'로 개념화되었으며, 5점 척도로 측정되었다.

김민정 외(2014)는 고객정보 보유량을 '기업에서 보유하고 있는 고객(이용자)의 개인정보 규모'로 정의하고, 이를 2011년도를 기준으로 총 6개 구간으로 나누어 추산하였다. 마지막으로 매출 규모는 '기업의 정보통신(IT)서비스 부문의 매출액'으로 개념화되었으며, 이 또한 2011년도를 기준으로 하여 7개 구간으로 측정되었다.

이에 의한 분석 결과, CEO의 의지와 고객정보 보유량은 개인정보보호 대책 활동에 정(+)의 영향을 주는 것으로 파악되었다. 반면 매출규모와 개인정보보호 대책 활동 간의 영향 관계는 드러나지 않았다. 이는 인적 요소와 절대적인 정보의 양이 개인정보보호 대책 활동에 통계적으로 유의미한 영향력을 행사하였음을 뜻한다.

다음으로 정보보호 법·제도와 관련한 연구로는 장상수 외(2013)가 있다. 장상수 외(2013)는 정보보호 관리체계(ISMS)의 운용이 기업의 정보보호 성과에 미치는 영향을 살펴보았는데, 그 과정에서 정보보호 관리과정인 PDCA(계획, 실행, 점검, 개선) 단계별로 그 영향력이 어떻게 달리 나타나는지를 확인하고자 하였다. 이때 해당 연구에서 정보보호 성과는

정보보호 안전 성과, 정보보호 기반 성과, 조직경영 달성 성과로 분류하여 측정되었다.

분석 결과, 정보보호 관리체계의 도입 및 활용이 정보보호 성과에 미치는 영향관계는 정보보호 관리 과정상의 계획단계(P), 실행단계(D) 및 점검단계(C)에서 두드러지게 나타나는 것으로 확인되었다. 장상수 외(2013)는 이를 통해 실증적 차원에서 정보보호 관리체계의 효과성을 분석함으로써 관리 과정 상 개별 기업이 보다 초점을 맞추어야 할 분야를 제시하였다.

한편 민간 기업이 아닌 공공기관의 정보보호 거버넌스 수준에 영향을 미치는 요인에 관한 연구도 있었다.

송정석 외(2011)는 정보보호를 강화하기 위한 차원에서 정보보호 거버넌스 체제를 도입한 공공기관에 대한 연구를 수행하였다.

이에 따르면, '정보보호 거버넌스'는 최고 경영층의 관점에서 정보보호를 총괄적으로 취급하는 프로세스이며, 업무 정보의 기밀성, 무결성, 가용성 등을 담보하기 위해서는 내·외부의 정보보호 요구 사항이 충족되어야 한다. 이때 외적 정보보호 요구 사항은 정보보호 관련 표준 및 최상의 업무 처리방식(best practice) 채택, 관련 법·규정의 준수 의무로 구분된다. 한편 내적 정보보호 요구사항은 업무 관련 이슈와 IT 인프라 이슈로 분류된다.

이 연구는 이러한 정보보호 거버넌스의 구현 수준을 측정하기 위해 정보보호관리체계(ISMS)를 평가 도구로 채택하였다. 즉, 조직의 정보보호 정책, 정보보호 대책 이행 여부에 관한 최고경영층에 대한 보고 등의 요소를 포함하는 정보보호관리체계의 평가 내용을 종속변수의 측정 기준으로 삼은 것이다.

분석 결과, 송정석 외(2011)는 정보보호 거버넌스 수준에 최종적으로 '최고 경영층의 지원' 요인이 정(+)의 영향을 미친다는 사실을 입증하였다. 이에 더해 정보보호 예산 및 정보화 담당 부서의 규모가 정보보호 거버넌스 수준에 영향을 준다는 분석 결과를 도출하였다. 이에 따라 이 연구는 정부가 공공기관으로 하여금 정보보호 관련 예산 및 인력을 확보

할 수 있도록 적극 보조해야 함을 주장하였다.

(2) 정보보호 성과 측정에 관한 연구

이처럼 기업 정보보호 성과에 영향을 미치는 요인(독립변수)을 규명하는 것 또한 중요하지만, 기업 정보보호의 성과를 측정하는 것 또한 기업 정보보호를 장려하기 위해 반드시 필요한 과정이다. 기업 정보보호의 성과를 합리적으로 측정하여 그 현황을 객관적으로 진단하는 것이 기업 정보보호 성과를 개선하기 위한 출발점이자 근거가 되기 때문이다.

기업 정보보호 성과의 측정과 관련하여서는 나윤지(2006) 등의 연구결과가 있다.

나윤지 외(2006)는 정보보호 요인을 기획, 환경, 지원, 기술, 관리 수준으로 세분화하여 이를 토대로 정보보호 성과 측정의 기준을 마련하고자 하였다.

먼저 정보보호 기획 수준에서는 보안정책 및 보안계획과 관련한 지표들을 구축하여 정보보호 정책의 수립 여부, 정책의 검토 및 평가, 정책의 문서화 현황을 점검할 수 있도록 하였다. 또 보안계획과 관련하여서는 정보보호 투자를 평가할 수 있어야 한다고 보았다. 이어서 환경 수준의 지표는 장비보안과 인사보안으로 구성되어야 한다고 보고, 정보보호 장비 구축 및 관련 시스템의 현황 등의 세부 지표를 제안하였다. 지원 수준에서는 지원 조직(담당자의 임명 등), 정보보호 교육 및 훈련을 포함하는 보안 지원활동 등을 평가하고자 하였다. 한편 기술 수준에서는 정보보호 관련 기술적 조치들을 점검하기 위한 지표를 제시하였고, 정보보호 관리 수준에서는 관리과정 요구사항 및 문서화 요구사항 등의 지표를 제안하였다.

장상수(2014)는 조직이 정보보호 목표를 달성함에 있어 정보보호 수준을 객관적으로 평가할 수 있는 지표가 필요하다고 보고, 균형성과표(BSC: Balanced Scorecard) 모형을 활용하여 정보보호 성과를 측정하고

자 하였다. 이때 정보보호 관점을 크게 정보보호성과, 정보보호활동, 정보보호정책, 정보보호투자의 체계로 구성하였으며, 각 영역에 따른 성과 목표와 지표를 도출하였다.

이에서 제안한 정보보호성과 관점의 지표로는 정보보호 매출액, 피해 감소 실적 등이 있고, 정보보호활동을 측정하는 지표는 설비 및 시설 점검율, 악성코드 일일점검 실적 등이 있다. 정보보호정책 관점을 구성하는 지표는 정보보호방침 수립실적, 정보보호조직 구성율 등이 있고, 정보보호투자 관련 지표로는 정보보호 전문 교육시간, IT관련 보안인력의 확보율, 정보보호 투자실적 등이 있다.

이러한 연구들을 토대로 보았을 때, 조직의 정보보호 성과 내지 대책 활동은 크게 정보보호 장비 및 시스템의 활용, 정보보호 관련 정책의 수립, 정보보호 투자 및 관련 예산의 확보, 정보보호 조직 구축 및 인력의 확보, 정보보호 시설 및 장비 점검 활동, 정보보호 교육 등을 통해 측정되고 있음을 유추할 수 있다.

제 2 절 정보보호 교육

1. 정보보호 교육의 개념 및 의의

‘정보보호 교육’은 선행연구를 종합하여보았을 때, ‘조직 내 인력의 보안 역량 강화와 보안 인식 수준 향상을 위해 수행하는 교육’으로 정의될 수 있다(오창규 외, 2003; 김동우 외, 2013).

뿐만 아니라, 정보보호의 중요성에 대한 의식 교육을 넘어 정보보호 전문 인력을 양성하기 위한 실질적인 훈련 프로그램의 필요성도 꾸준히 제기되고 있는데(문현정, 2009), 이러한 실무 인력 양성을 위한 훈련 또한 광의(廣義)의 ‘정보보호 교육’에 포함된다고 할 수 있다.

관련 선행연구를 살펴보았을 때, 기업의 정보보호 성과 및 조직원의 정보보호 인식 수준을 제고하기 위한 ‘정보보호 교육’의 중요성은 지속적으로 언급되고 있다.

그 예로 임채호(2006)는 정보보호 인식 수준을 제고하기 위한 방안으로서 정보보호 교육 및 기업 구성원의 자기 주도 학습이 중요함을 강조하였으며, 문현정(2009)은 안전한 디지털 경제 환경을 조성하기 위한 핵심 과제로서 정보보호 교육 훈련을 꼽았다.

그럼에도 불구하고 김동우 외(2013)는 범국가적 차원에서의 정보보호 교육 및 정보보호 인력관리 방안이 부족하다는 점을 지적하는 등 교육 현황의 한계에 대해 논의하였다.

기업 정보보호 관리 활동을 뒷받침할 만한 기술적인 수단을 구축하는 것도 중요하지만, 점점 고도화·지능화되는 보안 위협에 능동적으로 대처하기 위하여서는 조직 전반의 보안 역량을 강화할 필요성이 있다. 이때 정보보호 교육은 조직의 보안역량 강화를 위한 대표적인 수단 중 하나로서 정부 및 공공기관, 기업, 학계 등에서 보다 효과적인 정보보호 교육[3]

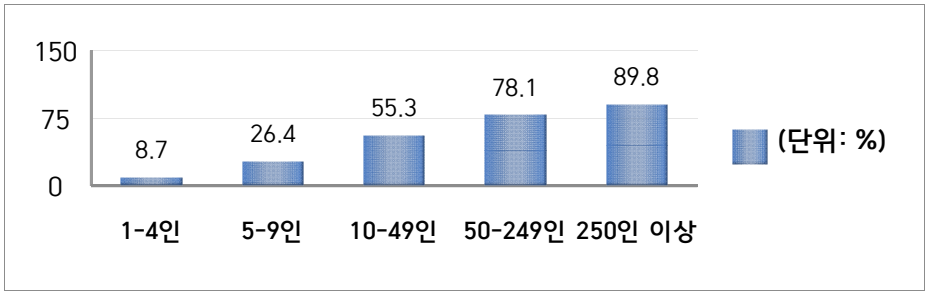
3) 정보보호 교육 이외의 수단으로는 캠페인, 홍보 활동과 같은 정보보호 인식 제고 프로그램이 있다.

을 위한 노력이 이어지고 있다(김건우 외, 2016).

2. 기업 정보보호 교육의 현황 및 효과

한국인터넷진흥원(2016)의 조사에 따르면, 2015년 한 해 동안 임직원을 대상으로 정보보호 및 개인정보보호 교육[4]을 실시한 사업체는 18%인 것으로 드러났다.

규모별로 정보보호 교육 실시 현황을 살펴보면, 규모가 클수록 정보보호 교육을 실시하는 비율이 높은 것으로 파악되었다.



[그림 3-1] 기업 규모별 정보보호 교육 실시 현황(2015년)

출처: 한국인터넷진흥원(2016)

정보보호 교육을 실시하는 사업체에 한해 교육 대상별 교육 운영 현황(복수 응답)을 살펴보면, '컴퓨터를 사용하는 일반 직원'을 대상으로 실시하는 비율이 86.7%로 가장 높게 나타났으며, '개인정보 취급자'와 '개인정보보호 책임자'가 각각 52.2%, 51.7%로 뒤를 이었다.

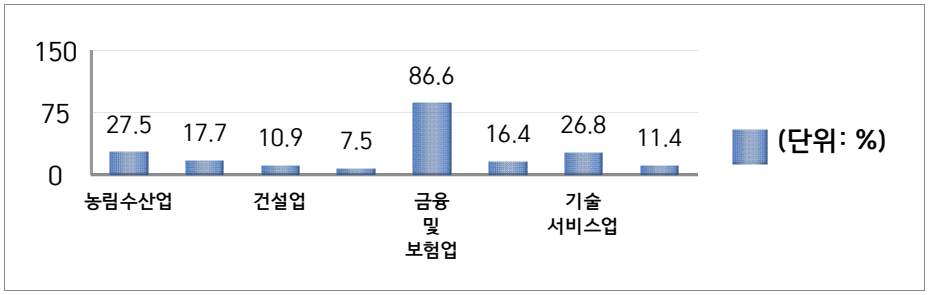
정보보호 교육 실시 대상 별 교육 시간과 관련하여서는 정보보호(개인정보보호 포함) 교육 대상자 가운데 개인정보보호 책임자, IT 및 정보보호 실무자에 대한 교육 시간이 연간 3.8시간으로 가장 높은 것으로 드러

4) 외부 위탁 교육을 포함한다.

났다.

정보보호 교육에 포함되는 내용 측면에서는 '관련 개념 이해 등 정보보호 일반'이 86.5%로 가장 높은 비중을 차지하고 있었고, 그 외에 '사례 중심의 정보보호 교육'과 '정보보호를 위한 관리적 조치사항'이 각각 78.7%, 49.5%로 나타났다.

한편, 업종에 따라서는 금융 및 보험업이 86.6%, 정보 서비스업이 46.4% 등으로 나타나, 이들 업종에서 정보보호 교육이 상대적으로 활발히 이루어지고 있음을 알 수 있었다.



[그림 3-2] 주요 업종별 정보보호 교육 실시 현황(2015년)

출처: 한국인터넷진흥원(2016)

3. 정보보호 교육에 관한 선행연구

정보보호 교육에 관한 선행연구로는 김건우 외(2016), 김동우 외(2013) 등이 있다.

김건우 외(2016)는 분석 대상을 기업에 국한하지 않고, 국내외의 다양한 저널 및 논문을 검토하여 정보보호 교육에 관한 연구 동향을 종합하였다. 그 결과, 해외에 비하여 국내에 게재된 정보보호 교육 관련 연구가 양적·질적 측면에서 부족하다는 사실이 확인되었다.

해외의 경우 정보보호 교육과 관련하여 일반적인 이론은 물론, 보안

전문가 등 정보보호 인력에게 요구되는 기본적인 소양 및 역량, 정보시스템의 취약점 분석을 위한 효과적인 실습방법, 개발자에게 필요한 기술적 교육 과정 등 보다 포괄적인 범위의 연구가 수행되었다.

반면, 국내에서는 해당 주제와 관련하여 교육기관—대학교 및 대학원—이 주요 분석대상으로서 선정되었으며, 세부적인 연구 분야는 정보보호 교육 과정·방법과 같은 전반적인 교육체계와 인력양성 방안 등에 집중되어 있었다. 이에 더하여 정보보호 교육의 효과성 측정에 관한 연구 또한 미흡하다는 점이 지적되었다.

한편, 김동우 외(2013)는 최근 들어 사이버 공격이 지능화되고 있어 그로 인한 피해가 크다고 보고, 이에 대응하기 위해서는 관련 인력이 중심이 되는 종합적인 정보보호 대책이 필요하다고 주장하였다. 그리고 이에 따라 이 논문은 정보보호 인력에 대한 교육활동이 중요하다고 보았다.

이때 김동우 외(2013)는 특히 국내 기업에서의 정보보호 관련 교육 활동이 매우 미흡한 수준이라고 보았다. 즉, 현재로서는 정보보호 교육과 관련한 정부 차원에서의 중장기적 계획이 부족하며, 관련 기관 간의 정보 교환이 미흡하고, 정보보호 교육 전문 인력(강사)의 확보가 어렵다는 것이다.

이 논문은 이러한 현황 진단을 토대로 하여 정부 차원에서 정보보호 교육 활동을 적극적으로 지원해야 한다고 보았으며, 단지 기업뿐 아니라 초·중·고 학생 및 일반인들도 대상으로 하는 보다 포괄적인 대책이 수립되어야 한다고 주장했다. 그리고 그 세부적인 방침으로서 김동우 외(2016)는 국가 정보보호 교육 마스터플랜의 기획 및 추진, 정보보호 교육 프로그램 인증제도의 도입, 정보보호 전문 인력 DB 운영, 정보보호 표준 교재의 개발 등을 제안하였다.

제 3 절 정보보호 점검 활동

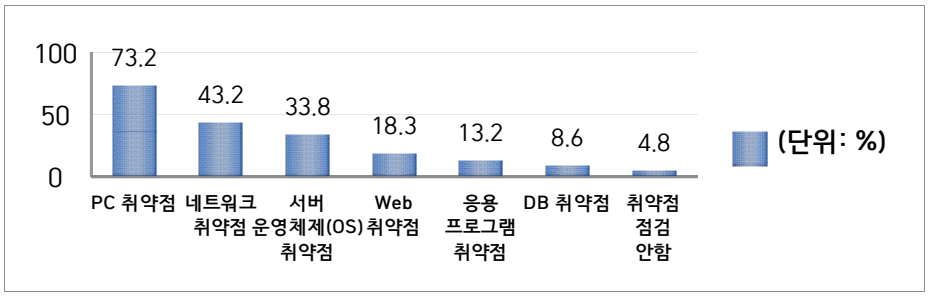
1. 정보보호 점검의 개념 및 의의

이 논문은 종속변수 가운데 하나로서 기업의 정보보호 점검 활동을 채택하고 있다. 한국인터넷진흥원(2016)의 설문조사 항목에서 정보보호 점검 활동은 빈도('정기적', '비정기적', '시행하지 않음')로 측정되었으며, 이외에도 정보보호 취약점 점검 항목, 보안패치 업데이트 현황, 백업 실시 여부 등이 조사되었다.

이를 토대로 할 때, 정보보호 점검 활동은 '정보보호 침해 사고를 사전에 예방하거나, 침해 사고 발생 이후 그에 대응하는 조치를 취하기 위해 정보보호 현황을 객관적으로 검토하는 활동'으로 정의될 수 있다.

2. 기업 정보보호 점검의 현황 및 효과

한국인터넷진흥원(2016)에 따르면, 정보 시스템에 대한 보안점검을 시행하는 사업체는 55.5%였으며, 정보시스템 보안 점검을 실시하는 사업체의 취약점 점검 항목(복수 응답)은 'PC 취약점'이 73.2%로 가장 높았다. 그 다음으로는 '네트워크 취약점' 점검이 43.2%, '서버 운영체제(OS) 취약점' 점검이 33.8%, 'Web 취약점' 점검이 18.3% 등인 것으로 나타났다.



[그림 4] 보안점검 실시 사업체 – 취약점 점검 항목(2015년)

출처: 한국인터넷진흥원(2016)

이외에도 정보보호 점검과 관련하여 자동 또는 수동으로 보안패치 업데이트를 실시하는 비율은 '외부와 연결된 서버'가 66.4%로 가장 높았으며, '직원 개인용 PC'가 59.2%, '정보보호시스템'이 55.8%, '로컬 서버'가 55.8% 순인 것으로 조사되었다.

3. 정보보호 점검에 관한 선행연구

현재까지 기업 실무에서 이루어지는 정보보호 점검 활동에 관한 연구는 많지 않다. 관련 선행연구로는 최주영 외(2015), 이근호(2014) 등이 있다.

일례로 최주영 외(2015)는 정보보호 사후대응 솔루션보다는, 사전 예방의 측면에서 정보 보안의 강화 방안을 연구하였다. 이때 주요 연구대상은 신규 정보통신서비스(SNS, 빅데이터, 클라우드 컴퓨팅, 사물인터넷 등)였으며, 한국인터넷진흥원이 2013년 발표한 『정보보호 사전점검』 권고제도의 활성화를 위한 개선방안을 마련하는 데에 주력하였다.

이 논문은 신규 정보통신서비스가 통상적으로 조직의 정보시스템과 연동되어 활용된다는 특성을 강조하며, 서비스 제공자와 이용자 모두 신규 정보통신서비스의 정보보안과 관련하여 보다 높은 수준의 안전성·신뢰성

을 요구하게 된다고 하였다.

이에 따라 기존의 『정보보호 사전점검』의 문제점을 지적하였다. 최주영 외(2015)에 따르면, 『정보보호 사전점검』의 내용상 점검 항목의 중복되고 있으며 이에 의한 정보보호 점검 이행 여부를 판단할 수 있는 산출물이 제대로 제시되지 않았다.

해당 연구는 이를 보완하기 위해 정보보호 시스템 운영단계에서뿐만 아니라 시스템의 개발단계에서부터 정보보호와 관련한 점검항목이 고려되어야 한다고 보았으며, 기존 자료에서 중복되어 있던 평가항목을 통합하여 간소화하는 방안을 제시하였다.

제 4 절 본 논문의 차별적 의의

이처럼 기업의 전반적인 정보보호 수준을 제고하기 위한 기업 정보보호 활동의 중요성이 거듭 제기되어왔지만, 정보보호 활동 수준을 점검하고 이에 영향을 미치는 요인을 규명한 선행연구는 여전히 미흡한 것이 실정이다.

일례로 정보보호 교육에 대한 연구는 기업이 아닌, 대학 및 대학원에서의 교육 과정에 대하여서만 집중적으로 이루어져왔다(김건우 외, 2016).

또한 기업 차원에서의 보안 점검 활동은 기업의 정보보호 현황을 객관적으로 진단하고, 그를 토대로 기업 정보보호 수준의 개선 방안을 제시하는 토대가 된다. 따라서 이는 기업의 정보보호 수준과 직결되는 요소라고 할 수 있다. 그럼에도 불구하고, 정보 침해 사고의 사전 예방 및 사후 조치로서의 정보보호 점검 활동에 대한 논의가 부족하다는 점이 지적되어왔다(최주영 외, 2015).

이에 본 논문은 기업의 전사적인 위험 관리 수단으로서 정보보호 교육과 정보보호 점검 활동이 중요한 의의를 갖는다고 전제하고, 이에 따라 정보보호 교육과 점검 활동을 종속변수로서 정의하고자 한다.

그리고 정보보호 체계 구축 수준을 독립변수로 선정하여, 해당 변수가 정보보호 교육과 정보보호 점검 활동 수준에 통계적으로 유의미한 영향력을 행사하는지를 검증하고자 한다.

'정보보호 체계'의 경우, 기존 연구와 한국인터넷진흥원(2016)의 설문조사 문항을 토대로 하여 정보보호 정책, 개인정보보호 정책, 정보보호 조직, 정보보호 관리자 인력, 정보보호 담당 인력, 정보보호 예산 등으로 그 범위를 한정하고자 한다.

이때 독립변수로 정보보호 체계를 선정한 근본적인 이유는, 정보보호 체계가 기업 차원에서 물적·인적 자원의 활용을 통해 직접 조작 및 제어할 수 있는 투입 요소(input)인 데에 있다. 즉, 정보보호 교육 및 점검 활동이 기업 차원에서 정책·조직·인력·예산 등을 투입함으로써 도출할

수 있는 산출 요소(output)라고 전제하였기 때문에 정보보호 체계를 독립변수, 정보보호 활동을 종속변수로 각각 설정한 것이다.

이러한 전제에 기초한 통계적 검증을 통해 본 논문은 기업 정보보호 활동의 전반적 수준을 높일 수 있도록 정부 차원에서 정책을 수립할 때, 어떤 분야에 보다 초점을 두고 관련 지원을 강화해야 하는지에 대한 시사점을 도출하고자 한다.

제 3 장 연구가설 및 연구설계

제 1 절 연구가설 및 모형

1. 연구문제

앞서 논의한 바와 같이, 이 논문은 기업의 정보보호 수준을 진단할 수 있는 변수로서 '정보보호 활동', 즉 정보보호 교육과 점검 활동을 선정하였다. 또한 이때 기업이 투입하는 정보보호 정책·조직·인력·예산 등에 의해 기업의 정보보호 활동 수준이 다르게 나타날 것이라는 가정을 하였다. 이를 토대로 도출한 연구문제는 다음과 같다.

"기업의 정보보호 체계 구축 수준에 따라 기업의 정보보호 활동 수준에 통계적으로 유의미한 차이가 존재하는가?"

2. 연구가설

이 논문에서는 위와 같은 연구문제 하에 크게 두 가지의 가설을 검증하고자 하며, 각 연구가설은 복수의 하위 가설들로 구성된다.

연구가설 1.

"기업의 정보보호 체계 구축 수준이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다."

- 기업의 정보보호 체계 구축 수준이 높을수록 기업의 정보보호 교육 수준이 높아질 것이다.

연구가설 1-1. 기업의 정보보호 정책 수립 여부가 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.

연구가설 1-2. 기업의 개인정보보호 정책 수립 여부가 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.

연구가설 1-3. 기업의 정보보호 조직 구축 여부가 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.

연구가설 1-4. 기업의 정보보호 관리자 인력의 활용이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.

연구가설 1-5. 기업의 정보보호 담당 인력의 활용이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.

연구가설 1-6. 기업의 정보보호 예산이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.

연구가설 2.

"기업의 정보보호 체계 구축 수준이 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다."

- 기업이 정보보호 체계 구축 수준이 높을수록 기업의 정보보호 점검 활동 수준이 높아질 것이다.

연구가설 2-1. 기업의 정보보호 정책 수립 여부가 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.

연구가설 2-2. 기업의 개인정보보호 정책 수립 여부가 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.

연구가설 2-3. 기업의 정보보호 조직 구축 여부가 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.

연구가설 2-4. 기업의 정보보호 관리자 인력의 활용이 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.

연구가설 2-5. 기업의 정보보호 담당 인력의 활용이 기업의 정보보호

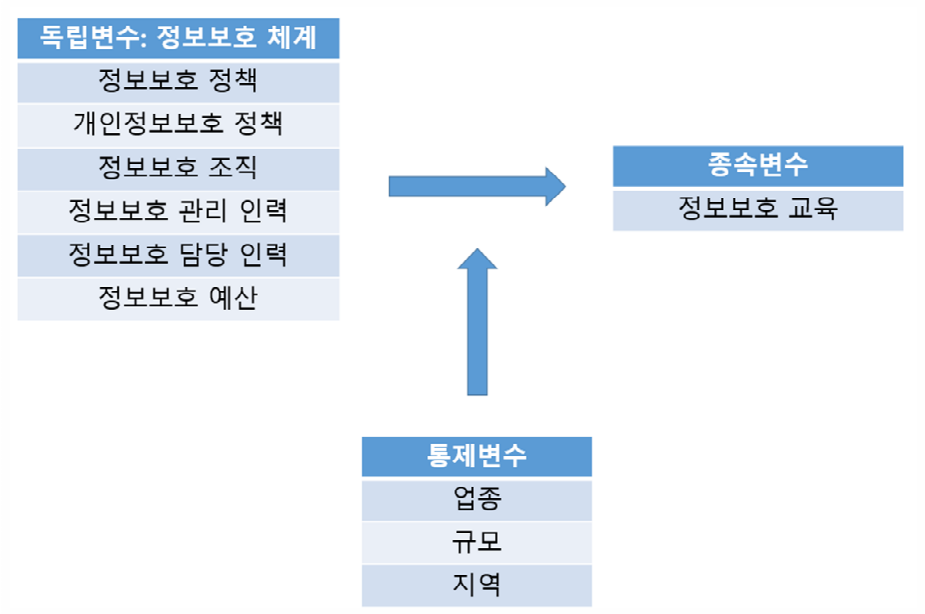
점검 활동 수준에 정(+)의 영향을 미칠 것이다.

연구가설 2-6. 기업의 정보보호 예산이 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.

3. 연구모형

이에 근거해 각 가설의 연구모형[5]을 도식화하면 다음의 그림과 같다.

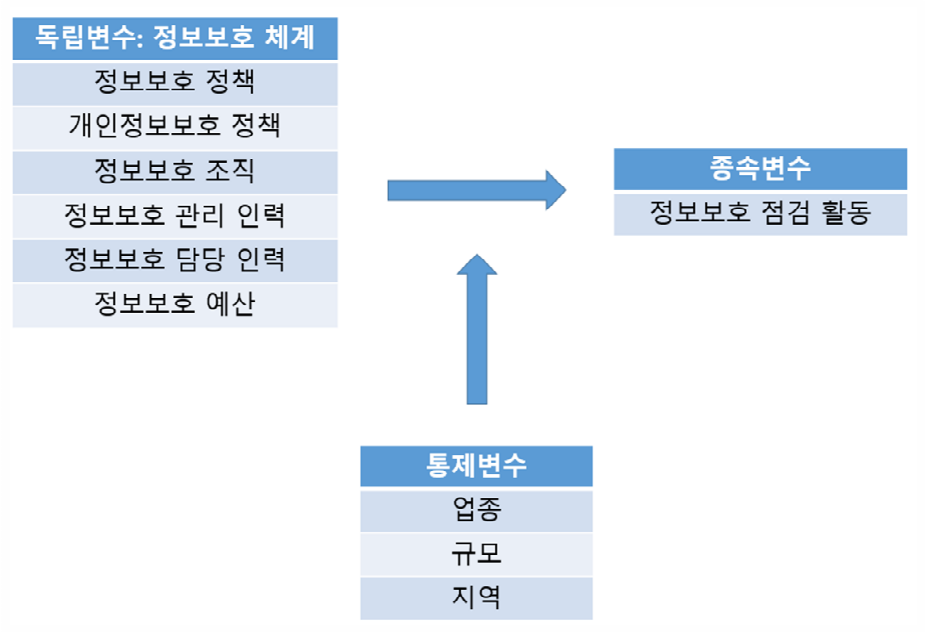
연구가설 1.



[그림 5-1] <연구가설 1>의 연구모형

5) 본 논문에서는 통제변수로 기업의 업종, 규모 및 소재 지역을 선정하였다. 이에 관한 자세한 내용은 아래에서 기술하도록 한다.

연구가설 2.



[그림 5-2] <연구가설 2>의 연구모형

제 2 절 자료 수집 및 분석 방법

1. 자료수집[6)]

이 논문에서는 2010년부터 2016년까지 이루어진 총 7차례의 민간기업 정보보호실태 조사의 원 데이터(raw data) 가운데 일부를 활용하고자 하며, 해당 설문조사는 정부(미래창조과학부) 주관 하에 한국인터넷진흥원이 전담하여 수행한 것이다. 이 조사는 정보통신망이용촉진 및 정보보호 등에 관한 법률 제 52조 제 3항과 통계법 제 18조에 근거하고 있다.

해당 설문조사의 주요 목적은, 빠르게 변화하는 인터넷 환경과 새로운 기술의 도입으로 인하여 사이버 세계의 위협이 현실세계로 확대되고 그 수준 또한 고도화되고 있는 현 시점에서 전 산업 분야에서의 정보보호 활동 및 대응 수준에 관한 진단을 내리기 위한 데에 있다.

이는 2001년 처음으로 국내 500개 기업체를 대상으로 실시된 이후 2016년에는 그 표본 수가 9,586개에 달하게 되었으며, 전문 조사원이 표본으로 선택된 사업체를 직접 방문하여 설문에 응답을 받는 형태로 시행되고 있다.

2016년 설문조사의 조사 모집단(Survey Population)은 종사자 수가 1인 이상이고 네트워크에 연결된 컴퓨터를 1대 이상 보유한 전국의 사업체였으며, 그 구체적인 현황[7)]은 다음의 [표 1]과 같다.

---

6) 한국인터넷진흥원(2016)에 근거하여 작성되었다.

7) 통계청의 『2014년 기준 전국사업체조사』 및 한국정보화진흥원의 『2015년 정보화 통계조사』에서 조사된 자료를 근거로 한다.

[표 1] 종사자 수 1명 이상 사업체 및 네트워크 구축 사업체 현황

구분	업종/규모	사업체 수	네트워크 구축 사업체 수
업종별	농림수산업(광업 포함)	5,197	2,714
	제조업	397,171	182,905
	건설업	128,215	59,478
	도매 및 소매업	997,120	447,380
	운수업	378,884	90,655
	숙박 및 음식점업	703,364	225,034
	출판/영상/방송 통신 및 정보서비스업	40,664	30,271
	금융 및 보험업	41,909	37,445
	부동산 및 임대업	141,186	70,824
	전문/과학 및 기술서비스업	96,376	66,982
	사업시설관리 및 사업지원 서비스업	50,785	29,660
	협회/단체/수리 및 기타 개인 서비스업	399,723	196,570
	기타	420,130	263,540
규모별	1~4명	3,097,951	1,222,598
	5~9명	412,960	259,704
	10~49명	245,904	182,646
	50~249명	39,968	34,919
	250~999명	3,458	3,108
	1,000명 이상	483	483
전체		3,800,724	1,703,458

표본 추출 시에는 다단계층화계통추출법을 사용하여 업종별·규모별로 2단 층화한 후 각 사업체들을 지역을 기준으로 정렬하여 계통추출을 시행하였다. 본 조사 결과 유효응답자 수는 9,586개로 나타났다. 이때 기업의 규모는 종사자 수를 기준으로 측정되었으며, 조사를 위한 업종 분류는 OECD의 분류 권고안과 한국표준산업 분류를 기준으로 하여 이루어졌다.

또 해당 설문조사는 국내 사업체의 정보보호 기반 및 환경, 침해사고 예방, 침해사고 경험 및 대응, 개인정보보호 관련 사항, 정보보호 인식, 신규서비스 정보보호 도입 및 투자 실태 등을 진단할 수 있는 문항들로 구성되어 있다.

논문 작성을 위하여 현재 확보된 총 7개의 원 데이터 파일 가운데 독립변수 및 종속변수를 측정하기 위해 선정한 문항의 유형·내용이 동일한 2015년과 2016년의 조사 결과 데이터를 일차적으로 선택하였고, 그 중에서도 세부적인 문항이 보다 많이 수록된 2016년의 데이터를 연구대상으로 삼고자 한다.

2. 자료 분석 방법

이 논문에서 채택하는 분석 방법론은 기술통계분석과 다중회귀분석이며, 분석 시 통계 프로그램인 SPSS 22.0을 활용한다.

먼저 연구 대상인 9,586개 기업의 일반적인 특성을 파악하기 위해 이에 대한 기술통계분석을 실시함으로써 업종·규모·소재지에 따른 기업의 현황을 제시하고자 한다.

이어서 <연구가설 1> 및 <연구가설 2>를 검증함에 있어서는 다중회귀분석 모형을 채택한다. 이 논문의 독립변수인 정보보호 체계는 정보보호 정책, 개인정보보호 정책, 정보보호 조직, 정보보호 관리자 인력, 정보보호 담당 인력, 정보보호 예산 등 복수의 변수로 구성되어 있으며, 그

척도의 특성 또한 상이하다.

따라서 종속변수인 정보보호 교육과 정보보호 점검 활동 각각에 미치는 독립변수의 영향력을 확인하기 위해 다중회귀분석 모형을 분석틀로 채택하는 것이다.

제 3 절 변수의 조작적 정의와 측정

1. 종속변수의 정의 및 측정

이 논문의 종속변수는 '정보보호 활동'이며, 이는 '정보보호 교육', '정보보호 점검 활동'으로 세분화된다.

(1) 정보보호 교육의 정의 및 측정

<연구가설 1>의 종속변수는 '정보보호 교육'이며, 이는 기업에서 1년간 실시한 정보보호 교육의 시간의 총계로 측정한다.

해당 설문조사에서는 [표 2-1]과 같이 CEO 등 경영진, 정보보호 책임자급 직원, 개인정보보호 책임자, 개인정보 취급자, IT 및 정보보호 실무자, 컴퓨터를 사용하는 일반 직원에 대하여 각각 정보보호 교육을 실시하고 있는지 여부와 연간 교육시간을 기입하도록 하였다.

[표 2-1] 종속변수의 정의 및 측정: 정보보호 교육

<table>
<tr><th>종속변수</th><th colspan="2">문항</th><th>변수 측정</th></tr>
<tr><td rowspan="13">정보보호
교육</td><td colspan="2">"귀사는 2015년 1년 간 다음의 임직원 대상 정보보호 교육(개인정보보호 포함)을 실시했습니까? (해당 교육의 교육시간과 교육평가 여부를 기입해 주십시오)"</td><td rowspan="13">각 교육대상에 대한 연간 교육시간의 총계를 측정</td></tr>
<tr><td rowspan="2">CEO 등
경영진</td><td>교육 실시 여부:
교육 실시, 미실시</td></tr>
<tr><td>교육 시간 기입</td></tr>
<tr><td rowspan="2">정보보호
책임자급 직원</td><td>교육 실시 여부:
교육 실시, 미실시</td></tr>
<tr><td>교육 시간 기입</td></tr>
<tr><td rowspan="2">개인정보보호
책임자</td><td>교육 실시 여부:
교육 실시, 미실시</td></tr>
<tr><td>교육 시간 기입</td></tr>
<tr><td rowspan="2">개인정보
취급자</td><td>교육 실시 여부:
교육 실시, 미실시</td></tr>
<tr><td>교육 시간 기입</td></tr>
<tr><td rowspan="2">IT 및
정보보호
실무자</td><td>교육 실시 여부:
교육 실시, 미실시</td></tr>
<tr><td>교육 시간 기입</td></tr>
<tr><td rowspan="2">컴퓨터
사용하는
일반 직원</td><td>교육 실시 여부:
교육 실시, 미실시</td></tr>
<tr><td>교육 시간 기입</td></tr>
</table>

이 논문에서는 이를 근거로 각 기업이 조직 구성원에 대하여 2015년 한 해 동안 실시한 교육 시간의 총합을 종속변수로 정의하여, 독립변수인 '정보보호 체계'가 이에 대하여 갖는 영향력을 확인하고자 한다.

(2) 정보보호 점검 활동의 정의 및 측정

다음으로 <연구가설 2>의 종속변수는 '정보보호 점검 활동'이며, 이는 [표 2-2]에서 볼 수 있듯 점검 빈도로 측정되었다. 이 논문에서는 정보보호 점검 활동을 측정하기 위하여, 응답된 빈도를 서열척도로 코딩하여 활용한다.

[표 2-2] 종속변수의 정의 및 측정: 정보보호 점검 활동

종속변수	문항	변수 측정
정보보호 점검 활동	"귀사는 정보시스템에 대한 보안점검(취약점 점검 등)을 어떻게 실시하십니까? 해당하는 항목을 체크해 주십시오." 1) 정기적(연 1회 이상) 2) 비정기적(연 1회 미만, 문제발생시 등) 3) 실시하지 않음	응답에 대하여 점수화하여 서열척도로 측정: 실시하지 않음=0 비정기적=1 정기적=2

2. 독립변수의 정의 및 측정

앞서 논의하였듯 본 연구에서는 선행 연구 결과와 설문조사 문항을 재구성하여 독립변수인 '정보보호 체계'를 크게 정보보호 정책, 개인정보보호 정책, 정보보호 조직, 정보보호 인력, 정보보호 예산의 영역으로 한정하여 측정하기로 한다.

이를 토대로 하여 이 논문은 기업의 정보보호 체계 구축 수준에 따라 기업의 정보보호 활동 수준에 통계적으로 유의미한 차이가 있는지를 검

증하고자 한다.

‘정보보호 체계’를 구성하는 세부 변수는 다음의 [표 3]과 같다.

[표 3] 독립변수의 정의 및 측정: 정보보호 체계

독립변수	문항	변수 측정
정보보호 정책	“귀사에는 공식 문서로 작성된 정보보호 정책이 있습니까?”	더미 변수로 측정: 예=1 아니오=0
개인정보보호 정책	“귀사에는 공식 문서로 작성된 개인정보보호 정책이 있습니까?”	더미 변수로 측정: 예=1 아니오=0
정보보호 조직	“귀사는 공식적인 정보보호(개인정보보호 포함) 조직을 운영하고 있습니까?”	더미 변수로 측정: 예=1 아니오=0
정보보호 관리자 인력	“귀사에는 다음의 책임자가 임명되어 있습니까?” 1) 정보관리책임자(CIO) 2) 정보보호최고책임자(CSO) 3) 개인정보관리책임자(CPO)	1)~3) 각각의 응답에 대하여 ’예=1’, ’아니오=0’으로 점수화하여 총계를 측정: <최저=0> CIO, CSO, CPO 중 어느 한 직급도 임명되어 있지 않을 경우 <최고=3> CIO, CSO, CPO가 모두 임명되어 있는 경우
정보보호	“귀사의 IT 인력 중 정보보호 담	응답에 대하여 다음과

담당 인력	당 인력이 차지하는 비중은 어떻게 됩니까?" 1) 1% 미만 2) 1%~3% 미만 3) 3%~5% 미만 4) 5%~7% 미만 5) 7%~10% 미만 6) 10% 이상 7) 정보보호 담당 인력 없음	같이 점수화하여 측정: 정보보호 담당 인력 없음=0 1% 미만=1 1%~3% 미만=2 3%~5% 미만=3 5%~7% 미만=4 7%~10% 미만=5 10% 이상=6
정보보호 예산	"귀사의 2015년도 1년간 IT 예산 총액 중 정보보호(개인정보보호 포함) 관련 예산 비중은 몇 퍼센트(%)였습니까?" 1) 1% 미만 2) 1~3% 미만 3) 3~5% 미만 4) 5~7% 미만 5) 7~10% 미만 6) 10% 이상 7) 정보보호 예산 없음	응답에 대하여 다음과 같이 점수화하여 측정: 정보보호 예산 없음=0 1% 미만=1 1~3% 미만=2 3~5% 미만=3 5~7% 미만=4 7~10% 미만=5 10% 이상=6

위의 표에서도 알 수 있듯 독립변수인 '정보보호 체계'를 측정하기 위한 문항은 그 척도의 특성과 각 문항이 구성하고 있는 개념이 상이하다. 따라서 독립변수가 종속변수에 미치는 영향력을 검증함에 있어서 세분화된 6개의 변수 각각의 영향력을 개별적으로 확인한다.

서열척도로 구성되어 있어 각 응답을 점수화하여 측정하는 변수의 경우, 점수가 높을수록 정보보호 체계의 수준이 상대적으로 높은 것으로 해석할 수 있다.

또한 위에서도 기술한 것과 같이 해당 설문조사에서 '정보보호'와 '개

인정보보호'가 독립적인 개념으로서 활용되었으나, '정보보호 조직' 변수에서 볼 수 있듯 일부 문항은 '정보보호'와 '개인정보보호'의 개념을 포괄하여 사용하기도 하였다. 이 논문에서도 기본적으로 기업의 '정보보호'를 '개인정보보호'를 포함하는 개념인 것으로 사용하되, 자료 분석 시에는 이러한 사항들을 명시하여 분석 결과의 왜곡이 없도록 한다.

3. 통제변수의 정의 및 측정

다음으로 통제변수는 업종, 규모, 지역이며, 그 구체적인 내용은 아래와 같다. 업종, 규모, 지역 외에도 조직 형태[8], 사업 형태[9]가 조사되었으나 원 데이터 파일에는 해당 내용이 없는 관계로 이는 통제변수에서 제외하고자 한다.

[표 4] 통제변수의 정의 및 측정: 업종, 규모, 지역

통제변수	문항	측정
업종	농림수산업 제조업 건설업 도매 및 소매업 운수업 숙박 및 음식점업 출판/영상/방송통신 및 정보서비스업 금융 및 보험업 부동산 및 임대업 전문/과학 및 기술서비스업 사업시설관리 및 사업지원 서비스업	더미 변수로 측정 (기타=0)

8) 조직 형태는 개인사업체, 회사법인, 회사 이외의 법인, 비법인단체로 분류된다.
9) 사업 형태는 단독사업체, 본사/본점 등, 공장/지사(점)/영업소의 항목을 통해 조사되었다.

	협회/단체/수리 및 기타 개인서비스업 기타	
규모[10)]	1) 1~4명 2) 5~9명 3) 10~49명 4) 50~249명 5) 250~499명 6) 500~999명 7) 1,000명 이상	연속 변수로 측정
지역	서울 부산 대구 인천 광주 대전 울산 세종 경기 강원 충북 전북 전남 경북 경남 제주	더미 변수로 측정 (서울=0)

10) 비정규직을 포함한 근로자 수를 기준으로 측정되었다.

제 4 장 연구결과의 분석 및 논의

제 1 절 연구대상의 일반적 특성 분석

1. 기업의 업종에 대한 기술통계량

본 논문의 연구대상이 된 기업, 즉 표본의 수는 총 9,586개였다. 그 가운데에서 기업의 업종[11]에 대한 기술통계량은 다음의 [표 5-1]과 같다.

전체 표본 가운데 농림수산업은 4.1%(394개), 제조업은 13.0%(1242개), 건설업은 7.9%(757개), 도매 및 소매업의 경우 10.1%(966개), 운수업은 7.1%(680개), 숙박 및 음식점업은 7.6%(731개), 출판/영상/방송통신 및 정보서비스업은 7.4%(711개), 금융 및 보험업의 경우 7.3%(699개), 부동산 및 임대업은 5.8%(560개), 전문/과학 및 기술서비스업은 8.0%(765개), 사업시설관리 및 개인 사업지원 서비스업의 경우 8.6%(823개), 협회/단체/수리 및 기타 개인서비스업은 6.3%(605개), 기타 업종은 6.8%(653개)의 분포를 보이고 있었다.

이로써 볼 때, 응답 업체의 업종 가운데 제조업이 가장 높은 비율(13.0%)을 차지하고 있음을 알 수 있으며, 이어 도매 및 소매업이 10.1%, 사업시설관리 및 개인 사업지원 서비스업이 8.6% 등으로 나타났다. 반면 표본 가운데 가장 낮은 비중을 차지하고 있는 업종은 농림수산업(4.1%)이었다.

11) 본 조사를 위한 업종 분류는 OECD의 분류 권고안과 한국표준사업 분류를 기준으로 하여 이루어졌다(한국인터넷진흥원, 2016).

[표 5-1] 기업의 업종에 대한 기술통계량

구분	내용	빈도(개)	비율(%)
업종	농림수산업	394	4.1
	제조업	1242	13.0
	건설업	757	7.9
	도매 및 소매업	966	10.1
	운수업	680	7.1
	숙박 및 음식점업	731	7.6
	출판/영상/방송통신 및 정보서비스업	711	7.4
	금융 및 보험업	699	7.3
	부동산 및 임대업	560	5.8
	전문/과학 및 기술서비스업	765	8.0
	사업시설관리 및 개인 사업지원 서비스업	823	8.6
	협회/단체/수리 및 기타 개인서비스업	605	6.3
	기타	653	6.8
합 계		**9,586**	**100**

2. 기업의 규모에 대한 기술통계량

다음으로 기업 규모에 관한 기술통계량을 살펴보도록 하겠다. 총 9,586개의 표본을 규모에 따라 분류하면 [표 5-2]와 같다. 본 설문조사에서 기업의 규모는 총 6개 집단으로 나뉘어 조사됐으며, 1~4명 규모의 기업이 20.6%(1972개), 5~9명 규모가 17.6%(1684개), 10~49명 규모가 24.6%(2361개), 50~249명 규모의 기업이 23.2%(2228명), 250~999명 규모가 11.5%(1099개), 그리고 1,000명 이상 규모의 기업이 2.5%(242개)의

분포를 보이고 있었다.

이를 토대로 볼 때, 응답 업체 가운데 10～49명 규모의 기업이 24.6%로 가장 많았으며, 50～249명(23.2%), 1～4명(20.6%), 5～9명(17.6%), 250～999명(11.5%), 1,000명 이상(2.5%) 규모의 기업이 뒤를 이었다.

[표 5-2] 기업의 규모에 대한 기술통계량

구분	내용	빈도(개)	비율(%)
규모	1~4명	1972	20.6
	5~9명	1684	17.6
	10~49명	2361	24.6
	50~249명	2228	23.2
	250~999명	1099	11.5
	1,000명 이상	242	2.5
합 계		**9,586**	**100**

3. 기업 소재 지역에 대한 기술통계량

이어 기업 소재 지역을 기준으로 기업을 분류하면 [표 5-3]과 같다. 전체 표본 가운데 서울 소재 기업이 27.6%(2647개), 부산 소재 기업이 6.5%(625개), 대구 소재 기업이 3.9%(371개), 인천 소재 기업이 4.7%(447개), 광주 소재 기업이 2.9%(277개), 대전 소재 기업이 3.4%(326개), 울산 소재 기업이 2.2%(212개), 세종 소재 기업이 0.3%(24개), 경기 소재 기업이 19.6%(1875개), 강원 소재 기업이 3.3%(315개), 충북 소재 기업이 3.4%(322개), 충남 소재 기업이 4.2%(398개), 전북 소재 기업이 3.1%(297개), 전남 소재 기업이 3.4%(328개), 경북 소재 기업이 4.3%(415개), 경남 소재 기업이 5.6%(541개), 제주 소재 기업이 1.7%(166개)를 구성하고 있

었다.

기업 소재 지역을 기준으로 할 경우, 서울이 27.6%로 표본 가운데 가장 큰 비율을 차지하고 있었으며, 경기가 19.6%로 그 뒤를 이었다. 이외의 지역은 대체적으로 비슷한 분포를 형성하고 있었으며, 세종 소재 기업이 0.3%, 제주 소재 기업이 1.7% 등으로 전체 기업 중 상대적으로 소수의 집단을 구성하고 있었다.

[표 5-3] 기업 소재 지역에 대한 기술통계량

구분	내용	빈도(개)	비율(%)
지역	서울	2647	27.6
	부산	625	6.5
	대구	371	3.9
	인천	447	4.7
	광주	277	2.9
	대전	326	3.4
	울산	212	2.2
	세종	24	0.3
	경기	1875	19.6
	강원	315	3.3
	충북	322	3.4
	충남	398	4.2
	전북	297	3.1
	전남	328	3.4
	경북	415	4.3
	경남	541	5.6
	제주	166	1.7

합 계	9,586	100

제 2 절 연구가설의 검증

1. 정보보호 체계 구축 수준이 기업의 정보보호 교육에 미치는 효과에 대한 검증

앞서 밝힌 바와 같이 <연구가설 1>은 정보보호 체계 구축 수준이 기업의 정보보호 교육에 미치는 효과를 검증하는 것을 내용으로 한다.

이때 독립변수인 정보보호 체계는 기업의 정보보호 정책 및 개인정보보호 정책, 정보보호 조직, 정보보호 관리자 인력 및 정보보호 담당 인력, 정보보호 예산 등의 변수로 구성된다.

한편 종속변수인 기업의 정보보호 교육 시간은 기업이 CEO를 비롯한 기업의 임원, 정보보호 관리자 인력과 일반 직원 등 조직원을 대상으로 시행한 연간(2015년) 정보보호 교육 시간의 총계로 측정된다. 이때 2015년에 이루어진 총 정보보호 교육 시간의 평균은 8.9360시간이었다.

<연구가설 1>을 검증하기 위해 SPSS 22.0를 이용하여 시행한 다중회귀분석 결과를 표로 요약하면 [표 6-1]과 같다. 이를 보면 독립변수인 정보보호 체계 가운데 정보보호 정책을 제외한 개인정보보호 정책, 정보보호 조직, 정보보호 관리자 인력 및 담당 인력, 정보보호 예산이 모두 종속변수인 정보보호 교육 시간에 통계적으로 유의미한 영향력을 행사하였음을 알 수 있다.

즉, 개인정보보호 정책(β=0.041, t=1.884 $p<0.1$), 정보보호 조직(β=0.055, t=3.045, $p<0.05$), 정보보호 관리자 인력(β=0.185, t=10.672, $p<0.01$), 정보보호 담당 인력(β=0.091, t=6.571, $p<0.01$), 정보보호 예산(β

=0.049, t=3.886, p<0.01)이 모두 종속변수인 정보보호 교육에 정(+)의 영향을 미치고 있었다.

이는 개인정보보호 정책이 수립되어 있을 때, 정보보호 조직이 구성되어 있을 때, 정보보호 관리자 인력(정보관리책임자, 정보보호최고책임자, 개인정보보호책임자)이 많이 임명되어 있을수록, 전체 IT 인력 가운데 정보보호 담당 인력의 비중이 높을수록, 전체 IT 예산 중 정보보호 예산의 비중이 높을수록 기업의 연간 정보보호 교육 시간이 증가함을 의미한다.

우선 개인정보보호 정책의 수립 여부가 정보보호 교육 수준에 정(+)의 영향을 미치는 것에 대해서는 다음과 같은 추론이 가능하다.

국민일보(2016), 조선일보(2016) 등에서 볼 수 있듯 최근 정보 유출의 피해 범위는 사회 전반으로 확대되고 있으며, 특히 기업 내부 고객의 개인정보를 표적으로 한 해킹이 증가하고 있는 추세이다. 이에 따라 김동우 외(2013), 박준경 외(2011) 등은 대규모화·지능화하고 있는 사이버 공격에 대응하기 위해 정보보호 활동을 강화함에 있어 기업 내부의 인적 자원에 대한 적극적인 교육 및 관리 활동을 강조하였다.

기업 차원에서는 개인정보보호 정책을 통해 고객의 정보를 보다 철저히 보호하기 위한 지침을 수립할 수 있으며, 이를 위해 기업 구성원을 대상으로 하는 정보보호 교육 등 정보보호 일반에 관한 세부 규정이 파생될 수 있다.

다음으로, 정보보호 조직이 있을 경우 정보보호 교육을 포함한 정보보호 업무 전반을 총괄하는 구심점이 형성될 수 있다. 따라서 정보보호 조직이 수립되어 있을 경우 정보보호 교육 등의 활동이 보다 활발히, 또 체계적으로 수행될 수 있다.

이와 더불어 정보보호 관리자 및 담당 인력이 충분히 투입될수록 정보보호 교육에 관한 사항을 지휘하고, 정보보호 교육을 수행할 수 있는 인적 토대가 마련되어 정보보호 교육의 수준이 높아질 수 있게 된다.

마지막으로, 이와 같은 전반적인 정보보호 활동은 기업의 관련 예산에 의해 뒷받침되므로 정보보호 예산의 비중이 높을수록 연간 정보보호 교

육 시간의 총계가 증가하는 것으로 해석할 수 있다.

한편, 정보보호 체계를 구성하는 다른 변수들에 비해 정보보호 관리자 인력이 정보보호 교육 수준에 미치는 영향력이 상대적으로 높게 나타났음을 알 수 있다(β=0.185, t=10.672, $p<0.01$). 이는 정보보호 관리자가 다수 임명되어 있을수록 이들이 정보보호 교육을 포함한 일련의 활동을 스스로의 과업으로 인식하여, 보다 적극적으로 정보보호를 위한 기술적·관리적 조치를 취할 수 있기 때문일 것이다.

이와 같은 결과는 기존 연구에서도 그 근거를 찾을 수 있다. 김지수 외(2012)는 조직 내 정보보호최고책임자(CISO)의 역할인식이 기업 정보보호 성과에 미치는 효과를 검증하였다. 해당 연구 결과, 조직 내 정보보호최고책임자의 역할 인식—'지적자산 가치 평가자', '정보통신 인프라의 전략적 활용 촉진자', '변화 관리자', '정보보안, 전략, 정책, 표준기술 확보자'로서의 역할 인식—이 기업 정보보호 대책 활동에 정(+)의 영향을 주는 것으로 확인된 바 있다.

다음으로 통제변수인 업종, 규모 및 지역에 관해 간략히 살펴보겠다. 첫번째로 업종은 '기타'를 기준으로 하여 더미 변수로 측정되었는데, 기타 업종과 비교하였을 때, 정보보호 교육에 대한 영향력이 큰 것으로 나타난 업종 변수는 금융 및 보험업(β=0.152, t=12.078, $p<0.01$)이었다.

금융 및 보험업의 경우 기업 내에서 고객의 금융 자산, 병력 등과 같은 민감한 정보가 보다 자세히 다뤄지게 되고, 이러한 정보가 유출될 시에는 기업 차원에서 금전적인 손실이 발생함은 물론, 조직 이미지에도 큰 타격이 있을 수 있다. 이로 인해 금융 및 보험업에서 기타 업종에 비해 정보보호 교육 등 관련 활동의 수준이 높게 나타나는 것으로 해석할 수 있다.

실제로 앞서 주지한 바와 같이, 2014년에 KB국민카드, NH농협은행, 롯데카드 등 3개 카드사에서 대량의 고객 정보가 유출되었으며, 이에 대해 법원은 롯데카드사가 개인정보 유출 피해자 3,577명에게 각각 10만원씩 배상할 책임이 있다는 판결을 내리기도 하였다(조선 비즈, 2017). 이러한 사례를 통해 보았을 때, 금융 및 보험업에서 특히 정보보안이 강조

될 수밖에 없으며 정보 유출 사태가 발생할 경우 소송 및 계약 해지 등으로 인해 기업 차원에서 큰 금전적 손실을 입게 됨을 알 수 있다.

한편 규모는 연속변수로 측정되었으며, 규모가 클수록 통계적으로 유의미하게 정보보호 교육 시간의 총계가 증가함을 알 수 있었다(β=0.071, t=6.252, p<0.01). 이는 일반적으로 기업의 규모가 클수록 정보보호 교육을 위한 조직, 인력, 예산 등이 작은 규모의 기업에 비해 보다 광범위하게 투입될 수 있기 때문인 것으로 보인다.

마지막으로 기업의 소재 지역 또한 더미 변수로 투입되었는데, 그 결과 서울에 비해 대구(β=0.037, t=3.993, p<0.01), 대전(β=0.046, t=5.010, p<0.01), 울산(β=0.029, t=3.214, p<0.05), 경기(β=0.023, t=2.111, p<0.05), 충북(β=0.034, t=3.661, p<0.01), 충남(β=0.038, t=3.965, p<0.01), 제주(β=0.018, t=2.007, p<0.05)에 근거지를 둔 기업의 연간 정보보호 교육 시간이 더 많은 것으로 나타났다.

[표 6-1] 정보보호 교육의 회귀분석 결과

변수 구분		회귀계수 (β) 추정치	표준오차 (Standard Error)	t-값	유의확률
독립변수	정보보호 정책 (더미)	0.030	0.938	1.426	0.154
	개인정보보호 정책 (더미)	0.041	0.966	1.884	0.060
	정보보호 조직 (더미)	0.055	0.797	3.045	0.002
	정보보호 관리자 인력	0.185	0.294	10.672	0.000
	정보보호 담당 인력	0.091	0.216	6.571	0.000
	정보보호 예산	0.049	0.206	3.886	0.000

통제변수	농림수산업	0.018	1.242	1.613	0.107
	제조업	-0.012	0.925	-0.831	0.406
	건설업	-0.022	1.034	-1.734	0.083
	도매 및 소매업	0.015	0.969	1.096	0.273
	운수업	-0.004	1.052	-0.331	0.740
	숙박 및 음식점업	-0.009	1.033	-0.693	0.489
	출판/영상/방송 통신 및 정보서비스업	-0.011	1.036	-0.862	0.389
	금융 및 보험업	0.152	1.054	12.078	0.000
	부동산 및 임대업	-0.009	1.102	-0.742	0.458
	전문/과학 및 기술서비스업	0.002	1.010	0.180	0.857
	사업시설관리 및 사업지원 서비스업	-0.022	0.999	-1.708	0.088
	협회/단체/수리 및 기타 개인 서비스업	-0.015	1.081	-1.211	0.226
	규모	0.071	0.179	6.252	0.000
	부산	0.011	0.847	1.150	0.250
	대구	0.037	1.059	3.993	0.000
	인천	0.007	0.972	0.793	0.428
	광주	-0.008	1.197	-0.850	0.395
	대전	0.046	1.109	5.010	0.000

	울산	0.029	1.352	3.214	0.001
	세종	0.004	3.856	0.415	0.678
	경기	0.023	0.585	2.111	0.035
	강원	0.004	1.134	0.459	0.647
	충북	0.034	1.128	3.661	0.000
	충남	0.038	1.033	3.965	0.000
	전북	0.014	1.173	1.482	0.138
	전남	-0.009	1.145	-0.947	0.344
	경북	-0.001	1.023	-0.083	0.934
	경남	0.015	0.911	1.587	0.112
	제주	0.018	1.518	2.007	0.045

1) n=9,586
2) 제외된 변수: (업종더미)기타, (지역더미)서울

한편, 정보보호 교육이 조직 구성원에 미치는 영향력이 모든 직급에서 동일하게 나타날 것이라고 보기는 어렵다. 일반적으로 CEO 등 경영진, 정보보호 책임자급 직원 및 정보보호 관련 실무자에 대해 수행하는 교육의 효과가 일반 직원에 대한 교육의 영향력보다 클 것이라 가정해볼 수 있다. 통상적으로 CEO 등 경영진을 비롯한 정보보호 관리자·실무자가 조직 전반의 정보보호 대책 활동을 결정할 수 있는, 보다 강력한 권한을 지니게 되기 때문이다.

이와 같은 문제의식 하에 CEO 등 경영진, 정보보호 책임자급 직원, 정보보호 책임자, 개인정보 취급자, IT 및 정보보호 실무자에 대해 시행한 연간 정보보호 교육 시간의 총계[12]와 일반 직원이 받은 정보보호 교육 시간의 총계에 대하여 별도의 회귀분석을 시행해보았다.

12) CEO 등 경영진, 정보보호 책임자급 직원, 정보보호 책임자, 개인정보 취급자, IT 및 정보보호 실무자를 아울러 편의상 '경영진 및 정보보호 인력'으로 칭하기로 한다.

검증 결과는 아래의 [표 6-2][13]를 통해 제시하였으며, 독립변수가 경영진 및 정보보호 인력에 대한 정보보호 교육과 일반 직원에 대한 정보보호 교육에 미치는 영향력의 양상이 서로 다르게 나타났다.

먼저 경영진 및 정보보호 인력의 교육 시간에 정(+)의 영향을 미치는 변수는 정보보호 조직(β=0.045, t=2.481, p<0.05), 정보보호 관리자 인력(β=0.205, t=11.800, p<0.01), 정보보호 담당 인력(β=0.099, t=7.145, p<0.01), 정보보호 예산(β=0.058, t=4.601, p<0.01)인 것으로 나타났다.

이는 정보보호 조직이 구축되어 있을 때, 정보보호 관리자 인력이 다수 임명되어 있을 때, IT 인력 가운데 정보보호 담당 인력의 비중이 높을수록, IT 예산 중 정보보호 관련 예산의 비중이 높을수록 경영진 및 정보보호 인력에 대한 정보보호 교육 시간이 증가함을 뜻한다.

이때 특히 정보보호 관리자 인력이 경영진 및 정보보호 인력의 교육 시간에 미치는 상대적인 영향력이 큰 것으로 드러났다(β=0.205, t=11.800, p<0.01). 이는 기업 경영진 및 정보보호 관련 인력에 대한 교육을 수행하는 데에 있어 정보관리책임자, 정보보호최고책임자, 개인정보관리책임자 등 정보보호 관리자의 추진 의지가 가장 강력한 동인이 되기 때문인 것으로 해석할 수 있다.

한편, 일반 직원의 정보보호 교육 시간 총계에 정(+)의 영향을 미치는 변수는 정보보호 정책(β=0.055, t=2.468, p<0.05), 개인정보보호 정책(β=0.080, t=3.521, p<0.01), 정보보호 조직(β=0.089, t=4.759, p<0.01), 정보보호 관리자 인력(β=0.070, t=3.898, p<0.01), 정보보호 담당 인력(β=0.042, t=2.899, p<0.05)이었다.

즉, 정보보호 정책이 있을 때, 개인정보보호 정책이 있을 때, 정보보호 조직이 구축되어 있을 때, 정보보호 관리자 인력이 임명되어 있을 때, IT 인력 가운데 정보보호 담당 인력의 비중이 높을수록 일반 직원에 대한 정보보호 교육 시간의 총계가 통계적으로 유의미하게 증가하는 것이다.

그리고 일반 직원의 정보보호 교육 시간에 대하여서는 정보보호 조직

13) 이 표에서는 회귀계수(β) 추정치와 t-값을 제시한다.
(* :p<0.1, **: p<0.05, ***: p<0.01)

(β=0.089, t=4.759, p<0.01)과 개인정보보호 정책(β=0.080, t=3.521, p<0.01) 등의 영향력이 상대적으로 큰 것으로 나타났다. 이는 곧 일반 직원에 대한 정보보호 교육을 수행함에 있어서는 정보보호 관리자의 의지보다는, 기업 내의 법·제도 등 의무적인 규정이 가장 큰 영향력을 행사함을 뜻한다.

[표 6-2] 정보보호 교육의 회귀분석 결과: 경영진 및 정보보호 인력과 일반 직원의 분류

변수 구분		경영진 및 정보보호 인력		일반 직원	
		회귀계수 (β) 추정치	t-값	회귀계수 (β) 추정치	t-값
독립변수	정보보호 정책 (더미)	0.024	1.103	0.055**	2.468**
	개인정보보호 정책 (더미)	0.031	1.395	0.080***	3.521***
	정보보호 조직 (더미)	0.045**	2.481**	0.089***	4.759***
	정보보호 관리자 인력	0.205***	11.800***	0.070***	3.898***
	정보보호 담당 인력	0.099***	7.145***	0.042**	2.899**
	정보보호 예산	0.058***	4.601***	0.002	0.168
통제변수	농림수산업	0.013	1.160	0.037**	3.151**
	제조업	-0.016	-1.129	0.008	0.560
	건설업	-0.023*	-1.820*	-0.014	-1.037
	도매 및 소매업	0.008	0.564	0.043**	3.066**
	운수업	-0.009	-0.747	0.019	1.446

	숙박 및 음식점업	-0.012	-0.949	0.007	0.498
	출판/영상/방송 통신 및 정보서비스업	-0.016	-1.259	0.012	0.944
	금융 및 보험업	0.138***	10.902***	0.190***	14.505***
	부동산 및 임대업	-0.012	-0.990	0.005	0.429
	전문/과학 및 기술서비스업	0.001	0.053	0.009	0.668
	사업시설관리 및 사업지원 서비스업	-0.026**	-2.002**	-0.002	-0.160
	협회/단체/수리 및 기타 개인 서비스업	-0.017	-1.442	0.000	-0.017
	규모	0.065***	5.751***	0.083***	7.066***
	부산	0.008	0.818	0.023**	2.290**
	대구	0.030**	3.234**	0.062***	6.321***
	인천	0.006	0.626	0.013	1.320
	광주	-0.006	-0.679	-0.013	-1.386
	대전	0.044***	4.769***	0.048***	5.003***
	울산	0.026**	2.854**	0.039***	4.057***
	세종	0.002	0.254	0.009	0.994
	경기	0.022**	2.023**	0.023**	2.051**
	강원	0.003	0.367	0.007	0.744
	충북	0.028**	3.036**	0.053***	5.502***
	충남	0.034***	3.618***	0.045***	4.600***
	전북	0.014	1.469	0.012	1.237
	전남	-0.008	-0.818	-0.013	-1.292

	경북	0.001	0.099	-0.008	-0.816
	경남	0.009	0.911	0.041***	4.054***
	제주	0.015	1.607	0.031**	3.250**

1) n=9,586
2) * :p<0.1, **: p<0.05, ***: p<0.01
3) 제외된 변수: (업종더미)기타, (지역더미)서울

2. 정보보호 체계 구축 수준이 기업의 정보보호 점검 활동에 미치는 효과에 대한 검증

다음으로 <연구가설 2>의 검증 결과를 살펴보겠다. <연구가설 2>의 독립변수는 <연구가설 1>과 마찬가지로 기업의 정보보호 체계이다.

한편 종속변수는 정보보호 점검 활동인데 이는 빈도—'정기적(연 1회 이상)', '비정기적(연 1회 미만, 문제발생시)', '실시하지 않음'—로 측정되었으며, 회귀분석을 위하여 각 빈도 문항에 대한 응답을 서열척도로 코딩하였다.

회귀분석 결과, 정보보호 체계를 구성하는 하위 변수 모두 정보보호 점검 활동에 정(+)의 영향을 미치는 것으로 파악되었다.

다시 말해, 정보보호 정책(β=0.094, t=4.965 p<0.01), 개인정보보호 정책(β=0.139, t=7.157 p<0.01), 정보보호 조직(β=0.096, t=6.091, p<0.01), 정보보호 관리자 인력(β=0.110, t=7.158, p<0.01), 정보보호 담당 인력(β=0.034, t=2.801, p<0.05), 정보보호 예산(β=0.057, t=5.129, p<0.01)의 모든 변수가 정보보호 점검 활동에 정(+)의 영향을 미치고 있었다.

이는 곧 정보보호 정책이 수립되어 있을 때, 개인정보보호 정책이 수립되어 있을 때, 정보보호 조직이 구성되어 있을 때, 정보보호 관리 인력이 다수 임명되어 있을수록, 전체 IT 인력 가운데 정보보호 담당 인력의 비중이 높을수록, 전체 IT 예산 중 정보보호 예산의 비중이 높을수록 기

업의 연내 정보보호 점검 빈도가 증가함을 뜻한다.

먼저 기업의 정보보호 정책 및 개인정보보호 정책의 수립 여부가 정보보호 점검 활동에 정(+)의 영향을 미치는 것에 관해서는 다음과 같은 설명이 가능하다.

이근호(2014)에 의하면, 정보 시스템의 안전성을 담보하기 위해서는 정보통신 서비스의 구축·설계 단계에서부터 정보보호 취약점 분석 등을 통해 사전에 시스템의 취약점이 제거되어야 한다. 그리고 정보 시스템의 점검 활동과 관련하여 정보보호 대책이 수립 및 적용되었는지에 대해서도 지속적인 확인이 필요하다.

<연구가설 2>의 검증을 위해 활용한 설문 문항에서는 정보 시스템의 실제 운영 단계에서 정기적인 점검 활동이 이루어지고 있는지에 대해서만 묻고 있다. 그러나 이근호(2014) 등에서 알 수 있듯 정보보호 점검 활동은 정보 시스템의 개발 단계, 관련 정책의 수립 및 활용, 시스템의 실제 운영 및 사후 점검 등 복수의 단계에 걸친 프로세스를 통해 수행된다. 또한 정보보호 점검 활동은 각 단계에 따라 시스템 설계자, 정보보호 담당자, 보안 전문가 등 여러 분야의 조직원이 관여함으로써 이루어지는 복잡한 과정이다.

그렇기 때문에 기업 차원에서 거시적인 정책을 수립하여 정보보호 점검 활동에 관한 일관적인 방향성과 세부적인 지침을 마련할 필요가 있으며, 관련 정책이 마련되어 있을 때 그에 의하여 보다 체계적인 정보보호 점검 활동이 이루어질 수 있다.

이 과정에서 정보보호 조직은 정보보호 점검 등 기업의 정보보호 활동을 실질적으로 수행하는 구심점으로서의 역할을 한다. 따라서 정보보호 조직의 존재 여부가 정보보호 점검 활동에 정(+)의 영향력을 행사할 수 있는 것이다. 이는 <연구가설 1>의 결과와도 유사한 해석이다.

한편, 정보보호 관리자 인력이 많이 임명되어 있을수록 보안 점검 활동의 빈도 또한 증가하였다. 이는 정보보호 관리자가 기업의 정보보호 수준을 제고하는 과정에서, 침해 사고의 위험성을 예방하고 사후 조치를 취하기 위한 수단으로 정보보호 점검 작업을 채택했기 때문인 것으로 가

정해볼 수 있다. 앞서 언급하였듯 김지수 외(2012)는 기업 정보보호 관리자의 역할인식이 정보보호 대책 활동에 정(+)의 영향을 미친다는 사실을 입증한 바 있다.

이러한 관리자의 방침 하에 정보보호 담당 인력은 실무 상 정보보호 점검 활동을 지휘 혹은 수행하는 주체가 된다. 또한, 정보보호 점검 등 일련의 정보보호 대책 활동을 추진하기 위해서는 관련 예산이 확보되어야 한다. 그렇기 때문에 IT 인력 가운데 정보보호 담당 인력의 비중이 높을수록, IT 예산 가운데 정보보호 예산의 비중이 높을수록 정보보호 점검 활동의 빈도 또한 늘어나게 되는 것으로 볼 수 있다.

정보보호 점검 활동과 관련하여서는, 개인정보보호 정책(β=0.139, t=7.157 $p<0.01$)과 정보보호 관리자 인력(β=0.110, t=7.158, $p<0.01$)의 영향력이 비교적 큰 것으로 나타났다.

다음으로 통제 변수 중 업종의 측면에서는, 기타 업종과 견주었을 때 제조업(β=0.078, t=6.215, $p<0.01$), 건설업(β=0.025, t=2.236, $p<0.01$), 도매 및 소매업(β=0.046, t=3.878, $p<0.01$), 운수업(β=0.018, t=1.652, $p<0.1$), 출판/영상/방송 통신 및 정보서비스업(β=0.062, t=5.656, $p<0.01$), 금융 및 보험업(β=0.114, t=10.232 $p<0.01$), 전문/과학 및 기술서비스업(β=0.049, t=4.448, $p<0.01$), 협회/단체/수리 및 기타서비스업(β=0.020, t=1.912, $p<0.1$)이 정보보호 점검 활동에 상대적으로 큰 영향력을 미치는 것으로 드러났다.

이에서도 금융 및 보험업(β=0.114, t=10.232, $p<0.01$)의 정보보호 점검 활동의 수준이 비교적 높은 것으로 나타났다. 이는 앞서 정보보호 교육과 관련하여 논의한 것과 같이 금융 및 보험업의 경우 타 업종에 비해 고객의 민감한 정보를 보다 많이 다루게 되며, 정보 유출 사고가 기업의 조직적 가치 및 존속 여부에 직접적인 타격을 입히기 때문인 것으로 해석될 수 있다.

기업은 정보보호 점검 활동을 통해 사전에 정보 유출 등의 사고 발생 가능성을 줄일 수 있고, 침해 사고 발생 이후에도 사후 점검을 수행함으로써 향후 정보보호 활동을 강화하는 근거로 활용할 수 있다.

한편 규모가 클수록 통계적으로 유의미하게 정보보호 점검 빈도가 높아짐을 알 수 있었다(β=0.183, t=18.169, p<0.01). 이 또한 기업의 규모가 커질수록 통상적으로 정보보호 점검 등 일련의 정보보호 조치를 위한 조직, 인력, 예산 등이 상대적으로 폭넓게 투입될 수 있기 때문인 것으로 파악된다.

마지막으로 기업의 근거지에 관하여서는, 분석 결과 서울에 비해 대전(β=0.036, t=4.407, p<0.01), 세종(β=0.018, t=2.347, p<0.05), 경기(β=0.016, t=1.652, p<0.1), 충북(β=0.079, t=9.574, p<0.01), 충남(β=0.067, t=8.005, p<0.01)에 소재한 기업의 정보보호 점검 빈도가 비교적 더 높은 것으로 나타났다.

[표 7] 정보보호 점검 활동의 회귀분석 결과

변수 구분		회귀계수 (β) 추정치	표준오차 (Standard Error)	t-값	유의확률
독립변수	정보보호 정책 (더미)	0.094	0.029	4.965	0.000
	개인정보보호 정책 (더미)	0.139	0.030	7.157	0.000
	정보보호 조직 (더미)	0.096	0.024	6.091	0.000
	정보보호 관리자 인력	0.110	0.009	7.158	0.000
	정보보호 담당 인력	0.034	0.007	2.801	0.005
	정보보호 예산	0.057	0.006	5.129	0.000
통제변수	농림수산업	-0.014	0.038	-1.406	0.160
	제조업	0.078	0.028	6.215	0.000
	건설업	0.025	0.032	2.236	0.025

	도매 및 소매업	0.046	0.030	3.878	0.000
	운수업	0.018	0.032	1.652	0.099
	숙박 및 음식점업	-0.039	0.032	-3.477	0.001
	출판/영상/방송 통신 및 정보서비스업	0.062	0.032	5.656	0.000
	금융 및 보험업	0.114	0.032	10.232	0.000
	부동산 및 임대업	-0.037	0.034	-3.548	0.000
	전문/과학 및 기술서비스업	0.049	0.031	4.448	0.000
	사업시설관리 및 사업지원 서비스업	0.000	0.031	0.034	0.973
	협회/단체/수리 및 기타 개인 서비스업	0.020	0.033	1.912	0.056
	규모	0.183	0.005	18.169	0.000
	부산	-0.018	0.026	-2.099	0.036
	대구	-0.012	0.032	-1.451	0.147
	인천	0.010	0.030	1.141	0.254
	광주	-0.010	0.037	-1.182	0.237
	대전	0.036	0.034	4.407	0.000
	울산	0.000	0.041	0.033	0.973
	세종	0.018	0.118	2.347	0.019
	경기	0.016	0.018	1.652	0.099

	강원	-0.008	0.035	-0.993	0.321
	충북	0.079	0.035	9.574	0.000
	충남	0.067	0.032	8.005	0.000
	전북	0.010	0.036	1.175	0.240
	전남	-0.008	0.035	-0.925	0.355
	경북	-0.001	0.031	-0.137	0.891
	경남	0.001	0.028	0.066	0.948
	제주	-0.026	0.047	-3.208	0.001

1) n=9,586

2) 제외된 변수: (업종더미)기타, (지역더미)서울

제 5 장 결 론

제 1 절 연구결과의 요약

이상에서 살펴본 이 논문의 연구결과는 [표 8]에 정리되어 있다.

먼저 <연구가설 1>과 관련하여서는, 기업의 개인정보보호 정책이 수립되어 있을 때, 정보보호 조직이 구축되어 있을 때, 정보보호 관리자 인력이 많이 임명되어 있을수록, IT 인력 중 정보보호 담당 인력의 비중이 높을수록, IT 예산 가운데 기업 정보보호 예산의 비중이 높을수록 연간 정보 교육시간의 총계가 많은 것으로 나타났다.

이에 대해서는 다음과 같은 해석이 가능하다. 정보보호 교육의 경우, 관련 선행연구들에 의해 그 중요성이 지속적으로 강조되어 오고 있다. 오늘날 사이버 공격은 정보 침해 방식이나 피해 범위의 측면에서 점차 진화하고 있으며, 기업 차원에서는 보다 전사적인 대응책을 마련해 그 피해를 예방 및 복구해야 한다. 이때 기업은 내부 조직원들에게 적극적으로 정보보호 교육·훈련의 기회를 제공함으로써 이들이 기업 내 정보보호 프로세스를 깊이 이해할 수 있도록 해야 하며, 이를 통해 궁극적으로 기업의 정보보호 수준이 제고될 수 있을 것이다.

이를 위해 기업은 개인정보보호 정책 등 관련 정책을 수립함으로써 정보보호 교육 등에 관한 의무사항을 규정하여 정보보호 교육 시간을 확보할 수 있다. 또한 정보보호 교육을 수행하는 공식적인 조직을 두고, 관련 실무를 담당할 정보보호 관리자 및 담당 인력을 임명함으로써 정보보호 교육이 원만히 이루어지도록 할 수 있다. 이때 기업은 이 과정에 필요한 예산을 일정 비율 확보함으로써 계획된 정보보호 교육 시간을 달성할 수 있다.

다음으로 <연구가설 2>의 검증 결과, 정보보호 정책이 수립되어 있을 때, 개인정보보호 정책이 수립되어 있을 때, 정보보호 조직이 구축되어

있을 때, 정보보호 관리자 인력이 많이 임명되어 있을수록, IT 인력 중 정보보호 담당 인력의 비중이 높을수록, IT 예산 가운데 기업 정보보호 예산의 비중이 높을수록 정보보호 점검 활동의 빈도가 높아지는 것을 확인할 수 있었다.

기업의 정보보호 점검 활동은 정보 시스템의 개발 단계, 관련 정책의 수립 및 활용, 시스템의 실제 운영 및 사후 점검 등의 프로세스 전반에 걸쳐 수행된다. 그리고 이때 각 단계에는 조직 내 여러 분야의 전문가 및 업무 담당자가 참여하게 된다.

따라서 기업은 정보보호 및 개인정보보호 정책을 수립하여 관련 규정을 마련함으로써 보안 점검 프로세스를 체계적으로 관리할 수 있게 된다. 그러므로 관련 정책의 수립 여부가 정보보호 점검 활동에 정(+)의 영향을 미칠 수 있다.

또한, <연구가설 1>에서와 마찬가지로 기업 내의 정보보호 조직이 점검 계획 및 방법론을 수립하는 등 정보보호 점검 활동을 총괄하는 구심점이 될 수 있다. 이때 정보보호 관리자와 담당 인력이 점검 실무를 추진하는 주체가 된다. 그렇기 때문에 정보보호 조직 및 인력이 정보보호 점검 빈도에 정(+)의 영향을 미치게 되는 것으로 해석할 수 있다.

정보보호 점검 활동은 사전·사후 점검 등 그 범위가 넓고 여러 프로세스에 걸쳐 수행되는 만큼 많은 비용을 수반하게 되는 작업이다. 따라서 IT 예산 가운데 정보보호 관련 예산의 비중이 높을수록 정보보호 점검 활동의 빈도 또한 증가하게 된다고 볼 수 있겠다.

한편 <연구가설 1>, <연구가설 2> 모두에서 다른 변수들에 비해 정보보호 관리자 인력이 종속변수에 미치는 영향력이 상대적으로 큰 것으로 나타났다.

앞서 언급하였듯 이와 같은 분석결과는, 유사한 연구를 수행한 김지수 외(2012) 등에 의해 뒷받침될 수 있다. 김지수 외(2012)에 따르면 조직내 정보보호최고책임자(CISO)의 역할인식이 정보보호 대책 활동에 정(+)의 영향을 미친다.

기업 내 정보보호 관리자는 기업의 정보보호 수준을 제고하는 것을 주

요 과업으로 삼는 조직원이다. 그렇기 때문에 이들은 기업의 정보보호 대책 활동을 수행하는 데에 필요한 기술적·관리적 조치를 총괄 및 지휘할 수 있는 권한을 지닌다. 따라서 정보보호 관리 인력의 임명 및 활용 여부는 기업의 정보보호 활동 수준과 직결되는 요인이라 할 수 있겠다.

[표 8] 연구결과의 요약

연구 가설		검증 결과
연구가설 1.	**기업의 정보보호 체계 구축 수준이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.** **- 기업의 정보보호 체계 구축 수준이 높을수록 기업의 정보보호 교육 수준이 높을 것이다.**	
연구가설 1-1.	기업의 정보보호 정책 수립 여부가 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.	기각
연구가설 1-2.	기업의 개인정보보호 정책 수립 여부가 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 1-3.	기업의 정보보호 조직 구축 여부가 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 1-4.	기업의 정보보호 관리자 인력의 활용이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 1-5.	기업의 정보보호 담당 인력의 활용이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 1-6.	기업의 정보보호 예산이 기업의 정보보호 교육 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 2.	**기업의 정보보호 체계 구축 수준이 기업의 정보보호 점검 활동에 정(+)의 영향을 미칠 것이다.**	

	- 기업이 정보보호 체계 구축 수준이 높을수록 기업의 정보보호 점검 활동 수준이 높을 것이다.	
연구가설 2-1.	기업의 정보보호 정책 수립 여부가 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 2-2.	기업의 개인정보보호 정책 수립 여부가 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 2-3.	기업의 정보보호 조직 구축 여부가 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 2-4.	기업의 정보보호 관리자 인력의 활용이 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 2-5.	기업의 정보보호 담당 인력의 활용이 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.	채택
연구가설 2-6.	기업의 정보보호 예산이 기업의 정보보호 점검 활동 수준에 정(+)의 영향을 미칠 것이다.	채택

제 2 절 연구의 정책적 함의 및 한계점

이상과 같이 이 연구는 정보보호 체계 구축 수준이 정보보호 교육 및 정보보호 점검 활동에 미치는 영향을 살폈으며, 이를 통해 장차 정부 차원에서 기업의 정보보호와 관련한 정책을 수립할 때 어떠한 분야의 법·제도 및 지원을 강화해야 할지에 대한 시사점을 도출하고자 하였다.

그 결과 독립변수인 정보보호 체계가 정보보호 교육과 정보보호 점검 활동에 미치는 영향력의 양상은 각기 다르게 나타났지만, 독립변수로 선정한 정보보호 정책, 개인정보보호 정책, 정보보호 조직, 정보보호 인력(정보보호 관리자 인력 및 담당 인력) 및 정보보호 예산 등 대부분의 하위 변수가 종속변수에 정(+)의 영향력을 행사함을 알 수 있었다.[14] 그리고 이때 다른 변수에 비해 정보보호 관리자 인력이 정보보호 활동에 미치는 영향력이 상대적으로 큰 것으로 드러났다.

이와 같은 결과에 근거하여, 정부는 기업 정보보호 관련 정책을 수립함에 있어 특히 정보보호 관리자 인력의 임명 및 활용과 관련한 규정을 강화하는 데에 보다 더 많은 자원을 투입할 수 있을 것이다.

이에서 더 나아가, 점차 정보보호 대책 활동에서 인적 자원 관리의 중요성이 높아지고 있음에도 김동우 외(2013), 박준경 외(2011) 등에서 지적되고 있는 것과 같이 국내에서는 정보보호 교육·훈련 체계가 미비한 것이 실정이다.

따라서 정부는 범국가적 차원에서 정보보호 교육 체계를 마련하여 정보보호 인력을 양성하기 위한 투자를 확대해나가야 할 것이다. 일례로 미국은 높아지는 정보 침해 위협에 대응하기 위해 2009년부터 국가 차원에서 정보보호 교육과 관련한 종합적인 대책을 수립 및 시행하고 있다(김동우 외, 2013). 우리나라에서도 이와 같은 조치를 통해 장차 정보보호 관리자 및 전문가로 성장할 인력을 적극적으로 양성하여야 한다.

한편 정보보호 점검 활동은 기업 차원에서 투자로 받아들여지기보다는

14) <연구가설 1>의 검증 결과, 정보보호 정책이 정보보호 교육에 미치는 영향력은 통계적으로 확인되지 않았다.

비용으로 인식되고 있으며, 특히 중소기업의 경우 보안 점검 등 정보보호를 위한 조치를 행함에 있어 보다 적절한 평가를 받지 못하고 있다(한국정보방송통신대연합, 2015).

보안 점검은 정보 침해 사고의 예방 및 사후 보완을 위한 조치로서의 성격을 지니며, 그 프로세스가 체계적으로 구성 및 운영되어야 한다. 그러나 이근호(2014) 등에 의하면, 현재의 보안 점검과 관련한 정부의 규정 및 평가체계는 소요되는 비용과 정책 효과의 측면에서 충분한 실효성을 갖추고 있지 못하다.

따라서 정부는 기존의 보안 점검과 관련한 규정 및 평가체계를 개선하고, 보안 점검 활동의 사각지대에 놓여 있는 중소기업 등을 대상으로 보다 활발한 홍보 및 평가 활동을 진행해야 할 것이다.

마지막으로 이 논문은 기업의 규모·업종을 통제변수로 투입하여 살펴보았는데 그 결과, 기업의 규모가 클수록, 업종의 경우 금융 및 보험업에서 상대적으로 정보보호 활동 수준이 높게 나타나는 것을 알 수 있었다. 김진형 외(2012) 등에서도 기업의 규모·업종의 차이에 근거한 보다 세부적인 정보보호 규정이 없음이 지적된 바, 정부는 규모·업종에 따라 발생하는 정보보호 수준의 편차를 개선하기 위한 노력을 기울여야 할 것이다.

그러나 이 논문은 이와 같은 정책적 시사점을 내포하고 있음에도 불구하고, 다음과 한계점 또한 지니고 있다.

먼저 방법론적 측면에서 역인과성(reverse causality)의 문제를 지적할 수 있다. 독립변수로 채택한 정보보호 체계는 정책, 조직, 인력, 예산 등의 하위 변수로 구성되며, 이는 종속변수로 선정한 정보보호 교육 및 점검 활동과 양방의 인과관계를 가질 수 있다.

또한 연구 자료가 된 설문에서는 기업의 CEO 및 임원, 일반직원의 정보보호 인식 또한 조사되었는데, 이 논문에서는 해당 자료를 활용하지 않았다.

기업의 정보보호 수준을 제고하는 과정에서 기업 구성원의 정보보호 인식이 중요하다는 주장은 임채호(2006) 등을 통해 제기되어 왔다. 김지

수 외(2012)도 정보보호최고책임자(CISO)의 역할 인식이 정보보호 대책 활동에 정(+)의 영향을 미친다는 사실을 입증하였다.

그러나 본 연구에서는 정보보호와 관련한 중요한 요인인 정보보호 인식이 다루어지지 않았으며, 체계에 포함되는 인적 요인으로서는 정보보호 관련 인력의 임명 여부 및 비중만이 고려되었다.

향후 연구들에서는 이러한 한계점이 극복되어, 기업의 정보보호 수준과 직결되는 정보보호 교육·훈련 및 정보보호 점검 활동에 관한 연구가 보다 활발히 진행되었으면 하는 바람이다.

참 고 문 헌

국민일보. (2016.10.22.). '카드3사 정보유출 손해배상 소송' 피해자 승소.
http://news.kmib.co.kr/article/view.asp?arcid=0011016396&code=61141311&sid1=eco

김건우·김정덕. (2016). 정보보호 교육에 대한 연구 동향 분석. 정보보호학회논문지, 26(2): 489-499.

김동우·채승완·류재철. (2013). 국내 정보보호 교육체계 연구. 정보보호학회논문지, 23(3): 549-559.

김민정·장세정·유진호. (2014). 중소기업의 개인정보보호 제도에 대한 이해가 개인정보보호 대책 활동에 미치는 영향 분석. 중소기업연구, 36(2): 227-240.

김용겸·최우승. (2009). 정보교육 및 실무활용을 위한 정보보호 관련 지식 및 기술에 대한 분류체계 연구. 상업교육연구, 23(3): 123-140.

김지수·김종배·신용태. (2012). 조직내 정보보호최고책임자(CISO)의 역할인식이 정보보호성과에 미치는 영향에 관한 연구. 경영컨설팅연구, 12(4): 21-34.

김진형·김형종. (2012). 기업의 규모와 특성을 고려한 개인정보보호 방안 연구. 보안공학연구논문지, 9(1): 77-85.

김환국·고규만·이재일. (2013). 정보통신망법 개정에 따른 기업 정보보호 제도 현황 및 정보보호 관리체계의 인증기준 비교. 정보보호학회지, 23(4): 53-58.

나윤지·조영석·고일석. (2006). 기업의 정보보호 수준 평가를 위한 평가지표. 융합보안논문지, 6(3): 135-144.

남길현. (2011). 국내외 개인정보보호법 동향과 기업의 대응전략. 정보보호학회지, 21(8): 60-69.

문현정. (2009). 우리나라 중소기업의 정보 보호 역량 강화를 위한 교

육 훈련 현황과 문제점. 정보보호학회지, 19(1): 29-39.
박재영. (2012). 정보보안 전문인력 양성을 위한 교육과정 분석. 경영정보연구, 31(1): 149-165.
박종일. (2013). 기업의 무선 환경 도입에 따른 정보보호정책 변화 방안. 한국정보보호학회지, 23(2): 43-47.
박준경·김범수·조성우. (2011). 기업정보보호 활동을 위한 조직 구성원들의 태도와 주요 영향 요인. 경영학연구, 40(4): 955-985.
송정석·전민준·최명길. (2011). 공공기관 정보보호 거버넌스 수준에 영향을 미치는 요인에 관한 연구. 한국전자거래학회지, 16(1): 133-151.
오창규·김종기. (2003). 효과적인 정보보호 교육 및 훈련을 위한 프레임워크 개발. 정보보호학회지, 13(2): 59-69.
이근호. (2014). 정보시스템의 정보보호를 위한 사전점검에 관한 연구. 디지털융복합연구, 12(2): 513-518.
임채호. (2006). 효과적인 정보보호인식제고 방안. 정보보호학회지, 16(2): 30-36.
임헌정·정태명. (2010). 정보보호 교육을 위한 정량적 분석 및 방법론 도출. 한국통신학회 학술대회논문집, 406-407.
장상수. (2014). 균형성과표(BSC) 기반의 정보보호 성과 지표 개발 및 측정 방법에 관한 연구. 융합보안논문지, 14(4): 41-53.
장상수·노봉남·이상준. (2012). 정보보호 관리체계의 지속적인 정보보호 관리과정(PDCA)이 정보보호 성과에 미치는 영향에 관한 실증 연구. 정보보호학회논문지, 22(5): 1123-1132.
조선 비즈. (2017.2.17.). 법원 “롯데카드 개인정보유출 피해자 3577명에 10만원씩 지급하라”. http://biz.chosun.com/site/data/html_dir/2017/02/17/2017021701092.html
조선일보. (2016.9.23.). 야후, 2014년 말 해킹 공격 5억명 개인정보 유출…사상 최대 피해.

http://news.chosun.com/site/data/html_dir/2016/09/23/2016092300598.html
컴퓨터월드. (2016.3.1.). 정보보호 사각지대, '중소기업'이 위험하다. http://www.comworld.co.kr/news/articleView.html?idxno=48952
한국인터넷진흥원. (2015). 2015년 정보보호실태조사(기업부문).
한국인터넷진흥원. (2016). 2016년 정보보호실태조사(기업부문).
한국정보방송통신대연합. (2015). 정보보호 준비도 평가.
한국정보보호진흥원. (2008). EU의 정보보호 인식제고 정책 현황 및 시사점.

Abstract

A Study on Corporate Information Protection Activities

— Focusing on the Information Protection System —

Kim, Yongjae
Master of Public Policy
Department of Public Administration
Graduate School of Public Administration
Seoul National University

Due to the development of ICT(Information and Communications Technology) and the widespread use of the Internet, corporations of all industries are now capable of making business processes more efficient and reducing costs. But at the same time, they are exposed to more intelligent and massive cyber attacks.

In order to cope with cyber attacks, the Korean government has endeavored to provide legal and institutional measures for corporate information protection. For example, the government introduced Personal Information Protection Act in 2011. However, there still is a lack of more detailed regulations which takes into account individual characteristics of companies such as size and type of business.

In addition, the importance of information protection education and information protection check as means for corporate information protection has been repeatedly emphasized. But still there are few precedent studies regarding these issues.

Information protection education and information protection check are directly related to the level of corporate information protection. So in this paper, 'information protection activities', which can be subdivided into 'information protection education' and 'information protection check', was defined as a dependent variable. Then, by identifying the factors influencing information protection activities, this paper aims to suggest the direction of the corporate information protection policies.

'Information protection system', which is an input of companies, was selected as an independent variable affecting information protection activities. In this research, it is assumed that information protection system is composed of 'information protection policy', 'privacy policy', 'information protection organization', 'information protection manager', 'information protection officer', 'information protection budget'.

For statistical verification, the raw data of '2016 Information Protection Survey for Enterprises' was utilized. It was conducted by 'Korea Internet and protection Agency(KISA)' and the total number of samples was 9,586.

As a result of multiple regression analysis, first of all, it was verified that all variables except for information protection policy had positive effect on the level of information protection education. That is, privacy policy, information protection organization, information protection manager, information protection officer, information protection budget had positive effect on information protection

education.

Secondly, all variables—information protection policy, privacy policy, information protection organization, information protection manager, information protection officer, information protection budget— had positive effect on information protection check.

Based on the results, It can be inferred that the government can raise the level of corporate information protection by reinforcing regulations regarding information protection system.

Finally, as for control variables, it was verified that the larger the size of the company, the higher the level of information protection activities. Also, is was found that the level of information protection activities was relatively high in financial and insurance industries compared to other industries.

Therefore, the government should also strive to improve the level of information protection which varies according to the size and the type of business.

Keywords: information protection, personal information protection, information protection system, information protection education, information protection check

Student Number: 2015-24509